



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

EESP Application

Evidence2e-Codex & EXEC Workshop

CETIC

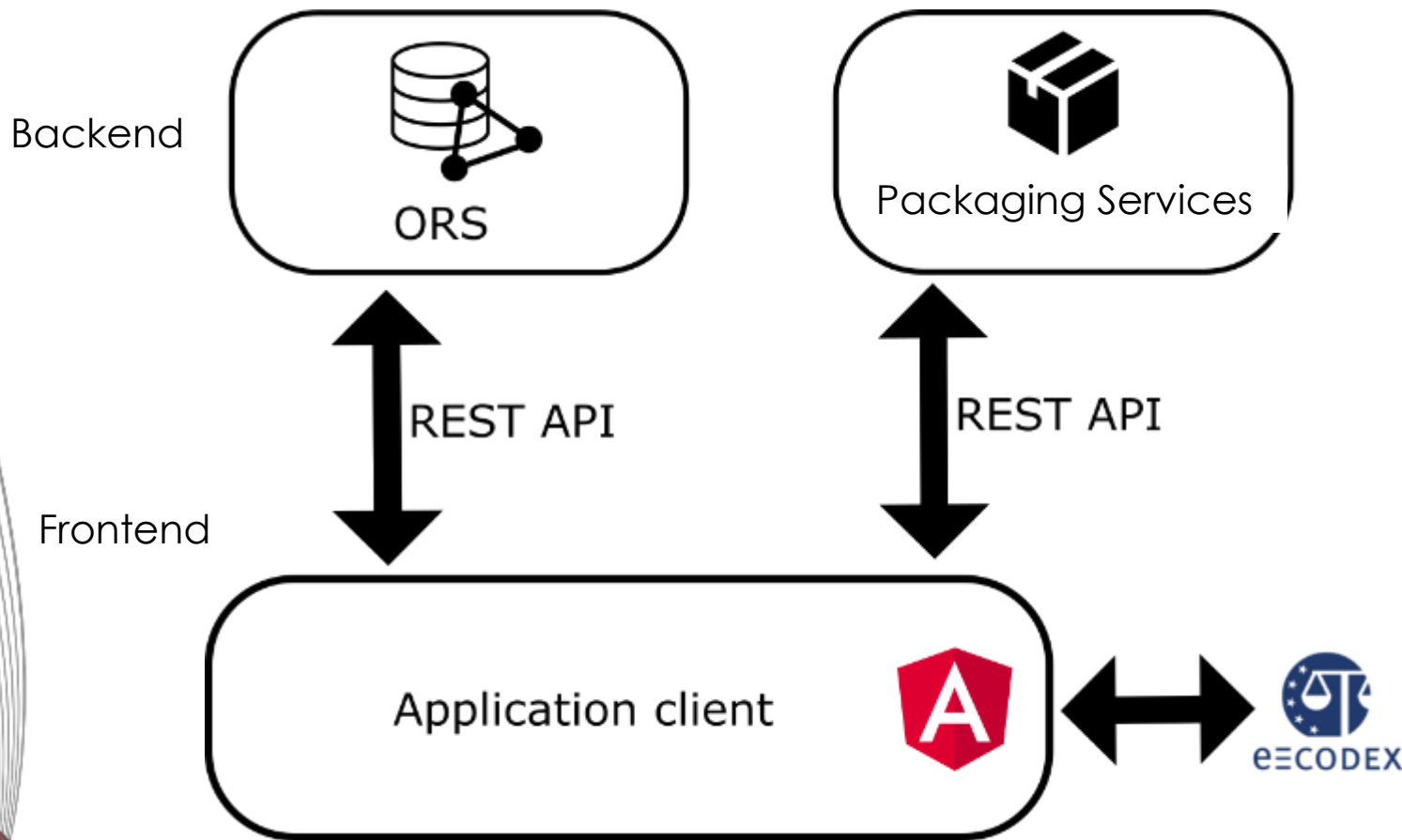


This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

E2E EESP Application

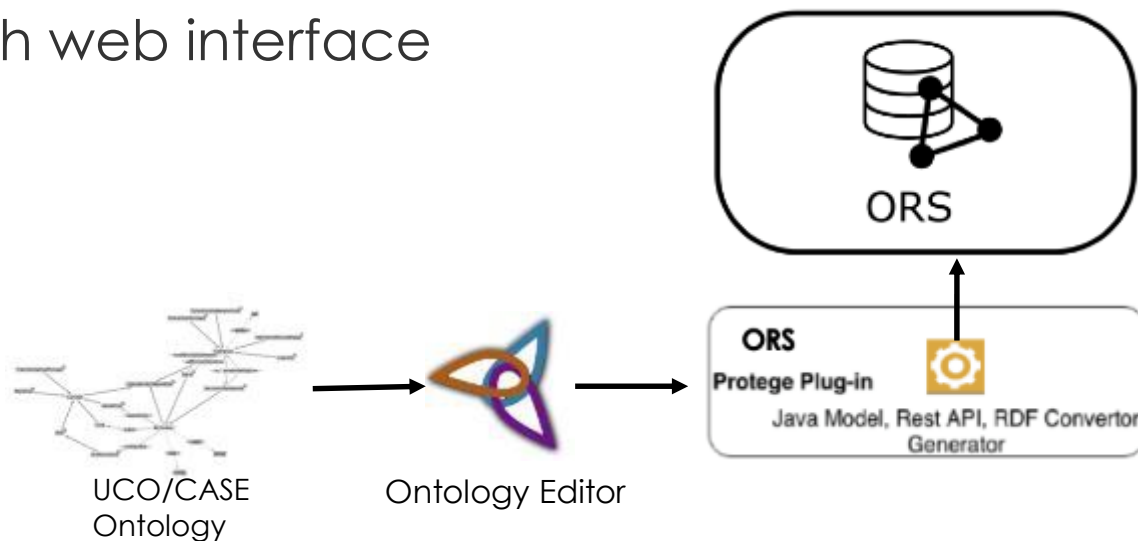
- Evidence Exchange Standard Package (EESP) Application
- Web Application for management and packaging of Cyber-Investigation information
 - <https://evidence2e-codex.cetic.be/>
- Uses the CASE Standard (<https://caseontology.org/>)
 - Data Model
 - Representation Language (JSON-LD format)

EESP Application Architecture



EESP Application Backend

- The Ontology Repository Services (ORS)
 - <https://github.com/cetic/ORS>
 - Backend generation from UCO/CASE Language
 - ORS Protégé Plug-in
 - REST API with web interface



Application Frontend (UI)

- <https://evidence2e-codex.cetic.be/>
- Display/edit of CASE documents
 - Hierarchical view with schema generated by ORS
 - Custom Views - using the tabs/accordion design
 - Forms for creating CASE
- **Report view** and **Chain of Evidence** based on a query graph

Grooming of a teenage girl, through Facebook [IT_2018_FA3G56]
Search Seizure and Extraction of evidence from suspect Mario Rossi for nude images of a minor.

Investigation Actions | Timeline | Identifier | Evidence Tracer | **Chain of Evidence** | Tools | Report

Analysts

Acquisition Hard Disk Inside the computer of Mario Rossi (suspect)

