DURCHFÜHRUNGSBESCHLUSS (EU) 2022/2519 DER KOMMISSION

vom 20. Dezember 2022

über die technischen Spezifikationen und Standards für das e-CODEX-System, einschließlich der Sicherheitsstandards und der Methoden zur Überprüfung der Integrität und Authentizität

(Text von Bedeutung für den EWR)

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Verordnung (EU) 2022/850 des Europäischen Parlaments und des Rates vom 30. Mai 2022 über ein EDV-System für den grenzüberschreitenden elektronischen Datenaustausch im Bereich der justiziellen Zusammenarbeit in Zivil- und Strafsachen (e-CODEX-System) und zur Änderung der Verordnung (EU) 2018/1726 ([1]), insbesondere Artikel 6 Absatz 1 Buchstabe a,

in Erwägung nachstehender Gründe:

(1) Gemäß Artikel 5 der Verordnung (EU) 2022/850 besteht das e-CODEX-System aus einem e-CODEX-Zugangspunkt, digitalen Verfahrensstandards, den unterstützenden Softwareprodukten, der unterstützenden Dokumentation und den im Anhang der genannten Verordnung aufgeführten unterstützenden Beständen.

(2) Der e-CODEX-Zugangspunkt besteht aus einem Gateway, das wiederum aus einer Software auf der Grundlage von einheitlichen Protokollen besteht, die den sicheren Austausch von Informationen über ein Telekommunikationsnetz mit anderen Gateways ermöglicht, die dieselben Protokolle verwenden, sowie aus einem Konnektor, mit dem vernetzte Systeme mit dem Gateway verbunden werden können, und der aus einer Software auf der Grundlage von einheitlichen, offenen Protokollen besteht.

(3) Für die erfolgreiche Übergabe und Übernahme des e-CODEX-Systems an eu-LISA und die erfolgreiche Erfüllung der Aufgaben, für die eu-LISA künftig verantwortlich ist, sollten die technischen Mindestspezifikationen und -standards, einschließlich der Sicherheitsstandards und der Methoden zur Überprüfung der Integrität und Authentizität, die den Komponenten des e-CODEX-Systems zugrunde liegen, festgelegt werden.

(4) Nach den Artikeln 1 und 2 des dem Vertrag über die Europäische Union und dem Vertrag über die Arbeitsweise der Europäischen Union beigefügten Protokolls Nr. 22 über die Position Dänemarks hat sich Dänemark nicht an der Annahme der Verordnung (EU) 2022/850 beteiligt und ist daher weder durch diesen Beschluss gebunden noch zu seiner Anwendung verpflichtet.

(5) Nach den Artikeln 1 und 2 und Artikel 4a Absatz 1 des dem Vertrag über die Europäische Union und dem Vertrag über die Arbeitsweise der Europäischen Union beigefügten Protokolls Nr. 21 über die Position des Vereinigten Königreichs und Irlands hinsichtlich des Raums der Freiheit, der Sicherheit und des Rechts und unbeschadet des Artikels 4 dieses Protokolls hat sich Irland nicht an der Annahme der Verordnung (EU) 2022/850 beteiligt und ist daher weder durch diesen Beschluss gebunden noch zu seiner Anwendung verpflichtet.

(6) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates ([2]) angehört und hat am 24. November 2022 eine Stellungnahme abgegeben.

(7) Die in diesem Beschluss vorgesehenen Maßnahmen stehen im Einklang mit der Stellungnahme des mit Artikel 19 Absatz 1 der Verordnung (EU) 2022/850 eingerichteten Ausschusses —

([1]) ABl. L 150 vom 1.6.2022, S. 1.

([2]) Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39).

HAT FOLGENDEN BESCHLUSS ERLASSEN:

Artikel 1

Die technischen Mindestspezifikationen und -standards, einschließlich der Sicherheitsstandards und der Methoden zur Überprüfung der Integrität und Authentizität, die den in Artikel 5 der Verordnung (EU) 2022/850 genannten Komponenten des e-CODEX-Systems zugrunde liegen, sind im Anhang dieses Beschlusses festgelegt.

