IZVEDBENI SKLEP KOMISIJE (EU) 2022/2519

z dne 20. decembra 2022

o tehničnih specifikacijah in standardih za sistem e-CODEX, vključno za varnost ter metode preverjanja celovitosti in avtentičnosti

(Besedilo velja za EGP)

EVROPSKA KOMISIJA JE –

ob upoštevanju Pogodbe o delovanju Evropske unije,

ob upoštevanju Uredbe (EU) 2022/850 Evropskega parlamenta in Sveta z dne 30. maja 2022 o računalniško podprtem sistemu za čezmejno elektronsko izmenjavo podatkov na področju pravosodnega sodelovanja v civilnih in kazenskih zadevah (sistem e-CODEX) ter spremembi Uredbe (EU) 2018/1726 ([1]) in zlasti člena 6(1), točka (a), Uredbe,

ob upoštevanju naslednjega:

(1) V skladu s členom 5 Uredbe (EU) 2022/850 sistem e-CODEX sestavljajo dostopovna točka e-CODEX, digitalni postopkovni standardi ter podporna programska oprema, dokumentacija in druga sredstva iz Priloge k Uredbi.

(2) Dostopovno točko e-CODEX sestavljata prehod, sestavljen iz programske opreme, ki temelji na skupnem sklopu protokolov in omogoča varno izmenjavo informacij prek telekomunikacijskega omrežja z drugimi prehodi z uporabo istega skupnega sklopa protokolov, ter konektor, ki omogoča povezavo povezanih sistemov s prehodom in sestoji iz programske opreme, ki temelji na skupnem sklopu odprtih protokolov.

(3) Za uspešen postopek predaje sistema e-CODEX agenciji eu-LISA in njen prevzem tega sistema ter za omogočanje izpolnjevanja nalog, za katere je odgovorna agencija eu-LISA, bi bilo treba določiti minimalne tehnične specifikacije in standarde, vključno za varnost ter metode preverjanja celovitosti in avtentičnosti, na katerih temeljijo sestavni deli sistema e-CODEX.

(4) V skladu s členoma 1 in 2 Protokola št. 22 o stališču Danske, ki je priložen Pogodbi o Evropski uniji in Pogodbi o delovanju Evropske unije, Danska ni sodelovala pri sprejetju Uredbe (EU) 2022/850, zato ta sklep zanjo ni zavezujoč in se v njej ne uporablja.

(5) V skladu s členoma 1 in 2 ter členom 4a(1) Protokola št. 21 o stališču Združenega kraljestva in Irske glede območja svobode, varnosti in pravice, ki je priložen Pogodbi o Evropski uniji in Pogodbi o delovanju Evropske unije, in brez poseganja v člen 4 navedenega protokola Irska ni sodelovala pri sprejetju Uredbe (EU) 2022/850, zato ta sklep zanjo ni zavezujoč in se v njej ne uporablja.

(6) V skladu s členom 42(1) Uredbe (EU) 2018/1725 Evropskega parlamenta in Sveta ([2]) je bilo opravljeno posvetovanje z Evropskim nadzornikom za varstvo podatkov, ki je mnenje podal 24. novembra 2022.

(7) Ukrepi iz tega sklepa so v skladu z mnenjem odbora, ustanovljenega s členom 19(1) Uredbe (EU) 2022/850 –

([1]) UL L 150, 1.6.2022, str. 1.

([2]) Uredba (EU) 2018/1725 Evropskega parlamenta in Sveta z dne 23. oktobra 2018 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah, organih, uradih in agencijah Unije in o prostem pretoku takih podatkov ter o razveljavitvi Uredbe (ES) št. 45/2001 in Sklepa št. 1247/2002/ES (UL L 295, 21.11.2018, str. 39).

SPREJELA NASLEDNJI SKLEP:

Člen 1

Minimalne tehnične specifikacije in standardi, vključno za varnost ter metode preverjanja celovitosti in avtentičnosti, na katerih temeljijo sestavni deli sistema e-CODEX iz člena 5 Uredbe (EU) 2022/850, se določijo v Prilogi k temu sklepu.

Člen 2

Ta sklep začne veljati dvajseti dan po objavi v *Uradnem listu Evropske unije*.

