COMMISSION IMPLEMENTING DECISION (EU) 2022/2519

of 20 December 2022

on the technical specifications and standards for the e-CODEX system, including for security and methods for integrity and authenticity verification

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2022/850 of the European Parliament and of the Council of 30 May 2022 on a computerised system for the cross-border electronic exchange of data in the area of judicial cooperation in civil and criminal matters (e-CODEX system), and amending Regulation (EU) 2018/1726 ([1]), and in particular Article 6(1), point (a), thereof,

Whereas:

(1) In accordance with Article 5 of Regulation (EU) 2022/850, the e-CODEX system is composed of an e-CODEX access point, digital procedural standards and supporting software products, documentation and other assets listed in the Annex to that Regulation.

(2) The e-CODEX access point is composed of a gateway consisting of software, based on a common set of protocols, enabling the secure exchange of information over a telecommunications network with other gateways using the same common set of protocols and of a connector, making it possible to link connected systems to the gateway, consisting of software, based on a common set of open protocols.

(3) For the successful handover and takeover process of the e-CODEX system to eu-LISA, and to make possible the fulfilment of the tasks for which eu-LISA is to be responsible, the minimum technical specifications and standards, including for security and methods for integrity and authenticity verification, underpinning the components of the e-CODEX system should be established.

(4) In accordance with Articles 1 and 2 of Protocol No 22 on the position of Denmark, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, Denmark did not take part in the adoption of Regulation (EU) 2022/850 and is therefore not bound by or subject to the application of this Decision.

(5) In accordance with Articles 1 and 2 and Article 4a(1) of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, and without prejudice to Article 4 of that Protocol, Ireland did not take part in the adoption of Regulation (EU) 2022/850 and is therefore not bound by or subject to the application of this Decision.

(6) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council ([2]) and delivered an opinion on 24 November 2022.

(7) The measures provided for in this Decision are in accordance with the opinion of the committee established by Article 19(1) of Regulation (EU) 2022/850,

([1]) OJ L 150, 1.6.2022, p. 1.

([2]) Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

HAS ADOPTED THIS DECISION:

Article 1

The minimum technical specifications and standards, including for security and methods for integrity and authenticity verification, underpinning the components of the e-CODEX system referred to in Article 5 of Regulation (EU) 2022/850 shall be as set out in the Annex to this Decision.

Article 2

This Decision shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

Done at Brussels, 20 December 2022.

For the Commission
The President
Ursula VON DER LEYEN

ANNEX

The technical specifications and standards for the e-CODEX system, including for security and methods for integrity and authenticity verification

1. INTRODUCTION

This Annex sets out the minimum technical specifications and standards for the e-CODEX components, including for the security and methods for integrity and authenticity verification.

2. e-CODEX SYSTEM COMPONENTS

2.1. According to Article 5 of Regulation (EU) 2022/850 of the European Parliament and of the Council [1], the e-CODEX system is composed of:

(a) an e-CODEX access point, composed of:

(i) a gateway;

(ii) a connector;

(b) digital procedural standards (DPS);

(c) the supporting software products, documentation and other assets listed in the Annex to Regulation (EU) 2022/850:

(i) the Central Testing Platform (CTP) source code;

(ii) the Configuration Management Tool (CMT) source code;

(iii) metadata Workbench (MDW);

(iv) the EU e-Justice Core Vocabulary;

(v) architecture documentation.

2.2. From a functional point of view, those elements are divided into two categories: the e-CODEX Toolbox and the e-CODEX deployable assets.

2.3. **The e-CODEX Toolbox is composed of:**

(a) The e-CODEX architecture documentation;

(b) The Connector suite source code;

(c) The Configuration Management Tool (CMT) source code;

(d) The Central Testing Platform (CTP) source code;

(e) A Metadata Workbench (MDW) licence from a third party;

(f) The EU e-Justice Core Vocabulary;

(g) Digital procedural standards (DPS).

