APROBAT
GUVERNANTA PMO
DORU VIJIIANU
JUDIT FEKETE
MIRELA OJOG

Politici și practici pentru Serviciul calificat de validare a semnăturilor/sigiliilor electronice calificate (Politica și practica pentru validarea semnăturii)

Istoria ediției			
Ediție	**Data și descrierea modificării**	**Pregătit**	**Aprobat**
1	20.10.2022 – Prima ediție	Judit Fekete	Mirela Ojog
2	24.10.2023 -Editia a II-a – Modificare minora in cap. 2, 12.5.2, 9, 14.7, 14.9, 14.13	Judit Fekete	Mirela Ojog
3	24.04.2024 – Editia a III-a	Judit Fekete	Mirela Ojog

ZIPPER

Conținut

1. Introducere

Acest document reprezinta Politica Zipper Services SRL [ZS] privind serviciul de validare, stabileste regulile de validare pentru semnaturile electronice calificate si avansate (QES/AdES), precum si pentru sigiliile electronice calificate si avansate (QEseal/AdESeal). Este în conformitate cu Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului și cu secțiunea I.6 din DECIZIA DE PUNERE ÎN APLICARE (UE) 2015/1506 A COMISIEI din 8 septembrie 2015 [în conformitate cu articolele 27 și 37 din Regulamentul (UE) nr. 910/20 14 al Parlamentului European șial Consiliului]:

> *"Semnăturile electronice avansate și sigiliile electronice avansate sunt similare din punct de vedere tehnic. Prin urmare, standardele pentru formatele semnăturilor electronice avansate ar trebui să se aplice mutatis mutandis și formatelor pentru sigiliile electronice avansate."*
>
> *ȘI*
>
> *"Articolele 32, 33* și *34 se aplică mutatis mutandis validării și păstrării sigiliilor electronice calificate."*

Politica de validare a semnăturilor electronice și a sigiliilor electronice indiferent de tipul legal al semnăturii sau sigiliului (conform Regulamentului (UE) nr. 910/2014), respectiv faptul că semnătura electronică sau sigiliul electronic este fie semnătură electronică avansată (AdES), AdES susținută de un certificat calificat (AdES/QC), fie de o semnătură electronică calificată (QES) nu modifică rezultatul total de validare a semnăturii.

Infrastructura de chei publice (PKI) a ZS CA este administrată în conformitate cuprevederile legale ale Regulamentului [UE] 910/2014 al Parlamentului European și cu Legea 6/2020, din 11 noiembrie, care reglementează anumite aspecte ale serviciilor electronice de încredere din România.

Acest document a fost elaborat în conformitate cu specificațiile și standardele paneuropene actualepentru prestarea de servicii de încredere. Structura sa urmează recomandarea **din anexa A ETSI TS 119 441**.

2. Prezentare generală

Prezentul document este intitulat "Politica și practica pentru serviciul de validare calificată a semnăturilor/sigiliilor electronice calificate" (Politica și practica pentru Serviciul de validare a semnăturilor). Scopul politicii și al declarației practice este de a îndeplini cerințele generale ale comunității internaționale de a oferi încredere în tranzacțiile electronice, inclusiv, printre altele, cerințele general aplicabile din Regulamentul (UE) nr. 910/2014 de stabilire a unui cadru juridic pentru semnătura electronică și sigiliul electronic, inclusiv validarea acestora.

Prezentul document specifică regulile pentru a stabilidacă o semnătură electronică sau un sigiliu electronic este valabil pe baza considerentelor specificate în prezentul document și constrângerile de validare se aplică procedurilor de verificare. În această perspectivă, utilizatorul și partenerul de încrederese pot adresa ZS, care, în calitatea sa de furnizor de servicii de validare a semnăturilor calificat (QSVP), va efectua validarea semnăturii digitale în numele lor. Rezultatul acestei proceduri este un raport de **validare a semnăturii**. Participanții la tranzacțiile electronic trebuie să aibă încredere că ZS a stabilit în mod corespunzător proceduri și măsuri de protecție pentru a minimiza amenințările și riscurile operaționale și financiare asociate semnăturilor digitale.

Serviciul de validare validează toate semnăturile și sigiliile aplicate aceluiași document de intrare și furnizează diagnosticele rezultate într-un singur raport, pentru toate semnăturile/sigiliile și marcajele temporale aplicate. Cu toate acestea, nu face nicio interpretare a diagnosticelor furnizate sau a relației reciproce dintre aceste semnături și sigilii. În concluzie, serviciul de validare nu permite utilizatorului să selecteze certificatul (certificatele) care urmează să fie utilizat pentru validare. Aplicația client, care va utiliza rezultatul validării acelor semnături și sigilii, va interpreta rezultatul în funcție de contextul de afaceri în care este aplicat. De asemenea, va permite selectarea, dacă este necesar, a semnăturii specifice care urmează să fie verificată în cazul în care conținutul verificat conține semnături multiple.

Politicile de validare specificate în prezentul document sunt potrivite pentru o gamă largă de domenii de aplicare și de afaceri, ori de câte ori este nevoie de validarea semnăturilor sau sigiliilor electronice.

ZS furnizează serviciul în conformitate cu cerințele prevăzute în Regulamentul (UE) nr. 91 0/2014 și garantează că acest serviciu:

- Aplică proceduri operaționale și proceduri de management al securității care exclud orice posibilitate de manipulare a datelor și a statutului certificatelor validate; sau
- Verifică valabilitatea semnăturii/sigiliului electronic în conformitate cu cerințele art. 33 din Regulamentul (UE) nr. 910/2014;
- Verifică starea certificatelor în conformitate cu Recomandarea RFC 6960: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP;
- Validează certificatele calificate și semnăturile/sigiliile electronice: verificarea calificării, integrității, autenticității și valabilității;
- Validează mărcile temporale electronice calificate: verificarea calificării, integrității,autenticității și valabilității;
- Îndeplinește procedurile tehnice de validare a semnăturilor în conformitate cu cerințele ETSI

Există trei procese de validare implementate, bazate pe ETSI EN 319 102-1:

- Procesul de validare a semnăturilor de bază;
- Procesul de validare a semnăturilor cu timp și semnături cu materiale de validare pe termen lung;
- Procesul de validare a semnăturilor care asigură disponibilitatea pe termen lung și integritatea materialului de validare, abreviat în raport ca "Procesul de validare a semnăturilor cu date de arhivă".

Aceste procese de validare se bazează, la rândul lor, pe componente, care sunt denumite în ETSI EN 319 102-1 ca:

- Blocurile de bază;
- blocul component de validare a mărcii temporale;
- Blocurile de construcție suplimentare.

QSVP poate furnizainformații addiționale despre semnătură sau sigiliu, de ex. dacă este o semnătură/sigiliu electronic avansat bazat pe un certificat calificat.

Pentru a garanta buna funcționare a serviciului de validare, ZS testează fiecare modificare a funcționalității serviciului de validare,iar testele sunt salvate în documentația internă a ZS. Testele sunt supuse verificării și declarațiilor.

3. Administrarea politicilor

Organizația care administrează prezentul document:

SERVICII ZIPPER
Strada Tăietura Turcului, Nr. 47, Imobilul Novis Plaza, Corp A, Et. 2,
Cluj-Napoca, 400285, România
Punct de lucru:
B-dul 1 Decembrie 1918 nr. 1G,
Sector 3, Bucuresti, 032451, Romania

Punct de lucru:
str. Nikola Tesla, nr. 2, cod 400221
Cluj-Napoca, 400285, Romania
https://ezipper.ro/en/

Adresa de e-mail: office@ezipper.ro
Telefon +40 21.340.4638 / +40 31.101.1020
Telefax: +40 21.340.4636 / +40 31.101.1022
(Luni-Vineri 09.00. – 18:00 ora Europei de Est)
Persoana de contact: Policy Administration Team

4. Aprobarea politicii

Aprobarea acestui document si a modificarilor ulterioare se face de catre persoanele dedicate de ZIPPER. Aceste persoane constituie echipa de administrare a politicilor. PMC aprobă noile versiuni ale acestui document. Versiunile sau actualizările modificate se încarcă în registrul ZIPPER, situat la https://pki.ca.ezipper.ro/repository/policies.php

Versiunile modificate înlocuiesc orice prevederi contradictorii din versiunile anterioare ale acestui document. Echipa de administrare a politicii (PMC) va determina dacă modificările aduse acestui document necesită o modificare a identificatorilor obiectului politicii TS din politicile privind certificatele.

