KOMMISSIONENS GENNEMFØRELSESAFGØRELSE (EU) 2022/2519

af 20. december 2022

om de tekniske specifikationer og standarder for e-CODEX-systemet, herunder for sikkerhed og metoder til verificering af integritet og ægthed

(EØS-relevant tekst)

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde,

under henvisning til Europa-Parlamentets og Rådets forordning (EU) 2022/850 af 30. maj 2022 om et IT-system til grænseoverskridende elektronisk udveksling af oplysninger på området civil- og strafferetligt samarbejde (e-CODEX-systemet) og om ændring af forordning (EU) 2018/1726 ([1]), særlig artikel 6, stk. 1, litra a), og

ud fra følgende betragtninger:

(1) Jf. artikel 5 i forordning (EU) 2022/850 består e-CODEX-systemet af et e-CODEX-adgangspunkt, digitale proceduremæssige standarder og understøttende softwareprodukter, dokumentation og andre aktiver, der er anført i bilaget til forordningen.

(2) e-CODEX-adgangspunktet består af en gateway bestående af software, der bygger på et fælles sæt protokoller, og som giver mulighed for sikker udveksling af oplysninger via et telekommunikationsnet med andre gateways, der benytter samme fælles sæt protokoller, og af en konnektor, der gør det muligt at forbinde tilsluttede systemer til gatewayen, og som består af software, der bygger på et fælles sæt åbne protokoller.

(3) For vellykket overtagelse og overdragelse af e-CODEX-systemet til eu-LISA, og for at gøre udførelsen af de opgaver, som eu-LISA er ansvarligt for, muligt, bør de tekniske minimumsspecifikationer og -standarder, herunder for sikkerhed og for metoder til verificering af integritet og ægthed, der ligger til grund for e-CODEX-systemets komponenter, oprettes.

(4) I medfør af artikel 1 og 2 i protokol nr. 22 om Danmarks stilling, der er knyttet som bilag til traktaten om Den Europæiske Union og til traktaten om Den Europæiske Unions funktionsmåde, deltog Danmark ikke i vedtagelsen af forordning (EU) 2022/850, og nærværende afgørelse er derfor ikke bindende for og ikke finder anvendelse i Danmark.

(5) I medfør af artikel 1 og 2 og artikel 4a, stk. 1, i protokol nr. 21 om Det Forenede Kongeriges og Irlands stilling for så vidt angår området med frihed, sikkerhed og retfærdighed, der er knyttet som bilag til traktaten om Den Europæiske Union og til traktaten om Den Europæiske Unions funktionsmåde, og med forbehold af artikel 4 i samme protokol, deltager Irland ikke i vedtagelsen af forordning (EU) 2022/850, og nærværende afgørelse er derfor ikke bindende for og ikke finder anvendelse i Irland.

(6) Den Europæiske Tilsynsførende for Databeskyttelse er hørt i overensstemmelse med artikel 42, stk. 1, i Europa-Parlamentets og Rådets forordning (EU) 2018/1725 ([2]) og afgav udtalelse den 24. november 2022.

(7) Foranstaltningerne i denne afgørelse er i overensstemmelse med udtalelsen fra det udvalg, der er nedsat ved artikel 19, stk. 1, i forordning (EU) 2022/850 —

([1]) EUT L 150 af 1.6.2022, s. 1.

([2]) Europa-Parlamentets og Rådets forordning (EU) 2018/1725 af 23. oktober 2018 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i Unionens institutioner, organer, kontorer og agenturer og om fri udveksling af sådanne oplysninger og om ophævelse af forordning (EF) nr. 45/2001 og afgørelse nr. 1247/2002/EF (EUT L 295 af 21.11.2018, s. 39).

VEDTAGET DENNE AFGØRELSE:

Artikel 1

De tekniske minimumsspecifikationer og -standarder, herunder for sikkerhed og for metoder til verificering af integritet og ægthed, som ligger til grund for e-CODEX-systemets komponenter, der er omhandlet i artikel 5 i forordning (EU) 2022/850, er fastsat i bilaget til denne afgørelse.

