KOMISIJOS ĮGYVENDINIMO SPRENDIMAS (ES) 2022/2519

2022 m. gruodžio 20 d.

dėl sistemos e. CODEX techninių specifikacijų ir standartų, be kita ko, susijusių su saugumu ir vientisumo bei autentiškumo tikrinimo metodais

(Tekstas svarbus EEE)

EUROPOS KOMISIJA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo,

atsižvelgdama į 2022 m. gegužės 30 d. Europos Parlamento ir Tarybos reglamentą (ES) 2022/850 dėl tarpvalstybinio elektroninio keitimosi duomenimis teisminio bendradarbiavimo civilinėse ir baudžiamosiose bylose srityje kompiuterinės sistemos (sistemos e. CODEX), kuriuo iš dalies keičiamas Reglamentas (ES) 2018/1726 ([1]), ypač į jo 6 straipsnio 1 dalies a punktą,

kadangi:

(1) pagal Reglamento (ES) 2022/850 5 straipsnį sistemą e. CODEX sudaro sistemos e. CODEX prieigos taškas, skaitmeniniai procedūrų standartai ir to reglamento priede išvardyti pagalbinės programinės įrangos produktai, dokumentai bei kiti ištekliai;

(2) sistemos e. CODEX prieigos tašką sudaro tinklų sietuvas, kurį sudaro programinė įranga, grindžiama bendru protokolų rinkiniu, kad būtų galima saugiai keistis informacija telekomunikacijų tinklu su kitais tinklų sietuvais, kuriems taikomas tas pats bendras protokolų rinkinys, ir jungtis, kuri leidžia sujungtąsias sistemas sujungti su tinklų sietuvu; jungtį sudaro programinė įranga, grindžiama bendru atvirųjų protokolų rinkiniu;

(3) kad sistema e. CODEX būtų sėkmingai perduota agentūrai eu-LISA ir ji ją sėkmingai perimtų, ir kad agentūra eu-LISA galėtų vykdyti užduotis, už kurias ji atsakinga, turėtų būti nustatytos minimalios techninės specifikacijos ir standartai, be kita ko, susiję su saugumu ir vientisumo bei autentiškumo tikrinimo metodais, kuriais grindžiami sistemos e. CODEX komponentai;

(4) pagal prie Europos Sąjungos sutarties ir Sutarties dėl Europos Sąjungos veikimo pridėto Protokolo Nr. 22 dėl Danijos pozicijos 1 ir 2 straipsnius Danija nedalyvavo priimant Reglamentą (ES) 2022/850, todėl šis sprendimas jai nėra privalomas ar taikomas;

(5) pagal prie Europos Sąjungos sutarties ir Sutarties dėl Europos Sąjungos veikimo pridėto Protokolo Nr. 21 dėl Jungtinės Karalystės ir Airijos pozicijos dėl laisvės, saugumo ir teisingumo erdvės 1 ir 2 straipsnius ir 4a straipsnio 1 dalį ir nedarant poveikio to protokolo 4 straipsniui, Airija nedalyvavo priimant Reglamentą (ES) 2022/850, todėl šis sprendimas jai nėra privalomas ar taikomas;

(6) vadovaujantis Europos Parlamento ir Tarybos reglamento (ES) 2018/1725 ([2]) 42 straipsnio 1 dalimi, buvo konsultuojamasi su Europos duomenų apsaugos priežiūros pareigūnu ir jis 2022 m. lapkričio 24 d. pateikė nuomonę;

(7) šiame sprendime numatytos priemonės atitinka pagal Reglamento (ES) 2022/850 19 straipsnio 1 dalį įsteigto komiteto nuomonę,

([1]) OL L 150, 2022 6 1, p. 1.

([2]) 2018 m. spalio 23 d. Europos Parlamento ir Tarybos reglamentas (ES) 2018/1725 dėl fizinių asmenų apsaugos Sąjungos institucijoms, organams, tarnyboms ir agentūroms tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, kuriuo panaikinamas Reglamentas (EB) Nr. 45/2001 ir Sprendimas Nr. 1247/2002/EB (OL L 295, 2018 11 21, p. 39).

