

PROVEDBENA ODLUKA KOMISIJE (EU) 2022/2519**od 20. prosinca 2022.****o tehničkim specifikacijama i standardima za sustav e-CODEX, među ostalim za sigurnost i metode za provjeru cjelovitosti i autentičnosti****(Tekst značajan za EGP)**

EUROPSKA KOMISIJA,

uzimajući u obzir Ugovor o funkcioniranju Europske unije,

uzimajući u obzir Uredbu (EU) 2022/850 Europskog parlamenta i Vijeća od 30. svibnja 2022. o računalnom sustavu za prekograničnu elektroničku razmjenu podataka u području pravosudne suradnje u građanskim i kaznenim stvarima (sustav e-CODEX) i izmjeni Uredbe (EU) 2018/1726 ⁽¹⁾, a posebno njezin članak 6. stavak 1. točku (a),

budući da:

- (1) U skladu s člankom 5. Uredbe (EU) 2022/850 sustav e-CODEX sastoji se od pristupne točke e-CODEX-a, digitalnih postupovnih standarda i popratnih softverskih proizvoda, dokumentacije i drugih resursa navedenih u Prilogu toj uredbi.
- (2) Pristupna točka e-CODEX-a sastavljena je od pristupnika, koji se sastoji od softvera utemeljenog na zajedničkom skupu protokola, a kojim se omogućuje sigurna razmjena informacija putem telekomunikacijske mreže s drugim pristupnicima koji upotrebljavaju isti zajednički skup protokola, i poveznika, koji omogućuje povezivanje povezanih sustava s pristupnikom i koji se sastoji od softvera utemeljenog na zajedničkom skupu otvorenih protokola.
- (3) Za uspješan proces predaje sustava e-CODEX agenciji eu-LISA te kako bi se omogućilo ispunjavanje zadaća za koje je odgovorna agencija eu-LISA, trebalo bi utvrditi minimalne tehničke specifikacije i standarde, među ostalim za sigurnost i metode za provjeru cjelovitosti i autentičnosti, na kojima se temelje sastavnice sustava e-CODEX.
- (4) U skladu s člancima 1. i 2. Protokola br. 22 o stajalištu Danske, priloženog Ugovoru o Europskoj uniji i Ugovoru o funkcioniranju Europske unije, Danska nije sudjelovala u donošenju Uredbe (EU) 2022/850 te ova Odluka za nju nije obvezujuća niti se na nju primjenjuje.
- (5) U skladu s člancima 1. i 2. te člankom 4.a stavkom 1. Protokola br. 21 o stajalištu Ujedinjene Kraljevine i Irske s obzirom na područje slobode, sigurnosti i pravde, priloženog Ugovoru o Europskoj uniji i Ugovoru o funkcioniranju Europske unije, i ne dovodeći u pitanje članak 4. tog protokola, Irska nije sudjelovala u donošenju Uredbe (EU) 2022/850 te ova Odluka za nju nije obvezujuća niti se na nju primjenjuje.
- (6) Provedeno je savjetovanje s Europskim nadzornikom za zaštitu podataka u skladu s člankom 42. stavkom 1. Uredbe (EU) 2018/1725 Europskog parlamenta i Vijeća ⁽²⁾, koji je dostavio mišljenje 24. studenoga 2022.
- (7) Mjere predviđene u ovoj Odluci u skladu su s mišljenjem odbora osnovanog člankom 19. stavkom 1. Uredbe (EU) 2022/850,

⁽¹⁾ SL L 150, 1.6.2022., str. 1.

⁽²⁾ Uredba (EU) 2018/1725 Europskog parlamenta i Vijeća od 23. listopada 2018. o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama, tijelima, uredima i agencijama Unije i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Uredbe (EZ) br. 45/2001 i Odluke br. 1247/2002/EZ (SL L 295, 21.11.2018., str. 39.).

DONIJELA JE OVU ODLUKU:

Članak 1.

Minimalne tehničke specifikacije i standardi, među ostalim za sigurnost i metode za provjeru cjelovitosti i autentičnosti, na kojima se temelje sastavnice sustava e-CODEX iz članka 5. Uredbe (EU) 2022/850 utvrđeni su u Prilogu ovoj Odluci.

Članak 2.

Ova Odluka stupa na snagu dvadesetog dana od dana objave u *Službenom listu Europske unije*.

Sastavljeno u Bruxellesu 20. prosinca 2022.

