Intelligence Network & Secure Platform for Evidence Correlation and Transfer

D2.4 e-CODEX infrastructure evaluation in the context of deployment in LLs

Data Management Plan

Grant Agreement No	833276	**Acronym**	INSPECTr
Full Title	Intelligence Network & Secure Platform for Evidence Correlation and Transfer		
Start Date	September 1st 2019	**Duration**	42 months
Project URL	https://inspectr-project.eu/		
Deliverable	D2.4		
Work Package	WP2		
Contractual due date	31.05.2021	**Actual submission date**	Resubmission: 13.01.2022
Nature	R	**Dissemination Level**	PU
Lead Beneficiary	CNR / ML MoJN		
Responsible Author	Huub Moelker		
Contributions from	All		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement No 833276.

Revision history (including peer reviewing & quality control)

Version	Issue Date	% Complete	Changes	Contributor(s)
V0.1			Initial Deliverable Structure	Huub Moelker (MoJN)
V0.2	25/07/21	Draft incomplete	Draft Review status: some outstanding queries with the author who is currently on annual leave.	Robert Dowdall (UCD CCI)
V0.9	25/08/21		Comments processed	Huub Moelker, Fabrizio Turchi, Robert Dowdall, Vivienne Kearns
V1.0	13.01.22	Draft complete	Interim Report Experts' comments addressed.	Huub Moelker

Disclaimer

The content of the publication herein is the sole responsibility of the publishers and it does not necessarily represent the views expressed by the European Commission or its services.

While the information contained in the documents is believed to be accurate, the authors(s) or any other participant in the INSPECTr consortium make no warranty of any kind with regard to this material including, but not limited to the implied warranties of merchantability and fitness for a particular purpose.

Neither the INSPECTr Consortium nor any of its members, their officers, employees or agents shall be responsible or liable in negligence or otherwise howsoever in respect of any inaccuracy or omission herein.

Without derogating from the generality of the foregoing neither the INSPECTr Consortium nor any of its members, their officers, employees or agents shall be liable for any direct or indirect or consequential loss or damage caused by or arising from any information advice or inaccuracy or omission herein.

Copyright message

© INSPECTr Consortium, 2019-2023. This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both. Reproduction is authorised provided the source is acknowledged.

Table of Contents

© INSPECTr 2019

List of Figures

© INSPECTr 2019

Glossary of terms and abbreviations used

Abbreviation / Term	Description
CCTS	Core Component Technical Specification
CEF	Connecting Europe Facility
CTP	Central Testing Platform
ebMS	Electronic business Message Specification
EC	European Commission
EU	European Union
e-CODEX	E-justice Communication via Online Data EXchange
e-EDES	Electronic Evidence Digital Exchange System
EIF	European Interoperability Framework
EIO	European Investigation Order
HCCH	Hague Conference on Private International Law / Conférence de La Haye de droit international privé
IRF	INSPECTr Reference Framework
JHA Council	Justice and Home Affairs Council (of the European Union)
JMS	Java Messaging Service
LEA	Law enforcement agency
LLs	Living Labs
MSH	Message Service Handler
PPO	Public Prosecution Office
SOA	Service Oriented Architecture

© INSPECTr 2019

1 Introduction

This deliverable D2.4 responds to the Subtask 2.3 in work package 2 (WP2). ST2.3.1 states the following:

> *Review e-CODEX[1] model and infrastructure in the context of LLs. E-CODEX infrastructure evaluation in the context of deployment in Living Labs. Living Labs analysis and deployment report. Technical specification for integration or interlinking of e-CODEX with the INSPECTr platform*

Deliverable 2.4 provides input for the achievement result R13 as defined in the INSPECTr project's 'Description of Work' as part of objective 2. It states the following:

> R13: *Integration of the e-CODEX common evidence exchange model and guide for interlinking the INSPECTr platform with the e-CODEX infrastructure.*

This means that e-CODEX is considered to be a building block in establishing the INSPECTr Reference Framework (IRF). The e-CODEX framework has been created to interconnect and make interoperable the e-Justice systems developed so far within Europe and to allow the cross-border provision of e-Justice services.

In the context of the objective and results related to produce the INSPECTr Reference framework, this deliverable describes how the characteristics of the e-CODEX framework can contribute to produce the IRF. Its main characteristics are:

- Content agnostic – The e-CODEX framework can be deployed in any domain. The modelling principles and methodologies applied in the process and semantic layer allow support to any business collaboration.
- Partner autonomy on business, information and infrastructure level – based on the SOA principle of Service Loose Coupling[2], no products or standards are enforced inside a partner's domain.
- Open standards based – Any product that supports this standard is admissible.
- Scalability.

1 https://www.e-codex.eu/

2 Service Loose Coupling: A SOA design principle profile. Thomas Erl (2007), SOA principles of Service Design – Chapter 7

© INSPECTr 2019

2 About e-CODEX

The goal of e-CODEX is to improve cross-border access to legal means in Europe and to improve the interoperability between legal authorities within the EU. Due to high mobility and European integration, procedures containing cross-border effects are increasing. These procedures require cooperation between different national judicial systems. A fully technically interoperable European e-Justice system has been designed. The technical solutions within this context respect both the Union principle of subsidiarity and the principle of independence of the judiciary.

The e-services and infrastructure that Member States have already established cover specific requirements of national legal systems. Generally, these national solutions are considerable investments which cannot simply be replaced by new centralized approaches. The objective of the e-CODEX project has always been neither to re-invent the wheel nor to duplicate one national solution at the European level. The ambition is to build on these national solutions in order to develop a pan-European interoperability layer. Connecting existing systems will allow communication and data exchange based on the development of common technical standards and foster cross-country operation in the area of European e-Justice as well.

2.1 e-CODEX services in relation to the EIF framework

e-CODEX is an interoperability framework that is fully compliant with the principles and recommendations described in the European Interoperability Framework[3] (EIF). Whereas the EIF is meant to be a generic interoperability framework applicable to all public administration in the EU, e-CODEX focuses on public administrations and legal practitioners in the judicial domain.