PRIĖMĖ ŠĮ SPRENDIMĄ:

1 straipsnis

Minimalios techninės specifikacijos ir standartai, be kita ko, susiję su saugumu ir vientisumo bei autentiškumo tikrinimo metodais, kuriais grindžiami sistemos e. CODEX komponentai, nurodyti Reglamento (ES) 2022/850 5 straipsnyje, nustatomi šio sprendimo priede.

2 straipsnis

Šis sprendimas įsigalioja dvidešimtą dieną po jo paskelbimo *Europos Sąjungos oficialiajame leidinyje*.

Priimta Briuselyje 2022 m. gruodžio 20 d.

Komisijos vardu
Pirmininkė
Ursula VON DER LEYEN

PRIEDAS

Sistemos e. CODEX techninės specifikacijos ir standartai, be kita ko, susiję su saugumu ir vientisumo bei autentiškumo tikrinimo metodais

1. **ĮVADAS**

Šiame priede nustatomos minimalios e. CODEX komponentų techninės specifikacijos ir standartai, be kita ko, susiję su saugumu ir vientisumo bei autentiškumo tikrinimo metodais.

2. **SISTEMOS e. CODEX KOMPONENTAI**

2.1. Pagal Europos Parlamento ir Tarybos reglamento (ES) 2022/850 ([1]) 5 straipsnį sistemą e. CODEX sudaro:

a) e. CODEX prieigos taškas, kurį sudaro:

i) tinklų sietuvas;

ii) jungtis;

b) skaitmeniniai procedūrų standartai (DPS);

c) pagalbinės programinės įrangos produktai, dokumentai ir kiti ištekliai, išvardyti Reglamento (ES) 2022/850 priede:

i) centrinės testavimo platformos (CTP) išeitinis kodas;

ii) konfigūracijos valdymo priemonės (CMT) išeitinis kodas;

iii) „Metadata Workbench“ (MDW);

iv) ES e. teisingumo bazinis žodynas;

v) architektūros dokumentai.

2.2. Funkciniu požiūriu šie elementai skirstomi į dvi kategorijas: sistemos e. CODEX priemonių rinkinį ir sistemos e. CODEX naudotinus išteklius.

2.3. **Sistemos e. CODEX priemonių rinkinį sudaro:**

a) sistemos e. CODEX architektūros dokumentai;

b) jungties paketo išeitinis kodas;

c) konfigūracijos valdymo priemonės (CMT) išeitinis kodas;

d) Centrinės testavimo platformos (CTP) išeitinis kodas;

e) trečiosios šalies išduota „Metadata Workbench“ (MDW) licencija;

f) ES e. teisingumo bazinis žodynas;

g) skaitmeniniai procedūrų standartai (DPS).

a) Sistemos e. CODEX architektūros dokumentai

Architektūros dokumentai – dokumentai, naudojami siekiant suteikti atitinkamiems suinteresuotiesiems subjektams techninių ir informatyvių žinių apie pasirinktinus standartus, kuriuos turi atitikti kiti sistemos e. CODEX ištekliai. Juose apibrėžiami reikalavimai ir principai, taikomi kuriant sąveikius tarpvalstybinius ryšius, siekiant palengvinti elektroninį keitimąsi duomenimis, įskaitant bet kokį elektroniniu būdu perduodamą turinį. Be to, juose išvardijami pasirinkti standartai ir metodikos, kuriais grindžiama sistema e. CODEX. Architektūra užtikrinamas sistemos e. CODEX savarankiškumas.

b) Jungties paketo išeitinis kodas

Jungties paketo išeitinis kodas naudojamas 2.4.2 skyriuje aprašytiems naudotiniems artefaktams sukurti.