Artikel 2

Denne afgørelse træder i kraft på tyvendedagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

Udfærdiget i Bruxelles, den 20. december 2022.

På Kommissionens vegne
Ursula VON DER LEYEN
Formand

BILAG

De tekniske specifikationer og standarder for e-CODEX-systemet, herunder for sikkerhed og metoder til verificering af integritet og ægthed

1. **INDLEDNING**

I dette bilag fastsættes de tekniske minimumsspecifikationer og -standarder for e-CODEX-systemets komponenter, herunder for sikkerhed og for metoder til verificering af integritet og ægthed.

2. **e-CODEX-SYSTEMETS KOMPONENTER**

2.1. Jf. artikel 5 i Europa-Parlamentets og Rådets forordning (EU) 2022/850 ([1]) består e-CODEX-systemet af:

a) et e-CODEX-adgangspunkt bestående af:

i) en gateway

ii) en konnektor.

b) digitale proceduremæssige standarder,

c) de(t) understøttende softwareprodukt(er), dokumentation og andre aktiver, der er anført i bilaget til forordning (EU) 2022/850:

i) kildekoden til den centrale testplatform

ii) kildekoden til konfigurationsstyringsværktøjet

iii) Metadata Workbench

iv) EU's centrale glossar for e-justice

v) arkitekturdokumentation.

2.2. Ud fra et funktionelt synspunkt er disse elementer opdelt i to kategorier: e-CODEX-værktøjskassen og e-CODEX-udrulningsaktiver.

2.3. **e-CODEX-værktøjskassen består af:**

a) e-CODEX-arkitekturdokumentationen

b) kildekoden til Connector Suite

c) kildekoden til konfigurationsstyringsværktøjet

d) kildekoden til den centrale testplatform

e) en tredjepartslicens til Metadata Workbench

f) EU's centrale glossar for e-justice

g) digitale proceduremæssige standarder.

a) e-CODEX-arkitekturdokumentationen

Arkitekturdokumentationen består af en række dokumenter, der anvendes til at give relevante interessenter teknisk og oplysende viden om valg af standarder, som andre aktiver i e-CODEX-systemet skal overholde. Den fastlægger de gældende krav og principper ved etablering af interoperabel, grænseoverskridende kommunikation til at lette elektronisk udveksling af oplysninger, hvilket omfatter ethvert indhold, der kan overføres i elektronisk form. Desuden indeholder den en fortegnelse over de valgte standarder og metoder, som e-CODEX-systemet bygger på. Arkitekturen sikrer e-CODEX-systemets autonomi.

b) Kildekoden til Connector Suite

Kildekoden til Connector Suite anvendes til at skabe de udrulningsartefakter, som er beskrevet i afsnit 2.4.2.

([1]) Europa-Parlamentets og Rådets forordning (EU) 2022/850 af 30. maj 2022 om et IT-system til grænseoverskridende elektronisk udveksling af oplysninger på området civil- og strafferetligt samarbejde (e-CODEX-systemet) og om ændring af forordning (EU) 2018/1726 (EUT L 150 af 1.6.2022, s. 1).

c) Konfigurationsstyringsværktøjet

Konfigurationsstyringsværktøjet er et webbaseret værktøj til administration af konfigurationsfiler i forbindelse med e-Delivery-gatewayen og konnektoren, der gør det muligt at håndtere konfigurationsworkflowet på en standardiseret måde. Enheden, der driver et autoriseret e-CODEX-adgangspunkt, kan tilgå konfigurationsstyringsværktøjet via en globalt tilgængelig portal og uploade deres e-Delivery-konfigurationsdata. De uploadede data skal indeholde konfigurationsoplysninger om gatewayens endepunkter i netværket, alle sikkerhedscertifikater til brug for tilkoblingen samt de specifikke projekter, miljøer og brugstilfælde, som enheden deltager i. Konfigurationsstyringsværktøjet skal automatisk kontrollere gyldigheden af de uploadede data og give feedback til enheden, der driver autoriserede e-CODEX-adgangspunkter, hvis der sker fejl.

