EVIDENCE2 / e-CODEX

Linking EVIDENCE into e-CODEX for EIO and MLA procedures in Europe

JUSTICE PROGRAMME (2014-2020)

JUST-JCOO-CRIM-AG-2016

Action Grants to Support Transnational Projects to Promote Judicial Cooperation in Criminal Matters

EVIDENCE2E-CODEX (GA 766468)

Linking EVIDENCE into e-CODEX for EIO and MLA procedures in Europe

&

EXEC (GA 785818)

Electronic Xchange of e-Evidences with e-CODEX

JOINT EVENT - WORKSHOP ON MERGING VIEWS

Meeting Technical and Legal community to cross- fertilize views

EVIDENCE2e-CODEX: EVIDENCE EXCHANGE IN A NUTSHELL

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

EVIDENCE2e-CODEX goal

The EVIDENCE2e-CODEX project, together with the other closely related projects - e-Evidence and EXEC, are working together to achieve a common goal:

exchange digital evidence in a digital manner,

among Competent Authorities in the EU Member States and beyond,

under the EIO/MLA instruments.

How can the goal be accomplished?

First, a secure platform/infrastructure for the evidence exchange is needed: this is provided by **e-CODEX**, being a content agnostic e-Delivery infrastructure that supports cross-border e-Justice services. The **EXEC** project is going to extend/strengthen some components of e-CODEX to manage the Evidence Exchange service (or use case). While e-CODEX operates at international level, on national level the respective national systems are in play along with the e-Evidence Digital Exchange System.

The **e-Evidence Digital Exchange System**, provided by the EC, is the system that manages the EIO/MLA procedures/instruments: e-Forms, business logic, statistics, log, etc. The **Reference Implementation** is the front-end portal of the e-Evidence Digital Exchange System and is also provided by the EC. This reflects the principle, followed by e-CODEX, that interoperability is achieved through common requirements, leaving to the participants the maximum level of autonomy in supporting those requirements.

Relying on the e-Evidence Digital Exchange System, it is possible:

- to prepare the EIO/MLA forms in a digital way and send them as a message;
- to attach a document to each message.

The stakeholders of the system are the Competent Authorities of each Member State, as depicted in Figure 1 'EIO/MLA management using the Reference Implementation'.