Za Komisiju
Predsjednica
Ursula VON DER LEYEN

PRILOG

Tehničke specifikacije i standardi za sustav e-CODEX, među ostalim za sigurnost i metode za provjeru cjelovitosti i autentičnosti**1. UVOD**

U ovom se Prilogu utvrđuju minimalne tehničke specifikacije i standardi za sastavnice sustava e-CODEX, među ostalim za sigurnost i metode za provjeru cjelovitosti i autentičnosti.

2. SASTAVNICE SUSTAVA e-CODEX

2.1 U skladu s člankom 5. Uredbe (EU) 2022/850 Europskog parlamenta i Vijeća ⁽¹⁾ sustav e-CODEX sastoji se od:

(a) pristupna točka e-CODEX-a koja se sastoji od sljedećeg:

- i. pristupnik;
- ii. poveznik;

(b) digitalni postupovni standardi (DPS);

(c) prateći softverski proizvodi, prateća dokumentacija i drugi prateći resursi navedeni u Prilogu Uredbi (EU) 2022/850:

- i. izvorni kod središnje platforme za testiranje (CTP);
- ii. izvorni kod alata za upravljanje konfiguracijom (*Configuration Management Tool*, CMT);
- iii. Metadata Workbench (MDW);
- iv. temeljni rječnik e-pravosuđa EU-a;
- v. dokumentacija o arhitekturi.

2.2 S funkcionalnog stajališta, ti su elementi podijeljeni u dvije kategorije: paket alata e-CODEX-a i resursi koji se mogu rasporediti u e-CODEX.

2.3 Paket alata e-CODEX-a sastoji se od sljedećeg:

(a) dokumentacija o arhitekturi sustava e-CODEX;

(b) izvorni kod paketa poveznika;

(c) izvorni kod alata za upravljanje konfiguracijom (CMT);

(d) izvorni kod središnje platforme za testiranje (CTP);

(e) licencija za Metadata Workbench (MDW) koju izdaje treća strana;

(f) temeljni rječnik e-pravosuđa EU-a;

(g) digitalni postupovni standardi (DPS).

(a) Dokumentacija o arhitekturi sustava e-CODEX

Dokumentacija o arhitekturi je skup dokumenata koji se upotrebljavaju za pružanje tehničkog i informativnog znanja relevantnim dionicima o odabiru standarda s kojima drugi resursi sustava e-CODEX moraju biti usklađeni. Njome se definiraju zahtjevi i načela koji se primjenjuju pri uspostavi interoperabilne prekogranične komunikacije za olakšavanje elektroničke razmjene podataka, što uključuje svaki sadržaj koji se prenosi u elektroničkom obliku. Osim toga, u njoj se navode odabrani standardi i metodologije na kojima se temelji sustav e-CODEX. Arhitekturom se osigurava autonomija sustava e-CODEX.

(b) Izvorni kod paketa poveznika

Izvorni kod paketa poveznika upotrebljava se za stvaranje prenosivih artefakata opisanih u poglavlju 2.4.2.

⁽¹⁾ Uredba (EU) 2022/850 Europskog parlamenta i Vijeća od 30. svibnja 2022. o računalnom sustavu za prekograničnu elektroničku razmjenu podataka u području pravosudne suradnje u građanskim i kaznenim stvarima (sustav e-CODEX) i izmjeni Uredbe (EU) 2018/1726 (SL L 150, 1.6.2022., str. 1.).

(c) Alat za upravljanje konfiguracijom (CMT)

Alat za upravljanje konfiguracijom (CMT) je alat utemeljen na *webu* za upravljanje konfiguracijskim datotekama povezanim s pristupnikom e-dostave i poveznikom te osigurava standardizirano upravljanje radnim tijekom konfiguracije. Subjekt koji upravlja odobrenom pristupnom točkom e-CODEX-a može pristupiti CMT-u putem globalno dostupnog portala i učitati podatke o konfiguraciji e-dostave. Učitani podaci moraju uključivati informacije o mrežnoj konfiguraciji krajnje točke pristupnika, sve sigurnosne certifikate potrebne za povezivanje te konkretne projekte, okruženja i slučajeve upotrebe u kojima subjekt sudjeluje. CMT automatski provjerava valjanost učitanih podataka i pruža povratne informacije subjektu koji upravlja odobrenim pristupnim točkama e-CODEX-a ako dođe do pogrešaka.