Når en meddelelse om ændringer af data fra en enhed, der driver et autoriseret e-CODEX-adgangspunkt er modtaget, skal der udarbejdes en ny e-CODEX-konfigurationspakke (jf. punkt 2.4.3.) ved hjælp af dette værktøj. Alle enheder, der driver autoriserede e-CODEX-adgangspunkter, skal underrettes om, at den nye e-CODEX-konfigurationspakke er blevet udviklet, og at den når som helst kan downloades direkte fra konfigurationsstyringsværktøjet. Konfigurationsstyringsværktøjet kan levere e-CODEX-konfigurationspakker til flere IT-miljøer som f.eks. TEST, GODKENDELSE eller PRODUKTION.

Nye e-CODEX-konfigurationspakker træder i kraft syv dage efter, de er udviklet, og enheder, der driver autoriserede e-CODEX-adgangspunkter, skal eventuelt installere den nye pakke i deres miljø inden da.

Konfigurationsstyringsværktøjet holder desuden den enhed, der driver autoriserede e-CODEX-adgangspunkter, ajour med deres sikkerhedscertifikats runtimes og underretter på forhånd via e-mail de autoriserede e-CODEX-adgangspunkter om, at deres certifikat er ved at udløbe. Hvis en enhed, der driver et autoriseret e-CODEX-adgangspunkt, lader sine sikkerhedscertifikater udløbe, skal de automatisk fjernes fra den næste pakke, der bliver udviklet.

Konfigurationsstyringsværktøjet skal hostes centralt og være tilgængeligt for e-CODEX-deltagerne døgnet rundt. Support er begrænset til almindelig arbejdstid.

d) Den centrale testplatform

Den centrale testplatform i e-CODEX-systemet er en automatisk testinfrastruktur. Den giver den enhed, der driver et autoriseret e-CODEX-adgangspunkt, mulighed for at foretage konnektivitetstest og end-to-end-test mellem sin e-CODEX-infrastruktur og et fast centralt testpunkt uden at skulle inddrage andre partnere (f.eks. et andet autoriseret e-CODEX-adgangspunkt) i test af kommunikationsfunktioner. Den giver mulighed for at sende og modtage tilpassede testmeddelelser og reducerer dermed de ressourcer, der er behov for til at teste e-CODEX-infrastrukturen både ved den første (installation) test og ved regressionstest. Individuel beskedstatus, dokumentation fra Det Europæiske Institut for Telestandarder (ETSI) og Registered Electronic Mail (REM) samt fejl-logs spores og forelægges for de enheder, der driver autoriserede e-CODEX-adgangspunkter via specielt designede visuelle processer.

Den centrale testplatform består af en e-CODEX-gateway, en konnektor, en konnektor-klient og en tilknyttet grafisk brugergrænseflade (indtil videre Web frontend/backend, der bygger på Nuxt.js), der kan bruges til at sende beskeder til en partners gateway samt til at se beskeder, der er sendt til den centrale testplatform fra den samme gateway. Den centrale testplatform lagrer vigtige driftsoplysninger (lokale variabler) om et MongoDB-tilfælde og læser (partens) konfigurationsoplysninger fra konnektordatabasen. Derudover anvender den konnektor-klientens Representational State Transfer (REST) Application Programming Interface (API) til at hente oplysninger om e-CODEX-meddelelser og sende nye meddelelser til konnektoren og gatewayen.

For at kunne levere en skræddersyet løsning til det enkelte e-CODEX-miljø bliver den centrale testplatform udrullet i forskellige eksemplarer (udgaver), som findes i forskellige e-CODEX-miljøer. Hvert eksemplar af den centrale testplatform bliver i øjeblikket udrullet i et UNIX (CentOS 7)-miljø, hvor alle komponenter findes side om side. Dette letter administrationen og adgangen til filsystemet, men den kan tilpasses, så den passer til installationer, hvor messaging-infrastrukturen i e-CODEX-systemet holdes adskilt.

