A BIZOTTSÁG (EU) 2022/2519 VÉGREHAJTÁSI HATÁROZATA

(2022. december 20.)

az e-CODEX-rendszerre, többek között a biztonságra, valamint az integritás és a hitelesség ellenőrzésének módszereire vonatkozó műszaki előírásokról és szabványokról

(EGT-vonatkozású szöveg)

AZ EURÓPAI BIZOTTSÁG,

tekintettel az Európai Unió működéséről szóló szerződésre,

tekintettel a polgári és büntetőügyekben folytatott igazságügyi együttműködés területén történő, határokon átnyúló elektronikus adatcserére szolgáló számítógépes rendszerről (e-CODEX-rendszer) és az (EU) 2018/1726 rendelet módosításáról (EGT-vonatkozású szöveg) szóló, 2022. május 30-i (EU) 2022/850 európai parlamenti és tanácsi rendeletre ([1]), és különösen annak 6. cikke (1) bekezdése a) pontjára,

mivel:

(1) Az (EU) 2022/850 rendelet 5. cikkével összhangban az e-CODEX-rendszer egy e-CODEX hozzáférési pontból, digitális eljárási szabványokból és támogató szoftvertermékekből, dokumentációból és az említett rendelet mellékletében felsorolt egyéb eszközökből áll.

(2) Az e-CODEX hozzáférési pont egy olyan, a közös protokollokon alapuló szoftverből álló átjáró, amely lehetővé teszi a távközlési hálózaton keresztül történő biztonságos információcserét az azonos protokollokat használó más átjárókkal, valamint egy csatlakozó, amely lehetővé teszi a kapcsolt rendszerek összekapcsolását az átjáróval, és amely közös nyílt protokollokon alapuló szoftverből áll.

(3) Az e-CODEX-rendszer eu-LISA részére történő sikeres átadási és átvételi folyamata, valamint az eu-LISA felelősségi körébe tartozó feladatok teljesítésének lehetővé tétele érdekében meg kell határozni az e-CODEX-rendszer komponenseinek alapjául szolgáló – többek között a biztonságra, valamint az integritás és a hitelesség ellenőrzésének módszereire vonatkozó – minimális műszaki előírásokat és szabványokat.

(4) Az Európai Unióról szóló szerződéshez és az Európai Unió működéséről szóló szerződéshez csatolt, Dánia helyzetéről szóló 22. jegyzőkönyv 1. és 2. cikke értelmében Dánia nem vett részt az (EU) 2022/850 rendelet elfogadásában, ezért e határozat rá nézve nem kötelező és nem alkalmazandó.

(5) Az Európai Unióról szóló szerződéshez és az Európai Unió működéséről szóló szerződéshez csatolt, az Egyesült Királyságnak és Írországnak a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség tekintetében fennálló helyzetéről szóló 21. jegyzőkönyv 1. és 2. cikkével és 4a. cikkének (1) bekezdésével összhangban, az említett jegyzőkönyv 4. cikkének sérelme nélkül, Írország nem vett részt az (EU) 2022/850 rendelet elfogadásában, ezért e határozat rá nézve nem kötelező és nem alkalmazandó.

(6) Az (EU) 2018/1725 európai parlamenti és tanácsi rendelet ([2]) 42. cikkének (1) bekezdésével összhangban a Bizottság egyeztetett az európai adatvédelmi biztossal, aki 2022. november 24-én véleményt nyilvánított.

(7) Az e határozatban előírt intézkedések összhangban vannak az (EU) 2022/850 rendelet 19. cikkének (1) bekezdésével létrehozott bizottság véleményével,

([1]) HL L 150., 2022.6.1., 1. o.

([2]) Az Európai Parlament és a Tanács (EU) 2018/1725 rendelete (2018. október 23.) a természetes személyeknek a személyes adatok uniós intézmények, szervek, hivatalok és ügynökségek általi kezelése tekintetében való védelméről és az ilyen adatok szabad áramlásáról, valamint a 45/2001/EK rendelet és az 1247/2002/EK határozat hatályon kívül helyezéséről (HL L 295., 2018.11.21., 39. o.).

