KOMMISSIONENS GENOMFÖRANDEBESLUT (EU) 2022/2519

av den 20 december 2022

om tekniska specifikationer och standarder för e-Codex-systemet, inbegripet för säkerhet och metoder för kontroll av integritet och äkthet

(Text av betydelse för EES)

EUROPEISKA KOMMISSIONEN HAR ANTAGIT DETTA BESLUT

med beaktande av fördraget om Europeiska unionens funktionssätt,

med beaktande av Europaparlamentets och rådets förordning (EU) 2022/850 av den 30 maj 2022 om ett datoriserat system för gränsöverskridande elektroniskt utbyte av uppgifter på området civil- och straffrättsligt samarbete (e-Codex-systemet) och om ändring av förordning (EU) 2018/1726 ([1]), särskilt artikel 6.1 a, och

av följande skäl:

(1) Enligt artikel 5 i förordning (EU) 2022/850 består e-Codex-systemet av en e-Codex-åtkomstpunkt, standarder för digitala förfaranden samt stödjande programvaruprodukter, dokumentation och andra tillgångar som förtecknas i bilagan till den förordningen.

(2) e-Codex-åtkomstpunkten är sammansatt av en nätsluss som består av programvara, baserad på en gemensam uppsättning protokoll, som möjliggör säkert informationsutbyte via ett telenät med andra nätslussar som använder samma gemensamma uppsättning protokoll samt av en anslutningstjänst som gör det möjligt att koppla anslutna system till nätslussen, som består av programvara, baserad på en gemensam uppsättning öppna protokoll.

(3) För en framgångsrik överlämnande- och övertagandeprocess för e-Codex-systemet till eu-Lisa och för att göra det möjligt för eu-Lisa att fullgöra sina uppgifter, bör man fastställa miniminivåer för de tekniska specifikationer och standarder, inbegripet för säkerhet och metoder för kontroll av integritet och äkthet, som ligger till grund för e-Codex-systemets komponenter.

(4) I enlighet med artiklarna 1 och 2 i protokoll nr 22 om Danmarks ställning, fogat till fördraget om Europeiska unionen och fördraget om Europeiska unionens funktionssätt, deltog Danmark inte i antagandet av förordning (EU) 2022/850, som därför inte är bindande för Danmark, och detta beslut är heller inte tillämpligt på Danmark.

(5) I enlighet med artiklarna 1, 2 och 4a.1 i protokoll nr 21 om Förenade kungarikets och Irlands ställning med avseende på området med frihet, säkerhet och rättvisa, fogat till fördraget om Europeiska unionen och fördraget om Europeiska unionens funktionssätt, och utan att det påverkar tillämpningen av artikel 4 i det protokollet, deltog Irland inte i antagandet av förordning (EU) 2022/850, som därför inte är bindande för Irland, och detta beslut är heller inte tillämpligt på Irland.

(6) Efter samråd i enlighet med artikel 42.1 i Europaparlamentets och rådets förordning (EU) 2018/1725 ([2]) avgav Europeiska datatillsynsmannen ett yttrande den 24 november 2022.

(7) De åtgärder som föreskrivs i detta beslut är förenliga med yttrandet från den kommitté som inrättats genom artikel 19.1 i förordning (EU) 2022/850.

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

([2]) Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG (EUT L 295, 21.11.2018, s. 39).

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

De miniminivåer för de tekniska specifikationer och standarder, inbegripet för säkerhet och metoder för kontroll av integritet och äkthet, som ligger till grund för de komponenter i e-Codex-systemet som avses i artikel 5 i förordning (EU) 2022/850 ska vara de som anges i bilagan till detta beslut.

Artikel 2

Detta beslut träder i kraft den tjugonde dagen efter att det har offentliggjorts i *Europeiska unionens officiella tidning*.

Utfärdat i Bryssel den 20 december 2022.

På kommissionens vägnar
Ursula VON DER LEYEN
Ordförande

BILAGA

Tekniska specifikationer och standarder för e-Codex-systemet, inbegripet för säkerhet och metoder för kontroll av integritet och äkthet

1. **INLEDNING**

I denna bilaga fastställs miniminivåerna för de tekniska specifikationerna och standarderna för e-Codex-systemets komponenter, inbegripet för säkerhet och metoder för kontroll av integritet och äkthet.

