EVIDENCE2 / e-CODEX

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

Cyber-Investigation information exchange in Europe via EIO and MLA procedures

DFRWS 2019 EU

Oslo – 24th April 2019

Mattia Epifani / CNR-ITTIG
mattia.epifani@ittig.cnr.it

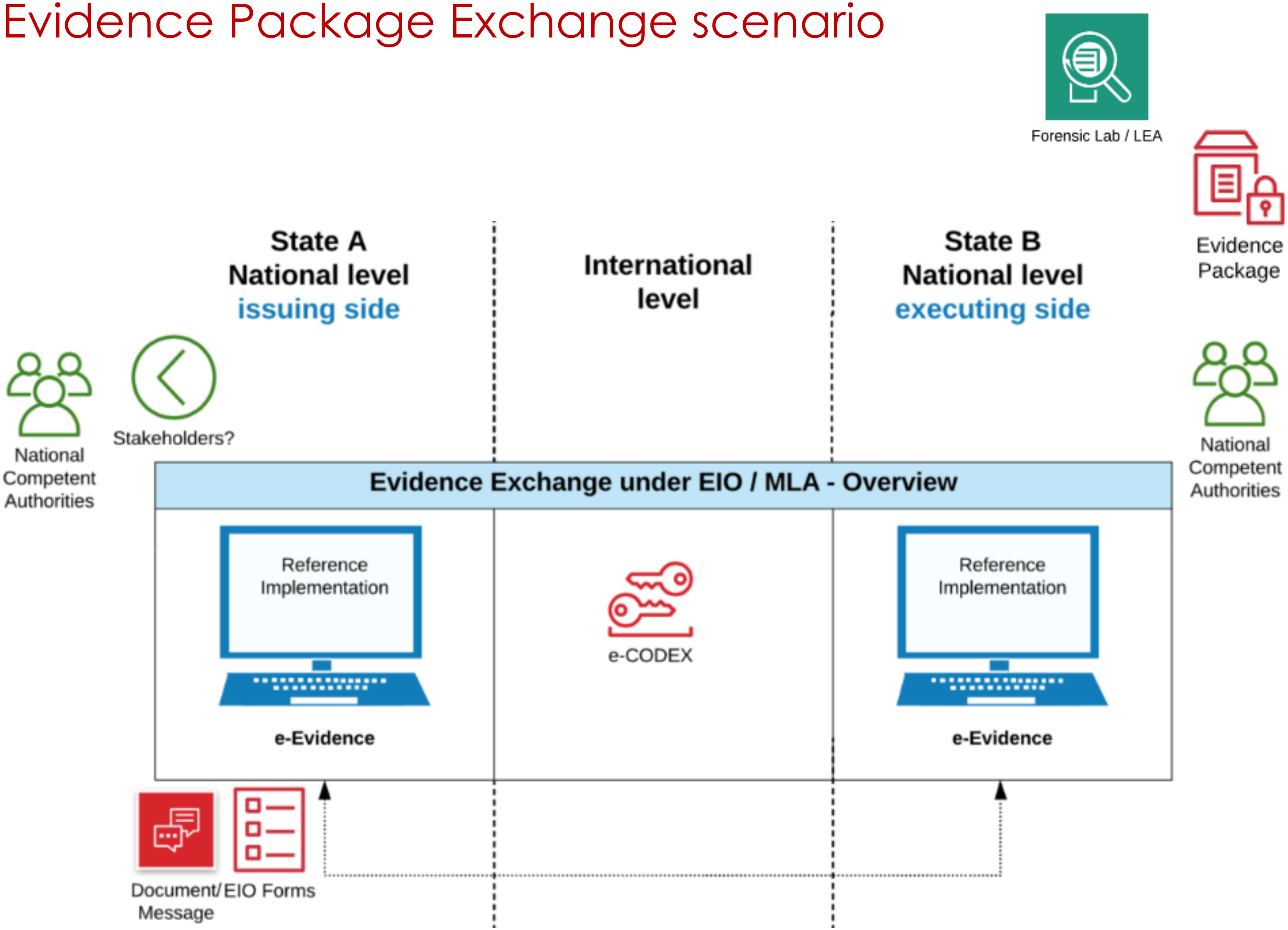
Nikolaos Matskanis / CETIC
nikolaos.matskanis@cetic.be