Den enkelte bruger af den centrale testplatform er forbundet til én gateway. For at kunne anvende den centrale testplatform til at foretage test er det eneste krav, at gatewayen til det pågældende autoriserede e-CODEX-adgangspunkt forekommer i P-Modes for det specifikke e-CODEX CMT-miljø.

e) Metadata Workbench

Metadata Workbench er et værktøj, hvori EU's centrale glossar for e-justice administreres. Det giver udviklerne af semantiske modeller mulighed for at ajourføre glossaret på en holdbar måde, som opfylder Core Component Technical Specification-standarden for modeller, jf. e-CODEX-arkitekturdokumentationen. Det er en webbaseret software-as-a-service (SaaS)-løsning, som kun administratorerne af EU's centrale glossar for e-justice har adgang til. Metadata Workbench er udviklet og drives på vegne af sikkerheds- og justitsministeriet i Nederlandene. På baggrund af en licensaftale, der indgås mellem sikkerheds- og justitsministeriet og eu-LISA, vil eu-LISA få adgang til Metadata Workbench med henblik på at administrere og drive EU's centrale glossar for e-justice.

f) EU's centrale glossar for e-justice

EU's centrale glossar for e-justice er et aktiv til genanvendelige semantiske udtryk og definitioner, der anvendes til at sikre datakonsistens og datakvalitet over tid og i alle brugstilfælde. Alle anvendelsesspecifikke meddelelsesstrukturer (XML-skemaer) er baseret på dets semantiske datalager.

Den videre udvikling af EU's centrale glossar for e-justice kan ske i overensstemmelse med det centrale glossar ([2]). Med henblik på at validere overensstemmelse med specifikationen kan der etableres en XML-baseret validator med hjælp fra Kommissionens Interoperability Test Bed-tjeneste.

g) Digitale proceduremæssige standarder

Ved digital proceduremæssig standard forstås de tekniske specifikationer for forretningsprocesmodeller og dataskemaer, der fastsætter den elektroniske struktur af de oplysninger, som udveksles via e-CODEX-systemet, på grundlag af EU's centrale glossar for e-justice. I forretningsprocesmodellen beskrives den tekniske gennemførelse af retsaktens elektroniske procedure, som understøttes af e-CODEX-systemet.

Forretningsprocesmodellen sammen med EU's centrale glossar for e-justice munder ud i XML-skemaer, der beskriver den elektroniske struktur af de digitale proceduremæssige standarder. XML-skemaerne gør det muligt for autoriserede adgangspunkter at sende og modtage dokumenter som fastsat i et instrument for grænseoverskridende retligt samarbejde.

2.4. **e-CODEX-udrulningsaktiver**

e-CODEX-udrulningsaktiver er e-CODEX-komponenter, som udrulles af enheder, der driver et autoriseret e-CODEX-adgangspunkt i deres e-CODEX-miljø. Bortset fra gatewayen skal de distribueres af eu-LISA til de enheder, der driver et autoriseret e-CODEX-adgangspunkt.

Udrulningsaktiverne omfatter:

a) Gateway (punkt 2.4.1)

b) Connector Suite (punkt 2.4.2)

c) e-CODEX-konfigurationspakken (herunder P-modes, offentlige certifikater og sikkerhedsindstillinger) (punkt 2.4.3)

d) Design eller procesmodel for forretningssamarbejdet som en del af de digitale proceduremæssige standarder

e) XML-skemaerne er meddelelsesstrukturer som en del af de digitale proceduremæssige standarder.

2.4.1. ***Gatewayen***

Gatewayen i e-CODEX-systemet er den grundlæggende forudsætning for kommunikationsudveksling. I øjeblikket er følgende standarder implementeret i en gateway:

a) OASIS ([3]) ebMS 3.0-standarden: Interchange-meddelelser mellem gateways i henhold til ebXML-standarden. Denne standard definerer den struktur, som en meddelelsesoverskrift skal have for at kunne forstås af e-CODEX-infrastrukturen.

b) OASIS Applicability Statement 4 (AS4) messaging-profilen: Dette er en overensstemmelsesprofil for OASIS ebMS 3.0-specifikationen

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

c) Den fælles profil for eDelivery AS4-profilen ([4]).

Alle gatewayløsninger, der opfylder disse krav, kan anvendes.

