European Commission

Cross-border Digital Criminal Justice

Final Report

Deloitte
June – *2020*

Deloitte.

Justice

and Consumers

EUROPEAN COMMISSION

Directorate-General for Justice and Consumers
Directorate B — Criminal justice
Unit B.1 — General criminal law and judicial training

Contact: Dick HEIMANS

E-mail: *eu-digital-criminal-justice@ec.europa.eu*

European Commission
B-1049 Brussels

Cross-border Digital Criminal Justice

Final Report

Directorate-General for Justice and Consumers

The European Commission is not liable for any consequence stemming from the reuse of this publication.

Luxembourg: Publications Office of the European Union, 2020

PDF ISBN 978-92-76-20890-7 doi:10.2838/118529 DS-04-20-443-EN-N

Directorate-General for Justice and Consumers

Document Control Information

Setting	Value
Document Title	Final Report
Project Title	Cross-Border Digital Criminal Justice
Document Author	Deloitte
Project Owner	DG JUST
Solution provider	Deloitte
Chef de File	Dick Heimans (DG JUST)
Project Officer	Tomasz Debski (DG JUST)
Contractor Project Manager	Éva Kamarás
Doc. Version	5.4
Sensitivity	Medium
Date	04/06/2020

Document Approver(s) and Reviewer(s)

Name	Role	Action	Date
Tomasz Debski (combined review of the European Commission services)	Project Manager	Review	Several review iterations, last feedback received on: 04/06/2020
Dick Heimans Tomasz Debski	Chef de File Project Manager	Review	Several review iterations, last feedback received on: 23/04/2020
Hans Verheggen	Contractor Engagement Partner	Review	06/03/2020
Wesley Bille	Contractor Project Director – Technical Leader	Review	05/03/2020
Wesley Bille	Contractor Project Director – Technical Leader	Review	26/02/2020
Éva Kamarás	Contractor Project Manager	Review	25/02/2020

Document history

The Document Author is authorised to make the following types of changes to the document without requiring that the document be re-approved:

- Editorial, formatting, and spelling
- Clarification

To request a change to this document, contact the Document Author or Owner.

Changes to this document are summarised in the following table in reverse chronological order (latest version first).

Revision	Version	Date	Created by	Short description of changes
05	5.4	04/06/2020	Deloitte	Final version, following the review by different stakeholders
04	5.1	29/05/2020	Deloitte	Draft final version, following the review by different stakeholders
03	4.0	30/04/2020	Deloitte	Updated draft of the report submitted for review to DG JUST
02	3.0	06/03/2020	Deloitte	First draft of the report submitted for review to DG JUST
01	2.0	28/02/2020	Deloitte	Preliminary draft of the report submitted for review to DG JUST

Executive summary

The upgrade and modernisation of judicial cooperation and information exchange in criminal cases across the EU are crucial in light of the evolving security threat landscape and the fast pace of technological development, as acknowledged by the European Council in its Conclusions of October 2018.[1] This need for immediate reaction and change has been further reinforced by the recent COVID-19 crisis and its impact on judicial cooperation in criminal matters. Many of the negative consequences of the crisis could have been avoided by having appropriate digital tools available.

Following the October 2018 Conclusions, Eurojust called to create 'Cross-Border Digital Criminal Justice', a fast, reliable and secure IT infrastructure that would enable national prosecution authorities to interact with their counterparts, JHA agencies and EU bodies in the Justice and Home Affairs (JHA) area.[2] Following the December 2018 Justice and Home Affairs Council Conclusions[3], the European Commission launched the Digital Criminal Justice project. The objective of this project is to shape a vision to design and implement a host of digital measures for the cross-border cooperation in criminal matters.

This study is the first element of the Digital Criminal Justice project.

Based on an online survey, country visits with national prosecutors and investigative judges as well as central authorities and stakeholder interviews with the Commission services, Joint Investigation Teams (JIT) members, the European Judicial Network (EJN) in criminal matters, JHA agencies (Eurojust, Europol, Frontex) and EU bodies (OLAF, the EPPO), as well as an Expert Group meeting with national representatives, the study team identified the needs and challenges to communicate and exchange case-related data in a digital and secure way when cooperating in cross-border cases.

Particularly, seven broad categories of business needs were identified via the data collection activities mentioned above.

First, it was found that stakeholders participating in judicial criminal cross-border cooperation need to securely communicate and exchange information via digital means. This requires solutions to allow stakeholders to communicate in a secure way, including sending and receiving sensitive and confidential data.

Second, interoperability across different systems needs to be ensured. Stakeholders at national and EU level are using their own tools, which were developed without necessarily taking into account other tools and systems. This interoperability is required in order to allow efficient and seamless communication.

Third, stakeholders need to easily manage the data and ensure its quality. This implies that the data exchanges should meet quality standards (e.g. the data is exchanged in a structured way),

[1] European Council meeting (18 October 2018), EUCO 13/18, https://www.consilium.europa.eu/media/36775/18-euco-final-conclusions-en.pdf
[2] Eurojust's paper: Towards Digital Criminal Justice in the EU, 14345/18, 15 November 2018, http://data.consilium.europa.eu/doc/document/ST-14345-2018-INIT/en/pdf
[3] See: https://www.consilium.europa.eu/media/37402/st15252-en18.pdf

allowing the stakeholders to properly make use of it (e.g. use the data as evidence in a given case).

Four, stakeholders investigating a given case should be able to identify links between cross-border cases. Therefore, solutions are needed to allow the stakeholder to search and find relevant information they need for the case they are handling.

Five, data protection principles need to be respected for all systems. Therefore, the data protection by design and by default approach should be a guiding principle when developing and implementing tools to be used in judicial criminal cross-border cooperation.

Six, the process of setting up and operating a JIT should be simplified. A specific tool is needed to support stakeholders in the different processes related to JITs.

Lastly, access to the necessary digital tools should be ensured. Stakeholders need to have access to a wide range of tools, such as training materials and a translation engine, allowing smooth and efficient cooperation.

The study presents seven solutions to address the above business needs categories and to implement the Digital Criminal Justice concept:

- Secure Communication Channel
- Communication Tool
- Redesigned Eurojust Case Management System
- The JIT Collaboration Platform
- Exchange of data between the JHA agencies and EU bodies
- Judicial Cases Cross-Check
- Large Files Solution

The table below provides an overview of these solutions, which are subsequently described in more detail.

Table 1: Solutions overview

Solution	Option	Legal base (and relevant funding prescriptions)	Stakeholders involved (development, hosting, and connection to the solution)	Existing solution?	Nature of the solution
Secure Communication Channel	eDelivery (with e-CODEX connector) over the TESTA Eurodomain	N/a	Development: not necessary (solution already existing) Users: Member States and JHA agencies and EU bodies	Yes, existing solution to be re-used	Technical solution
	eDelivery (with e-CODEX connector) over the internet	N/a	Development: not necessary (solution already existing) Users (connection): Member States and JHA agencies and EU bodies	Yes, existing solution to be re-used	Technical solution
	eDelivery (with another connector) over the internet	N/a	Development: not necessary (solution already existing) Users (connection): Member States and JHA agencies and EU bodies	Yes, existing solution to be re-used	Technical solution
	eDelivery (with another connector) over the TESTA EuroDomain	N/a	Development: not necessary (solution already existing) Users (connection): Member States and JHA agencies and EU bodies	Yes, existing solution to be re-used	Technical solution
	TESTA (Eurodomain or another dedicated domain)	N/a	Development: not necessary (solution already existing) Users (connection): Member States and JHA agencies and EU bodies	Yes, existing solution to be re-used	Technical solution

Solution	Option	Legal base (and relevant funding prescriptions)	Stakeholders involved (development, hosting, and connection to the solution)	Existing solution?	Nature of the solution
	SIENA	N/a	Development: not necessary (solution already existing) Users (connection): Member States and JHA agencies and EU bodies	Yes, existing solution to be re-used	Technical solution
Communication Tool	Evolution of e-EDES	Possible new legal basis to cover the evolution of the e-EDEs platform (if necessary), and amendment of eu-LISA Regulation (if this item is hosted by eu-LISA)	Development: European Commission or eu-LISA Hosting: eu-LISA Users: Member States and JHA agencies and EU bodies	Yes	Technical solution
Redesigned Eurojust CMS (incl. Eurojust integration layer)	Redesigned Eurojust CMS (COTS product)	Eurojust Regulation	Development and hosting: Eurojust Users: Eurojust and Member States	Yes	Technical solution
JIT Collaboration Platform	JIT Collaboration Platform (COTS product)	Adoption of a new legal basis, and amendment of eu-LISA Regulation (if this item is hosted by eu-LISA)	Development: eu-LISA Hosting: eu-LISA Users (connection): Member States and JHA agencies and EU bodies.	No	Technical solution
Exchange of data between the JHA agencies and EU bodies	Hit/no-hit Task Force	Current legal bases of the JHA agencies and EU bodies (Eurojust, Europol, Frontex, the EPPO and OLAF)	The Commission, JHA agencies and EU bodies would be part of the Task Force, and Member States can partake in as observers.	No	Task Force
Judicial Cases Cross-Check	Centralised repository of metadata	Adoption of a new legal basis, and amendment of eu-LISA Regulation (if this item is hosted	Development: eu-LISA Hosting: eu-LISA (possibly) Users (connection): Member States, Eurojust, the EPPO	No	Technical solution

Solution	Option	Legal base (and relevant funding prescriptions)	Stakeholders involved (development, hosting, and connection to the solution)	Existing solution?	Nature of the solution
		by eu-LISA)			
	Decentralised	Adoption of a new legal basis (if necessary)	Development: Member States Hosting: Member States	No[4]	Technical solution
Large Files Solution	Centralised	New regulation needed, and amendment of eu-LISA Regulation (if this item is hosted by eu-LISA)	Development: eu-LISA Hosting: eu-LISA Users (connection): Member States and JHA agencies and EU bodies	No[5]	Technical solution
	Decentralised	Legal basis at national level	Development: European Commission Hosting: Member States Users (connection): Member States and JHA agencies and EU bodies	No	Technical solution

[4] The solution is however inspired by the EPRIS-ADEP project.

[5] Although there is no solution currently existing, this option is inspired by the Large File Exchange (LFE) system developed by Europol.

Following this overview, a more detailed description on each solution is provided below.

1. Secure Communication Channel

This solution refers to an underlying secure communication channel to allow for the exchange of messages, information and evidence electronically across borders in a secure way. The report presents the assessment of different implementation options for a secure communication channel: eDelivery (with e-CODEX connector, or with another connector) over the internet, eDelivery (with e-CODEX connector, or with another connector) over TESTA EuroDomain, TESTA (EuroDomain or dedicated domain) and SIENA. Based on the technical and security assessments conducted, it can be concluded that there are different communication channels that can be used for the different stakeholders and types of exchanges of information in the context of Cross-Border Digital Criminal Justice.

The re-use of eDelivery (with e-CODEX connector) over the TESTA EuroDomain is preferred for communication between Member States, and Member States and JHA agencies and EU bodies for the exchange of non-classified information. On the other hand, the exchange of EU classified information between Member States, and Member States and JHA agencies and EU bodies requires an end to end accreditation. The preferred option here is the re-use of eDelivery (with the e-CODEX connector) over the TESTA EuroDomain.

For hit/no-hit and the exchange of unclassified and EU classified data between JHA agencies and EU bodies, the same recommendations and remarks are applicable on the whole. However, certain specific exchanges of information between JHA agencies and EU bodies (notably for SIS II, VIS and ECRIS-TCN in the future), require the use of SIS/VIS communication channels (a dedicated domain managed by eu-LISA) to do hit/no-hit searches.

In terms of legal and data protection implications, it was found that there are no specific legal barriers preventing the use of any of the options considered. There are no legal amendments, nor specific new legal instruments, required to allow the use of the options presented. Regardless of the option retained, the communication channel should allow for the logging of all communication activities and provide a thorough audit trail in order to be compliant with data protection requirements.

2. Communication Tool

A communication tool to enable the secure electronic exchange of judicial cooperation requests and mutual recognition/mutual legal assistance forms, information, messages and evidence is required. For this solution, the report envisages different scenarios, being: purchasing a commercial off-the-shelf product, creating a custom-built tool, re-using the SIENA application, or re-using the e-Evidence Digital Exchange System (e-EDES).

Based on a preliminary analysis, the report recommends e-EDES as the preferred option to implement the Communication Tool for Cross-Border Digital Criminal Justice. The tool is tailored to the needs of the European criminal justice community: indeed, e-EDES and the underlying digital infrastructure on which it is based, e-CODEX (and e-Delivery), were built by and for the justice community. Besides this, it is based on common open standards/specifications and open source implementations (i.e. e-CODEX connector and the Domibus Gateway). Lastly, e-EDES will be available to all Member States in 2020.

As previously mentioned, the future evolution of e-EDES would be based on the same technical solution as the one currently being developed by the European Commission. The technical assessment of this solution, however, indicates that additional integration and/or developments would need to be added in order to implement all envisaged functionalities.

In terms of security, this report concludes that e-EDES fulfils the security objectives at the transport layer. For the application layer, an additional risk assessment should be performed in order to identify potential risks at that level.

As for the legal basis, it should be noted that while a specific legal basis is not necessary for the e-EDES platform to operate, the enactment of a legal basis would be useful to strengthen and reinforce the platform, which would become the Communication Tool. Besides this, an amendment to the eu-LISA Regulation might be necessary if the agency is mandated (by a legal basis for the e-EDES platform) with the hosting of the solution.

From a data protection perspective it should be investigated to which extent the platform's functionalities should be further developed to ensure that applicable data protection principles and procedures can effectively be taken into account.

3. Redesigned Eurojust Case Management System

Redesign of the Eurojust Case Management System (CMS) would allow its proper functioning and ensure it addresses the needs of its users. The Redesigned Eurojust CMS would be composed of the following components: the Core CMS, the Counter-Terrorism Register, the JIT Admin Portal, the Action Day Collaboration Platform and an Integration Layer.

The technical assessment considers several vendor solutions for each of the components. For the Core CMS, the report explains that Case@EC is the system in place for several entities within the European environment. Nevertheless, it should be noted that using a custom built system may entail a risk as it may not follow the latest technological trends and evolutions, which might impact how future-proof it will remain. The assessment takes into account two other vendor solutions that might fit the current high-level requirements for the Eurojust Core CMS. This report recommends to conduct a more in-depth assessment in order to select the most appropriate solution, based on the elements discussed.

The security assessment explains the security capabilities, considerations and features that are relevant for each of the components, and which should be translated to security requirements and controls, at the design and implementation phase of the target architecture.

In terms of legal basis, the revamp of the Eurojust CMS can be conducted based on the current legal framework, which is the Eurojust Regulation.

The data protection assessment highlights the legal framework the Redesigned Eurojust CMS should comply with. This refers to the applicable provisions from the Eurojust Regulation and Regulation 2018/1725, and more specifically the following principles: lawfulness and fairness, purpose limitation, quality and accuracy of personal data, data minimisation, data protection by design and by default, special categories of operational data, storage limitation, integrity and confidentiality, accountability, data subject requests and automated individual decision-making (including profiling).

4. The JIT Collaboration Platform

A JIT Collaboration Platform to set up, plan and coordinate JIT operations, allowing easy communication, as well as the electronic sharing of large amounts of information and evidence between JIT partners.

The technical assessment describes three possible scenarios for the implementation of this solution: re-use of OLAF's VOCU tool, off the shelf products (Wire, Zimbra, eXo, Microsoft Teams, Cisco WeBex Teams) and implementation from scratch. Based on the assessment, this report recommends to re-use a COTS product for the implementation of this solution. However, none of the vendor solutions presented can cover all the requirements for the future JIT Collaboration Platform. Therefore, the report concludes that the final solution should consist of a combination of products used together.

The security assessment highlights the need to ensure the confidentiality of data being exchanged by the stakeholders using this solution. Strong encryption algorithms should be used to encrypt data, as a minimum in the transport layer. Besides this, the solution should also establish patch and vulnerability management processes, and should be integrated with the target architecture. Concerning the three scenarios, the security assessment concludes that a business impact assessment as well as a risk assessment should be carried out before pursuing design choices.

The legal and data protection assessment explains that a legal basis would be necessary, in order to provide a clear framework (including on some sensitive points such as data controllership) on the use of this tool. Besides this, the JITs model agreement should also be adjusted in order to be aligned with the new legal basis. Moreover, in case eu-LISA is confirmed as the hosting entity, its establishing Regulation must be amended accordingly.

5. Exchange of data between the JHA agencies & EU bodies

The JHA agencies and EU bodies (Eurojust, Europol, Frontex, the EPPO and OLAF) should allow the exchange of information between them (but also with EU systems, i.e. SIS II and ECRIS-TCN for both Eurojust and Europol, and the EPPO for the latter), including on the basis of a hit/no-hit system. As the legal bases concerned do not provide technical specifications on the concept of the hit/no-hit access, nor on the exchange of information following a hit, this report suggests setting up a Task Force to discuss and implement these specifications.

This Task Force would be composed of the JHA agencies and EU bodies mentioned above, together with the Member States as observers. The Task Force would be in charge of further examining and defining the hit/no-hit concept, which can be done either manually, i.e. triggered by users, or as an automatic cross-checking of the databases. Besides this, the Task Force should take into account the measures and requirements to ensure the hit/no-hit system and the subsequent exchange of information is compliant with the data protection principles and requirements.

6. Judicial Cases Cross-Check

A Judicial Cases Cross-Check facility to be able to search for case-related information and identify links among cases that are being investigated in other Member States or by JHA agencies and EU bodies. Two solutions are considered for its implementation: a decentralised, and a central repository of metadata (either with hit/no-hit or blind search).

Based on the technical assessment, it was found that the main differences between the options concern the hosting, the governance of the solution, as well as the storage of data. Both scenarios present some disadvantages. The centralised option entails a risk of being a single point of failure, which therefore requires additional measures to be deployed, while the decentralised one would be more complex to implement (data index to be determined by Member States and the availability of the data; the different national IT landscapes would also affect the implementation of the solution). Therefore, a clear recommendation of the option to be retained from a technical perspective cannot be provided at this stage.

From a security perspective, both options can reach an acceptable security level. Therefore, a further risk analysis and business impact assessment would have to be conducted in order to decide which option to retain.

As for the legal assessment, the two options (decentralised and centralised) are legally possible. The centralised scenario would require the enactment of a new legal basis, and an amendment to an existing legal instrument (i.e. eu-LISA Regulation – if the agency is designated as the hosting entity). The decentralised scenario would not necessarily require a legal basis at EU level. However, an EU level legal instrument could be considered to ensure that all Member States provide for access to their local storage of metadata, and to define common elements on the control of that access, including the purposes for which such access would be allowed and any other necessary safeguards.

As for the data protection consideration, the processing of personal data by means of cross-checking index databases via a Judicial Cases Cross-Check is deemed lawful. The solution needs to be built based on the data protection by design and by default principle.

7. Large Files Solution

A Large Files Solution to overcome the limited attachment sizes authorised by current communication facilities and exchange large amounts of information electronically. Two options for the implementation are presented: a centralised, and a decentralised one.

From a technical perspective, the main differences between the two implementation options of the Large Files Solution concern the hosting, governance of the solution and the storage of data. Besides this, the central option presents a disadvantage in comparison to the decentralised option since it presents the risk of being a single point of failure. However, the decentralised option would require more efforts for its implementation, and would be more complicated to govern. Therefore, a recommendation on the solution to retain cannot be provided from a technical perspective at this stage.

In terms of security, it can be concluded that both proposed options could ensure an acceptable security assurance level for the target architecture. Therefore, a further risk analysis should be conducted in order to identify the best solution for the Large Files Solution.

The legal assessment concludes that the central option would require a new legal basis to duly regulate it. Besides this, the eu-LISA Regulation would also need to be amended to specify the agency's responsibilities in terms of hosting and maintenance of the solution. On the contrary, if the option retained is the decentralised one, a legal basis would be required at national level only.

As for data protection measures, the solution, regardless of the option implemented, should ensure the purpose limitation principle, data minimisation, data accuracy, storage limitation, confidentiality, integrity, availability and privacy.

The report also presents an estimation of the Total Cost of Ownership (over 5 years) associated with the implementation of the solutions proposed in this report. The Total Cost of Ownership is composed of build costs (i.e. one-off investment costs, such as costs for technical specifications, implementation, testing, data migration (where required), practical adoption), and operation & maintenance costs (i.e. recurring costs for the operation of the system, such as costs for maintenance, operation etc.). Besides this, the costs are broken down into owner (i.e. institution or entity that would be responsible for hosting and managing the solution) and users (i.e. any institution or entity making use of the solution in its daily job) costs. Under a certain number of assumptions, the Total Cost of Ownership of all solutions over five years is approximately EUR 201 million. Besides the costs, the report also describes the different possible sources for funding. The report considers several EU programmes, being the Digital Europe Programme, the European Regional Development Fund, the Recovery and Resilience Facility and the Justice Programme, as well as the own budget of some of the JHA agencies (i.e. Eurojust and eu-LISA) which would be developing some of the solutions.

The report subsequently provides a roadmap for the implementation of the different solutions. Overall, two main categories are devised. First, the solutions that would be implemented in the short term (1-3 years), which are: the Secure Communication Channel, the Communication Tool, the Redesigned Eurojust CMS, the Judicial Cases Cross-Check (decentralised option), the Large Files Solution (decentralised option) and the exchange of data between the JHA agencies and EU bodies. Second, the medium term category for the solutions to be developed in the coming 3 to 5 years. This refers to the JIT Collaboration Platform, the Judicial Cases Cross-Check (centralised option) and the Large Files Solution (centralised option).

To ensure delivering on the roadmap this study suggests a governance structure. The Digital Criminal Justice Expert Group, composed of Member States representatives, the European Commission, and the JHA agencies and EU bodies would be mandated with the overarching strategic governance of the project. The Expert Group would be monitoring the development of each of the solutions, in order to ensure their coordinated and timely development.

Below the Expert Group, a strategic governance structure would be created. The entities at this level would be responsible to lead and supervise the solutions from a policy point of view. These entities would be either subgroups of the Expert Group (five subgroups would be in place for the following solutions: the Secure Communication Channel, the Communication Tool, the JIT Collaboration Platform, the Judicial Cases Cross-Check - centralised option, and the Large Files Solution - centralised option), or the European Commission itself (for the exchange of data between the JHA agencies and EU bodies).

After this strategic governance layer, the IT implementation would follow. This layer refers to the entities driving the IT implementation of the solutions. The entities would vary depending on the solution to be developed. The European Commission or eu-LISA would develop the Communication Tool; Eurojust would be in charge of the redesign of its CMS; eu-LISA would develop the JIT Collaboration Platform, the Judicial Cases Cross-Check (centralised) and the Large Files Solution (centralised); and the JHA agencies and EU bodies would implement the exchange of data between them. As for the decentralised options of the Judicial Cases Cross-Check and the Large Files Solution, the Member States would be in charge.

The last layer of the governance refers to the contributors to the IT implementation. This category includes the different future users of the solutions that should be involved and contribute to the development in order to ensure it is properly tailor to their needs.

1 Table of Content

2 Table of Figures

3 Table of Tables

1 Introduction

Cross-border crime is an increasingly dynamic and complex phenomenon, leveraging from the progressive elimination of physical controls at the internal borders of the European Union (EU), the opportunities brought by digital innovation and legislative loopholes, amongst other factors. In order to tackle it, the Treaty on the Functioning of the European Union (TFEU)[6] has set the legal basis (articles 82 to 86) for the development of the area of freedom, security and justice, including measures for judicial cooperation in criminal matters.

Member States have at their disposal not only legal instruments to facilitate their coordination regarding judicial cooperation in criminal matters in cross-border cases, such as the European Investigation Order and the European Arrest Warrant, but can also cooperate with and receive support from JHA agencies (Eurojust, Europol, Frontex) and EU bodies (OLAF [7], the EPPO) to tackle cross-border crime or make use of EJN in criminal matters.

However, **national prosecution authorities are not yet fully equipped with state-of-the-art technologies to efficiently cooperate in cross-border criminal matters**. Their national systems were designed without taking into account the need for information exchange with other Member States, or EU JHA agencies/bodies. Likewise, improvement opportunities at EU level are also noticeable, e.g.: Eurojust Case Management System (CMS) would benefit from enhanced automation and interoperability with other systems and databases.

The lack of appropriate tools in cross-border cooperation can raise significant risks, such as: shared information is incomplete, or not updated; time is lost; data may be transmitted in an unsecure way; links between cases are not identified; and conflicts of jurisdiction are not detected or solved on time. Prosecution authorities of the Member States need to be able to communicate promptly and efficiently between each other, as well as with relevant JHA agencies and EU bodies when involved to support investigation of serious cross-border crimes. Likewise, JHA agencies and EU bodies are called to cooperate, and thus require a communication channel to share relevant data seamlessly.

The recent COVID-19 crisis and its impact on judicial cooperation in criminal matters has endorsed the need for further digitalisation of justice and has increased the need for immediate reaction and change. Based on information provided by the Member States on the impact of the measures taken by governments to combat the spread of COVID-19 on judicial cooperation in criminal matters in the European Union (and Iceland and Norway), most of the experienced issues could be easily overcome by having available appropriate digital tools, thereby allowing most of the cooperation to continue as normal.

The overarching objective of this study is to adopt a comprehensive and holistic approach to determine the elements needed to further discuss, develop and implement the concept of Digital Criminal Justice in cross-border cases.

[6] Consolidated version of the Treaty of the Functioning of the European Union, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN

[7] OLAF is a Commission service acting as an independent investigative EU Body. It conducts administrative investigations into fraud, corruption and irregularities against the EU financial interests. It participates in JITs when invited by judicial authorities, in order to share its expertise, and cooperates with judicial and law enforcement authorities when carrying out its own investigations.

To achieve such objective, the study aims to:

- Analyse the current policy landscape within the Member States and at the EU level (status quo).
- Assess the business needs of the stakeholders (problem definition).
- Identify and examine in detail the most promising possible solutions.
- Prepare appropriate recommendations.

This document is the study's **Final Report**, and its main purpose is to present the complete assessment of the retained solutions for the implementation of Cross-border Digital Criminal Justice. Therefore this report contains the following sections:

- **Executive summary**: provides a summary of this report.
- **Chapter 1 – Introduction (this Chapter)**: describes the scope, purpose and objective of this document.
- **Chapter 2 – Methodology**: explains the methodology used in the study, and for this report.
- **Chapter 3 – Summary of the business needs**: displays the business needs identified for each stakeholder group and the user journey.
- **Chapter 4 – High-level considerations:** presents the data protection, security, interoperability and funding considerations.
- **Chapter 5 – Solutions**: provides the detailed assessment of the different solutions from a technical, security, legal and data protection, and as well as funding perspective.
- **Chapter 6 – Cost estimation**: presents the cost assessment for the solutions.
- **Chapter 7 – Recommendations**: provides the main recommendations of the study in terms of implementation roadmap, governance, possible legal amendments, architecture and technology choices, and as well as horizontal recommendations.

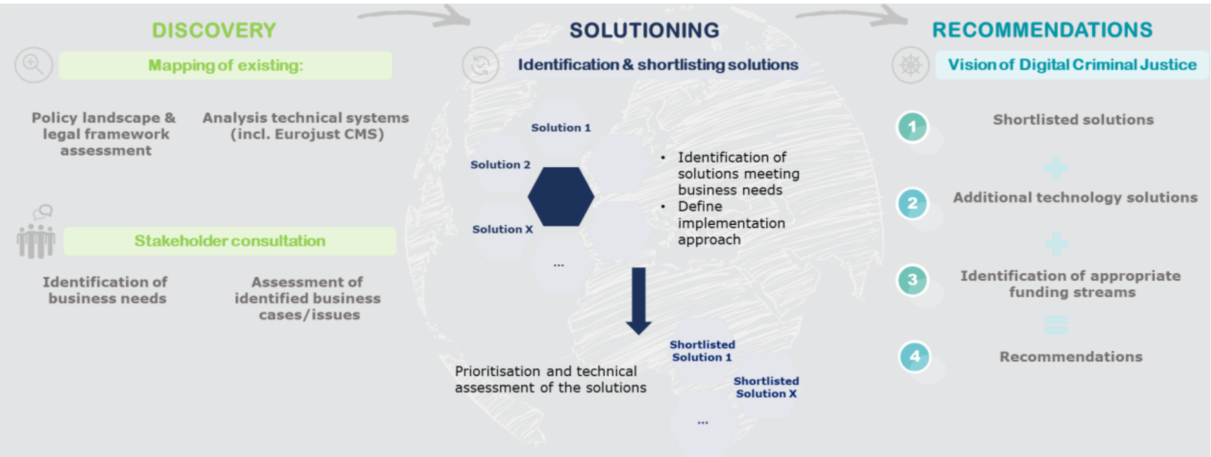
2 Methodology

This section outlines the methodology used throughout the study, as well as the different data collection activities carried out.

2.1 Study logic

As explained in the introduction section, the overarching objective of the study is to identify possible solutions that are needed to further discuss, develop and implement the concept of Digital Criminal Justice in cross-border cases. To achieve this purpose, the study is structured in three main phases: discovery, solutioning and recommendations as displayed in the figure below.

Figure 1: The study logic


DISCOVERY
Mapping of existing:
Policy landscape & legal framework assessment
Analysis technical systems (incl. Eurojust CMS)
Stakeholder consultation
Identification of business needs
Assessment of identified business cases/issues
SOLUTIONING
Identification & shortlisting solutions
Solution 1
Solution 2
Solution X
...
• Identification of solutions meeting business needs
• Define implementation approach
Prioritisation and technical assessment of the solutions
Shortlisted Solution 1
Shortlisted Solution X
...
RECOMMENDATIONS
Vision of Digital Criminal Justice
1
Shortlisted solutions
2
Additional technology solutions
3
Identification of appropriate funding streams
4
Recommendations

In the first phase, *Discovery*, the study team has conducted the following data collection activities:

- **Desk research** to conduct an in-depth analysis of the legal and policy environment around cross-border cooperation and interoperability in the area of criminal justice.
- **Strategic interviews** with the European Commission (DG HOME, DG JUST, DIGIT), JHA agencies (Eurojust, Europol, eu-LISA, Frontex), EU bodies (OLAF, the EPPO), JIT members, EJN in criminal matters and Eurojust national desks.
- **Online web-based survey** targeting respondents from at the time 28 Member States[8] (launched on 28 October and closed on 22 November) aimed to collect the business needs of the stakeholders as well as a first impression of the solutions preliminarily identified, which collected 238 replies.

During the second phase, *Solutioning*, the study team identified a wide range of possible solutions for the implementation of Digital Criminal Justice based on the previous phase's output and input collected during:

[8] At the moment the online survey was conducted, the United Kingdom was still a Member State of the European Union.

- **Field visits** in selected Member States (Croatia, Finland, Germany, the Netherlands and Romania), and phone interviews (France and Italy, as well as additional phone interviews with stakeholders from Finland and Germany).
- **Expert Group meeting** with representatives of the Member States, JHA agencies and EU bodies held in Brussels on 13-14 January 2020, during which the business needs were validated and the solutions discussed.

The Interim Report was prepared based on the findings of the field visits, and shared with the national representatives in view of the Expert Group meeting. The report included a detailed overview of the current situation, the business needs of the stakeholders involved in cross-border cases, and described the solutions for Digital Criminal Justice in terms of objectives and functionalities, as well as possible vendor solutions.

Lastly, in the third phase *Recommendations*, the study team has fine-tuned the solutions based on the Expert Group meeting findings and conducted an in-depth assessment from a technical, security, legal, data protection, and funding perspectives. For the latter, a specific data collection activity was conducted:

- **Funding interviews** with the European Commission (DG JUST, DG HOME and DIGIT) and Eurojust to identify possible funding sources for the development and implementation of the solutions.

The outcome of this analysis is this report at hand, which presents the findings of the overall study.

2.2 Limitations

In terms of challenges and limitations of the study, it must be noted that the qualitative replies gathered through the survey were not complete or detailed enough. Furthermore, under fieldwork, only one phone interview (with national authorities of each country) could take place for France and Italy, due to time constraints and the unavailability to schedule the interviews with a larger number of stakeholders. This challenge reduced the amount of insights that was possible to be collected from the national level. These challenges have thus limited the analysis feasible under this assignment. Nevertheless, the interviews conducted at EU and national level, as well as the Expert Group meeting, have served to counterbalance these challenges and gather more qualitative insights.

As for the cost estimation, due to the scarcity of data for some elements, appropriate assumptions were made to quantify the costs. The limitations faced in this exercise, as well as the mitigation measures, i.e. the assumptions, are explained in detail in section 6.1.

Additionally, the unexpected COVID-19 outbreak has impacted the duration of the study. Due to the challenging working conditions, it was agreed to extend the period for preparation of this report.

3 Summary of business needs

This section presents the business needs of the stakeholders involved in cross-border cases.

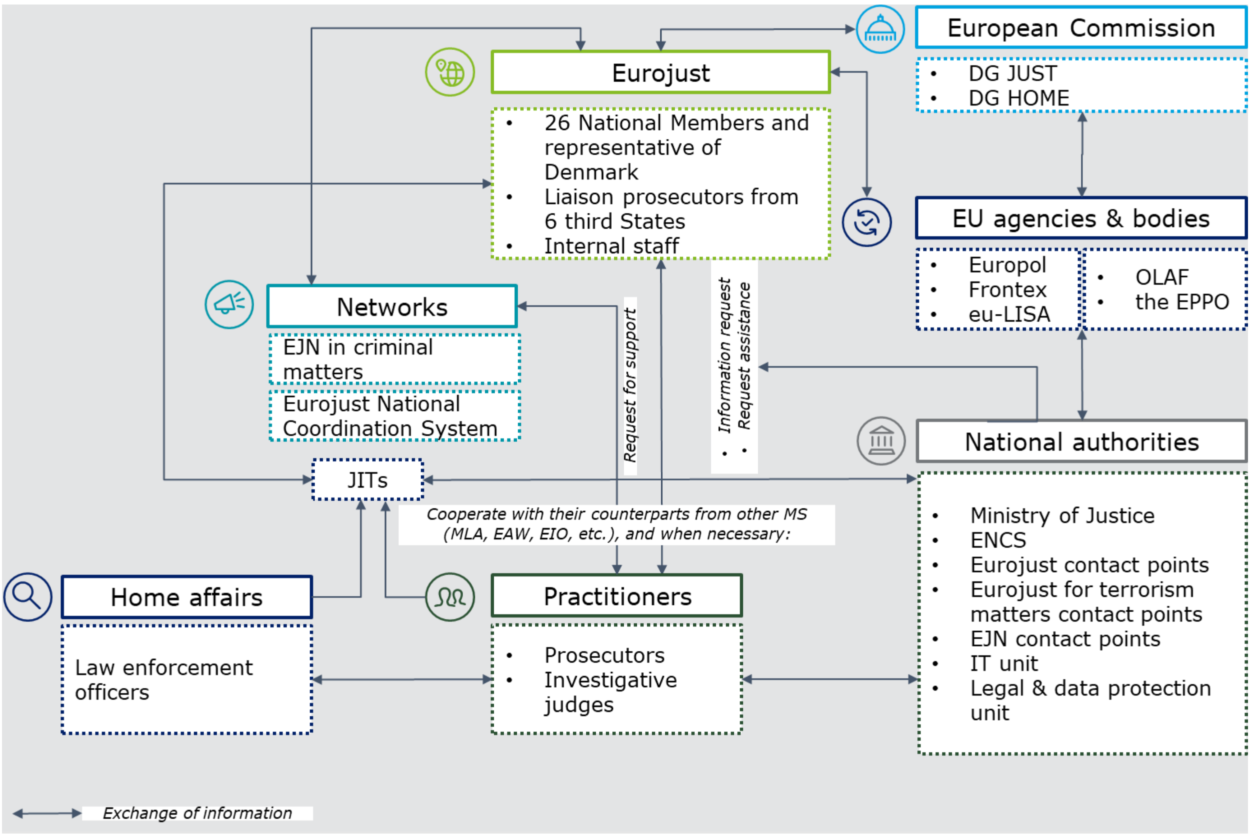
3.1 Business needs overview

The identification of the business needs is key step of the project to understand the problems and challenges faced by the stakeholders, and thus identify their needs, which should be addressed by possible new solutions. This section first presents an overview of the stakeholders involved (i.e. stakeholder mapping), and secondly, provides a detailed explanation of the business needs per each stakeholder group.

3.1.1 Stakeholder mapping

A wide range of stakeholders are involved in cross-border criminal justice. The figure below aims to provide an overview of the ecosystem in order to allow a better understanding of the interactions between the stakeholders.

Figure 2: Stakeholder mapping



3.1.2 Personas and business needs

This section provides, for the stakeholders involved in the practical handling of cross-border judicial cooperation in criminal cases, a description of their goals and tasks, as well as issues and constraints. These aspects, following the *design thinking methodology*[9], are presented aggregated to personas.[10] Based on the personas, and particularly the issues and constraints of each of them, the business needs were mapped. The business needs refer to the future situation, i.e. going beyond the as-is situation.

The personas identified as involved in cross-border judicial cooperation in criminal cases are:

- Prosecutors/Investigative Judges and Prosecutors General in Member States
- Ministries of Justice/National Authorities (incl. national correspondents for Eurojust, EJN in criminal matters and ENCS contact points)
- JIT members/participants[11]
- Eurojust
- Other JHA Agencies and EU bodies (incl. Europol Liaison Officers, the EPPO European Prosecutors and European Delegated Prosecutors, OLAF investigators, Frontex staff).

The development of personas was conducted based on validation by the project's owners, and was based on the data gathered during the study's different data collection activities.

[9] Design thinking is a methodology, which assesses the relevance and utility of an intervention/action by adopting the perspective and views of a "user persona".

[10] A persona is a realistic but fictional user, representing one segment/user group of a targeted audience.

[11] When OLAF or Europol are invited to take part in a JIT by the national judicial authorities (recital 3 of the Council Framework Decision 2002/465 of 13 June 2002 on joint investigation teams), they are legally not members but participants.

Table 2: Prosecutors / Investigative Judges persona

	Prosecutors / Investigative Judges
Goals & tasks	As a prosecutor (or an investigative judge), my main goal is to receive from other stakeholders information I need for my case. For that purpose, I use the legal instruments at my disposal. To achieve my goal, I perform the following tasks: *A.* *Exchange information* • I receive the information collected by law enforcement officers during their investigation. • I validate some forms to be issued by law enforcement officers or request validation of others by a judge. • I request law enforcement officers to issue some forms. • I request, receive but also provide information to other Member States in cross-border related cases. I also follow-up in the matter with them (via email or phone, but also I sometimes travel to the country in question). I appreciate meeting my counterparts face-to-face as it helps creating a trustful relationship between us. • I decide whether support from Eurojust is necessary in a given case, and if so, I send the relevant information. • I exchange information on a given case with Eurojust when the case I am involved in becomes a Eurojust case. • I sometimes request support from EJN in criminal matters (usually via email). • As a member/participant of/in a JIT, I exchange information with its other members (or sometimes only with a few due to the sensitivity of the data). *B.* *Authentication* • In order to prove the validity of my documents, I need to print them and sign them manually. *C.* *Record information* • I upload the information collected on my case to the national CMS (if any). *D.* *Translate information* • I request an official translation of the documents that I need to send to either other Member States or Eurojust.
Issues & constraints	In my daily work, I face the following issues and constraints: *A.* *Search information* • I do not have a single user friendly space to access all the tools I need to conduct my tasks (digital electronic forms, handbooks and guidelines) or to access different forums (e.g. EJN in criminal matters forum).

- I cannot access Eurojust CMS, therefore I cannot search for information related to my cases or even have a complete overview of them as well as a status of the different tasks to be performed.
- I do not have technical means to verify whether the crimes/suspects I am prosecuting have links in criminal proceedings in other countries. 50% of the respondents to the survey faced this issue to a great extent, and 29% to some extent.

B. *Communication channel*

- As I do not have a unique communication channel to communicate with all relevant stakeholders, the information on my case is exchanged between the different stakeholders (law enforcement, my counterparts in other Member States, Ministry of Justice, Eurojust, members of JITs) via different channels.
- I usually send confidential documents via post, as I do not have a technical solution allowing me to send or receive large data files in an electronic and secure way. If I want to share pictures, videos or voice records, I need to send electronic devices via post, as well due to the lack of technical means.
    - 29% of the respondents faced this difficulty (i.e. lack of secure communication channel) to a great extent, and 32% to some extent.
    - For 18% of the respondents the lack of technical means to exchange large amount of data with Eurojust and other JHA agencies and EU bodies is a difficulty to a great extent, and to some extent for 25% of them.
    - For 23% of the respondents the lack of technical means to exchange large amount of data with other countries is a difficulty to a great extent, and to some extent for 29% of them.

C. *Exchange of information*

- I have no information/tracking on the status of my cross-border cases.
- As several stakeholders are (most of the time) involved in cross-border cases, the information on the status of my request(s) is very scattered and fragmented.
- The stakeholders in the requested Member State do not notify me of the reception of my request(s).
- I do not receive notifications concerning the execution of my request(s) in other Member States. And when there is no response, I have no automated tool that would allow me to send reminders.
- I do not have digital means to exchange large amounts of data in a secure and trustworthy manner.
- I either lack digital tools to conduct my daily tasks and cooperate in cross-border cases, or my tools have been designed without taking into account the exchange of information with other parties (being Member States or JHA agencies and EU bodies), i.e. lack of interoperability.

D. *Procedures*

- I usually face delays (i.e. weeks, sometimes months) as well as late (and even lack of) responses to my requests. 7% of the prosecutors/investigative prosecutors who have replied to the survey face this issue to a great extent, and 74% of them to some extent.
- I also face long delays in receiving replies that relate to sending requests and evidence by post. 22% of respondents face this issue to a great extent, and 57% to some extent.
- The only efficient way I have to follow up on my request is via phone and email.

	• If I do not receive any response at all, I need to launch the procedure again. • Lack of clear overview on the organisation of other Member States: sometimes it is not very clear, who within the requested Member State is responsible for my request (this issue is faced to a great extent by 11% of the respondents to the survey, and to some extent by 44%). I thus need to follow up by calling, or requesting support from my central authority, EJN in criminal matters or Eurojust. Unfortunately, the Atlas of the EJN in criminal matters is not complete: it lists relevant authorities but not contact points within these authorities. *E.* *Translate information* • When receiving a document from another Member State, I sometimes need to wait for the official translation instead of starting working on it as soon as possible.

Table 3: Ministries of Justice/National Authorities persona

	Ministries of Justice/National Authorities
Goals & tasks	As the person responsible for coordinating investigations on cross-border cases, I have several hats, meaning that I may be in charge of working with people from Ministries of Justice/National Authorities in other countries on bilateral investigations, and/or of coordinating with the Eurojust National Desk of my country and other JHA agencies. In this capacity, I often also have the role of EJN in criminal matters and/or Eurojust National Coordination System (ENCS) contact point. To be able to carry out my duty, I execute the following tasks: • *Exchange information* • I exchange messages and case-related information about cases with prosecutors, courts or judges in my country. To do so, I either use a secure communication channel if there is one (i.e. secure emails, and/or a national case management system). If not, I use normal emails and phone calls. • I guide prosecutors to identify the relevant stakeholders in other Member States to reach out. • I exchange messages and information about cases with counterparts in Ministries of Justice/National authorities of other countries. To do so, I use email and phone calls. • I exchange messages and information about cases with the Eurojust National Desk of my country. To do so, I use a secure communication channel if there is one, or a normal email if not. I sometimes use my personal email, or mobile phone. • I must transfer documents (such as case-related information or requests) to counterparts in other Ministries of Justice/National authorities, as well as official requests (for instance, an EIO). In both cases, the request and evidence must be sent using postal mail, or delivered physically by a carrier. • If my country already has a functional e-CODEX[12] access point, and if the Ministry I work in is responsible for this, I may use e-CODEX to send official requests (MLAs and EIOs respectively) and e-Evidence data to the other Member State. • I must send reminders to other stakeholders when no response is received.
Issues & constraints	I face a certain number of issues and constraints in my daily work: *A. Communication channel* • Sending requests and evidence through post mail is time consuming (i.e. not always appropriate for urgent cases), and

[12] e-CODEX offers technical solutions to EU Member States to ensure secure cross-border communication in the e-Justice domain. More information is available here: https://www.e-codex.eu/technical-solutions

expensive.

  - I do not have digital means to exchange large amounts of data in a secure and trustworthy manner. If I want to share pictures, videos or voice records, I sometimes need to send electronic devices via post due to the lack of technical means.
  - Sending large documents using email is very cumbersome, as it must be sent over several emails due to the capacity limit of the mail server. This also often causes confusion as the data is scattered in different places, and thus fragmented.
    - For 24% of the respondents the lack of technical means to exchange large amount of data with Eurojust and other EU bodies/agencies is a difficulty to a great extent, and to some extent for 29% of them.
    - For 24% of the respondents the lack of technical means to exchange large amount of data with other countries is a difficulty to a great extent, and to some extent for 38% of them.
  - Often, the information I send to recipients outside of my Member State is not secure and encrypted (unless there is a secure communication channel), and thus there is a risk of hacking. 29% of the respondents consider the lack of a secure communication a difficulty to a great extent, 29% to some extent.
  - Although the e-CODEX projects work well, they do not cover all types of requests which are used. Moreover, they do not cover the exchange of messages following requests (for instance, if there are questions), which are thus sent using normal email.
  - I either lack digital tools to conduct my daily tasks and cooperate in cross-border cases, or my tools have been designed without taking into account the exchange information with other parties (being Member States or JHA agencies and EU bodies), i.e. lack of interoperability.
- *Search information*
  - I cannot access Eurojust CMS, therefore I cannot search for information related to my pending requests.

Table 4: JIT members and participants personas

	JIT members and participants
Goals & tasks	As a member or participant of a JIT (or a participant to an action day[13]), I participate in joint investigations with law enforcement officers, prosecutors or investigative judges, judges from other countries. A. *Exchange information* • I need to exchange information with my counterparts, either via email and phone, or during meetings which are organised by Eurojust. • I often use non-secure messaging and communication tools because of their ease to use and convenient functionalities (in particular, when quick communication is needed during action days). • I need to communicate with Eurojust for several matters (financial, legal and practical support). • I need to collaborate with the relevant private sector stakeholders, as well as third countries (when applicable). • When results of the JIT are available, I need to evaluate the JIT/action day. B. *Planning* • I need to plan and organise meetings (JIT meetings, action days). These meetings can be organised with the support of Eurojust while arranging a coordination meeting or setting up a coordination centre to facilitate cooperation during simultaneous operations. C. *Translate information* • I need to translate documentary evidence into a common working language we use with a given counterpart (e.g. English).
Issues & constraints	In my daily work, I face the following issues and constraints: A. *Communication channels* • I sometimes use non-secure communication channels, such as instant messaging or other similar commercial tools, because they are immediate and offer useful functionalities for my tasks (e.g. sending files like pictures, videos, voice records). • I do not have digital means to exchange large amounts of data in a secure and trustworthy manner. B. *Exchange of information*

[13] An action days are a judicial tools used by Eurojust to coordinate investigations across different EU Member States. This coordination allows to carry out "simultaneous and minutely planned arrests, searches, interviews of suspects and victims, seizures of evidence and the freezing of assets in real time", see: http://eurojust.europa.eu/press/PressReleases/Pages/2019/2019-11-29.aspx

	• Information is fragmented and scattered, hampering the legal traceability of the data gathered. There is no single space of communication and information exchange within JITs. • Difficulties to share and store information/documents, in conditions facilitating the traceability and admissibility of the evidence exchanged. • Coordination among JIT members and participants is difficult when requesting information to a stakeholder not involved in the JIT. *C. Search information* • I need to be able to identify relevant JIT members in other EU Member States or third countries. • I struggle finding information about domestic rules regarding the setting up of a JIT. *D. Procedures* • I would need to speed up the internal procedures (at Member States level) to set up a JIT and to obtain the necessary signatures. Also, to collect the official signatures from the JIT parties is very cumbersome since there is no way to do it electronically for all parties involved. • I may be able to have the possibility to maintain the JIT during the trial phase.

Table 5: Eurojust persona

	Eurojust
Goals & tasks	My goal is to coordinate collaboration between judicial practitioners in my Member State and in one or several other Member States on cross-border criminal cases for which the help of Eurojust has been requested. To do so, I must be able to: *A. <u>Exchange information</u>* • Refer questions via email to the EJN in criminal matters contact points. • Exchange messages, case-related information (sometimes, in a large volume) and requests (both in forms and unstructured) securely with practitioners and national authorities (including EJN in criminal matters and ENCS contact points) in my Member State. Information may take different types of format per Member State. • Exchange all information (including unclassified and classified information) through a secure and encrypted communication channel with stakeholders in my Member State and/or officers in other JHA agencies and EU bodies. • Exchange messages and information with my Member State's Europol Liaison Officer (and other EU bodies such as OLAF, the EPPO) to verify whether a person of interest in one of my National Desk's cases is included in one of their databases. • Exchange messages and other information with JIT members and participants within the same JIT I am involved. • Share information about my cases with other staff within Eurojust in order to get operational support from them. • Receive documents signed electronically to be certain about their authenticity. *B. <u>Planning</u>* • Organise meetings at Eurojust between practitioners from my Member State and from other Member States. • I need a centralised place to have an overview of all my cases and keep track of those I am working on, as well as of the related messages and follow-up actions to be taken for the different cases (including reminders or notifications). • Take part in the planning, organisation, running and follow up of JITs, as well as of action days. *C. <u>Search information</u>* • Verify information about case-related data in my Member State's judicial databases (directly or indirectly with the help of a national practitioner) or consult national practitioners from my Member State to gather information on a given case. • Search for information about case-related data in the judicial databases available or planned at EU level (for instance, the hit/no-hit access in the new ECRIS-TCN system via the European Search Portal (ESP)). • Search for information about case-related data in the Eurojust CMS to identify links and relevant information on the case I am working on.

	• Extract analyses and reports from the Eurojust CMS. • Search for information about case-related data in the Case Information Form (CIF) application, where organisational lessons learned in judicial cooperation are maintained. D. *Record information* • Register the cases I worked on in the Eurojust CMS, as well as relevant case-related information. • Register anonymised information about the outcome of my cases in the Eurojust CIF application. • Record, access and search data related to the Counter-Terrorism Register at Eurojust. • Carry out data management and data quality activities on the data in the Eurojust CMS (e.g. ensuring that there are no incomplete cases, cases open for too long, etc.). E. *Translate information* • Translate and summarise information about a case, which I received from my Member State into English (usually), in order to send it to my colleagues at other Eurojust National Desks. F. *Data protection and security* • I need Eurojust CMS to notify me about the data retention period, so I can delete the personal data in a timely manner – or if necessary, request an extension of the retention period. • Ensure that the data I register in the Eurojust CMS is protected according to secure and private standards.
Issues & constraints	I face a certain number of issues and constraints in my daily work: A. *Communication channel* • I do not have a secure and encrypted communication channel to exchange messages and information with practitioners and national authorities in my Member State. In order to circumvent the problems, I remove personal data from the emails I send. • Often I have to send several emails in order to exchange large files, because they exceed the limit on the email server. This is very cumbersome. • For exchanging classified information, I might use the SIENA network[14], using the terminals at Europol. However, the use of SIENA is cumbersome, as there are several intermediaries (from the law enforcement domain) both on my side and on the side of the recipient at Member State level, and therefore it takes time. • I use non digital means of exchanging information, such as personal delivery via a colleague or myself, or using CDs, USB sticks, postal mail, etc. In urgent matters, these means of exchanging information involve a carrier physically transporting the information or evidence (e.g. DHL). • I do not have digital means to exchange large amounts of data in a secure and trustworthy manner. B. *Exchange information* • As several stakeholders are (most of the time) involved in cross-border cases, the information on the status of my request(s)

[14] SIENA is a communication channel built and maintained by Europol, which is dedicated to information exchange across borders in the law enforcement community.

is very scattered and fragmented.

- I either lack digital tools to conduct my daily tasks and cooperate in cross-border cases, or my tools (incl. Eurojust CMS) have been designed without taking into account the exchange information with other parties (being Member States or JHA agencies and EU bodies), i.e. lack of interoperability.
- I have difficulties to share information about my cases with operational staff working at Eurojust, as I cannot manage easily the access rights related to the cases that I have inserted into the CMS. Therefore, most of the times they are not able to see the content of my cases so I have to share manually and/or via emails such information, which is cumbersome.

C. *Planning*

- I must keep track of my cases and related tasks using either a structure of files in Outlook, or an Excel file, which are shared by all members of my National Desk. The current CMS cannot be used for this purpose as it is not user friendly, and does not have enough capacity to support me on this task.

D. *Search information*

- If I do not have access to national databases, I am not able to search for information related to a specific case (for instance, information about a suspect in particular).
- If I believe that other National Desks are working on a case involving the same suspect as me, I call them or send them an email in order to ask them about it. I cannot perform this search using the Eurojust CMS as the limitations in the visibility level will not allow me to see all persons inserted in the CMS. Additionally, being the insertion of personal data in CMS delayed sometimes, even if I would be able to search across the whole database the result will not be conclusive either.
- Search functionality in the Eurojust CIF application is very limited, so I am not able to easily identify how similar cases to the one I am working on were handled in the past.
- If I am informed that Europol or OLAF are working on a relevant case for me, I phone or send an email to a national representative in the other agency to ask him/her for information.
- To sum up, I do not have the possibility to cross-check data against Eurojust CMS, the EPPO CMS, Europol CMS, OLAF systems, ECRIS-TCN and SIS II automatically, with a view to knowing whether there is (or has been) information related to my case or an investigation ongoing about a case linked to the one I am currently coordinating.

E. *Record information*

- In most cases, I (or a member of staff of my National Desk) register the cases I am working on in Eurojust CMS. However, this takes a lot of time as the CMS is cumbersome to use, and sometimes case registration is delayed.
- Sometimes, I register the outcome of a case in Eurojust CIF application, however I often do not have the time to do so, and hence the insertion is delayed.
- To carry out data quality checks in Eurojust CMS is very cumbersome since there is no general profile due to the limitations to visibility of data and the technical tools available.

F. *Translate information*

- I use translation tools to translate part of the case-related documents. The translation is not without mistakes, but it can at least serve as a starting point. Official translations take long time, which may result in an obstacle for a quick response in the

	case.

Table 6: JHA agencies and EU bodies

	JHA agencies and EU bodies
Goals & tasks	As a representative of a JHA agency (either Europol or Frontex) or EU body (either the EPPO or OLAF), I must sometimes collaborate on specific cases with my counterparts at the other JHA agencies or EU bodies. To do so, I carry out the following tasks: *A. <u>Exchange information</u>* • Using a SIENA terminal, if possible. • Through regular email, which is not secured (I must anonymise the data) and sometimes cumbersome if large amounts of data have to be shared. • By follow-up calls. • By meeting physically and exchanging documents. • (When part of a JIT or an action day) I need to exchange case-related information with all or a selected numbers of members (data cannot always be shared with everyone due to its sensitivity). B. *<u>Search information:</u>* • When I believe that another agency is investigating a similar case (for instance, involving the same suspect), I must contact my counterpart at that agency via email or phone in order to ask him/her to verify this hypothesis.
Issues & constraints	I face the following constraints in my daily work: *A. <u>Communication channel</u>* • I have no secured and encrypted communication channel (similar to email) to exchange sometimes sensitive, and also in large amount, (case-related) data. • (When part of a JIT or an action day) I have no means to securely work and collaborate with the rest of the stakeholders involved. *B. <u>Search information</u>* • I have no systematic way to check whether investigators in other agencies are working on related cases. There is no automated way to cross-check data between JHA agencies and EU bodies.

Based on an analysis of the business needs of the different stakeholders related to the same topic, several business needs categories have been created. All these business needs categories have been mapped with IT solutions, as displayed in Table 7 below. The seven solutions identified by this study are as follows:

- An underlying Secure Communication Channel to allow for exchange of messages, information and evidence electronically across borders in a secure way.
- A Communication Tool to enable the secure electronic exchange of judicial cooperation requests and mutual recognition/mutual legal assistance forms, information, messages and evidence.
- The Redesigned Eurojust Case Management System to allow its proper functioning and ensure it addresses the needs of its users.
- A JIT Collaboration Platform to set up, plan and coordinate JIT operations, allowing easy communication, as well as the electronic sharing of large amounts of information and evidence between JIT partners.
- Exchange of data between the JHA agencies and EU bodies active in the area of judicial cooperation (Eurojust, Europol, Frontex, the EPPO and OLAF).
- Judicial Cases Cross-Check to be able to search for case-related information and identify links among cases that are being investigated in other Member States or JHA agencies and EU bodies.
- Large Files Solution to overcome the limited attachment sizes authorised by their mail servers and exchange large amounts of information electronically.

In addition to these main 7 solutions, the study has included additional solutions:

- A Common services platform to be used by all stakeholders in the domain of Digital Criminal Justice to provide ‘services’ (e.g. information exchange).
- A Judicial One-Stop-Shop Portal, i.e. a web portal through which stakeholders (law enforcement officers, prosecutors, investigative judges, judges, and central authorities) could securely access a range of services supporting their tasks in cross-border criminal cooperation.
- A training platform to centralise existing training materials related to cross-border judicial criminal cooperation.
- Extended EJN Atlas (directory) to identify the prosecutors or investigative judges to be contacted in other Member States for cross-border judicial criminal cooperation.
- The reusability of some relevant Common Europe Facility (CEF) Building Blocks (i.e. eSignature, eTranslation, and eDelivery), which could be part of some of the solutions presented above.

For a detailed description and assessment of the solutions, see section 5.

Annex C includes a detailed mapping of the individual business needs mapped to the different solutions.

Table 7: Mapping business needs vs solutions

Business need category	**Description and business needs examples**	**Persona**[15]	**Solution**
Securely communicate and exchange information via digital means	- Allow a secure communication between the stakeholders, including sending and receiving (sensitive and confidential) data. Examples: - Send/receive requests (forms set out in the legal instruments, and their supporting documents) in a secure and digital way. - Send large amounts of data over a secure and digital communication channel.	National authorities JHA agencies JIT Prosecutors Eurojust	- Secure Communication Channel - Communication Tool - Redesigned Eurojust CMS - JIT Collaboration Platform - Exchange of data between the JHA agencies and EU bodies (hit/no-hit) - Large Files Solution - Judicial One-Stop-Shop Portal
Ensure interoperability across systems	- Ensure that the solutions used by the stakeholders are interoperable, allowing for an efficient and seamless cooperation. Examples: - Ensure that practitioners at national level have faster, seamless and more systematic access to information about relevant cases owned by prosecutors from other Member States, or the JHA agencies and EU bodies. - Use a unique identifier for each case to ease their identification and avoid confusions. - Use a standardised data exchange format (e.g. UMF) that allows disparate systems to communicate data sets in a	National authorities JHA agencies JIT Prosecutors Eurojust	- Secure Communication Channel - Communication Tool - Redesigned Eurojust CMS - JIT Collaboration Platform - Exchange of data between the JHA agencies and EU bodies (hit/no-hit) - Common Services Platform

[15] For the sake of simplicity, the National Authorities and the Ministries of Justice are presented jointly in this column under the icon National authorities. Likewise, Prosecutors and Investigative Judges are represented jointly in the icon Prosecutors.

	consistent manner, reducing complexity, data errors and reduces processing overheads.		
Easily manage data and ensure its quality	• Ensure that the data exchange meets quality standards, and that stakeholders can easily use it. Examples: • Ensure the traceability of the data collected during a JIT. • Exchange of cross-border cases related data between Member States in a structured way. • Extract analyses and reports from the Redesigned Eurojust CMS. • To be able to easily and rapidly record information about a closed case into the CIF database.	National authorities JHA agencies JIT Prosecutors Eurojust	• Secure Communication Channel • Communication Tool • Redesigned Eurojust CMS • JIT Collaboration Platform • Large Files Solution
Identify links between cases	• Ensure that stakeholder can search and find the relevant information they need for their cases. Examples: • Identify potential links between my (national) case and other cross-border cases, in order to determine whether my national case has an external dimension and involves other countries. • Need to be able to cross-check against the data in: the Redesigned Eurojust CMS, the EPPO CMS, Europol IS, ECRIS-TCN, SIS II, to identify links between the Eurojust case and other ongoing cases.	Prosecutors JHA agencies Eurojust JIT	• Secure Communication Channel • Communication Tool • Redesigned Eurojust CMS • Judicial Cases Cross-Check • Exchange of data between the JHA agencies and EU bodies

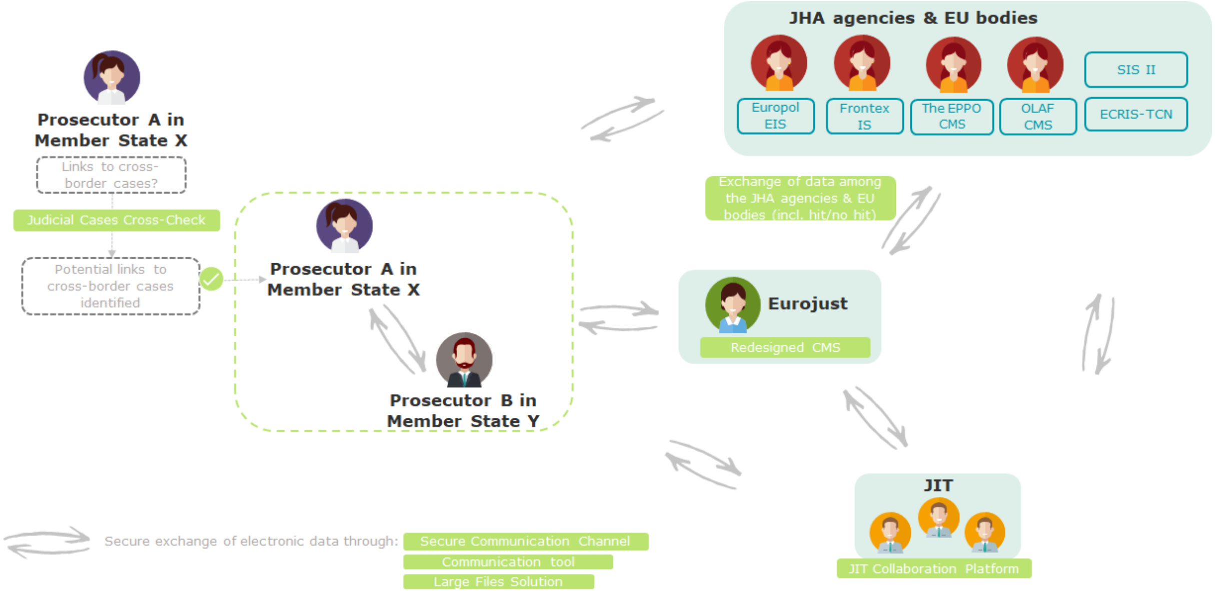
Ensure data protection principles for all systems	• Ensure data protection by design and by default by implementing the tools used in cross-border cooperation in compliance with the data protection principles and requirements. Examples: • Manage access rights. • Enforce data protection rules, as well as security and privacy standards. • Receive notification from the Redesigned Eurojust CMS to delete the personal data after the retention period.	Prosecutors Eurojust National authorities JHA agenc	• Secure Communication channel • Communication Tool • Redesigned Eurojust CMS • JIT Collaboration Platform • Judicial Cases Cross-Check • Exchange of data between the JHA agencies and EU bodies • Large Files Solution
Ease the process of setting up and operating JITs	• Ensure that stakeholders have access to a tool allowing them to easily set-up and run a JIT. Examples: • To set up the JIT swiftly. • Need a tool for instant messaging/communication and planning with JIT partners.	National authorities JHA agencies JIT Prosecutors Eurojust	• Redesigned Eurojust CMS JIT Collaboration Platform
Access digital support tools	• Have access to digital tools for cross-border criminal cooperation. Examples: • Identify the correct stakeholder (i.e. another prosecutor or central authority) to be contacted. • Have access to handbooks, guidelines on the different procedures to be conducted (e.g. how to fill in MLA forms).	National authorities JHA agencies JIT Prosecutors Eurojust	• Redesigned Eurojust CMS • Common Services Platform • JIT Collaboration Platform • Judicial One-Stop-Shop Portal • Training Platform • Extended EJN Atlas (Directory) • eSignature (CEF BB) • eTranslation (CEF BB)

3.2 User journey

Building on the business needs, the user journey aims to illustrate the experience from the stakeholders' perspective (i.e. the personas). As depicted in the stakeholder mapping figure (see below), there are several stakeholders involved in cross-border criminal cases, and thus several different user journeys. In this section, the report presents the user journey of Prosecutor A in Member State X.

The figure below presents the **current flow of a cross-border case from the perspective of the Prosecutor A through the usage of the future Digital Criminal Justice solutions (green boxes)**. These solutions are described in detail and assessed in section 5.

Figure 3: User journey


JHA agencies & EU bodies
Europol EIS
Frontex IS
The EPPO CMS
OLAF CMS
SIS II
ECRIS-TCN
Prosecutor A in Member State X
Links to cross-border cases?
Judicial Cases Cross-Check
Potential links to cross-border cases identified
Prosecutor A in Member State X
Prosecutor B in Member State Y
Exchange of data among the JHA agencies & EU bodies (incl. hit/no hit)
Eurojust
Redesigned CMS
JIT
JIT Collaboration Platform
Secure exchange of electronic data through:
Secure Communication Channel
Communication tool
Large Files Solution

The figure above presents several possibilities for the stakeholders of Digital Criminal Justice:

- Prosecutor A in Member State X cross-checks whether the case s/he is handling has links with other cross-border cases. The tool to be used to identify these links is the Judicial Cases Cross-Check.
- Once a potential link to a cross-border case has been confirmed, Prosecutor A exchanges (via the Communication Tool and/or Large Files Solution) legal forms and relevant data with the identified Member State(s), in this case Prosecutor B in Member State Y.
- Prosecutor A requests the support of Eurojust (or EJN in criminal matters, depending on a case), due to the cross-border dimension of the case, the complexity of the case, the number of stakeholders involved, the nature of the crime (e.g. serious organised crime), need for prosecution on common bases, amongst others. Eurojust receives the request for support (via the Communication Tool) and assesses whether the received case qualifies as a Eurojust case. Eurojust provides mutual legal assistance, proceeds with the case coordination, registers the case information in the Redesigned CMS, searches for links with other cross-border cases in the system etc., depending on the request. Eurojust also verifies (via an automated exchange of information, i.e. hit/no-hit) whether the other JHA agencies (Europol, Frontex) or EU bodies (the EPPO, OLAF), have relevant information.

- Prosecutor A exchanges information and receives support from other JHA agencies or EU bodies (via the Communication Tool and Large Files Solution).
- If agreed upon, a Joint Investigation Team (JIT) can be set up, via the JIT Collaboration Platform, to facilitate the coordination of investigations and prosecutions conducted in parallel across several Member States.

4 High-level considerations

This section presents key high-level considerations to be taken into account for the design of conceptual architecture for the implementation of Digital Criminal Justice, and the different solutions.

4.1 Data protection considerations

The communication and sharing of relevant data between competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, is a key objective on the EU policy agenda. Yet, it should be ensured that personal data information flows, especially at cross-country level, take full account of data protection requirements enshrined in the applicable legal instruments and embody data protection by design and by default. Accordingly, the Digital Criminal Justice project enhances cooperation between Member States on combating cross-border criminal activities but may also affect the rights and freedoms of the persons whose personal data are processed by the Member States, Union institutions, agencies and bodies in this context. Therefore, and taking into account the scope of the project, respecting and building upon the existing approach for protecting privacy and personal data while the critical elements of the Cross-border Digital Criminal Justice concept are constructed, is of paramount importance.

In addition to the founding Regulations of the bodies and agencies involved, Regulation 2018/1725 (hereinafter Regulation 1725) on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies[16], especially Chapter IX, sets forth the general rules that apply to the processing of operational personal data.[17] The legal act specifying the rules on processing of personal data by national competent authorities is Directive 2016/680[18], providing for a harmonised use of personal data for criminal law enforcement purposes and regulating international data transfers related to criminal offences.

It is important to mention that the specific legal instruments regulating the functioning of and the cooperation between the JHA agencies and EU bodies involved in the Digital Criminal Justice context explicitly provide for the interpretation and application of data protection rules and principles established by Regulation 1725[19] and Directive 2016/680 to ensure a strong and

[16] Regulation (EU) No 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32018R1725

[17] Operational personal data means all personal data processed by Union bodies, offices or agencies when carrying out activities which fall within the scope of Chapter 4 and 5 of Title V of Part Three TFEU. It encompasses as personal data processed for the purposes of a criminal investigation and activities executed in the fields of judicial cooperation in criminal matters and police cooperation.

[18] Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0089.01.ENG

[19] Please note that some of the legal instruments refer to Regulation (EU) 2018/1725's predecessor, namely Regulation (EC) No 45/2001.

coherent data protection framework and the protection of individuals with regard to the processing of personal data in the area of judicial and police cooperation in the Union.[20]

4.2 Security considerations

Security has become a strategic necessity inside any organisation's environment. With data breaches now costing dozens of millions of euros or more alongside with judicial data and other types of sensitive data getting sold on dark markets this is particularly relevant within the context of Digital Criminal Justice. System security should always be a main concern when designing IT architectures, with the main goal being the protection of any individual who might get affected by any leakage of sensitive data.

A significant amount of security considerations and challenges must be taken into account while designing, implementing and operating the Digital Criminal Justice architecture. The complexity of the architecture resides in:

- The data exchanged: transferring judicial data and other types of sensitive data increases the complexity of the architecture as it needs to support the transit of that information while ensuring the confidentiality, integrity and operational availability of the data exchanged. It is a compromise to be evaluated based on technical availabilities, operational and business requirements.
- The interactions: the number and complexity of communications are critical in the architecture as security needs to be addressed and supported between different IT systems. Communication protocol design should take into account the interoperability of the different systems alongside with the compatibility of the security measures being implemented.
- The stakeholders: the number of stakeholders is critical and complex in terms of decision and governance. The amount of impacted stakeholders calls for thorough testing procedures before deploying any solution in a production environment.

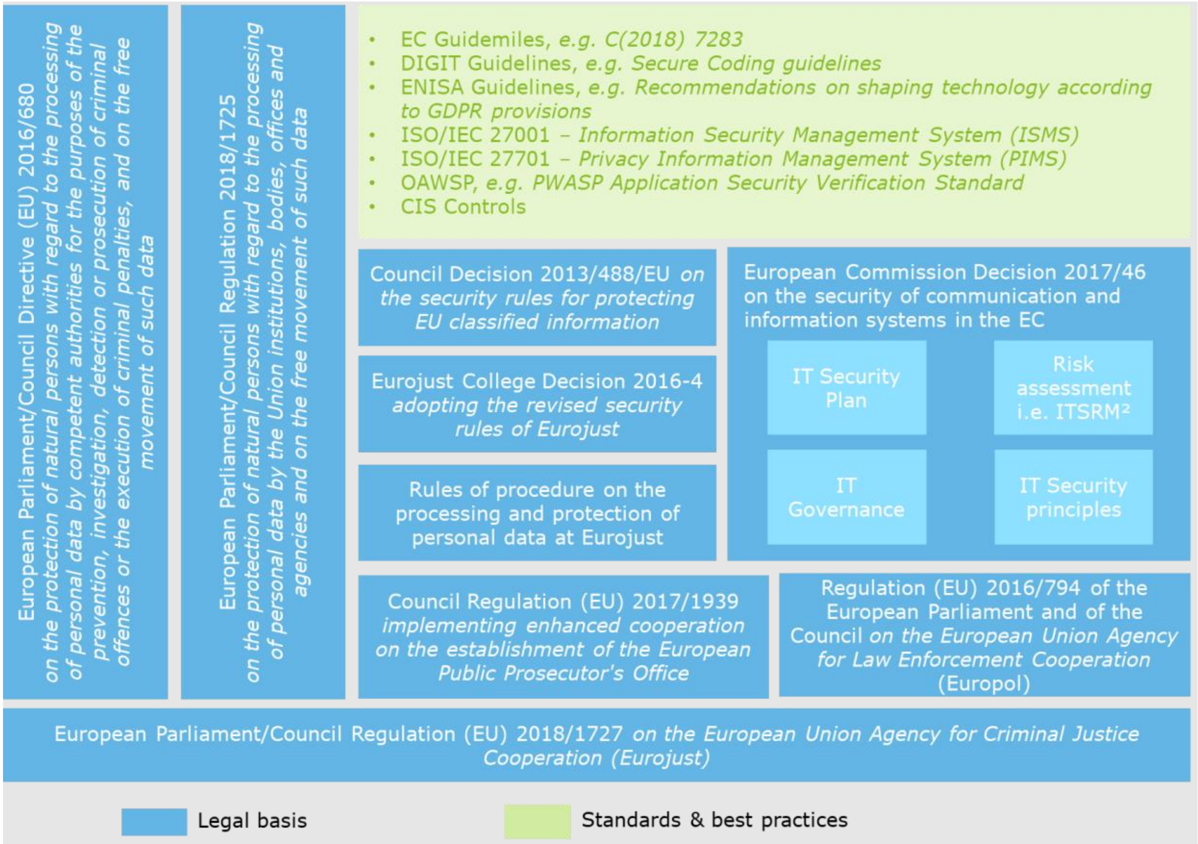
This requires security measures at different levels and layers to make sure that overall security assurance is reaching a discussed, analysed and agreed upon acceptable level, in line with business requirements, legal instruments and contractual obligations.

Security is an overarching concern that should be considered and managed across the whole architecture landscape. The focus needs to be on the communication channels used to exchange information on cases between the different stakeholders (e.g. Member States, Eurojust, Europol, OLAF, etc.) and at the underlying infrastructure, systems, applications and components that store and/or process operational data.

Security measures need to be implemented in a way to protect against malice, mistakes and mischance. If these were to materialise, they could impact the reliability of the whole Digital Criminal Justice ecosystem by compromising systems, applications and services. As a result, this could lead to compromised (personal/sensitive) data, as well as disruption of Digital Criminal Justice services, in some instances preventing legitimate end-users from getting access to Digital Criminal Justice data.

[20] Europol Regulation, Recital 40; EPPO Regulation, Recitals 90 and 93; Frontex Regulation, Recital 98; OLAF Regulation, Recital 35 and eu-LISA Regulation, Recital 39.

Figure 4: Legal, Standards and best practices landscape


European Parliament/Council Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data
European Parliament/Council Regulation 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data
EC Guidemiles, e.g. C(2018) 7283
DIGIT Guidelines, e.g. Secure Coding guidelines
ENISA Guidelines, e.g. Recommendations on shaping technology according to GDPR provisions
ISO/IEC 27001 – Information Security Management System (ISMS)
ISO/IEC 27701 – Privacy Information Management System (PIMS)
OAWSP, e.g. PWASP Application Security Verification Standard
CIS Controls
Council Decision 2013/488/EU on the security rules for protecting EU classified information
Eurojust College Decision 2016-4 adopting the revised security rules of Eurojust
Rules of procedure on the processing and protection of personal data at Eurojust
European Commission Decision 2017/46 on the security of communication and information systems in the EC
IT Security Plan
Risk assessment i.e. ITSRM²
IT Governance
IT Security principles
Council Regulation (EU) 2017/1939 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office
Regulation (EU) 2016/794 of the European Parliament and of the Council on the European Union Agency for Law Enforcement Cooperation (Europol)
European Parliament/Council Regulation (EU) 2018/1727 on the European Union Agency for Criminal Justice Cooperation (Eurojust)
Legal basis
Standards & best practices

The figure above depicts the most relevant legal instruments, as well as the relevant standards and best practices that were considered, from security and data protection angles, to identify the high-level security considerations.

On top of this, several Regulations and Decisions apply to the Digital Criminal Justice target architecture, for instance European Commission Decision 2017/46, which covers the security of communications and information systems used within the European Commission. This decision embodies four pillars which are also considered relevant for the Digital Criminal Justice target architecture:

1. IT Security plan, corresponds to the required documentation of the IT security measures required to meet the IT security needs of the key systems, applications and tools in the Digital Criminal Justice target architecture.

2. Risk assessment, following the IT Security Risk Management (ITSRM²) methodology, as required by DIGIT.

3. IT governance covers the mandatory roles and responsibilities related to the secure communications and information systems in the European Commission; these roles should be assigned or mapped to their equivalent within the DCJ target architecture organisational scope.

4. And finally, the IT Security principles covering the authenticity, availability, confidentiality, integrity, non-repudiation, protection of personal data and professional secrecy.

In fact, according to Article 3 of European Commission Decision 2017/46[21], applying to all communication and information systems (CISs) which are owned, procured, managed or operated by or on behalf of the Commission and all usage of those CISs by the Commission, effective IT security is described as having appropriate levels of:

- Authenticity: the guarantee that information is genuine and from bona fide sources.
- Availability: the property of being accessible and usable upon request by an authorised entity.
- Confidentiality: the processes to ensure that information is not disclosed to unauthorised individuals, entities or processes.
- Integrity: the means of safeguarding the accuracy and completeness of assets and data.
- Non-repudiation: the ability to prove an action or event has taken place, so that this event or activity cannot subsequently be denied.
- Protection of personal data: the provision of appropriate safeguards in regard to personal data in full compliance with Regulation (EC) No 45/2001[22] [23].
- Professional secrecy: the protection of information of the kind covered by the obligation of professional secrecy, in particular information about undertakings, their business relations or their cost components as laid down in Article 339 of the TFEU.

Moreover, Article 3 of Commission Decision 2017/46 provides the following security-related considerations relevant for IT security in the Commission (which need to be put in the target architecture's perspective and tailored to it):

- IT security should rely on a risk management process.
- All CIS should be identified, assigned to a system owner and recorded in an inventory.
- Security requirements of all CIS should be determined based on their security needs and of the security needs of the information they process. The design of CIS to CIS services may support specified levels of security needs.
- IT security plans and IT security measures should be proportionate to the security needs of the CIS.

Organisation and responsibilities

Security is an overarching concern that involves several (e.g. internal and external) stakeholders, and it is therefore important to clearly understand and delineate the organisational scope.

A trade-off has to be found in terms of defining, formalising and enforcing security roles and responsibilities for the target architecture, considering the following side effects:

- Increased development and testing efforts and costs.

[21] Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission

[22] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

[23] Regulation (EC) No 45/2001 is no longer in force, it has been repealed by Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data.

- Increased operational processes complexity.
- Complex security management process, maintenance and troubleshooting.

As depicted in Figure 4 Legal, Standards and best practices landscape, in addition to the Commission Decision described above, which applies to the security of communication and information systems used within the European Commission, there are security rules and procedures detailed in College Decision 2016-4 regarding the adoption of the revised security rules of Eurojust, in conformance with the Article 39(a) of the Eurojust Decision[24] [25], which requires Eurojust to apply the security principles and minimum standards as set out in the rules adopted by Council Decision 2013/488/EU on the security rules for protecting EU classified information. Besides these, the EPPO and Europol Regulation also include security and data protection rules.

According to the security rules for protecting EU classified information (i.e. Council Decision 2013/488/EU), any information or material designated by an EU security classification, the unauthorised disclosure of which could cause varying degrees of prejudice to the interests of the European Union or one or more of its Member States is considered EU classified information.

The aforementioned security rules apply to all actors in the Digital Criminal Justice landscape having access to classified information, any Communication and Information System or media processing classified information, and all premises and installations containing such information. A detailed overview of Eurojust's current security rules is included in Annex E.

As depicted in Figure 4 Legal, Standards and best practices landscape, from a data protection and privacy perspective, the DCJ target architecture must comply with Regulation 2018/1725, as well as Directive 2016/680, which the DCJ target architecture aims to support. Both instruments, as well as specific provisions regarding the processing of operational personal data of the Eurojust Regulation, have data protection and security related requirements and controls that need to be considered for the design of the DCJ target architecture.

The last two pieces of the legal framework are Council Decision 2013/488, which is a decision that defines security rules for protecting EU classified information (EUCI), and Eurojust College Decision 2016-4. They contain essential considerations that could influence the design choices of the DCJ target architecture (e.g. TESTA cannot be used for the transmission of classified information) Moreover, Eurojust College Decision 2016-4 (i.e. Eurojust security rules), which is partially built on top of the Council Decision 2013/488, provides the basic principles and minimum standards of security applicable in the Eurojust domain.

Besides the legal framework, from a security perspective, the target architecture should also be in line with available industry standards and best practices, as depicted in Figure 4 Legal, Standards and best practices landscape, e.g. EC guidelines, ISO27001 and 27701, DIGIT, ENISA, CIS and OWASP. Security requirements and controls should be elaborated at the design level based on the chosen standards and industry best practices, tailored to the DCJ target architecture to comply with legal and contractual obligations. Security controls and requirements should be sound and consistent in covering the following architecture aspects:

[24] Council Decision 2009/426/JHA of 16 December 2008 on the strengthening of Eurojust and amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime.

[25] Council Decision 2009/426/JHA is no longer in force, it has been replaced and repealed by Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust)

- Infrastructure Security considerations – e.g. network boundaries and devices, protection of network perimeters, Distributed Denial of Service (DDoS) protection, load balancing, IDS/IPSs, reverse proxies etc.
- Network Security considerations - secure communication channel, secure transfer protocols, network segregation and isolation, network filtering, firewalls, proxies, etc.
- Data Security considerations - e.g. data storage, data classification (i.e. EUCI) and labelling, etc.
- Organisational Security considerations – e.g. security Roles and responsibilities, human resource security, etc.
- Operational Security considerations - e.g. backup management, vulnerability management, password management, change management, secure software development lifecycle, etc.
- System and Application Security considerations - e.g. system hardening, end-point security, containers, web-application firewalls (WAF), electronic certificates, etc.
- Business continuity and disaster recovery considerations – Business Continuity Plans (BCP) & Disaster Recovery (DR) Plans, Service Level Agreements (SLA), redundancy, etc.

However, it is important to mention that a trade-off has to be found with regards to the level of maturity and granularity in terms of defence layers and security mechanisms, which should be dependent on the risk profile of the target architecture ecosystem. The level of granularity in which security design should be considered has to take into account the following side effects:

- Redundant Organisation policies and processes.
- Complex Security management process, maintenance and troubleshooting.
- Impractical infrastructure, systems or applications.
- Difficult infrastructure, systems or applications recovery.