ELFOGADTA EZT A HATÁROZATOT:

1. cikk

Az e-CODEX-rendszernek az (EU) 2022/850 rendelet 5. cikkében említett komponenseinek alapjául szolgáló – többek között a biztonságra, valamint az integritás és a hitelesség ellenőrzésének módszereire vonatkozó – minimális műszaki előírásokat és szabványokat e határozat melléklete tartalmazza.

2. cikk

Ez a határozat az *Európai Unió Hivatalos Lapjában* való kihirdetését követő huszadik napon lép hatályba.

Kelt Brüsszelben, 2022. december 20-án.

a Bizottság részéről
az elnök
Ursula VON DER LEYEN

MELLÉKLET

Az e-CODEX-rendszerre, többek között a biztonságra, valamint az integritás és a hitelesség ellenőrzésének módszereire vonatkozó műszaki előírások és szabványok

1. **BEVEZETÉS**

Ez a melléklet az e-CODEX-rendszer alkotóelemeire, többek között a biztonságra, valamint az integritás és a hitelesség ellenőrzésének módszereire vonatkozó minimális műszaki előírásokat és szabványokat állapítja meg.

2. **AZ e-CODEX RENDSZER ALKOTÓELEMEI**

2.1. Az (EU) 2022/850 európai parlamenti és tanácsi rendelet ([1]) 5. cikke szerint az e-CODEX-rendszert a következők alkotják:

a) az e-CODEX hozzáférési pont, amely a következőkből áll:

i. egy átjáró;

ii. egy csatlakozó;

b) digitális eljárási szabványok; és

c) az (EU) 2022/850 rendelet mellékletében felsorolt támogató szoftvertermékek, dokumentáció és egyéb eszközök:

i. a központi tesztelési platform (KTP) forráskódja;

ii. a konfigurációkezelő eszköz forráskódja;

iii. a metaadat workbench;

iv. az uniós e-igazságügyi alapszókészlet;

v. az architektúradokumentáció.

2.2. Funkcionális szempontból ezek az elemek két kategóriába sorolhatók: az e-CODEX eszköztárára és az e-CODEX telepíthető eszközeire.

2.3. **Az e-CODEX eszköztára a következőkből áll:**

a) Az e-CODEX architektúradokumentációja;

b) a csatlakozócsomag forráskódja;

c) a konfigurációkezelő eszköz forráskódja;

d) a központi tesztelési platform (KTP) forráskódja;

e) a metaadat workbench harmadik féltől származó licence;

f) az uniós e-igazságügyi alapszókészlet;

g) digitális eljárási szabványok.

a) Az e-CODEX architektúradokumentációja

Az architektúradokumentáció olyan dokumentumok összessége, amelyek arra szolgálnak, hogy az érdekelt felek számára technikai és tájékoztató ismereteket nyújtsanak azon választható szabványokkal kapcsolatban, amelyeknek az e-CODEX-rendszer egyéb eszközeinek meg kell felelniük. Meghatározza az elektronikus adatcserét – ideértve az elektronikus formában átvihető tartalmakat is – elősegítő, határokon átnyúló interoperábilis kommunikáció létrehozásakor alkalmazandó követelményeket és elveket. Emellett felsorolja azokat a kiválasztott szabványokat és módszereket, amelyeken az e-CODEX-rendszer alapul. Az architektúra biztosítja az e-CODEX-rendszer autonómiáját.

b) A csatlakozócsomag forráskódja

A csatlakozócsomag forráskódja a 2.4.2. fejezetben leírt telepíthető műtárgyak létrehozására szolgál.