Artikel 2

Dieser Beschluss tritt am zwanzigsten Tag nach seiner Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Brüssel, den 20. Dezember 2022

Für die Kommission
Die Präsidentin
Ursula VON DER LEYEN

ANHANG

Die technischen Spezifikationen und Standards für das e-CODEX-System, einschließlich der Sicherheitsstandards und der Methoden zur Überprüfung der Integrität und Authentizität

1. **EINLEITUNG**

In diesem Anhang werden die technischen Mindestspezifikationen und -standards für das e-CODEX-System, einschließlich der Sicherheitsstandards und der Methoden zur Überprüfung der Integrität und Authentizität, festgelegt.

2. **KOMPONENTEN DES e-CODEX-SYSTEMS**

2.1. Gemäß Artikel 5 der Verordnung (EU) 2022/850 des Europäischen Parlaments und des Rates ([1]) besteht das e-CODEX-System aus:

a) einem e-CODEX-Zugangspunkt, zusammengesetzt aus:

i) einem Gateway;

ii) einem Konnektor.

b) digitalen Verfahrensstandards (DPS) und

c) den unterstützenden Softwareprodukten, der unterstützenden Dokumentation und den unterstützenden Beständen, die im Anhang der Verordnung (EU) 2022/850 aufgeführt sind:

i) dem Quellcode der zentralen Testplattform (CTP);

ii) dem Quellcode des Konfigurationsmanagementwerkzeugs (CMT);

iii) der Metadata-Workbench (MDW);

iv) dem EU-Kernvokabular zur E-Justiz;

v) der Dokumentation der Architektur.

2.2. Aus funktionaler Sicht werden diese Elemente in zwei Kategorien eingeteilt: das e-CODEX-Instrumentarium und die verfügbaren e-CODEX-Bestände.

2.3. **Das e-CODEX-Instrumentarium besteht aus:**

a) der Dokumentation der e-CODEX-Architektur;

b) dem Quellcode der Connector Suite;

c) dem Quellcode des Konfigurationsmanagementwerkzeugs (CMT);

d) dem Quellcode der zentralen Testplattform (CTP);

e) einer Metadata-Workbench-Lizenz (MDW-Lizenz) eines Drittanbieters;

f) dem EU-Kernvokabular zur E-Justiz;

g) digitalen Verfahrensstandards (DPS).

a) Die Dokumentation der e-CODEX-Architektur

Die Dokumentation der Architektur ist eine Dokumentensammlung, die verwendet wird, um einschlägigen Interessengruppen technisches und informatives Wissen über die Wahl der Standards zu vermitteln, denen andere Bestände des e-CODEX-Systems entsprechen müssen. Sie legt die Anforderungen und Grundsätze fest, die bei der Schaffung einer interoperablen grenzüberschreitenden Kommunikation zur Erleichterung des elektronischen Datenaustauschs gelten, zu dem alle in elektronischer Form übertragbaren Inhalte gehören. Darüber hinaus werden ausgewählte Standards und Methoden aufgeführt, auf denen das e-CODEX-System beruht. Die Architektur gewährleistet die Autonomie des e-CODEX-Systems.

b) Der Quellcode der Connector Suite

Der Quellcode der Connector Suite wird verwendet, um die in Abschnitt 2.4.2 beschriebenen verfügbaren Artefakte zu erstellen.

([1]) Verordnung (EU) 2022/850 des Europäischen Parlaments und des Rates vom 30. Mai 2022 über ein EDV-System für den grenzüberschreitenden elektronischen Datenaustausch im Bereich der justiziellen Zusammenarbeit in Zivil- und Strafsachen (e-CODEX-System) und zur Änderung der Verordnung (EU) 2018/1726 (ABl. L 150 vom 1.6.2022, S. 1).

c) Das Konfigurationsmanagementwerkzeug (CMT)