(a) The e-CODEX architecture documentation

The architecture documentation is a set of documents used to provide technical and informative knowledge to relevant stakeholders on the choice of standards with which other assets of the e-CODEX system must comply. It defines the requirements and principles that apply when creating interoperable cross-border communication for facilitating the electronic exchange of data, which include any content transmissible in electronic form. In addition, it lists chosen standards and methodologies on which the e-CODEX system is based. The architecture ensures the autonomy of the e-CODEX system.

(b) The Connector suite source code

The Connector suite source code is used to create the deployable artefacts described in Chapter 2.4.2.

[1] Regulation (EU) 2022/850 of the European Parliament and of the Council of 30 May 2022 on a computerised system for the cross-border electronic exchange of data in the area of judicial cooperation in civil and criminal matters (e-CODEX system), and amending Regulation (EU) 2018/1726 (OJ L 150, 1.6.2022, p. 1).

(c) The Configuration Management Tool (CMT)

The Configuration Management Tool (CMT) is a web-based tool for managing configuration files associated with the e-Delivery Gateway and Connector and provides a standardised way of handling the configuration workflow. The entity operating an authorised e-CODEX access point can access the CMT through a globally available portal and upload their e-Delivery configuration data. The uploaded data is to include the Gateway endpoint network configuration information, all security certificates needed for the connection, as well as the specific projects, environments and use cases they participate in. The CMT is to automatically check the validity of the uploaded data and is to provide feedback to the entity operating authorised e-CODEX access points if errors occur.

When a notification of any changes to the data provided by an entity operating an authorised e-CODEX access point is received, a new e-CODEX configuration package (see point 2.4.3) is to be produced using this tool. All entities operating authorised e-CODEX access points are to be notified about the creation of the new e-CODEX configuration package and can download it directly from the CMT at any time. The CMT can provide e-CODEX configuration packages for multiple IT environments, such as TEST, ACCEPTANCE or PRODUCTION.

New e-CODEX configuration packages are to go into effect seven days after their creation and, if applicable, entities operating authorised e-CODEX access points are to install the new package in their environment by that time.

The CMT also keeps the entity operating authorised e-CODEX access points updated on their security certificate runtimes and notifies authorised e-CODEX access points in advance, via email, about their upcoming certificate expiration. Should an entity operating an authorised e-CODEX access point let their security certificates expire, they are to be automatically removed from the next package creation.

The CMT is to be hosted centrally and be available 24/7 for e-CODEX participants. Support is to be limited to business hours.

(d) The Central Testing Platform (CTP)

The e-CODEX Central Testing Platform (CTP) is an automated testing infrastructure. It enables the entity operating an authorised e-CODEX access point to perform connectivity tests and end-to-end tests between their e-CODEX infrastructure and a fixed central testing point without the need to involve any further partner (e.g. another authorised e-CODEX access point) for testing communication functionalities. It allows sending and receiving customisable test messages and thus reduces the effort needed for testing of an e-CODEX infrastructure both at initial (installation) and regression testing time. Individual message progress, European Telecommunications Standards Institute (ETSI) Registered Electronic Mail (REM) evidences and error logs are tracked and presented to the entities operating authorised e-CODEX access points via specifically designed visual processes.

The CTP consists of an e-CODEX gateway, Connector, Connector-client and an associated Web Graphical User Interface (for now Web frontend/backend built on Nuxt.js) that can be used to send messages to a partner's gateway as well as to view messages that are sent to the CTP by the same gateway. The CTP currently stores important operating information (local variables) on a MongoDB instance and reads configuration (party) information from the connector database. Additionally, it uses the connector-client Representational state transfer (REST) Application Programming Interface (API)to retrieve information about e-CODEX messages and submit new messages to the connector and gateway.

