EVIDENCE2e-CODEX

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

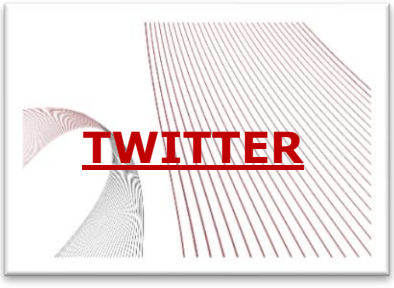
EVIDENCE2e-CODEX Newsletter #5

15 February 2019 – 14 May 2019

February – May period brought us busy schedules and lots of technological project advancements. Some of the most important legal findings were also produced in that period! You can find a detailed summary of all our activities and events in fifth issue of the EVIDENCE2e-CODEX Newsletter!

Dr. Maria Angela Biasiotti, CNR-ITTIG, Italy

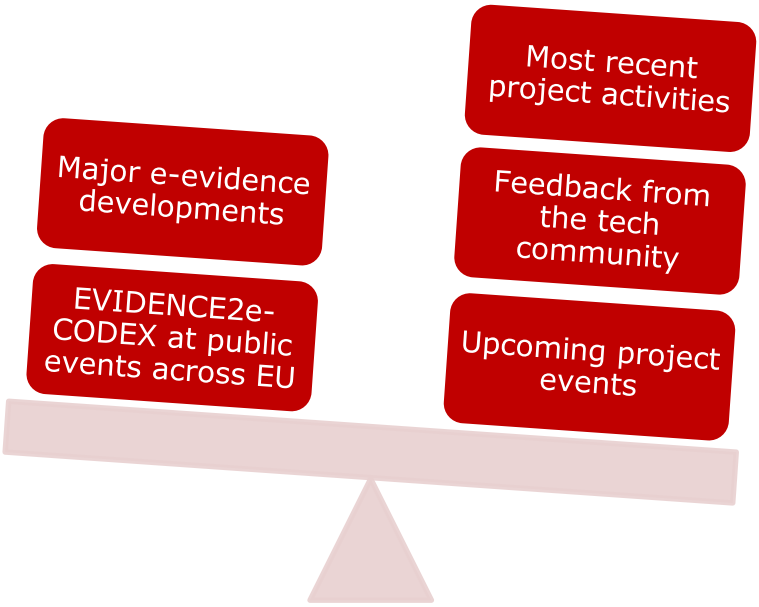
EVIDENCE2e-CODEX Project Coordinator



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

In this issue

Project updates



Get in contact

office@evidence2e-codex.eu

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

Major e-Evidence Developments

Council Agrees Its Position on Rules to Appoint Legal Representatives for the Gathering of Evidence

Source: Council of the European Union

The EU is taking steps to improve cross-border access to e-evidence by creating a legal framework that will enable judicial orders to be addressed directly to service providers operating in the EU.

On 8 March 2019, the Council of the European Union reached its position on the directive on the appointment of legal representatives for the gathering of evidence in criminal proceedings. This directive will be an essential tool for the application of the future regulation on European production and preservation orders for electronic evidence in criminal matters, on which the Council adopted its position in December 2018, as it sets out the rules for the appointment of service providers' legal representatives, whose role is to receive and respond to such orders. The creation of legal representatives was necessary because of the lack of a general legal requirement for non-EU service providers to be physically present in the Union when providing services within the Union. Moreover, the legal representatives designated under this directive could be used for domestic procedures as well.

This directive is part of the e-evidence package tabled by the Commission in April 2018 towards the improvement of cross-border access to e-evidence by creating a legal framework for judicial orders addressed directly to service providers or their legal representative in another member state. The directive complements the regulation on European production and preservation orders for electronic evidence in criminal matters on which the Council adopted its position in December 2018.