V Bruslju, 20. decembra 2022

Za Komisijo
predsednica
Ursula VON DER LEYEN

PRILOGA

Tehnične specifikacije in standardi za sistem e-CODEX, vključno za varnost ter metode preverjanja celovitosti in avtentičnosti

1. **UVOD**

Ta priloga določa minimalne tehnične specifikacije in standarde za sestavne dele sistema e-CODEX, vključno za varnost ter metode preverjanja celovitosti in avtentičnosti.

2. **SESTAVNI DELI SISTEMA e-CODEX**

2.1 V skladu s členom 5 Uredbe (EU) 2022/850 Evropskega parlamenta in Sveta ([1]) sistem e-CODEX sestavljajo:

(a) dostopovna točka e-CODEX, ki jo sestavljata:

(i) prehod;

(ii) konektor;

(b) digitalni postopkovni standardi;

(c) podporna programska oprema, dokumentacija in druga sredstva iz Priloge k Uredbi (EU) 2022/850:

(i) izvorna koda osrednje testne platforme;

(ii) izvorna koda orodja za upravljanje konfiguracije Configuration Management Tool (CMT);

(iii) Metadata Workbench (MDW);

(iv) osnovno besedišče e-pravosodja EU;

(v) strukturna dokumentacija.

2.2 S funkcionalnega vidika so ti elementi razdeljeni v dve kategoriji: nabor orodij e-CODEX in namestljiva sredstva e-CODEX.

2.3 **Nabor orodij e-CODEX sestavljajo:**

(a) strukturna dokumentacija e-CODEX;

(b) izvorna koda nabora programske opreme konektorja;

(c) izvorna koda orodja za upravljanje konfiguracije Configuration Management Tool (CMT);

(d) izvorna koda osrednje testne platforme;

(e) licenca za orodje Metadata Workbench (MDW) od tretje osebe;

(f) osnovno besedišče e-pravosodja EU;

(g) digitalni postopkovni standardi (DPS).

(a) Strukturna dokumentacija e-CODEX

Strukturna dokumentacija je nabor dokumentov, ki se uporabljajo za zagotavljanje tehničnega in informativnega znanja ustreznim deležnikom o izbiri standardov, ki jih morajo izpolnjevati druga sredstva sistema e-CODEX. V njej so opredeljene zahteve in načela, ki se uporabljajo pri vzpostavljanju interoperabilne čezmejne komunikacije za lažjo elektronsko izmenjavo podatkov, vključno z vsemi vsebinami, ki se lahko prenašajo v elektronski obliki. Poleg tega so navedeni izbrani standardi in metodologije, na katerih temelji sistem e-CODEX. Struktura zagotavlja avtonomijo sistema e-CODEX.

(b) Izvorna koda nabora programske opreme konektorja

Izvorna koda nabora programske opreme konektorja se uporablja za ustvarjanje namestljivih artefaktov, opisanih v poglavju 2.4.2.

([1]) Uredba (EU) 2022/850 Evropskega parlamenta in Sveta z dne 30. maja 2022 o računalniško podprtem sistemu za čezmejno elektronsko izmenjavo podatkov na področju pravosodnega sodelovanja v civilnih in kazenskih zadevah (sistem e-CODEX) ter spremembi Uredbe (EU) 2018/1726 (UL L 150, 1.6.2022, str. 1).

(c) Orodje za upravljanje konfiguracije Configuration Management Tool (CMT)

CMT je spletno orodje za upravljanje konfiguracijskih datotek, povezanih s prehodom e-dostave in konektorjem, ter zagotavlja standardiziran način za vodenje poteka konfiguracije. Subjekt, ki upravlja odobreno dostopovno točko e-CODEX, lahko do CMT dostopa prek globalno dostopnega prehoda in naloži svoje podatke o konfiguraciji e-dostave. Naloženi podatki morajo vključevati informacije o omrežni konfiguraciji za končno točko prehoda, vsa varnostna potrdila, potrebna za povezavo, ter specifične projekte, okolja in primere uporabe, v katerih sodelujejo. CMT mora samodejno preveriti veljavnost naloženih podatkov in v primeru napak subjektu, ki upravlja odobrene dostopovne točke e-CODEX, sporočiti povratne informacije.

