DECIZIA DE PUNERE ÎN APLICARE (UE) 2022/2519 A COMISIEI

din 20 decembrie 2022

privind specificațiile și standardele tehnice pentru sistemul e-CODEX, inclusiv cele privind securitatea și metodele de verificare a integrității și a autenticității

(Text cu relevanță pentru SEE)

COMISIA EUROPEANĂ,

având în vedere Tratatul privind funcționarea Uniunii Europene,

având în vedere Regulamentul (UE) 2022/850 al Parlamentului European și al Consiliului din 30 mai 2022 privind un sistem informatizat pentru schimbul electronic transfrontalier de date în domeniul cooperării judiciare în materie civilă și penală (sistemul e-CODEX) și de modificare a Regulamentului (UE) 2018/1726 ([1]), în special articolul 6 alineatul (1) litera (a),

întrucât:

(1) În conformitate cu articolul 5 din Regulamentul (UE) 2022/850, sistemul e-CODEX este compus dintr-un punct de acces e-CODEX, standarde procedurale digitale și produse software, documentație și alte active de asistență enumerate în anexa la regulamentul respectiv.

(2) Punctul de acces e-CODEX este compus dintr-un gateway care constă într-un software, bazat pe un set comun de protocoale, care permite schimbul securizat de informații, în cadrul unei rețele de telecomunicații, cu alte gateway-uri utilizând același set comun de protocoale, și un conector care permite stabilirea de legături între sistemele conectate și gateway și care constă într-un software, bazat pe un set comun de protocoale deschise.

(3) Pentru buna desfășurare a procesului de predare și preluare a sistemului e-CODEX către eu-LISA și pentru a face posibilă îndeplinirea atribuțiilor care îi vor reveni eu-LISA, ar trebui stabilite specificațiile și standardele tehnice minime, inclusiv cele privind securitatea și metodele de verificare a integrității și a autenticității, care stau la baza componentelor sistemului e-CODEX.

(4) În conformitate cu articolele 1 și 2 din Protocolul nr. 22 privind poziția Danemarcei, anexat la Tratatul privind Uniunea Europeană și la Tratatul privind funcționarea Uniunii Europene, Danemarca nu a participat la adoptarea Regulamentului (UE) 2022/850, prin urmare, nu are obligații în temeiul prezentei decizii și nu face obiectul aplicării acesteia.

(5) În conformitate cu articolele 1 și 2 și cu articolul 4a alineatul (1) din Protocolul nr. 21 privind poziția Regatului Unit și a Irlandei cu privire la spațiul de libertate, securitate și justiție, anexat la Tratatul privind Uniunea Europeană și la Tratatul privind funcționarea Uniunii Europene, și fără a aduce atingere articolului 4 din protocolul respectiv, Irlanda nu a participat la adoptarea Regulamentului (UE) 2022/850, prin urmare nu are obligații în temeiul prezentei decizii și nu face obiectul aplicării acesteia.

(6) Autoritatea Europeană pentru Protecția Datelor a fost consultată în conformitate cu articolul 42 alineatul (1) din Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului ([2]) și a emis un aviz la 24 noiembrie 2022.

(7) Măsurile prevăzute în prezenta decizie sunt conforme cu avizul comitetului instituit în temeiul articolului 19 alineatul (1) din Regulamentul (UE) 2022/850,

([1]) JO L 150, 1.6.2022, p. 1.

([2]) Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului din 23 octombrie 2018 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii și privind libera circulație a acestor date și de abrogare a Regulamentului (CE) nr. 45/2001 și a Deciziei nr. 1247/2002/CE (JO L 295, 21.11.2018, p. 39).

ADOPTĂ PREZENTA DECIZIE:

Articolul 1

Specificațiile și standardele tehnice minime, inclusiv cele privind securitatea și metodele de verificare a integrității și a autenticității, care stau la baza componentelor sistemului e-CODEX menționate la articolul 5 din Regulamentul (UE) 2022/850 sunt stabilite în anexa la prezenta decizie.

Articolul 2

Prezenta decizie intră în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

Adoptată la Bruxelles, 20 decembrie 2022.