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

EVIDENCE2e-CODEX Project

- Standards and tools for the **electronic exchange of cyber-investigation information** (Evidence Package or EP)
- Scenarios and methods for the exchange via **European Investigation Order** (EIO) and **Mutual Legal Assistance** (MLA) procedures
- **Secure Transfer via the EU-wide tested e-CODEX platform** in support of an EIO

Evidence Package Exchange scenario



E2E project

- Standard representation for the cyber-investigation analysis: UCO/CASE
- Tools for converting Forensic Tool output to UCO/CASE
- Application for creating, importing and editing Evidence Packages

provides trustworthy information

enables more advanced analysis

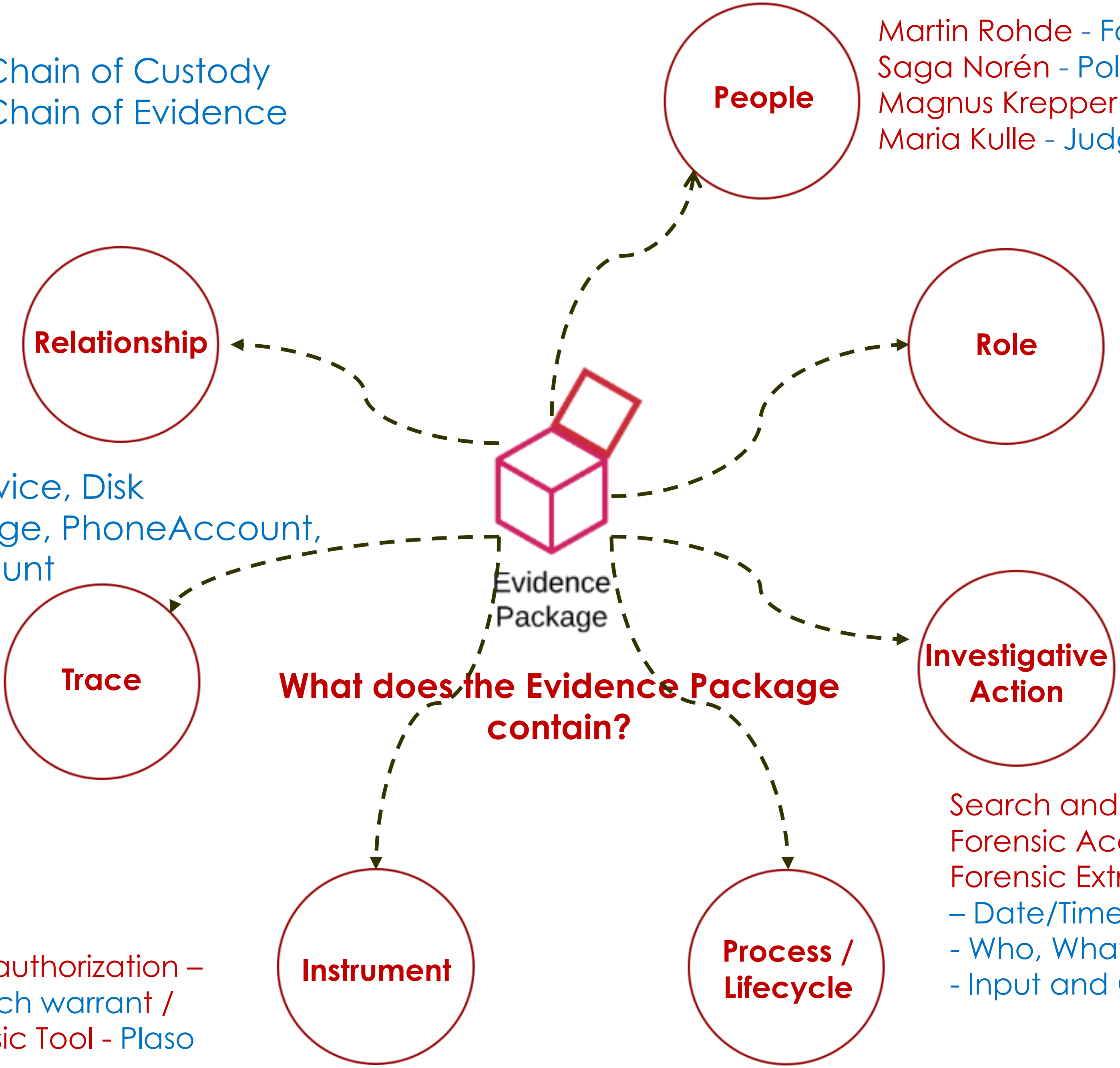
strengthens admissibility (authenticity, provenance)