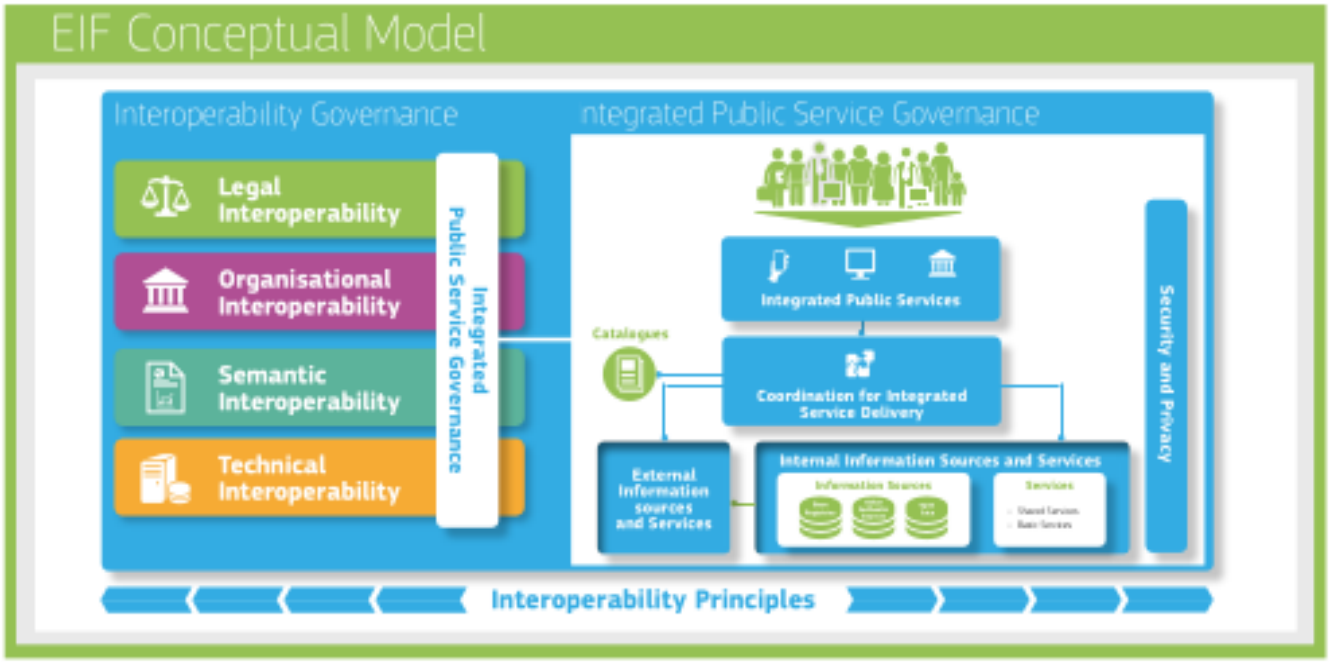

Figure 1: EIF Conceptual model

Though often perceived as an infrastructural system, e-CODEX services also cover the higher interoperability levels of the EIF. The EIF defines *4 levels of interoperability* that, when combined, deliver *integrated public*

3 https://ec.europa.eu/isa2/eif_en

services. As shown in the image above, the EIF Conceptual Model also addresses *interoperability governance, interoperability principles* and *security and privacy* aspects. The e-CODEX framework adopts all of these aspects for specific application in the European legal domain. In the context of INSPECTr, the project's outcome is to be perceived as an integrated public service in the area of digital forensic law enforcement investigations in which e-CODEX building blocks may deliver specific elements of that integrated public service.

2.1.1 The four interoperability layers in EIF and its relation to IRF

Legal interoperability: From e-CODEX perspective, legal interoperability is a given. The e-CODEX service delivery takes no effort in aligning respective national legislations or to create legislation at European Union level. These tasks are the exclusive prerogative of the JHA council, the e-Justice Working Party and national and European Parliament.

For the establishment of EU e-Justice services, the JHA council and e-Justice Working Party are considered to be the senior business executives giving political and policy direction to the e-CODEX consortium's activities. Based on JHA council priorities and established EU legislation, the (legal) conditions are met to start building e-Justice integrated public services. Without an established EU legal framework for a specific legal procedure, the e-CODEX service support for such legal procedures is likely to fail.

Organisational interoperability: In order to exchange and process information and in the case of INSPECTr activities, digital evidence in a legal admissible way, the e-CODEX services in the *organisational interoperability* layer ensure that the common collaboration design for cross-border fits and respects existing national legal traditions.

Typically, the nature of collaboration procedures at EU level is not new to the collaborating partners. For them these often are existing national processes that have been executed for many years between domestic partners. The main difference between a national procedure and a cross-border procedure is that in a cross-border setting a foreign partner assumes a role of a domestic partner making the exact same process an international affair rather than a domestic affair.

The challenge of *organisational interoperability* is to integrate the existing national operations into a common international operation defining the cross-border process and adhering to international legal frameworks. In effect the EU legislation does not establish new procedures, but provides legal validity to interlink existing national procedures and ensuring that the business information is exchanged in a 'court-proof' manner.

The e-CODEX service on *organisational interoperability* provides for a methodology empowering the collaborating partners to co-create a business collaboration design that:

- respects the existing national operations
- creates a common understanding of the cross-border cooperation
- provides insight in and input to the procedure's information requirement necessary to establish *semantic interoperability*
- provides input for the configuration of the building blocks in the *technical interoperability* layer.

Semantic interoperability: *'Semantic interoperabilities ensures that the precise format and meaning of exchanged data and information is preserved and understood throughout exchanges between parties, in other words 'what is sent is what is understood'*[4].

4 Source: https://ec.europa.eu/isa2/eif_en

By means of maintaining a European e-Justice Core Vocabulary, based on which all business message structures are developed, *semantic interoperabilit*y is created at trans-national level. Not only is a common understanding of exchanged information created between partners in a specific use-case, but even so across use-cases. This approach enables a service loose coupled, multi-hop architecture for cross-domain interoperability. These concepts are addressed in more detail in section 3.3.
Besides the core concept of terms used in EU information exchanges, the e-Justice Core Vocabulary also contains reference data and code lists.

Technical interoperability: In cross-domain digitization, the *technical interoperability* layer is the most obvious one. It's obviousness usually results in the fact that most digitization initiatives have a main focus (if not an exclusive focus) on the components in this layer. It is clear that only the components in this layer actually physically connect partners, whereas the higher level components logically connect the partners operational.

In line with EIF (recommendation #33), e-CODEX technical interoperability is established by using open specifications. The most prominent of which is the ebMS 3.0[5] open standard used as the transport protocol on the AS/4 profile[6]. It meets (among others) requirements such as *reliable messaging, non-repudiation* and *track & trace* functionality. In addition to that ETSI REM standard [7]is used for *message evidence* between end-to-end partners in a multi-hop transport environment, also referred to as '*the 4-corner mode*l'.

E-CODEX has developed software components adhering to these standards. In section 3 the components are described in more detail. The Domibus Gateway complies to the ebMS 3.0 standard and is the actual Message Service Handler (MSH) between partners. The Domibus Connector operates in conjunction with an ebMS 3.0 compliant Gateway, providing support to the ETSI REM Evidence handling, facilitating the semantic mapping between EU level and domain level data structures, and provides content integrity checks.

Domibus Gateway and Connector being the de facto standard in the e-CODEX community, the usage of these products is not mandatory. Compliance to the open standards that they are on built is mandatory. There are numerous compliant products on the market that participants can make use of. Just an example of a translation of how the Union principle of subsidiarity and proportionality is materialized at the technical level.

The fact that there is an array of products available that support the chosen standard [8]allows users to choose an implementation that fits their specific IT environments. As most supported products can be operated on different operating systems, no operating systems constraints are imposed on the e-CODEX users. In the specific case of CEF Domibus Gateway, various middleware configurations are supported. In practice, most common implementations are run on Apache Tomcat in combination with MySQL. Supporting documentation is provided on the CEF digital website[9].

5 http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/core/ebms_core-3.0-spec.pdf

6 http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/AS4-profile/v1.0/os/AS4-profile-v1.0-os.html

7 https://www.etsi.org/deliver/etsi_ts/102600_102699/10264001/02.01.01_60/ts_10264001v020101p.pdf

[8] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+AS4+conformant+solutions

[9] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Domibus

© INSPECTr 2019

2.1.2 Interoperability governance

As interoperability can be defined as *the ability to interact between operations* and that the domains in which these distinct operations take place enjoy full autonomy, ownership and governance of the common components establishing the interoperability needs to be arranged. In the context of European e-Justice the group of partners involved is one of equal peers. Exclusive ownership cannot be allocated to a single one of these peers. In each layer of interoperability certain common assets are created and to be maintained;

- At the organisational level business process collaboration designs are sustained at the common level. Prioritisation and allocation of initiatives supporting European legal procedures by means of e-CODEX should be agreed upon by all stakeholders.
- In the semantic layer the Core Vocabulary, the methodology for its maintenance and the XML schemas tailored for each specific use-case, require consensus from the parties involved.
- The development of software components in the technical level and keeping security requirements and the choice of standards up-to-date.