Ko se prejme obvestilo o kakršnih koli spremembah podatkov, ki jih zagotovi subjekt, ki upravlja odobreno dostopovno točko e-CODEX, je treba z uporabo tega orodja pripraviti nov konfiguracijski paket e-CODEX (glej točko 2.4.3). O ustvaritvi novega konfiguracijskega paketa e-CODEX je treba obvestiti vse subjekte, ki upravljajo odobrene dostopovne točke e-CODEX, in ti ga lahko kadar koli prenesejo neposredno s CMT. CMT lahko zagotovi konfiguracijske pakete e-CODEX za več okolij informacijske tehnologije, kot so TEST, SPREJETJE ali PRODUKCIJA.

Novi konfiguracijski paketi e-CODEX se začnejo uporabljati sedem dni po ustvaritvi, subjekti, ki upravljajo odobrene dostopovne točke e-CODEX, pa morajo po potrebi novi paket do takrat namestiti v svojem okolju.

CMT tudi obvešča subjekt, ki upravlja odobrene dostopovne točke e-CODEX, o trajanju varnostnih potrdil in odobrene dostopovne točke e-CODEX po elektronski pošti vnaprej obvesti o bližajočem se izteku veljavnosti potrdila. Če se veljavnost varnostnih potrdil subjekta, ki upravlja odobreno dostopovno točko e-CODEX, izteče, se morajo samodejno odstraniti iz naslednje ustvaritve paketa.

CMT bo gostoval centralno in bo udeležencem sistema e-CODEX stalno na voljo. Podpora pa je omejena na delovni čas.

(d) Osrednja testna platforma

Osrednja testna platforma e-CODEX je avtomatizirana infrastruktura za testiranje. Subjektu, ki upravlja odobreno dostopovno točko e-CODEX, omogoča, da za testiranje komunikacijskih funkcij izvaja teste povezljivosti in teste od konca do konca med svojo infrastrukturo e-CODEX in fiksno centralno testno točko, ne da bi bilo treba vključiti dodatnega partnerja (npr. drugo odobreno dostopovno točko e-CODEX). Omogoča pošiljanje in prejemanje prilagodljivih testnih sporočil ter tako zmanjšuje napor, potreben za testiranje infrastrukture e-CODEX, ob začetnem (namestitev) in regresijskem testiranju. Potek posameznih sporočil, dokazila storitve priporočene elektronske pošte (REM) na podlagi standarda Evropskega inštituta za telekomunikacijske standarde (ETSI) in dnevniki napak se spremljajo in subjektom, ki upravljajo odobrene dostopovne točke e-CODEX, prikažejo z namensko zasnovanimi vizualnimi postopki.

Osrednja testna platforma je sestavljena iz prehoda e-CODEX, konektorja, odjemalca konektorja in povezanega spletnega grafičnega uporabniškega vmesnika (za zdaj spletni čelni/zaledni sistem, ki temelji na Nuxt.js), ki se lahko uporablja za pošiljanje sporočil partnerjevemu prehodu in za ogled sporočil, ki jih isti prehod pošlje osrednji testni platformi. Osrednja testna platforma trenutno shranjuje pomembne operativne informacije (lokalne spremenljivke) na instanci MongoDB in bere informacije (stranke) o konfiguraciji iz podatkovne zbirke konektorjev. Poleg tega za pridobivanje informacij o sporočilih e-CODEX in pošiljanje novih sporočil konektorju in prehodu uporablja vmesnik za aplikacijsko programiranje odjemalca konektorja, in sicer vmesnik tipa REST (prenos reprezentativnega stanja).

Za zagotovitev prilagodljive rešitve v okolju e-CODEX se osrednja testna platforma uporablja v različnih instancah (kopijah), ki obstajajo v različnih okoljih e-CODEX. Vsaka instanca osrednje testne platforme se trenutno uporablja v okolju UNIX (CentOS 7), v katerem soobstajajo vsi sestavni deli. To olajšuje skrbništvo in dostop do datotečnega sistema, vendar se lahko prilagodi za namestitve, v katerih je infrastruktura za pošiljanje sporočil e-CODEX ločena.

Vsak uporabnik centralne testne platforme je povezan z enim (1) prehodom. Edina zahteva za uporabo centralne testne platforme za testiranje je, da prehod zadevne odobrene dostopovne točke e-CODEX obstaja v načinih obdelave za to posebno okolje osrednje testne platforme e-CODEX.