([1]) 2022 m. gegužės 30 d. Europos Parlamento ir Tarybos reglamentas (ES) 2022/850 dėl tarpvalstybinio elektroninio keitimosi duomenimis teisminio bendradarbiavimo civilinėse ir baudžiamosiose bylose srityje kompiuterinės sistemos (sistemos e. CODEX), kuriuo iš dalies keičiamas Reglamentas (ES) 2018/1726 (OL L 150, 2022 6 1, p. 1).

c) Konfigūracijos valdymo priemonė (CMT)

Konfigūracijos valdymo priemonė (CMT) yra internetinė konfigūracijos failų, susijusių su „eDelivery“ tinklų sietuvu ir jungtimi, valdymo priemonė, kuria naudojantis galima standartizuotai valdyti konfigūracijos darbo srautą. Patvirtintą sistemos e. CODEX prieigos tašką eksploatuojantis subjektas gali prisijungti prie CMT per visame pasaulyje prieinamą portalą ir įkelti savo „eDelivery“ konfigūracijos duomenis. Įkelti duomenys turi apimti tinklų sietuvo galinių įrenginių tinklo konfigūracijos informaciją, visus prisijungimui reikalingus saugumo sertifikatus, taip pat konkrečius projektus, aplinkas ir naudojimo atvejus, kuriuose jie dalyvauja. CMT turi automatiškai patikrinti įkeltų duomenų tinkamumą ir, įvykus klaidoms, teikti grįžtamąją informaciją patvirtintus sistemos e. CODEX prieigos taškus eksploatuojančiam subjektui.

Gavus pranešimą apie bet kokius patvirtintą sistemos e. CODEX prieigos tašką eksploatuojančio subjekto pateiktų duomenų pakeitimus, naudojant šią priemonę parengiamas naujas sistemos e. CODEX konfigūracijos paketas (žr. 2.4.3 punktą). Visiems patvirtintus sistemos e. CODEX prieigos taškus eksploatuojantiems subjektams pranešama apie naujo sistemos e. CODEX konfigūracijos paketo sukūrimą ir jie bet kuriuo metu gali jį tiesiogiai atsisiųsti iš CMT. CMT gali teikti sistemos e. CODEX konfigūracijos paketus įvairioms IT aplinkoms, pavyzdžiui, TEST, ACCEPTANCE ar PRODUCTION.

Nauji sistemos e. CODEX konfigūracijos paketai įsigalioja praėjus septynioms dienoms po jų sukūrimo ir, jei taikytina, iki tos dienos patvirtintus sistemos e. CODEX prieigos taškus eksploatuojantys subjektai naują paketą įdiegia savo aplinkoje.

CMT taip pat nuolat informuoja patvirtintus sistemos e. CODEX prieigos taškus eksploatuojantį subjektą apie jų saugumo sertifikatų vykdymo aplinką ir iš anksto e. paštu praneša apie būsimą patvirtintų sistemos e. CODEX prieigos taškų sertifikatų galiojimo pabaigą. Jei patvirtintą sistemos e. CODEX prieigos tašką eksploatuojančio subjekto saugumo sertifikatų galiojimo laikas pasibaigia, jie automatiškai pašalinami iš kito paketo kūrimo.

CMT priegloba turi būti centralizuota ir ja sistemos e. CODEX dalyviai gali naudotis visą parą kasdien. Parama teikiama tik darbo valandomis.

d) Centrinė testavimo platforma (CTP)

Centrinė sistemos e. CODEX testavimo platforma (CTP) yra automatinė testavimo infrastruktūra. Ji suteikia galimybę patvirtintą sistemos e. CODEX prieigos tašką eksploatuojančiam subjektui atlikti savo sistemos e. CODEX infrastruktūros ir fiksuoto centrinio testavimo taško ryšio testavimą ir visapusį testavimą, nenaudojant jokio kito partnerio (pvz., kito patvirtinto sistemos e. CODEX prieigos taško), ryšių funkcijų testavimo tikslais. Ji suteikia galimybę siųsti ir gauti individualiems poreikiams pritaikomus testavimo pranešimus ir taip sumažina pastangas, kurių reikia sistemos e. CODEX infrastruktūros testavimui atlikti pradiniu (diegimo) ir regresinio testavimo laikotarpiu. Atskirų pranešimų eiga, Europos telekomunikacijų standartų instituto (ETSI) registruoto elektroninio pašto (REM) įrodymai ir klaidų žurnalai yra sekami ir pateikiami patvirtintus sistemos e. CODEX prieigos taškus eksploatuojantiems subjektams, taikant specialiai suprojektuotus vizualinius procesus.