Das CMT ist ein webbasiertes Instrument für die Verwaltung von Konfigurationsdateien, die mit dem e-Delivery-Gateway und dem Konnektor verbunden sind; es bietet eine standardisierte Methode für die Abwicklung des Konfigurations-Workflows. Die Stelle, die einen autorisierten e-CODEX-Zugangspunkt betreibt, kann über ein weltweit verfügbares Portal auf das CMT zugreifen und ihre e-Delivery-Konfigurationsdaten hochladen. Die hochgeladenen Daten beinhalten die Informationen über die Netzwerkkonfiguration des Gateway-Endpunktes, alle für die Verbindung erforderlichen Sicherheitszertifikate sowie die spezifischen Projekte, Umgebungen und Anwendungsfälle, an denen die Stelle teilnimmt. Das CMT prüft die Gültigkeit der hochgeladenen Daten automatisch und informiert die Stelle, die autorisierte e-CODEX-Zugangspunkte betreibt, über etwaige Fehler.

Wenn eine Mitteilung über Änderungen der Daten eingeht, die von einer Stelle bereitgestellt wurden, die einen autorisierten e-CODEX-Zugangspunkt betreibt, ist unter Verwendung dieses Instruments ein neues e-CODEX-Konfigurationspaket (siehe Abschnitt 2.4.3) zu erstellen. Alle Stellen, die autorisierte e-CODEX-Zugangspunkte betreiben, sind über die Erstellung des neuen e-CODEX-Konfigurationspakets, das sie jederzeit direkt aus dem CMT herunterladen können, zu benachrichtigen. Das CMT kann e-CODEX-Konfigurationspakete für mehrere IT-Umgebungen wie TEST, ACCEPTANCE oder PRODUCTION bereitstellen.

Neue e-CODEX-Konfigurationspakete werden sieben Tage nach ihrer Erstellung anwendbar; gegebenenfalls müssen die Stellen, die autorisierte e-CODEX-Zugangspunkte betreiben, das neue Paket bis zu diesem Zeitpunkt in ihrer IT-Umgebung installieren.

Das CMT hält die Stelle, die autorisierte e-CODEX-Zugangspunkte betreibt, auch über die Laufzeit ihres Sicherheitszertifikats auf dem neuesten Stand und informiert die autorisierten e-CODEX-Zugangspunkte vorab per E-Mail über das bevorstehende Ablaufdatum des Zertifikats. Wenn eine Stelle, die einen autorisierten e-CODEX-Zugangspunkt betreibt, ihre Sicherheitszertifikate auslaufen lässt, wird sie automatisch aus der nächsten Erstellung eines Konfigurationspakets entfernt.

Das CMT wird zentral betrieben und für e-CODEX-Teilnehmer rund um die Uhr zur Verfügung stehen. Supportdienstleistungen werden auf die Geschäftszeiten beschränkt.

d) Die zentrale Testplattform (CTP)

Die e-CODEX-CTP ist eine automatisierte Testinfrastruktur. Sie ermöglicht der Stelle, die einen autorisierten e-CODEX-Zugangspunkt betreibt, die Durchführung von Konnektivitätstests und End-to-End-Tests zwischen ihrer e-CODEX-Infrastruktur und einer fixen zentralen Teststelle, ohne dass weitere Partner (z. B. ein anderer autorisierter e-CODEX-Zugangspunkt) für die Erprobung von Kommunikationsfunktionen einbezogen werden müssen. Sie dient dem Senden und Empfangen von individualisierbaren Testnachrichten und verringert somit den für das Testen einer e-CODEX-Infrastruktur erforderlichen Aufwand sowohl bei der Installation als auch im Rahmen von Regressionstests. Statusmeldungen zu einzelnen Nachrichten, Nachweise für registrierte E-Mail-Sendungen (REM-Nachweise) des Europäischen Instituts für Telekommunikationsnormen (ETSI) und Fehlerprotokolle werden erfasst und an die Stellen, die autorisierte e-CODEX-Zugangspunkte betreiben, über eigens konzipierte visuelle Verfahren übermittelt.