In order to provide a customisable solution per e-CODEX environment, the CTP is deployed in various instances (copies) that exist in various e-CODEX environments. Each instance of the CTP is currently deployed in a UNIX (CentOS 7) environment, where all components co-exist. This facilitates administration and access to the file system but can be adapted to cater for installations where the e-CODEX messaging infrastructure is kept separate.

Each CTP user is linked to one (1) gateway. To use the CTP for testing, the only requirement is that the gateway of that authorised e-CODEX access point exists in the P-Modes for that specific e-CODEX CMT environment.

(e) The Metadata Workbench

The metadata workbench is a tool in which the EU e-Justice Core Vocabulary is being administered. It allows the semantic modellers to maintain the vocabulary in a sustainable manner adhering to the Core Component Technical Specification modelling standard as defined in the e-CODEX architecture documentation. It is a web-based Software as a Service (SaaS) solution with restricted access to EU e-Justice Core Vocabulary administrators only. The Metadata Workbench is developed and operated on behalf of the Ministry of Justice and Security of the Netherlands. On the basis of a licence agreement to be concluded between the Ministry of Justice and Security and eu-LISA, eu-LISA will be granted access to Metadata Workbench in order to administer and operate the EU e-Justice Core Vocabulary.

(f) The EU e-Justice Core Vocabulary

The EU e-Justice Core Vocabulary is an asset for reusable semantical terms and definitions used to ensure data consistency and data quality over time and across use cases. On its semantic repository all use-case specific message structures (XML schemas) are based.

Future evolutions of the e-Justice Core Vocabulary could be done in compliance with the Core Vocabularies. ([2]) In order to validate conformance to the specification, an XML-based validator could be set up using the Interoperability Test Bed service offered by the Commission.

(g) Digital procedural standards (DPS)

A digital procedural standard means the technical specifications for business process models and data schemas which set out the electronic structure of the data exchanged through the e-CODEX system based on the EU e-Justice Core Vocabulary. The business process model describes the technical implementation of the electronic procedure of the legal instrument that is supported by the e-CODEX system.

The business process model together with the EU e-Justice Core Vocabulary results in XML schemas describing the electronic structure of DPS. The XML schemas enable authorised access points to send and receive documents as provided by a cross-border judicial cooperation instrument.

2.4. **The e-CODEX deployable assets**

e-CODEX deployable assets are e-CODEX components deployed by entities operating an authorised e-CODEX access point in their e-CODEX environment. Except for the gateway they are to be distributed by eu-LISA to the entities operating an authorised e-CODEX access point.

The deployable assets are:

(a) The Gateway (point 2.4.1);

(b) The Connector Suite (point 2.4.2);

(c) The e-CODEX configuration package (including the P-modes, public certificates and security settings) (point 2.4.3);

(d) The business collaboration design or process model as part of the DPS;

(e) The XML schemas are message structures as part of the DPS.

2.4.1. ***The Gateway***

The Gateway within e-CODEX system is the building block responsible for the basic communication exchange. Currently a gateway has the following standards implemented:

(a) OASIS ([3]) ebMS 3.0 standard: Gateway interchange messages complying with the ebXML standard. This standard defines the structure a message header must have to be understood among the e-CODEX infrastructure;

(b) OASIS Applicability Statement 4 (AS4) messaging profile: This is a conformance profile of the OASIS ebMS 3.0 specification;

([2]) https://joinup.ec.europa.eu/collection/semantic-interoperability-community-semic/core-vocabularies.
([3]) Organization for the Advancement of Structured Information Standards.

(c) The Common Profile of the eDelivery AS4 profile ([4]).

Any gateway solution fulfilling those requirements can be used.