CTP sudaro sistemos e. CODEX tinklų sietuvas, jungtis, jungties paketo kliento komponentas ir susijusi saityno grafinė vartotojo sąsaja (kol kas saityno pradinė ir galinė sistemos, sukurtos naudojant „Nuxt.js“), kuria galima naudotis siunčiant pranešimus į partnerio tinklų sietuvą, taip pat peržiūrėti pranešimus, kurie per tą patį tinklų sietuvą siunčiami į CTP. Šiuo metu CTP saugo svarbią veiklos informaciją (vietinius kintamuosius) „MongoDB“ egzemplioriuje ir nuskaito konfigūracijos (subjekto) informaciją iš jungties duomenų bazės. Be to, siekiant gauti informaciją apie sistemos e. CODEX pranešimus ir pateikti naujus pranešimus į jungtį ir tinklų sietuvą, joje naudojama jungties paketo kliento komponento reprezentacinės perdavimo būsenos (REST) programų sąsaja (API).

Siekiant suteikti kiekvienai sistemos e. CODEX aplinkai pritaikytą sprendimą, CTP diegiama įvairiuose egzemplioriuose (kopijose), kurie egzistuoja įvairiose sistemos e. CODEX aplinkose. Kiekvienas CTP egzempliorius šiuo metu yra įdiegtas UNIX („CentOS 7“) aplinkoje, kurioje kartu veikia visi komponentai. Taip palengvinamas administravimas ir prieiga prie failų sistemos, tačiau tai gali būti pritaikyta įrenginiams, kuriuose sistemos e. CODEX pranešimų siuntimo infrastruktūra yra atskira.

Kiekvienas CTP naudotojas yra susietas su vienu (1) tinklų sietuvu. Norint naudoti CTP testavimui, vienintelis reikalavimas yra tas, kad to patvirtinto sistemos e. CODEX prieigos taško tinklų sietuvas egzistuotų tos konkrečios sistemos e. CODEX CMT aplinkos apdorojimo režimuose.

e) „Metadata Workbench“

„Metadata Workbench“ yra priemonė, kurioje administruojamas ES e. teisingumo bazinis žodynas. Ji suteikia galimybę semantinio modeliavimo specialistams tvariai tvarkyti žodyną, laikantis Pagrindinių komponentų techninės specifikacijos modeliavimo standarto, apibrėžto sistemos e. CODEX architektūros dokumentuose. Tai internetinės paslauginės programinės įrangos (SaaS) sprendimas, prie kurio prieigą turi tik ES e. teisingumo bazinio žodyno administratoriai. „Metadata Workbench“ sukurta ir eksploatuojama Nyderlandų teisingumo ir saugumo ministerijos vardu. Remiantis Teisingumo ir saugumo ministerijos ir agentūros eu-LISA sudaroma licencine sutartimi, agentūrai eu-LISA bus suteikta prieiga prie „Metadata Workbench“, kad ji galėtų administruoti ir eksploatuoti ES e. teisingumo bazinį žodyną.

f) ES e. teisingumo bazinis žodynas

ES e. teisingumo bazinis žodynas – pakartotinai vartotinų semantinių terminų ir apibrėžčių išteklius, naudojamas siekiant ilgainiui ir visais naudojimo atvejais užtikrinti duomenų nuoseklumą ir duomenų kokybę. Jo semantine saugykla grindžiamos visos konkrečiam naudojimo atvejui būdingos pranešimų struktūros (XML schemos).

Ateityje e. teisingumo bazinis žodynas galėtų būti tobulinamas remiantis baziniais žodynais ([2]). Siekiant patvirtinti atitiktį specifikacijai, būtų galima sukurti XML pagrįstą tikrintuvą, naudojantis Komisijos siūloma „Interoperability Test Bed“ paslauga.

g) Skaitmeniniai procedūrų standartai (DPS)

Skaitmeninis procedūrų standartas – veiklos procesų modelių ir duomenų schemų techninės specifikacijos, kuriomis nustatoma duomenų, kuriais keičiamasi per sistemą e. CODEX remiantis ES e. teisingumo baziniu žodynu, elektroninė struktūra. Veiklos procesų modelyje aprašomas sistemos e. CODEX remiamos teisinės priemonės elektroninės procedūros techninis įgyvendinimas.

