Directorate-General for Justice and Consumers

Unit JUST H.4 – IT, Document and Knowledge Management

Functional Analysis Document (FAD)
for the
Reference Implementation Software
Competent Authorities Module
connected to the e-evidence Decentralised IT System

Revision History

Date	Version	Updated sections	Description
31.07.2024	0.1	All	Initial version.
07.08.2024	1.0	All	First version sent for review to Member States and Service Providers
31.10.2024	1.1	All	Update with feedback from the Member States and Service Providers
08.01.2025	1.2	All	Update with feedback from the Member States and Service Providers after the consolidation meeting

Table of Contents

Table of Contents 3
1 Introduction 6
1.1 Objective of this Document 6
1.2 Structure of the Document 6
1.3 Intended Audience 6
Part I – Requirements Definition 7
2 Requirements Analysis 8
2.1 Business requirements 8
2.2 Functional requirements 9
2.3 Non-Functional Requirements 22
2.3.1 Usability 22
2.3.2 Security 23
2.3.3 Personal Data Protection Aspects 24
2.3.4 Business Continuity 25
2.3.5 Development Qualities 26
2.3.6 Compliance 26
Part II – Functional Analysis 27
3 Overview 28
3.1 Business Objective of the Process 28
3.2 Domains 28
3.3 Actors 29
3.4 User roles 30
3.4.1 Functional user roles 31
3.4.2 Technical user roles 31
3.5 Roles & Permissions within the Issuing Authority for EPOC 32
3.6 Roles & Permissions within the Enforcing Authority for EPOC 36
3.7 Roles & Permissions within the Issuing Authority for EPOC-PR 39
3.8 Roles & Permissions within the Enforcing Authority for EPOC-PR 43
3.9 User management 44

3.10 EPOC and EPOC-PR Global Business Processes and Sub-Processes 44
4 EPOC and EPOC-PR Business Processes 47
4.1 Time Limits 47
4.1.1 Legal deadlines for the execution of the European Production Order Certificate (EPOC): 47
4.1.2 Legal deadlines for the execution of the European Preservation Order Certificate (EPOC-PR): 49
4.1.3 Legal deadlines for the Enforcement Procedures (EPOC & EPOC-PR) 50
5 Functional Messages 51
5.1 Messages 51
5.1.1 From the Issuing Authority 51
5.1.2 From the Enforcing Authority 53
5.1.3 From the Service Providers 55
5.1.4 From the Court in Issuing State to the Issuing Authority and the Service Provider 56
5.2 Technical messages 56
5.3 Errors and Warnings 57
5.3.1 Syntactic Validation 57
5.3.2 Semantic Validation 57
5.4 User notifications 58
6 Workflows 60
6.1 Internal workflow 60
6.2 External workflow 60
7 Case lifecycle/statuses 61
7.1 Table of Lifecycle Stages: EPOC Draft case 61
7.2 Table of Lifecycle Stages: EPOC Issued case 62
7.3 Table of Lifecycle Stages: EPOC Received case 65
7.4 Table of Lifecycle Stages: EPOC-PR Draft case 67
7.5 Table of Lifecycle Stages: EPOC-PR Issued case 68
7.6 Table of Lifecycle Stages: EPOC-PR Received case 71
8 Logging and Statistics 73
9 System Architecture 75

9.1 Direct Access to the national IT system / Reference Implementation software (RI) for Service Providers through a web-based interface 76
9.2 Service Provider's System-to-System Access to the decentralised IT system through the national IT system / Reference Implementation Software via API's 78
10 Security Aspects 81
10.1 Confidentiality 81
10.2 Integrity 81
10.3 Availability 82
10.4 Legitimate Use of the System 82
11 Assumptions, Constraints and Risks Analysis 84
11.1 Assumptions 84
11.2 Constraints 84
11.3 Risks 85
12 ANNEXES 86
12.1 Errors and Warnings list 86
12.1.1 Error messages based on HTTP response status codes 86
12.1.2 Error messages from backend 87
13 Related Documents 88
13.1 Applicable Documents 88
13.2 Reference Documents 89
13.3 Abbreviations & Acronyms 89
13.4 List of tables 89
13.5 List of figures 90

1 Introduction

1.1 Objective of this Document

The Functional Analysis Document serves as a comprehensive guide for the development and implementation of the Reference Implementation module meant for use by the Competent Authorities in the context of the *Regulation 2023/1543* on European Production Orders and European Preservation Orders. The primary purpose of the document is to ensure a clear understanding of the system's capabilities and requirements, facilitating effective communication and alignment among all parties involved.

It should be noted that this FAD does not address aspects related to communication between competent national authorities and service providers, which are elaborated in a separate FAD.

This document is supported by the Business Collaboration Document (BCD), which establishes the scope of exchanges of European Production Order Certificates (EPOC) and European Preservation Order Certificates (EPOC-PR);

1.2 Structure of the Document

The Functional Analysis Document is divided into two parts. The first one, Requirements Definition, lists the functional and non-functional requirements of the Reference Implementation, with their prioritization. The second one provides the functional analysis of the RI.

1.3 Intended Audience

The target audience for this document includes the following stakeholders:

- The Member States' competent authorities;
- Service Providers and their legal representatives and/or designated establishments;
- The Directorate-General for Justice and Consumers (DG JUST);
- The writers of the technical specifications for the implementation of the decentralised IT system;
- The team supporting the testing processes of the decentralised IT system implementation.

Part I – Requirements Definition

2 Requirements Analysis

The requirements levels will be categorised using the MoSCoW prioritisation method (Mo - Must have, S - Should have, Co - Could have, W - Won't have). The various categories are listed below:

- **"Must Have"**: This is an absolute requirement of the specification and is critical to the system;
- **"Should Have"**: This means that there may exist valid reasons in particular circumstances to ignore the requirement, but the full implications must be understood and carefully weighed before choosing a different course.
- **"Could have"**: These requirements are "nice to have" features but are not necessary to the functioning of the system. They could improve user experience or customer satisfaction for little development cost. These will typically be included if time and resources permit.
- **"Won't have"** (this time): These requirements are the least-critical, lowest-payback items, or not appropriate at that time. As a result, "Won't have" requirements are not planned into the schedule for the current release. These requirements will be reconsidered for inclusion in a later stage and their category might change depending on the needs.

They are detailed in the following section.

2.1 Business requirements

This section describes the business requirements of the system, with their prioritization.

ID	Title	Description	Priority
BR-01.	Supported Languages	The system shall support multiple languages to cater to diverse EU member states, providing interfaces and information in at least the official languages of all EU countries	Must
BR-02.	User Authentication	The system should allow users to securely create accounts, log in, and recover passwords.	Must
BR-03.	User Roles and Permissions	The software should provide varying levels of access based on user roles.	Must
BR-04.	Integration with National Systems	The system ensures seamless integration with the national systems of the stakeholders.	Must

ID	Title	Description	Priority
BR-05.	Scalability	The system needs to handle increased user loads and data volumes as the business grows.	Must
BR-06.	Performance	The application should maintain acceptable response times and handle a certain number of concurrent users.	Must
BR-07.	Usability and Accessibility	The system should be user-friendly and accessible to all users, including those with disabilities.	Must
BR-08.	Security and Compliance	The software must adhere to industry security standards and ensure compliance with the General Data Protection Regulation (GDPR).	Must
BR-09.	Notification System	The system should send notifications to users via email or other means for important events or updates.	Must
BR-010.	Logging transmissions carried out by alternative means	The system shall record the transmission carried out by alternative means in the decentralised IT system.	Must
BR-011.	Encryption	The system ensures end to end encryption of data both in transit and at rest.	Must
BR-012.	Training and Support	The system should include features for users to contact the support team and receive assistance.	Should
BR-013.	Communication with stakeholders	A "before/after issuing" communication in form of exchange of messages (like e-mails) between central authorities should be possible.	Could
BR-014.	Dashboard	The system should allow users to search for specific items or content within the application.	Must

Table 1: Business Requirements

2.2 Functional requirements

This section describes the functional requirements of the RI system, with their respective prioritization category.

ID	Title	Description	Priority
Supported languages Requirements			

ID	Title	Description	Priority
FR-01.	GUI template languages	The RI supports the same templates/forms in all official EU languages.	Must
FR-02.	GUI languages – All official EU languages	All translatable texts contained in the RI are available in all official EU languages.	Must
FR-03.	Support multilingualism (EU languages)	The RI must support all official EU languages. Labels, data fields and buttons contained in RI must be displayable in all national alphabets. The system must therefore support the character set of all official EU languages.	Must
FR-04.	Encoding scheme – Support official EU alphabets	The e-Forms implementation must support the same template of e-Form in all official EU languages. Labels, data fields and buttons contained in the e-Forms must be supported in all official EU languages.	Must
FR-05.	e-Forms translation functionality	If the sender and the recipient of an e-Form do not use the same language, they must be able to forward the e-Form to a translator who will translate the text fields from/to a common language.	Should
FR-06.	e-Forms alphabet transliteration functionality	If the sender and the recipient of an e-Form do not use the same character set (for example names and addresses in Cyrillic or Greek), an extra transliteration field could be foreseen.	Could
e-Forms Management Requirements			
FR-07.	Support the EPOC and EPOC-PR paper forms as e-Forms functionality	The EPOC and EPOC-PR paper forms must be reproduced as e-Forms. The RI must be capable of generating/processing messages derived from this e-Form and exchanging them through the e-CODEX system.	Must
FR-08.	Maintain an e-Form functionality	The Competent Authority user can maintain an e-Form.	Must
FR-09.	Add an e-Form functionality	The Competent Authority user can add a new and empty e-Form.	Must

ID	Title	Description	Priority
FR-010.	Open an e-Form functionality	The Competent Authority user must be able to open an existing e-Form.	Must
FR-011.	View an e-Form functionality	The Competent Authority user can view an existing e-Form.	Must
FR-012.	e-Forms edit functionality	The Competent Authority user must be able to edit an e-Form up to the signing step. Once the form is signed, it is locked for editing. In particular, the Competent Authority user must be able to partially fill in an e-Form and edit data he has already entered, including undoing changes to the e-Form.	Must
FR-013.	e-Forms load functionality	The Competent Authority user must be able to load an e-Form i.e. populate the e-Form with structured data.	Must
FR-014.	Update an e-Form	The Competent Authority user can update an existing e-Form. In particular, this user can partially fill in an e-Form and edit data she/he has already entered.	Must
FR-015.	Validate an e-Form	The Competent Authority user can validate an e-Form. The validation consists of a full set of syntactical and semantical validations of the data contained in the e-Form.	Must
FR-016.	Save an e-Form functionality	The Competent Authority user must be able to save an e-Form. In particular, this user must be able to save an e-Form, even after having it only partially filled in. This requirement also covers the “save as” functionality.	Must
FR-017.	Send an e-Form functionality	The Competent Authority user must be able to send an e-Form to Service Provider and another Member State Authority.	Must
FR-018.	Partially filled in e-Forms no-sending functionality	The Competent Authority user should not be able to send an e-Form if mandatory fields are not filled in.	Must

ID	Title	Description	Priority
FR-019.	Search for competent authority – CDB functionality	The Competent Authority user can send an e-Form to Service Provider and another Member State Authority via e-CODEX. In particular, the Competent Authority user can search and select the recipient's address to use within a list available in the Court Database (CDB).	Must
FR-020.	Send an e-Form - Attach files functionality	The RI must provide the possibility to send attachments together with the e-Forms. Attachments can consist of different formats to be defined.	Must
FR-021.	Send an e-Form - Collect information	The RI can collect statistical information on the e-Forms sent through the decentralized IT system. This general information is also used for the message tracking and the workflow follow-up.	Must
FR-022.	Send an e-Form - Encode the recipient's address manually	The Competent Authority user can encode manually a recipient to which to send the e-Form.	Could
FR-023.	Send an e-Form - Printable confirmation	When the e-Form is sent, a printable confirmation is generated by the RI. It contains information about the form and the list of the attached files.	Could
FR-024.	Selective printing of an e-Form	The Competent Authority user can select the parts of an e-Form to display in a printing task.	Could
FR-025.	Print preview an e-Form	The Competent Authority user can print preview an e-Form. The print preview is opened in a new page.	Could
FR-026.	Print an e-Form	The Competent Authority user can print an e-Form. The print preview of the e-Form has to be performed previously.	Could
FR-027.	Export an e-Form	The Competent Authority user can export an e-Form.	Must
FR-028.	Export an e-Form - PDF file	The Competent Authority user can export an e-Form as a PDF file.	Must
FR-029.	Export an e-Form - Microsoft Word file	The Competent Authority user can export an e-Form as a Microsoft Word file.	Should

ID	Title	Description	Priority
FR-030.	Export an e-Form - Selective exporting and saving	The Competent Authority user can export and save the e-Form and/or its content after selecting parts.	Could
FR-031.	Close an e-Form	The Competent Authority user can close an opened e-Form.	Must
FR-032.	Show all fields	The Competent Authority user can show all the fields of an e-Form when some are hidden.	Must
FR-033.	Hide the empty sections in an e-Form	The Competent Authority user can hide the empty sections of an e-Form.	Should
FR-034.	Show only the invalid fields	After a semantic or syntactic validation, the Competent Authority user can hide all the fields of an e-Form except the invalid ones.	Should
FR-035.	Import a field set in an e-Form	The Competent Authority user can import data corresponding to a field set in an e-Form through an XML file.	Must
FR-036.	Extract a field set in an e-Form	The Competent Authority user can extract data corresponding to a field set in an e-Form as an XML file.	Must
FR-037.	Multiple tabs	It should be possible to open several e-Forms in several tabs without any impact on each other.	Should
FR-038.	e-Form backwards compatibility	The backwards compatibility of an e-Form is managed per type of e-Form.	Should
FR-039.	Support previous versions of the e-Forms	The Competent Authority user can open an e-Form of a version older than the current production version. The number and the versions supported, and how they are opened depends on the impact of the changes and on the e-Forms domain.	Must
FR-040.	Support previous versions of the e-Forms - Conversion of an e-Form to a newer version	The application can migrate an e-Form from one version to a more recent one. The workflow, fields and labels of the older version are converted to the new one.	Should

ID	Title	Description	Priority
FR-041.	Support previous versions of the e-Forms - Preservation of older versions of e-Forms	The application can open previous versions of an e-Form as they used to be. The workflow, fields and labels of that older version are preserved, and the newer version has no impact on this.	Must
FR-042.	e-Form navigation menu	A navigation menu is displayed on the left side of the page to improve the navigation within the e-Form.	Should
FR-043.	e-Form navigation menu - Validation errors	When validating an e-Form, the navigation menu displays the number of validation errors per component of the navigation menu.	Should
FR-044.	e-Form navigation menu – Highlight current e-Form's part	The current e-Form's part is highlighted in the navigation menu allowing the Competent Authority user to know which part specific part they are working on.	Should
FR-045.	e-Form navigation menu – View progression of the e-Form's part	A progress bar is contained into each item of the navigation menu in order to know at a glance the number of mandatory fields filled in according to the total number of mandatory fields in this e-Form's part.	Could
FR-046.	e-Form dashboard	A dashboard displays an overview of the e-Form content. The following information can be displayed by default: • The MS sending the e-Form; • The SP/MS receiving the e-Form; • The current step in the e-Form workflow. • List of cases sent or received.	Must
FR-047.	e-Form dashboard - Additional information	The additional and specific information available in the dashboard is customisable by type of e-Form.	Could
FR-048.	Tooltips	Tooltips are available on some fields of an e-Form. This help provides information on the expected content of a field as well as further actions to be performed by the user.	Must