A risk-driven compilation of security measures, data privacy requirements and controls needs to be prepared and provided by Digital Criminal Justice system owners in the form of a security baseline to the contracted service providers that would implement the target architecture. The security baseline of the target architecture should be composed of relevant security and data privacy requirements and controls that are consolidated with the aim of:

- Meeting functional and non-functional requirements.
- Ensuring compliance with applicable regulation, laws and contractual obligations.
- Enabling for security and data protection by design and by default.
- Mitigating, or reducing to an acceptable level, potential risks identified upon risk assessment exercise.

Overall, security should follow a defence in depth approach, which consists of multiple protection layers that ensure that security remains relatively under control even though a protection layer gets compromised.

Target architecture security should be designed in a way to not rely on a single point of security or failure, every physical and logical level must be secured, and failures must be stopped at one level propagating.

The key recommendation is to perform threat analysis and a risk assessment to cover all the architecture assets (i.e. systems, applications, components, processes, etc.). Hence, focusing on most relevant cyber threats, based on a risk management process that aims at determining the levels of IT security risks and defining security measures to reduce such risks to an appropriate level and at a proportionate cost. This analysis helps in prioritising the design and implementation of security measures, controls and requirements in the function of their associated risks.

As a consequence to the complexity of the target architecture, many issues would have to be resolved along the way, and compromises made to find viable trade-offs. Some of these issues and compromises would need to be decided pro-actively before the various implementation contracts can be procured. In contrast, many others could be resolved instead by the contracted service providers. While there is a proactive need to specify the essential characteristics, features and requirements of the new architecture, experience in this field has shown that it is impractical and unnecessary to try and specify the whole detailed architecture at once.

Nevertheless, to ensure alignment, quality of outcomes and compliance across systems, applications, services and suppliers, all architecture assets designed for the target architecture should be compliant with the following high-level security principles:

- P1 - *Security and data protection by design and by default.*
  - Every system managed within the Digital Criminal Justice architecture must guarantee the fulfilment of the following security requirements: confidentiality, integrity, availability, accountability and non-repudiation, in line with Commission Decision 2017/46 on the security of communication and information systems used within the European Commission.
  - Business and IT Processes must be designed from the start to adhere to data protection principles so that operational personal data is processed lawfully and fairly; that only personal data that is adequate, relevant, and not excessive in relation to the specific purpose is processed. This applies to the amount of personal data collected, the extent of its processing, the period of its storage and its accessibility, in accordance with the Directive 2016/680 with regard to the processes carried out on the national level by the competent authorities and Data Protection Regulation 2018/1725 with regard to the processes carried out by Union bodies, offices and agencies, without prejudice to specific data protection rules applicable to such Union bodies, office or agencies.
  - Fail securely & use secure defaults: establish secure defaults when system goes in error or exception status, or at default state. This would lower the risks associated with misconfigurations. Secure defaults must be determined and configured, as well as regularly tested.
- P2 – *Implement Defence in depth protection – Do not trust infrastructure and its underlying components – Assume that vulnerabilities could be everywhere, in hardware and in any piece of software (e.g. firmware, virtualisation technologies, middleware and application layers) - Do not trust and assume security of other objects, assets and services.*
- P3 - *Assume that external systems and services are insecure.*
- P4 - *Authenticate users, systems and processes.*
- P5 - *Authorize after identification and authentication.*
- P6 - *Clearly delineate the physical and logical security boundaries.*
- P7 - *Security responsibilities and accountability are made explicit.*
- P8 - *Security should be periodically reviewed and reassessed.*
  - Any set of security requirements must be able to adapt and evolve to deal with new and emerging risks, technologies, threats, and legal and organisational contexts.
- P9 - *Data is always protected and secured at rest and in transit.*

- P10 – *Audit and monitor security related events and logs.*[26]
- P11 – *Assign the least privilege possible on a need to know basis.*
- P12 - *Check regularly compliance with applicable regulations and standards.*
- P13 – *Consider open and simple designs and Standard solutions to improve portability and interoperability*.
    - Security should not depend on secrecy of a design and implementation (e.g. encryption algorithm).
- P14 – *Follow a Risk Based Approach to Security*.
- P15 - *Use only secure and approved protocols and algorithms.*

4.3 Interoperability considerations

In any IT system landscape with the need of information exchange across different systems and components, interoperability must always be ensured. First, this section gives a brief overview of what interoperability means. Afterwards, the subsequent sections explain the relevance thereof in this context.

The considerations explained in this section serve as a basis based on which the solutions and architecture presented in the subsequent sections have been devised.

4.3.1 What is interoperability?

While interoperability is often defined at different levels, for the scope of this work it suffices to define interoperability as *"the ability of computer systems or software to exchange and make use of information".*[27] In other words, two or more systems must agree on how they will communicate, and how the received messages must be interpreted.

With the growing digitalisation of the European landscape, and the constantly rising number of digital public services offered by the Commission, interoperability within this IT landscape becomes increasingly important. For this purpose, and with the ultimate goal to create a Digital Single Market, the European Interoperability Framework (EIF)[28] was published on 23 March 2017. This framework puts forward 47 recommendations and 12 principles for public administrations to consider for their digital public services. As interoperability is a key driver for IT developments, all solutions proposed in the following section are mapped to the relevant parts of the EIF.

4.3.2 Interoperability in the future Digital Criminal Justice landscape

As explained in section 3.1.2 above, the future use case of the Digital Criminal Justice landscape involves information exchange within and across three domains. This means that, to facilitate this communication, the systems in these domains must be made interoperable. In particular, the following exchanges of information must be supported:

[26] As per Article 88 of Regulation 2018/1725, logs are also necessary from a data protection compliance point of view.

[27] Lexico; https://www.lexico.com/en/definition/interoperability

[28] European Commission; New European Interoperability Framework – Promoting seamless services and data flows for European public administrations; https://ec.europa.eu/isa2/sites/isa/files/eif_brochure_final.pdf

- Member State to Member State;
- Member State to JHA Agencies and EU bodies; and
- JHA Agencies and EU bodies to JHA Agencies and EU bodies.

The following sections will briefly show why this interoperability is needed, and what concepts should be taken into account when developing the solutions, from an interoperability perspective.

4.3.2.1 Member State to Member State

According to the use case presented in section 3.1.2, the future DCJ landscape should support two key functionalities:

- Checking whether another Member State has related information related to an ongoing investigation (through a hit/no-hit query); and
- The actual data exchange between Member States.

In terms of interoperability, the former could prove to be a challenge. Currently, each Member State has its own repository in which case related information is stored. Implementing a 'hit/no-hit' tool basically means it needs to integrate with each national database. Since each Member State has been responsible for the management and operation of their own databases, there is no 'standard' in how these databases are structured, and what information is stored. Furthermore, as up to now only the Member States themselves have addressed these databases, the way in which data is retrieved also differs from Member State to Member State.

In order to make a 'hit/no-hit tool' possible, interoperability between these databases must be ensured in one of five ways:

- Standardising the databases, i.e. a common data model and a uniform way of accessing the database.
- Defining a common language between Member States to communicate, i.e. databases remain as they are but Member States ensure they translate messages to this uniform language. For the exchange of messages, Member States would be responsible to connect and dispatch messages to other Member States directly, i.e. peer to peer.
- Similar to the previous option, a common language is defined between Member States to communicate. However, for the exchange of messages, Member States now connect to a centrally managed integration layer which handles the exchange of messages between Member States, i.e. spoke-hub.
- Implementing a centrally managed integration layer that handles both the translation of messages and the exchange of messages between the different Member States. Member States are only responsible to connect to this central layer.
- Creating and maintaining a central database that contains a minimal subset of the required data from the national databases. This would also require each Member State to translate to this central data format.

Each of these five solutions would guarantee the interoperability between the systems. However, they each have different implications from a technical and governance perspective. These implications will be explored in more detail in the solution assessments in the following section.

After the hit/no-hit query has returned its result, a prosecutor might want to request access to the detected documents. For this, s/he would reach out to the relevant Member State which would then send the documentation to this prosecutor. Since this is more of an exchange of information between two parties, and not between systems, interoperability should not prove to be a challenge from a technical perspective. A secure communication infrastructure could take care of secure document exchange, given the necessary security controls are in place. This functionality thus becomes more of a security consideration than an interoperability one.

Aside from the technical side of the information exchange described in the previous paragraph, it must be ensured that the request for information and the provided documentation is actually interpretable by the involved parties. Imagine a scenario where a French prosecutor requests information from a Danish authority. Ensuring the received information is interpretable by all parties also relates to interoperability. To ensure interoperability on this level, it must be ensured that a set of guidelines is established so that the end-to-end process of exchanging information becomes interoperable. Examples of such guidelines could be a template through which documents can be requested or a guideline on the language content should be delivered in.

4.3.2.2 Member State to JHA Agencies and EU bodies

According to the user journey presented in section 3.1.2, after consultation of other Member States, a prosecutor might request support from e.g. Eurojust, for instance through a JIT or by requesting additional information. For this, the national end-users must be able to integrate in various ways with the systems in the Eurojust domain. As, in this case, the Member States consume a service exposed by the Eurojust systems, typically it is the Member States' responsibility to adhere to the exposed interfaces. In other words, the Eurojust systems would expose a set of interfaces that Member States could use, but the Member States are responsible for adapting their national systems so that communication can be established. Two examples of interfaces that could be exposed on the central level are Application Programming Interfaces (APIs) or web interfaces. These interfaces on the central level must be stable, well-documented and their evolution carefully managed. Otherwise, the risk arises that interoperability cannot be maintained over prolonged periods of time.

In the scenario that it is Eurojust which adapts to each Member State, it would essentially mean that every Eurojust service would need over twenty interfaces, each tailored to a specific Member State. If a Member State would then change something in their system, the Eurojust systems would also need to be adjusted. This is of course a scenario that should be avoided.

4.3.2.3 JHA Agencies and EU bodies and JHA Agencies and EU bodies

The third, and arguably most complex, domain in which interoperability must be ensured is between systems in the EU domain. The various agencies and bodies in the European Commission are often evolving their IT landscape independently of what other agencies and bodies are doing. This has led to a segregated landscape with a low degree of standardisation overall.

In order to give a complete overview of the interoperability considerations relevant in the context of this project, this information exchange must really be split in two separate categories:

- Exchange of information between systems in the Eurojust domain.
- Exchange of information between systems in the Eurojust domain and systems belonging to other agencies and EU bodies.

It is important to analyse both scenarios in this split as there is a key difference that cannot be forgotten: e.g. Eurojust has direct control over the systems in its own domain, but it cannot directly mandate another Agency to change one of its systems to guarantee interoperability between both domains.

4.3.2.3.1 Exchange of information between systems in the Eurojust domain

The future DCJ IT landscape is likely to evolve tremendously over the coming years. When more and more systems are introduced in a single domain, it becomes harder and harder to maintain the landscape efficiently.

A key issue many organisations face with their evolving IT landscape is that initially, they start from a small set of often siloed systems, with no connections (and thus no interoperability) between them. As data has become arguably the largest asset of any organisation, the seamless exchange and interpretation of this data across different system becomes ever so important. However, since systems have often evolved from siloed ways of working, it becomes difficult to integrate them.

A commonly used approach to guarantee interoperability between a set of systems covering both siloed and newly developed systems is to implement an integration layer 'on top'. This integration layer is responsible for managing the interconnectivity between different systems, and could even incorporate some reusable components, to further support the management of an organisation's ecosystem. Such an integration layer has the added benefit that it can incorporate 'translation' components that are able to communicate between systems that have different taxonomies. This is exceptionally beneficial in IT landscapes where systems have historically evolved in siloed mode, and thus often operate different data models and taxonomies.

The alternative would be to connect systems directly to other systems with 'point-to-point' connections. While this approach works well and is highly performant to connect a small number of systems, it quickly becomes unmanageable as soon as the number of systems starts to increase. Since the study proposes a scalable DCJ architecture, this approach is not taken forward when devising the future architecture due to interoperability constraints.

In the scope of the future DCJ IT landscape, this study proposes a variety of solutions. To ensure interoperability between these systems, an integration layer is advised for the reasons explained above. The use of such an integration layer would ensure the DCJ IT landscape can continue to evolve beyond what is proposed in this study.

While an integration layer, when implemented correctly, guarantees interoperability between systems, there is one more important aspect that should be considered when implementing the chosen solutions. Since many components would need to be developed from scratch all parties involved would benefit enormously if they standardise the taxonomy used within their ecosystem. Such standardisation would typically result in a higher level of interoperability, and, result in a higher performance since the aforementioned translator components would no longer be needed to translate messages between systems.

An example of such a taxonomy is the Universal Messaging Format (UMF) which is covered in more detail in a following section.

4.3.2.3.2 Exchange of information between systems belonging to different agencies and EU bodies

Achieving interoperability between systems belonging to JHA agencies and EU bodies is likely prove to be e challenging. This is mainly attributed to the fact that agencies and bodies have no direct control over the interfaces exposed by other parties.

In order to guarantee interoperability with systems located in other domains, it would be the responsibility of the agency or body concerned to integrate its own systems, possibly through the integration layer explained in the previous section. This scenario is largely similar to the one described in Section 4.3.2.2 in which Member States need to connect to the central domain.

However, it would be beneficial to agree on a common messaging format, e.g. the Universal Messaging Format (UMF), also mentioned above. This would ensure semantic interoperability between all EU systems which would greatly contribute to the overall level of interoperability between these systems. As explained in the section below, achieving such semantic interoperability across the entire IT landscape could prove to be a difficult exercise.

4.3.3 Ensuring semantic and technical interoperability

The concepts introduced in the previous sections show how interoperability can be achieved between various systems in the same or different domains with a high-level description. To fully understand how these would be put into practice, it is important to understand two concepts of interoperability:

- Semantic interoperability.
- Technical interoperability.

Semantic interoperability relates to the idea that elements, e.g. data fields, have the same meaning across systems when communicating. For example, if a system A wants to transmit a data record consisting of the field 'firstName' to system B, both systems need to have a common understanding of what this 'firstName' indicates. To ensure such semantic interoperability the data models of the databases themselves could be harmonised, or, as already touched upon in a previous section, the system on top of the database could translate its data model to this common format for communication purposes.

As should be clear from the text above, ensuring semantic interoperability between systems in a single domain could be challenging, let alone agreeing on a data format with systems in other domains. A common format that has been mentioned throughout the text is the Universal Messaging Format (UMF) - a candidate for ensuring semantic interoperability across the entire IT landscape considered here.

It must be noted however that UMF is still evolving. While it already consists of a strong baseline, each stakeholder has its own needs. Those needs are not always supported by the UMF. It is therefore advised that, if e.g. Eurojust wants to adopt the UMF in the future, it should join the UMF working group and actively contribute to its development. This way the further evolution of UMF can be influenced and so it can be ensured that it eventually covers the business needs of the agency. As an example, eu-LISA is also looking to adopt UMF as the taxonomy for its systems and has also taken up a position as active contributor to the format.

A second aspect is to guarantee technical interoperability. Without going into details that would be out of scope for this study, technical interoperability mainly relates to ensuring systems are technically able to communicate with one another, e.g. through an agreement on a protocol with which to communicate. Ensuring this could prove difficult, especially for existing systems, as it could be challenging, if not impossible, to change a tightly coupled legacy system's communication components to a new protocol.

Both semantic and technical interoperability heavily rely on a proper governance structure that actively monitors, maintains and evolves the information exchange channels based on the business needs. Especially in the specific situation of the European Union landscape, consisting of Member States and a variety of agencies and bodies, this governance would prove to be extremely important.

5 Solutions

This section presents the conceptual architecture and the general feasibility assessment of each of the solutions identified during the study.

Following the identification of business needs (through data collection activities with Member States) and the Expert Group Meeting of 13-14 January 2020, a certain number of solutions to solve the current needs in the domain of cross-border judicial cooperation were identified and prioritised.

Therefore, this section (in sub-sections 5.1 to 5.8) provides the designed conceptual architecture for the future Cross-Border Digital Criminal Justice ecosystem, as well as an in-depth assessment from a technical, security, legal and data protection perspective of seven solutions in particular:

- Secure Communication Channel
- Communication Tool
- Redesigned Eurojust CMS
- JIT Collaboration Platform
- Exchange of data between the JHA agencies & EU bodies
- Judicial Cases Cross-Check

Large Files Solution

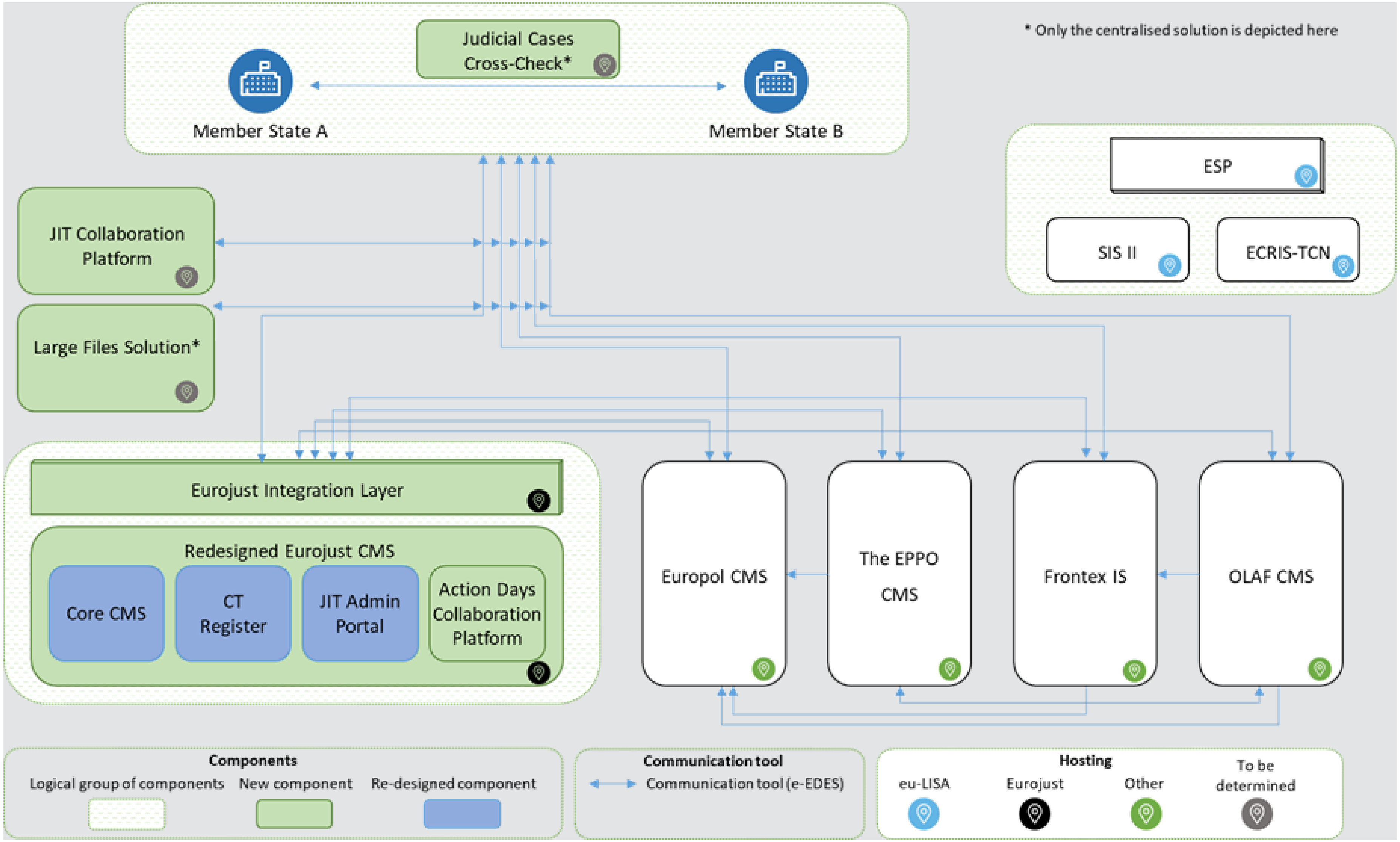
Some of these solutions (i.e. Secure Communication Channel, JIT Collaboration Platform, Judicial Cases Cross-Check and Large Files Solution) include several scenarios, which are individually assessed. Hence, the structure of the subsections below is not always the same across solutions. In addition, this section presents some additional solutions (in section 5.9) which were not analysed to the same extent as the seven key solutions above, namely:

- Common Services Platform
- Judicial One-Stop-Shop
- Training Platform
- Extended EJN Atlas (directory)
- CEF Building Blocks

5.1 Conceptual architecture

The figure below presents the conceptual architecture designed for the implementation of Cross-border Digital Criminal Justice.

Figure 5: Conceptual architecture



All the solutions depicted in Figure 5 are key to the creation of a Cross-Border Digital Criminal Justice ecosystem that will answer the needs of stakeholders involved in it, thereby improving cooperation in judicial criminal matters. The roles of the solutions are the following:

- Secure Communication Channel: The Secure Communication Channel is the technical infrastructure underlying all communications between different stakeholders in the ecosystem (be it at national or European level), to ensure information is exchanged digitally and securely to the maximum extent possible. The Secure Communication Channel would also underlie communication to and from the other six solutions presented. For the sake of clarity, it is no represented in the figure above.
- Communication Tool: The Communication Tool is a secure and easy to use interface for end-users in the ecosystem that would be used as the default way to exchange all messages and information related to cross-border criminal justice cases. This includes sending and receiving mutual legal assistance requests, as well as messages, and files. The Communication Tool would be used on top of the Secure Communication Channel.
- Redesigned Eurojust CMS: The Redesigned Eurojust CMS (and its different components, incl. the Integration Layer) are the core business systems needed for Eurojust to perform its mission to support cross-border criminal cases. As such, it would be used by internal Eurojust users, as well as external users (e.g. from Member States) and external systems (that would exchange information with systems in the Eurojust domain through the Integration Layer). The Redesigned CMS would be integrated with the Communication Tool, so that all interactions between Eurojust and its stakeholders are linked and secured.
- JIT Collaboration Platform: The JIT Collaboration Platform would be used to support all collaboration and exchanges of information in the context of a JIT, from set-up of a JIT through the JIT action days to closure of the JIT. It would be integrated with the Communication Tool, so that all interactions between JIT members are linked and secured.
- Exchange of data between the JHA agencies & EU bodies: The Exchange of data is a solution that would aim to further examine how to implement legislative requirements of hit/no-hit and exchange of information between JHA agencies and EU bodies. It would ensure further interoperability between the different parties involved (and their systems).
- Judicial Cases Cross-Check: The Judicial Cases Cross-Check would allow prosecutors and national authorities in Member States to search for information about ongoing judicial cases in other Member States. It would ensure an easier and more systematic way to identify links between cases at European level. It would be integrated with the Communication Tool, so that all interactions or exchanges of information following the identification of a link could be done digitally via the Communication Tool and a secured channel.
- Large Files Solution: The Large Files Solution is a complement to the Communication Tool, which would allow for exchange of large amounts of data digitally (when not possible to do so via the Communication Tool). It would also be integrated with the Communication Tool.

In addition, a critical issue to examine is that of the exchange and storage of EU classified information as this would have consequence on the design and accreditation of the systems processing this type of information. In particular, the processing of information classified as EU CONFIDENTIAL[29] has heavy consequences from a financial, resources and operational perspective. For instance, all systems accredited to process this type of information must have a TEMPEST accreditation, must have a boundary protection system, and their accreditation must be reviewed yearly and renewed every three years. As a consequence, the systems that are envisaged to

[29] EU information security classification levels are defined in Council Decision 2013/488/EU (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013D0488&from=EN)

process EU CONFIDENTIAL information are the systems that would be used to digitally exchange this information, i.e. the Secure Communication Channel, the Communication Tool and the Large Files Solution. As a second priority, it may be envisaged that the Redesigned Eurojust CMS and the JIT Collaboration Platform store such information as well. However, the decision to allow systems to process and store EU Classified information must be based on further analysis, and a balance of the additional opportunities and constraints that would be required. At a minimum, all solutions in the Cross-Border Digital Criminal Justice landscape must be accredited for the processing of EU RESTRICTED information.

Finally, it needs to be underlined that Figure 5 depicts only one of the implementation options for the Judicial Cases Cross-Check and the Large Files Solution (the centralised one).

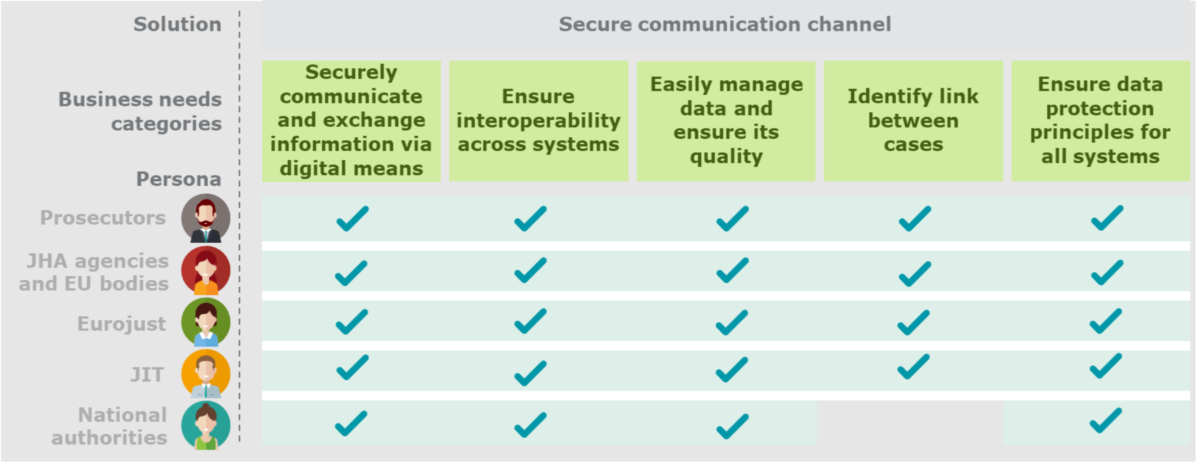
5.2 Secure Communication Channel

The need for a secure communication channel was clearly identified in our survey results, where the vast majority of respondents were in favour of establishing a robust and secure (i.e. encrypted and accredited) channel for communication. Indeed, 41% of respondents (to this question) consider having a secure communication channel as essential, while 39% believe it is necessary. Only a small minority, 7% of the respondents, mentioned that a communication channel is slightly necessary, and 1% stated this is not needed at all. 11% of the respondents have no opinion in the matter. Additionally, this need was confirmed during the field visits conducted in several Member States and the interviews conducted with JHA agencies and EU bodies.

Moreover, the following requirements were noted during the Expert Group meeting of 13-14 January 2020 and taken into account for the analysis below:

- There is a need to ensure security by design for any communication channel (or combination of channels) to be used in the context of Cross-Border Digital Criminal Justice.
- Should different communication channels be used by different stakeholders and in different Member States, the interoperability between all these channels should be ensured.
- The choice of communication channels to be used should take into account recent investments made by the Member States.

Figure 6: Secure communication channel - Business needs mapping



Solution	Secure communication channel				
Business needs categories	Securely communicate and exchange information via digital means	Ensure interoperability across systems	Easily manage data and ensure its quality	Identify link between cases	Ensure data protection principles for all systems
Persona					
Prosecutors	✓	✓	✓	✓	✓
JHA agencies and EU bodies	✓	✓	✓	✓	✓
Eurojust	✓	✓	✓	✓	✓
JIT	✓	✓	✓	✓	✓
National authorities	✓	✓	✓		✓

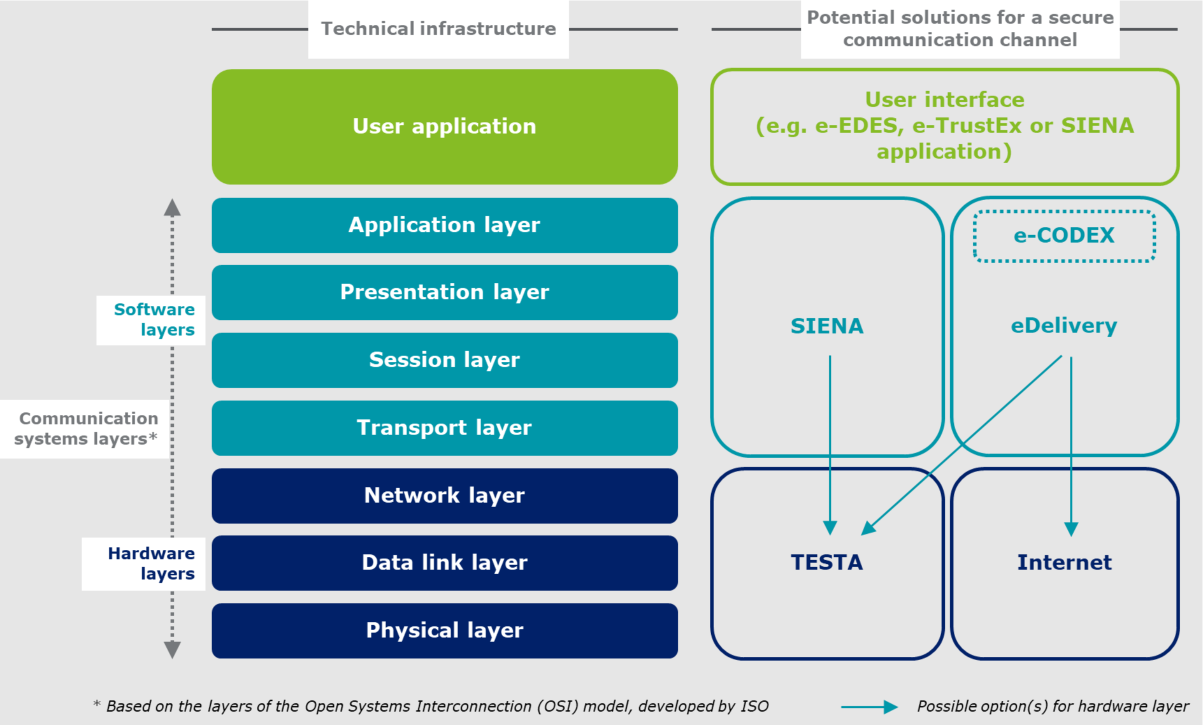
Therefore, this section investigates the possible options to implement a secure communication channel between the different stakeholders to exchange messages, information and evidence electronically across borders in a secure way, as well as to discover links (or "hits") between cases and communicate following the discovery of a link.[30] Stakeholders involved include national authorities, prosecutors in Member States, JIT members as well as JHA agencies and EU bodies. As well as covering flows between different stakeholders, the secure communication channel must cover exchanges of non-classified and classified data. Indeed, this channel would be used to

[30] Please refer to sections 5.6 and 5.7 for more information about the identification of links between cases at the level of the JHA agencies, EU bodies and Member States respectively.

exchange classified information (up to the level of EU CONFIDENTIAL). In short, the secure communication channel would support all exchanges of data in the area of criminal justice.

The definition of a secure communication channel includes the combination of all technology assets needed to implement end-to-end secure communication. Therefore, as shown in the figure below, the solutions examined below refer to the hardware, and/or the software and/or the services[31] (when applicable) required for the communication channel. The solutions examined are based on already existing communication channels in the EU which could be re-used for the purpose of cross-border judicial cooperation.

Figure 7: Communication channels layers



* Based on the layers of the Open Systems Interconnection (OSI) model, developed by ISO

Consequently, the communication channel options to be used in the context of Cross-Border Digital Criminal Justice could be based either 1) on the eDelivery Building Block (possibly using the e-CODEX connector), 2) on the TESTA network[32] or 3) on the SIENA network. These solutions are described in detail below, and different scenarios for their re-use in the context of the Digital Criminal Justice project are assessed from a technical, security, legal and data protection perspective. One should note that this report contains a high level preliminary assessment of the different options, which should be further detailed before a decision on the communication channel(s) to re-use is taken.

[31] In computer networking, a network service is an application running at the network application layer and above, that provides data storage, manipulation, presentation, communication or other capability which is often implemented using a client-server or peer-to-peer architecture (source: Wikipedia). Application services and other network services are included in the "Application layer" in Figure 7.

[32] TESTA is a generic service provided under the ISA² Programme, available to all national and European administrations.

As far as the EIF and the Sharing and re-use framework are concerned, this solution addresses the following recommendations:

Table 8: EIF and Sharing and re-use recommendations addressed by the secure communication channel solution

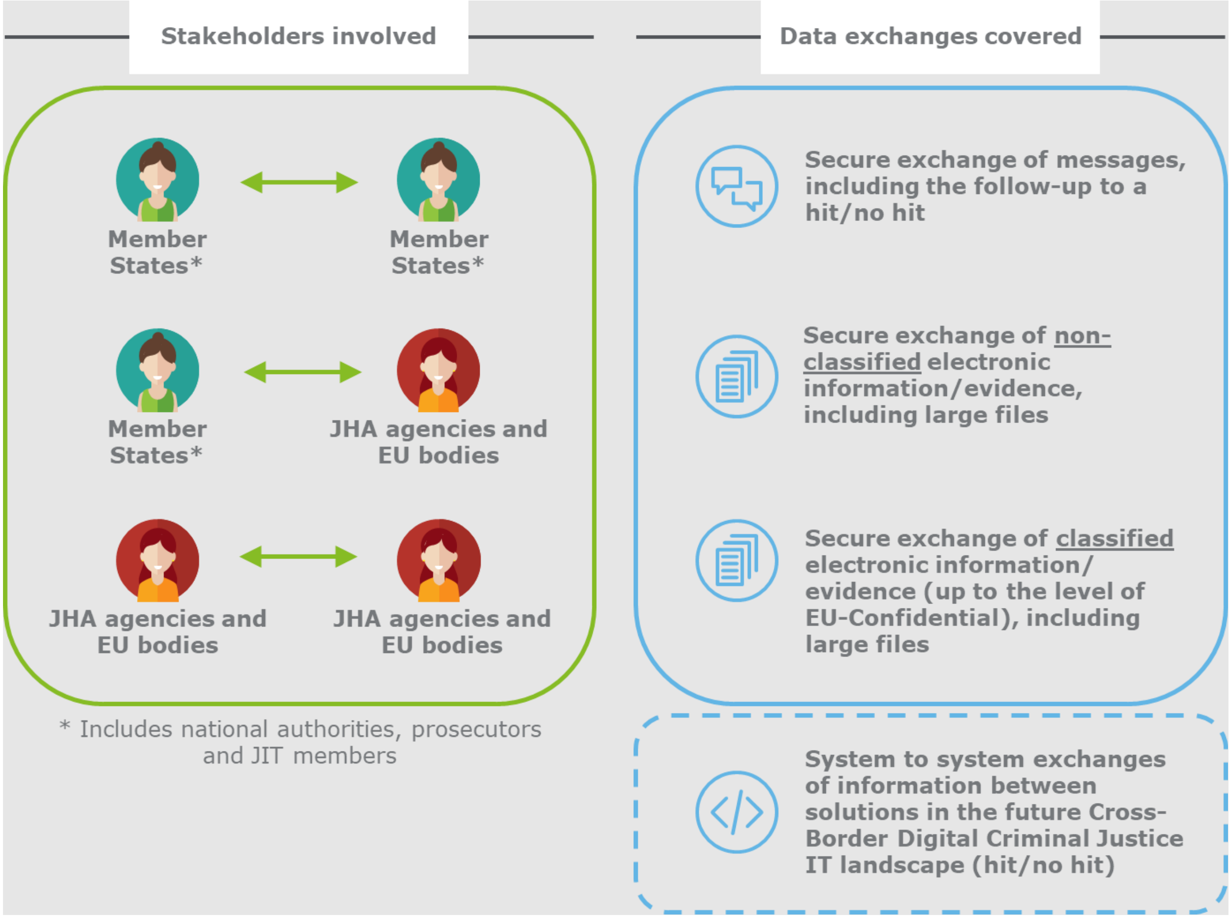
European Interoperability Framework	Sharing and re-use framework
#5: Ensure internal visibility and provide external interfaces for European public services	#3: Communicate your needs
#6: Re-use and share solutions, and cooperate in the development of joint solutions when implementing European public services	#4: Define set of requirements supporting common business processes
#8: Do not impose any technological solutions on citizens, businesses and other administrations that are technology specific or disproportionate to their real needs	#10: Decide the type of rights' attribution approach to be used as early as possible and inform all involved
#10: Use multiple channels to provide the European public service, to ensure that users can select the channel that best suits their needs	#18: Check the reusability of existing solutions before developing a new one
#15: Define a common security and data protection framework and establish processes for public services to ensure secure and trustworthy data exchange between public administrations and in interactions with citizens and businesses	
#17: Simplify processes and use digital channels whenever appropriate for the delivery of European public services, to respond promptly and with high quality to users' requests and reduce the administrative burden on public administrations, businesses and citizens	
#19: Evaluate the effectiveness and efficiency of different interoperability solutions and technological options considering user needs, proportionality and balance between costs and benefits	
#30: Perceive data and information as a public asset that should be appropriately generated, collected, managed, shared, protected and preserved	
#46: Consider the specific security and data protection requirements and identify	

measures for the provision of each public service according to risk management plans

5.2.1 Presentation of the possible solutions

As explained in the introduction (and as shown in the figure below), there are numerous different use cases for the secure communication channel in the context of Cross-Border Digital Criminal Justice. Indeed, this channel must enable the secure exchange of different types of information (classified or non-classified, "normal" messages or files), between many different stakeholders across the EU at regional, national or European level. It must also enable system to system exchanges of information (which are not triggered by a human) between the solutions in the future Digital Criminal Justice landscape. An overview of these solutions is available in section 5.1 of this report.

Figure 8: Use cases for the secure communication channel


Stakeholders involved
Member States*
Member States*
Member States*
JHA agencies and EU bodies
JHA agencies and EU bodies
JHA agencies and EU bodies
* Includes national authorities, prosecutors and JIT members
Data exchanges covered
Secure exchange of messages, including the follow-up to a hit/no hit
Secure exchange of non-classified electronic information/evidence, including large files
Secure exchange of classified electronic information/evidence (up to the level of EU-Confidential), including large files
System to system exchanges of information between solutions in the future Cross-Border Digital Criminal Justice IT landscape (hit/no hit)

This section presents a combination of the different solutions that could be re-used for the implementation of a secure communication channel supporting cross-border collaboration in the field of criminal justice, namely:

- The TESTA network that provides the physical, data link and transport layers.
- The SIENA platform which works on top of TESTA and offers a secure communication channel (the SIENA network) and is completed with the SIENA application in the user application layer.
- The eDelivery Building Block that works both on top of TESTA or the internet and which, at the application layer, supports connectors such as e-CODEX for user applications.

In sections 5.2.2 to 5.2.5 several scenarios for the re-use of these solutions are assessed.

5.2.1.1 eDelivery[33]

The eDelivery Building Block is a message exchange solution for public administrations to exchange data and information electronically with other public administrations, businesses and citizens in an interoperable, secure, trusted and reliable way.

eDelivery was initially designed to be decoupled from private networks and offer the required security level over the internet in order to serve both G2G[34] and G2B[35] communication. At its core, eDelivery consists of technical specifications and implementation guidelines to set up a message exchange solution that is compliant with the OASIS AS4 (Applicability Statement 4) messaging protocol and the security requirements of the eIDAS regulation. This means that eDelivery users can securely exchange messages with all participants in a given eDelivery "network" (each participant has to install an eDelivery gateway, and these access points form the "eDelivery network"). eDelivery can be implemented by public administrations in different ways: either by developing their own compliant solution, by reusing a compliant solution available on the market, or by reusing the reference implementation developed by the European Commission (Domibus). It is to be noted that several JHA agencies (including Eurojust) and some Member States do not yet have an eDelivery connection node (i.e. a Domibus access point) for use in the domain of Justice & Home Affairs (they may also have an eDelivery connection used in another context).

The eDelivery building block is designed to offer substantial security at the transport layer, so that the internet can be used as a communication channel. However, it can also be used over private networks, e.g. TESTA (please refer to Figure 7 above). The added value of using TESTA as the underlying network for eDelivery is the managed services and SLAs offered by TESTA, which would not be offered by other internet service providers (see TESTA features below). Regarding security, eDelivery is based on Transport Layer Security, which is ensured with software measures, while the TESTA network implements the IPSec protocol supported at the hardware level. However, currently eDelivery cannot be used to exchange EU classified information, as it is not accredited to do so.

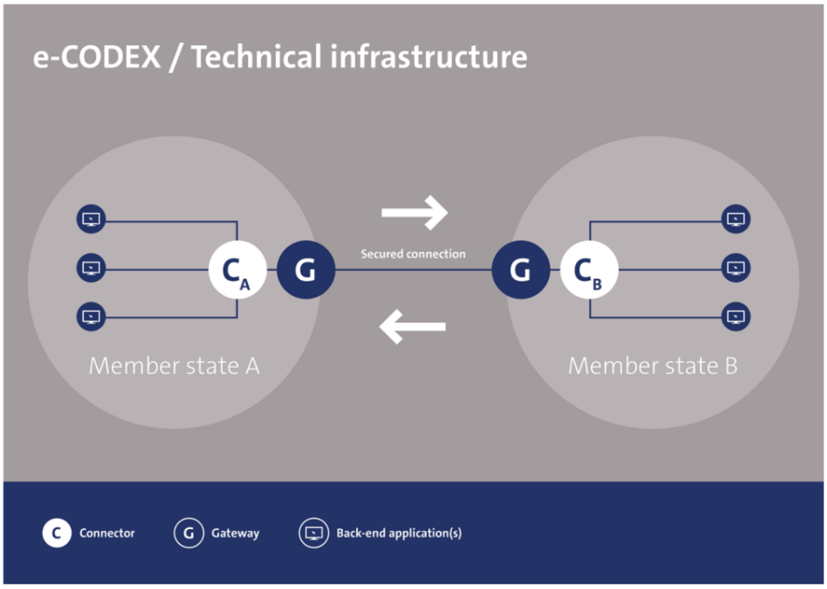
5.2.1.1.1 e-CODEX connector[36]

eDelivery can be used together with different connectors, which may be built, bought on the market, or re-used. One of these connectors is the e-CODEX connector, implemented and offered by the e-CODEX consortium (composed of several EU Member States and third countries, European chambers of legal professionals and other institutions). Currently, eDelivery and e-CODEX are used in the context of the e-Evidence Digital Exchange System project (e-EDES)[37], and e-CODEX is the proven and re-used connector in the judicial domain.

[33] Please refer to section 5.9.5.1 for a detailed description of eDelivery.
[34] Government to Government (G2G)
[35] Government to Business (G2B)
[36] For more information about e-CODEX, please refer to https://www.e-codex.eu/.
[37] The e-Evidence Digital Exchange System project is detailed in section 5.3.

The e-CODEX connector is used to connect the eDelivery access point (or "gateway")[38] to national and European IT systems in the e-Justice domain. An e-CODEX connector has to be installed by every participating country or institution, after which the operation of the system is also managed by participants. A high level view of the e-CODEX technical infrastructure is shown in the figure below.

Figure 9: e-CODEX technical infrastructure



In terms of functionalities, the gateway (i.e. the eDelivery access point) mainly serves to send/receive messages to/from backend systems, to sign and encrypt messages, and to transfer messages to other gateways. It cannot see the content of the messages or documents shared. The e-CODEX connector mainly serves to communicate with the national systems. It is a flexible solution as multiple gateways could be used for different institutions in one Member State (e.g. if there are different security requirements in these institutions). Moreover, it is possible to connect multiple connectors to one gateway (e.g. if different backend solutions are used to receive different types of messages).

Security is ensured at multiple levels: at transmission level (through the use of the TLS cryptographic protocol), at message level (though the use of the AS4 and WS (Web Services) messaging standards to securely exchange messages over the internet) and at document level (through the use of digital signatures). However, currently e-CODEX cannot be used to exchange EU classified information, as its underlying infrastructure (eDelivery) is not accredited to do so.

In addition, an important concept in the context of e-CODEX is that of the "Circle of Trust". Indeed, e-CODEX does not change existing solutions or laws in participating countries. Therefore, the Circle of Trust concept means that participating countries accept the legal validity of documents, and of information on identity and signatures coming from other countries in the network. Moreover, to

[38] Having access to a gateway is a pre-requisite to install e-CODEX, although the gateway itself is not managed by e-CODEX.

cope with the different legal systems, the e-CODEX technical infrastructure includes a methodology to ensure the mutual equal interpretation of legal terms.

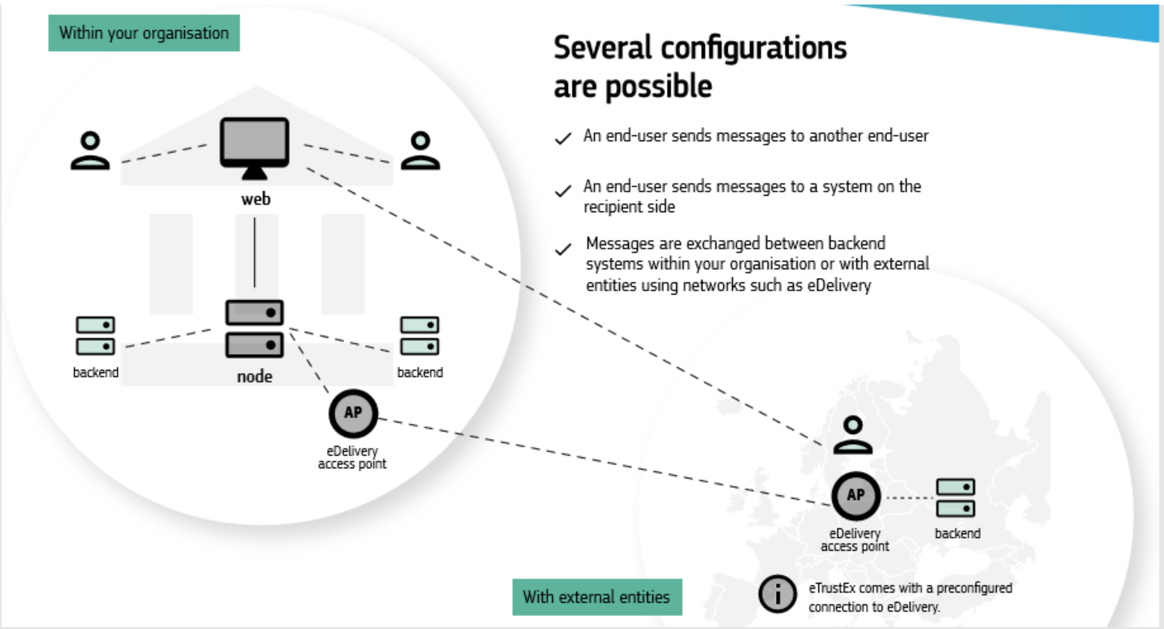
Finally, it is noted that by 2021, all Member States will have e-CODEX installed in the context of e-EDES. The amount of e-CODEX connectors (and underlying access points) across the different Member States will likely not be consistent, with some having only a few connectors and others having many.

Therefore, the implementation of the complete eDelivery implementation in any EU JHA body/agency or Member State (including the Domibus access point (or any other AS4-conformant software), and the e-CODEX connector) could constitute a future proof solution for the automated exchange of structured information between all stakeholders. In such a case, any form of structured or unstructured information could be exchanged between Eurojust, Member States and any other bodies/agencies which can connect and implement the eDelivery/e-CODEX architecture.

5.2.1.1.2 eTrustEx web application

eTrustEx is an open-source platform offered to Public Administrations at European, national and regional level to set up a secure exchange of any type of data between end-users or system-to-system. The platform is a web application that is based on eDelivery (it comes with a pre-configured connection to eDelivery), and offers an interface similar to that of an email client. Therefore, it is considered in this study as an option for a reusable user interface in case eDelivery is chosen as a communication channel for cross-border criminal justice cooperation. The figure below shows how eDelivery can be implemented.

Figure 10: eTrustEx configuration



Several configurations are possible

- ✓ An end-user sends messages to another end-user
- ✓ An end-user sends messages to a system on the recipient side
- ✓ Messages are exchanged between backend systems within your organisation or with external entities using networks such as eDelivery

eTrustEx comes with a preconfigured connection to eDelivery.

The application can be used standalone or as a managed service (or SaaS[39]) offered by DIGIT as part of the Reusable Solutions Platform offering (more specifically, the EU Send offering).

1. Standalone version of the open eTrustEx web application.[40]

This application can be deployed as a standalone implementation having the features for uploading structured and unstructured information (documents, mails) and for exchanging e-mails (inbox/outbox) for end users. This could then be integrated with CMS of the various stakeholders (at national and European level) for the consumption of the received information.

2. Managed service of eTrustEx at DIGIT with the EU Send offering.

The EU Send offering is part of the Reusable Solutions Platform[41], which is a set of managed services offered by the European Commission (DG DIGIT) to EU Institutions and Agencies. EU Send is used to exchange electronic data and documents in a secure and reliable way with other EU Institutions, Agencies and any private or public entity in the Member States, or elsewhere in the world. EU Send offers eDelivery as a managed service as part of its service offering, as it operates the sample implementation developed by DIGIT (Domibus). This option is not preferred since the data exchanged via eDelivery would transit via the DIGIT datacentre.

In addition, eTrustEx cannot be used to exchange EU classified information, as its underlying infrastructure (eDelivery) is not accredited to do so.

In conclusion, whereas the scope of eTrustEx covers several policy domains, in the context of this study eTrustEx cannot be considered as an alternative to e-CODEX for JHA agencies and EU bodies and Member States to securely exchange messages and information using the eDelivery digital infrastructure (including EU classified information). Therefore, given the additional advantages given by e-CODEX (notably, the Circle of Trust between participants in the network), and the planned future developments that are based on e-CODEX (in the context of e-EDES), e-CODEX is the preferred solution to be re-used together with eDelivery.

5.2.1.2 TESTA network services

TESTA is the private IP-based network of the European Union. It uses the Internet Protocol (IP) to ensure universal reach, but is operated by the European Commission separately from the internet. The network has been upgraded several times through the years. Its four generations (TESTA, TESTA II, sTESTA and TESTAng) were developed respectively under the IDA, IDABC, ISA and ISA2 programmes managed by DIGIT. DIGIT is also the technical system owner for TESTA. The current framework contract under which TESTA is operated ends in June 2020. Once the tendering process led by DIGIT comes to an end, the successor of TESTAng (which will be the 5th generation of TESTA) will be implemented. According to DIGIT, the service catalogue and costs of TESTA (which are described in the sections below), as well as possibly the underlying technology, will likely change with the implementation of the 5th generation. However, no information is available yet on these changes.

[39] Software as a Service

[40] See: https://joinup.ec.europa.eu/solution/open-e-trustex

[41] More information here: https://webgate.ec.europa.eu/fpfis/wikis/pages/viewpage.action?spaceKey=DIGITD3&title=Digital+Solutions.

TESTA is adopted in over 120 policy projects & services. There are 26 applications in various EU policy domains, mostly supporting exchanges between all the Member States, while there are 9 Services at the Member States level and 90 Services for European bodies.

Indeed, TESTA is a preferred solution for pan-European information exchange between administrations requiring guaranteed service levels for network availability, performance and/or security. It interconnects all EU Institutions, EU Agencies, Member States Administrations and European Economic Area (EEA) countries. As far as the judicial world is concerned, TESTA is available in all 27 Member States, 2 EFTA countries (Norway and Iceland), the UK and Liechtenstein. More specifically, out of 31 countries[42]:

- 19 countries are declaring their entities (Ministry of Justice, Prosecution Offices) to be already connected to their National Network, therefore these entities can access TESTA.
- 2 countries are declaring some of their entities (Ministry of Justice, Prosecution Offices) to be already connected to their National Network, which can therefore access TESTA, and some entities not yet connected to their National Network.
- 7 countries are declaring their entities (Ministry of Justice, Prosecution Offices) to be ready to be connected to their National Network, therefore they could access TESTA if they request it and configuration is done.
- 3 countries are declaring their entities (Ministry of Justice, Prosecution Offices) as not yet connected to their National Network, but it could be feasible if they request access (the procedure to request access varies per country).

TESTA's services could be re-used in the context of Digital Criminal Justice as the backbone for the secure exchange of e-mails and case-related information, but it would require commitment from the Member States authorities to connect all relevant entities at national level. Third countries, however, would still not be able to use these services. TESTA is also available in the JHA agencies and EU bodies, which are connected to the EuroDomain (or specific domains), and its services could be easily used for the exchange of information among them and the Member States, if the difficulties currently experienced were to be solved. These difficulties are described in section 3.1 and include the limitation in the size of messages that can be exchanged, the fact that information cannot be securely exchanged with all relevant entities at Member State level (as they may not be connected to the National Network), etc.

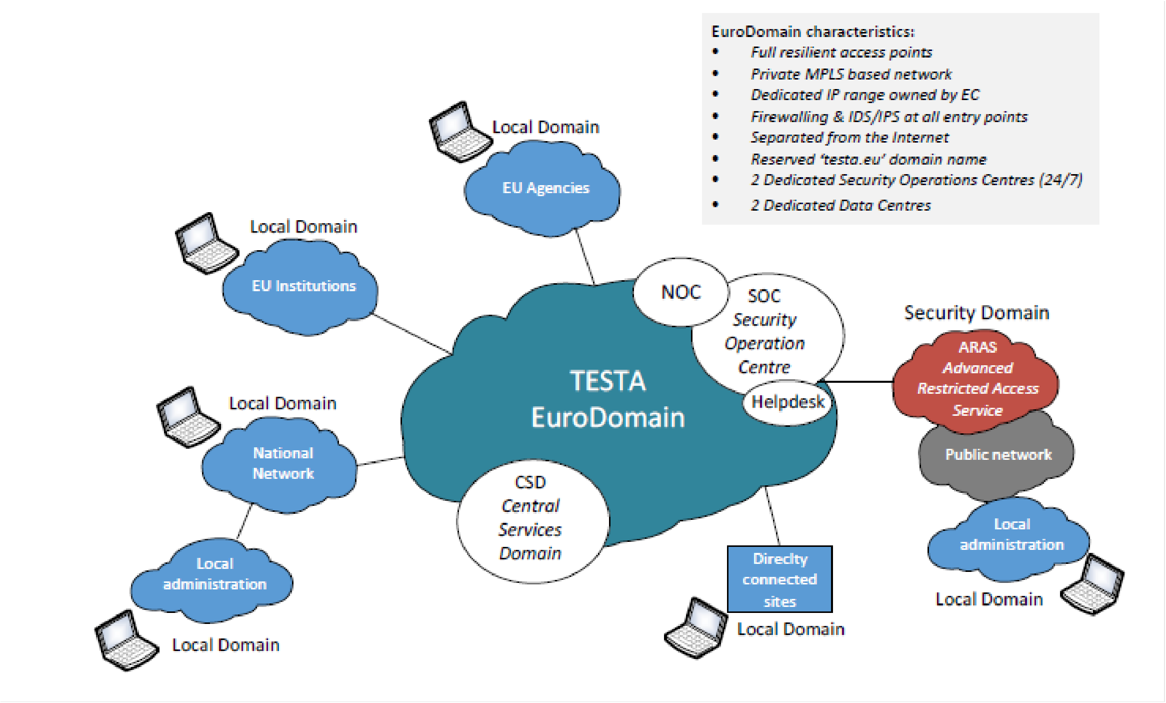
Although the European Commission implemented TESTA for the exchange of non-classified information, the TESTA infrastructure has been built to be subject to a security accreditation process to allow the exchange of EU classified information up to the EU RESTRICTED level. The TESTA network itself does not cover the end-to-end needs for security at the end user level, meaning EU RESTRICTED accreditation is achieved only from gateway to gateway. The end-to-end security could be provided by additional devices and cryptographic software at the end user's side (in JHA agencies and EU bodies, and Member States). Moreover, IT applications using TESTA services may have their own security requirements covering access control and data sensitivity levels. Each administration will seek accreditation for its LDCP (Local Domain Connection Point) in accordance with the Council Decision 2013/488/EU of 23 September 2013.[43]

The sub-sections below provide a more detailed and technical description of the TESTA infrastructure.

[42] The status of the TESTA connection provided by DIGIT's TESTA team dates from 28/11/2019.

[43] https://www.consilium.europa.eu/en/council-eu/preparatory-bodies/security-committee/

Figure 11: TESTA Infrastructure[44]


EuroDomain characteristics:
Full resilient access points
Private MPLS based network
Dedicated IP range owned by EC
Firewalling & IDS/IPS at all entry points
Separated from the Internet
Reserved 'testa.eu' domain name
2 Dedicated Security Operations Centres (24/7)
2 Dedicated Data Centres
Local Domain
EU Agencies
Local Domain
EU Institutions
Local Domain
National Network
Local administration
Local Domain
TESTA EuroDomain
NOC
SOC Security Operation Centre
Helpdesk
CSD Central Services Domain
Security Domain
ARAS Advanced Restricted Access Service
Public network
Local administration
Local Domain
Direclty connected sites
Local Domain

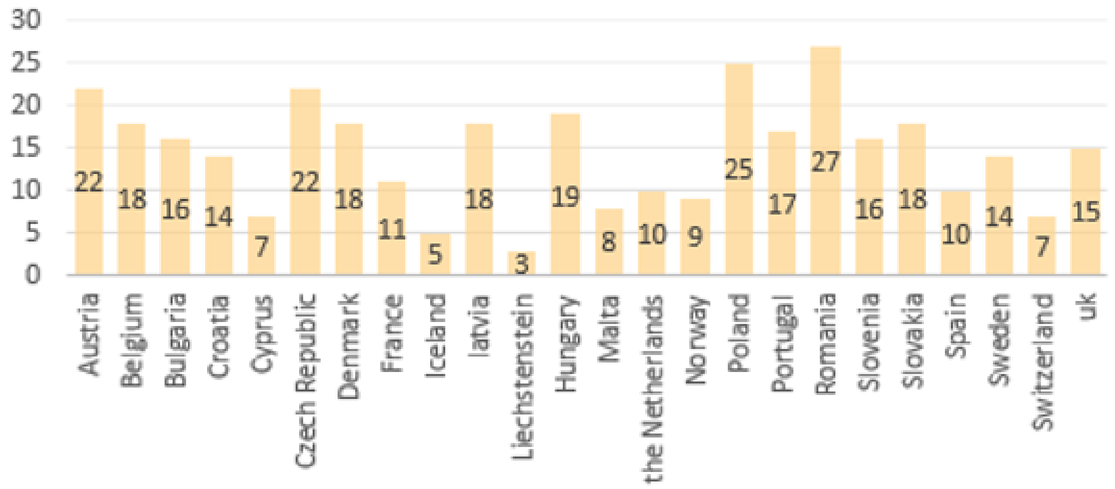
5.2.1.2.1 EuroDomain

The EuroDomain is a central TESTA Building Block that allows data transfer and services between TESTA stakeholders such as the European Commission, various European Agencies, other European Institutions, Member States' administrations, the Security Operation Centre (SOC) and the Central Services Domain (CSD). All connections to the EuroDomain are encrypted using certified IPSec technology. DIGIT is responsible for the EuroDomain[45], including its Central Services and the Security Operation Centre (SOC).

[44] Source : https://ec.europa.eu/isa2/sites/isa/files/testa_overview_-_july_2018.pdf

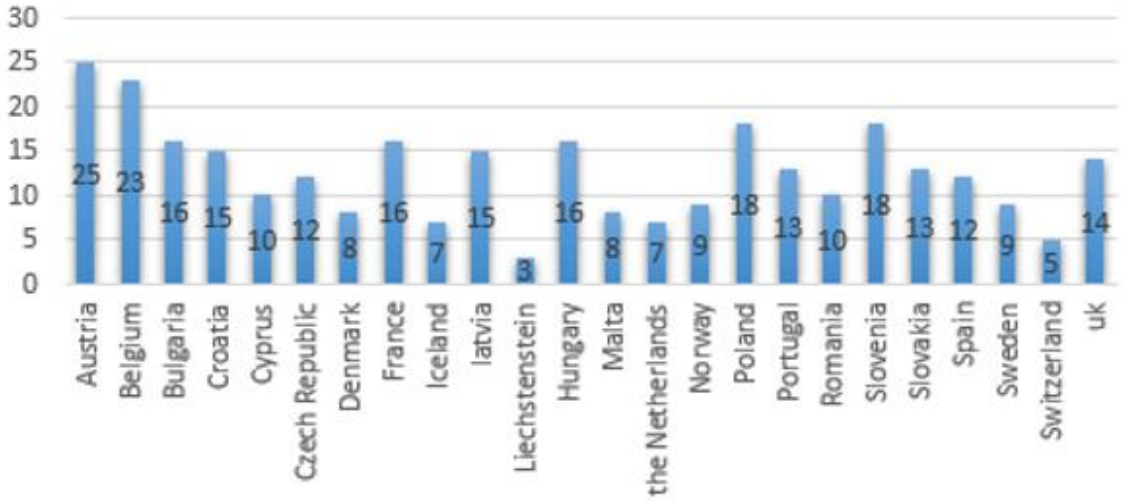
[45] A domain is a grouping of multiple private computer networks or hosts within the same infrastructure. Domains are identified using a domain name. (Source: Wikipedia) The TESTA network covers several domains: EuroDomain, which the most used, and other domains dedicated to specific users (for Europol, VIS, SIS II and the Council of the EU).

Figure 12: Number of public administrations using the EuroDomain national gateway



Source: DIGIT 2019

Figure 13: Number of information systems using the EuroDomain national gateway



Source: DIGIT 2019

5.2.1.2.2 Local Domains

The Local Domains are the domains related to a specific end-user. They are all specific and are typically based on various LAN architectures and vary from one Local Domain to another. The EuroDomain interconnects various Local Domains and provides them with central services via the Central Service Domain.

In addition to firewalls and encryption devices, IT applications using TESTA services may have their own security requirements covering access control and data sensitivity levels. Each administration would seek accreditation for its LDCP (Local Domain Connection Point).

5.2.1.2.3 Services and features

Central Service Domain (CSD)

The Central Service Domain (CSD) provides facilities for EU users to exchange data. It contains dedicated services such as DNS, (secured) Mail, SFTP, NTP, Time stamping and Web services (web portal, web cooperation services). The portal provides access to the end-users and administrations by offering a view of the set of services that are accessible over TESTA and giving information on how to obtain these services. Information concerning the configuration and the performance of the network can also be retrieved and managed.

Network Operation Centre (NOC)

The Network Operation Centre operates the provision of network transport (Backbone services, local loop services and the monitoring thereof). The NOC is available on a 24/7 basis, 365 days a year.

Security Operation Centre (SOC)

Includes crypto management, firewall management, management of all the services that are protected by the TESTA security environment e.g. mail relay, secured mail, secured FTP, NTP, DNS, web portal, web cooperation tool, Advanced Restricted Access VPN management. The management infrastructure of the SOC is dedicated to TESTA and is responsible for ensuring quality and operational support for the TESTA EuroDomain Services. The personnel assigned to operate these dedicated services have a minimum security clearance of National Confidential.

Helpdesk services

The helpdesk is acting as a single point of access that registers and coordinates all incidents problems and requests coming from authorised users (helpdesk, support teams of the connected local domains or helpdesks of application owners). The Helpdesk is available on a 24/7 basis, 365 days a year and registers requests via telephone, mail and web portal. The personnel assigned to operate the helpdesk have a minimum-security clearance of National Confidential.

5.2.1.3 SIENA platform

SIENA is a communication channel built and maintained by Europol, which is dedicated to information exchange across borders in the law enforcement community. Europol's SIENA platform is a secure tailor-made messaging system implemented and deployed over a dedicated TESTA domain managed by Europol. Therefore, SIENA cannot be considered as a communication channel only, as it also includes a custom application of Europol through which information can be exchanged up to the EU CONFIDENTIAL level, given that the required cryptographic equipment is in-place along with the SIENA software.

In this study, it is not recommended to re-use Europol's SIENA application for exchanging information in the context of judicial cooperation, but rather to re-use the specific TESTA domain managed by Europol and the associated SIENA hardware (i.e. cryptographic equipment), which are accredited to exchange EU classified information. Indeed, the information exchanged using the Europol's SIENA platform is mostly visible to Europol (unless specific security configurations are made, e.g. in terms of mailbox security), and furthermore the re-use of the SIENA application in judicial co-operation cannot be easily decoupled from its use in police co-operation. An alternative option could be to re-use SIENA only for the exchange of EU CONFIDENTIAL information since the EU CONFIDENTIAL security requirements are not supported by the other communication channels examined.

During the fieldwork conducted in several Member States, it was found that SIENA is rarely used in cases where EU classified information must be exchanged with judicial practitioners in other countries due to practical constraints. Indeed, to do so, judicial practitioners have to physically move to the SIENA endpoint locations in their Member State, i.e. the Europol National Units which are mostly located at the Ministry of Interior or the police. The fixed locations from which the practitioners can send/receive EU CONFIDENTIAL information are located there. In order to connect judicial authorities to SIENA for its re-use in the context of Cross-Border Digital Criminal Justice, three options could be envisaged:

- Option 1: This option is to keep to the status quo. However, as explained in the paragraph above this option is unsatisfactory to judicial practitioners having to exchange EU classified information. Moreover, it is unsustainable given that the volume of classified information exchanged electronically would increase in the future Cross-Border Digital Criminal Justice ecosystem.
- Option 2: Judicial authorities are connected to SIENA through the Europol National Unit, making use of the national network. However, it must be noted that to exchange EU classified information, the national network must be accredited and users must have a security clearance.
- Option 3: A separate secure line (with the associated rack) is set up in a second location in the Member State. Although this option is feasible, it is not preferred as it is more cumbersome and entails additional costs for the rack and associated security equipment.

Although option 2 is preferred by Europol as it would be easier to configure for them, both options 2 and 3 would entail an effort for all Member States to accredit their national network to exchange EU classified information. Indeed, every single judicial body would have to have their computer systems accredited to handle EU classified information, and every single workstation must offer TEMPEST protection.[46]

The sub-sections below give more information about the functioning of the SIENA network.

5.2.1.3.1 Access to SIENA

Regarding connections with Member States, Europol is responsible for connecting the Europol HQ to Europol National Units located in each Member State and financing the set-up of this connection.[47] To set up a connection, a secure rack (with encryptions and other IT equipment) must be set up in the Europol National Unit. Usually these racks are located in police authorities (i.e. the Ministry of Interior), but sometimes also in customs authorities (i.e. Ministries of Finance).

National Competent Authorities can also obtain access to SIENA. The extension of the SIENA connection to the competent authorities has to be arranged by the countries themselves and is dependent on the national network in place. Currently, 1700 competent authorities are connected to SIENA. These authorities are not limited to the police, and may also include custom authorities, some judicial authorities (in the context of the Prüm Decision), etc. The majority of the competent authorities are connected to SIENA via an agreement with the Europol National Unit (if they are not part of the police).

[46] According to Council Security Rules 2013/488/EU Article 9.5.

[47] The cost of a rack is approximately € 20,000 – 25,000 and is financed by Europol. The cost of the secure lines maintenance varies from country to country, because the costs are dependent on the set up of the national networks. The expenses spent on the maintenance of connection between Europol and countries' competent authorities are usually very low because, in most of these cases, the countries use the internet instead of leased lines.

In addition to national authorities, the EU Institutions, JHA agencies and EU bodies that have access to SIENA are the European Commission, Eurojust, EUNAVFORMED, EMCDDA, OLAF[48], ECB, ECDC, CEPOL, Frontex, CSDP missions, Interpol, WCO and INTCEN. Some of these institutions are not connected online to SIENA, meaning that a message arrives to Europol and then it has to be forwarded to OLAF via another secure mean. However, it is foreseen that in the near future OLAF and the EPPO would get an online connection to SIENA.

5.2.1.3.2 Usage of SIENA

SIENA can be used to exchange non-classified (referred to by Europol as Basic Protection level), as well as classified information (up to level of EU CONFIDENTIAL). However, its configuration/set-up varies based on the required security level:

1. Basic Protection Level: For the exchange of non-classified information and information classified up to the Basic Protection Level (BPL). This is a new SIENA channel currently being built by Europol and for which lower security is required.
2. EU RESTRICTED: For exchange of information classified up to the EU RESTRICTED level.
3. EU CONFIDENTIAL: For exchange of information classified up to the EU CONFIDENTIAL level. This variant has restrictions because it can only be accessed from a fixed location (i.e. there are dedicated end user machines at fixed location – no portable devices).

Currently, there is a limit on the size of messages that can be sent over SIENA. The maximum size of a message is 50 MB, and there is no limit on the number of attached files. For this reason, large files must be exchanged using Europol's Large File Exchange System (more information in section 5.8.1). However, Europol is currently developing an upgraded uploading mechanism that will accept 50 MB per file and a few hundred MB per message.

Moreover, SIENA has implemented the concept of the digital case file identifier, which is applied at two levels: message and case. Every message and case has a unique identifier. Every message is linked to one (or several) case(s) and every case can be linked to different messages, it is not possible to send a message not related to a case. This means it is possible to trace the information exchange flows. In practice:

- After a request is received, a case is created with a unique identifier (or case marker).
- All messages sent include the case marker in their identification number.

All exchanges of information using the SIENA platform are audited and monitored by Europol.

5.2.1.3.3 Confidentiality, integrity and availability

The security of SIENA is ensured by Europol at different levels:

- Accreditation:

The SIENA network and platform have been accredited up to the EU CONFIDENTIAL level, which requires two-factor authentication access. However, SIENA is also accessible to EU RESTRICTED (or equivalent) networks. Moreover, in the future, it will be possible to exchange information via SIENA by using unaccredited national networks.

Currently, around 95% of the information exchanged is on the Basic Protection Level (BPL), 5% of the SIENA messages are EU RESTRICTED and less than 1% of the messages exchanged are

[48] For OLAF, the technical implementation of the connection is still under construction.

classified as EU CONFIDENTIAL. Almost all EU agencies' mailboxes are configured on the EU-R level and only a few mailboxes are configured on the BPL.

- Accounts, roles and permissions:

Individual users have their own accounts and are assigned different roles and permissions. There is also a control mechanism that allows for checking the access to SIENA cases. Moreover, actions such as logging of all transmission and auditing further ensure the security of the SIENA application.

- Mailbox security:

It is possible to have separate mailboxes via the SIENA application, which would not be visible to the law enforcement authorities in charge of SIENA. This is currently done in the field of counter-terrorism.

5.2.2 Technical assessment

The technical assessment analyses several scenarios for the re-use of existing communication channels in the context of cross-border judicial cooperation, according to a number of business and technical criteria. It is important to note that the scenarios are not mutually exclusive. Indeed, there may be a need for a separate channel to be used for the exchange of classified data. Also, different channels may be used by different stakeholders due to factors such as the ease to access each channel, the secure communication networks in place at national level, etc.

The re-use scenarios examined are:

- **Scenario 1 – eDelivery (with e-CODEX connector) over the internet:** This scenario assesses the re-use of eDelivery with the e-CODEX connector, as described in the "e-CODEX connector" section above
- **Scenario 2 – eDelivery (with another connector) over the internet**: This scenario assess the re-use of eDelivery alone, as described in the "eDelivery" section above
- **Scenario 3 – eDelivery (with e-CODEX connector) over TESTA EuroDomain:** This scenario is a combination of the eDelivery (used with the e-CODEX connector) and TESTA scenarios
- **Scenario 4 – eDelivery (with another connector) over TESTA EuroDomain:** This scenario is a combination of the classic eDelivery and TESTA scenarios and could bring additional benefits, for instance in terms of improved availability
- **Scenario 5 – TESTA:** This scenario is based on the description in the "TESTA network services" section above, and assesses the re-use of the TESTA EuroDomain versus a dedicated (local) domain (differences are highlighted where relevant in the table below)
- **Scenario 6 - SIENA:**– This scenario is based on the description in the "SIENA platform" section above, and assesses the re-use of the SIENA network (which as a specific TESTA domain managed by Europol) and the associated hardware (i.e. cryptographic equipment)

Table 9: Secure communication channel - Technical assessment

Criteria	**Scenario 1 – eDelivery (with e-CODEX connector) over the internet**	**Scenario 2 – eDelivery (with another connector) over the internet**	**Scenario 3 – eDelivery (with e-CODEX connector) over TESTA EuroDomain**	**Scenario 4 – eDelivery (with another connector) over TESTA EuroDomain**	**Scenario 5 – TESTA**	**Scenario 6 – SIENA**
Scope/ coverage	Could be used for the transport of non-classified messages, information and evidence between: • Member States (incl. Ministries of Justice and national/regional Prosecutors' Offices) • Member States (incl. Ministries of Justice and national/regional Prosecutors' Offices) and JHA agencies & EU bodies • JHA agencies & EU bodies Could be used potentially to send requests to **private service providers**.	Could be used for the transport of non-classified messages, information and evidence between: • Member States (incl. Ministries of Justice and national/regional Prosecutors' Offices) • Member States (incl. Ministries of Justice and national/regional Prosecutors' Offices) and JHA agencies & EU bodies • JHA agencies & EU bodies Could be used potentially to send requests to **private service providers**.	Could be used for the transport of non-classified messages, information and evidence between: • Member States (incl. Ministries of Justice and national/regional Prosecutors' Offices) • Member States (incl. Ministries of Justice and national/regional Prosecutors' Offices) and JHA agencies & EU bodies • JHA agencies & EU bodies	Could be used for the transport of non-classified messages, information and evidence between: • Member States (incl. Ministries of Justice and national/regional Prosecutors' Offices) • Member States (incl. Ministries of Justice and national/regional Prosecutors' Offices) and JHA agencies & EU bodies • JHA agencies & EU bodies	Could be used for the transport of non-classified messages, information and evidence between: • Member States (incl. Ministries of Justice and national/regional Prosecutors' Offices) • Member States (incl. Ministries of Justice and national/regional Prosecutors' Offices) and JHA agencies & EU bodies • JHA agencies & EU bodies	Could be used for the transport of EU **classified messages, information and evidence (up to level of EU CONFIDENTIAL)** between: • Member States (incl. Ministries of Justice and national/regional Prosecutors' Offices) • Member States (incl. Ministries of Justice and national/regional Prosecutors' Offices) and JHA agencies & EU bodies • JHA agencies & EU bodies
Legal basis for the recognition of exchanged documents	In e-CODEX, the **Circle of Trust** (a "soft" legal basis) means that participating Member States recognise the legal validity of the documents exchanged, and of	e-Delivery doesn't have such a legal basis.	In e-CODEX, the **Circle of Trust** means that participating Member States recognise the legal validity of the documents exchanged, and of information on	e-Delivery doesn't have such a legal basis.	TESTA doesn't have such a legal basis.	SIENA doesn't have such a legal basis.

Table 9: Secure communication channel - Technical assessment

	information on identity and signatures coming from other participants.		identity and signatures coming from other participants.			
EU accreditation	e-CODEX/eDelivery is **not accredited.**	eDelivery is **not accredited.**	e-CODEX/eDelivery is **not accredited.**	eDelivery is **not accredited.**	TESTA is not accredited. However, the **TESTA infrastructure fulfils the requirements for a security accreditation** (up to level of **EU RESTRICTED**) from gateway to gateway, and accreditation would require the application layer to be EU RESTRICTED compliant as well as end-to-end security being provided by additional devices and cryptographic software at the end user's side.	SIENA is **accredited** up to level of **EU CONFIDENTIAL.**
Max message size/ bandwidth	**2 GB** (as the e-CODEX scenario is also based on the e-Delivery technical infrastructure), but could increase thanks to the future "split and join" for e-	**2 GB** (Domibus reference implementation & certain commercial products), but could increase thanks to the future "split and join" for e-Delivery.[49]	**2 GB** (as the e-CODEX scenario is also based on the e-Delivery technical infrastructure), but could increase thanks to the future "split and join" for e-	**2 GB** (Domibus reference implementation & certain commercial products), but could increase thanks to the future "split and join" for e-Delivery.	Currently Member States Turnkey Access Points (TAP) are connected to TESTA via a 10 Mbps redundant capacity, which could influence the maximum	**50 MB** with no limit on the number of attached files, but this will increase in the future.[50]

[49] In theory, there is no message size limitation for the Commission's eDelivery AS4 profile. In practice, due to limitations in the code or libraries used in AS4 implementations, there is a 2 GB message size limitation in Domibus and in some other AS4 implementations. To overcome this limitation, the eDelivery team has drafted

Table 9: Secure communication channel - Technical assessment

	Delivery.		Delivery.		message size (as well as the limitations of the application running over TESTA).	
Service availability	Reliant on **internet availability.**	Reliant on **internet availability.**	**Guaranteed service availability** of TESTA thanks to Memorandum of Understanding (MoU) with DIGIT.	**Guaranteed service availability** of TESTA thanks to Memorandum of Understanding (MoU) with DIGIT.	**Guaranteed service availability** of TESTA thanks to MoU with DIGIT.	**Service availability is dependent** on both TESTA (on which SIENA is based) thanks to MoU with DIGIT and Europol.
Required effort to deploy access points in Member States	Several Member States have deployed an eDelivery/e-CODEX access point for judicial cooperation in criminal matters through their participation in e-CODEX pilot projects. However, **by 2021, all Member States will have e-CODEX installed.**	**Several** Member States have deployed an eDelivery access point for judicial cooperation in criminal matters through their participation in e-CODEX pilots (which are based on the e-Delivery digital infrastructure) and other projects based on eDelivery. **The other Member States would need to deploy an eDelivery access point (and a compliant connector).**	**All EU Member States** and 4 other countries have access to TESTA. Most countries have connected their Ministries of Justice and Prosecution Offices, or are ready to (please note that there is also some reluctance in certain Member States). In addition, several Member States have deployed an eDelivery/e-CODEX access point for judicial cooperation in criminal matters through their participation in e-	**All EU Member States** and 4 other countries have access to TESTA. Most countries have connected their Ministries of Justice and Prosecution Offices, or are ready to (please note that there is also some reluctance in certain Member States). However, for **eDelivery access points (and a compliant connector) for judicial cooperation in criminal matters would need to be**	**All EU Member States** and 4 other countries have access to TESTA.	**All 27 Europol Member States**, as well as 20 other countries have access to SIENA through their Europol National Unit (ENU).

an update to the eDelivery AS4 profile to include an optional 'split and join' module. These specifications are still under review and therefore have not yet been implemented by other AS4 solutions. (Source: information provided by DIGIT).

[50] Europol is currently developing an upgraded uploading mechanism that will accept 50 MB per file and a few hundred MB per message. (Source: information provided by Europol).

Table 9: Secure communication channel - Technical assessment

			CODEX pilot projects. However, **by 2021, all Member States will have e-CODEX installed.**	**deployed** in those countries not already connected.		
Accessibility to end users in Member States	**Access to the secure communication channel for end users (e.g. prosecutors) is foreseen in the context of e-CODEX.** Moreover, all Member States (and thereby, judicial authorities), should be connected by 2021.	Access to the secure communication channels for end users (e.g. prosecutors) depends on the secure communication network at national level. Indeed, it needs to be configured to connect the back-end systems used by judicial practitioners to an eDelivery access point.	**Access to the secure communication channel for end users (e.g. prosecutors) would require some additional effort at Member State level**, to: • Connect the national network to TESTA and make all end users (e.g. prosecutors) have access to it. • Deploy an eDelivery access point over TESTA.	Access to the secure communication channels for end users (e.g. prosecutors) depends on the secure communication network at national level. Indeed, it needs to be configured to connect the back-end systems used by judicial practitioners to an eDelivery access point.	Access to the secure communication channels for end users (e.g. prosecutors) depends on the secure communication network at national level. However, most countries have their Ministries of Justice and Prosecution Offices to TESTA EuroDomain, or are ready to.	Access to SIENA is currently **limited to law enforcement authorities in most cases**. To connect judicial authorities to SIENA is feasible from a technical and legal perspective, and a secure connection would need to be established at Member State level between the Europol National Unit (ENU) and the judicial authorities, using the secure communication network(s) available a national level. Three options to do so are detailed in section 5.2.1.3.
Required effort to connect at the side of JHA agencies & EU bodies	Although some JHA agencies & EU bodies already have one, **several others would need to deploy an eDelivery/e-CODEX access point**.	Although some JHA agencies & EU bodies already have one, **several others would need to deploy an eDelivery access point**.	Although some JHA agencies & EU bodies already have one, **several others would need to deploy an eDelivery/e-CODEX access point**.	**All JHA agencies & EU bodies** are connected to the TESTA EuroDomain (or a specific TESTA domain). However, several of them **would also need to deploy an**	All **JHA agencies** are connected to the TESTA EuroDomain (or a specific TESTA domain).	**Most JHA agencies** (Europol, Eurojust, Frontex, EMCDDA, and CEPOL) are connected to SIENA. According to Europol, the EPPO should also be connected shortly upon its creation.

Table 9: Secure communication channel - Technical assessment

				eDelivery access point.		
Security	Security in e-CODEX is ensured at multiple levels: at **transport level** (through the use of the TLS cryptographic protocol), at **message level** (though the use of the AS4 and WS messaging standards to securely exchange messages over the internet) and at **document level** (through the use of digital signatures). The transport and message level security features pertain to the underlying eDelivery digital infrastructure.	eDelivery is based on **Transport Layer Security**, which is ensured with software measures. In addition, the Connecting Europe Facility offers a **Public Key Infrastructure** (PKI) service for eDelivery.	Security in e-CODEX is ensured at multiple levels: at **transport level** (through the use of the TLS cryptographic protocol), at **message level** (though the use of the AS4 and WS messaging standards to securely exchange messages over the internet) and at **document level** (through the use of digital signatures). The transport and message level security features pertain to the underlying eDelivery digital infrastructure. **TESTA also offers security features** (please refer to scenario 5).	Would **combine the security features of TESTA and eDelivery**. For TESTA security features, please refer to scenario 5. For eDelivery security features, please refer to scenario 2.	TESTA EuroDomain is a private network ensuring security by two dedicated **Security Operation Centres** (active 24/7), and which implements **IPSec protocol supported at hardware level.** These Security Operations Centres are operated by a private contractor on behalf of DG DIGIT. For other dedicated TESTA domains (such as the one of Europol, the Council of the EU, and eu-LISA for SIS II and VIS), security operations are ensured by the owner of the domain.	SIENA uses the **Europol sub-domain of TESTA**, with **additional encryption devices** providing additional security at network/ infrastructure level.[51]
Financing	There are **several funding opportunities** for this scenario, both for Member States and	There are **several funding opportunities** for this scenario, both for Member States and	There are **several funding opportunities** for this scenario, both for Member States and	There are **several funding opportunities** for this scenario, both for Member States and	The cost related to the operation of the TESTA EuroDomain (by a private contractor)[52] is	The cost of connecting the Europol HQ and Europol National Units is borne by

[51] Note that Europol's SIENA Platform, which is not in scope of the scenario envisaged in this report, provides additional security at software and user level (through the management of user accounts, roles and responsibilities).