(e) Metadata Workbench

Metadata Workbench je orodje, s katerim se upravlja osnovno besedišče e-pravosodja EU. Semantičnim modelirnikom omogoča, da besedišče vzdržujejo trajnostno in v skladu s standardom modeliranja na podlagi tehničnih specifikacij osnovnih sestavnih delov, kot je opredeljeno v strukturni dokumentaciji e-CODEX. Gre za spletno programsko opremo kot storitev (SaaS), dostop do katere je omejen na skrbnike osnovnega besedišča e-pravosodja EU. Metadata Workbench se razvija in upravlja v imenu nizozemskega ministrstva za pravosodje in varnost. Agenciji eu-LISA bo na podlagi licenčnega sporazuma, ki bo sklenjen med navedenim ministrstvom za pravosodje in varnost ter agencijo eu-LISA, omogočen dostop do orodja Metadata Workbench za upravljanje osnovnega besedišča e-pravosodja EU in skrbništvo nad njim.

(f) Osnovno besedišče e-pravosodja EU

Osnovno besedišče e-pravosodja EU je sredstvo semantičnih izrazov in opredelitev, ki jih je mogoče ponovno uporabiti, in se uporablja za zagotavljanje doslednosti podatkov in njihove kakovosti skozi čas in med različnimi primeri uporabe. Na njegovem semantičnem odložišču temeljijo vse strukture sporočil za posamezne primere uporabe (sheme XML).

Prihodnji razvoj osnovnega besedišča e-pravosodja bi lahko potekal v skladu z osnovnimi besedišči ([2]). Za potrditev skladnosti s specifikacijo bi se lahko z uporabo storitve preizkuševalne naprave za interoperabilnost, ki jo ponuja Komisija, vzpostavil preverjalnik na podlagi XML.

(g) Digitalni postopkovni standardi (DPS)

Digitalni postopkovni standard pomeni tehnične specifikacije za modele poslovnih procesov in podatkovne sheme, ki določajo elektronsko strukturo podatkov, izmenjanih prek sistema e-CODEX, na podlagi osnovnega besedišča e-pravosodja EU. Model poslovnega procesa opisuje tehnično izvajanje elektronskega postopka pravnega instrumenta, ki ga podpira sistem e-CODEX.

Model poslovnega procesa skupaj z osnovnim besediščem e-pravosodja EU zagotavlja sheme XML, ki opisujejo elektronsko strukturo DPS. Sheme XML omogočajo odobrenim dostopovnim točkam pošiljanje in prejemanje dokumentov, kot je določeno v instrumentu čezmejnega pravosodnega sodelovanja.

2.4 Namestljiva sredstva e-CODEX

Namestljiva sredstva e-CODEX so sestavni deli sistema e-CODEX, ki jih v svojem okolju e-CODEX uvedejo subjekti, ki upravljajo odobreno dostopovno točko e-CODEX. Razen prehoda jih bo agencija eu-LISA razdelila subjektom, ki upravljajo odobreno dostopovno točko e-CODEX.

Namestljiva sredstva so:

(a) prehod (točka 2.4.1);

(b) nabor programske opreme konektorja (točka 2.4.2);

(c) konfiguracijski paket e-CODEX (vključno z načini obdelave, javnimi potrdili in varnostnimi nastavitvami) (točka 2.4.3);

(d) zasnova poslovnega sodelovanja ali model procesa v okviru DPS;

(e) sheme XML so strukture sporočil v okviru DPS.

2.4.1 *Prehod*

Prehod v okviru sistema e-CODEX je gradnik, odgovoren za osnovno komunikacijo. Trenutno se na prehodu uporabljajo naslednji standardi:

(a) standard organizacije OASIS ([3]) ebMS 3.0: sporočila za izmenjavo med prehodi, ki so v skladu s standardom ebXML. S tem standardom je opredeljeno, kako mora biti strukturirana glava sporočila, da se razume v okviru infrastrukture e-CODEX;

(b) profil sporočanja AS4 (Applicability Statement 4) organizacije OASIS: to je profil skladnosti specifikacije ebMS 3.0 organizacije OASIS;

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

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

(c) skupni profil profila eDelivery AS4 ([4]).

Za prehod se lahko uporabi vsaka rešitev, ki izpolnjuje te zahteve.