Veiklos procesų modelis kartu su ES e. teisingumo baziniu žodynu sudaro XML schemas, kuriomis aprašoma elektroninė DPS struktūra. XML schemos suteikia galimybę patvirtintiems prieigos taškams siųsti ir gauti dokumentus, kaip numatyta tarpvalstybinio teisminio bendradarbiavimo priemonėje.

2.4. **Sistemos e. CODEX naudotini ištekliai**

Sistemos e. CODEX naudotini ištekliai yra sistemos e. CODEX komponentai, kuriuos savo e. CODEX aplinkoje naudoja patvirtintą sistemos e. CODEX prieigos tašką eksploatuojantys subjektai. Išskyrus tinklų sietuvą, agentūra eu-LISA juos išplatina patvirtintą sistemos e. CODEX prieigos tašką eksploatuojantiems subjektams.

Naudotini ištekliai yra:

a) tinklų sietuvas (2.4.1 punktas);

b) Jungties paketas (2.4.2 punktas);

c) sistemos e. CODEX konfigūracijos paketas (įskaitant apdorojimo režimus, viešuosius sertifikatus ir saugumo nustatymus) (2.4.3 punktas);

d) bendradarbiavimo modelis arba proceso modelis, kuris yra DPS dalis;

e) XML schemos yra pranešimų struktūros, kurios yra DPS dalis.

2.4.1. ***Tinklų sietuvas***

Sistemos e. CODEX tinklų sietuvas yra sudedamoji dalis, atsakinga už pagrindinių ryšių mainus. Šiuo metu tinklų sietuvams taikomi šie standartai:

a) OASIS ([3]) ebMS 3.0 standartas: tinklų sietuvų keitimosi duomenimis pranešimai, atitinkantys ebXML standartą. Pagal šį standartą apibrėžiama struktūra, kuri turi būti taikoma, kad pranešimo antraštė būtų suprantama sistemos e. CODEX infrastruktūroje;

b) OASIS taikymo pareiškimo 4 (AS4) pranešimų siuntimo profilis: tai OASIS ebMS 3.0 specifikacijos atitikties profilis;

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

([3]) Struktūrinės informacijos standartų tobulinimo organizacija.

c) bendras „eDelivery“ AS4 profilio profilis ([4]).

Gali būti naudojamas bet koks šiuos reikalavimus atitinkantis tinklų sietuvo sprendimas.

2.4.2. ***Jungties paketas***

Jungtis yra jungiamasis komponentas, kuriuo konkrečios nacionalinės DPS taikomosios programos sujungiamos su tinklų sietuvo bendraisiais pranešimų siuntimo standartais. Taigi, šis komponentas papildo pagrindinį ryšį, jau užmegztą per tinklų sietuvo komponentą, šiomis funkcijomis:

a) **ETSI-REM įrodymais**. Tai jungties sukuriami įrodymai pasirašyto XML formatu. Šių įrodymų paskirtis – informuoti pranešimo siuntėją apie sėkmingą arba nesėkmingą pranešimo apdorojimą. Jungtis sukuria ir pateikia įrodymus skirtingais pranešimo apdorojimo etapais;

b) **„TrustOK“ prieigos raktu**. Siunčiančioji jungtis patvirtina pranešime esančio veiklos dokumento vientisumą ir autentiškumą. Šio patvirtinimo rezultatas įrašomas į „TrustOK“ prieigos raktą. Šį prieigos raktą sukuria jungties submodulis: saugumo biblioteka;

c) **ASiC-S talpykle.** Pagal ETSI standartą EN 319 162–1 „Elektroniniai parašai ir infrastruktūros bei susietųjų parašų talpyklės (ASiC)“. Talpyklė užtikrina jungties perduodamo paketo turinio autentiškumą ir vientisumą;

d) **Žiniatinklio paslaugų (WS) saugumas**. Kad padidintų pranešimų perdavimo saugumą, jungtis naudoja žiniatinklio paslaugų saugumą tinklų sietuvo atžvilgiu, taip pat sujungtosios sistemos atžvilgiu. Tai reiškia, kad kiekvienas jungties pateikiamas arba gaunamas pranešimas užšifruojamas ir pasirašomas;

e) **Bendra API**. Jungtis suteikia stabilią API, kurioje apibrėžtos saityno paslaugos, naudojamos prisijungiant prie tinklų sietuvo ir sujungtųjų sistemų programos (-ų). Pranešimų, kuriais keičiamasi su jungtimi, struktūra taip pat aprašyta jungties API.