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

2.1 Enligt artikel 5 i Europaparlamentets och rådets förordning (EU) 2022/850 ([1]) består e-Codex-systemet av

a) en e-Codex-åtkomstpunkt bestående av

i) en nätsluss,

ii) en anslutningstjänst.

b) standarder för digitala förfaranden,

c) följande stödjande programvaruprodukter, dokumentation och andra tillgångar som förtecknas i bilagan till förordning (EU) 2022/850:

i) Källkoden till den centrala testplattformen (CTP).

ii) Källkoden till Configuration Management Tool (CMT).

iii) Metadata Workbench (MDW).

iv) EU:s basvokabulär inom e-juridik.

v) Arkitekturdokumentation.

2.2 Ur funktionell synpunkt är dessa komponenter indelade i två kategorier: e-Codex-systemets verktygslåda och e-Codex-systemets användbara tillgångar.

2.3 **e-Codex-systemets verktygslåda består av följande:**

a) Arkitekturdokumentationen för e-Codex-systemet.

b) Källkoden till anslutningstjänstens programvarupaket.

c) Källkoden till Configuration Management Tool (CMT).

d) Källkoden till den centrala testplattformen (CTP).

e) Metadata Workbench (MDW)-licens från tredje part.

f) EU:s basvokabulär inom e-juridik.

g) Standarder för digitala förfaranden.

a) Arkitekturdokumentationen för e-Codex-systemet.

Arkitekturdokumentationen är en uppsättning dokument som används för att förse relevanta aktörer med teknisk och informativ kunskap om valet av standarder som andra tillgångar i e-Codex-systemet måste uppfylla. I dokumentationen fastställs de krav och principer som ska tillämpas vid skapandet av interoperabel gränsöverskridande kommunikation för att underlätta elektroniskt utbyte av uppgifter, vilket inbegriper allt innehåll som kan överföras i elektronisk form. Dokumentationen innehåller även en förteckning över utvalda standarder och metoder som e-Codex-systemet bygger på. Arkitekturen garanterar e-Codex-systemets självständighet.

b) Källkoden till anslutningstjänstens programvarupaket

Källkoden till anslutningstjänstens programvarupaket används för att skapa de användbara artefakter som avses i punkt 2.4.2.

([1]) Europaparlamentets och rådets förordning (EU) 2022/850 av den 30 maj 2022 om ett datoriserat system för gränsöverskridande elektroniskt utbyte av uppgifter på området civil- och straffrättsligt samarbete (e-Codex-systemet) och om ändring av förordning (EU) 2018/1726 (EUT L 150, 1.6.2022, s. 1).

c) Configuration Management Tool – CMT

Configuration Management Tool (CMT) är ett webbaserat verktyg för att hantera de konfigurationsfiler som är kopplade till nätslussen för e-Delivery och anslutningstjänsten och tillhandahåller ett standardiserat sätt att hantera arbetsflödet för konfigurering på. Enheter som driver en auktoriserade e-Codex-åtkomstpunkt kan komma åt CMT via en globalt tillgänglig portal och ladda upp sina konfigurationsuppgifter för e-Delivery. De uppladdade uppgifterna ska innehålla information om nätkonfigurationen för nätslussens ändpunkt, alla säkerhetscertifikat som krävs för anslutningen, samt de specifika projekt, miljöer och användningsfall som de medverkar i. CMT ska automatiskt kontrollera giltigheten i de uppladdade uppgifterna och ge återkoppling till enheterna som driver auktoriserade e-Codex-åtkomstpunkter om det uppstår problem.

Om det inkommer ett meddelande om ändring av de uppgifter som lämnats av en enhet som driver en auktoriserad e-Codex-åtkomstpunkt ska ett nytt konfigurationspaket för e-Codex-systemet (se punkt 2.4.3.) genereras med hjälp av detta verktyg. Alla enheter som driver auktoriserade e-Codex-åtkomstpunkter ska meddelas om att det skapats ett nytt konfigurationspaket för e-Codex-systemet och kan när som helst ladda ned det direkt från CMT. CMT kan tillhandahålla konfigurationspaket för e-Codex-systemet till flera IT-miljöer, exempelvis TEST, ACCEPTANCE eller PRODUCTION.