2.4.2 ***Nabor programske opreme konektorja***

Konektor je povezovalni sestavni del za povezavo nacionalnih aplikacij s specifičnimi DPS s splošnimi standardi sporočanja prehoda. V okviru tega ta sestavni del osnovni komunikaciji, ki je že vzpostavljena s sestavnim delom prehoda, dodaja naslednje značilke:

(a) **dokazila ETSI-REM**: to so dokazila, ki jih konektor ustvari v podpisani obliki XML. Namen teh dokazil je obvestiti pošiljatelja sporočila o uspešni ali neuspešni obdelavi sporočila. Konektor ustvarja in pošilja dokazila v različnih fazah obdelave sporočil;

(b) **žeton TrustOK**: konektor pošiljatelj potrdi celovitost in avtentikacijo poslovnega dokumenta v sporočilu. Rezultat te potrditve je zapisan v žetonu TrustOK. Žeton se ustvari s podmodulom konektorja: varnostno knjižnico;

(c) **vsebnik ASiC-S**: v skladu s standardom ETSI EN 319 162-1 o elektronskih podpisih in infrastrukturi ter pripadajočih vsebnikih podpisov (ASiC). Vsebnik zagotavlja avtentičnost in celovitost koristne vsebine, ki jo prenaša konektor;

(d) **WS-Security**: za povečanje varnosti prenosa sporočil konektor uporablja WS-Security za prenos tako na strani prehoda kot tudi na strani povezanega sistema. To pomeni, da je vsako sporočilo, ki ga konektor pošlje ali prejme, šifrirano in podpisano;

(e) **skupni API**: konektor ponuja stabilen vmesnik za aplikacijsko programiranje (API), v katerem so opredeljene spletne storitve, ki se uporabljajo za povezavo s prehodom in aplikacijami povezanih sistemov. Struktura sporočil, ki se izmenjujejo s konektorjem, je opisana tudi v vmesniku API konektorja.

Nabor programske opreme vsebuje poleg same programske opreme konektorja tudi aplikacijski odjemalec, ki je namenjen podpori ali nadomestitvi povezanega sistema za upravljanje sporočanja e-CODEX.

Poleg tega je bil razvit vtičnik posebej za prehod Domibus ([5]), da je skupni vmesnik API konektorja povezan z obdelovalnim jedrom prehoda.

2.4.3 ***Konfiguracijski paket e-CODEX***

V komunikaciji na podlagi ebMS 3.0 način obdelave (imenovan tudi P-Mode) ureja prenos vseh sporočil, ki so del komunikacije med dvema rutinama za obravnavanje sporočanja (messaging service handlers, MSH). Konfiguracijski paket e-CODEX vključuje zbirko parametrov za konfiguracijo sporočanja (datoteke načinov obdelave, več shramb zaupanja vrednih potrdil, omrežni naslovi), ki podrobno določajo, kako poteka sporočanje.

Konfiguracijske parametre sporočanja je mogoče razvrstiti v naslednjih pet kategorij:

(a) parametri, ki se nanašajo na pošiljatelja, kot so:

  (i) identifikator pošiljatelja;

  (ii) potrdilo, ki ga pošiljatelj uporablja za podpisovanje sporočil;

  (iii) overitelji potrdil, ki jim pošiljatelj zaupa;

  (iv) omrežni naslov (ali naslovi), s katerega bo pošiljatelj začel komunikacijo;

(b) parametri, ki se nanašajo na prejemnika, kot so:

  (i) identifikator prejemnika;

  (ii) potrdilo, uporabo katerega prejemnik pričakuje za šifriranje sporočil;

  (iii) overitelji potrdil, ki jim prejemnik zaupa;

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

([5]) Prehod Domibus vzdržuje Komisija (https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/Domibus).

(iv) omrežni naslov (ali naslovi), s katerega bo prejemnik sprejel dohodno komunikacijo;

(c) parametri, ki se nanašajo na par pošiljatelja in prejemnika, kot so:

(i) identifikator dogovora, identifikator načina obdelave;

(d) parametri, ki se nanašajo na DPS, kot so:

(i) vloga(-e) pošiljatelja;

(ii) vloga(-e) prejemnika;

(iii) storitev(-ve);

(iv) ukrep(-i) v okviru storitve;

(e) parametri, povezani z rabo protokola za sporočanje ali profilom protokola za sporočanje.