([1]) Az Európai Parlament és a Tanács (EU) 2022/850 rendelete (2022. május 30.) a polgári és büntetőügyekben folytatott igazságügyi együttműködés területén történő, határokon átnyúló elektronikus adatcserére szolgáló számítógépes rendszerről (e-CODEX-rendszer) és az (EU) 2018/1726 rendelet módosításáról (HL L 150., 2022.6.1., 1. o.).

c) A konfigurációkezelő eszköz

A konfigurációkezelő eszköz az e-Delivery átjárójához és a csatlakozójához kapcsolódó konfigurációs fájlok kezelésére szolgáló webalapú eszköz, amely szabványosított módon kezeli a konfigurációs munkafolyamatot. Az engedélyezett e-CODEX hozzáférési pontot működtető szervezet egy globálisan elérhető portálon keresztül férhet hozzá a konfigurációkezelő eszközhöz, és töltheti fel az e-Delivery-ben használt konfigurációs adatait. A feltöltött adatoknak tartalmazniuk kell az átjáró végponti hálózati konfigurációjára vonatkozó információkat, a csatlakozáshoz szükséges valamennyi biztonsági tanúsítványt, valamint azokat a konkrét projekteket, környezeteket és használati eseteket, amelyekben részt vesznek. A konfigurációkezelő eszköznek automatikusan ellenőriznie kell a feltöltött adatok érvényességét, és hibák esetén visszajelzést kell adnia az engedélyezett e-CODEX hozzáférési pontokat működtető szervezetnek.

Amennyiben az engedélyezett e-CODEX hozzáférési pontot működtető szervezet által szolgáltatott adatokban bekövetkező bármely változásról szóló értesítés érkezik, ezen eszköz használatával új e-CODEX konfigurációs csomagot kell készíteni (lásd a 2.4.3. pontot). Az engedélyezett e-CODEX hozzáférési pontokat működtető valamennyi szervezetet értesíteni kell az új e-CODEX konfigurációs csomag létrehozásáról, amelyet bármikor közvetlenül letölthetnek a konfigurációkezelő eszközből. A konfigurációkezelő eszköz többféle informatikai környezet (például TESZT, ELFOGADÁS vagy ELŐÁLLÍTÁS) számára biztosít e-CODEX konfigurációs csomagokat.

Az új e-CODEX konfigurációs csomagok a létrehozásuk után hét nappal lépnek hatályba, és adott esetben az engedélyezett e-CODEX hozzáférési pontokat működtető szervezeteknek addigra kell beépíteniük az új csomagot a környezetükbe.

A konfigurációkezelő eszköz emellett folyamatosan tájékoztatja az engedélyezett e-CODEX hozzáférési pontokat üzemeltető szervezetet biztonsági tanúsítványai futási idejéről, és e-mailben előre értesíti az engedélyezett e-CODEX hozzáférési pontokat tanúsítványaik közelgő lejáratáról. Amennyiben egy engedélyezett e-CODEX hozzáférési pontot működtető szervezet biztonsági tanúsítványai lejárnak, azokat automatikusan el kell távolítani a következő csomag létrehozásából.

A konfigurációkezelő eszközt központilag kell üzemeltetni, és a hét minden napján, napi 24 órában elérhetővé kell tenni az e-CODEX résztvevői számára. A támogatás csak munkaidőben vehető igénybe.

d) A központi tesztelési platform (KTP)

Az e-CODEX központi tesztelési platformja (KTP) egy automatizált tesztelési infrastruktúra. Lehetővé teszi az engedélyezett e-CODEX hozzáférési pontot működtető szervezet számára, hogy konnektivitási teszteket és végpontok közötti teszteket végezzen saját e-CODEX infrastruktúrája és egy állandó központi tesztelési pont között anélkül, hogy bármilyen további partnert (pl. egy másik engedélyezett e-CODEX hozzáférési pontot) be kellene vonnia a kommunikációs funkciók tesztelésébe. Ezenkívül lehetővé teszi testre szabható tesztüzenetek küldését és fogadását, és ezáltal csökkenti az e-CODEX-infrastruktúra kezdeti (telepítési) és regresszióvizsgálati idő alatti teszteléséhez szükséges erőfeszítéseket. Nyomon követi és az engedélyezett e-CODEX hozzáférési pontokat működtető szervezetek számára külön erre a célra kialakított vizuális folyamatokon keresztül bemutatja az egyes üzenetek előrehaladását, az Európai Távközlési Szabványügyi Intézet (ETSI) által regisztrált e-mailek (REM) bizonyítékait és hibanaplóit.