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

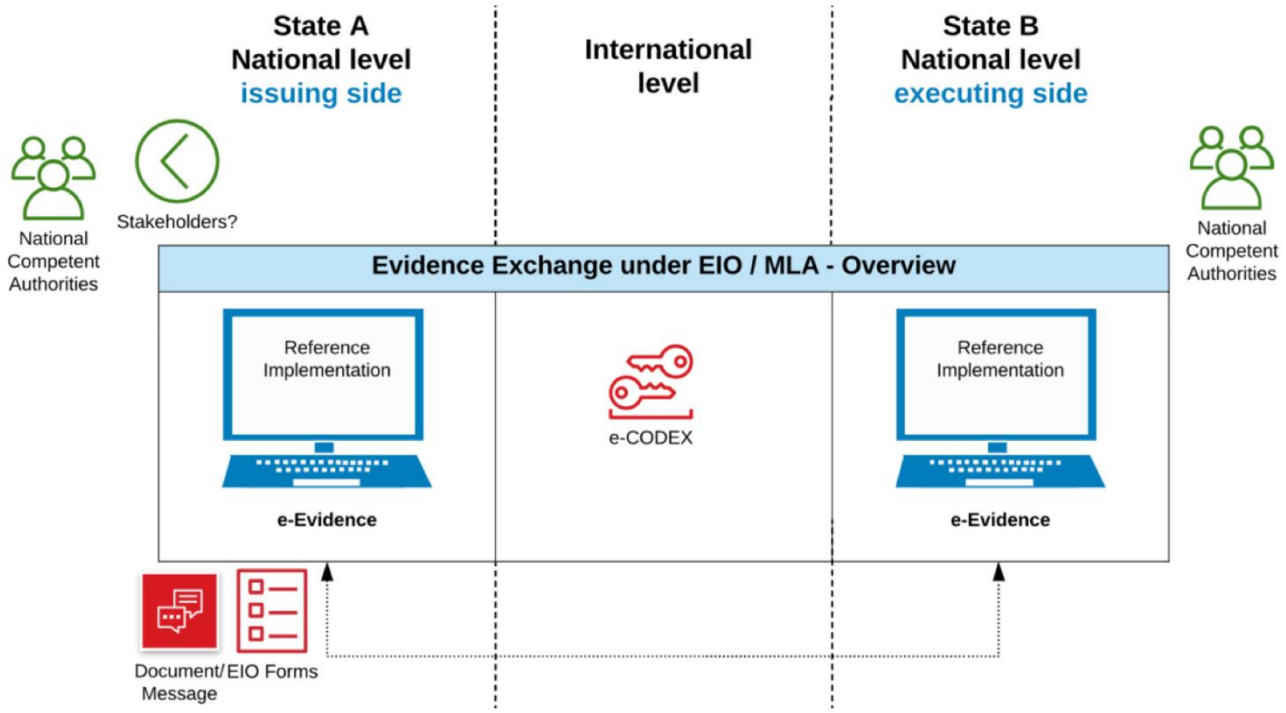

Figure 1: EIO/MLA management using the Reference Implementation

What is missing from this scenario?

Exchanging EIO/MLA forms in a digital way and handling all the business logic behind these legal instruments represent a step forward on the judicial cooperation arena. However, an essential element missing in this scenario is the Evidence File or the Evidence Package, containing all the data and metadata related to an evidence.

In Annex A of the EIO Directive[1] it is said that "…the evidence obtained as a result of the execution of the EIO has to be transferred...". With respect to that another important stakeholder is at stake: the trusted forensic laboratory or the law enforcement agency (LEA) that is able to address the evidence handling. To deal with digital evidences requires a specific expertise - not just an IT background but also a special training for handling different kinds of digital evidences.

In the scenario, illustrated in *Figure 1*, a message, with the Evidence Package attached, will be transferred via the Reference Implementation and over e-CODEX, so it can be affirmed that an Evidence Package could be exchanged as

[1] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

a simple attachment without any specific representation or structure. However, the use of a standard to represent the Evidence Package is of utmost importance.

Why is it important/necessary the use of UCO/CASE?

Benefits in using a standard for the evidence representation include, but are not limited to the following:

- Fostering interoperability: to enable the exchange of cyber-investigation information between tools, organizations, and countries. For example, standardising how cyber-information is represented addresses the current problem of investigators receiving the same kind of information from different sources in a variety of formats;
- Strengthening admissibility (authenticity, provenance);
- Providing trustworthy information;
- Helping in dual/multiple tools validation or results validation/comparison (deduplication of results);
- Enabling more advanced and comprehensive correlation and analysis: In addition to fusing together disparate sources of information, CASE expresses information in a fully structured form that supports a multitude of analysis methods. With respect to searching for specific keywords or characteristics within a single case or across multiple cases, having a structured representation of cyber-investigation information allows pattern searching, graph query, data mining, and other sophisticated analytics. Improved capabilities to find important items can help solve a case, and more effective approaches to finding non-obvious similarities between cases can help overcome linkage blindness.[2]

Scenario where the evidence exchange can take place

Figure 2 shows a real scenario on how the evidence exchange may take place under the umbrella of the EIO/MLA legal instruments.

The right part represents the Executing State or Recipient[3], from EIO flow point

[2] Linkage blindness is a term coined by a criminologist Steve Egger in the context of serial homicides to describe the failure to recognize a pattern that links one crime to another, such as crimes committed by the same offender in different jurisdictions.

[3] It is important to bear in mind that from the Evidence Exchange point of view the role of the Sender is played by the Executing State and the Receiver is played by the Issuing State, being the destination of the exchange flow of the Evidence Package.

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

of view, the left part depicts the Issuing State or Sender, again - from EIO flow point of view, and in the middle, there is the e-CODEX platform where the actual Evidence Exchange takes place.