Die CTP besteht aus einem e-CODEX-Gateway, einem Konnektor, einem Konnektor-Client und einer zugehörigen grafischen Web-Benutzeroberfläche (derzeit „Web Frontend/Backend“ auf der Grundlage von „Nuxt.js“), mit der Nachrichten an das Gateway eines Partners gesendet und Nachrichten angezeigt werden können, die von diesem Gateway an das CTP gesendet werden. Gegenwärtig speichert die CTP wichtige Betriebsinformationen (lokale Variablen) in einer MongoDB-Instanz und liest Informationen über die Konfiguration (Partei) aus der Konnektor-Datenbank. Darüber hinaus nutzt die Plattform die REST-API (Representational State Transfer — REST; Anwendungsprogrammierschnittstelle — API) des Konnektor-Client, um Informationen über e-CODEX-Nachrichten abzurufen und neue Nachrichten an den Konnektor und das Gateway zu übermitteln.

Um eine individualisierbare Lösung für jede e-CODEX-Umgebung zu bieten, wird die CTP in verschiedenen Instanzen (Kopien) eingesetzt, die in verschiedenen e-CODEX-Umgebungen bestehen. Jede CTP-Instanz wird derzeit in einer UNIX-Umgebung (CentOS 7) eingesetzt, in der alle Komponenten nebeneinander bestehen. Dies erleichtert die Verwaltung des und den Zugang zum Dateisystem; für Installationen, in denen die e-CODEX-Nachrichteninfrastruktur getrennt bleibt, können jedoch Anpassungen vorgenommen werden.

Jeder CTP-Nutzer ist mit einem (1) Gateway verbunden. Die einzige Voraussetzung für die Nutzung der CTP für Tests ist, dass das Gateway des autorisierten e-CODEX-Zugangspunkts in den P-Modi für diese spezifische e-CODEX-CMT-Umgebung vorhanden ist.

e) Die Metadata-Workbench

Die Metadata-Workbench ist ein Instrument, mit dem das EU-Kernvokabular zur E-Justiz verwaltet wird. Sie ermöglicht es den semantischen Modellierern, das Vokabular nachhaltig zu pflegen und dabei den in der Dokumentation der e-CODEX-Architektur festgelegten Modellierungsstandard „Core Component Technical Specification" einzuhalten. Es handelt sich um eine webbasierte Software-as-a-Service-Lösung (SaaS) mit beschränktem Zugang nur für Administratoren des EU-Kernvokabulars zur E-Justiz. Die Metadata-Workbench wird im Auftrag des niederländischen Ministeriums für Justiz und Sicherheit entwickelt und betrieben. Auf der Grundlage einer zwischen diesem Ministerium und eu-LISA abzuschließenden Lizenzvereinbarung wird eu-LISA Zugang zur Metadata-Workbench gewährt, um das EU-Kernvokabular zur E-Justiz zu verwalten und zu betreiben.

f) Das EU-Kernvokabular zur E-Justiz

Das EU-Kernvokabular zur E-Justiz ist ein Bestand wiederverwendbarer semantischer Begriffe und Definitionen, der zur Sicherung der Datenkonsistenz und -qualität im Zeitverlauf und über Anwendungsfälle hinweg verwendet wird. Auf seinem semantischen Speicher basieren alle anwendungsfallspezifischen Nachrichtenstrukturen (XML-Schemata).

Künftige Entwicklungen des EU-Kernvokabulars zur E-Justiz könnten im Einklang mit den Kernvokabularen ([2]) erfolgen. Zur Überprüfung der Konformität mit der Spezifikation könnte unter Verwendung der von der Kommission angebotenen Prüfstände für die Interoperabilität (Interoperability Test Bed Service) ein XML-gestützter Validator eingerichtet werden.

g) Digitale Verfahrensstandards (DPS)

Unter einem „digitalen Verfahrensstandard" versteht man die technischen Spezifikationen für Geschäftsprozessmodelle und Datenschemata, mit denen auf der Grundlage des EU-Kernvokabulars zur E-Justiz die elektronische Struktur der im Rahmen des e-CODEX-Systems ausgetauschten Daten bestimmt wird. Das Geschäftsprozessmodell beschreibt die technische Umsetzung des elektronischen Verfahrens des vom e-CODEX-System unterstützten Rechtsinstruments.

Zusammen mit dem EU-Kernvokabular zur E-Justiz ergibt das Geschäftsprozessmodell XML-Schemata, die die elektronische Struktur von DPS beschreiben. Mithilfe der XML-Schemata können autorisierte Zugangspunkte Dokumente nach Maßgabe eines Instruments für die grenzüberschreitende justizielle Zusammenarbeit versenden und empfangen.