Ako se primi obavijest o promjenama podataka koje je dostavio subjekt koji upravlja odobrenom pristupnom točkom e-CODEX-a, s pomoću tog alata se izrađuje novi konfiguracijski paket e-CODEX-a (vidjeti točku 2.4.3.). Svi subjekti koji upravljaju odobrenim pristupnim točkama e-CODEX-a moraju biti obaviješteni o izradi novog konfiguracijskog paketa e-CODEX-a i u svakom trenutku imati mogućnost preuzeti ga izravno s CMT-a. CMT može osigurati konfiguracijske pakete e-CODEX-a za više IT okruženja, kao što su TEST, PRIHVATANJE ili PRODUKCIJA.

Novi konfiguracijski paketi e-CODEX-a moraju se početi upotrebljavati sedam dana nakon njihove izrade, a subjekti koji upravljaju odobrenim pristupnim točkama e-CODEX-a dužni su do tog trenutka instalirati novi paket u svojem okruženju.

Osim toga, CMT redovito obavješćuje subjekt koji upravlja odobrenim pristupnim točkama e-CODEX-a o podstavima *runtime* njegova sigurnosnog certifikata i unaprijed e-porukom obavješćuje odobrene pristupne točke e-CODEX-a o predstojećem isteku certifikata. Ako subjekt koji upravlja odobrenom pristupnom točkom e-CODEX-a dopusti da njegovi sigurnosni certifikati isteknu, automatski se uklanjaju iz sljedećeg paketa.

CMT je smješten na središnjoj lokaciji i dostupan je sudionicima e-CODEX-a 24 sata dnevno svaki dan u tjednu. Podrška je ograničena na uobičajeno radno vrijeme.

(d) Središnja platforma za testiranje (CTP)

Središnja platforma za testiranje e-CODEX-a (CTP) infrastruktura je za automatizirano testiranje. Njome se subjektu koji upravlja odobrenom pristupnom točkom e-CODEX-a omogućuje da provodi testove povezivosti i cjelovite testove između svoje infrastrukture e-CODEX-a i fiksne središnje točke za testiranje, a da pritom nije potrebno uključiti nekog drugog partnera (npr. drugu odobrenu pristupnu točku e-CODEX-a) za testiranje komunikacijskih funkcija. Omogućuje slanje i primanje poruka o testiranju koje se mogu prilagoditi, čime se olakšava rad pri inicijalnom (instalacija) i regresijskom testiranju infrastrukture e-CODEX-a. Napredak u slanju pojedinačnih poruka te dokazi i popis pogrešaka registrirane elektroničke pošte (REM) Europskog instituta za telekomunikacijske norme (ETSI) prate se i predstavljaju subjektima koji upravljaju odobrenim pristupnim točkama e-CODEX-a s pomoću posebno osmišljenih vizualnih procesa.

CTP se sastoji od pristupnika e-CODEX-a, poveznika, klijenta poveznika i povezanog internetskog grafičkog korisničkog sučelja (za sada *web* sučelje/pozadina izgrađena na Nuxt.js) koje se može upotrebljavati za slanje poruka partnerskom pristupniku te za pregledavanje poruka koje isti pristupnik šalje CTP-u. Na CTP-u se trenutačno pohranjuju važne operativne informacije (lokalne varijable) na instanci MongoDB i očitavaju konfiguracijske informacije (koje se odnose na jednu od strana) iz baze podataka poveznika. Osim toga, upotrebljava se sučelje za programiranje aplikacija (API) reprezentativnog prijenosa stanja (REST) klijenta poveznika za dohvaćanje informacija o porukama e-CODEX-a i slanje novih poruka povezniku i pristupniku.

Kako bi se osiguralo rješenje koje se može prilagoditi svakom okruženju e-CODEX-a, CTP se upotrebljava u različitim instancama (kopijama) koje postoje u različitim okruženjima e-CODEX-a. Svaka instanca CTP-a trenutačno se primjenjuje u okruženju UNIX-a (CentOS 7), u kojem su prisutne sve sastavnice. To olakšava administraciju i pristup sustavu datoteka, ali se može prilagoditi kako bi se obuhvatile instalacije u kojima je infrastruktura za razmjenu poruka e-CODEX-a odvojena.

Svaki korisnik CTP-a povezan je s jednim (1) pristupnikom. Za upotrebu CTP-a za testiranje jedini je zahtjev da pristupnik te odobrene pristupne točke e-CODEX-a postoji u načinima obrade (P-Mode) za to specifično okruženje CMT-a e-CODEX-a.