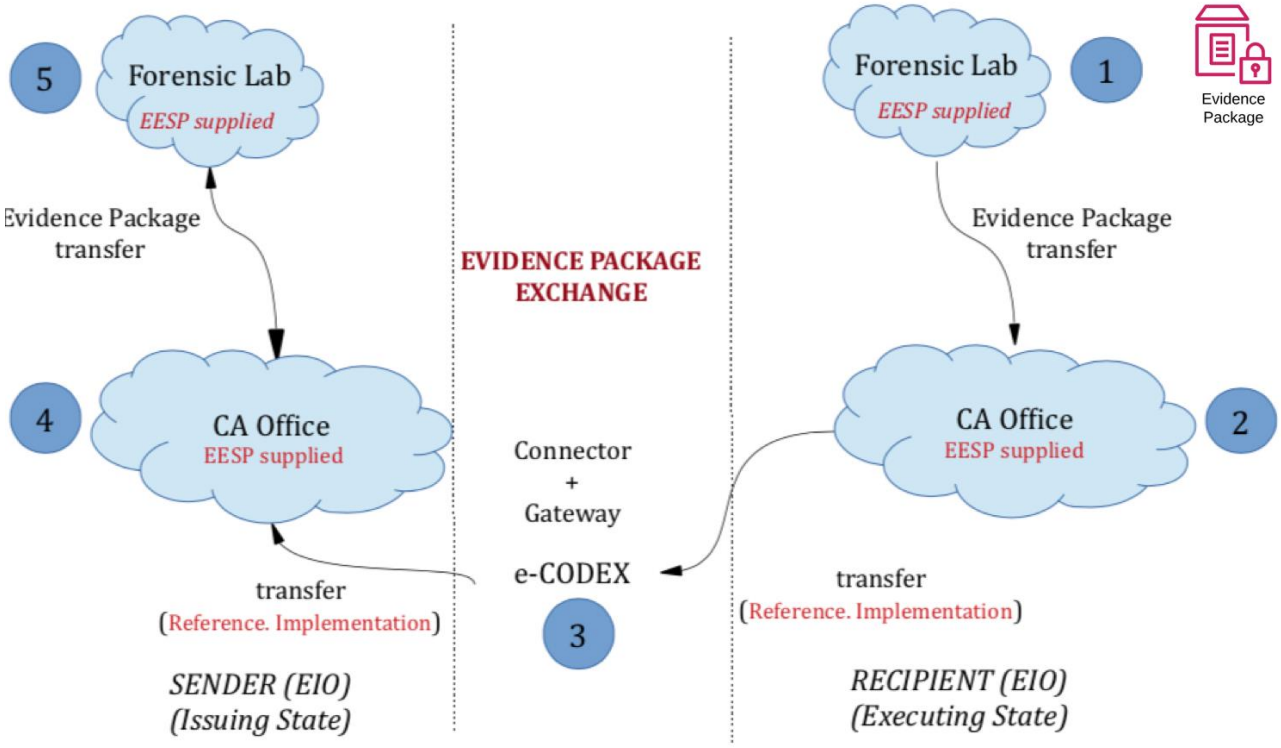

Figure 2: Evidence Exchange Scenario - Overview

The scenario has been broken down into five items. The starting and the end points are the *Forensic Labs (FLs)/LEAs*, supplied with the *Evidence Exchange Standard Package* (*EESP) Application*. When a *Forensic Lab* is requested or needs to send/transfer an *Evidence Package (EP)* to a *Competent Authority (CA)* it has to adopt the proper measures to guarantee the confidentiality, the integrity and the authenticity of the Evidence Package transferred, and ultimately to avoid that someone can tamper with its content.

It is important to point out that:

- Between the trusted *Forensic Lab* and the *Competent Authority* (national level) there is no exchange but the transfer of the *Evidence Package*.

  Evidence Package or Evidence CASE are synonyms; both terms refer to the metadata of an Evidence represented in a standard way through the language CASE that leverages the ontology UCO.

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

- The *EESP* application must be distributed/installed/used in all trusted *Forensic Labs* that will carry out the *Evidence Package* transferring with their *Competent Authority* of reference. Moreover, the *EESP* application will be at disposal of the *Competent Authority* for checking the integrity of the *Evidence Package* and, optionally, reading the content to verify that it contains what is expected. The EESP will communicate with the Reference Implementation, but in case a Member State uses its national solution the compatibility with the EESP must be verified.
- The transfer of the *Evidence Package* along with all data related to an *EIO* (e-Forms, etc.) between *Competent Authority* and *e-CODEX* oversees the *Reference Implementation*.
- The Evidence Exchange occurs in *e-CODEX* (international) environment. It is important to highlight that the e-CODEX project plays the role of controller, not the role of processor or viewer of the *Evidence Package*.