Vse konfiguracijske datoteke v zvezi z MSH ali domeno so v sistemu e-CODEX združene v eno glavno datoteko, ki se lahko uporabi za konfiguracijo prehoda in konektorja.

V glavni datoteki je opredeljeno posamezno komunikacijsko omrežje, na katero lahko MSH med delovanjem usmeri komunikacijo. Konfiguracijo je treba ustvariti centralno, saj morajo biti za ustvarjanje konfiguracijskega paketa e-CODEX, ki se ustvari z orodjem Configuration Management Tool, na voljo vse informacije o vseh odobrenih dostopovnih točkah e-CODEX.

3. VARNOST IN METODE ZA PREVERJANJE CELOVITOSTI IN AVTENTIČNOSTI SISTEMA E-CODEX

Sistem e-CODEX je komunikacijski sistem, ki zagotavlja močno podporo pri izpolnjevanju zahtev glede varnosti in varstva podatkov. Sistem e-CODEX zlasti zagotavlja tehnične funkcije, potrebne za izpolnjevanje vseh zahtev iz Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta ([6]).

3.1 Vgrajena varnost

Sistem e-CODEX je s tehničnega vidika mehanizem za prenos. Za varnost so pomembne različne plasti:

(a) omrežna plast;

(b) transportna plast;

(c) plast sporočila;

(d) plast dokumenta.

Varnostni ukrepi se uporabljajo na vsaki od teh plasti.

3.1.1 *Omrežna plast*

Sistem e-CODEX se lahko uporablja za različne vrste omrežnih plasti. Običajno se uporablja po rednih internetnih povezavah. Varnost zato sledi običajnim varnostnim rabam internetne tehnologije (in je razširjena z drugimi plastmi, opisanimi v tej točki). Za večino primerov uporabe e-CODEX taka omrežna plast zadostuje. V primeru višjih varnostnih zahtev pa bi se lahko uporabila tudi katera druga omrežna plast. V poštev se lahko vzamejo tudi druga omrežja.

3.1.2 *Transportna plast*

Transportna plast je običajno zaščitena s protokolom TLS ali mTLS. Je uveljavljen standard internetnih tehnologij za zaščito transportne plasti in se po vsem svetu uporablja za številne storitve. TLS/mTLS zagotavlja šifriranje in avtentikacijo na transportnem kanalu. Zagotavlja transportno pot med vsakim zvezdiščem transportne poti. Vsako zvezdišče mora dešifrirati (le) podatke o naslovu, da lahko sporočilo posreduje naslednjemu zvezdišču. Pred posredovanjem sporočila vsako zvezdišče podatke o naslovu znova zašifrira. Enostavna (enosmerna) avtentikacija TLS je mogoča in se včasih še vedno uporablja, vendar se priporoča dvosmerna avtentikacija TLS (mTLS), saj postaja sedanji standard zaščite transportne plasti.

([6]) Uredba (EU) št. 910/2014 Evropskega parlamenta in Sveta z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in o razveljavitvi Direktive 1999/93/ES (UL L 257, 28.8.2014, str. 73).

3.1.3 ***Plast sporočila***

Na plasti sporočila različni sestavni deli e-CODEX uporabljajo različne standarde:

(a) protokol, ki se uporablja za prenos med prehodoma (kot plast sporočila), je AS4, ki podpisuje in šifrira sporočila – odvisno od varnostne konfiguracije na ravni prehoda;

(b) osrednji sestavni del sistema e-CODEX je konektor. Varnost na plasti sporočila povečuje z uporabo protokola WS-Security za podpisovanje in šifriranje sporočil za spletne storitve v smeri prehoda in zalednega(-ih) sistema (-ov). Zato se dodatno uporablja šifriranje med konektorjema;

(c) za funkcijo podpisovanja in šifriranja se v vseh sistemih e-CODEX uporabljajo digitalna potrdila. Ta digitalna potrdila za šifriranje in podpisovanje so skladna s standardom X.509.

3.1.4 ***Plast dokumenta***

Sporočila vsebujejo dokumente in priloge. Ti so pakirani v paket, imenovan „vsebnik“. Vsebnik je strukturiran v skladu s standardom ASiC-S. Konektor, ki sporočilo pošlje, podpiše vsebnik ASiC-S, podpis pa po prejemu potrdi konektor prejemnik.