(e) Metadata Workbench

Metadata Workbench alat je kojim se upravlja temeljnim rječnikom e-pravosuđa EU-a. Omogućuje stručnjacima za semantičko modeliranje da održavaju rječnik na održiv način u skladu sa standardom modeliranja tehničke specifikacije jezgrene sastavnice kako je definirano u dokumentaciji o arhitekturi e-CODEX-a. Riječ je o softveru kao usluzi (SaaS) utemeljenom na *webu* s pristupom temeljnom rječniku e-pravosuđa EU-a ograničenim samo na administratore. Metadata Workbench razvija se i njime se upravlja u ime Ministarstva pravosuđa i sigurnosti Nizozemske. Na temelju sporazuma o licenciranju koji će sklopiti Ministarstvo pravosuđa i sigurnosti i agencija eu-LISA, agenciji eu-LISA odobrit će se pristup Metadata Workbenchu kako bi upravljala i rukovala temeljnim rječnikom e-pravosuđa EU-a.

(f) Temeljni rječnik e-pravosuđa EU-a

Temeljni rječnik e-pravosuđa EU-a je resurs za semantičke pojmove i definicije koji se mogu ponovno upotrijebiti koji se rabi kako bi se osigurala trajna dosljednost i kvaliteta podataka u svim scenarijima upotrebe. Na njegovu se semantičkom repozitoriju temelje sve strukture poruka specifične za određeni slučaj upotrebe (XML sheme).

Budući razvoj temeljnog rječnika e-pravosuđa mogao bi se provesti u skladu s temeljnim rječnicima ^(?). Kako bi se potvrdila sukladnost sa specifikacijom, mogao bi se uspostaviti validator temeljen na XML-u s pomoću usluge testa interoperabilnosti koju nudi Komisija.

(g) Digitalni postupovni standardi (DPS)

Digitalni postupovni standard znači tehničke specifikacije za modele poslovnih procesa i sheme podataka kojima se određuje elektronička struktura podataka razmijenjenih putem sustava e-CODEX na osnovi temeljnog rječnika e-pravosuđa EU-a. Model poslovnih procesa opisuje tehničku provedbu elektroničkog postupka pravnog instrumenta koji se podupire sustavom e-CODEX.

XML sheme utemeljene na modelu poslovnih procesa i temeljnom rječniku e-pravosuđa EU-a opisuju elektroničku strukturu DPS-a. One omogućuju odobrenim pristupnim točkama slanje i primanje dokumenata u skladu s instrumentom za prekograničnu pravosudnu suradnju.

2.4 Resursi koji se mogu rasporediti u okviru e-CODEX-a

Resursi koji se mogu rasporediti u okviru e-CODEX-a su sastavnice e-CODEX-a koje u svojem okruženju e-CODEX-a raspoređuju subjekti koji upravljaju odobrenom pristupnom točkom e-CODEX-a. Isključujući pristupnik, eu-LISA će ih distribuirati subjektima koji upravljaju odobrenom pristupnom točkom e-CODEX-a.

Resursi koji se mogu rasporediti su sljedeći:

- (a) pristupnik (točka 2.4.1.);
- (b) izvorni kod paketa poveznika (točka 2.4.2.);
- (c) konfiguracijski paket e-CODEX-a (uključujući načine obrade, javne potvrde i sigurnosne postavke) (točka 2.4.3.);
- (d) oblik poslovne suradnje ili model procesa kao dio DPS-a;
- (e) XML sheme su strukture poruke kao dio DPS-a.

2.4.1 Pristupnik

Pristupnik u sustavu e-CODEX element je odgovoran za osnovnu komunikacijsku razmjenu. Trenutačno se primjenjuju sljedeći standardi pristupnika:

- (a) standard OASIS ^(?) ebMS 3.0: Poruke za razmjenu između pristupnika koje su u skladu sa standardom ebXML. Tim se standardom definira struktura koju zaglavlje poruke mora imati kako bi se moglo razumjeti u okviru infrastrukture e-CODEX-a;
- (b) profil za razmjenu poruka OASIS Applicability Statement 4 (AS4): Ovo je profil usklađenosti specifikacije OASIS ebMS 3.0;

^(?) <https://joinup.ec.europa.eu/collection/semantic-interoperability-community-semic/core-vocabularies>

^(?) Organizacija za unaprjeđivanje strukturiranih informacijskih normi.