A KTP egy e-CODEX átjáróból, csatlakozóból, csatlakozó-kliensből és egy kapcsolódó webes grafikus felhasználói felületből (jelenleg a Nuxt.js-re épülő webes frontend/backend) áll, amely egy partner átjárójához küldött üzenetek küldésére, valamint az ugyanazon átjáró által a KTP-re küldött üzenetek megtekintésére használható. A KTP jelenleg a fontos működési információkat (helyi változókat) egy MongoDB-példányon tárolja, a felektől származó konfigurációs információkat pedig a csatlakozó adatbázisából olvassa. Ezenkívül a csatlakozó-kliens REST (Representational state transfer) alkalmazásprogramozási felületét (API) használja az e-CODEX-üzenetekre vonatkozó információk lekérdezésére, valamint új üzeneteknek a csatlakozóhoz és az átjáróhoz küldésére.

Az e-CODEX-környezetenként testre szabható megoldás biztosítása érdekében a KTP-t a különböző e-CODEX-környezetekben létező különböző példányokban (másolatokban) telepítik. Jelenleg a KTP minden egyes példánya UNIX (CentOS 7) környezetben van telepítve, ahol az összes komponens egymás mellett létezik. Ez megkönnyíti az adminisztrációt és a fájlrendszerhez való hozzáférést, de kiigazítható azon létesítmények számára, ahol az e-CODEX üzenetküldő infrastruktúra elkülönül.

Minden KTP-felhasználó egy (1) átjáróhoz kapcsolódik. A KTP tesztelésre történő használatának egyetlen feltétele, hogy az adott engedélyezett e-CODEX hozzáférési pont átjárója az adott e-CODEX konfigurációkezelő eszköze környezetének P-módjaiban rendelkezésre álljon.

e) A metaadat workbench

A metaadat workbench az az eszköz, amelyben az uniós e-igazságügy alapszókészletét kezelik. Lehetővé teszi a szemantikai modellezők számára, hogy a szókészletet fenntartható módon, az e-CODEX architektúradokumentációjában meghatározott, az alapkomponensre vonatkozó műszaki előírások modellezési szabványának megfelelően tartsák fenn. Webalapú szoftverszolgáltatási (SaaS) megoldás, amelyhez csak az uniós e-igazságügyi alapszókészlet adminisztrátorai rendelkeznek hozzáféréssel. A metaadat workbenchet a Holland Igazságügyi és Biztonsági Minisztérium megbízásából fejlesztik és működtetik. Az Igazságügyi és Biztonsági Minisztérium és az eu-LISA között megkötendő licencmegállapodás alapján az eu-LISA hozzáférést kap a metaadat workbenchhez az uniós e-igazságügyi alapszókészlet kezelése és működtetése érdekében.

f) Az uniós e-igazságügyi alapszókészlet

Az uniós e-igazságügyi alapszókészlet egy újrafelhasználható szemantikai kifejezéseket és fogalommeghatározásokat tartalmazó eszköz az adatok időbeli és használati eseteken átívelő egységességének és minőségének biztosítására. Szemantikai adattárán alapul minden használati esetre jellemző üzenetstruktúra (XML-sémák).

Az e-igazságügy alapszókészletének jövőbeli fejlesztése az alapszókészletekkel összhangban történhetne ([2]). Az előírásoknak való megfelelés ellenőrzése érdekében XML-alapú validátort lehetne létrehozni a Bizottság által kínált interoperabilitási tesztpadszolgáltatás segítségével.

g) Digitális eljárási szabványok

A „digitális eljárási szabvány” az üzleti folyamatmodellekre és az adatsémákra vonatkozó olyan műszaki előírások összessége, amelyek az uniós e-igazságügyi alapszókészlet alapján meghatározzák az e-CODEX-rendszer keretében megosztott adatok elektronikus struktúráját. Az üzleti folyamatmodell az e-CODEX rendszer által támogatott jogi eszköz elektronikus eljárásának technikai megvalósítását írja le.