2.4. Die verfügbaren e-CODEX-Bestände

Die verfügbaren e-CODEX-Bestände sind e-CODEX-Komponenten, die von Stellen, die einen autorisierten e-CODEX-Zugangspunkt betreiben, in ihrer e-CODEX-Umgebung eingesetzt werden. Mit Ausnahme des Gateways werden sie von eu-LISA an die Stellen verteilt, die einen autorisierten e-CODEX-Zugangspunkt betreiben.

Die verfügbaren Bestände sind:

a) das Gateway (Abschnitt 2.4.1),

b) die Connector Suite (Abschnitt 2.4.2),

c) das e-CODEX-Konfigurationspaket (einschließlich der P-Modi, öffentlichen Zertifikate und Sicherheitseinstellungen) (Abschnitt 2.4.3),

d) das Kooperationsmuster oder das Prozessmodell als Teil der DPS,

e) die XML-Schemata, die Nachrichtenstrukturen sind, als Teil der DPS.

2.4.1. *Das Gateway*

Das Gateway innerhalb des e-CODEX-Systems ist der für den grundlegenden Kommunikationsaustausch verantwortliche Baustein. Derzeit finden in einem Gateway folgende Standards ihre Umsetzung:

a) der OASIS ([3])-ebMS-3.0-Standard: Austausch von Nachrichten im ebXML-Standard zwischen Gateways. Dieser Standard definiert die Struktur, die ein Nachrichtenkopf haben muss, um innerhalb der e-CODEX-Infrastruktur verstanden zu werden;

b) das Nachrichtenprofil des OASIS-„Applicability Statement 4 (AS4)": Dies ist ein Konformitätsprofil der OASIS-ebMS3.0-Spezifikation;

([2]) https://joinup.ec.europa.eu/collection/semantic-interoperability-community-semic/core-vocabularies

([3]) Organization for the Advancement of Structured Information Standards.

c) das gemeinsame Profil des eDelivery-AS4-Profils ([4]).

Jede Gateway-Lösung, die diese Anforderungen erfüllt, kann genutzt werden.

2.4.2. ***Die Connector Suite***

Der Konnektor ist eine Verbindungskomponente, die nationale DPS-spezifische Anwendungen mit den generischen Nachrichtenübermittlungsstandards des Gateways verbindet. Diese Komponente ergänzt somit die von der Gateway-Komponente bereits geschaffene grundlegende Kommunikation um folgende Funktionen:

a) **ETSI-REM-Nachweise:** Dabei handelt es sich um Nachweise, die vom Konnektor in einem signierten XML-Format generiert werden. Zweck dieser Nachweise ist es, den Absender über die erfolgreiche oder nicht erfolgreiche Verarbeitung der Nachricht zu informieren. Sie werden vom Konnektor in verschiedenen Phasen der Nachrichtenverarbeitung generiert und übermittelt;

b) **TrustOK-Token:** Der sendende Konnektor validiert in der Nachricht die Integrität und Authentifizierung des Geschäftsdokuments. Das Ergebnis dieser Validierung wird im TrustOK-Token festgehalten. Dieses Token wird von einem Untermodul des Konnektors generiert: der Sicherheitsbibliothek;

c) **ASIC-S-Container:** gemäß der ETSI-Norm EN 319 162-1 über elektronische Signaturen und Infrastrukturen und zugehörige Signatur-Container (ASiC). Der Container gewährleistet die Authentizität und Integrität der vom Konnektor übermittelten Nutzdaten;

d) **WS-Security:** Zur Erhöhung der Übertragungssicherheit von Nachrichten verwendet der Konnektor sowohl auf der Seite des Gateways als auch auf jener des vernetzten Systems WS-Security für die Übertragung. Das bedeutet, dass jede vom Konnektor gesendete oder empfangene Nachricht verschlüsselt und signiert ist;

e) **Gemeinsame API:** Der Konnektor bietet eine stabile API, in der die Web-Dienste festgelegt werden, die für die Verbindung mit dem Gateway und der/den Anwendung/en der vernetzten Systeme verwendet werden. Auch die Struktur der mit dem Konnektor ausgetauschten Nachrichten wird in der Konnektor-API beschrieben.