Nya konfigurationspaket för e-Codex-systemet ska börja gälla sju dagar efter att de skapats och enheter som driver auktoriserade e-Codex-åtkomstpunkter ska vid det laget, i tillämpliga fall, ha installerat det nya paketet i sina miljöer.

CMT ska även hålla de enheter som driver auktoriserade e-Codex-åtkomstpunkter informerade om körtiderna för säkerhetscertifikaten och meddela de auktoriserade e-Codex-åtkomstpunkterna på förhand via e-post om certifikatens sista giltighetsdag. Om en enhet som driver en auktoriserad e-Codex-åtkomstpunkt låter säkerhetscertifikatet löpa ut ska denna automatiskt avlägsnas från skapandet av nästa paket.

CMT ska hysas centralt och vara tillgängligt dygnet runt alla dagar i veckan för e-Codex-systemets användare. Support ska vara tillgänglig under kontorstid.

d) Den centrala testplattformen – CTP

Den centrala testplattformen (CTP) för e-Codex-systemet är en automatisk testinfrastruktur. Den gör det möjligt för enheter som driver auktoriserade e-Codex-åtkomstpunkter att utföra anslutningstester och end-to-end-tester mellan sin e-Codex-infrastruktur och en fast central testpunkt utan att någon annan partner (t.ex. en annan auktoriserad e-Codex-åtkomstpunkt) behöver involveras för att testa kommunikationsfunktionerna. Testplattformen gör det även möjligt att skicka och ta emot anpassningsbara testmeddelanden och minskar därmed de insatser som krävs för att testa en e-Codex-infrastruktur både under den inledande testperioden (installationen) och under regressionstestningen. Status för enskilda meddelanden, bevis för registrerad e-post enligt Europeiska institutet för telekommunikationsstandarder (Etsi) samt felloggar spåras och redovisas för de enheter som driver auktoriserade e-Codex-åtkomstpunkter via särskilt utformade visuella processer.

CTP består av en e-Codex-nätsluss, en anslutningstjänst, ett klientprogram för anslutningstjänsten och ett tillhörande webbaserat grafiskt användargränssnitt (för närvarande webbaserad frontend/backend som bygger på Nuxt.js) som kan användas för att skicka meddelanden till en partner nätsluss och för att läsa meddelanden som skickats till CTP via samma nätsluss. För närvarande lagrar CTP viktig driftsinformation (lokala variabler) på en MongoDB-instans och läser av (partens) konfigurationsuppgifter från anslutningstjänstens databas. Därtill används ett REST-programmeringsgränssnitt (REST API) för anslutningstjänstens klientprogram för att hämta information om e-Codex-meddelanden och skicka nya meddelanden till anslutningstjänsten och nätslussen.

För att kunna tillhandahålla en anpassningsbar lösning per e-Codex-miljö driftsätts CTP i olika instanser (kopior) som finns i olika e-Codex-miljöer. Varje instans av CTP drivs för närvarande i en miljö som bygger på Unix (CentOS 7), där alla komponenter samexisterar. Detta underlättar administrationen och åtkomsten till filsystemet, men kan anpassas efter installationer där infrastrukturen för meddelanden i e-Codex är separat.