facilitate dual tools validation

fosters interoperability (tools, organisations, countries)

Benefits/Fruits of the standard

Chain of Custody
Chain of Evidence



What does the Evidence Package contain?

Martin Rohde - Forensic Expert
Saga Norén - Police Officer
Magnus Krepper - Suspect
Maria Kulle - Judge

Mobile Device, Disk
File, Message, PhoneAccount, EmailAccount

Search and seizure
Forensic Acquisition,
Forensic Extraction
– Date/Time
- Who, What, When
- Input and Output

Legal authorization –
Search warrant /
Forensic Tool - Plaso

E2E project

- Standard representation for the cyber-investigation analysis: UCO/CASE
- Tools for converting Forensic Tool output to UCO/CASE
- Application for creating, importing and editing Evidence Packages

Report tool conversion

- caseConverter application
  - PoC intermediate software layer developed to **convert the output of a forensic tool in UCO/CASE standard**
  - As an example we used the **XML report generated by the Cellebrite UFED and by the Logicube Falcon hardware duplicator**

Logicube report conversion: data source

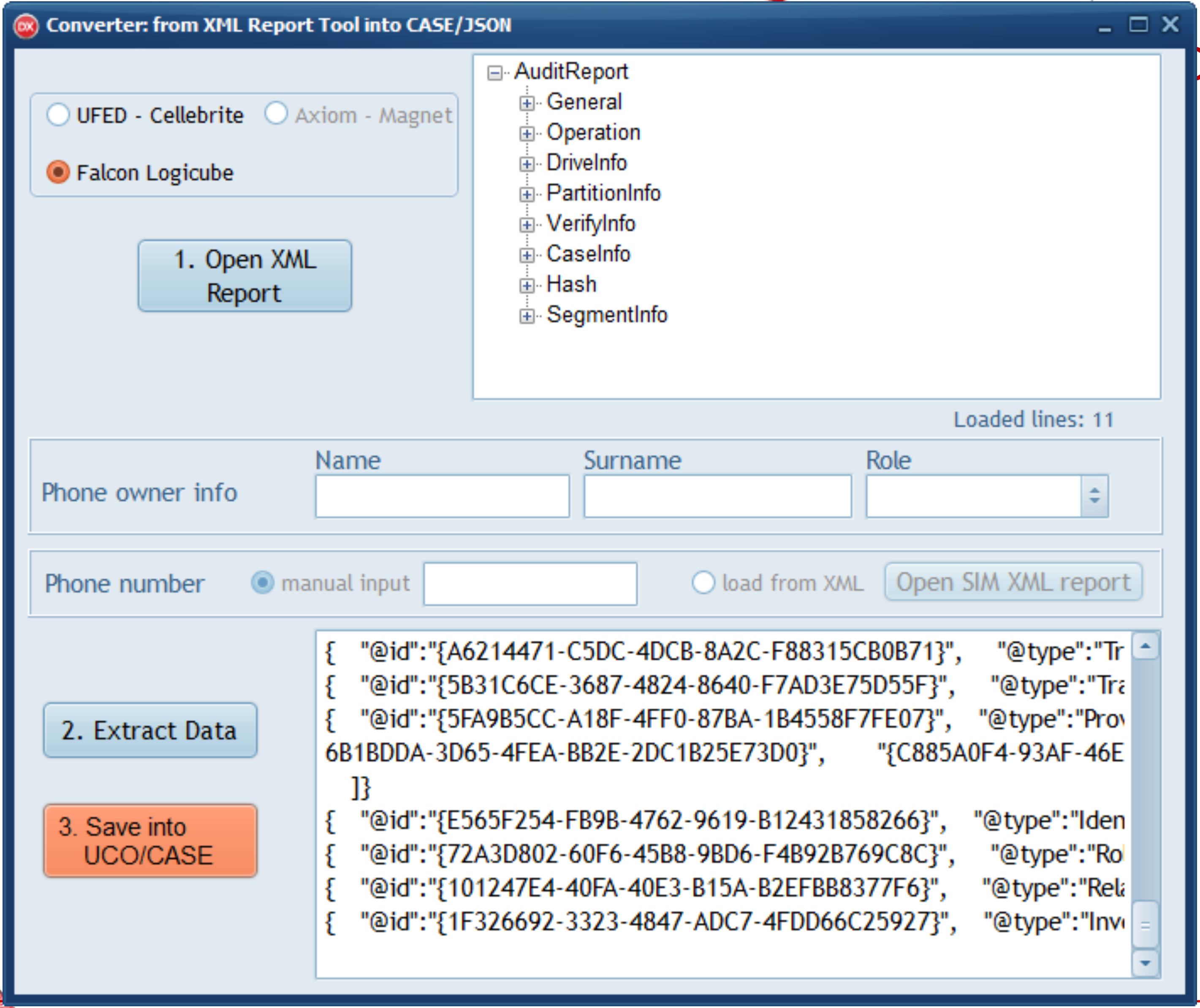
- configuration
  - Mode: DriveToFile
  - Method: E01Capture
  - Hash: SHA-1+MD5
  - SegmentSize: 4GB