During the project phases (e-CODEX, me-CODEX and me-CODEX II) interoperability governance is arranged for within the e-CODEX project consortium, acting as the e-Justice service provider. Management Board and General Assembly decision making processes ensure empowerment of the e-CODEX / e-Justice service consumers; the Member States, legal professions and European Commission (EC). With a view on the transition from a project phase to a sustainable run-time operation of e-CODEX, interoperability governance is defined in the e-CODEX regulation. The legislative procedure formally establishing the e-CODEX system as the means for interoperability between Member States in a European Regulation, was completed in December 2021. By means of this 'REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a computerised system for communication in cross-border civil and criminal proceedings (e-CODEX system)' , e-CODEX is formally recognised as the communication system specifically designed to facilitate the cross-border exchange of messages in the justice area in Europe.

The resulting e-CODEX regulation will address the above mentioned concerns at each level of interoperability. In its current version, balance of power between the future service provider (eu-LISA), the service consumers (Member States & legal professions) and service sponsor (European Commission) is ensured. It results in a sustained e-service provision in the legal domain, satisfying the needs of participants.

© INSPECTr 2019

2.1.3 Interoperability principles

Figure 2: EIF Interoperability Principles

In designing and deploying the e-CODEX building blocks in cross-border collaborations, EIF interoperability principles are not only respected, but explicitly advocated for by the e-CODEX consortium giving support to the respective collaborating partners.

Most importantly the European Union treaty principles of subsidiarity and proportionality are the main drivers behind the EU e-Justice service. It is with good reason that these Union principles are listed first in EIF interoperability principles. On many occasions over the course of the project, certain design decisions had to be weighed and the operational autonomy of Member States (as a reflection of the first EIF principle) generally prevailed in that process.

In addition to the 12 general EIF principles, more IT specific design principles in obtaining optimal interoperability solutions are embraced. Service Oriented Architecture design principles such as 'Service Loose Coupling' and 'Service granularity' are recurring considerations in creating integrated public services for the European legal domain.

Some principles are at first glance contradictory however, for example, a question that is often asked is, how many gateways a Member State or partner may deploy.

Underlying reason for the question is that for some participants, determining which domestic authority is competent in a specific case is fuzzy or dispatching information to multiple executing authorities may be hard for the partner to establish.
Based on the principle of solving complexity in the domain where the complexity exists one would draw the conclusion that the specific reasoning would not allow for the deployment of multiple Gateways to be addressed by the sending partner. The receiving partner now has conveyed its complexity to its foreign business partner, which now has to figure out which authority in the other Member State would be competent.

However, the (prevailing) principle of subsidiarity (thus operational autonomy) allows any partner to configure their domain to their liking. Neither the e-CODEX consortium nor the future service provider will take a stand in the matter, but would moderate the discussion and merely provides recommendations.

2.1.4 Security & privacy

Not surprisingly the security and privacy demands have had full attention when creating the e-CODEX interoperability framework. By means of complying to European legislation on the matter and adhering to several international standards and best practices, the security recommendations for deployment and usage of the e-CODEX framework have been created.

As with the other components in the framework, the approach to establishing security and privacy measures has been subject to the principles of subsidiarity and proportionality. This means that the e-CODEX consortium believes that a top-down approach at EU level to national level will not work. As there are no central

© INSPECTr 2019

components, no data is created or stored at EU level, the complete e-CODEX setup 'lives' inside the domains of the participants. Hence the e-CODEX setup inside such domains needs first and foremost to comply to the security and privacy rules of that domain. As all independent participants, by default are to comply to EU regulations, transposed into national legislation, they would automatically fulfil the requirements at EU level too.

By laying down security and privacy recommendations, the e-CODEX consortium has sought interoperability on this specific subject, respecting the participants legislative and operational autonomy and common measures at EU level.

3 The main e-CODEX components

In order to better understand the working of e-CODEX and the components deployed at the (EIF) interoperability levels (operational, semantic, and technical) a brief description of the components is provided in the following paragraphs

3.1 Business collaboration support – creating predictable behaviour

Being able to cooperate with partners beyond the borders of your domain is not as straight forward as it may seem. Even if you both operate on the same European legal basis and if, in essence your tasks are similar, there still may be substantial differences in the way your respective operations are designed. Country A may have allocated all tasks within one entity whereas country B may have distributed task for the same international procedure to several organisations. This task allocated and distribution may be different in all Member States of the Union.

However, as a single Member State you do not want to bring this kind of complexity into your domain resulting in a possible 26 different implementations to execute the exact same procedure. In order to overcome this, a single common business collaboration design is created with which all partners can comply. Touch points of each national procedure are mapped based on roles rather than organisations. The complexity of different domestic implementations is to be overcome by process orchestration and choreography within that implementation. At EU level, this creates predictable behaviour which makes digitization of the procedures less complex.

The methodology for creating the business collaboration design is applicable to any procedures thinkable. In the context of e-CODEX it is applied in the domain of Justice, but it would be just as applicable in e.g. agriculture, health, et cetera. The e-CODEX Common Evidence Exchange model has been created accordingly and it allows for the creation of any other exchange model that may be required in the scope of the INSPECTr project. It relates to result:

R13 – Integration of the e-CODEX Common Evidence Exchange Model and guide for interlinking the INSPECTr platform with the e-CODEX infrastructure

3.2 EU e-Justice Core Vocabulary – a pivot language understood by all

When the touch points of a procedure are charted, the information requirement for each touch point is articulated. It defines which information is necessary to be able to perform the task initiated in that touch point. Typically this information requirement is modelled into XML message structures.

In judicial procedures, information related to cases, persons, types of crimes, locations, objects and many other are recurring business information entities. In order to be able to map these terms to terms with the same semantic meaning in the language of the partners involved, definitions of the terms at common level are laid down in the e-Justice Core Vocabulary. The e-Justice Core Vocabulary is comparable with the CASE language [10]used in INSPECTr for the articulation of specific forensic data attributes. In INSPECTr the e-Justice Core Vocabulary may be deployed to create data structures for the exchange of procedural information between authorities, complying to the information requirements as laid down in the legal forms linked to the legal procedures being executed

The e-Justice Core Vocabulary is the base for each XML schema used in the e-CODEX information exchange. It can be viewed as the ‘semantic supermarket’. From the available semantic building blocks, you fill you cart in

10 https://caseontology.org/

order to obtain the 'ingredients' for your specific data requirements. The CCTS standard allows for 'leaving out' (omitting) components that you do not need. It does not allow for manually creating new components. However new components can be created in common understanding, which will result in adding a new semantic building block to the shelves of the semantic supermarket.

As a result, this approach creates consistency and sustainability in the usage of the business information entities. Not only within a single use-case which may have several iterations over time, but also across use-cases. As indicated previously, the term 'witness' will occur in many procedures. Having a common understanding of what 'witness' represents helps in mapping to your local information household. Not only the business information entities are reusable, also the mapping building blocks (e.g. XSLT) are reusable easing the implementation

3.3 The infrastructure layer

At infrastructure layer the two main components are the Gateway and the Connector. Combined they directly or indirectly interconnect the partners involved. They have distinct meaning and are explained below. The infrastructure is designed in a way that partners have the ability to choose in what constellation it will be applied.

By default a single point of contact at domain level is advocated for. One Gateway/Connector setup can serve multiple back-end organisations and systems. This setup is referred to as a multi-hop connection or a 4-corner model. The end to end collaboration is executed over multiple parties; the sending business entity 'hops' to the sending service provider, the sending service provider 'hops' to the receiving service provider and the receiving service provider 'hops' to the receiving business entity, hence 'multi-hop'. The access point of a partner acts as the Single Point of Contact for that domain to any cross-border partner of organizations in that specific domain. The organization are not confronted with standards and practices that are applied at the common (in this case EU) level. The organizations keep operating on the standards applicable in the domestic domain. Protocol translation and data transformation at the domain border ensures interoperability with partners outside that domain.