Pentru Comisie
Președinta
Ursula VON DER LEYEN

ANEXĂ

Specificațiile și standardele tehnice pentru sistemul e-CODEX, inclusiv cele privind securitatea și metodele de verificare a integrității și a autenticității

1. **INTRODUCERE**

Prezenta anexă stabilește specificațiile și standardele tehnice minime pentru componentele sistemului e-CODEX, inclusiv cele privind securitatea și metodele de verificare a integrității și a autenticității.

2. **COMPONENTELE SISTEMULUI e-CODEX**

2.1. În conformitate cu articolul 5 din Regulamentul (UE) 2022/850 al Parlamentului European și al Consiliului ([1]), sistemul e-CODEX este compus din:

(a) un punct de acces e-CODEX, compus din:

(i) un gateway;

(ii) un conector;

(b) standarde procedurale digitale (*digital procedural standards* – DPS);

(c) produsele software, documentația și alte active de asistență enumerate în anexa la Regulamentul (UE) 2022/850:

(i) codul sursă al platformei centrale de testare (*Central Testing Platform* – CTP);

(ii) codul sursă al instrumentului de gestionare a configurației (*Configuration Management Tool* – CMT);

(iii) metadata Workbench (MDW);

(iv) vocabularul de bază al UE în domeniul e-justiției;

(v) documentația referitoare la arhitectură.

2.2. Din punct de vedere funcțional, aceste elemente sunt împărțite în două categorii: setul de instrumente e-CODEX și activele implementabile e-CODEX.

2.3. **Setul de instrumente e-CODEX este compus din:**

(a) documentația referitoare la arhitectura e-CODEX;

(b) codul sursă al suitei conectorului;

(c) codul sursă al Configuration Management Tool (CMT);

(d) codul sursă al platformei centrale de testare (CTP);

(e) o licență Metadata Workbench (MDW) din partea unui terț;

(f) vocabularul de bază al UE în domeniul e-justiției;

(g) standarde procedurale digitale (DPS).

(a) Documentația referitoare la arhitectura e-CODEX

Documentația referitoare la arhitectură este un set de documente utilizat pentru a furniza părților interesate relevante cunoștințe tehnice și informative cu privire la alegerea standardelor pe care trebuie să le respecte alte active ale sistemului e-CODEX. Aceasta definește cerințele și principiile care se aplică atunci când se creează comunicații transfrontaliere interoperabile pentru facilitarea schimbului electronic de date, care include orice conținut transmisibil în format electronic. În plus, aceasta enumeră standardele și metodologiile alese pe care se bazează sistemul e-CODEX. Arhitectura asigură autonomia sistemului e-CODEX.

(b) Codul sursă al suitei conectorului

Codul sursă al suitei conectorului este utilizat pentru a crea artefactele implementabile descrise în capitolul 2.4.2.

([1]) Regulamentul (UE) 2022/850 al Parlamentului European și al Consiliului din 30 mai 2022 privind un sistem informatizat pentru schimbul electronic transfrontalier de date în domeniul cooperării judiciare în materie civilă și penală (sistemul e-CODEX) și de modificare a Regulamentului (UE) 2018/1726 (JO L 150, 1.6.2022, p. 1).

(c) Configuration Management Tool (CMT)

Configuration Management Tool (CMT) este un instrument web pentru gestionarea fișierelor de configurare asociate cu portalul e-Delivery și cu conectorul și oferă o modalitate standardizată de execuție a procesului de configurare. Entitatea care operează un punct de acces e-CODEX autorizat poate accesa CMT prin intermediul unui portal disponibil la nivel mondial și își poate încărca propriile date de configurare e-Delivery. Datele încărcate trebuie să includă informații privind configurația de rețea a punctului terminal al gateway-ului, toate certificatele de securitate necesare pentru conectare, precum și proiectele, mediile și cazurile de utilizare specifice la care participă. CMT trebuie să verifice automat valabilitatea datelor încărcate și să ofere feedback entităților care operează punctele de acces e-CODEX autorizate, în cazul în care apar erori.