5. REFERINȚE NORMATIVE

Serviciul de validare ZS a fost conceput și dezvoltatîn conformitate cu:

- **ETSI EN 319 401**: Cerințe generale de politică pentru prestatorii de servicii de încredere;
- **ETSI TS 119 441: Cerințe de** politică pentru TSP care furnizează servicii de validare a semnăturii;
- **ETSI TS 119 101: Semnături și** infrastructuri electronice (ESI) – Cerințe de politică și de securitate pentru cererile de creare a semnăturii și de validare a semnăturii;
- **ETSI TS 119 442: Profiluri de** protocol pentru furnizorii de servicii de încredere care furnizează servicii de validare a semnăturilor digitale AdES;
- **ETSI TS 119 172-4:** (Proiect) Politica de semnătură, Partea 4: Politica de validare a semnăturilor pentru semnăturile/sigiliile electronice europene calificate utilizând liste sigure;
- **ETSI EN 319 102-1:** Semnături și infrastructuri electronice (ESI); proceduri pentru crearea și validarea semnăturilor digitale AdES; Partea 1: Creare și validare; 2;
- **ETSI TS 119 102-1:** Proceduri pentru crearea și validarea semnăturilor digitale AdES - Partea 1: Crearea și validarea;
- **ETSI TS 119 102-2:** Proceduri pentru crearea și validarea semnăturilor digitale AdES, Partea 2: Raport de validare a semnăturii;
- **ETSI EN 319 122-1**: Semnături digitale CAdES, Partea1: Blocuri componente și semnături de referință CAdES;
- **ETSI EN 319 122-2**: Semnături digitale CAdES, Partea 2: Semnături CAdES extinse;
- **ETSI EN 319 132-1**: Semnături digitale XAdES, Partea1: Blocuri g încorporateși semnături de referință XAdES;
- **ETSI EN 319 132-** 2: Semnături digitale XAdES, Partea 2: Semnături XAdES extinse;
- **ETSI EN 319 142-1**: Semnături digitale PAdES, Partea1: Blocuri componente și semnături de referință PAdES;
- **ETSI EN 319 142-2**: Semnături digitale PAdES, Partea2: Profiluri suplimentare de semnare PAdES;
- **ETSI EN 319 412:** [semnături și infrastructuri electronice (ESI): profiluri de certificate];
- **IETF RFC 3647:** "Internet X.509 Public Key Infrastructure Certificate Policy and Certification PractiCest Framework;
- **ETSI TS 119 172-1:** Politici de semnătură, Partea 1: Blocuri componente și cuprins pentru documente

de politică privind semnăturile lizibile pentru om;

- **ETSI TS 119 172-2: Politici de semnătură** , Partea 2: Format XML pentru politicile de semnătură;

6. Identificarea TSP

Zipper Services SA [ZS] este furnizorul de servicii calificat pentru validarea semnăturilor și sigiliilor electronice calificate (QSVSP) și este identificat cu un identificator de obiect înregistrat (OID): **1.3.6.1.4.1.57570.**

ZS se asigură că nu modifică în niciun caz identificatorul obiectului acestui document, precum și identificatorii de obiect ai politicilor, practicilor și altor documente de recomandare. Dacă există o extensie/actualizare în politică și practică care nu va afecta certificatele emise anterior, ZS prezintă un nou identificator de obiect care acoperă noile certificate sau cele extinse/actualizate.

7. Politica (politicile) serviciului de validare a semnăturilor acceptate

QSVSP funcționează pe baza unei politici de validare a semnăturilor ca intrare, adică validareasig naturilor / sigiliilor, se efectuează întotdeauna împotriva unei politici de validare. Politicile de validare acceptate și ale căror cerințe sunt utilizate pentru desfășurarea procesului sunt:

ETSI TS 119 441 OIDs pentru politica serviciului de validare a semnăturilor:

- ITU-t(0) organizatie-identificata(4) etsi(0) VAL SERVICE-politici(9441) identificatori de politici(1) principala (1)
- ITU-T(0) identificat – organizație(4) ETSI(0) VAL SERVICE – politici(9441) politică – identificatori(1) calificat (2)

Adică

- OID 0.4.0.9441.1.1 ca politică principală OID pentru serviciile de validare a semnăturilor și
- OID 0.4.0.9441.1.2 ca politică OID pentru servicii de validare a semnăturilor care identifică serviciile de validare calificate, astfel cum sunt definite în articolele 32 și 33 din Regulamentul UE 910/2014 (EIDAS)

În conformitatecu ETSI EN 319 401, este obligatoriu ca un TSP să identifice politicile de servicii pe care le sprijină. Pentru serviciile de validare, un astfel de identificator este comunicat de SVSP prin răspunsurile și/sau rapoartele de validare și prin documentația furnizată subscriberilor și beneficiarilor.

Tipuri de semnătură digitală

Aceste OID-uri indică faptul că semnătura digitală la care este asociat OID este o semnătură digitală de următorul tip corespunzător:

- Semnătura electronică calificată UE - ID-ETSI-DST-EUQESIG - 0.4.0.191724.1.2.1
- Sigiliu electronic calificat UE - ID-ETSI-DST-EUQESEAL - 0.4.0.191724.1.2.4
- Marca temporală electronică calificată UE - ID-ETSI-DST-EUQTST - 0.4.0.191724.1.2.7

8. Componentele serviciului de validare a semnăturilor

8.1 Actori SVS

Cei doi actori principali sunt **ZS** (**QSVSP**), care este un prestator de servicii de încredere calificat (QTSP) și abonatul său.

QSVP poate oferi unul sau mai multe servicii de validare a semnăturilor pe baza relațiilor contractuale.

Serviciul de validare a semnăturii electronice/sigiliului poate fi combinat cu alte servicii pentru îmbunătățirea fiabilității semnăturii (de exemplu, marcarea temporală, augmentarea cu semnătura calificată) în conformitate cu protocolul indicat în ETSI TS 119 442, care sprijină ordinul de sporire a fiabilității semnăturii cu serviciul de validare.

Abonatul interacționează cu cererea de validare a semnăturii și poate fi:

- o cerere sau
- o ființă umană (utilizator)

Alți actori implicați în furnizarea serviciilor de validare a semnăturilor pot fi:

- Semnatarul - semnatarul poate stabili constrângeri asupra semnăturii (de exemplu, prin intermediul unei politici de creare a semnăturii) și acest lucru poate influența validarea semnăturii;
- Prestatorii de servicii de încredere (TSP) ai semnatarilor:
  - TSP care a eliberat certificatul semnatarului (AC);
  - Orice TSP care poate fi implicat în generarea semnăturii:
- Alte TSP (TSA); QSVSP etc.)
- furnizorii de liste sigure europene sau străine;
- Comisia Europeană furnizează lista sigură a furnizorilor de servicii calificați.

ETSI ESI a elaborat mai multe standarde pentru a exprima normele de aplicabilitate a semnăturii sau "politica de semnare" în două **forme**:

- **Într-o forma mai lizibila pentru om**: poate fi evaluat pentru a îndeplini cerințele contextului juridic și contractual în care este aplicat (cf. ETSI TS 119 172-1).
- **Într-o formă prelucrabilă de mașină (XML sau ASN.1):** Pentru a facilita prelucrarea automată a acesteia utilizând normele electronice (cf. E STI TS 119 172-2 și ETSI TS 119 172-3).