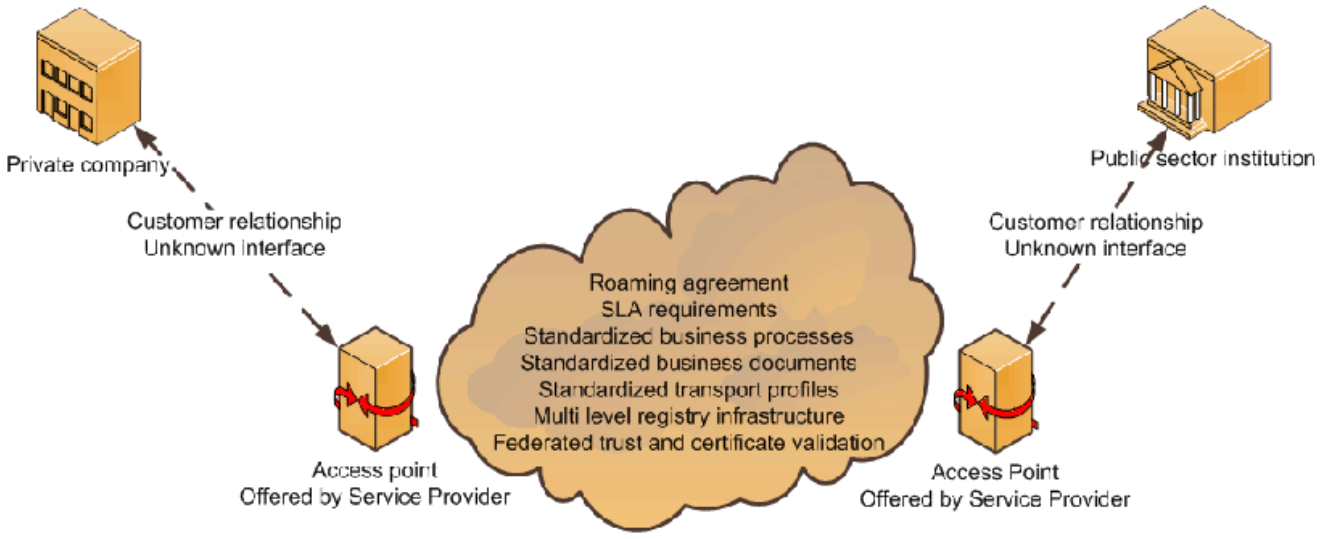

Figure 3: 4 corner model / multi-hop

Alternatively organizations may be in direct contact with a specific non-domain partner or with another entire domain. Organizations that choose such setup, deploy their own private Gateway and Connector which become a 'single use access point'. Organizations choosing this setup must realize that they confront their

foreign partners with the burden of interconnecting multiple access points of the entities that live in your domain. E.g. if the Ministry of Justice in Portugal chooses to connect their PPO offices, the courts, the penitentiaries, the bailiffs on an individual bases, their foreign peers must establish and maintain connections with all these individual partners, rather than establishing and maintaining a single connection with an overarching Portuguese judicial domain service provider. In this example Member State complexity is being conveyed to cross-border partners.

3.4 The Gateway – physically interconnecting the partners

The Gateway operates on the ebMS 3.0 standard. There are many products available supporting this standard. E-CODEX does not dictate which product a partner needs to use. Any standard compliant gateway suffices. A list of ebMS 3.0 AS/4 conformant products is available on the CEF website[11]. The de facto standard among e-CODEX participants is the CEF Domibus Gateway. This is an open source product initially developed by the e-CODEX project, but handed over to DG Digit of the European Commission. Since this hand over the gateway is referred to as the CEF Gateway. The CEF gateway is available free of charge by download from the CEF website[12].

Regardless of the chosen setup (multi-hop or peer-to-peer), gateway interconnection is established by means of a PKI infrastructure approach. For security reasons, specific but not uncommon requirements on the certificate usage are set. Obviously self-signed certificates are not admissible. Between gateways both channel encryption and payload encryption is applied. In the context of current e-CODEX business collaborations , connection is established over the internet as non-governmental partners as lawyers, notaries and bailiffs are not allowed to access the sTesta network[13]. If, as is the case for INSPECTr, governmental partners in a closed community decided to deploy the e-CODEX building blocks on such a private network, that may be possible.

Especially important in a multi-hop setup, the payload encryption feature ensures that the content of the payload is not exposed to the e-CODEX service provider. Only routing information for dispatching within the receiving domain is exposed to the e-CODEX service provider.

3.4.1 Managing your digital front door

The gateway (and connector) setup allow for the support of multiple business processes to multiple partners. However your gateway, being your digital front door, is not automatically open to any business partner. Access and e-service support for each individual gateway is governed by so called pMode configuration. These pModes are the key to your front door, describing partners web addresses, supported procedures and ebMS 3.0 reliability and security settings. As the owner of a gateway you are in control of which partner may collaborate with you in which e-service that is supported by your gateway. For instance if your organization only participates in the EU legal procedures European Investigation Order, the Small Claims and Service of Documents e-services, your gateway will reject any messaging related to the common EU e-service for Financial Penalties. Additionally, if you collaborate with Public Prosecution Office Milano Italy in the European Investigation Order and Service of Documents, PPO Milano will not be able to send you messages related to Small Claims even though you participate in Small Claims with other entities.

The pModes are centrally created by the e-CODEX service provider and distributed to collaborating partners.

11 https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+AS4+conformant+solutions

12 https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Domibus

13 https://ec.europa.eu/isa2/sites/default/files/testa_overview_-_july_2018.pdf

© INSPECTr 2019

Collaborating partners will load the pMode configuration files on their gateway maintaining control over their front door. The pMode configuration files may be compared to the concept or 'rules of engagement' as referenced in INSPECTr work package 3 related to the pub-sub functionality.

3.5 Domibus Connector – integrating EU collaborations in national back-end operations

The connector serves three main purposes;

- facilitating semantic mapping from EU structures to national domain structures. Data structures agreed upon at EU level can be mapped to data structures at domestic level, allowing participants to communicate internally on domestic information structures, but externally on European data structures.
- authentication/ validation of sending entities – Federated trust is established as the origin of a message might not be possible to establish by an entity in the receiving domain. As there is a trust relation between corners 2 and 3 (the access points) the 'sending' access points validates the origin of the message by putting a so called 'Trust OK token' to the message. The receiving access points conveys this trust OK token with the actual business message to the final recipient.
- handling of sending and receiving message evidence. Between the gateways, message reliability and non-repudiation is covered by the message acknowledgements within the ebMS 3.0 standard. In a multi-hop environment message reliability and non-repudiation is created by using ETSI REM evidence. In a peer-to-peer connection, the gateway's default message acknowledgements would establish reliability and non-repudiation.

3.6 The Central Testing Platform

For the purpose of testing your gateway and connector setup, the Central Testing Platform (CTP) has been created by the Aristotle University of Thessaloniki which has been a consortium partner since the very beginning of e-CODEX. Before actually connecting to one of your business partners or their e-CODEX service providers, it is advised that you connect to the CTP first.

On individual basis you can perform bug fixing without consuming time of your partners helping you to setup your gateway/connector configuration correctly. The CTP is accessible only via an internet connection and not via a private network such as sTESTA.

