Justice Action Grant

Me-CODEX II

Call identifier: CEF-TC-2018-CSP-ECODEX
Topic: e-CODEX Core Service Platform (CSP)
Project full title: Continued management, development and maintenance of the e-CODEX Core Service Platform (CSP) – Me-CODEX II
Grant agreement n°: JUST/CEF-TC-2018-CSP-ECODEX-01

eIDAS for e-CODEX – Impact Analysis

Deliverable Id:	-
Deliverable Name:	-
Status:	Final
Dissemination Level:	Public
Due date of deliverable:	-
Actual submission date:	29/11/2021
Work Package:	3
Organisation name of lead partner for this deliverable:	AT BMJ
Author(s):	Mathias Maurer
Partner(s) contributing:	Jean-Marc Pellet (HCCH), Martin Hackl (AT BMJ), Bernhard Rieder (AT BRZ)

Abstract:
eIDAS has established new standards for electronic communication. e-CODEX is a communication network that is highly affected by those standards. This document shall therefore analyse the relevant eIDAS provisions, lay out the affected e-CODEX functionality and draw conclusions how eIDAS affects e-CODEX.

History

Version	Date	Changes made	Modified by
0.1	21/10/2021	Initial Version	Mathias Maurer
0.9	17/11/2021	Internal Review	Bernhard Rieder, Mathias Maurer
0.92	23/11/2021	Review AT BMJ: order of chapter 4 Review HCCH	Mathias Maurer, Martin Hackl Jean-Marc Pellet
1.0	29/11/2021	Executive Summary Final Version	Mathias Maurer

Table of contents

Executive Summary

Since the eIDAS regulation came into force it has provided a set of standards or standardized tools for electronic services to facilitate the cross-border exchange of data, especially with added trust in the authenticity of data. e-CODEX is highly related to such provisions as it also applies standards for the same purpose. This document therefore describes (i) the most e-CODEX-relevant tools, which eIDAS provides and (ii) the architecture of the e-CODEX system for a better understanding where eIDAS and e-CODEX correlate.

In the main chapter 4 “Conclusions” this document analyses the impacts of eIDAS on e-CODEX. Main conclusions are:

- eIDAS treats different ways to apply signatures and seals equally. There is no legal difference depending on the way a digital signature or seal is applied.
- eIDAS provides an optional set of standards or tools, which can be used by applying systems. There is no obligation to use the eIDAS tools.
- e-CODEX provides all technical means to use eIDAS tools. It does not, however, impose an obligation to do so. The business owner of a use case can decide to increase the level of authenticity by applying higher eIDAS standards. e-CODEX is capable of supporting higher eIDAS standards, as well.
- e-CODEX is – from a technical perspective – a transportation mechanism. It therefore adds authentication on the message level. Additional authentication can be applied to single documents of a message and will be supported by e-CODEX. But this decision is to be taken by the business owner and must be supported by each individual e-CODEX participant and their backend systems.
- An increased authentication level is therefore possible with e-CODEX. Since e-CODEX is capable of supporting different authentication levels, it is up to the business owner to decide if an increased level of authenticity should be applied.

Finally, the document elaborates, where e-CODEX can be equipped with additional functionality to add support for further eIDAS tools or to increase the usability of eIDAS tools in e-CODEX.

1 Introduction

1.1 eIDAS[1]

eIDAS (**e**lectronic **ID**entification, **A**uthentication and trust **S**ervices) is an EU regulation on electronic identification and trust services for electronic transactions in the European Single Market. It was established in EU Regulation 910/2014 of 23 July 2014 on electronic identification and repeals 1999/93/EC from 13 December 1999.[2]

eIDAS oversees electronic identification and trust services for electronic transactions in the European Union's internal market. It regulates electronic signatures, electronic transactions, involved bodies, and their embedding processes to provide a safe way for users to conduct business online like electronic funds transfer or transactions with public services. Both the sender and the recipient can have more convenience and security. Instead of relying on traditional methods, such as mail or facsimile, or appearing in person to submit paper-based documents, they may now perform transactions across borders.

eIDAS has created standards for which electronic signatures, qualified digital certificates, electronic seals, timestamps, electronic registered delivery services, and other proof for authentication mechanisms enabling electronic transactions, with the same legal standing as transactions that are performed on paper.

The provisions on trust services applied from 1 July 2016, as a means to facilitate secure and seamless electronic transactions within the European Union. For the use of public services, Member states are required to recognise electronic signatures that meet the standards of eIDAS (this requirement applies from the advanced level).