2.4.2. ***Connector Suite***

Konnektoren er en sammenkædende komponent, der forbinder nationale DPS-specifikke applikationer med gatewayens generiske messaging-standarder. Denne komponent tilføjer således følgende funktioner til den grundlæggende kommunikation, der allerede er etableret af gateway-komponenten:

a) **ETSI-REM dokumentation**: Herved forstås dokumentation, der genereres af konnektoren i underskrevet XML-format. Formålet med denne dokumentation er at underrette afsenderen af en meddelelse om, hvorvidt meddelelsen er behandlet eller ej. Dokumentationen genereres og sendes til konnektoren på forskellige trin i meddelelsesprocessen.

b) **TrustOK Token**: Den afsendende konnektor validerer integriteten og ægtheden af forretningsdokumentet i meddelelsen. Resultatet af valideringen er skrevet i TrustOK Token. Denne token genereres af et undermodul til konnektoren: sikkerhedsbiblioteket.

c) **ASiC-S container**: Jf. ETSI Standard EN 319 162-1 on Electronic Signatures and Infrastructures and Associated Signature Containers (ASiC). Containeren sikrer ægtheden og integriteten af de data, som konnektoren overfører.

d) **WS-Security**: For at øge sikkerheden ved overførsel af meddelelser anvender konnektoren WS-Security både på gateway-siden og på siden for det forbundne system. Det betyder, at hver meddelelse, som konnektoren sender eller modtager, bliver krypteret og signeret.

e) **Fælles API**: Konnektoren har en stabil API, som definerer de webtjenester, der anvendes til at oprette forbindelse til gatewayen og de sammenkoblede systemers applikation(er). Strukturen på meddelelser, der udveksles med konnektoren er også beskrevet i konnektorens API.

Ud over selve konnektorsoftwaren indeholder suiten desuden en klientapplikation, der har til formål at understøtte eller erstatte et tilkoblet system til håndtering af meddelelser i e-CODEX-systemet.

Der er også blevet udviklet et plugin specielt til Domibus-gatewayen ([5]) for gøre det muligt at forbinde konnektorens fælles API til gatewayens processorkerne.

2.4.3. ***e-CODEX-konfigurationspakke***

Ved ebMS 3.0-baseret kommunikation finder P-Mode (eller processeringsmodus) anvendelse på overførslen af alle meddelelser i forbindelse med udveksling af en meddelelse mellem to messaging-tjenester. En e-CODEX-konfigurationspakke indeholder en samling af messaging-konfigurationsparametre (filer i P-Mode, adskillige Trusted Certificate Stores, netværksadresser), der i detaljer redegør for, hvordan behandling af meddelelser foregår.

Messaging-konfigurationsparametre kan opdeles i følgende fem kategorier:

a) parametre vedrørende afsenderen, såsom:

   i) identifikatoren for den afsendende part

   ii) certifikatet, som afsenderen anvender til at signere meddelelser

   iii) certificeringsmyndigheder, som afsenderen har tillid til

   iv) netværksadressen (eller -adresserne), hvorfra afsenderen vil indlede kommunikation.

b) Parametre vedrørende modtageren, såsom:

   i) identifikatoren for den modtagende part

   ii) det certifikat, som modtageren forventer vil blive anvendt til at kryptere meddelelser

   iii) certificeringsmyndigheder, som afsenderen har tillid til

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

([5]) Domibus-gatewayen administreres af Kommissionen (https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/Domibus)

iv) netværksadressen (eller -adresserne), hvorfra modtageren vil godkende indgående kommunikation.

c) Parametre vedrørende afsender-modtager-parret, såsom (evt.):

i) aftale-ID, P-Mode-ID

d) Parametre vedrørende de digitale proceduremæssige standarder, såsom:

i) den afsendende parts rolle(r)

ii) den modtagende parts rolle(r)

iii) tjeneste(r)

iv) handling(er) inden for tjenesten.

e) Parametre vedrørende anvendelsen af den meddelelsesoverførende protokol eller den meddelelsesoverførende protokols profil.