Evidence Exchange Standard Package application

Considering that the use of a standard (USO/CASE language) for the representation of the Evidence Package is essential, it is needed to rely on an application being able to supports UCO/CASE. This is the task of the EESP Application.

The main features of EESP are:

- It supports the UCO/CASE language, being the standard for the representation of the Evidence Package meta data;
- It is a web application for managing the Evidence Package; and
- It aims at preparing the Evidence Package and facilitating its exchange through the Reference Implementation and e-CODEX.

In order to explain where the EESP comes to play, a real investigative case is presented below (see *Figure 3* as a reference of the numbered points).

0. The case is related to a child grooming of Maria, a teenager girl living in Berlin, through Facebook. The German Competent Authority authorizes the acquisition of the girl's phone (Maria's parents voluntarily hand it over to the LEA).
1. The forensic acquisition is assigned to a German Forensic Lab and they use a specific forensic tool to perform the acquisition. An Evidence Package is created with the EESP application. Then, the Evidence Package is transferred to the German Competent Authority.

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

2. The German Competent Authority receives the Evidence Package and reads its content. The extracted data reveals that an Italian guy is involved in the crime, therefore the German Competent Authority issues an EIO to the Italian Competent Authority, using the Reference Implementation, asking them to carry out a search and seizure of the devices of the suspect and to extract evidence from those seized items.
3. The Italian Competent Authority authorizes a search and seizure and assigns to an Italian FL to carry out the action including the extraction of the data from the seized devices. The Italian Forensic Lab carries out the search and seizure, creates a forensic image of the hard disk of the seized computer and carries out a forensic extraction of the data, including some images of Maria. An Evidence Package is created with the EESP application and then the Evidence Package is transferred to the Italian Competent Authority.
4. The Italian Competent Authority receives the Evidence Package, reads its content and sends back the Evidence Package including the images found on the hard disk to the German Competent Authority, using the Reference Implementation.

In the description of the investigative case and in *Figure 3* are described situations where the EESP is used, when it is necessary:

- to create an Evidence Package (after a Search and Seizure; not implemented yet)
- to import a report from a forensic tool in an Evidence Package (after a Forensic Acquisition)
- to read the content of an Evidence Package (i.e. by the Competent Authority of the Executing State, before sending it to the Competent Authority of the Issuing State, through the R.I. and over e-CODEX);
- to import an Evidence Package from the Competent Authority of the Executing State in the Evidence Package already in the hands of the Competent Authority of the Issuing State (i.e. the Investigation begins in the Issuing State and then in the Executing State after the issue of an EIO)
- to prepare an Evidence Package, including the final report, for the Competent Authority in the Issuing State which is going to present the potential evidence before the Court.