If not otherwise stated, all references to Articles in this document are referring to the eIDAS regulation.

1.2 e-CODEX

e-CODEX provides easy access to cross-border justice for citizens, business and legal professionals all over Europe.[3] On a technical level e-CODEX provides a transport mechanism for transmitting especially judicial data and messages cross-border in Europe in a secure and reliable manner. e-CODEX further provides an interoperability framework guaranteeing that an e-CODEX message

[1] https://en.wikipedia.org/wiki/EIDAS
[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG
[3] https://www.e-codex.eu/

complies with e-CODEX standards and thus can be understood and processed automatically in the recipient's sphere.

In order to provide its service in a secure and reliable manner, e-CODEX heavily relies on up-to-date security provisions and standards.[4]

1.3 Correlation of eIDAS and e-CODEX

As pointed out above, eIDAS is a provider of security standards and e-CODEX is a user of security standards. It is therefore the question whether and how e-CODEX can benefit from the standards established by eIDAS.

The e-CODEX Consortium has often been asked whether e-CODEX is compliant with eIDAS. In the subsequent chapters it will be shown that this is not the correct question to ask. The question to be answered in this document is: can e-CODEX be used with the standards which eIDAS establishes? Additionally, it will be analysed, what e-CODEX can do to support additional levels of security or authentication.

Finally, it is necessary to point out that according to Art 2/2, "this Regulation does not apply to the provision of trust services that are used exclusively within closed systems resulting from national law or from agreements between a defined set of participants."

At first glance it might seem, that thus the eIDAS regulation does not apply to e-CODEX, as it is mostly used by a restricted circle of participants. However, e-CODEX was designed to be used by everybody interested in cross-border judicial proceedings. As such, e-CODEX can be used and is open nowadays e.g. for all Austrian lawyers (approx. 5000 persons) for the use case of the European Payment Order. Further, once the e-Justice Portal of the European Commission[5] connects its online forms[6] for the European Payment Order and the forms for Small Claims to the e-CODEX system (currently planned for late 2021), then e-CODEX can and will be used by potentially all European citizens. Therefore, e-CODEX cannot be regarded as a closed system (anymore) and is thus subject to the eIDAS regulation.

[4] See https://www.e-codex.eu/tech, section "Security"

[5] https://e-justice.europa.eu/

[6] https://e-justice.europa.eu/155/EN/online_forms

2 eIDAS Toolbox

As described in the introduction above, eIDAS provides a vast set of standards for different levels of security. It describes the requirements to meet these standards, but it does not oblige communication participants to implement those standards. (It does, however, establish the principle of mutual recognition of electronic identification under certain circumstances [Art 6, 27]). eIDAS can therefore be seen as a toolbox where communication participants can choose the most appropriate tools from to secure and authenticate their communication.

This chapter intends to highlight the most e-CODEX-relevant tools of this eIDAS toolbox.

2.1 Certificates

Certificates are the main basis for authentication means such as signatures and seals. A certificate is an "electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person" (Art 3/14). There are different quality levels of certificates. A **regular** certificate is defined in Article 3 Paragraph 14. Article 3 Paragraph 15 defines a "**qualified** certificate for electronic signature" as a "certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in Annex I".

- The first requirement – issued by a qualified trust service provider – refers to the definitions of a "trust service" (Art 3/16), "qualified trust service" (Art 3/17), "trust service provider" (Art 3/19), "qualified trust service provider" (Art 3/20) and others. This impact analysis follows these definitions without going further into the details.
- The second requirement – "requirements laid down in Annex I" – refers to the requirements for qualified certificates for electronic signatures. These requirements basically demand a higher level of certainty for issued electronic certificates and sets out a specific set of data which the qualified certificate needs to contain.

2.2 Electronic Signatures

Electronic signatures are one of the main tools that the eIDAS regulation sets up standards for. The main intention for electronic signatures is to provide a tool for authenticating electronically and thus participate in communication activities where the communication participants are authenticated. For electronic signatures there are again different levels of quality:

1. [**regular**] "electronic signature" means data in electronic form which is attached to or logically associated with other data in electronic form, and which is used by the signatory to sign (Art 3/10)
2. "**advanced** electronic signature" means an electronic signature which meets the requirements set out in Article 26 (Art 3/11)

3. "**qualified** electronic signature" means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures (Art 3/12)

The definition for a "qualified electronic signature" requires a "qualified electronic signature creation device". This latter term again refers to requirements laid down in Annex II and shall ensure that a reasonable amount of confidentiality, uniqueness, protection against forgery and against use by others is applied to electronic signatures.