© INSPECTr 2019

4 Deployment support

Interconnecting the Living Labs of the Law Enforcement Agencies through e-CODEX entails the transportation of message content and related digital evidence that is created within the INSPECTr platform. Within the platform e-CODEX has no role. The platform creates content in any shape or form to which e-CODEX is agnostic. It does not need to know what is 'inside the package'. It just needs to know where it is coming from and where it needs to go. E-CODEX is found at the borders of the INSPECTr platform depicted in the image below under '1. INSPECTr Network of LEA Living Labs'

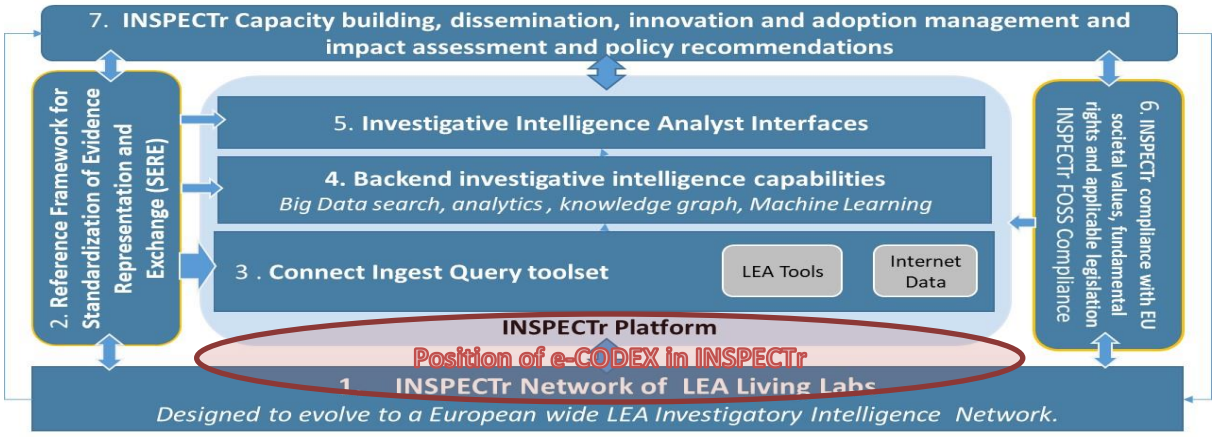

Figure 4: INSPECTr framework

As the e-CODEX platform is completely content agnostic, it can carry any type of payload. Typically it is used to carry civil and criminal justice case information interlinking the domestic business processes of the collaboration partners. These may be governmental administrations but also legal professionals such as lawyers, notaries and bailiffs and others. Generally the conveyed payload content populates the respective case management systems of these entities enabling them to domestically coordinate and execute the required legal tasks.

Additionally any type of attachment may be linked to the payload. In the scenarios within the scope of the INSPECTr project, it would be possible to exchange the developed queries and the returned results. Files in CASE format can be transported as an attachment to the e-CODEX messages formatted on the EU e-Justice Core Vocabulary populating the authorities case management systems. Transport of digital forensic evidence in disk-dump, image or video format is supported, however supported file size may be limited due to domestic or common level capacity restrictions.

For the INSPECTr Living Lag, the e-CODEX system interlinks the various INSPECTr nodes in order to create a network of independent nodes. Any data collection, aggregation, dissemination or interpretation is done inside these nodes. Concerns as articulated in INSPECTr D8.5 and related to ethics, transparency and accountability apply on actions performed in the nodes. E-CODEX assumes that any output of these nodes is compliant to all requirements set for the INSPECTr Living Labs. As e-CODEX is completely content agnostic, it performs no checks on the INSPECTr requirement compliancy, nor does e-CODEX read or process any of the information the node output entails. Most likely such output shall be delivered to e-CODEX in encrypted format. E-CODEX just boxes, addresses and dispatches the (encrypted) output for secured delivery at its intended recipient.

For the e-CODEX system similar requirements have been set in its architecture and have been materialised in the various components of the system. The system has been evaluated by a Commission's scrutiny board and has been approved at the time. As a result e-CODEX has obtained the status of an established service by European

regulation. Whereas most deliverable of the INSPECTr system are newly created and experimental, e-CODEX is not a deliverable of INSPECTr but merely a commodity enabling linkage of INSPECTr nodes. The expected outcome of the Living Lab tests for e-CODEX is therefore not to assess its security or its quality, but to assess its applicability in the context of INSPECTr Living Labs exchanges.

4.1 Legally valid information exchange between foreign authorities

Preserving the chain of evidence, by linking legal case management information to digital forensic case management information is paramount for executing 'court-proof' digital forensic investigations, prosecution and court ruling. In order to perform the INSPECTr task in a legally valid manner, the participants have to comply to applicable European and national legislation. Typically legal validity is established by adhering to European legal frameworks specifically allowing the exchange of information for a certain task. The European Investigation Order (EIO) procedure establishes the legal validity for the majority of the tasks performed in INSPECTr context. However other legislative frameworks may be applicable.

4.1.1 Digitally supporting EU legal frameworks

In earlier e-CODEX initiatives, the digital support for executing the EIO was created and is ready to be used within the INSPECTr context. The process collaboration and XML structure building blocks have been created, according to the approach described in paragraphs 3.1 and 3.2. These are ready for use with the competent judicial authorities linked to the selected Law Enforcement Agencies that will participate in the INSPECTr living labs. Members of the e-CODEX consortium are available to provide context and explanation on how to interpret and use the created building blocks when the provided written documentation raises any questions.

Should it be necessary to provide business collaboration and semantic support for other legislative bases than the EIO, specific procedure building blocks can be created. Business collaboration or semantic building blocks could also be created without having a formalized European legal basis. E.g. for the purpose of supporting the pub-sub interactions between INSPECTr nodes.

However, the main focus of e-CODEX support to the INSPECTr project is expected to be on exchange infrastructure level.

4.2 Infrastructure

4.2.1 Choice of network

In order to setup the infrastructure, the collaborating partners need to reach agreement on what type of network is to be used. Such decision should be made with a future-proof vision in mind. Considerations like extending the number of participants and their country of origin or the business domain in which they operate will provide main guidance for this decision.

At this point in time the living lab will be limited to law enforcement agencies of five European Member States. The LEAs may be subject to their domestic Ministry of Home Affairs. However, in order to obtain legal validity for actions taken in the INSPECTr framework, cooperation with a competent authority may be required. If the competent authority is a public prosecution office (PPO) or an investigative judge, collaboration between a HOME and JUST domain is necessary and requires the selection of a network that they both can access.

© INSPECTr 2019

When upscaling the amount of participating law enforcement agencies, scalability and accessibility are key factors. Presumably upscaling will initially entail other EU Member State LEAs and judicial competent authorities. However, the nature of the crimes subject to digital forensic investigations dictate that focus may also lie beyond the borders of the European Union. Eventually cooperation with non-EU entities may be a realistic scenario.

Choosing a closed European network in the current Living Lab phase may lead to a massive network migration for all connected participants in the future. It is advised to interlink the INSPECTr nodes via e-CODEX gateways over the internet. Arguments leading to a deviation of network choice should be well documented for future reference.

4.2.2 Choosing a topology

A second major decision to take, but now on individual basis for each individual LEA participant is determine whether to use a multi-hop or a peer-to-peer topology. Again long-term sustainability and common interoperability principles should be taken into account. Depending on the organisational structure of the Member State or domain within a Member State the outcome varies from LEA to LEA. Some Member States have implemented a strict functional and technical separation between e.g. HOME and JUST authorities whereas other Member States may have implemented shared infrastructure between ministerial domains.