Atunci când se primește o notificare asupra oricăror modificări ale datelor furnizate de o entitate care operează un punct de acces e-CODEX autorizat, trebuie generat un nou pachet de configurare e-CODEX (a se vedea punctul 2.4.3) utilizând acest instrument. Toate entitățile care operează puncte de acces e-CODEX autorizate trebuie notificate cu privire la crearea noului pachet de configurare e-CODEX, pe care îl pot descărca oricând, direct din CMT. CMT poate furniza pachete de configurare e-CODEX pentru multiple medii informatice, cum ar fi TESTARE, ACCEPTARE sau PRODUCȚIE.

Noile pachete de configurare e-CODEX intră în vigoare la șapte zile de la crearea lor și, dacă este cazul, entitățile care operează puncte de acces e-CODEX autorizate trebuie să instaleze noul pachet în propriile medii până la momentul respectiv.

De asemenea, CMT ține la curent entitățile care operează puncte de acces e-CODEX autorizate cu privire la durata de execuție a certificatelor lor de securitate și notifică în prealabil, prin e-mail, punctele de acces e-CODEX autorizate atunci când se apropie data de expirare a certificatului. În cazul în care o entitate care operează un punct de acces e-CODEX autorizat permite expirarea certificatelor sale de securitate, aceasta va fi eliminată automat atunci când se generează următorul pachet.

CMT trebuie să fie găzduit la nivel central și să fie disponibil pentru participanții la e-CODEX 24 de ore din 24, șapte zile din șapte. Asistența va fi limitată la programul de lucru.

(d) Platforma centrală de testare (CTP)

Platforma centrală de testare e-CODEX (CTP) este o infrastructură de testare automatizată. Aceasta permite unei entități care operează un puncte de acces e-CODEX autorizat să efectueze teste de conectivitate și teste de la un capăt la altul între infrastructura sa e-CODEX și un punct central de testare fix, fără a fi necesară implicarea unui alt partener (de exemplu, un alt punct de acces e-CODEX autorizat) pentru testarea funcționalităților de comunicare. Aceasta permite trimiterea și primirea de mesaje de testare personalizabile și, prin urmare, reduce efortul necesar pentru testarea unei infrastructuri e-CODEX atât la momentul testării inițiale (instalare), cât și la momentul testării de regresie. Progresele înregistrate în ceea ce privește mesajele individuale, dovezile stabilite de către Institutul European de Standardizare în Telecomunicații (ETSI) pentru mesajele de poștă electronică recomandată (*Registered Electronic Mail* – REM) și jurnalele de erori sunt urmărite și prezentate entităților care operează puncte de acces e-CODEX autorizate prin intermediul unor procese vizuale special concepute.

CTP constă într-un gateway e-CODEX, un conector, un conector client și o interfață grafică cu utilizatorul web asociată (în prezent, interfață web frontend/backend bazată pe Nuxt.js), care pot fi utilizate pentru a trimite mesaje către gateway-ul unui partener, precum și pentru a vizualiza mesajele care sunt trimise către CTP prin același gateway. În prezent, CTP stochează informații operaționale importante (variabile locale) într-o instanță de MongoDB și citește informații privind configurația (specifice unei anumite părți) din baza de date a conectorului. În plus, aceasta utilizează interfața de programare a aplicațiilor (*Application Programming Interface* – API) de tip REST (Representational state transfer) conector-client pentru a extrage informații cu privire la mesajele e-CODEX și pentru a transmite noi mesaje către conector și gateway.

Pentru a oferi o soluție personalizată pentru fiecare mediu e-CODEX, CTP este implementată în diferite instanțe (copii), care există în diferite medii e-CODEX. Fiecare instanță a CTP este implementată în prezent într-un mediu UNIX (CentOS 7), în care coexistă toate componentele. Acest lucru facilitează administrarea și accesul la sistemul de fișiere, dar se poate adapta pentru a permite o instalare în care infrastructura de mesagerie e-CODEX este păstrată separat.

Fiecare utilizator al CTP este conectat la un (1) gateway. Pentru a utiliza CTP pentru testare, singura cerință este ca gateway-ul punctului de acces e-CODEX autorizat să existe în modurile P al respectivului mediu CMT al e-CODEX.