Varje CTP-användare är ansluten till en (1) nätsluss. Det enda kravet för att använda CTP för testning är att nätslussen för den auktoriserade e-Codex-åtkomstpunkten finns i behandlingsläget för den specifika CMT-miljön.

e) Metadata Workbench

Metadata Workbench är ett verktyg för administration av EU:s basvokabulär inom e-juridik. Verktyget gör det möjligt för de som utformar semantiska modeller att underhålla vokabulären på ett hållbart sätt i enlighet med modelleringsstandarden för tekniska specifikationer för kärnkomponenter såsom den definieras i arkitekturdokumentationen för e-Codex-systemet. Det är en webbaserad programvarutjänst (SaaS) med begränsad åtkomst enbart för administratörer för EU:s basvokabulär inom e-juridik. Metadata Workbench utvecklas och drivs på uppdrag av Nederländernas justitie- och säkerhetsministerium. eu-Lisa får åtkomst till Metadata Workbench inom ramen för ett licensavtal med justitie- och säkerhetsministeriet för att kunna administrera och driva EU:s basvokabulär inom e-juridik.

f) EU:s basvokabulär inom e-juridik

EU:s basvokabulär inom e-juridik är en resurs för återanvändbara semantiska termer och definitioner som används för att säkerställa uppgifternas enhetlighet och kvalitet över tid och inom flera användningsområden. Alla användningsfallsspecifika meddelandestrukturer (XML-scheman) bygger på basvokabulärens semantiska databas.

Framtida versioner av basvokabulären inom e-juridik kan skapas i enlighet med basvokabulärerna ([2]). För att kunna kontrollera överensstämmelse med specifikationen kan en XML-baserad validerare skapas med hjälp av kommissionens provbänk för driftskompatibilitet (*Interoperability Test Bed*).

g) Standarder för digitala förfaranden

En standard för digitala förfaranden är de tekniska specifikationer för verksamhetsmodeller och datascheman som anger den elektroniska strukturen för de uppgifter som utbyts genom e-Codex-systemet baserat på EU:s basvokabulär inom e-juridik. Verksamhetsmodellen beskriver det tekniska genomförandet av det elektroniska förfarandet för det rättsliga instrument som stöds av e-Codex-systemet.

Verksamhetsmodellen och EU:s basvokabulär inom e-juridik utgör grunden till XML-scheman som beskriver den elektroniska strukturen för standarderna för digitala förfaranden. Dessa XML-scheman gör det möjligt för auktoriserade åtkomstpunkter att skicka och ta emot dokument från instrument för gränsöverskridande rättsligt samarbete.

2.4 Användbara tillgångar i e-Codex-systemet

Användbara tillgångar i e-Codex-systemet är de komponenter i e-Codex-systemet som används av enheter som driver auktoriserade e-Codex-åtkomstpunkter i sina e-Codex-miljöer. Med undantag av nätslussen ska dessa distribueras av eu-Lisa till de enheter som driver auktoriserade e-Codex-åtkomstpunkter.

De användbara tillgångarna är följande:

a) Nätslussen (punkt 2.4.1).

b) Anslutningstjänstens programvarupaket (punkt 2.4.2).

c) Konfigurationspaketet för e-Codex-systemet (inbegripet behandlingslägen, öppna certifikat och säkerhetsinställningar) (punkt 2.4.3).

d) Samarbetsmodellen eller verksamhetsmodellen som en del av standarderna för digitala förfaranden.

e) XML-schemana är meddelandestrukturer som en del av standarderna för digitala förfaranden.

2.4.1 *Nätslussen*

Nätslussen i e-Codex-systemet är den byggsten som svarar för det grundläggande kommunikationsutbytet. För närvarande gäller följande standarder för nätslussen:

a) Oasis ([3]) standard ebMS 3.0: Meddelandeutbytet i nätslussen uppfyller ebXML-standarden. Denna standard definierar den struktur som en meddelanderubrik måste ha för att kunna avläsas i e-Codex-infrastrukturen.

b) Oasis fjärde förklaring om tillämplighet (AS4) för meddelandeprofiler: Detta är en överensstämmelseprofil för Oasis specifikation ebMS 3.0.

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

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

c) Den gemensamma profilen för eDelivery AS4-profilen ([4]).

Alla nätslussar som uppfyller dessa krav kan användas.