Neben der Konnektor-Software selbst enthält die Reihe auch einen Anwendungs-Client, der ein vernetztes System für die Bearbeitung von e-CODEX-Nachrichten unterstützen oder ersetzen soll.

Außerdem wurde speziell für das Domibus-Gateway ([5]) ein Plugin entwickelt, um die gemeinsame API des Konnektors mit dem Prozessorkern des Gateways zu verknüpfen.

2.4.3. ***e-CODEX-Konfigurationspaket***

In ebMS-3.0-basierter Kommunikation regelt ein P-Modus (oder Verarbeitungsmodus) die Übertragung aller Nachrichten, die an einem Austausch zwischen zwei „Messaging Service Handlern (MSH)" beteiligt sind. Ein e-CODEX-Konfigurationspaket umfasst eine Reihe von Nachrichten-Konfigurationsparametern (P-Modus-Dateien, mehrere „Certificate Trust Stores", Netzwerkadressen), in denen genau festgelegt ist, wie die Nachrichtenübermittlung erfolgt.

Die Nachrichten-Konfigurationsparameter können in die folgenden fünf Kategorien eingeteilt werden:

a) Parameter mit Bezug zum Absender, wie z. B.:

   i) die Kennung des Absenders;

   ii) das Zertifikat, das der Absender zum Signieren von Nachrichten verwendet;

   iii) die Zertifizierungsstellen, denen der Absender vertraut;

   iv) die Netzadresse/n, von der/denen aus der Absender die Kommunikation aufnimmt.

b) Parameter mit Bezug zum Empfänger, wie z. B.:

   i) die Kennung des Empfängers;

   ii) das Zertifikat, das der Empfänger für die Verschlüsselung von Nachrichten erwartet;

   iii) die Zertifizierungsstellen, denen der Empfänger vertraut;

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

([5]) Das Domibus-Gateway wird von der Kommission gewartet (https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/Domibus).

iv) die Netzadresse/n, von der/denen der Empfänger eingehende Nachrichten annimmt.

c) Parameter (falls verwendet) mit Bezug zum Absender-Empfänger-Paar, wie z. B.:

i) Kennung der Vereinbarung, P-Modus-Kennung.

d) Parameter mit Bezug zu den DPS, wie z. B.:

i) Rolle/n der Absenderpartei;

ii) Rolle/n der Empfängerpartei;

iii) Dienstleistung(en);

iv) Maßnahmen innerhalb des Dienstes.

e) Parameter mit Bezug zur Verwendung des Benachrichtigungsprotokolls oder zu dessen Profil.

In e-CODEX werden alle Konfigurationsdateien zu einem MSH oder einer Domäne in einer Masterdatei gebündelt, die für die Konfiguration von Gateway und Konnektor verwendet werden kann.

Die Masterdatei definiert ein individuelles Kommunikationsnetz, an das sich der MSH während des Betriebs richten kann. Die Konfiguration muss zentral erstellt werden, da alle Informationen aller autorisierten e-CODEX-Zugangspunkte für die Generierung des vom CMT erstellten e-CODEX-Konfigurationspakets verfügbar sein müssen.

3. SICHERHEITSSTANDARDS UND METHODEN ZUR ÜBERPRÜFUNG DER INTEGRITÄT UND AUTHENTIZITÄT DES e-CODEX-SYSTEMS

Das e-CODEX-System ist ein Kommunikationssystem, das umfassende Unterstützung bei der Erfüllung von Sicherheits- und Datenschutzanforderungen bietet. Insbesondere verfügt das e-CODEX-System über die für die Erfüllung aller Anforderungen der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates ([6]) notwendigen Funktionen.

3.1. Eingebaute Sicherheit:

Aus technischer Sicht ist das e-CODEX-System ein Transportmechanismus. Es gibt verschiedene sicherheitsrelevante Ebenen:

a) eine Netzwerk-Ebene;

b) eine Transport-Ebene;

c) eine Nachrichten-Ebene;

d) eine Dokumenten-Ebene.