[52] These costs are likely to change as the TESTA framework contract will be renewed in 2020.

Table 9: Secure communication channel - Technical assessment

	JHA agencies and EU bodies. For more information, please refer to section 7.3 on candidate funding sources.	JHA agencies and EU bodies. For more information, please refer to section 7.3 on candidate funding sources.	JHA agencies and EU bodies. For more information, please refer to section 7.3 on candidate funding sources.	JHA agencies and EU bodies. For more information, please refer to section 7.3 on candidate funding sources.	supported by the Commission, and the **costs at Member State level are variable.**[53] For dedicated TESTA domains, these costs are higher and must be carried by the owner of the dedicated domain.[54] Please refer to section 7.3 for more information on candidate funding sources to help Member States.	Europol. **The extension of the SIENA connection to the competent authorities in Member States has to be arranged and financed by the countries themselves**. Please refer to section 7.3 for more information on candidate funding sources to help Member States and JHA Agencies and EU bodies.
Cost	-70% for eDelivery access point (for the Domibus reference implementation of the Commission), and e-CODEX	-60% for eDelivery access point: €0 (for the Domibus reference implementation of the Commission),	23.100€ for eDelivery access point (for the Domibus reference implementation of the Commission), and e-CODEX	eDelivery access point: +10% (for the Domibus reference implementation of the Commission). Connectors provided	EuroDomain: -100% as the existing default connection of each Member State as well as JHA Agencies & EU	Connection to Europol National Unit: €0 in terms of developments, as the solution already exists.

[53] Assuming that the legal basis of the Cross Border Digital Criminal Justice project is directly deriving from a Union legal act, two technical situations must be distinguished:

1) A national authority (e.g. Ministries of Justice, prosecutors' offices) can make use of an existing default connection to TESTA paid by the Union budget (e.g. the TESTA connection/TAP onto the national network). Hence there is no setup neither operational costs to be envisaged by that National Authority for the use of TESTA services. Also no financial participation will be required (this might change in the future but today there are no instructions in that sense).
   The only costs that the national authority might be facing are:
   a) A local connection cost to connect that national authority to the national network of the country (if not yet done); or
   b) Some configuration cost to root the traffic from that national authority to the existing TESTA default connection point in the country.
2) One new direct connection to TESTA is required by a national authority (e.g. Ministries of Justice, prosecutors' offices) as that Authority cannot be plugged to the existing default connection to TESTA in that country. In which case the installation and recurring costs for this new connection will be integrally and directly covered by that national authority requiring it. Since the TESTA fees depend on the location, the speed and the type of setup, this will be determined on a case by case basis.
   In addition, based on the outcome of the survey performed with the Member States, it looks like – at this stage - the Ministries of Justice and prosecutors' offices could fall under 1a or 1b above and therefore benefit from the existing default connection to TESTA.

Source: information provided by DIGIT

[54] For instance, eu-LISA indicated that the total cost of running the VIS/SIS private TESTA-ng domain is currently approximately € 1,045 million/month.

Table 9: Secure communication channel - Technical assessment

	connector. Configuration cost: see estimates here: https://www.e-codex.eu/faq-e-codex	with another connector over the internet. Connectors provided by commercial companies are available, for which pricing must be requested to vendors. Configuration cost: see estimates here: https://www.e-codex.eu/faq-e-codex	connector, over TESTA. Configuration cost: see estimates here: https://www.e-codex.eu/faq-e-codex	by commercial companies are available, for which pricing must be requested to vendors. TESTA: please refer to scenario 5. Configuration cost: see estimates here: https://www.e-codex.eu/faq-e-codex	bodies is already covered by the Union budget. Additional costs to connect judicial authorities to the TESTA connection point in a Member State are variable and cannot be estimated. Dedicated domain: example of eu-LISA: "The total cost of running TESTA-ng is currently € 1,045 Mio/month. It is VIS/SIS TESTA-ng network combined though."	Additional costs to connect judicial authorities to the SIENA: • Option A: judicial authorities are connected to ENU. The cost for Europol is €0, and the cost for Member is variable and cannot be estimated (depends on the configurations and maintenance costs for the national network, and the national accreditation process). It could rage between € 50 000 – 1 million.[55] • Option B: install additional secure SIENA rack for judicial authorities. The cost for Europol is € 20k – 25k to set up the racks. The cost for Member States is variable and cannot be

[55] Please note that this is a very conservative estimation as a single VPN connector approved to process EU classified information costs more than € 50 000.

Table 9: Secure communication channel - Technical assessment

						estimated (depends on the configurations and maintenance costs for the national network, and the national accreditation process). It could rage between € 50k – 1 mo.
Maintenance	The eDelivery Domibus implementation is **maintained by the European Commission** (as a Building Block of the Connecting Europe Facility), whereas the e-CODEX connector is **maintained by a consortium of Member States** receiving grants from the Commission. In the future, the maintenance of e-CODEX might be passed on to an established institution within the European Commission.	The eDelivery Domibus implementation is **maintained by the European Commission** (as a Building Block of the Connecting Europe Facility).	The eDelivery Domibus implementation is **maintained by the European Commission** (as a Building Block of the Connecting Europe Facility), whereas the e-CODEX connector is **maintained by a consortium of Member States** receiving grants from the Commission. In the future, the maintenance of e-CODEX might be passed on to an established institution within the European Commission.	The eDelivery Domibus implementation is **maintained by the European Commission** (as a Building Block of the Connecting Europe Facility), whereas the TESTA network is **managed by DIGIT** (through a private service provider).	Network **managed by DIGIT** (through a private service provider).	Network **managed by Europol**.
Risks	• **Uncertainty** regarding the **future maintenance of the e-CODEX**	• **Uncertainty** regarding the **future funding of eDelivery grants**, given	• **Uncertainty** regarding the **future maintenance of the e-CODEX**	• The current TESTA framework contract ends in June 2020. There	• The current TESTA framework contract ends in June 2020. There	• Different options are possible to extend SIENA to judicial authorities.

Table 9: Secure communication channel - Technical assessment

	connector. • **Uncertainty** regarding the **future funding of eDelivery grants**, given that the successor of the Connecting Europe Facility (the Digital Europe Programme) is currently being elaborated. • For the same reasons, there is **uncertainty** regarding the **future maintenance of the eDelivery services and solution**.	that the successor of the Connecting Europe Facility (the Digital Europe Programme) is currently being elaborated. • For the same reasons, there is **uncertainty** regarding the **future maintenance of the eDelivery services and solution**.	**connector.** • **Uncertainty** regarding the **future funding of eDelivery grants**, given that the successor of the Connecting Europe Facility (the Digital Europe Programme) is currently being elaborated. • For the same reasons, there is **uncertainty** regarding the **future maintenance of the eDelivery services and solution**. • The current TESTA framework contract ends in June 2020. There is **uncertainty** regarding the terms (incl. service agreements and pricing) of the **future contract**. • The deployment of eDelivery over TESTA may entail **several issues**	is **uncertainty** regarding the terms (incl. service agreements and pricing) of the **future contract**. • The deployment of eDelivery over TESTA may entail **several issues in practice**: **complex setup**, **deployment and maintenance issues**, misalignment in the evolution of TESTA and eDelivery due to the fact that they are **governed independently**, etc.	is **uncertainty** regarding the terms (incl. service agreements and pricing) of the **future contract**.	However, to do so the national networks would need to **undergo a national accreditation process** in order to be able to exchange classified information.

Table 9: Secure communication channel - Technical assessment

	in practice: **complex setup**, **deployment and maintenance issues**, misalignment in the evolution of TESTA and eDelivery due to the fact that they are **governed independently**, etc.	

Legend: **Strength** **Weakness**

In conclusion, there are different communication channels that can be used for the different stakeholders and types of exchanges of information in the context of Cross-Border Digital Criminal Justice. Conclusions are presented below according to the different types of exchange of information:

- For the exchange of unclassified data between Member States, and Member States and JHA agencies and EU bodies:

  For the exchange of non-classified information, the re-use of eDelivery (with the e-CODEX connector) over the TESTA EuroDomain (scenario 3) is preferred because e-CODEX offers elements that are not offered by any of the other options, i.e. the Circle of Trust between participating countries, the possibility to make the solution available to all end users (e.g. prosecutors, courts, judicial authorities) and the investments already made by Member States in installing an eDelivery/e-CODEX access point and connector which could be leveraged (all Member States will be connected to e-CODEX over the internet by 2021). Moreover, the use of the TESTA EuroDomain for the exchange of non-classified is recommended, as the availability and maintenance of the network is guaranteed by DIGIT, and all Member States and JHA agencies and EU bodies are already connected to it (the cost of it being borne by the Union budget). In terms of security, the encryption at application level (as done by eDelivery) alleviates concerns regarding the fact that the operators of the Security Operations Centres may have a view on the information being exchanged via the TESTA EuroDomain.

  However, the increased complexity and risks brought by this set-up must be carefully evaluated before choosing an option. Indeed, although national authorities have access to TESTA, it would need to be extended to be made available to end users (by connecting it to the national network), and moreover, the eDelivery/e-CODEX access point and connector would need to be redeployed over TESTA in each Member State. This would also increase the required maintenance effort for Member States.

- For the exchange of EU classified data between Member States, and Member States and JHA agencies and EU bodies:

  For the exchange of EU classified information, end to end accreditation of the secure communication channel is required. The preferred option would be to re-use eDelivery (with the e-CODEX connector) over TESTA EuroDomain, in order to simplify the architecture of the whole ecosystem by having a single communication channel. However, this would imply that both TESTA EuroDomain and eDelivery undergo the accreditation process to be able to exchange EU classified information. In practice, this would entail purchasing approved cryptographic devices and boundary protection solutions, and accrediting the end points/terminals used to connect to the solution.

  Because SIENA is accredited up to level of EU CONFIDENTIAL (up to level of the Europol National Unit in Member States), it is an alternative option to the re-use of eDelivery (with the e-CODEX connector) over TESTA EuroDomain. Regarding extending the access to SIENA access points to judicial authorities and practitioners in Member States, based on the specific constraints of each country, it is recommended to:

  - Either connect judicial authorities in Member States to Europol National Units, using the national secure communication network. From the perspective of Europol this is the easiest and least costly option. However, this would entail a significant effort and cost on Member State side that depends on the set-up of the national network infrastructure, and would mean that the national communication network, but also all terminals and connected systems have to be accredited to exchange classified information. Moreover, every single workstation would need to offer TEMPEST protection.[56]

   - Or maintain the status quo, whereby judicial practitioners have to access a SIENA end point in a law enforcement authority to send EU classified information. This option is recommended if the cost and effort to connect national authorities is too high. Moreover, the volume of EU classified information currently sent over SIENA is low (approximately 5% of all information exchanged).

- For hit/no-hit and the exchange of unclassified and EU classified data between JHA agencies and EU bodies:

  Certain specific exchanges of information between JHA agencies and EU bodies (notably for SIS II, VIS and ECRIS-TCN in the future), require the use of specific communication channels to do hit/no-hit searches.

  Other exchanges of information and hit/no-hits are not bound by any channels, and are therefore covered by the same recommendations and remarks as those presented in the paragraphs above for the exchange of (un)classified data between Member States, and Member States and JHA agencies and EU bodies.

5.2.3 Security assessment

The following general security considerations should be taken into account while assessing the security level of the communication channels, in conformance with Commission Decision 2017/46 and Eurojust security rules, as well as with industry good practices.

- Classification of networks, systems and information.
- Data classification and labelling.
- Secure, restrict and investigate email communications – e.g. anti-spoofing mechanisms.
- Secure, restrict and investigate incoming and outgoing network communications.
- Control remote accesses to and from Eurojust domain.
- Implement multi-layered anti-malware solution.
- Define secure data transfer procedures.
- Authorise only secure transfer protocols.

The table below compares the different proposed options, in terms of what an effective IT security should guarantee, according to the Commission Decision 2017/46.

Table 10: Proposed options security objectives comparison

	e-Delivery (over the internet)	**e-Delivery (over TESTA)**	**TESTA**	**SIENA**

[56] According to Council Security Rules 2013/488/EU Article 9.5.

	e-Delivery (over the internet)	e-Delivery (over TESTA)	TESTA	SIENA
Authenticity	Enabled by PKI. Electronically sealing ensuring non-repudiation of data origin - WS-Security 1.1 using XML Signature 1.1	Enabled by PKI. It applies Electronically sealing that ensures non-repudiation of data origin – using WS-Security 1.1 using XML Signature 1.1	Enabled by IPSEC which might provide non-repudiation, depending on which cryptographic algorithm is used and how keying is performed.	*Missing information*
Availability	Special measures have to be designed and implemented in order to ensure availability requirements. In case a service provider is involved, an SLA should be established and maintained by different stakeholders when, availability of systems, applications and services supporting the eDelivery exchange of data over the internet, should be ensured.	Guaranteed by SLA thanks to TESTA, which supports systems and applications with high-availability profile. TESTA guarantees both Data and System availability.	Guaranteed by SLA, which supports system and application with high-availability profile. TESTA guarantees both Data and System availability.	*Missing information*
Confidentiality	It ensures a secure communication channel using TLS (WS-Security 1.1 using XML Encryption 1.1) at transport layer which relies on digital certificates to ensure confidentiality. However, the confidentiality level will be highly dependent on the security hardening of the underlying networks and	This solution would guarantee confidentiality by applying a multi-layer encryption at both network (IPSec) and transport levels (TLS). In addition, to the possibility of encrypting application data. It is actually combining both the confidentiality enabling capabilities provided by both	TESTA network implements IPSec protocol to ensure confidentiality, which operates at network layer. Cannot be used to send classified EU information.	SIENA is accredited for the exchange of information up to and including EU CONFIDENTIAL. SIENA can be accessed from EU RESTRICTED (or equivalent) networks, and in the future also from unaccredited national networks.

	e-Delivery (over the internet)	**e-Delivery (over TESTA)**	**TESTA**	**SIENA**
	systems.	eDelivery and TESTA.		
Integrity	Guaranteed at transport layer by using TLS protocol which also ensures authentication & non-repudiation of data origin - WS-Security 1.1 using XML Signature 1.1. However, the integrity level will be highly dependent on the security hardening of the underlying networks and systems.	Integrity is preserved at the network layer, transport layer and could also be applied at the application (business) level, if needed, combining so the measures that ensure integrity of both eDelivery and TESTA.	Guaranteed at network layer by using IPSec protocol which ensures integrity of transmitted data.	*Missing information*
Non-repudiation	Ensured by PKI. Non-repudiation of receipt, where the receipt signal message is electronically signed by the receiver using his/her own private key.	Ensured by PKI. For both technical and business levels.	Enabled by IPSEC which might provide non-repudiation, depending on which cryptographic algorithm is used and how keying is performed.	*Missing information*

Note that the comparison above is not taking into consideration the type of connector used by an eDelivery solution (e.g. e-CODEX), as the different types of connectors are able to achieve, under certain assumptions, an acceptable security assurance level in line with the risk appetite. Consequently, it has to be decided from a functional point of view, which connector is more suitable for the DCJ target architecture. Note that some variations exist between the different connectors, mainly related the following areas.

- **Information exchange model**
  - Network topology:
    - 3-corner model
    - 4-corner model
    - etc. (i.e. n-corner model)
  - Protocol in use:
    - e-SENS AS4 profile
    - PEPPOL AS2 profile
    - etc.

  - Integration approach:
    - Service provider
    - Specific connector
    - etc.
- **Discovery model of network participants**
  - Dynamic (e.g. PEPPOL)
  - Static (e.g. e-CODEX)
- **Security Model**
  - Trust circle:
    - Public Key Infrastructure
    - Mutual trust
    - Etc.
  - Security controls:
    - *Liberal inner security*, which means that internal security controls have to be designed and implemented to secure the connector and its communication channels. (e.g. PEPPOL).
    - *Inner security with connector*, which means that the connector comes with its own security controls. The focus should be on the integration of the connector with the existing architecture landscape.

Note: It is important to have in mind, that connectors are open-source and that anyone can modify an existing implementation (e.g. e-CODEX) to extend it, introducing new security capabilities or enhancing its internal security controls, with the aim of accreditation or certification.

Note that from security viewpoint e-CODEX seems to be a valid candidate for the DCJ target architecture, as it allows, by design, a secure communication and information exchange between different stakeholders. Especially that it is already used between Member States in the field of justice, as an interoperable environment building upon national systems and infrastructures supporting the e-Justice activities. It is important to be noted that the e-CODEX and the eDelivery platforms are composed of two main components:

- A **national connector**: a piece of software that implements the interface between the national information exchange infrastructure of a given participating Member State and a national gateway of that Member State.
  - It transforms the format of the outgoing message received from national application to the e-CODEX standard.
  - It also checks the validity of the electronic signature of the received messages. In the case of the ”Circle of Trust” agreement, allowed by e-CODEX, the receiving country can trust the received messages or documents and is not required to validate them again.
  - It transforms the incoming messages received from the e-CODEX gateway (or eDelivery access point) from the e-CODEX standard to the national standard.
  - It verifies the authenticity and the integrity of the received messages to make sure that the received data has not been altered and that it is coming from a genuine source. So that the receiving Member State has no obligation to carry out a verification of the authenticity and integrity of the received data.
- A **national gateway**: a technical and organisational infrastructure provided and managed by a Member State mainly for routing incoming and outgoing electronic communication with another Member State in the same e-CODEX ecosystem.

- An e-Delivery access point is responsible for the secure and reliable transport of data and files between network nodes.
- For outgoing messages, the national gateway provides signature and timestamp at transport layer.
- For incoming messages, it checks the signature at the transport layer. It also provides a timestamp and sends acknowledgments of receipts.
- It uses ebMS which supports electronic signature and encryption (based on XML Signature standard and XML encryption standard) of business messages according to Web Services Security (WSS) 1.0 and 1.1, as well as the WSS X.509 Certificate Token Profile.

Note: It is important to be noted that in principle, the e-CODEX or the eDelivery platform are content agnostic, which means that, in theory, both platforms do not have access to the application layer data, under the assumption that end-to-end encryption is applied.

Note: Note that the e-CODEX connector might also perform protocol and "semantic translation", if needed.

As observed in Table 10, the three proposed solutions could achieve, under certain assumptions, the security objectives required for the DCJ target architecture.

Note that as a result of using eDelivery over TESTA network, it is possible to reach a higher security assurance level than the other scenarios, as it is a consequence of their complementarities. Indeed, considering on the one hand, the decentralisation aspects offered by the eDelivery deployment model, and on the other, the centralisation of common services offered by TESTA infrastructure (e.g. Common Services Domain (CSD) (i.e. secure FTP, DNS, etc.), SOC, and NOC etc.) the level of the security assurance increases.

In addition to that, while eDelivery is securing the confidentiality and integrity of the business messages and transactions, above the transport layer, TESTA infrastructure would provide secure network services and communication channels that ensure confidentiality, integrity and availability of DCJ target architecture data and systems that are processing them. Applying both solutions would be an enabler to achieve security in depth principle for the overall DCJ target architecture. However, a more in-depth performance analysis should be conducted in order to evaluate whether the combination of both solutions still meets the performance requirements of DCJ target architecture.

On the other hand, the SIENA network lays on top of TESTA infrastructure, which makes it, to a certain extent, physically dependent on TESTA infrastructure. However, the SIENA network is accredited, and therefore, can handle European classified data (up to EU CONFIDENTIAL, or equivalent), which is not allowed with only TESTA network, except if the solution built on top of it, is accredited. The use of the SIENA network to handle classified information in the context of DCJ target architecture is conceptually a valid option that meets the security requirements.

Note: The SIENA delegated authorisation model allows Member States and third parties to create their own users via Identity and Access Management (IAM) services. It also allows the system-to-system integration using Simple Object Access Protocol (SOAP) and Representational State Transfer (REST) Application Programming Interfaces (API).

However, due to the fact that some involved stakeholders might not have access to the SIENA network (e.g. prosecutors) in addition to the accountability issues that it emerges, it is then not advisable to use the SIENA network as a mean for exchanging messages in the DCJ target ecosystem. Instead, the aim should be to use TESTA as a backbone network, extending the capabilities of the solution combining eDelivery and TESTA by implementing capabilities re-using or overriding SIENA services, which would then allow to obtain similar confidentiality and integrity levels than the ones offered by the SIENA services. In any case, a solution which is relying on eDelivery and TESTA has to be accredited before being able to exchange European Classified Information (EUCI) or make use of EU Council approved cryptographic products to encrypt EU RESTRICTED level communications.

The suggested solution, from security standpoint would be, as previously mentioned, to use eDelivery information exchange system over TESTA for unclassified information exchanges. Regarding classified information exchanges, it is recommended to extend eDelivery over TESTA solution by implementing a secure communication channel relying on or inspired from the SIENA services that ensures the same confidentiality and integrity levels as the ones guaranteed by the SIENA network. The proposed solution should be accredited and certified once implemented, in order to be able to exchange European classified information, up to EU CONFIDENTIAL level.

This would be using the same infrastructure as the solution that exchanges non-classified information, with a separated communication channel that has more strict security measures in line with EUCI regulation. It is therefore essential to conduct further low-level analysis to evaluate risks, performance and compliance aspects for the design of such option in DCJ target architecture.

5.2.4 Legal and data protection assessment

The use of a secure communication channel between the stakeholders involved in criminal justice aims to ensure a secure exchange of messages, information and evidence electronically across borders.

The exchange of information and evidence, including personal data, between the stakeholders at national level mentioned above is regulated by the judicial cooperation legal instruments. These are for example: the European Arrest Warrant Council Framework Decision[57], Council Decision on the exchange of information and cooperation concerning terrorist offences[58], the European Investigation Order Directive[59], amongst others (see Annex D | for a more detailed overview of these instruments). The legal basis for the exchange of information is therefore already in place.

In addition, the data protection and data security aspects are largely regulated, including legal provisions of the JHA agencies and EU bodies funding instruments, as well as other EU-wide instruments such as Data Protection Law Enforcement Directive (LED).[60] These aspects are therefore duly covered, and do not require additional legal instruments.

[57] Council Framework Decision 2002/584/JHA of 13 June 2002 on the European Arrest Warrant and the surrender procedures between Member State, https://eur-lex.europa.eu/resource.html?uri=cellar:3b151647-772d-48b0-ad8c-0e4c78804c2e.0004.02/DOC_1&format=PDF

[58] Council Decision 2005/671/JHA of 20 September 2005 on the exchange of information and cooperation concerning terrorist offences, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005D0671&from=GA

[59] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters of 3 April 2015, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0041&from=EN

[60] Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the

This overall legal framework, consisting of the legal bases and the data protection and security provisions and instruments, is sufficient in and of itself for the exchange of information in cross-border criminal cases. Therefore, the question raised here is whether the use of the secure communication channels (described in section 5.2.1) requires new elements to be established, and how these should be regulated.

One of the options for the secure communication channel is to use the CEF (Connecting Europe Facility)[61] building block e-Delivery, whose objective is to help public administrations to exchange electronic data and documents with other public administrations (G2G)[62], businesses (G2B and B2G)[63] and citizens (G2C and C2G).[64]

The use of eDelivery as secure communication channel does not require a specific legal basis. eDelivery offers technical specifications, sample software and support services to set up this type of exchanges, ensuring they occur in an interoperable, secure, reliable, and trusted way. eDelivery's technical specifications can be used in any domain, including in the field of justice.[65] Nevertheless, as indicated in the security assessment (see section 5.2.3), the use of this solution for classified information would require the extension of eDelivery over TESTA solution by implementing a secure communication channel relying on or inspired from the SIENA services.

Based on this, it can be concluded there are no legal barriers preventing the use of eDelivery in the area of criminal justice. On the contrary, eDelivery is aimed to ensure secure data exchanges amongst administrations. Member States, JHA agencies and EU bodies can thus use it for cross-border cooperation in criminal justice.

eDelivery can be used with different connectors, such as **e-CODEX**, to connect the eDelivery access point to national and European IT systems (see section 5.2.1 for more details). e-CODEX's legal basis is the Agreement on a Circle of Trust, which every participant (Member State) willing to deploy the e-CODEX connector is required to sign. It should be noted that this approach for the legal basis of e-CODEX constitutes a weakness of this solution, as the Agreement on a Circle of Trust is not a binding document for the parties. Therefore, it could be envisaged to enact a legal binding document to regulate the use of e-CODEX as the secure communication channel.

eDelivery can be run over the internet, or it can also be used over private networks such as **TESTA**. As the use of the internet has no legal implication, the report will focus here on TESTA. Developed under the ISA² Community Programme[66], the objective of the TESTA project developed is to exchange data effectively between European and Member States administrations. In other words, it aims to facilitate the cooperation between public administrations, regardless the policy area in which they are involved.[67] As indicated the ISA² Programme, all European public

prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN

[61] Regulation (EU) No 1316/2013 of the European Parliament and of the Council of 11 December 2013 establishing the Connecting Europe Facility, amending Regulation (EU) No 913/2010 and repealing Regulations (EC) No 680/2007 and (EC) No 67/2010, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013R1316&from=EN

[62] Government to government

[63] Government to business, and vice versa.

[64] Government to citizen, and vice versa.

[65] See: https://ec.europa.eu/inea/sites/inea/files/building_block_dsi-introdocument_edelivery_v1_00.pdf, p. 8.

[66] Decision 2015/2240 of the European Parliament and of the Council of 25 November 2015, establishing a programme on interoperability solutions and common frameworks for European public administrations, businesses and citizens (ISA2 Programme) as a means for modernising the public sector, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015D2240&from=EN

[67] See: https://ec.europa.eu/isa2/sites/isa/files/testa_overview_-_july_2018.pdf

administrations are part of its material scope. Likewise, as explained in the TESTA Overview & Service Catalogue[68], there is no specific restriction to the use of TESTA in the field of justice.[69] There is therefore no need to enact a legal basis, nor to make a legal amendment to allow the use of TESTA in cross-border criminal cases.

Alternatively, instead of using eDelivery, the use of the **SIENA communication channel** could be considered. It should be highlighted that this solution was developed by Europol to meet the communication needs of EU law enforcement.[70] This implies that the communication tool SIENA has been tailored for specific exchange of information between the national competent authorities for police cooperation. SIENA's functionalities have been thus developed and implemented to address the needs of these stakeholders. Nevertheless, there is a legal difference between police cooperation and judicial cooperation to take into account when considering the use of the same channel for the two.

The European Data Protection Supervisor (EDPS) has already studied the use of SIENA, and its functionalities. As indicated in one of its opinion[71], the EDPS does not consider SIENA's functionalities appropriate for the exchange of information in a different context and purpose than the original (i.e. for law enforcement cooperation purposes). Therefore, in case SIENA is retained as the secure communication channel to be used for cross-border judicial criminal cooperation, it would be advisable to tailor it to the needs of the target audience: judicial practitioners, being prosecutors, and investigative judges mainly.

Although a specific legal basis is not specifically required to tailor the SIENA communication tool, the question to what extent Europol could support this exercise is raised. Judicial cooperation does not fall within Europol's realm. However, as SIENA was developed by this agency, it could be envisaged to involve Europol in the tailoring exercise in order to ensure its knowledge and expertise is leveraged.

Based on the above, it can be concluded that the use of a secure communication channel does not require a legal amendment or legal basis per se. Nevertheless, the European Commission cannot impose the uniform use of a given channel. Therefore, Member States are free to use different channels for different use cases. To avoid this fragmented landscape, which would hamper the efficiency required in cross-border cases, this report recommends to reach an agreement at EU level on the channel to be used in criminal cross-border cooperation.

Besides these legal considerations, a key aspect to take into account regarding the secure communication channels is the **data protection dimension**. The communication and document exchange between relevant stakeholders are key to enable the investigation of cross-border

[68] See: https://ec.europa.eu/isa2/sites/isa/files/testa_overview_-_july_2018.pdf

[69] TESTA is actually already providing secure and reliable communication infrastructure to information systems for the fight against crime. These systems include (i) ECRIS (Council Decision 2009/316/JHA on the establishment of the European Criminal Records Information System), (ii) Prüm (EU Council Decision (2008/616/JHA) on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime), and (iii) System of Control of Explosives for the Prevention and Fights against the terrorism (see: https://ec.europa.eu/isa2/sites/isa/files/testa_-_20_years_-_isa2_june_2018.pdf).

[70] As indicated in Article 6 of the Swedish Framework Decision (Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, see: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32006F0960&from=EN), law enforcement authorities may exchange information via any existing channels for international law enforcement cooperation.

[71] Opinion of the European Data Protection Supervisor on the EXIM, par (28) and (29), https://edps.europa.eu/sites/edp/files/publication/13-04-29_eixm_en.pdf

criminal offences and are a *conditio sine qua non* for the cooperation and functioning of the JHA agencies and EU bodies involved in criminal matters. However, in the context of Digital Criminal Justice, the exchange of personal data is intensified and facilitated, triggering further data protection considerations.

The exchange of messages, information and evidences using communication channels is *per* se a processing operation, under the scope of the Data Protection Regulation 1725[72], Directive 2016/680[73] and more specific data protection legislation applicable to EU institutions and agencies.[74] Each transmitting competent authority should ensure that the sharing of information is backed by the appropriate legal basis[75] and fit for the purpose under national and Union law, before data is transmitted to other recipients. To this end, further considerations are taken as regards to the accountability on the transmission of personal data: both abovementioned legal instruments provide that the controller should be able to verify and establish the bodies to which personal data have been or may be transmitted while using communication channels.[76] Practically, it means that solutions must embed a communication control which allows for the logging of all communication activities and provides a thorough audit trail. Furthermore, solutions should enable the transmitting authority to specify and restrict the processing of the personal data transmitted by means of providing handling codes[77] and that security controls are in place to enforce them (e.g. by preventing message rerouting). Restrictions may reflect specific Union or Member State law requirements and can include, for instance, the prohibition against further transmission of personal data or use for a different purpose to which the data was transmitted.

5.2.5 Governance

Refer to section 8.2 for an overview of the overall project governance.

This section presents the possible governance for the secure communication channel solution. Regardless of the option implemented, this report suggests that a subgroup of the Digital Criminal Justice Expert Group oversees the implementation of this solution. In other words, the subgroup would be driving the implementation and monitoring of the overall solution (which might combine several of the options as described in section 5.2.1).

The subgroup would assess the different options and proceed with the necessary adjustments in order to implement the Secure Communication Channel. The stakeholders to be involved in the process might slightly vary depending on the final solution retained to be implemented. As

[72] Regulation 1725/2018 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1725&from=EN

[73] Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN

[74] With regard to more specific data protection legislation we can think of, e.g. The Rules of procedure of 24 February 2020 on the processing and protection of personal data at Eurojust, http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/dataprotection2/Rules%20of%20procedure%20on%20the%20processing%20and%20protection%20of%20personal%20data%20at%20Eurojust/Eurojust-Data-Protection-Rules-Procedure-2019_EN.pdf.

[75] Reg. 1725/2018 Art. 72 and Directive 680/2018 Art. 8.

[76] Reg. 1725/2018 Art. 91 (2) (f) and Directive 680/2018 Art.29 (2) (f).

[77] Directive 680/2018, Recital 36.

explained in section 5.2.1, the options have been already developed/implemented, and thus an initial effort in terms of IT development won't be required (although other effort would be necessary, e.g. accreditation).

For the implementation of eDelivery with e-CODEX, it should be noted that several Member States have deployed an eDelivery access point (through their participation in e-CODEX pilots), and all Member States will have e-CODEX installed by 2021. The Expert Group subgroup should thus oversee that the remaining Member States deploy eDelivery access points, and that the e-CODEX implementation takes place within the timing foreseen. If the solution does not include e-CODEX, but another connector, the Commission should thus proceed to the development, and subsequent deployment in the Member States. The development of this connector could be carried out by a consortium of Member States (as in the case of e-CODEX).

In case TESTA is added to the solution as recommend by this study, most countries have already connected their Ministries of Justice and Prosecution Offices to TESTA EuroDomain, or are ready to. Therefore, no significant efforts would be expected in this case. The subgroup should thus monitor that the remaining countries do connect to TESTA. In any case, each Member States would be responsible to grant access to the end-users (e.g. prosecutors), which would depend on their own national communication network. Therefore, the subgroup can only oversee that this access is granted.

If SIENA is the communication channel retained, the subgroup would liaise with Europol, together with the input from Member States and the rest of the JHA agencies and EU bodies, to tailor the SIENA tool to the needs of judicial practitioners.

Lastly, depending on the solution to be implemented, the maintenance scenarios would vary. For eDelivery and TESTA, the stakeholder concerned would be the European Commission (DIGIT). For e-CODEX, at the moment a consortium is responsible for its maintenance. Nevertheless, it should be noted that the maintenance of e-CODEX might change hands. The consortium has invited the Commission to assume the responsibility for the continued maintenance of the e-CODEX solution, and mandate eu-LISA with its maintenance as of 2023.[78]

5.2.6 Conclusion

A secure communication channel would allow stakeholders involved in cross-border judicial cooperation in criminal matters to exchange messages, information and evidence electronically across borders in a secure way.

The report presents the assessment of different implementation options for the Secure Communication Channel: eDelivery (with e-CODEX connector, or with another connector) over the internet, eDelivery (with e-CODEX connector, or with another connector) over TESTA EuroDomain, TESTA (EuroDomain or dedicated domain), and SIENA. As indicated in the technical and security assessments, there are different preferred communication channels that can be used for the different stakeholders and types of exchanges of information.

The re-use of eDelivery (with e-CODEX connector) over the TESTA EuroDomain is preferred for communication between Member States and Member States and JHA agencies and EU bodies for

[78] See: https://www.e-codex.eu/sites/default/files/2019-11/e-CODEX%20D7.6%20Hands%20on%20Material%20v2.pdf

the exchange of non-classified information. e-CODEX offers key elements that are not provided by the rest of options (e.g. the Circle of Trust), and it's also key for the implementation of other solutions brought forward by this report (i.e. the Communication Tool, e-EDES, see section 5.3.2). As for the TESTA EuroDomain, stakeholders are already connected to it, and it's encrypted at application level (as for eDelivery). Moreover, operating eDelivery over the TESTA network allows to reach a higher security assurance level, as consequence of their complementarities. As inspired by SIENA, additional approved encryption devices can be used to complement the security levels of the TESTA network allowing the transfer of classified information up to the level of EU CONFIDENTIAL. However, this would require additional effort for Member States to connect their national networks to TESTA, and to deploy and eDelivery access point over TESTA.

For the exchange of EU classified information between Member States, and Member States and JHA agencies and EU bodies, however, an end to end accreditation is required. The preferred option here is the re-use eDelivery (with the e-CODEX connector) over TESTA EuroDomain, for the sake of simplification and using one unique communication channel, provided that both TESTA and eDelivery undergo the accreditation process to be able to exchange EU classified information. As explained in section 5.2.2, this is cumbersome and costly process, which would need to be done by all Member States. Alternatively, SIENA could also be implemented as it is already accredited up to level of EU CONFIDENTIAL. To be used by end-users (e.g. prosecutors), further effort would also be required in Member States to connect the national network to SIENA, and accredit it where necessary.

For hit/no-hit and the exchange of unclassified and EU classified data between JHA agencies and EU bodies, the same recommendations and remarks are applicable on the whole. However, certain specific exchanges of information between JHA agencies and EU bodies (notably for SIS II, VIS and ECRIS-TCN in the future), require the use of SIS/VIS communication channels (a dedicated domain managed by eu-LISA) to do hit/no-hit searches.

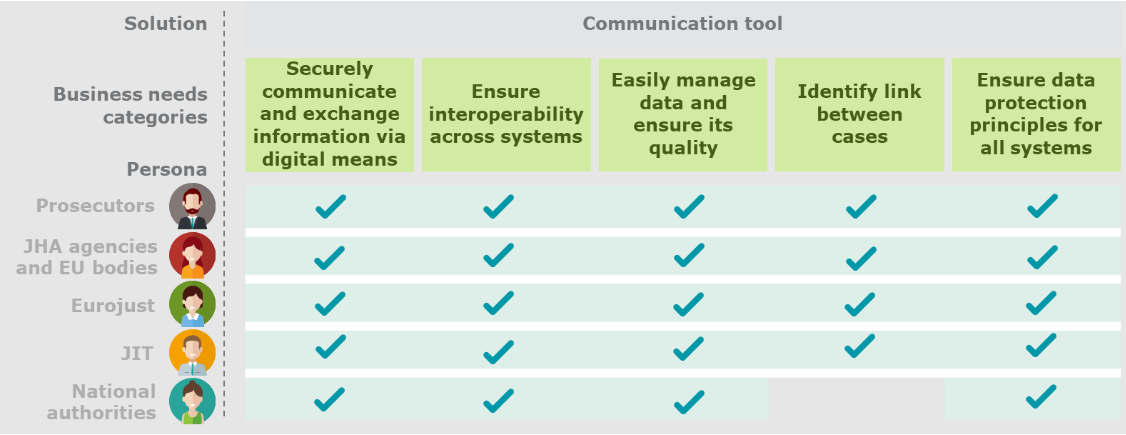
In terms of legal and data protection implications, it was found that there are no specific legal barriers preventing the use of any of the options considered. There are no legal amendments, nor specific new legal instruments, required to allow the use of the options presented. Regardless of the option retained, the communication channel should allow for the logging of all communication activities and provide a thorough audit trail in order to be compliant with the data protection requirements.

Lastly, in terms of governance, this report suggests that a subgroup of the Digital Criminal Justice Expert Group oversees the deployment of the solution. As it would be a complex solution, combining different elements, that subgroup should be responsible for the overall solution, avoiding a fragmented governance.

5.3 Communication Tool

The need to exchange requests for Mutual Legal Assistance, European Investigation Orders, European Arrest Warrants, etc., as well as messages, information and evidence related to a request or a case, in a secure and digital way, was clearly identified by practitioners in Member States, as well as practitioners in JHA Agencies and EU bodies, during the fieldwork conducted in the context of this study. Specifically, the business needs of the stakeholders in the cross-border criminal justice ecosystem which would need to be addressed by this solution are outlined in the figure below.

Figure 14: Communication Tool - Business needs mapping



Solution	Communication tool				
Business needs categories / Persona	Securely communicate and exchange information via digital means	Ensure interoperability across systems	Easily manage data and ensure its quality	Identify link between cases	Ensure data protection principles for all systems
Prosecutors	✓	✓	✓	✓	✓
JHA agencies and EU bodies	✓	✓	✓	✓	✓
Eurojust	✓	✓	✓	✓	✓
JIT	✓	✓	✓	✓	✓
National authorities	✓	✓	✓		✓

Consequently, there is a need for a communication tool that would:

- Enable the secure and structured electronic exchange of requests, MLAs, EIOs, etc., requests for support from Eurojust, follow up messages, information and evidence between all stakeholders in the Cross-Border Digital Criminal Justice ecosystem (for an overview of all exchanges of information to be covered, please refer to Figure 16 below).
- Be user friendly and accessible to all relevant end users.
- Ensure all information exchanged electronically is recognised by the judicial authorities and judicial practitioners in different Member States.
- Provide appropriate security and confidentiality.

This study considered several options to implement the required communication tool. These options were: to purchase a commercial off-the-shelf (COTS) product, to create a custom tool, to re-use the SIENA application developed by Europol, or to re-use the e-Evidence Digital Exchange System (e-EDES) being developed by the Commission.

Out of these options, e-EDES was found to be the most adapted to the needs of the Communication Tool because it is built specifically to cater to the needs of the European criminal justice community, it is based on common open standards/specifications and open source software, and is available to all Member States as of 2020.

Hence, this section focuses on the description of the e-Evidence Digital Exchange System (e-EDES) project, and proposes a vision for its future evolution in order to address all the business needs above.

As far as the EIF and the Sharing and re-use framework are concerned, this solution addressed the following recommendations:

Table 11: EIF and Sharing and re-use recommendations addressed by the e-EDES

European Interoperability Framework	Sharing and re-use framework
#6: Re-use and share solutions, and cooperate in the development of joint solutions when implementing European public services	#3: Communicate your needs
#8: Do not impose any technological solutions on citizens, businesses and other administrations that are technology specific or disproportionate to their real needs	#4: Define set of requirements supporting common business processes
#9: Ensure data portability, namely that data is easily transferable between systems and applications supporting the implementation and evolution of European public services without unjustified restrictions, if legally possible	#6: Apply business models that facilitate the co-creation, sharing and re-use of IT solutions
#15: Define a common security and privacy framework and establish processes for public services to ensure secure and trustworthy data exchange between public administrations and in interactions with citizens and businesses	#10: Decide the type of rights' attribution approach to be used as early as possible and inform all involved
#17: Simplify processes and use digital channels whenever appropriate for the delivery of European public services, to respond promptly and with high quality to users' requests and reduce the administrative burden on public administrations, businesses and citizens	#19: Design your IT solution to be extensible and modular
#18: Formulate a long term preservation policy for information related to European public services and especially for information that is exchanged across borders	#20: Design your IT solution to be scalable
#30: Perceive data and information as a public asset that should be appropriately generated, collected, managed, shared, protected and preserved	
#46: Consider the specific security and privacy requirements and identify measures for the	

provision of each public service according to risk management plans	

5.3.1 Possible scenarios

This section presents the possible scenarios to implement a communication tool between the different stakeholders in the Digital Criminal Justice ecosystem, and recommends the option to be pursued (which is further analysed in the following sections).

Indeed, four possible scenarios are envisaged for the implementation of the Communication Tool:

- **Scenario 1: Purchase a commercial off-the-shelf (COTS) product**

This scenario envisages the re-use of a commercial product to implement a communication tool for the all stakeholders involved in Cross-Border Digital Criminal Justice. There are multiple candidate products on the market, which can be customized to fit the specific needs described in this study.

- **Scenario 2: Create a custom-built tool**

This scenarios envisages to build a custom tool from scratch, using as a basis the high level requirements (i.e. business needs) defined in this study. This development could be done by the European Commission itself, an EU agency or body, or a consortium of Member States.

- **Scenario 3: Re-use the SIENA application**

This scenario proposes to re-use the SIENA application, which is a custom communication tool built and maintained by Europol to support cross-border communication and exchange of information in the domain of law enforcement.

- **Scenario 4: Re-use the e-Evidence Digital Exchange System (e-EDES)**

This scenario proposes to re-use the e-EDES solution currently being developed by the European Commission. The current e-EDES solution enables the digital exchange of European Investigation Order (EIO) and Mutual Legal Assistance (MLA) requests via a secure communication channel, as well as the exchange of subsequent messages and replies between competent national authorities in the Member States.

Specifically, the e-EDES solution is a reference implementation of a platform for users to exchange messages and information that is currently being developed by the European Commission together with Member States, with support of various projects (e.g. EVIDENCE2e-CODEX, Electronic Xchange of e-Evidences). The main technical element underlying e-EDES and used as “means of transmission” is e-CODEX, which is itself based on the e-Delivery technical infrastructure (for more information about e-CODEX, please refer to section 5.2.1.1.1). Figure 15 below provides an overview of the architecture of e-EDES.

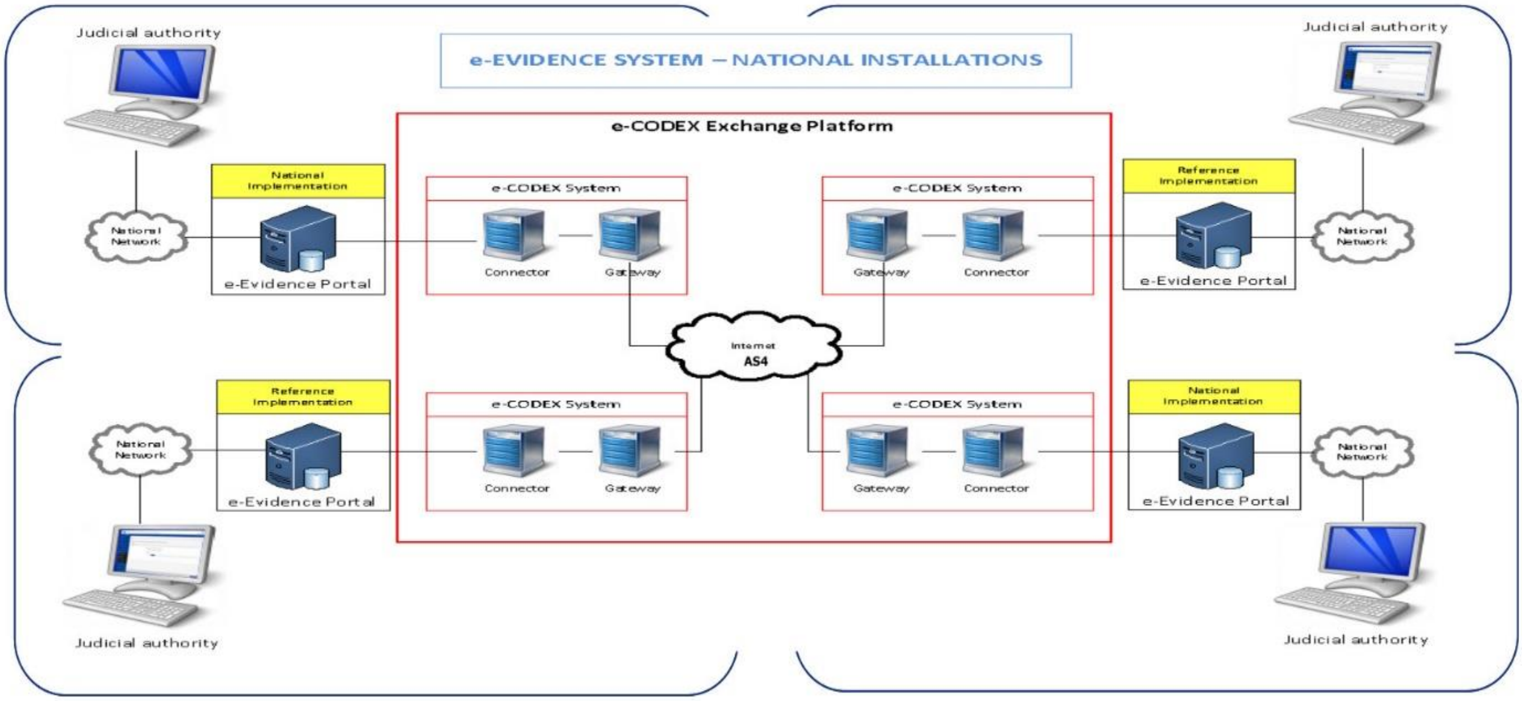


Figure 15: e-EDES – Architecture

As the development of e-EDES is ongoing, there are a number of planned developments that are being (or are planned to be) implemented in e-EDES in the near future. These developments are:

- The platform will not only allow the exchanges on the basis of European Investigation Order (EIOs) and Mutual Legal Assistance (MLAs), but it is also expected to be expanded to cover additional judicial cooperation instruments in the future.
- The platform will allow instant communication between stakeholders (similar to Europol's SIENA application), even if it not related to the exchange of a legal form.
- Support for electronic signatures[79] will be included.
- Machine translation[80] is included.
- Implementation of web services for Member States to access e-EDES is included.
- Eurojust will be given access to e-EDES. Currently Eurojust as an agency is not copied in exchanges of information over e-EDES (although Eurojust National Desks may receive the form in their capacity of prosecutor at national level). However, it was noted in the course of this study that it would be useful for Eurojust to be copied in the exchange of requests for mutual legal assistance, for the cases in which it is involved.

Therefore, this report suggests that Eurojust national members are given access to e-EDES, but initially only in their capacity as national judicial authorities. Eurojust national members, when involved by their national authorities in the issuing or executing phase of an EIO (or in the future for other instruments), should be able to receive information and communicate through e-EDES.

[79] More information about eSignature in section 5.9.5.2.

[80] More information about the machine translation solution of the European Commission, eTranslation, in section 5.9.5.3.

Moreover, future versions of e-EDES will contain implementation of features complementing the current Atlas tool of the EJN in criminal matters, so that the users of e-EDES are provided with a user friendly way to find a competent authority in another Member State.

In conclusion, this report recommends e-EDES as the preferred option to implement the communication tool for Cross-Border Digital Criminal Justice for the following reasons:

- It is tailored to the needs of the European criminal justice community: indeed, e-EDES and the underlying digital infrastructure on which it is based, e-CODEX (and e-Delivery), were built by and for the criminal justice community. Knowledge of the ways of working and legal instruments used by judicial practitioners in the EU is used for the design and implementation of e-EDES.
- It is based on common open standards/specifications and open source implementations: e-EDES is based on e-CODEX connector and the Domibus Gateway (which the reference implementation of eDelivery offered by the Commission), which are both open source. In addition, eDelivery is based on the AS4 open messaging standard. Consequently, both the e-CODEX connector and the Domibus Gateway are available for free.
- It will be available to all Member States in 2020: e-EDES and e-CODEX projects have already been piloted in several Member States. Moreover, by 2021 both projects are planned to be operational in all Member States.

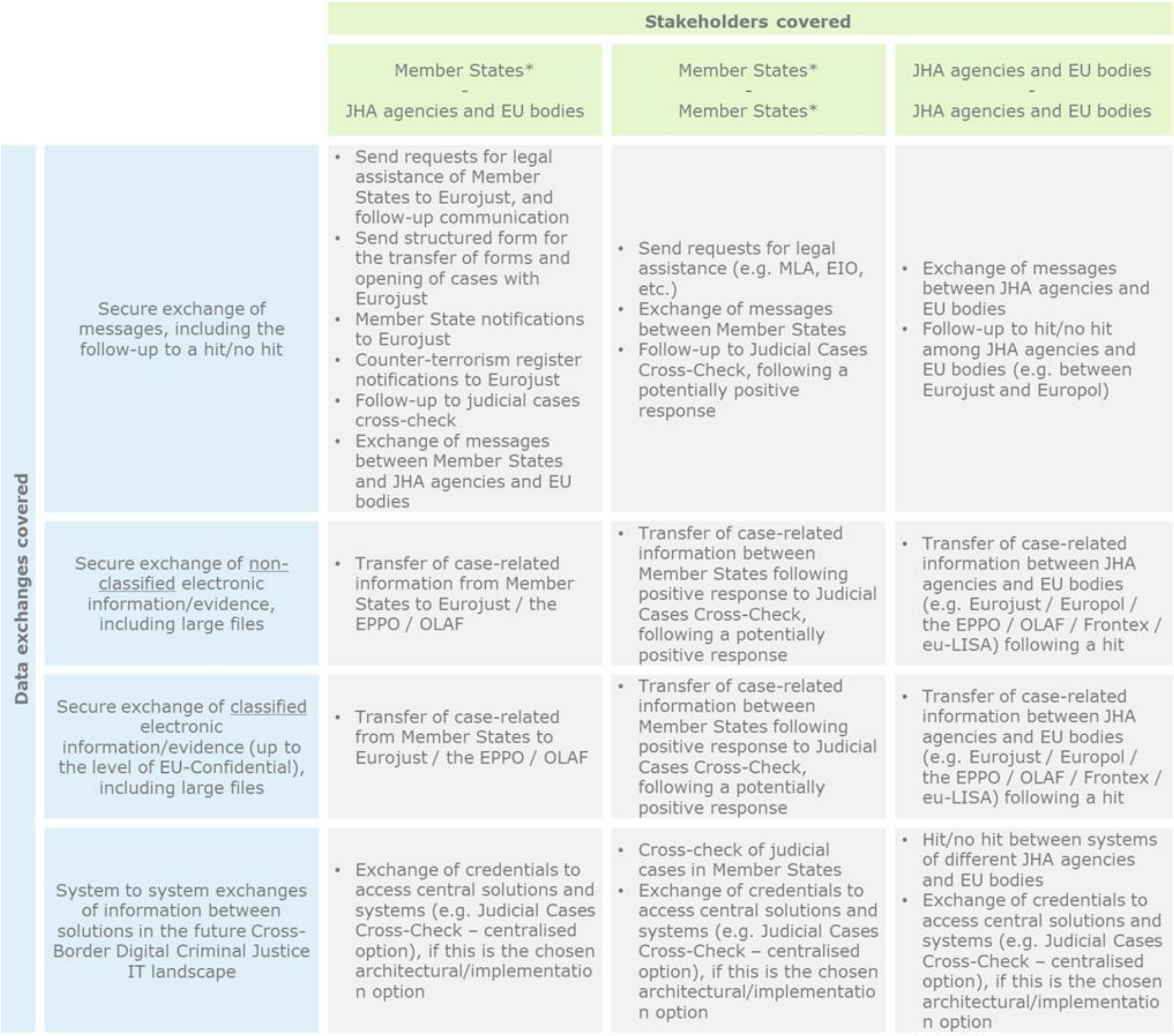
5.3.2 Presentation of the solution: future evolution of e-EDES

This report envisages e-EDES as becoming the reference means of communication for cross-border exchange of information and collaboration in the domain of criminal justice, much like the SIENA application developed by Europol is for the law enforcement community.[81] Indeed, it could be conceived as the future solution covering the majority of requests and exchanges of legal instruments, follow-up messages, information and evidence related to cross-border cases of criminal justice.

Moreover, the future e-EDES could be accessible to all stakeholders in the ecosystem, including practitioners and central authorities in Member States and JHA agencies and EU bodies, and it would cover all types of information exchanged in the context of Cross-Border Digital Criminal Justice. Examples of practical uses cases are described in Figure 16 below.

[81] Here we differentiate between the user application component of SIENA, which offers functionalities related to messaging, managing requests, handling codes for sensitive information, etc., and the secure communication channel component of SIENA, which is described in section 5.2.1.3.

Figure 16: Communication Tool - Use cases



		Stakeholders covered		
		Member States* - JHA agencies and EU bodies	Member States* - Member States*	JHA agencies and EU bodies - JHA agencies and EU bodies
Data exchanges covered	Secure exchange of messages, including the follow-up to a hit/no hit	• Send requests for legal assistance of Member States to Eurojust, and follow-up communication • Send structured form for the transfer of forms and opening of cases with Eurojust • Member State notifications to Eurojust • Counter-terrorism register notifications to Eurojust • Follow-up to judicial cases cross-check • Exchange of messages between Member States and JHA agencies and EU bodies	• Send requests for legal assistance (e.g. MLA, EIO, etc.) • Exchange of messages between Member States • Follow-up to Judicial Cases Cross-Check, following a potentially positive response	• Exchange of messages between JHA agencies and EU bodies • Follow-up to hit/no hit among JHA agencies and EU bodies (e.g. between Eurojust and Europol)
	Secure exchange of non-classified electronic information/evidence, including large files	• Transfer of case-related information from Member States to Eurojust / the EPPO / OLAF	• Transfer of case-related information between Member States following positive response to Judicial Cases Cross-Check, following a potentially positive response	• Transfer of case-related information between JHA agencies and EU bodies (e.g. Eurojust / Europol / the EPPO / OLAF / Frontex / eu-LISA) following a hit
	Secure exchange of classified electronic information/evidence (up to the level of EU-Confidential), including large files	• Transfer of case-related from Member States to Eurojust / the EPPO / OLAF	• Transfer of case-related information between Member States following positive response to Judicial Cases Cross-Check, following a potentially positive response	• Transfer of case-related information between JHA agencies and EU bodies (e.g. Eurojust / Europol / the EPPO / OLAF / Frontex / eu-LISA) following a hit
	System to system exchanges of information between solutions in the future Cross-Border Digital Criminal Justice IT landscape	• Exchange of credentials to access central solutions and systems (e.g. Judicial Cases Cross-Check – centralised option), if this is the chosen architectural/implementatio n option	• Cross-check of judicial cases in Member States • Exchange of credentials to access central solutions and systems (e.g. Judicial Cases Cross-Check – centralised option), if this is the chosen architectural/implementatio n option	• Hit/no hit between systems of different JHA agencies and EU bodies • Exchange of credentials to access central solutions and systems (e.g. Judicial Cases Cross-Check – centralised option), if this is the chosen architectural/implementatio n option

** Includes national authorities and prosecutors*

e-EDES should also fulfil the role of a secure telecommunication connection for the purposes of the EJN in criminal matters, as described in Article 9 paragraph 2 of the EJN Decision[82]. In addition, during the interviews conducted, the possibility of providing access to e-EDES to JIT members was requested (for those JIT members that do not have access to e-EDES in another capacity, e.g. prosecutor), to cover use cases which are specific to the running of JITs such as the setting up of JITs. The feasibility of this option could be further examined by comparing the functionalities offered by future e-EDES to those that would be required from the JIT Collaboration Platform (see section 5.5.1 for more information). It should also be assessed from a security and legal perspective.

Finally, in the future, e-EDES could be extended to private parties from which information may be requested in the context of certain investigations, and notably Online Service Providers (OSPs) from Europe and further afield.[83] Extending e-EDES to OSPs could offer EU authorities with a direct

[82] Council Decision 2008/976/JHA of 16 December 2008 on the European Judicial Network

[83] Example of European Online Service Providers (OSPs) include DE-CIX and Seznam. Other OSPs include Google, Microsoft, Facebook, Airbnb, etc.

and more rapid access to these companies, ensuring their requests would be handled faster and communication, which would be handled through a dedicated channel, is easier.

5.3.3 Technical assessment

The future evolution of e-EDES could be based on the same technical solution as the one currently being developed by the European Commission (which is based on e-CODEX[84]), to which additional integration and/or developments would need to be added in order to implement all envisaged functionalities.

The following technical requirements and/or constraints would have to be taken into account when designing the future e-EDES solution:

- Availability of the software for all prosecutors and other actors involved in cross-border cooperation:

  The future e-EDES should be available to all end users (i.e. prosecutors and other actors involved in cross-border cooperation) and be part of the tools they use to carry out their daily activities. To do so, it must be made available to end users through an easily accessible and user friendly user interface, and access management must be appropriately managed at Member State level (see below for more information about these activities).

- User interface:

  Member States can either re-use the e-EDES reference implementation built by the Commission or their own national implementation based on guidelines published by the Commission. When reusing the Commission's reference implementation, Member States can either re-use only the user interface (or platform), or a pre-configured e-CODEX node (the back-end), or both.

- Unique case/message numbering:

  The future e-EDES should ensure that each case file or messages that it handles has a unique identifier, to make it possible to trace all information flows. To implement this approach, a similar concept to the one implemented in Europol's SIENA application could be used, following the principles below:

  - A unique case identifier must be assigned to each case.
  - Each request, form, message, or document sent via e-EDES must be associated to a new or existing case.
  - Each request, form, message or document sent also has a unique identifier, which refers to the identifier of the associated case.

- User access (management) in Member States:

  User access would need to be managed at Member State level. In each Member State, there would be a different landscape of users involved.

[84] For more information about e-CODEX and the eDelivery digital infrastructure, please refer to section 5.9.5.1.

Moreover, the eDelivery and e-CODEX models on which e-EDES is based both offer built-in (or associated) mutual trust mechanisms. In eDelivery, the use of a Public Key Infrastructure (PKI) service ensures that information is exchanged between trusted parties in the network only and facilitates the dynamic registration and discovery of participants in the network. e-CODEX has implemented a "Circle of Trust", meaning that participating Member States accept the legal validity of documents and of information on identity and signatures coming from other Member States in the network. The assessment of the Circle of Trust and other legal requirements for e-CODEX can be found in section 5.2.1.1.1.

- Ensuring traceability and admissibility of evidence:

  The e-EDES solution is designed in order to ensure the traceability and subsequent admissibility of the evidence exchanged in front of court. To do so, it builds on the findings of the Evidence2e-CODEX project as well as on related publications.[85]

- Using a common vocabulary:

  During fieldwork in Member States, it was noted that the exchange of structured data forms is sometimes complicated due to the different interpretations of certain terms in the different legal systems of Member States (for instance, the definition and implications of the term 'victim' may vary from country to country). Therefore, a common set of definitions or interpretations of the terms is needed. This is already (partially) covered by e-EDES, as the e-CODEX technical infrastructure includes a methodology to ensure the mutual equal interpretation of legal terms. However, it could be further expanded to include more terms, and practitioners in Member States should be trained to use it.

- User training:

  It was also noted during field visits that practitioners (mainly prosecutors and judges) require training in order to learn how to use the EIO and MLA forms, and therefore it is strongly recommended to foresee trainings for the usage of the different legal forms for mutual legal assistance, as well as for the usage of the e-EDES tool, which would be radically extended in the future (based on the planned developments of the Commission, and the recommendations provided in this report).

- Maintenance of the eDelivery, e-CODEX and e-EDES specifications and solutions:

  The re-use of the eDelivery, e-CODEX and e-EDES reference implementation would imply that the software solutions and underlying specifications are maintained and kept up to date with regards to evolving technology on the long-term.

  Currently, the eDelivery Access Point is based on open specifications (AS4 profile) which is itself based on the ebMS 3.0 standard of OASIS, and other associated eDelivery services are also based on OASIS standards.[86] The eDelivery reference implementation is maintained by the European Commission (DIGIT). e-CODEX is currently maintained by a consortium of Member States, and the e-EDES reference implementation is maintained by the European Commission (DG JUST).

[85] For more information, please consult: https://evidence2e-codex.eu/a/deliverables and https://evidence2e-codex.eu/a/publications.

[86] More information here: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Services+eDelivery .

In the future however, the maintenance of these solutions might need to change and be transferred to an EU Institution (notably in the case of e-CODEX) in order to guarantee their sustainability. Potential candidates to do so include the Commission (DIGIT or DG JUST), or eu-LISA. For a further discussion on governance, please refer to section 5.3.6.

5.3.4 Security assessment

Without any doubt, all the described scenarios in section 5.3.1 have the ability to achieve an acceptable security assurance level, under certain assumptions. However, as explained in the same section, e-EDES is considered the best candidate as a communication tool for the DCJ target architecture.

The future evolution of e-EDES would offer a secure transport of messages, as it relies on e-CODEX e-Delivery platform. The messages exchanged by the future evolution of the e-EDES solution would support the follow-up of the hit/no-hit operation, as well as the secure transport of EU non-classified information and evidence, including large files. Furthermore, it would allow the secure transport of EU classified information and evidence, up to the level EU CONFIDENTIAL, including large files. Finally, the to-be e-EDES is foreseen to enable system to system exchanges of information between solutions in the DCJ target IT landscape.

The future evolution of the e-EDES solution would be chiefly operating at application layer and it is mainly relying on the CEF e-Delivery Building Block for the lower layers (i.e. transportation of its messages). From a security standpoint, e-EDES is fulfilling the security objectives for, at least, up to the transport level (refer to 5.2.3), which is sufficient at this level of analysis.

Securing the e-EDES enabled data exchanges at application layer requires a more in depth analysis. In principle, a risk assessment should be performed by the e-EDES enabled system owners in the DCJ target architecture, in order to identify potential risks at the application level. Based on which, security controls and requirements should be elaborated in order to make sure that e-EDES supporting systems and data are managed, operated and deployed in a secure manner.

The security controls and requirements for the future e-EDES solution should be designed, implemented and integrated in a secure way, but also, monitored for their operative effectiveness. They should cover the e-EDES interfaces and their associated communication channels. But also, the security hardening of information systems, including frontend and backend systems, supporting or involved in the e-EDES data exchanges, as part of the DCJ target architecture.

And finally, the security controls and requirements for the future e-EDES solution should define data security safeguards and measures required to protect data involved in e-EDES information exchange, against unauthorised access, in conformance with the DCJ target architecture's security policy and the applicable data protection regulations.

5.3.5 Legal and data protection assessment

In order to improve the possibilities to exchange electronic evidence between judicial authorities, the Council Conclusions of 9 June 2016 called for the establishment of a "secure online portal" for requests and responses concerning electronic evidence.[87] The European Commission is hence setting up the e-EDES platform, which would allow digital exchanges of requests for evidence and subsequent correspondence, including evidence, between EU competent authorities related to European Investigation Orders (EIOs) and Mutual Legal Assistance requests (MLAs) (the e-EDES platform does not itself have a legal basis). In the future, the platform is also expected to facilitate similar exchanges regarding additional mutual judicial cooperation instruments.

Nevertheless, as indicated in the technical assessment of the e-EDES solution in section 5.3.3, in order for it to function well, as a user-friendly communication tool for Cross-border Digital Criminal Justice, the following technical requirements should be taken into account when designing the evolution of e-EDES:

- Availability of the software for all prosecutors and other actors involved in cross-border cooperation.
- Unique case/message numbering.
- User access (management) in Member States.
- Using a common vocabulary.
- Maintenance.

These features are needed to correctly address the business needs of stakeholders. As the scope of e-EDES would be enlarged with new features and functionalities, it should be assessed to what extent a specific legal basis for these is required, while taking into account that Member States may have provided for a specific legal basis for exchanges over the system at the national level. These changes (specified in the bullet points above) are not changing the essence of e-EDES, but are adding significant elements bringing the solution to the next level. The e-EDES platform would become the Communication Tool for the exchange of information between stakeholders in criminal cross-border cases, becoming a key element in the area of Digital Criminal Justice.

Although a specific legal basis is not required for the system to be built or to operate (as per the Council conclusions of 9 June 2016), it would still be useful to endow e-EDES with a legal basis. This would allow strengthening the solution, which would become the mandatory communication tool for Cross-border Digital Criminal Justice in the future. It is advisable that this legal basis avoids relying on a circle of trust approach, in order to ensure the legal validity of transmitted documents and the participation in the system of all EU Member States.

The enactment of a new legal instrument should include elements such as the aim and objectives of the e-EDES platform, the high-level technical requirements, data protection requirements and security and privacy safeguards. As indicated in the technical assessment, the future e-EDES could be extended to private parties, from which information may be requested in the context of an investigation. Such access should be enshrined in the provisions of the legal basis.

As regards hosting, the initial solution is being developed by the Commission (DG JUST) as a reference implementation offered to the Member States, which are themselves legally responsible for its implementation within their national structures and in accordance with national law. The evolution of e-EDES could be thus remain in the hands of the Commission, or other entities could be considered. As the e-EDES platform would become the Communication Tool, eu-LISA could be

[87] Council conclusion on improving criminal justice in cyberspace, 9 June 2016, https://www.consilium.europa.eu/media/24300/cyberspace-en.pdf

involved either for its further technical development, or eventual hosting. In the latter case, the e-EDES legal basis should specify it, and the eu-LISA Regulation should be amended accordingly.

A relevant aspect to be considered is to which extent the platform functionalities can be further developed to ensure that applicable data protection principles and procedures can effectively be taken into account:

- As it is inherent to the requests and responses concerning evidences in the course of an investigation that personal data relating to different categories of data subjects are processed, the deployment of effective controls (procedures and IT measures) relative to the quality of the personal data are necessary to ensure that a distinction is made between suspects, persons convicted of a criminal offence, victims and other parties, such as witnesses, persons possessing relevant information or contacts, and associates of suspects and convicted criminals.[88] To the extent that personal data of vulnerable data subjects may fall into the described categories (e.g. children, elderly person), additional data protection measures are to be considered, such as the segregation of data flows or the interjection conditional steps (e.g. authorization) before the evidence is exchanged. The admissibility of the request falls under the types of proceedings for which the EIO can be issued[89] and the evidence sought in the course of an investigative measure is necessary only and insofar to fulfil the purpose of the investigation (e.g. no cross-border surveillance) and only in between the concerned Member States judicial authorities. To this end, procedures and security measures related to the monitoring of access rights of authorised end-users in the platform (e.g., prosecutors, judges or judicial authorities in Member States) and logging transactions' and monitoring capabilities are to be considered.
- If, in the event of an investigative procedure and evidence exchange, any inaccuracies are detected by the validating authority (e.g. erroneous data entries), the platform must allow for the interjection of sub-tasks procedures or flagging capabilities to raise the inconsistency and the deployment of cooperative sub-tasks to duly investigate and/or rectify it is initiated.
- Given the sensitivity of the personal data exchanged, data retention rules are considered to ensure that 1) when the transferring of the evidence is obtained, the executing authority should indicate whether it requires the evidence to be returned when no longer required by the issuing State[90]; 2) the storage of personal data in the platform to fulfil a transaction (exchange of evidence) is temporary and automatic deletion is deployed.
- Data security measures are considered to effectively address and mitigate the potential risks to the rights arising from the deployment of the platform (e.g. end-to-end encryption). To this end, a data protection impact assessment, covering all the personal processing operations foreseen in the platform, is recommended.

5.3.6 Governance

Refer to section 8.2 for an overview of the overall project governance.

[88] Directive 2016/680, Article 7.
[89] EIO Directive, Article 4.
[90] Supra, Article 13(3).

The e-EDES solution has been developed by the European Commission, in the framework of the e-Evidence Expert Group. Nevertheless, the solution would need to be to largely extended, and should thus be supervised by a different governance model.

In terms of strategic governance, a subgroup of the Digital Criminal Justice Expert Group should drive the development of the solution. The subgroup would thus monitor the status of the solution, providing the necessary strategic guidance, particularly in the context of the necessary synergies with the other DCJ solutions.

The IT implementation of the solution would be either in the hands of the European Commission, or eu-LISA. Concerning the latter, a Programme Management Board and an Advisory Group would be set up by the agency for the development of the solution. In both cases, the entity in charge of the implementation would cooperate with the subgroup.

Additionally, the Member States and the JHA agencies and EU bodies would need to support the IT implementation of the solution. The involvement of these stakeholders is key, as they would be the users of the final product. Their contribution would thus ensure that the solution offers the functionalities tailored to their needs.

5.3.7 Conclusion

This report envisages e-EDES as becoming the reference means of communication for cross-border exchange of information and collaboration in the domain of criminal justice. This solution would allow the exchange of requests for judicial cooperation, as well as subsequent messages, information and evidence digitally and securely. In addition to its main purpose of creating a trustworthy channel of communication between Member State authorities, the tool could be used for example by national prosecutors to transfer to Eurojust the case related data for the opening of cases in the Redesigned Eurojust CMS.

From a technical perspective, the future evolution of e-EDES would be based on the same technical solution as the one currently being developed by the European Commission (which is based on e-CODEX[91]). However, additional integrations and/or developments would need to be added in order to implement all envisaged functionalities.

In terms of security, this report concludes that e-EDES, which is based on e-CODEX and eDelivery, fulfils the security objectives at the transport layer. For the application layer, an additional risk assessment should be performed in order to identify potential risks on that level.

As for the legal basis, it should be noted that, while a specific legal basis is not necessary for the e-EDES platform to operate, the enactment of a legal basis would be useful to strengthen and reinforce the platform, which would become the DCJ Communication Tool. Besides this, an amendment to the eu-LISA Regulation might be necessary if the agency is mandated (by the legal basis of the e-EDES platform) with the hosting of the solution.

From a data protection perspective it should be investigated to which extent the platform functionalities can be further developed to ensure that applicable data protection principles and procedures can effectively be taken into account.

[91] For more information about e-CODEX and the eDelivery digital infrastructure, please refer to section 5.9.5.1.

Lastly, in terms of governance, a subgroup of the Digital Criminal Justice Expert Group could be in charge of the strategic governance of the solution. This implies that the subgroup would monitor and guide the development of the solution. However, the IT development of the solution would be under either the European Commission’s or eu-LISA’s responsibility. Lastly, the future users of the solution, being the Member States and the JHA agencies and EU bodies, would need to contribute to its IT implementation.

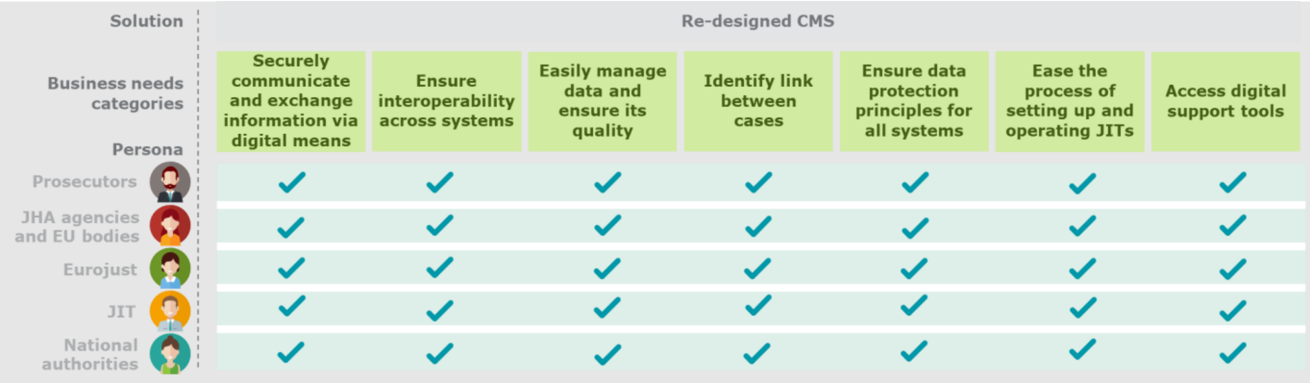
5.4 Redesigned Eurojust CMS

The redesign of the Eurojust Case Management System (CMS) is one of the key elements of the re-defined IT landscape for Cross-Border Digital Criminal Justice proposed in this study.

Indeed, according to the results of the survey conducted with Member States, 56% of respondents (to this question) were of the opinion that such a redesign is an essential need or necessary. Only 14% of the respondents indicated that it is slightly necessary, while only 5% mentioned it is not necessary.[92]

Moreover, according to interviews with representatives of JHA agencies and EU bodies and practitioners from several Member States, the redesign of the CMS is very much needed and would help solve several of the business needs identified. Please see the figure below for an overview of the business needs and personas concerned, and refer to section 3 for more details.

Figure 17: Redesigned Eurojust CMS - Business needs mapping



Solution	Re-designed CMS						
Business needs categories Persona	Securely communicate and exchange information via digital means	Ensure interoperability across systems	Easily manage data and ensure its quality	Identify link between cases	Ensure data protection principles for all systems	Ease the process of setting up and operating JITs	Access digital support tools
Prosecutors	✓	✓	✓	✓	✓	✓	✓
JHA agencies and EU bodies	✓	✓	✓	✓	✓	✓	✓
Eurojust	✓	✓	✓	✓	✓	✓	✓
JIT	✓	✓	✓	✓	✓	✓	✓
National authorities	✓	✓	✓	✓	✓	✓	✓

This report presents key functionalities, implementation options, as well as security, legal and data protection, and technological considerations for the Redesigned Eurojust CMS. However, these functionalities and considerations must be further assessed and detailed when launching the design process, during which system specifications would be drafted. As noted during the Expert Group Meeting of 13-14 January 2020, Member States may be involved in the design of the CMS given that, on the one hand, they are key users of the Eurojust CMS in their capacity of Eurojust contact points at national level or Eurojust National Desks, and, on the other hand, national prosecutors may have direct access to it in accordance with Article 25 of the Eurojust Regulation.

As far as the EIF and the Sharing and re-use framework are concerned, this solution addresses the following recommendations:

[92] 29% of the participants have no opinion of the matter. In this regard, it must be noted that the majority of respondents to the survey do not use Eurojust CMS.

Table 12: EIF and Sharing and re-use recommendations addressed by the Redesigned Eurojust CMS

European Interoperability Framework	Sharing and re-use framework
#5: Ensure internal visibility and provide external interfaces for European public services	#3: Communicate your needs
#8: Do not impose any technological solutions on citizens, businesses and other administrations that are technology specific or disproportionate to their real needs	#10: Decide the type of rights' attribution approach to be used as early as possible and inform all involved
#9: Ensure data portability, namely that data is easily transferable between systems and applications supporting the implementation and evolution of European public services without unjustified restrictions, if legally possible	#18: Check the reusability of existing solutions before developing a new one
#12: Put in place mechanisms to involve users in analysis, design, assessment and further development of European public services	
#15: Define a common security and privacy framework and establish processes for public services to ensure secure and trustworthy data exchange between public administrations and in interactions with citizens and businesses	
#17: Simplify processes and use digital channels whenever appropriate for the delivery of European public services, to respond promptly and with high quality to users' requests and reduce the administrative burden on public administrations, businesses and citizens	
#19: Evaluate the effectiveness and efficiency of different interoperability solutions and technological options considering user needs, proportionality and balance between costs and benefits	
#30: Perceive data and information as a public asset that should be appropriately generated, collected, managed, shared, protected and preserved	
#46: Consider the specific security and privacy requirements and identify measures for the provision of each public service according to risk management plans	

5.4.1 Presentation of the solution

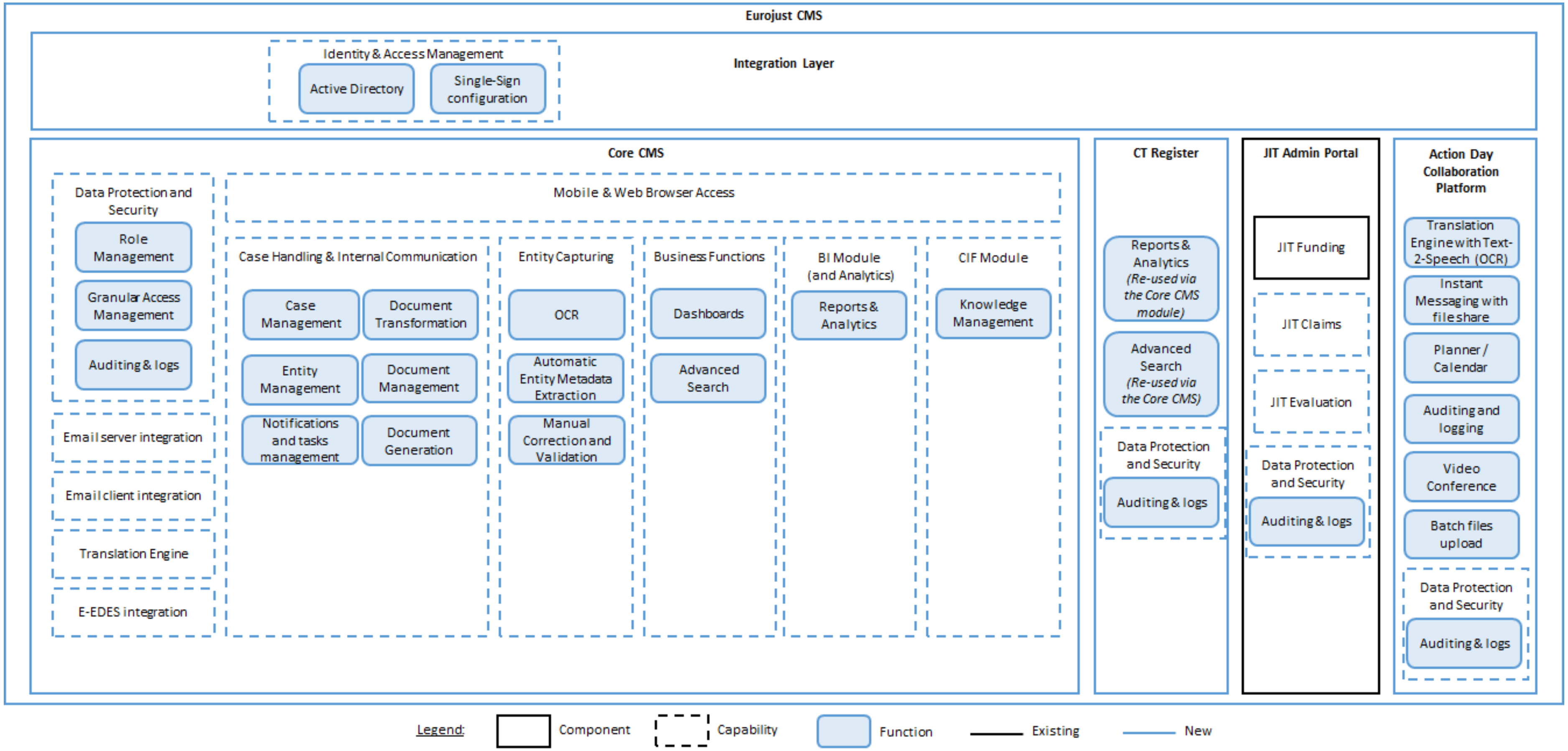
This section describes the high-level components, capabilities and functionalities of the Redesigned Eurojust CMS. For an overview of all capabilities and functionalities, please refer to the figure below.

The Redesigned Eurojust CMS would be composed of five main logical components, which in turn are composed of one or several capabilities and/or functions. The main logical components are:

- The Core CMS.
- The Counter-Terrorism Register.
- The JIT Admin Portal.
- The Action Day Collaboration Platform.
- The Integration Layer.

These logical components are further described in the following sub-sections.

Figure 18: Re-designed Eurojust CMS



5.4.1.1 Core CMS

The Core CMS component[93], as part of the Redesigned Eurojust CMS, is the main operational system supporting the daily activities of the Eurojust National Desks, i.e. the registration, handling and recording of all cases of cross-border judicial cooperation which are supported by Eurojust. To be able to do so, the core CMS must support certain capabilities and functionalities.[94] These capabilities of the core CMS, which are further detailed in the section below, are the following:

1. Identity & Access Management (IAM)
2. Email server integration (inbound)
3. Email client integration (outbound)
4. e-EDES integration
5. Translation engine
6. Mobile & web browser access
7. Case handling & internal communication
8. Entity capturing
9. Business functions
10. Data protection and security
11. Business Intelligence (BI) Module
12. Case Information File (CIF) Module

5.4.1.1.1 Capabilities

1. Identity & Access Management (IAM)

This capability would allow the secure management of user identities and access permissions for internal Eurojust users to access Eurojust applications. It would ensure that users are who they say they are (authentication) and that they can access the cases and resources that they have permission to use (authorisation).

This capability would include several functions:

- Active Directory: this function would enable storage and management of user identities and access permissions to applications in the Eurojust domain.
- Single Sign-On configuration: this function would allow configuration and integration to a Single Sign-On facility, if available at the time of development, to enable the user to securely sign-on to multiple independent applications while using just one set of authentication credentials.

It should be noted that although this IAM component is conceptually represented as being outside of the Redesigned Eurojust CMS in Figure 18 (as from an architectural perspective, Eurojust should ideally have one IAM component federating identity and access management for all of its applications), in practice it may be included as part of a vendor solution.

This report also recommends that authentication and authorisation for external users is managed by the Eurojust Integration Layer (see section 5.4.1.5). The Integration Layer would notably

[93] An application component is defined as an encapsulation of application functionality aligned to implementation structure, which is modular and replaceable. It encapsulates its behavior and data, provides services, and makes them available through interfaces (source: ArchiMate Glossary).