2.4.2 ***Anslutningstjänstens programvarupaket***

Anslutningstjänsten är en länkningskomponent för att ansluta nationella applikationer som uppfyller standarderna för digitala förfaranden till nätslussens allmänna meddelandestandarder. I och med denna komponent utökas den grundläggande kommunikation som redan inrättats genom nätslusskomponenten med följande funktioner:

a) **Etsi-bevis för registrerad e-post**: Detta är bevis som genereras av anslutningstjänsten i signerat XML-format. Syftet med dessa bevis är att informera avsändaren av ett meddelande om huruvida behandlingen av meddelandet lyckades eller inte. Bevis genereras och skickas av anslutningstjänsten vid olika skeden i meddelandeprocessen.

b) **TrustOK-token**: Den avsändande anslutningstjänsten kontrollerar integriteten och äktheten för affärsdokumentet i meddelandet. Resultatet av denna kontroll uttrycks i form av en TrustOK-token. Denna token genereras via en undermodul till anslutningstjänsten: säkerhetsbiblioteket.

c) **ASiC-S-behållare**: I enlighet med Etsi-standarden EN 319 162–1 om elektroniska underskrifter och infrastrukturer och behållare för tillhörande underskrifter (ASiC). Behållaren säkerställer äktheten och integriteten för den nyttolast som överförs av anslutningstjänsten.

d) **WS-Security**: För att öka säkerheten vid överföring av meddelanden använder anslutningstjänsten WS-Security på både nätslussens sida och det anslutna systemets sida för överföringen. Detta innebär att alla meddelanden som skickas eller tas emot av anslutningstjänsten är krypterade och undertecknade.

e) **Gemensamt API**: Anslutningstjänsten erbjuder ett stabilt API som definierar de webbtjänster som används för att ansluta till nätslussen och de anslutna systemens applikationer. Strukturen för de meddelanden som skickas och tas emot av anslutningstjänsten beskrivs även i anslutningstjänstens API.

Programvarupaketet innehåller utöver själva programvaran för anslutningstjänsten även ett klientprogram vars syfte är att stötta eller ersätta ett anslutet system för hantering av meddelanden i e-Codex-systemet.

Ett insticksprogram har även tagits fram särskilt för nätslussen Domibus ([5]) för att ansluta anslutningstjänstens gemensamma API till nätslussens processorkärna.

2.4.3 ***Konfigurationspaket för e-Codex-systemet***

Vid ebMS 3.0-baserad kommunikation styrs överföringen av alla meddelanden i en meddelandeväxling mellan två meddelandetjänstförvaltare av ett behandlingsläge. Ett konfigurationspaket för e-Codex-systemet omfattar en samling konfigurationsparametrar för meddelanden (behandlingslägesfiler, flera arkiv över betrodda certifikat, nätverksadresser) som anger i detalj hur meddelandeförmedlingen går till.

Konfigurationsparametrarna för meddelanden kan delas in i följande fem kategorier:

a) Parametrar som rör avsändaren, såsom

   i) avsändarens identitet,

   ii) vilket certifikat avsändaren använder för att underteckna meddelanden,

   iii) avsändarens betrodda certifikatutfärdare,

   iv) den eller de nätverksadresser som avsändaren inleder kommunikationen från.

b) Parametrar som rör mottagaren, såsom

   i) mottagarens identitet,

   ii) vilket certifikat mottagaren förväntar sig används för att kryptera meddelanden,

   iii) mottagarens betrodda certifikatutfärdare,

([4]) https://ec.europa.eu/digital-building-blocks/wikis/x/RqbXGw.
([5]) Nätslussen Domibus drivs av kommissionen (https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/Domibus).

iv) den eller de nätverksadresser som mottagaren tar emot kommunikationen på.

c) Parametrar som rör avsändar-mottagarparet, såsom (i tillämpliga fall)

i) identifierare för avtal och behandlingsläge.

d) Parametrar som rör standarderna för digitala förfaranden, såsom

i) avsändarens roller,

ii) mottagarens roller,

iii) tjänster,

iv) åtgärder inom ramen för tjänsten.

e) Parametrar som rör användandet av meddelandeprotokollet, eller profilen för meddelandeprotokollet.

I e-Codex-systemet är alla konfigurationsfiler som rör en meddelandetjänstförvaltare eller domän kombinerade i en huvudfil som kan användas för att konfigurera nätslussen och anslutningstjänsten.