- source
  - Hard Disk: TOSHIBA_MQ01ABD100
  - Serial Number: Z612S32MS
  - Capacity: 1 TB

Logicube report conversion: data source

caseConverter demo on Logicube report

ce



Converter: from XML Report Tool into CASE/JSON

○ UFED - Cellebrite ○ Axiom - Magnet

● Falcon Logicube

1. Open XML Report

```
⊟ AuditReport
    ⊞ General
    ⊞ Operation
    ⊞ DriveInfo
    ⊞ PartitionInfo
    ⊞ VerifyInfo
    ⊞ CaseInfo
    ⊞ Hash
    ⊞ SegmentInfo
```

Loaded lines: 11

Phone owner info — Name: — Surname: — Role:

Phone number ● manual input ○ load from XML — Open SIM XML report

2. Extract Data

3. Save into UCO/CASE

```
{   "@id":"{A6214471-C5DC-4DCB-8A2C-F88315CB0B71}",   "@type":"Tr
{   "@id":"{5B31C6CE-3687-4824-8640-F7AD3E75D55F}",   "@type":"Tra
{   "@id":"{5FA9B5CC-A18F-4FF0-87BA-1B4558F7FE07}",   "@type":"Pro
6B1BDDA-3D65-4FEA-BB2E-2DC1B25E73D0}",     "{C885A0F4-93AF-46E
  ]}
{   "@id":"{E565F254-FB9B-4762-9619-B12431858266}",   "@type":"Iden
{   "@id":"{72A3D802-60F6-45B8-9BD6-F4B92B769C8C}",   "@type":"Ro
{   "@id":"{101247E4-40FA-40E3-B15A-B2EFBB8377F6}",   "@type":"Rel
{   "@id":"{1F326692-3323-4847-ADC7-4FDD66C25927}",   "@type":"Inv
```

Logicube report conversion: CASE Objects

Object	**Items number**
Tool	1
Trace (kind File)	38
Trace (kind Disk)	1
Trace (kind DiskPartition)	5
Relationship (contained_within)	5
Relationship (has_role)	1
Identity	1
Investigative_Action	1
ProvenanceRecord	2
Total	**55**

Cellebrite UFED report conversion CASE Objects

- configuration
  - Smartphone: Android
  - Method: Physical acquisition

- source
  - Contacts (PhoneAccount)
  - SMSs (Message)