Also in countries that have a federated structure as for example Germany has or have 'autonomous regions' as is the case in Spain, a functional domain may be split in sub-structures. A domain or sub-structure may be serviced by a dedicated single point of contact for that structure interconnecting all relevant authorities inside that structure. This would allow for deploying a multi-hop or 4-corner model setup for an e-CODEX gateway.

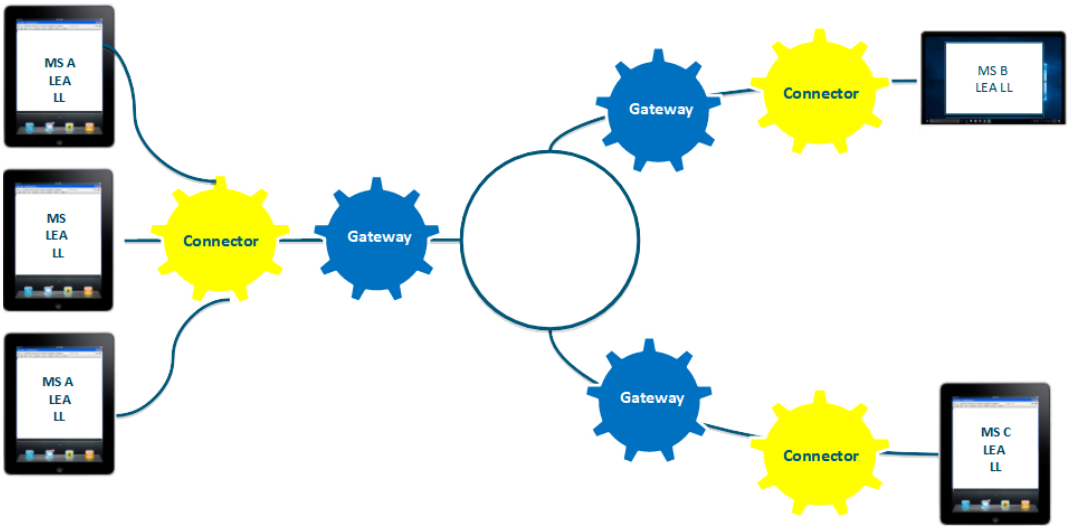

Figure 5: Mixed topologies

In general a peer-to-peer topology directly interconnecting local and regional participants in cross-border collaborations is strongly discouraged, but explicitly not prohibited from e-CODEX consortium perspective. The number of gateways across Europe would grow significantly leading to a massive maintenance and administration burden. Not only for the Member State choosing a peer-to-peer topology, but also for its partners which may be in a multi-hop topology, collaborating with that particular Member State. If, for example, the judiciary in Romania chose to deploy a dedicated gateway for each individual court, over 200 gateways would be added to the e-CODEX network. As connections between gateways is established by

© INSPECTr 2019

deploying pMode configuration files and PKI infrastructure not only the initial setup has to be done 200+ times, also maintenance effort as a result of expiring validity of certificates and pModes grows exponentially. For this reason the so called multi-hop or four-corner model topology is strongly advocated for, having a 'national contact point' servicing regional and local participants in cross-border

Quite possibly collaborating authorities are already organised into existing network structures on which INSPECTr participants have been in collaboration with national partners in domestic procedures for many years already. Ideally these network structures are interlinked as a whole, by deploying an e-CODEX gateway as a domain 'gatekeeper'.

In the current e-CODEX participant community both multi-hop and peer-to-peer implementations are found. Experiences of participants may support participants in the INSPECTr community in their decision making process.

4.2.3 Setting up the Gateway and Connector

Based on considerations described in 4.1.1 and 4.1.2 the implementation location of the Gateway and Connector setup for each participant is determined. The actual installation of both gateway and connector is extensively documented by DG DIGIT[14] and e-CODEX consortium respectively. Installation and operations manuals are freely available. The Commission's CEF team is at the disposal of the INSPECTr participants that choose to implement the CEF Domibus Gateway. As the use of the CEF Domibus Gateway is not mandatory, participants may choose to deploy another ebMS 3.0 compliant gateway product. Support on any such product is to be obtained from its distributor. The technicians within the e-CODEX consortium can at any time be contacted [15]for hints and advice on gateway and connector deployment.

In addition to that, the e-CODEX consortium provides hands-on workshops. These workshops are aimed at familiarizing new participants with the infrastructural components in a local or sandbox environment. As a result of the current pandemic, the hands-on workshops are not presently organised. The e-CODEX consortium will be offering an alternative in the form e-CODEX 'lab-box' or 'starter kit'. The concept of this lab-box is that new implementers can individually familiarize themselves with the component's functions and prepare for an installation in formal test and production environments. However, to date the lab-box package is not yet available for distribution, but will soon be available.

4.2.4 Creating the pMode configuration files to enable the INSPECTr workflow

Although it is possible for INSPECTr participants to create the so called pModes within the project, it is strongly advised not to do so. Only if the INSPECTr partners are sure that during the proof of concept or in future run-time, their network will never show any overlap with networks in which e-CODEX partners operate, an INSPECTr specific set of pModes can be created.

Between e-CODEX and related initiatives, overlap has already occurred and has led to addressing and routing problems. Certain parameters need to be uniquely set in order for a gateway to determine which partner information is to be delivered.

To provide a very simple example a so called 'PartyID' is allocated for all partners in e-CODEX collaborations. This partyID is to be unique across all participants. , There are French entities involved in the EU collaborations

14 https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Domibus

15 https://www.e-codex.eu/contact

© INSPECTr 2019

on Financial Penalties, iSupport (global child maintenance obligations), and e-EDES (European Investigation Order) . In all of these a specific French authority has been given the PartyID 'FR'. The e-CODEX project team allocated 'FR' to the ANTAI organisation (French fine collecting agency). In e-EDES, the European Commission allocated 'FR' to the Public Prosecution Office, and in iSupport[16] the HCCH allocated 'FR' to central authority for maintenance obligations. Based on PartyID a sending gateway is now unable to determine which receiving FR gateway to address. Even though more routing parameters come into play, it is obvious that some initiative overarching coordination on the allocation of parameters is advisable. It is not unlikely that the other distinctive parameters would also overlap between initiatives.

For this reason, the INSPECTr community is urged to obtain their pMode files from the e-CODEX consortium. Consortium members can assist the INSPECTr participants in articulating their configuration requirements and in preventing such parameter overlap with other projects. For the consortium staff pMode creation is fast and simple as they have a specific pMode creation toolkit available. Besides being fast and flexible, the toolkit also ensures reproducibility and sustainability over time.

4.2.5 Securing and signing the information exchange

In order to establish a secure connection between gateways encryption and authentication is done through mutual SSL. The use of certificates is subject to a number of requirements. Self-signed certificates or certificates that are not obtained from a Certificate Authority are not admissible. Also the strength of the certificate needs to be of an up-to-date standard.

E-CODEX provides a document on security recommendations, these are intended only as recommendations and not as a definitive guide. Like other components of the e-CODEX framework the Gateway and Connector components are implemented within the domain borders of the individual participants. Consequently they will be subject to security policies applicable within that domain. Very likely the e-CODEX components will not live in isolation in a domain's data centre. A less strict security EU level policy on e-CODEX components may jeopardize the non-eCODEX components in that facility. A stricter EU policy may lead to a non-conformance with domain policy. Between the various domain specific policies and the e-CODEX security policy recommendation a common denominator needs to be found.