Main elements of the Council's position

- The **criteria for defining the location of the legal representatives** remain as in the Commission's proposal. Legal representatives shall be in one of the member states in which the service provider is established or offers services;
- The Council further emphasized that legal representatives should have **enough resources and powers** to perform their tasks;

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

- Service providers and legal representatives may be **held jointly and severally liable** for non-compliance;
- Legal representatives may be used for **gathering types of evidence other than e-evidence**, and for receiving other requests related to law enforcement such as European investigation orders, without prejudice to the specific procedures provided for in other legal instruments for judicial cooperation in criminal matters;
- Specific arrangements to **limit the burden on SMEs** have been added. Those include the possibility for SMEs to 'share' the same legal representative and that individual sanctions against a service provider should consider its financial capacity;
- On sanctions, the text remains as proposed by the Commission and provides that **sanctions shall be effective, proportionate and dissuasive**;
- A **full list of legal representatives shall be made publicly available** to ensure easy access by law enforcement authorities, mainly but not only, via the European Judicial Network on criminal matters;
- The Council has provided for a **transposition deadline of 18 months** in order to make sure that the legal representatives are up and running once the regulation on e-evidence enters into force 6 months later.

Next steps

The Council is to start trialogue negotiations on the whole e-evidence package as soon as the Parliament has adopted its position. This is not expected to be before the forthcoming European elections.

EDPS Released an Opinion on the Negotiating Mandate of an EU-U.S. Agreement on Cross-border Access to Electronic Evidence

Source: EDPS

On 2 April 2019, EDPS released an opinion on an agreement between the EU and U.S. on cross-border access to electronic evidence in response to the European Commission's adoption of a recommendation to start negotiations with the U.S. on electronic evidence access for criminal investigations. The European Data Protection Supervisor wrote he supports the Commission's assessment that the EU "has an interest in a comprehensive agreement with the U.S., both from the

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

perspective of protecting European rights and values such as privacy and personal data protection, and from the perspective of our own security interests." He also added the Umbrella Agreement, which provides a minimum level of safeguards for data transferred to U.S. law enforcement, should be included in the negotiations.

Full text of the Opinion can be found here.

Background

On 17 April 2018, the Commission issued a package of two legislative proposals: a Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters, and a Proposal for a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings. While work is ongoing at the European Parliament, the Council of the European Union (the Council) has reached a general approach on those two proposals.

On 5 February 2019, the Commission adopted two recommendations for Council Decisions: a Recommendation to authorise the opening of negotiations in view of an international agreement between the European Union (EU) and the United States of America (US) on cross-border access to electronic evidence for judicial cooperation in criminal matters, and a Recommendation to authorise the participation of the Commission on behalf of the EU in negotiations on a second Additional Protocol to the Council of Europe Convention on Cybercrime (CETS No. 185). The Annex to the Recommendation is of utmost importance since it lays down the recommended Council's directives to the Commission to negotiate the agreement on behalf of the EU. The latter recommendation is the subject of a separate EDPS Opinion.

Digital Evidence in Focus during 6th European Judicial Cybercrime Network Plenary Meeting

Source: EUROJUST

Judicial practitioners from across Europe gathered at Eurojust, the EU's Judicial Cooperation Unit, for the 6th European Judicial Cybercrime Network (EJCN) plenary meeting (4-5 April 2019), to strengthen the fight against ever-evolving threats posed by cybercrime.

The EJCN provides a cross-border platform to exchange national experience and best practice, get inspiration from other legal systems, discuss real case examples, and find practical solutions in countering cybercrime. It explores the boundaries of

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

the existing legal frameworks in the Member States and works to best interpret these systems to step up the investigation and prosecution of cybercriminals and produce evidence that can hold up in court.

As legal frameworks develop slowly, they are often not in line with the rapidly changing digital technologies that are exploited by criminals. Legal systems were initially created for real-world crimes, and, therefore, provide a limited and often outdated legal basis to tackle cybercrime (virtual-world crime). The EJCN helps to find a way forward, considering the lack of a solid and updated legal basis, by comparing different jurisdictions and extracting successful national case law to be applied in similar cases in other Member States.

The 6th EJCN plenary meeting was attended by members of the Eurojust Cybercrime Team, as well as other key representatives from Eurojust, Europol, the Council, the Commission, and the European Judicial Network (EJN). The main topics of the 6th EJCN plenary meeting were the **direct transborder access to digital evidence** and takedown of domains used for criminal purposes. The second day's discussions centred on investigating darknet criminality and the handling of virtual currencies in criminal procedures.