Az üzleti folyamatmodell az uniós e-igazságügy alapszókészletével együtt olyan XML-sémákat eredményez, amelyek leírják a digitális eljárási szabvány elektronikus struktúráját. Az XML-sémák lehetővé teszik az engedélyezett hozzáférési pontok számára a határokon átnyúló igazságügyi együttműködési eszközök által biztosított dokumentumok küldését és fogadását.

2.4. **Az e-CODEX-rendszer telepíthető eszközei**

Az e-CODEX telepíthető eszközei az engedélyezett e-CODEX hozzáférési pontot működtető szervezetek által a saját e-CODEX-környezetükben telepített e-CODEX-összetevők. Ezeket – az átjáró kivételév – az eu-LISA osztja szét az engedélyezett e-CODEX hozzáférési pontot üzemeltető szervezetek között.

A telepíthető eszközök a következők:

a) az átjáró (2.4.1. pont);

b) a csatlakozócsomag (2.4.2. pont);

c) az e-CODEX konfigurációs csomag (beleértve a P-módokat, a nyilvános tanúsítványokat és a biztonsági beállításokat) (2.4.3. pont);

d) a digitális eljárási szabvány részét képező üzleti együttműködési terv vagy folyamatmodell;

e) az XML-sémák a digitális eljárási szabvány részét képező üzenetstruktúrák.

2.4.1. ***Az átjáró***

Az e-CODEX rendszerben az átjáró az alapvető kommunikációért felelős építőelem. Az átjárók jelenleg a következő szabványokat alkalmazzák:

a) OASIS ([3]) ebMS 3.0 szabvány: az ebXML-szabványnak megfelelő átjárók közötti üzenetváltás. Ez a szabvány meghatározza azt a struktúrát, amellyel az üzenet fejlécének rendelkeznie kell ahhoz, hogy az e-CODEX Infrastruktúra számára érthető legyen;

b) OASIS Applicability Statement 4 (AS4) üzenetküldő profil: ez az OASIS ebMS 3.0 specifikáció megfelelőségi profilja;

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

c) az e-Delivery AS4 profil közös profilja ([4]).

Bármely, az említett követelményeknek megfelelő átjárómegoldás alkalmazható.

2.4.2. ***A csatlakozócsomag***

A csatlakozó egy olyan összekötő elem, amely összekapcsolja a nemzeti digitális eljárási szabványok specifikus alkalmazásait az átjáró általános üzenetküldési szabványaival. Így ez a komponens a következő funkciókkal egészíti ki az átjáró komponens által már létrehozott alapvető kommunikációt:

a) **ETSI-REM bizonyítékok**: ezeket a bizonyítékokat a csatlakozó generálja aláírt XML formátumban. E bizonyítékok célja, hogy tájékoztassák az üzenet feladóját az üzenet sikeres vagy sikertelen feldolgozásáról. A csatlakozó az üzenetfeldolgozás különböző szakaszaiban bizonyítékokat hoz létre és nyújt be;

b) **TrustOK Token**: a küldő csatlakozó validálja az üzenetben szereplő üzleti dokumentum integritását és hitelesítését. A validálás eredményét a TrustOK Token tartalmazza. Ezt a tokent a csatlakozó egyik almodulja, a biztonsági könyvtár hozza létre;

c) **ASiC-S konténer**: az elektronikus aláírásokról és infrastruktúrákról, valamint az ASiC-konténerekről szóló EN 319 162-1 ETSI-szabványnak megfelelően. A konténer biztosítja a csatlakozó által továbbított hasznos adatok hitelességét és sértetlenségét;

d) **WS-Security (a webes szolgáltatások biztonsága)**: az üzenetek átviteli biztonságának növelése érdekében a csatlakozó a ws-securityt használja az átvitelhez mind az átjáró, mind a csatlakoztatott rendszer oldalán. Ez azt jelenti, hogy a csatlakozó által benyújtott vagy fogadott minden üzenet titkosított és aláírt;

e) **közös API**: a csatlakozó stabil API-t kínál, amely meghatározza az átjáróhoz és a csatlakoztatott rendszerek alkalmazásaihoz való csatlakozáshoz használt webszolgáltatásokat. A csatlakozóval váltott üzenetek szerkezetét szintén a csatlakozó API-ja írja le.