(e) Metadata Workbench

Metadata Workbench este un instrument în care se administrează Vocabularul de bază al UE în domeniul e-justiției. Aceasta permite modelatorilor semantici să mențină Vocabularul într-un mod sustenabil, respectând standardul de modelare al Specificațiilor Tehnice pentru Componentele de Bază, astfel cum este definit în documentația referitoare la arhitectura e-CODEX. Este o soluție online de software ca serviciu (*Software as a Service* – SaaS), cu acces limitat exclusiv la administratorii Vocabularului de bază al UE în domeniul e-justiției. Metadata Workbench este dezvoltat și operat în numele Ministerului Justiției și Securității din Țările de Jos. Pe baza unui contract de licență care urmează să fie încheiat între Ministerul Justiției și Securității și eu-LISA, eu-LISA va primi acces la Metadata Workbench pentru a administra și a exploata Vocabularul de bază al UE în domeniul e-justiției.

(f) Vocabularul de bază al UE în domeniul e-justiției

Vocabularul de bază al UE în domeniul e-justiției este o resursă pentru termenii și definițiile semantice reutilizabile utilizate pentru a asigura coerența datelor și calitatea datelor în timp și în toate cazurile de utilizare. Pe repertoriul său semantic se bazează toate structurile de mesaje specifice cazurilor de utilizare (scheme XML).

Evoluția viitoare a Vocabularului de bază în domeniul e-justiției s-ar putea adapta la Vocabularele de bază ([2]). Pentru a valida conformitatea cu specificația, ar putea fi creat un validator bazat pe XML, utilizând serviciul de testare a interoperabilității oferit de Comisie (*Interoperability Test Bed*).

(g) Standarde procedurale digitale (DPS)

„Standard procedural digital" înseamnă specificațiile tehnice pentru modelele de procese operaționale și pentru schemele de date, care stabilesc structura electronică a datelor transmise prin intermediul sistemului e-CODEX pe baza Vocabularului de bază al UE în domeniul e-justiției. Modelul de proces operațional descrie implementarea tehnică a procedurii electronice a instrumentului juridic care este sprijinit de sistemul e-CODEX.

Modelul de proces operațional, împreună cu Vocabularul de bază al UE în domeniul e-justiției, generează scheme XML care descriu structura electronică a DPS. Schemele XML permit punctelor de acces autorizate să trimită și să primească documente, astfel cum se prevede într-un instrument de cooperare judiciară transfrontalieră.

2.4. **Activele implementabile e-CODEX**

Activele implementabile e-CODEX sunt componente e-CODEX implementate de către entități care operează puncte de acces e-CODEX autorizate în mediile lor e-CODEX. Cu excepția gateway-ului, acestea urmează să fie distribuite de eu-LISA entităților care operează puncte de acces e-CODEX autorizate.

Activele implementabile sunt:

(a) gateway-ul (punctul 2.4.1);

(b) suita conectorului (punctul 2.4.2);

(c) pachetul de configurare e-CODEX (inclusiv modurile P, certificatele publice și setările de securitate) (punctul 2.4.3);

(d) modelul de colaborare operațională sau de proces operațional ca parte a DPS;

(e) schemele XML sunt structuri de mesaje ca parte a DPS.

2.4.1. ***Gateway-ul***

Gateway-ul din cadrul sistemului e-CODEX este modulul responsabil pentru schimbul de mesaje de bază. În prezent, gateway-ul are implementate următoarele standarde:

(a) standardul ebMS 3.0 al OASIS ([3]): mesaje de interschimbare între gateway-uri în conformitate cu standardul ebXML. Acest standard definește structura pe care trebuie să o aibă antetul unui mesaj pentru a fi comprehensibil în cadrul infrastructurii e-CODEX;

(b) profilul de mesagerie al declarației de aplicabilitate 4 (AS4) a OASIS: acesta este un profil de conformitate al specificației ebMS 3.0 a OASIS;

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

([3]) Organization for the Advancement of Structured Information Standards (Organizația pentru promovarea standardelor privind informațiile structurate).

(c) profilul comun al profilului eDelivery AS4 ([4]).

Se poate utiliza orice soluție de gateway care îndeplinește cerințele respective.