Denna huvudfil definierar ett enskilt kommunikationsnät som meddelandetjänstförvaltaren kan använda vid driften. Konfigurationen måste göras centralt eftersom all information om alla auktoriserade e-Codex-åtkomstpunkter måste vara tillgänglig för CMT för att skapa konfigurationspaketet för e-Codex-systemet.

3. SÄKERHET OCH METODER FÖR KONTROLL AV INTEGRITET OCH ÄKTHET I E-CODEX-SYSTEMET

e-Codex-systemet är ett kommunikationssystem med starkt stöd för att uppfylla kraven på säkerhet och dataskydd. I synnerhet innehåller e-Codex-systemet de tekniska egenskaper som krävs för att uppfylla alla kraven i Europaparlamentets och rådets förordning (EU) 910/2014 ([6]).

3.1 Inbyggd säkerhet

e-Codex-systemet är tekniskt sett en transportmekanism. Det finns följande lager som är relevanta för säkerheten:

a) Ett nätverkslager.

b) Ett transportlager.

c) Ett meddelandelager.

d) Ett dokumentlager.

Säkerhetsåtgärder tillämpas på alla dessa lager.

3.1.1 *Nätverkslagret*

e-Codex-systemet kan användas med olika sorters nätverkslager. Det tillämpas oftast på vanliga internetanslutningar. Därför följer säkerheten de vanliga säkerhetsapplikationerna för internetteknik (och utökas av de övriga lagren som beskrivs i detta avsnitt). För de flesta användningsfall av e-Codex-systemet räcker det med ett sådant nätverkslager. För högre säkerhetskrav kan ytterligare ett nätverkslager tillämpas. Även andra nätverk kan övervägas.

3.1.2 *Transportlagret*

Transportlagret skyddas vanligtvis med Transport Layer Security (TLS) eller ömsesidig TLS (mTLS). Detta är en väletablerad standard för att skydda transportlagret i internetteknik som tillämpas över hela världen på ett stort antal tjänster. TLS/mTLS möjliggör kryptering och autentisering i transportkanalen. Det skyddar transportrutten mellan varje nav i transportrutten. Vid varje nav måste (endast) adressuppgifterna dekrypteras för att skicka meddelandet vidare till nästa nav. Innan meddelandet skickas vidare krypteras adressuppgifterna på nytt av navet. Enkel (enkelriktad) TLS är möjlig och tillämpas ännu ibland, men dubbelriktad TLS (mTLS) rekommenderas, eftersom det håller på att bli den aktuella standarden för skydd av transportlagret.

([6]) Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (EUT L 257, 28.8.2014, s. 73).

3.1.3 ***Meddelandelagret***

På meddelandelagret tillämpas följande standarder av olika komponenter i e-Codex-systemet:

a) Det protokoll som används för överföring mellan nätslussar (som meddelandelager) är AS4, som undertecknar och krypterar meddelandena, beroende på säkerhetskonfigurationen på nätslussnivå.

b) Kärnkomponenten i e-Codex-systemet är anslutningstjänsten. Den skyddar meddelandelagret genom att använda WS-Security för att underteckna och kryptera meddelanden från webbtjänsterna till nätslussen och servrarna. Därför tillämpas även kryptering mellan anslutningstjänster.

c) Digitala certifikat används för underskrift- och krypteringsfunktionen i hela e-Codex-systemet. Dessa digitala certifikat för kryptering och underskrift uppfyller X.509-standarden.

3.1.4 ***Dokumentlagret***

Meddelanden innehåller dokument och bilagor. Dessa förpackas i ett paket som kallas ”behållare”. Behållaren är byggd enligt ASiC-S-standarden. Den avsändande anslutningstjänsten undertecknar ASiC-S-behållaren och underskriften kontrolleras när behållaren tas emot av den mottagande anslutningstjänsten.