9. Arhitectura serviciilor

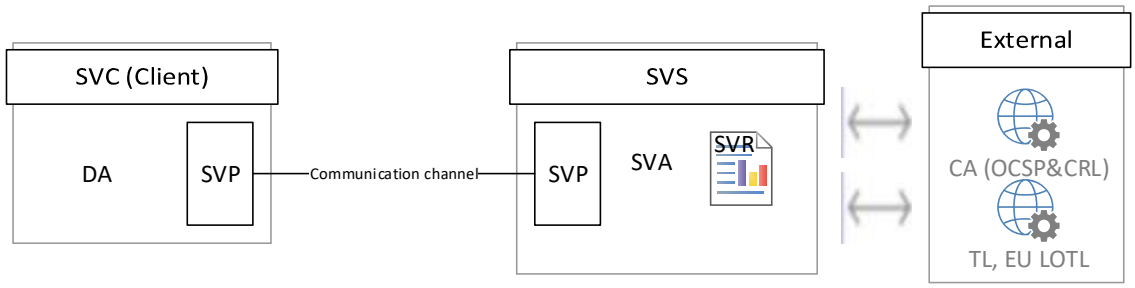
Serverul de servicii de validare a semnăturilor (SVS Serv) implementează SVA, care este componenta serviciului care implementează protocolul de validare a semnăturii (SPV) pe partea QSVSP. Aplicația include implementarea algoritmului devalidare de amendat în ETSI TS 119 1 02-1.

În acest scop, ZS permite serviciului să apeleze factori externi, cum ar fi:

- AC care a eliberat certificatul semnatarului;
- servicii de informare privind starea (OCSP) sau
- listele de certificate revocate (LCR);
- AC ale TSA care au furnizat mărci temporale;
- alte QSVSP pentru controale complementare;
- listele sigure ale statelor membre ale UE;
- lista sigură a Comisiei Europene etc.

SVA construiește răspunsul de validare a semnăturiipe algoritmul de validare, care include:

- verificarea formatului;
- identificarea certificatului semnatarului;
- contextul validării;
- Validare X.509,
- validarea criptografică;
- acceptarea semnăturii (adică cerințele de validare a semnăturii) etc.



Aplicațiile de semnătură / validare (VA) ale ZS pot fi configurate să funcționeze pe serverul ZS (prin conexiune la Internet la serverul Signature Validation Service (SVS Serv)).

- Solicită validarea semnăturii la serviciul de validare a semnăturii(SVSServ);
- Este posibil să se solicite validarea semnăturilor multiple în conformitate cu ETSI TS 119 442;
- Execută protocolul de validare a semnăturii (SVP) pe partea utilizatorului;
- Când este cazul, se ocupă de prezentarea raportului de validare ;

Clientul poate încorpora:

- O interfață utilizator pentru introducerea manuală a cererii; sau
- O interfață mașină pentru solicitări automate; Cererea trebuie încorporată în aplicația 3rd party (de exemplu, aplicația de arhivare Zipper RepoLTA)
- O interfata utilizator pentru a prezenta raportul.
- Raportul de validare trebuie să conțină marca temporală calificată Zipper Services, care este în conformitate cu Regulamentul (UE) nr. 910/2014;
- Verificarea aplicabilitatii, respectiv decizia finala de "acceptare" a unei semnaturi/sigilii pe baza raportului de validare se poate face de catre utilizator (manual), sau de catre client sau server (in functie de implementarea SVS). Acest lucru se poate face în conformitate cu regulile de aplicabilitate a semnăturilor specificate în ETSI TS 119 172-1;
- În cazul semnăturilor/sigiliilor multiple pe același raport, aplicația client (DA) va utiliza rezultatul validării semnăturilor/sigiliilor respective și va interpreta rezultatul în funcție de contextul de business în care este aplicat. De asemenea, va permite selectarea, dacă este necesar, a semnăturii specifice care urmează să fie verificată în cazul în care conținutul verificat conține semnături multiple.

NOTĂ: Prezentul document nu impune cerințe clientului. Doar elementele DA implementate pe partea de server sunt supuse cerințelor.

10. DEFINIȚII ȘI ABREVIERI

10.1 DEFINIȚII

Se aplică termenii și definițiile date în ETSI EN 319 401 și ETSI TR 119 001, precum și următoarele:

verificarea aplicabilității - determinarea conformității unei semnături cu regulile de aplicabilitate a semnăturii. Verificarea aplicațiilorcompletează serviciul de validare a semnăturilor.

tipul angajamentului (semnătură) - implicația semnăturii;

constrângere de creare (semnătură) - criterii utilizate la crearea unei semnături digitale;

DSS (Digital Signature Service) - este o bibliotecă software open-source, menită să asigure implementarea standardelor pentru crearea, augmentarea și validarea semnăturilor electronice avansate în conformitate cu legislația europeană și Regulamentul eIDAS în special.

aplicație de conducere (DA) - o aplicație care utilizează un sistem de creare a semnăturii pentru a crea sau valida o semnătură. În procesul semnătură valiniere, aplicația furnizează semnătura digitală AdES și alte date de intrare către o aplicație de validare a semnăturii (SVA);

serviciu calificat de validare a semnăturilor electronice calificate – conform prevederilor art. 33 din Regulamentul (UE) nr. 910/2014;

serviciu calificat de validare a sigliiilor electronice calificate - astfel cum se specifică la art. 40 din Regulamentul (UE) nr. 910/2014;

furnizor de servicii de validare calificat (QSVSP) - furnizor de servicii care oferă servicii de validare calificată pentru validarea electronică calificată a ignatures/sigiliilor;

acceptarea semnăturii - un proces tehnic definit în ETSI TS 119 102-1 care face parte din procesul de validare a semnăturii. Se realizează prin depunerea unei cereri de validare a semnăturii;

Reguli de aplicabilitate a semnăturii - un set de reguli aplicabile uneia sau mai multor semnături digitale care definesc cerințele pentru a determina dacă o semnătură este potrivită pentru un anumit scop comercial sau juridic. Aceste reguli includ politici de validare a semnăturilor care conțin constrângeri de validare. ETSI TS 119 172-1 se aplică în aceste scopuri.

clasa semnăturii - un set de semnături care realizează o anumită funcționalitate (de exemplu, o semnătură cu timpul, o semnătură pentru validare pe termen lung etc.).

dispozitiv de creare a semnăturii - software sau hardware configurat utilizat pentru crearea unei semnături electronice;

cerere de validare a semnăturii (SVA) - o aplicație care validează o semnătură în raport cu o politică de validare a semnăturii și care produce o indicație a stării validării semnăturii și un raport de validarea semnaturii. Cererea de validare a semnăturii este specificată în ETSI TS 119 1 02 1;

client de validare a semnăturii (SVC) - o componentă sau un software care implementează protocolul de validare a semnăturii din partea utilizatorului;

Politica de validare a semnăturii - un set de constrângeri de validare a semnăturii procesate sau care urmează să fie prelucrate de SVA. Politica de validare a semnăturilor este un concept pur tehnic. Politica de validare a semnăturii definește regulile de aplicabilitate a semnăturii;

raport de validare signature (SVR) - un raport cuprinzător al validării furnizat de cererea de validare a semnăturii către DA și care permite aplicației de conducere și oricărei părți din afara aplicației de conducere să inspecteze detaliile luate în timpul validăriișisă investigheze cauzele detaliate ale indicației de stare furnizate semnăturii. Raportul poate fi în conformitate cu ETSI TS 119 1 02-2, iar cerințele minime privind conținutul său sunt definite în clauza 5.1.3 din ETSI TS 119 102-1;