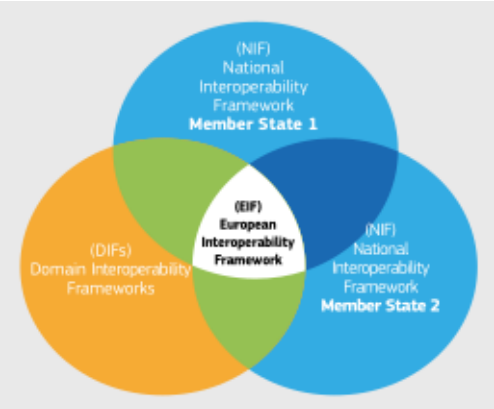

Figure 6: Interoperability frameworks common ground

16 Hcch.net/en/instruments/conventions/publications1/?dtid=80&cid=131

As depicted in the image above, in this case to be interpreted as a depiction of varying security policies.

Lastly if the result of this does not satisfy a participant's requirements, that participant cannot be forced into opening up its domain to business partners weakening its security strength.

4.3 Integrating the 'back-end systems'

One of the main objectives of the e-CODEX project has been and still is to build on existing national implementations and to deploy these implementations in a European wide interoperability framework servicing legal procedures. Back end systems are connected to the Domibus Connector, provided by the e-CODEX consortium. The Connector integrates with a Gateway which performs the actual exchange of information between domains.

4.3.1 The de facto back end system e-EDES

Extending on the business collaboration design and the provided XML structure for EIO, DG JUST of the European Commission has invested considerably in building a business application for Member States which do not have a native case management system capable of supporting the EIO or MLA procedure. The result of the Commission's initiative goes by the name of e-EDES (e-Evidence Digital Exchange System).

This system was specifically developed to enable its users to digitally execute and legally adhere to the EIO and MLA procedures. It natively integrates with the e-CODEX infrastructure components gateway and connector. In the 'evidence2e-CODEX[17]' project the deployment of e-EDES in conjunction with e-CODEX components was successfully demonstrated. The e-EDES system comes with a default connection to the Domibus connector.

Within the team of DG JUST that has developed the e-EDES system extensive knowledge and support is available to e-EDES users.

4.3.2 Native back end systems

Any native back end system can be integrated with the Domibus Connector. This may be a case management system of a court or public prosecution office, but just as well any other system that is in use in the respective domains.

There are various ways in which back-end systems can be integrated. e.g. JMS queueing or a web-service. An introduction to JMS usage is provided on the Oracle website[18]. As the characteristics of the partner specific back-end systems may vary greatly, this document cannot provide an exhaustive description on how to integrate. Again, the staff of the e-CODEX consortium can be of assistance to INSPECTr participants.

4.3.3 Next step

In order to provide a detailed description how to interlink LEA nodes through the e-CODEX infrastructure components, detailed analysis of the LEA node specifications versus the e-CODEX Domibus connector back end integration specifications is to be performed. However, as indicated in this document, the e-CODEX components are both content agnostic and largely technology agnostic (an implementation is available for any operating system and for many middleware solutions) it is not a matter of IF e-CODEX components can be deployed in INSPECTr context. The detailed analysis of LEA node and DOMIBUS connector should merely show

17 https://evidence2e-codex.eu/

18 https://www.oracle.com/technical-resources/articles/java/intro-java-message-service.html

HOW LEA nodes can be interlinked. For piloting purposes re-using and adapting existing implementations will demonstrate the usability of the concept. Such is described in chapter 5.

5 Implementing INSPECTr Living Labs

The INSPECTr Living Labs will be implemented in a two-phase approach. Initially, both the INSPECTr nodes and e-CODEX components will be run on-site at University College Dublin. In a second phase these components will be deployed on premise of the respective Living Lab participants inside their Member States. Both phases are intended to demonstrate the functionality and the practical usability of the INSPECTr framework, including e-CODEX. At this point an implementation in an operational environment dealing with real criminal data is not yet foreseen. In fact, during the real data experiments that are scheduled for later in the project, an ethical and legal requirement of participating in this activity is for e-codex and the publish/subscribe (data discovery) features will be removed from the platform.

For this reason this chapter will elaborate on implementations in the UCD environment and the implementation in the piloting partners' "mocked data" test environments only. Some of the detailed described in earlier chapters will be out of scope for in the context of the current Living Lab phases.

- In the first phase in which all components are installed at UCD, the aspect of choosing a network as described in section 4.2.1 is not relevant.
- Section 4.2.2 described the choice of a national topology in which an array of domestic participants generically use the e-CODEX components in a variety of legal procedures. In both phases of INSPECTr implementation this aspect does not apply either.

For the first phase of the INSPECTr Living Lab a more compact implementation will still demonstrate the working of the framework without fully adhering to certain specific requirements related to e-CODEX. One will need all the items mentioned in this document, but less strict requirements can be applied to items as certificate origin, reused XML schemas and process models from other projects rather than tailor made for INSPECTr. Taking existing assets from existing implementations outside INSPECTr and tweaking them to specific INSPECTr needs will suffice and speed up the completion of the task.

Section 5.1 describes what items are to be implemented in which way for INSPECTr deployment at UCD. Section 5.2 focuses on the deployment in the second phase and elaborates only on the deviating aspects in comparison with UCD deployment.

5.1 e-CODEX support to INSPECTr on-site at UCD

5.1.1 Setting up the Gateway and Connector

Downloading, installing and configuring both the Gateway and the Connector is exhaustively described in documentation provided by the Commission and the e-CODEX consortium respectively (see paragraph 4.2.3). The system administrator of the Living Lab environment at UCD should be able to have these components installed by following the instruction provided. For each piloting partner envisaged, one set of Gateway and Connector needs to be made available and integrated with an INSPECTr Living Lab instance for that specific partner.

Feedback from e-CODEX users in other projects shows that the installation is not considered to be the most cumbersome of activities. Familiarizing with all applicable features these components host in order to swiftly perform configuration tasks is mentioned as a time consuming step in the process. In order to facilitate the familiarisation process, e-CODEX has developed the e-CODEX LabBox.

© INSPECTr 2019

This LabBox features a completely configured Gateway and Connector setup of up to nine instances of Gateway/Connector pairs. It comes with pre-defined pMode, certificates and message structures. In this 'sandbox setup' the administrators can build experience in connecting to new partners, configuring message flows, et cetera. The LabBox does not allow to integrate with back end systems, so it cannot be used for the actual INSPECTr framework implementation. For that purpose individual Gateway/Connector software needs to be installed for each participant. By training on the LabBox, the configuration and interconnection between instances should be less time consuming.

5.1.2 Obtaining pMode files for the INSPECTr use-cases

The pMode files act as the key to your digital front door, expressing in which use-case a partner collaborates with which other partner(s), based on which certificates communication between Gateways is accepted and how long and how often the sending Gateway should execute retries in case of unavailability of the receiving Gateway. These and other settings are loaded on the Gateway by inserting the pMode files which holds these parameters.

The most convenient way of obtaining pMode files is to have them constructed by the German colleagues in the e-CODEX consortium. In order for them to create the pMode the INSPECTr project needs to provide the required routing information. An example of the required routing information and how the features works is described in document 'use-case stories e-CODEX addressing' attached to this document. For INSPECTr, the parameters are yet to be defined. Some are obvious, others may need some elaboration within the project. For each of the actors in the 'service:INSPECTr', a PartyID, PartyIDType and addressing parameters (e.g. IP addresses) should be defined. Business execution parameters should be derived from back-end integration activities described in 5.1.4.

Based on a complete set of service parameters, the e-CODEX consortium can create a set of pModes that can be loaded on each Gateway/Connector instance in the UCD environment.

Alternatively, an existing pMode can be taken and amended manually for INSPECTr needs. In the context of INSPECTr the pMode in use between Germany and The Netherlands for the 'Mutual Legal Assistance' use-case would be a logical choice. See 5.1.4 for more information on the topic.