Finally, it must be pointed out that electronic signatures are usually used by natural persons to authenticate themselves and to guarantee the origin and integrity of communication activities.

2.3 Electronic Seals

Electronic seals serve a very similar intention as electronic signatures. Thus, they are also available in different levels of quality:

1. [**regular**] "electronic seal means data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity" (Art 3/25)
2. "**advanced** electronic seal" means an electronic seal, which meets the requirements set out in Article 36" (Art 3/26)
3. "**qualified** electronic seal" means an advanced electronic seal, which is created by a qualified electronic seal creation device, and that is based on a qualified certificate for electronic seal" (Art 3/27)

The requirements for the "qualified electronic seal" follow the same principles as for "qualified electronic signatures". The main difference to electronic signatures is, that electronic seals are usually used by legal persons to guarantee the origin and integrity of their communication activities. An electronic signature is necessary if the individual author of a communication activity needs to be known. If it is sufficient to know the issuing organisation/legal person, then an electronic seal would suffice.

2.4 Electronic Timestamps

"Electronic time stamp means data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time" (Art 3/33).

Time data is important for technical reasons, e.g. in log files to retrace user actions or systems events that happened before the occurrence of an incident. Time stamps are also used for synchronising events across several systems. But time data is also of importance for legal reasons: when has a message been sent or received? When was the reception confirmed? Legal consequences rely on proper declaration of time data.

Besides the above-mentioned **regular** time stamps, the eIDAS regulation also defines the requirements for **qualified** electronic time stamps, which is "an electronic time stamp which meets the requirements laid down in Article 42" (Art 3/34). The requirements of Art 42 demand a certain level of binding date and time to data, an accurate time source and signed or sealed by a qualified trust service provider. The higher legal quality of qualified electronic time stamps is then laid out in Art 41.

2.5 Electronic registered delivery services

Article 3(36) defines electronic registered delivery services as services that make it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protect transmitted data against the risk of loss, theft, damage or any unauthorised alterations.
Article 43 gives the following legal effects to electronic registered delivery services:
"1. Data sent and received using an electronic registered delivery service shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic registered delivery service.
2. Data sent and received using a qualified electronic registered delivery service shall enjoy the presumption of the integrity of the data, the sending of that data by the identified sender, its receipt by the identified addressee and the accuracy of the date and time of sending and receipt indicated by the qualified electronic registered delivery service."
Qualified electronic registered delivery services are defined in Article 44.

2.6 List of trusted service providers

The list of trusted service providers contains information about available providers of trusted services per Member State and which trusted services they provide (Art 22/1).[7] "Trusted lists are essential elements in the building of trust among market operators as they indicate the qualified status of the service provider at the time of supervision." (Recital 46). Recipients of trusted services by listed service providers can rely on the authenticity of the service and thus do not need to establish their own process of verifying the authenticity of the service. This brings a relevant simplification and thus more efficiency to daily operations with trusted services.

[7] See the combined list here: https://esignature.ec.europa.eu/efda/tl-browser

3 e-CODEX Architecture

In order to understand e-CODEX' mode of operation and usage of security provisions better, this chapter will highlight some of the basic technical principles, e-CODEX is based on. A complete description of the e-CODEX architecture would go beyond the scope of this document. Therefore, after a basic introduction, a few selected aspects with relevance for eIDAS topics will be presented.

3.1 Overview[8]

The e-CODEX architecture implements the so-called 4-corner-model. Corners 1 and 4 are the original sender and final recipient of an e-CODEX message. They do not communicate directly with each other but use Gateways to intermediate the communication. Each participant uses a separate Gateway – corners 2 and 3. Corners 2 and 3 would typically be situated in the sphere of each participant. There is no central node in place which is used for the intermediation of communication.

In e-CODEX there is an additional component between corner 1 (the backend system of the sender) and corner 2 (the Gateway of the sender) and also between corner 3 (Gateway of recipient) and corner 4 (backend system of the recipient): the DOMIBUS Connector. This DOMIBUS Connector adds additional functionality to the communication.

The following figures show a very general overview of the describe e-CODEX architecture (Figure 1) and a more detailed picture of the e-CODEX components (Figure 2) and how they work together.