Be pačios jungties programinės įrangos, pakete taip pat yra programos klientas, kurio paskirtis – palaikyti arba pakeisti sujungtąją sistemą e. CODEX pranešimų siuntimui valdyti.

Be to, buvo sukurtas papildinys, visų pirma skirtas „Domibus“ tinklų sietuvui ([5]), kad bendra jungties API būtų susieta su tinklų sietuvo apdorojimo pagrindu.

2.4.3. ***Sistemos e. CODEX konfigūracijos paketas***

EbMS 3.0 pagrįsto ryšio atveju apdorojimo režimais reguliuojamas visų pranešimų, susijusių su dviejų pranešimų siuntimo paslaugų teikėjų (MSH) keitimusi pranešimais, perdavimas. Į sistemos e. CODEX konfigūracijos paketą įtrauktas pranešimų siuntimo konfigūracijos parametrų (apdorojimo failų, kelių sertifikatų patikimumo saugyklų, tinklo adresų) rinkinys, kuriame išsamiai nurodoma, kaip keičiamasi pranešimais.

Pranešimų siuntimo konfigūracijos parametrai gali būti skirstomi į šias penkias kategorijas:

a) su siuntėju susiję parametrai, pvz.:

   i) siunčiančios šalies identifikatorius;

   ii) sertifikatas, kurį siuntėjas naudoja pranešimams pasirašyti;

   iii) sertifikavimo institucijos, kuriomis pasitiki siuntėjas;

   iv) tinklo adresas (arba adresai), iš kurio siuntėjas siųs pranešimą;

b) su gavėju susiję parametrai, pvz.:

   i) gaunančios šalies identifikatorius;

   ii) sertifikatas, kuris, kaip numato gavėjas, bus naudojamas pranešimams šifruoti;

   iii) sertifikavimo institucijos, kuriomis pasitiki gavėjas;

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

([5]) „Domibus“ tinklų sietuvą prižiūri Komisija (https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/Domibus).

iv) tinklo adresas (arba adresai), iš kurio gavėjas priims gaunamą pranešimą;

c) su siuntėjo ir gavėjo pora susiję parametrai, pvz. (jei naudojama):

i) susitarimo identifikatorius, apdorojimo režimo identifikatorius;

d) su DPS susiję parametrai, pvz.:

i) siunčiančios šalies vaidmuo (-enys);

ii) gaunančios šalies vaidmuo (-enys);

iii) paslauga (-os);

iv) paslaugos veiksmai;

e) parametrai, susiję su pranešimų siuntimo protokolo arba pranešimų protokolo profilio naudojimu.

Sistemoje e. CODEX visi konfigūracijos failai, susiję su MSH arba domenu, sujungiami į vieną pagrindinį failą, kuris gali būti naudojamas tinklų sietuvui ir jungčiai konfigūruoti.

Pagrindiniame faile apibrėžiamas individualus ryšių tinklas, kuriuo MSH gali naudotis vykdydamas savo veiklą. Būtina, kad konfigūracija būtų generuojama centralizuotai, nes visa informacija, susijusi su visais patvirtintais sistemos e. CODEX prieigos taškais, turi būti prieinama generuojant e. CODEX konfigūracijos paketą, kurį parengia CMT.

3. SISTEMOS E. CODEX SAUGUMAS IR VIENTISUMO BEI AUTENTIŠKUMO TIKRINIMO METODAI

Sistema e. CODEX yra ryšių sistema, kuria užtikrinama stipri parama saugumo ir duomenų apsaugos reikalavimų laikymuisi. Visų pirma sistemoje e. CODEX numatytos techninės funkcijos, būtinos visiems Europos Parlamento ir Tarybos reglamente (ES) Nr. 910/2014 ([6]) numatytiems reikalavimams įvykdyti.

3.1. Pritaikytasis saugumas

Techniniu požiūriu sistema e. CODEX yra transportavimo mechanizmas. Saugumo požiūriu svarbūs skirtingi lygmenys:

a) tinklo lygmuo;

b) transporto lygmuo;

c) pranešimo lygmuo;

d) dokumento lygmuo.