U.S. Department of Justice Releases White Paper on the CLOUD Act

Source: U.S. Department of Justice

In April 2019, the U.S. Department of Justice (DOJ) released a white paper and FAQ on the Clarifying Lawful Overseas Use of Data (CLOUD) Act, which was enacted in March 2018 and creates a new framework for government access to data held by technology companies worldwide. The paper, titled "Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act", addresses the scope and purpose of the CLOUD Act and responds to 29 frequently asked questions about the Act.

Part I of the CLOUD Act provides that orders issued pursuant to the Electronic Communications Privacy Act (ECPA) to certain technology providers can reach data within those providers' possession, custody, or control, regardless of where that data is stored. Part II of the CLOUD Act creates a framework for new bilateral agreements with foreign governments for cross-border data requests. The DOJ White Paper and FAQ focus in large part on the framework for new agreements created under Part II of the CLOUD Act. Where entered, these new bilateral agreements can be used to remove restrictions under each country's laws so that

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

technology companies may comply with qualifying, lawful orders issued by the other country.

In the new white paper, DOJ describes the CLOUD Act as "represent[ing] a new paradigm: an efficient, privacy and civil liberties-protective approach to ensure effective access to electronic data that lies beyond a requesting country's reach due to the revolution in electronic communications, recent innovations in the way global technology companies configure their systems, and the legacy of 20th century legal frameworks."

As the DOJ paper explains, technology companies often store data worldwide, and the data can accordingly be subject to multiple conflicting laws. For example, conflicting legal obligations may arise when a technology company receives an order from one government requiring the disclosure of data, but another government restricts disclosure of the same data. The DOJ white paper recognizes that "[i]f national laws conflict, [technology companies] may be forced to choose which country's laws to follow, knowing that they may face consequences for violating another country's laws." Those conflicts, the DOJ white paper states, also "pose serious problems for governments seeking data and can frustrate important investigations."

The DOJ white paper explains how new bilateral agreements negotiated under the CLOUD Act's framework can reduce such conflicts of laws. Any such agreements would "lift any restrictions under U.S. law on companies disclosing electronic data directly to foreign authorities for covered orders in investigations of serious crime." In doing so, the agreements "would permit U.S.-based global [technology companies] to respond directly to foreign legal process in many circumstances." The DOJ paper also makes clear that CLOUD Act agreements are to supplement, rather than replace, existing Mutual Legal Assistance Treaties (or "MLATs"). However, by creating a streamlined mechanism for authorities to request evidence in another country, they may have the effect of reducing the number of demands made under MLATs.

The FAQs accompanying the DOJ white paper also address several common questions about the CLOUD Act, including about the extraterritorial reach of US warrants codified in Part I of the CLOUD Act. For example, the FAQ responses note that the CLOUD Act did not give US courts expanded jurisdiction over companies. Rather, DOJ explains that Part I of the CLOUD Act requires companies *already* subject to jurisdiction in the US to provide data in response to US legal process, regardless of where the data is stored. In addition, the DOJ white paper notes that if a US order conflicts with foreign law, "U.S. courts can be expected to apply long-

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

standing U.S. and international principles regarding conflicts of law to ensure appropriate respect for international comity by applying a multi-factor balancing test, taking into account the interests of both the United States and the foreign country."

1.1.1.1

EVIDENCE2e-CODEX at Public Events across EU

The projects achievements of both legal and technical nature found their way to the EVIDENCE2e-CODEX stakeholders via a series of public events across EU:

- **Criminal Justice in Cyberspace Conference**, 25-27 February 2019, Bucharest, Romania

  More than 100 criminal justice experts from some 40 countries, including from public and private sectors as well as international organisations, participated in this Conference on **Criminal Justice in Cyberspace**. The EVIDENCE2e-CODEX project was represented by Alexandra Tsvetkova (LIBRe Foundation, Bulgaria).

  The event was jointly organised by the **Romanian Presidency of the Council of the European Union** and the **Council of Europe**. It was opened by the Minister of Justice of Romania and the Deputy Secretary General of the Council of Europe. The Conference on 26 and 27 February was preceded by a special event on the 5th anniversary of the Cybercrime Programme Office of the Council of Europe (C-PROC) in Bucharest.