ID	Title	Description	Priority
FR-049.	Warn before leaving an e-Form Edit page	The application must warn a user when she/he leaves an e-Form Edit page. This will mitigate the risk of losing unsaved work.	Must
FR-050.	Navigate through the editable parts	The Competent Authority user can navigate through the different editable sections of the e-Form displayed inside the editable part.	Should
FR-051.	Navigate through the e-Form's parts	The Competent Authority user can navigate through the various parts of the e-Form without using the navigation menu.	Could
FR-052.	e-Form section - Validation errors	When filling-in an e-Form, the number of missing mandatory fields and some client validation errors are displayed per section in the summary part. By performing a semantic and syntactic validation of the e-Form, the total number of validation errors is displayed per section too.	Should
FR-053.	Interoperability between the e-Forms implementations	RI must be able to export data as structured data, capable of being interpreted by other e-Forms implementations compliant to the e-Forms Functional Specifications. The e-Forms implementation must be able to import data from structured data, received from other e-Forms implementations compliant to the e-Forms Functional Specifications.	Must
FR-054.	e-Forms syntactical validation	RI must support a full and consistent set of syntactical validations of the data contained in the e-Forms (and not the meaning/content of the data). This must be supported: • Upon request from the end-user filling in the e-Form; • When generating the structured data from the e-Form; • When importing the structured data into the e-Form.	Must

ID	Title	Description	Priority
FR-055.	e-Forms partial response functionality	RI must support a functionality to allow a Competent Authority user to provide partial responses to a request submitted by a competent authority, and, in specific circumstances, to provide multiple responses to a single request.	Must
FR-056.	e-Forms forward functionality	The Competent Authority user must be able to forward an e-Form to another Competent Authority within the same Member State for internal processing purposes.	Must
FR-057.	e-Forms forward functionality - Forward an e-Form to national backend systems via e-CODEX	The Competent Authority user should be able to forward an e-Form received via e-CODEX to the national back-end system for further processing.	Could
FR-058.	Receive an e-Form from national backend systems via e-CODEX	The Competent Authority user must be able to receive an e-Form from a national back-end system for further processing.	Must
e-Forms domains support			
FR-059.	Support several e-Forms domains	The RI implementation can process e-Forms for several e-Forms domains.	Must
FR-060.	Support EPOC e-Forms	The RI can process EPOC e-Forms.	Must
FR-061.	Support EPOC-PR e-Forms	The RI can process EPOC-PR e-Forms.	Must
FR-062.	Support another e-Forms application domain	A new e-Form application domain (instrument) can be integrated in the Reference Implementation.	Should
Access, authorisation and security Requirements			
FR-063.	Access to the application	The RI can be accessed by several users having various roles or authorisations.	Must
FR-064.	Access to the application - Authentication	The RI can be accessed using a two-factor authentication mechanism.	Must

ID	Title	Description	Priority
FR-065.	Access to the application - Authorised users	Only authorized users can access the Reference Implementation Software.	Must
FR-066.	Access to the application - Competent Authority user	The Competent Authority user can access the Reference Implementation Software through EU Login. The access is provided by e-Forms domain.	Could
FR-067.	Access to the application – Users Groups	The RI can support "User groups" within an Authority. A "User group" could contain one or more users. The "User group" could be granted access to a subset or all messages within the Authority.	Should
FR-068.	Prevent from filling in specific fields	When displaying an e-Form, RI can prevent users from filling in specific fields, either by hiding them or by showing read-only values.	Must
FR-069.	Encryption – sending	RI provides an encryption functionality that will be used prior to sending e-Forms messages.	Must
FR-070.	Encryption – storage	RI provides an encryption functionality that will be used prior to storing data at rest.	Must
FR-071.	e-Signature / e-Seal	RI provides an e-Signature or e-Seal functionality that can be used prior to sending e-Forms messages.	Must
FR-072.	e-Signature / e-Seal validation	The digital signature or seal contained in a message must be verifiable. It should be possible to validate the origin of any message, and to determine its integrity.	Should
Additional Requirements			
FR-073.	Maintain a FAQ	The Administrator user can maintain a FAQ in RI.	Could
FR-074.	Add a FAQ	The Administrator user can add a new FAQ in RI.	Could
FR-075.	Update a FAQ	The Administrator user can update an existing FAQ in RI.	Could

ID	Title	Description	Priority
FR-076.	Delete a FAQ	The Administrator user can delete a FAQ in RI.	Could
FR-077.	View a FAQ	The Competent Authority users can view a FAQ in RI.	Could
FR-078.	Maintain a message on the Home page	The Administrator user can maintain a message on the Home page of RI. There can be one common message and one message specific for each e-Forms domain on the Home page.	Should
FR-079.	Add a message on the Home page	The Administrator user can add a new message displayed on the Home page of the RI.	Should
FR-080.	Update a message on the Home page	The Administrator user can update a message displayed on the Home page of the RI.	Should
FR-081.	Delete a message on the Home page	The Administrator user can delete a message displayed on the Home page of the RI.	Should
FR-082.	View a message on the Home page	The Competent Authority users can view the common message and the message specific to their e-Forms domain displayed on the Home page of the RI.	Should
FR-083.	View System information	The Technical Administrator user can view the installed domains and system information of the RI.	Must
FR-084.	Download the User Manual	The users can download the User Manual of the RI from the FAQ page.	Could
Additional Features Requirements			
FR-085.	Search feature	The Competent Authority user can search for an e-Form exchanged by her/his MS Competent Authority and to which they have access through Reference Implementation Software by the following parameters: title, reference number, national case number, request type, executing authority, status, date issued. Information on all the e-Forms, which are part of the exchange involving the e-Form searched, are displayed.	Must

ID	Title	Description	Priority
FR-086.	View the summary of the workflow follow-up	The Competent Authority user can view the number of complete, pending and out of time e-Forms received by his/her Competent Authority according to the selected e-Forms pertaining to the legal act that is being implemented.	Must
FR-087.	View the workflow follow-up	The Competent Authority user can view general information on the complete, pending and out of time case received by her/his Competent Authority within RI.	Must
FR-088.	Compute deadlines	The RI computes deadlines for an e-Form based on the metadata and content of that e-Form or of a related e-Form.	Must
FR-089.	Send data via a Web Service	The Competent Authority user can send data to the Service Provider/Competent Authority via a Web Service instead of using the User Interface of the RI.	Must
FR-090.	Validate data via a Web Service	The Competent Authority user can validate data to the Competent Authority of another Member State via a Web Service instead of using the User Interface validation of RI. In case of problems, error messages are delivered to the user.	Should
FR-091.	Business monitoring	The RI can aggregate information that can be used to monitor exchanges. Furthermore, the input may be split by e-Forms application domain.	Could

ID	Title	Description	Priority
FR-092.	Change e-Form display	The RI offers to the user the opportunity to change the display of the current e-Form: • Show the e-Form in Full Screen mode; • Collapse/Expand all sections from the current part in the summary side of the e-Form side-by-side view. The purpose of this is to ease the readability of all sections of an e-Form.	Could
FR-093.	Change e-Form display – View full/normal screen	The Competent Authority users can display the current e-Form in read-only mode. Once the Full Screen view is activated, the user can come back to the Normal Screen mode.	Could
FR-094.	Change e-Form display – Collapse/Expand the sub-sections	The Competent Authority users can collapse or expand all the sections of the current e-Form part in the summary side.	Must
FR-095.	Display tooltips for the tool icons	The RI displays tooltips when the user rolls over a key tool icon.	Must
FR-096.	Deselect previously selected options	The RI allows emptying the choice previously selected among several options in case this set of fields is not mandatory.	Must
FR-097.	Deletion of Information	The RI must, whenever required, ensure that all copies of the information can be permanently deleted.	Must
FR-098.	Copy an e-Form functionality	The Competent Authority user should be able to copy an existing e-Form with a possibility to edit fields.	Must
FR-099.	Upload a signed e-Form functionality	The Competent Authority user must be able to upload a signed e-Form to the RI.	Must
FR-0100.	Send an e-Form multiple times functionality	The Competent Authority user should be able to send an e-Form/ a message more than once within an exchange.	Must
FR-0101.	Remove a draft of an e-Form/ message	The Competent Authority user should have a possibility to remove a draft of a message/an e-Form.	Must

ID	Title	Description	Priority
FR-0102.	Standards support for the forms	The RI implementation of the forms should support agreed standards.	Must
FR-0103.	API Provision	The RI should provide Member State with API.	Must
FR-0104.	APIs coverage	Every action that is implemented in the UI must have a corresponding mechanism to do via an API	Must
FR-0105.	Logging transmissions carried out by alternative means	The RI should provide the possibility to record the transmission carried out by alternative means (outside of the decentralized IT system), including the date and time of transmission, the sender and recipient, the file name and its size.	Could
FR-0106.	Logging transmissions carried out by alternative means - Manifest	For each exchange carried out outside of the system, a manifest possibly containing a link, access information (e.g. access credentials), a hash digest of the data package is transferred through the national IT system or RI over the e-CODEX stack.	Must
FR-0107.	Notification system	The RI should send notifications to users via email or other means for important events or updates.	Should
FR-0108.	File size of attachments	The RI should display information about the maximum size of attachments that can be sent to the selected recipient.	Could
FR-0109.	e-Forms transmission to multiple recipients	The RI must allow Competent Authority users to send an e-Form to multiple recipients.	Must
FR-0110.	Confirmation prompts for critical actions (deletion and transmission actions)	The RI should prompt users with a confirmation dialog before performing critical actions such as deletion or transmission of data. This is to ensure that users are aware of and confirm their intention to proceed with these actions, thereby preventing accidental deletions or transmissions.	Must
FR-0111.	Registration, configuration, and management of SP user accounts	The RI must provide functionality that allows of the Enforcing Authority to register, configure, and manage their own user accounts.	Must

ID	Title	Description	Priority
FR-0112.	Communication e-Form received outside the decentralized IT system	The RI should allow Competent Authority to respond to or otherwise communicate regarding an e-Form that was received outside the decentralized IT system.	Must
FR-0113.	Communication channel between Competent Authorities	The RI should enable Competent Authorities from different Member States to communicate before and after the issuance of an EPOC or EPOC-PR.	Could
FR-0114.	PDF upload	The RI should allow the user to upload a digitally signed PDF with all mandatory fields to send an e-Form, bypassing the full internal workflow.	Could
FR-0115.	Scanning and Upload of the Attachments	The system shall support efficient scanning and uploading of attached files. When a user attaches a file to the system, it will automatically undergo a scanning process for viruses, malware, and other security threats. Attachments will only be marked as being safe or potentially dangerous, there will be no blocking of any user actions.	Must
FR-0116.	Adding comments to the case	The system must allow users assigned to a case to add, edit, and remove comments related to the case, with the ability to attach and remove files to these comments. Additionally, the system must restrict visibility of these comments to internal users only and prevent their transmission through an e-Form to external parties.	Must

Table 2: Functional Requirements

2.3 Non-Functional Requirements

The following sections list the non-functional requirements that the technical architecture of the RI will be expected to meet.

2.3.1 Usability

Usability requirements concentrate on the ability of the system supporting the exchange of e-Forms using the Reference Implementation Software to be used by the end-users. It includes all the facilities developed or put into place to assist new end-users in getting operative.

ID	Title	Description	Priority
Non-Functional Requirements – Usability			
NFR-01.	Usability – Ease of use	The RI must have an intuitive and user-friendly interface for all user roles.	Must
NFR-02.	Usability – Error messages	The RI must produce clear error messages that give users a clear information on how to take corrective action.	Must
NFR-03.	Accessibility	The RI should be accessible to users with disabilities, adhering to relevant accessibility standards.	Must
NFR-04.	Usability - Alerts	The RI should to have an alert associated with any messages delay/error/urgency for that case.	Must

Table 3: Non-functional requirements – Usability

2.3.2 Security

Security requirements focus on the measures to be put into place to ensure good protection of the interconnected systems and of the information circulating between those systems.

ID	Title	Description	Priority
Non-Functional Requirements – Security			
NFR-05.	Overall level of security in the common domain	The level of security of the RI and the e-CODEX exchange system must fulfil the necessary security measures to ensure the confidentiality, integrity and availability of the entire system.	Must
NFR-06.	Overall level of security in national domain	The Member State authority in charge of the respective RI instance must ensure the overall system security and effectively implement the necessary measures for the proper functioning of that instance and the underlying national infrastructure.	Must
NFR-07.	Security – System reliability	The technical architecture of the RI is required to ensure a high level of reliability, resulting in a high level of confidence of the users of the system. The RI must perform consistently and according to its specifications.	Must

ID	Title	Description	Priority
NFR-08.	Security – System Confidentiality	The RI must ensure the confidentiality of all data assets protecting the information from loss or disclosure to unauthorized parties. It shall ensure that access must be restricted only to authorized users involved in each exchange.	Must
NFR-09.	Security – System Integrity	RI must ensure the integrity of data by maintaining its consistency, accuracy, and trustworthiness over its entire life cycle. Integrity of the data does not only refer to integrity of information itself but also to the origin integrity, that is, integrity of the source of information.	Must
NFR-10.	Security – System Availability	RI should never be the cause for data loss or for an unacceptable delay in the transmission of data.	Must
NFR-11.	Legitimate Use of the System	Security measures (referring to authentication, access control, and secure audit logs) shall be implemented such as to secure session management to prevent unauthorized access.	Must

Table 4: Non-functional requirements - Security

2.3.3 Personal Data Protection Aspects

Recital (90) of the e-evidence Regulation states that the RI should be designed, developed and maintained in compliance with the data protection requirements and principles laid down in *Regulation (EU) 2018/1725*, *Regulation (EU) 2016/679*, and *Directive (EU) 2016/680*, in particular the principles of data protection by design and by default as well as a high level of cybersecurity.

For example, Article 5(1)(f) of the Data Protection Regulation [REG 02] states that personal data shall be:

"processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')".

In practice, it means that appropriate security measures must be put in place to prevent the personal data held being accidentally or deliberately compromised. In particular, the Competent

Authorities and the Reference Implementation Software will need to ensure that the right physical and technical security, backed up by robust policies and procedures are implemented.

ID	Title	Description	Priority
Non-Functional Requirements – Data Protection			
NFR-12.	Data Protection	The RI must be designed and implemented in a manner that allows its users to ensure compliance with their obligations under the General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED) in processing personal data.	Must

Table 5: Non-functional requirements – Data Protection

2.3.4 Business Continuity

The business continuity requirements qualify the ability of the system to continue to reach its objectives after an unexpected event with minor or major consequence (disaster). These requirements are principally achieved through the deployment of redundant hardware and software, the use of fault tolerant systems, as well as a solid backup and recovery strategy.

ID	Title	Description	Priority
Non-Functional Requirements - Business Continuity			
NFR-13.	Business continuity – Fall-back procedure	The RI must foresee fall-back procedures in case the system is down. Fall-backs must be applied in two specific cases: • When the RI is not able to load an e-Form; • When the e-Form is not capable of being sent to the competent authority of the State concerned, due to communication failure. The fall-back procedures must ensure at least the same level of security as the primary transmission system.	Must

Table 6: Non-functional requirements - Business continuity

2.3.5 Development Qualities

Development qualities requirements consider the level of quality of the development process, including the effort and cost associated with current development as well as support for future changes or uses. Those qualities provide business value and have to do with the long-term use of the technical architecture.

ID	Title	Description	Priority
Non-Functional Requirements – Development Qualities			
NFR-14.	System configurability	The RI should be configurable in order to easily accept changes in the business requirements.	Should
NFR-15.	System testability	The RI implementation must be easy to test (automatically as much as possible).	Must
NFR-16.	System extensibility	The RI implementation should be easily extendable to other e-Forms application domains (instruments).	Must

Table 7: Non-functional requirements - Development qualities

2.3.6 Compliance

ID	Title	Description	Priority
Non-Functional Requirements - Compliance			
NFR-17.	Compliance to development standards	The RI implementation should be compliant with standards of development of IT systems.	Should

Table 8: Non-functional requirements – Compliance

Part II – Functional Analysis

3 Overview

The overview describes the processes and the actors involved in the exchanges under the *Regulation 2023/1543* to take place through the decentralised IT system.