[8] https://www.e-codex.eu/technical-overview

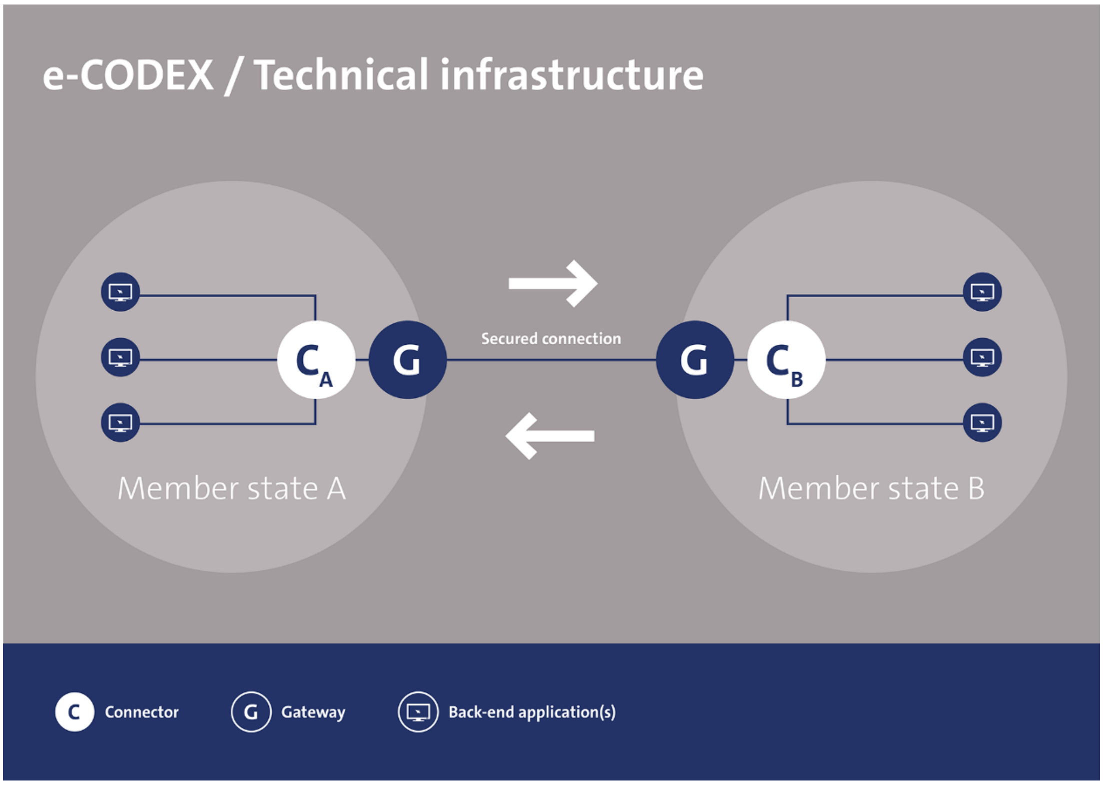


Figure 1: e-CODEX technical overview

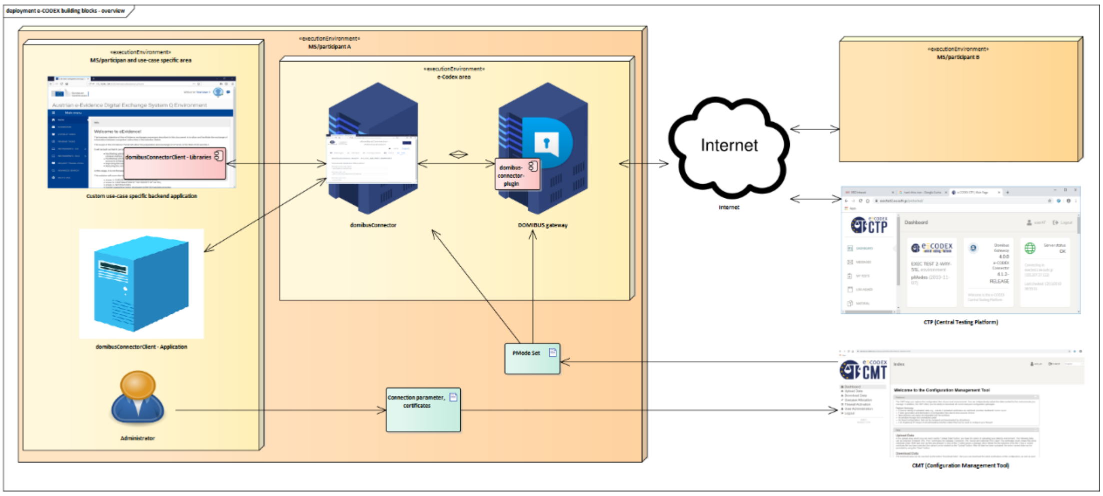

deployment e-CODEX building blocks - overview
«executionEnvironment»
MS/participant A
«executionEnvironment»
MS/participan and use-case specific area
domibusConnectorClient - Libraries
Custom use-case specific backend application
domibusConnectorClient - Application
Administrator
«executionEnvironment»
e-Codex area
domibusConnector
domibus-connector-plugin
DOMIBUS gateway
PMode Set
Connection parameter, certificates
Internet
«executionEnvironment»
MS/participant B
CTP
Dashboard
EXEC TEST 2-WAY-SSL environment
Domibus Gateway 4.0.0
e-CODEX Connector 4.1.2-RELEASE
Server status OK
CTP (Central Testing Platform)
CMT
Index
Welcome to the Configuration Management Tool
CMT (Configuration Management Tool)

Figure 2: e-CODEX detailed architecture

The Gateway ensures the connection and message exchange with the Gateway in another Member State. It uses the AS4 messaging standard by OASIS and the OASIS ebms 3.0 standard for the data exchange over the Internet. Each participant has to set up his own Gateway to participate in the communication. The recommended Gateway product is developed and maintained by the Connecting Europe Facility (CEF). e-CODEX uses SSL (TLS and mTLS) to communicate between the national Gateways. The communication between Gateway and Connector is performed through a web service interface using the ws-security standard by OASIS.

The "pModes" are part of the configuration files created for every participating country or organization necessary to establish the Gateway connections. Those files are centrally created based on the configuration data received by the participants. The pModes contain data such as the public web address of the Gateway, the use-cases that are supported by the system and sender/recipient data. Additionally, the configuration includes public certificates of all participants.