Politica Signature Validation Service (SVS) - acesta este un set de reguli care indică calitatea și aplicabilitatea unui serviciu de validare a semnăturilor. Documentul determină aplicabilitatea serviciului la o anumită comunitate și/sau clasă de aplicații cu cerințe comune de securitate . Politica SVS se aplică unui serviciu de încredere, astfel cum este definit în ETSI EN 31 9 401;

declarație practică privind serviciul de validare a semnăturilor (SVS) - aceasta este o declarație privind practicile și procedurile utilizate pentru a răspunde tuturor cerințelor identificate pentrufurnizarea serviciului de validare a semnăturilor. Declarația de practică se aplică unui serviciu de încredere care face parte din documentația QSVSP în conformitate cu ETSI EN 319 401;

server de servicii de validare a semnăturilor - componentă care implementează protocolul devalidare a semnăturii și procesează validarea semnăturii din partea QSVSP;

starea validării semnăturii - una dintre următoarele indicații: TOTAL-PROMOVAT, TOTAL-EȘUAT sau NEDETERMINAT;

validarea semnăturii - proces de verificare și confirmare a validitățiitehnice a semnăturii unei săpături;

verificarea semnăturii - proces de verificare a valorii criptografice a unei semnături utilizând datele de verificare a semnăturii;

semnatar - o entitate care este creatorul unei semnături digitale;

constrângere de validare a semnăturii - criterii tehnice pe baza cărora poate fi validată o semnătură digitală, astfel cum se specifică în ETSI TS 119 1 02-1;

utilizator - o aplicatie sau o fiinta umana care interactioneaza cu aplicatia de validare a semnaturii;

validare - procesul de verificare și confirmare a validității semnăturii sau sigiliului electronic;

date de validare - date care sunt utilizate pentru validarea unei semnături electronice sau a unui sigiliu electronic;

validarea unei semnături electronice calificate – conform prevederilor art. 32 din Regulamentul (UE) nr. 910/2014;

validarea sigiliilor electronice calificate - astfel cum se specifică la art. 40 din Regulamentul (UE) nr. 910/2014;

serviciu de validare - sistem accesibil prin intermediul unei rețele de comunicații, care validează o semnătură digitală;

verificator - entitate care dorește să valideze sau să utilizezeo semnătură digitală.

10.2ABREVIERI

Se aplică termenii și definițiile date în ETSI EN 319 401 și ETSI TR 119 001, precum și următoarele:
AdES - Semnătură electronică avansată
API - Interfață de programare a aplicațiilor
ASiC - Containere de semnătură asociate
BB - Blocul de construcție (DIGITAL)
CA Autoritatea de certificare
CAdES CMS - Semnături electronice avansate

CMS - Sintaxa mesajelor criptografice
CRL - Lista de revocare a certificatelor
CSP - Furnizor de servicii criptografice
DA - aplicație de conducere;
DER Reguli decodificare distinse ed
EC DIGITAL BLOCUL DIGITAL
DSA Digital Signature Algorithm - un algoritm pentru criptografie cu chei publice
DSS Serviciul de semnătură digitală al Comisiei Europene Digital Building Blocks
ESI Semnături și infrastructuri electronice
ETSI Institutul European de Standardizare în Telecomunicații
EUPL Licența publică a Uniunii Europene
HSM Module de securitate hardware
OCSP Protocolul de stare a certificatului online
ODF Open Document Format
ODT Open Document Text
PAdES PDF Semnături electronice avansate
PMC Organismul de guvernanță internă al TSP
PoE Dovada existenței**;**
PKCS Standarde criptografice cu cheie publică
PKCS#12 Acesta definește un format de fișier utilizat în mod obișnuit pentru a stoca cheia privată X.509 care însoțește certificatele de cheie publică, protejate prin parolă simetrică
PKIX Internet X.509 Infrastructura de chei publice
RSA Rivest Shamir Adleman - un algoritm pentru criptografie cu cheie publică
OVR - OveRall/Cerințe generale aplicabile mai mult de 1 (una) componentă;
QES - semnătură electronică calificată sau sigiliu electronic calificat;
(Q) SCD - dispozitiv de creare a semnăturii (calificat);
QSVSP - furnizor de servicii calificate de validare a semnăturilor;
SCA Aplicație de creare a semnăturilor
SD - Documentul semnatarului;
SDO - obiect de date semnat;
DST - reprezentarea documentelor semnate;
SSCD Secure Signature-Creatipe dispozitiv
SVA – Cerere de validare a semnăturii/sigiliului;
SVP – Protocol de validare a semnăturii/sigiliului;
SVR – Raport de validare a semnăturii/sigiliului;
SVS – Serviciul de validare a semnăturilor/sigiliilor;
SVSServ – Server de servicii de validare a semnăturilor/sigiliilor;
TL Lista sigură
TSA Autoritatea Marca temporala
TSL Lista de stare a serviciului de încredere
TSP Furnizor de servicii de încredere
TST Token cu marcaj temporal
UCF Formatul universal al containerului
XAdES XML Semnături electronice avansate
ZIP Format de fișier utilizat pentru compresia și arhivarea datelor
VPR – Procesul de validare semnaturi/seal.

11. Politici și practici

Politica SVS este integrată în acest document și conține informații despre aplicabilitatea serviciului. Beneficiarii serviciilor pot fi persoane fizice sau juridice și beneficiari. Politica oferă informații despre nivelul serviciului.

Identificatorul acestei Politici de Certificare va fi modificat numai dacă există modificări substanțiale care afectează aplicabilitatea acesteia.

– Arborele OID	
1.3.6.1.4.1.57570	Numărul de identificare (OID) al Zipper Services SRL, înregistrat la IANA
1.3.6.1.4.1.57570.4.2.1.1	Serviciul de validare **respectă criteriile de validare ETSI TS 119 441**
1.3.6.1.4.1.57570.4.2.2.3	Serviciul de validare calificat **respectă criteriile de validare calificată ETSI TS 119 441**

4 (validare) .2 (serviciu calificat de validare a semnăturilor). X(Politica). Y(versiune)

Această politică de validare este actualizată permanent și publicată la https://pki.ca.ezipper.ro/repository/policies.php

Notă: Raportul de validare specifică cheia și nivelul semnăturii/ sigiliului electronic validat. Partea terță de încredere este responsabilă pentru determinarea aplicabilității sale în scopul comercial și, prin urmare, acceptarea sau respingerea acesteia.

ZS se asigură că nu modifică identificatorul obiectului acestui document, precum și identificatorul obiectului politicilor, practicilor și altor documente de recomandare în niciun caz. Dacă există o extensie/actualizare în politică și practică care nu va afecta certificatele emise anterior, ZS prezintă un nou identificator de obiect care acoperă noile certificate sau cele extinse/actualizate.

Serviciul de validare a semnăturii (QSVSP) este integrat în acest document și a fost elaborat, aplicat și actualizat conform specificațiilor ETSI EN 31 9 401. Declarația de practică SVS descrie modul în care ZS implementează serviciul și este deținută de QSVSP. Declarația de practică este accesibilă auditorilor, utilizatorilor și beneficiarilor. Prezentul document descrie metoda de îndeplinire a cerințelor care au fost identificate ca fiind necesare pentru menținerea calității ridicate a serviciului de validare a semnăturilor .

12. UTILIZAREA CERTIFICATULUI ȘI APLICABILITATEA SERVICIULUI DE VALIDARE

ZS oferă un serviciu de validare calificată a semnăturilor și sigiliilor electronice care permite beneficiarilor să primească un raport privind procesul de validare a semnăturii/sigiliului într-un mod automat și fiabil.

Serviciul SV poate fi combinat cu alte servicii pentru îmbunătățirea semnăturii, în conformitate cu protocolul indicat în ETSI TS 119 442 care susține ordinul de sporire a fiabilității semnăturii cu validarease rvice.

Raportul SV trebuie generat independent în format XML și criptat pentru a proteja integritatea. Criptarea are loc prin aplicarea unei semnături de arhivă pe termen lung (semnătură de nivel LTA) cu un furnizor calificat de mărci temporale și garantează căaturile de semnătură și sigiliile sunt generate și validate în conformitate cu legislația europeană (eIDAS).

O altă soluție pe care ZS a implementat-o este validarea semnăturii electronice a documentului dat înainte ca documentul să fie aprobat pentru arhivare. Documentul care urmează să fie arhivat este ambalat într-un container digital împreună cu Raportul SV, precum și alte metadate care detaliază procesul de arhivare. În pasul următor,

containerul este criptat pentru a proteja integritatea. Criptarea are loc prin aplicarea unei semnături de arhivă pe termen lung (semnătură la nivel LTA) cu un furnizor calificat de mărci temporale și marcată electronic prin servicii de marcare temporală calificată ZIPPER. Containerul este creat pe baza profilului de bază Associated Signature Container (ASiC) pentru container și CMS Advanced Electronic Signature (CAdES) pentru criptare.

13. Gestionarea și operarea serviciilor de încredere

13.1 Managementul securității

ZS QSVP asigură aplicarea procedurilor administrative și de gestionarecare sunt adecvate și corespund celor mai bune practici recunoscute.