3.1 Business Objective of the Process

The business objective of the EPOC and EPOC-PR exchanges processes described in this document is to allow and facilitate the digitalised exchange of information between Service Providers and competent authorities of the Member States. The scope of the Reference Implementation Software will allow the preparation and exchange of e-Forms in the field of EPOC and EPOC-PR.

This solution will, inter alia, cover exchanges based on the following forms:

- Annex I: European Production Order Certificate (EPOC) for the Production of Electronic Evidence;
- Annex II: European Preservation Order Certificate (EPOC-PR) for the Preservation of Electronic Evidence;
- Annex III: Information on the Impossibility of Executing an EPOC / EPOC-PR;
- Annex V: Confirmation of Issuance of a Request for Production following a European Preservation Order;
- Annex VI: Extension of the Preservation of Electronic Evidence.

3.2 Domains

As depicted on Figure , the overall exchange domain for the purposes of the RI can be divided into three domains: Common domain, National domain, and External domain. These domains are described in Table 9.

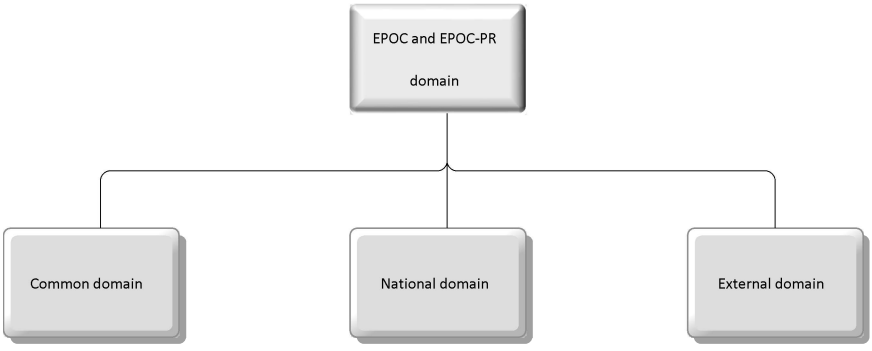

Figure 3-1: EPOC and EPOC-PR Exchange Domains

Domain	Definition
Common domain	The Common domain is the environment that allows the various Member State Administrations and Service Providers to intercommunicate.
National domain	The National domain is located in the Member State Administration environment. The National domain operates on one hand as a national network, which allows the national stakeholders to communicate with each other. On the other hand, it provides the national application, which allows the Member States Authorities to exchange information with the national applications of other Member States and of Service Providers.
External domain	The External domain is the environment that is outside the decentralised IT system, which is used for communication in the EPOC and EPOC-PR framework.

Table 9: Domains

3.3 Actors

The actors section describes the different actors involved in the EPOC and EPOC-PR exchange processes under the *Regulation 2023/1543*. These participants, or actors, are expected to utilize or operate the Reference Implementation Software.

Business Actors:

- Issuing State / Requesting Member State;
- Issuing Authority / Authority of the Requesting Member State;
- Legal representative and/or designated establishment of service provider;
- Enforcing State / Notified Member State;
- Enforcing Authority / Authority of the Notified Member State;
- Validating Authority;
- Central Authority;

The Table below provides the definition of the business actors according to the Regulation **[REG 01/Art.3]**.

Actors	Definition from the legal base
Issuing Authority	the competent authority in the issuing State, which can issue a European Production Order or a European Preservation Order.

Actors	Definition from the legal base
Enforcing Authority	the authority in the enforcing State, which, is competent to receive a European Production Order or a European Preservation Order transmitted by the issuing authority for notification or for enforcement.
Service Provider	any natural or legal person that provides one or more of the following categories of services, with the exception of financial services: (a) electronic communications services as defined in Article 2, point (4), of Directive (EU) 2018/1972; (b) internet domain name and IP numbering services, such as IP address assignment, domain name registry, domain name registrar and domain name-related privacy and proxy services; (c) other information society services as referred to in Article 1(1), point (b), of Directive (EU) 2015/1535 that: (i) enable their users to communicate with each other; or (ii) make it possible to store or otherwise process data on behalf of the users to whom the service is provided, provided that the storage of data is a defining component of the service provided to the user.
Validating Authority	the authority that validates the order. The types of validating authority: - judge, court or investigating judge; - public prosecutor.
Central Authority	an authority responsible for the administrative transmission and receipt of requests/orders, as well as for other official correspondence relating to requests/orders.

Table 10: Actors

3.4 User roles

The RI will implement **role-based access control** to ensure that access to data and system features are restricted according to the roles assigned to users. This approach guarantees that users can only access the data and functionalities that their roles permit.

1. **Role-Based Access Control**:

- Access to data and features within the RI are regulated based on user roles.

- Each role defines a specific set of access rights and permissions.

2. **Combined Access Rights**:

- A user's total access rights are the sum of the access rights associated with all the roles assigned to them.
- This means that if a user has multiple roles, they will have access to all the features and data allowed by each of those roles.

User roles and associated subsequent access rights are described below.

3.4.1 Functional user roles

The roles below correspond to operational user roles which a user can be granted in the RI . These roles are further described below:

1. Author;
2. Reviewer;
3. Signer 1 and Signer 2: for the purposes of signing Annex I and Annex II, where a signature of two authorities is necessary, two roles have been implemented to allow an EPOC/ EPOC-PR to be signed by an issuing authority and a validating authority;
4. Sender;
5. Supervisor;
6. Assigner;
7. Viewer.

3.4.2 Technical user roles

The following role handles the administration of the system. It is not implemented inside the RI and the activities related to it are completely handled outside of the system.

- Administrator:

  The “Administrator” user role is responsible for performing administration of the RI and typically has the following special access rights:
  - managing custom folders;
  - managing user accounts;
  - manage user roles;
  - manage communication with Service Providers and Member States end points.

While a distinction should be made between the following two profiles, there currently is no split implemented:

- **Technical administrator** to deal with technical aspects of the system, such as configuration, SSL certificates;
- **Business administrator** to grant the needed access rights to end users (practitioners) in the system. This is handled in KeyCloak

3.5 Roles & Permissions within the Issuing Authority for EPOC

Users with a particular role are granted certain permissions. In the table hereafter, the rights and permissions for EPOC Draft creation are listed.

ISSUING AUTHORITY	
Role	**Rights & Permissions**
Author	The "Author" user role is responsible for creating/editing draft EPOC and other messages using the RI and has the following rights and permissions: - Initiating an EPOC by creating a new case; - Editing an EPOC in draft status; - Attaching/deleting files to/from the EPOC until it is signed and sent to Service Provider/ Enforcing Authority; - Submitting a draft EPOC to the next step (review); - Deleting a draft, closed or withdrawn EPOC; - Searching EPOC cases; - Scheduling the download of the entire EPOC case as a ZIP file and then downloading the completed file once it is ready; - Importing an EPOC via web service into the RI; - Printing the content of an EPOC. Once the EPOC has been issued, the Author can: - View all types of incoming messages; - Editing all types of messages available under the workflow dropdown list; - Sending all types of messages available under the workflow dropdown list; - Close a case; - Reopen a closed case.
Reviewer	The "Reviewer" user role is responsible for reviewing a draft EPOC, and where applicable other communication messages, in the RI before it is

	signed and transmitted. The Reviewer has the following rights and permissions: - Reviewing the content of the EPOC. Based on this review, the user can: o **Edit** the data in the e-Form. o **Return the e-Form** to Author to make the necessary amendments as indicated in the comments. o **Reject the e-Form:** Send back to the Author (with comments). This is also a final workflow state, no further actions can be taken on this e-Form once rejection is done. o **Accept the e-Form:** Push the e-Form to the next step of the workflow: signing**.** - Deleting a draft, closed or withdrawn EPOC; - Searching EPOC cases; - Scheduling the download of the entire EPOC case as a ZIP file and then downloading the completed file once it is ready; - Printing the content of an EPOC; - Attaching/deleting files to/from the EPOC until it is signed and sent to Service Provider/ Enforcing Authority. Once the EPOC has been issued, the Reviewer can: - View all types of incoming messages; - Editing all types of messages available under the workflow dropdown list; - Sending all types of messages available under the workflow dropdown list; - Close a case; - Reopen a closed case.
Signer 1	The "Signer 1" user role is responsible for signing an EPOC, and where applicable other communication messages, as a member of the issuing authority and has the following rights and permissions: - Reviewing the content of the EPOC. After the review, Signer 1 can: o **Edit** the fields within an e-Form. o **Return the e-Form** to the Reviewer to make the necessary amendments as indicated in the comments. o **Reject the e-Form**: Send the e-Form back to the "Reviewer" (with comments). This is also a final workflow state, no further actions can be taken on this e-Form.

	○ **Sign the e-Form (Sections A-L)** as a member of the issuing authority and: ▪ In case a signature of the validating authority is required, push it to the next step of the workflow - second signature performed by Signer 2. ▪ In case a validating authority is not involved in EPOC Draft creation, Signer 1 fills in and signs Section M of the e-Form. - Deleting a draft, closed or withdrawn EPOC; - Searching EPOC cases; - Scheduling the download of the entire EPOC case as a ZIP file and then downloading the completed file once it is ready; - Printing the content of an EPOC; - Attaching/deleting files to/from the EPOC until it is signed and sent to Service Provider/ Enforcing Authority. Once the EPOC has been issued, the Signer 1 can: - View all types of incoming messages; - Editing all types of messages available under the workflow dropdown list; - Sending all types of messages available under the workflow dropdown list; - Close a case; - Reopen a closed case.
Signer 2	The "Signer 2" user role is responsible for signing an e-Form as a member of the validating authority before it is sent out to an Service Provider/ Enforcing Authority uing the RI. The Signer 2 has the following rights and permissions: - Reviewing the content of the EPOC (read only). After the e-Form review, the following actions can be taken: ○ **Return the e-Form** to "Reviewer" to make the necessary amendments as indicated in the comments. ○ **Reject the e-Form:** Send the e-Form back to the "Signer 1" (with comments). This is also a final workflow state, no further actions can be taken on this e-Form. ○ **Sign the e-Form (Sections A-L)** as a member of the validating authority. ○ In case a notification to the enforcing authority is required, Signer 2 fills in and signs Section M of an

	e-Form, thereby pushing it to the next step of the workflow: Sending. - Searching EPOC cases; - Scheduling the download of the entire EPOC case as a ZIP file and then downloading the completed file once it is ready; - Printing the content of an EPOC. Once the EPOC has been issued, the Signer 2 can: - View all types of incoming messages; - Editing all types of messages available under the workflow dropdown list; - Sending all types of messages available under the workflow dropdown list; - Close a case; - Reopen a closed case.
Sender	The "Sender" user role is responsible for sending a signed EPOC to a Service Provider and, if applicable, the Enforcing Authority. The Sender has the following roles and permissions: - Scheduling the download of the entire EPOC case as a ZIP file and then downloading the completed file once it is ready; - Printing the content of an EPOC. - Sending an EPOC.
Supervisor	The "Supervisor" user role is responsible for all possible actions listed in this table (applicable to previous roles). That role is able to perform the whole workflow without any additional role in the RI. Additionally, Supervisor has the following rights and permissions: - Viewing all incoming communication in the authority; - Searching EPOC cases; - Assigning users to an EPOC case; - Adding and/or removing users from an EPOC case; - Sharing an EPOC with a user with the "Supervisor" role in a different authority (within the same installation); - Reading permissions for all cases in the authority; - Creating, signing (where applicable) and sending communication messages to other competent authorities and the Service Provider; - Scheduling the download of the entire EPOC case as a ZIP file and then downloading the completed file once it is ready; - Printing the content of an EPOC; - Editing all types of messages available under the workflow dropdown list;

	- Sending all types of messages available under the workflow dropdown list; - Close a case; - Reopen a closed case.
Viewer	The "Viewer" user role is intended for read-only access to the case or draft shared with them. A Viewer cannot edit or modify the case, nor can they send messages to the Service Provider or Enforcing Authority. However, a Viewer can add comments to the case timeline and attach files to those comments.
Assigner	The 'Assigner' user role is designed for providing support to other roles in performing administrative tasks. The assigner can't edit the data in the e-Form but can attach/delete files to/from the EPOC until it is signed and sent out. The Assigner has the following rights and permissions: - Viewing all incoming communication in the authority; - Adding and/or removing users to/from the EPOC case; - Attaching/deleting files to/from an e-Form until it is signed and sent out. - Scheduling the download of the entire EPOC case as a ZIP file and then downloading the completed file once it is ready; - Printing the content of the EPOC; - Reading permissions for all cases in the authority.

Table 11: Roles and Descriptions within the Issuing Authority for EPOC

3.6 Roles & Permissions within the Enforcing Authority for EPOC

Please note that user roles and permissions on the Enforcing Authority's side have been implemented taking into account the following information:

- Users with Assigner and Supervisor role see all incoming cases and can also take all actions on those cases (editing answers, adding attachments, sending messages). They assign other users to the cases (users with the same roles as those defined for the issuing authority) to work on them.
- The main difference between the Supervisor and the Assigner role is that the latter can only assign users from their own authority, while the Supervisor can share cases with users from other authorities.

ENFORCING AUTHORITY

Role	Rights & Permissions
Author	Users with "Author" role, if assigned to a particular EPOC, can: - View all incoming communication; - Send Grounds for Refusal to Service Provider and Issuing Authority; - Send 'Confirmation about the end of transaction' message after receiving 'Withdrawal' message; - Provide decision about the outcome of the enforcement procedure ('Not Recognise' /'Recognition Decision' message); - Send 'Agree/Disagree with Objections' message upon receiving an objection to comply with enforcement decision from Service Provider; - Send a request for additional information to all parties involved in EPOC processing; - Send other information to all parties involved in EPOC processing; - Schedule the download of the entire EPOC case as a ZIP file and then download the completed file once it is ready; - Close a case; - Reopen a closed case.
Reviewer	Users with "Reviewer" role, if assigned to a particular EPOC, can: - View all incoming communication; - Send Grounds for Refusal to Service Provider and Issuing Authority; - Send 'Confirmation about the end of transaction' message after receiving 'Withdrawal' message; - Provide decision about the outcome of the enforcement procedure ('Not Recognise' /'Recognition Decision' message); - Send 'Agree/Disagree with Objections' message upon receiving an objection to comply with enforcement decision from Service Provider; - Send a request for additional information to all parties involved in EPOC processing; - Send other information to all parties involved in EPOC processing; - Schedule the download of the entire EPOC case as a ZIP file and then download the completed file once it is ready; - Close a case; - Reopen a closed case.
Signer 1 and Signer 2	Users with "Signer 1" and "Signer 2" role, if assigned to a particular EPOC, can: - View all incoming communication;

	- Send Grounds for Refusal to Service Provider and Issuing Authority; - Send 'Confirmation about the end of transaction' message after receiving 'Withdrawal' message; - Provide decision about the outcome of the enforcement procedure ('Not Recognise' /'Recognition Decision' message); - Send 'Agree/Disagree with Objections' message upon receiving an objection to comply with enforcement decision from Service Provider; - Send a request for additional information to all parties involved in EPOC processing; - Send other information to all parties involved in EPOC processing; - Schedule the download of the entire EPOC case as a ZIP file and then download the completed file once it is ready; - Close a case; - Reopen a closed case.
Sender	Users with "Sender" role, if assigned to a particular EPOC, can: - View all incoming communication; - Send Grounds for Refusal to Service Provider and Issuing Authority; - Send 'Confirmation about the end of transaction' message after receiving 'Withdrawal' message; - Provide decision about the outcome of the enforcement procedure ('Not Recognise' /'Recognition Decision' message); - Send 'Agree/Disagree with Objections' message upon receiving an objection to comply with enforcement decision from Service Provider; - Send a request for additional information to all parties involved in EPOC processing; - Send other information to all parties involved in EPOC processing; - Schedule the download of the entire EPOC case as a ZIP file and then download the completed file once it is ready; - Close a case; - Reopen a closed case.
Supervisor	Users with "Author" role, if assigned to a particular EPOC, can: - View all incoming communication; - Forward the EPOC; - Send Grounds for Refusal to Service Provider and Issuing Authority; - Send 'Confirmation about the end of transaction' message after receiving 'Withdrawal' message;

	- Provide decision about the outcome of the enforcement procedure ('Not Recognise' /'Recognition Decision' message); - Send 'Agree/Disagree with Objections' message upon receiving an objection to comply with enforcement decision from Service Provider; - Send a request for additional information to all parties involved in EPOC processing; - Send other information to all parties involved in EPOC processing; - Schedule the download of the entire EPOC case as a ZIP file and then download the completed file once it is ready; - Close a case; - Reopen a closed case.
Viewer	Users with "Viewer role"can: - View (read-only) all EPOCs that the user is assigned to; - View all incoming communication; - Schedule the download of the entire EPOC case as a ZIP file and then download the completed file once it is ready.
Assigner	This role can: - View all incoming communication in the authority; - Add and/or remove users to/from the received EPOC case; - Schedule the download of the complete case to a ZIP file and then download the completed file once it is ready; - Read permissions for all cases in the authority.