Magán a csatlakozószoftveren kívül a csomag tartalmaz egy olyan alkalmazásklienst is, amelynek célja, hogy támogassa vagy helyettesítse a csatlakoztatott rendszert az e-CODEX üzenetkezelésben.

Emellett kifejlesztettek egy kifejezetten a Domibus átjáróhoz ([5]) készült plugint is, amely a csatlakozó közös API-ját köti össze az átjáró feldolgozó magjával.

2.4.3. ***Az e-CODEX konfigurációs csomag***

Az ebMS 3.0 alapú kommunikációban a P-mód (vagy feldolgozási mód) szabályozza a két üzenetkezelő (MSH) közötti üzenetváltásban részt vevő valamennyi üzenet továbbítását. Az e-CODEX konfigurációs csomag üzenetkonfigurációs paraméterek (P-mód fájlok, több tanúsítványmegbízhatósági tároló, hálózati címek) gyűjteményét tartalmazza, amelyek részletesen meghatározzák az üzenetküldés módját.

Az üzenetküldés konfigurációs paraméterei a következő öt kategóriába sorolhatók:

a) A küldő félre vonatkozó paraméterek, például:

   i. a küldő fél azonosítója;

   ii. a küldő fél által az üzenetek aláírására használt tanúsítvány;

   iii. a küldő fél által megbízhatónak ítélt hitelesítésszolgáltatók;

   iv. az a hálózati cím (vagy címek), amely(ek)ről a küldő fél kommunikációt kezdeményez.

b) A fogadó félre vonatkozó paraméterek, például:

   i. a fogadó fél azonosítója;

   ii. az a tanúsítvány, amelyet a fogadó fél elvárásai szerint az üzenetek titkosítására használnak;

   iii. a fogadó fél által megbízhatónak ítélt hitelesítésszolgáltatók;

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

([5]) A Domibus átjárót a Bizottság tartja fenn (https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/Domibus).

iv. az a hálózati cím (vagy címek), amely(ek)ről a fogadó fél bejövő kommunikációt fogad.

c) A küldő-fogadó párosra vonatkozó paraméterek, például (ha használják):

i. megállapodás-azonosító, P-mód-azonosító.

d) A digitális eljárási szabványra vonatkozó paraméterek, például:

i. a küldő fél szerepe(i);

ii. a fogadó fél szerepe(i);

iii. szolgáltatás(ok);

iv. a szolgáltatáson belüli tevékenység(ek).

e) Az üzenetküldő protokoll használatával vagy az üzenetküldő protokoll profiljával kapcsolatos paraméterek.

Az e-CODEX-rendszerben az üzenetkezelőkre (MSH) és a doménekre vonatkozó összes konfigurációs fájlt egyetlen törzsfájlban egyesítik, amely felhasználható az átjáró és a csatlakozó konfigurációjához.

Ez a törzsállomány meghatározza azt az egyedi kommunikációs hálózatot, amelyet az MSH a működése során használni tud. A konfigurációt központilag kell létrehozni, mivel a konfigurációkezelő eszköz által létrehozott e-CODEX konfigurációs csomag létrehozásához az összes engedélyezett e-CODEX hozzáférési pontra vonatkozó valamennyi információnak rendelkezésre kell állnia.

3. AZ E-CODEX RENDSZER BIZTONSÁGA ÉS AZ INTEGRITÁS ÉS HITELESSÉG ELLENŐRZÉSÉRE SZOLGÁLÓ MÓDSZEREI

Az e-CODEX-rendszer olyan kommunikációs rendszer, amely erőteljes támogatást nyújt a biztonsági és adatvédelmi követelmények teljesítéséhez. Az e-CODEX-rendszer biztosítja különösen a 910/2014/EU európai parlamenti és tanácsi rendeletben ([6]) előírt valamennyi követelmény teljesítéséhez szükséges műszaki jellemzőket.