  The aim of the event was to add further momentum to solutions tackling these **cross-border criminal activities**, promoting **multilateral co-operation** at all levels to strengthen the rule of law in cyberspace. The conference was opened by the Minister of Justice of Romania, Tudorel Toader and by the Council of Europe Deputy Secretary General, Gabriella Battaini-Dragoni.

  Sessions were arranged around the following topics:

  - Threats, victims and impact of crime in cyberspace: predictions for 2019?

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

- Reconciling security and fundamental rights: implications of court decisions and data protection rules on access to electronic evidence?
- Challenges for criminal justice in cyberspace
- Solutions: Capacity building programmes of the European Union and the Council of Europe

Full information about the event, including programme, participants, resources, key messages, etc. can be found here.

DFRWS EU 2019, 24-26 April 2019, Oslo, Norway

DFRWS EU was held for a sixth year in a row and took place at the KRIPOS Headquarters at Bryn, Oslo, Norway on 24-26 April 2019. The DFRWS conference brings together leading researchers, practitioners, industry, tool developers, academics, law enforcement, and military from around the globe to tackle current and emerging challenges in digital forensics.

The EVIDENCE2e-CODEX Project representatives – Mattia Epifani (CNR-ITTIG, Italy) and Nikolaos Matskanis (CETIC, Belgium), actively participated in the Conference discussions on electronic evidence exchange, by

- **Participating in a dedicated CASE Workshop**: CASE is an international open-source and community-developed ontology/specification language that aims at covering this gap in the most inclusive manner possible. More on the use of CASE in the EVIDENCE2e-CODEX developments can be found here.
- **Presenting during Day 3** on "Advancing the Exchange of Cyber-Investigation Information Between Organizations and Across Borders Using CASE" over the EVIDENCE2e-CODEX advancements in the field.

More about the event can be found here.

'e' Meets Justice Conference, 2-3 May 2019, Lisbon, Portugal

On 2 and 3 May 2019, academics, IT and legal professionals met in Lisbon to discuss how to improve the collaboration between these communities in cross-border civil procedures. The aim of the conference was to offer a platform for different stakeholders to meet, engage in discussions and exchange ideas in order to find a meeting point between the legal world and the digital world, arriving at 'e-justice'. Focusing on e-CODEX as a potential

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

tool to improve the current situation, participants were encouraged to propose ideas, engage in discussions and develop a mind-set to foster the future of e-Justice in the EU.

The event was organised by the e-CODEX Plus Project and the 'Building EU Civil Justice' Project of the Erasmus School of Law of the Erasmus University in Rotterdam. All presentations and other materials can be found here.

EVIDENCE2e-CODEX was represented by Alexandra Tsvetkova (LIBRe Foundation, Bulgaria) with respect to the further potential of the project in civil matters.

Most Recent Project Activities

The Interim Technical Results Approved by EC

To achieve WP3 'Matching EVIDENCE into e-CODEX and Linking to other EU Member States' goals, it is of utmost importance to break down the electronic evidence life cycle in simple phases in order to verify the capacity of the formal language to store the forensic and legal information related to the current status of the evidence. Five different phases can be easily distinguished: initialization of the case, search and seizure, acquisition, analysis taking into consideration the preservation and the chain of custody. Relying on pseudo-anonymization of real cases, a simulation on how the formalism represents all the involved information will be prepared in order to evaluate the strengths and the weakness of the chosen formalism within the EVIDENCE2e-CODEX Project. For each phase the needed amendments will be applied and verified with the main stakeholders involved in the electronic evidence handling.

The verification of the structure under development, was discussed within a serious of workshops in order to include feedback from the scientific community and judicial authorities (public prosecutors, judges, LEAs, etc.), that took place in November 2018 in The Hague, the Netherlands:

- Workshop on the Formal Language for Evidence Exchange Representation, and
- Interim Workshop on Evidence Exchange Standard Package Application.

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

The EVIDENCE2e-CODEX team produced two reports on WP3 achievements so far, the workshops' discussions and the post-discussion implementation of the feedback gathered. Both reports were approved by the EC in February and April 2019 respectfully.

The reports are published online on the EVIDENCE2e-CODEX Website.