Lastly the INSPECTr team may decide to create a pMode file from scratch as the pMode specifications are based on open international standards. However this approach is not advised for deployment in an environment outside the UCD implementation.

5.1.3 Securing and signing the connections and message payload

Though the threats inside the secure data centre of UCD are very limited compared to a situation in which information shared across networks, also in this environment certificates have to be deployed. Without these the components simply will not run properly. Also, it is good practice to simulate tasks before migrating to an environment in which the requirements do apply and benefit from the lessons learned in earlier implementations.

Certificates can be deployed for channel and message encryption and for message signing. Typically in cross-domain implementations, the certificates used may not be self-signed. They must originate from a Certificate Authority for which the root certificate can be traced back. As for the UCD implementation no external communication is required, the risk of unauthorised access to the system by faulty certificate use is non-

© INSPECTr 2019

existing. Self-signed certificates can be deployed without risk.

5.1.4 Integrating the INSPECTr nodes with the e-CODEX exchange platform

For the purpose of integrating the Domibus Connector with any backend system, the interface is described in an API. The attached document 'DomibusConnectorAPI' provides the details of this API. By using this API, automatic integration between the INSPECTr node and e-CODEX components is established. Without any manual operation, (encrypted) node output is picked up by the e-CODEX connector which packages it as an attachment to an XML structured message containing only routing information and case metadata.

Next, the requesting authorities' Gateway will setup a secure connection with the Gateway of the executing authority abroad. Upon successful delivery an acknowledgment is sent back to the sender, making the transaction non-repudiable. Should for some reason, the receiving Gateway not be available, the sending Gateway will make a number of retries, based on pMode settings until delivery is successful or when the retry settings expire, resulting in a non-delivery notification, making the transaction result reliable.

Upon reception, delivery security and quality checks are performed and the received message container is handed over to the Connector of the executing authority. Here, a number of validation checks are performed and additional transaction evidences are returned to the sender. Message payload will be conveyed to the INSPECTr node of the executing authority. Not until the information is loaded onto the INSPECTr node, the case information is exposed to a user. The use of the DomibusConnectorAPI or other integration option (paragraph 4.2.3) is a likely scenario for the publication/subscribe transactions or when the e-EDES application will not be used.

When manual operation of a (third party) authority such as a public prosecutor or an investigative judge is required, using the e-EDES Reference Implementation by the Commission (DG JUST) would be a very logical choice. Output from an INSPECTr node is stored on some file system. Contrary to the described scenario above, case information is not directly exchanged between INSPECTr node and a Connector. Instead the operator of the Public Prosecution Office or court fills out the legal assistance request in the e-EDES application. By drag-and-drop the output CASE file is added as an attachment to the Legal Assistance form and XML. Message structure and pMode examples is arranged for when using the e-EDES system. The (existing) interface between e-EDES system and Connector will handle the delivery to the connector, from which point on the scenario described above applies. This option embodies the description provided in paragraph 3.1 and addresses INSPECTr result 13 (*R13 – Integration of the e-CODEX Common Evidence Exchange Model and guide for interlinking the INSPECTr platform with the e-CODEX infrastructure*).

According to the use-case descriptions 'fraud', 'terror' and 'CSAM' acting roles for PPO or judges is foreseen in some, but not all cross-domain exchanges in the INSPECTr context. For fully automated backend-to-backend exchanges the DomibusConnector API or other integration solutions such as described in paragraph 4.3.2 may be applied. In that case the business collaboration design of the MLA use-case (see attachment: UC009 analysis Criminal Legal Assistance) provides guidance on how the INSPECTr use-cases can be supported.

The business collaboration (page 11 of the attached document) is subdivided into a number of Business Transactions. For INSPECTr support only the business transactions 'Ask for Assistance' (sending the request) and 'Wrap up' (providing the requested information) would be applicable for Living Lab purposes. On respectively pages 17 and 24, the business transactions are linked to business documents (the actual messages). Linked to each of these message, existing XML structures are available. Like is the case for the e-EDES application, CASE format structures can be attached to the XML legal request message as payload and be

conveyed to piloting partners INSPECTr node through the e-CODEX infrastructure.

The current use-case descriptions of 'Fraud', 'CSAM' and 'Terror' provide a detailed analysis of what type of evidence is obtained from who. The exact context, sequence and details of interaction with foreign authorities may be translated into a collaboration design analysis as provided for in the attached document on criminal legal assistance if the INSPECTr use-cases should migrate to a productive situation in the future. For the objectives of this project where it should be demonstrated that the concept works, the re-use and tweaked components from other implementations will be fit for purpose.

5.2 e-CODEX support to INSPECTr piloting partners

This paragraph only focuses on the differences between implementation in the UCD environment and the respective environment of the Member State actors.

5.2.1 Setting up the Gateway and Connector

Before setting up a Gateway/Connector pair at the location of a piloting partner, the partner is advised to set up a LabBox implementation as described in paragraph 5.1.1 first. The authorities administrators will rapidly experience the do's and don'ts of the e-CODEX configuration and benefit from that when setting up the actual Gateway and Connector components. In preparation of the start of the second piloting phase, individual piloting partners can already immediately install a LabBox in their environment.

Contrary to the setup in the UCD environment a piloting partner would only have to set up one pair of Gateway and Connector. A partner needs at least one other piloting partner who has setup a Gateway/Connector pair in his own environment. As these implementations now live in separate domains, complexity of cross-domain access through the organisation's firewalls is added. Experience from other projects and use-cases indicate that cross-domain access between formally controlled environments is time consuming. An early start with making preparations is recommendable. Also the LabBox cannot provide any guidance or training on the matter as this is very much Member State specific.

5.2.2 Obtaining pMode files for the INSPECTr use-cases

Additional information is to be provided for this stage of the piloting. Partner URL need to be added and certificate reference required.

5.2.3 Securing and signing the connections and message payload

In this phase information will be exchanged over external infrastructures. Most likely it will be over the internet. For obvious reasons these connections will have to be properly secured. For this implementation, the requirement of deployed non-self-signed certificates originating from a listed Certificate Authority will apply.

If the e-CODEX consortium is to provide the pMode files for INSPECTr, the public key needs to be uploaded to the pMode Toolkit hosted by the German team of the e-CODEX consortium. Reference to that key will be incorporated in the pMode file during creation.

5.2.4 Integrating the INSPECTr nodes with the e-CODEX exchange platform

At this point it is not possible to describe the applicable situation for each individual piloting partner. For testing purposes the respective partners may decide to copy the chosen approach in paragraph 5.1.4 in their individual environment. By default the approach described in 5.1.4 applies to Member State implementations.

© INSPECTr 2019

However if a piloting partner want to use a native backend application, such is possible.

As the Member States of the INSPECTr piloting authorities participate in other e-CODEX related implementations, some domestic synergy between INSPECTr efforts and that of other implementations may be possible. For Proof of Concept purposes INSPECTr participants may choose to limit the scope to a dedicated INSPECTr implementation only.

5.3 Evaluation of e-CODEX-INSPECTr test outcomes

As the core functionality of e-CODEX and related security and reliable requirements have been exhaustively tested and approved in earlier European projects, the main focus of the evaluation should not be on these aspects.

The applicability of e-CODEX functionality in the context of INSPECTr deployment should be examined with a focus on 'ease of INSPECTr node integration', speed of message handling over e-CODEX components, file size capacity and configurability for the various types of information transaction for the respective use-case that are to be supported.

© INSPECTr 2019

6 Attachments

- Use-case stories e-CODEX addressing
- DomibusConnectorAPI
- UC009 analysis Criminal Legal Assistance