[94] An application function is defined as automated behaviour that can be performed by an application component (source: ArchiMate Glossary).

manage system to system interactions, by authorising external systems to send requests to Eurojust applications (or not).
Finally, all incorporated and interconnected systems (e.g. search engine) must be compatible or configurable with the permission requirements for the case handling, and on an entity level. For instance, if one Member State gives access to a case to another Member State (and the remaining Member States don't have access to it), these permission limitations must be respected in the search engine as well.

2. Email server integration (inbound)

This capability would allow users to add emails to existing cases and file them in the CMS, to create new Temporary Work File (TWF) IDs from selected mails and to add calendar records to existing cases (or store them as calendar records in the case history).

3. Email client integration (outbound)

This capability would allow users to send outgoing mails or meeting invitations from the CMS to external parties.

4. e-EDES integration

This report recommends the use of e-EDES amongst all stakeholders involved in Cross-border Digital Criminal Justice (including national authorities and prosecutors in Member States, as well as JHA agencies and EU bodies), and as such, there is a need to integrate the Redesigned Eurojust CMS with it. This capability would allow the internal CMS users to add e-EDES messages to existing cases and file them in the CMS and to create new Temporary Work File (TWF) IDs from selected e-EDES messages.

This integration could be done either through connecting the Redesigned Eurojust CMS to its future e-CODEX connector (or the e-Delivery access point). Alternatively, there could be an integration with the front end provided by e-EDES.

In addition, e-EDES should contain a workflow allowing national authorities to request support or exchange information with Eurojust through a structured form.

5. Translation engine

Eurojust's involvement in cross-border cases requires receiving, understanding and translating documents and information drafted in different languages, and therefore there is a need for a capability enabling automatic translations. This module might be offered as an internal functionality of the chosen CMS solution or by using the CEF eTranslation Building Block, which is further described in section 5.8.

Moreover, sizing and processing requirements must be taken into account when selecting a solution to implement this capability, as there might be a need for a software that can support large quantities of data (for instance, if each document is multiplied by all official languages).

6. Mobile & web browser access

This capability would allow users to access the CMS either using their corporate laptops/PCs or via a web browser using their mobile devices. In both cases, users would be able to create Temporary

Work File (TWF) IDs, access the case overview, case history and initiate/manage specific requests. While designing this functionality the following aspects need to be taken into account:

- Multi factor authentication should be used to access CMS information.
- Browser based access to CMS should only be available on Eurojust phones.
- It should not be possible to access the CMS from phones if the CMS contains EU CONFIDENTIAL information.

7. Case handling & internal communication

This capability would include the following functions:

- Case management: this function would be responsible for the handling of TWFs and related supporting documents and communication. It should provide functionalities enabling general case management, the digital filing of the case files, and the use of keywords for tagging/flagging cases. It would also allow to manage meetings/events related to cases.
- Entity[95] management: this function would be responsible for the management of create, read, update and delete operations (also called "CRUD operations") on different entities.
- Notifications and tasks management: this function would allow users to manually send out tasks and notifications to other CMS users, facilitating Eurojust internal communication. It would also allow users to set up the automatic generation of tasks and notifications based on events in the Redesigned Eurojust CMS (such as the creation of a new case).
- Document transformation: it would allow users to convert documents between formats (e.g. Word to PDF, ODT, etc.) or to split/merge PDFs.
- Document management: it would allow users to attach/store documents and emails to a case and manage them. This would include functionalities such as versioning control and document annotation.
- Document generation: it would allow users to manage templates and to generate documents based on these templates with existing meta-data from the CMS.

8. Entity capturing

This capability, being implemented as a part of the onsite solution, would include the following functions:

- Optical Character Recognition (OCR): it would allow users to convert images of typed, handwritten or printed text (coming from scanned documents or photos) into digital text.
- Automatic Entity Metadata Extraction: it would allow users to automatically identify metadata and entity types within documents/emails with the help of different algorithms. It would also allow crosschecks against existing entities (to identify potential matches) or look-ups against other data (for the purpose of metadata enrichment).
- Manual Correction and Validation: it would allow users to perform changes on identified entities, such as adding fields not identified by the system, correcting names, etc.

9. Business functions

This capability would include the following functions:

[95] In IT language, an entity refers to any singular, identifiable and separate object. In the context of the Core Eurojust CMS, examples of case entities include physical and legal persons (suspects), address, bank account, criminal or terrorist organisations, identity documents.

- Dashboards: it would allow the visualisation of the most important operational or analytical report information, providing at-a-glance information for monitoring and decision-making.
- Advanced search: it would allow users to find back information stored in the Redesigned Eurojust CMS, within the constraints of users' access permissions, through the following access points:
  - Search within a case.
  - Search within communications/emails across cases.
  - Search within documents across cases.
  - Search within entities across cases.
  - Search within the Case Information Files (CIF) across cases.

  Searches could be set up to run in a manual way, as described above, or in an automatic way, meaning for instance that the user could be notified when there is a match between an entity in the case s/he is working on, and an entity in another case.

10. Data protection and security

This capability would include the following functions:

- Role management: it would allow the secure management of user identities and access permissions for applications in the Eurojust domain. It would allow authentication and authorisation of the logged-in users.
- Granular access management: it would allow managing the access permissions to the CMS and also case-by-case granular access permissions, to determine who can see or modify a specific case or even some elements within that case, e.g. entities, documents, etc. (based on the identities provided by the IAM capability).
- Auditing: it would allow to keep a trail of who did what and when regarding a certain operation. The CMS should support the logging of all users actions, such as entries, transactions, modifications, sharing, disclosure, transfers, printing, editing, erasure, searching of data and should provide a complete audit trail. It would also enable the consolidated reporting across the different log stores.

11. Business Intelligence (BI) Module

The BI module may be offered by a module part of the CMS solution or an add-on module, and would also be tightly integrated with the Counter-Terrorism Register component, which in turn is tightly integrated with the CMS system. This capability would be used to produce reports, dashboards and analytics.

More specifically, it would allow the production of operational reports based on case metadata and entities data, that can be used as input for dashboards as well as analytical reports (predictive and prescriptive). It would also allow for interpreting and discovering patterns and trends through data and process mining.

12. Case Information File (CIF) Module

The CIF module would be the knowledge management capability of the CMS, and would allow knowledge sharing, i.e. the sharing of lessons learned.

It would incorporate the following high-level functions (which are to be assessed against the business functions currently covered by the CIF application at Eurojust):

- Prefilling information from the TWF and the case during the case handling phase.
- Sending standard event-based notifications to user, in order to document lessons learned.
- Provide a user interface (i.e. a page) for documenting lessons learned in each step of the process (and not only when case is closed). This would include generating notifications/tasks for case workers when relevant facts happen, such as the change of crime type while the handling of the TWF, so that they can record lessons learned linked to that fact.
- Making documented knowledge easily accessible and searchable, thus supporting proper knowledge management.

5.4.1.2 Counter-Terrorism Register

Council Decision 2005/671/JHA requires Member States to provide Eurojust with information concerning terrorist offences. Therefore, a Counter-Terrorism Register (CT Register) was launched at Eurojust on 01/09/2019 to help prosecutors coordinate more actively and to identify the suspects or networks that are being investigated in different countries. The existing CT Register is an application which has limited functionalities and requires extensive manual intervention. It is supported by a special template which is filled-in and provided to Eurojust by the Member States. Eurojust then manually feeds this information provided to the CMS.

However, Council Decision 2005/671/JHA is not fully implemented due to the absence of secure and automated means of transmission fitting the sensitivity of the data concerned. Indeed, Eurojust implemented the current CT Register as an intermediary solution in order to address the Council Decision’s requirement, while aiming to eventually set up in the near future a proper application in order to register any of the ongoing counter-terrorism proceedings. This would be achieved through the development of a specific component in the Redesigned Eurojust CMS, which would be associated to a secure channel of communication.

Therefore, the CMS should include specific user interfaces for data entry, consultation and related services. It could also potentially need to be exposed to Member States’ client applications as well as potentially provide access to designated persons in the Member States who are entitled to register such information.

We note that Member States have identified the need for a ‘European judicial counter-terrorism register’ at Eurojust. Indeed, based on our survey results, 26% of respondents consider the counter-terrorism register as an essential need, 35% as necessary, only 8% as slightly needed, and only 1% indicated it is not necessary.[96]

The capabilities detailed below are:

1. Reports & Analytics
2. Data Entry and Advanced Search

5.4.1.2.1 Capabilities

This section describes the functions of the future CT Register as an integral part of the Redesigned Eurojust CMS.

[96] 29% of the respondents had no opinion.

1. **Reports & Analytics**

The Core CMS business intelligence and advanced search functions should be integrated and re-used in the context of the CT Register. This would allow for the identification of links between data contained in the Core CMS and the CT Register, by ensuring that both datasets are cross-matched, analysed and classified properly.

2. **Data Entry and Advanced Search**

Users who would be granted access to this function of the CMS would be able to make combined searches on data contained in the Core CMS and the CT Register, to identify links between ongoing judicial proceedings and convictions related to counter-terrorism investigations.

Moreover, in the scenario where Member States would receive direct access to the Redesigned Eurojust CMS, the customisation and development of the aforementioned CMS functions would be required, as well as the development of special pages and services for Member States to enter information about judicial proceedings and convictions in the context of counter-terrorism investigations.

While the architecture model incorporates the CT Register component into the CMS, in practice there are **two implementation options**:

a) Re-use and refactor the existing CT Register to be tightly integrated with the CMS (through a common advanced search functionality and data synchronisation with the CMS), while providing new pages and possibly exposing services to Member States systems.
b) Re-build the CT Register as an internal functionality of the CMS with configurable pages for data searching and entry. This option must be examined against the off-the-shelf capabilities of the chosen CMS solution (when designing the Redesigned Eurojust CMS).

5.4.1.3 JIT Admin Portal

A Joint Investigation Team (JIT) is an international cooperation tool based on an agreement between competent authorities (both judicial, such as prosecutors and investigative judges, and law enforcement) of two or more Member States, established for a limited duration and a specific purpose, to accomplish criminal investigations in one or more of the involved Member States.

Since 2009, Eurojust has been supporting JITs' operational activities via financial means. The financing of JITs by Eurojust helps to ensure that JITs' activities are not hampered by financial and organisational constraints linked to the cross-border nature of the cases. The types of costs covered by Eurojust's funding are: travel and accommodation costs, interpretation and translation costs, costs related to the transport of items (e.g. evidence), and logistical support in the form of the loan of equipment.

The JIT Admin Portal was launched in January 2018 to simplify the submission of funding applications and ensure it is done through an online secure platform. The application for funding is open to judicial and/or law enforcement authorities, for JITs involving EU Member States and JITs involving EU and non-EU states, as well as Eurojust National Desks that are invited to participate in the JIT.

The current JIT Admin Portal is a tool supporting the administration of JIT grants. More specifically, to ease the grant application process, JIT members can fill in the web forms and submit their requests for grants via the JIT Admin Portal. It is thus used for the administration of the grants for a JIT, rather than for tasks linked to the actual judicial co-operation (e.g. evaluating the performance of the JITs).

However, based on the feedback received from representatives of JHA agencies and EU bodies, practitioners from several Member States and experts from Member States (during specific interviews and the Expert Group Meeting of 13-14 January 2020), it is recommended to extend the current system to cover two additional processes: the administration of JIT claims, and the evaluation of JITs. Accordingly, the conceptual architecture proposes to include the following capabilities in the JIT Admin Portal:

1. JIT Funding
2. JIT Claims
3. JIT Evaluation

5.4.1.3.1 Capabilities

1. JIT Funding

This capability supports the drafting and submission of applications for financial assistance for cross-border operations related to JITs. It is based on the functionalities already offered by the JIT Admin Portal.

More specifically, the following functionalities would be provided:

- Performing basic checks on the funding applications, for instance to check that one JIT has not already received funding in the call for proposals of the preceding period (already existing in the current JIT Admin Portal).
- Supporting the process of handling applications at the side of Eurojust, for instance by setting tags and statuses on the different cases (already existing in the current JIT Admin Portal).
- Sending tasks, reminders and notifications to the different parties involved in the application process, for instance when the deadline to submit the funding request is approaching (new functionality).
- Enabling the collaborative online drafting of funding application forms for the different Member State representatives involved (new functionality).
- Providing a messaging functionality to help the different parties (both at the side of the JIT and at the side of the Eurojust JITs Network Secretariat) collaborate on applications (new functionality).
- Enable the electronic signature of forms by the different parties involved (new functionality).
- Enable the online (secure) submission of the forms to Eurojust (already existing in the current JIT Admin Portal).

2. JIT Claims

This capability would support the claiming of reimbursement of eligible costs foreseen under the JIT funding agreement. It would be a new functionality which is not supported by the current JIT Admin Portal. As a general rule, these costs must be incurred in the three-month action period following the awarding of JIT funding.

To do so, the following functionalities would be provided:

- Sending tasks, reminders and notifications to the different parties involved in the claims process.
- Supporting the process of handling requests at the side of Eurojust, for instance by setting tags and statuses on the different cases.
- Providing a messaging functionality to help the different parties (both at the side of the JIT and at the side of the Eurojust JITs Network Secretariat) collaborate on claims.
- Enabling the online submission of the supporting documents (such as invoices and transport tickets) to Eurojust.
- Providing a repository of reference documents (such as the reimbursement checklist).

Other functionalities already developed in the context of JIT Funding capability could be re-used in the JIT Claims one, such as:

- Enabling the collaborative online drafting of the funding application forms for the different (Member) State representatives involved.
- Enabling the electronic signature of forms by the different parties involved.
- Enabling the online (secure) submission of the forms to Eurojust.

In addition, Eurojust may want to consider the integration of the payment process into the JIT Admin Portal. This would include supporting the workflows related to payment approval, and integration of a payment tool, in order to be able to provide rapid reimbursement to the different parties.

3. JIT Evaluation

This capability would support the process of evaluating a JIT, once its operations are over.

To do so, the following functionalities would be provided:

- Filling in and submitting the JIT evaluation forms electronically into Eurojust JIT Admin Portal.
- Extracting reports and analysing the evaluation results.
- Recording any additional (unstructured) information provided regarding the evaluation of a JIT (for instance, if the output of the JIT is discussed during a meeting).

5.4.1.4 Action Day Collaboration Platform

In the course of this study, interviewed practitioners and experts from Member States expressed the need for a collaboration and information platform to be used during action days, to support collaboration between different parties not formalised under the structure of a JIT.

5.4.1.4.1 Capabilities

Consequently, the Action Day Collaboration Platform would need to support the following capabilities:

- Integration with Eurojust Core CMS (through the Eurojust integration layer), which would offer possibilities to:
  - Extract mutual legal assistance request forms (European Investigation Orders, European Arrest Warrants, etc.) from the Core CMS to use them during the action day and allow participants to update them in real time. This is currently burdensome as it is all done manually in Excel, requires coordination by phone, etc.

    - Access the CMS to retrieve the judicial cooperation instruments (JCI) used for a particular case, as additional JCI may be exchanged on the action day.
    - Enable the transfer of data at the end of the action day (including results such as pictures, documents, etc.) to the Core CMS, and potentially to Europol.
- Monitoring of activities during the action day.
- Status of actions, to be visible to all participants.
- Live status updates.
- Large files transfer for the upload of evidence to the Core CMS integrated with the Large Files Solution.
- Secure storage of the information and evidence exchanged.
- Approval workflow (for all parties) for the creation of press releases on the action day. Currently press releases are created on the action day, and the documents are exchanged in order to get approval to publish.
- Reporting of the results of the meeting (e.g. number of confiscations etc.).
- Send/receive messages instantly, which may include pictures, videos, etc. Messages could be sent only to one recipient, or to many recipients (e.g. all participants in the action day).
- Do video calls/conferences.
- Enable real-time planning during action days.
- Ease collaboration and coordination, using tasks and notifications.
- Enable automatic translation.
- Ensure the traceability (and admissibility) of the information and evidence exchanged.

This Action Day Collaboration Platform would need to offer to a large extent the same functionalities as those that would be offered by the JIT Collaboration Platform, such as the secure exchange of instant messages, as well as information and evidence, the possibility to do video conferences, etc.

However, there are three notable differences between both platforms. First, the above-mentioned functionalities need to be adapted to the different timeframes during which both platforms would be used. Indeed, while a JIT can last from a few months up to a few years, the collaboration linked to an action day will only last a few months at most. Second, due to the different purposes and the different applicable legal bases[97], the two collaboration platforms should be hosted in different places. The Action Days are coordinated by Eurojust, and are thus based on the Eurojust Regulation. It should be therefore based in the Eurojust domain. On the other hand, JITs are a cooperation instrument used by Member States and JHA agencies and EU bodies. A JIT might take place without Eurojust being involved. Consequently, it is advisable to host the JIT Collaboration Platform outside the Eurojust domain, i.e. in another entity.

5.4.1.5 Integration Layer

Within the domain of Eurojust, the architecture would contain different components. In order to avoid that each component would have one on one integration with other components, there is a need to have a clear integration layer. Such an integration layer would ensure that all components within the Eurojust domain are well integrated in a sustainable and maintainable way. Furthermore, the Integration Layer would also provide the functionality to allow communication

[97] The possibility of setting up a Joint Investigation Team between Member States is provided in Article 13 of the 2000 Mutual Legal Assistance Convention, and the Framework Decision 2002/465/JHA, while the Action Days are coordinated by Eurojust, and are thus based on the Eurojust Regulation.

with external stakeholders by allowing Eurojust components to offer services to the external stakeholders via this gateway, as far as possible in line with the applicable legal framework.

5.4.2 Technical assessment

The technical assessment below provides an assessment of possible implementation options, vendor solutions, and general technical considerations (see section 0) to be taken into account when designing the Redesigned Eurojust CMS.

5.4.2.1 Core CMS

5.4.2.1.1 Market overview

This section aims at presenting an overview of the CMS market, the key players, as well as their relevant offerings. The scope includes the possible solutions to replace the current Eurojust CMS with an improved solution.

The present study re-assesses the findings of previous studies for the redesign of the CMS and has come up with the list of solutions found below. The approach has as a basis the set of requirements identified in the previous studies and builds on them with additional requirements linked to interoperability and integration with new solutions proposed in this study to support the future of Cross-border Digital Criminal Justice.

Historically, customer-introduced customisations of commercial off-the-shelf (COTS) case management applications have been difficult and complex to maintain, mainly because of the need to merge the custom changes with ongoing vendor changes and enhancements. The introduction of model-driven Business Process Management (BPM) platforms, i.e. Case Management Platforms, tries to address this challenge. Indeed, solutions based on a Case Management Framework (CMF) are faster to develop and easier to adapt, without major limitations in applying unique requirements.

The market sees the CMFs as a faster and easier approach to creating and maintaining a unique solution for a CMS. CMFs can be dynamically configured and reconfigured, extended, integrated, and they are interoperable with other applications. Case Management Frameworks implement "out of the box" case management entities and provide architectural patterns and capabilities relevant for the implementation of a case management solution.

In line with previous studies on the redesign of the Eurojust CMS and Eurojust vision of the CMS as a platform, this study also sees the best potential for replacing the Eurojust CMS in a CMF solution. However, it must be pointed out that additional services should be required to build the more specialised requirements.

Finally, other business domains would benefit from a CMF on case management that can be re-used in several domains. Such opportunity is already taken into account by the European Commission. The Secretariat-General (SG) of the European Commission as well as DIGIT partake the steering of the Case Management Rationalisation project which realised the CASE@EC case management platform developed by several European Commission DGs and evaluated in this study.

5.4.2.1.2 Possible vendor solutions

The following vendors and their solutions have good potential for inclusion into the future IT landscape of Cross-Border Digital Criminal Justice. This choice is supported by analyses and rankings of the vendors and their products produced by third parties.

The following 3 solutions were analysed in the context of this study:

- IBM's Business Automation Workflow
- Pega's Investigative Case Management
- CASE@EC

Table 13: Description of CMS Solution 1 - IBM Business Automation Workflow

CMS Solution 1	
Vendor	IBM
Solution	IBM® Business Automation Workflow
Solution Type	Case Management Framework (CMF)
Description	IBM® Business Automation Workflow combines IBM Business Process Management with IBM Case Manager, and is now an available product in the IBM Digital Business Automation offering. The new IBM® Business Automation Workflow combines business process management and case management capabilities in one workflow solution. It integrates the capabilities of business process and case management into a single workflow offering. It unites information, process, and users to provide a full view of work.
EU integrators / service providers	Extended network of partners/services providers from leading consulting firms in the EU.
Strengths	• Available as a hosted service and for on-premises installation. • IBM offers a more complete list of modular solutions in the same platform, thus covering most of the capabilities in the EJ CMS architecture. • Large certified partner network for IBM Case Manager. • Mentions by Analysts Sources: Leader in the Gartner magic quadrant for BPM-Platform-Based Case Management Frameworks.
Weaknesses	IBM is not committed to providing application solutions — its strategy for this emerging market depends on partners.

Table 14: Description of CMS Solution 2 - Pega investigative case management

CMS Solution 2	
Vendor	Pega Systems
Solution	Pega investigative case management on Pega Government Platform
Solution Type	Case Management Framework (CMF)
Description	PegaSystems is no/low-code application development platform which includes BPM and Case Management, Mobility, Robotic Process Automation (RPA), Social (chatbots and virtual assistant), Analytics and Artificial Intelligence (AI) powered decision-making tools. Pega's Investigative Case Management (ICM) framework is built specifically for government organizations to accelerate solution delivery, improving overall total cost of ownership. ICM offers efficient, user-friendly tools, including investigative-specific case types, portals, processes, geospatial capabilities, dashboards, visualization tools, and pre-built integrations. Pega Government Platform delivers a robust set of investigative management specific processes, portals, and dashboards that are fully configurable and extensible to align with specific organizational missions on any architecture – cloud, on premise, or both.
EU integrators / service providers	Extended network of partners/services providers from leading consulting firms in the EU.
Strengths	• Available as a hosted service and for on-premises installation. • Mentions by Analysts Sources: Named a leader in the Gartner Intelligent Business Process Management Suites report.
Weaknesses	• All components of the EJ CMS might not be covered via Pega's platform modular solutions. Additional capabilities would need to be purchased to complete the architecture. • Methodology and programming model for developing Pega functionalities is unique and highly dependent on the Pega platform. • Hardcoding business logic outside Pega's models would hinder follow-up of global changes in the Pega business model. Therefore, data management follows business flows and not vice versa, which potentially has impact on custom functionality. • Pega architecture is usually not data-driven but rather driven by BPM and workflow.

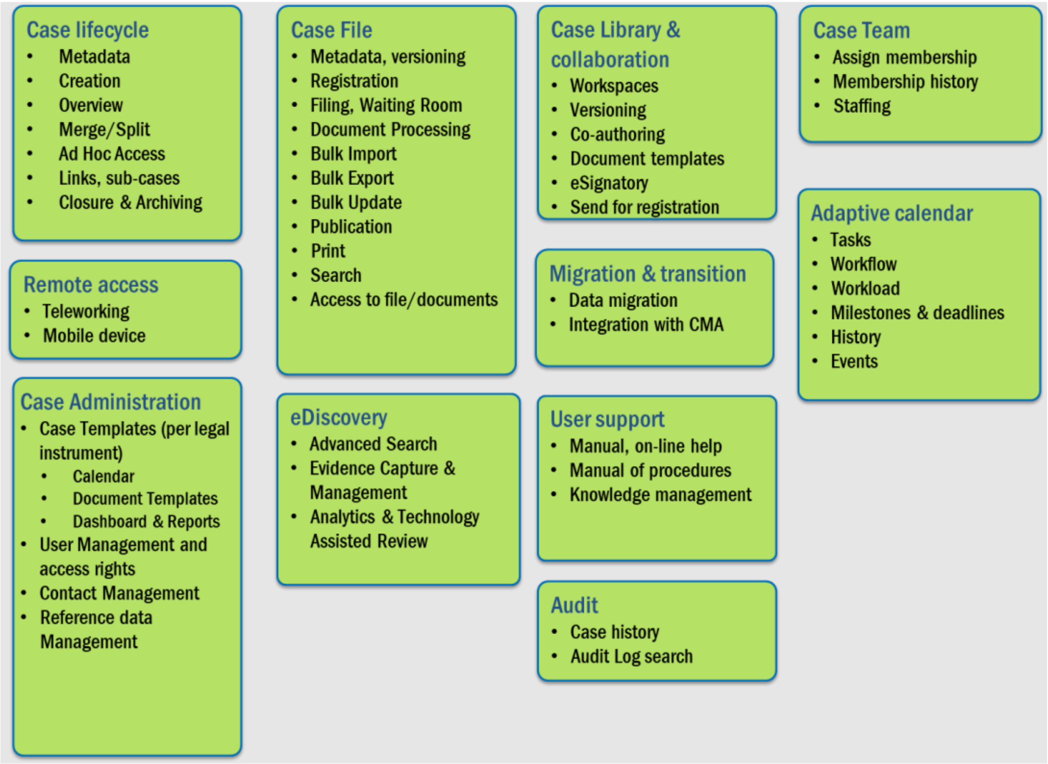
Table 15: Description of CMS solution 3 - Case@EC

CMS Solution 3	
Vendor	European Commission
Solution	Case Management at the EC (CASE@EC)
Solution Type	Case Management Framework (CMF)
Description	The main goal of the project is to deliver a Case Management solution, which fulfils the common business needs of the participating DGs. The following Commission Services participate in the Case Management Rationalisation project: • The Directorate-General for Competition (DG COMP) – leading DG • The Directorate-General for Agriculture and Rural Development (DG AGRI) • The Directorate-General for Maritime Affairs and Fisheries (DG MARE) • The European Commission's department for budget (DG BUDG) • The European Anti-Fraud Office (OLAF) • The Directorate-General for Trade (DG TRADE) Further Commission Services might later join and use CASE@EC if the tool responds satisfactorily to their user needs in the context of Case Management. The latest version (version 2) of the CASE@EC supports the functionalities described in Figure 19: CASE@EC functionalities below. Finally, the solution is based on IBM CMF products and additional functionalities built by the EC as depicted in the architecture (Figure 20: CASE@EC architecture below).
EU integrators / service providers	n/a
Strengths	• Re-usable solution built for the EC. It can introduce cost reduction. • System of choice for DGs and institutions including the future solution for the EPPO. • Possible DIGIT Hosting with Secure Hosting Solution (SHS).

	• Central reference data repository.
Weaknesses	• This solution is based on a previous offering of IBM products (notably, the IBM Case Manager, IBM Datacap and IBM Filenet). Given that the IBM product offering has evolved since, the licensing model and flexibility of this product with regards to IBM global product updates must be examined.

The figures below give an overview of the architecture of the Case@EC solution. Unfortunately, similar views could not be found for the IBM and Pega solutions in the context of this report.

Figure 19: CASE@EC functionalities



Case lifecycle
- Metadata
- Creation
- Overview
- Merge/Split
- Ad Hoc Access
- Links, sub-cases
- Closure & Archiving

Remote access
- Teleworking
- Mobile device

Case Administration
- Case Templates (per legal instrument)
  - Calendar
  - Document Templates
  - Dashboard & Reports
- User Management and access rights
- Contact Management
- Reference data Management

Case File
- Metadata, versioning
- Registration
- Filing, Waiting Room
- Document Processing
- Bulk Import
- Bulk Export
- Bulk Update
- Publication
- Print
- Search
- Access to file/documents

eDiscovery
- Advanced Search
- Evidence Capture & Management
- Analytics & Technology Assisted Review

Case Library & collaboration
- Workspaces
- Versioning
- Co-authoring
- Document templates
- eSignatory
- Send for registration

Migration & transition
- Data migration
- Integration with CMA

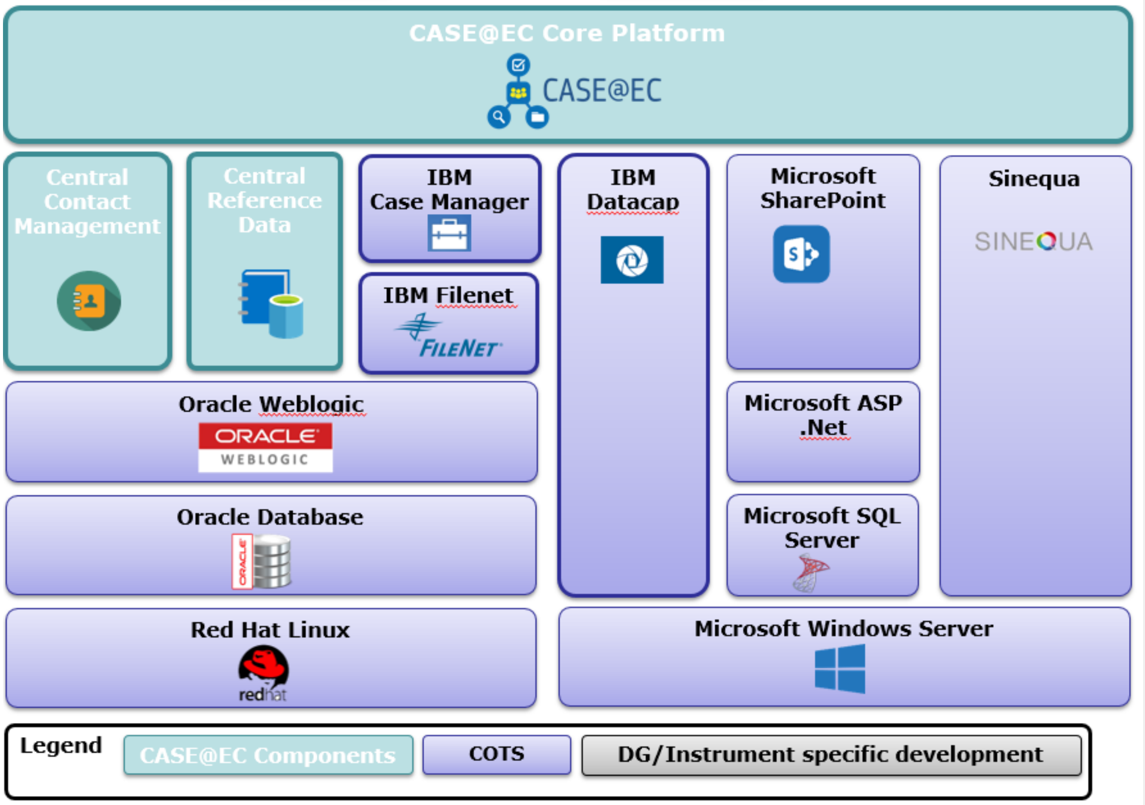
User support
- Manual, on-line help
- Manual of procedures
- Knowledge management

Audit
- Case history
- Audit Log search

Case Team
- Assign membership
- Membership history
- Staffing

Adaptive calendar
- Tasks
- Workflow
- Workload
- Milestones & deadlines
- History
- Events

Figure 20: CASE@EC architecture



5.4.2.1.3 Comparative view

A comparative view of the solutions strengths and weaknesses is presented below:

Table 16: Comparative view of CMS solutions

	IBM	**Pega**	**Case@EC**
Market presence in the EU	**Strongest presence** via extended partner network.	**Good presence** via extended partner network.	Not a commercial solution, it is only used in the European Institutions.
Fit with the IT ecosystem of EU bodies and JHA agencies	**Good fit.**	**Good fit.**	Re-usable solution **built for the European Commission**, which could imply cost reductions.
Fit in the overall future transformation	**Good fit.**	**Good fit.**	**System of choice** for various parts of the institutions, including various DGs and the EPPO.
Implementation partners	Has implementation/ integration/ service partners in the **top 100 IT companies and leading implementation consulting firms.**	Has implementation/ integration/ service partners in the **top 100 IT companies and leading implementation consulting firms.**	**Technical support** provided by DIGIT (for hosting), and by DG TRADE for central contact management.
Hosting	**On-premise** hosting is an option.	**On-premise** hosting is an **option.**	**Two alternative hosting options**: • DIGIT hosting with Secure Hosting Solutions (SHS). • On premise implementation (such as in the case of the EPPO).
Functionalities	• **Complete list of modular solutions in one platform**,	• The modular solutions in the platform **do not cover all**	**Central reference data repository**

	covering all capabilities in the Core CMS architecture. • **Collaboration functionalities are not the best**, and are better accomplished by IBM's native technologies.	**capabilities** in the Core CMS architecture. • **Binding** development environment and approach.	
Current and future product development	Not data but **workflow-driven** (BPM), whereas the Eurojust business need is to have a system that is data-driven.	Not data but **workflow-driven** (BPM), whereas the Eurojust business need is to have a system that is data-driven.	• Based on **previous offering** by IBM (Case Manager, Datacap and Filenet), therefore licensing and flexibility with regards to global product updates must be examined • Moreover, this poses a **risk as it may not follow the current technological trends and evolutions (i.e. it does not get the latest product updates)**, whereas vendors solutions do.
Analyst assessment	**Leader** in the BPM[98] platform-based Case Management Framework.[99]	**Leader** in the BPM[100] platform-based Case Management Framework.[101]	Not available assessment, as it is not a commercial solution.

Legend: **Strength** **Weakness**

[98] Business Process Management (BPM)
[99] Source: Gartner
[100] Business Process Management (BPM)
[101] Source: Gartner

In conclusion, although Case@EC is the system of choice for several entities in the European Institutions, it was noted that using a custom built system may cause a risk as it may not follow current technological trends and evolutions (e.g. in terms of product updates), and may therefore not be future-proof. Moreover, the default hosting option for this solution is to be hosted by DIGIT.

The assessment above also presents two vendor solutions which both fit the current high-level requirements for the Eurojust Core CMS. However, this is not an exhaustive analysis, and additional vendor solutions exist on the market which could also fit these requirements. Consequently, this report recommends to conduct a more in-depth assessment to select the most appropriate solution, for which a "playing the market" approach should be followed to obtain insights from the solution vendors themselves on the best fitting solution.

5.4.2.1.4 Required interfaces

1. External interfaces

This section documents the interfaces required between the Redesigned Eurojust CMS and the different applications that appear in the architecture (see Figure 5). This includes applications from which the Redesigned Eurojust CMS is retrieving information from and applications providing information to the CMS. The internal interfaces are the interfaces within the Eurojust domain. The external interfaces are the interfaces required for the Redesigned Eurojust CMS to communicate with external domains such as the relevant EU bodies/agencies and the Member States. Therefore, this section serves as a register of interoperability requirements.

Moreover, the authentication and authorisation of external users to the Eurojust domain would be managed by the Eurojust Integration Layer, which would thus manage the system to system interactions described in this section by authorising external systems to send requests to Eurojust applications (or not).

Table 17: External interfaces required for the Redesigned Eurojust CMS

Systems	Description			
	Required[102]	Interaction assumptions	Exchange of information direction	Connection description
System 1: EJ CMS				
System 2:				
Europol EIS	MUST. Required by the Eurojust and Europol Regulations.	EJ CMS to re-use services for extraction of data at Europol. EJ CMS to introduce service interface for external consumers.	Bi-directional	Hit / no-hit consultation.
The EPPO CMS	MUST. Required by the Eurojust and the EPPO Regulations.	Re-use of EPPO exposed interfaces. EJ CMS to introduce service interface for external consumers.	Bi-directional	Hit /no-hit consultation + information exchange.
Frontex IS	MUST. Required by the Eurojust Regulation and the Frontex Regulation.	Frontex to introduce service interface for external consumers.	Bi-directional	Information exchanges and consultation of cases.
OLAF OCM	SHOULD. Required by the Eurojust Regulation and the OLAF Regulation.	EJ CMS to introduce service interface for external consumers. OLAF OCM to introduce service interface for external consumers.	Bi-directional	To be investigated (Possibly hit/no-hit consultation and operational files).
National Authorities systems (MS and Third Countries) - Via e-EDES for MS	MUST. Required by the Eurojust Regulation.	EJ CMS to introduce service interface for external consumers. MS to introduce service interface for external consumers.	Bi-directional	(Semi) Automated Messaging Exchange. Mail communication and information exchange (minimised as much as possible).
ECRIS-TCN	MUST. Required by the ECRIS-TCN Regulation.	EJ CMS to introduce service interface for external consumers.	ESP->EJ ECRIS-TCN->EJ	Hit /no-hit consultation via the ESP and direct interface.

[102] This column refers to the required external interfaces by the Redesigned Eurojust CMS. This means that some external might be displayed in this table, although the current legal framework might not require them (e.g. interaction between Eurojust and OLAF).

		Re-use ECRIS-TCN interfaces. Re-use ESP interfaces.		
SIS II	MUST Required by SIS II Council Decision.	EJ CMS to introduce service interface for external consumers. Re-use SIS II exposed interfaces. Re-use ESP interfaces.	ESP->EJ SIS II->EJ	Hit /no-hit consultation via the ESP and direct interface.
Large Files Solution – centralised option	SHOULD	Direct database access / Introduce service interface for external consumers.	Large Files Solution -> EJ	Hit /no-hit consultation and retrieve relevant information.
Large Files Solution – decentralised option	SHOULD	Direct database access / Introduce service interface for external consumers	Large Files Solution -> EJ	Hit /no-hit consultation and retrieve relevant information.
ESP	MUST	Re-use ESP exposed interfaces for EJ access to ECRIS-TCN and SIS II.	ESP->EJ SIS II->EJ	Hit /no-hit consultation.
JIT Collaboration Platform	SHOULD	EJ CMS to introduce service interface for external consumers.	Bi-directional	Information exchange and consultation of cases.
Eurojust Integration Layer	MUST	EJ CMS to introduce service interface for external consumers.	Bi-directional	All exchanges of information between EJ systems and the outside world.
Judicial Cases Cross-Check – decentralised like option	SHOULD. Only if JCCC is extended to JHA agencies and EU bodies.	EJ CMS to introduce service interface for external consumers.	EJ->JCCC	Hit / no-hit consultation.
Judicial Cases Cross-Check – centralised option	SHOULD. Only if JCCC is extended to JHA agencies and EU bodies.	EJ CMS to introduce service interface for external consumers.	EJ->JCCC	Hit / no-hit consultation.
e-EDES	MUST	EJ CMS to introduce service interface	Bi-directional	(Semi) Automated Messaging

		for external consumers.		Exchange. Mail communication and information exchange.

2. Internal interfaces

The internal interfaces of the Redesigned Eurojust CMS are described in Table 18 below. It is important to note that these integrations should be done via the Eurojust Integration Layer, rather than point to point.

Table 18: Internal interfaces required for the Redesigned Eurojust CMS

Attribute	Description			
Component 1	**EJ Core CMS**			
Component 2	JIT Admin Portal	CT Register	Action Day Collaboration Platform	Integration Layer
Required	MUST	MUST	MUST	MUST
Interaction Description	Existing system to integrate or rebuilt in the CMS. Eurojust domain integration.	New CMS functionality or separate component integrated with the CMS.	New component to integrate with the CMS.	New component. Part of the CMS.

5.4.2.2 Counter-Terrorism Register

The technical considerations related to the implementation of the Counter-Terrorism Register are the same as those related to the Core CMS, as both components would be built within one technical solution.

5.4.2.3 JIT Admin Portal

This section presents technical considerations for the implementation of the JIT Admin Portal.

5.4.2.3.1 Implementation options

The current JIT Admin Portal is a custom built application based on SharePoint 2013 (for the user interface), which is supported by an underlying IIS application server and SQL server engine. It enables JIT members to get information about financial assistance to JITs, and to manage their funding application (i.e. manage the funding application form, submit the request to Eurojust, and monitor the status of the request).

Three implementation options could be considered for the implementation of the new and improved capabilities of the JIT Admin Portal:

- Option 1: making further developments using the same technology as the one used to develop the current version of the JIT Admin Portal.
- Option 2: developing a new portal using the same suite of technology as the one that would be used to implement the Redesigned Eurojust CMS (possibly using a separate instance to ensure information and documents are managed separately).
- Option 3: developing a new portal using a Business Process Management (BPM) solution available on the market.

5.4.2.3.2 Market overview

In nature, CMS and BPM solutions are similar due to the fact that they involve processes, business rules, workflow management, document management, etc. However, BPM assumes that the processes to be executed are fully pre-determined and structured, and the execution of the process is linked to one specific person. Case management, on the other hand, is used to organise, compile and track all activities related to a case. These activities may be executed by different people, and the activities and process followed may vary based on the case. The only fixed element is the goal to be attained. Therefore, the most appropriate tool should be chosen based on the nature of the activities to be executed.

Furthermore, it would seem that modern business process management suites are evolving towards a more flexible model, closer to adaptive case management. Indeed, analyst resources such as Gartner[103] describe modern intelligent BPM (iBPM) software as being intelligent, in that it supports the creation of highly adaptive and intelligent processes, which enable dynamic changes of operating procedures (including process flows, business rules, decision models, data models and other) based on the operational environment. This requires a blend of contextual awareness, effective decision management, responsiveness to events and advanced analytics. Also, these platforms are developed based on low-code development, meaning they are faster to customise, deploy and adapt. The leading iBPM suites are those provided by Pegasystems (Pega Infinity), Appian (Appian development platform) and IMB (IBM Digital Business Automation Enterprise and IBM Digital Business Automation Express).

However, besides the best-in-class intelligent BPM suites, multiple BPM tools exist on the market, and notably open source ones, which could be adapted to the relatively simple functionalities and low volume of processes and requests managed by the JIT Admin Portal. Examples of such solutions include jBPM, Bitrix24 and Alfresco.

5.4.2.3.3 Comparative view

The table below offers a high-level comparative view of the different options. However, this comparison should be further detailed based on a more detailed analysis of specific solutions available on the market and their cost.

Table 19: Comparative view of JIT Admin Portal solution

	Option 1: Re-use current JIT Admin Portal	**Option 2: New portal based on CMS solution**	**Option 3: New portal based on BPM solution**
Pros	- **Capitalise on the pre-existing in-house knowledge and investments** made in the tool.	- The requirements for the JIT Admin Portal could be **covered by the functionalities offered by the CMS**	- Custom tool that would **best fit the requirements** for the new JIT Admin Portal, given that the

[103] Gartner Magic Quadrant for Intelligent Business Process Management Suites (30 January 2019).

	• **Ease the change process for users**, who would only need to adapt to one new tool/ interface.	solutions examined in section 5.4.1.3.[104] • **Capitalise on the investment made in the EJ CMS**. • **Ease the change process for users**, who would only need to adapt to one new tool/ interface.	administered processes are relatively predictable. • An open-source BPM solution might be **cost effective**.
Cons	• **Extra developments costs** in addition to the foreseen investment in the CMS.	• Developing the workflows of the JIT Admin Portal in the CMS solution **might be more burdensome and less cost-effective** than implementing a BPM solution.	• The **integration capability** of the new tool with the CMS must be examined. • **Users might possibly find it complicated** to have to use two new tools.

Legend: **Strength** **Weakness**

In conclusion, this report would recommend to develop a new JIT Admin Portal based on the technology used to develop the CMS. It would help providing improved functionalities while capitalising on the investments made and easing the change process for users.

5.4.2.4 Action Day Collaboration Platform

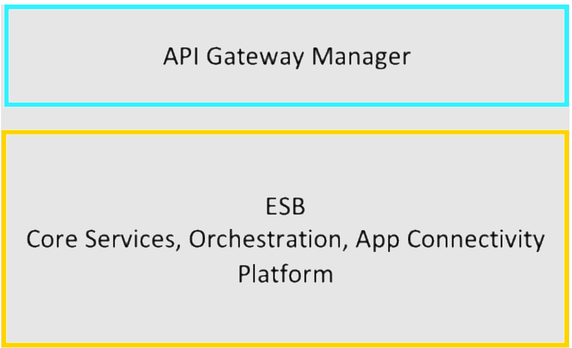
The technical considerations of the Action Day Collaboration Platform are the same as those to be taken into account for the implementation of the JIT Collaboration Platform. Therefore, please refer to section 5.5 for a description of these components.

5.4.2.5 Integration Layer

Typically, a multi-tier approach for this type of solution is used. It is not the intention of this report to provide a very detailed overview on the implementation of this type of solution, although we would like to point out two parts of such a multi-tier approach which play an important role in the context of the Eurojust Integration Layer.

[104] Based on a high level analysis of the requirements provided by the Case@EC solutions. Further analysis is needed for a more detailed assessment.

Figure 21: API Gateway Manager & ESB



API Gateway Manager is the gateway through which requestors can consume a service or an application programme interface (API). API Management refers to the processes for distributing, controlling, and analysing the APIs that connect applications and data across the enterprise and clouds. The goal of API management is to allow organisations to monitor activity and ensure the APIs are meeting the needs of the developers and applications using the API.

The API Gateway Manager needs to embody the following functionalities:

- Gateway: server acting as request moderator. It allows to manage incoming requests and build security and capacity policies. In the context of the common services platform, the API Gateway Manager would receive requests from one of the parties in the domain of Digital Criminal Justice, it would analyse this request to conclude if that party is allowed to place the request, and if so, it would trigger the process for orchestrating the answering of the request.
  In the context of the Eurojust Integration Layer, it would do more or less the same but on a smaller scale within the Eurojust domain. In this case we are talking about orchestration of requests between Eurojust internal components (e.g. exchange/integration between the core CMS and the collaboration platform).
- Publishing tools: when providing service for information exchange, it is important to have a clear and unambiguous governance on the services offered (think about versioning of the services). Therefore a set of tools tailored to define APIs, generate documentation, build access and usage policies besides testing and debugging functionalities is necessary.
  For the Eurojust Integration Layer, the importance might be a bit lower following the lower complexity of integrating Eurojust components, since they are all governed within one organisation. Nevertheless, following best practices, this functionality should also be present in the Eurojust Integration Layer.
- Reporting and analytics: aims to monitor API usage and load. This functionality aims to give visuals on data and data analytics.

Enterprise Service Bus (ESB) is a system that aims to reduce the complexity of the communication of a large number of applications. It is a middleware that provides secured interoperability between applications via interfaces. It allows to route messages between enterprise applications and handles events.

Below is a list of standard functionalities included in an ESB:

- Route messages between services: can be achieved through multiple patterns, the idea is that the ESB receives a request and forwards it to another system.
- Monitor and control routing of message exchange between services: consist of alerts or visual assessing the successful processing of a transfer.
- Resolve contention between communicating service components: is the capability to view and operate in case of error or issues on a communication process.
- Orchestration of the flow between multiple consumers: is the process of integrating two or more applications to automate a process or synchronize data in real-time.
- Transaction management: is responsible for coordinating the transactions across the resources. It helps to initiate a trade, coordinating, defining the context but also recover from failure.
- Message format transformation: is the capacity to translate a message written in one format to another.
- Integration between all components: components are the exercise that application execute when collaborating.

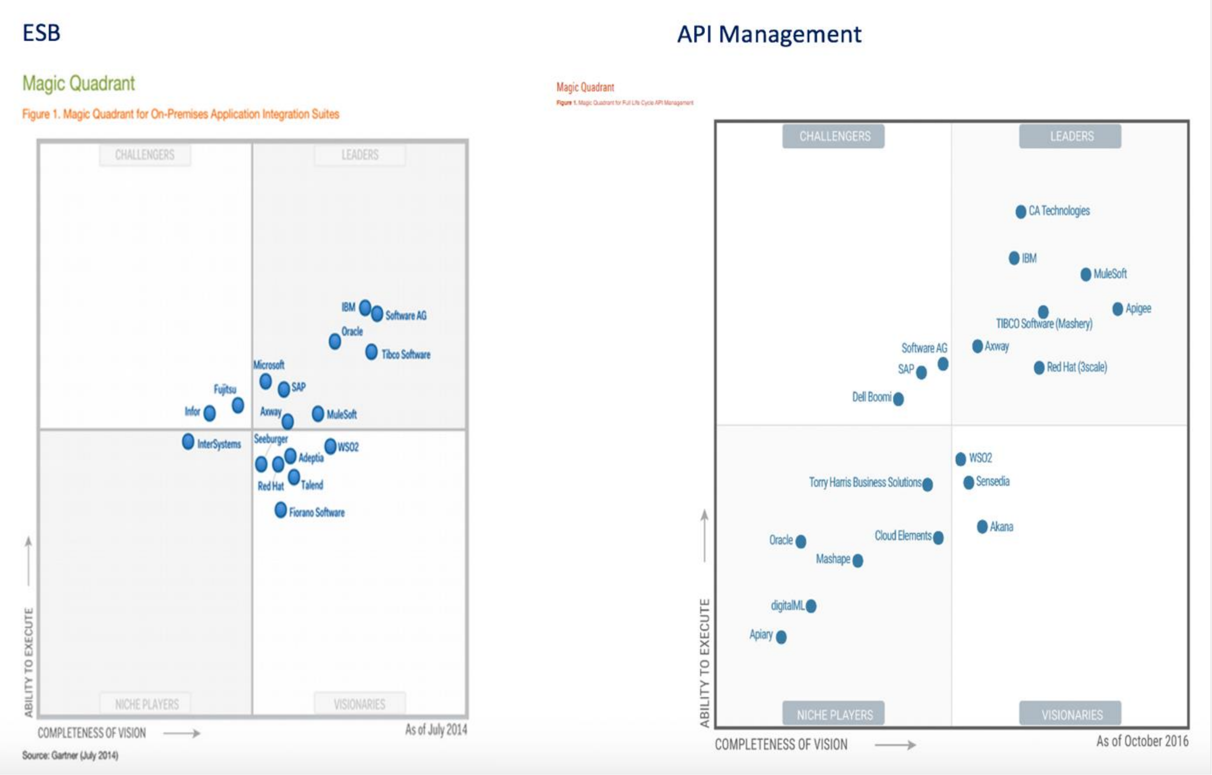
5.4.2.5.1 Possible vendor solutions

The market of integration solutions is quickly evolving. In order to illustrate the availability of this type of solutions, we will provide an overview of three possible solutions:

- MuleSoft
- Dell
- IBM

These solutions were selected from the Gartner Magic Quadrant for ESB and API Management as shown in the figure below:

Figure 22: ESB and API Management Gartner Magic Quadrant



MuleSoft Anypoint

It is provided by MuleSoft and provides integrated solutions for connecting software, hardware and data. MuleSoft has extended partnerships in Europe for the implementation and service provision of the Anypoint solution.

MuleSoft ESB provides the following functionalities:

- Service creation and hosting — expose and host reusable services, using the ESB as a lightweight service container.
- Service mediation — shield services from message formats and protocols, separate business logic from messaging, and enable location-independent service calls.
- Message routing — route, filter, aggregate, and re-sequence messages based on content and rules.
- Data transformation — exchange data across varying formats and transport protocols.

Anypoint is a platform that includes multiple sub-components that allow seamless integration:

- API Portals that bridges the API providers with the consumers through the lifecycle of the API. It allows to expose, provision user access, generate client keys along with other functionalities that can help to interact with them. It provides a registry of applications, credentials management, share and interact with the documentation of the APIs and provide feedback on the quality and bugs they retain.
- Exchange is a global repository storing all the technical assets of an API application's lifecycle. It generates automatically documentation, mappings and connections policies. It is a registry that contains connectors for specific applications and a bunch of other tools to ease the development.

- Design Center, which gives them tools to build connectors, implement data and application flows, design, re-use and test APIs. It includes a studio, API designer and connector devkit to ease up all the processes of developing the API.
- Management Center, which enables a user to manage APIs, users, analyse traffic, monitor SLAs, fix integration flows and contains many more capabilities. This service is provided by three components, API Manager, Runtime Manager and Analytics
- API Manager allows the user to have visibility upon the structure and connections of an API. Through this functionality, you can see the different APIs and their links through visuals. Through the Analytics, you can visualise and monitor in real-time how your system collaborates and track performances. It allows you to customize your view in various ways and filter your search upon the general information's provided. The Runtime portal allows seeing how your instances are working by showing performance graphs with details on how they are processing are behaving. It also allows the user to see logs and identify issues related to the systems, requests and response time.
- Connector, which is a set of prebuild solutions that you can use to connect APIs between them, databases and many other applications. The large variety of connectors available allows you to connect APIs with multiple protocols, however, it also allows you to build your own.
- ESB from MuleSoft Any point is composed of multiple services for developers in terms of message formats, component types, legacy re-use, ease of deployment and designed respecting staged event-driven architecture that enables high scalability.
- Since MuleSoft has a certain reputation and a strong and growing presence in Europe, it should be considered as a good competitor.

Below is a table listing all the functionalities, practical requirements and security requirements that the solution should meet within this component.

Table 20 MuleSoft Anypoint Requirements

MuleSoft Anypoint		
ESB	Route messages between services	V
	Monitor and control routing of message exchange between services	V
	Resolve contention between communicating service components	V
	Orchestration	V
Common shared services	Transaction management	V
	Message format transformation	V
	Authentication and authorisation system	V
	Audit and traceability system	V
	Centralised logging	V

MuleSoft Anypoint		
Requirement	Encryption	On-Premise/Cloud
	Scalability	V
	Centralized access	V
	EU Data Centre	V
Security	LDAP	V
	SAML 2.0	V
	OAuth	V
	Credential vault	V
	Security filters	V
	Message encryption	V
	Digital signatures	V
	Authentication and Authorization register	V
Nice to have	Cross-platform	V
Clients	Usage over the EU Landscape	N/A

Below is a list of considerations listed as pros and cons for the vendor solution based on review sites and user experiences:

Table 21: MuleSoft Anypoint Pros & Cons

MuleSoft Anypoint	
Pros	Cons
Can be deployed on premises, in the cloud or across a hybrid ecosystem.	None of notice compared to the other solutions.
Sponsored for soon granting the U.S. Federal Risk and Authorization Management Program (FedRAMP) Authorization.	
The Anypoint platform offers the options for an ESB in case a SoA approach is selected for integration services.	
Based on open-source software minimising the vendor lock-in.	
Modular addition of an ESB in case the final architecture requires a combination of ESB and API-led development of APIs.	
Mentions by Analysts sources: ○ Leader in the Gartner Magic Quadrant for Enterprise Integration Platform as a Service.	

MuleSoft Anypoint	
○ Leader in the Gartner Magic Quadrant for Full Lifecycle API Management. ○ Leader in the Forrester wave for strategic iPaaS and hybrid integration platforms.	

Dell Boomi

Dell Boomi Platform is a single instance, multi-tenant enterprise platform covering many different use cases. The critical features identified are the following:

- Integration - building, deploying and managing integrations.
- API Management - creating, publishing and managing APIs throughout their lifecycle.
- EDI Management - managing trading partner network and transactions.
- Master Data Management - align and improve data across applications.
- Workflow - improving efficiency and effectiveness of any business process.

Dell Boomi is a set of several tools including Integration tools, Master Data Hub, API Management and Flow Management.

- Integration tools offer the possibility to quickly set up all the connections needed for the integration process. This tool owns a drag and drop UI functionality along with data mapping tools and a set of connectors coupled with various integration patterns. It also offers operational intelligence, reusable business logic and data flow recommendations to tackle the challenges of the processes. With all these capabilities, it provides the possibility to tailor the integration fully. One can quickly build, deploy and manage the integration.
- Master Data Hub allows in one hand, shortening the feedback loop on data and the cost of ownership, on the other hand, it would enable improving operational efficiency by breaking down data silos and expand trusted data to enterprises. The user can model data entities through low-code and visuals. Once this is defined, it would publish into the Hub repository before identifying the systems that would be involved in processing the data. Additionally, it offers the capability to consolidate and merge records cross systems.
- API Management challenges are addressed by Atomsphere, which comes as a single platform that tackles complexity upon development, compilation, testing, configuration, deployment and monitoring. This API management tool enables the design of integration processes between multiple applications hosted on cloud or on-premises. It comes with a broad range of views to seamlessly gather the needed information's. The deployment is tailored based on customer needs by enabling deployment for Saas, Paas or cloud integrations. It includes an integration engine based on run-time engine, allowing users to follow the different steps and monitor the health of the processes they engage. Once deployed, it offers tools and visuals to enquire and observe the various applications that are running. On top of those functionalities, it provides possibilities for seamless integration.
- A Flow Management engine also belongs in the package of this solution. It helps the developers to customise and implement flows.

Below is a table listing all the functionalities, practical requirements and security requirements that the solution should meet within this component.

Table 22 Dell Boomi Requirements

Dell Boomi		
ESB	Route messages between services	V
	Monitor and control routing of message exchange between services	V
	Resolve contention between communicating service components	V
	Orchestration	V
Common shared services	Transaction management	V
	Message format transformation	V
	Authentication and authorisation system	V
	Audit and traceability system	V
	Centralised logging	V
Requirement	Encryption	
	Hosting	On-Premise/Cloud
	Scalability	V
	Centralized access	V
	EU Data Centre	V
Security	LDAP	V
	SAML 2.0	V
	OAuth	V
	Credential vault	V
	Security filters	V
	Message encryption	V
	Digital signatures	V
	Authentication and Authorization register	V
Nice to have	Cross-platform	V
Clients	Usage over the EU Landscape	N/A

Below is a list of considerations listed as pros and cons for the vendor solution based on review sites and user experiences:

Table 23: Dell Boomi Pros & Cons

Dell Boomi	
Pros	Cons
Can be deployed on premises, in the cloud or across a hybrid ecosystem.	The platform recently incorporated an API management solution that still needs to be proven by wide usage.
Granted the U.S. Federal Risk and Authorization Management Program (FedRAMP) Authorization.	Purely on-premise deployment is not available. A hybrid and secure deployment model is however available.
Mentions by Analysts sources: • Leader in the Gartner Magic Quadrant for Enterprise Integration Platform as a Service. • Leader in the Forrester wave for strategic iPaaS and hybrid integration platforms.	Still a challenger in the Gartner Magic Quadrant for Full Life Cycle API Management.

IBM Application Integration Suite

IBM Application Integration Suite provides the tooling to connect your cloud and on-premise applications, build microservices and expose and manage APIs; helping to create a hybrid environment.

IBM Application Integration Suite is a new on-premise offering, built on the best in breed offerings that IBM already has for on-premises integration, cloud integration and API management and creation; it combines the following capabilities in a single solution:

- Connect: rapid access to hundreds of applications and data sources both in the cloud and on-premise, with secure communication.
- Transform: extensive set of pre-built objects that transform, join, aggregate, restructure, cleanse and enrich data to satisfy simple & complex requirements.
- Deliver: seamlessly scale workloads to route and deliver data in real-time with quality of service guarantees.
- Compose: quickly assemble APIs into a coherent flow to provide higher grained business value. Expose: Provide secure and managed access to enterprise assets across internal and external developer communities.

To address those business requirements, IBM is providing this solution with three core components:

- Integration Bus connects applications without caring about the message format or protocol. It allows to interact and exchange data with various system and therefore stands for a flexible, dynamic and scalable infrastructure. It would enable to route, transform and enrich messages from one end to the link to another.
  It supports a wide range of protocols including HTTP, HTTPS, SOAP and REST, files, SAP and TCP/IP. It can ingest different formats as well as binary formats, XML SWIFT, EDI, HIPAA and even custom formats. On top of this flexibility, it supports operations as route,

transforming, filtering, enriching, monitoring, distributing, collecting, correlating and detection.

For the application development and journey to production, it offers reusable solutions, including patterns that can tailor specific ecosystems and requirements.

In includes capabilities linked to message flows and nodes which contains the connectivity logic and integration logic that operates on your data once processed.

As the following functionality, it introduces the description of the message tree, defining the structure of the messages and allows the user to directly operate no matter what the original message format is.

A graphical mapping, Java, ESQL and XSL help to achieve the transformation, considering the skills of the transformation team.

For the operational management and performance tracking, this set of tools also includes administration and system management options for an advanced solution. It supports a wide range of operating systems and hardware platforms. It provides an extensible and performing architecture based on transaction processing environments. Hence it allows integration with multiple vendors.

- WebSphere Cast Iron is a hub that offers to integrate cloud application to on-premise systems. Cast Iron initially was designed to host and deploy on-premise with a physical appliance, virtual appliance or cloud-based service. It provides a broad set of connectors to many enterprise applications like SAP, Oracle ESB, JDE and more. It allows connecting multiple software in the environment that suits more to the technical requirements. The functionalities provided by this solution are comparable to an ESB. However, the difference is that it works with data as a source and destination rather than messages and end-points.
- IBM API Connect Professional provides API lifecycle management to lower the complexity of their development. It allows you to develop, test, control, monitor, scale, and manage the whole ecosystem needed for an enterprise.

Below a table listing all the functionalities, practical requirements and security requirements that the solution should meet within this component:

Table 24: IBM Application Integration Suite Requirements

IBM Application Integration Suite		
ESB	Route messages between services	V
	Monitor and control routing of message exchange between services	V
	Resolve contention between communicating service components	V
	Orchestration	V
Common shared services	Transaction management	V
	Message format transformation	V
	Authentication and authorisation system	V

	Audit and traceability system	V
	Centralised logging	V
Requirement	Encryption	V
	Hosting	On-Premise/Cloud
	Scalability	V
	Centralized access	V
	EU Data Centre	V
Security	LDAP	V
	SAML 2.0	V
	OAuth	V
	Credential vault	V
	Security filters	V
	Message encryption	V
	Digital signatures	V
	Authentication and Authorization register	V
Nice to have	Cross-platform	V
Clients	Usage over the EU Landscape	N/A

Below a list of consideration listed as pros and cons for the vendor solution based on review sites and users' experiences:

Table 25: IBM Application Integration Suite Pros & Cons

IBM Application Integration Suite	
Pros	Cons
Can be deployed on premises, in the cloud or across a hybrid ecosystem.	None of notice compared to the other solutions
Granted the U.S. Federal Risk and Authorization Management Program (FedRAMP) Authorization.	
Modular addition of an ESB in case the final architecture requires a combination of ESB and API-led development of APIs.	
Mentions by Analysts sources: • Visionary in the Gartner Magic	

Quadrant for Enterprise Integration Platform as a Service. • Strong performer in the Forrester wave for strategic iPaaS and hybrid integration platforms.	

5.4.2.6 General technical considerations

A few general considerations were underlined during the Expert Group Meeting of 13-14 January 2020. These considerations are described here at high level. However, they must be taken into account, and further analysed before the design and implementation of the redesigned CMS.

5.4.2.6.1 Access to CMS by the Member States

Several options could be envisaged regarding the way in which Member States send requests and information to Eurojust. These options are presented below (and further detailed below):

- Option 0 (status quo): Information is sent to Eurojust by Member States in structured and unstructured way, and it is then manually inserted into the CMS by Eurojust, using the existing operational model of Eurojust.
- Option 1: Designing and building the new Redesigned Eurojust CMS so that the front-end is exposed to stakeholders at national level making the request. This option requires that Member States are enabled to have access to the Redesigned Eurojust CMS.
- Option 2: Information is sent to Eurojust by Member States using structured forms, and it is then manually inserted into the CMS by Eurojust, using the existing operational model of Eurojust.
- Option 3: Using structured forms for stakeholders at national level to send requests to CMS, which a robot can use to enter the information from the form into the CMS (using simple Robotic Process Automation technology).
- Option 4: Using a robot to extract the relevant information from the unstructured information received (e.g. in a document or an email), and enter it into a structured form in the CMS (using Robotic and Intelligent Automation technology).

It is important to note that while option 1 is an alternative to the other options, option 4 builds on option 3, as the technology to implement is more complex.

Moreover, all future communication in the Digital Criminal Justice domain would need to run over the Secure Communication Channel and e-EDES, including communications between Member States and Eurojust Core CMS. As explained in section 5.2, the Secure Communication Channel to be used may consist of more than one channel, due to the implications and constraints linked to its choice.

5.4.2.6.2 Data model for cases

Following the principle of interoperability and the once only principle[105], steps could be taken in order to ensure that cases and case information can be traced and exchanged more easily between the various stakeholders involved in Cross-border Digital Criminal Justice cases (be it from JHA agencies and EU bodies or Member States). To do so, several propositions were put forward during

[105] More information about the Once Only Principle is here: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Once+Only+Principle

the Expert Group Meeting which should be further examined by Eurojust when designing its new CMS:

- Having a unique identifier, to be able to link cases across the EU. To do so, a similar approach as the one used in the SIENA application and e-EDES should be used (see sections 5.2.1.3 and 5.3.3 respectively). In the context of the Redesigned Eurojust CMS, this would mean that each case would have a unique identifier used for that case in all connected DCJ systems. Then, each incoming request, message or document would be linked to an existing or new case. Each of these items would also have a unique identifier, which would contain the digital identifier of the case to which it is linked.
- Having a unique data model for cases, based on the UMF, to enable the exchange of case information between systems.

These propositions fit into the interoperability considerations for the overall architecture of the Cross-Border Digital Criminal Justice IT landscape, which are presented in section 4.

5.4.2.6.3 Level of classification of the information exchanged and stored

The level of classification of the information exchanged and stored in the Redesigned Eurojust CMS (non-classified, classified EU RESTRICTED or classified EU CONFIDENTIAL) would have a high impact on the security requirements for the Redesigned Eurojust CMS, which would in turn impact its design and implementation. More information about these considerations is provided in section 5.4.3.

5.4.3 Security assessment

Hereafter, a security assessment is performed on each component and capability of the Redesigned Eurojust CMS solution. The objective is to provide security capabilities, considerations and features that are relevant for each of its underlying components. These security capabilities, considerations and features should be translated to security requirements and controls, at the design and implementation phase of the target architecture.

- **Core CMS:**
  - **IAM Component:**
    - **Goal:** Ensure that the right individuals have controlled access to the right resources at the right time for the right reasons.
    - Generally, this building block is responsible for Identity management services or ID services. It can be split into four different IAM services:
      - Roles and groups management services.
      - Authentication services.
      - Authorisation services.
      - Identity governance.
    - The IAM component should – at least – have the following security capabilities and features:
      - Enable Immutable private identifiers/Mutable Public Identifiers.
      - Decouple Core/Static Personally Identifiable Information (PII) from Transactional Data.
      - Ability to externalise access control rules.
      - Cross-platform device support (i.e. Windows, Mac, and Linux), multi-protocol (Lightweight Directory Access Protocol - LDAP,

Secure Shell - SSH, Security assertion markup language - SAML, Remote Authentication Dial-In User Service - RADIUS, and more)[106] and location agnostic (i.e. cloud, on-premises, or remote).
        - Credentials storage - one-way password hashing and salting.
        - Enforce Strong password policies (e.g. password length and rotation, etc.).
        - Key and certificate management need to be supported by automated means allowing people to leverage keys, revoke certificates, and allows to rotate them, when needed.
        - Enforce and support Multi-Factor Authentication for key systems and applications.
        - Enable Auditing and logging for tracking IAM related actions and activities.
    - **Note:** IAM building block is deemed as part of "Data protection and Security" building block.
- **Exchange integration:**
    - The integration with Exchange or any other similar email service provider, should – at least – have the following security capabilities, features and needs:
        - Classified data and personal data should be encrypted using cryptographic products approved by the Council while processed, stored or sent by exchange services.
        - Only secure protocols (i.e. transfer protocols, authentication protocols and storage protocols) should be allowed, while integrating, using or configuring exchange services, to guarantee the confidentiality and integrity of data at rest and in transit.
        - Email sending and receiving should be limited to only authorised email systems and domains. All email communications should be denied by default for unknown systems and domains (whitelist principle).
        - Both incoming and outgoing email should be investigated on the Eurojust domain boundary and on the endpoint using investigation methods :
            - Incoming email should be scanned using reputation, categorisation and classification rules.
            - All email attachments entering the Eurojust email gateway using unknown and executable file types are blocked (to reduce the risk on infections).
            - Use sandboxing to analyse and block inbound email attachments with (probable) malicious behaviour (e.g. active content) to reduce the risk of infections (e.g. malware outbreak, ransomware, etc.).
        - Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification, as well as the Sender Policy Framework (SPF) and the Domain Keys, in order to lower the chance of spoofed or altered emails from valid domains.

[106] Those are examples of protocols widely used in order to ensure a secure authentication. The choice of a specific protocol depends on the use case it should be applied to alongside with its technical requirements.

- **Translate Engine:** This component requires security considerations to ensure secure integration with the target architecture, and data protection considerations including aspects related to confidentiality (e.g. lists of documents that can be translated by the engine, storage period of documents sent for translation, access, etc.).
- **Mobile & Web Browser Access:**
  Please refer to IAM building block as it provides the access control capabilities required for the target architecture.
- **Case Handling & Internal communication (CH&IC):**
  - **Goal:** Enable Eurojust users to exchange and manage business cases through a web portal, in line with the business functions, while guaranteeing the confidentiality, integrity and the availability of systems, services and data it uses.
  - This building block consists of the main case management system that would be used within Eurojust domain.
  - This building block should– at least – have the following security capabilities, features and needs:
    - The case handling and internal communications tools should store data in their dedicated data repositories in a secure manner using secure protocols that guarantee data confidentiality and integrity when stored in the backend systems (i.e. encryption at rest – e.g. DBMS level encryption), as well as when transferred to them (i.e. encryption in transit – e.g. TLS and HTTPS).
    - In certain sensitive cases, it might be necessary to implement security controls that guarantee the confidentiality of data in processing.
    - Availability of Case Handling & Internal Communication (CH&IC) data and services should be ensured, by different technical means, such as data and system backups and recovery, redundancy plan, data clusters, etc.
      - Extra considerations might be required for CH&IC systems, application or services with high-availability requirement.
    - The CH&IC tools, supporting systems and infrastructure should be covered by both business continuity and disaster recovery plans.
    - When required to guarantee a quality of service (e.g. time sensitive applications), an SLA should be established for services provided by or relying on third parties.
    - Both the CH&IC tools should be logged and monitored, logs of the CH&IC should cover at least the following aspects:
      - End-users access to the web-portal of the case handling tool, as well as the accesses for the internal communication tool.
      - (Administrative) Accesses for the backend and supporting systems that support both the Case Handling & Internal communication tools, including access to their logs.
      - (Administrative) Actions, configuration and permission changes performed on the backend and supporting systems that support both the Case Handling & Internal communication tools.
      - Security incidents and events – e.g. malware.

        - Performance related issues, alerts and warnings.
      - Logs of CH&IC should be continuously monitored, any anomalies should be investigated and appropriate actions should be taken in line with Eurojust incident response process.
  - **Entity Capturing:** This component only requires security considerations to ensure secure integration with the target architecture.
  - **Data Protection and Security:** IAM building block is deemed as part of this building block.
  - **Business Functions:** Security considerations related to business functions should be evaluated separately following a risk driven approach while conducting a business impact assessment.
  - **BI Module (and Analytics):** Not applicable, as it represents a low security risk.
  - **CIF Module**: Not applicable, as it represents a low security risk.

- **CT Register:** Not applicable, as it represents a low security risk using functions only allowed to retrieve data and not input new data into the systems. For security considerations related to business functions it needs to be evaluated separately following a risk driven approach while conducting a business impact assessment.

- **JIT Admin Portal:** This portal mainly consists of a web application (i.e. frontend) with its associated backend systems. Besides the system hardening for both web-servers and database systems and the communication security measures, security considerations should be taken into account to mitigate common web application security risks - i.e. OWASP Top 10:
  1. Injection
  2. Broken authentication
  3. Sensitive Data exposure
  4. XML External Entities (XXE)
  5. Broken Access control
  6. Security misconfiguration
  7. Cross-site scripting XSS
  8. Insecure Deserialization
  9. Using components with known vulnerabilities
  10. Insufficient logging and monitoring
- **Action Day Collaboration Platform:** This component only requires security considerations to ensure secure integration with the target architecture. For similar security consideration, please refer to section 5.5.3 about the JIT Collaboration Platform.

Additionally, the Eurojust Integration Layer should have, at least, the following security services, capabilities and features:

- Identity and access management:
  - Basic authentication.
  - Integrated authentication (Lightweight Directory Access Protocol - LDAP).
  - Authorisation service and Role Based Access Control (RBAC).
  - Strong authentication mechanism (e.g. Multifactor Authentication - MFA and SSO).
  - PKI management to ensure:
    - End-to end encryption, if required.
    - Authenticity and non-repudiation.

    - Session management to ensure that user sessions are handled properly in the communication layer.
- WEB-API protection measures:
    - Perform Input validation checking to protect against Cross-Site Scripting (XSS), JSON and XML based injections.
    - Enforce HTTP size limits to lower the likelihood of Distributed Denial of service attacks exploiting undefined HTTP size limit flaw.
    - API gateway should be used in order to control, in a secure way, exposed APIs to internal and external systems in the target architecture. API gateways offer the following advantages that need to be investigated for Eurojust systems:
        - Granularity of services – e.g. considering a fine-grained granularity on the integration layer, the stakeholders' systems do not require to know in detail all the individual internal services (at the Integration Layer) necessary to answer a given request, same time data that need to be processed first or that should not be accessible to a specific stakeholder, would not be made available to the service from which they are consuming. In other words, the API gateway would act as a filter to restrict accesses to non-exposed APIs – improve interoperability and security.
        - Different clients may require different information and details, in different forms (e.g. mobile and desktop clients) – improve the interoperability and scalability.
        - Adapt Network communications based on end-users network performance, e.g. server-side web application can adjust the number of requests to backend services to avoid impacting the user experience when using mobile device or client with low bandwidth – improve scalability.
- Incoming/outgoing communication filtering to make sure that no malicious traffic is entering or exiting Eurojust domain perimeters.
- DDoS protection to protect the target architecture infrastructure against DDoS attacks.
- Audit, Logging and monitoring relevant security related events, actions and configurations.
- Establish a formal SSDLC process for both components, ensuring that changes applied on them are performed in a controlled way, guaranteeing full traceability and accountability.
    - A testing and acceptance approaches and environments (e.g. testing and acceptance environments) should be designed and implemented in order to test, at least, software releases, configuration changes and security patches before applying them on production systems, applications or services.
    - Changes should be tested and approved from business and technical standpoint in a dedicated acceptance environment.
    - Similarly, a development approach and environment should be designed and implemented, in case development activities are foreseen for the communication layer.
    - In case of changes impacting the communication layer, an impact assessment should be performed before moving the changes to Eurojust production instances, as it might require further integration and regression testing. This includes configuration changes, integration with new systems, etc.

5.4.4 Legal and data protection assessment

As indicated in Article 23 of Regulation 2018/1727 (Eurojust Regulation), Eurojust is called to set up a Case Management System. The CMS should be composed of temporary work files and an index containing personal and non-personal data. As stated in Article 23(2) of the Eurojust Regulation, the purpose of the CMS is to:

a) Support the management and coordination of investigations and prosecutions for which Eurojust is providing assistance, in particular by cross-referencing information.
b) Facilitate access to information on on-going investigations and prosecutions.
c) Facilitate the monitoring of the lawfulness of Eurojust's processing of personal data and its compliance with the applicable data protection rules.

There is therefore an already existing legal basis for the Redesigned Eurojust CMS. As indicated in the technical assessment, we suggest to include in the Redesigned Eurojust core CMS the following set of capabilities and functionalities:

- Identity & Access Management (IAM)
- Email service integration (inbound)
- Email client integration (outbound)
- e-EDES integration
- Translation engine
- Mobile & web browser access
- Case handling & internal communication
- Entity capturing
- Business functions
- Data protection and security
- Business Intelligence (BI) Module
- Case Information File (CIF) Module

The revamp of the CMS aims to equip the system with these capabilities and functionalities, which would improve the support to the daily activities of the Eurojust National Desks. Although some of these capabilities and functionalities are new (i.e. not included in the current Eurojust CMS), the nature and aim of the CMS remains unchanged. Therefore, an amendment to the legal basis is not required.

It should be noted that the solution suggested by this report includes the Core CMS, the Counter-Terrorism Register, the JIT Admin Portal, the Action Day Collaboration Platform and the Integration Layer.

According to Council Decision 2005/671/JHA[107] national authorities must provide Eurojust with information[108] relating to prosecutions and convictions for terrorist offences that affect or may affect two or more Member States. Moreover, Article 21 (10) of the Eurojust Regulation foresees the obligation to submit information in a structured way to Eurojust, including information according to Council Decision 2005/671/JHA. The Counter-Terrorism Register was established in September 2019 in order to manage this information. The Counter Terrorism Register is thus already running, and is stored within the Eurojust CMS. A legal amendment to the Eurojust Regulation is not required.

[107] Council Decision 2005/671/JHA of 20 September 2005 on the exchange of information and cooperation concerning terrorist offences.

[108] Such as: data which identify the person, group or entity that is the object of a criminal investigation or prosecution; the offence concerned and its specific circumstances; amongst others.

As for the JIT Admin Portal, as stated in Article 4(1) of the Eurojust Regulation, Eurojust should provide not only operational and technical support to JITs, but also financial support. The JIT Admin Portal was created for this purpose allowing the reimbursement of costs incurred by Member States and by third states involved in JIT, if any. The JIT Admin Portal is therefore an administrative system, supporting Eurojust's tasks concerning JITs. The solution presented in this report suggests to expand the JIT Admin Portal, to include JIT Evaluation and JIT Claims. These two new modules would allow Eurojust to use the portal for these tasks that they are already conducting. Both the evaluation of and claims related to JITs are part of the support Eurojust provides for the implementation of JITs. Therefore, the nature of the JIT Admin Portal would remain administrative, hence a new legal basis is not required for this solution.

The Action Day Collaboration Platform would allow for the coordination and support for this type of collaboration. This collaboration is aligned with the tasks and competences of Eurojust as stated in Article 2 and 3 of the Eurojust Regulation. Therefore, Article 2 and 3 of the Regulation can be used as a legal basis for the Action Day Collaboration Platform.

Lastly, the Eurojust Integration Layer would be a technical component, necessary to ensure the integration of the rest of the technical components being part of the Eurojust architecture in a sustainable and maintainable way. The Eurojust Integration Layer would be thus hosted within the agency. Besides this internal functionality, the Integration Layer would also allow the communication with external stakeholders. Overall, the component is necessary to ensure a smooth functioning and overall functioning of the Redesigned Eurojust CMS, which has its legal basis in the Eurojust Regulation. Taking into account the purpose of this technical component, and its hosting, it can be concluded that a specific legal basis for this technical component is not required.

Overall, it can be concluded that the Redesigned Eurojust CMS can be revamped based on the Eurojust Regulation in force as a legal basis.

Following the general legal assessment, a more in-depth assessment is provided below from a data protection point of view.

When choosing and deploying the possible solutions, legal obligations of all parties involved and key requirements on the processing of personal data as per the applicable regulatory framework have to be taken into account.[109]

The cornerstone rules and principles to be considered, as laid down in the Eurojust Regulation[110], are:

Lawfulness and Fairness: processing personal data in the context of this project should be lawful only if and to the extent that processing is necessary for the performance of task carried out by Eurojust on supporting and coordinating the cooperation between national authorities on the prevention, investigation, detection or prosecution of criminal offences. The Eurojust Regulation provides for a list of serious crimes that Eurojust is competent to deal with, namely cases of terrorism, organised crime, environment crimes, crimes against humanity, and others.[111] It means

[109] The key requirements on the processing of operational personal data by Eurojust are laid down in the Eurojust Regulation and in Article 3 and Chapter IX of Regulation 1725/2018.

[110] In what follows, we only describe the key rules and principles laid down in the Eurojust Regulation. However, other important and more general principles established in Regulation 1725/2018 are of equal importance.

[111] Eurojust Regulation, Art. 3(1) and Annex 1.

that any processing of personal data which is not strictly necessary to fulfil the abovementioned purposes, or which falls outside the scope of the authority of Eurojust in the context of the CMS, may be deemed unlawful.

Data Minimisation: solutions must facilitate that personal data within the functionalities is adequate, relevant and not excessive in relation to the purposes for which they are processed. For instance, temporary work files must not contain any personal data other than those referred to in points (1)(a) to (i), (k), and (m) and 2 of Annex II of Eurojust Regulation[112], i.e. name, date and place of birth, nationality, description and nature of alleged offences, criminal category and others.[113]

Special categories of operational data: The processing of personal data related to criminal convictions and offences is by nature considered to be sensitive in virtue of the fundamental rights and freedoms at stake. Therefore, such processing is worth of stricter protection. Notwithstanding the sensitivity of the criminal-related personal data, the Data Protection Regulation 1725 provides for further specific categories of personal data that are deemed to be special and merits even higher protection. Processing of personal data related to special categories is allowed only where strictly necessary for the operational purposes. This limitation is particularly relevant in the further development of the Counter-Terrorism Register component. The nature of data processed in the context of counter-terrorism investigations is likely linked to categories of data deemed special. The re-use of the CMS business intelligence and advanced search functions in the Register to automate the cross-match of datasets might result in unlawful discriminatory profiling. A detailed data protection impact assessment is to be performed prior to the deployment of such capability, envisaging measures and safeguards to address the risks of such processing operation.

Notably, the Eurojust Regulation prohibits the processing of such data in the index of the CMS.[114] Procedural measures to immediately inform the Data Protection Officer on such insertions in the registry might be considered, as it is explicitly prescribed by the Eurojust Regulation.

Storage Limitation: solutions should allow for the defining and deploying of appropriate (maxima and minima) time schedules that should result in the automated erasure of personal data. Technical or procedural means that would allow for the periodic review of the data in order to assess the need for their retention and/or deletion should also be considered. The Eurojust Regulation sets forth the time limits applicable, rules on the procedural measures for continued storage and the returning of original documents to national authorities, when applicable.[115] Therefore, the new CMS must allow for IT capabilities or a combination of the latter with procedural measures to ensure that data retention/deletion requirements are effectively addressed.

Integrity and Confidentiality: At the design of the CMS, a risk assessment should take place to identify the security risks that involves the new system architecture and how these are, at present, or could be, mitigated. To the extent a security plan or a security risk assessment has already covered the previous system, it is worthwhile checking the relevance of the plan and the need to update it. Practically, appropriate security measures, translated into IT specific controls, but also policies and procedures, must be put in place to ensure that the integrity, confidentiality and availability of the data is preserved throughout the data communications and exchanges enabled

[112] Eurojust Reg. 1727/2018 Art. 23 (1) (4) and Art 27.

[113] See Eurojust Reg. 1727/2018 Annex II.

[114] Eurojust Reg. 1727/2018 Art. 27 (4).

[115] Eurojust Regulation, Article 29, provides a set of date triggers and limits applicable in which personal data may not be stored beyond.

through the CMS. Relevant controls worth to being checked are on equipment access, data media and transport, storage, user and data access, communication and input.[116] Additionally, systems should ensure recovery and integrity of data.

Data Subject Request: Eurojust must comply and respond to data subject requests.[117] Individuals have the right obtain from Eurojust, to the extent allowed by law, a confirmation whether or not personal data concerning him or her are processed, and where that is the case, have the right to access operational personal data; they also have a right to rectification of inaccurate personal data or erasure where the processing infringes Data Protection Regulation, or where data must be erased in order to comply with a legal obligation Eurojust is subject to. Considered solutions should accommodate the data subject request's workflow or allow for interoperable integration with other solutions used by Eurojust to this end. Workflow includes, but is not limited to, receiving the notification, validating the identity, verifying admissibility of the request with the competent authority, complying with the request (when applicable) and informing the decision to the data subject.