Table 12: Roles and Descriptions within the Enforcing Authority for EPOC

3.7 Roles & Permissions within the Issuing Authority for EPOC-PR

Users with a particular role are granted certain permissions. In the table hereafter, the rights and permissions for EPOC-PR Draft creation are listed.

ISSUING AUTHORITY	
Role	**Rights & Permissions**
Author	The "Author" user role is responsible for creating/editing EPOC-PR Draft and other communication messages using the RI and has the following rights and permissions: - Initiating an EPOC-PR by creating a new case;

	- Editing an EPOC-PR in draft status; - Attaching/deleting files to/from the EPOC-PR until it is signed and sent to Service Provider/ Enforcing Authority; - Submitting a draft EPOC-PR to the next step (review); - Deleting a draft, closed or withdrawn EPOC-PR; - Searching EPOC-PR cases; - Scheduling the download of the entire EPOC-PR case as a ZIP file and then downloading the completed file once it is ready; - Importing an EPOC-PR via web service into the RI; - Printing the content of an EPOC-PR. Once the EPOC has been issued, the Author can: - View all types of incoming messages; - Editing all types of messages available under the workflow dropdown list; - Sending all types of messages available under the workflow dropdown list; - Close a case; - Reopen a closed case.
Reviewer	The "Reviewer" user role is responsible for reviewing a draft EPOC-PR, and where applicable other communication messages, in the RI before it is signed and transmitted. The Reviewer has the following rights and permissions: - Review the EPOC-PR contents. Based on this review, the user can: o **Edit** the data in the e-Form; o **Return the e-Form** to Author to make the necessary amendments as indicated in the comments. o **Reject the e-Form:** Send the e-Form back to the Author (with comments). This is also a final workflow state, no further actions can be taken on this e-Form once rejection is done. o **Accept:** Push the e-Form to the next step of the workflow: Signing. - Attaching/deleting files to/from the EPOC-PR until it is signed and sent to Service Provider/ Enforcing Authority; - Deleting a draft, closed or withdrawn EPOC-PR; - Searching EPOC-PR cases; - Scheduling the download of the entire EPOC-PR case as a ZIP file and then downloading the completed file once it is ready; - Printing the content of an EPOC-PR.

	Once the EPOC has been issued, the Reviewer can: - View all types of incoming messages; - Editing all types of messages available under the workflow dropdown list; - Sending all types of messages available under the workflow dropdown list; - Close a case; - Reopen a closed case.
Signer 1	The "Signer 1" user role is responsible for signing an EPOC-PR, and where applicable other communication messages, as a member of an issuing authority and has the following rights and permissions: - Review the content of the EPOC-PR. After the review, the Signer 1 can: o ~~Edit the fields within Section A-G.~~ o **Return the e-Form** to "Reviewer" to make the necessary amendments as indicated in the comments. o **Reject the e-Form**: Send the e-Form back to the "Reviewer" (with comments). This is also a final workflow state, no further actions can be taken on this e-Form. o **Sign the e-Form** (Sections A-G), thereby pushing it to the next step of the workflow (either second signature or sending phase). - Attaching/deleting files to/from the EPOC-PR until it is signed and sent to Service Provider/ Enforcing Authority; - Deleting a draft, closed or withdrawn EPOC-PR; - Searching EPOC-PR cases; - Scheduling the download of the entire EPOC-PR case as a ZIP file and then downloading the completed file once it is ready; - Printing the content of an EPOC-PR. Once the EPOC has been issued, the Signer 1 can: - View all types of incoming messages; - Editing all types of messages available under the workflow dropdown list; - Sending all types of messages available under the workflow dropdown list; - Close a case; - Reopen a closed case.

Signer 2	The "Signer 2" user role is responsible for signing an EPOC-PR, and where applicable other communication messages, as member of validating authority before it is sent out to a Service Provider using the RI. The Signer 2 has the following rights and permissions: - Review the content of the EPOC-PR(read only). After the e-Form review, the following actions can be taken: o **Return the e-Form to** "Reviewer" to make the necessary amendments as indicated in the comments. o **Reject:** Send the e-Form back to the "Signer 1" (with comments). This is also a final workflow state, no further actions can be taken on this e-Form. o **Sign the e-Form** (Sections A-G), thereby pushing it to the next step: Sending. - Deleting a draft, closed or withdrawn EPOC-PR; - Searching EPOC-PR cases; - Scheduling the download of the entire EPOC-PR case as a ZIP file and then downloading the completed file once it is ready; - Printing the content of an EPOC-PR. Once the EPOC has been issued, the Signer 2 can: - View all types of incoming messages; - Editing all types of messages available under the workflow dropdown list; - Sending all types of messages available under the workflow dropdown list; - Close a case; - Reopen a closed case.
Sender	The "Sender" user role is responsible for sending a signed EPOC-PR to a Service Provider. A Sender has the following roles and permissions: - Scheduling the download of the entire EPOC case as a ZIP file and then downloading the completed file once it is ready; - Printing the content of an EPOC-PR. - Sending an EPOC-PR.
Supervisor	The "Supervisor" user role is responsible for all possible actions listed in this table (applicable to previous roles). That role is able to perform the whole workflow without any additional role in the RI. Additionally, Supervisor has the following rights and permissions: - Viewing all incoming communication in the authority; - Searching EPOC-PR cases;

	- Assigning users to an EPOC-PR case; - Adding and/or removing users from an EPOC-PR case; - Sharing an EPOC-PR with a user with the "Supervisor" role in a different authority (within the same installation); - Reading permissions for all cases in the authority; - Creating, signing (where applicable) and sending communication messages to other competent authorities and the Service Provider; - Scheduling the download of the entire EPOC-PR case as a ZIP file and then downloading the completed file once it is ready; - Printing the content of an EPOC-PR; - Editing all types of messages available under the workflow dropdown list; - Sending all types of messages available under the workflow dropdown list; - Close a case; - Reopen a closed case.
Viewer	The "Viewer" user role is intended for read-only access to the case or draft shared with them. A Viewer cannot edit or modify the case, nor can they send messages to the Service Provider. However, a Viewer can add comments to the case timeline and attach files to those comments.
Assigner	The 'Assigner' user role is designed for providing support to other roles in performing administrative tasks. The assigner can't edit the data in the e-Form but can attach/delete files to/from the EPOC-PR until it is signed and sent out. The Assigner has the following rights and permissions: - Viewing all incoming communication in the authority; - Adding and/or removing users to/from the EPOC-PR case; - Attaching/deleting files to/from an e-Form until it is signed and sent out.

Table 13: Roles and Descriptions within the Issuing Authority for EPOC-PR

3.8 Roles & Permissions within the Enforcing Authority for EPOC-PR

As far as EPOC-PR is concerned, the Enforcing Authority may receive the following forms and messages:

- Form 3 from the Service Provider;
- Request for Additional Information;
- Send Other Information;

In these scenarios, the Enforcing Authority has not received the original parent form (Form 2). As a result, only the Supervisor/Assigner has the ability to view and respond to the incoming messages, unless they assign them to another user from their own authority.

3.9 User management

User login is currently handled by the Keycloak REST API. This component is interfaceable with the EU-Login or, if required, with other authentication methods used by Member States.

The Administrator within the Competent Authority of a Member State is responsible for assigning one or more User Roles (as defined in Section 3.4.2) to the specific user, granting her/him the defined rights and permissions.

- Each user should be linked to only one Competent Authority of a Member State;
- Each user will have at least one User Role assigned. Without a role assigned, a user has access to no Case at all.
- Users may be assigned at any level (authority and/or department).
- A user can be associated to only one authority, if by mistake the user will be associated to multiple authorities, the RI will consider only the first one found during the retrieve process to be valid.
- User with Supervisor and/or Assigner role within the Competent Authority of a Member State is able to see all the cases that are sent/ received in that Competent Authority, working like a functional mailbox, subject to restrictions based on the user roles.

3.10 EPOC and EPOC-PR Global Business Processes and Sub-Processes

The following section defines the main processes and Sub-Processes of the RI. They are presented in the figures below.

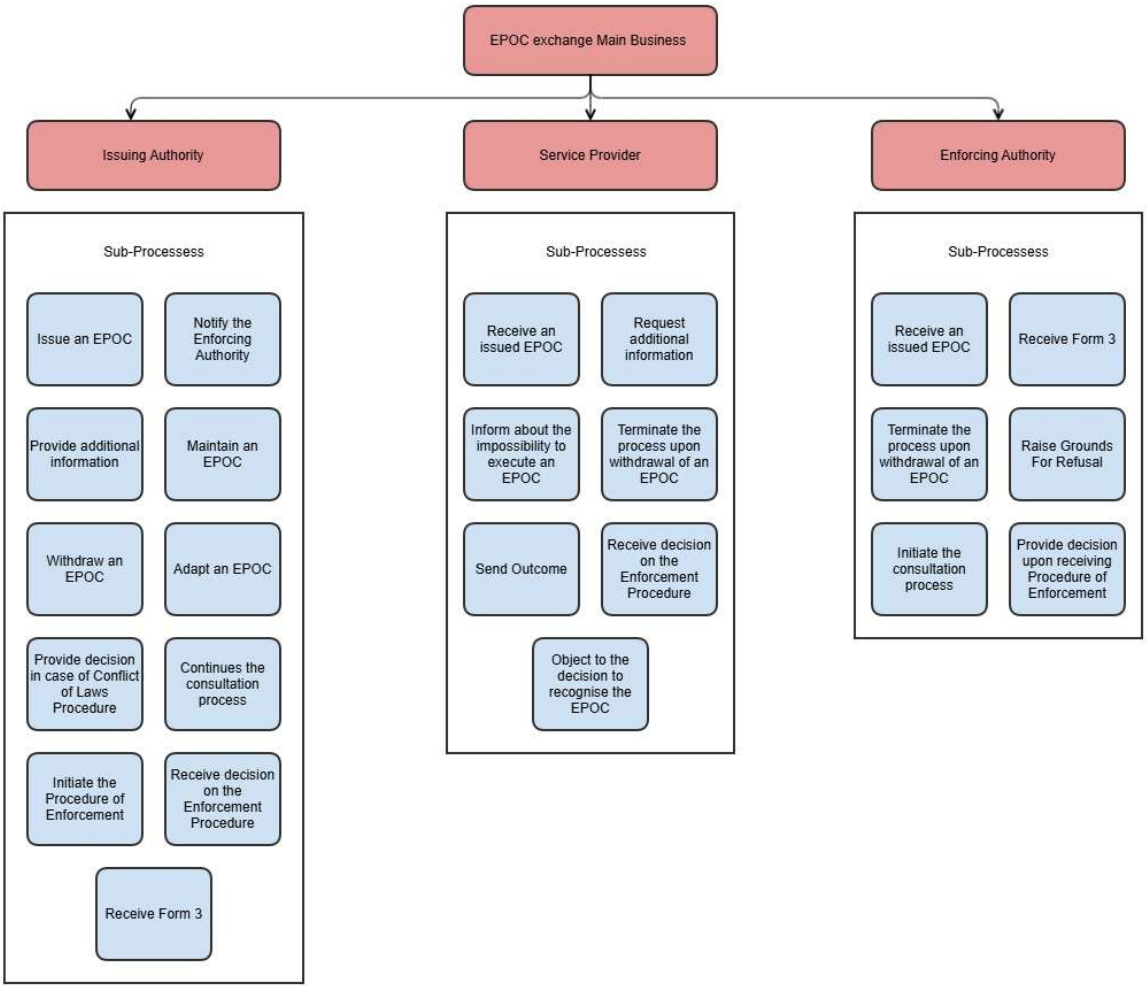

Figure 3-2: EPOC exchange Main Business

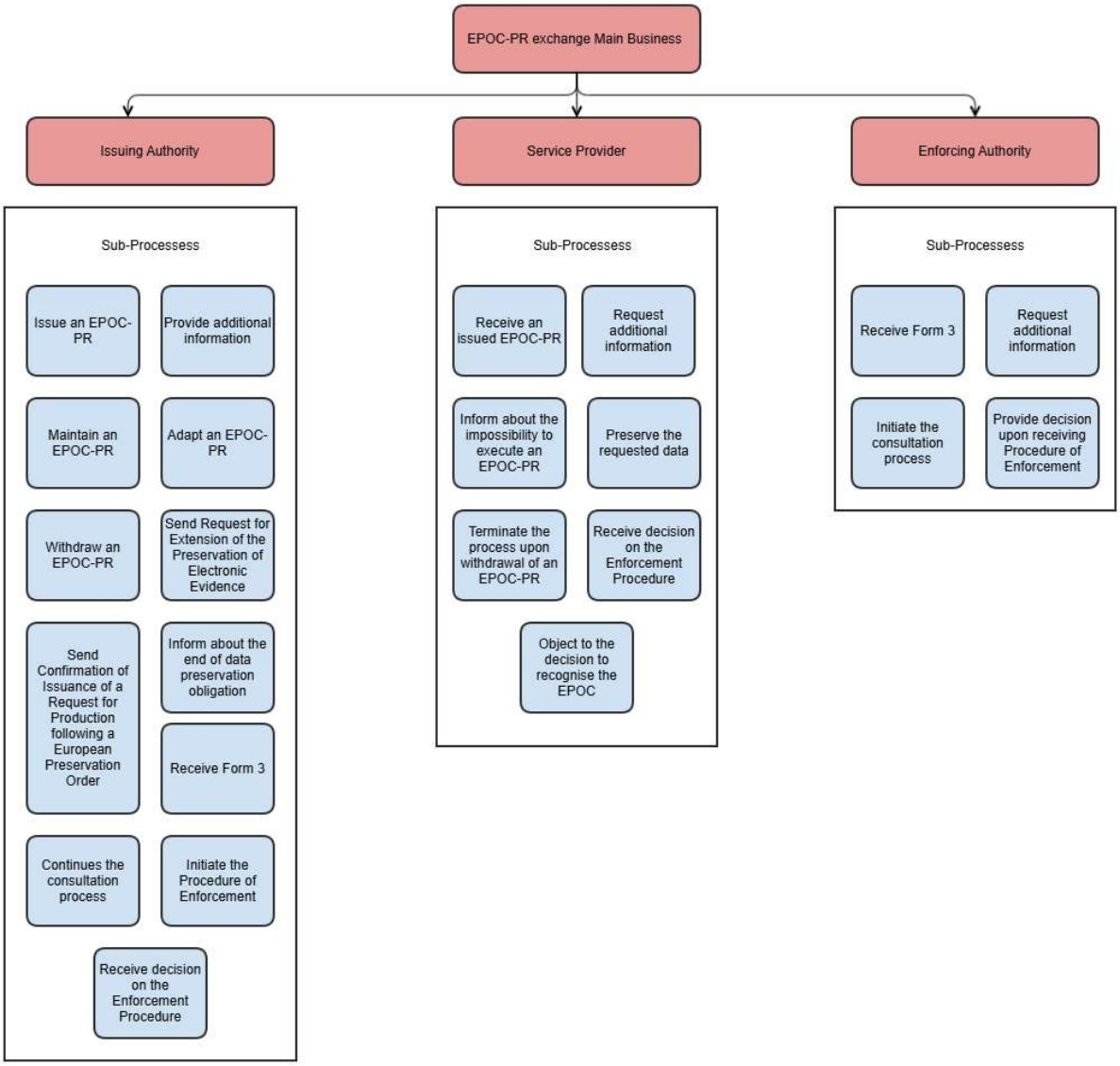

Figure 3-3: EPOC-PR exchange Main Business Processes

4 EPOC and EPOC-PR Business Processes

The e-Evidence processes listed in this document are defined in the high-level diagrams.