The Connector resides between the national backend Systems and the national Gateway. It is a web application that communicates with the Gateway, carries out the message routing to the (potentially multiple) backend systems and creates the secure ASiC-S containers for the messages. The optional Connector Client Library can be integrated in the national backend system. It carries out the adaptations to map the national XML content. Mapping is a transformation process at the level of a Member State where data elements from e-CODEX are aligned to data elements from the Member State. The (standalone) Connector-Client targets users that do not want to connect their national infrastructure with e-CODEX or that do not have the respective backend services. The Connector is developed and currently maintained by the Me-CODEX II Consortium. The connection of the Connector to the national Backend System must be provided by the MS.

The Member States remain responsible for the authentication of their respective users that use the system. The so-called "Circle of Trust" is a multilateral agreement between the participating countries which is understood as the "mutual recognition between MS of an electronic document within the existing legal framework." The so-called "Trust-Ok-Token" is generated as a separate document by the Connector of the sending MS and sent together with the document. It confirms that the document was created in adherence with the rules of the sender MS and it confirms its integrity.

The connected Backend System must support the specific e-CODEX use case. It should be able to send and receive the business documents in both XML and PDF format plus optional attachments.

e-CODEX has developed and maintains a Central Testing Platform (CTP) for e-CODEX partners to test their national infrastructure against the Central Testing Platform.

e-CODEX has also developed and maintains the Configuration Management Tool (CMT) to manage the configuration data (pModes) of each participant.

3.2 e-CODEX Connector[9]

As pointed out above the e-CODEX Connector adds crucial functionality to the e-CODEX infrastructure. The most relevant features for the purpose of this document are:

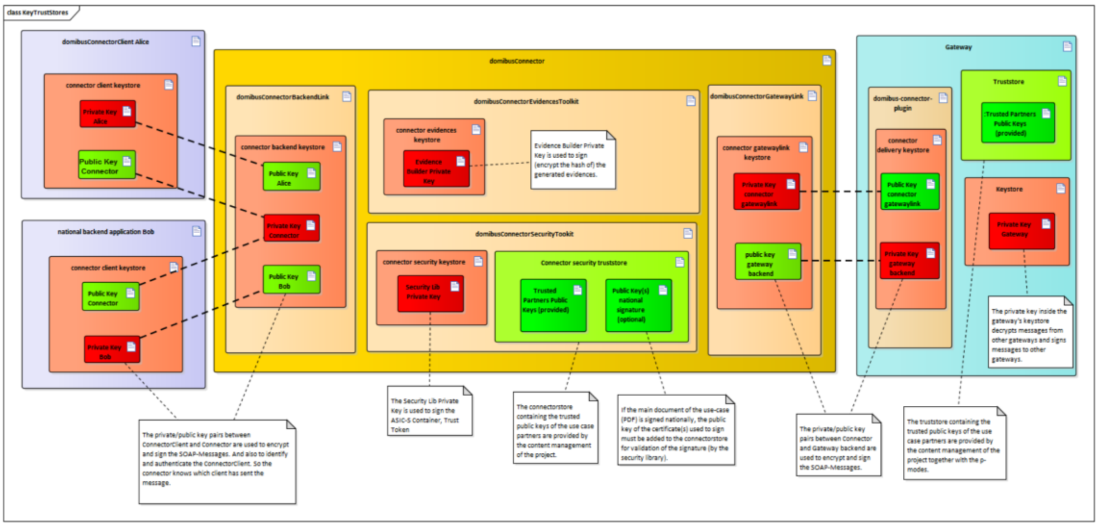
- **Creation of ETSI-REM evidences**; see description below in the chapter “Use of Time Stamps”
- **Creation of a TrustOK Token**: the sending domibusConnector validates the signature of the business document of a message. The outcome of this validation is written in a so called TrustOK Token. This token is generated by a sub-module of the domibusConnector: the security library generates an XML file and a PDF file with the output of the validation.
  The TrustOK Token also includes information about the way a message was originally authenticated.
  - In case of an **authentication-based** advanced electronic system the TrustOK Token confirms that the sending authentication-bases advanced electronic system has authenticated the sender successfully.
  - In case of a **signature-based** advanced electronic system the TrustOK Token confirms that individual sent document has been signed with a qualified or an advanced electronic signature.
- **Creation of an ASiC-S container**: Once the validation of the business document and the generation of the TrustOK Token is done (either successfully or unsuccessfully, as it is the responsibility of the receiver to check the TrustOKToken and whether to trust the document or not) and transmitted, the domibusConnector builds a container that holds the documents that are included in a message. Those documents are:
  - The business document itself
  - Every business attachment
  - The TrustOK Token PDF file

  The container then is signed by the domibusConnector. Within the message, the documents that are included in the ASiC-S container are replaced by the container.
  On the receiving side, the domibusConnector validates the signature of the ASiC-S container, unpacks it (if signature validation is successful) and replaces it within the message with the contents of the container.
  This way it is ensured that business documents cannot be manipulated on their way from the sending connector to the receiving connector.

3.3 Use of Certificates

Certificates are used at various levels. The figure below shows which components require which kind of private and public keys. The red boxes represent the usage of private keys and green boxes represent public keys.

[9] https://www.e-codex.eu/node/47


class KeyTrustStores
domibusConnectorClient Alice
connector client keystore
Private Key Alice
Public Key Connector
national backend application Bob
connector client keystore
Public Key Connector
Private Key Bob
domibusConnector
domibusConnectorBackendLink
connector backend keystore
Public Key Alice
Private Key Connector
Public Key Bob
domibusConnectorEvidencesToolkit
connector evidences keystore
Evidence Builder Private Key
domibusConnectorSecurityTookit
connector security keystore
Security Lib Private Key
Connector security truststore
Trusted Partners Public Keys (provided)
Public Key(s) national signature (optional)
domibusConnectorGatewayLink
connector gatewaylink keystore
Private Key connector gatewaylink
public key gateway backend
Gateway
domibus-connector-plugin
connector delivery keystore
Public Key connector gatewaylink
Private Key gateway backend
Truststore
:Trusted Partners Public Keys (provided)
Keystore
Private Key Gateway

Evidence Builder Private Key is used to sign (encrypt the hash of) the generated evidences.

The private/public key pairs between ConnectorClient and Connector are used to encrypt and sign the SOAP-Messages. And also to identify and authenticate the ConnectorClient. So the connector knows which client has sent the message.

The Security Lib Private Key is used to sign the ASIC-S Container, Trust Token

The connectorstore containing the trusted public keys of the use case partners are provided by the content management of the project.

If the main document of the use-case (PDF) is signed nationally, the public key of the certificate(s) used to sign must be added to the connectorstore for validation of the signature (by the security library).

The private/public key pairs between Connector and Gateway backend are used to encrypt and sign the SOAP-Messages.

The truststore containing the trusted public keys of the use case partners are provided by the content management of the project together with the p-modes.

The private key inside the gateway's keystore decrypts messages from other gateways and signs messages to other gateways.