(c) zajednički profil profila eDelivery AS4 ⁽⁴⁾.

Može se upotrijebiti svako rješenje za pristupnik koje ispunjava te zahtjeve.

2.4.2 **Paket poveznika**

Poveznik je povezujuća sastavnica koja povezuje nacionalne posebne aplikacije DPS-a s generičkim standardima za razmjenu poruka pristupnika. Stoga se tom sastavnicom u osnovnu komunikaciju koja je već uspostavljena sastavnicom pristupnika dodaju sljedeće značajke:

- (a) **dokazi ETSI-REM**: to su dokazi koje generira poveznik u potpisanom XML formatu. Svrha je tih dokaza obavijestiti pošiljatelja o uspješnoj ili neuspješnoj obradi poruke. Poveznik generira i podnosi dokaze u različitim fazama obrade poruke;
- (b) **token TrustOK**: poveznik pošiljatelja validira cjelovitost i autentičnost poslovnog dokumenta u poruci. Ishod te validacije sadržava Token TrustOK. Taj se token generira u podmodulu poveznika: sigurnosnoj biblioteci;
- (c) **spremnik ASIC-S**: u skladu s normom ETSI EN 319 162-1 Elektronički potpisi i infrastrukture; pridruženi spremnici potpisa (ASIC) (*Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC)*). Spremnik osigurava autentičnost i cjelovitost korisnih podataka koje prenosi poveznik;
- (d) **WS-Security**: kako bi se povećala sigurnost prijenosa poruka, poveznik upotrebljava WS-Security na strani pristupnika, kao i povezani sustav za prijenos. To znači da je svaka poruka koju poveznik šalje ili prima šifrirana i potpisana;
- (e) **zajedničko sučelje za programiranje aplikacija (zajednički API)**: poveznik nudi stabilan API koji definira web servise koji se upotrebljavaju za povezivanje s pristupnikom i aplikacijama povezanih sustava. Struktura poruka koje se razmjenjuju s poveznikom opisana je i u API-ju poveznika.

Osim samog softvera poveznika, paket sadržava i klijent aplikacije koji je namijenjen podupiranju ili zamjeni povezanog sustava za obradu poruka e-CODEX-a.

Osim toga, posebno je razvijen dodatak za pristupnik Domibus ⁽⁵⁾ radi povezivanja zajedničkog API-ja poveznika s procesorskom jezgrom pristupnika.

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

U komunikaciji koja se temelji na ebMS-u 3.0, način obrade (P-Mode) upravlja prijenosom svih poruka uključenih u razmjenu poruka između dvaju uređaja za upravljanje servisom za razmjenu poruka (*Messaging Service Handlers, MSH*). Konfiguracijski paket e-CODEX-a uključuje skup parametara konfiguracije za razmjenu poruka (datoteke načina obrade, nekoliko pohrana pouzdanih certifikata, mrežne adrese) kojima se detaljno određuje način slanja poruka.

Parametri konfiguracije za razmjenu poruka mogu se razvrstati u sljedećih pet kategorija:

- (a) parametri koji se odnose na pošiljatelja, kao što su:
 - i. identifikacijska oznaka pošiljatelja;
 - ii. certifikat koji pošiljatelj upotrebljava za potpisivanje poruka;
 - iii. tijela nadležna za izdavanje certifikata kojima pošiljatelj vjeruje;
 - iv. mrežna adresa (ili adrese) s koje će pošiljatelj započeti komunikaciju;
- (b) parametri koji se odnose na primatelja, kao što su:
 - i. identifikacijska oznaka primatelja;
 - ii. certifikat za koji primatelj očekuje da će se koristiti za šifriranje poruka;
 - iii. tijela nadležna za izdavanje certifikata kojima pošiljatelj vjeruje;

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

⁽⁵⁾ Pristupnik Domibus održava Komisija (<https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/Domibus>).

- iv. mrežna adresa (ili adrese) na kojoj će primatelj prihvatiti dolaznu komunikaciju;
- (c) parametri koji se odnose zajednički na pošiljatelja i primatelja, kao što su (ako se koriste):
 - i. identifikacijska oznaka sporazuma, identifikacijska oznaka načina obrade;
- (d) parametri koji se odnose na DPS, kao što su:
 - i. uloge pošiljatelja;
 - ii. uloge primatelja;
 - iii. usluge;
 - iv. radnje unutar servisa;
- (e) parametri koji se odnose na upotrebu protokola za razmjenu poruka ili profil protokola za razmjenu poruka.