2.4.2. ***Suita conectorului***

Conectorul este o componentă de legătură pentru conectarea aplicațiilor specifice DPS naționale la standardele generice de mesagerie ale gateway-ului. Astfel, această componentă adaugă următoarele caracteristici la comunicarea de bază deja stabilită de componenta gateway:

(a) **Dovezi ETSI-REM**: acestea sunt dovezi generate de conector într-un format XML semnat. Scopul acestor dovezi este de a informa expeditorul unui mesaj cu privire la prelucrarea reușită sau nereușită a mesajului. Dovezile sunt generate și transmise de conector în diferite etape ale prelucrării mesajului;

(b) **Tokenul TrustOK**: conectorul expeditor validează integritatea și autentificarea documentului care face obiectul mesajului (*business document*). Rezultatul acestei validări se scrie în Tokenul TrustOK, generat de un submodul al conectorului: biblioteca de securitate;

(c) **Containerul ASIC-S**: în conformitate cu standardul ETSI EN 319 162-1 privind semnăturile electronice și infrastructurile și containerele de semnături asociate (ASiC). Containerul asigură autenticitatea și integritatea sarcinii utile transmise de conector;

(d) **WS-Security**: pentru a spori securitatea transmiterii mesajelor, conectorul utilizează certificatul WS-Security pentru partea gateway-ului, precum și pentru partea de sistem conectată pentru transmisie. Aceasta înseamnă că fiecare mesaj pe care conectorul îl transmite sau îl primește este criptat și semnat;

(e) **API comună**: Conectorul oferă o API stabilă care definește serviciile web care sunt utilizate pentru a se conecta la gateway și la aplicația (aplicațiile) sistemelor conectate. Structura mesajelor schimbate cu conectorul este, de asemenea, descrisă în API a conectorului.

Pe lângă software-ul conectorului în sine, suita mai conține o aplicație client care este destinată să sprijine sau să înlocuiască un sistem conectat pentru gestionarea mesageriei e-CODEX.

De asemenea, un plugin a fost creat special pentru gateway-ul Domibus ([5]), pentru a face legătura între API comună a conectorului și nucleul de prelucrare al gateway-ului.

2.4.3. ***Pachetul de configurare e-CODEX***

În comunicarea bazată pe ebMS 3.0, modul P (sau modul de prelucrare) reglementează transmiterea tuturor mesajelor implicate într-un schimb de mesaje între două entități de gestionare a serviciului de mesagerie (*Messaging Service Handlers* – MSH). Un pachet de configurare e-CODEX include o colecție de parametri de configurare a mesageriei (fișiere ale modului P, mai multe depozite de încredere pentru certificate, adrese de rețea) care specifică în detaliu modul în care se desfășoară mesageria.

Parametrii de configurare a mesageriei pot fi clasificați în următoarele cinci categorii:

(a) parametri referitori la expeditor, cum ar fi:

  (i) identificatorul părții expeditoare;

  (ii) certificatul utilizat de expeditor pentru a semna mesaje;

  (iii) autoritățile de certificare în care are încredere expeditorul;

  (iv) adresa (adresele) de rețea de la care expeditorul va iniția comunicarea;

(b) parametri referitori la destinatar, cum ar fi:

  (i) identificatorul părții destinatare;

  (ii) certificatul preconizat de către destinatar a fi utilizat pentru criptarea mesajelor;

  (iii) autoritățile de certificare în care are încredere destinatarul;

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

([5]) Gateway-ul Domibus este întreținut de Comisie (https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/Domibus)

(iv) adresa (adresele) de rețea de la care destinatarul va accepta comunicările primite;

(c) parametri referitori la perechea expeditor-destinatar, cum ar fi (dacă este cazul):

(i) identificatorul acordului, identificatorul modulului P;

(d) parametri referitori la DPS, cum ar fi:

(i) rolul (rolurile) părții expeditoare;

(ii) rolul (rolurile) părții destinatare;

(iii) serviciul (serviciile);

(iv) acțiunea (acțiunile) în cadrul serviciului;

(e) parametri referitori la utilizarea protocolului de mesagerie sau la profilul protocolului de mesagerie.

În e-CODEX, toate fișierele de configurare privind o MSH sau un domeniu sunt grupate într-un singur fișier master care poate fi utilizat pentru configurarea gateway-ului și a conectorului.