3.2 **Metoder för kontroll av integritet och äkthet**

3.2.1 ***Åtkomst till konfigurationen för e-Codex-systemet***

Kommunikationen mellan e-Codex-åtkomstpunkterna behöver förkonfigureras. Denna konfiguration utförs med hjälp av konfigurationspaketet för e-Codex-systemet. Konfigurationspaketet innehåller adressuppgifter, tillämpad säkerhetspolicy och andra uppgifter. Det innehåller även listor över betrodda öppna certifikat för alla deltagande e-Codex-åtkomstpunkter. Konfigurationsfilerna skapas för varje partner konfiguration av en central ”konfigurationssamordnare” med hjälp av Configuration Management Tool (CMT). Åtkomsten till CMT beviljas och begränsas till varje partner endast på personlig och individuell begäran. Administrativ åtkomst ges endast till konfigurationssamordnare och hanteras av eu-Lisa.

3.2.2 ***Stöd för elektroniska underskrifter och stämplar***

e-Codex-systemet ska ha stöd för alla typer av elektroniska stämplar och underskrifter enligt förordning (EU) 910/2014.

3.2.3 ***e-Codex-systemets TrustOK-token***

Den avsändande anslutningstjänsten ska kontrollera meddelandets underskrift för standarderna för digitala förfaranden. Resultatet av denna kontroll uttrycks i e-Codex-systemets TrustOK-token. Denna token genereras via ett säkerhetsbibliotek, som är en undermodul till anslutningstjänsten. Den elektroniska underskriften kontrolleras av anslutningstjänsten för e-Codex-systemet med hjälp av verktyg för digitala underskrifter.

3.2.4 ***Maskinläsbara token (XML)***

Maskinläsbara token kommer i form av XML-filer i ett visst schema som innehåller alla uppgifter om underskriften för berörd verksamhetstoken och valideringsrapporten med resultatet av den rättsliga och tekniska valideringen.

3.2.5 ***Mänskligt läsbar token (PDF)***

PDF-filen består av tre delar. Den första delen som visas på första sidan av token-filen innehåller allmän information om det avancerade elektroniska systemet och en bedömning av affärsdokumentets rättsliga giltighet. Längst ned på sidan visas även en ansvarsfriskrivning och en ”valideringsstämpel” med resultatet av den rättsliga valideringen (godkänt/ej godkänt).

Ett avancerat elektroniskt system är ett anslutet system som på ett säkert sätt kan identifiera användaren och intyga integriteten för de meddelanden som skickas genom systemet mellan klientprogrammet och anslutningstjänsten för e-Codex-systemet.

Den andra delen, på andra sidan, innehåller en standardiserad teknisk översikt över informationen från den ursprungliga valideringsrapporten. Informationen i den tekniska översikten varierar beroende på vilket system som är anslutet (autentiserings- eller underskriftsbaserat). En underskriftsbaserad token innehåller de uppgifter som finns i det underliggande certifikatet, inbegripet attribut (i tillämpliga fall). En autentiseringsbaserad token innehåller namnet på den myndighet som skickat dokumentet och, i tillämpliga fall, namnet på dokumentets författare.

Längst ned på sidan finns en stämpel i den färg som motsvarar resultatet för den tekniska valideringen av dokumentet (grön/gul/röd) och en kort beskrivning, exempelvis ytterligare upplysningar om varför ett dokument har fått gult resultat i den tekniska bedömningen.

Den tredje delen av dokumentet innehåller den ursprungliga valideringsrapporten så som den skapades av den utfärdande medlemsstatens valideringsprogramvara.

4. STANDARDER FÖR DIGITALA FÖRFARANDEN, UTVECKLADE OCH UPPDATERADE

e-juridiktjänsten	Standarder för digitala förfaranden: processmodell	Standarder för digitala förfaranden: XML-schema	Projektkälla
Europeiskt betalningsföreläggande	√	√	e-Codex
Småmål	√	√	e-Codex
Europeisk arresteringsorder	√	√	e-Codex
Straffavgifter	√	√	e-Codex
Ömsesidig rättslig hjälp	√	√	e-Codex
Rambeslut 909 (frihetsberövande åtgärder)	√	√	e-Codex
Äktenskapsmål	√	√	e-Sens
Europeiskt beslut om kvarstad på bankmedel	√	√	e-Sens
Testamentsregister	√	√	e-Sens
Delgivning av handlingar	√	√	e-Codex