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

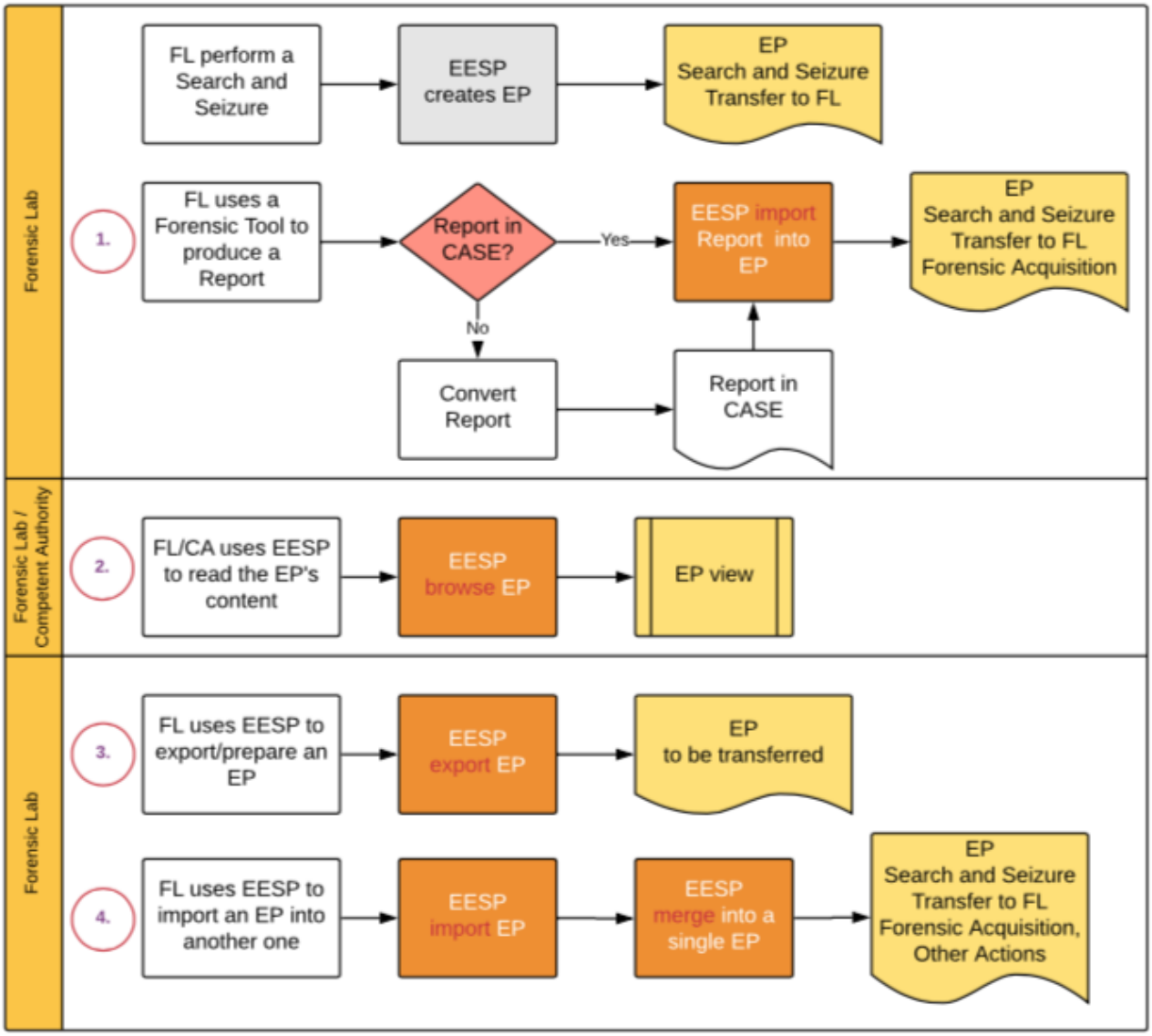

Figure 3: EESP uses in the communication between FL/LEA and CA

Interactions between the EESP application and the Reference Implementation Portal

Evidence Package transfer from the Forensic Lab/LEA to the Competent Authority at national level using the EESP application.

SCENARIO 1: FL/LEA and CA systems information are separated

EESP is separately installed in both the Forensic Lab/LEA and the Competent Authority's systems. No data/database sharing is present except for their Public Key.

Objective

The Forensic Lab/LEA must prepare the Evidence Package (EP) for the national

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

Competent Authority:

The Forensic Lab/LEA has completed the forensic action (search and seizure, acquisition, extraction, analysis) and they must prepare the Evidence Package (data and metadata) to be transferred to the CA.

EESP Forensic Lab/LEA side workflow

The Forensic Lab/LEA prepares and sends to the Competent Authority the following files:

1. the EP: the EP-CASE meta data related to the evidence, expressed in CASE/JSON format, encrypted with the symmetric key (SK), automatically generated at random by the EESP;
2. the EP-DATA-ZIP-ENC[4]: the data related to the evidence, compressed in ZIP format and encrypted with the same SK used for the Evidence Package. Alternatively, if the data size is greater than 2GB another file is generated: the EP-LARGE-FILE-ZIP-ENC. This is the large data file related to the evidence, compressed in ZIP format and encrypted with the same SK used for the Evidence Package.
3. the EP-MANIFEST-RECEIVER-PKI: the *Manifest* of the Evidence Package, encrypted with the Public Key of the Competent Authority of Executing State.

Details of the EESP Forensic Lab/LEA side workflow are shown in *Figure 4*.

EESP Competent Authority side workflow

1. The Competent Authority decrypts the EP-MANIFEST-RECEIVER-PKI file, using its own private key, and reads the content of the EP-MANIFEST.
2. The Competent Authority checks the integrity of EP, EP-DATA-ZIP-ENC or EP-LARGE-FILE-ZIP-ENC (if data size greater than 2GB), using the correspondent's hash values in the EP-MANIFEST. In case of mismatch an error is displayed, and the process stops.
3. The Competent Authority decrypts the EP, EP-DATA-ZIP-ENC and EP-LARGE-FILE-ZIP-ENC (optional), using the SK found in the EP-MANIFEST.