Kiekviename iš šių lygmenų taikomos saugumo priemonės.

3.1.1. *Tinklo lygmuo*

Sistema e. CODEX gali būti naudojama įvairiais tinklo lygmenimis. Tinklo lygmuo paprastai taikomas įprastiems interneto ryšiams. Todėl saugumas atitinka įprastą saugumą, taikomą interneto technologijai (ir yra išplečiamas kitais šiame punkte aprašytais lygmenimis). Daugumai sistemos e. CODEX naudojimo atvejų pakanka tokio tinklo lygmens. Aukštesnių saugumo reikalavimų atveju taip pat galėtų būti taikomas kitas tinklo lygmuo. Taip pat galima atsižvelgti į kitus tinklus.

3.1.2. *Transporto lygmuo*

Transporto lygmuo paprastai apsaugomas transporto lygmens saugumo (TLS) arba mTLS (abipusio TLS) priemonėmis. Tai yra nusistovėjęs interneto technologijų transporto lygmens apsaugos standartas, visame pasaulyje taikomas daugeliui paslaugų. TLS/mTLS užtikrina šifravimą ir autentiškumo patvirtinimą transporto kanale. Juo užtikrinamas transporto maršrutas tarp kiekvieno transporto maršruto centro. Kiekvienas centras turi iššifruoti (tik) adreso duomenis, kad pranešimas būtų perduotas kitam centrui. Prieš persiuntimą kiekvienas centras dar kartą užšifruoja adreso duomenis. Paprastas (vienkyptis) TLS yra įmanomas ir kartais vis dar taikomas, tačiau rekomenduojama taikyti dvikryptį TLS (mTLS), nes jis tampa dabartiniu transporto lygmens apsaugos standartu.

([6]) 2014 m. liepos 23 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB (OL L 257, 2014 8 28, p. 73).

3.1.3. ***Pranešimo lygmuo***

Pranešimų lygmeniu skirtingi e. CODEX komponentai taiko kelis standartus:

a) perduodant iš tinklų sietuvo į tinklų sietuvą naudojamas AS4 protokolas (kaip pranešimo lygmuo), kuris pasirašo ir užšifruoja pranešimus, priklausomai nuo tinklų sietuvo lygmens saugumo konfigūracijos;

b) pagrindinis sistemos e. CODEX komponentas yra jungtis. Ji padidina pranešimo lygmens saugumą, naudodama WS saugą saityno paslaugų pranešimų pasirašymui ir šifravimui, nukreiptam į tinklų sietuvą ir galinę sistemą (-as). Todėl papildomai taikomas jungties su jungtimi šifravimas;

c) visose e. CODEX sistemose pasirašymo ir šifravimo funkcijoms atlikti naudojami skaitmeniniai sertifikatai. Tie skaitmeniniai šifravimo ir pasirašymo sertifikatai atitinka X.509 standartą.

3.1.4. ***Dokumento lygmuo***

Pranešimuose pateikiami dokumentai ir priedai. Jie supakuojami į paketą, vadinamą talpykle. Talpyklė suformuojama pagal ASiC-S standartą. Siunčiančioji jungtis pasirašo ASiC-S talpyklę, o parašas patvirtinamas gaunančiajai jungčiai jį gavus.

3.2. **Vientisumo ir autentiškumo tikrinimo metodai**

3.2.1. ***Prieiga prie sistemos e. CODEX konfigūracijos***

Ryšį tarp sistemos e. CODEX prieigos taškų reikia iš anksto sukonfigūruoti. Ši konfigūracija atliekama naudojant sistemos e. CODEX konfigūracijos paketą. Konfigūracijos pakete pateikiami adresavimo duomenys, taikoma saugumo politika ir kita informacija. Be to, jame taip pat yra visų dalyvaujančių sistemos e. CODEX prieigos taškų viešųjų sertifikatų patikimumo saugyklos. Kiekvieno partnerio konfigūracijos failus sukuria centrinis konfigūracijos koordinatorius (CfC), naudodamas konfigūracijos valdymo priemonę (CMT). Prieiga prie šios CMT suteikiama tik kiekvienam partneriui pateikus asmeninį ir individualų prašymą. Administracinė prieiga suteikiama tik CfC ir ją valdo agentūra eu-LISA.