2.4.2. ***The Connector Suite***

The Connector is a linking component to connect national DPS specific applications to the generic messaging standards of the gateway. Thus, this component adds the following features to the basic communication already established by the gateway component:

(a) **ETSI-REM evidences**: Those are evidences generated by the Connector in a signed XML format. The purpose of those evidences is to inform the sender of a message on the successful or non-successful processing of the message. Evidences are generated and submitted by the Connector at different stages of message processing;

(b) **TrustOK Token**: The sending connector validates the integrity and authentication of the business document in the message. The outcome of this validation is written in TrustOK Token. This token is generated by a sub-module of the Connector: the security library;

(c) **ASiC-S container**: In accordance with ETSI Standard EN 319 162-1 on Electronic Signatures and Infrastructures and Associated Signature Containers (ASiC). The container ensures the authenticity and integrity of the payload transmitted by the Connector;

(d) **WS-Security**: To increase the transmission security of messages, the Connector uses the ws-security on the gateway side, as well as the connected system side for transmission. This means that every message the Connector submits or receives is encrypted and signed;

(e) **Common API**: The Connector offers a stable API which defines the web services that are used to connect to the gateway and the connected systems' application(s). The structure of messages exchanged with the Connector is also described in the Connector API.

In addition to the Connector software itself, the suite also contains an application client that is intended to support or substitute a connected system for handling e-CODEX messaging.

Also, a plugin was developed especially for the Domibus gateway ([5]) to link the common API of the Connector to the gateway's processing core.

2.4.3. ***e-CODEX configuration package***

In ebMS 3.0 based communication, a P-Mode (or Processing Mode) governs the transmission of all messages involved in a message exchange between two Messaging Service Handlers (MSHs). An e-CODEX configuration package includes a collection of messaging configuration parameters (P-Mode files, several certificate trust stores, network addresses) that specify in detail how messaging takes place.

Messaging configuration parameters can be classified in the following five categories:

(a) Parameters relating to the sender, such as:

  (i) the sender party identifier;

  (ii) the certificate the sender uses to sign messages;

  (iii) certificate authorities the sender trusts;

  (iv) the network address (or addresses) from which the sender will initiate communication.

(b) Parameters relating to the receiver, such as:

  (i) the receiver party identifier;

  (ii) the certificate the receiver expects to be used to encrypt messages;

  (iii) certificate authorities the receiver trusts;

([4]) https://ec.europa.eu/digital-building-blocks/wikis/x/RqbXGw.

([5]) The Domibus Gateway is maintained by the Commission (https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/Domibus).

(iv) the network address (or addresses) from which receiver will accept incoming communication.

(c) Parameters relating to the sender-receiver pair, such as (if used):

(i) agreement identifier, P-Mode identifier.

(d) Parameters relating to the DPS, such as:

(i) sender party role(s);

(ii) receiver party role(s);

(iii) service(s);

(iv) actions(s) within the Service.

(e) Parameters relating to the use of the messaging protocol, or the profile of the messaging protocol.

In e-CODEX all configuration files concerning a MSH or domain are bundled in one master file that can be used for the configuration of the Gateway and the Connector.

The master file defines an individual communication network that the MSH can address during its operation. It is necessary that the configuration is generated centrally because all information of all authorised e-CODEX access points must be available for the generation of the e-CODEX configuration package, which is created by the CMT.

3. SECURITY AND METHODS FOR INTEGRITY AND AUTHENTICITY VERIFICATION OF THE E-CODEX SYSTEM

The e-CODEX system is a communication system that provides strong support for addressing security and data protection requirements. In particular, the e-CODEX system provides the technical features necessary to meet all the requirements provided for in Regulation (EU) No 910/2014 of the European Parliament and of the Council ([6]).

3.1. Security by design

The e-CODEX system is, from a technical point of view, a transportation mechanism. There are different layers relevant for the security:

(a) a network layer;

(b) a transport layer;

(c) a message layer;

(d) a document layer.

On each of these layers security measures are applied.

3.1.1. *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 in this point). For most e-CODEX use cases such a network layer is sufficient. For higher security requirements another network layer could be applied, as well. Other networks can also be taken into consideration.