ZIPPER îndeplinește toate funcțiile SV folosind sisteme de încredere care îndeplinesc cerințele ZIPPER ISMS.

13.2 Clasificarea și gestionarea activelor

ZIPPER menține un inventar al tuturor activelor și atribuie acestor active o clasificare a cerințelor de protecție în conformitate cu analiza riscurilor.

13.3 Securitatea personalului

ZIPPER menține controale adecvate ale personalului, îndeplinind cele mai bune practici de securitate și cerințele standardelor relevante.
Personalul de conducere și operațional posedă abilitățile și cunoștințele adecvate despre SV, semnăturile digitale și serviciile de încredere, precum și procedurile de securitate pentru personalul cu responsabilități de securitate , securitatea informațiilor și evaluarea riscurilor.
ZIPPER implementează Politica privind rolurile de încredere pentru toți acei angajați care au acces la sau controlează operațiunile criptografice. Persoanele și rolurile de încredere includ, dar nu se limitează la:

- Personal pentru operațiuni criptografice de afaceri,
- personalul de securitate,
- personalul administrativ al sistemului,
- Personal de inginerie desemnat și
- Directori care sunt desemnați să gestioneze credibilitatea infrastructurii.

Înainte de a începe angajarea într-un rol de încredere, ZIPPER efectuează verificări ale antecedentelor, care pot include, cu titlu indicativ, următoarele:

- Verificarea identității
- Verificarea angajării anterioare și a referințelor profesionale;
- Confirmarea celui mai înalt sau cel mai relevant grad educațional obținut;
- Verificarea faptului că nu există o condamnare penală;
- Verificarea înregistrărilor financiare.

ZIPPER solicită ca personalul care dorește să devină Persoane de încredere să prezinte dovada pregătirii, calificărilor și experienței necesare pentru a-și îndeplini responsabilitățile viitoare de serviciu, așa cum se specifică în contractul de muncă și în fișa postului, înainte de a îndeplini orice funcții operaționale sau de securitate.
Contractele de muncă semnate de angajați includ dispoziții de confidențialitate pentru informațiile care le vin la cunoștință în cursul prestării lor.
ZIPPER se asigură că personalul a obținut statutul de încredere și că aprobarea departamentală a fost dată înainte ca acest personal să fie:

- Dispozitivele de acces emise și accesul acordat la facilitățile necesare;
- A emis acreditări electronice pentru a accesa și a efectua funcții specifice pe SVA sau alte sisteme IT.

Conturile de utilizator sunt create pentru personalul cu roluri specifice care au nevoie de acces la sistemul în cauză. Toți utilizatorii trebuie să se conecteze cu un cont dedicat, iar comenzile administrative sunt disponibile numai cu permisiunea explicită. Permisiunile sistemului de fișiere și alte caracteristici disponibile în modelul de securitate al sistemului de operare sunt utilizate pentru a preveni orice altă utilizare. Conturile de utilizator sunt blocate cât mai curând posibil atunci când schimbarea rolului dictează.

13.4 Securitatea fizică și a mediului

ZIPPER QSVP implementează Politica de Securitate Fizică, care susține cerințele de securitate ale acestei Declarații SV Policy &; Practice.
Operațiunile ZIPPER QSVP se desfășoară într-un mediu protejat fizic care descurajează, previne și detectează utilizarea, accesul sau divulgarea neautorizată a informațiilor și sistemelor sensibile.
ZIPPER menține, de asemenea, facilități de recuperare în caz de dezastru pentru operațiunile sale de servicii de validare a semnăturilor. Facilitățile ZIPPER de recuperare în caz de dezastru suntprotejate de mai multe niveluri de securitate fizică comparabile cu cele ale instalației principale a ZIPPER.
Operațiunile ZIPPER sunt protejate folosind controale fizice de acces, făcându-le accesibile numai persoanelor autorizate în mod corespunzător. Accesul în zonele securizate ale clădirilor necesită utilizarea unui card de "acces" și/sau a datelor biometrice. Utilizarea cardului de acces este înregistrată de sistemul de securitate al clădirii.
Jurnalele cardurilor de acces sunt revizuite în mod regulat.
Facilitățile securizate ale ZIPPER sunt echipate cu echipamente primare și de rezervă:

- Sistemul de alimentare pentru a asigura accesul continuu, neîntrerupt la energia electrică și
- Sisteme de încălzire/ventilație/aer condiționat pentru controlul temperaturii și umidității relative.

ZIPPER a luat măsuri de precauție rezonabile pentru a minimiza impactul expunerii la apă a instalațiilor sale, precum și pentru a preveni și stinge incendiile sau alte expuneri dăunătoare la flacără sau fum.
Toate suporturile care conțin software și date de producție, informații de audit, arhivă sau backup sunt stocate în instalațiile ZIPPER sau în instalații de depozitare securizate în afara amplasamentului, cu controale de acces fizice și logice adecvate, concepute pentru a limita accesul personalului autorizat și pentru a proteja astfel de medii împotriva deteriorării accidentale.
ZIPPER stochează în siguranță toate suporturile amovibile și hârtia care conțin informații sensibile legate de operațiunile sale în containere sigure. Documentele și materialele sensibile sunt mărunțite înainte de eliminare. Suporturile utilizate pentru colectarea sau transmiterea informațiilor sensibile sunt de culoare roșie, ilizibile înainte de eliminare. Dispozitivele criptografice sunt distruse fizic înainte de eliminare.

13.5 Managementul operațiunilor

ZIPPER QSVP se asigură că procedurile, procesele și infrastructura respectă managementul operațional, echipamentele procedurale de securitate, managementul accesului la sistem, implementarea și întreținerea sistemelor de încredere, managementul continuității afacerii și gestionarea incidentelor, așa cum sunt definite în ETSI EN 319 421.
Procedurile de gestionare a operațiunilor pentru ZIPPER QSVP sunt încorporate în procedurile generale de gestionare a operațiunilor interne ZIPPER.

13.6 Compromiterea Serviciului SV

În cazul compromiterii serverului care oferă SV Service, ZIPPER nu va emite validarea semnăturii până când nu se iau măsuri pentru restaurarea serverului.

13.7 Validarea semnaturii si Terminarea serviciului

Serviciul SV este reziliat:

- cu o decizie a Consiliului de Administrație al ZIPPER;

- cu o decizie a autorității care exercită supravegherea asupra serviciilor de validare a semnăturilor;
- cu o hotărâre judecătorească;
- la lichidarea sau încetarea operațiunilor ZIPPER
- încetarea activității ca urmare a unui dezastru sau a unui motiv semnificativ din care nu este posibilă o recuperare satisfăcătoare.

ZIPPER se asigură că potențialele perturbări ale abonaților și beneficiarilor sunt reduse la minimum ca urmare a încetării serviciilor ZIPPER și, în special, asigură menținerea continuă a informațiilor necesare pentru verificarea corectitudinii serviciilor.

13.8 Conformarea cu cerințele legale

ZS, în calitate de QSVP, aplică cerințele specificate în clauza 7.13 din ETSI EN 31 9 401 pentru a asigura conformitatea cu cerințele legale:

- Garantează că funcționează într-o manieră legală și demnă de încredere;
- Oferă dovezi cu privire la modul în care îndeplinește cerințele legale aplicabile;
- Serviciile de încredere prestate șiprodusele utilizatorilor utilizate pentru furnizarea acestor servicii sunt accesibile persoanelor cu handicap, acolo unde este posibil;

Sunt luate măsuri tehnice și organizatorice adecvate împotriva prelucrării neautorizate sau ilegale a datelor cu caracter personal și împotrivapierderii, distrugerii sau deteriorării accidentale a datelor cu caracter personal. ZS garantează că datele cu caracter personal sunt prelucrate în conformitate cu Regulamentul (UE) nr. 2016/679. În această privință, autentificarea pentru un serviciu online privește prelucrarea numai a acelor date de identificarecare sunt adecvate, relevante și neexcesive.

În plus, se aplică următoarele cerințe specifice:

- QSVSP nu stochează documentul semnatarului (SD) după procesare atunci când nu este necesar. În cazul în care serviciul de validare funcționează în combinație cu un serviciu de conservare pe termen lung (de exemplu, un serviciu de arhivare), ar putea fi necesară păstrarea acestor date, pe baza unui acord contractual.