Auf jeder dieser Ebenen werden Sicherheitsmaßnahmen angewendet.

3.1.1. *Netzwerk-Ebene*

e-CODEX kann mit verschiedenen Arten von Netzwerkebenen verwendet werden. Es wird in der Regel bei normalen Internetanschlüssen angewendet. Die Sicherheit wird daher durch die üblichen Sicherheitsanwendungen der Internettechnologie gewährleistet (und durch die anderen in diesem Abschnitt beschriebenen Ebenen erweitert). Für die meisten Anwendungsfälle von e-CODEX ist eine solche Netzwerkebene ausreichend. Für höhere Sicherheitsanforderungen könnte auch eine andere Netzwerkebene angewendet werden. Auch andere Netze können in Betracht gezogen werden.

3.1.2. *Transport-Ebene*

Die Transportebene wird in der Regel durch Transport Layer Security (TLS) oder mTLS (gegenseitige TLS) geschützt. Dies ist ein etablierter Standard für den Schutz der Transportebene in Internettechnologien, der weltweit bei einer Vielzahl von Diensten Anwendung findet. TLS/mTLS sorgt für die Verschlüsselung und Authentifizierung des Transportkanals. Dadurch wird der Transportweg zwischen den einzelnen Knotenpunkten der Transportroute gesichert. Jeder Knotenpunkt muss (nur) die Adressdaten entschlüsseln, um die Nachricht an den nächsten Knotenpunkt weiterzuleiten. Vor der Weiterleitung verschlüsselt jeder Knotenpunkt die Adressdaten erneut. Eine einfache (einseitige) TLS ist möglich und findet manchmal noch Anwendung; es wird jedoch die zweiseitige TLS (mTLS) empfohlen, da sie mittlerweile Standard beim Schutz der Transportebene ist.

([6]) Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (ABl. L 257 vom 28.8.2014, S. 73).

3.1.3. ***Nachrichten-Ebene***

Auf der Nachrichtenebene werden mehrere Standards von verschiedenen e-CODEX-Komponenten angewendet:

a) Das für die Gateway-to-Gateway-Übertragung (als Nachrichtenebene) verwendete Protokoll ist AS4, das abhängig von der Sicherheitskonfiguration auf Gateway-Ebene die Nachrichten signiert und verschlüsselt;

b) Die Kernkomponente des e-CODEX-Systems ist der Konnektor. Er erhöht die Sicherheit auf der Nachrichtenebene, indem er WS-Security für das Signieren und Verschlüsseln von Nachrichten für die Web-Dienste zum Gateway und zum Backend bzw. den Backends verwendet. Daher wird zusätzlich eine Konnektor-zu-Konnektor-Verschlüsselung vorgenommen;

c) Für die Signier- und Verschlüsselungsfunktion werden in allen e-CODEX-Systemen digitale Zertifikate verwendet. Diese digitalen Signier- und Verschlüsselungszertifikate entsprechen dem X.509-Standard.

3.1.4. ***Dokumenten-Ebene***

Nachrichten enthalten Dokumente und Anlagen. Diese werden zu einem als „Container" bezeichneten Paket geschnürt. Der Container ist nach dem ASiC-S-Standard aufgebaut. Der sendende Konnektor signiert den ASiC-S-Container, und die Signatur wird nach Eingang durch den empfangenden Konnektor validiert.

3.2. **Methoden zur Überprüfung der Integrität und Authentizität**

3.2.1. ***Zugang zur e-CODEX-Konfiguration***

Die Kommunikation zwischen e-CODEX-Zugangspunkten muss zuvor konfiguriert werden. Diese Konfiguration erfolgt über das e-CODEX-Konfigurationspaket. Das Konfigurationspaket enthält die Adressdaten, das angewandte Sicherheitssystem und weitere Informationen. Darüber hinaus enthält es auch die „Trust Stores" mit den öffentlichen Zertifikaten aller teilnehmenden e-CODEX-Zugangspunkte. Die Konfigurationsdateien werden für die Konfiguration jedes Partners von einem zentralen „Koordinator für die Konfiguration" (CfC) mithilfe des CMT erstellt. Der Zugang zu diesem CMT wird jedem Partner nur auf persönlichen und individuellen Antrag hin gewährt und beschränkt. Der administrative Zugang ist auf CfCs beschränkt und soll von eu-LISA verwaltet werden.