3.1. Beépített biztonság

Az e-CODEX-rendszer technikai szempontból egy szállítási mechanizmus. Biztonsági szempontból több réteg vonatkoztatható rá:

a) a hálózati réteg;

b) a szállítási réteg;

c) az üzenet rétege;

d) a dokumentum rétege.

E rétegek mindegyikén biztonsági intézkedéseket alkalmaznak.

3.1.1. *A hálózati réteg*

Az e-CODEX különböző hálózati rétegekkel használható. Általában rendszeres internetkapcsolaton alkalmazzák. A biztonság ezért az internettechnológia szokásos biztonsági alkalmazásait követi (és az ebben a pontban leírt egyéb rétegekkel bővül). Az e-CODEX legtöbb használati esetében elegendő egy ilyen hálózati réteg. Magasabb biztonsági követelmények tekintetében más hálózati réteg is alkalmazható. További hálózatokat is figyelembe lehet venni.

3.1.2. *A szállítási réteg*

A szállítási réteget általában a Transport Layer Security (TLS) vagy az mTLS (kölcsönös TLS) védi. Ez az internetes technológiák közlekedési rétegének védelmére szolgáló jól bevált szabvány, amelyet világszerte számos szolgáltatásnál alkalmaznak. A TLS/mTLS biztosítja a szállítási csatornán történő titkosítást és hitelesítést. Biztosítja a szállítási útvonalat a közlekedési útvonal egyes csomópontjai között. Minden csomópontnak (csak) a címadatokat kell visszafejtenie ahhoz, hogy az üzenetet továbbítani tudja a következő csomópontnak. A továbbítás előtt minden csomópont újra titkosítja a címadatokat. Az egyszerű (egyirányú) TLS lehetséges, és néha még mindig alkalmazzák, de a kétirányú TLS (mTLS) ajánlott, mivel ez a szállítási réteg védelmének jelenlegi szabványa.

([6]) Az Európai Parlament és a Tanács 910/2014/EU rendelete (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről (HL L 257., 2014.8.28., 73. o.).

3.1.3. ***Az üzenet rétege***

Az üzenetrétegben a különböző e-CODEX-összetevők számos szabványt alkalmaznak:

a) Az átjárók közötti átvitelhez (mint üzenetréteg) az AS4 protokoll használatos, amely aláírja és titkosítja az üzeneteket – az átjárószintű biztonsági konfigurációtól függően.

b) Az e-CODEX-rendszer központi eleme a csatlakozó. Ez azáltal növeli az üzeneti réteg biztonságát, hogy a WS-Security segítségével írja alá és titkosítja a webszolgáltatások átjáró és backend(ek) felé irányuló üzeneteit. Ezért csatlakozók közötti titkosítást is alkalmaznak.

c) Az aláírási és titkosítási funkció az e-CODEX-rendszerek egészében digitális tanúsítványokat használ. Ezek a titkosításra és aláírásra szolgáló digitális tanúsítványok megfelelnek az X.509 szabványnak.

3.1.4. ***A dokumentum rétege***

Az üzenetek dokumentumokat és mellékleteket tartalmaznak. Ezeket egy „konténernek” nevezett csomagba csomagolják. A konténer az ASiC-S szabvány szerint készül. A küldő csatlakozó aláírja az ASiC-S konténert, majd az aláírást a fogadó csatlakozó a beérkezéskor érvényesíti.

3.2. **Az integritás és a hitelesség ellenőrzésének módszerei**

3.2.1. ***Hozzáférés az e-CODEX-konfigurációhoz***

Az e-CODEX hozzáférési pontok közötti kommunikációhoz előzetes konfigurációra van szükség. Ez a konfiguráció az e-CODEX konfigurációs csomagon keresztül történik. A konfigurációs csomag tartalmazza a címadatokat, az alkalmazott biztonsági intézkedéseket és egyéb információkat. Emellett tartalmazza az összes részt vevő e-CODEX hozzáférési pont nyilvános tanúsítványait tartalmazó bizalmi tárolókat is. A konfigurációs fájlokat minden partner konfigurációjához egy központi konfigurációs koordinátor (CfC) hozza létre a konfigurációkezelő eszközzel (CMT). Az ehhez az eszközhöz való hozzáférés korlátozott: minden egyes partner számára csak személyes és egyéni kérésre, csak az adott partner számára biztosítható. Az adminisztratív hozzáférés az eu-LISA által kezelt CfC-kre korlátozódik.