QSVSP are responsabilitatea generală pentru îndeplinirea cerințelor definite mai sus atunci când unele sau toate funcțiile salesunt asumate de subcontractanți.

Serviciul este furnizat în conformitate cu cerințele pentru validarea calificată a semnăturilor electronice calificate prevăzute în Regulamentul (UE) nr. 91 0/2014 (eIDAS: articolele 32 și 33) și a sigiliilor (eIDAS: articolul 40)

Articolul 32 - Cerințe pentru validarea semnăturilor electronice calificate

Procesul de validare a unei semnături electronice calificate confirmă valabilitatea unei semnături electronice calificate, cu condiția ca:

-certificatul care stă la baza semnăturii era, la momentul semnării, certificat calificat pentru semnătură electronică conform cu anexa I;	Procesul de validare a semnăturilor electronice calificate îndeplinește cerințele UE pentru prestatorii de servicii de încredere calificați și este conformcu anexa I (Cerințe pentru certificatele calificate pentru semnăturile electronice)
- certificatul calificat a fost emis de un prestator de servicii de încredere calificat și era valabil la momentul semnării;	Procesul de validare a semnăturilor electronice calificate impunecerințele UE pentru prestatorii de servicii de încredere calificați care emit certificate calificate pentru o semnătură electronică și pentru un sigiliu electronic.

- datele de validare a semnăturii corespund datelor furnizate beneficiarului;	Acest lucru este garantat prin formatele acceptate pentru semnătură/sigiliu electronic.
-setul unic de date reprezentand semnatarul in certificat este furnizat corect beneficiarului;	Serviciul creează automat un **raport de validare** care conține datele din certificatele de semnătură/sigiliu electronic utilizate pentru semnarea documentului pe care serviciul l-a validat în mod corespunzător.
-utilizarea oricărui pseudonim este indicată în mod clar beneficiarului dacă la momentul semnării a fost utilizat un pseudonim;	Pseudonimul este scris într-un atribut special în câmpul Subiect și acest lucru asigură că există o indicație clară a acestui fapt pentru partea de încredere.
-semnătura electronică a fost creată printr-un dispozitiv de creare a semnăturilor electronice calificat;	Procesul calificat devalidare a semnăturii lectronice îndeplinește cerințele UE pentru a verifica dacă semnătura electronică a fost creată de un dispozitiv calificat de creare a semnăturilor electronice (SSCD pentru QSign/QSeal).
-integritatea datelor semnate nu a fost compromisă;	Acest lucru este asigurat prin metodologia de verificare și validare a documentelor semnate electronic descrise în această politică.
- cerințele prevăzute în art. 26 au fost îndeplinite în momentul semnării.	Validarea semnăturii process îndeplinește cerințele UE pentru verificarea cerințelor articolului 26 (cerințe pentru o semnătură electronică avansată): -este legată în mod unic de semnatar; - este capabil să identifice semnatarul;este creată utilizând date de creare a semnăturilor electronice pe care semnatarul le poate utiliza, cu un nivel ridicat de încredere, exclusiv sub controlul său; și este legată de datele semnate astfel încât orice modificare ulterioară a datelor să poată fi detectată. Aceste verificări sunt efectuate pentru toate formatele acceptate de serviciu.
Sistemul utilizat pentru validarea semnăturii electronice calificate furnizează beneficiarului rezultatul corect al procesului de validare și permite beneficiarului să detecteze orice probleme relevante din punctul de vedere al securității.	Acest lucru este asigurat prin metodologia de verificare și validare a documentelor semnate electronic descrise în această politică și practică.

Articolul 33 – Serviciul calificat de validare a semnăturilor electronice calificate

Un serviciu de validare calificat pentru semnăturile electronice calificate poate fi prestat numai de un prestator de servicii de încredere calificat care: - asigură validarea în conformitate cu articolul 32 alineatul (1) și permite beneficiarilor să primească rezultatul procedurii de validare într-un mod automat, care este fiabil, eficient și poartă semnătura electronică avansată sau sigiliul electronic avansat al prestatorului serviciului de validare calificat.	Respectarea articolului 32 este prezentată la alineatul precedent.
Comisiapoate, prin intermediul actelor de punere în aplicare, să stabilească numere de referință ale standardelor pentru serviciul de validare calificat menționat la alineatul (1). În cazul în care serviciul de validare pentru o semnătură electronică calificată îndeplinește standardele respective, se presupune că respectă cerințele prevăzute la alineatul (1). Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (2).	Acest lucru este asigurat prin metodologia pentru Verificarea și validarea electronică documente semnate și prin procesul de primire a raportului de validare descris în această politică.

Articolul 40 Validarea și păstrarea sigiliilor electronice calificate

Articolele 32, 33 și 34 se aplică mutatis mutandis validării și păstrării sigiliilor electronice calificate.	Serviciul acoperă, de asemenea, validarea sigiliilor electronice în conformitate cuarticolul 40.

13.9 Înregistrarea serviciilor de validare a semnăturilor

ZIPPER QSVP se asigură că toate informațiile relevante privind operațiunile serviciilor ZIPPER SV sunt înregistrate pentru o perioadă definită, în special pentru furnizarea de dovezi în scopul procedurilor judiciare. Se păstrează următoarele înregistrări:

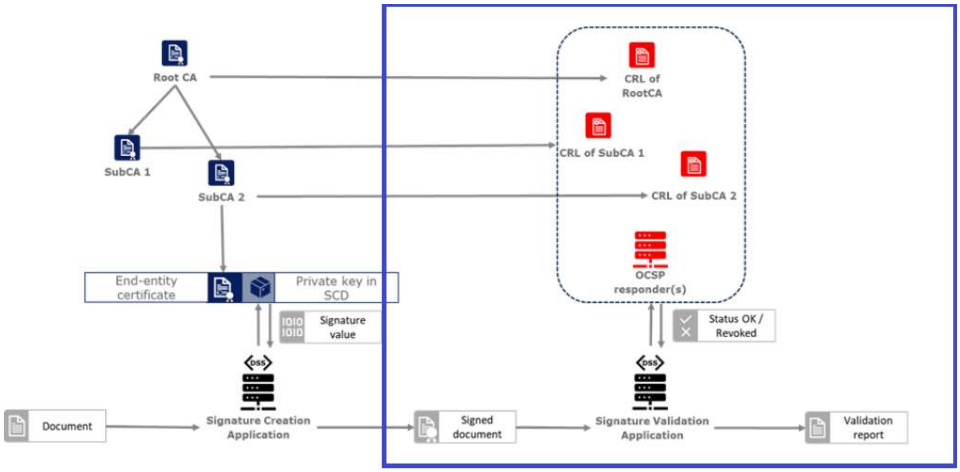
- SV solicită toate informațiile pertinente, transmise de solicitant sau colectate electronic pentru validarea semnăturii electronice sau a sigiliului electronic, incluzând cel puțin data și ora validării semnăturii sau sigiliului electroniccalificat, datele furnizate de solicitant pentru validarea semnăturii sau sigiliului (valoarea semnăturii electronice sau a sigiliului electronic, dacă acesta din urmă poate fi separat degned document sau reprezentare unică a documentului semnat în caz contrar), precum și identitatea solicitantului (IP de unde accesează serviciul), raportul care conține rezultatul validării semnăturii sau sigiliului electronic calificat cu datele externe (liste sigure, LOTL UE, liste de certificate revocate, răspunsuri OCSP utilizate pentru validarea semnăturii sau a sigiliului.

13.10 Fiabilitate organizațională

ZIPPER TSA se asigură că organizarea sa este fiabilă, conform cerințelor ETSI EN 319 421. ZIPPER dispune de stabilitatea financiară și resursele necesare pentru a funcționa în conformitate cu prezenta Declarație de politică și practică TSA.

13.11 Proiectarea serviciului de validare a semnăturilor

Standardul ETSI EN 319 102-1 specifică un model complet de validare și proceduri pentru validarea "semnăturilor digitale AdES", care sunt implementate în aplicația ZS SVA.