Figure 3: e-CODEX usage of certificates

Although the individual usage of these keys is not relevant for the purpose of this document, their purposes should still be summarised: keypairs of public/private keys are necessary for

- Sending messages from the backend to the Connector
- Sending messages from the Connector to the backend
- Encrypting the (hash code) of ETSI-REM evidences for confirming the transmission status of messages
- Signing the secure “ASiC-S” container for the messages
- Sending messages from the Connector to the Gateway
- Sending messages from the Gateway to the Connector
- Sending messages from the Gateway to other Gateways

All these authentication and encryption functionalities rely on certificates. e-CODEX itself does not impose any requirements which kinds of certificates must be used. At the same time, it can process all kinds of certificates – be it regular qualified certificates.
Although e-CODEX does not impose any requirements it recommends applying a minimum level of security. The e-CODEX security recommendations are available at the e-CODEX Website.

3.4 Use of Time Stamps

e-CODEX makes of course intensive use of time stamps. As described at the beginning, time stamps are used for several technical purposes. From an organisational point of view the most relevant timestamps are used for the ETSI-REM evidences. These are different status messages of Connectors to inform the sender about the processing of its message throughout the transmission chain. They can thus be used to find out and even proof that and when a message has been sent by the original sender, if and when it has reached the sphere of the final recipient and if and when it was delivered to the final recipient.

From a technical point of view, there are currently no special requirements regarding the time stamps. e-CODEX relies on the time stamps provided by the technical infrastructure, where the e-CODEX components are operated on.

4 Conclusions

4.1 Equal treatment of different ways to apply signatures and seals

First, it needs to be pointed out, that although the eIDAS regulation sets up several requirements for signatures and seals, **it does not mandate any difference between individual signatures** (e.g. applied via the usage of a chip-card or mobile phone) **or remote signatures**, which are applied by a service on some kind of server. **It also does not differentiate between the appliance of a signature or seal by software or hardware** (Art 3/22 and Art 3/31). It is therefore not required to apply individual signatures or seals on each document individually. **Signatures and seals could thus also be applied in a batch process by a server for a huge number of documents.**

4.2 eIDAS as an (optional) toolbox

eIDAS defines standards for a variety of tools. However, **it does not oblige to use those tools.** Therefore, the business decision, which of the tools shall be applied to a communication activity and thus which level of authentication is required, is subject to the business requirements and needs to be determined by the business owners, communication partners or other legal provisions such as European regulations.

4.3 e-CODEX is capable of using eIDAS standards

e-CODEX is – for the purpose of this document – a transport mechanism. This transport mechanism already provides adequate security and authentication means for a secure and reliable transmission of data in cross-border legal (judicial and other) proceedings.[10] It applies – for example – certificates and signatures on multiple layers. e-CODEX demands, however, still a minimum (though sufficient) level of authentication and only recommends (see [10]) using a higher level of authentication. The decision, which level of authentication is applied, is to be taken by the business owners or might be requested by specific legal provisions. e-CODEX is in any case capable of supporting higher levels of authentication – e.g., qualified electronic certificates.

In addition, Section 3 has shown that e-CODEX as a transport mechanism is in line with the requirements of Article 3(36) defining electronic registered delivery services as service that make it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations. Even though no special legal effect is attached by Article 43 to this “simple” level, it can be remarked that the level of assurance provided by e-CODEX, as defined by Article 3(36) is already of a fairly high

[10] See also the e-CODEX Security Recommendations: https://www.e-codex.eu/tech, section “Security”.

standard. As emphasised, this level of assurance needs to be taken into account and compared with the requirements of the procedures using e-CODEX, including in particular their risk analysis.

The main conclusion therefore is that e-CODEX can already be used with eIDAS standards. But business owners need to define the appropriate level of security and authentication for their business and e-CODEX participants need to apply those levels to their communication.

4.4 e-CODEX adds authentication on message level

As described in the e-CODEX architecture the main components for applying authentication means are the e-CODEX Connector and the Gateway. As such, these components can add authentication means only to the whole message package, including business documents and attachments.

If authentication is required by the business owner for individual documents, then the creating business applications must provide this authentication. Such a functionality cannot be provided by the e-CODEX components.

4.5 Increasing the authentication level in e-CODEX with eIDAS tools

There are various options available to use eIDAS tools for increasing the authentication level of an e-CODEX communication:

- **Use of advanced electronic seals with a qualified certificate**: the qualified certificate increases the level of authenticity of an advanced seal.

- **Use of advanced electronic signatures with a qualified certificate**: the qualified certificate increases the level of authenticity of an advanced signature. The advanced electronic signature with a qualified certificate might be preferred by business owners over the use of advanced electronic seals with a qualified certificate.

- **Use of qualified electronic seals**: in addition to the “advanced seal with a qualified certificate” such a qualified seal must be “created by a qualified electronic seal creation device” (Art 3/12) and thus increases the authenticity (and complexity according to Annex II of the regulation) level even more.