U e-CODEX-u sve konfiguracijske datoteke koje se odnose na MSH ili domenu objedinjene su u jednu glavnu datoteku koja se može upotrijebiti za konfiguraciju pristupnika i poveznika.

Glavna datoteka definira pojedinačnu komunikacijsku mrežu koju MSH može primijeniti tijekom svojeg rada. Konfiguraciju je potrebno generirati na središnjoj razini jer sve informacije o svim odobrenim pristupnim točkama e-CODEX-a moraju biti dostupne za generiranje konfiguracijskog paketa e-CODEX-a koji izrađuje CMT.

3. SIGURNOST I METODE ZA PROVJERU CJELOVITOSTI I AUTENTIČNOSTI SUSTAVA E-CODEX

Sustav e-CODEX je komunikacijski sustav koji pruža snažnu potporu ispunjavanju zahtjeva u pogledu sigurnosti i zaštite podataka. Konkretno, sustav e-CODEX ima tehničke značajke potrebne za ispunjavanje svih zahtjeva iz Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća ⁽⁹⁾.

3.1 Integrirana sigurnost

Sustav e-CODEX je, s tehničkog stajališta, mehanizam prijenosa. Postoje različiti slojevi relevantni za sigurnost:

- (a) sloj mreže;
- (b) sloj prijenosa;
- (c) sloj poruke;
- (d) sloj dokumenta.

Na svakom od tih slojeva primjenjuju se sigurnosne mjere.

3.1.1 Sloj mreže

e-CODEX može se upotrebljavati s različitim vrstama slojeva mreže. Obično se primjenjuje na redovite internetske veze. U okviru sigurnosti stoga se primjenjuju uobičajene sigurnosne aplikacije internetske tehnologije (i proširuje se drugim slojevima opisanima u ovoj točki). Za većinu slučajeva upotrebe e-CODEX-a takav je sloj mreže dovoljan. Za strože sigurnosne zahtjeve mogao bi se primijeniti i još jedan sloj mreže. Mogu se uzeti u obzir i druge mreže.

3.1.2 Sloj prijenosa

Sloj prijenosa obično ima zaštitu Transport Layer Security (TLS) ili mTLS (uzajamni TLS). To je dobro uhodan standard za zaštitu sloja prijenosa u internetskim tehnologijama koji se u cijelom svijetu primjenjuje na velik broj usluga. TLS/mTLS omogućuje šifriranje i autentifikaciju na prijenosnom kanalu. Njime se osigurava ruta prijenosa između svakog čvorišta rute prijenosa. Svako čvorište mora dešifrirati (samo) podatke o adresi kako bi se poruka prosljedila sljedećem čvorištu. Prije prosljeđivanja svako čvorište ponovno šifrira podatke o adresi. Jednostavan (jednosmjern) TLS moguć je i ponekad se i dalje primjenjuje, ali se preporučuje dvosmjerni (TLS) (mTLS) jer postaje trenutni standard zaštite sloja prijenosa.

⁽⁹⁾ Uredba (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ (SL L 257, 28.8.2014., str. 73.).

3.1.3 **Sloj poruke**

Kad je riječ o sloju poruke, različite sastavnice sustava e-CODEX primjenjuju nekoliko standarda:

- (a) protokol koji se upotrebljava za prijenos između pristupnika (kao sloj poruke) jest AS4 kojim se potpisuju i šifriraju poruke, ovisno o sigurnosnoj konfiguraciji na razini pristupnika;
- (b) jezgrena sastavnica sustava e-CODEX je poveznik. Njime se dodaje sigurnost sloju poruke upotrebom sustava WS-Security za potpisivanje i šifriranje poruka za web servise prema pristupniku i pozadinama. Stoga se dodatno primjenjuje šifriranje između poveznika;
- (c) za potpisivanje i šifriranje u svim sustavima e-CODEX upotrebljavaju se digitalni certifikati. Ti digitalni certifikati za šifriranje i potpisivanje u skladu su sa standardom X.509.

3.1.4 **Sloj dokumenta**

Poruke sadržavaju dokumente i priloge. Oni se pakiraju u paket koji se naziva „spremnik”. Spremnik je izrađen u skladu s normom ASiC-S. Poveznik pošiljatelja potpisuje spremnik ASiC-S-a, a poveznik primatelja po primitku validira potpis.