The list of these diagrams covers all the main and common processes defined in section 3.10:

- Request Production of Electronic Evidence Process;
- Provide Electronic Evidence Process;
- Request Preservation of Electronic Evidence Process;
- Preserve Electronic Evidence Process - Confirmation;
- Request Enforcement Procedure Process;
- Execute Enforcement Procedure Process.

For further details on those processes, please refer to the e-Evidence Business Collaboration Document [RD 01].

4.1 Time Limits

The *Regulation 2023/1543* outlines specific procedures and deadlines for the execution of European Production Order Certificates (EPOCs) and European Preservation Order Certificates (EPOC-PRs). By adhering to these deadlines, Member States and Service Providers can ensure efficient and lawful handling of electronic data. This chapter details the mandatory deadlines and actions required upon receipt of an EPOC and/or EPOC-PR.

4.1.1 Legal deadlines for the execution of the European Production Order Certificate (EPOC):

Upon receipt of an EPOC, the addressee (the legal representative or a designated establishment of a Service Provider) is required to act promptly to preserve the requested data. Immediate action ensures that evidence remains intact and accessible for the duration of the legal proceedings.

4.1.1.1 Non-emergency cases

In case notification to the Enforcing Authority is required:

- **Initial Period**: If a notification to the Enforcing Authority is mandated, and no grounds for refusal are raised by the Enforcing Authority within 10 days of receiving the EPOC, the Service Provider must transmit the requested data directly to the indicated authority(ies) of the issuing State at the end of this 10-day period.

- **Early Confirmation**: If the Enforcing Authority does not raise any grounds for refusal, they still need to inform the Service Provider about that before the end of the 10-day period. The Service Provider must act as soon as possible upon receiving this confirmation and, at the latest, by the end of the 10-day period.

In case notification to the Enforcing Authority is not required, the Service Provider must transmit the requested data directly to the Issuing Authority or law enforcement authorities within 10 days of receiving the EPOC.

4.1.1.2 Emergency cases

In emergency cases, the *Regulation* stipulates an accelerated timeline:

- **Immediate Response**: If there was no notification to the Enforcing Authority, the Service Provider must transmit the requested data without undue delay and within 8 hours upon receiving the EPOC.

- **Enforcing Authority Objection**: If a notification to the Enforcing Authority is required and it decides to raise grounds for refusal, it must notify the Issuing Authority and the Service Provider within 96 hours of receiving the notification. If the data has already been transmitted, the Issuing Authority must either delete or restrict the use of the data or comply with any specified conditions imposed by the Enforcing Authority.

4.1.1.3 Clarification and Correction

If the EPOC is incomplete or contains errors or insufficient information, the addressee must inform the Issuing Authority and the Enforcing Authority (if applicable) without undue delay and seek clarification using Annex III of the *Regulation*. The Issuing Authority must respond expeditiously, within 5 days, providing the necessary clarification or correction.

Note: Sending Annex III in that scenario pauses the 10-day deadline on the side of the Service Provider until clarification from the Issuing Authority is received.

At the same time, the Service Provider must preserve the data until they are transmitted, irrespective of whether the production is ultimately requested via a clarified EPOC or other legal channels, or until the EPOC is withdrawn. If data preservation is no longer necessary, the Issuing and, if applicable, Enforcing Authority must inform the addressee without undue delay.

4.1.1.4 Setting new deadline by the Issuing Authority

A new deadline may be set by the Issuing Authority after sending “Maintain” message to the Service Provider and the Enforcing Authority, in case of impossibility to execute the EPOC due to any other reason. It is essential for the Issuing Authority to communicate any changes in

deadlines clearly and promptly to all relevant parties, ensuring transparency and fairness in the process.

4.1.1.5 Conflict of Laws and Effective Remedies

If the Service Provider believes that complying with an EPOC conflicts with a third country's legal obligations, they must inform both the Issuing and Enforcing Authority. This is done by using Annex III, detailing the conflicting obligations. This objection must be submitted no later than 10 days after receiving the EPOC. Upon receiving the reasoned objection, the Issuing Authority reviews the EPOC. If the authority decides to uphold the order, it must request a review by the competent court of the Issuing State. The execution of the EPOC is suspended pending the court's review. The time limits should be calculated based on the national law of the Issuing Authority.

Additionally, individuals whose data were requested via an EPOC, have the right to effective remedies against the order. This includes challenging the legality, necessity, and proportionality of the order in the Issuing State's courts. The same time limits and conditions for seeking remedies in similar domestic cases apply to EPOCs. This ensures the effective exercise of rights.

4.1.2 Legal deadlines for the execution of the European Preservation Order Certificate (EPOC-PR):

Upon receiving an EPOC-PR, the Service Provider must, without undue delay, preserve the requested data. This obligation is crucial to ensure that the data remains intact and available for subsequent legal processes.

If preservation is no longer necessary, the Issuing Authority must inform the Service Provider without undue delay. Upon receiving this notification, the obligation to preserve the data ceases immediately.

4.1.2.1 Standard Preservation Timeline

Upon receipt of an EPOC-PR, the data must be preserved for 60 days. This period provides the Issuing Authority sufficient time to confirm whether a subsequent request for production will be made.

If the Issuing Authority confirms, using the form set out in Annex V, that a subsequent request for production has been issued, the Service Provider must continue to preserve the data as long as necessary to fulfill the production request.

4.1.2.2 Extension of Preservation Period

During the initial 60-day period, the Issuing Authority may extend the preservation obligation by an additional 30 days if necessary, to allow time for issuing a subsequent production request. This extension must be communicated using Annex VI of the *Regulation*.

4.1.2.3 Handling Incomplete or Erroneous EPOC-PRs

If the EPOC-PR is incomplete, contains manifest errors, or lacks sufficient information, the addressee must notify the issuing authority without undue delay and seek clarification using the Annex III. The Issuing Authority must respond expeditiously, within 5 days, to provide the necessary information or corrections.

4.1.3 Legal deadlines for the Enforcement Procedures (EPOC & EPOC-PR)

Upon receipt of the "Procedure of Enforcement Form", the Enforcing Authority must recognize and take necessary measures without further formalities. The decision must be made without undue delay and within five working days of receiving the order.

Before deciding not to recognize or enforce the order, the enforcing authority must consult with the Issuing Authority and may request additional information. The Issuing Authority must respond to such message within five working days.

4.1.3.1 Notification and Data Transmission

The Enforcing Authority must immediately notify the Issuing Authority and the Service Provider of its decisions.

If the Enforcing Authority obtains the requested data, it must transmit the data to the Issuing Authority without undue delay.

5 Functional Messages

The exchange of information is based on message-oriented approach. This chapter lists the business messages in the context of EPOC and EPOC-PR exchanges. This document will not specify the way these messages are encoded, nor the protocol used to transport them, which are more technical issues.

In the decentralised IT system, we can distinguish three groups of messages:

1. Messages for which a form already exists and is clearly defined. These messages are those based of the forms attached to the Regulation (EU) 2023/1543. These are namely:
    a. Annex I – European Production Order Certificate (EPOC) for the Production of Electronic Evidence;
    b. Annex II – European Preservation Order Certificate (EPOC-PR) for the Preservation of Electronic Evidence;
    c. Annex III – Information on the Impossibility of Executing an EPOC / EPOC-PR;
    d. Annex V – Confirmation of Issuance of a Request for Production Following a European Preservation Order;
    e. Annex VI – Extension of the Preservation of Electronic Evidence.
2. Messages for which the corresponding form does not exist but the foreseen XML format has a more complex structure than a simple text form.
3. Messages identified during the business workflow analysis for which the corresponding form does not exist but a simple free form message can be used.

The messages that can be foreseen are listed in the following section.

5.1 Messages

5.1.1 From the Issuing Authority

5.1.1.1 To the Enforcing Authority

The following messages can be sent:

- **Annex I –** European Production Order Certificate (EPOC) for the Production of Electronic Evidence (with section M filled);

- **'Set New Deadline'** message - The purpose of the message is to set a new deadline for the Service Provider (SP) to deliver the requested data. This can be sent after a "Maintain" message in case of impossibility to execute due to any other reason;
- **'Adapt'** message - A decision of the Issuing Authority to adapt the initial reques upon receipt of Annex III, where reasons for non-execution of the request are explained by the Service Provider, or after discussion with the notified Enforcing Authority;
- **'Inform about Going to Court'** message - The message notifies the Enforcing Authority that the Issuing Authority, disagreeing with the reasons given in Annex III, is upholding the EPOC and intends to proceed to court;
- '**Maintain**' message - A decision of the Issuing Authority to maintain the initial request upon receipt of Annex III, where reasons for non-execution of the request are explained by the Service Provider, or after discussion with the notified Enforcing Authority;
- **'Send Other Information'** message - A service message initiating a consultation process which can be sent at any time of case processing once an e-Form is issued;
- **'Procedure of Enforcement'** message - The message allows the Issuing Authority to initiate enforcement procedure if the Service Provider fails to comply with an EPOC or EPOC-PR;
- **'Withdrawal'** message - A decision of the Issuing Authority to withdraw the initial request, thereby terminating the process when it is no longer needed;
- **'Reply to Request For Additional Information'** message - Reply to the received Request for Additional Information.

5.1.1.2 To the Service Providers

The following messages can be sent:

- **Annex I** – European Production Order Certificate (EPOC) for the Production of Electronic Evidence;
- **Annex II** – European Preservation Order Certificate (EPOC-PR) for the Preservation of Electronic Evidence;
- **Annex V** – Confirmation of Issuance of a Request for Production Following a European Preservation Order;
- **Annex VI** – Extension of the Preservation of Electronic Evidence;

- **'Set New Deadline'** message - The purpose of the message is to set a new deadline for the Service Provider (SP) to deliver the requested data. This can be sent after a "Maintain" message in case of impossibility to execute due to any other reason;
- **'Adapt'** message - A decision of the Issuing Authority to adapt the initial request upon receipt of Annex III, where reasons for non-execution of the request are explained by the Service Provider, or after discussion with the notified Enforcing Authority;
- **'Inform about Going to Court'** message - The message notifies the Service Provider and that the Issuing Authority, disagreeing with the reasons given in Annex III, is upholding the EPOC and intends to proceed to court;
- **'Maintain'** message - A decision of the Issuing Authority to maintain the initial request upon receipt of Annex III, where reasons for non-execution of the request are explained by the Service Provider, or after discussion with the notified Enforcing Authority;
- **'No Longer Need to Preserve Data'** message - The message notifies the Service Provider that data preservation is no longer required, ending the preservation obligation;
- **'Send Other Information'** message - A service message initiating a consultation process which can be sent at any time of case processing once an e-Form is issued;
- **'Procedure of Enforcement'** message - The message allows the Issuing Authority to initiate enforcement procedure if the Service Provider fails to comply with an EPOC or EPOC-PR;
- **'Reply to Request For Additional Information'** message - Reply to the received Request for Additional Information;
- **'Withdrawal'** message - A decision of the Issuing Authority to withdraw the initial request, thereby terminating the process when it is no longer needed.

5.1.1.3 To the Court in Issuing Member State

The following messages can be sent:

- **'Go to Court to Decide'** message – The message is sent to the Court in issuing State to assesses the EPOC and the objections from the SP for not providing data.

5.1.2 From the Enforcing Authority

5.1.2.1 To the Issuing Authority

The following messages can be sent:

- **'Grounds For Refusal'** message - The message enables the Enforcing Authority to communicate whether it has grounds for refusal or not after reviewing Annex I (with Section M completed) or Annex III from the Service Provider;
- **'Agree with Objection'** message - A decision of the Enforcing Authority after receiving an "Objection" message from the Service Provider;
- '**Confirmation about the end of the transaction'** message – Confirmation of Withdrawal;
- **'Disagree with Objection'** message - A decision of the Enforcing Authority after receiving an "Objection" message from the Service Provider;
- **'Not Recognise'** message - The message allows the Enforcing Authority to provide a decision not to recognise the order upon receipt of the 'Procedure of Enforcement' message;
- **'Request for Additional Information'** message - Consultation process is initiated;
- **'Send Other Information'** message - A service message initiating a consultation process which can be sent at any time of case processing once an e-Form is issued;
- **'Recognition Decision'** message - Upon receipt of the 'Procedure of Enforcement' message, the Enforcing Authority sends the "Recognition Decision" formally requiring the addressee to comply with the order.

5.1.2.2 To the Service Providers

The following messages can be sent:

- **'Grounds For Refusal'** message - The message enables the Enforcing Authority to communicate whether it has grounds for refusal or not after reviewing Annex I (with Section M completed) or Annex III from the Service Provider;
- **'Agree with Objection'** message - A decision of the Enforcing Authority after receiving an "Objection" message from the Service Provider;
- **'Disagree with Objection'** message - A decision of the Enforcing Authority after receiving an "Objection" message from the Service Provider;
- **'Not Recognise'** message - The message allows the Enforcing Authority to provide a decision not to recognise the order upon receipt of the 'Procedure of Enforcement' message;

- **'Send Other Information'** message - A service message initiating a consultation process which can be sent at any time of case processing once an e-Form is issued;
- **'Recognition Decision'** message - Upon receipt of the 'Procedure of Enforcement' message, the Enforcing Authority sends the "Recognition Decision" formally requiring the addressee to comply with the order.

5.1.3 From the Service Providers

5.1.3.1 To the Issuing Authority

The following messages can be sent:

- **Annex III** – Information on the Impossibility of Executing an EPOC / EPOC-PR;
- **'Status of the Preservation Request'** message - The Service Provider sends a confirmation about preserving the requested data to the Issuing Authority;
- **'Request For Additional Information'** message - Consultation process is initiated;
- **'Reply to Request for Additional Information'** message - Reply to the received Request for Additional Information;
- **'Confirmation about the end of the transaction'** message - Confirmation of Withdrawal;
- **'Send Other Information'** message - A service message initiating a consultation process which can be sent at any time of case processing once an e-Form is issued;
- **'Outcome'** message - The message allows the Service Provider to send the requested data to the respective authority in the issuing State. In case of large file sizes, only the manifest would be sent through the RI, indicating how to download the requested data outside of the decentralised IT system. Outcome can be sent in several parts whenever needed.