Involvement of the DPO: National members should allow the Data Protection Officer access to the temporary work file in which they are working on the individual cases. The Data Protection Officer must be informed by the national member of the opening of each new temporary work file that contains personal data.[118]

Prohibition to establish automated data files: Eurojust may not establish any other automated file than the Case Management System. However, the national member may temporarily store and analyse personal data for the purpose of determining whether such data are relevant to Eurojust's tasks and can be included in the Case Management System. That data may be held for up to three months.[119]

Lastly, it is important to note that the Integration Layer, by means of facilitating the interoperability and integration in between systems involved in the Digital Criminal Justice landscape, naturally allows for an increased number of personal data processing operations between stakeholders, triggering considerations on the responsibilities over the personal data in *transmission*. In this context, the Integration Layer must be designed in a manner which allows for the deployment, accountability and enforcement of the applicable data protection rules to ensure compliance throughout the entire personal data lifecycle, no matter where it resides.

Concerning its Integration Layer, Eurojust remains the controller of the personal data and must ensure that its data protection and security obligations[120] are adequately implemented and followed.[121] To the extent that the layer would enable the communication between Eurojust and external parties within the Eurojust domain, solutions' authorisation and authentication capabilities must reflect Eurojust's access rules to operational personal data[122], as well as to accommodate specific access authorisation provisions to the Case Management System, as laid down by Eurojust's data protection Rules of Procedures.[123] Additionally, solutions must also allow for the

[116] Eurojust Regulation, Article 30, explicitly provides for the applicability of Article 91 of Regulation 2018/1725 on the mechanisms to ensure the security of operational data.

[117] Eurojust Reg. 1727/2018 Art. 31-33, Reg. 1725/2018 Art. 80-84.

[118] Eurojust Reg. 1727/2018, Art. 23.5.

[119] Eurojust Reg. 1727/2018, Art. 23.6.

[120] For detailed information, please refer to sections 5.3.3 and 5.3.4.

[121] Rules of Procedure on the Processing and Protection of Personal Data at Eurojust, OJ L 50, 24.2.2020, Articles 3 and 6.

[122] Eurojust Regulation, Article 34.

[123] Rules of Procedure, *supra*, Article 12.

enforcement of data protection rules applicable in the course of the services transactions in the communication layer: even if temporarily, there is processing of personal data[124] (to the extent necessary to fulfil a transaction, e.g. creation of a link), and data protection and security rules should be observed by Eurojust (e.g. by setting up automatic retention periods for transactions in the queue, by minimizing access to only information on existing links in between systems, etc.) to prevent unlawful processing of personal data (e.g. misrouting, unauthorized message alteration, unauthorized disclosure.).

5.4.5 Governance

Eurojust would be driving the redesign of its CMS and would be in charge of its maintenance. It would be advisable that Member States are invited to provide their input in the preparation of the revamp, in their capacity of Eurojust National Desks, as they are users of the CMS, and are thus part of the CMS data flows.

5.4.6 Use of innovative technologies

This section presents potential use cases for the use of innovative technologies for cross-border judicial cooperation in the implementation of the Redesigned Eurojust CMS. The use cases explore how the following technologies could be leveraged: Robotic Process Automation (RPA) and Artificial Intelligence (specifically, Natural Language Processing and Generation).

However, these use cases were identified based on insights collected in the course of this study, and are not an exhaustive list of all potential use cases. Creating a complete list of all potential use cases would be the object of separate studies, which could fit under the actions 11 (‘Artificial Intelligence for Justice’) and 18 (‘Blockchain for Justice’) of the 2019-2023 Action Plan for the European e-Justice.

5.4.6.1 Registering cases into the Eurojust CMS using Robotic and Intelligent Automation

The table below presents a use case on the possible use of Robotic and Intelligent Automation.

Table 26: Innovative technologies - Use case for Robotic and Intelligent Automation

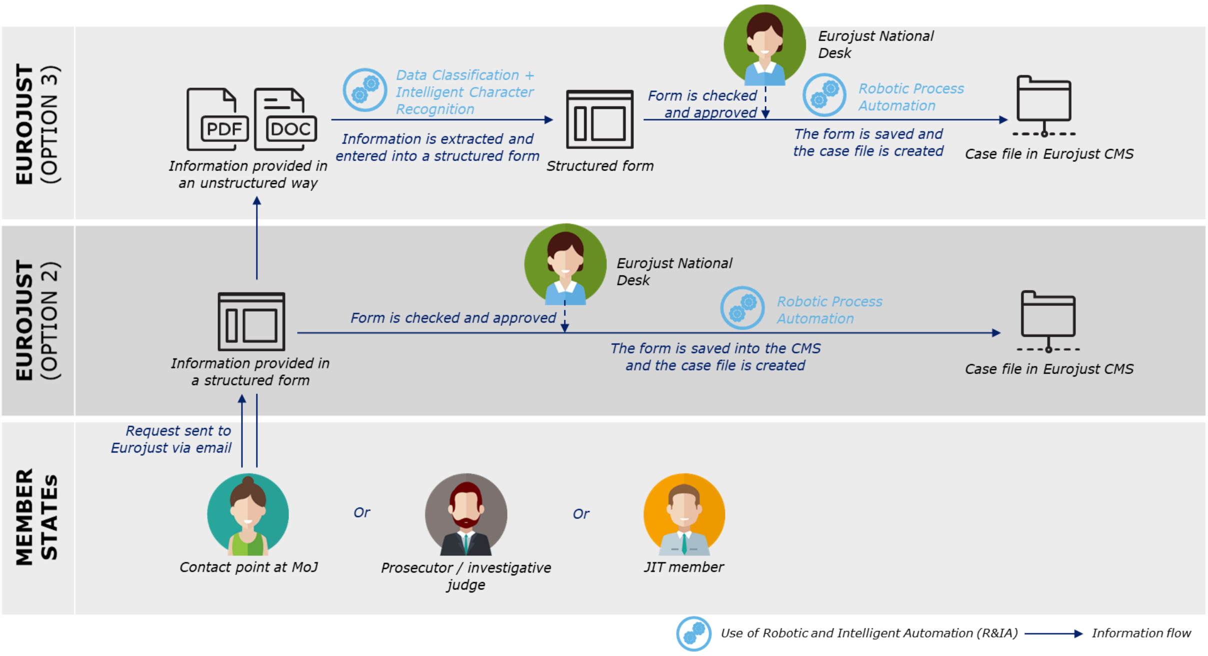
Use case: Registering cases into the Eurojust CMS using Robotic and Intelligent Automation	
Problem statement	Currently, information about temporary work files (TWFs) is sent by various stakeholders at national level and entered manually into the CMS by a member of the National Desk of a country. Because of the difficulty to use the CMS, this is a lengthy and cumbersome process.
Use case	This use case proposes to ease this process by automatically enabling the registration of TWFs into the CMS. To do so, 3 implementation options are possible: • *Option 1*: design and build the new EJ CMS so that the front-end is exposed to stakeholders at national level making the request. In this case, there is no need to use Robotic and Intelligent Automation technology.

[124] Please note that the use of encryption techniques to enhance the security of the personal data transmitted and the processing of metadata does not, by default, prevent the applicability of data protection rules under the Regulation 1725/2018 and the Directive 2016/680 as the material scope of both legal instruments is any information related to an *identified or identifiable* natural person.

	- *Option 2*: use structured forms for stakeholders at national level to send requests to CMS, which a robot can use to enter the information from the form into the CMS (simple RPA). - *Option 3*: use a robot to extract the relevant information from the unstructured information received (e.g. a document or an email), and enter it into a structured form in the CMS. This form will have to be verified and approved by the National Desk before it is saved into the CMS.
Added value	- Ease and speed up the process of registering TWFs (or cases) into the CMS. - Ensure the National Desks can focus on other operational related work. - Improved quality of data entered into the CMS. - Improved throughput time (end to end time to put case into the system) – case is entered real time and the flow is triggered much faster.
Key considerations	- Need a big set of data to extract info from, to train the tool to classify it and ensure it enters the CMS in a consistent way. - Need to know which data fields should be entered into the CMS. - Need to re-educate people to change the way they work (the biggest difficulty).
Potential technologies to use	In the case of option 3, several technologies would have to be combined: for Robotic Process Automation (RPA), for text extraction and classification and for Intelligent Character Recognition (ICR) if the text provided is not readable. Examples of technologies to be used are: - RPA: Blueprism, UI Path. - Classification: Expert Systems or custom-made. - Intelligent Character Recognition (ICR): ABBYY.

The figure below displays the process flow in this use case.

Figure 23: Robotic and Intelligent Automation example - Process flow


EUROJUST (OPTION 3)
PDF
DOC
Information provided in an unstructured way
Data Classification + Intelligent Character Recognition
Information is extracted and entered into a structured form
Structured form
Eurojust National Desk
Form is checked and approved
Robotic Process Automation
The form is saved and the case file is created
Case file in Eurojust CMS
EUROJUST (OPTION 2)
Information provided in a structured form
Eurojust National Desk
Form is checked and approved
Robotic Process Automation
The form is saved into the CMS and the case file is created
Case file in Eurojust CMS
MEMBER STATES
Request sent to Eurojust via email
Contact point at MoJ
Or
Prosecutor / investigative judge
Or
JIT member
Use of Robotic and Intelligent Automation (R&IA)
Information flow

5.4.6.2 Creating CIFs using Artificial Intelligence

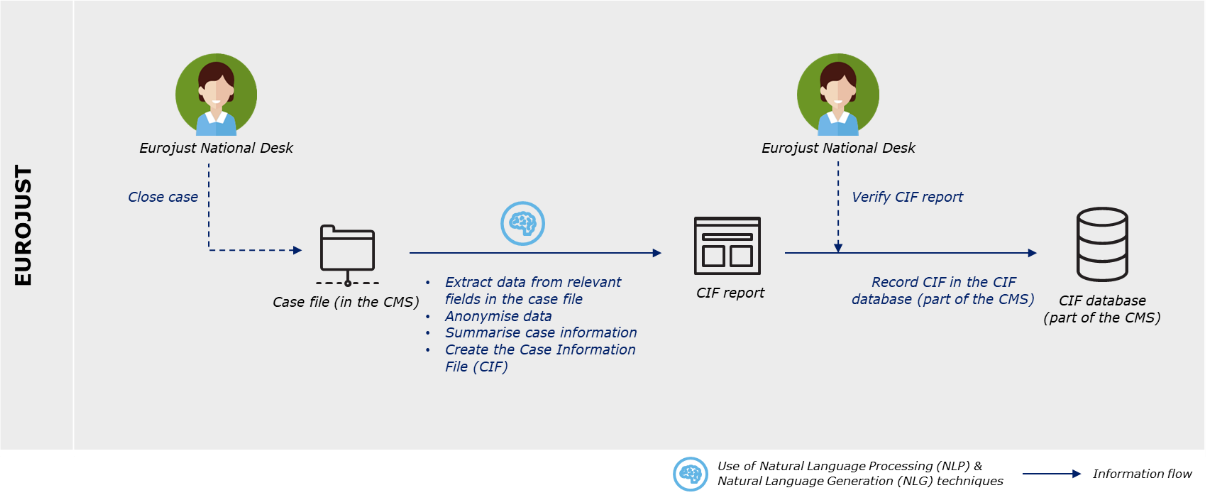
The table below presents a use case on the possible use of Artificial Intelligence.

Table 27: Innovative technologies - Use case for Artificial Intelligence

Use case: Creating CIFs using Artificial Intelligence	
Problem statement	• Currently, Case Information Files (CIFs) are not all recorded in the CIF database because of the lack of time of National Desk staff to do so.
Use case	• This use case proposes to use Artificial Intelligence (namely, Natural Language Processing (NLP) and Natural Language Generation (NLG) tools) to automatically create CIF forms once a case is closed. The National Desk staff will only have to verify that the information in the form is correct before it is recorded in the CIF database.
Added value	• Less time spent creating Case Information Files (CIFs). • Ensure all CIFs are recorded for all cases handled by Eurojust, thereby improving the knowledge management capability of the organisation.
Key considerations	• Algorithms would be needed to: ◦ Understand the language used to describe the case and turn it into structured data - covered by NLP algorithm. ◦ Transform the data (e.g. to anonymise it) and generate a report (in text) about the case - covered by NLG algorithm. • Need to define which type of information should be contained in the CIF. • Need a big set of data to train the algorithm on, and ensure it can learn to create reports containing reliable information. • Translation is not an issue as a translation tool can be used if needed.
Potential technologies to use	• NLP: IBM (Watson), Amazon (Lex), Microsoft. • NLG: Narrative Science, ARRIA, Automated Insights or custom. • Translation: Google API.

The figure below displays the process flow in this use case.

Figure 24: Artificial Intelligence use case - Process flow


EUROJUST
Eurojust National Desk
Close case
Case file (in the CMS)
• Extract data from relevant fields in the case file
• Anonymise data
• Summarise case information
• Create the Case Information File (CIF)
CIF report
Eurojust National Desk
Verify CIF report
Record CIF in the CIF database (part of the CMS)
CIF database (part of the CMS)
Use of Natural Language Processing (NLP) & Natural Language Generation (NLG) techniques
Information flow

5.4.7 Conclusion

The redesign of the Eurojust CMS is one of the key elements of the re-defined IT landscape for Cross-Border Digital Criminal Justice proposed in this study. The new Redesigned Eurojust CMS would be composed of five main logical components, which in turn are composed of one or several components and/or functions. The main logical components would be: the Core CMS, the Counter-Terrorism Register, the JIT Admin Portal, the Action Day Collaboration Platform and the Integration Layer (the different functionalities and capabilities for these components are presented in section 5.4.1).

The technical assessment of this solution presents a market overview together with a preliminary analysis of possible vendor solutions as well as general technical considerations. In terms of technical implementation, the assessment presents different vendor solutions for each of the components. For the core CMS (including the Counter-Terrorism register, and the JIT Admin Portal), the report explains that the Case@EC is the system in place for several entities within the European institutions. Nevertheless, it should be noted that using a custom built system may entail a risk as it may not follow current technological trends and evolutions, hampering its future proofness. The assessment takes into account two other vendor solutions that might fit the current high-level requirements for the Eurojust Core CMS. Therefore, this report recommends to conduct a more in-depth assessment to select the most appropriate solution.

The security assessment explains the security capabilities, considerations and features that are relevant for each of the components, and which should be translated to security requirements and controls, at the design and implementation phase of the target architecture.

In terms of legal basis, the re-design of the Eurojust CMS can be conducted based on the current legal framework, which is the Eurojust Regulation.

As for data protection, the Redesigned Eurojust CMS should first and foremost comply with the applicable provisions from the Eurojust Regulation and Regulation 2018/1725. This legal framework implies that the solution must be in line with the following data protection rules and principles: lawfulness and fairness, purpose limitation, quality and accuracy of personal data, data minimisation, data protection by design and by default, special categories of operational data, storage limitation, integrity and confidentiality, accountability, data subject requests, and automated individual decision-making (including profiling). Before the deployment of this solution, it should be noted that a data protection impact assessment is needed, especially concerning necessity and proportionality of data processing, an evaluation of the risks to the rights and freedoms of the data subjects, the measures contemplated to address the risks, safeguards, security measures and mechanisms to ensure the protections of the operational personal data. In addition, the Redesigned Eurojust CMS should take into account specific provisions regarding the involvement of the Data Protection Officer and the prohibition to establish automated data files, as set out in the Eurojust Regulation.

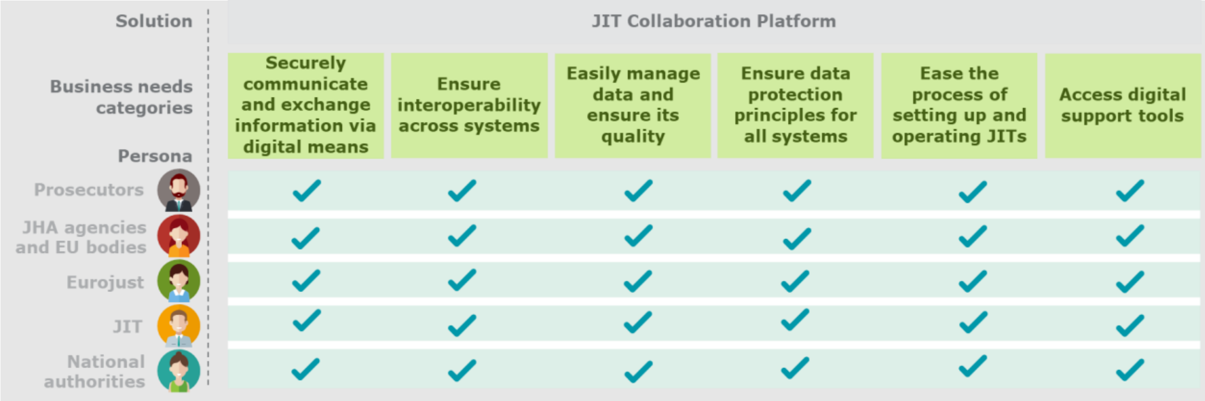
From a governance perspective, this solution would be developed, hosted, and subsequently maintained by Eurojust itself. Member States would be invited to provide input and their views on the redesign of the solution in their capacity of Eurojust National Desks.

Lastly, the report presents two use cases to use innovative technologies (i.e. Robotic and Intelligent Automation, and Artificial Intelligence) in the Redesigned Eurojust CMS.

5.5 JIT Collaboration Platform

The fact that Joint Investigation Teams lack a secure tool for collaboration and exchange of information was clearly identified during the interviews with the Member States, JHA agencies and EU bodies conducted in the context of this study. Indeed, currently messages, information and evidence about ongoing investigations are exchanged between JIT members either by non-secured email, or using unsecure digital communication tools, or in non-digital ways (e.g. physically during meetings, or using registered mail services). The current ways of working do not comply with security requirements (e.g. to ensure that data about national criminal cases remains in Europe) and do not make use of the possibilities offered by digital technologies to improve online communication and collaboration. Therefore, this report proposes to create an online collaborative platform to support the functioning of JITs, which would be part of the future landscape of Cross-Border Digital Criminal Justice. The JIT Collaboration Platform would support the business needs presented in the table below.

Figure 25: JIT Collaboration Platform - Business needs mapping



Solution	JIT Collaboration Platform					
Business needs categories Persona	Securely communicate and exchange information via digital means	Ensure interoperability across systems	Easily manage data and ensure its quality	Ensure data protection principles for all systems	Ease the process of setting up and operating JITs	Access digital support tools
Prosecutors	✓	✓	✓	✓	✓	✓
JHA agencies and EU bodies	✓	✓	✓	✓	✓	✓
Eurojust	✓	✓	✓	✓	✓	✓
JIT	✓	✓	✓	✓	✓	✓
National authorities	✓	✓	✓	✓	✓	✓

This solution is supported by:

- Practitioners in EU Member States: in the survey we conducted, out of the 220 participants replying to this question, more than half indicated that the platform is an essential need (27%) or necessary (48%). Only 10% indicated it is slightly necessary, and 1% said it was not necessary.
- Member States representatives: during the Expert Group Meeting of 13-14 January 2020, Member States representatives recognised that there is a clear need from practitioners for such a tool. They also suggested that this tool could be extended to cover the process of setting up a JIT.
- The second JIT evaluation report[125] published by Eurojust: the report proposes to assess the feasibility of an 'operational online collaborative environment', which should enable law enforcement and judicial authorities involved in a JIT (including agencies such as Europol)

[125] http://www.eurojust.europa.eu/doclibrary/JITs/JITsevaluation/Second%20JIT%20Evaluation%20Report%20(February%202018)/2018-02_2nd-Report-JIT-Evaluation_EN.pdf

to securely 'post' information and evidence. Moreover, it should ensure the traceability (and consequently, further admissibility) of the evidence exchanged.

Consequently, the JIT Collaboration Platform would be a secure online collaboration tool that would allow easy communication through instant messages and video conferences, as well as the electronic sharing of large amounts of information and evidence between two or more JIT partners. This tool would also allow the planning and coordination of JIT operations, as well as enabling the set-up of JITs.

Crucially, as the JIT partners would use the tool to collect and exchange evidence, the JIT Collaboration Platform must ensure a chain of evidence that can be used in judicial proceedings.

Finally, as the platform would be re-used by the various parties involved in JITs (including JIT members such as prosecutors from the Member States, but also third countries, JHA agencies and EU bodies and national authorities) which are geographically spread across Europe, all communications must go over the secure communication channel to be used in the context of Cross-Border Digital Criminal Justice. Moreover, an integration with e-EDES should be envisaged.

As far as the EIF and the Sharing and re-use framework are concerned, this solution addressed the following recommendations:

Table 28: EIF and Sharing and re-use recommendations addressed by the JIT Collaboration Platform

European Interoperability Framework	Sharing and re-use framework
#5: Ensure internal visibility and provide external interfaces for European public services	#3: Communicate your needs
#6: Re-use and share solutions, and cooperate in the development of joint solutions when implementing European public services	#4: Define set of requirements supporting common business processes
#8: Do not impose any technological solutions on citizens, businesses and other administrations that are technology specific or disproportionate to their real needs	#10: Decide the type of rights' attribution approach to be used as early as possible and inform all involved
#12: Put in place mechanisms to involve users in analysis, design, assessment and further development of European public services	#18: Check the reusability of existing solutions before developing a new one
#15: Define a common security and privacy framework and establish processes for public services to ensure secure and trustworthy data exchange between public administrations and in interactions with citizens and businesses	
#17: Simplify processes and use digital channels whenever appropriate for the delivery of European public services, to respond promptly and with high quality to	

European Interoperability Framework	Sharing and re-use framework
users' requests and reduce the administrative burden on public administrations, businesses and citizens	
#19: Evaluate the effectiveness and efficiency of different interoperability solutions and technological options considering user needs, proportionality and balance between costs and benefits	
#30: Perceive data and information as a public asset that should be appropriately generated, collected, managed, shared, protected and preserved	
#46: Consider the specific security and privacy requirements and identify measures for the provision of each public service according to risk management plans	

5.5.1 Presentation of the solution

As explained in the introduction to this section, the aim of the JIT Collaboration Platform is to allow for:

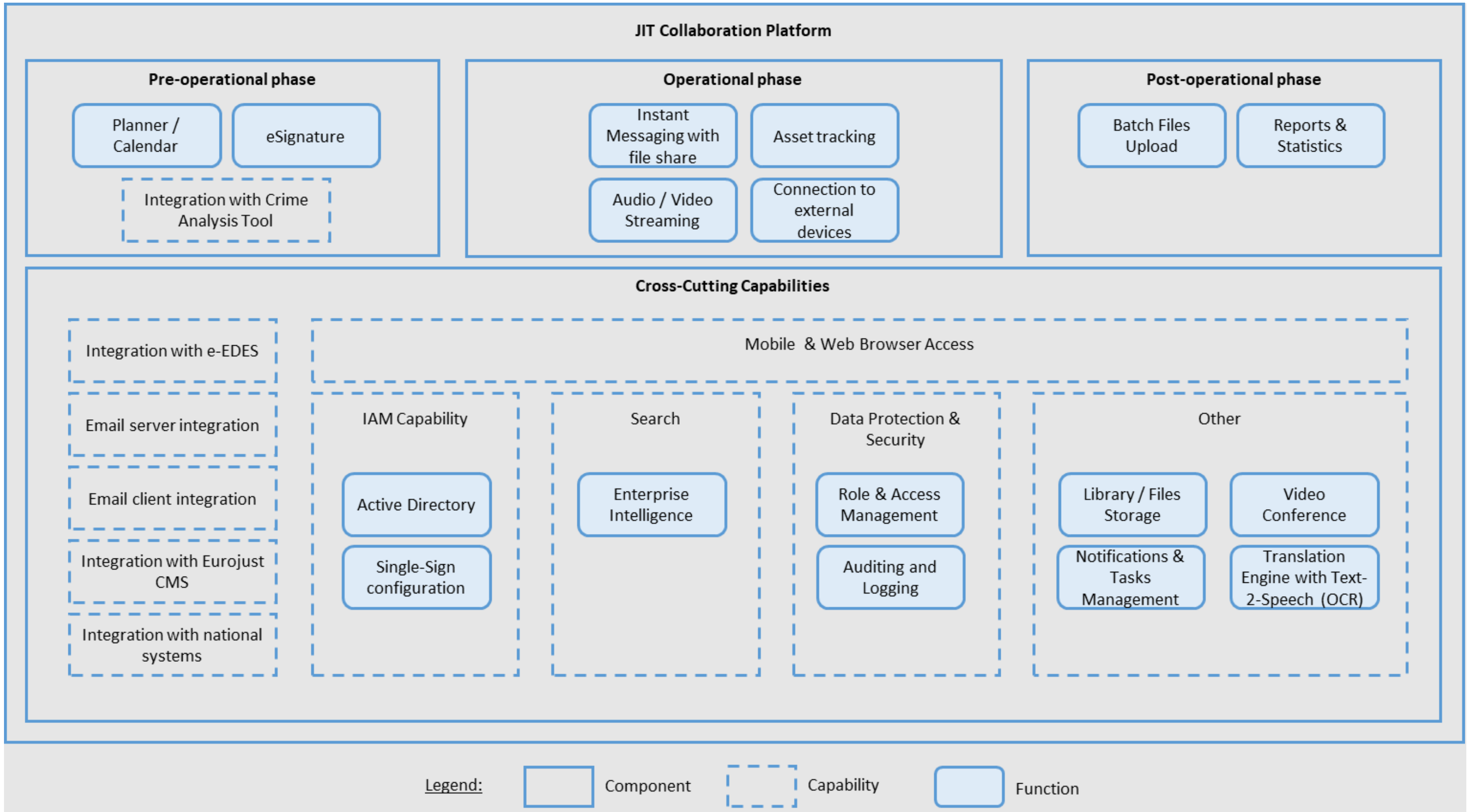
- The set-up of JITs.
- The planning and coordination of JIT operations.
- Secure online communication, during JIT action days as well as during the preparation and follow-up to a JIT.
- Storage facility and evidence traceability.

The section below details the technical capabilities needed in order for the JIT Collaboration Platform to fulfil its objectives.

5.5.1.1 Capabilities

Figure 26 below shows the capabilities and functionalities of the future JIT Collaboration Platform.

Figure 26: JIT Collaboration Platform



These capabilities/functions can be further grouped into four areas in the JIT Collaboration Platform: the capabilities/functions specific to the pre-operational phase, those specific to the operational phase, those specific to the post-operational phase, and cross-cutting capabilities and functions. These different capabilities and functions are further detailed below.

Table 29: JIT Collaboration Platform – JIT Collaboration Platform

Capability / Function	Description
Pre-operational phase	
Planner/Calendar	This feature would enable the setting up of online meetings and video conference calls (together with the "Video Conference" functionality). In addition, it would help to swiftly adjust operational plans thanks to real-time updates of the planning of meeting participants (e.g. in case of an unexpected change of route during JIT action day).
eSignature	This function would enable the electronic signature of forms/documents by the different parties involved in a JIT, in particular during the set-up phase.
Integration with a Crime Analysis Tool	This capability would enable integrations between the JIT Collaboration Platforms and a Crime Analysis Tool that may be used by JIT members when investigating crimes.
Operational phase[126]	
Instant Messaging with file share	This function would support the need for secure instant messaging between JIT participants.
Asset tracking	This function would enable seeing which users are using the platform at a given moment, and where they are located. This functionality would be particularly useful in the context of JIT action days.
Audio/Video Streaming	This function would allow live audio and video streaming between participants, for multiple devices at a time.
Connection to external devices	This function would allow connections with external devices (such as drone cameras, cameras, beacons, etc.) that would provide video footage visible in a video feed.
Post-operational phase	

[126] The functionalities of the JIT Collaboration Platform that will be used during the JIT operational phase are inspired from those offered by Europol's Virtual Command Post.

Batch upload file	This function or integrated software component would allow to upload multiple files at the same time.
Reports & Statistics	This function would allow to create reports and statistics on the outcome of a JIT, once the JIT is closed.
Cross-cutting capabilities	
Integration with e-EDES	As this report recommends the use of e-EDES amongst all stakeholders involved in cross-border criminal justice (including national authorities and prosecutors in Member States, as well as JHA agencies and EU bodies), the JIT Collaboration Platform would need to be integrated with it. This capability would allow users to send and receive e-EDES messages from the JIT Collaboration Platform, which would be useful in case a JIT member needs to communicate with a person or entity that is not part of the JIT (for instance, a national authority from a Member State that is not part of the JIT).
Email server integration	This capability would allow users to add emails to a JIT case file, for other JIT members to have access to it.
Email client integration	This capability would allow users to send outgoing mails or meeting invitations from the JIT Collaboration Platform to external parties that do not have access to e-EDES (for instance, an online service provider).
Integration with the Redesigned Eurojust CMS	This capability would allow for a JIT case file (including information and evidence) to be transferred and stored in the Redesigned Eurojust CMS following the closure of the JIT.
Integration with national systems	This capability would allow for information and evidence exchanged in the context of a JIT to be transferred between national systems and the JIT Collaboration Platform.
Mobile & Web Browser Access	This capability would allow users to access the JIT Collaboration Platform either using their corporate laptops/PCs or via a web browser using their mobile devices.
Active Directory	This function would enable storage and management of user identities and access permissions in the context of Cross-Border Digital Criminal Justice.
Single-Sign configuration	This function would allow configuration and integration to a Single Sign-On facility, if available at the time of development, to enable the user to securely sign-on to multiple independent applications while using just one set of authentication credentials.
Enterprise Intelligence	This function would allow users of the JIT Collaboration Platform to make searches on the data contained in it, and would allow the visualisation of the links between main suspects and possibly other entities.

Library/Files Storage	Both the batch files upload and the file storage/library would allow for the secure upload and storage of all communication, information and evidence exchanged over the course of a JIT.
Integration with Large Files Solution	This capability would allow for access to large files stored in LFS.
Video Conference	This function would support the need for a secure video conferencing facility during JIT meetings or online meetings.
Notifications & Tasks Management	This function would allow to list and distribute tasks between JIT members, and to follow-up on tasks. It would also allow JIT members to receive notifications, for instance a reminder to complete a task, or if a new message was received.
Translation Engine with Text-2-Speech (OCR)	Currently, interpretation within JITs is provided during coordination meetings, and translation services are covered via Eurojust's financial assistance. This report identified the need for a translation engine (i.e. machine translation) with a Text-2-Speech functionality for immediate translation and consultation during JIT meetings. While this technology might currently lack precision in less widely spoken languages, given the limited terminology in judicial cooperation matters, it is worth investigating available solutions. It must be noted that as it stands, the CEF eTranslation Building Block does not incorporate Text-2-Speech functionality.
Roles & Access Management	Roles and access management would allow for the secure management of user identities and access permissions within the JIT Collaboration Platform, including case-by-case granular access permissions. It would allow authentication and authorisation of the logged-in users.
Auditing and logging	Auditing and logging would allow to keep a trail of who did what and when regarding a certain operation in the JIT Collaboration Platform, including the logging of all entries, transactions, modifications, sharing, printing, editing, searching of data, and would provide a complete audit trail. It would also enable consolidated reporting across the different log stores. This function would support the need to ensure the traceability (and thus, further admissibility in front of court) of the information and the evidence exchanged in the context of a JIT.

5.5.2 Technical assessment

The technical assessment presents possible scenarios for the implementation of the JIT Collaboration Platform, and compares these scenarios based on different technical criteria.

5.5.2.1 Possible scenarios

This report identified three possible scenarios of software products that could be purchased or re-used to provide the functionalities of the JIT Collaboration Platform:

- Scenario 1: re-use OLAF's Virtual Operations Coordination Unit (VOCU) tool.
- Scenario 2: purchasing a commercially available off-the-shelf (COTS) product.
- Scenario 3: building a custom implementation from scratch.

5.5.2.1.1 Scenario 1: Re-use OLAF's VOCU tool

The Virtual Operations Coordination Unit (VOCU) tool is a custom tool created and maintained by OLAF in order to support coordination and the exchange of information in the context of Joint Customs Operations. Although it is based on pre-existing requirements, the VOCU tool was rebuilt in 2013 in order to be based on Java technology. All data contained in VOCU is hosted by OLAF.

VOCU is web-based application accessible through the AFIS Portal. Because the AFIS Portal is a closed environment dedicated to customs authorities, it cannot be re-used for the purpose of Cross-Border Digital Criminal Justice. However, this scenario envisages the re-use of VOCU independently from the AFIS Portal, which would require it to be decoupled from the AFIS mail, the library and the access management functionalities of the AFIS Portal. Nevertheless, reusing a tool like VOCU outside the AFIS platform could be compared to developing a new custom application from scratch from a cost perspective, if the interrelationship of the code with the AFIS platform services is taken into consideration.

Indeed, VOCU helps solve similar business needs to those required in the context of the JIT Collaboration Platform, such as communication and secure exchange of information, as well as supporting joint operations. Moreover, VOCU is similar to the JIT Collaboration Platform because it is available only to nominated users (i.e. participants in an operation) from different Member States, who can only access information about the operation in which they are involved, and a Joint Customs Operation is broken down into phases (pre-operation, operation, post-operation) that are similar to the different phases of a JIT operation.

In short, VOCU offers the following functionalities which could be useful in the context of the JIT Collaboration Platform (following some adjustments):

- Integrated mailbox (currently the AFIS mailbox, which would need to be replaced by an e-EDES integration in the context of Cross-Border Digital Criminal Justice).
- Document library (with generic document and documents specific to the operation).
- Structured (customisable) reports, which serve as the support to exchange information as they edited by all participants in the operation.
- Active/connected users can be seen.
- Reports and statistics, as reports can be exported to Excel and VOCU is integrated with Tableau.
- Identity & access management (currently coupled with the identity & access management of the AFIS Portal, which should be changed in the context of the JIT Collaboration Platform).

- Automated notifications.
- Audit and logging of changes to the report.

However, the following functionalities of the future JIT Collaboration Platform are missing from it:

- Instant messaging
- Video conferences and audio/video streaming
- Planner/calendar function
- Integration with an electronic signature module
- Workflow and task management
- Integration with a translation engine
- Mobile access

Finally, Table 30 below summarises the pros and cons of reusing OLAF's VOCU tool.

Table 30: OLAF VOCU - Pros and cons

OLAF VOCU	
Pros	**Cons**
Ready to use and proven solution in the context of Joint Customs Operations.	Does not cover all the requirements for the JIT Collaboration Platform.
Could re-use the code built by OLAF at a relatively low cost.	Tool based on old requirements and technology, which may not be in line with the possibilities offered by more modern products.
	It is burdensome to develop additional features and maintain the tool in house.
	Needs to be decoupled from the AFIS Portal.

5.5.2.1.2 Scenario 2: Purchase a commercial off-the-shelf (COTS) product

The following vendor solutions were short-listed as they satisfy a certain level of high-level criteria (including functionalities and security requirements) for the JIT Collaboration Platform. However, it must be noted that this analysis is not exhaustive, and the solutions below must be further assessed against the features required for the JIT Collaboration Platform.

This analysis was based mainly on analysts' assessment of products for "Workstream Collaboration".[127] In addition, the basic requirement for on premise deployment was applied, which limits the number of candidate products identified. Indeed, only a few vendors have on premise options, and cloud offerings dominate the market.

5.5.2.1.2.1 Wire

Wire is based in Switzerland. Its collaboration suite is an open-source code and is featuring messenger, voice, video, conference calls, file-sharing, and external collaboration protected by secure TLS end-to-end-encryption[128] for all its features – making it the most secure of the on-premises solutions mentioned in this section. It is used by companies, governments and international organisations in Europe (e.g. UNICEF) and can be deployed on premise in its

[127] Gartner - Market Guide for Workstream Collaboration, ID G00374469

[128] See: https://wire-docs.wire.com/download/Wire+Security+Whitepaper.pdf

Enterprise version.[129] It offers a broad set of integrations with open APIs and built in Single Sign-On support with SAML 2.0. However, Wire does not support mail integration.

Wire comes with the following features:

- Voice and video messages
- Timed conversations
- Edit and delete conversations
- File sharing and productivity
- Screen sharing
- Unlimited chats
- History backup

Below a list of consideration listed as pros and cons for this solution based on review sites and users experiences:

Table 31: Wire Collaboration platform for Enterprise - Pros & Cons

Wire Collaboration platform for Enterprise	
Pros	**Cons**
Easy to setup.	High costs.
Very good quality in communication (voice, video, messages).	Slow in loading image format messages.
Strong encryption.	Limited numbers of caller in a call.

5.5.2.1.2.2 Zimbra

Zimbra is operated by the US-based company Synacor. The Zimbra Collaboration Network Edition is a leading open source messaging and collaboration solution, trusted by more than 5,000 companies and public sector customers in over 140 countries. It also leverages more than 1,900 partners globally including Europe.

It includes complete email, contacts, calendar, file sharing, tasks and messaging/videoconferencing, all accessed from the Zimbra Web Client via any device and can be deployed as a traditional on premise installation. It can cover most of the requirements of the JIT Collaboration Platform based on its features.[130] It supports web services SOAP APIs for integration with external applications as well as mail client/messaging server and active directory integration.

Zimbra comes with the following features:

- Sharing resources, email and calendar:
    - Tagging and conversation
    - Search- based inbox
    - Cross-platform
    - Offline Access
    - Mobile and desktop synchronization
- Calendar

[129] See: https://wire.com/en/products/technology/
[130] See: https://www.zimbra.com/email-server-software/product-edition-comparison/

  - Web based advanced calendar
  - Multi-calendar management
  - Sharing and delegating
  - Interoperability with Microsoft Exchange
- Documents and files
  - Daily workflow
  - Share and manage inboxes, files, documents and calendars
  - Roles definition management
  - Publication options
  - Email and workflow integrations
  - Microsoft Outlook compatible

Below a list of consideration listed as pros and cons for this solution based on review sites and users experiences:

Table 32: Zimbra Collaboration platform for Enterprise - Pros & Cons

Zimbra Collaboration platform for Enterprise	
Pros	**Cons**
Good organizer and note features.	Effort in customization.
Easy and efficient email service.	Can be slow, pages are heavy to load.
Very good email service.	Linux based system administration.
Works on VPN.	
Cost efficient.	

5.5.2.1.2.3 eXo

eXo Platform Digital Workplace is a full-featured open-source digital workplace. It is used by governments (French Ministry of Foreign Affairs), administrations (NATO) and law enforcement (French National Gendarmerie) and can be deployed on premise in its Enterprise version.[131] This report estimates that it can cover most of the requirements of the JIT Collaboration Platform based on its features[132] listed below. It is built on open source and open standards and provides a wide range of APIs and open standards for integration[133].

eXo Platform comes with the following features:

- Social Network
- Content Management and Distribution
- Calendars
- Built to localize
- Integration and Extensibility
- Cloud-Ready
- Collaboration tools
- Video calls

[131] https://www.exoplatform.com/product-offer/#table-2
[132] https://www.exoplatform.com/product-offer/#table-2
[133] https://www.exoplatform.com/technology/

- Chats
- Forums
- Wikis
- Dashboards
- Task Management and Scheduling
- Mobile
- Enterprise Portal

Below a list of consideration listed as pros and cons for this solution based on review sites and users experiences:

Table 33: eXo Collaboration platform for Enterprise - Pros & Cons

eXo Collaboration platform for Enterprise	
Pros	**Cons**
Nice functionalities.	Big effort for developers to get used to it.
Easy to use.	Can be very slow.
Java based & open source.	Not much trainings or tutorial available.
Good support.	Customization effort is high.

5.5.2.1.2.4 Microsoft Teams

Microsoft Teams is part of Microsoft's Office 365 offering. It is a unified communication and collaboration platform. This solution includes many functionalities such as a virtual workplace, chat, video meetings, file storage, including collaboration on files, and application integration. This solution allows to integrate third-party application as well, which could be useful for the JIT Collaboration Platform. Indeed, if in the future, more needs come into place, it would be easy to add them upon the core platform. The solution can integrate all the software that is part of the Microsoft Office 365 suite. This means that it is possible to open Microsoft Office documents or trigger conversations via other Microsoft Office tools like Skype for Business or Word, Excel and PowerPoint documents, and open these documents without leaving the workspace.

Microsoft Teams comes with the following features:

- Teams: allows a group of people to join a team through an URL or invitation sent by a team administrator or owner.
- Channels: within the teams, members can set up channels on diverse topics to communicate without using emails or texting. The communication is similar to a group chat application, allowing instant messaging.
- Calls: people can communicate over this feature via multiple possibilities such as instant messaging, VoIP, video conferencing.
- Meeting: meetings can be scheduled directly via this solution and can integrated with Outlook via a plugin.

The Microsoft products are well known in the market and reliable, and they are used in numerous institutions and companies. This platform can be used on mobile devices as well as on workstations.

It must be noted, however, that following the latest privacy discussions between DG COMM and Microsoft about Office 365, Operational Personal Data[134], as defined in Regulation (EU) 2018/1725[135], cannot be used in the Office 365 products as Microsoft cannot ensure sufficient security levels for the processing of such data.

Below a list of consideration listed as pros and cons for this solution based on review sites and users experiences:

Table 34: Microsoft Teams - Pros & Cons

Microsoft Teams	
Pros	**Cons**
Seamless integration with other Microsoft tools.	Effort to setup governance.
Easy to use.	Security concerns regarding the processing of Operational Personal Data.
Well known in the market.	
Good support.	

5.5.2.1.2.5 Cisco Webex

Thanks to the wide range of applications provided by the Cisco Webex suite, Webex allows to create secured collaborative workspaces. Similar to its competitors, it includes many capabilities.

Indeed, the Cisco Webex suite comes with the following features:

- Chat: instant messaging system
- Meet: video conferences
- Whiteboard: real-time collaboration whiteboard
- Schedule: allows to schedule meetings
- Files: secure files storage

It offers capabilities via the Webex App Hub by integrating or developing and connecting new applications. In addition, it includes Microsoft Office 365 integration capabilities. This platform can be used on mobile devices as well as on workstations. Some of the WebEx solutions are already in use by eu-LISA for calls and collaboration.

Below a list of consideration listed as pros and cons for this solution based on review sites and users experiences:

Table 35: Cisco Webex Teams - Pros & Cons

Cisco Webex Teams

[134] Operational Personal Data includes for instance personal data processed for the purposes of a criminal investigation by Union bodies, offices or agencies when carrying out activities in the fields of judicial cooperation in criminal matters and police cooperation.

[135] See here: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1725&from=EN.

Pros	Cons
Seamless integration with other Microsoft tools.	Effort to setup governance.
Easy to use.	Price.
Well known in the market.	
Good support.	

5.5.2.1.2.6 Additional considerations

While the solutions above focus more on communication, there is a possibility to combine specific communication applications to applications that used for tracking or documenting.

For instance, the European Commission is already using Atlassian's Confluence for information exchange and documentation. Besides, a ticketing/tracking system could complete the previous vendor solutions offerings as it would provide functionalities to create and plan tasks, assign them and track them. As an example, JIRA is a tool offered by Atlassian which is broadly used and was initially designed for this specific purpose.

5.5.2.1.2.7 Comparative view of COTS solutions

Table 36 below presents a comparative view of the vendor solutions described in the sections above based on requited functionalities/capabilities for the JIT Collaboration Platform and other technical and security criteria.

Functionalities/capabilities of the JIT Collaboration Platform[136]:

- Instant Messaging
- Video Conference
- Planner/Calendar
- File sharing
- Batch upload file
- Translation Engine with Text-2-Speech (OCR)
- Enterprise Intelligence
- Auditing and logging

Additional technical and security criteria:

- Hosting: the location that would support the application (e.g. cloud, on premise, private cloud).
- EU Data Centre: whether the vendor's data centres are located in the EU.
- Scalability: possibility to incorporated additional capacity (such as additional users) to the application.
- Integration: possibility to integrate the solution into another application platform, which could be useful in case the solution alone does not cover all requirements for the JIT Collaboration Platform.
- End-to-End Encryption: encryption from the sender to the receiver.
- Development effort.
- Deployment effort.

[136] Please refer to section 5.5.1.1 for a description of these functionalities/capabilities.

Other criteria:

- Similar clients in the EU: Reflects the experience of the vendor in serving comparable clients in the EU.

Table 36: Comparative view of COTS solutions

Business needs / COTS solutions		**Wire**	**Zimbra**	**eXo**	**Cisco Webex**	**Microsoft Teams**
Functionalities / capabilities of the JIT Collaboration Platform	Instant Messaging	Yes	No	Yes	Yes	Yes
	Video Conference	Yes	Yes	Yes	Yes	Yes
	Planner/Calendar	No	Yes	Yes	Yes	Yes
	File sharing	Yes	Yes	Yes	Yes	Yes
	Batch upload file	No	Yes	Yes	Yes	Yes
	Translation Engine with Text-2-Speech (OCR)	No	No	No	Yes	Yes
	Enterprise Intelligence	No	Not Native	Not Native	Not Native	Not Native
	Auditing and logging	No	Yes	Yes	Yes	Yes
Technical and security considerations	Hosting	On-Premise/Cloud	On-Premise/Cloud	On-Premise/Cloud	On-Premise/Cloud	On-Premise/Cloud
	EU Data Centre	Yes	Yes	Yes	Yes	Yes
	Scalability	Yes	Yes	Yes	Yes	Yes
	Integration	No	Yes	Yes	Yes	Yes
	End-to-End Encryption	Yes	Yes	Yes	Yes	Yes
	Development effort	Medium	Medium	Medium	Low	Medium
	Deployment effort	Medium	Medium	Medium	Low	Medium
Other considerations	Similar clients in the EU	Unknown	Unknown	French Ministry of Foreign Affairs /NATO	eu-LISA	Multiple large companies

First, it must be noted that none of the vendor solutions presented in this section is able to provide alone all capabilities needed in the context of the JIT Collaboration Platform. Therefore, additional integrations would have to be envisaged with specialised tools used in the context of judicial investigations/ law enforcement (e.g. for crime analysis, asset tracking and connections to external devices). However, based on the preliminary analysis presented in the table above and given the fact that Microsoft solutions were deemed not secure enough to process Operational Personal Data, the most appropriate solution would seem to be the Cisco Webex solution.

5.5.2.1.3 Scenario 3: Build a custom implementation

Building a complete collaboration platform from scratch is feasible, and OLAF's VOCU tools is a pertinent example of this. The flexibility brought by a custom implementation has some advantages and disadvantages. The biggest advantage is of course the fact that the application can be completely customised to suit the needs of its users. Also, the hosting location can be as desired. However, building an application from scratch should be subject to certain technical considerations, which are further detailed in the paragraphs below.

To develop applications, you have to choose specific frameworks that can ease development. Those frameworks are called libraries in technical terms. It means that you re-use some prebuild code. This re-use is practical but has to follow-up on the upgrade of all the libraries. For instance, it is possible to use the libraries that provide the possibilities to build secure applications.

On the market, there are lots of solutions to build applications that meet business needs. However, developing applications from scratch requires a lot of maintenance - code maintenance, library maintenance, amongst others.

Indeed, the libraries used can deprecate, which is a risk. At some point, in the lifecycle of an application, libraries may be replaced by new ones. That can imply rework of code segments to meet the latest standards.

While existing solutions provide by default a range of support from the build phase to the run phase, this scenario would require to hire and train that support to have it in-house. Additionally, it is challenging to ensure 24/7 support for an application. In brief, there is a level of complexity to consider.

One can tailor the deployment of this homemade solution. This is a freedom that is quite important and doesn't have the limitations of the previous vendor solutions. Moreover, it is possible to change the location of the application more quickly since there are no vendor constraints.

The knowledge transmission should happen through documentation as for every software. The difference is on the control and ownership of the knowledge. There is a gain of transparency over the roles and responsibilities of the application and stakeholders.

There might be some licence costs to take into account, as some of the tools used to develop and deploy might come at a cost.

Where vendor solution comes as "finished" products, one should foresee time to put the platform to production and be usable. Additionally, whereas vendor solutions come with a mature application, a custom implementation might face some maturity issues during the process before reaching the stage of completeness and acceptance for all the users.

In conclusion, it would be feasible to build a custom JIT Collaboration Platform, but the costs and efforts considerations are different. As a result, a different risk category needs to be considered when comparing with vendor solutions. However, the main advantage is to increase flexibility and address precisely the needs of the stakeholders.

Table 37: Custom implementation - Pros & Cons

Custom implementation	
Pros	**Cons**
Tailored to include only what is needed.	Time consuming for developers.
Full control over scale, customisation and functionality.	Time consuming for stakeholders and users.
Seamless updates, enhancements and growth.	Costs are unpredictable since they depend highly on development, testing and deployment choices.
No direct licensing costs.	No support.
Complete ownership and rights to the software.	No trial prior to investment.

5.5.2.2 Comparative view

The table below compares the three high level option presented in this section for the implementation of the JIT Collaboration Platform.

Table 38: JIT Collaboration Platform - Technical assessment

	Scenario 1 – Re-use OLAF's VOCU tool	**Scenario 2 – Purchase a commercial off-the-shelf (COTS) product**	**Scenario 3 - Build a custom implementation**
Coverage of the capabilities of the JIT Collaboration Platform	The current implementation of VOCU **does not cover all the capabilities** of the JIT Collaboration Platform. Further developments (or integrations) would be needed to ensure it is the case.	The COTS products examined **do not cover all the capabilities** of the JIT Collaboration Platform alone, and they would need to be integrated with additional tools.	A custom implementation would be developed to be **perfectly tailored to user needs.**
Hosting	VOCU is currently hosted by OLAF, but the possibility of reusing the underlying code and **hosting it anywhere in the EU Institutions could be explored**.	The COTS solutions examined offer **both on premise and cloud** hosting options.	The custom implementation could be **hosted at the preferred location**.
Implementation complexity	**Medium**, as the VOCU tool would need to be	**Low**, as the vendor tools would only need to be	**High**, as the new state-of-the-art

	further developed.	customised.	platform would need to be built from scratch, based on new requirements.
Maintenance	The current VOCU tool is maintained by OLAF. It is **unclear who would maintain the tool** should it be re-used and adapted for the purpose of cross-border judicial cooperation.	**Product updates would be provided by the vendor**. In addition, the entity in charge could be assisted in maintaining the tool by the vendor or a third party.	The chosen entity to develop and host the platform, would be in charge of maintaining it. **No vendor support** would be provided.
EU accreditation	The solution would need to be accredited in order to receive and store EU classified information.	The solution would need to be accredited in order to receive and store EU classified information.	The solution would need to be accredited in order to receive and store EU classified information.
Security & data protection	OLAF's VOCU tool is considered sufficiently secure to exchange data in the context of Joint Customs Operations. However, this should be **reconfirmed** as the future JIT Collaboration Platform would be hosting Operational Personal Data (as defined in Regulation (EU) 2018/1725).	The COTS solutions should be **further assessed to determine if they are secure enough to host Operational Personal Data** (as defined in Regulation (EU) 2018/1725).	The solution should be **developed bearing in mind requirements stemming from the need to exchange and host Operational Personal Data**.
Costs	The cost to re-use the current VOCU tool should be **inexistent to low**, whereas the cost of **additional developments should be further assessed (including decoupling from the**	In case a COTS product (or a combination of products) is chosen, **license prices** would most likely have to be paid. **There would be also a cost concerning integration/development of capabilities not covered by the COTS**	The **costs to develop the platform from scratch are highly uncertain**, since they depend on development, testing and deployment choices.

	AFIS portal).	**product.**	
Risks	The current VOCU tool is built on **old technology** (it was rebuilt in 2013) and **older requirements**. A custom development **may not be in phase with latest technological developments** as it does not receive product updates.	The **security and data protection aspects** of potential COTS solutions should be **assessed carefully**.	Risk of a **costly and lengthy development cycle** to build the JIT Collaboration Platform. A custom development **may not be in phase with latest technological developments** as it does not receive product updates.

Legend: **Strength** **Weakness**

Based on the business needs and capabilities required from the JIT Collaboration Platform, and the assessment presented above, it is recommended to re-use a COTS product for the implementation of the platform. Indeed, the business needs require a modern platform, based on latest technological developments, which leads to a preference for a new solution. Moreover, a custom development presents additional risks related to the uncertain development and maintenance of the platform. Consequently, this report recommends to conduct a more in-depth assessment to select the most appropriate COTS solution, for which a "playing the market" approach should be followed to obtain insights and demonstrations from the solution vendors themselves on the best fitting solution.

However, as highlighted above with the example of Microsoft Teams, the assessment of COTS solutions should pay particular attention to the aspects of data security and privacy, as the JIT Collaboration Platform would be hosting Operational Personal Data (as defined in Regulation (EU) 2018/1725).

Finally, it must be noted that none of the COTS solutions presented above can solve alone all the requirements for the future JIT Collaboration Platform, based on the initial high-level analysis conducted. Therefore, the COTS scenario may consist of a combination of products used together, and the compatibility of these products must be examined.

5.5.3 Security assessment

The means of the JIT Collaboration Platform are to integrate different tools that aim to handle internal/external communications with involved stakeholders in a collaborative way and to provide storage facility and evidence traceability.

From a security perspective, the focus is to guarantee the confidentiality of exchanged data by using robust encryption algorithms to encrypt data in transit or at rest. Encryption of data must at least occur at the transport layer (e.g. TLS channels). A risk assessment shall be performed (preferably) at the design phase by the system owner of the JIT Collaboration Platform to see what type of encryption is required for data at rest. Encryption should be based on the cryptographic products approved by the European Council.[137]

Furthermore, the system owner of the JIT Collaboration Platform needs to establish patch and vulnerability management processes. The purpose is to ensure the JIT Collaboration Platform is not using outdated modules, libraries or software with known vulnerabilities to avoid the compromising of the JIT Collaboration Platform.

Besides, the identity and access management process should be put into place, in order to assure that only authorised personnel have access to the platform.

And finally, the JIT Collaboration Platform should be covered by a Helpdesk incident management process making sure that incidents linked to this platform are recorded, investigated and mitigated in a timely manner. The same applies to the business continuity and disaster recovery processes which should ensure the continuity of services provided by the JIT Collaboration Platform should an unexpected disruptive event occur.

With regards to the scenarios discussed under section 5.5.2.1, we note that all three of them have the potential to fulfil the security objectives and assurance level required for the JIT Collaboration Platform. All three scenarios allow, if well designed, implemented and configured, to ensure at an acceptable level the confidentiality, integrity and availability of Digital Criminal Justice architecture components and data.

However, for choosing the exact vendor solution(s) which would require a separate assessment taking into consideration preferences and business requirements, the following security aspects should be looked into:

1. Re-use of VOCU: security should focus more on the integration aspects when integrating VOCU to the target Digital Criminal Justice architecture. Making sure that VOCU components are incorporated in the target architecture in a secure manner without impacting the security of the existing components.
2. Off the shelf product: as for the first scenario, the security focus should be put on the integration with the target architecture.
3. Implementation from scratch: in this case, the security focus should be put on the Software development lifecycle (SDLC) process in order to ensure that the developed solution is fulfilling security requirements in the different steps of the development activities.

Overall, regardless of the chosen option, a business impact assessment, as well as risk assessment, should be performed by the JIT Collaboration Platform system owner(s) before pursuing design choices. These would be important to make sure that the chosen solution is operating without security impact on other architecture elements and that the risks associated with the implementation of a given option are within the risk appetite.

5.5.4 Legal and data protection assessment

Council Framework Decision 2002/465[138] sets out the rules for the setting up and functioning of the JITs. The rationale behind this legal instrument is that cross-border crime is more effectively

[137] https://www.consilium.europa.eu/en/general-secretariat/corporate-policies/classified-information/information-assurance/

tackled by coordinated and concerted action from several Member States. For this purpose, a JIT can be set up for a fixed period of time following an agreement between the countries involved. This agreement is normally based on the model agreement for setting up a JIT[139] as appended to Council Resolution 2017/C 18/01.[140] The solution presented in this report suggests to create a tool to support setting up, organising and deploying a JIT. This solution can be either (i) developed at EU level, or (ii) deployed in the JIT environment of the Member State leading the JIT. The legal implication of these two scenarios are explained below.

In case this solution is created and developed at EU level, it could consist of a service offered by eu-LISA to Member States that would decide on an ad hoc basis whether to use it in their JITs, ensuring the flexibility of this cooperation tool. The use of the platform would raise some data protection issues (e.g. access rights, controllership of the data, amongst others, see below for further details). Therefore, a legal basis would be necessary in order to establish a clear framework on the use of this instrument. This legal basis would likely be a stand-alone legal instrument, regulating the objective and functionalities of the tool. As indicated above, eu-LISA would be hosting this tool (as enshrined in the provisions of the new legal basis). A relevant amendment to the legal basis of this agency[141] would thus be necessary.

Alternatively, the JIT Collaboration Platform could be envisaged as a technical solution deployed within the IT environment of the Member State leading the JIT. In this case, a legal basis at EU level would not be necessary. However, the question on how exchanges of information (i.e. joint controllership) within the context of the operations of JITs would function should still be considered. This option is however less appropriate, as a legal basis at EU level would allow to establish a specific framework, highly required to duly regulate this tool.

Before the enactment of a new Regulation, a thorough impact assessment needs to be conducted. The operationalisation of an online collaborative environment to serve as single point of communication and exchange of evidence between law enforcement and judicial authorities involved in a JIT raises relevant data protection considerations. The main point to be considered is the controllership of the personal data processed in the platform. A dedicated legal instrument at EU level for JITs that provides clarity on the discussion around controllership is advised, as this would ensure that the environment does not need to be tailored to function under the national law of one or the other Member State.

By nature, a JIT is designed as a provisional entity: established for a limited duration and for a specific purpose in one or more of the Member States involved. The terms under which a JIT operates vary from case to case, but they are normally based on the JIT model agreement as explained above. Under the JIT model agreement, clauses are provided on the access to information, mainly on specific rules on access, handling and use of information and evidence, both for information processed at the time of a JIT formation and information obtained prior to the formation of a JIT. However, once JIT operations are managed on a JIT Collaboration Platform,

[138] Council Framework Decision 2002/465/JHA of 13 June on joint investigation teams , see: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002F0465&from=EN

[139] See: https://www.europol.europa.eu/publications-documents/model-agreement-for-setting-joint-investigation-team

[140] Council Resolution on a model agreement for setting up a Joint Investigation Team (JIT), see: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017G0119(01)&from=EN

[141] Regulation (EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and amending Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) No 1077/2011, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1726&from=EN

further consideration should be given to the JIT members' responsibilities regarding the data protection rules applicable to the processing of personal data.

Considering the functionalities envisaged in the JIT Collaboration Platform (communication through instant messages and video conferences, electronic sharing of information and evidence, planning and coordination of JIT operations) – a significant amount of personal data flows is expected. In this context, Directive 2016/680[142] comes into play to define the controllership for competent authorities which define, or by virtue of Union law has defined, the purposes and means of processing of the processing of the personal data.[143] Further legal consideration should be given to the possibility that the purposes and means of processing may be determined *alone* or *jointly* with other competent authorities, enabling the constitution of a *joint-controllership*.[144] In the context of a JIT formation and by virtue of the mutual agreement in which it already operates, it is reasonable to conclude that a joint-controllership would/should be established as regards to the processing of personal data in the JIT Collaboration Platform. In this case, however, it should also be considered how the platform would interact with the national system of the EU Member States, or third countries. It would thus be advisable to enact a legal basis to provide clarity on this point.

In practice, this would mean that members of a JIT are jointly responsible to ensure that:

- Personal data in the JIT Collaboration Platform is
    - lawfully processed;
    - limited to serve the purpose for which it was obtained.
- Retention periods for personal data processed in the platform are defined and enforced (e.g. duration of the JIT).
- Personal data is accurate and up-to-date.
- Personal data transfer to third countries (by virtue of the participation of a non-EU state in a JIT) is done on the basis of the relevant international instruments and with the adequate safeguards.
- The rights of the data subjects involved are duly addressed.

To this end, it is recommended to review the JIT model agreement included in annex of Council Resolution 2017/C 18/01 in order to ensure that JIT members' responsibilities for compliance with applicable data protection rules, as prescribed by Directive 2016/680[145] would be compatible with the new legal basis proposed for the platform.

Another important point to be considered in the context of the JIT Collaboration Platform is the broad conceptual spectrum of processing operations. Processing, by its legal definition, means any operation or set of operations which is performed on personal data or on sets of personal data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction or erasure.[146] It means that envisaged functionalities on the JIT Collaboration Platform – video conferences, instant messaging, file uploads and exchanges, etc.

[142] Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN

[143] Directive 2016/680, Art. 3 (8).

[144] Supra, Art. 21.

[145] Supra.

[146] Supra, Art. 3 (2).

– should be conceived as a personal data processing operation to the extent in which they are used to coordinate investigations and prosecutions. Practically, this means that all functionalities should be customised to embed core data protection principles requirements (such as storage and purpose limitation, data minimisation), as discussed in section 5.3.5, as well as to provide privacy-protective default settings to ensure the confidentiality of the data and enable accountability, while serving business needs (e.g. end-to-end encryption of communication, limited free text in forms and calendars, automatic deletion/anonymisation of conversation histories and collaboration whiteboards, auditing and logging of events, etc.).

With regard to access rights and usage of data, the choice for an EU level instrument would be helpful to uniformly arrange this matter. This can be beneficial with regard to the implementation of logging obligations, and would make it possible to have a clear regulation for all cases concerning the access of Europol and Eurojust duly authorised personnel, and how this would relate to their CMS or AWF structures.

Finally, as highlighted in the above technical assessment, with the example of Microsoft Teams, the assessment of COTS solutions should pay particular attention to the aspects of data security and privacy, as the JIT Collaboration Platform would be hosting Operational Personal Data (as defined in Regulation (EU) 2018/1725). Therefore, this report recommends to further assess the COTS solutions to determine if they are secure enough to host Operational Personal Data. To this end, it must be noted that following the latest privacy discussions between DG COMM and Microsoft about Office 365, Operational Personal Data, as defined in Regulation (EU) 2018/1725, cannot be used in the Office 365 products as Microsoft cannot ensure sufficient security levels for the processing of such data.

5.5.5 Governance

Refer to section 8.2 for an overview of the overall project governance.

In terms of strategic governance, a subgroup of the Digital Criminal Justice Expert Group would supervise the development and subsequent deployment of the solution. The subgroup would provide the necessary input form a policy perspective.

The IT implementation would be carried out by eu-LISA. In terms of governance, a Programme Management Board and an Advisory Group would be set up by the agency for the development of the solution.

Lastly, the users of the solution, being the Member States, but also the JHA agencies and EU bodies, would be involved in the IT implementation process. Consulting the users would ensure that the JIT Collaboration Platform is fully adjusted to their needs.

5.5.6 Conclusion

The JIT Collaboration Platform would be a common data-sharing platform to support JITs, particularly in terms of setting up a JIT, operational planning, communicating, sharing, storage, tracing of case related data, and post operational aspects.

The technical assessment describes three possible scenarios for the implementation of this solution: (i) re-use of OLAF's VOCU tool, (ii) off the shelf products (Wire, Zimbra, eXo, Microsoft Teams, Cisco WeBex Teams), and (iii) implementation from scratch. Based on the assessment, this report recommends to re-use a COTS product for the implementation of this solution. However, none of the vendor solutions presented can cover all the requirements for the future JIT Collaboration Platform. Therefore, the report concludes that the final solution should consist of a combination of products used together.

The security assessment highlights the need to ensure the confidentiality of data being exchanged by the stakeholders using this solution. Strong encryption algorithms should be used to encrypt data, at least in the transport layer. Besides this, the solution should also establish patch and vulnerability management processes, and should be integrated with the target architecture. As for the three different scenarios concerned, the security assessment provides some security considerations to be taken into account, but concludes that a business impact assessment as well as a risk assessment should be performed before pursuing design choices.

Concerning the legal basis of this solution, this report acknowledges that JITs rules are set out in Council Framework Decision 2002/465. The JIT Collaboration Platform could be offered by eu-LISA as a central tool, to be used by JIT members and participants. For this platform, a legal basis would be necessary, in order to provide a clear framework (including on some sensitive points such as data controllership) on the use of this tool. Besides this, the model agreement should also be adjusted in order to be aligned with the legal basis. Moreover, in case eu-LISA is confirmed as the hosting entity, its establishing Regulation must be amended accordingly.

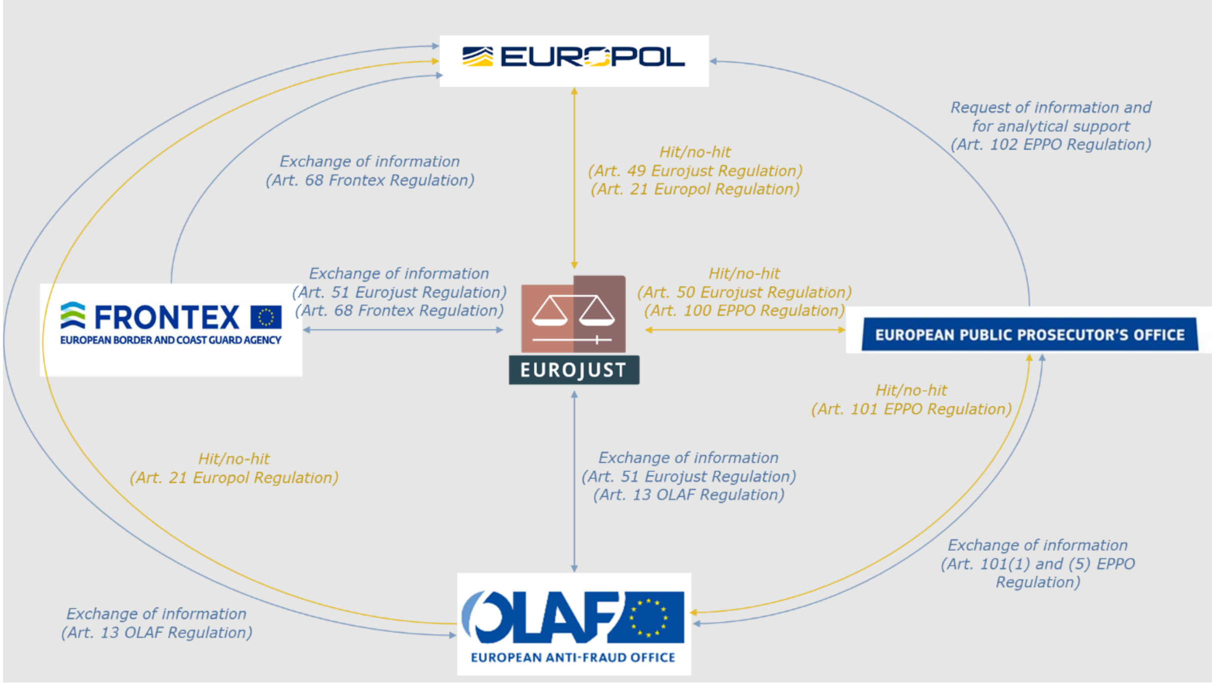
In terms of data protection, the operationalisation of an online collaborative environment to serve as single point of communication and exchange of evidence in a JIT raises relevant data protection considerations. The main point raised by the data protection assessment concerns controllership of the personal data processed in the platform. Due to the number of stakeholders involved in a JIT, the report concludes that a joint-controllership should be established with regard to the processing of personal data in the JIT Collaboration Platform. For this purpose, it is also advisable to review the JIT model agreement, in order to clearly define the JIT members' responsibilities to comply with data protection rules. A dedicated EU-level legal instrument for JITs that provides clarity on the discussion around controllership is advised.

Lastly, in terms of governance, this report recommends that this solution is driven and supervised from a strategic and policy perspective by a subgroup of the Digital Criminal Justice Expert Group. The IT implementation would be under eu-LISA's responsibility, and supported by the future users of the solution (Member States, and the JHA agencies and EU bodies).

5.6 Exchange of data between the JHA agencies and EU bodies

Cooperation and exchange of data between JHA agencies and EU bodies active in the area of judicial cooperation (the EPPO, Eurojust, Europol, Frontex, and OLAF) is key to ensuring a coordinated EU response to criminal activities and providing crucial support to Member States in tackling criminal activities.

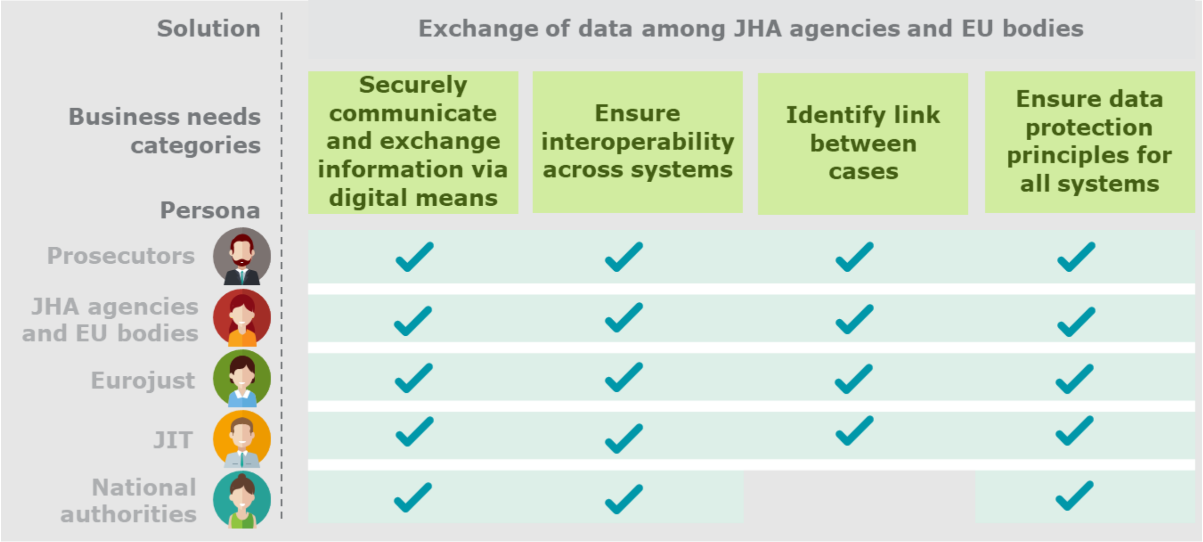
Figure 27: Cooperation links between JHA agencies and EU bodies


EUROPOL
Exchange of information (Art. 68 Frontex Regulation)
Hit/no-hit (Art. 49 Eurojust Regulation) (Art. 21 Europol Regulation)
Request of information and for analytical support (Art. 102 EPPO Regulation)
FRONTEX EUROPEAN BORDER AND COAST GUARD AGENCY
Exchange of information (Art. 51 Eurojust Regulation) (Art. 68 Frontex Regulation)
EUROJUST
Hit/no-hit (Art. 50 Eurojust Regulation) (Art. 100 EPPO Regulation)
EUROPEAN PUBLIC PROSECUTOR'S OFFICE
Hit/no-hit (Art. 101 EPPO Regulation)
Hit/no-hit (Art. 21 Europol Regulation)
Exchange of information (Art. 51 Eurojust Regulation) (Art. 13 OLAF Regulation)
Exchange of information (Art. 101(1) and (5) EPPO Regulation)
Exchange of information (Art. 13 OLAF Regulation)
OLAF EUROPEAN ANTI-FRAUD OFFICE

As shown in the figure above, the legal bases of the JHA agencies and EU bodies allow for the exchange information, requiring in some cases a hit/no-hit connection (indicated in yellow in the figure above).

This exchange of data via hit/no-hit system would allow the stakeholders to search for case-related data as displayed in the figure below.

Figure 28: Exchange of data between the JHA agencies and EU bodies - Business needs mapping



Solution	Exchange of data among JHA agencies and EU bodies			
Business needs categories / Persona	Securely communicate and exchange information via digital means	Ensure interoperability across systems	Identify link between cases	Ensure data protection principles for all systems
Prosecutors	✓	✓	✓	✓
JHA agencies and EU bodies	✓	✓	✓	✓
Eurojust	✓	✓	✓	✓
JIT	✓	✓	✓	✓
National authorities	✓	✓		✓

5.6.1 Presentation of the solution

As previously explained, the underlying legal bases of the JHA agencies and EU bodies involved in the Digital Criminal Justice ecosystem allow the exchange of information, and requires in some cases a hit/no-hit connection between some of the JHA agencies' and EU bodies' systems (see Figure 24). In addition, a follow-up to the hit/no-hit requests is required.

As indicated in Figure 27 above, there are different types of cooperation links. On the one hand, JHA agencies and EU bodies might exchange relevant information, either unilaterally or bilaterally, for the execution of their mandates. On the other hand, JHA agencies and EU bodies might exchange information on the basis of a hit/no-hit system. This implies that the agencies and bodies allow each other an indirect access to their data for the identification of links. When a hit is confirmed, a follow-up procedure is launched to share the required information.

5.6.1.1 Exchange of information

As previously identified in this report, all exchanges of information in the context of Cross-Border Digital Criminal Justice must be covered by a secure communication channel, including exchange of information and the follow-up to a hit/no-hit. Indeed, once a "hit" is discovered between the systems of two agencies, the requesting party must send a message to the requested party to confirm the hit, and request additional information needed for the case investigation.

Moreover, this report recommends e-EDES as the future Communication Tool to be used in the exchanges of information between all stakeholders involved, including relevant JHA agencies and EU bodies.

A summary of the exchange of information requirements is provided in the table below.

Table 39: Exchange of information between JHA agencies, EU bodies and EU systems

System 1	System 2	Type of exchange	Source
Eurojust	Frontex	Exchange of information (bilateral)	Art. 51 Eurojust Regulation Art. 68 Frontex Regulation[147]
Eurojust	OLAF	Exchange of information (bilateral)	Art. 51 Eurojust Regulation Art. 13 OLAF Regulation[148]
The EPPO	Europol	Exchange of information (unilateral)	Art. 102 EPPO Regulation
Europol	OLAF	Exchange of information (bilateral)	Art. 13 OLAF Regulation
Europol	Frontex	Exchange of information (unilateral)	Art. 68 Frontex Regulation
The EPPO	OLAF	Exchange of information (bilateral)	Art. 101 EPPO Regulation

[147] Regulation (EU) 2019/1896 of the European Parliament and of the Council of 13 November 2019 on the European Border and Coast Guard and repealing Regulations (EU) No 1052/2013 and (EU) 2016/1624, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R1896&from=EN

[148] Regulation (EU, EURATOM) No 883/2013 of the European parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) and repealing Regulation (EC) No 1073/1999 of the European Parliament and of the Council and Council Regulation (Euratom) No 1074/1999, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02013R0883-20170101&from=EN

5.6.1.2 Hit/no-hit

A summary of hit/no-hit requirements between JHA agencies and EU bodies is provided in the table below.

Table 40: Hit/no-hit between JHA agencies, EU bodies and EU systems

System 1	System 2	Type of exchange	Source
Eurojust	Europol	Hit/no-hit (bilateral)	Art. 49 Eurojust Regulation[149] Art. 21 Europol Regulation[150]
Eurojust	The EPPO	Hit/no-hit (bilateral)	Art. 50 Eurojust Regulation Art. 100 EPPO Regulation[151]
Eurojust	ESP (for ECRIS-TCN and SIS II)	Hit/no-hit (unilateral)	Art. 14 ECRIS-TCN Regulation[152] Art. 42 SIS II Council Decision[153]
The EPPO	OLAF	Hit/no-hit (bilateral)	Art. 101 EPPO Regulation
The EPPO	ECRIS-TCN	Hit/no-hit	Art. 14 ECRIS-TCN Regulation
Europol	ESP (for ECRIS-TCN and SIS II)	Hit/no-hit (unilateral)	Art. 14 ECRIS-TCN Regulation Art. 41 SIS II Council Decision

On top of the hit/no-hit connection, Table 40 above also refers to two EU systems: ECRIS-TCN and SIS II. These two systems would provide strategic information to the agencies and bodies (only Eurojust[154], Europol, the EPPO, and Frontex (for SIS II) are concerned) on identity information of third-country nationals who have been subject to convictions in the Member States, and alerts on persons and objects respectively. Eurojust will have access to ECRIS-TCN also for carrying out its tasks as a contact point for third countries and international organisations for the purpose of criminal proceedings (Article 17 of the ECRIS-TCN Regulation). The ECRIS-TCN system is not set up yet, it is expected to be up and running by the end of 2022. Besides this, both ECRIS-TCN and SIS II will be queried via the ESP, which will be only live in 2023. However, until the ESP is available, an interface will be required for external systems to access ECRIS-TCN and SIS II directly. It has to be noted that even when the ESP will be available, communication with Eurojust and its CMS should be established.

[149] Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0179&from=EN

[150] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0794&from=EN

[151] Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office (EPPO), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R1939&from=EN

[152] Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0816&from=EN

[153] Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32007D0533&from=EN

[154] Eurojust has access to ECRIS-TCN for the purpose of not only identifying the Member States holding criminal records on a third-country national, but also for the purpose of carrying out its tasks as a contact point for third countries and international organisations for the purpose of criminal proceedings. See Article 17 ECRIS-TCN Regulation.

Moreover, all system to system hit/no-hits described above should take place over the Secure Communication Channel to be used in the context of Cross-Border Digital Criminal Justice.

As the legal basis concerned do not provide technical specifications on the concept of the hit/no-hit access, there is a need for a common Task Force to drive a collaborative approach to define the hit/no-hit access by the JHA agencies and EU bodies mentioned above. It should be noted that Eurojust and Europol have started discussions on how to implement the hit/no-hit on their side. The Task Force could be thus built on these preliminary discussions between these two agencies. Besides the JHA agencies and EU bodies, Member States could also be involved in this Task Force as observers.

The table below presents a preliminary framework that the Task Force could use to ease and structure the discussion on the hit/no-hit concept.

Table 41: Hit/no-hit discussion framework

Issues to be discussed	Description	Framework
1. Query	List and definition of the fields to be provided when querying a JHA agency or EU body, and agreement on the mandatory fields to be provided in the request.	The request fields could be: • Biographic data of the suspect • Biographic data of the victim • Case number ID • Type of crime • Biometrics (DNA, fingerprints, eye retinas and irises, voice patterns, facial patterns, hand measurements)[155]
	Channel to be used for the hit/no-hit	JHA agencies and EU bodies should discuss which channel should be used for the hit/no-hit. Eurojust, Europol, the EPPO and Frontex should query ECRIS-TCN and SIS II via the ESP. The access to the data stored in these EU systems is clearly defined. However, it should be discussed how (i.e. via which channel) the hit/no-hit connections between the JHA agencies and EU bodies would take place. This report suggests eDelivery (with the e-CODEX connector) over TESTA to be re-used as the communication channel of choice.
2. Content and format of the response after a hit	Content and format of the response (after a hit)	The Task Force should define how (i.e. format and channel) the requesting agency or body should be informed about the outcome of its request.
3. Technical implementation	Either manual or automatic cross-checking of case information in the systems	The Task Force should define which of the two implementation models is preferred.
4. Content and format of the response after a no-hit	Content and format of the response (after a no-hit)	The Task Force should define how (i.e. format and channel) the requesting agency or body should be informed about the outcome of its request.
5. Follow-up procedure	After a hit, the requested agency or body should initiate the procedure by which the information that generated the hit may be shared	Discussion on the operational procedures to be launched by the requested JHA agency or body, e.g.: • Information to be returned. • Possible use of UMF. • Procedure to verify whether the information that triggered the hit can be shared in

[155] Biometrics data will be included in ECRIS-TCN.

		accordance with the entity that provided the information in question. • Channel and tool to be used • Deadlines to send the information that triggered the hit.
6. Possible legal amendments	Identification of possible legal amendments to accommodate the hit/no-hit concept agreed by the Task Force	Legal analysis should be conducted to assess whether changes to existing legal provisions or new legal instruments are necessary to accommodate the solution agreed by the Task Force. As previously explained, the hit/no-hit connection is not required for the exchange of information between all JHA agencies and EU bodies in their legal bases. Nevertheless, it could be agreed that a hit/no-hit system would be useful for the exchange of information. Therefore, it should be assessed to what extent an amendment is necessary to the legal bases of those JHA agencies and EU bodies, which do not require a hit/no-hit connection. This being said, it can be argued to what extent such connection could be established without a specific legal requirement in the applicable agency or body founding act. The Task Force should thus examine this issue and determine the most appropriate approach.

In terms of planning, the Task Force should be set up as soon as possible in order to start the discussion. As previously explained, the ESP will be set up in 2023. The timing of this component is key, as it will be used for the hit/no-hit connections with the EU systems ECRIS-TCN and SIS II, and (depending on the outcome of the Task Force) it could be used for the hit/no-hits between the JHA agencies and EU bodies within the Digital Criminal Justice space (taking into account the consideration pointed out in the table above). The Task Force should reach an agreement on the hit/no-hit concept as soon as possible, given the fact that there is a legal requirement for the operational exchange of data between the agencies/bodies to be established as soon as possible.

5.6.2 Technical assessment

Two scenarios can be envisaged for the technical implementation of the exchange of data and hit/no-hit between agencies:

- Option 1: cross-checking of case information in the systems manually triggered by users.
- Option 2: automatic cross-checking of case information in the databases. As this may impact the performance of the systems, it could for instance happen overnight, with results (i.e. found links) being notified to administrators and reviewed by them in the morning. It would mean that any time a new entity is included in the system of either of the two JHA agencies/EU bodies, an automatic cross-check is performed, which comes back with a hit/no-hit result. Such a solution would be much more effective than relying on the choice of an individual whether or not to make use of this facility.

A further assessment of both scenarios for the technical implementation of the exchange of data between agencies should be conducted in parallel to the discussions of hit/no-hit Task Force described above, to ensure it can be implemented as soon as possible.

5.6.3 Security assessment

Due to the nature of this solution, a security assessment is not required.

5.6.4 Legal and data protection assessment

This section provides some legal and data protection considerations on the hit/no-hit concept.

The current legal bases of Eurojust, Europol, the EPPO, and OLAF require these JHA agencies and EU bodies to allow, in some cases (i.e. to some other JHA agencies or EU bodies, see Figure 24 for a detailed overview), an indirect access to their information on the basis of a hit/no-hit system. The legal bases of Eurojust and the EPPO indicate that these two entities should have access to each other's case management systems. The same applies in relation to the EPPO and OLAF. Both entities should be informed of a hit, as well as the Member States which provided the data (unless the data came from the EPPO and OLAF own investigations). It appears that the requesting entity would receive a "yes" or "no" answer, or "hit" or "no-hit". However, the legal bases do not specify whether additional information (such as type of data) could be provided nor how the follow-up would take place. These topics are suggested to be discussed by the Task Force.

