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

e-CODEX' Security and Data Protection by Design and by Default

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:	-

Abstract:
e-CODEX is a communication system which provides strong support for security requirements and data protection requirements. This document intends to show, how both aspects – security and data protection – are incorporated into the DNA of e-CODEX.

History

Version	Date	Changes made	Modified by
1.0	29/11/2021	First Version	Mathias Maurer

Table of contents

History 2

Table of contents 3

1 Introduction 4

2 Security by Design 5

2.1 Network layer 5

2.2 Transport layer 5

2.3 Message layer 6

2.4 Document layer 6

2.5 Access to e-CODEX configuration 6

2.6 e-CODEX Security Recommendations 7

3 Data Protection by Design 9

Conclusion 11

1 Introduction

Security and data protection are nowadays even more relevant than ever before, and their importance is increasingly rising. Multiple IT systems – especially legacy systems – might have applied security and data protection measures on top of their functionality, but their design is not driven by security and data protection. They do not deal with both aspects in a native way. Such an approach usually leads to non-consistent appliance of those measures and thus creates security leaks and/or insufficient data protection.

When creating software components, it is therefore nowadays necessary to apply security measures not only as a feature but as an integral part of the architecture of the software. The design – and not only features – of the software must already implement security aspects. Same goes for data protection aspects.

e-CODEX is a secure system. It additionally respects privacy requirements as stated by the GDPR[1] and other legal acts about data protection. This document intends to provide information about how e-CODEX has incorporated security and data protection in its design.

[1] https://eur-lex.europa.eu/eli/reg/2016/679/oj

2 Security by Design

e-CODEX has always claimed that it is a secure system. How does e-CODEX come to this conclusion?

From a technical point of view, e-CODEX is a transportation mechanism. It transports (usually judicial) messages and documents over a network infrastructure. There are different layers relevant for this transportation:

- A **network layer** provides the basic connection between nodes.
- A **transport layer** provides the transport mechanism between those nodes of the network layer.
- A **message layer** provides the message structure and definition for the messages to be transported via the transport layer.
- A **document layer** adds documents to the messages of the message layer.

On each of these layers security measures are applied. The basic approach for e-CODEX is to rely on well-established and standardised security measures instead of implementing its own proprietary measures. But relying on established and well-used security standards, e-CODEX can also rely on the constant further development of such standards, usually by the open-source community. Updated versions of the security components are constantly being provided and just need to be integrated (and tested) in new versions of e-CODEX releases. **As long as those well-established security standards are considered as secure, e-CODEX can also be considered as secure.**

2.1 Network layer

e-CODEX can be used with different kinds of network layers. It is usually applied on regular internet connections. Security therefore follows the usual **security applications of internet technology** (and is extended by the other layers described below). For most e-CODEX use cases such a network layer is sufficient.

For higher security requirements another network layer could be applied, as well. E.g., **TESTA**[2] could also be used as the network to exchange e-CODEX messages. Other networks can also be taken into consideration.

2.2 Transport layer

The transport layer is usually protected by **TLS** or **mTLS**[3]. This is a well-established standard for protecting the transport layer in internet technologies and applied worldwide on a vast number of services. TLS/mTLS provides for the encryption and authentication of the transport channel. It secures the transportation route between each hub of the transport route. Each hub needs to

[2] https://ec.europa.eu/isa2/solutions/testa_en

[3] https://tools.ietf.org/html/rfc5246

decrypt (only) the address data to forward the message to the next hub. Before forwarding, each hub encrypts the address data again.
Simple (one-way) TLS is possible and sometime still applied, but two-way-TLS (mTLS) is recommended as it is becoming the current standard of protecting the transport layer.

2.3 Message layer

On the message layer several standards are applied by different e-CODEX components:

1. The protocol used for gateway-to-gateway transmission (as the message layer) is **AS4**[4] which signs and encrypts the messages - depending on the security configuration on gateway level.

2. The core component of the e-CODEX system is the domibusConnector. It adds security to the message layer by using **WS-Security**[5] for signing and encryption of messages for the webservices towards the gateway and the backend(s). Therefore, a connector-to-connector encryption is applied additionally.

3. For signing and encrypting functionality throughout the e-CODEX systems digital certificates are used. Those digital certificates for encryption and signing are compliant with the **X.509** standard[6].

2.4 Document layer

Messages contain documents and attachments. These are packed into a package, called “container”. The container is built according to the **ASiC-S**[7] standard. The sending domibusConnector signs the ASiC-S container and the signature is validated upon receipt by the receiving domibusConnector.

2.5 Access to e-CODEX configuration

The chapters above have pointed out, how e-CODEX applies security measures by applying security standards to the channel from one e-CODEX Access Point to another. Therefore, the route of an e-CODEX message can be considered secured.

However, security breaches cannot only happen during the transportation of messages. They can also happen when setting up e-CODEX Access Points. The communication between e-CODEX Access Points needs prior configuration. This configuration is done via so-called pModes (Processing

[4] http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/AS4-profile/v1.0/os/AS4-profile-v1.0-os.html
[5] https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss
[6] https://tools.ietf.org/html/rfc5280
[7] https://en.wikipedia.org/wiki/Associated_Signature_Containers#ASiC_Simple_(ASiC-S) and https://www.etsi.org/deliver/etsi_en/319100_319199/31916201/01.01.01_60/en_31916201v010101p.pdf

Modes). Such pModes contain the addressing data, the applied security policy and other information. Also, they contain the trust stores with the public certificates of all participating e-CODEX Access Points.

Such pModes are created for each partner's configuration by a central "Coordinator for Configuration" (CfC) using a Configuration Management Tool (CMT). The access to this CMT is provided and restricted to each partner only upon personal and individual request. The administrative access is restricted to CFCs.