- **Use of qualified electronic signatures**: in addition to the “advanced signatures with a qualified certificate” such a qualified signature must be “created by a qualified electronic signature creation device” (Art 3/12) and thus increases the authenticity (and complexity according to Annex II of the regulation) level even more. The qualified electronic signature might be preferred by business owners over the use of qualified electronic seals.

For all eIDAS tools, which increase the authentication level, it needs to be taken into consideration, that such tools do not come for free. Usually, such tools increase the technical complexity of systems, but also the organisational and financial costs. E.g., qualified electronic certificates usually require a certain process to be obtained and to verify the authentication of the certificate requester, they require a more elaborate process to apply qualified certificates to documents or messages and finally, they are more expensive.

Therefore, the business owner should take into account the authentication and security level that is already provided by regular e-CODEX means and evaluate if the additional costs for higher levels of security and authentication are worth the additional value for its business communication.

4.6 Future e-CODEX support for further eIDAS tools

Several enhancements to the e-CODEX components can be done to add support for further eIDAS tools or to increase the usability of eIDAS tools in e-CODEX.

- **Use of qualified electronic time stamps**: with the use of such time stamps the electronic communication via e-CODEX would profit from the legal benefits laid out in Art 41/2 (presumption of the accuracy of the date and the time it indicates and the integrity of the data to which the date and time are bound) and Art 41/3 (a qualified electronic time stamp issued in one Member State shall be recognised as a qualified electronic time stamp in all Member States). e-CODEX could support this requirement by making the used time stamp server configurable and thus support the use of qualified electronic time stamps.

  Validation of seals and signature at Connector level: currently, business document signatures are validated at the level of the sending Connector. By accessing the e-CODEX Circle of Trust, the e-CODEX participants have agreed to trust the signature validation of the sending Connector. However, a validation of seals and certificates might increase the trust in the transmitted data and messages, if the validation is also done within the sphere of the receiving participant. Such a feature may be taken into consideration for future developments. It will still need further up-front analysis to avoid increasing complexity (every public certificate of participant used for signatures must be shared. This will lead to a higher number of certificates) or to specify additional requirements for certificates (e.g. certificates used to sign business documents must be from a CA that can be validated public (TLOL, CRLs).

  Validation of signatures of ETSI-REM evidences at reception: currently, the above-explained ETSI-REM messages are created and signed by the sending Connector. The signature is not validated at the receiving Connector as the evidences should not have left the e-CODEX sphere. Still, to increase the trust in the evidences such a feature could be considered.

4.7 e-CODEX Security Recommendations

All advanced authentication proposals of this and the previous chapter must be optional. As laid out before, the decision whether to apply such measures to an e-CODEX communication must remain with the business owner, probably based on the requirements of legal acts. Therefore, the authentication levels might differ from use case to use case. e-CODEX is not in the position to decide on these requirements. Therefore, it is necessary to support all these measure on a non-mandatory basis.

Still, e-CODEX has created security recommendations to set up a voluntary minimum level of security. The e-CODEX security recommendations are available at the e-CODEX Website.

I Lists

I.1. List of Figures

I.2. List of Abbreviations

Acronym	Explanation
ASIC-S	Associated Signature Containers - Simple
CEF	Connecting Europe Facility
CMT	Configuration Management Tool
CTP	Central Testing Platform
ebms (3.0)	Electronic Business using eXtensible Markup Language
eIDAS	**e**lectronic **ID**entification, **A**uthentication and trust **S**ervices EU Regulation 910/2014 of 23 July 2014
Me-CODEX II	Project "Maintenance of e-CODEX II"
MS	Member State (of the European Union)
OASIS	Organization for the Advancement of Structured Information Standards
pModes	Processing Mode – Configuration data for Gateway
SOAP	formerly an acronym for Simple Object Access Protocol; now generic term
SSL	Secure Socket Layer
TLS	Transport Layer Security
ws-security	Web Services Security (extension to SOAP)

Table 1: Abbreviations

II References

Documentation used in this document:

- eIDAS Regulation: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG
- e-CODEX Website: https://www.e-codex.eu/
- e-CODEX Security Recommendations: https://www.e-codex.eu/sites/default/files/2020-11/e-Justice%20Security%20recommendations%20v1.0_0.pdf
- e-CODEX document “Required certificates, key- and truststores in the e-Codex environment”: https://www.e-codex.eu/sites/default/files/2019-08/e-Codex_key_trust_stores_0.pdf