3.2 **Metode za preverjanje celovitosti in avtentičnosti**

3.2.1 ***Dostop do konfiguracije e-CODEX***

Za komunikacijo med dostopovnimi točkami e-CODEX je potrebna predhodna konfiguracija. Ta konfiguracija poteka prek konfiguracijskega paketa e-CODEX. Konfiguracijski paket vsebuje podatke o naslovih, uporabljeni varnostni politiki in druge informacije. Poleg tega vsebuje tudi shrambe zaupanja vrednih javnih potrdil vseh sodelujočih dostopovnih točk e-CODEX. Konfiguracijske datoteke za vsako konfiguracijo partnerja ustvari osrednji „koordinator za konfiguracijo“ z orodjem Configuration Management Tool. Dostop do tega orodja je omejen na posameznega partnerja in mu je omogočen le na podlagi osebne in individualne zahteve. Skrbniški dostop je omejen na koordinatorje za konfiguracijo, kar ureja agencija eu-LISA.

3.2.2 ***Podprti elektronski podpisi in žigi***

Sistem e-CODEX mora podpirati vse vrste elektronskih žigov in elektronskih podpisov, kot je določeno v Uredbi (EU) št. 910/2014.

3.2.3 ***Žeton TrustOK e-CODEX***

Konektor, ki pošilja sporočilo, potrdi podpis DPS sporočila. Rezultat te potrditve je zapisan v žetonu TrustOK e-CODEX. Žeton ustvari varnostna knjižnica, ki je podmodul konektorja. Potrditev elektronskega podpisa opravi konektor e-CODEX z orodji DSS (digital signature service).

3.2.4 ***Strojno berljiv žeton (XML)***

Strojno berljiv žeton je datoteka XML, na kateri temelji določena shema, ki vsebuje vse informacije o podpisu poslovnega žetona in poročilo o potrditvi na podlagi pravnega in tehničnega potrjevanja.

3.2.5 ***Žeton, ki ga lahko prebere človek (PDF)***

Datoteka PDF je sestavljena iz treh delov. Prvi del, predstavljen na prvi strani dejanskega žetona, vključuje splošne informacije o naprednem elektronskem sistemu in oceno pravne veljavnosti poslovnega dokumenta. Poleg tega sta na dnu strani prikazana izjava o omejitvi odgovornosti in „validacijski žig“, ki prikazuje rezultat pravne potrditve (uspešna/neuspešna).

Napredni elektronski sistem je povezan sistem, ki lahko varno identificira uporabnika in zagotavlja celovitost sporočil, ki se pošiljajo prek njega med odjemalcem in konektorjem e-CODEX.

Drugi del na drugi strani vsebuje standardiziran tehnični pregled informacij iz prvotnega poročila o potrditvi. Informacije, navedene v tehničnem pregledu, se razlikujejo glede na povezani sistem (na podlagi avtentikacije ali podpisa). Žeton, ki temelji na podpisu, vsebuje informacije, ki jih zagotavlja osnovno potrdilo, vključno z atributi (če so na voljo). Žeton, ki temelji na avtentikaciji, vsebuje ime institucije, iz katere je bil dokument poslan, in, če je na voljo, ime avtorja dokumenta.

Spodnji del te strani je sestavljen iz žiga v barvi rezultata tehnične potrditve dokumenta (zelena/rumena/rdeča) in kratkega opisa, npr. z dodatnimi informacijami o tem, zakaj je dokument prejel rumeno tehnično oceno.

Tretji del dokumenta je izvirno poročilo o potrditvi, ki je bilo ustvarjeno s programsko opremo za potrjevanje države članice izdajateljice.

4. DO ZDAJ RAZVITI DIGITALNI POSTOPKOVNI STANDARDI (DPS)

Storitev e-pravosodja	DPS: model procesa	DPS: shema XML	Vir projekta
evropski plačilni nalog	√	√	e-CODEX
spori majhne vrednosti	√	√	e-CODEX
evropski nalog za prijetje	√	√	e-CODEX
denarne kazni	√	√	e-CODEX
medsebojna pravna pomoč	√	√	e-CODEX
Okvirni sklep 909 (zaporne kazni)	√	√	e-CODEX
zakonski spori	√	√	e-SENS
nalog EU za zamrznitev bančnih računov	√	√	e-SENS
register oporok	√	√	e-SENS
vročanje pisanj	√	√	e-CODEX