3.2.2. ***Támogatott elektronikus aláírások és bélyegzők***

Az e-CODEX-rendszernek támogatnia kell a 910/2014/EU rendeletben előírt elektronikus bélyegzők és elektronikus aláírások valamennyi típusát.

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

A küldő csatlakozó érvényesíti az üzenet digitális eljárási szabvány szerinti aláírását. A validálás eredményét beírja az e-CODEX TrustOK Tokenbe. Ezt a tokent egy biztonsági könyvtár generálja, amely a csatlakozó almodulja. Az elektronikus aláírás hitelesítését az e-CODEX csatlakozó végzi DSS (digitális aláírási szolgáltatást nyújtó) eszközök használatával.

3.2.4. ***Géppel olvasható token (XML)***

A géppel olvasható token egy bizonyos séma alapjául szolgáló XML-fájlként érkezik, amely tartalmazza az üzleti token aláírására vonatkozó összes információt, valamint a jogi és technikai validálás eredményeként készült validálási jelentést.

3.2.5. ***Ember által olvasható Token (PDF)***

A PDF-fájl három részből áll. A tényleges Token első oldalán bemutatott első rész a fejlett elektronikus rendszerre vonatkozó általános információkat és az üzleti dokumentum jogi érvényességének értékelését tartalmazza. Emellett az oldal alján szerepel egy felelősségkizáró nyilatkozat és egy „érvényesítési bélyegző”, amely a jogi érvényesítés eredményét (sikeres/sikertelen) mutatja.

A fejlett elektronikus rendszer olyan összekapcsolt rendszer, amely képes a felhasználó biztonságos azonosítására és a rajta keresztül az ügyfél és az e-CODEX csatlakozó között küldött üzenetek sértetlenségének biztosítására.

A második oldalon található második rész az eredeti validálási jelentésben szereplő információk szabványosított műszaki áttekintését tartalmazza. A csatlakoztatott (hitelesítésen vagy aláíráson alapuló) rendszertől függően a műszaki áttekintés által megadott információk eltérőek. Az aláírásalapú token az alapul szolgáló tanúsítványban szereplő információkat tartalmazza, beleértve az attribútumokat is (amennyiben rendelkezésre állnak). A hitelesítésen alapuló token annak az intézménynek a nevét tartalmazza, ahonnan a dokumentumot küldték, valamint – amennyiben rendelkezésre áll – a dokumentum szerzőjének nevét.

Az oldal alján a dokumentum technikai érvényesítési eredményének színével megegyező színű bélyegző (zöld/sárga/vörös) és egy rövid leírás található, amely további információkat tartalmaz például arról, hogy a dokumentum miért kapott sárga technikai értékelést.

A dokumentum harmadik része az eredeti validálási jelentésből áll, ahogyan azt a kiállító tagállam validálási szoftvere létrehozta.

4. AZ EDDIG KIDOLGOZOTT DIGITÁLIS ELJÁRÁSI SZABVÁNYOK (DPS)

E-igazságügyi szolgáltatások	Digitális eljárási szabvány: folyamatmodell	Digitális eljárási szabvány: XML-séma	Projektforrás
Európai fizetési meghagyás	√	√	e-CODEX
Kis értékű követelések	√	√	e-CODEX
Európai elfogatóparancs	√	√	e-CODEX
Pénzbüntetések	√	√	e-CODEX
KÖLCSÖNÖS JOGSEGÉLY	√	√	e-CODEX
FD 909 (Szabadságvesztés)	√	√	e-CODEX
Házassági ügyek	√	√	e-SENS
Ideiglenes számlazárolást elrendelő európai uniós végzés	√	√	e-SENS
Végrendeletek nyilvántartása	√	√	e-SENS
Iratkézbesítés	√	√	e-CODEX