Rezultatul unui proces de validare efectuat în conformitate cu aceste procedurieste un raport de validare și o indicație care poate fi:

- TOTAL-TRECUT indicând faptul că semnătura a trecut verificarea și respectă politica de validare a semnăturii.
- NEDETERMINAT, indicând faptul că verificările formatului și semnăturii digitale nu au eșuat, dar nu există informații suficiente pentru a determina dacă semnătura electronică este validă.
- TOTAL_FAILED indicând fie că formatul semnăturii este incorect, fie că valoarea semnăturii digitale nu trece verificarea.

În general, validation a unei semnături se face împotriva unui set de constrângeri, din care constrângerile criptografice fac parte, care este, de asemenea, uneori menționată ca o politică de validare a semnăturii.

Pentru fiecare verificare/restricție de validare (de exemplu, formatul semnăturii, valabilitatea certificatului de semnare), procesul de validare trebuie să furnizeze informații care să justifice motivele indicării statutului rezultat ca urmare a verificării în raport cu constrângerile aplicabile. În plus, standardul ETSI definește o modalitate consecventă și precisă de justificare a stărilor în temeiul unui set de subindicații. Acest lucru permite utilizatorului să determine dacă validarea semnăturii a reușit și motivul în caz de eșec.

13.12 Formate de semnătură acceptate

Aplicația SV acceptă **formate de semnătură**:

XAdES - pentru semnături electronice XML Advanced;

CAdES - pentru semnături electronice avansate CMS;

PAdES - pentru semnături electronice avansate PDF (cf. [R03]);

JAdES - pentru semnăturile electronice avansate JSON (cf. [R05]);

ASIC – pentru containerele asociate semnatura (ETSI EN 319 162) sunt posibile combinații XAdES și CAdES.

În conformitate cu:

a) ETSI TS 103 171 (profilul de referință XAdES);

b) ETSI TS 103 172 (profilul de referință al PAdES);

c) ETSI TS 103 173 (profilul de referință CAdES);

d) ETSI TS 103 174 (profilul de referință ASiC); și

e) Standardele ETSI privind profilurile de referință pentru semnăturile digitale CAdES (ETSI EN 319 122-1), semnăturile digitale XAdES (ETSI EN 319 132-1) și semnăturile digitale PAdES (ETSI EN 319 142-1).

13.13 Procese de validare implementate

- ***Procesul de validare pentru semnăturile de bază (-*** B) (a se vedea ETSI EN 319 102-1 clauza 5.3): ar trebui aplicat semnăturilor în cazul în care momentul validării se află în perioada de valabilitate a certificatului de semnare și certificatul de semnare nu a fost revocat.

- **Procesul de validare pentru semnăturile cu timp (-T) și semnăturile cu material de validare pe termen lung (-LT)** (a se vedea ETSI EN 319 102-1 clauza 5.5). SVA poate utiliza datele de validare stocate în semnătură pentru validare.

- **Procesul de validare pentru semnaturi asigură disponibilitatea pe termen lung și integritatea materialului de validare (-LTA) (** a se vedea ETSI EN 319 102-1 clauza 5.6).

Reguli:

- Procesul de validare pentru semnătura de bază este executat în raport cu prima dată, care este timpul (curent) de validare;

- Procesul de validare pentru semnături cu timpși semnături cu material de validare pe termen lung este executat pentru a doua oară, care este "cel mai bun timp de semnătură" care este determinat folosind marca temporală a semnăturii;

- Procesul de validare a semnăturilor cu date de arhivă este executat în raport cu o a treia oară, care este "cel mai bun timp de semnătură" determinat folosind toate afirmațiile de timp prezente în semnătură.

Rezultatul global al validării este furnizat ca indicația returnată de procesul de validare pe baza căruiaa fost efectuată validarea.

SVA este compatibil cu următoarele profiluri de bază:

XAdES	CAdES	PAdES	JAdES
XAdES-B-B	CAdES-B-B	PAdES-B-B	JAdES-B-B
XAdES-B-T	CAdES-B-T	PAdES-B-T	JAdES-B-T

XAdES-B-LT	CAdES-B-LT	PAdES-B-LT	JAdES-B-LT
XAdES-B-LTA	CAdES-B-LTA	PAdES-B-LTA	JAdES-B-LTA

13.14 Rezultatul procesului de validare

În funcție de formatul semnăturii/sigiliului electronic utilizat, serviciul sprijină procesele de validare pentru formatele de bază ale semnăturii/sigiliului și formatele avansate (cu date suplimentare de verificare electronică a mărcii temporale sau a orei), după cum urmează (Pentru o descriere detaliată a semnificației acestora, consultați ETSI EN 319 102-1):

Informații introduse în raport		**Semantică**
Semn	**Raportați datele**	
TOTAL PROMOVAT	Procesul de validare generează lanțul de certificate validat, inclusiv certificatul pentru semnătură/sigiliu electronic utilizat în procesul de validare.	Procesul de validare calificată a semnăturilor și sigiliilor electronice are ca rezultat TOTAL-TRECUT pe bazaurmătoarelor considerente: • verificările criptografice ale semnăturii/sigiliului electronic cu succes (inclusiv verificări ale hash-urilor obiectelor de date individuale care au fost semnate indirect); • orice restricții aplicabile certificării identității semnatarului au fostvalidate pozitiv (adică certificatul de semnătură a fost considerat demn de încredere); și • Semnătura/sigiliul electronic a fost validat pozitiv în raport cu constrângerile de validare și, prin urmare, este considerat conform cu aceste constrângeri.
TOTAL-EȘUAT	Rezultatele procesului de validare informații suplimentare pentru a explica indicația TOTAL-RESPINS pentru fiecare dintre constrângerile de	Procesul de validare a semnăturilor și sigiliilor electronice calificate are ca rezultat TOTAL-EȘUAT deoarece verificările criptografice ale semnăturii/sigiliului electronic au eșuat (inclusiv

	validare care au fost luate în considerare și pentru care a avut loc un rezultat negativ.	verificările hash-urilor obiectelor de date individuale care au fost semnate indirect) sau s-a dovedit că generarea semnăturii/sigiliuluia avut loc după revocarea acesteia.
NEDETERMINAT	Rezultatele procesului de validare Informații suplimentare pentru explicați NEDETERMINATUL pentru a ajuta verificatorii să identifice datele care lipsesc pentru a finaliza procesul de validare.	Informațiile disponibile sunt insuficiente pentru proces de validare pentru a stabili TOTAL-Starea ADMIS sau TOTAL RESPINS a mnătură/sigiliu electronic.

13.15 Cerințe privind procesul de validare a semnăturii

Procesul implementat de validare a semnăturii urmează algoritmul ETSI TS 119 102-1.

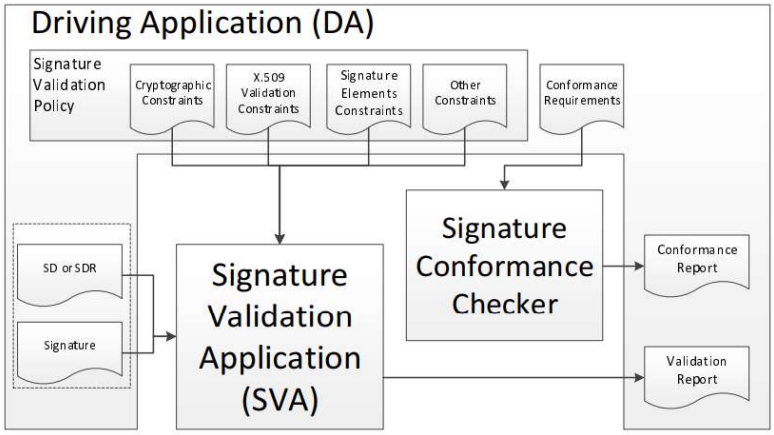


Fig.. Model conceptual de validare

Standardul definește modelul conceptual prin împărțirea software-ului cu funcții de validare a semnăturii în două părți:

- o semnătură validatila cerere (SVA); și
- o aplicație de conducere (DA).