EVIDENCE2e-CODEX Finalized Major Overview of the Legal Context on the Implementation of EIO

The EVIDENCE2e-CODEX project aims at pre-piloting the EVIDENCE[1] proposal and achievements together with e-CODEX for the specific purposes of allowing the secure and trusted exchange of digital evidence among EU Member States in the European Investigation Order and Mutual Legal Assistance context. One of the building blocks of the project is understanding the status of implementation of Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters.

Work Package 2 of the EVIDENCE2e-CODEX project is dedicated to understanding the legal context on the implementation of EIO (in Deliverable D2.1 'Report on the implementation of the European Investigation Order'), of MLA procedures (in Deliverable D2.2 'Report on EIO and MLA') and on data protection issues (in Deliverable D2.3 'Report on data protection and other fundamental rights issues'[2]).

This Deliverable, D2.1 'Report on the implementation of the European Investigation Order' (hereinafter 'Deliverable D2.1'), describes how selected EU Member States have transposed the EIO Directive. The selection of countries includes most of the member states party to this project and ensures that different legal cultures around Europe are represented. The deliverable seeks to understand the existing and potential issues that affect the full implementation of the EIO in the EU MSs and consequently the exchange of electronic evidence in Europe. It

[1] EVIDENCE – European Informatics Data Exchange Framework for Court and Evidence Project (2014-2016), Grant Agreement No. 608185

[2] In November 2018, EVIDENCE2e-CODEX published its Deliverable D2.3 'Report on data protection and other fundamental rights issues' examining how data protection implications in European Investigation Orders and Mutual Legal Assistance procedures are being handled, highlighting recent legislative developments in the EU and the potential implications of the Regulation on European Production and Preservation Orders for electronic evidence in criminal matters on current electronic evidence exchange procedures. This report was presented in details in Newsletter #3.

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

analyses the legal and operational measures required to "establish successful execution of EIO between Member States".[3]

The findings in Deliverable D2.1 are based on responses to a questionnaire developed within the project asking different stakeholders in 16 implementing EU Member States to describe how the EIO Directive has been transposed, explaining procedures that have been developed on the basis of the EIO Directive and the operational (including with respect to information and communication technology) structures that are in place. A specific questionnaire was also sent to practicing lawyers in some Member States: the aim of this questionnaire was to understand the working of Article 1(3) of the EIO Directive. Where possible the findings from both questionnaires were compared to findings from other sources found in literature.

Furthermore, this deliverable reflects feedback received by different stakeholders with whom the EVIDENCE2e-CODEX project interacted during the first year of activity and in events carried out in collaboration with the EXEC Project[4]. Stakeholders of interest for the purposes of this deliverable were the following:

- Ministries of Justice of the EU MSs and non-EU States: this category includes different judicial authorities (judges, public prosecutors, and investigative judges), court staff including administrative and ICT staff, institutional training authorities;
- Lawyers: representatives from the criminal law area;
- European institutions dealing with cross-border cooperation: EUROPOL, EUROJUST, OLAF, EJN;
- LEAs: law enforcement agencies of several Member States.

Based on the information collected, the deliverable groups the problems shared by the 16 implementing MSs into four main groupings:

a. teething problems
b. operational problems
c. technical realities
d. training needs.

[3] EVIDENCE2e-CODEX Linking EVIDENCE into e-CODEX for EIO and MLA procedures in Europe (2018-2019), Grant Agreement No. 766468, Work Package 2 'Legal Issues' Description.

[4] EXEC - Electronic Xchange of e-Evidences with e-CODEX (2018-2020), Grant Agreement No. 785818

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

For each of these sets of problems Deliverable D2.1 recommends measures that can be taken by Member States, the EC and/or other stakeholders to address the problems and ensure cooperation between Member States working together in the EIO.

The preliminary findings will be presented during the e-Justice Conference, 20-21 May 2019, Bucharest, Romania.

EVIDENCE2E-CODEX Follows Closely the e-MLA Initiative

Formal mutual legal assistance (MLA) exchanges still follow a cumbersome, paper-heavy and time-consuming process. Traditional means of transmission of MLA requests are either slow or operated through non-secure channels (postal service, email, diplomatic pouch). Those **drawbacks jeopardize criminal proceedings in cross-border cases**, particularly when MLA is needed in cases of emergency or for large-scale criminal activities, such as terrorism, cybercrime or fraud. National authorities and international organizations have called for the development of a secure, global network and expressed their support for the **e-MLA Initiative** to respond to this **pressing need**.