I e-CODEX-systemet er alle konfigurationsfiler vedrørende en messaging-tjeneste eller et domæne er samlet i én masterfil, der kan benyttes til konfiguration af gatewayen og konnektoren.

Masterfilen definerer et individuelt kommunikationsnetværk, som messaging-tjenesten kan benytte under sin behandling. Konfigurationen skal genereres centralt, fordi alle oplysninger om samtlige autoriserede e-CODEX-adgangspunkter skal være tilgængelige for at generere e-CODEX-konfigurationspakken, hvilket sker ved hjælp af konfigurationsstyringsværktøjet.

3. SIKKERHED OG METODER TIL VERIFICERING AF INTEGRITET OG ÆGTHED I E-CODEX-SYSTEMET

e-CODEX-systemet er et kommunikationssystem, der giver et solidt grundlag for håndtering af sikkerheds- og databeskyttelseskrav. e-CODEX-systemet giver navnlig de tekniske funktioner, der er nødvendige for at opfylde kravene i Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 ([6]).

3.1. Security by design

e-CODEX-systemet er ud fra et teknisk synspunkt en transportmekanisme. Der er forskellige lag, som er relevante for sikkerheden:

a) netværkslaget

b) transportlaget

c) meddelelseslaget

d) dokumentlaget.

Der anvendes sikkerhedsforanstaltninger på hvert af disse lag.

3.1.1. *Netværkslaget*

e-CODEX-systemet kan anvendes med forskellige former for netværkslag. Det anvendes normalt på almindelige internetforbindelser. Sikkerhed følger derfor de normale sikkerhedsapplikationer for internetteknologi (og udvides med de andre lag, som er beskrevet under dette punkt). I de fleste tilfælde, hvor e-CODEX-systemet anvendes, er et netværkslag tilstrækkeligt. Ved højere sikkerhedskrav kan et ekstra netværkslag også anvendes. Andre netværk kan også komme i betragtning.

3.1.2. *Transportlaget*

Transportlaget er normalt beskyttet af Transport Layer Security (TLS) eller mTLS (gensidig TLS). Dette er en veletableret standard for beskyttelse af transportlaget i internetteknologier og anvendes verden over på en lang række tjenester. TLS/mTLS giver mulighed for kryptering og autentifikation på transportkanaler. Det sikrer transportvejen mellem hver hub på overførselsvejen. Hver hub behøver (kun) at dekryptere adresseoplysningerne for at videresende meddelelsen til den næste hub. Inden videresendelse krypterer den enkelte hub adresseoplysningerne igen. Simpel TLS (én vej) er mulig og anvendes stadig til tider, men tovejs-TLS (mTLS) anbefales, da det er ved at blive den gældende standard for beskyttelse af transportlaget.

([6]) Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF (EUT L 257 af 28.8.2014, s. 73).

3.1.3. ***Meddelelseslaget***

På meddelelseslaget anvendes flere standarder på forskellige e-CODEX-komponenter:

a) Protokollen, der anvendes til overførsel fra gateway til gateway (som meddelelseslaget), er AS4, som signerer og krypterer meddelelserne — afhængigt at sikkerhedskonfigurationen på gateway-niveau.

b) Den centrale komponent i e-CODEX-systemet er konnektoren. Den tilføjer sikkerhed til meddelelseslaget ved hjælp af WS-Security for signering og kryptering af meddelelser til webtjenester over for gatewayen og backend(s). Derfor anvendes der kryptering fra konnektor til konnektor derudover.

c) Til signering og kryptering i forbindelse med alle e-CODEX-systemerne anvendes digitale certifikater. Disse digitale certifikater til kryptering og signering er i overensstemmelse med X.509-standarden.

3.1.4. ***Dokumentlaget***

Meddelelser indeholder dokumenter og vedhæftede filer. Disse bliver pakket i en pakke kaldet en »container«. Containeren bygger på ASiC-S-standarden. Den afsendende konnektor signerer ASiC-S-containeren, og signaturen bliver valideret ved modtagelsen af den modtagende konnektor.