On the other hand, hit/no-hit against Europol's data seems to be more restrictive. As indicated in its Regulation, Europol should take appropriate measures to enable both Eurojust and OLAF to have indirect access to the data specified in Article 18(2) (a), (b), and (c) of the Europol Regulation[156] on the basis of a hit/no-hit. In addition, if a hit occurs, Europol (or Eurojust) should initiate the procedure to share the information that triggered the hit (in accordance with the decision of the provider of the information in question). Furthermore, it should also be noted that the information that has triggered the hit should be shared only to the extent that the data in question are necessary for the performance of the mandate of the agency or body requesting it.

The Task Force should thus take into account these different legal requirements when designing the solution to implement the hit/no-hit between the JHA agencies and EU bodies.

Besides these legal considerations, a key aspect to take into account regarding the exchange of data between JHA agencies and EU bodies is the data protection dimension.

Article 49(1) of Regulation 2018/1727 (Eurojust Regulation)[157] provides for Europol to have indirect access to information stored by Eurojust based on a hit/no-hit system. In compliance with the data quality requirement, this report recommends that Article 49(2) of the Eurojust Regulation is to be understood in a way that, in case of a hit, (i) Europol should specify which data it needs and (ii) Eurojust may share the data with Europol only to the extent that the data that generated the hit are necessary for the legitimate performance of its tasks. Equally, the obligation to log access should be implemented.

As for the hit/no-hit between the EPPO and OLAF, Article 101(5) of Regulation 2017/1939 (the EPPO Regulation) stipulates that "*The EPPO shall have indirect access to information in OLAF's case management system on the basis of a hit/no-hit system. Whenever a match is found between data entered into the case management system by the EPPO and data held by OLAF, the fact that there is a match shall be communicated to both OLAF and the EPPO. The EPPO shall take appropriate measures to enable OLAF to have access to information in its case management system on the basis of a hit/no-hit system*". In addition, the Commission proposal for the revision of Regulation (EU, Euratom) No 883/2013 Regulation (OLAF Regulation), currently under negotiations between the European Parliament and the Council, includes a similar provision.

5.6.5 Governance

Refer to section 8.2 for an overview of the overall project governance.

The European Commission would be leading this solution from a strategic governance point of view. The future solution to put in place the hit/no-hit system would be implemented by the JHA agencies and EU bodies. Lastly, Member States would be invited to be involved in the IT implementation as part of the data to be exchanged by the JHA agencies and EU bodies is coming from their systems.

[156] This article refers to personal data that may be processes for the purpose of (a) cross-checking aimed at identifying connection or other relevant links between information related to suspects, (b) analyses of a strategic or thematic nature, (c) operational analyses.

[157] Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0179&from=EN

5.6.6 Conclusion

As stated in their different legal bases, JHA agencies (Eurojust, Europol, and Frontex) and EU bodies (the EPPO, OLAF) are requested to allow the exchange of information between them (but also with EU systems, i.e. SIS II and ECRIS-TCN for both Eurojust and Europol, and the EPPO for the latter) including on the basis of a hit/no-hit system. As the legal bases concerned do not provide technical specifications on the concept of the hit/no-hit access, nor on the exchange of information following a hit, this report suggests to set up a Task Force to discuss and implement these specifications. This entity, composed of the JHA agencies and EU bodies mentioned above, together with the Member States as observers, would be mandated to drive a collaborative approach to define the hit/no-hit access and the exchange of information following a hit.

As indicated in the technical assessment, the hit/no-hit can be done either manually, i.e. triggered by users, or as an automatic cross-checking of the databases. Nevertheless, it should be noted that the legal bases of the different JHA agencies and EU bodies do not specifically indicate that the hit/no-hit refers to an automatic cross-check. Therefore, the Task Force should further examine this issue and determine the nature of the hit/no-hit.

Besides this, the Task Force should take into account the measures and requirements to ensure the hit/no-hit system and the subsequent exchange of information is compliant with the data protection principles and requirements.

In terms of governance, the European Commission (both DG JUST and DG HOME) would be driving the solution. The subsequent IT implementation would be carried out by the JHA agencies and EU bodies, supported by the Member States.

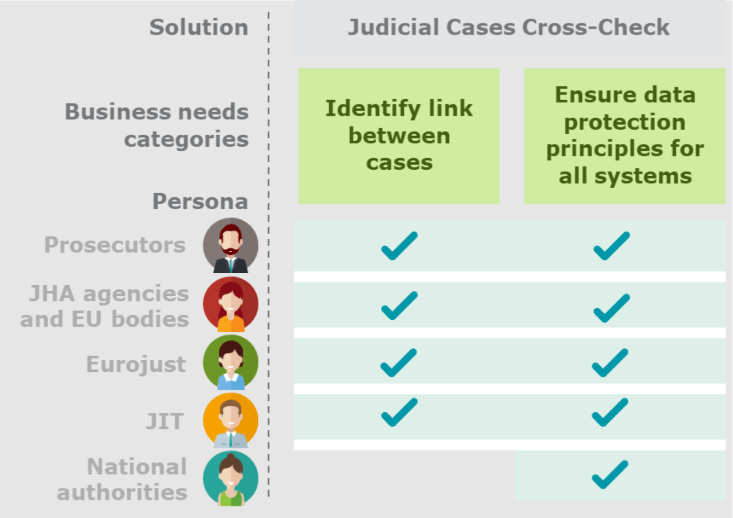
5.7 Judicial Cases Cross-Check

During interviews with EU Member States and JHA agencies, the need to be able to search for case-related information and identify links with cases being investigated in other Member States/JHA agencies and EU bodies was clearly identified.

Although this need was clearly recognized, a number of concerns were voiced during the Expert Group meeting of 13-14 January 2020:

- Some Member States are not in favour of storing information about criminal cases in a central database at EU level, and have concerns regarding potential data protection issues.
- The establishment of any kind of central database would require a legal basis.
- The ways to ensure data interoperability and possibility to store the metadata only should be examined before designing specific tools, to avoid the same data being stored in multiple systems. By doing so, information/evidence could be kept at national level and searched from abroad.

Figure 29: Judicial Cases Cross-Check- Business needs mapping



Solution	Judicial Cases Cross-Check	
Business needs categories	Identify link between cases	Ensure data protection principles for all systems
Persona		
Prosecutors	✓	✓
JHA agencies and EU bodies	✓	✓
Eurojust	✓	✓
JIT	✓	✓
National authorities		✓

Therefore, this report proposes to create a Judicial Cases Cross-Check solution, which would consist of a technical solution to be able to identify links between cases being investigated across Europe. Taking into account the concerns described above, two potential options were identified in order to implement the Judicial Cases Cross-Check:

- A decentralised solution, similar to the one developed in the context of the ADEP-EPRIS project for law enforcement.
- A central solution, the central repository of metadata.

Whereas the first option would mainly serve to identify links between cases, the second would also enable users to search for case-related information. Both options are described in further detail and assessed in the sections below.

As far as the EIF and the Sharing and re-use framework are concerned, this solution addressed the following recommendations:

Table 42: EIF and Sharing and re-use recommendations addressed by the Judicial Cases Cross-Check

European Interoperability Framework	Sharing and re-use framework
#5: Ensure internal visibility and provide external interfaces for European public services	#3: Communicate your needs
#6: Re-use and share solutions, and cooperate in the development of joint solutions when implementing European public services	#4: Define set of requirements supporting common business processes
#8: Do not impose any technological solutions on citizens, businesses and other administrations that are technology specific or disproportionate to their real needs	#10: Decide the type of rights' attribution approach to be used as early as possible and inform all involved
#9: Ensure data portability, namely that data is easily transferable between systems and applications supporting the implementation and evolution of European public services without unjustified restrictions, if legally possible	#18: Check the reusability of existing solutions before developing a new one
#12: Put in place mechanisms to involve users in analysis, design, assessment and further development of European public services	
#15: Define a common security and privacy framework and establish processes for public services to ensure secure and trustworthy data exchange between public administrations and in interactions with citizens and businesses	
#17: Simplify processes and use digital channels whenever appropriate for the delivery of European public services, to respond promptly and with high quality to users' requests and reduce the administrative burden on public administrations, businesses and citizens	
#19: Evaluate the effectiveness and efficiency of different interoperability solutions and technological options considering user needs, proportionality and balance between costs and benefits	
#30: Perceive data and information as a public asset that should be appropriately generated,	

collected, managed, shared, protected and preserved	
#36: Develop a shared infrastructure of reusable services and information sources that can be used by all public administrations	
#46: Consider the specific security and privacy requirements and identify measures for the provision of each public service according to risk management plans	

5.7.1 Presentation of the solution

The scope of these solutions is primarily to identify links between cases at Member States level, to identify any synergies/overlaps in investigations being carried out by national authorities. Once synergies/overlaps are identified, Member States could coordinate their investigations and/or exchange information in order to reduce the amount of duplicate work, identify new information and progress faster on the investigations they are conducting. This solution could also be used by JHA agencies and EU bodies involved in cross-border judicial cases (such as Eurojust and the EPPO). Although the solution serves to identify links, the follow-up communication would be done via e-EDES.

In addition, it is important to note that system-to-system searches and exchange of information between JHA agencies and EU bodies required by EU legislation (under the name of "hit/no-hit") are examined separately in section 5.6.

5.7.1.1 Decentralised solution

A decentralised solution could be based on the concept implemented by the law enforcement world, i.e. the ADEP-EPRIS system.

The necessary first step of any police investigation is to research information about a person. Usually, these searches are labour and time-consuming processes which are carried out manually and for which a large amount of requests for information sent are answered with "no information available" (in 70% of cases in France, and 80% of cases for Europol[158]). To solve this issue, in July 2017 the European Police Records Index System (ADEP-EPRIS) pilot project was launched as collaboration between law enforcement authorities of several EU Member States and funded by an EU grant of €1.5 million. The pilot partners were France, Finland, Germany, Ireland, Spain and Europol. Additional Member States acted as observers: Hungary, Belgium and Austria (temporarily).

The pilot project aimed at creating a technical system for crosschecking index databases provided by each participant, containing an extract of police records (with pseudonymised[159] biographical data such as family name, surname, any other names/aliases, date of birth, place of birth, gender).

[158] Source: Interview with the German Federal Criminal Police Office about the ADEP-EPRIS project.

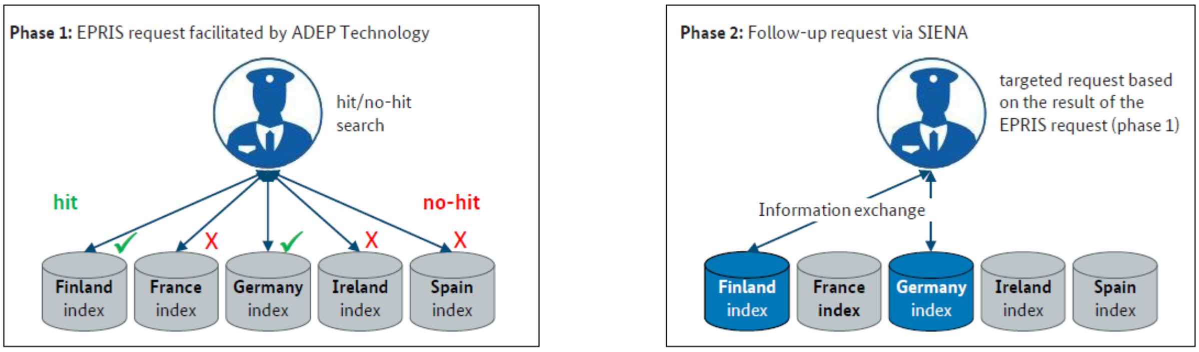
[159] Pseudonymisation refers to the process of de-associating a data subject's identity from the personal data being processed for that data subject. Typically, such a process may be performed by replacing one or more personal identifiers, i.e. pieces of information that can allow identification (such as e.g. name, email address, social security number, etc.), relating to a data subject with the so-called pseudonyms, such as a randomly

The key characteristics of the solution developed are the following:

- It is a tool to automate the search of biographic data in other Member States' police records databases.
- The tool aims at reducing the need for manual verification on the presence of data in national databases.
- In a matter of minutes, requesting Member States are automatically alerted of a hit/no-hit for searches on biographic data.
- The searches and decentralised databases are pseudonymised in a similar manner to ascertain the privacy-by-design principle.
- The validation of the hit and the follow-up messages and exchanges of information are UMF compliant and done using the SIENA application.
- Biographic data can be exchanged with Europol if deemed appropriate by the Member States.

In practice, there is an index database located in each participating Member State. Searches are initiated to target Member States resulting in the indication of a "hit" or "no-hit". In case of a hit, additional data has to be requested using Europol's SIENA application.

Figure 30: Overview of the ADEP-EPRIS solution



Each partner country in the consortium has a different definition of what a police record is, and therefore each partner must define which information would be available in its index. In each country, the index may be linked to one or several databases based on the national infrastructure. In ADEP-EPRIS, data protection is ensured by design through the pseudonymisation of both search data and data in the index. The use of this technique means that original data (behind the pseudonymised data) cannot be retrieved, even if one has the key used for pseudonymisation. A particularity of the solution is that not only exact matches are determined, but also similar results. In practical terms, this means that the requested Member State does not know whom a specific request is about. This is only disclosed in the follow-up request sent via SIENA by the requesting Member State to the receiving one.

The technical solution was developed during the 1st pilot phase (between July 2017 and December 2018) by a non-profit research institute (Fraunhofer FOKUS). The solution consists of a compilation of micro services in one package, including index, pseudonymisation, searching, matching, etc. which has been implemented by all consortium partners. There are two implementation options for

generated values. Source: European Union Agency for Network and Information Security (ENISA), Recommendations on shaping technology according to GDPR provisions - An overview on data pseudonymisation, 2018.

the solution within the project: either to build one's own software based on guidelines provided by Fraunhofer (for instance, Germany did this), or to plug-in a reference implementation in the national environment (for instance, Spain did this). As one of the objectives of the pilot was to ensure cost efficiency, the application re-uses the Europol Operations Network[160] (a secure communication network managed by Europol which runs over TESTA).

A second pilot has been recently launched, which will run until June 2021 and received a grant of €1 million from the European Commission. The aim of this second pilot is mainly to improve the accuracy of the matching functionalities of the software (currently there are many false positives). Belgium was included as a consortium partner (and Hungary as an observer), but no additional countries could be included due to the limited amount of funding available. For the future, however, two other countries have shown interest: the Netherlands and Sweden.

The current governance of the EPRIS-ADEP project involves the current consortium partners. However, during interviews it was noted that it would be more efficient if the lead for the product design would be taken up by an EU agency (potentially Europol or eu-LISA).

In the judicial world, the need for a similar solution was identified for the Region between Belgium, Netherlands and the western part of Germany: North Rhine-Westphalia. As a consequence, the Criminal Information Data Referral (CiDaR) concept was created. It was brought forward by the Bureau for Euroregional criminal cooperation (BES) active in the Meuse-Rhine and Rhine-Meuse-North Euroregions, parts of which are located in the respective regions. In that area, there is a lot of cross border criminal activity, with criminals benefiting from the fact that there are major differences between the police and judicial systems and authorities in the three countries, and that information exchange between the services that are responsible for investigation and prosecution is not as good as it should be.

Therefore, the aim of CIDaR was to solve the information gap created by the absence of a system to query information about ongoing judicial cases in different Member States (as ECRIS only provides information about final convictions). Consequently, CIDaR was conceived as a digital interface between the file recording systems of the public prosecutor's offices, which would automatically run a check on a suspect when s/he is recorded in the file recording system of a public prosecutor's office. CIDaR would then return an answer (on a hit/no-hit basis), based on the personal details of the suspect and an additional criteria (e.g. a listed act or a punishment threshold). This idea was discussed by the BES with the public prosecution services, IT experts from public prosecution services and representatives of the Ministries of Justice and Security of the different countries involved. It was deemed useful at the regional and European level (e.g. for a more efficient and effective application of Framework decision 2009/948/JHA). Moreover, a potential tool was identified to support the implementation of CIDaR: the Ma^{3}tch tool owned by the Dutch Ministry of Security and Justice, which is used by Financial Intelligence Units in Europe to exchange information. However, a legal basis on which to carry out a CIDaR test could not be identified, and therefore CIDaR was never implemented and tested. Moreover, at the time of its discussion (in 2016), there was no available or expected EU funding that could support the piloting

[160] Europol maintains a technically advanced, reliable, efficient and secure telecommunications infrastructure, in order to support its operations and deliver operational and strategic services to Member States, non-EU countries and third parties. The backbone of this infrastructure is the Europol Operations Network (EON), which connects law enforcement agencies in all Member States, as well as a growing number of non-EU countries and third parties with which Europol has cooperation agreements. The EON is a specific sub-domain of TESTA dedicated to and managed by Europol.

of CIDaR. Therefore, it was requested by the BES to their national authorities to bring this project to the attention of the European Commission.[161]

In conclusion, as demonstrated above, there is a similar use case to be solved in both the judicial and the law enforcement domains, which is to identify links between cases currently under investigation in different Member States. There are two potential options for the implementation of this solution: either to re-use the existing software developed in the context of the ADEP-EPRIS pilot, or to build another solution dedicated to the domain of criminal justice based on the concept of ADEP-EPRIS (for instance, the implementation of the CIDaR concept described above).

5.7.1.2 Central repository of metadata

This option proposes to store metadata about all ongoing criminal cases in the EU in a central repository. This would include not only cases for which cross-border cooperation is requested or ongoing, but also national cases. It is important to note that the data itself would remain stored in the local systems of its owner (i.e. Member States). In order to implement this solution, metadata would have to be automatically extracted from the national case management systems or other relevant systems (e.g. suspect name and surname, type of crime, etc.), and it would have to be confirmed and possibly enriched by the owner of the data.

The main functionalities of the central repository of metadata would be:

- Automated cross-match allowing to establish links between case metadata (also allowing for fuzzy matching).
- Automated translation of the information.
- Statistical analysis tool.

The first use case for this solution would be to allow authorised users (i.e. prosecutors, judges, judicial authorities in Member States and relevant JHA agencies and EU bodies) to search the database to identify potential ongoing investigations about cases linked to the ones they are working on. The second use case would be to allow users to search for case-related information amongst all ongoing cases at European level. Once a potential match is identified, however, the user would need to follow-up by sending a request for information to the relevant authority. Building on the vision presented earlier in this report to make e-EDES the system of choice for all communication related to cross-border cooperation on criminal justice cases, the subsequent requests and messages (once a match is identified) should be sent via the e-EDES system.

In addition, there are two implementation options for the central repository:

- **Option 1**: The central system is based on hit/no-hit, meaning that a search would only return answers such as "yes/no" or "hit/no-hit".
- **Option 2**: The central system is based on a blind search, meaning that it does not provide any reply to the requesting entity. The only outcome of a search is a notification to the owner of the data (requested entity) that another country or entity was searching for his/her information.

From a technical perspective, the development of such a solution would be based on custom development, primarily exposing the required hit/no-hit interface or blind search interface. However, the completeness of data (i.e. storing all exchanges) and the additional functionalities,

[161] Source: Bureau of Euregional criminal cooperation (BES), Criminal Information Data Referral - From an idea to a concept, 2016.

such as translation and statistical analysis should be examined when designing the solution both from a legal perspective and in agreement with all the stakeholders.

In addition, in case the central repository of metadata would be used to store EU classified metadata (instead of only non-classified metadata), it would have to undergo an EU accreditation process, and additional security measures would have to be applied (further discussed in section 5.7.3).

Finally, different possibilities to host this central component would need to be examined and discussed with Member States and JHA agencies and EU bodies involved in exchanging the data. Potential candidates for hosting could be either the European Commission, or an agency such as Eurojust and eu-LISA. Governance aspects are further discussed in section 5.7.5.

In conclusion, the options presented here are also candidate options to implement the Judicial Cases Cross-Check solution. Based on insights received from practitioners in Member States (through a survey), they seem to be plausible options. Indeed, when asked whether they would be in favour of a "Central Repository" (which differs from the present option as it would not store any information centrally, only metadata), respondents to our survey seem to be in favour of this solution. Based on the survey results, 31% of the respondents (to this question) consider a "Central Repository" as essential, and 47% as necessary. On the other hand, 8% consider this repository as slightly needed, and 2% do not think it is necessary. 12% of the respondents have no opinion in the matter. It must be noted however that the proposal to have a central repository containing a full set of data is not supported by some of the Member States, who expressed their concerns during the Expert Group Meeting of 13-14 January 2020. Their hesitations were due to data protection concerns, but more importantly to concerns regarding the confidentiality of criminal investigations and prosecutions (which include national security matters), and the risks of prejudice to the criminal proceedings involved.

5.7.2 Technical assessment

The technical assessment compares the two scenarios presented above for the implementation of the Judicial Cases Cross-Check, according to a number of business and technical criteria.

Table 43: Judicial Cases Cross-Check - Technical assessment

	Decentralised solution (ADEP-EPRIS-like)	**Central repository of metadata –** **With hit/no-hit (option 1)**	**Central repository of metadata –** **With blind search (option 2)**
Scope	**All metadata related to criminal cases** which are stored at Member State level.	**All metadata related to criminal cases** which are stored at Member State level.	**All metadata related to criminal cases** which are stored at Member State level.
EU accreditation	The national indexes would need to undergo a **national**	The solution would need to undergo an **EU accreditation process**	The solution would need to undergo an **EU accreditation process**

	accreditation process in order to store reference data about EU classified information.	in order to store metadata about EU classified information.	in order to store metadata about EU classified information.
Storage of data	All case data is **stored locally** in the databases of its owner in the MS.	**Some case metadata is stored in a central repository** at European level, and the rest is stored locally in the database of its owner in the MS.	**Some case metadata is stored in a central repository** at European level, and the rest is stored locally in the database of its owner in the MS.
Implementation complexity	**Low to medium implementation complexity, depending on the implementation option chosen** (either to re-use the software developed as part of the ADEP-EPRIS pilot project, or to build a new solution based on a similar concept).	**Medium complexity** (to be confirmed in the design phase of the system as the solution does not yet exist).	**Medium complexity** (to be confirmed in the design phase of the system as the solution does not yet exist).
Data security and data protection	**Data security and data protection** would also have to be embedded in the design and implementation of the national solution. In the case of an ADEP-EPRIS-like solution, the **pseudonymisation technique** is used to guarantee the privacy of data. The solution of the ADEP-EPRIS pilot project is designed to perform a hit/no-hit search.	• **Access right management** would ensure the security of data. • **Data security and data protection** would also have to be embedded in the design and implementation of the solution, as the central repository would contain some personal data. • The solution could be designed to perform **hit/no-hit or blind searches.**	• **Access right management** would ensure the security of data. • **Data security and data protection** would also have to be embedded in the design and implementation of the solution, as the central repository would contain some personal data. • The solution could be designed to perform **hit/no-hit or blind searches.**

Governance	The governance of an ADEP-EPRIS like solution would have to be **steered by Member States**. However, it could possibly be **coordinated by a JHA agency**.	Governance of the solution would have to be **managed at EU level** by the Commission or a JHA agency or EU body, and should **involve the Member States** (for instance, in the context of a Task Force).	Governance of the solution would have to be **managed at EU level** by the Commission or a JHA agency or EU body, and should **involve the Member States.**
Risks	The implementation and available data would **vary from Member State to Member State, as it depends on the national IT landscape**.	• **Concerns of Member States** regarding the security and privacy of the information stored in the central repository. • The central repository is a possible **single point of failure from a security perspective**.	• **Concerns of Member States** regarding the security and privacy of the information stored in the central repository. • The central repository is a possible **single point of failure from a security perspective**.

Legend: **Strength** **Weakness**

Based on the assessment presented above, the main differences between the two implementation options of the Judicial Cases Cross-Check solution concern the hosting, the governance of the solution, and the storage of data. In addition, a centralised solution presents the risk of being a single point of failure (e.g. in case of a security breach), whereas a decentralised solution might be less complex to implement as the existing software could be re-used.

Consequently, this report cannot provide a clear recommendation on the option to choose from a technical perspective. The choice between these options must be the consequence of a legal and security assessment (see sections below), and of a political agreement between EU Institutions and the Member States.

5.7.3 Security assessment

In both proposed options, the Judicial Cases Cross-Check component is in reality an indexed database, with its underlying and supporting systems and components. From the security viewpoint it is important to cover the following aspects related to database security regardless the chosen option:

1. Database Connection: applying transport layer protection (e.g., TLS) to avoid the transmission of (sensitive) data in a clear way on the communication channel (e.g. database credentials) which may lead to identity theft.
2. Database Authentication: enforcing strong authentication, including connections from the local server. Database accounts should be:
    a. Protected with strong and unique passwords.
    b. Unique and assigned to an owner.
    c. Used by a single application or service.
    d. Configured with the minimum permissions required.
3. Database Permissions: permissions assigned to database user accounts should be based on the principle of least privilege (i.e. the accounts should only have the minimal permissions required for the application to function) by defining granular levels linked to the functionalities available in the database. Depending on the criticality of the Judicial Cases Cross-Check, if considered as security-critical database, then the following permissions at more granular levels should be considered:
    a. Table-level permissions.
    b. Column-level permissions.
    c. Row-level permissions.
    d. Blocking access to the underlying tables.
    e. Requiring all access through restricted views.
4. Database configuration and hardening: the database application should also be properly configured and hardened. The following principles should apply to any database application and platform:
    a. Install any required security updates and patches – i.e. patch management.
    b. Configure the database services to run under a low privileged user account – i.e. least privilege principle.
    c. Remove any default accounts and databases – i.e. secure defaults.
    d. Store transaction logs on a separate disk to the main database files – i.e. logs isolation.
    e. Schedule a regular backup of the database and the secure configuration baseline – i.e. backup management.
    f. Ensure that the backups are protected with appropriate permissions, and ideally encrypted and isolated from operational networks – i.e. backup protection and isolation.

It is to be noted that both proposed options can achieve an acceptable security level that meets the security needs and requirements of the DCJ target architecture.

Decentralised option: It is a fairly proven approach that would work relatively well. Similarly to the decentralised Large Files Solution (see section 5.8), its distributed nature would offer a few advantages such as resiliency to failure, as it does not have a single point of failure. However, it does have a few drawbacks as it is difficult to maintain a harmonised security assurance level across all the involved participants. Security controls and measures should be duplicated in each environment and should be similarly implemented locally in each Member State, which would increase the overall implementation efforts and cost, as there are no central security capabilities that centralise security functions for the entire architecture (e.g. IAM, Logging and monitoring, etc.).

- In other words, the overall architecture can be seen as secure as the weakest point in the whole security chain. Without any centralisation aspect, data security and protection controls would vary from an environment to another, which may potentially lead to bypassing of the security rules and measures in place. A special focus should be put on ensuring the confidentiality and integrity of each indexed database in the whole ecosystem to make sure that the overall architecture is achieving the target security assurance level.

- Similarly, it is more challenging to ensure compliance with applicable regulations and standards in a decentralised ecosystem. For instance, it is technically a bit more challenging to apply GDPR principles, especially the ones related to data subject rights in decentralised databases, as opposed to the centralised option which recommends a central indexed database. However, this option makes data breaches much less costly as only partial data would be stored on a given indexed database and not the entire dataset, which is the case in the other option.
- And finally, this option raises certain data quality related concerns, for instance, how to make sure that data stored in X separated indexed databases, as well as their underlying systems, are consistent and reliable.

Centralised option: Thanks to its centralisation aspect, this option offers certain benefits such as being able to manage common security functions and the data safeguards in a centralised manner. Consequently, the security requirements and controls can be designed, implemented and enforced in a more harmonised way, in line with an overall target security assurance level. Since data resides in the same location, it is therefore easier to apply data security controls and safeguards as well as to ensure data quality, as opposed to a decentralised data storage approach.

- However, besides the fact that centralising data does not seem to be an ideal option for Member States, for privacy and accountability reasons, it is important to also stress the fact that this option suffers from a single point of failure, which means that if the storage systems supporting the central repository are down, for any reason (e.g. cyber-attack), this affects the availability of the entire dataset that is stored in the central repository. Whereas in the decentralised option, if a system supporting an indexed database is down, it only affects the data stored in this specific indexed database and not the availability of the entire dataset, data from other indexed databases can still be requested and shared.
- This means that the impact of unavailability is much higher for the centralised option than it is for the decentralised one. Therefore more strict measures have to be implemented in order to guarantee and preserve central repository availability (e.g. data clusters, redundancy, load balancing, backups, recovery planning, etc.).

In conclusion, and as previously mentioned, both options are valid candidates for achieving the desired security assurance level for Digital Criminal Justice target architecture. With some variation in terms of advantages and drawbacks, a further risk analysis and a business impact assessment would have to be conducted in order to decide which option to choose, considering the exposed risks of each option and taking into account views of the Member States.

5.7.4 Legal and data protection assessment

The Judicial Cases Cross-Check is a solution that would support mutual assistance between Member States, enabling identification of links between cases currently under investigation in different Member States. This report presents different options for this solution. The Judicial Cases Cross-check could be either designed in a centralised or a decentralised manner.

There are two implementation options for a centralised solution. On the one hand, the Judicial Cases Cross-check could be based on a hit/no-hit, implying that only "yes/no" or "hit/no-hit" answers would be returned to the searches. On the other hand, the second option would consist of a blind search, where no answer is provided to the requester, but only a notification to the owner of the data informing that the data was searched and a hit established.

In terms of legal implications, this centralised solution would require a legal basis. The Judicial Cases Cross-Check would store metadata about all ongoing criminal cases in the EU, both cross-border and national cases. Such a centralised system would clearly require a legal basis.

A standalone legal basis could be adopted, providing a detailed framework on the tool. In addition, if this legal basis designates eu-LISA as the hosting entity, the founding Regulation of the agency should be amended accordingly. The amendment to the eu-LISA Regulation would consist of introducing a new article in Chapter II Tasks of the agency, entitled "Tasks relating to Judicial Cases Cross-Check", explaining the tasks and responsibilities of the agency in relation to this solution. In any case, both legal procedures would require a certain amount of time to be set aside for the policy and legislation making process necessary for the Regulation's amendment and the new legal basis.

As for the decentralised scenario, an ADEP-EPRIS-like solution could be implemented. In this scenario, the case data would remain stored locally in the databases of its owner.

In other words, this scenario does not imply the transfer of data to any central repository (contrary to the centralised scenario). Therefore, the decentralised scenario would not require a legal basis at EU level, but at national level. However, an EU level legal instrument could be considered to ensure that all Member States provide for access to their local storage of metadata, and to define common elements on the control of that access, including the purposes for which such access would be allowed, and any other necessary safeguards.

From a data protection perspective, in the centralised solution, besides the points addressed in the legal assessment, the development of a Judicial Cases Cross-Check solution to store metadata raises mainly the following considerations:

- The automated hit/no-hit interface in the Judicial Cases Cross-Check solution should be used only and in so far as necessary to reveal potential matches. Further prescriptive or predictive analyses, including the evaluation of certain personal aspects relating to a natural person (e.g. profiling), should be deemed discriminatory and therefore unlawful.[162]
- Hit/no-hit or blind search access should be favoured against the provision of full access (i.e. all data about a case is made available to users provided they have the required access rights).[163] Indeed, in case of a hit, (i) authorised users (i.e. prosecutors, judges, judicial authorities in Member States and relevant JHA agencies and EU bodies) should specify which data they need and (ii) the authorised authority may share the data with the authorised users only to the extent that the data that generating the hit are necessary for the legitimate performance of its tasks. Equally, an obligation to log access should be included.
- The hit/no-hit capability is a personal data processing operation in itself. As such, retention periods should be considered so that the data is not kept for longer than what is needed to

[162] Regulation 2018/1725, Article 77.
[163] Following the principles of purpose limitation and data minimisation as set forth in article 4 (b) and (c) of Regulation 2018, 1725.

fulfil the purpose to which it was processed (e.g. setting up of automatic deletion of queries which do not result in matches or are pending for a certain period).[164]

5.7.5 Governance

Refer to section 8.2 for an overview of the overall project governance.

The governance of this solution would vary depending on the scenario (centralised, or decentralised) to be implemented. The decision would be reflected in the legal basis, enacted before the development of the solution. Below, this report examines the two possible governance models for the two scenarios.

In both cases, a subgroup of the Digital Criminal Justice Expert Group would supervise the development and subsequent deployment of the solution. The subgroup would provide the necessary input from a policy perspective.

The IT implementation of the centralised scenario would be under eu-LISA's responsibility. In terms of governance, a Programme Management Board and an Advisory Group would be set up by the agency for the development of the solution. On the other hand, a consortium of the Member States would be in charge of the implementation of the decentralised scenario (work could also be coordinated by a JHA agency).

Lastly, the users of the solution, being the Member States, but also Eurojust and the EPPO, would be involved in the IT implementation process.

5.7.6 Conclusion

A Judicial Cases Cross-Check system would be a solution allowing the identification of links between cases being investigated across Europe.

In terms of implementation, two solutions are possible: a decentralised (i.e. an ADEP-EPRIS like solution) and a central repository of metadata (either with hit/no-hit or blind search). Based on the technical assessment, it was found that the main differences between the options concern the hosting, the governance of the solution, as well as the storage of data. In terms of disadvantages, it was found that the centralised option entails a risk of being a single point of failure, which therefore requires additional measures to be deployed, while the decentralised one would be more complex to implement (data index to be determined by Member States and the availability of the data; the different national IT landscapes would also affect the implementation of the solution). Therefore, a clear recommendation of the option to be retained from a technical perspective cannot be provided at this stage.

This technical assessment is also confirmed from a security point of view. Both options can reach an acceptable security level. Therefore, a further risk analysis and business impact assessment would have to be conducted in order to decide which option to retain.

[164] Another suggestion would be to keep the data only as long as they are retained in the Member State system.

From a legal point of view, it was found that the two options (decentralised and centralised) are possible. On the one hand, the centralised solution would require a legal basis: the enactment of a new legal basis, and an amendment to an existing legal instrument (i.e. eu-LISA Regulation – if the agency is designated as the hosting entity). On the other hand, the decentralised solution would not imply any transfer of data to a central element, and would thus not require an EU level legal instrument as such. Nevertheless, an EU level legal instrument could be useful to ensure that all Member States provide for the access required to allow this solution to be effective, and to set common requirements in terms of that access.

As for the data protection consideration, the processing of personal data by means of cross-checking index databases via a Judicial Cases Cross-Check is deemed lawful. The solution needs to be built based on the data protection by design and by default principle. The automated hit/no-hit mechanism should only be used to reveal potential matches, while profiling would be unlawful. Retention periods should also be considered.

Lastly, in terms of governance, this report recommends that this solution is driven and supervised from a strategic perspective by a subgroup of the Digital Criminal Justice Expert Group. The IT implementation would be either under eu-LISA's responsibility (for the centralised scenario), or the Member States' (for the decentralised scenario). In both cases, the IT implementation would be supported by the future users of the solution (the Member States, Eurojust and the EPPO).

5.8 Large Files Solution

All practitioners interviewed in the context of this study universally agreed on the difficulty to exchange large amounts of information electronically with their peers, due to the limited attachment sizes authorised by their mail servers and the currently available systems.

Although the need for a solution to exchange large files was recognised, a number of concerns were voiced during the Expert Group meeting of 13-14 January 2020:

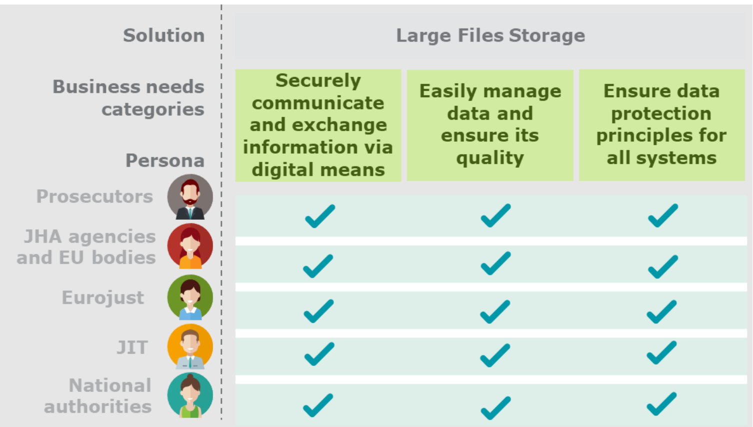
- The establishment of any kind of central database would require a legal basis.
- It is not practical to be sending (large) case files around, it would be easier to keep data in its original source and reference to it.
- The ways to ensure data interoperability and possibility to store the metadata only should be examined before designing specific tools, to avoid the same data being stored in multiple systems. By doing so, information/evidence could be kept at national level and downloaded from abroad.

This is why this report presents a solution to enable the exchange of large files, and proposes two ways to implement the solution:

- A centralised Large Files Solution inspired from the Large File Exchange solution for law enforcement.
- A decentralised Large Files Solution.

The solution would help to address several of the needs of the stakeholders in the Digital Criminal Justice ecosystem, as demonstrated in the table below.

Figure 31: Large Files Solution - Business needs mapping



Solution	Large Files Storage		
Business needs categories	Securely communicate and exchange information via digital means	Easily manage data and ensure its quality	Ensure data protection principles for all systems
Persona			
Prosecutors	✓	✓	✓
JHA agencies and EU bodies	✓	✓	✓
Eurojust	✓	✓	✓
JIT	✓	✓	✓
National authorities	✓	✓	✓

Regarding the EIF and the Sharing and re-use framework, this solution addresses the following recommendations:

Table 44: EIF and Sharing and re-use recommendations addressed by the Large Files Solution

European Interoperability Framework	**Sharing and re-use framework**
#5: Ensure internal visibility and provide external interfaces for European public services	#3: Communicate your needs
#6: Re-use and share solutions, and cooperate in the development of joint solutions when implementing European public services	#4: Define set of requirements supporting common business processes
#8: Do not impose any technological solutions on citizens, businesses and other administrations that are technology specific or disproportionate to their real needs	#10: Decide the type of rights' attribution approach to be used as early as possible and inform all involved
#9: Ensure data portability, namely that data is easily transferable between systems and applications supporting the implementation and evolution of European public services without unjustified restrictions, if legally possible	
#12: Put in place mechanisms to involve users in analysis, design, assessment and further development of European public services	
#15: Define a common security and privacy framework and establish processes for public services to ensure secure and trustworthy data exchange between public administrations and in interactions with citizens and businesses	
#17: Simplify processes and use digital channels whenever appropriate for the delivery of European public services, to respond promptly and with high quality to users' requests and reduce the administrative burden on public administrations, businesses and citizens	
#30: Perceive data and information as a public asset that should be appropriately generated, collected, managed, shared, protected and preserved	
#43: Communicate clearly the right to access and re-use open data. The legal regimes for facilitating access and re-use, such as licences,	

should be standardised as much as possible	
#46: Consider the specific security and privacy requirements and identify measures for the provision of each public service according to risk management plans	

5.8.1 Presentation of the possible solutions

The Large Files Solution would be a system to electronically exchange large volumes of information in a secure way between the different stakeholders in the Cross-Border Digital Criminal Justice ecosystem. Currently, large files are mostly exchanged in a "non-digital" way. In practice, this means that the information is collected onto a support medium (such as paper, a USB key or a hard drive) by the sending party, and transported to the receiving party by a member of staff or using postal services.

It should be underlined that other DCJ solutions, e.g. JIT Collaborative Platform and e-EDES, could benefit from the establishment of such a system.

Two options for the implementation of this solution are presented and compared in the sections below: a centralised solution and a decentralised one.

5.8.1.1 Centralised Large Files Solution

This option is inspired by the Large File Exchange (LFE) system developed by Europol, which is used by law enforcement officers in Member States. This system is used for the exchange of large volumes of unclassified information, because it is currently not possible to do so using SIENA. Because this solution is not accredited, large volumes of EU classified information are still exchanged in the law enforcement domain using mostly non digital means, examples of which are given in the introduction to this section.

LFE is based on File Transfer Protocol (FTP), which is a standard network protocol used for the transfer of computer files between a client and a server on a computer network. Therefore, in LFE files are transferred through the internet and they are double encrypted. In practice, this means that first a request is sent using SIENA from the sender to the receiver which contains the number of the file. Then, the file to be sent is uploaded into LFE. Afterwards, the receiver must collect the right file from the FTP server, and decrypt it using a password which is also sent through SIENA (in a separate communication). It is important to note that, without the SIENA message, it is impossible to upload or download any data from the FTP server.

A similar concept could be re-used to exchange large amounts of electronic evidence or information between judicial practitioners (mainly, prosecutors and investigative judges) in different Member States. The implementation of this solution would be done through the implementation of a secure File Transfer Protocol system. This is a relatively simple technical solution, which requires the use of an FTP client and server, and the definition of guidelines for its use. Moreover, similar to what is done in Europol's LFE system, this solution would need to be complemented by the use of a secure communication tool (as suggested in this report, the evolution of e-EDES) for the exchange of information and messages prior to the file being uploaded on or downloaded from the FTP server.

Regarding the exchange of EU classified information, there are also two options: either to transmit only unclassified information, or to transmit unclassified and classified information. In the former case, EU classified information would have to be exchanged either in a "non-digital" way, as done today, or via the SIENA application used in the law enforcement domain.[165] In the latter case, the Large Files Solution would need to undergo the accreditation process to be authorised to exchange EU classified information (up to level of EU CONFIDENTIAL). This would imply that the associated Secure Communication Channel, and the Communication Tool would also need to be accredited. Additional security measures would need to be defined, as discussed in section 5.8.3 below.

Moreover, the implementation of this solution would need to take into account the issues of traceability and admissibility of evidence in front of court, for instance by providing an audit trail of the handling of the files. These issues should be taken into account when designing the system.

Finally, several options must be examined for the hosting of this solution, including the European Commission, Eurojust or eu-LISA. Given the political sensibilities related to the hosting of member State data, and the mandate of eu-LISA, it is recommended to host this solution at eu-LISA.

5.8.1.2 Decentralised Large Files Solution

Technology wise, the decentralised option would work in the same way as the centralised one, i.e. using FTP. First, a request would be sent using e-EDES from the sender to the receiver, which would contain the file identification number (or a link to it), after which the file would be uploaded in the FTP-based solution to store the data. The receiver would collect the file from the FTP server (based on the identification number sent via e-EDES), and decrypt it using a password sent via a separate e-EDES message.

However, there is one important difference in the second option: the central component (the FTP server) would be replaced by national components (one per Member State) located at the Member States level. This means that Member States would upload their data to their national storage components, instead of transferring it to a central one. Then, they would send the information needed to access the file (e.g. identifier, link or password) to the receiving Member State or JHA agency or EU body using e-EDES, as described above.

5.8.2 Technical assessment

The technical assessment compares the two options presented above for the implementation of the Large Files Solution, according to a number of business and technical criteria.

	Centralised Large Files Solution	Decentralised Large Files Solution
Scope	All large information files concerning criminal cases which should be exchanged between Member States and/or JHA Agencies and EU bodies in the context of cross-border	All large information files concerning criminal cases which should be exchanged between Member States and/or JHA Agencies and EU bodies in the context of cross-border

[165] As explained in section 5.2.1.3, developments are ongoing so that in the future larger volumes of information can be exchanged via the SIENA application.

	judicial cooperation.	judicial cooperation.
EU accreditation	For the solution to be used to exchange EU classified information, it would have to undergo **an EU accreditation process**. The associated Secure Communication Channel and the Communication Tool should also be accredited end to end.	For the solution to be used to exchange EU classified information, it would have to **undergo a national accreditation process**. The associated Secure Communication Channel and the Communication Tool should also be accredited end to end.
Hosting	The solution would be **hosted at central/EU level**.	The solution would be hosted at national level.
Storage of data	Data would be **stored at central/EU level**.	Data would be stored at national level.
Implementation complexity	The technical solution, and therefore the complexity of implementation, is the same in both options.	• The technical solution, and therefore the complexity of implementation, is the same in both options. • Implementing the solution in all Member States would likely take **more time and resources** than a central implementation.
Data security and privacy	• Access right management would ensure the security of data. It would have to be ensured by each Member State/ JHA agency or EU body using the Large Files Solution, and would also be managed at EU level (for access to the communication tool). • Files uploaded on the Large Files Solution would be encrypted. However, data security and data protection would also have to be embedded in the design and implementation of the solution, for instance regarding the exchange of passwords to decrypt files.	• Access right management would ensure the security of data. It would have to be ensured by each Member State/ JHA agency or EU body using the Large Files Solution, and would also be managed at EU level (for access to the Communication Tool). • Files uploaded on the Large Files Solution would be encrypted. However, data security and data protection would also have to be embedded in the design and implementation of the solution, for instance regarding the exchange of passwords to decrypt files.
Governance	The **governance** of the solution would be done by an **EU**	The governance of the solution would be done at Member State

	Institution.	level.
Risks	- All data would be stored in a **central location**, which could potentially be a **single point of failure**. - Security and data protection measures would be managed by the EU Institution hosting the solution.	- Each Member State has control over the security and data protection measures in place to protect the data hosted in its instance of the Large Files Solution. - **The governance and maintenance of a decentralised solution could prove more complicated** (e.g. if an update is needed).

Legend: **Strength** **Weakness**

Based on the assessment presented above, the main differences between the two implementation options of the Large Files Solution concern the hosting and governance of the solution, and the storage of data. In addition, a centralised solution presents the risk of being a single point of failure (e.g. in case of a security breach), whereas a decentralised solution might be more resource consuming to implement and more complicated to govern. Other technical aspects such as the complexity to implement do not differ although implementing the solution in all Member States might take more time and resources than a central implementation.

Consequently, this report cannot provide a clear recommendation on the option to choose from a technical perspective. The choice of option must be the consequence of a legal assessment (see section 5.8.4 below), and of a political agreement between EU Institutions and the Member States.

5.8.3 Security assessment

As described in section 5.8.1, there are two ways for the set-up of the Large Files Solution, i.e. centralised and decentralised. Regardless of the chosen solution, the system would mainly consist of a secure FTP server that aims to store large volume of data, possibly including EU classified data. In fact, the differences between the two proposed options mainly concern the deployment aspects, as in the decentralised solution, every Member state has to maintain an FTP server at the national level.

The benefits of having a central data storage as opposed to a decentralised one, are well-known, it mainly improves the data quality and its related controls and simplifies the security management process, as security controls might be centralised in a similar manner. This is not possible in the decentralised option, as every Member State would have to set up and maintain a local national storage and secure it, in line with the DCJ target architecture. This last point might be a bit risky, as it would be challenging to ensure relatively harmonised security controls and requirements across all the local Large Files Solution deployments. However, it should be noted that the decentralised solution offers a better resiliency against failures.

On the other hand, a centralised solution might suffer from a single point of failure and security, if the necessary measures are not implemented (e.g. redundancy, data clusters, etc.). The centralised Large Files Solution should be deployed with controls that ensure the continuity of services provided by the solution (e.g. in case of a network or system failures). Moreover, security should be addressed at different layers (e.g. security in-depth model), avoiding the fact that if a security layer is bypassed, the entire system is compromised. Furthermore, it has to be noted that data breaches are more costly in a centralised landscape than in a decentralised one, as data are stored in a single location.

Conceptually and from a security viewpoint, both proposed solutions could again ensure an acceptable security assurance level for the target architecture. However, a further low-level risk analysis should be conducted in order to identify the best solution for the Large Files Solution, considering the compromises described above, between centralised and decentralised systems, as well as the risks associated with both proposed solutions.

Regardless of the chosen deployment scenario (i.e. centralised vs decentralised), the following considerations should be taken into account in order for a Large Files Solution, based on secure FTP server, to operate securely in the DCJ target architecture, in line with RFC2577[166] about FTP security considerations:

- Protection against well-known FTP targeting attacks (e.g*. Bounce Attack*).
- Strong access control mechanisms to avoid unauthorised access to FTP server.
- Password management ensuring FTP administrative accounts credentials are securely stored and managed.
- A strong password policy profile should be enforced on the FTP servers in production environment, to avoid brute force-based attacks leading to potential password guessing. Also, limit the number of allowed successive unsuccessful authentication attempts – e.g. after a small number of attempts (3-5), the server should close the control connection with the client.
- Confidentiality and privacy of data transmitted over FTP channels should be guaranteed by the use of a strong encryption scheme and a data transfer protocol that guarantees data confidentiality in transit (e.g. FTPS).
- Integrity of the data stored in the Large Files Solution, as well as the integrity of its underlying systems and components should be ensured by cryptographic means such as hashing to avoid unauthorised alteration of FTP data.
- Randomising FTP ports to avoid FTP ports stealing based attacks that consist of guessing the next allocated FTP port, which may allow an attack to hijack a legitimate end-user session.

Note that the following FTP features have been abused from security viewpoint, in one way or another in the past. Therefore, it is highly advisable to treat them with great care in the future Large Files Solution that would operate in the DCJ target architecture:

- Anonymous FTP: anonymous FTP refers to the ability of a client to connect to an FTP server with minimal authentication profile and gain access to only public files. Security problems arise when authorisations are badly managed – e.g. an anonymous user can read all files on the file system.
- Remote Command Execution: an optional sensitive FTP extension, "SITE EXEC", allows clients to execute arbitrary commands on the server. This feature should remain disabled unless really needed and well security hardened.

[166] For more information about FTP Security Considerations, please refer to https://tools.ietf.org/html/rfc2577.

- Debug Code: several previous security compromises related to FTP can be attributed to software that was installed with debugging features enabled.

Regardless of the chosen solution, in order for the solution to be able to support a secure exchange of EU classified information across Member States, more strict security requirements and controls would need to be defined and the final solution would need to be accredited.

5.8.4 Legal and data protection assessment

This section examines both centralised and decentralised scenario from a legal point of view.

In the **centralised scenario**, the Large Files Solution would require a legal basis, i.e. a new Regulation, for its development. This new legal basis should include legal provisions on the purpose and objectives of the tool, the users authorised to access to it, its functioning, the type of data to be exchanged and the data protection and security standards to be applied. Before the adoption of such a specific Regulation, an impact assessment would be necessary, to carefully consider the proportionality and necessity of this solution, as well as the data protection implications as explained below.

Besides this, the decision on the hosting of this centralised solution would also have legal implications. If eu-LISA is selected as the hosting entity of the Large Files Solution, an amendment to its legal basis[167] would be necessary. This amendment would mainly consist of a new article in Chapter II Tasks of the agency, entitled "Tasks relating to the Large Files Solution", explaining the duties to be performed by the agency in relation to this solution. This approach would provide a stronger legal basis as the solution would be specifically mentioned in the eu-LISA Regulation, but would also require a certain amount of time to be set aside for the policy and legislation making process necessary for the Regulation's amendment. Nevertheless, this obstacle is usually overcome by enacting the same legal instrument to set up the new system (in this case, the Large Files Solution) and amend the eu-LISA's legal basis.

The **decentralised scenario** would entail a different set of legal implications. In this case, Member States wouldn't transfer the data to a central component, but would upload the data to be exchanged to their own national Large Files Solution, and only share with the relevant recipients the necessary credentials to retrieve the data. Therefore, the decentralised scenario would not require a legal basis at EU level, but at national level.

From a data protection perspective, in the centralised scenario, besides the points addressed in section 5.8.3, the development of the Large Files Solution to store personal data (i.e. evidence) at a European level rather than in the national databases of the issuing and executing Member States, raises mainly the following considerations:

- The Large Files Solution must be designed to, by default, minimise the personal data collection to the minimum adequate, be relevant and not excessive in relation to the purposes for which they are processed.

[167] Regulation (EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and amending Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) No 1077/2011, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1726&from=EN

- Given the sensitivity of the personal data exchanged, data retention rules are considered necessary to ensure that 1) when the transferring of the electronic evidence or information is obtained, the executing authority should indicate whether it requires the evidence to be returned when no longer required by the issuing Member State; 2) the storage of personal data in the system to fulfil a transaction (exchange of evidence) is temporary and automatic deletion is deployed.
- Data security measures are considered to effectively address and mitigate the potential risks to the rights of individuals arising from the deployment of the system (e.g. end-to-end encryption). To this end, a data protection impact assessment, covering all the personal processing operations foreseen in the platform, is highly recommended.

5.8.5 Governance

Refer to section 8.2 for an overview of the overall project governance.

Similar to the previous solution (Judicial Cases Cross-Check), the governance of this solution would vary depending on the scenario (centralised, or decentralised) to be implemented. The decision would be reflected in the legal basis, enacted before the development of the solution. Below, the two possible governance models for the two scenarios are presented.

In both cases, this report suggests that a subgroup of the Digital Criminal Justice Expert Group supervises the development of the solution. The subgroup would provide the necessary input from a strategic perspective.

The IT implementation of the centralised scenario would be under eu-LISA's responsibility. In terms of governance, a Programme Management Board and an Advisory Group would be set up by the agency for the development of the solution. On the contrary, the Member States would be in charge of the implementation of the decentralised scenario.

Lastly, the users of the solution, being the Member States, the JHA agencies and EU bodies, would be involved in the IT implementation process.

5.8.6 Conclusion

The Large Files Solution would be is a system to exchange large volumes of information in a secure and digital way. In addition, other DCJ solutions, e.g. JIT Collaborative Platform and e-EDES, could benefit from it. Two options for the implementation are presented: a centralised (based on the LFE system for law enforcement by Europol) and a decentralised one. From a technical perspective, the main differences between the two implementation options of the Large Files Solution concern the hosting, governance of the solution and the storage of data. Besides this, the central option presents a disadvantage in comparison to the decentralised option since it presents the risk of being a single point of failure. However, the decentralised option would require more efforts for its implementation, and would be more complicated to govern. Therefore, a recommendation on the solution to retain cannot be provided from a technical perspective at this stage.

In terms of security, it can be concluded that both proposed options could ensure an acceptable security assurance level for the target architecture. Therefore, a further low-level risk analysis should be conducted in order to identify the best solution for the Large files Storage.

The central option would require a new legal basis, which should include legal provisions covering the purpose and objectives of this tool, the users authorised to access to it, its functioning, the type of data to be exchanged, and the data protection and security standards to be applied. Besides this, the eu-LISA Regulation would also need to be amended to specify that the agency's responsibilities in terms of hosting and maintenance of the solution. On the contrary, if the option retained is the decentralised one, a legal basis would only be required at the national level.

As for data protection measures, the solution, regardless of the option implemented, should ensure the purpose limitation principle, data minimisation, data accuracy, storage limitation, confidentiality, integrity, availability and privacy.

In terms of governance, the two options would require different models to some extent. A subgroup of the Digital Criminal Expert Group would closely follow the development of the solution, providing strategic guidance and support. In terms of IT implementation, the centralised option would be developed by eu-LISA, while the decentralised one would be in hands of the Member States. In both cases, the Member States together with the JHA agencies and EU bodies would be contributing to the IT implementation.

5.9 Additional solutions

The solutions presented in this subsection are additional solutions identified based on the business needs collected, which are not considered crucial/timely at this stage based on the input received during the DCJ Expert Group meeting. Therefore, this report only provides a description of these foreseeable solutions, without presenting an in-depth assessment as for the previously presented ones. The Common Services Platform is, however, presented more in detail to ensure the understanding of this solution.

5.9.1 Common Services Platform

While the Eurojust integration layer could take care of all exchanges between Eurojust and its external stakeholders as far as legally allowed, it would not be appropriate to use this integration layer as a "service" hub to be used by all partners in the domain of DCJ given their different roles and responsibilities. Therefore, the idea behind the Common Services Platform is to have a central hub which could be used by all parties in the domain of Digital Criminal Justice to offer "services" to other parties in the DCJ domain.

Amongst the possible functionalities of this Common Services Platform, the following can be identified:

- Authentication and authorisation: the Common Services Platform should ensure that DCJ parties can only access services or request information for which they are allowed to access.
- Routing of service requests and answers: when one of the stakeholders submits a request (e.g. a hit/no-hit request), this might result in consultation of (the systems of) several other stakeholders in the DCJ domain. It would be the responsibility of the Common Services Platform to analyse the incoming request, to redirect the request to the involved stakeholders, to collect the answers and to route the consolidated answer back to the requesting stakeholder.

- Monitor and control: when exchanging information in the context of criminal justice, it is extremely important (and often prescribed by law) to monitor and control this exchange. For this reason, the Common Services Platform would need to contain the necessary functionality allowing to follow-up on the exchange flows, to alert when something goes wrong and to provide a root cause analysis of any exchange failures.
- Message format transformation: if stakeholders exchange information, it is important they understand the same vocabulary and interpret the information in the same way. Nevertheless, each stakeholder would have their own particularities. Therefore it is important for the Common Services Platform to transform messages into a common format where necessary.

The idea behind this Common Services Platform is not new. One can recognize similar solutions being put in place by governments in the context of interoperability. Some examples are:

- The Federal Service Bus[168] (FSB) which has been set-up by the Belgian Federal Government to exchange information between governmental institutions. It allows for information to be communicated only once to the government. The information may include personal, company and government data. Governmental institutions can for example request the FSB to retrieve information about one or more (Belgian) citizens. The FSB will take care of the authorization of the requesting party, will redirect the request to the relevant authentic data sources, and will route back the answer to the requestor.
- Another example of such a communication or data exchange platform is the Visa Information System[169] (VIS) managed by eu-LISA. This platform allows stakeholders from Schengen states to exchange information on VISA applications to avoid so called VISA shopping.

5.9.1.1 Technical assessment

The same vendor solutions presented for the Eurojust Integration Layer could be used for the Common Services Platform (see section 5.4.2.5).

5.9.1.2 Security assessment

Although the Common Services platform and Eurojust Integration Layer have different business purposes and objectives, these two architecture components face the same security challenges and should therefore be equipped with more or less similar security measures and capabilities. Of course, these two components would have their own security requirements and controls in function of their risk exposure and their legal basis, nevertheless the same security concepts apply to both of them.

The security requirements explained in section 5.4.3 for the Integration Layer apply to the Common Services Platform. On top of these, the Common Service platform should have business validation rules in order to make sure that business logic remain consistent and reliable. This component should have the ability to enforce and validate business rules, at application layer, on every single message it transmits.

5.9.1.3 Legal and data protection

The Common Services Platform would require a legal instrument. The purpose of the Common Services Platform would be to act as a central hub offering “services” to all the parties in the

[168] https://dt.bosa.be/en/gegevensuitwisseling
[169] https://www.eulisa.europa.eu/Activities/Large-Scale-It-Systems/Vis

domain of Digital Criminal Justice. These "services" aim to ensure that the different parties have the necessary information at their disposal to conduct the necessary tasks within their mandate. Two scenarios could be envisaged to accommodate a legal basis for the Common Services Platform.

First, a new legal instrument would need to be adopted. Given the nature of the solution at hand, a Regulation would be necessary, to ensure its automatic and uniform implementation. The legal instrument should provide the key elements of the Common Services Platform, such as:

- Objectives of the component
- Use of the component
- Profiles for the users of the component
- Keeping of the logs
- Fall-back procedures in case of technical impossibility to use the component

The specific functionalities and technical requirements of the components can be defined at a later stage via delegated and implementing acts, if such powers are laid down in the Regulation in the first place, and in the technical specifications to be drafted for the subsequent development and implementation of the solution.

The second scenario would be to amend the Interoperability Regulation[170] and include a new legal provision on the Common Services Platform. This Regulation establishes a framework to ensure the interoperability between EU information systems in the area of justice and home affairs. The Common Services Platform would contribute to the overall interoperability in the area of judicial cooperation, as it would improve the data management architecture, ensuring the interoperability between the agencies' databases. Therefore, the Common Services Platform would complement and complete the overall interoperability landscape. Besides this, the eu-LISA establishing Regulation would need to be changed, if the agency is selected as the hosting entity.

The two scenarios would entail different implications. The first scenario refers to the enactment of a new legal instrument, which needs to be prepared, drafted, and negotiated in its entirety. On the contrary, the second option refers to an amendment of an already existing piece of legislation.

The level of details in the legal provisions might also vary from one scenario to the other. While a legal instrument fully dedicated to the Common Services Platform (first scenario), would provide room for details, the same level of granularity is not likely to be achieved via amendments (second scenario), which would consist of introducing some new legal provisions, and adjusting the Regulation where necessary.

In terms of data protection, the same rationale as in the Integration Layer (see section 5.4.4) should apply to the processing of personal data in the course of services transactions in the Common Services Platform. Considerations on the applicability of data protection rules in the set of operations deriving therefrom should be consistently in line with the Interoperability Regulation and its rules on establishing a framework for the interoperability between information systems in the

[170] Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0818&from=EN

EU domain and eu-LISA hosting systems (if eu-LISA is confirmed as the hosting entity) for the exchange of personal data.[171]

The Interoperability Regulation sets forth the controllership of each Member State authority over the personal data they enter into each relevant shared EU information system.[172] Correspondingly, the Regulation establishes eu-LISA as the data processor in respect to the personal data processed in the above mentioned systems and the responsible entity to ensure their interoperability, which includes the adoption of quality controls to automatically identify incorrect or inconsistent data submissions on the interoperability components and their related communication infrastructure.[173] Considering that the Common Services Platform should be future-proof to accommodate all relevant stakeholders of the Digital Criminal Justice ecosystem (therefore, serving a broader audience), personal data processing provisions should be aligned with the data protection rules included in the abovementioned Regulation and mainly ensure:

- The definition of responsibilities among systems owners: the Common Service Platform would require monitoring controls during operations, as it would effectively integrate all systems in the DCJ landscape. In this context, the cooperation to secure compliance with applicable data protection and data security rules, including service agreements with external providers, should be duly defined in between the competent authorities.
- Due to the sensitivity of the personal data processed in the context of Digital Criminal Justice and with respect to the core principle of personal data minimization, interoperability components and related communication infrastructure should not provide for the storage of any new personal data, with the exception of the links existing in between the involved systems. To the extent that personal data is temporarily stored during a transaction (e.g. identity confirmation files or links) automated retention periods should apply and automatic deletion should be automatically enforced.
- An access control policy should be established, documented and deployed dependent upon the need for manual verification of different identities by competent authorities when a link between data from different systems is created.
- Data processors[174] (e.g. eu-LISA), including staff of external service providers should not have access to any personal data processed in the systems and interoperable components. To the extent needed to fulfil reporting and statistics purposes under national or Union law, authorized staff of competent authorities should only have access to consult the metadata processed on the Common Service Platform (e.g. number of queries and searches conducted, which EU information system contain the linked data, etc.).
- Logs are kept of all the queries on the Common Services Platform to monitor the lawfulness of the personal data processing operations and ensure compliance with data security requirements.

5.9.1.4 Conclusion

The Common Services Platform would ensure interoperability between the components displayed in the architecture. In other words, the Common Services Platform would be a central hub, which could be used by all parties in the domain of Digital Criminal Justice offering "services" to the stakeholders of the DCJ ecosystem, i.e. Member States, JHA agencies and EU bodies.

[171] Regulation (EU) 2019/818.
[172] Supra, Article 40.
[173] Supra, Recital 48, Articles 41 and 42 (a).
[174] Within the meaning of Article 3 (12)(a) of Regulation (EU) 2018/1725.

In terms of security, this technical component could offer security services, capabilities and features. These refer to: identity and access management, protection measures, incoming/outgoing communication filtering, DDoS protection, audit, logging and monitoring, and establishing a formal software development lifecycle process for both components. On top of that, the Common Service Platform should have business validation rules in order to make sure that business logic remain consistent and reliable.

From a legal perspective, it can be concluded that the Common Services Platform would require a specific legal basis. Two options are considered, either a new legal basis or the amendment of an existing legal basis, in particular the Interoperability Regulation to include new provisions on this solution. In both cases, a legislative procedure would need to be launched.

As for data protection considerations, this solution would aim to facilitate the interoperability between and integration of systems involved in the Digital Criminal Justice landscape. This would lead to an increased number of personal data processing operations in between stakeholders. Therefore, the design of the solution should take into account the deployment, accountability and enforcement of the applicable data protection rules to ensure compliance throughout the entire personal data lifecycle, regardless of where the data resides.

5.9.2 Judicial One-Stop-Shop Portal

The Judicial One-Stop Shop Portal is envisioned as a web portal through which law enforcement officers, prosecutors, investigative judges and central authorities could securely access a range of services supporting their tasks in cross-border criminal cooperation.

The portal would serve as a central access point to the applications and tools needed by all stakeholders to perform their daily tasks related to cross-border criminal judicial cooperation.

Stakeholders from both the law enforcement and the judicial side have manifested a high interest in such a solution. According to the survey results, more than half of the respondents to the question believed that such a portal is essential (23%) or necessary (40%). 8% considered it is slightly necessary, and 2% indicated it was not necessary at all.[175]

For the implementation of this solution, there are two scenarios possible:

1. **Single UI page with redirection to tools and applications**:
This alternative would serve as a simplified implementation of a single UI page by simply re-directing the user to the underlying applications/tools sign-in page. It would include access to all solutions proposed in this report.

2. **A more sophisticated application which would act as a front-end for the stakeholders involved** offering access to:

- Single Sign-On to the different applications/tools with different access rights depending on the profile.
- A set of custom services/APIs and UI pages to all solutions proposed in this report.

[175] 27% of the respondents had no opinion in the matter.

This second implementation alternative is an attractive option that would allow stakeholders to have access to a wide range of services as explained above. Different access rights would need to be set up, in order to ensure that only duly authorised stakeholders can use the services relevant for their tasks.

As discussed in the Expert Group meeting, despite its potential added value, the implementation of this solution is not a priority for the time being. The focus should be first on the different components that would ease the cross-border cooperation (i.e. the solutions presented above), and then the set-up of the Judicial One-Stop-Shop Portal.

5.9.3 Training Platform

Judicial training is currently the main responsibility of Member States, as highlighted during the Expert Group meeting. Therefore, the EU should respect the principle of subsidiarity and complement when necessary, the existing national, regional, and local training curricula.

During the fieldwork interviews, practitioners (mainly prosecutors and judges) explained that training activities could be provided in order to support their daily tasks, especially in relation to the filling in of judicial forms pertaining to cross-border instruments. It should be noted, however, that training materials already exist, amongst others, either on the European e-Justice Portal, the SIRIUS platform[176], the EJN in criminal matters website[177] and the website of the European Judicial Training Network[178]. The main problem is therefore that information is scattered.

To address this challenge, while respecting the principle of subsidiarity, this solution aims to centralise all existing training materials in one given platform, easing its access for the stakeholders. Such a Training Platform could be hosted in different places:

- The SIRIUS platform[179] aiming to support practitioners to cope with the complexity and volume of information by providing guidelines, tools, sharing experiences. The platform also gives access to e-learning modules (available in the CEPOL platform).
- The e-Justice Portal[180], which currently provides training materials in different areas, including criminal law. The e-learning modules on judicial forms could be thus added in this section of the Portal. In addition, the Portal will soon contain a European Training Platform.
- The EJN in criminal matters website[181] could also host the training platform.

As agreed at the Expert Group meeting, a Training Platform could be useful for the centralisation of the relevant training material, and to ensure stakeholders have access to the information and are duly informed on how to use (potential new) systems and solutions. However, the solution was not considered as a priority for the time being because training materials are already available (in different places), and stakeholders are not willing to invest resources and effort in creating such a new platform.

[176] See: https://www.europol.europa.eu/activities-services/sirius-project
[177] See: https://www.ejn-crimjust.europa.eu/ejn/EJN_Home.aspx
[178] See: http://www.ejtn.eu/
[179] See: http://www.eurojust.europa.eu/Practitioners/Pages/SIRIUS.aspx#links
[180] See: https://beta.e-justice.europa.eu/?action=home&plang=en
[181] See: https://www.ejn-crimjust.europa.eu/ejn/EJN_Home.aspx

5.9.4 Extended EJN Atlas (directory)

As explained in the business needs section (see section 3), practitioners have expressed the need to have a directory in order to identify the prosecutors or investigative judges to be contacted in other Member States for cross-border criminal cooperation.

For the time being, no tool with this level of granularity exists. However, EJN in criminal matters currently provides on its website the EJN Judicial Atlas[182], which is an online platform allowing the identification of the locally competent authority that can receive the request for judicial cooperation in the different Member States. EJN is currently working to improve this tool. Although the improved version of the EJN Judicial Atlas would provide a clear explanation on where the information needs to be sent, it would not include the contact details of the stakeholder to be contacted.

The solution responding to the need mentioned above could be either a further improved version of the EJN Judicial Atlas, or a directory including not only the competent authorities, but also the contact details of individual practitioners. However, an obvious constraint identified for this type of tool is the burden placed on Member States to ensure the directory is up to date, and includes the relevant information. In this case, the platforms 'Find a lawyer'[183], 'Find a notary'[184], 'Find a bailiff'[185] could be considered as inspiration for the design of the Extended EJN Atlas although it must be noted that the data they offer do not change that often compared to the data concerning judicial cooperation in criminal matters. These platforms, although available to the general public, via the e-Justice Portal, aim to provide a comprehensive directory of professionals in these categories across Member States.

As agreed at the Expert Group meeting, this solution should be discussed with the European Commission and the EJN. On the one hand, the European Commission is building the Criminal Court Database. On the other hand, EJN aims to enhance the EJN Judicial Atlas by implementing webservices, although it is facing some budgetary constraints in this regard. Therefore, the solution is not considered a priority for the time being.

5.9.5 CEF Building Blocks

The CEF Building Blocks are not "solutions" as defined in the present study, but rather architectural assets which can be re-used in the context of the possible solutions presented in the previous sections. Therefore, in this section, we discuss the potential re-usability of the relevant Building Blocks for one or more solutions in the architecture.

The CEF Building Blocks, which are funded by the Connecting Europe Facility (CEF), aim to ensure interoperability between various IT systems and to provide reusable services. As a consequence, businesses, administrations and citizens would benefit from improved public services across the EU.

[182] See: https://www.ejn-crimjust.europa.eu/ejn/AtlasChooseCountry/EN
[183] See: https://e-justice.europa.eu/content_find_a_lawyer-334-en.do
[184] See: https://e-justice.europa.eu/content_find_a_notary-335-en.do
[185] See: http://eubailiff.eu/fab-2-project/

To facilitate this, the European Commission provides a Core Service Platform per building block consisting of the following layers:

- A layer of technical specifications and standards.
- A layer of sample software in order to facilitate the implementation of any technical specification or standard.
- A layer of services such as conformance testing in order to facilitate the adoption of any technical specification or standard.

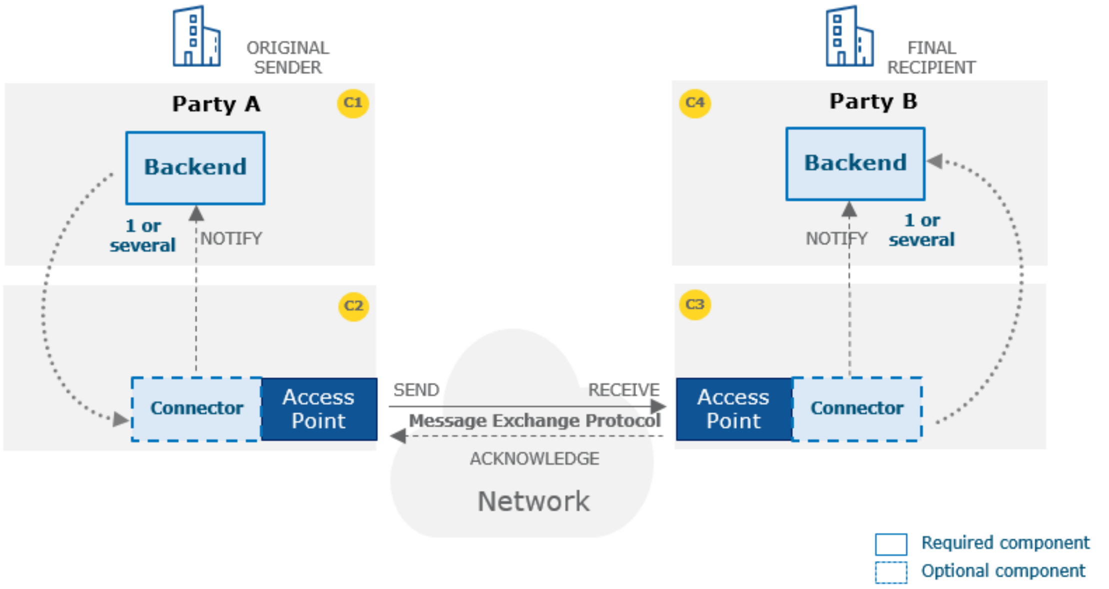
5.9.5.1 eDelivery

The option to exchange information with the eDelivery Building Block is analysed under section 5.2. This section provides an overview of the Building Block and high level technical information for its implementation.

The eDelivery Building Block serves as a means for the exchange of messages and information. The system for this Building Block is based on the 4-corner model. Regarding the 4-corner model, when a country wants to exchange messages with another country this exchange is not happening directly, instead it has to pass over the national deployments of eDelivery access points. In more detail, the following 4 steps take place:

- The sender (Party A) wants to send a message to the receiver (Party B). This means that the back-end system of country A sends a message to the access point of country A.
- This access point validates-signs-encrypts the message and using the AS4 protocol sends the message by contacting the relevant eDelivery access point of country B. This communication also takes place over a TLS encrypted channel.
- Access point B receives-decrypts-verifies the message as well as it decompresses and validates the original message while it acknowledges receipt to access point A.
- Access point B delivers an acknowledgment message to the back-end system of the receiver (Party B).

Figure 32: eDelivery integration approach



Source: DIGIT

The following elements are used by the communication infrastructure:

- An eDelivery access point (e.g. the Domibus provided free of charge by the Commission) and optional plugin/connector (e.g. the e-CODEX ASiC Domibus Connector, handling encryption, signing and timestamping).
- Domibus Connector client, handling PDF or XML files.

eDelivery makes use of a messaging protocol, the Applicability Statement 4 (AS4), which is used for secure and reliable data and document exchange. The present protocol contains some well-known web-services specifications, such as WS-Security and Simple Object Access Protocol (SOAP).

One of the main advantages of the eDelivery is the Dynamic Service Location. It enables the sending access point to dynamically discover the IP address and capabilities of the receiving access point. Instead of looking at a static list of IP addresses, the sender consults a Service Metadata Publisher (SMP) where information about every participant in the data exchange network is kept up to date. As at any point in time there can be several SMPs, every participant must be given a unique ID that must be published by the Service Metadata Locator (SML) on the network’s Domain Name System (DNS). By knowing this URL, the sender is able to dynamically locate the right SMP and therefore the right receiver.

The possible re-usability of this building block in the context of Cross-border Digital Criminal Justice is high. The level of digital maturity at the Member States in the judicial co-operation outside the e-EDES project is not uniform. Throughout interviews and identification of the business needs, system-to-system communication with the JHA agencies/EU bodies is not a short-term reality. The preferred solution would focus on secure mail exchange and the possibility of an extraction tool at the level of the Member States in the view of the adoption of the UMF. However, given the availability of a Domibus gateway instance in all Member States, eDelivery could be re-used as a long-term solution for exchange of not only structured, but also unstructured information between the Member States and JHA agencies/EU bodies.

5.9.5.2 eSignature

The eSignature software Building Block accelerates the creation, as well as the verification of electronic signatures used by other parties in the European Union, and guarantees their authenticity. The purpose of electronic signatures is to replace hand written ones. Indeed, out of the three types of electronic signatures (Simple-Advanced-Qualified), only the Qualified one is clearly recognized to have the legal value of a hand written signature in all over the European Union.

The functionality of the CEF eSignature, of which the Building Block is free to use and interoperable with all MS, is presented below:

- First, the party, which creates and sends the signature, needs a Digital Signature Service (DSS). This service will create and validate the signature per se. Moreover, an electronic signature creation device is required for qualified signatures.
- Secondly, the side that receives the electronically signed document needs a Digital Signature Service (DSS) in order to validate it as well.
- Finally yet importantly, the receiving party, except from the DSS, needs a Trusted List manager. This automated machine includes a readable list of trusted signatures as well as with ID schemas. Moreover, the automated machine is able to access trusted lists with EU schemes, defined by eIDAS Regulation.

The possible re-usability of this building block in the context of Cross-border Digital Criminal Justice is medium. The eSignature block may be used in the Redesigned Eurojust CMS and at national level for judicial authorities to operationally use trusted documents. There is no strong identified need for a common solution on electronic signatures. However, this block can be used in the context of the JIT Collaboration Platform.

5.9.5.3 eTranslation

CEF eTranslation Building Block is based on the Commission's earlier machine translation service, MT@EC, which was developed by DG Translation under the ISA Programme.[186]

The eTranslation Building Block is used to exchange information across language barriers inside the European Union. It can be used either as stand-alone service or as integrated in any other digital service, where both services are free to use. In addition, it provides capabilities equal to machine translation. These capabilities allow any infrastructure of a digital service to be multilingual.

When a CEF eTranslation acts as a stand-alone service, then its functions are as follows:

- A person registers with the EU login.
- S/he logs in to the translation service.
- S/he submits the relevant document that needs translation.
- The translated document is stored on his/her space or it can be sent to his/her email.

When a CEF eTranslation acts as integrated service, then its functions are as follows:

- An online digital system X is provided.

[186] For more information, please see: https://ec.europa.eu/isa2/isa2_en

- The online system X connects to the eTranslation service by an API.
- The API translates the content into the user's desired language.

The possible re-usability of this building block in the context of Cross-border Digital Criminal Justice is high. The identified business need is for a facility to securely upload files for machine translation in order to create summary of cases (unofficial translation). It can be used to upload files via a human user interface or integrate service calls directly via a system. eTranslation has a great potential for inclusion and excels against commercial solutions.[187]

The building block eTranslation could be re-used for the Redesigned Eurojust CMS, JIT Collaboration Platform, e-EDES and Judicial Cases Cross-Check.

5.9.5.4 Comparative view

The table below provides a comparative view of the three building blocks.

Table 45: Comparative view of the CEF building blocks

	eDelivery	eSignature	eTranslation
Purpose	Secure and encrypted asynchronous message exchange of electronic data and documents.	Creation and validation of electronic signatures.	Automated machine translation in all EU languages.
Features	Secure and encrypted message exchange. Asynchronous communication. Authentication of sender and receiver. Support for files up to 2GB and support for larger files in the future via a "split & join" function.	No printing, faxing and scanning of documents needed. Security of identification.	Understand specific EU policy and legal terminology. In all 24 official EU languages. Automatic language detection.
Utilising	AS4 4-Coner Model	eIDAS Regulation Digital Signature Service Trusted List Manager	Standalone translation application. Integrated translation application.
Availability as a service (by DIGIT)	EU Send	EU Sign	Not available
Re-usability for DCJ	**HIGH**	**MEDIUM**	**HIGH**

[187] See: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/2019/10/17/eTranslation+excels+at+WMT+2019%3A+amongst+top+ranking+engines+with+over+150+other+machine+translation+systems

6 Cost estimation

This section provides the cost estimation for the solutions.

The section provides an estimation of the Total Cost of Ownership (over 5 years) associated with the implementation of the solutions proposed in this report, namely (1) the Secure Communication Channel, (2) the Communication Tool, (3) the Redesigned Eurojust CMS, (4) the JIT Collaboration Platform, (5) the exchange of data between the JHA Agencies and EU Bodies, (6) the Judicial Cases Cross-Check, and (7) the Large Files Solution. For a detailed view of the model and estimations, please refer to the detailed cost model in Annex F.

The Total Cost of Ownership (as represented in Figure 33) is composed of:

- **Build costs** – one-off investment costs, such as costs for design, development, testing, deployment data migration (where required), practical adoption (process and hardware costs related to EU accreditation, etc.).
- **Operation & Maintenance Costs** – recurring costs for the operation of the system, such as costs for maintenance, operation, etc.

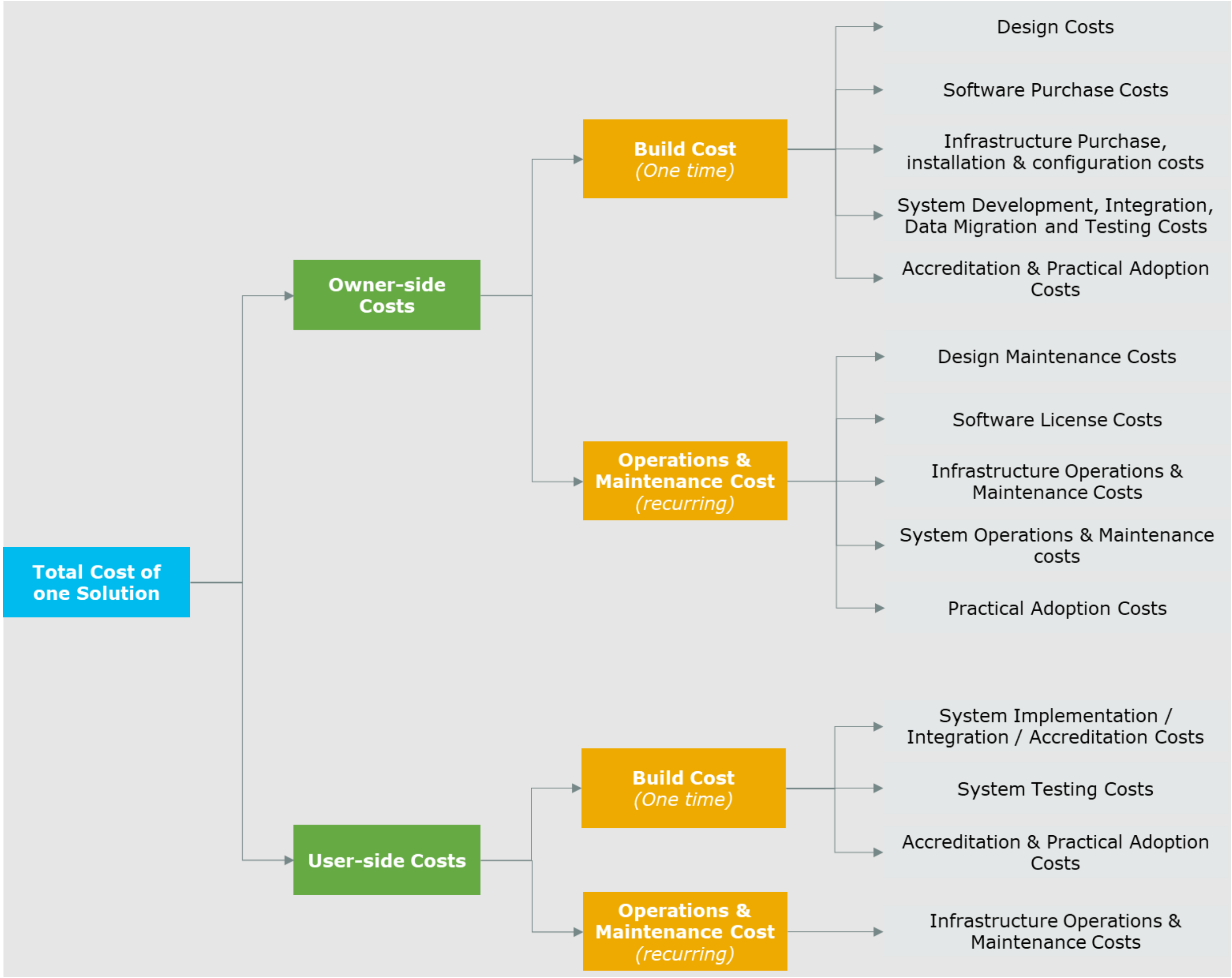
Moreover, the costs are broken down into Owner and User costs, where for each solution:

- The **Owner** is the entity (i.e. Member State, JHA Agency or EU Body) that will be responsible for implementing, hosting and managing the solution. As such, **owner-side costs** include the cost related to design, development, testing, deployment, and operations & maintenance borne by the owner.
- The User is any entity making use of the solution in its daily work. As such, **user-side costs** are calculated 'per' user-entity (i.e. Member State, JHA Agency or EU Body), and include development efforts required to build the user-facing modules of the centralised solution(s) and ensure secured connectivity with it, as well as costs related to the operations & maintenance of the solution.