Goal and objectives of the e-MLA System

The e-MLA system will eventually enable all 192 INTERPOL Member Countries to exchange, electronically and securely, formal MLA requests and responses (investigative and evidentiary information) via a dedicated means of transmission.

The electronic communications through e-MLA will necessarily meet the formal requirements that are traditionally attached to MLA exchanges and respect the current chain of transmission between the competent authorities. Thus, the e-MLA system should allow the central and diplomatic authorities of all participating countries to exchange MLA communications, thereby providing enhanced security.

The ultimate objectives of the e-MLA Initiative are to:

- foster international cooperation in judicial matters,
- guarantee the security and integrity of all documents transmitted electronically between the competent authorities,
- enable the admission into evidence of a broad spectrum of information transmitted electronically.

Purpose and outputs of the First Phase of the e-MLA Initiative

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

With the support of the European Commission, the legal phase of the e-MLA Initiative took place over two years (2017-2018) and was led by the INTERPOL General Secretariat along with its two partners, France and Austria. The three main outputs of this phase were:

- a legal feasibility study,
- the INTERPOL Rules governing the use of the future e-MLA system,
- the functional specifications of the e-MLA system (i.e. the outline of the technical features in terms of security requirements and practical needs).

The legal study into the feasibility of such a global system was undertaken in consultation with the e-MLA Working Group, composed of legal practitioners dedicated to judicial cooperation in criminal matters from a wide range of countries. The study involved:

- an assessment of the actual and current demand from national authorities for an INTERPOL-hosted system dedicated to MLA,
- identifying common characteristics and constraints in MLA procedures,
- an evaluation of their impact on the feasibility of creating the e-MLA system pursuant to existing international legal instruments.

Based on the positive outcomes of the feasibility study, the INTERPOL General Secretariat will prepare a set of rules for the e-MLA system that will be submitted to the INTERPOL General Assembly for approval. The e-MLA Rules will be enshrined in INTERPOL's legal framework and will allow all INTERPOL Member Countries to participate in the e-MLA Initiative.

The legal study's findings were presented during 'EVIDENCE2e-CODEX: Meeting the Legal Community' Workshop in January 2019.

Way forward

In the wake of the positive outcomes of the e-Extradition Initiative, the e-MLA Initiative has established a clear need for national practitioners to have access to a secure, paperless and fast mean of transmission of requests for MLA. Building on its experience and technical know-how in data exchange, as well on the legal framework of e-MLA and e-Extradition tools, INTERPOL should be able to launch the technical development of both systems as of 2019.

Also, EVIDENCE2e-CODEX is still to produce Deliverable D2.2 'Report on EIO and MLA' (due in the second half of 2019).

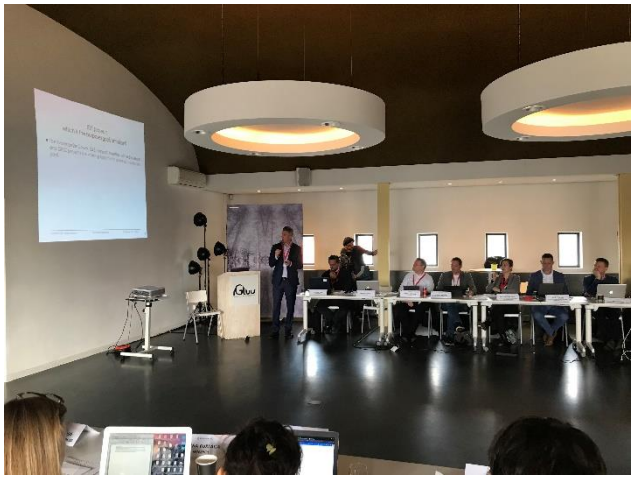
This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

Feedback from the Tech Community

One of the main EVIDENCE2e-CODEX goals is to produce a **'true to life' working solution** by integrating a formal language for representing and supporting the electronic evidence exchange process in an electronic evidence platform based on e-CODEX architecture, i.e. the **Evidence Exchange Standard Package (EESP) Application**. To achieve this goal, the project team broke down the electronic evidence life cycle in simple phases in order to verify the capacity of the formal language to store the forensic and legal information related to the current status of the evidence: initialization of the case, search and seizure, acquisition, analysis taking into consideration the preservation and the chain of custody. Relying on pseudo-anonymization of real cases, a simulation on how the formalism represents all the involved information was prepared in order to evaluate the strengths and the weakness of the chosen formalism within the EVIDENCE2e-CODEX Project.