[4] The CASE/JSON file contains, for each Object/Trace of @type=File two properties: *filePath* that is the path in the original device (i.e. /Users/Fabrizio/Documents/Personal/Maria/Images/) and the *extractionPath* that is the local path created by the tool during the extraction phase (i.e. Files/Documents/Personal/Maria/Images/). The tool is responsible to create this information inside its report/output.

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

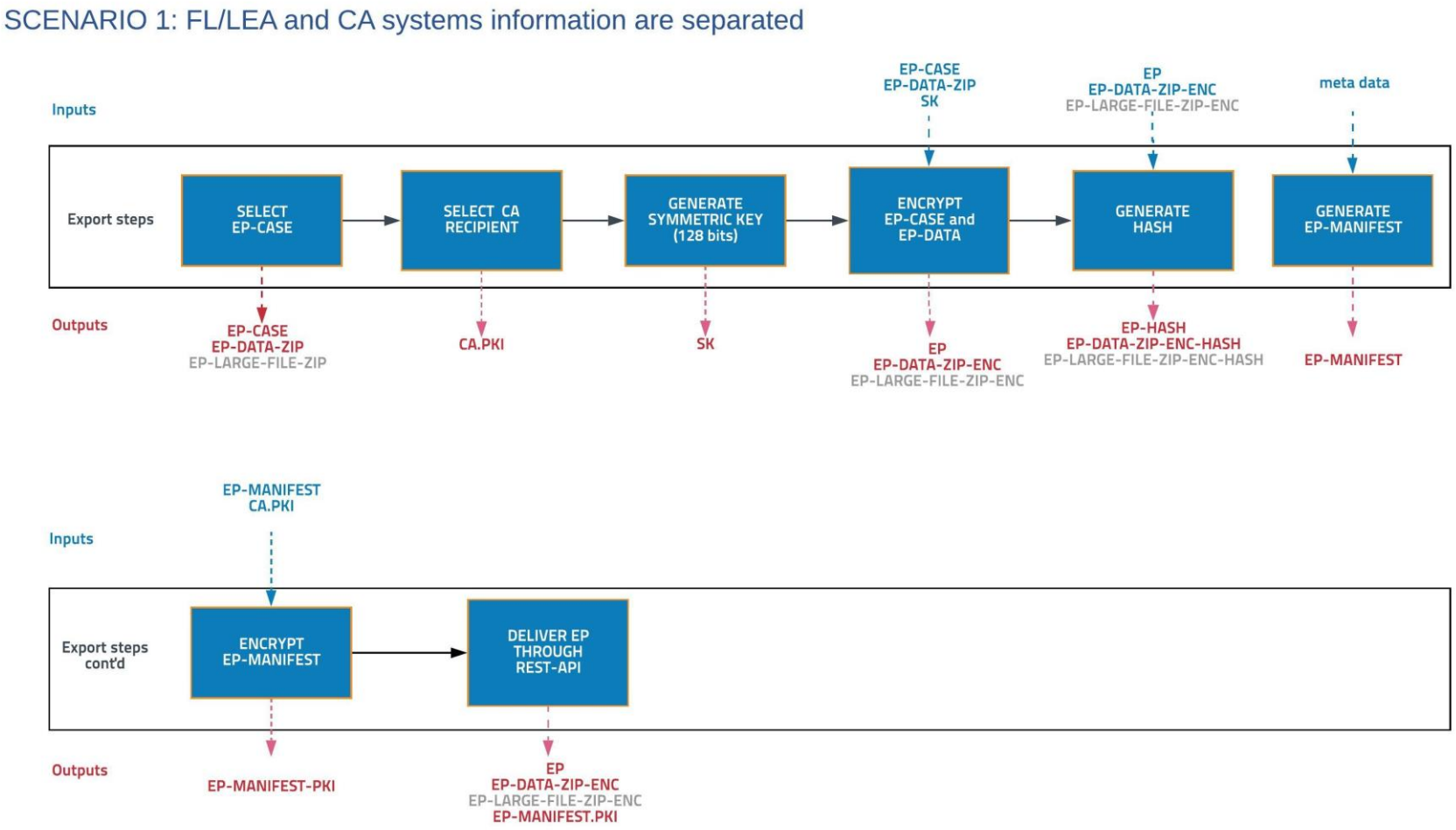

Figure 4: EP export process flow from FL/LEA to the national CA - Scenario

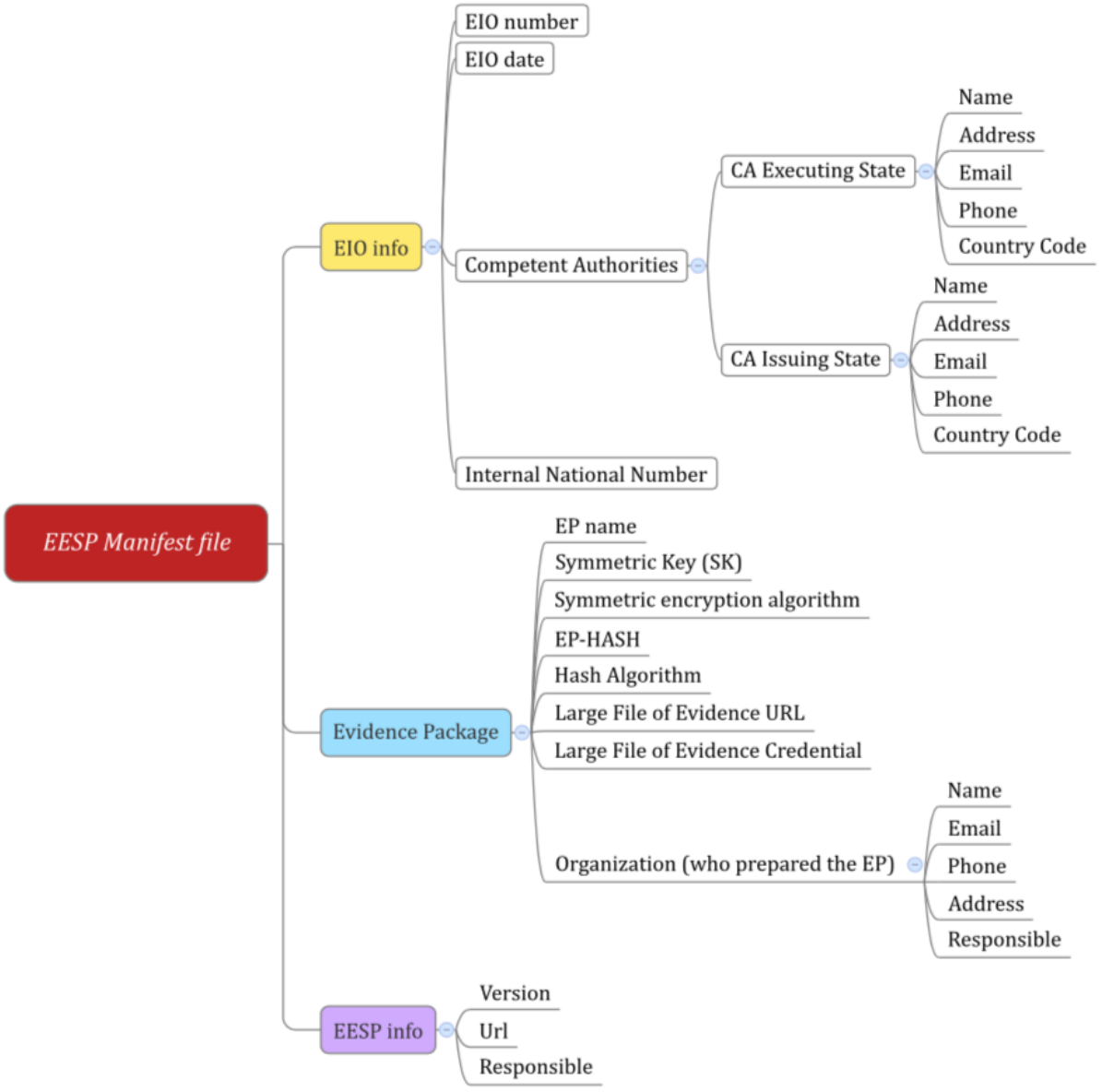

Figure 5: EP Manifest

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468