3.2.2. ***Unterstützte elektronische Signaturen und Siegel***

Das e-CODEX-System unterstützt alle Arten von elektronischen Siegeln und elektronischen Signaturen gemäß der Verordnung (EU) Nr. 910/2014.

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

Der sendende Konnektor validiert die Signatur der DPS einer Nachricht. Das Ergebnis dieser Validierung wird im e-CODEX-TrustOK-Token festgehalten. Dieses Token wird von einer Sicherheitsbibliothek, einem Untermodul des Konnektors, generiert: Die Validierung der elektronischen Signatur erfolgt durch den e-CODEX-Konnektor unter Verwendung von DSS-Tools (Digital Signature Service; digitaler Signaturdienst).

3.2.4. ***Maschinenlesbares Token (XML)***

Das maschinenlesbare Token wird als XML-Datei geliefert, die einem bestimmten Schema unterliegt und alle Informationen über die Signatur des Geschäftstokens und den Validierungsbericht (Ergebnis der rechtlichen und technischen Validierung) enthält.

3.2.5. ***Vom Menschen lesbares Token (PDF)***

Die PDF-Datei besteht aus drei Teilen. Der erste Teil auf der ersten Seite des eigentlichen Tokens enthält allgemeine Informationen über das fortgeschrittene elektronische System und eine Bewertung der Rechtsgültigkeit des Geschäftsdokuments. Darüber hinaus werden am Ende der Seite ein Haftungsausschluss und ein „Validierungsstempel" mit dem Ergebnis der rechtlichen Validierung (erfolgreich/nicht erfolgreich) angezeigt.

Ein fortgeschrittenes elektronisches System ist ein vernetztes System, das den Benutzer sicher identifizieren und die Integrität der Nachrichten gewährleisten kann, die über dieses System zwischen dem Client und dem e-CODEX-Konnektor übermittelt werden.

Der zweite Teil (auf der zweiten Seite) bietet einen standardisierten technischen Überblick über die Informationen aus dem ursprünglichen Validierungsbericht. Je nach Art des vernetzten Systems (authentifizierungs- oder signaturbasiert) variieren die in der technischen Übersicht enthaltenen Informationen. Ein signaturbasiertes Token enthält die vom zugrunde liegenden Zertifikat gelieferten Informationen, einschließlich der Attribute (sofern verfügbar). Ein authentifizierungsbasiertes Token enthält den Namen des Organs, von dem aus das Dokument versandt wurde, und, sofern verfügbar, den Namen des Verfassers des Dokuments.

Der untere Teil dieser Seite besteht aus einem Stempel in der Farbe des technischen Validierungsergebnisses des Dokuments (grün/gelb/rot) und einer kurzen Beschreibung, z. B. mit zusätzlichen Informationen darüber, warum ein Dokument eine gelbe technische Bewertung erhalten hat.

Der dritte Teil des Dokuments besteht aus dem ursprünglichen Validierungsbericht, wie er von der Validierungssoftware des ausstellenden Mitgliedstaats erstellt wurde.

4. BISLANG ENTWICKELTE DIGITALE VERFAHRENSSTANDARDS (DPS)

E-Justiz-Dienst	DPS: Prozessmodell	DPS: XML-Schema	Projektquelle
Europäischer Zahlungsbefehl	√	√	e-CODEX
Geringfügige Forderungen	√	√	e-CODEX
Europäischer Haftbefehl	√	√	e-CODEX
Finanzielle Sanktionen	√	√	e-CODEX
Rechtshilfe	√	√	e-CODEX
Rahmenbeschluss 909 (Freiheitsstrafen)	√	√	e-CODEX
Ehesachen	√	√	e-SENS
EU-Beschluss zur vorläufigen Kontenpfändung	√	√	e-SENS
Testamentsregister	√	√	e-SENS
Zustellung von Schriftstücken	√	√	e-CODEX