5.1.3.2 To the Enforcing Authority

The following messages can be sent:

- **Annex III** – Information on the Impossibility of Executing an EPOC / EPOC-PR;
- **'Objection'** message - The message notifies that the Service Provider objects to comply with the order upon receiving "Recognition Decision" from the Enforcing Authority;
- **'Send Other Information'** message - A service message initiating a consultation process which can be sent at any time of case processing once an e-Form is issued;

- **'Request for Additional Information'** message - Consultation process is initiated;
- **'Reply to Request for Additional Information'** message - Reply to the received Request for Additional Information.

5.1.4 From the Court in Issuing State to the Issuing Authority and the Service Provider

- **'Court Decision'** message - The decision of the Court in issuing State after assessing the EPOC and the objections from the SP for not providing data.

5.2 Technical messages

During the exchange of information, the RI and the respective instance of the e-CODEX system should generate technical messages at different points of the message transfer.

These technical messages will inform about the progress of the technical transaction. The evidence generated by e-CODEX Connector in a signed XML format consist of:

- SUBMISSION_ACCEPTANCE/SUBMISSION_REJECTION: This evidence is generated by the sending connector and informs the original sender of the message (via national backend application) if the message was processed successfully by the sending connector and submitted to the sending Domibus gateway. This evidence is also attached to the message as business attachment.
- RELAY_REMMD_FAILURE: If the message was submitted to the gateway, but the gateway cannot submit it to the recipients' gateway, this evidence is generated and sent to the original sender by the sending connector. To be able to do so, the e-CODEX Connector relies on the information from the Domibus gateway that the submission has failed.
- RELAY_REMMD_ACCEPTANCE/REJECTION: Once the message arrives at the recipients' e-CODEX Connector, this connector generates the evidences, adds it to the message, but also sends it back to the original sender. Once received, an original sender can conclude, that the message was received by the recipients' gateway and connector, but not, if the processing of the message on the recipients' side was successful.
- DELIVERY / NON_DELIVERY: In case the processing of the message on the receiver side fails, a NON_DELIVERY is generated by the connector and sent back to the original sender. Once the message could be processed successfully and is delivered to the national backend application, the Domibus Connector depends on the trigger of the national backend application if the delivery to the final recipient was successful or not.

If triggered, the e-CODEX Connector generates the DELIVERY (if successful) or NON_DELIVERY (if not successful) and send it back to the original sender.

- RETRIEVAL / NON_RETRIEVAL: This evidence type is optional and hardly used by participants. This is due to the fact that it is not easy for national backend systems to acknowledge the retrieval of a message. But, if triggered by the backend application, the e-CODEX Connector generates such an evidence and sends it back to the original sender.

5.3 Errors and Warnings

Various components of the RI setup generate error and warning messages. In this section, the specific transmission related errors are highlighted. A full list of errors/warnings generated by the other components can be found in the Annex Section (Chapter 12).

The errors are conditions under which a message cannot be processed by the e-CODEX system or the recipient as it does not fulfil some technical or business constraints. The list consists of:

- SUBMISSION_REJECTION
- RELAY_REMMD_FAILURE
- RELAY_REMMD_REJECTION
- NON_RETRIEVAL
- NON_DELIVERY

The last element of this list indicates that the message could not be successfully delivered to the national backend application, thus the sender must ensure that the message is compliant with the rules in order to have a smooth operation of the system that avoids generation of error indications by the recipient.

When the message reaches the recipient, it is validated, and any error thrown during that validation results in the NON_DELIVERY message. If this happens, it means one of the following could have occurred:

5.3.1 Syntactic Validation

- Message not well formed: The message is not well-formed and cannot be decoded.
- Message not compliant: The message cannot be validated against the XML schema.

5.3.2 Semantic Validation

Semantic validation takes place on any field of the message structure.

Possible examples are:

- Different country code: when the country code of the receiving authority is different than the country code of the system receiving the message.
- Received message is not of expected type: if the message type does not match one of the expected types, for example a withdrawal message is expected to be sent by the issuing authority following Annex I submission, but 'Grounds for Refusal' form is not.
- Validation that specific forms are submitted only by designated entity types. For example: Annex III can only be submitted by a Service Provider, Annex I and Annex II can only be submitted by an Issuing Authority.
- Missing any of the following: message type; xml form; main PDF; issuing authority; service provider, enforcing authority, missing formId, misssing senderProtocolVersion, missing issuerProtocolVersion, missing or invalid globalCaseId, invalid AuthorityId, invalid parentFormId.

5.4 User notifications

When certain events occur in the system, user notifications will be generated by the system. These will be visible inside the RI under the notification bell.

Additionally, if an e-mail address is set up for the particular user, an e-mail will also be sent. The e-mail addresses are defined in KeyCloak.

Currently, the following events will lead to the generation of such notifications:

Event
1. Message/notification exchanges
Receive an EPOC
Receive an EPOC-PR
Sending a message for a case (EPOC/EPOC-PR) which had already been deleted by the message recipient
2. Message sending issues
SENDING_INFRA_REJECTION
RECEIVING_INFRA_REJECTION
TRANSMISSION_INFRA_FAILURE
RECEIVING_BACKEND_NON_DELIVERY

3. Case assignment
New case assigned to a user
Case shared with a user
4. Form Translation via eTranslate service processed and attached to case

Table 14: Events generating User Notifications

6 Workflows

In the context of the Reference Implementation Software, it is necessary to define two types of workflows:

6.1 Internal workflow

The internal workflow illustrates the processes within a Member State for creating, reviewing, and sending messages to Service Provider and other competent authorities within another Member State. Integrating this process will streamline procedures between services within National Authorities and law enforcements. The implementation of the internal workflow will enhance quality control before sending out messages, thereby minimizing the risk of errors or message rejections.

The proposed workflow consists of the following user roles:

- Author: responsible for creating and completing the e-Form;
- Reviewer: responsible for reviewing the form and either accepting or rejecting it;
- Signer 1 (member of the issuing authority): responsible for singing the e-Form, and Section M in case the notification to the Enforcing Authority is required;
- Signer 2 (member of the validating authority): responsible for singing the e-Form, and Section M in case the notification to the Enforcing Authority is required;
- Sender: responsible for sending the form to the competent authority in the issuing Member State.

Additionally, the Supervisor user role has the authority to perform all activities associated with the roles mentioned above. More details about user roles in chapter 3.4

6.2 External workflow

The external workflow refers to the exchanges between different Member States and Service Providers. For more detailed information on the workflows, please refer to the e-Evidence Business Collaboration Document [RD 01].

7 Case lifecycle/statuses

The Reference Implementation software follows a structured approach to case management by providing clear definitions and transitions between various case statuses throughout its lifecycle. The objective of this chapter is to provide a comprehensive guide to the underlying principles, workflow stages, and status transitions that define the processing of a case from initiation to resolution.

7.1 Table of Lifecycle Stages: EPOC Draft case

Workflow Action	Timeline Status Issuing Authority	Description	Status displayed on draft case and case list
CREATE	**Case created**	User (Author or Supervisor) from an Issuing Authority initiated an EPOC (Form 1)	**Draft**
COMPLETE	**Completed A L**	Author (or Supervisor) has completed the form and requested the Reviewer within its Competent Authority to review the EPOC.	**Completed A-L**
ACCEPT REVIEW	**Accepted**	The Reviewer (or Supervisor) has positively reviewed Form 1 and the case is passed to the next step of the Workflow > Signature.	**Positively Reviewed**
REJECT	**Rejected**	The Reviewer, Signer or Supervisor has rejected the request. Once the case is rejected, it is no longer possible to perform actions on the case.	**Rejected**
RETURN FOR AMENDMENT	**Returned**	The Reviewer, Signer or Supervisor has returned the request for amendment.	**Draft or Completed**
READY TO SIGN	**Ready to sign**	The Signer has reviewed sections A to L and the EPOC (Form 1) is pushed to the actual Signature step.	**Ready to Sign**

SIGN FIRST or SIGN SECOND	**Signed 1/ Signed 2**	EPOC is signed (sections A-L) by the 'Signer' (Signer 1 or 2) within the Competent Authority). The e-Form is ready to be sent out by "Sender" or , in case a notification is required, Section M is to be filled-in and signed.	**Signed (Sections A-L)**
UPLOAD EXTERNALLY	**Signed externally**	A signed (externally) EPOC is uploaded (that EPOC should have a qualified electronic signature by the Competent Authority of the Issuing/Validating Authority).	**Signed (externally)**
COMPLETE	**Completed M**	Section M is filled in by the "Signer" (either Signer 1 or Signer 2) and is ready to be signed.	**Completed M**
SIGN SECOND	**Signed 2**	Form 1 with Section M filled in is signed by the 'Signer' (Signer 1 or 2) within the Competent Authority. The e-Form is ready to be sent out to the Service Provider/Enforcing Authority.	**Signed (Section M)**

Table 15: Lifecycle Stages: EPOC Draft case

7.2 Table of Lifecycle Stages: EPOC Issued case

Workflow Action/Messages received/Message sent in reply	Timeline Status Issuing Authority	Description	Status displayed on issued case and case list
SEND	**Form 1 Sent**	An EPOC has been sent by the Issuing Authority and the Issuing Authority is now awaiting the Confirmation of Receipt.	**Issued**
EPOC CONFIRMATION	**Confirmation of Receipt Received**	Confirmation of Receipt of Form 1 is received from the Service Provider/ Executing Authority.	**Issued**

OF RECEIPT IS RECEIVED			
REQUEST FOR ADDITIONAL INFORMATION IS RECEIVED	**Request for additional information received**	Enforcing Authority / Service Provider has requested additional information.	**Issued** - The corresponding icon on the overview tab is marked in bold.
REPLY TO REQUEST FOR ADDITIONAL INFO	**The reply is displayed below the initial Request**	The Issuing Authority provides additional information to the Enforcing Authority/ Service Provider.	**Issued**
GROUNDS FOR REFUSAL IS RECEIVED	**Grounds for Refusal**	The Issuing Authority receives "Grounds for Refusal" message from the Enforcing Authority.	**Issued**
FORM 3 IS RECEIVED	**Form 3**	The Issuing Authority receives Form 3 from the Service Provider. There may be a need to provide additional information.	**Issued - The corresponding icon on the overview tab is marked in bold**
OUTCOME IS RECEIVED	**Outcome**	Issuing Authority receives Outcome message from the Service Provider.	**Issued - The corresponding icon on the overview tab is marked in bold**
ADAPT FORM IS SENT	**Adapt message**	Upon receipt of Form 3 or as a result of discussions with the Enforcing Authority, the initial EPOC will be adapted by the Issuing Authority.	**Issued**
MAINTAIN FORM IS SENT	**Maintain message**	Upon receipt of Form 3 or as a result of discussions with the Enforcing Authority , the initial EPOC will be Maintained by the Issuing Authority.	**Issued**
WITHDRAW	**Withdrawal**	The Issuing Authority has decided to withdraw an order. *not to be mistaken with Case closed as withdrawal is a 'legal action'. This is considered as the end of case processing.	**Withdrawn**

CONFIRMATION OF END OF TRANSACTION MESSAGE IS RECEIVED	**Confirmation of End of Transaction Received**	The Service Provider (and Enforcing Authority if applicable) notifies the Issuing Authority that they have acted upon the request to Withdraw the case.	**Withdrawn – The corresponding icon on the Overview Tab is displayed in bold.**
INFORM ABOUT GOING TO COURT MESSAGE IS SENT	**Inform About Going to Court**	The Issuing Authority informs the Service Provider about going to Court to decide on the EPOC.	**Issued**
PROCEDURE OF ENFORCEMENT IS SENT	**Procedure of Enforcement**	The Issuing Authority informs initiates the Enforcement Procedure.	**Issued**
NOT RECOGNISED DECISION IS RECEIVED	**Not Recognised Decision**	The Issuing Authority is notified that the Service Provider does not need to comply with the initial order upon the enforcement procedure.	**Issued**
RECOGNITION DECISION RECEIVED	**Recognition Decision**	The Issuing Authority is notified that the Service Provider needs to comply with the initial order upon the enforcement procedure.	**Issued**
AGREE WITH OBJECTION DECISION IS RECEIVED	**Agree with Objection**	The Issuing Authority is informed that the Enforcing Authority agrees with the objection Service Provider had raised to the recognition decision. The process is closed on all sides (IA, EA and SP) and all resources allocated to it may be released.	**Issued**
DISAGREE WITH OBJECTION DECISION IS RECEIVED	**Disagree with Objection**	The Issuing Authority is informed that the Enforcing Authority informs that they do not agree with the objection they had raised to the recognition decision. The Service Provider must produce the requested data.	**Issued**
CLOSE	**Case Closed**	Case is closed manually, not necessarily at the same point	**Closed**

		in time at all involved parties.	

Table 16: Lifecycle Stages: EPOC Issued case

7.3 Table of Lifecycle Stages: EPOC Received case

Workflow Action/Messages received/Messages sent	Timeline Status Enforcing Authority	Description	Status displayed on received case and case list
NEW CASE RECEIVED	**Received**	An EPOC (Form 1) has been received by an Enforcing Authority. To confirm the receipt, a "Confirmation of receipt" should be filled in and sent to the Issuing Authority.	**Received**
EPOC CONFIRMATION OF RECEIPT IS SENT	**Confirmation of Receipt Sent**	Confirmation of Receipt of Form 1 is sent to the Issuing Authority.	**Received**
SEND GROUNDS FOR REFUSAL	**Grounds for Refusal**	The Enforcing Authority sends Grounds for Refusal to both Issuing Authority and Service Provider.	**Received**
REQUEST FOR ADDITIONAL INFORMATION	**Request for additional Information Sent**	Additional information is needed to further EPOC processing.	**Received - The corresponding icon (Decision) on the overview tab is marked in bold**
REPLY TO REQUEST FOR ADDITIONAL INFORMATION	**The reply is displayed below the initial Request**	The Enforcing Authority has replied with additional information.	**Received**
FORM 3 IS RECEIVED	**Form 3**	The Enforcing Authority receives Form 3 from the Service Provider.	**Received - The corresponding icon on the overview tab is marked in bold**
WITHDRAWAL MESSAGE RECEIVED	**Case Withdrawn**	The Issuing Authority notifies the Enforcing Authority that the case is withdrawn.	**Received**

CONFIRMATION OF END OF TRANSACTION	**Confirmation of End of Transaction Sent**	The Enforcing Authority notifies the Issuing Authority that they have acted upon the request to Withdraw the case. This is the end of case processing	**Withdrawn – The corresponding icon on the Overview Tab is displayed in bold.**
INFORM ABOUT GOING TO COURT MESSAGE IS RECEIVED	**Inform About Going to Court**	The Issuing Authority informs the Enforcing Authority about going to Court to decide on the EPOC.	**Received**
PROCEDURE OF ENFORCEMENT IS SENT	**Procedure of Enforcement**	The Issuing Authority initiates the Enforcement Procedure and sends it to the Enforcing Authority.	**Received**
NOT RECOGNISED DECISION IS SENT	**Not Recognised Decision**	The Enforcing Authority notifies that the Service Provider does not need to comply with the initial order upon the enforcement procedure.	**Received**
RECOGNITION DECISION SENT	**Recognition Decision**	The Enforcing Authority notifies that the Service Provider needs to comply with the initial order upon the enforcement procedure.	**Received**
OBJECTION TO RECOGNITION DECISION IS RECEIVED	**Objections Received**	The Service Provider notifies that they object to the Recognition Decision of the Enforcing Authority.	**Received**
AGREE WITH OBJECTION DECISION IS SENT	**Agree with Objection**	The Enforcing Authority agrees with the objection Service Provider had raised to the recognition decision. The process is closed on all sides (IA, EA and SP) and all resources allocated to it may be released.	**Received**
DISAGREE WITH OBJECTION DECISION IS SENT	**Disagree with Objection**	The Enforcing Authority informs that they do not agree with the objection they had raised to the recognition decision. The	**Received**