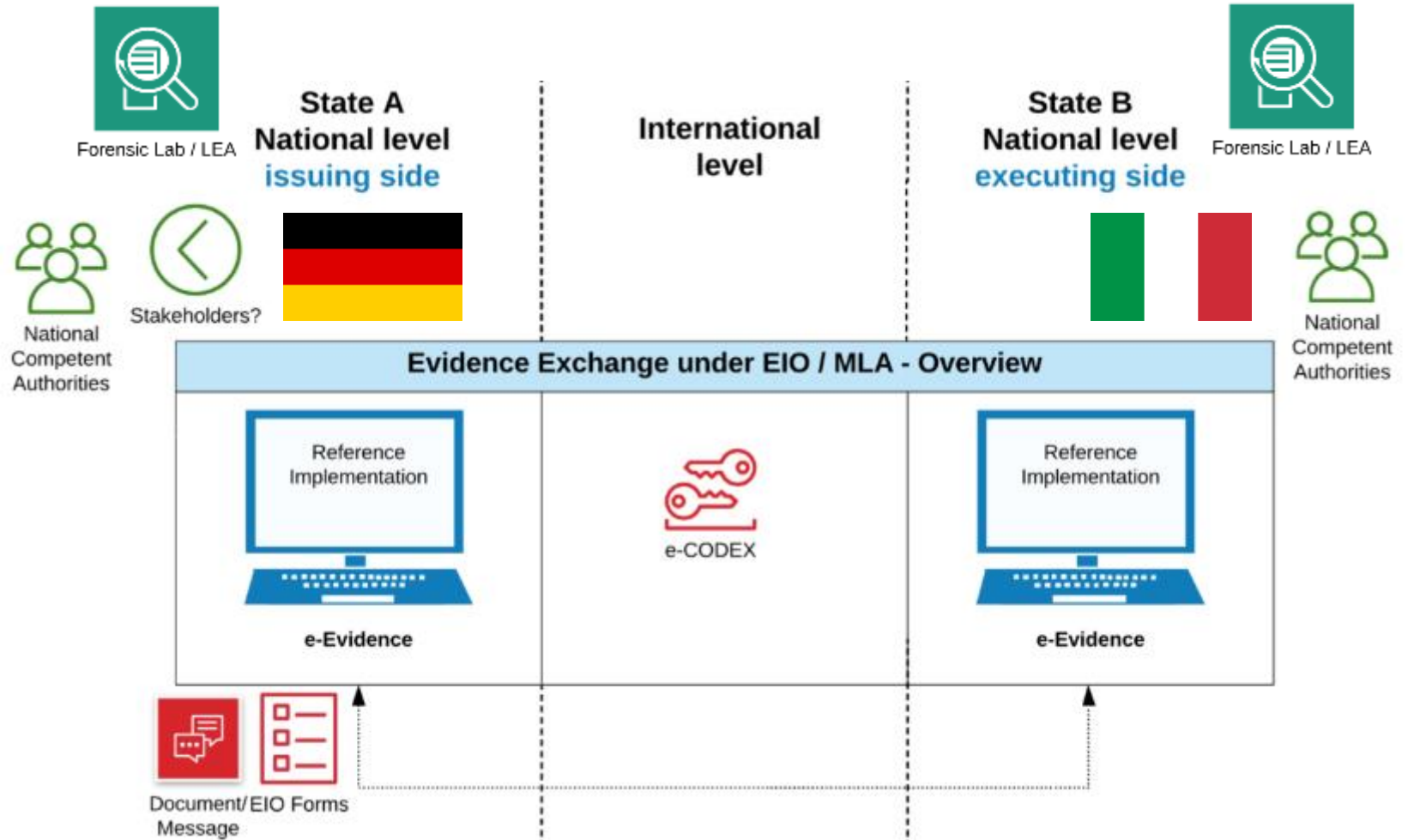
Extraction 10 Images from hard disk of computer (Mario Rossi)

Acquisition (Image of HD Toshiba, computer Mario Rossi)

Images (10) from the hard disk from Computer of Mario Rossi

Serial No.	Modified Time	Writable Changed Time	Is Directory	Is Allowed	File Path	File Name	Extension	Created Time	Acquired Time	Details
5216			false		evidence\	44269428_10.jpg		Mon 08 Oct 2018 22:19:40 GMT		
375808			false		evidence\	44269428_18.jpg		Mon 08 Oct 2018 22:20:40 GMT		
2168			false		evidence\	44269428_19.jpg		Mon 08 Oct 2018 22:20:40 GMT		
5170			false		evidence\	44269428_11.jpg		Mon 08 Oct 2018 22:19:40 GMT		
5216			false		evidence\	44269428_10.jpg		Mon 08 Oct 2018 22:19:40 GMT		
44032			false		evidence\	44269428_16.jpg		Mon 08 Oct 2018 22:19:40 GMT		

Demo Video



Architecture – EESP Packaging API