3.2. **Metoder til verificering af integritet og ægthed**

3.2.1. ***Adgang til e-CODEX-konfiguration***

Kommunikation mellem e-CODEX-adgangspunkterne kræver forudgående konfiguration. Denne konfiguration sker via e-CODEX-konfigurationspakken. Konfigurationspakken indeholder adresseoplysninger og oplysninger om den anvendte sikkerhedspolitik samt andre oplysninger. Desuden indeholder den Trusted Stores med de offentlige certifikater for alle deltagende e-CODEX-adgangspunkter. Der oprettes konfigurationsfiler for den enkelte partners konfiguration af en central »konfigurationskoordinator« (CfC) ved hjælp af konfigurationsstyringsværktøjet. Der gives adgang til dette konfigurationsstyringsværktøj, som er begrænset til den enkelte partner alene på personlig og individuel anmodning. Den administrative adgang er begrænset til konfigurationskoordinatorer og skal forvaltes af eu-LISA.

3.2.2. ***Understøttede elektroniske signaturer og segl***

e-CODEX-systemet skal understøtte alle former for elektroniske segl og elektroniske signaturer, jf. forordning (EU) nr. 910/2014.

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

Den afsendende konnektor validerer signaturen på de digitale proceduremæssige standarder i en meddelelse. Resultatet af valideringen er skrevet ind i e-CODEX TrustOK Token. Denne token genereres af et sikkerhedsbibliotek, som er et undermodul til konnektoren. Valideringen af den elektroniske signatur foretages af e-CODEX-konnektoren ved hjælp af digitale signaturtjenester.

3.2.4. ***Maskinlæsbar token (XML)***

Den maskinlæsbare token er en XML-fil, som er underlagt et bestemt skema, der indeholder alle oplysninger om signaturen på den pågældende forretningstoken og valideringsrapporten som følge af den retlige og tekniske validering.

3.2.5. ***Menneskeligt læsbar token (PDF)***

PDF-filen består af tre dele. Den første del, som vises på første side af den aktuelle token, indeholder generelle oplysninger om det avancerede elektroniske system og en vurdering af den juridiske gyldighed af forretningsdokumentet. Derudover vises en ansvarsfraskrivelse og et »godkendelsesstempel«, hvoraf fremgår resultatet af den retlige validering (vellykket/mislykket) nederst på siden.

Et avanceret elektronisk system er et tilkoblet system, der kan identificere brugeren på en sikker måde og sikre integriteten af de meddelelser, der er sendt gennem det mellem klienten og e-CODEX-konnektoren.

Anden del på anden side giver et standardiseret teknisk overblik over oplysningerne fra den oprindelige valideringsrapport. Afhængigt af det tilkoblede system (autentifikations- eller signaturbaseret) varierer oplysningerne i den tekniske oversigt. En signaturbaseret token indeholder oplysninger fra det underliggende certifikat, herunder kendetegn (hvor disse foreligger). En autentifikationsbaseret token indeholder navnet på den institution, hvorfra dokumentet er sendt og, hvor det foreligger, navnet på dokumentets forfatter.

Nederst på denne side er der et stempel i samme farve som dokumentets tekniske valideringsresultat (grøn/gul/rød) og en kort beskrivelse, f.eks. med yderligere oplysninger om, hvorfor et dokument har fået en gul teknisk vurdering.

Tredje del af dokumentet består af den oprindelige valideringsrapport, som den er oprettet af den indberettende medlemsstats valideringssoftware.

4. DIGITALE PROCEDUREMÆSSIGE STANDARDER UDVIKLET TIL DATO

E-justice-service	DPS: procesmodel	DPS: XML-skema	Projektkilde
Europæisk betalingspåkrav	√	√	e-CODEX
Småkrav	√	√	e-CODEX
Den europæiske arrestordre	√	√	e-CODEX
Gebyrer	√	√	e-CODEX
MLA	√	√	e-CODEX
FD 909 (frihedsstraffe)	√	√	e-CODEX
Ægteskabssager	√	√	e-SENS
EU-kendelse til sikring af bankindeståender	√	√	e-SENS
Testamenteregister	√	√	e-SENS
Forkyndelse af dokumenter	√	√	e-CODEX