An estimation of the Total Cost of Ownership for all solutions is presented in section 6.2, and an estimation of the cost per solution is presented in section 6.3.

Finally, an assessment of these estimations must take into account the assumptions and limitations outlined in section 6.2.

Figure 33: Breakdown of the Total Cost of Ownership (TCO)


Total Cost of one Solution
Owner-side Costs
Build Cost (One time)
Design Costs
Software Purchase Costs
Infrastructure Purchase, installation & configuration costs
System Development, Integration, Data Migration and Testing Costs
Accreditation & Practical Adoption Costs
Operations & Maintenance Cost (recurring)
Design Maintenance Costs
Software License Costs
Infrastructure Operations & Maintenance Costs
System Operations & Maintenance costs
Practical Adoption Costs
User-side Costs
Build Cost (One time)
System Implementation / Integration / Accreditation Costs
System Testing Costs
Accreditation & Practical Adoption Costs
Operations & Maintenance Cost (recurring)
Infrastructure Operations & Maintenance Costs

6.1 Assumptions and limitations

This section presents the most important assumptions and limitations used to build the cost estimations presented below. For detailed and solution-specific assumptions, please refer to the detailed cost model in in Annex F |.

6.1.1 Assumptions and limitations related to the approach to the model

- The Total Cost of Ownership is calculated over 5 years.
- For individual solutions, the duration of development (and associated 'Build' costs) is assumed to be 1 year (12 months) and the recurring Operations & Maintenance ('O&M') costs have been calculated for the following 4 years.
- The User – Build costs as well as User – Operations & Maintenance costs are for a single user-entity (i.e. Member State or JHA agency or EU body). The 'Total Cost' of the entire solution therefore takes into consideration all user-entities (27 Member States and 5 JHA agencies and EU bodies), and has been calculated as follows (also see the figure above):

Total Cost of complete solution = Owner Build Cost (all solutions) + Owner O&M cost (all solutions) + User Build Cost (all user entities, all solutions) + User O&M cost (all user entities, all solutions)

6.1.2 Assumptions and limitations related to the solutions

- The model focuses on a detailed assessment of a package of solution implementations (i.e. choosing one option for the implementation of each solution), which was chosen based on the assessments provided in section 5. However, because an alternative implementation may be pursued following the close of the present study, an assessment of the cost of the alternative implementation options for each solution is provided (taking as a basis the cost of the recommended option).
- All estimations concerning license prices for on-premise commercial off-the-shelf (COTS) product offerings, as well as estimations of effort for configuration and custom development are based on inputs from subject-matter experts at Deloitte.
- The cost estimation does not take into account additional cost on the user side (i.e. Member States or JHA agencies/bodies) to ensure secure connectivity to DCJ solutions or adapt their own systems where needed. This is because these costs depend largely on the individual specificities of each Member State/JHA agency or EU body in terms of systems, network, etc., and these specificities should be the object of an assessment in a further study.
- Similarly, adaptation preparation costs for Member States are not included.
- Secure Communication Channel:
    - The detailed cost estimation was made for the following scenario: eDelivery (with e-CODEX connector) over the TESTA EuroDomain. Although this report envisages that several secure communication channels could be used in the context of Cross-Border Digital Criminal Justice, in the cost model it is assumed that all stakeholders use e-Delivery (with the e-CODEX connector) over TESTA EuroDomain. This is because it is impossible to know at this stage which scenario will be chosen by each user.
    - The cost estimation does not take into account the additional bandwidth that might be required for TESTA EuroDomain in the future because of the additional information exchanged, the additional cost of which could be borne by stakeholders in the Cross-Border Digital Criminal Justice ecosystem.
    - Likewise, the costs of maintaining the national communication network are not taken into account.
- Communication Tool:
    - The cost estimation is made for the following scenario: evolution of the e-Evidence Digital Exchange System (e-EDES).
- Redesigned Eurojust CMS:
    - The detailed cost estimation is made for the following scenario: purchase and customisation of a COTS product.
    - The model assumes that the solution will be accessed by users through a web interface because (1) security measures (e.g. secure/multi-factor authentication) are easier to apply, and (2) no integration with the back-end systems of the Member States/JHA agency or EU body is required. As a result, there wouldn’t be any User-side O&M cost.
- JIT Collaboration Platform

  - The detailed cost estimation was made for the following scenario: purchase and customisation of a COTS product.
  - The model assumes that the solution will be accessed by users through a web interface because of (1) security measures (e.g. secure/multi-factor authentication) are easier to apply, and (2) no integration with the back-end systems of the Member States/JHA agency or EU body is required. As a result, there wouldn't be any User-side O&M cost.
- Exchange of data between the JHA agencies & EU bodies:
  - As this solution consists of the setting up of a taskforce, and is not supported by any technical solution, the costs associated to it are only those of the taskforce meetings.
  - The costs for JHA agencies and EU bodies to implement hit/no-hit is not included in the model, as it will be done after the Task Force (i.e. the solution presented in this report) has concluded its work.
- Judicial Cases Cross-Check
  - The detailed cost estimation was made for the following scenario: Centralised repository of metadata.
  - The model assumes that the solution will be accessed by users through a web interface because of (1) security measures (e.g. secure/multi-factor authentication) are easier to apply, and (2) no integration with the back-end systems of the Member States/JHA agency or EU body is required. As a result, there wouldn't be any User-side O&M cost. This means that metadata would have to be provided by Member States to the solution via the web interface.
- Large Files Solution
  - The detailed cost estimation was made for the following scenario: Centralised Large Files Solution.
  - The model assumes that the solution will be accessed by users through a web interface because of (1) security measures (e.g. secure/multi-factor authentication) are easier to apply, and (2) no integration with the back-end systems of the Member States/JHA agency or EU body is required. As a result, there wouldn't be any User-side O&M cost.

6.1.3 Assumptions and limitations related to the infrastructure

- Two options are provided in the report, and in Table 49 below:
  - Either all the solutions can be hosted in the already existing data centres of the stakeholders' part of the Cross-Border Digital Criminal Justice landscape (e.g. the Eurojust or the eu-LISA data centres).
  - Or a new data centre has to be built. The cost model also provides an estimate of the cost to build a new data centre, details of which are available in the 'Infra Assumptions' worksheet of the Detailed Cost Assessment (see in Annex F).
- We assume that the data centre maintenance costs would be the same, whichever data centre is used to host the solution.
- For the new data centre, the total infrastructure one-time cost and the yearly operations and maintenance cost of the datacentre has been distributed across different solutions based on their assumed size and complexity.

6.1.4 Assumptions and limitations related to security

- The model includes a high level estimation encompassing all costs related to the accreditation of systems, both on the user's side and on the owner's side.
- This cost includes all the processes required to get a system accredited with security requirements approved by a Security Accreditation Board as well as the implementation of those requirements. It also includes the 'hardware' costs (e.g. for approved cryptographic equipment), as well as security testing costs.
- For the Redesigned Eurojust CMS, the JIT Collaboration Platform, the Judicial Cases Cross-Check and the Large Files Solution, the assumption is that end-users (both internal and/or external) would access the system through a web-portal, thereby requiring no separate installation of software or configuration of hardware at user-end. Thus all development and security accreditation costs are only at owner-side, with the expectation of testing costs at user-end.

6.1.5 Assumptions and limitations related to training

- The training costs are based on the estimated number of users to be trained at the owner and user side of each individual solution.
  - On the owner side:
    - Training will be provided for both the 'business' users (who will receive training related to using the different functionalities of the solution) as well as the 'IT admin' users of the solutions (who will receive training related to the configuration of the solution).
    - This includes both classroom-based training and e-learning for all types of users.
    - Recurring training only includes e-learning.
  - On the user side:
    - Training will be provided for both the 'business' users (who will receive training related to using the different functionalities of the solution) as well as the 'IT admin' users of the solutions (who will receive training related to the configuration of the solution, e.g. to integrate it with the Member State's or the JHA agency/EU body's systems).
    - Only e-learning is provided, for all types of users.
- Both classroom-based training as well as online training have been considered to arrive at the final training cost.
- Third states (e.g. such as those which have a liaison prosecutor at Eurojust) may have access to the Redesigned CMS. For the JIT Collaboration Platform, access by third states is on an ad hoc basis, and therefore not accounted for in the model.
- The number of users to be trained was assumed to be as follows:

Table 46: Cost model - training assumptions

Solution	Secure Communication Channel	Communication Tool	Redesigned Eurojust CMS	JIT Collaboration Platform	Judicial Cases Cross-Check	Large Files Solution

Average number of users at Owner-side (internal users, incl. IT Admins)	3	3	130	3	3	3
Average number of Business users at User-side (per User entity)	100	100	10	15	100	10
Average number of IT Admin users at User-side (per User entity)	10	2	0	0	0	0
Average number of User entities	32	32	35	28	27	32

For a description of the owner(s) and user(s) of each solution, please refer to Table 48 below.

6.2 Total Cost of Ownership

This section provides an overview of the estimated Total Cost of Ownership (TCO) of all the solutions proposed in this report, for both the owner and the users of the solutions. The TCO includes the costs related to the solutions themselves (which are further detailed in section 6.3), as well as additional costs such as the cost of building a new data centre, project management costs, training costs etc. As the cost of building a new data centre is the most important one, Table 47 presents the TCO for all solutions with and without the building of a new data centre. In the first case, we assume that all new solutions implemented in the context of Cross-Border Digital Criminal Justice will be hosted in the existing data centres of institutions that are part of this ecosystem (e.g. the European Commission, Eurojust, eu-LISA, etc.). Under this assumption, the TCO of all solutions is approximately € 201 million. In the second case, we assume that a new data centre will be built to host (at least partially) the solutions presented in this report. Under this assumption, the TCO of all solutions is approximately € 233 million. It is important to note that a **25% error margin** should be applied to these estimations.

Table 47: Total Cost of Ownership of all solutions, with and without a new data centre

Phase	Year	Cost estimate	Minimum	Maximum
Build (all solutions)	1	150,103,860 €	112,577,895 €	187,629,825 €
Build (new data centre)	1	32,420,000 €	24,315,000 €	40,525,000 €
Operation & Maintenance	2	12,785,253 €	9,588,939 €	15,981,566 €
	3	12,785,253 €	9,588,939 €	15,981,566 €
	4	12,785,253 €	9,588,939 €	15,981,566 €
	5	12,785,253 €	9,588,939 €	15,981,566 €
Total (without new data centre)		**201,244,870 €**	**150,933,653 €**	**251,556,088 €**
Total (with new data centre)		**233,664,870 €**	**175,248,653 €**	**292,081,088 €**

6.3 Estimated costs per solution

This section provides a high level estimation of the costs to build and maintain, from a technical perspective, each of the solutions presented and assessed in the previous sections of this report. The estimated costs of the implementation of each solution (for the chosen implementation option) are detailed in the detailed cost model (in Annex F). The estimated costs of the alternative implementation options are based on an estimation of the variation in costs that would be incurred with regards to the retained options.

The table below presents the Total Cost of Ownership for each solution, split between the owner and users of the solution. This includes the costs to build the solution and to operate and maintain it for 4 years, as well as additional costs such as costs related to training, project management, etc.

Concretely, for each solution, Table 48 provides the following information:

- For chosen implementation option – Total Cost of Ownership (TCO) for owners and users.
- For chosen implementation option – Costs to be borne by the owner of the solution (first to build, then to operate and maintain the solution).
- For chosen implementation option – Costs to be borne by the users of the solution (first to build, then to operate and maintain the solution).
- For alternative implementation options – Impact on Total Cost of Ownership (TCO) of alternative implementation options

Also, the user costs presented below are the costs **for each user**, they must be **multiplied by the total number of user-entities (32 entities, including 27 Member States and 5 JHA agencies and EU bodies[188]) in order to arrive to the TCO**.

Finally, a **25% error margin** must be applied to these estimations, and these costs do not include the costs to build a new data centre (which are included above).

[188] Eurojust, the EPPO, Europol, Frontex and OLAF

Table 48: Estimated costs per solution

Solution	**Option**	**TCO for owners and users** (for chosen solution) **/ Impact on costs** (for alternative solution)	**Owner**	**Owner – Build costs** (for 1 year)	**Owner – Operations & maintenance costs** (for 4 years)	**Users**	**User – Build costs** (for 1 year)	**User – Operations & maintenance costs** (for 4 years)
Secure Communication Channel	eDelivery (with e-CODEX connector) over the TESTA EuroDomain	47 207 505 €	The European Commission (DG JUST)	1 562 334 €	1 589 571 €	Judicial authorities & prosecutors in EU Member States JHA Agencies & EU Bodies (Eurojust, the EPPO, Europol, Frontex, OLAF)	1 353 638 €	23 100 €
	Alternative: eDelivery (with e-CODEX connector) over the internet	*-70 %*	*The costs will be lower, as e-CODEX will be implemented (over the internet) in all Member States by 2021 under the e-Evidence related projects. Therefore, only the JHA Agencies & EU bodies will be required to implement it in order for it to be reusable in the context of Cross-Border Digital Criminal Justice, and Member States will only be required to accredit their e-CODEX implementation to exchange EU classified information.* *The impact was calculated by removing the costs to implement e-CODEX (i.e. build costs) for Member States.*					
	Alternative: eDelivery (with another connector) over the internet	*-60 %*	*The costs will be lower, as the e-CODEX technical infrastructure (i.e. the eDelivery access point) will already be implemented (over the internet) in all Member States by 2021 under the e-Evidence related projects. Therefore, only the JHA Agencies & EU bodies will be required to implement an eDelivery access point. However, additional costs may be required for the implementation and accreditation of a different connector (either a commercial product, or a custom-made one).* *To calculate the impact, we assumed an additional 10% of costs would be needed to implement another connector, compared to the previous option (eDelivery (with e-CODEX connector) over the internet).*					

Solution	**Option**	**TCO for owners and users** (for chosen solution) **/ Impact on costs** (for alternative solution)	**Owner**	**Owner – Build costs** (for 1 year)	**Owner – Operations & maintenance costs** (for 4 years)	**Users**	**User – Build costs** (for 1 year)	**User – Operations & maintenance costs** (for 4 years)
	Alternative: eDelivery (with another connector) over the TESTA EuroDomain	*+10 %*	*The costs will be similar, as the main costs associated with this solution are costs for the configuration and accreditation of e-CODEX. With this alternative, these costs would be replaced by those incurred to configure and accredit another connector.* *To calculate the impact, we assumed an additional 10% of costs would be needed to implement another connector than e-CODEX, compared to the recommended option (eDelivery (with e-CODEX connector) over the TESTA EuroDomain).*					
	Alternative: TESTA (EuroDomain or dedicated domain)	*Reusing EuroDomain: -100 %* *For reusing or operating a new dedicated domain: depends on arrangement with owner of existing dedicated domain*	*The existing default connection of each Member State as well as JHA Agencies & EU bodies to the TESTA EuroDomain is already covered by the Union budget (under the assumptions on potential changes in the costs of the TESTA EuroDomain taken in section 6.1).* *To re-use an existing dedicated domain, the costs would depend on the financial arrangement with the owner of that domain. To operate a dedicated domain, the costs would be much higher. As an example, it currently costs eu-LISA € 1,045 Mio/month to run TESTA-ng (for the VIS/SIS TESTA-ng network combined).*					
	Alternative: SIENA	*Depends on national network*	*The costs of this would depend largely on the ability to connect judicial authorities in Member States to the SIENA national unit already installed by Europol. These costs would vary from Member State to Member State, depending on the national IT landscape.*					
Communication Tool	Evolution of e-EDES	51 341 228 €	The European Commission (or eu-LISA)	4 069 687 €	3 172 885 €	Judicial authorities & prosecutors in EU Member	1 354 983 €	23 100 €

Solution	**Option**	**TCO for owners and users** (for chosen solution) **/ Impact on costs** (for alternative solution)	**Owner**	**Owner – Build costs** (for 1 year)	**Owner – Operations & maintenance costs** (for 4 years)	**Users**	**User – Build costs** (for 1 year)	**User – Operations & maintenance costs** (for 4 years)
						States JHA Agencies & EU Bodies (Eurojust, the EPPO, Europol, Frontex, OLAF)		
Redesigned Eurojust CMS	COTS product	51 895 430 €	Eurojust	17 601 629 €	21 560 801 €	Eurojust National Desks and Eurojust staff Judicial authorities & prosecutors in EU Member States (external users that may access the CMS)	282 406 €	115 500 €
	Alternative: Case@EC	*Similar cost*	*The Case@EC solution would need to be configured and customised heavily to suit the requirements of Eurojust, similar to a commercial solution.*					
JIT Collaboration Platform	COTS product	20 777 574 €	eu-LISA	5 328 440 €	5 901 135 €	JIT members	182 875 €	115 500 €
	Alternative: Re-use of OLAF's VOCU tool	*+25 %*	*The OLAF VOCU tool as it is today could be re-used at low cost, but would need to be customized heavily to suit the needs of JITs. We assume an additional 25% in costs to do so.*					

Solution	**Option**	**TCO for owners and users** (for chosen solution) **/ Impact on costs** (for alternative solution)	**Owner**	**Owner – Build costs** (for 1 year)	**Owner – Operations & maintenance costs** (for 4 years)	**Users**	**User – Build costs** (for 1 year)	**User – Operations & maintenance costs** (for 4 years)
	Alternative: Custom implementation	*+100 %*	*In a custom implementation, everything has to be built from scratch, including the solution but also all attached services (e.g. training).*					
Exchange of data between the JHA agencies & EU bodies	Hit/no-hit Task Force	400 000 €	JHA agencies and EU bodies	400 000 €	- €	JHA Agencies & EU Bodies (Eurojust, the EPPO, Europol, Frontex, OLAF)	- €	- €
Judicial Cases Cross-Check	Centralised repository of metadata	16 258 353 €	eu-LISA (centralised option)	4 427 430 €	3 789 324 €	Judicial authorities & prosecutors in EU Member States	205 100 €	46 200 €
	Alternative: Decentralised	4 403 961 € x 27	*In this option Member States will have to bear the cost for development, COTS license, the required hardware (one-time purchase and maintenance costs), implementation of the ready-for-deployment solution, design maintenance costs, system operations and maintenance costs, security accreditation costs and practical adoption costs.*					
Large Files Solution	Centralised	13 364 780 €	eu-LISA (centralised option)	3 479 084 €	3 300 096 €	Judicial authorities & prosecutors in EU Member States JHA Agencies & EU Bodies (Eurojust, the EPPO, Europol, Frontex, OLAF)	159 600 €	46 200 €

Solution	**Option**	**TCO for owners and users** (for chosen solution) **/ Impact on costs** (for alternative solution)	**Owner**	**Owner – Build costs** (for 1 year)	**Owner – Operations & maintenance costs** (for 4 years)	**Users**	**User – Build costs** (for 1 year)	**User – Operations & maintenance costs** (for 4 years)
	Alternative: Decentralised	3 508 296 € x 32	*In this option Member States will have to bear the cost for development, COTS license, the required hardware (one-time purchase and maintenance costs), implementation of the ready-for-deployment solution, design maintenance costs, system operations and maintenance costs, security accreditation costs and practical adoption costs.*					
Total (without new data centre)		**201,244,870 €**	**-**	**36,868,604 €**	**39,313,810 €**	**-**	**3,538,602 €**	**369,600 €**

7 Funding sources

This section describes the possible funding sources that could be used for the development of the solutions.

The seven proposed DCJ solutions in this report require funding for their implementation. As multiple stakeholders are involved in developing, hosting, maintaining and connecting to the solutions, funding for these activities may come from several sources. This report provides an indicative matching of EU-level funding sources only (i.e. not Member-State-level funding sources), with this section presenting identified candidate EU-level funding sources which could in theory most logically fund (part of) the seven DCJ solutions based on their characteristics if relevant additional steps were taken by the competent authorities to secure this. The confirmation of funding sources to be used and additional actions to secure this are not within the scope of this report.

7.1 Methodology

Three steps were followed for the identification and indicative matching of candidate EU-level funding sources:

- Step 1 – Characterisation of the DCJ solutions (as presented in section 5): in order to identify appropriate EU-level funding sources for the solutions, a number of characteristics were first defined for the DCJ solutions (see section 7.2).
- Step 2 – Identification of candidate EU-level funding sources which could be used to finance the DCJ solutions: taking into account the EU Treaties and Financial Regulation, as well as the legal bases underpinning EU-level action in the areas tackled by the DCJ solutions, and the high-level nature of the funding required for DCJ solutions, a range of possible EU-level funding sources was identified (see section 7.3).
- Step 3 – Indicative matching and identification of considerations regarding different candidate EU level funding sources which could be used to finance the specific DCJ solutions: candidate EU level funding sources were indicatively matched with the seven proposed DCJ solutions and considerations identified – as relevant - where multiple candidates were envisaged (see section 7.4).

7.2 DCJ solutions’ characteristics

The following characteristics were identified for each proposed DCJ solution and summarised in Table 49 for the seven solutions:

- The legal base for the solution, and its prescriptions (where applicable) in terms of funding (e.g. if it is an existing solution, from where is it funded? If not, was funding requested or not?).
- The stakeholders involved in developing and hosting the solution.
- Whether the solution already partly exists or is entirely new.

- The nature of the solution (e.g. whether it is a fully fledged digital technical solution or not, and if so, the type of the digital technical solution).

Table 49: Characteristics of the DCJ solutions

Solution	Option	Legal base (and relevant funding prescriptions)	Stakeholders involved (development, hosting, and connection to the solution)	Existing solution?	Nature of the solution
Secure Communication Channel	eDelivery (with e-CODEX connector) over the TESTA Eurodomain	N/a	Development: not necessary (solution already existing) Users: Member States and JHA agencies and EU bodies	Yes, existing solution to be re-used	Technical solution
	eDelivery (with e-CODEX connector) over the internet	N/a	Development: not necessary (solution already existing) Users (connection): Member States and JHA agencies and EU bodies	Yes, existing solution to be re-used	Technical solution
	eDelivery (with another connector) over the internet	N/a	Development: not necessary (solution already existing) Users (connection): Member States and JHA agencies and EU bodies	Yes, existing solution to be re-used	Technical solution
	eDelivery (with another connector) over the TESTA EuroDomain	N/a	Development: not necessary (solution already existing) Users (connection): Member States and JHA agencies and EU bodies	Yes, existing solution to be re-used	Technical solution
	TESTA (Eurodomain or another dedicated domain)	N/a	Development: not necessary (solution already existing) Users (connection): Member States and JHA agencies and EU bodies	Yes, existing solution to be re-used	Technical solution

Solution	Option	Legal base (and relevant funding prescriptions)	Stakeholders involved (development, hosting, and connection to the solution)	Existing solution?	Nature of the solution
	SIENA	N/a	Development: not necessary (solution already existing) Users (connection): Member States and JHA agencies and EU bodies	Yes, existing solution to be re-used	Technical solution
Communication Tool	Evolution of e-EDES	Possible new legal basis to cover the evolution of the e-EDEs platform (if necessary), and amendment of eu-LISA Regulation (if this item is hosted by eu-LISA)	Development: European Commission or eu-LISA Hosting: eu-LISA Users: Member States and JHA agencies and EU bodies	Yes	Technical solution
Redesigned Eurojust CMS (incl. Eurojust integration layer)	Redesigned Eurojust CMS (COTS product)	Eurojust Regulation	Development and hosting: Eurojust Users: Eurojust and Member States	Yes	Technical solution
JIT Collaboration Platform	JIT Collaboration Platform (COTS product)	Adoption of a new legal basis, and amendment of eu-LISA Regulation (if this item is hosted by eu-LISA)	Development: eu-LISA Hosting: eu-LISA Users (connection): Member States and JHA agencies and EU bodies.	No	Technical solution
Exchange of data between the JHA agencies and EU bodies	Hit/no-hit Task Force	Current legal bases of the JHA agencies and EU bodies (Eurojust, Europol, Frontex, the EPPO and OLAF)	The Commission, JHA agencies and EU bodies would be part of the Task Force, and Member States can partake in as observers.	No	Task Force
Judicial Cases Cross-Check	Centralised repository of metadata	Adoption of a new legal basis, and amendment of eu-LISA Regulation (if this item is hosted	Development: eu-LISA Hosting: eu-LISA (possibly) Users (connection): Member States, Eurojust, the EPPO	No	Technical solution

Solution	Option	Legal base (and relevant funding prescriptions)	Stakeholders involved (development, hosting, and connection to the solution)	Existing solution?	Nature of the solution
		by eu-LISA)			
	Decentralised	Adoption of a new legal basis (if necessary)	Development: Member States Hosting: Member States	No[189]	Technical solution
Large Files Solution	Centralised	New regulation needed, and amendment of eu-LISA Regulation (if this item is hosted by eu-LISA)	Development: eu-LISA Hosting: eu-LISA Users (connection): Member States and JHA agencies and EU bodies	No[190]	Technical solution
	Decentralised	Legal basis at national level	Development: European Commission Hosting: Member States Users (connection): Member States and JHA agencies and EU bodies	No	Technical solution

[189] The solution is however inspired by the EPRIS-ADEP project.

[190] Although there is no solution currently existing, this option is inspired by the Large File Exchange (LFE) system developed by Europol.

7.3 Candidate EU level funding sources

All EU expenditure requires a legal base entitling the Institutions or third parties selected by the Institutions to spend EU funds (Article 310 TFEU). The legal base can take different forms depending on the type of the expenditure (e.g. administrative or operational expenditure), or the area of expenditure.

For operational expenditure, the first legal reference is a basic act, which is a law containing the instructions to implement Union policies. It is generally approved by the Council and the European Parliament, and it can take the form of a Regulation, Directive or Decision.

Operational expenditure may also be covered by:

- Pilot projects to test new ideas before a basic act has been submitted to the legislative authority. If the idea is considered viable, it would lead to drafting and adopting a basic act. The duration of such projects is of a maximum of two successive budgetary years with a limited overall ceiling per year for the Commission, hence limited in scope.
- Preparatory actions which may be launched for preparing an actions implementation while a basic act is being drafted and until it is adopted. The maximum duration of such projects is three successive years with a maximum ceiling per year for new actions and for the total amount committed for the Commission, hence again limited in scope.

The Financial Regulation[191] itself is the legal base for administrative expenditure incurred for the functioning of the Institutions.

To allow for long term planning, the EU moreover establishes Multiannual Financial Frameworks (MFFs), currently covering a period of seven years. The MFFs define maximum amounts (“ceilings”) by broad category of expenditure (“headings”) for their duration. The EU is currently committing funds and spending under the 2014-2020 MFF and in the process of negotiating the 2021-2027 MFF.

In the context of Digital Criminal Justice, we identified the following candidate funding sources for the DCJ solutions based on our desk research and interviews:

For **operational expenditure:**

- Existing programmes under the current MFF from which funding might be obtained in the short term if requested. These programmes include the Justice Programme[192], ISA² Programme[193], CEF Programme[194], H2020 Programme[195] and SRS Programme[196]. Some of

[191] Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union, amending Regulations (EU) No 1296/2013, (EU) No 1301/2013, (EU) No 1303/2013, (EU) No 1304/2013, (EU) No 1309/2013, (EU) No 1316/2013, (EU) No 223/2014, (EU) No 283/2014, and Decision No 541/2014/EU and repealing Regulation (EU, Euratom) No 966/2012.

[192] Regulation (EU) No 1382/2013 of the European Parliament and of the Council of 17 December 2013 establishing a Justice Programme for the period 2014 to 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013R1382&from=EN

[193] Decision (EU) 2015/2240 of the European Parliament and of the Council of 25 November 2015 establishing a programme on interoperability solutions and common frameworks for European public administrations, businesses and citizens (ISA2 Programme) as a means for modernising the public sector, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015D2240&from=EN

these programmes already fund initiatives on which the proposed DCJ solutions build, such as e-CODEX, co-funded under the Justice Programme and the CEF Programme, and some of the CEF building blocks, funded by the CEF Programme. However, these programmes would not be used to commit EU funds from 2021 onwards, and are hence not appropriate to fund forward-looking DCJ solutions requiring financing in the next years given the time necessary to initiate and develop these.

- New programmes proposed by the Commission under its proposed MFF 2021-2027 from which funding might be obtained, if requested. These include the new Justice Programme[197], the Digital Europe Programme[198], the Recovery and Resilience Facility (ex Structural Reform Support Programme) and the Horizon Europe Programme. At the moment of writing this report:

    - Negotiations on the MFF 2021-2027 and on the EU budget for 2021 are ongoing. Final amounts for the MFF envelopes and programmes are unknown, but requests for funding sources should already have been made by stakeholders in order to be taken into account in the negotiations being held, based on relevant legal bases.

    - DG JUST has:

        - Envisaged budget under the future Justice Programme e.g. for training and coordination activities, but not for the technical development and hosting of technical DCJ solutions as the restricted overall level of funding under the programme is not appropriate for funding IT development programmes.

        - Requested that budget should be foreseen under the future Digital Europe Programme in 2021 and 2022 for two objectives to which the DCJ solutions should contribute:

            - *Maintain and extend the BRIS and e-Justice Digital Service Infrastructure*: this provides for the continued evolution and maintenance of the e-Evidence Digital Exchange System developed and maintained by DG JUST and allows for continued support to Member States with respect to the rollout of the e-Justice Generic Services developed in the context of CEF.

[194] Regulation (EU) No 1316/2013 of the European Parliament and of the Council of 11 December 2013 establishing the Connecting Europe Facility, amending Regulation (EU) No 913/2010 and repealing Regulations (EC) No 680/2007 and (EC) No 67/2010, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013R1316&from=EN

[195] Regulation (EU) No 1291/2013 of the European Parliament and of the Council of 11 December 2013 establishing Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020) and repealing Decision No 1982/2006/EC, https://ec.europa.eu/research/participants/data/ref/h2020/legal_basis/fp/h2020-eu-establact_en.pdf

[196] Regulation (EU) 2017/825 of the European Parliament and of the Council of 17 May 2017 on the establishment of the Structural Reform Support Programme for the period 2017 to 2020 and amending Regulations (EU) No 1303/2013 and (EU) No 1305/2013, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0825&from=EN

[197] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing the Justice Programme COM/2018/384 final - 2018/0208 (COD).

[198] Proposal for a Regulation of the European Parliament and of the Council establishing the Digital Europe Programme for the period 2021-2027 {SEC(2018) 289 final} - {SWD(2018) 305 final} - {SWD(2018) 306 final}, https://eur-lex.europa.eu/resource.html?uri=cellar:321918fd-6af4-11e8-9483-01aa75ed71a1.0003.03/DOC_1&format=PDF

- *Digitalisation of Justice*: the envisaged funding would allow for revamping the Eurojust Case Management System and to support all other projects under the Digital Criminal Justice policy strand, as far as these are not mentioned separately, i.e. a Secure Communication Channel; a Communication Tool to exchange data among the Member States and with the relevant JHA agencies/EU bodies; a Collaboration Platform for Joint Investigations Teams; and support for hit/no-hit exchanges between the relevant EU bodies/agencies. It would support both the EU actors involved and Member State authorities.

- Not made any requests for budget under the Horizon Europe or Recovery and Resilience Facility. Nevertheless, Member States may make requests for technical assistance under the Recovery and Resilience Facility (for expertise rather than IT development).

- Not requested specific budget increases in the budgets of Eurojust or other JHA agencies and EU bodies linked to DCJ solutions (e.g. the DCJ initiative is mentioned in Eurojust's latest Single Programming Document[199], but no specific additional budget is foreseen linked to this).

For **administrative expenditure**: the administrative budget of the Justice and Consumers policy area.

Overall, it can be concluded that due to their characteristics, the Justice Programme, ERDF and RSP present some limitations as funding sources for the Digital Criminal Project. The DEP seems thus the most suitable candidate to finance the needs of the project. The section below provides a detailed matching between the funding sources and the solutions.

The following information about programmes mentioned above is interesting to keep in mind when reading the analysis in the section below:

- The Digital Europe Programme and Justice Programme allow for direct and indirect management by Agencies through grants, contribution agreements and other financial instruments.
- The Recovery and Resilience Facility has a so called "Technical Support Instrument" that allows for shared, direct and indirect management, also through grants.
- The European Regional Development Fund (ERDF) allows only for shared management (by Member States).

7.4 Indicative matching and identification of considerations regarding candidate EU level funding sources

The seven proposed DCJ solutions were matched with candidate EU-level funding sources based on their characteristics. Our analysis identified candidate EU-level funding sources to finance (part of) all seven proposed DCJ solutions. The table below presents this matching exercise for the DCJ solutions hereunder, including considerations regarding different candidates where appropriate.

[199] Eurojust Single Programming Document 2020 – 2022, 10 December 2019

Table 50: Funding sources

Solution	Option	Stakeholders involved (development, hosting, and connection to the solution)	Candidate funding sources	Considerations
Secure Communication Channel	eDelivery (with e-CODEX connector) over the TESTA	Member States	For the implementation eDelivery: • Digital Europe Programme (under objective Digitalisation of Justice) • Recovery and Resilience Facility • ERDF and Cohesion Funds	By 2021, all Member States will have e-CODEX installed in the context of e-EDES. The Internal Security Fund, Recovery and Resilience Facility, ERDF and Cohesion Funds could be used to source funding for (part of) Member States' connection to the Secure communication channels (as is done for SIENA under the current Internal Security Fund).
		JHA agencies and EU bodies	For the implementation of eDelivery (and the e-CODEX connector): • Digital Europe Programme (under objective Digitalisation of Justice or the objective Deployment of Building Blocks) • Own Budgets (JHA agencies and EU bodies)	Implementation could be funded by the Digital Europe Programme under the objective Deployment of Building Blocks if it is limited to eDelivery.
	eDelivery (with e-CODEX connector) over the internet	Member States	For the implementation of the solution: • Digital Europe Programme (under objective Digitalisation of Justice) • Recovery and Resilience Facility • ERDF and Cohesion Funds	The Internal Security Fund, Recovery and Resilience Facility, ERDF and Cohesion Funds could be used to source funding for (part of) MS connectors to the Secure communication channels. The CEF Programme can only be used during the current 2014-2020 MFF.

Solution	Option	Stakeholders involved (development, hosting, and connection to the solution)	Candidate funding sources	Considerations
		JHA agencies and EU bodies	For the implementation of eDelivery: • Digital Europe Programme (under objective Digitalisation of Justice) • Own Budget (JHA agencies/EU bodies)	
	TESTA	Member States	For the implementation of the solution: • Digital Europe Programme (under objective Digitalisation of Justice) • Recovery and Resilience Facility • ERDF and Cohesion Funds	
		JHA agencies and EU bodies	N/a	JHA agencies and EU bodies already have TESTA.
	SIENA	Member States	For the connection to the solution: • Digital Europe Programme (under objective Digitalisation of Justice) • Recovery and Resilience Facility • ERDF and Cohesion Funds	All Member States already have access to SIENA via their Europol National Units, and can proceed to its extension to other competent authorities (in this case, judicial authorities).
		JHA agencies and EU bodies	• Digital Europe Programme (under objective Digitalisation of Justice) • Own budget	While Eurojust and OLAF already have access to SIENA, the remaining JHA agencies and EU bodies would be required to install it.
Communication Tool	Evolution of e-EDES	Member States	For the connection to the solution • Digital Europe Programme (under objective *Maintain and extend the BRIS and e-Justice Digital Service Infrastructure*) • Recovery and Resilience Facility • ERDF and Cohesion Funds	Recovery and Resilience Facility, ERDF and Cohesion Funds could be used to source funding for (part of) Members States' connection to the Communication Tool. Currently Member States also receive EU funding grants under the Justice Programme for connection. If this cannot systematically be the case going forward, alternative funding sources are not managed by DG JUST, hence again complicating oversight and

Solution	Option	Stakeholders involved (development, hosting, and connection to the solution)	Candidate funding sources	Considerations
				governance.
		European Commission	For the development of the solution: - Justice Programme - Digital Europe Programme (under objective *Maintain and extend the BRIS and e-Justice Digital Service Infrastructure*)	Where this is currently funded by Justice Programme, and CEF, DG JUST has foreseen funding it under the Digital Europe Programme (under objective Maintain and extend the BRIS and e-Justice Digital Service Infrastructure) going forward.
		JHA agencies and EU bodies	For the connection to the solution: - JHA agencies and EU bodies' budget amended accordingly.	
		eu-LISA	For the development of the solution: - Digital Europe Programme (under objective *Maintain and extend the BRIS and e-Justice Digital Service Infrastructure*) For the maintenance of the solution - eu-LISA own budget amended accordingly	
Redesigned Eurojust CMS (incl. Eurojust Integration Layer)	Redesigned Eurojust CMS	Eurojust	For the development, and maintenance: - Digital Europe Programme (under objective *Digitalisation of Justice*) - Eurojust budget amended accordingly	The Digital Europe Programme is sizeable and foreseen for IT projects like those proposed for this solution. Eurojust's budget does not currently foresee resources for this.
JIT Collaboration Platform	JIT Collaboration Platform	Member States	For the connection to the solution: - Digital Europe Programme (under objective *Digitalisation of Justice*) - Internal Security Fund	The Digital Europe Programme is sizeable and foreseen for IT projects like those proposed for this solution.

Solution	Option	Stakeholders involved (development, hosting, and connection to the solution)	Candidate funding sources	Considerations
			• Recovery and Resilience Facility • ERDF and Cohesion Funds	
		eu-LISA	For the development of the solution: • Digital Europe Programme (under objective *Digitalisation of Justice*) • eu-LISA own budget amended accordingly	This item is not currently foreseen in eu-LISA's budget, hence would require a full budgetary amendment and possibly a legislative process to materialise.
Exchange of data between the JHA agencies & EU bodies	Task Force	JHA agencies and EU bodies part of the Task Force	For the deployment and running of the Task Force: • Administrative budget of the DG JUST policy area For the implementation of the future hit/no-hit: • Digital Europe Programme (under objective Digitalisation of Justice) • Justice Programme	
		Member States (observers)	For their (voluntary) participation to the Task Force: • n/a (national administrative budget)	
Judicial Cases Cross-Check	Centralised repository of metadata	Member States	For the connection to the solution: • Digital Europe Programme (under objective *Digitalisation of Justice*) • Recovery and Resilience Facility • ERDF and Cohesion Funds	
		JHA agencies and	For the connection to the solution	The Digital Europe Programme is sizeable and foreseen

Solution	Option	Stakeholders involved (development, hosting, and connection to the solution)	Candidate funding sources	Considerations
		EU bodies	(Eurojust, and the EPPO): • Own Budgets • Digital Europe Programme (under objective *Digitalisation of Justice*)	for IT projects like those proposed for this solution.
		eu-LISA	For the development of the solution: • Digital Europe Programme (under objective *Digitalisation of Justice*) For the maintenance of the solution: • eu-LISA own budget amended accordingly	This item is not currently foreseen in eu-LISA's budget, hence would require a full budgetary amendment and possibly a legislative process to materialise.
	Decentralised	Member States	For the development and connection to the solution: • Digital Europe Programme (under objective Digitalisation of Justice)	
		JHA agencies and EU bodies	For the connection to the solution: • Digital Europe Programme (under objective Digitalisation of Justice) • Own Budgets (JHA agencies/EU bodies)	
Large Files Solution	Centralised	Member States	For the connection to the solution: • Digital Europe Programme (under objective *Digitalisation of Justice*)	The Digital Europe Programme is sizeable and foreseen for IT projects like those proposed for this solution.
		JHA agencies and EU bodies	For the connection to the solution: • Digital Europe Programme (under	The Digital Europe Programme is sizeable and foreseen for IT projects like those proposed for this solution.

Solution	Option	Stakeholders involved (development, hosting, and connection to the solution)	Candidate funding sources	Considerations
			objective *Digitalisation of Justice*) - Own Budgets (JHA agencies and EU bodies)	
		eu-LISA	For the development and maintenance of the solution: - Digital Europe Programme (under objective *Digitalisation of Justice*) - eu-LISA own budget amended accordingly	This item is not currently foreseen in eu-LISA's budget, hence would require a full budgetary amendment and possibly a legislative process to materialise.
	Decentralised	Member States	For the development and implementation of the solution: - Digital Europe Programme (under objective Digitalisation of Justice) - Recovery and Resilience Facility - ERDF and Cohesion Funds	
		JHA agencies and EU bodies	For the connection to the solution: - Digital Europe Programme (under objective Digitalisation of Justice)Own Budget (JHA agencies/EU bodies)	

8 Recommendations

This final section provides the recommendations of the study.

8.1 High level roadmap for the development and deployment of DCJ solutions

A roadmap aims to provide an overview of the necessary activities to implement the DCJ solutions. It should be noted that these activities vary, not only depending on the solution, but also on the scenario of the solution (e.g. centralised vs decentralised scenario). The roadmap needs therefore to display a sequence of activities tailored to each of the solutions (and scenario).

The figure below presents the roadmap suggested for the DCJ solutions, and a more detailed explanation follows.

Figure 34: Roadmap

Dependencies

#	Solution		Activities(*)															
			Policy implementation		Legal implementation				IT implementation									
1	Secure Communication Channel		**1.A** Set up project governance and team	**1.B** Define vision for the future secure communication channel	**1.C** Assess the different options for secure communication channel	**1.D** Security & data protection assessment	**1.E** Create technical requirements for each recipient	**1.F** Implement secure communication channel	**1.G** Accreditation	**1.H** Testing	**1.I** MS/JHA agencies & EU bodies adaptation & preparation	**1.J** Deployment of the solution	**1.K** Training activities					
2.1	Communication Tool (developed by EC)		**2.A** Decide on the approach for its development: **2.1** By EC **2.2** By eu-LISA)	**2.1.B** Preparation and enactment of legal basis (if necessary)	**2.1.C** Set up project governance and team	**2.1.D** Create technical requirements to further develop e-EDES	**2.1.E** Tender process	**2.1.F** Implement the evolution of e-EDES	**2.1.G** Accreditation	**2.1.H** Testing of the evolution of e-EDES	**2.1.I** MS/JHA agencies & EU bodies adaptation & preparation	**2.1.J** Roll-out of the evolution of e-EDES	**2.1.K** Training activities					
2.2	Communication Tool (developed by eu-LISA)			**2.2.B** Preparation and enactment of legal basis, amendment of eu-LISA Regulation (if necessary)	**2.2.C** Set up project governance and team	**2.2.D** Create technical requirements to further develop e-EDES	**2.2.E** Tender process	**2.2.F** Implement the evolution of e-EDES	**2.2.G** Accreditation	**2.2.H** Testing of the evolution of e-EDES	**2.2.I** MS/JHA agencies & EU bodies adaptation & preparation	**2.2.J** Roll-out of the evolution of e-EDES	**2.2.K** Training activities					
3.1	Redesigned Eurojust CMS	Core CMS	**3.1.A** Set up project governance and team	**3.1.B** Analyse and draft functional and non-functional requirements for the EJ CMS	**3.1.C** Assess fit of market solutions vs Case@EC	**3.1.D** Tender process	**3.1.E** Design of the solution	**3.1.F** Proof of concept	**3.1.G** Security & data protection assessment	**3.1.H** Implementation	**3.1.I** Accreditation	**3.1.J** Testing	**3.1.K** MS/JHA agencies & EU bodies adaptation & preparation	**3.1.L** Roll-out	**3.1.M** Training activities			
3.2		Counter-Terrorism Register	**3.2.A** Set up project governance and team	**3.2.B** Analyse and draft functional and non-functional additional requirements	**3.2.C** Tender process	**3.2.D** Proof of concept	**3.2.E** Security & data protection assessment	**3.2.F** Implementation	**3.2.G** Accreditation	**3.2.H** Testing	**3.2.I** Deployment	**3.2.J** Training activities						
3.3		JIT Admin Portal	**3.3.A** Set up project governance and team	**3.3.B** Analyse and draft functional and non-functional requirements	**3.3.C** Assess fit of market solutions	**3.3.D** Tender process	**3.3.E** Design of the solution	**3.3.F** Proof of concept	**3.3.G** Security & data protection assessment	**3.3.H** Implementation	**3.3.I** Accreditation	**3.3.J** Testing	**3.3.K** MS/JHA agencies & EU bodies adaptation & preparation	**3.3.L** Deployment	**3.3.M** Training activities			
3.4		Action Day Collaboration Platform	**3.4.A** Set up project governance and team	**3.4.B** Analyse and draft functional and non-functional requirements	**3.4.C** Assess fit of market solutions	**3.4.D** Tender process	**3.4.E** Design of the solution	**3.4.F** Proof of concept	**3.4.G** Security & data protection assessment	**3.4.H** Implementation	**3.4.I** Accreditation	**3.4.J** Testing	**3.4.K** MS/JHA agencies & EU bodies adaptation & preparation	**3.4.L** Roll-out	**3.4.M** Training activities			
3.5		Integration Layer	**3.5.A** Set up project governance and team	**3.5.B** analyse and draft functional and non-functional requirements	**3.5.C** Assess fit of market solutions	**3.5.D** Tender process	**3.5.E** Design of the solution	**3.5.F** Proof of concept	**3.5.G** Security & data protection assessment	**3.5.H** Implementation	**3.5.I** Accreditation	**3.5.J** Testing	**3.5.K** Deployment					
4	JIT Collaboration Platform		**4.A** Impact assessment, set up project governance and team	**4.B** Preparation and enactment of legal basis	**4.C** Define functional & technical requirements	**4.D** Assess fit of market solution vs solution developed by the EUI	**4.E** Tender process	**4.F** Design of the solution	**4.G** Proof of concept	**4.H** Security & data protection assessment	**4.I** Implementation	**4.J** Accreditation	**4.K** Testing	**4.L** MS/JHA agencies & EU bodies adaptation & preparation	**4.M** Roll-out	**4.N** Training activities		
5	Exchange of data between the JHA agencies and EU bodies		**5.A** Create Hit / No Hit Task Force	**5.B** Define technical requirements for information to be exchanged	**5.C** Design of the solution	**5.D** Security & data protection assessment	**5.E** Implementation of requirements in systems for all stakeholders	**5.F** Testing	**5.G** JHA agencies & EU bodies adaptation & preparation	**5.H** Roll-out	**5.I** Training activities							
6.1	Judicial Cases Cross-Check	Centralised	**6.A** Define concept, vision & identify synergies with existing initiatives	**6.B** Decide on the approach: **6.1.** Centralised scenario **6.2** Decentralised scenario	**6.1.C** Preparation and enactment of legal basis	**6.1.D** Set up project governance and team	**6.1.E** Security and data protection assessment	**6.1.F** Define technical requirements	**6.1.G** Tender process	**6.1.H** Design of the solution	**6.1.I** Proof of concept	**6.1.J** Implementation	**6.1.K** Accreditation	**6.1.L** Testing	**6.1.M** MS/JHA agencies & EU bodies adaptation & preparation	**6.1.N** Roll-out	**6.1.O** Training activities	
6.2		Decentralised			**6.2.C** Preparation and enactment of legal basis (if necessary)	**6.2.C** Set up project governance and team	**6.2.D** Security and data protection assessment	**6.2.E** Define requirements (based on the ADEP-EPRIS project)	**6.2.F** Tender process	**6.2.G** Design of the solution	**6.2.H** Proof of concept	**6.2.I** Security & data protection assessment	**6.2.J** Implementation	**6.2.K** Accreditation	**6.2.L** Testing	**6.2.M** MS/JHA agencies & EU bodies adaptation & preparation	**6.2.N** Roll-out	**6.2.O** Training activities
7.1	Large Files Solution	Centralised	**7.A** Define concept, vision & identify synergies with existing initiatives	**7.B** Decide on the approach: **7.1.** Centralised scenario **7.2** Decentralised scenario	**7.1.C** Preparation and enactment of legal basis	**7.1.D** Set up project governance and team	**7.1.E** Security and data protection assessment	**7.1.F** Define technical requirements	**7.1.G** Tender process	**7.1.H** Design of the solution	**7.1.I** Proof of concept	**7.1.J** Implementation	**7.1.K** Accreditation	**7.1.L** Testing	**6.1.M** MS/JHA agencies & EU bodies adaptation & preparation	**7.1.N** Roll-out	**7.1.O** Training activities	
7.2		Decentralised			**7.2.C** Set up project governance and team	**7.2.D** Security and data protection assessment	**7.2.E** Define technical requirements	**7.2.F** Tender process	**7.2.G** Design of the solution	**7.2.H** Proof of concept	**7.2.I** Security & data protection assessment	**7.2.J** Implementation	**7.2.K** Accreditation	**7.2.L** Testing	**7.2.M** MS/JHA agencies & EU bodies adaptation & preparation	**7.2.N** Roll-out	**7.2.O** Training activities	

(*): the implementation of these activities is subject to available financing.

As indicated in the figure, the activities to be carried out fall within three main implementation categories, differentiated by a colour coding:

- Policy implementation (in blue) refers to the preparatory activities prior to the enactment of a legal basis (i.e. impact assessment analysis), which would allow to answer key questions such as the scenario (i.e. decentralised or decentralised) to be implemented for some solutions (i.e. Judicial Cases Cross-Check and Large Files Solution), or the stakeholder in charge of the IT development (e.g. the Communication Tool can be developed either by the European Commission, or eu-LISA). When a legal basis is not required, the policy implementation consists of the coordination activities necessary to launch the IT implementation (e.g. further define the solution or set up the project governance and team).
- Legal implementation (in grey) indicates when a legal basis, or amendments to an already existing legal instrument are required.
- IT implementation (in green) includes the different activities for the development and the subsequent deployment/roll-out of a solution. This process usually starts with the preparation of the functional and non-functional requirements, which will allow to have a clear overview of the necessary resources to mobilise. On that basis, the tender process will be prepared and launched. Subsequently, the contractor will design the solution, based on the requirements previously identified. A proof of concept if necessary should be carried out to ensure the feasibility of the solution. Following this step, an in-depth security and data protection assessment should be conducted. The solution should be then implemented, accredited, and tested. Lastly, the stakeholders (mainly the Member States, as well as the JHA agencies and EU bodies) should be prepared to be connected to the solution, and properly trained to use it. The solution is then launched, and made available for its use.

As part of the IT implementation process, the solutions must go through an accreditation process to handle classified information. This process is laid down in Council Decision 2013/488/EU[200], and its accompanying security guidelines developed by the Security Committee of the Council (in accordance with Article 6(2) of the Council Decision mentioned). The accreditation process explained in these legal documents apply to all DCJ solutions. Nevertheless, it should be noted that all agencies and bodies concerned have their own set of security rules[201], which are based and aligned with Council Decision 2013/488/EU.

Concerning the steps, the accreditation process is kicked-off by carrying out a risk assessment, based on the business needs, technical implementation, and the accreditation scope. Following this, the system requirement statement is prepared and reviewed, and subsequently approved by a Security Accreditation Authority. The system is then implemented, together with the security requirements established in the system requirement statement. If deemed necessary, an external evaluation of the security implementation can be requested. The implementation, together with the draft accreditation documentation is prepared. Lastly, the accreditation of the solution implementation shall be approved by a Security Accreditation Authority.

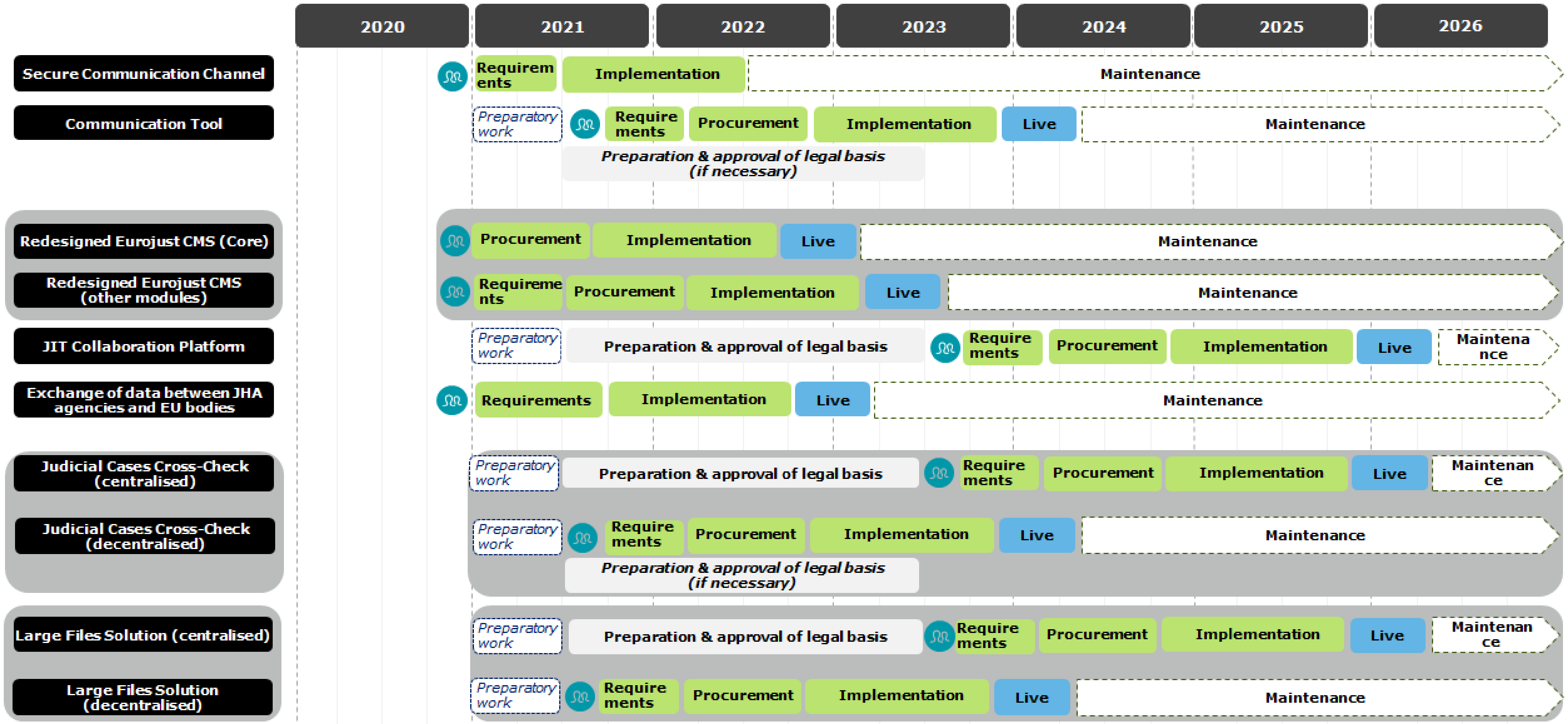
As part of the roadmap, indications in general terms regarding the necessary expected timeframe are important. Therefore, the time element should be added in order to ensure an appropriate

[200] Council Decision of 23 September 2013 on the security rules for protecting EU classified information, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013D0488&from=EN

[201] College Decision 2016-4 adopting the revised security rules of Eurojust.

planning. However, in terms of timeline, no precise planning can be provided at this stage due to the large number of unknowns and co-dependencies related to the different solutions. However, we suggest the following high level timeline for the development of the DCJ solutions.

Figure 35: Timeline



Disclaimer: all timings are purely indicative and should not be taken strictly.

● Setting up the governance and the project team

The timing indicated is indicative and the following assumptions were made:

- Preparatory work: 6 months.
- Preparation and approval of legal bases: 2 years.
- Procurement: 8 months.
- Implementation: 1 year.

This indicative high level framework takes into account several factors:

- The urgency for the solution to be developed. This refers to the necessity for the stakeholders to have the solution in place (e.g. the Redesigned CMS), or political and legal deadlines (i.e. the exchange of data between the JHA agencies and EU bodies).
- Envisaged interdependencies amongst the solutions (identified through the analysis of the necessary activities for the development of the solutions, and indicated in the roadmap – see figure 33).
- Expected additional timeframe needed for preparing and adoption legislative measures.

As displayed in the figure, the preparation of all DCJ solution would start at the beginning of 2021. However, the governance and the project teams of some solutions (i.e. the Secure Communication Channel, the Redesigned Eurojust CMS, and the Task Force hit/no-hit) could already start by the end of 2020.

Depending on the nature of the solution, the preparation would directly start the policy implementation (i.e. set up the governance and team project), followed by the IT implementation (i.e. requirements, process, etc.), or with the legal implementation (i.e. the preparation and approval of the legal basis).

Concerning the latter, the following solutions require a legal basis: the JIT Collaboration Platform, the Judicial Cases Cross-Check (centralised solution), and Large Files Solution (centralised). If deemed necessary, the Communication Tool, as well as the Judicial Cases Cross-Check (decentralised) might require a legal basis. The preparatory work for these solutions mainly refers to the impact assessment that needs to be conducted. For the decentralised scenario of the Judicial Cases Cross-Check and the Large Files Solution, this phase (subject to financing and allocation of resources) refers to preliminary analysis, identification of possible funding sources and preparation of the relevant documentation. Frontloading this type of tasks would allow to set the scene, and ensure time and efficiency gains.

8.2 Governance

Governance is at the heart of the success of the Digital Criminal Justice roadmap implementation. The appropriate overarching governance would ensure the correct development and implementation of the solutions.

The DCJ roadmap needs a governance structure involving different entities which would need to supervise and implement the activities for each solution. These entities are groups of stakeholders, with different objectives, roles and responsibilities.

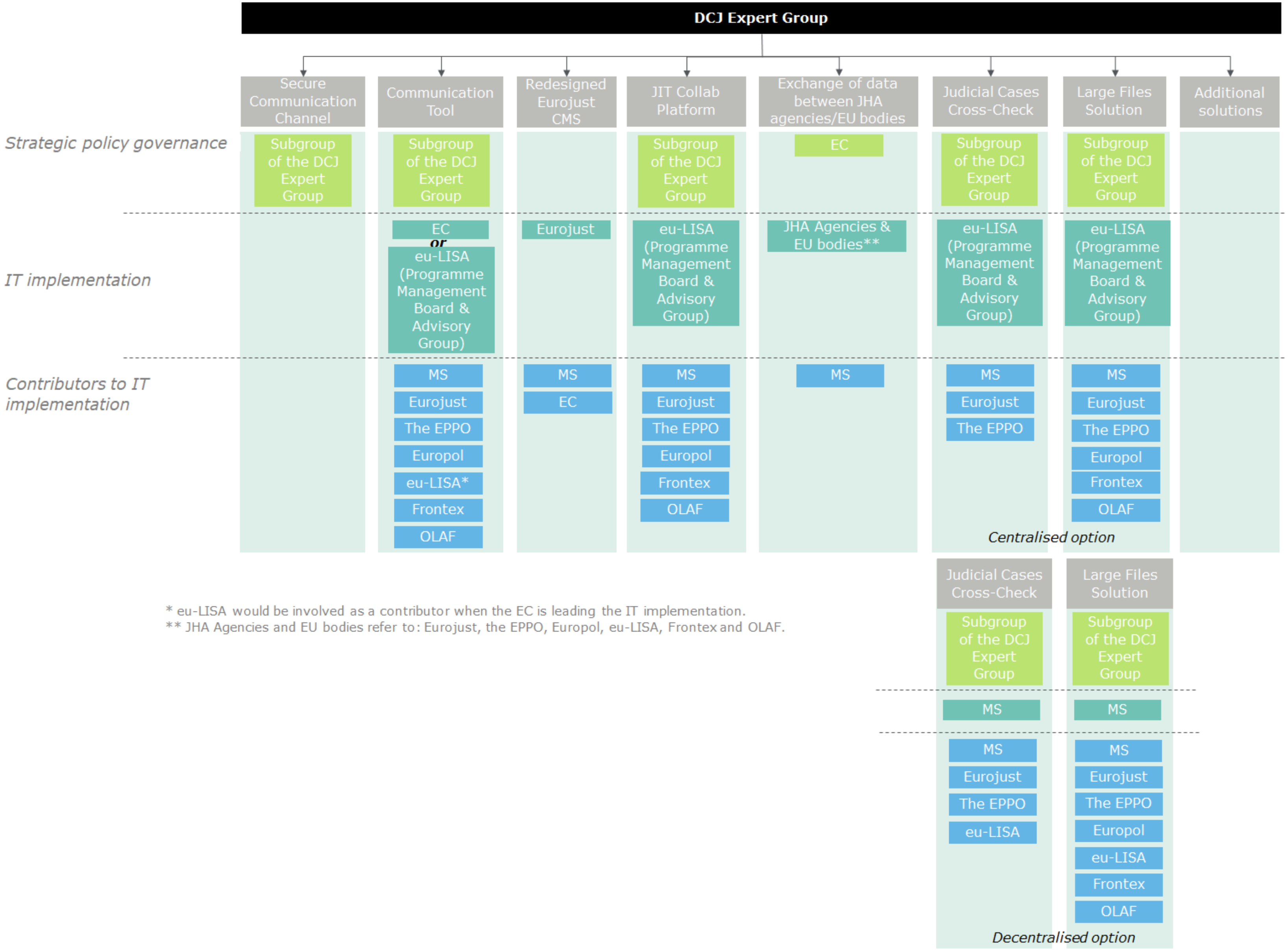
We suggest considering three different layers in the governance:

- Strategic governance: refers to the overarching governance of the Digital Criminal Justice project.
- IT implementation: assigns the stakeholder responsible to carry out the development and implementation of a specific solution.
- Contribution to the IT implementation: includes the stakeholders supporting the IT implementation.

The figure below illustrates these three layers, and indicates across all the solutions the specific entity responsible for the different governance layers.

It must be underlined that in addition to this overall governance of the Digital Criminal Justice Project, the European Commission, together with the European Parliament and the Council would be involved in the legislative procedure of adopting the necessary legal instruments.

Figure 36: Governance model overview



DCJ Expert Group

	Secure Communication Channel	Communication Tool	Redesigned Eurojust CMS	JIT Collab Platform	Exchange of data between JHA agencies/EU bodies	Judicial Cases Cross-Check	Large Files Solution	Additional solutions
Strategic policy governance	Subgroup of the DCJ Expert Group	Subgroup of the DCJ Expert Group		Subgroup of the DCJ Expert Group	EC	Subgroup of the DCJ Expert Group	Subgroup of the DCJ Expert Group	
IT implementation		EC *or* eu-LISA (Programme Management Board & Advisory Group)	Eurojust	eu-LISA (Programme Management Board & Advisory Group)	JHA Agencies & EU bodies**	eu-LISA (Programme Management Board & Advisory Group)	eu-LISA (Programme Management Board & Advisory Group)	
Contributors to IT implementation		MS Eurojust The EPPO Europol eu-LISA* Frontex OLAF	MS EC	MS Eurojust The EPPO Europol Frontex OLAF	MS	MS Eurojust The EPPO	MS Eurojust The EPPO Europol Frontex OLAF	

Centralised option

Judicial Cases Cross-Check	Large Files Solution
Subgroup of the DCJ Expert Group	Subgroup of the DCJ Expert Group
MS	MS
MS Eurojust The EPPO eu-LISA	MS Eurojust The EPPO Europol eu-LISA Frontex OLAF

Decentralised option

* eu-LISA would be involved as a contributor when the EC is leading the IT implementation.
** JHA Agencies and EU bodies refer to: Eurojust, the EPPO, Europol, eu-LISA, Frontex and OLAF.

Below, each of the governance layers is explained in more detail.

8.2.1 Strategic governance

The overall strategic governance would be ensured by the Digital Criminal Justice Expert Group. This Expert Group already exists and is composed of the Member States' representatives, the European Commission, and the JHA agencies and EU bodies.

The overall objective of the Expert Group would be to ensure the overall vision and coordination of the DCJ roadmap and the implementation of the different solutions. In practical terms, however, the Expert Group itself would not have the capacity to monitor all the solutions. Therefore, it is advisable that subgroups are created, each of them leading and supervising a given solution.

As indicated in the figure above, there would be 5 different subgroups for the following solutions: Secure Communication Channel, Communication Tool, JIT Collaboration Platform, Judicial Cases Cross-Check and the Large Files Solution. This would provide the Expert Group with some flexibility and would simplify the governance. For the remaining solutions, the Redesigned Eurojust CMS and the exchange of data between the JHA agencies and EU bodies, a specific subgroup would not be necessary. The redesign of the CMS would be led by Eurojust itself, which would be reporting to the Expert Group directly. On the other hand, the European Commission would be driving the solution related to the exchange of data between the JHA agencies and EU bodies.

In terms of roles and responsibilities, the Expert Group would closely monitor the development of the solutions to ensure they are aligned with the general vision and initial objectives, make strategic decisions for the development of the solutions, and agree on mitigation measures when some risks are identified during the IT implementation. For this purpose, the Expert Group, and its different subgroups, would liaise with the different stakeholders carrying out the IT implementation.

As for the frequency of the meetings, it is advisable that the Expert Group holds three/four yearly meetings, while the subgroups meet once or twice per two months.

8.2.2 IT implementation

Following the strategic governance, an IT implementation layer is necessary in order to designate a stakeholder with the actual development of the solution. As displayed in the figure above, the IT implementation would vary depending on the solution. The stakeholders suggested to lead the implementation of the solutions are the European Commission, eu-LISA, Eurojust, and the JHA agencies and EU bodies.

The European Commission could continue to develop the Communication Tool (e-EDES). eu-LISA on its side could be mandated with the development of the Communication Tool (if not developed by the European Commission), the JIT Collaboration Platform and the centralised options, if selected, of the Judicial Cases Cross-Check and the Large Files Solution. For the development of these different solutions, eu-LISA would put in place respective Programme Management Boards and Advisory Groups, composed of representatives of the Member States, the European Commission, and the relevant JHA agencies and EU bodies. The Member States would be in charge of the decentralised versions of the Judicial Cases Cross-Check and the Large Files Solution (if selected). Eurojust would implement the Redesigned Eurojust Case Management System. Lastly, the JHA agencies and EU bodies would implement the hit/no-hit system.

These stakeholders would lead the technical development of the solutions. This implies that they would organise and coordinate the necessary analysis activities for the development of the solution. These activities could be summarised overall in five main categories: the organisation management (tender process and funding application), operational management (time management, monitor the use of resources and liaise with the Expert Group), solution development (data flow analysis, impact analysis and requirements), stakeholder management, compliance management (data protection, security analysis and proof of concept) and technical management (technical developments, tests, and configuration). For a more detailed overview of these activities per solution, see section 8.1.

8.2.3 Contribution to IT implementation

This layer, contribution to IT implementation, refers to the stakeholders who, although not driving the implementation process, would be actively contributing to it. The stakeholders involved at this layer would vary from one solution to the other, depending on who the users of the solution would be.

For the Communication Tool, contributors would be the Member States, together with JHA agencies and EU bodies. It should be noted regarding this solution that eu-LISA would be involved as a contributor if the IT implementation is carry out by the European Commission. The implementation of the Redesigned Eurojust CMS would be supported by the Member States, and the European Commission. As for the JIT Collaboration Platform and the Large Files Solution (both centralised and decentralised) all stakeholders should be contributing to their implementation. This refers to the Member States, and the JHA agencies and EU bodies. In the case of the Judicial Cases Cross-Check, the contributors would be the Member States, together with Eurojust and the EPPO. Lastly, the Member States would also be involved in the IT implementation of the exchange of data between the JHA agencies and EU bodies.

It is key to involve these stakeholders in the development of the solutions, as they would be the future users of the tool, and would thus be part of the data flows. Moreover, it would also allow to fully tailor the solutions to their needs.

8.3 Possible legal amendments

The solutions presented in this report have different legal implications. While some require a new legal basis (either at EU or national level), others can be introduced via amendments to already existing ones, as summarised below. In some cases, the solution presented does not need a specific legal basis for its implementation.

First, the use of a Secure Communication Channel does not require a legal amendment or legal basis per se. All the options considered by the report can be used for the purpose of communication in cross-border judicial cooperation in criminal matters. Nevertheless, as pointed out in the legal assessment of this solution (see section 5.2.4), the European Commission cannot impose the uniform use of a given channel. Therefore Member States are free to use different channels for different use cases. To avoid this fragmented landscape, which would hamper the efficiency required in cross-border cases, this report recommends to reach an agreement at EU level on the channel to be used. This could consist of a non-binding agreement amongst the Member States. The Expert Group could monitor to what extent this approach is appropriate, and determine whether a legal basis is necessary to ensure the same secure communication channel is used across Member States.

Secondly, the future e-EDES platform would become the Communication Tool for cross-border judicial cooperation in criminal matters. Although a specific legal basis is not necessary for this system to operate, it would still recommended to enact a legal basis to strengthen the e-EDES platform. A new standalone legal instrument could be adopted, and specific provisions on this solution could be introduced in the eu-LISA Regulation if this agency is mandated with its hosting.

Third, the redesign of the Eurojust CMS can be conducted based on the Eurojust Regulation. This also applies to the Eurojust Integration Layer, which would be a technical component ensuring the proper functioning of the CMS.

Fourth, JIT rules are set out in Council Framework Decision 2002/465, supported by the JIT model agreement. However, none of the provisions of these instruments foresee the use of a platform to set up and deploy a JIT. The use of such a platform raises some questions, particularly from a data protection perspective (in terms of access rights, and joint data controllership). Therefore, it is advisable to enact an EU legal basis, providing a clear framework for the use of this tool. In addition, this report recommends to review and amend the JIT model agreement in order to ensure it is aligned with the new legal basis.

Fifth, the Judicial Cases Cross-Check and the Large Files Solution (if a centralised approach is adopted) would require a new legal basis, as well as an amendment to the eu-LISA Regulation if this agency is designated by the legal bases as the hosting entity. As for the decentralised options, the Judicial Cases Cross-check would require a legal basis at national level, while the Large Files Solution should be operationalised at national level.

8.4 Architecture and technology choices

The implementation of Digital Criminal Justice requires new technical solutions, and the revamp of existing ones. This report proposes a conceptual architecture (see section 5.1) bringing together different solutions: a Secure Communication Channel, a Communication Tool, the Redesigned Eurojust CMS (including the Eurojust Integration Layer), a JIT Collaboration Platform, Judicial Cases Cross-Check and a Large Files Solution. In terms of technical implementation of these different solutions, this report assesses different options and gives an indication of the most appropriate ones. Nevertheless, it should be noted that interesting alternative solutions are available on the market. Therefore, this report recommends to follow the principle *buy before build*. This approach would allow the solution drivers in charge of the different solutions to save time and resources, relying on the vendors' expertise and support to provide future-proof solutions.

To implement this principle, the report suggests to conduct a market exploration by inviting vendors to present their solutions to the Commission and other stakeholders. By letting the market play, it would be ensured that vendors design the most tailored solution for the Commission and the other stakeholders involved.

A public procurement process would allow stakeholders to follow this approach, bringing a wide range of solutions at the most advantageous price. These two principles apply to all solutions, but particularly to the Redesigned Eurojust CMS, the Eurojust Integration Layer and the JIT Collaboration Platform.

For the Secure Communication Channel, this report recommends different options for different stakeholders and use cases. eDelivery (with e-CODEX) over TESTA EuroDomain is preferred for communication between Member States and between JHA agencies and EU bodies in the context of the exchange of non-classified information. For the exchange of classified information, this same solution (i.e. eDelivery with e-CODEX over TESTA EuroDomain) would be ideally accredited. However, the required accreditation would have burdensome practical and financial consequences. Therefore, SIENA could be used alternatively, as it is accredited up to the level of EU CONFIDENTIAL already. Finally, certain exchanges of information between agencies may require specific communication channels to be used, notably in the context of SIS II, VIS and ECRIS-TCN (in the future).

Concerning the Communication Tool, the report recommends to implement the evolution of e-EDES with additional functionalities (based on e-CODEX).

The report presents different vendor solutions for the Redesigned Eurojust CMS: Case@EC, IBM’s Business Automation Workflow, and Pega’s Investigative Case Management. At this stage, the report is not able to provide a clear recommendation on the most appropriate solution, and suggests thus to conduct a more in-depth assessment.

The JIT Collaboration Platform could be implemented in three different possible ways, either reusing OLAF’s VOCU tool, implementing off the shelf products (such as Wire, Zimbra, eXo, Microsoft Teams, Cisco WeBex Teams) or building it from scratch. The report advises to use an off the shelf product as the basis for development. However, it should be noted that none of the vendor solutions is able to cover all the requirements identified for the JIT Collaboration Platform at this stage. Therefore, the report concludes that the final solution should consist of a combination of commercial products used together, which may also require some additional development (e.g. to integrate the components).

Although the data exchanges in the form of hit/no-hit among JHA agencies and EU bodies is not per se a technical solution (but a Task Force), the technical assessment indicates some key questions to be taken into account. The Task Force should discuss the type of hit/no-hit to be implemented: either an automatic cross-checking of the databases, or a manual hit/no-hit triggered by the users.

Concerning the Judicial Cases Cross-Check, this report assesses two implementation options: a decentralised (i.e. ADEP-EPRIS-like solution), and a central repository of metadata (either with hit/no-hit or blind search). Although both options present advantages and disadvantages, it is not possible to clearly indicate which option should be retained from a technical perspective, and this decision is dependent on legal and political considerations.

Likewise, a centralised and decentralised scenarios are considered for the implementation of the Large Files Solution. Again, both options present advantages and disadvantages, and it is thus not possible to provide a clear recommendation from a technical point of view.

The implementation of these solutions from a costs perspective will depend largely on the individual specificities of each Member State/JHA agency or EU body in terms of systems, network, etc., and these specificities should be the object of an assessment in a further study.

8.5 Horizontal recommendations

Besides the technical recommendations explained above on each of the specific solutions brought forward by this report, there are horizontal recommendations to be taken into account for the achievement of Digital Criminal Justice.

Due to the high number of stakeholders involved in cross-border judicial cooperation in criminal matters, as well as the large amount of information exchanged in this context, it was found that case-related data is scattered and fragmented. This challenge leads to the risk of a lack of traceability, and eventually to the potential refusal of the evidence by the courts. In order to address this issue, this report suggests to adopt a unique identifier at EU level for each cross-border case. This identifier would allow a seamless cross-border cooperation by ensuring that all data related to a given case is duly tagged with this identifier.

In the same vein, this report also recommends to implement UMF to facilitate cross-border cooperation. UMF provides a standardised data exchange format, allowing disparate systems to communicate data sets in a consistent manner. Again, the high number of stakeholders involved, as well as the substantial amount of data exchanged in criminal cross-border cooperation, call for an approach to ease the exchanges, reducing the complexity and data errors.

Annex A | Current situation

This section gives an overview of the policy and legal background to Digital Criminal Justice, as well as the ongoing and planned initiatives in this field.

Policy and legal background

The cross-border nature of criminal activities calls for an action at EU level and a close cooperation between Member States and JHA agencies/EU bodies in the fight against crime. In order to strengthen this cooperation, the use of digital solutions is key. New technologies bring an opportunity to improve the efficiency and flexibility of procedures, including the cross-border cooperation, in the prosecution phase (amongst others).

The digitalisation and the use of new technologies is now an increasingly important trend across EU policies, including justice. Although the policy documents described below are not directly related to criminal justice, but rather focus on public services and civil law, they introduce and promote the use of technologies in these fields. The presentation and description of such documents is thus necessary to have a comprehensive overview of the policy background. Besides, some of these documents have led to the creation of some solutions that could be re-used in the assignment at hand.

The Digital Single Market (DSM) Strategy[202] aims to support an inclusive society by ensuring that both citizens and businesses can benefit from e-Justice. New technologies are challenging the traditional ways to deliver justice and conduct judicial proceedings, and can be used to reduce the burden on the stakeholders involved.

The DSM Strategy is supported by an eGovernment Action Plan.[203] This Action Plan stresses the need to use digital technologies to deliver more efficient public services, reducing the burden on businesses and citizens. The digital transformation of government is indeed "a key element to the success of the Single Market".[204]

The e-Justice Strategy[205] calls for the use of technologies in order to improve the functioning of justice systems. In particular, it states the three objectives for e-Justice: access to information, e-Communication in the field of justice, and interoperability, as well as the general vision for what to include into the Action Plan and how to implement it. However, the Strategy does not include any specification regarding the concrete projects: those are described in the Action Plan.

[202] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe, COM(2015) 192 final, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN

[203] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - EU eGovernment Action Plan 2016-2020, Accelerating the digital transformation of government, COM(2016)179 final, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0179&from=EN

[204] Ibid. p. 2.

[205] 2019-2021 Strategy on e-Justice, 2019/C 96/04, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019XG0313(01)&rid=7

The current e-Justice Action Plan[206] is the third iteration,[207] and contains a list of the projects considered for implementation in the 2019-2023 period. It includes the participants (including the designated leader for the action), the different contributions expected from each stakeholder group, a description of the project and the actions to be undertaken. As explained during our strategic interviews, the most relevant actions to take into account to define the possible solutions in this study are the following:

- Action #4 - *Criminal Court Database*: this project was proposed by Austria and aims to establish a central contact point for the data of competent authorities concerning a number of legal instruments in criminal matters, such as the European Investigation Order or Mutual Legal Assistance in Criminal Matters.
- Action #14 - *Cooperation in digital criminal proceedings*: this project was proposed by Estonia with objective to explore and analyse the possibilities for exchanging data digitally in criminal proceeding. However, this is a placeholder action, i.e. an action that is planned to be conducted, but has not been launched yet.
- Action #23 - *Harmonisation of back-end systems*: this project was also proposed by Austria with the aim to generate common and harmonised backend systems for specific legal instruments. However, as for the Action#14, this is a placeholder action, and has not been launched yet either.

As indicated in the e-Justice Strategy, each Member States needs to ensure that their national systems are compatible between each other in order to allow a smooth and seamless cooperation (c.f. interoperability objective). In this context, the principles laid down in the European Interoperability Framework[208] apply. This Framework aims to remove barriers to the DSM by promoting the digitalisation of public services. In particular, it provides specific guidance on how to set up interoperable digital public services.

These strategic policy documents stress the need to use new technologies to improve public administrations, justice systems, and access to justice. The EU is committed to transform its public administrations providing end-to-end public services to all citizens and businesses, as indicated in the Tallinn Declaration. Digitalisation should also be introduced in criminal justice in order to improve the cooperation between Member States, as well as with Eurojust and other JHA agencies/EU bodies.

The EU Criminal Justice policy brings a framework for the cooperation between the different Member States and JHA agencies/EU bodies to combat crime efficiently. A wide range of legal instruments supports this framework, establishing different tools to allow the cooperation in criminal matters.

Amongst the legal instruments assessed by our team in the scope of this study,[209] stakeholders indicated that the following ones are the most relevant and most frequently used by practitioners:

[206] Action Plan European e-Justice 2019-2023, 2019/C 96/05, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019XG0313(02)&rid=6

[207] Previous e-Justice Action Plans: Multi-annual European e-Justice Action Plan 2009-2013; Multiannual European e-Justice Action Plan 2014-2018.

[208] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - European Interoperability Framework - Implementation Strategy, COM(2017)134 final, https://eur-lex.europa.eu/resource.html?uri=cellar:2c2f2554-0faf-11e7-8a35-01aa75ed71a1.0017.02/DOC_1&format=PDF

[209] Please refer to the Policy Matrix for a full overview of the legal instruments (Annex B).

- European Investigation Order (EIO):[210] this Directive lays down one of the core instruments for judicial cooperation, the EIO. This instrument allows national authorities to request evidence located in another EU country.
- European Arrest Warrant (EAW):[211] this Decision establishes the EAW, allowing national judicial authorities to request the surrender of a citizen from another EU country.
- Mutual Legal Assistance (MLA):[212] this Convention aims to promote and facilitate mutual assistance between national authorities in criminal matters, as well as to improve the efficiency of the judicial cooperation. In addition to this Convention, it must be noted that the term of mutual legal assistance refers to the rest of requests, which do not fall under the EIO or concern countries not part of the EIO (i.e. Denmark and Ireland).

Although these were the three main legal instruments mentioned during our stakeholders' consultations, interviewees also mentioned: the Decision on the exchange of information and cooperation concerning terrorist offences,[213] the Regulation on mutual recognition of freezing orders,[214] the Framework Decision on orders freezing property or evidence,[215] and the Framework Decision on mutual recognition to judgments and probation decisions.[216]

These legal instruments describe which information needs to be exchanged (some instruments even include a form to be used), how it has to be exchanged, and between which stakeholders. These instruments thus give an indication of the business needs of practitioners (described in section 3.1.2).

In addition to the stakeholders at national level, JHA agencies/EU bodies are crucial for the cross-border cooperation.

As per Art. 49 of the Eurojust Regulation, Eurojust and Europol should exchange information. Eurojust should enable Europol to have an indirect access, on the basis of a hit/no-hit system, to information provided by Eurojust. In case of a hit, Eurojust should initiate the procedure to share the information that triggered the hit. Likewise, Europol should also enable the same access to Eurojust to its information, on the basis of a hit/no-hit system (Art. 21 Regulation 2016/794[217]).