Fișierul master definește o rețea de comunicare individuală către care MSH se poate direcționa în timpul funcționării sale. Este necesar să fie generată configurația la nivel central, deoarece toate informațiile din toate punctele de acces e-CODEX autorizate trebuie să fie disponibile pentru generarea pachetului de configurare e-CODEX, care este creat de CMT.

3. SECURITATEA ȘI METODELE DE VERIFICARE A INTEGRITĂȚII ȘI A AUTENTICITĂȚII SISTEMULUI E-CODEX

Sistemul e-CODEX este un sistem de comunicații care oferă o bază solidă pentru a răspunde cerințelor în materie de securitate și de protecție a datelor. În special, sistemul e-CODEX oferă caracteristicile tehnice necesare pentru a îndeplini toate cerințele prevăzute în Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului ([6]).

3.1. Securitate de la stadiul conceperii

Din punct de vedere tehnic, sistemul e-CODEX este un mecanism de transport. Există diferite niveluri relevante pentru securitate:

(a) un nivel de rețea;

(b) un nivel de transport;

(c) un nivel de mesaj;

(d) un nivel de document.

Pentru fiecare dintre aceste niveluri se aplică măsuri de securitate.

3.1.1. *Nivelul de rețea*

e-CODEX poate fi utilizat cu diferite tipuri de niveluri de rețea. De obicei, se aplică conexiunilor la internet obișnuite. Prin urmare, securitatea urmează aplicațiile obișnuite de securitate ale tehnologiei internetului (și este extinsă prin celelalte niveluri descrise la prezentul punct). Pentru majoritatea cazurilor de utilizare e-CODEX, un astfel de nivel de rețea este suficient. Pentru cerințe de securitate mai ridicate, ar putea fi aplicat, de asemenea, un alt nivel de rețea. Pot fi luate în considerare și alte rețele.

3.1.2. *Nivelul de transport*

Nivelul de transport este, de obicei, protejat de protocolul de securitate pe nivelul de transport (*Transport Layer Security* – TLS) sau mTLS (TLS reciproc). Acesta reprezintă un standard bine stabilit pentru protejarea nivelului de transport în tehnologiile de internet și aplicat la nivel mondial unui număr mare de servicii. TLS/mTLS asigură criptarea și autentificarea pe canalul de transport. Acesta garantează securitatea rutei de transport între oricare dintre huburile rutei de transport. Fiecare hub trebuie să decripteze (numai) datele referitoare la adresă pentru a transmite mesajul către următorul hub. Înainte de a-l transmite, fiecare hub criptează din nou datele privind adresa. Deși există un protocol TLS simplu (unidirecțional) și, uneori, continuă să se aplice, se recomandă aplicarea protocolului TLS bidirecțional (mTLS), întrucât acesta este pe cale să devină standardul actual de protecție a nivelului de transport.

([6]) Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE (JO L 257, 28.8.2014, p. 73).

3.1.3. ***Nivelul de mesaj***

La nivelul de mesaj, diferite componente e-CODEX aplică diverse standarde:

(a) protocolul utilizat pentru transmisia de la gateway la gateway (ca nivel de mesaj) este AS4, care semnează și criptează mesajele – în funcție de configurația de securitate la nivel de gateway;

(b) componenta de bază a sistemului e-CODEX este conectorul. Acesta adaugă securitate la nivelul de mesaj prin utilizarea protocolului WS-Security pentru semnarea și criptarea mesajelor pentru serviciile web către gateway și sistemul (sistemele) backend. Prin urmare, se aplică suplimentar o criptare de la conector la conector;

(c) pentru funcționalitatea de semnare și criptare în toate sistemele e-CODEX se utilizează certificate digitale. Aceste certificate digitale pentru criptare și semnare sunt conforme cu standardul X.509.

3.1.4. ***Nivelul de document***

Mesajele conțin documente și anexe, grupate într-un pachet denumit „container". Containerul este construit în conformitate cu standardul ASiC-S. Conectorul expeditor semnează containerul ASiC-S, iar semnătura este validată în momentul primirii de către conectorul destinatar.