		Service Provider must produce the requested data.	
CLOSE CASE	**Case Closed**	Case is closed as a result of the Enforcing Authority having sent the 'Confirmation about the end of the transaction 'upon receiving 'Withdrawal' from the Issuing Authority. This is a manual action.	**Closed**

Table 17: Lifecycle Stages: EPOC Received case

7.4 Table of Lifecycle Stages: EPOC-PR Draft case

Workflow Action	Timeline Status Issuing Authority	Description	Status displayed on draft case and case list
CREATE	**Case created**	User (Author or Supervisor) from an Issuing Authority initiated an EPOC-PR (Form 2)	**Draft**
COMPLETE	**Completed A L**	Author (or Supervisor) has completed the form and requested the Reviewer within its Competent Authority to review the EPOC-PR.	**Completed A-L**
ACCEPT REVIEW	**Accepted**	The Reviewer (or Supervisor) has positively reviewed Form 2 and the case is passed to the next step of the Workflow > Signature.	**Positively Reviewed**
REJECT	**Rejected**	The Reviewer, Signer or Supervisor has rejected the request. Once the case is rejected, it is no longer possible to perform actions on the case.	**Rejected**
RETURN FOR AMENDMENT	**Returned**	The Reviewer, Signer or Supervisor has returned the request for amendment.	**Draft or Completed**

READY TO SIGN	**Ready to sign**	The Signer has reviewed sections A to G and the EPOC-PR (Form 2) is pushed to the actual Signature step.	**Ready to Sign**
SIGN FIRST or SIGN SECOND	**Signed 1/ Signed 2**	EPOC-PR is signed (sections A-G) by the 'Signer' (Signer 1 or 2) within the Competent Authority). The e-Form is ready to be sent out by "Sender".	**Signed (Sections A-G)**
UPLOAD EXTERNALLY	**Signed externally**	A signed (externally) EPOC-PR is uploaded (that EPOC-PR should have a qualified electronic signature by the Competent Authority of the Issuing/Validating Authority).	**Signed (externally)**

Table 18: Lifecycle Stages: EPOC-PR Draft case

7.5 Table of Lifecycle Stages: EPOC-PR Issued case

Workflow Action/Messages received/Message sent in reply	Timeline Status Issuing Authority	Description	Status displayed on issued case and case list
SEND	**Form 2 Sent**	An EPOC-PR has been sent by the Issuing Authority and the Issuing Authority is now awaiting the Confirmation of Receipt.	**Issued**
EPOC-PR CONFIRMATION OF RECEIPT IS RECEIVED	**Confirmation of Receipt Received**	Confirmation of Receipt of Form 2 is received from the Service Provider.	**Issued**
REQUEST FOR ADDITIONAL INFORMATION IS RECEIVED	**Request for additional information received**	Enforcing Authority / Service Provider has requested additional information.	**Issued** - The corresponding icon on the overview tab is marked in bold.
REPLY TO REQUEST FOR ADDITIONAL INFO	**The reply is displayed below the initial Request**	The Issuing Authority provides additional information to the Enforcing Authority/ Service Provider.	**Issued**

FORM 3 IS RECEIVED	**Form 3**	The Issuing Authority receives Form 3 from the Service Provider. There may be a need to provide additional information.	**Issued - The corresponding icon on the overview tab is marked in bold**
DATA HAS BEEN PRESERVED IS RECEIVED	**Data Has Been Preserved**	Issuing Authority receives 'Data Has Been Preserved' message from the Service Provider.	**Issued**
NO LONGER NEED TO PRESERVE DATA IS SENT	**No Longer Need To Preserve Data**	The Issuing Authority informs the Service Provider that they no longer need to preserve the requested data.	**Issued**
FORM 5 IS SENT	**Form 5**	The Issuing Authority informs the Service Provider that a subsequent request for Production following an EPOC-PR has been issued	**Issued**
FORM 6 IS SENT	**Form 6**	The Issuing Authority informs the Service Provider about the extension of the initial EPOC-PR.	**Issued**
ADAPT FORM IS SENT	**Adapted message**	Upon receipt of Form 3 or as a result of discussions with the Enforcing Authority, the initial EPOC-PR will be adapted by the Issuing Authority.	**Issued**
MAINTAIN FORM IS SENT	**Maintain message**	Upon receipt of Form 3 or as a result of discussions with the Enforcing Authority , the initial EPOC-PR will be Maintained by the Issuing Authority.	**Issued**
WITHDRAW	**Withdrawal**	The Issuing Authority has decided to withdraw An order. *not to be mistaken with Case closed as withdrawal is a 'legal action'. This is considered as the end of case processing.	**Withdrawn**

CONFIRMATION OF END OF TRANSACTION MESSAGE IS RECEIVED	**Confirmation of End of Transaction Received**	The Service Provider (and Enforcing Authority if applicable) notifies the Issuing Authority that they have acted upon the request to Withdraw the case.	**Withdrawn – The corresponding icon on the Overview Tab is displayed in bold.**
PROCEDURE OF ENFORCEMENT IS SENT	**Procedure of Enforcement**	The Issuing Authority informs initiates the Enforcement Procedure.	**Issued**
NOT RECOGNISED DECISION IS RECEIVED	**Not Recognised Decision**	The Issuing Authority is notified that the Service Provider does not need to comply with the initial order upon the enforcement procedure.	**Issued**
RECOGNITION DECISION RECEIVED	**Recognition Decision**	The Issuing Authority is notified that the Service Provider needs to comply with the initial order upon the enforcement procedure.	**Issued**
AGREE WITH OBJECTION DECISION IS RECEIVED	**Agree with Objection**	The Issuing Authority is informed that the Enforcing Authority agrees with the objection Service Provider had raised to the recognition decision. The process is closed on all sides (IA, EA and SP) and all resources allocated to it may be released.	**Issued**
DISAGREE WITH OBJECTION DECISION IS RECEIVED	**Disagree with Objection**	The Issuing Authority is informed that the Enforcing Authority informs that they do not agree with the objection they had raised to the recognition decision. The Service Provider must preserve the requested data.	**Issued**
CLOSE	**Case Closed**	Case is closed manually, not necessarily at the same point in time at all involved parties.	**Closed**

Table 19: Lifecycle Stages: EPOC-PR Issued case

7.6 Table of Lifecycle Stages: EPOC-PR Received case

Workflow Action/Messages received/Message sent in reply	Timeline Status Issuing Authority	Description	Status displayed on issued case and case list
REQUEST FOR ADDITIONAL INFORMATION IS RECEIVED	**Request for additional information received**	Issuing Authority / Service Provider has requested additional information.	**Received**
REPLY TO REQUEST FOR ADDITIONAL INFO	**The reply is displayed below the initial Request**	The Issuing Authority provides additional information to the Enforcing Authority/ Service Provider.	**Received**
FORM 3 IS RECEIVED	**Form 3**	The Issuing Authority receives Form 3 from the Service Provider. There may be a need to provide additional information.	**Received - The corresponding icon on the overview tab is marked in bold**
PROCEDURE OF ENFORCEMENT IS SENT	**Procedure of Enforcement**	The Issuing Authority initiates the Enforcement Procedure and sends it to the Enforcing Authority.	**Received**
NOT RECOGNISED DECISION IS SENT	**Not Recognised Decision**	The Enforcing Authority notifies that the Service Provider does not need to comply with the initial order upon the enforcement procedure.	**Received**
RECOGNITION DECISION SENT	**Recognition Decision**	The Enforcing Authority notifies that the Service Provider needs to comply with the initial order upon the enforcement procedure.	**Received**
OBJECTION TO RECOGNITION DECISION IS RECEIVED	**Objections Received**	The Service Provider notifies that they object to the Recognition Decision of the Enforcing Authority.	**Received**
AGREE WITH OBJECTION DECISION IS SENT	**Agree with Objection**	The Enforcing Authority agrees with the objection Service Provider had raised to the recognition decision. The process is closed on all sides (IA, EA and SP) and	**Received**

		all resources allocated to it may be released.	
DISAGREE WITH OBJECTION DECISION IS SENT	**Disagree with Objection**	The Enforcing Authority informs that they do not agree with the objection they had raised to the recognition decision. The Service Provider must preserve the requested data.	**Received**

Table 20: Lifecycle Stages: EPOC-PR Received case

8 Logging and Statistics

For audit purposes the system will maintain a log of all actions performed by the users. Moreover, some of the collected information will be used to produce the data that will be used for the generation of statistics and reports.

The statistics that will be provided will cover mainly traffic exchanges. These reports will provide information on:

- Per Member State and per year: the number of EPOCs and EPOC-PRs issued, by the type of data requested, the addressees and the situation (emergency case or not);
- Per Member State and per year: the number of EPOCs issued under emergency case derogations;
- Per Member State and per year: the number of fulfilled and non-fulfilled EPOCs and EPOC-PRs, by the type of data requested, the addressees and the situation (emergency case or not);
- Per Member State and per year: the number of notifications to enforcing authorities pursuant to Article 8, and the number of EPOCs that were refused, by the type of data requested, the addressees, the situation (emergency case or not) and the ground for refusal raised;
- Per Member State and per year: for fulfilled EPOCs, the average period between the moment the EPOC was issued and the moment the data requested were obtained, by the type of data requested, the addressees and the situation (emergency case or not);
- Per Member State and per year: for fulfilled EPOC-PRs, the average period between the moment the EPOC-PR was issued and the moment the subsequent request for production was issued, by the type of data requested and the addressees;
- Per Member State and per year: the number of European Production Orders or European Preservation Orders transmitted to and received by an enforcing State for enforcement, by the type of data requested, the addressees and the situation (emergency case or not) and the number of such orders fulfilled;

- Per Member State and per year: the number of legal remedies used against European Production Orders in the issuing State and in the enforcing State, by the type of data requested;
- Per Member State and per year: the number of cases where ex post validation in accordance with Article 4(5) was not granted;
- Per Member State and per year: an overview of the costs claimed by service providers in relation to the execution of EPOCs or EPOC-PRs and the costs reimbursed by the issuing authorities.

More specific reports can also be generated. Some possible examples are listed below:

- Per Member State and per year: a number of EPOCs received by Enforcing State broken down by Issuing State;
- Per Member State and per year: number of withdrawals of EPOCs and EPOC-PRs received by the Enforcing State, broken down by Issuing State;
- Per Member State and per year: number of Annexes III of EPOCs and EPOC-PRs received by the Issuing State, broken down by Service Providers;
- Per Member State and per year: number of Annexes III of EPOCs and EPOC-PRs received by the Enforcing State, broken down by Service Providers;
- Per Member State and per year: number of Annexes V within EPOC-PR cases sent to Service Provider;
- Per Member State and per year: number of Annexes VI within EPOC-PR cases sent to Service Provider.

Statistics reports will be automatically generated by the RI on 1 January for the preceding year in Excel (XLS) and PDF formats. Operators will have the possibility to review these reports prior to confirming their submission to the Commission, which will be then done automatically by RIS to a predefined e-mail address.

At all times, the data generated or collected by the RI for logging and audit trails purposes, belong solely and is under the responsibility of the Member States where the RI is installed and running.

9 System Architecture

This chapter describes the high-level architecture of the decentralised IT system that is compliant with the *Regulation*.

It takes into account a scenario where a Competent Authority in one Member State (on the left of the diagrams) issues an EPOC/EPOC PR to a Service Provider in another Member State and receives the relevant reply. It also provides for the possibility to notify a Competent Authority in the Member State of the Service Provider as foreseen by the *Regulation*.

The *Regulation* foresees that the Competent Authorities communicate via the decentralised IT system through national IT systems under their responsibility. Instead of a national IT system, Member State may instead choose to use the RI developed by the Commission.

With regard to Service Providers, the Regulation foresees that access to the decentralised IT system can take place via the national IT system (or RI) of the enforcing State, either through a web-based interface or via an API.

An important aspect in the exchange of messages between Competent Authorities and Service Providers is to determine where the message should be addressed. To achieve this, the system will make use of the Court Database tool. The court database is a central data store entity containing all imported data of the Member States' competent authorities and Service Providers legal representatives or designated establishments.

9.1 Direct Access to the national IT system / Reference Implementation software (RI) for Service Providers through a web-based interface

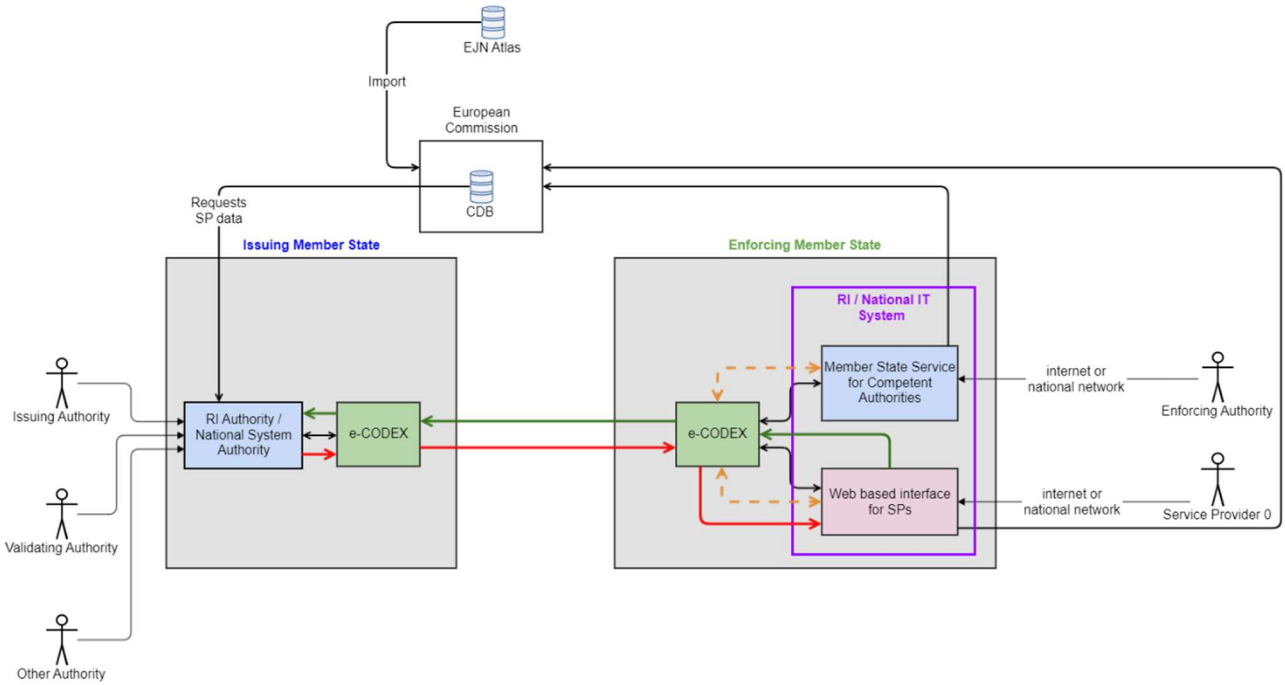

Figure 9-1: Direct access to the system for Service Providers through through a web-based interface

Description

- The SP accesses directly the national IT system or the RI through a web-based interface (see "pink box" in Figure 9-1 above);
- The national IT system or RI is hosted and maintained by the Member State, where the legal representative or designated establishment of the SP is located;
- Exchange protocols and business logic are implemented in the national IT system or RI;
- Forms and data exchanged under the Regulation remain in/are removed from the national IT system / RI (including the web interface for Service Providers) following configuration rules to be established by each MS;
- On the e-CODEX stack, data stays only until the message is successfully transmitted to the receiving e-CODEX access point or expires in a waiting queue (e.g. due to non-delivery, this is configurable as well);
- Communication is point-to-point encrypted;

- The entire stack (national IT system/RI including the web interface for Service Providers) is meant to be installed in the same secure environment.
- "Large files" (when "the volume of data to be transferred is hampered by technical capability constraints" – actual threshold to be agreed) should be transferred through alternative means that can ensure the swift, secure and reliable exchange of information. At the same time, a manifest possibly containing a link, access information (e.g. access credentials), a hash digest of the data package is transferred through the national IT system or RI over the e-CODEX stack;
- In this scenario, the access of the SPs to the decentralised IT system is via the web-based interface for Service Providers;
- The hosting MS manages the user access of the SPs on their territory to the web-based interface for Service Providers.