Logicube report conversion: data source

caseConverter demo on Cellebrite/UFED report

Cellebrite report conversion: CASE Objects

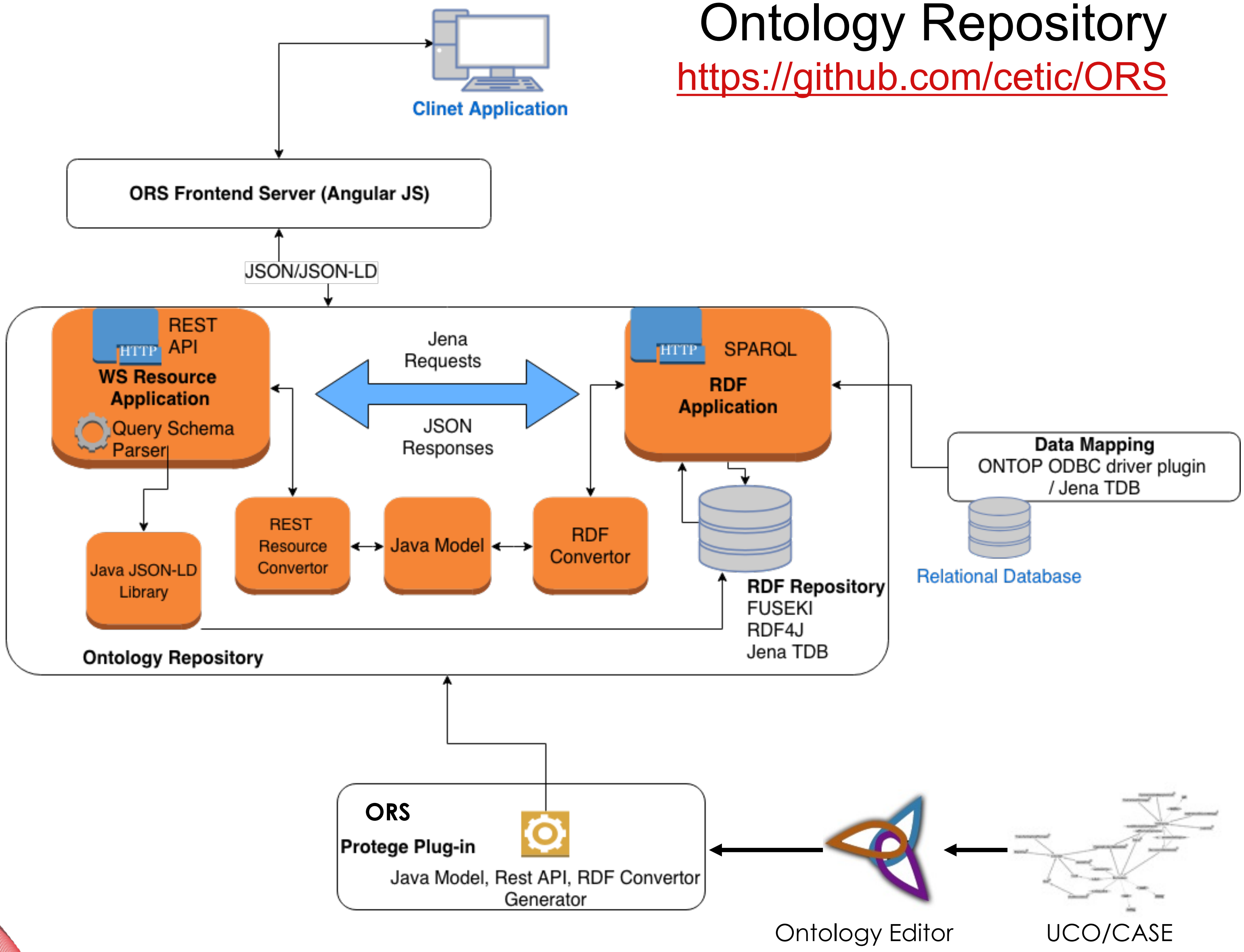
Object	Items number
Tool	2
Trace (kind Mobile device)	1
Trace (kind FIle)	3
Trace (kind PhoneAccount)	15
Trace (kind Message)	9
Relationship (has_role)	2
Identity	2
Investigative_Action	2
ProvenanceRecord	5
Total	**41**

E2E project

- Standard representation for the cyber-investigation analysis: UCO/CASE
- Tools for converting Forensic Tool output to UCO/CASE
- Application for creating, importing and editing Evidence Packages