3.2. **Metode de verificare a integrității și a autenticității**

3.2.1. ***Accesul la configurația e-CODEX***

Comunicarea între punctele de acces e-CODEX necesită configurare prealabilă. Această configurare se realizează prin intermediul pachetului de configurare e-CODEX. Pachetul de configurare conține datele referitoare la adresă, politica de securitate aplicată și alte informații. În plus, acesta mai conține depozitele de încredere cu certificatele publice ale tuturor punctelor de acces e-CODEX participante. Fișierele de configurare sunt create pentru configurația fiecărui partener de către un coordonator central pentru configurare (*Coordinator for Configuration* – CfC), cu ajutorul CMT. Accesul la acest CMT este acordat și limitat la fiecare partener numai la cererea personală și individuală. Accesul administrativ este limitat la CfC, drepturile de acces urmând a fi gestionate de eu-LISA.

3.2.2. ***Semnături și sigilii electronice acceptate***

Sistemul e-CODEX trebuie să accepte toate tipurile de sigilii electronice și de semnături electronice, astfel cum se prevede în Regulamentul (UE) nr. 910/2014.

3.2.3. ***Tokenul TrustOK al e-CODEX***

Conectorul expeditor validează semnătura DPS a unui mesaj. Rezultatul acestei validări este scris în tokenul TrustOK al e-CODEX. Acest token este generat de către o bibliotecă de securitate, care este un submodul al conectorului. Validarea semnăturii electronice este efectuată de conectorul e-CODEX, utilizând instrumente DSS (*digital signature service* – serviciu de semnătură digitală).

3.2.4. ***Tokenul citibil automat (XML)***

Tokenul citibil automat se prezintă sub forma unui fișier XML subiacent unei anumite scheme care conține toate informațiile privind semnătura tokenului mesajului (*business token*) și raportul de validare, ca urmare a validării juridice și tehnice.

3.2.5. ***Token citibil pentru om (PDF)***

Fișierul PDF cuprinde trei părți. Prima parte, prezentată pe prima pagină a tokenului propriu-zis, include informații generale privind sistemul electronic avansat și o evaluare a valabilității juridice a documentului care face obiectul mesajului (*business document*). În plus, în partea de jos a paginii sunt afișate o declarație de declinare a responsabilității și o „ștampilă de validare" care indică rezultatul validării juridice (reușită/nereușită).

Un sistem electronic avansat este un sistem conectat, capabil să identifice în mod sigur utilizatorul și să asigure integritatea mesajelor trimise prin intermediul acestuia între client și conectorul e-CODEX.

A doua parte de pe a doua pagină oferă o sinteză cu caracter tehnic standardizată a informațiilor din raportul de validare inițial. În funcție de sistemul conectat (pe bază de autentificare sau de semnătură), informațiile furnizate de sinteza cu caracter tehnic variază. Un token bazat pe semnătură conține informațiile furnizate de certificatul subiacent, inclusiv atributele (dacă sunt disponibile). Un token bazat pe autentificare conține numele instituției de unde a fost trimis documentul și, atunci când este furnizat, numele autorului documentului.

Partea de jos a acestei pagini conține o ștampilă de culoarea rezultatului validării tehnice a documentelor (verde/galben/roșu) și o scurtă descriere, de exemplu, furnizând informații suplimentare cu privire la motivul pentru care un document a primit o evaluare tehnică galbenă.

A treia parte a documentului constă în raportul de validare inițial, astfel cum a fost creat de software-ul de validare al statului membru emitent.

4. STANDARDE PROCEDURALE DIGITALE (DPS) ELABORATE PÂNĂ ÎN PREZENT

Serviciul e-justiție	DPS: model de proces	DPS: schema XML	Sursa proiectului
Somația europeană de plată	√	√	e-CODEX
Cereri cu valoare redusă	√	√	e-CODEX
Mandat european de arestare	√	√	e-CODEX
Sancțiuni financiare	√	√	e-CODEX
Asistență judiciară reciprocă	√	√	e-CODEX
DC 909 (pedepse privative de libertate)	√	√	e-CODEX
Chestiuni în materie matrimonială	√	√	e-SENS
Ordonanța asigurătorie a UE de indisponibilizare a conturilor bancare	√	√	e-SENS
Registrul testamentelor	√	√	e-SENS
Notificarea sau comunicarea actelor	√	√	e-CODEX