[210] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters of 3 April 2015, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0041&from=EN

[211] Council Framework Decision 2002/584/JHA of 13 June 2002 on the European Arrest Warrant and the surrender procedures between Member State, https://eur-lex.europa.eu/resource.html?uri=cellar:3b151647-772d-48b0-ad8c-0e4c78804c2e.0004.02/DOC_1&format=PDF

[212] Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000F0712(02)&from=EN and https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:42000A0712(01)&from=EN

[213] Council Decision 2005/671/JHA of 20 September 2005 on the exchange of information and cooperation concerning terrorist offences, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005D0671&from=GA

[214] Regulation (EU) 2018/1805 of the European Parliament and of the Council of 14 November 2018 on the mutual recognition of freezing and confiscation orders, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1805&from=EN

[215] Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32003F0577&from=EN

[216] Council Framework Decision 2008/947/JHA, on the application of the principle of mutual recognition to judgments and probation decisions with a view to the supervision of probation measures and alternative sanctions, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008F0947&from=EN

[217] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0794&from=EN

Eurojust and the European Public Prosecutor Office (the EPPO) are also requested to cooperate together. The EPPO has been established by means of enhanced cooperation, thus, its founding Regulation 2017/1939[218] only applies to Member States that participate in that cooperation. For those Member States which do not cooperate in the EPPO, Eurojust remains fully competent in crimes against the financial interests of the Union.

As for the cooperation between this agency and this EU body, Art. 50 of the Eurojust Regulation and Art. 100 of the EPPO Regulation state the mutual access to each other's information on a hit/no-hit basis.

Eurojust also cooperates with OLAF by exchanging operational or technical information to protect the financial interests of the Union. The cooperation between the agency and this EU body belonging to the Commission is regulated in Art. 51(1) of the Eurojust Regulation and Art. 13 of Regulation 883/2013.[219]

Eurojust also cooperates with the European Border and Coast Guard Agency (Frontex), as mentioned in Art. 51(3) of the Eurojust Regulation and Art. 68 of Regulation 2019/1896.[220]

Europol and OLAF cooperate together by exchanging operational, strategic and technical information (Art. 13 OLAF Regulation). In particular, Europol should grant indirect access to OLAF on the basis of a hit/no-hit system to information (Art. 21 Europol Regulation).

Frontex/Europol: the two agencies should closely cooperate together, coordinate their activities and exchange information (Art. 68 Frontex Regulation).

The EPPO/Europol: the EPPO shall establish and maintain a close relationship with Europol. For the purpose of its investigations, the EPPO may request information held by Europol, as well as to ask Europol to provide analytical support to a specific investigation (Art. 102 EPPO Regulation).

The EPPO and OLAF shall closely cooperate and exchange information. They both shall have a bidirectional indirect access to information in each other's CMS on the basis of a hit/no-hit system (Art. 101 EPPO Regulation).

In addition to these cooperation links, these JHA agencies and EU bodies can also query some EU IT systems:

- Eurojust can query SIS II[221] (Art. 42 SIS II Decision) and ECRIS-TCN (Art. 14 ECRIS-TCN Regulation).[222]

[218] Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office (EPPO), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R1939&from=EN

[219] Regulation (EU, EURATOM) No 883/2013 of the European parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) and repealing Regulation (EC) No 1073/1999 of the European Parliament and of the Council and Council Regulation (Euratom) No 1074/1999, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02013R0883-20170101&from=EN

[220] Regulation (EU) 2019/1896 of the European Parliament and of the Council of 13 November 2019 on the European Border and Coast Guard and repealing Regulations (EU) No 1052/2013 and (EU) 2016/1624, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R1896&from=EN

[221] The SIS legal framework is composed of: Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32006R1987&from=EN and Council Decision 2007/533/JHA of 12 June 2007

- Europol can query SIS II (Art. 41 SIS II Decision) and ECRIS-TCN (Art. 14 ECRIS-TCN Regulation).
- The EPPO can query ECRIS-TCN (Art. 14 ECRIS-TCN Regulation).

Ongoing and planned projects and initiatives

Currently, the European Commission and Member States are working on several projects and initiatives that could be potentially re-used in the framework of this assignment. The following projects and initiatives have been identified during the data collection activities:

- EXEC project[223] (will be part of e-EDES): the Electronic Xchange of e-Evidences project provides an up and running network for the fully electronic exchange of EIOs and related e-Evidences between Member States.
- Evidence2e-CODEX[224] (will also be part of e-EDES): this project brings together the two former projects EVIDENCE and e-CODEX in order to investigate the possible exchange of e-Evidence between Member States.
- ECLI: is an identifier for a legal document, developed to make European case law databases more usable.
- Find a bailiff[225] and Find a Lawyer[226] projects: these two projects are search engines allowing citizens, businesses and legal practitioners to find easily a bailiff or a lawyer throughout the European Union.
- CEF Building Blocks (eDelivery, eSignature, eTranslation).

Besides, the following projects have been identified at national level (either via the survey, or the fieldwork interviews):

- Prontuario (Spain): this platform provides Spanish judicial practitioners with guidelines on cross-border cooperation (either for civil or criminal purposes). In criminal matters, it helps practitioners to identify the relevant legal instrument to be used, explains who are the different stakeholders involved, and includes a directory.[227]
- e-CODEX pilot project (Germany - the Netherlands): transmission of EIO between Public Prosecutors Offices (PPOs) in North Rhine-Westphalia and the Netherlands. Currently, six PPOs are connected, all PPOs are expected to be connected by 2020.
- International module (Estonia): Estonia is creating an international module in their prosecution information system that can exchange information (i.e. EIO, MLA, EAW) with other countries in the context of e-EDES.

on the establishment, operation and use of the second generation Schengen Information System (SIS II), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32007D0533&from=EN

[222] Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0816&from=EN

[223] See: https://www.e-codex.eu/EXEC

[224] See: https://evidence2e-codex.eu/a/matching-evidence-to-ecodex

[225] See: http://eubailiff.eu/fab-2-project/

[226] See: https://elf-fae.eu/find-a-lawyer-3/

[227] See: http://www.prontuario.org/prontuario/es/Penal/Consulta/?id0=1

Annex B | Policy Matrix

The document attached is the Policy Matrix, displaying a full overview of the legal and policy background to Digital Criminal Justice.

DCJ_policy%20matri
x_v1.2.xlsx

Annex C | Business needs and solutions

The table below displays the detailed mapping of the business needs and the solutions.

Table 51: Business needs and solutions

ID		Business need category	Description business need	Related persona	Similar business needs	Related solution
1	PR.1	Access digital support tools	Identify the correct stakeholder (i.e. another prosecutor or central authority) in the other MS to be contacted	Prosecutors/investigative judges	JIT.10	Extended EJN Atlas (Directory)
2	PR.2	Access digital support tools	Receive training to fill in the forms electronically in an user friendly way	Prosecutors/investigative judges	PR.23, PR.27, PR.29	Training platform
3	PR.3	Securely communicate and exchange information via digital means	Send/receive requests (forms set out in the legal instruments, and their supporting documents) in a secure and digital way	Prosecutors/investigative judges	PR.4, PR.5, PR.6, PR.20, MOJ.1, MOJ.2; MOJ.3, MOJ.4, JIT.2, JIT.4, EJ.14, EJ.15, EJ.16, EJ.17, JHA.2, JHA.3	Secure communication channel Communication tool
4	PR.4	Securely communicate and exchange information via digital means	Send/receive forms to/from law enforcement officers (validate some of their forms)	Prosecutors/investigative judges	PR.3, PR.5, PR.6, PR.20, MOJ.1, MOJ.2, MOJ.3, MOJ.4, JIT.2, JIT.4, EJ.14, EJ.15, EJ.16, EJ.17, JHA.2, JHA.3	Secure communication channel Communication tool
5	PR.5	Securely communicate and exchange information via digital means	Send/receive (electronic) evidence in a secure way	Prosecutors/investigative judges	PR.3, PR.4,PR.6, PR.20, MOJ.1, MOJ.2, MOJ.3, MOJ.4, JIT.2, JIT.4, EJ.14, EJ.15, EJ.16, EJ.17, JHA.2, JHA.3	Secure communication channel Communication tool
6	PR.6	Securely communicate and exchange information via digital means	Exchange (confidential) information (in different formats) in a digital and secure way	Prosecutors/investigative judges	PR.3, PR.4, PR.5, PR.20, MOJ.1, MOJ.2, MOJ.3, MOJ.4, JIT.2, JIT.4, EJ.14, EJ.15, EJ.16, EJ.17, JHA.2, JHA.3	Secure communication channel Communication tool
7	PR.7	Securely communicate and exchange information via digital means	Have an easy tool to receive/send notifications and reminders	Prosecutors/investigative judges	PR.14, PR.15, PR.16, PR.17, PR.18, PR.19, PR.20, JIT.2, JIT.3, JIT.4, JIT.5, JIT.6, JIT.7, JIT.9, JIT.13, EJ. 20, EJ.21, JHA.3, JHA.4	Re-designed CMS
8	PR.8	Access digital support tools	Electronically sign the documents to be sent in order to authenticate them	Prosecutors/investigative judges	PR.9, EJ.27, EJ.28	eSignature (CEF Building Block)

9	PR.9	Access digital support tools	Receive the documents electronically signed to be certain of their authenticity	Prosecutors/investigative judges	PR.8, EJ.27, EJ.29	eSignature (CEF Building Block)
10	PR.10	Securely communicate and exchange information via digital means	Contact counterparts to follow-up on the case (via email/direct messages/videoconference)	Prosecutors/investigative judges	PR.14, PR.15, PR.16, PR.17, PR.18, PR.19, PR.20, JIT.2, JIT.3, JIT.4, JIT.5, JIT.6, JIT.7, JIT.9, JIT.13, EJ. 20, EJ.21, JHA.3, JHA.4	Re-designed CMS
11	PR.11	Securely communicate and exchange information via digital means	Request an official translation of the documents to be sent	Prosecutors/investigative judges	PR.3, PR.4, PR.5, PR.6, PR.20, MOJ.1, MOJ.2, MOJ.3, MOJ.4, JIT.2, JIT.4, EJ.14, EJ.15, EJ.16, EJ.17, JHA.2, JHA.3	Re-designed CMS
12	PR.12	Access digital support tools	Direct translation of documents (i.e. not official) to start working on the case (instead of waiting for the official translation	Prosecutors/investigative judges	JIT.17, EJ.25, EJ.26	eTranslation (CEF Building Block)
13	PR.13	Securely communicate and exchange information via digital means	Receive the official translation of documents	Prosecutors/investigative judges	PR.3, PR.4, PR.5, PR.6, PR.20, MOJ.1, MOJ.2, MOJ.3, MOJ.4, JIT.2, JIT.4, EJ.14, EJ.15, EJ.16, EJ.17, JHA.2, JHA.3	Secure communication channel Communication tool
14	PR.14	Securely communicate and exchange information via digital means	Contact central authorities for support digitally	Prosecutors/investigative judges	PR.15, PR.16, PR.17, PR.18, PR.19, PR.20, JIT.2, JIT.3, JIT.4, JIT.5, JIT.6, JIT.7, JIT.9, JIT.13, EJ. 20, EJ.21, JHA.3, JHA.4	Judicial One-Stop-Shop Portal
15	PR.15	Securely communicate and exchange information via digital means	Contact EJN for support digitally	Prosecutors/investigative judges	PR.14, PR.16, PR.17, PR.18, PR.19, PR.20, JIT.2, JIT.3, JIT.4, JIT.5, JIT.6, JIT.7, JIT.9, JIT.13, EJ. 20, EJ.21, JHA.3, JHA.4	Judicial One-Stop-Shop Portal
16	PR.16	Securely communicate and exchange information via digital means	Contact Eurojust for support digitally	Prosecutors/investigative judges	PR.14, PR.15, PR.17, PR.18, PR.19, PR.20, JIT.2, JIT.3, JIT.4, JIT.5, JIT.6, JIT.7, JIT.9, JIT.13, EJ. 20, EJ.21, JHA.3, JHA.4	Judicial One-Stop-Shop Portal
17	PR.17	Securely communicate and exchange information via digital means	Contact law enforcement officers	Prosecutors/investigative judges	PR.14, PR.15, PR.16, PR.18, PR.19, PR.20, JIT.2, JIT.3, JIT.4, JIT.5, JIT.6, JIT.7, JIT.9, JIT.13, EJ. 20, EJ.21, JHA.3, JHA.4	Judicial One-Stop-Shop Portal
18	PR.18	Securely communicate and exchange information via digital means	Contact judges	Prosecutors/investigative judges	PR.14, PR.15, PR.16, PR.17,PR.19, PR.20, JIT.2, JIT.3, JIT.4, JIT.5, JIT.6, JIT.7, JIT.9, JIT.13, EJ. 20, EJ.21, JHA.3, JHA.4	Judicial One-Stop-Shop Portal
19	PR.19	Ease the process of setting up and operating JITs	Liaise with the rest of the JITs members	Prosecutors/investigative judges	PR.14, PR.15, PR.16, PR.17, PR.18, PR.20, JIT.2, JIT.3, JIT.4, JIT.5, JIT.6, JIT.7, JIT.9, JIT.13, EJ. 20, EJ.21, JHA.3, JHA.4	JIT Collaboration Platform
20	PR.20	Securely communicate and exchange information via digital means	Exchange information with the JITs members	Prosecutors/investigative judges	PR.3, PR.4, PR.5, PR.6, MOJ.1, MOJ.2; MOJ.3, MOJ.4, JIT.2, JIT.4, EJ.14, EJ.15, EJ.16, EJ.17, JHA.2,	JIT Collaboration Platform

					JHA.3	
21	PR.21	Identify links between cases	Identify links between my case and other cross-border cases	Prosecutors/investigative judges	EJ.1, EJ.2, EJ.3, EJ.4, EJ.5, JHA.1	Judicial Cases Cross-Check Exchange of data between JHA agencies and EU bodies (hit/no-hit)
22	PR.22	Identify links between cases	Have an overall overview on the status of my case	Prosecutors/investigative judges	PR.24, PR.33, EJ.18, EJ.19, EJ.22	Re-designed CMS
23	PR.23	Access digital support tools	Have information on which legal instrument I need to use	Prosecutors/investigative judges	PR.2, PR.27, PR.29	Training platform
24	PR.24	Identify links between cases	Have all the case-related information (sent or received) centralised	Prosecutors/investigative judges	PR.22, PR.33, EJ.18, EJ.19, EJ.22	Re-designed CMS
25	PR.25	Easily manage data and ensure its quality	Register automatically in the CMS the information included in the forms (like Art. 13 EJ Regulation)	Prosecutors/investigative judges	PR.30, EJ.10, EJ.11, EJ.23, EJ.24	Re-designed CMS
26	PR.26	Access digital support tools	Have a user-friendly stop-shop-portal with all the tools	Prosecutors/investigative judges	PR.28, PR.31, PR.32	Judicial One-Stop-Shop Portal
27	PR.27	Access digital support tools	Have access to handbooks, guidelines on the different procedures I need to conduct (e.g. request eEvidence)	Prosecutors/investigative judges	PR.2, PR.23, PR.29	Training platform
28	PR.28	Access digital support tools	Have access to different forums (e.g. from networks like EJN)	Prosecutors/investigative judges	PR.26, PR.31, PR.32	Judicial One-Stop-Shop Portal
29	PR.29	Access digital support tools	Have access to tutorials (videos) explaining how to access and use the one-stop-shop	Prosecutors/investigative judges	PR.2, PR.23, PR.27	Training platform
30	PR.30	Easily manage data and ensure its quality	Have an easy way to identify the different cases	Prosecutors/investigative judges	PR.25, EJ.10, EJ.11, EJ.23, EJ.24	Re-designed CMS
31	PR.31	Access digital support tools	Have a unique password allowing the log in and access to the different tools	Prosecutors/investigative judges	PR.26, PR.28, PR.32	Judicial One-Stop-Shop Portal Integration layer/Common Services Platform
32	PR.32	Access digital support tools	Access to the one-stop-shop portal from laptop and mobile devices	Prosecutors/investigative judges	PR.26, PR.28, PR.31	Judicial One-Stop-Shop Portal
33	PR.33	Identify links between cases	Emails exchange via outlook on a given case should be automatically saved in the CMS	Prosecutors/investigative judges	PR.22, PR.24, EJ.18, EJ.19, EJ.22	Re-designed CMS

34	PR.34	Identify links between cases	Need to be able to search in the CMS the information related to a given case (i.e. similar to the search functions in Outlook)	Prosecutors/investigative judges	EJ.6, EJ.7, EJ. 9	Re-designed CMS
35	PR.35	Ensure data protection principles for all systems	Receive notification from the CMS on the deadline to delete the data (data protection deadlines)	Prosecutors/investigative judges	PR.36, EJ.8, EJ.12, EJ.13	Re-designed CMS
36	PR.36	Ensure data protection principles for all systems	Delete the data, or extend the deadline for 1 year	Prosecutors/investigative judges	PR. 35, EJ.8, EJ.12, EJ.13	Re-designed CMS
37	PR.37	Ensure interoperability across systems	Use interoperable tools to ensure an efficient and seamless cooperation	Prosecutors/investigative judges	MOJ.5, JIT.20, EJ.29, JHA.5	Re-designed CMS Common Services Platform/Integration Layer Exchange of data between JHA agencies & EU bodies (hit/no-hit)
38	PR.38	Ensure interoperability across systems	Use a unique identifier for each case to ease their identification and avoid confusions	Prosecutors/investigative judges	MOJ.6, JIT.21, EJ.30, JHA.6	Secure communication channel Communication tool Re-designed CMS JIT Collaboration Platform
39	PR.39	Ensure interoperability across systems	Use a standardised data exchange format (e.g. UMF) that allows disparate systems to communicate data sets in a consistent manner, reducing complexity, data errors and improves processing overheads	Prosecutors/investigative judges	MOJ.7, JIT.22, EJ.31, JHA.7	Secure communication channel Communication tool Re-designed CMS JIT Collaboration Platform
40	PR.40	Easily manage data and ensure its quality	Ensure the quality of the data being exchanged	Prosecutors/investigative judges	MOJ.8, JIT.23, EJ.32, JHA.8	Secure communication channel Communication tool Re-designed CMS Large Files Solution
41	PR.41	Ensure data protection principles for all systems	Share data in compliance with data protection rules, as well as security and privacy standards	Prosecutors/investigative judges	MOJ.9, JIT.24, EJ.33, JHA.9	Secure communication channel Communication tool Re-designed CMS Judicial Cases Cross-Check Large Files Solution
42	MOJ.1	Securely communicate and exchange information via digital means	Send/receive requests and case related information via a fast and secure communication channel	Ministries of Justice	PR.3, PR.4, PR.5, PR.6, PR.20, MOJ.2, MOJ.3, MOJ.4, JIT.2, JIT.4, JHA.2, EJ.14, EJ.15, EJ.16, EJ.17, JHA.3	Secure communication channel Communication tool

43	MOJ.2	Securely communicate and exchange information via digital means	Send large amounts of data over a secure and digital communication channel	Ministries of Justice	PR.3, PR.4, PR.5, PR.6, PR.20, MOJ.1, MOJ.3, MOJ.4, JIT.2, JIT.4, EJ.14, EJ.15, EJ.16, EJ.17, JHA.2, JHA.3	Secure communication channel Large Files Solution
44	MOJ.3	Securely communicate and exchange information via digital means	Use the channel to send follow-up messages	Ministries of Justice	PR.3, PR.4, PR.5, PR.6, PR.20, MOJ.1, MOJ.2, MOJ.4, JIT.2, JIT.4, EJ.14, EJ.15, EJ.16, EJ.17, JHA.2, JHA.3	Communication tool
45	MOJ.4	Securely communicate and exchange information via digital means	Use the same communication channel to reach out the same stakeholders	Ministries of Justice	PR.3, PR.4, PR.5, PR.6, PR.20, MOJ.1, MOJ.2, MOJ.3, JIT.2, JIT.4, EJ.14, EJ.15, EJ.16, EJ.17, JHA.2, JHA.3	Secure communication channel
46	MOJ.5	Ensure interoperability across systems	Use interoperable tools to ensure an efficient and seamless cooperation	Ministries of Justice	PR.37, JIT.20, EJ.29, JHA.5	Re-designed CMS Common Services Platform/Integration Layer Exchange of data between JHA agencies & EU bodies (hit/no-hit)
47	MOJ.6	Ensure interoperability across systems	Use a unique identifier for each case to ease their identification and avoid confusions	Ministries of Justice	PR.38, JIT.21, EJ.30, JHA.6	Secure communication channel Communication tool Re-designed CMS JIT Collaboration Platform
48	MOJ.7	Ensure interoperability across systems	Use a standardised data exchange format (e.g. UMF) that allows disparate systems to communicate data sets in a consistent manner, reducing complexity, data errors and improves processing overheads	Ministries of Justice	PR.39, JIT.22, EJ.31, JHA.7	Secure communication channel Communication tool Re-designed CMS JIT Collaboration Platform
49	MOJ.8	Easily manage data and ensure its quality	Ensure the quality of the data being exchanged	Ministries of Justice	MOJ.8, JIT.23, EJ.32, JHA.8	Secure communication channel Communication tool Re-designed CMS Large Files Solution JIT Collaboration Platform
50	MOJ.9	Ensure data protection principles for all systems	Share data in compliance with data protection rules, as well as security and privacy standards	Ministries of Justice	PR.41, JIT.24, EJ.33, JHA.9	Secure communication channel Communication tool Re-designed CMS Large Files Solution

	MOJ.10	Ease the process of setting up and operating JITs	Need to speed up internal procedures (at MS level) to set up JIT and obtain signatures.	Ministries of Justice	JIT.1, JIT.5, JIT.6, JIT.8, JIT.11, JIT.12, JIT.13, JIT.14, JIT.15, JIT.16, JIT.18, JIT.19	JIT Collaboration Platform
51	JIT.1	Ease the process of setting up and operating JITs	Need a single point of communication in JITs (especially when more than two parties are involved).	JIT Members	JIT.5, JIT.6, JIT.8, JIT.11, JIT.12, JIT.13, JIT.14, JIT.15, JIT.16, JIT.18, JIT.19	JIT Collaboration Platform
52	JIT.2	Ease the process of setting up and operating JITs	Need to have a secure tool for law enforcement and judicial authorities to share and store information/documents, in conditions facilitating the traceability and admissibility of the evidence exchanged.	JIT Members	PR.3, PR.4, PR.5, PR.6, PR.20, MOJ.1, MOJ.2, MOJ.3, MOJ.4, JIT.4, EJ.14, EJ.15, EJ.16, EJ.17, JHA.2, JHA.3	JIT Collaboration Platform
53	JIT.3	Ease the process of setting up and operating JITs	Need for a tool to facilitate discussions/the exchange of messages between JIT partners.	JIT Members	PR.14, PR.15, PR.16, PR.17, PR.18, PR.19, PR.20, JIT.2, JIT.4, JIT.5, JIT.6, JIT.7, JIT.9, JIT.13, EJ. 20, EJ.21, JHA.3, JHA.4	JIT Collaboration Platform
54	JIT.4	Securely communicate and exchange information via digital means	Need to be able to exchange information in a digital and secure way.	JIT Members	PR.3, PR.4, PR.5, PR.6, PR.20, MOJ.1, MOJ.2; MOJ.3, MOJ.4, JIT.2, EJ.14, EJ.15, EJ.16, EJ.17, JHA.2, JHA.3	JIT Collaboration Platform
55	JIT.5	Ease the process of setting up and operating JITs	Need to be able to make decisions in real time.	JIT Members	JIT.1, JIT.6, JIT.8, JIT.11, JIT.12, JIT.13, JIT.14, JIT.15, JIT.16, JIT.18, JIT.19	JIT Collaboration Platform
56	JIT.6	Ease the process of setting up and operating JITs	Need to be able to share tasks with other JIT members (e.g. to collaborate and send together an MLA towards a third state not involved in a JIT).	JIT Members	JIT.1, JIT.5, JIT.8, JIT.11, JIT.12, JIT.13, JIT.14, JIT.15, JIT.16, JIT.18, JIT.19	JIT Collaboration Platform
57	JIT.7	Ease the process of setting up and operating JITs	Need to be able to communicate with Eurojust.	JIT Members	PR.14, PR.15, PR.16, PR.17, PR.18, PR.19, PR.20, JIT.2, JIT.3, JIT.4, JIT.5, JIT.6, JIT.9, JIT.13, EJ. 20, EJ.21, JHA.3, JHA.4	JIT Collaboration Platform
58	JIT.8	Ease the process of setting up and operating JITs	Need to be able to evaluate a JIT.	JIT Members	JIT.1, JIT.5, JIT.6, JIT.11, JIT.12, JIT.13, JIT.14, JIT.15, JIT.16, JIT.18, JIT.19	JIT admin tool
59	JIT.9	Ease the process of setting up and operating JITs	Need a tool for instant messaging/communication with JIT partners.	JIT Members	PR.14, PR.15, PR.16, PR.17, PR.18, PR.19, PR.20, JIT.2, JIT.3, JIT.4, JIT.5, JIT.6, JIT.7, JIT.13, EJ. 20, EJ.21, JHA.3, JHA.4	JIT Collaboration Platform
60	JIT.10	Access digital support tools	Need for a mean to identify relevant JIT partners in other EU Member States or Third States.	JIT Members	PR.1	JIT Collaboration Platform

61	JIT.11	Ease the process of setting up and operating JITs	Need to find information about domestic rules regarding the setting up of a JIT.	JIT Members	JIT.1, JIT.5, JIT.6, JIT.8, JIT.12, JIT.13, JIT.14, JIT.15, JIT.16, JIT.18, JIT.19	JIT Collaboration Platform
62	JIT.12	Ease the process of setting up and operating JITs	Need to speed up internal procedures (at MS level) to set up JIT and obtain signatures.	JIT Members	MOJ.10, JIT.1, JIT.5, JIT.6, JIT.8, JIT.11, JIT.13, JIT.14, JIT.15, JIT.16, JIT.18, JIT.19	JIT Collaboration Platform
63	JIT.13	Ease the process of setting up and operating JITs	Need to plan and organise meetings (JIT meetings).	JIT Members	JIT.1, JIT.5, JIT.6, JIT.8, JIT.11, JIT.12, JIT.14, JIT.15, JIT.16, JIT.18, JIT.19	JIT Collaboration Platform
64	JIT.14	Ease the process of setting up and operating JITs	Need to plan and organise meetings related to action days.	JIT Members	JIT.1, JIT.5, JIT.6, JIT.8, JIT.11, JIT.12, JIT.13, JIT.15, JIT.16, JIT.18, JIT.19	Re-designed CMS (Action Days Collaboration Platform)
65	JIT.15	Ease the process of setting up and operating JITs	Need the possibility to establish/maintain the JIT during and after the trial phase.	JIT Members	JIT.1, JIT.5, JIT.6, JIT.8, JIT.11, JIT.12, JIT.13, JIT.14, JIT.16, JIT.18, JIT.19	JIT Collaboration Platform
66	JIT.16	Ease the process of setting up and operating JITs	Need to set up coordination centres at Eurojust for common action days to facilitate cooperation during simultaneous operations.	JIT Members	JIT.1, JIT.5, JIT.6, JIT.8, JIT.11, JIT.12, JIT.13, JIT.14, JIT.15, JIT.18, JIT.19	Re-designed CMS (Action Days Collaboration Platform)
67	JIT.17	Access digital support tools	Need to translate documentary evidence between a common working language (e.g. English).	JIT Members	PR.12, EJ.25, EJ.26	Redesigned Eurojust CMS eTranslation (CEF Building Block)
68	JIT.18	Ease the process of setting up and operating JITs	Exchange information with the action days participants	JIT Members	JIT.1, JIT.5, JIT.6, JIT.8, JIT.11, JIT.12, JIT.13, JIT.14, JIT.15, JIT.16, JIT.19	Re-designed CMS (Action Days Collaboration Platform)
69	JIT.19	Ease the process of setting up and operating JITs	Contact (incl. instant messaging) with the rest of action days participants via a secure communication channel	JIT Members	JIT.1, JIT.5, JIT.6, JIT.8, JIT.11, JIT.12, JIT.13, JIT.14, JIT.15, JIT.16, JIT.18	Re-designed CMS (Action Days Collaboration Platform)
70	JIT.20	Ensure interoperability across systems	Use interoperable tools to ensure an efficient and seamless cooperation	JIT Members	PR.37, MOJ.5, EJ.29, JHA.5	Re-designed CMS Common Services Platform/Integration Layer Exchange of data between JHA agencies & EU bodies (hit/no-hit)
71	JIT.21	Ensure interoperability across systems	Use a unique identifier for each case to ease their identification and avoid confusions	JIT Members	PR.38, MOJ.6, EJ.30, JHA.6	Secure communication channel Communication tool Re-designed CMS JIT Collaboration Platform
72	JIT.22	Ensure interoperability across systems	Use a standardised data exchange format (e.g. UMF) that allows disparate systems to communicate data sets in a consistent manner, reducing complexity, data errors and improves processing overheads	JIT Members	PR.39, MOJ.7, EJ.31, JHA.7	Secure communication channel Communication tool Re-designed CMS JIT Collaboration Platform

73	JIT.23	Easily manage data and ensure its quality	Ensure the quality of the data being exchanged	JIT Members	PR.40, MOJ.8, EJ.32, JHA.8	Secure communication channel Communication tool JIT Collaboration Platform Large Files Solution JIT Collaboration Platform
74	JIT.24	Ensure data protection principles for all systems	Share data in compliance with data protection rules, as well as security and privacy standards	JIT Members	PR.41, MOJ.9, EJ.33, JHA.9	Secure communication channel Communication tool Re-designed CMS Large Files Solution JIT Collaboration Platform
75	EJ.1	Identify links between cases	Need to be able to cross-check against the data in the Eurojust CMS if there is (or has been) an investigation ongoing about a case linked to the one I am currently coordinating.	Eurojust	PR.21, EJ.2, EJ.3, EJ.4, EJ.5, JHA.1	Exchange of data between JHA agencies and EU bodies (hit/no-hit)
76	EJ.2	Identify links between cases	Need to be able to cross-check against the data in the EPPO CMS if there is (or has been) an investigation ongoing about a case linked to the one I am currently coordinating.	Eurojust	PR.21, EJ.1, EJ.3, EJ.4, EJ.5, JHA.1	Exchange of data between JHA agencies and EU bodies (hit/no-hit)
77	EJ.3	Identify links between cases	Need to be able to cross-check against the data in the Europol CMS if there is (or has been) an investigation ongoing about a case linked to the case I am currently coordinating.	Eurojust	PR.21, EJ.1, EJ.2, EJ.4, EJ.5, JHA.1	Exchange of data between JHA agencies and EU bodies (hit/no-hit)
78	EJ.4	Identify links between cases	Need to be able to cross-check against the data in the ECRIS-TCN / SISII for the criminal records of the suspect(s) of the case I am currently coordinating.	Eurojust	PR.21, EJ.1, EJ.2, EJ.3, EJ.5, JHA.1	Exchange of data between JHA agencies and EU bodies (hit/no-hit)
79	EJ.5	Identify links between cases	Need to be able to cross-check against the data in the SIS database for elements on the suspect(s) of the case I am currently coordinating.	Eurojust	PR.21, EJ.1, EJ.2, EJ.3, EJ.4, JHA.1	Exchange of data between JHA agencies and EU bodies (hit/no-hit)
80	EJ.6	Identify links between cases	Need to be able to search in the CIF database (part of the Eurojust CMS) how similar cases to the one I am working on were handled in the past.	Eurojust	PR.34, EJ.7, EJ. 9	Re-designed CMS
81	EJ.7	Identify links between cases	Need to be able to easily search the content of messages and files attached to a case that I am authorised to see (including pdf documents, etc.).	Eurojust	PR.34, EJ.6, EJ. 9	Re-designed CMS
82	EJ.8	Ensure data protection principles for all systems	Need to be able to easily manage the access rights related to the cases that I have entered into the Eurojust CMS. All information should be shared on a 'need to know' basis.	Eurojust	PR. 35, PR.36, EJ.12, EJ.13	Re-designed CMS
83	EJ.9	Identify links between cases	Need for the data in the Counter-Terrorism register to be recorded, accessed and searched in the Eurojust CMS (given that I have the right to	Eurojust	PR.34, EJ.6, EJ.7	Re-designed CMS

			access the data).			
84	EJ.10	Easily manage data and ensure its quality	Need to be able to extract analyses and reports from the Eurojust CMS.	Eurojust	PR.25, PR.30, EJ.11, EJ.23, EJ.24	Re-designed CMS
85	EJ.11	Easily manage data and ensure its quality	Need to be able to carry out data management and data quality activities on the data in the Eurojust CMS.	Eurojust	PR.25, PR.30, EJ.10, EJ.23, EJ.24	Re-designed CMS
86	EJ.12	Ensure data protection principles for all systems	Need to ensure the Eurojust CMS enables the respect of the data protection rules of procedure followed by Eurojust.	Eurojust	PR. 35, PR.36, EJ.8, EJ.13	Re-designed CMS
87	EJ.13	Ensure data protection principles for all systems	Need for the security and privacy of the data registered in the Eurojust CMS to be ensured.	Eurojust	PR. 35, PR.36, EJ.8, EJ.12	Re-designed CMS
88	EJ.14	Securely communicate and exchange information via digital means	Need to be able to easily exchange large volumes of information with all stakeholders that I collaborate with.	Eurojust	PR.3, PR.4, PR.5, PR.6, PR.20, MOJ.1, MOJ.2, MOJ.3, MOJ.4, JIT.2, JIT.4, EJ.15, EJ.16, EJ.17, JHA.2, JHA.3	Secure communication channel Large Files Solution
89	EJ.15	Securely communicate and exchange information via digital means	Need to be able to easily exchange data in different formats (incl. eEvidence).	Eurojust	PR.3, PR.4, PR.5, PR.6, PR.20, MOJ.1, MOJ.2; MOJ.3, MOJ.4, JIT.2, JIT.4, EJ.14, EJ.16, EJ.17, JHA.2, JHA.3	Secure communication channel Communication tool
90	EJ.16	Securely communicate and exchange information via digital means	Need to be able to exchange unclassified information (including sensitive information) through a secure and encrypted communication channel with Eurojust National Desks and EJN secretariat, stakeholders in my home country and /or officers in other JHA agencies and EU bodies	Eurojust	PR.3, PR.4, PR.5, PR.6, PR.20, MOJ.1, MOJ.2; MOJ.3, MOJ.4, JIT.2, JIT.4, EJ.14, EJ.15, EJ.17, JHA.2, JHA.3	Secure communication channel Communication tool
91	EJ.17	Securely communicate and exchange information via digital means	Need to be able to exchange classified information through a secure and encrypted communication channel (that is compliant with the 'EU-Restricted' accreditation) with Eurojust National Desks, stakeholders in my home country and /or officers in other JHA agencies and EU bodies	Eurojust	PR.3, PR.4, PR.5, PR.6, PR.20, MOJ.1, MOJ.2; MOJ.3, MOJ.4, JIT.2, JIT.4, EJ.14, EJ.15, EJ.16, JHA.2, JHA.3	Secure communication channel Communication tool
92	EJ.18	Identify links between cases	Need to centralise all information, messages, and documents about a case I am working on in the Eurojust CMS, that would be accessible through a 'digital workspace'-like user interface.	Eurojust	PR.22, PR.24, PR.33, EJ.19, EJ.22	Re-designed CMS
93	EJ.19	Identify links between cases	Need to be able to keep track of the status of the cases I am working on, as well as of the follow-up actions to be carried out (e.g. through reminders or notifications).	Eurojust	PR.22, PR.24, PR.33, EJ.18, EJ.22	Re-designed CMS

94	EJ.20	Ease the process of setting up and operating JITs	Need to be able to easily exchange messages with the members of the JIT I am working on.	Eurojust	PR.14, PR.15, PR.16, PR.17, PR.18, PR.19, PR.20, JIT.2, JIT.3, JIT.4, JIT.5, JIT.6, JIT.7, JIT.9, JIT.13, EJ.21, JHA.3, JHA.4	JIT Collaboration Platform
95	EJ.21	Ease the process of setting up and operating JITs	Need a tool for instant messaging/communication with JIT partners.	Eurojust	PR.14, PR.15, PR.16, PR.17, PR.18, PR.19, PR.20, JIT.2, JIT.3, JIT.4, JIT.5, JIT.6, JIT.7, JIT.9, JIT.13, EJ. 20, JHA.3, JHA.4	JIT Collaboration Platform
96	EJ.22	Identify links between cases	Need to be able to easily and rapidly record the information about a case that is sent to National Desks into the Eurojust CMS (including the extraction of case entities).	Eurojust	PR.22, PR.24, PR.33, EJ.18, EJ.19	Re-designed CMS
97	EJ.23	Easily manage data and ensure its quality	Need to be able to easily and rapidly record information about a closed CMS case into the CIF database.	Eurojust	PR.25, PR.30, EJ.10, EJ.11, EJ.24	Re-designed CMS
98	EJ.24	Easily manage data and ensure its quality	Need for data quality of the data entered into the CMS to be checked	Eurojust	PR.25, PR.30, EJ.10, EJ.11, EJ.23	Re-designed CMS
99	EJ.25	Access digital support tools	Need for the certain (pieces of) document to be automatically translated, in a good-quality translation, for me to send them to other National Desks for information.	Eurojust	PR.12, JIT.17, EJ.26	Redesigned Eurojust CMS eTranslation (CEF Building Block)
100	EJ.26	Access digital support tools	Need for information about case entities and metadata to be automatically translated into English in the Eurojust CMS.	Eurojust	PR.12, JIT.17, EJ.25	Redesigned Eurojust CMS eTranslation (CEF Building Block)
101	EJ.27	Access digital support tools	Electronically sign the documents to be sent in order to authenticate them	Eurojust	PR.8, PR.9, EJ.28	Redesigned Eurojust CMS eSignature (CEF Building Block)
102	EJ.28	Access digital support tools	Receive the documents electronically signed to be certain of their authenticity	Eurojust	PR.8, PR.9, EJ.27	Redesigned Eurojust CMS eSignature (CEF Building Block)
103	EJ.29	Ensure interoperability across systems	Use interoperable tools to ensure an efficient and seamless cooperation	Eurojust	PR.37, MOJ.5, JIT.20, JHA.5	Re-designed CMS Common Services Platform/Integration Layer Exchange of data between JHA agencies & EU bodies (hit/no-hit)
104	EJ.30	Ensure interoperability across systems	Use a unique identifier for each case to ease their identification and avoid confusions	Eurojust	PR.38, MOJ.6, JIT.21, JHA.6	Secure communication channel Communication tool Re-designed CMS JIT Collaboration Platform

105	EJ.31	Ensure interoperability across systems	Use a standardised data exchange format (e.g. UMF) that allows disparate systems to communicate data sets in a consistent manner, reducing complexity, data errors and improves processing overheads	Eurojust	PR.39, MOJ.7, JIT.22, JHA.7	Secure communication channel Communication tool Re-designed CMS JIT Collaboration Platform
106	EJ.32	Easily manage data and ensure its quality	Ensure the quality of the data being exchanged	Eurojust	PR.40, MOJ.8, JIT.23, JHA.8	Secure communication channel Communication tool Exchange of data between JHA agencies & EU bodies (hit/no-hit) Large Files Solution
107	EJ.33	Ensure data protection principles for all systems	Share data in compliance with data protection rules, as well as security and privacy standards	JIT Members	PR.41, MOJ.9, JIT.24, JHA.9	Secure communication channel Communication tool Re-designed CMS Large Files Solution
108	JHA.1	Identify links between cases	Exchange information with Eurojust (hit/no-hit between our systems)	JHA Agencies and EU bodies	PR.21, EJ.1, EJ.2, EJ.3, EJ.4, EJ.5	Exchange of data between JHA agencies and EU bodies (hit/no-hit)
109	JHA.2	Securely communicate and exchange information via digital means	Exchange case-related information with Eurojust/Frontex/Europol/OLAF/the EPPO via a digital and secure communication channel	JHA Agencies and EU bodies	PR.3, PR.4, PR.5, PR.6, PR.20, MOJ.1, MOJ.2; MOJ.3, MOJ.4, JIT.2, JIT.4, EJ.14, EJ.15, EJ.16, EJ.17, JHA.3	Secure communication channel Communication tool
110	JHA.3	Ease the process of setting up and operating JITs	Exchange information with the JITs members via a secure communication channel	JHA Agencies and EU bodies	PR.3, PR.4, PR.5, PR.6, PR.20, MOJ.1, MOJ.2; MOJ.3, MOJ.4, JIT.2, JIT.4, EJ.14, EJ.15, EJ.16, EJ.17, JHA.2	JIT Collaboration Platform
111	JHA.4	Ease the process of setting up and operating JITs	Contact (incl. instant messaging) the rest of the JITs members via a secure communication channel	JHA Agencies and EU bodies	PR.14, PR.15, PR.16, PR.17, PR.18, PR.19, PR.20, JIT.2, JIT.3, JIT.4, JIT.5, JIT.6, JIT.7, JIT.9, JIT.13, EJ. 20, EJ.21, JHA.3	JIT Collaboration Platform
112	JHA.5	Ensure interoperability across systems	Use interoperable tools to ensure an efficient and seamless cooperation	JHA Agencies and EU bodies	PR.37, MOJ.5, JIT.20, EJ.29	Re-designed CMS Common Services Platform/Integration Layer Exchange of data between JHA agencies & EU bodies (hit/no-hit)
113	JHA.6	Ensure interoperability across systems	Use a unique identifier for each case to ease their identification and avoid confusions	JHA Agencies and EU bodies	PR.38, MOJ.6, JIT.21, EJ.30	Secure communication channel Communication tool Re-designed CMS JIT Collaboration Platform

114	JHA.7	Ensure interoperability across systems	Use a standardised data exchange format (e.g. UMF) that allows disparate systems to communicate data sets in a consistent manner, reducing complexity, data errors and improves processing overheads	JHA Agencies and EU bodies	PR.39, MOJ.7, JIT.22, EJ.31	Secure communication channel Communication tool Re-designed CMS JIT Collaboration Platform
115	JHA.8	Easily manage data and ensure its quality	Ensure the quality of the data being exchanged	JHA Agencies and EU bodies	PR.40, MOJ.8, JIT.23, EJ.32	Secure communication channel Communication tool Exchange of data between JHA agencies & EU bodies (hit/no-hit) Large Files Solution
116	JHA.9	Ensure data protection principles for all systems	Share data in compliance with data protection rules, as well as security and privacy standards	JHA Agencies and EU bodies	PR.41, MOJ.9, JIT.24, EJ.33	Secure communication channel Communication tool Re-designed CMS Large Files Solution

Annex D | Legal instruments

The table below presents the legal instruments established at EU level for judicial cooperation in criminal matters.

Table 52: Legal instruments for judicial cooperation in criminal matters

Legal instrument	Stage of the procedure	Form to be exchanged (Yes, No)	If No, how information is exchanged:	Channel used to exchange the information:	Information exchanged	Authority involved
Council Decision 2005/671/JHA of 20 September 2005 on the exchange of information and cooperation concerning terrorist offences	All stages	No	*Not defined*	*Not specified*	Art. 2(4): The information to be transmitted in accordance with paragraph 3 to Europol shall be the following: (a) data which identify the person, group or entity; (b) acts under investigation and their specific circumstances; (c) the offence concerned; (d) links with other relevant cases; (e) the use of communication technologies; (f) the threat posed by the possession of weapons of mass destruction	• Specialised service within its police services/law enforcement authorities • One authority, or an appropriate judicial or other competent authority
Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union	Investigation	Yes	*Not applicable*	Via any existing channel for international law enforcement cooperation	Art.(d) (i): Any type of information or data which is held by law enforcement authorities (ii) Any type of information or data, which is held by public enforcement authorities or by private entities and which is available to law enforcement authorities without the taking of coercive measures, in accordance with article 1(5).	Law enforcement authorities
Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters of 3 April 2015	Investigation	Yes	*Not applicable*	Any possible or relevant means of transmission, e.g. the secure telecommunications system of the European Judicial Network, Eurojust, or other channels used by judicial or law enforcement	Art. 5(1): The EIO shall, in particular, contain the following information: (a) data about the issuing authority and, where applicable, the validating authority; (b) the object of and reasons for the EIO; (c) the necessary information available on the person(s) concerned; (d) a description of the criminal act, which is the subject of the investigation or proceedings, and the applicable provisions of the criminal law of the issuing State; (e) a description of the investigative measures(s) requested	• Issuing authority: judge, court, investigating judge or public prosecutor; or any other competent authority • Executing authority: authority having competence to recognise an EIO

Legal instrument	Stage of the procedure	Form to be exchanged (Yes, No)	If No, how information is exchanged:	Channel used to exchange the information:	Information exchanged	Authority involved
				authorities	and the evidence to be obtained	
Council Regulation 2185/96 of 11 November 1996 concerning on-the-spot checks and inspections carried out by the Commission in order to protect the European Communities' financial interests against fraud and other irregularities	Investigation	No, but information notified by the Commission shall be in written (Art. 6)	*Not defined*	*Not specified*	The Commission shall notify the object, purpose, and legal basis of the checks and inspections. The Commission shall report to the competent authority of the State any fact or suspicion relating to an irregularity. In any event, the Commission shall be required to inform the aforementioned authority of the result of such checks and inspections. The following material and supporting documents shall be annexed to the said reports (Art. 7): (a) professional books and documents such as invoices, lists of terms and conditions, pay slips, statements of materials used and work done, and bank statements held by economic operators, (b) computer data, (c) production, packaging and dispatching systems and methods, (d) physical checks as to the nature and quantity of goods or completed operations, (e) the taking and checking of samples, (f) the progress of works and investments for which financing has been provided, and the use made of completed investments, (g) budgetary and accounting documents, (h) the financial and technical implementation of subsidized projects	• European Commission's inspectors • Member States authorities
Council Decision 2009/917/JHA of 30 November 2009 on the use of information technology for customs purposes	Prevention, Investigation and prosecution	No	Customs Information System	Anti-Fraud Information System (AFIS)	Art. 1 (2): The aim of the Customs Information System, in accordance with this Decision, shall be to assist in preventing, investigating and prosecuting serious contraventions of national laws by making information available more rapidly, thereby increasing the effectiveness of the cooperation and control procedures of the customs administrations of the Member States. Art. 3: The Customs Information System shall consist of a central database facility, accessible through terminals in each Member State. It shall comprise exclusively data necessary to achieve its aim as stated in Article 1(2), including personal data, in the following categories:	• Competent authorities of the Member States, EUROJUST and EUROPOL

Legal instrument	Stage of the procedure	Form to be exchanged (Yes, No)	If No, how information is exchanged:	Channel used to exchange the information:	Information exchanged	Authority involved
					(a) commodities; (b) means of transport; (c) businesses; (d) persons; (e) fraud trends; (f) availability of expertise; (g) items detained, seized or confiscated; (h) cash detained, seized or confiscated. 2. The Commission shall ensure the technical management of the infrastructure of the Customs Information System in accordance with the rules provided for by the implementing measures adopted by the Council. Art. 5. Data in the categories referred to in Article 3(1)(a) to (g) shall be entered into the Customs Information System only for the purpose of sighting and reporting, discreet surveillance, specific checks and strategic or operational analysis. Data in the category referred to in Article 3(1)(h) shall be entered into the Customs Information System only for the purpose of strategic or operational analysis. Art. 11: 1. Europol shall, within its mandate and for the fulfilment of its tasks, have the right to have access to the data entered into the Customs Information System in accordance with Articles 1, 3 to 6 and 15 to 19 and to search those data. 2. Where a search by Europol reveals the existence of a match between information processed by Europol and an entry in the Customs Information System, Europol shall, through the channels defined in Council Decision 2009/371/JHA of 6 April 2009 establishing a European Police Office (Europol) (1), inform the Member State which made the entry. 3. Use of information obtained from a search in the Customs Information System is subject to the consent of the Member State which entered the data into the System. If that Member State allows the use of such information, the handling thereof shall be governed by the Decision 2009/371/JHA. Europol may transfer such information to third countries and	

Legal instrument	Stage of the procedure	Form to be exchanged (Yes, No)	If No, how information is exchanged:	Channel used to exchange the information:	Information exchanged	Authority involved
					third bodies only with the consent of the Member State which entered the data into the System. Article 12 1. The national members of Eurojust, their deputies, assistants and specifically authorised staff shall, within their mandate and for the fulfilment of Eurojust's tasks, have the right to have access to the data entered into the Customs Information System in accordance with Articles 1, 3 to 6 and 15 to 19 and to search those data. 2. Where a search by a national member of Eurojust, their deputies, assistants or specifically authorised staff reveals the existence of a match between information processed by Eurojust and an entry in the Customs Information System, he or she shall inform the Member State which made the entry. Any communication of information obtained from such a search may be communicated to third countries and third bodies only with the consent of the Member State which made the entry. CHAPTER VI CREATION OF A CUSTOMS FILES IDENTIFICATION DATABASE Article 15 1. The Customs Information System shall contain data in accordance with this Chapter, in addition to data contained in accordance with Article 3, in a special database (hereinafter referred to as the customs files identification database). … 2. The aim of the customs files identification database shall be to enable the national authorities responsible for carrying out customs investigations designated pursuant to Article 7, when opening a file on or investigating one or more persons or businesses, and for Europol and Eurojust, to identify competent authorities of other Member States which are investigating or have investigated those persons or businesses, in order, through information on the existence of investigation files, to achieve the aim referred to in Article 1(2). CHAPTER VII OPERATION AND USE OF THE CUSTOMS FILES	

Legal instrument	Stage of the procedure	Form to be exchanged (Yes, No)	If No, how information is exchanged:	Channel used to exchange the information:	Information exchanged	Authority involved
					IDENTIFICATION DATABASE Article 16 1. Data from investigation files will be entered into the customs files identification database only for the purposes set out in Article 15(2). The data shall only cover the following categories: (a) a person or a business which is or has been the subject of an investigation file opened by a competent authority of a Member State, and which: (i) in accordance with the national law of the Member State concerned, is suspected of committing or having committed, or participating or having participated in the commission of, a serious infringement of national laws; (ii) has been the subject of a report establishing that such an infringement has taken place; or (iii) has been the subject of an administrative or judicial sanction for such an infringement; (b) the field covered by the investigation file; (c) the name, nationality and contact information of the Member State's authority handling the case, together with the file number. Data referred to in points (a) to (c) shall be entered in a data record separately for each person or business. Links between data records shall not be permitted. 2. The personal data referred to in paragraph 1(a) shall consist of only the following: (a) for persons: name, maiden name, forenames, former surnames and aliases, date and place of birth, nationality and sex; (b) for businesses: business name, name under which trade is conducted, address, VAT identifier and excise duties identification number.	
Council Regulation (EC) No 515/97 of 13 March 1997 on mutual assistance between the administrative authorities of the Member States	Prevention Investigation	No	Customs Information System	*Not specified*	National authorities shall communicate (Art. 3): (a) any information thus obtained concerning the application of customs and agricultural legislation, or at least (b) that part of the file required to put a stop to a fraudulent practice	Competent authorities of the Member States, and designated Commission departments

Legal instrument	Stage of the procedure	Form to be exchanged (Yes, No)	If No, how information is exchanged:	Channel used to exchange the information:	Information exchanged	Authority involved
and cooperation between the latter and the Commission to ensure the correct application of the law on customs and agricultural matters					The requested authority shall transmit to it any information which may enable it to ensure compliance with the provisions of customs or agricultural legislation, and in particular those concerning (Art. 4): (a) the application of customs duties and charges having equivalent effect together with agricultural levies and other charges provided for under the common agricultural policy or the special arrangements applicable to certain goods resulting from the processing of agricultural products, (b) operations forming part of the system of financing by the European Agricultural Guidance and Guarantee Fund At the request of the applicant authority, the requested authority shall supply it with any attestation, document or certified true copy of a document in its possession or obtained in the manner referred to in Article 4 (2) which relates to operations covered by customs or agricultural legislation (Art. 5). Article 7: At the request of the applicant authority, the requested authority shall as far as possible keep a special watch or arrange for a special watch to be kept within its operational area: (a) on persons, and more particularly their movements, where there are reasonable grounds for believing that they are breaching customs or agricultural legislation; (b) on places where goods are stored in a way that gives grounds to suspect that they are intended to supply operations contrary to customs or agricultural legislation; (c) on the movements of goods indicated as being the object of potential breaches of customs or agricultural legislation; (d) on means of transport, where there are reasonable grounds for believing that they are being used to carry out operations in breach of customs or agricultural legislation. At the request of the applicant authority, the requested authority shall make available any information in its possession or obtained in the manner referred to in Article 4 (2), and particularly reports and other documents or certified true copies or extracts thereof, concerning operations detected or planned which constitute, or	

Legal instrument	Stage of the procedure	Form to be exchanged (Yes, No)	If No, how information is exchanged:	Channel used to exchange the information:	Information exchanged	Authority involved
					appear to the applicant authority to constitute, breaches of customs or agricultural legislation or, where applicable, concerning the findings of the special watch carried out pursuant to Article 7 (Art. 8). The requested authority shall communicate the results of such administrative enquiries to the applicant authority (Art. 9(2)). The competent authorities of each Member State shall immediately send to the competent authorities of the other Member States concerned all relevant information concerning operations which constitute, or appear to them to constitute, breaches of customs or agricultural legislation, and in particular concerning the goods involved and new ways and means of carrying out such operations (Art. 15) Art. 23 : 1. An automated information system, the 'Customs Information System', hereinafter referred to as the 'CIS', is hereby established to meet the requirements of the administrative authorities responsible for applying the legislation on customs or agricultural matters, as well as those of the Commission. 2. The aim of the CIS, in accordance with the provisions of this Regulation, shall be to assist in preventing, investigating and prosecuting operations which are in breach of customs or agricultural legislation by making information available more rapidly and thereby increasing the effectiveness of the cooperation and control procedures of the competent authorities referred to in this Regulation. The items to be included in the Customs Information System (CIS) are determined by the COMMISSION IMPLEMENTING REGULATION (EU) 2016/346 of 10 March 2016 Art. 25: Items to be included in CIS in respect of personal data shall comprise no more than: (a) name, maiden name, forenames and aliases; (b) date and place of birth; (c) nationality;	

Legal instrument	Stage of the procedure	Form to be exchanged (Yes, No)	If No, how information is exchanged:	Channel used to exchange the information:	Information exchanged	Authority involved
					(d) sex; (e) any particular objective and permanent physical characteristics; (f) reason for inclusion of data; (g) suggested action; (h) a warning code indicating any history of being armed, violent or escaping; (i) registration number of the means of transport. TITLE Va CUSTOMS FILES IDENTIFICATION DATABASE Chapter 1 Establishment of a customs files identification database Article 41a: 1. The CIS shall also include a specific database called the 'Customs files identification database' (FIDE). Subject to the provisions of this Title, all the provisions of this Regulation relating to the CIS shall also apply to the FIDE, and any reference to the CIS shall include that database. 2. The objectives of the FIDE shall be to help to prevent operations in breach of customs legislation and of agricultural legislation applicable to goods entering or leaving the customs territory of the Community and to facilitate and accelerate their detection and prosecution. Article 41b: Operation and use of the FIDE 1. The competent authorities may enter data from investigation files in the FIDE for the purposes defined in Article 41a(3) concerning cases which are in breach of customs legislation or agricultural legislation applicable to goods entering or leaving the customs territory of the Community and which are of particular relevance at Community level. The data shall cover only the following categories: (a) persons and businesses which are or have been the subject of an administrative enquiry or a criminal investigation by the relevant service of a Member State, and — are suspected of committing or of having committed a breach of customs or agriculture legislation or of participating in or of having participated in an operation in breach of such	

Legal instrument	Stage of the procedure	Form to be exchanged (Yes, No)	If No, how information is exchanged:	Channel used to exchange the information:	Information exchanged	Authority involved
					legislation, — have been the subject of a finding relating to such an operation, or — have been the subject of an administrative decision or an administrative penalty or judicial penalty for such an operation; (b) the field concerned by the investigation file; (c) the name, nationality and details of the relevant service in the Member State and the file number. The data referred to in points (a), (b) and (c) shall be introduced separately for each person or business. The creation of links between those data shall be prohibited. 2. The personal data referred to in paragraph 1(a) shall consist only of the following: (a) for persons: the name, maiden name, forename, former surnames and alias, date and place of birth, nationality and sex; (b) for businesses: the business name, trading name, address of the business, VAT identification number and excise duties identification number. Article 41c: 1. The introduction and consultation of data in the FIDE shall be reserved exclusively to the authorities referred to in Article 41a. 2. Any consultation of the FIDE must specify the following personal data: (a) for persons: the forename and/or name and/or maiden name and/or former surnames and/or alias and/or date of birth; (b) for businesses: the business name and/or trading name and/or VAT identification number and/or excise duties identification number.	
Regulation (EU) 2018/1805 of the European Parliament and of the Council of 14 November 2018 on the mutual recognition of freezing and confiscation orders	Execution judgment	Yes	*Not applicable*	*Not specified*	The freezing certificate shall: (a) be accompanied by a confiscation certificate transmitted in accordance with Article 14; or (b) contain an instruction that the property is to remain frozen in the executing State pending the transmission and execution of the confiscation order in accordance with Article 14, in which case the issuing authority shall indicate the estimated date of this transmission in the freezing certificate.	• Issuing authority means: (a) in respect of a freezing order: (i) a judge, court, or public prosecutor competent in the case concerned; or ii) another competent authority which is designated as such by the issuing State and which is competent in criminal matters to order the freezing of property or to execute a freezing order in accordance with national law. • Executing authority

Legal instrument	**Stage of the procedure**	**Form to be exchanged (Yes, No)**	**If No, how information is exchanged:**	**Channel used to exchange the information:**	**Information exchanged**	**Authority involved**
Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings	Trial	No	Any means whereby a written record can be produced (Art. 7)	*Not specified*	(a) the contact details of the competent authority; (b) a description of the facts and circumstances that are the subject of the criminal proceedings concerned; (c) all relevant details about the identity of the suspected or accused person and about the victims, if applicable; (d) the stage that has been reached in the criminal proceedings; and (e) information about provisional detention or custody of the suspected or accused person, if applicable.	Judges
Council Framework Decision 2009/829/JHA, on the application, between Member States of the European Union, of the principle of mutual recognition to decisions on supervision measures as an alternative to provisional detention	All stages	Yes	*Not applicable*	*Not specified*	• A decision on supervision measures may be forwarded, accompanied by a certificate, the standard form set out in Annex I. • Reasons why a supervision measure is rejected. • Reasons justifying whether a monitoring of the measures is still needed.	Competent Judicial Authorities
Council Framework Decision 2008/947/JHA, on the application of the principle of mutual recognition to judgments and probation decisions with a view to the supervision of probation measures and alternative sanctions	Execution judgment	Yes	*Not applicable*	*Not specified*	The form of the certificate is drafted in such a way so that the essential elements of the judgement and, where applicable, of the probation decision are comprised in the certificate, which should be translated into the official language or one of the official languages of the executing State.	• Issuing States • Executing States
Council Framework Decision 2008/909/JHA of 27 November 2008 on the application of the principle of mutual recognition to judgments in criminal matters imposing custodial sentences or measures involving deprivation of	Execution judgment	Yes	*Not applicable*	*Not specified*	1. The competent authority of the issuing State shall forthwith inform the competent authority of the executing State of any decision or measure as a result of which the sentence ceases to be enforceable immediately or within a certain period of time. 2. The competent authority of the executing State shall terminate enforcement of the sentence as soon as it is informed by the competent authority of the issuing State of the decision or measure referred to in paragraph 1. The competent authority of the executing State shall without	• Issuing States • Executing States

Legal instrument	Stage of the procedure	Form to be exchanged (Yes, No)	If No, how information is exchanged:	Channel used to exchange the information:	Information exchanged	Authority involved
liberty for the purpose of their enforcement in the European Union					delay inform the competent authority of the issuing State by any means which leaves a written record: (a) of the forwarding of the judgment and the certificate to the competent authority responsible for its execution in accordance with Article 5(5); EN L 327/36 Official Journal of the European Union 5.12.2008 (b) of the fact that it is in practice impossible to enforce the sentence because after transmission of the judgment and the certificate to the executing State, the sentenced person cannot be found in the territory of the executing State, in which case there shall be no obligation on the executing State to enforce the sentence; (c) of the final decision to recognise the judgment and enforce the sentence together with the date of the decision; (d) of any decision not to recognise the judgment and enforce the sentence in accordance with Article 9, together with the reasons for the decision; (e) of any decision to adapt the sentence in accordance with Article 8(2) or (3), together with the reasons for the decision; (f) of any decision not to enforce the sentence for the reasons referred to in Article 19(1) together with the reasons for the decision; (g) of the beginning and the end of the period of conditional release, where so indicated in the certificate by the issuing State; (h) of the sentenced person's escape from custody; (i) of the enforcement of the sentence as soon as it has been completed.	
Council Framework Decision 2002/584/JHA of 13 June 2002 on the European Arrest Warrant and the surrender procedures between Member State	All stages	Yes	*Not applicable*	*Not specified*	(a) the identity and nationality of the requested person; (b) the name, address, telephone and fax numbers and e-mail address of the issuing judicial authority;- Art.8 (c) evidence of an enforceable judgment, an arrest warrant or any other enforceable judicial decision having the same effect, coming within the scope of Articles 1 and 2; (d) the nature and legal classification of the offence, particularly in respect of Article 2; (e) a description of the circumstances in which the offence was committed, including the time, place and degree of participation in the offence by the requested person; (f) the penalty imposed, if there is a final judgment, or the	Competent Judicial Authorities

Legal instrument	Stage of the procedure	Form to be exchanged (Yes, No)	If No, how information is exchanged:	Channel used to exchange the information:	Information exchanged	Authority involved
					prescribed scale of penalties for the offence under the law of the issuing Member State; (g) if possible, other consequences of the offence.	
Directive 2011/99/EU of the European Parliament and of the Council of 13 December 2011 on the European protection order	Execution judgment	Yes	*Not applicable*	*Not specified*	The Commission shall make the information received available to all Member States. Member States shall inform the Commission of any change to the information referred to in paragraph 1.	• Issuing States • Executing States
Council Framework Decision 2003/577/JHA, on the execution in the European Union of orders freezing property or evidence (after 12/2020 this would be only used for cooperation with IE and DK, who are not bound by the regulation (EU) 2018/1805	Execution judgment	Yes	*Not applicable*	*Not specified*	Adequate information to interested parties	• Issuing States • Executing States

Annex E | Eurojust security rules

Eurojust security rules are structured as following in two different parts:

Part I:

- Basic Principles and minimum standards of Security

- Classification Markings consists of applying data classification and labelling on Eurojust data.
  - E.g. EUCI shall be identified as classified information, and retain its classification level for only as long as necessary.
- Protection of classified information, which consists of designing and implementing safeguards that ensure EUCI items are protected based on their classification.
  - E.g. Where the Member States introduce classified information bearing a national security classification marking into Eurojust domain, Eurojust shall protect that information following the requirements applicable to EUCI as an equivalent level as set out in the table of the equivalent of security classification contained in Appendix 2 of Eurojust security rules
- Security Risk management, which consists of having a risk management process covering risks associated with EUCI.
  - E.g. Risks associated with EUCI shall be managed as an organisational process which aims at determining known security risks. Moreover, it should also define the mitigation measures to reduce such risks to an acceptable level following the basic principles and minimum standards described in Eurojust security rules. Security measures shall be designed following the concept of defence in depth. A process shall continuously evaluate the operative effectiveness of the identified measures once implemented.
- Confidentiality and Classification consist of defining the confidentiality requirements based on the classification model.
  - E.g. In places where confidentiality is required, care and experience are needed in the selection of information and material to be protected. Moreover, it should help to assess the degree of protection necessary. Steps shall be taken to avoid both over- and under-classification. Furthermore, the classification review cycle shall be as short as possible.
  - Personnel Security, to ensure that Eurojust personnel is managed in a secure way considering human resource related security risks and threats.
    - E.g. Personnel security measures shall be applied at Eurojust to ensure that access to EUCI is granted only to individuals who have:
      i. A need to know;
      ii. Been security cleared to the relevant level, where appropriate;
      iii. Been briefed on their responsibilities.
  - Physical Security, to ensure that technical physical security measures are in place to protect against unauthorised access at the physical layer.
    - E.g. Eurojust shall put in place physical and technical protective measures to prevent unauthorised access to EUCI.
  - Management of classified information, which consists of protecting EUCI items.
    - E.g. Administrative measures for managing EUCI throughout its lifecycle shall be put in place to help deter and recover from deliberate or accidental compromise or loss of such information. Such measures relate in particular to

the creation, registration, copying, translation, downgrading, declassification, carriage and destruction of EUCI items.

- Protection of EUCI handled in communications and Information systems, which enumerates communication and information systems related security measures while handling EUCI items.
  - E.g. All communication and information systems (CIS) handling EUCI items in Eurojust domain shall do so in accordance with the concept of information assurance (IA) in order to ensure appropriate levels of confidentiality, integrity, availability, non-repudiation and authenticity. The IA measures shall be based on a risk management process.
- Industrial Security, which enumerates required security measures applicable to supplier relationships.
  - E.g. Security measures shall be applied to ensure the protection of EUCI by contractors or subcontractors in pre-contract negotiations and throughout the lifecycle of classified contracts. Such contracts shall not involve access to information classified TRES SECRET UE/EU TOP SECRET.
- Sharing EUCI with other union institution, bodies or agencies, which enumerates security safeguards to have in place while exchanging EUCI items with other union institution, bodies or agencies.
  - E.g. The College shall determine the conditions under which it may share EUCI held by it with other Union institutions, bodies, offices or agencies. An appropriate framework may be put in place to that effect, including by entering into inter-institutional agreements or other arrangement where necessary for that purpose.
- Exchange of classified information with third states and international organisations, which enumerates security safeguards to have in place while exchanging classified information with third states and international organisations.
  - E.g. Where the College determines that there is a need to exchange EUCI items with a third state or international organisation, an appropriate framework shall be put in place to that effect.

Part II:

- The organisation of Security at Eurojust, which aims to delineate the organisation scope by clearly defining and formalising security roles and responsibilities for the different stakeholders involved in Eurojust ecosystem.
  - E.g. College, President, national members, Administrative Director, Security Committee, Head of Security, etc.
- Classification Markings, which describes the different levels of classification according to EUCI:
  1. TRES SECRET UE/EU TOP SECRET;
  2. SECRET UE/EU SECRET;
  3. CONFIDENTIEL UE/EU CONFIDENTIAL;
  4. RESTREINT UE/ EU RESTRICTED (EUROJUST);
  - Note: Where information or material classified in accordance with the above classification levels, originate from Eurojust, it shall bear an additional marking "Eurojust" under the classification marking.
  - Note: A comparative table of national security classifications may be found in the Appendix 2 of the Eurojust security rules. Further practical guidance on the classification of information is contained in Appendix 3 of the same document.

  - Note: A caveat marking may be used for specifying the field covered by the document or a particular distribution on a need-to-know basis.
- Management of classified information, which consists of setting out provisions for implementing the management of EUCI laying down the administrative measures for controlling EUCI throughout its lifecycle in order to help deter and detect deliberate or accidental compromise or loss of such information.
  - E.g. Information shall be classified where it requires protection with regard to its confidentiality.

  It covers the following aspects related to information classification and handling:
  - Classification Management;
  - Registration of EUCI for security purposes;
  - Copying and translating EU classified documents;
  - Carriage of EUCI;
  - Destruction of EUCI.
- Physical Security, which consists of setting out provisions for implementing physical security measures laying down minimum requirements for a secure physical protection of Eurojust premises, buildings, offices, rooms and other areas where EUCI items are handled and stored, including areas hosting CIS with the aim of preventing unauthorised access to EUCI assets.
  - E.g. Physical security measures shall be selected on the basis of a threat assessment made by the competent authorities. Eurojust shall apply a risk management process for protecting EUCI on its premises to ensure that a commensurate level of physical protection is afforded against the identified risks. The risk management process shall take account of all relevant factors in particular:
    1. i. The classification level of EUCI;
    2. ii. The form and volume of EUCI, bearing in mind large quantities or a compilation of EUCI may require more stringent protective measure to be applied;
    3. iii. The surrounding environment and structure of the buildings or areas hosting EUCI;
    4. iv. The assessed threat from intelligence services which target the Union or Member States and from sabotage, terrorist, subversive or other criminal and malicious activities.

  It covers the following aspects related to Physical security:
  - Physical security requirements and measures;
  - Equipment for the physical protection of EUCI;
  - Physically protected areas;
  - Physical protective measures for handling and storing EUCI;
  - Control of keys and combinations used for protecting EUCI.
- Security measures to be applied at the time of specific meetings held outside the Eurojust premises and involving EUCI, which describes the general rule regarding meetings involving EUCI at Eurojust premises.
  - E.g. the meeting room may be established as a technically secured area in accordance with Eurojust security rules. It shall be made technically secure by a technical security team, which may also conduct electronic surveillance during the meeting.

  It covers the following aspects related to security measures for meetings involving EUCI items in Eurojust premises:
  - Responsibilities;

    - Security measures.
- Breaches of security and compromise of EUCI, which describes the required security measures to deal with breach of security and the compromising of EUCI items.
    - E.g. All post-holders who handle EUCI shall be thoroughly briefed on their responsibilities in this domain. They shall report immediately to the Eurojust Security and Safety Services any breach of security which may come to their notice impacting EUCI items.
- Protection of EUCI handled in CIS, which consists of setting out provisions in Part I of the Eurojust security rules regarding the protection of EUCI handled in CIS.
    - E.g. The accreditation process of CIS at Eurojust that handle EUCI, shall be aligned with the relevant security guidelines developed by the Security Committee of the Council in accordance with Article 6(2) of Council Decision 2013/488/EU on the security rules for protecting EU classified information.

  It covers the following aspects related to the protection of EUCI handled in CIS:
    - The accreditation process;
    - Information assurance principles;
    - Information assurance functions and authorities;
- Industrial Security, which provides general security provisions applicable to industrial or other entities in pre-contract negotiation and throughout the lifecycle of classified contracts let by Eurojust.
    - E.g. Prior to launching a call for tender or letting a classified contract, Eurojust, as the contracting authority, shall determine the security classification of any information to be provided to bidders and contractors, as well as the security classification of any information to be created by the contractor. For that purpose, Eurojust shall prepare a Security Classification guide (SCG) to be used for the performance of the contract.

  It covers the following aspects related to industrial security:
    - Security element in a classified contract;
    - Facility security clearance (PSC);
    - Classified contracts and sub-contracts;
    - Visits in connection with classified contracts;
    - Transmission and carriage of EUCI;
    - Transfer of EUCI to contractors located in third states;
    - Information classified RESTREINT UE/EU RESTRICED.
- Exchange of classified information with third states and international organisations, which consists of setting out provisions for implementing provisions regarding the exchange of classified information with thirds states and international organisations.
    - E.g. No EUCI shall be exchanged under a security of information agreement by electronic means unless explicitly provided for in the agreement or in corresponding technical implementing agreements.

  It covers the following aspects related to the exchange of classified information with third states and international organisations:
    - Frameworks governing the exchange of classified information;
    - Security of information agreements;
    - Administrative arrangements;
    - Exceptional ad-hoc release of EUCI;
    - Authority to release EUCI to third states or international organisations.

Eurojust security rules document contains the three (3) following appendices:

1. List of National Security Authorities;
2. Comparison of National Security classifications;
3. Practical classification guide.

Annex F | Detailed cost model

The document attached includes the detailed cost assessment.

DCJ_CostModel_final version.xlsx

Annex G | Abbreviations and acronyms

For a better understanding of the present document, the following table provides a list of the principal abbreviations and acronyms used.

Table 53: Abbreviations and acronyms

Abbreviation/Acronym	Definition
AI	Artificial Intelligence
API	Application Programme Interface
CEF	Connecting European Facility
CMF	Case Management Framework
CH&IC	Case Handling & Internal Communication
CMS	Case Management System
COTS	Commercial of The Shelf
CRUD	Create Read Update Delete
DCJ	Digital Criminal Justice
DG	Directorate General
DIGIT	Directorate-General for Informatics
EAW	European Arrest Warrant
EC	European Commission
EIO	European Investigation Order
EIS	Europol Information System
ECRIS	European Criminal Records Information System
The EPPO	The European Public Prosecutor’s Office
ESP	European search portal
EU	European Union

EUI	European University Institute
ICM	Investigate Case Management
IEEE	Institute of Electrical and Electronics Engineers
iPaaS	Integration Platform as a Service
IS	Information System
ISA	Interoperability solutions for public administrations, businesses and citizens
iSaaS	Integration Software as a Service
IT	Information Technology
JHA	Justice and Home Affairs Agencies
MLA	Mutual Legal Assistance
MFA	Multifactor Authentication
LDAP	Lightweight Directory Access Protocol
OLAF	European Anti-fraud Service
PaaS	Platform as a Service
RADIUS	Remote Authentication Dial-In User Service
RBAC	Role Based Access Control
RSP	Re-usable Solution Platform
SAML	Security assertion markup language
SaaS	Software as a Service
SME	Small Medium Enterprises
SSH	Secure Shell
TOGAF	The Open Group Architecture Framework
TWF	Temporary Work File
XSS	Cross-Site Scripting

Annex H | Definitions

Table 54: Definitions

Term	Definition
Architecture Building Block (ABB)	A constituent of the architecture model that describes a single aspect of the overall model. *Source: TOGAF 9.2*
Application Component	An encapsulation of application functionality aligned to implementation structure, which is modular and replaceable. It encapsulates its behaviour and data, provides services, and makes them available through interfaces. *Source: ArchiMate Glossary*
Application Function	Automated behaviour that can be performed by an application component. *Source: ArchiMate Glossary*
Building Block	A (potentially re-usable) component of enterprise capability that can be combined with other Building Blocks to deliver architectures and solutions. Note: Building Blocks can be defined at various levels of detail, depending on what stage of architecture development has been reached. For instance, at an early stage, a Building Block can simply consist of a name or an outline description. Later on, a Building Block may be decomposed into multiple supporting Building Blocks and may be accompanied by a full specification. Building Blocks can relate to "architectures" or "solutions". *Source: TOGAF 9.2*
Case Information File (CIF)	A case information form that summarises lessons learned from handing the case, which is created after a case is closed. *Source: PWC study*
Case Management Solutions	Applications designed to support a complex process that requires a combination of human tasks and electronic workflow, such as an incoming application, a submitted claim, a complaint, or a claim that is moving to litigation. These solutions support the workflow, management collaboration, storage of images and content, decisioning, and processing of electronic files or cases. Some come with insurance workflow/process templates to help implementation. *Source: Gartner*
COTS	COTS solutions are third-party solutions that are bought, licensed, or acquired; often, they are integrated into a larger system. *Source: PMI ORG*[228]
Entity	A single unique object in the real world that is being mastered. Examples of an entity are a case, or a suspect. *Source: IBM*
SaaS	The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure2. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
PaaS	The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using

[228] https://www.pmi.org/learning/library/custom-off-the-shelf-strategy-6137

	programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
iPaaS	Is a suite of cloud services enabling development, execution and governance of integration flows connecting any combination of on premises and cloud-based processes, services, applications and data within individual or across multiple organizations. *Source: Gartner*
Solution Building Block (SBB)	A candidate solution which conforms to the specification of an Architecture Building Block (ABB). *Source: TOGAF 9.2*
System	A collection of components organized to accomplish a specific function or set of functions (Recommended Practice for Architectural Description IEEE P1471/D5.2).
Temporary Work File (TWF)	Temporary Work Files, as referred in Art. 16(1) of Eurojust Decision, are opened by the National Members concerned for every initial request/information which needs to be handled by Eurojust within the framework of its competence and in order to carry out its tasks. *Source: PWC study*

Annex I | Bibliography

Legal documents

Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0816&from=EN

Proposal for a Regulation of the European Parliament and of the Council establishing the Digital Europe Programme for the period 2021-2027 {SEC(2018) 289 final} - {SWD(2018) 305 final} - {SWD(2018) 306 final}, https://eur-lex.europa.eu/resource.html?uri=cellar:321918fd-6af4-11e8-9483-01aa75ed71a1.0003.03/DOC_1&format=PDF

Regulation (EU) 2019/1896 of the European Parliament and of the Council of 13 November 2019 on the European Border and Coast Guard and repealing Regulations (EU) No 1052/2013 and (EU) 2016/1624, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R1896&from=EN

Regulation (EU) 2018/1805 of the European Parliament and of the Council of 14 November 2018 on the mutual recognition of freezing and confiscation orders, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1805&from=EN

Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0179&from=EN

Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office (EPPO), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R1939&from=EN

Regulation (EU) 2017/825 of the European Parliament and of the Council of 17 May 2017 on the establishment of the Structural Reform Support Programme for the period 2017 to 2020 and amending Regulations (EU) No 1303/2013 and (EU) No 1305/2013, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0825&from=EN

Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0794&from=EN

Decision (EU) 2015/2240 of the European Parliament and of the Council of 25 November 2015 establishing a programme on interoperability solutions and common frameworks for European public administrations, businesses and citizens (ISA2 Programme) as a means for modernising the public sector, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015D2240&from=EN

Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters of 3 April 2015, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0041&from=EN

Regulation (EU) No 1382/2013 of the European Parliament and of the Council of 17 December 2013 establishing a Justice Programme for the period 2014 to 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013R1382&from=EN

Regulation (EU) No 1316/2013 of the European Parliament and of the Council of 11 December 2013 establishing the Connecting Europe Facility, amending Regulation (EU) No 913/2010 and repealing Regulations (EC) No 680/2007 and (EC) No 67/2010, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013R1316&from=EN

Regulation (EU) No 1291/2013 of the European Parliament and of the Council of 11 December 2013 establishing Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020) and repealing Decision No 1982/2006/EC, https://ec.europa.eu/research/participants/data/ref/h2020/legal_basis/fp/h2020-eu-establact_en.pdf

Regulation (EU, EURATOM) No 883/2013 of the European parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) and repealing Regulation (EC) No 1073/1999 of the European Parliament and of the Council and Council Regulation (Euratom) No 1074/1999, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02013R0883-20170101&from=EN

Council Framework Decision 2008/947/JHA, on the application of the principle of mutual recognition to judgments and probation decisions with a view to the supervision of probation measures and alternative sanctions, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008F0947&from=EN

Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32007D0533&from=EN

Council Decision 2005/671/JHA of 20 September 2005 on the exchange of information and cooperation concerning terrorist offences, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005D0671&from=GA

Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32003F0577&from=EN

Council Framework Decision 2002/584/JHA of 13 June 2002 on the European Arrest Warrant and the surrender procedures between Member State, https://eur-lex.europa.eu/resource.html?uri=cellar:3b151647-772d-48b0-ad8c-0e4c78804c2e.0004.02/DOC_1&format=PDF

Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000F0712(02)&from=EN

and https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:42000A0712(01)&from=EN

Policy documents

Eurojust's paper: Towards Digital Criminal Justice in the EU, 14345/18, 15 November 2018, http://data.consilium.europa.eu/doc/document/ST-14345-2018-INIT/en/pdf

European Council meeting (18 October 2018), EUCO 13/18, https://www.consilium.europa.eu/media/36775/18-euco-final-conclusions-en.pdf

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - European Interoperability Framework - Implementation Strategy, COM(2017)134 final, https://eur-lex.europa.eu/resource.html?uri=cellar:2c2f2554-0faf-11e7-8a35-01aa75ed71a1.0017.02/DOC_1&format=PDF

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - EU eGovernment Action Plan 2016-2020, Accelerating the digital transformation of government, COM(2016)179 final, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0179&from=EN

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe, COM (2015) 192 final, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN

Previous e-Justice Action Plans: Multi-annual European e-Justice Action Plan 2009-2013; Multiannual European e-Justice Action Plan 2014-2018.

2019-2021 Strategy on e-Justice, 2019/C 96/04, 2019,https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019XG0313(01)&rid=

Action Plan European e-Justice 2019-2023, 2019/C 96/05, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019XG0313(02)&rid=6

Studies

PwC, Solution outline report – Case management system.

Eurojust, Second JIT Evaluation Report, Ferbruary 2018, http://www.eurojust.europa.eu/doclibrary/JITs/JITsevaluation/Second%20JIT%20Evaluation%20Report%20(February%202018)/2018-02_2nd-Report-JIT-Evaluation_EN.pdf

Europol, Data Protection at Europol, 2012, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=2ahUKEwi-iZnY2p7mAhXIZ1AKHYfZDRAQFjABegQIBRAC&url=https%3A%2F%2Fwww.europol.europa.eu%2Fs

ites%2Fdefault%2Ffiles%2Fdocuments%2Feuropol_dpo_booklet_0.pdf&usg=AOvVaw2cl2ecq9O7_gKh-QKuZ-dS

Wire Swiss GmbH ,Wire Security Whitepaper, 17 August 2018, https://wire-docs.wire.com/download/Wire+Security+Whitepaper.pdf

Others

Open e-Trust Ex , https://ec.europa.eu/isa2/solutions/open-e-trustex_en

European Commission, DIGIT D3, TESTA Overview and Service Catalogue, July 2018, https://ec.europa.eu/isa2/sites/isa/files/testa_overview_-_july_2018.pdf

Judicial Atlas, https://www.ejn-crimjust.europa.eu/ejn/AtlasChooseCountry/EN

API-led Connectivity, https://blogs.mulesoft.com/dev/api-dev/what-is-api-led-connectivity/

European Commission, CEF e-translation, https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/2019/10/17/eTranslation+excels+at+WMT+2019%3A+amongst+top+ranking+engines+with+over+150+other+machine+translation+systems

European Lawyers Foundation, Find-A-Lawyer 3, https://elf-fae.eu/find-a-lawyer-3/

JITs Portal, https://jit.eurojust.europa.eu/Pages/Home.aspx

IBM Digital Business Automation V19.1 delivers enhanced capabilities with electronic records management, SAP integration, and information governance, 25 June 2019, https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=an&subtype=ca&appname=gpateam&supplier=897&letternum=ENUS219-308#availx

Zimbra Collaboration Product Edition Comparison, https://www.zimbra.com/email-server-software/product-edition-comparison/

EY announces acquisition of SAP consulting business, 2 December 2019, https://www.ey.com/en_uk/news/2019/12/ey-announces-acquisition-of-sap-consulting-business

Mulesoft Partner Finder, https://www.mulesoft.com/integration-partner/finder?field_partner_industr_target_id=166&field_partner_region_value=Europe

Magic Quadrant for Intelligent Business Process Management Suites, http://faragozin.com/2019/02/02/magic-quadrant-for-intelligent-business-process-management-suites/

DS-04-20-443-EN-N

Publications Office
of the European Union

doi: 10.2838/118529