Currently, the Ministry of Justice of North-Rhine-Westphalia (and its IT provider IT.NRW) serve as CfC, since they were the Coordinator of all relevant e-CODEX projects. This task will be handed over in the future to eu-LISA[8] as the future competent authority for the maintenance of e-CODEX.

2.6 e-CODEX Security Recommendations

As described in the previous chapters, e-CODEX has implemented a vast set of security measures, mostly by adopting well-established security standards. Still, e-CODEX provides flexibility to a certain extent, to apply a security level which reflects the security requirements of the different use cases. For each e-CODEX use case it can be decided (to a certain extent) which security level is applied. There are several minimum requirements, but it can be decided per use case to apply stricter requirements. E.g., it has been mentioned before that on transport layer TLS or the stricter mTLS can be applied. Also, the requirements for signatures (simple, advanced, qualified) can differ. The decision, which security level is applied, must be made by the business owner of an e-CODEX use case.

e-CODEX provides some guidance by providing **e-CODEX Security Recommendations**[9]. There, several specifications of security measures are described with a recommendation which level should – at least – be applied. To name a few examples:

- The security recommendations should apply to all environments that are exposed to external partners.
- Two-way-TLS (mTLS) should be applied to all cross-border e-Justice services.
- Only certificates that originate from a Certificate Authority listed in the Trusted Services List (TSL) are accepted.
- The RSA-key length should be above 2048bit, to be safe for the next couple of years.
- Etc.

As elaborated, these security recommendations are to be seen as recommendations. However, it is the intention of the e-CODEX Consortium to further develop these recommendations and subsequently transform them into a security policy. Such a policy would not be optional anymore, and e-CODEX participants would need to comply with it before accessing the e-CODEX communication.

[8] https://www.eulisa.europa.eu/

[9] https://www.e-codex.eu/sites/default/files/2020-11/e-justice%20Security%20recommendations%20v1.0_0.pdf

Finally, it needs to be taken into account that higher security usually comes with a price. Additional security levels do not only demand additional costs (e.g., for qualified certificates). Even more, they result in higher complexity of the system, resulting in additional effort for configuring, testing and maintaining the system. Therefore, it needs to be thoroughly considered which security level is appropriate and still efficient for the use case under discussion.

3 Data Protection by Design

The main legal source for data protection is of course the GDPR[10]. There are other provisions[11], though, which need to be taken into account for a deep Data Protection Impact Assessment (DPIA). Work Package 2 of the Me-CODEX II project has worked out such a DPIA for e-CODEX and came to the final conclusion of a positive validation result. This document therefore does not intend to repeat the DPIA but focusses on the justification, why data protection is applied to e-CODEX data not only as an added feature but by the design of the concept.

It has been pointed out above an in previous documents, that e-CODEX provides an infrastructure for communication (mainly between judicial authorities). For judicial use cases it is clear, that data is transferred, on which data protection regulations are applicable. The GDPR foresees that personal data can be transferred (i.e., processed) if it is based on one of the listed justifications. Further, personal data needs to be avoided where it is not necessary. Finally, if personal data is processed, appropriate measures need to be installed, to reduce the risk of a privacy breach with due dilligence.

e-CODEX applies such measures – again – not as extra features, but as an integral part of its design:

- As pointed out in the chapter 2 ”Security by Design” encryption is applied on several layers. The Gateway-to-Gateway communication is done via an encrypted channel and additionally, the Connector-to-Connector communication is encrypted, as well, to add even further security. Messages are signed to proof their authenticity.
- Additional encryption and authentication levels can be applied per e-CODEX use case.
- Participation in e-CODEX use cases is only possible for mutually acknowledged and authorised partners.
- For the transmission of data, the data needs to be processed. For this processing the data is stored temporarily. Then, after the processing, the data is automatically deleted. No personal data is stored permanently whatsoever.
- The temporary storage is done on the local instances of the e-CODEX Access Points. By design, there is no central data storage in place, as e-CODEX is a mere decentralised, peer-to-peer communication network without any central authority in between.

The high level of various data protection measures of e-CODEX is good starting point for privacy-compliant judicial communication. Still, the final responsibility lies with the operators of national e-CODEX participants and needs to take additional – national – systems into account.

e-CODEX participants are the controllers of the data. Therefore, also their national backend systems and IT infrastructure need to comply with data protection provisions. As controllers they have the

[10] https://eur-lex.europa.eu/eli/reg/2016/679/oj

[11] To name a few: Directive (EU) 2016/680, Regulation (EU) 2018/1725, National Data Protection law

responsibility to apply further measures on their national instances of e-CODEX Access Points and related systems:

- Strong authentication means for the users who have access to the e-CODEX infrastructure.
- Keeping their IT infrastructure (including the e-CODEX components) secure by applying recent updates of the software components.

As a result, e-CODEX facilitates compliance with data protection by its design. Still, national e-CODEX implementers need to make use of these facilities to provide a privacy-compliant environment.

Conclusion

The description in the previous chapters has shown that security and data protection is incorporated in e-CODEX not as an additional feature, but by design. Already, the overall architecture e-CODEX is driven by security and privacy considerations as it was clear from the beginning of the development of e-CODEX that it will have to serve judicial use cases with a high sensitivity regarding security and privacy requirements.

Still, technical evolution needs to be monitored closely and subsequently adopted into e-CODEX components. The technical environment is changing constantly and so are the risks of security and privacy breaches. This is a task which does not end at the end of Me-CODEX II but will need to be taken over by a competent authority for the maintenance of such a security- and privacy-designed system.