3.2 **Metode za provjeru cjelovitosti i autentičnosti**

3.2.1 **Pristup konfiguraciji e-CODEX-a**

Za komunikaciju među pristupnim točkama e-CODEX-a potrebna je prethodna konfiguracija. Konfiguracija se provodi putem konfiguracijskog paketa e-CODEX-a. Konfiguracijski paket sadržava podatke o adresama, primijenjenu sigurnosnu politiku i druge informacije. Nadalje, sadržava i pohrane s pouzdanim javnim certifikatima svih uključenih pristupnih točaka e-CODEX-a. Konfiguracijske datoteke za konfiguraciju svakog partnera izrađuje središnji „koordinator za konfiguraciju” (CfC) s pomoću alata za upravljanje konfiguracijom (CMT). Pristup tom CMT-u omogućuje se i ograničava svakom partneru samo na osobni i pojedinačni zahtjev. Administrativni pristup ograničen je na CfC-ove, a njime upravlja eu-LISA.

3.2.2 **Podržani elektronički potpisi i pečati**

Sustavom e-CODEX podupiru se sve vrste elektroničkih pečata i elektroničkih potpisa kako je predviđeno Uredbom (EU) br. 910/2014.

3.2.3 **Token TrustOK e-CODEX-a**

Poveznik pošiljatelja validira potpis DPS-a poruke. Ishod te validacije sadržava token TrustOK e-CODEX-a. Taj se token generira u sigurnosnoj biblioteci koja je podmodul poveznika. Elektronički potpis validira poveznik e-CODEX-a s pomoću alata DSS-a (*digital signature service*, usluga digitalnog potpisa).

3.2.4 **Strojno čitljiv token (XML)**

Strojno čitljiv token dolazi kao XML datoteka na kojoj se temelji određena shema koja sadržava sve informacije o potpisivanju poslovnog tokena i izvješću o validaciji kao rezultat pravne i tehničke validacije.

3.2.5 **Token čitljiv čovjeku (PDF)**

PDF datoteka sastoji se od tri dijela. Prvi dio prikazan na prvoj stranici stvarnog tokena uključuje opće informacije o naprednom elektroničkom sustavu i ocjenu pravne valjanosti poslovnog dokumenta. Osim toga, na dnu stranice prikazani su izjava o ograničenju odgovornosti i „validacijski pečat” koji prikazuju rezultat pravne validacije (uspješan/neuspješan).

Napredni elektronički sustav povezani je sustav koji može sigurno identificirati korisnika i osigurati cjelovitost poruka koje se putem njega šalju između klijenta i poveznika e-CODEX-a.

Drugi dio na drugoj stranici sadržava standardizirani tehnički pregled informacija iz izvornog izvješća o validaciji. Informacije navedene u tehničkom pregledu razlikuju se ovisno o povezanom sustavu (na temelju autentifikacije ili potpisa). Token koji se temelji na potpisu sadržava informacije iz osnovnog certifikata, uključujući atribute (ako su dostupni). Token koji se temelji na autentifikaciji sadržava ime institucije iz koje je dokument poslan i, ako je dostavljeno, ime autora dokumenta.

Dno ove stranice sastoji se od pečata u boji rezultata tehničke validacije dokumenata (zeleno/žuto/crveno) i kratkog opisa, npr. navođenja dodatnih informacija o tome zašto je dokument dobio žutu tehničku ocjenu.

Treći dio dokumenta sastoji se od izvornog izvješća o validaciji jer ga je izradio softver za validaciju države članice izdavateljice.

4. AŽURIRANI DIGITALNI POSTUPOVNI STANDARDI (DPS)

Služba za e-pravosuđe	DPS: model postupka	DPS: XML shema	Izvor projekta
Europski platni nalog	√	√	e-CODEX
Sporovi male vrijednosti	√	√	e-CODEX
Europski uhidbeni nalog	√	√	e-CODEX
Novčane kazne	√	√	e-CODEX
Uzajamna pravna pomoć	√	√	e-CODEX
Okvirna odluka 909 (kazne zatvora)	√	√	e-CODEX
Bračni sporovi	√	√	e-SENS
EU-ov nalog za blokadu računa	√	√	e-SENS
Registar oporuka	√	√	e-SENS
Dostava pismena	√	√	e-CODEX