3.2.2. ***Palaikomi elektroniniai parašai ir spaudai***

Sistema e. CODEX palaiko visų rūšių elektroninius spaudus ir elektroninius parašus, kaip numatyta Reglamente (ES) Nr. 910/2014.

3.2.3. ***Sistemos e. CODEX „TrustOK“ prieigos raktas***

Siunčiančioji jungtis patvirtina pranešimo DPS parašą. Šio patvirtinimo rezultatai įrašomi į sistemos e. CODEX „TrustOK“ prieigos raktą. Šį prieigos raktą sukuria saugumo biblioteka, kuri yra jungties submodulis. Elektroninį parašą patvirtina sistemos e. CODEX jungtis, naudodama skaitmeninio parašo paslaugos priemones.

3.2.4. ***Kompiuterio skaitomas prieigos raktas (XML)***

Kompiuterio skaitomas prieigos raktas pateikiamas kaip XML failas, kuriuo grindžiama tam tikra schema, kurioje pateikiama visa informacija apie veiklos prieigos rakto pasirašymą ir tikrinimo ataskaitą, parengtą atlikus teisinį ir techninį patikrinimą.

3.2.5. ***Žmogaus skaitomas prieigos raktas (PDF)***

PDF failą sudaro trys dalys. Pirma dalis, pateikta pirmame faktinio prieigos rakto puslapyje, apima bendrą informaciją apie pažangiąją elektroninę sistemą ir veiklos dokumento teisinio galiojimo vertinimą. Be to, puslapio apačioje pateikiamas atsakomybės ribojimo pareiškimas ir patvirtinimo spaudas, nurodantys teisinio patikrinimo rezultatą (sėkmingas/nesėkmingas).

Pažangioji elektroninė sistema yra sujungtoji sistema, galinti saugiai identifikuoti naudotoją ir užtikrinti per ją tarp kliento ir sistemos e. CODEX jungties siunčiamų pranešimų vientisumą.

Antroje antrojo puslapio dalyje pateikiama standartizuota techninė pirminės patvirtinimo ataskaitos informacijos apžvalga. Priklausomai nuo sujungtosios sistemos (pagrįstos autentiškumo patvirtinimu arba parašu), techninėje apžvalgoje pateikiama informacija skiriasi. Parašu pagrįstame prieigos rakte pateikiama pagrindinio sertifikato informacija, įskaitant atributus (jei yra). Autentiškumo patvirtinimu pagrįstame prieigos rakte nurodomas institucijos, iš kurios dokumentas buvo išsiųstas, pavadinimas ir, jei pateikiama, dokumento autoriaus vardas ir pavardė.

Šio puslapio apačioje pateikiamas spaudas, atitinkantis dokumento techninio patikrinimo rezultato spalvą (žalia/geltona/raudona), ir trumpas aprašymas, pvz., papildoma informacija apie tai, kodėl dokumentui skirta geltona techninio įvertinimo spalva.

Trečiąją dokumento dalį sudaro originali patvirtinimo ataskaita, kokia buvo parengta naudojantis išduodančiosios valstybės narės patvirtinimo programine įranga.

4. IKI ŠIOL PARENGTI SKAITMENINIAI PROCEDŪRŲ STANDARTAI (DPS)

E. teisingumo paslauga	DPS: proceso modelis	DPS: XML schema	Projekto šaltinis
Europos mokėjimo įsakymas	√	√	e. CODEX
Ieškiniai dėl nedidelių sumų	√	√	e. CODEX
Europos arešto orderis	√	√	e. CODEX
Finansinės baudos	√	√	e. CODEX
Savitarpio teisinė pagalba	√	√	e. CODEX
Pamatinis sprendimas 909 (laisvės atėmimo bausmės)	√	√	e. CODEX
Santuokos klausimai	√	√	e. SENS
ES sąskaitos blokavimo įsakymas	√	√	e. SENS
Testamentų registras	√	√	e. SENS
Dokumentų įteikimas	√	√	e. CODEX