3.1.2. *Transport layer*

The transport layer is usually protected by Transport Layer Security (TLS) or mTLS (mutual TLS). 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 on the transport channel. It secures the transportation route between each hub of the transport route. Each hub needs to 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 sometimes still applied, but two-way-TLS (mTLS) is recommended as it is becoming the current standard of protecting the transport layer.

([6]) Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73).

3.1.3. ***Message layer***

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

(a) The protocol used for gateway-to-gateway transmission (as the message layer) is AS4 which signs and encrypts the messages – depending on the security configuration on gateway level;

(b) The core component of the e-CODEX system is the Connector. It adds security to the message layer by using WS-Security for signing and encryption of messages for the web services towards the gateway and the backend(s). Therefore, a connector-to-connector encryption is applied additionally;

(c) 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.

3.1.4. ***Document layer***

Messages contain documents and attachments. These are packed into a package, called 'container'. The container is built according to the ASiC-S standard. The sending Connector signs the ASiC-S container and the signature is validated upon receipt by the receiving Connector.

3.2. **Methods for integrity and authenticity verification**

3.2.1. ***Access to e-CODEX configuration***

The communication between e-CODEX Access Points needs prior configuration. This configuration is done via e-CODEX configuration package. The configuration package contains the addressing data, the applied security policy and other information. Furthermore, it also contains the trust stores with the public certificates of all participating e-CODEX Access Points. The configuration files are created for each partner's configuration by a central 'Coordinator for Configuration' (CfC) using the 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, which is to be managed by eu-LISA.

3.2.2. ***Supported electronic signatures and seals***

The e-CODEX system is to support all types of electronic seals and electronic signatures as provided for in Regulation (EU) No 910/2014.

3.2.3. ***e-CODEX TrustOK Token***

The sending connector validates the signature of the DPS of a message. The outcome of this validation is written into the e-CODEX TrustOK Token. This token is generated by a security library which is a submodule of the Connector. The validation of the electronic signature is done by the e-CODEX connector using DSS (digital signature service) tools.

3.2.4. ***Machine Readable Token (XML)***

The machine-readable token comes as an XML file underlying a certain schema containing all the information on the signature of the business token and the validation report as a result of the legal and technical validation.

3.2.5. ***Human Readable Token (PDF)***

The PDF-file consists of three parts. The first part presented on the first page of the actual Token includes general information on the advanced electronic system and an assessment of the legal validity of the business document. In addition, a disclaimer and a 'validation stamp' showing the legal validation result (successful/unsuccessful) are shown at the bottom of the page.

An advanced electronic system is a connected system capable of securely identifying the user and assuring the integrity of the messages sent through it between the client and the e-CODEX connector.

The second part on the second page provides a standardised technical overview of the information from the original validation report. Depending on the connected system (authentication- or signature-based), the information given by the technical overview varies. A signature-based token contains the information provided by the underlying certificate, including attributes (where available). An authentication-based token contains the name of the institution from where the document was sent, and, when provided, the name of the author of the document.

The bottom of this page consists of a stamp in the colour of the documents technical validation result (green/yellow/red) and a short description, e.g. providing additional information about why a document received a yellow technical assessment.

The third part of the document consists of the original validation report as it has been created by the issuing Member State's validation software.

4. DIGITAL PROCEDURAL STANDARDS (DPS) DEVELOPED UP TO DATE

E-Justice Service	DPS: process model	DPS: XML schema	Project source
European Payment Order	√	√	e-CODEX
Small Claims	√	√	e-CODEX
European Arrest Warrant	√	√	e-CODEX
Financial Penalties	√	√	e-CODEX
MLA	√	√	e-CODEX
FD 909 (Custodial Sentences)	√	√	e-CODEX
Matrimonial Matters	√	√	e-SENS
EU Account Preservation Order	√	√	e-SENS
Register of Wills	√	√	e-SENS
Service of Documents	√	√	e-CODEX