9.2 Service Provider's System-to-System Access to the decentralised IT system through the national IT system / Reference Implementation Software via API's

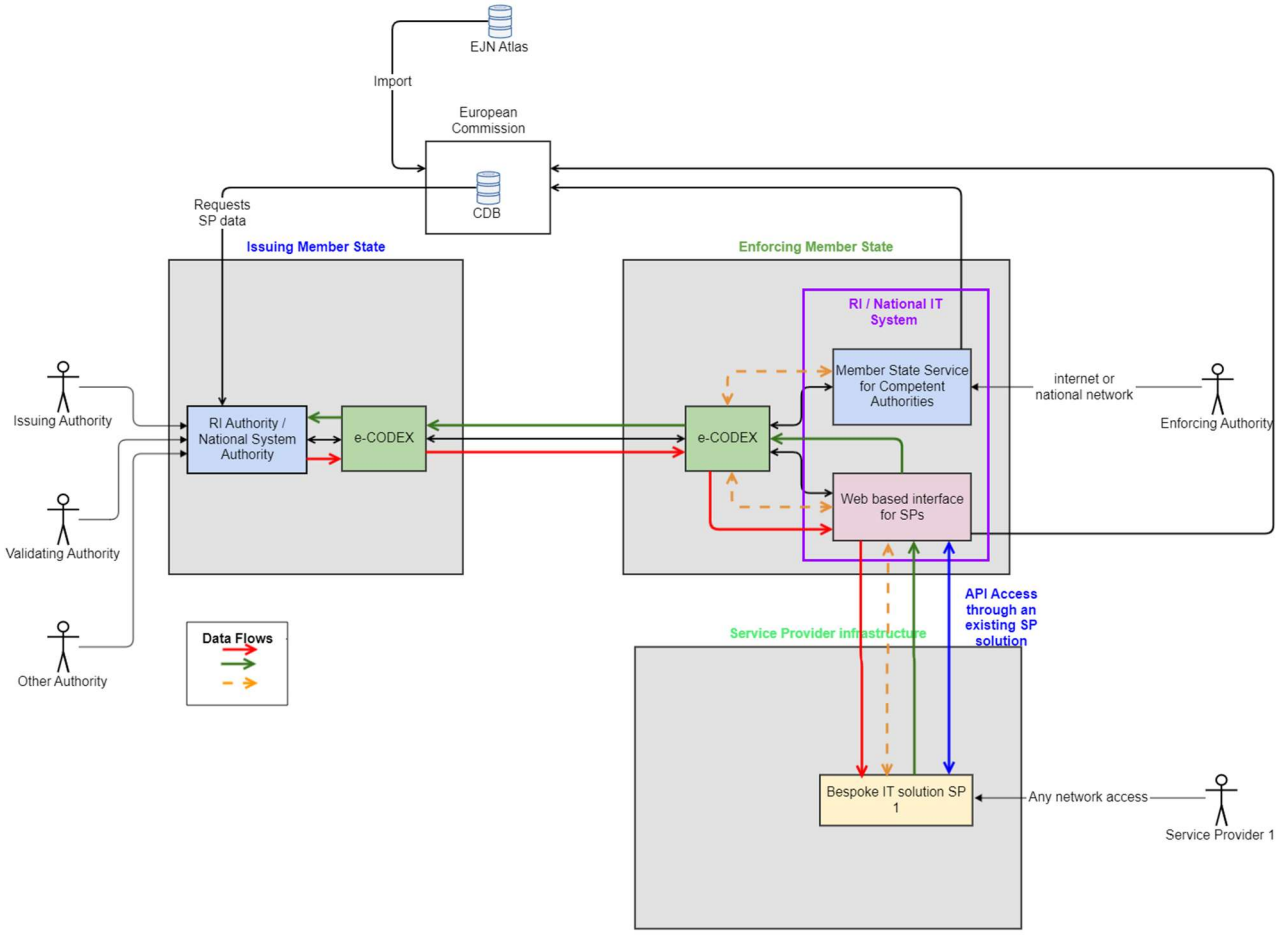

Figure 9-2: Service Provider's access to the system through API

Description

- In this scenario the SP has a bespoke IT solution that is connected to the decentralised system;
- The SP connects its bespoke IT solution to the national IT system or the RI through dedicated API's;

- The instance of the national IT system or RI is fully hosted and operated by the Member State where the legal representative or designated establishment of the SP are located;
- Exchange protocols and business logic are implemented in national IT system/the RI. They are not implemented on the SP bespoke IT solution;
- Forms and data exchanged under the Regulation and the data requested will be (automatically) removed from the national IT system/RI following configuration rules to be established by each MS;
- Forms and data exchanged by the SP bespoke IT solution will be removed following configuration rules to be established by each SP;
- On the e-CODEX stack, data only stays until the message is successfully transmitted to the receiving e-CODEX access point or expires in a waiting queue (e.g. due to non delivery, this is configurable);
- Support concerning issues pertaining to the API will be either provided by the MS, in case of a national IT system or, where relevant, by the Commission, if the RI is used as IT solution;
- Communication is point-to-point encrypted;
- The national e-CODEX access point and the national IT system/RI are installed on the same secure infrastructure stack;
- The bespoke IT solution is installed on the infrastructure of the SP;
- "Large files" (when "the volume of data to be transferred is hampered by technical capability constraints" – actual threshold to be agreed) should be transferred through alternative means that can ensure the swift, secure and reliable exchange of information. At the same time, a manifest possibly containing a link, access information (e.g. access credentials), a hash digest of the data package is transferred through the national IT system or RI over the e-CODEX stack;
- In this scenario, SPs can access the decentralised IT system in two ways:
  - via their connected bespoke IT solution (connected to the national IT System/RI); or
  - via the web-based interface for Service Providers referred to in Scenario 1, which needs to be available as well.
- The hosting MS manages the user access of the SPs on their territory:
  - to the web-based interface for Service Providers;

- of their bespoke IT solutions to their national IT system/RI APIs.

10 Security Aspects

The security aspects of the decentralised IT system are critical to ensure effective judicial cooperation and the secure exchange of information between service providers and competent authorities of Member States. These aspects are designed to meet the stringent security requirements including confidentiality, integrity, availability of e-evidence assets, and legitimate use of the system.

10.1 Confidentiality

Confidentiality is paramount to protect sensitive information from unauthorized access or disclosure. The decentralised IT system shall ensure confidentiality through robust measures:

- **Access Control**: Access to Reference Implementation portal shall be strictly controlled using strong authentication methods, including multi-factor authentication (MFA). Only authorized users involved in specific exchanges should have access to the transmitted, received, or stored content. Role-Based Access Control ensures that access rights are tailored to user roles, preventing unauthorized access;
- **Encryption**: End to end encryption should be employed to encrypt data both at rest and in transit. Advanced Encryption Standard (AES-256) could be utilized to safeguard data integrity and confidentiality across the system's infrastructure and transmission channels.

10.2 Integrity

Maintaining data integrity ensures that information remains accurate, consistent, and trustworthy throughout its lifecycle. The decentralised IT system shall uphold data integrity with the following measures:

- **Data Validation and Protection**: Stringent data validation processes will prevent unauthorized changes or tampering during transmission or storage. Use of strong cryptographic hashing algorithms, such as the Secure Hashing Algorithm-256 (SHA-256), will allow to verify data integrity at various infrastructure layers, including user access data and business data;
- **Auditing and Monitoring**: Comprehensive audit trails will track all user activities and system events, ensuring transparency and accountability. Audit logs provide a secure record of system use, supporting non-repudiation and ensuring that any unauthorized modifications are promptly detected.

10.3 Availability

Ensuring continuous availability of the decentralised IT system and its services is crucial for uninterrupted cooperation and data exchange. Measures to maintain availability include:

- **Redundancy and Backup**: The system should incorporate redundancy and backup mechanisms at both infrastructure and application levels. Equipment redundancy and backup solutions mitigate the risk of service interruptions and ensure data availability during unexpected events or failures;
- **Business Continuity Planning**: A robust business continuity plan needs to be put in place to manage and mitigate risks that could impact system availability. This plan outlines procedures for rapid response, recovery, and restoration of services in the event of disruptions.

10.4 Legitimate Use of the System

Ensuring the legitimate use of the decentralised IT system involves implementing security measures to prevent misuse and maintain accountability:

- **Authentication and Access Control**: Strong authentication mechanisms and dynamic authorization controls prevent unauthorized access to protected resources. Access rights are dynamically adjusted based on user roles and permissions, minimizing the risk of unauthorized use;
- **Secure Audit Logs**: Cryptographically protected audit logs provide verifiable records of user and application activities. These logs support non-repudiation by ensuring that all system interactions are traceable and cannot be altered without detection.

To fully address these security objectives, the following detailed aspects shall be addressed:

- Establishing clear roles and responsibilities for information security management;
- Identifying and protecting critical assets through effective asset management practices;
- Implementing policies and procedures to ensure personnel security and awareness;
- Safeguarding physical facilities and resources that house the RI system;
- Securing network communications and operational processes to prevent unauthorized access;
- Implementing role-based access control and strict access control policies to limit system access based on user roles;
- Integrating security into the software development lifecycle to mitigate vulnerabilities;

- Establishing procedures to detect, respond to, and recover from security incidents;
- Planning and testing procedures to ensure continuity of operations during disruptions;
- Conducting regular risk assessments and implementing measures to mitigate identified risks effectively.

11 Assumptions, Constraints and Risks Analysis

This chapter outlines the assumptions, constraints, and risks associated with the design and implementation of the decentralised IT system as per *EU Regulation 2023/1543*. These factors are critical in guiding the project and ensuring its successful execution.

11.1 Assumptions

The assumptions form the foundation upon which the e-evidence system specifications are based. They provide the context and framework for the system's development and deployment.

- **Unified e-Forms Structure**: It is assumed that the structure of the e-Forms has been agreed upon and approved by all Member States involved. This common agreement is essential for ensuring interoperability and consistent communication;
- **Flexibility for Business Changes**: It is assumed that any future business changes to the e-Forms will necessitate corresponding modifications to the specifications document. This ensures that the system remains adaptable and responsive to evolving requirements.

11.2 Constraints

Constraints are limitations or restrictions that impact the design, development, and deployment of the decentralised IT system. These must be carefully managed to ensure project success.

- **Regulatory Compliance**: Adherence to EU Regulation 2023/1543: The system must comply with all the stipulations of the Regulation, which mandates stringent security and data protection measures;
- **Data Protection Laws**: Compliance with the General Data Protection Regulation (GDPR) and other relevant data protection laws is mandatory. This includes ensuring the confidentiality, integrity, and availability of personal data;
- **Interoperability**: The system must be interoperable with existing systems and platforms used by Member States, requiring standardization of protocols and data formats;
- **Performance Requirements**: The system must meet high-performance standards to handle large volumes of data and transactions without compromising on speed or reliability.

11.3 Risks

Risks are potential events or conditions that could negatively impact the project. Identifying and mitigating these risks is crucial for the successful implementation of the decentralised IT system.

- **Cybersecurity Threats**: The system may be vulnerable to cyber-attacks, including data breaches, hacking, and malware. Robust security measures must be implemented to mitigate these risks;
- **Scalability Concerns**: As the volume of data and number of users increase, the system must be able to scale without performance degradation;
- **Timeline Delays**: Unforeseen challenges in development, testing, or deployment could cause delays, impacting the overall project timeline and delivery;
- **Resource Availability**: Constraints on budget, personnel, and technical resources may impact the timeline and scope of the project.

12 ANNEXES

12.1 Errors and Warnings list

12.1.1 Error messages based on HTTP response status codes

These messages with translations are defined in frontend source code.

Error code	Message	Description
app.401_error.label	You are not authorized. Access is denied. Please try login again to your account.	Upon receiving HTTP 401 – indicates that the client must authenticate itself to get the requested response.
app.403_error.label	You are trying to do forbidden action	Upon receiving HTTP 403 - the client does not have access rights to the content.
app.404.label	Not found	Upon receiving HTTP 404 - the server cannot find the requested resource.
app.404_error.label	The information you are looking for was not found.	Upon receiving HTTP 404 - the server cannot find the requested resource.
app.500_error.label	Problem with connection to the server. Please try again in few minutes or contact with administrator.	Upon receiving HTTP 500 – internal server error.
app.503_error.label	The server is down for maintenance. Please try again in few minutes or contact with administrator.	Upon receiving HTTP 503 – service unavailable.
app.0_error.label	Problem with your internet connection. Please check the network and try again.	Upon receiving other status code

Table 21: Errors based on HTTP response status codes

12.1.2 Error messages from backend

This chapter will be updated at a later stage.

13 Related Documents

13.1 Applicable Documents

ID	Title	Reference
[REG 01]	Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings	*Regulation 2023/1543*
[REG 02]	Regulation (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)	*Regulation 2016/679*
[REG 03]	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, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance.)	*Regulation 2018/1725*
[DIR 01]	Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings.	*Directive 2023/1544*
[DIR 02]	Directive (EU) 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	*Directive 2016/680*

Table 22: Applicable documents

13.2 Reference Documents

ID	Title	Reference	Version	Date
[RD 01]	e-Evidence Business Collaboration Document			
[RD 02]	Glossary Document			

Table 23: Reference Documents

13.3 Abbreviations & Acronyms

Related and applicable Abbreviations and Acronyms are defined in a separate, dedicated document: "Glossary Document" [**RD 02**].

13.4 List of tables

Table 1: Business Requirements 9
Table 2: Functional Requirements 22
Table 3: Non-functional requirements – Usability 23
Table 4: Non-functional requirements - Security 24
Table 5: Non-functional requirements – Data Protection 25
Table 6: Non-functional requirements - Business continuity 25
Table 7: Non-functional requirements - Development qualities 26
Table 8: Non-functional requirements – Compliance 26
Table 9: Domains 29
Table 10: Actors 30
Table 11: Roles and Descriptions within the Issuing Authority for EPOC 36
Table 12: Roles and Descriptions within the Enforcing Authority for EPOC 39
Table 13: Roles and Descriptions within the Issuing Authority for EPOC-PR 43
Table 14: Events generating User Notifications 59
Table 15: Lifecycle Stages: EPOC Draft case 62
Table 16: Lifecycle Stages: EPOC Issued case 65
Table 17: Lifecycle Stages: EPOC Received case 67
Table 15: Lifecycle Stages: EPOC-PR Draft case 68
Table 16: Lifecycle Stages: EPOC-PR Issued case 70
Table 16: Lifecycle Stages: EPOC-PR Received case 72
Table 18: Errors based on HTTP response status codes 86

Table 19: Applicable documents 88
Table 20: Reference Documents 89

13.5 List of figures

Figure 3-1: EPOC and EPOC-PR Exchange Domains 29
Figure 3-2: EPOC exchange Main Business 45
Figure 3-4: EPOC-PR exchange Main Business Processes 46
Figure 9-1: Direct access to the system for Service Providers through through a web-based interface 76
Figure 9-2: Service Provider's access to the system through API 78