EVIDENCE2e-CODEX is currently at the final stages of validating different aspects and functionalities of the EESP Application and the project team sought the opinions and views of both the technical and legal communities over its achievements.

'Meeting the Technical Community: Validation of the Evidence Exchange Standard Package Application' Workshop took place on 26-27 March 2019 in The Hague and was designed around six major topics seeking the feedback from practitioners toward the EESP Application's validation.



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

More than 50 experts from the digital justice and forensics community gathered to discuss and network over presentations from project partners and stakeholders. The event opened with a project introduction to the evidence exchange scenario, the benefits of using a standard for evidence representation, the CASE language[5], and the architecture, API and main functionalities of the EESP Application.

Further on, the workshop was designed around six main discussion topics:

- The first panel debated on the **functionality and GUI of the EESP Application**:
  - what kind of needs would judicial authorities/practitioners have using the EESP Application in terms of Evidence Package integrity and authenticity checks, opening and/or verifying the Evidence Package content, etc.;
  - what kind of needs would forensic labs and law enforcement agencies have using the EESP Application with respect to Evidence Package preparation, browsing, encryption, review, etc.;
  - validation of the EESP use cases designed within the project; etc.
- A second discussion was dedicated once more to the EESP Application – this time within the context of the e-Evidence project, developed by the EC, and the potential **integration of the EESP Application** with other platforms, including issued of exchanging messages, links, automatisms, Evidence Package encryption and manifest file, etc.
- The first day finished with two more stakeholders' discussions over:
  - the forensic tools that are already able to produce a report compatible with the CASE standard, highlighting a growing awareness and sensibility toward the importance to adopt this language as a standard in the future, and what is the **forensic tools software development companies' perspective on CASE**, and
  - the **data protection issues and other concerns of legal nature** such as Evidence Package data retention, Evidence Package disposal,

[5] A community-developed ontology to support reporting of digital traces, exchanging of digital traces, and tool validation (express ground truth), in the context of digital forensic science; incident response; counter-terrorism; criminal justice; forensic intelligence; and situational awareness. The CASE language is used as a formal language for representing and supporting the electronic evidence exchange process for the EVIDENCE2e-CODEX EESP Application.

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

the need for special legal grounds the Evidence Exchange Scenario to be accepted in the Member States, etc.

- The second day of the event continued with two sessions dedicated to:
  - dealing with **exchange of large file of evidence**; and
  - a discussion on the **other platforms currently in use for purposes of evidence exchange** and the issues/solutions that these platforms are experiencing.

Each session was organized around a technical overview and/or demo of the specific features, followed by a panel discussion.

The participation of the major stakeholders in the EU arena helps EVIDENCE2e-CODEX to develop and promote the 'true to life' example for electronic evidence exchange. The event welcomed DG Justice and Consumers and e-CODEX representatives, officials from INTERPOL, EUROJUST, EUROPOL, OLAF, International Criminal Court, National Chambers of Judicial Officers, European Judicial Network, and the Ministries of Justice and/or Prosecutor's Office from Austria, Bulgaria, Estonia, Germany, Italy, Netherlands, Portugal, Spain, as well as experts from digital forensics companies, academia and national/international organizations working in the field of judicial cooperation.

The Dutch Ministry of Justice and Security kindly hosted the event in the premises at Igluu Den Haag, Louis Couperusplein 2, 2514 HP, The Hague, the Netherlands.

Upcoming Project Events

The next six months of the project will bring us the EVIDENCE2e-CODEX: Merging Views, to take place in September 2019 in Florence, Italy.

Stay tuned!

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