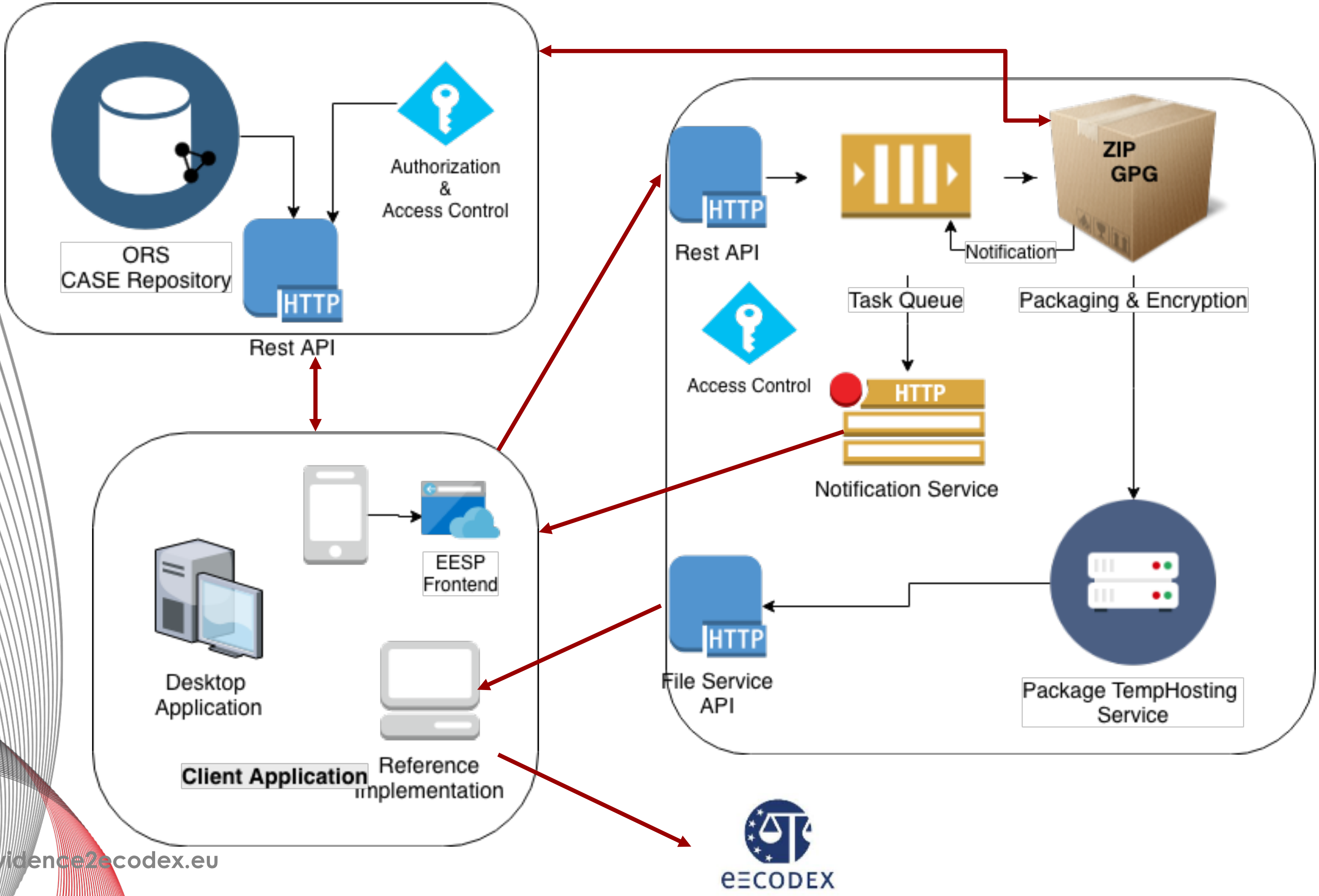
EESP Application Architecture - Ontology Repository

https://github.com/cetic/ORS



EESP Application – Component interactions

https://evidence2e-codex.cetic.be/



Thanks for your attention

Questions?

Mattia Epifani / CNR-ITTIG
mattia.epifani@ittig.cnr.it

Nikolaos Matskanis / CETIC
nikolaos.matskanis@cetic.be