Aplicația de validare a semnăturii (SVA) primește o semnătură digitală AdES și alte informații de la aplicația de conducere (DA). SVA validează semnătura în raport cu o politică de validare asemnăturii, constând într-un set de constrângeri de validare, și emite o indicație de stare și un raport de validare care furnizează detalii privind validarea tehnică a fiecăreia dintre constrângerile aplicabile, care pot fi relevante pentru DA în interpretarea results.

ZS a implementat DSS (European ComissionDigital-building-blocks Digital Signature Service) în infrastructura internă pentru SV Application. DA ar trebui să reprezinte diferite aplicații de conducere, implementate în infrastructura ZS (de exemplu, aplicația de arhivare). Documentul deretrimitere nu prevede niciun comportament necesar din partea DA, în

special nicio cerință de prelucrare pentru niciuna dintre informațiile returnate, deoarece aceasta este specifică aplicației și în afara domeniului de aplicare al prezentului document.

Pe baza rezultatelor SVA:

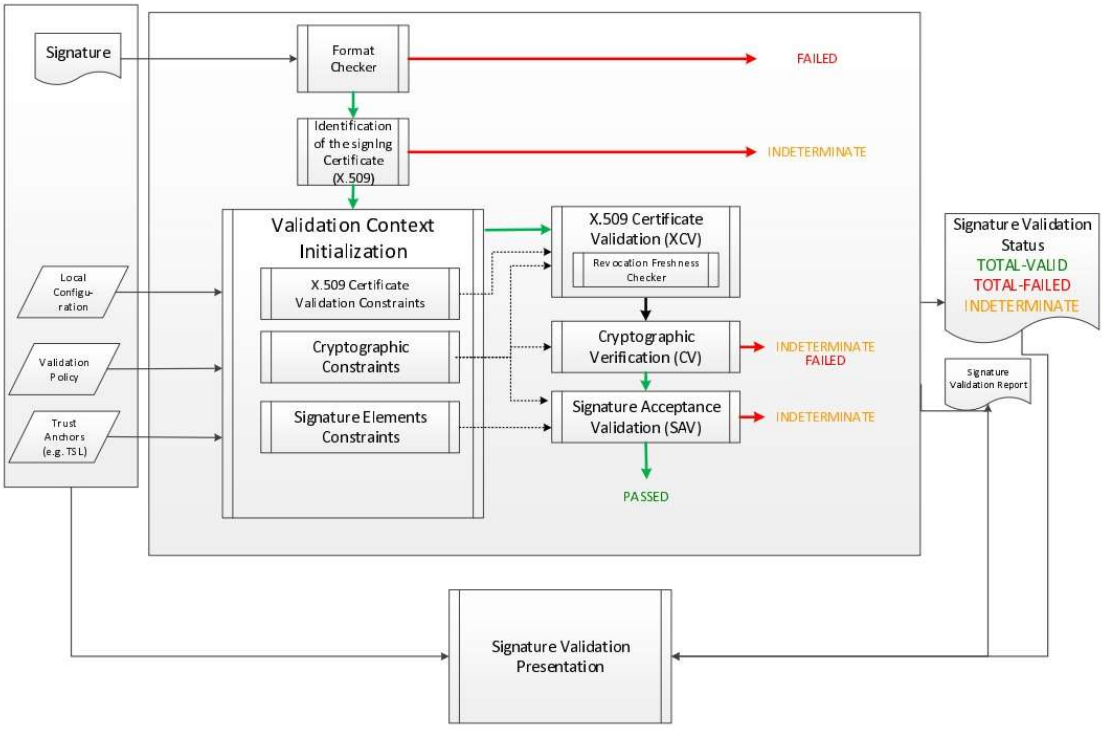
- Dacă SVA rtransformă TOTAL-PASSED pentru o anumită semnătură, DA ar trebui să considere semnătura ca fiind o semnătură valabilă din punct de vedere tehnic în conformitate cu constrângerile de validare.
- Dacă SVA returnează TOTAL-FAILED, DA nu ar trebui să considere semnătura ca fiind valabilă din punct de vedere tehnic.
- În cazulîn care SVA returnează NEDETERMINAT, dacă subindicația indică faptul că rezultatul se poate schimba la rerularea algoritmului, DA poate reîncerca validarea pe baza unor informații suplimentare sau ulterior. În toate celelalte cazuri, acceptarea semnăturiitrebuie să fie determinată de DA sau, ulterior, de utilizator, ca parte a verificării normelor de aplicabilitate.

SVS este implementat, cum ar fi:

- ca serviciu web;
- o aplicație web independentă.

13.16 PROCESUL DE VALIDARE A SEMNĂTURII

Procesul de validare se bazează pe standardul ETSI EN 319 102-1. Diagrama simplificată de mai jos prezintă procesul de validare a semnăturii, cu relațiile dintre fiecare bloc component care reprezintă un set logic de verificări utilizate în procesul de validare:



13.16. 1 Validarea lantului de certificare (path)

Validarea semnăturii începe de la validarea unui lanț de certificate. Validarea căii certificatului este un algoritm care încearcă să verifice legătura dintre cheia publică și subiectul unui certificat, utilizând informații ancoră de încredere. Prelucrarea completă este descrisă în RFC 5280 secțiunea 6.1 și, după cum se menționează acolo, verifică, printre altele, dacă o cale potențială de certificare (o secvență de n certificate) îndeplinește următoarele condiții:

a. pentru toate x din {1, ..., n-1}, subiectul certificatului x este emitentul certificatului x+1;
b. certificatul 1 este emis de ancora de încredere;
c. certificatul n este certificatul care trebuie validat (adică certificatul țintă); și
d. Pentru toate x din {1, ..., n}, certificatul era valabil la momentul respectiv.

În ETSI EN 319 102-1, un lanț de certificate prospective este definit ca o secvență de certificate care îndeplinește condițiile de la a. la c. de mai sus și pentru care ancora de încredere este de încredere în conformitate cu politica de validare utilizată.

În aplicația SV, pentru un anumit certificat, cadrul construiește o cale de certificat până când o ancoră de încredere cunoscută (listă de încredere, keystore), validează fiecare certificat găsit (OCSP / CRL) și determină "calificarea" europeană a acestuia.

13.16. 2 Verificare calificarea certificat

Cadrul respectă standardul ETSI TS 119 615. Acesta analizează proprietățile certificate (QCStatements, Certificate Policies etc.) și aplică eventualele reguli generale din lista de încredere aferentă.

SVA calculează întotdeauna starea în 2 momente diferite: emiterea certificatului și timpul de semnare / validare. Calificarea certificatului poate evolua în timp, statutul său nu este imuabil (de exemplu: un prestator de servicii de încredere poate pierde statutul acordat). Regulamentul eIDAS definește în mod clar aceste momente diferite la articolul 32 și în anexa I aferentă.

Atunci când serviciul de validare a semnăturilor urmărește să aplicesemnături sau sigilii electronice calificate, astfel cum sunt definite la articolul 32 alineatul (1) din Regulamentul (UE) nr. 910/2014, procesul de validare va respecta cerințele ETSI TS 119 172-4 (faza de proiect).

O semnătură poate fi considerată calificată dacă:

- Rezultatul derulării "procesului de validare a semnăturilor care asigură disponibilitatea pe termen lung și integritatea materialului de validare" definit în ETSI EN 319 102-1 este TOTAL_PASSED;

- Certificatul de semnare este determinat ca calificat la "cel mai bun timp de semnare" și la "momentul emiterii" (ora la care a fost emis certificatul, adică valoarea câmpului "notBefore");

- Cheia privată corespunzătoare certificatului de semnare este determinată ca fiind deținută într-un dispozitiv calificat de creare a semnăturii (QSCD).

13.16.3 Verificarea revocarii

Constrângerea de prospețime a revocării (RFC) este un interval de timp care indică faptul că validarea acceptă LCR-uri care au fost emise la un moment dat după timpul de validare minus *RFC: valTime - RFC < CRL.thisUpdate.*

Dacă RFC este respectat de un LCR, atuncise poate utiliza CRL. În caz contrar, LCR se respinge și nu se utilizează

pentru a stabili dacă certificatul este revocat sau nu. Un alt CRL poate fi căutat online. În cazul în care nu se constată nicio LCR care să respecte RFC, atunci nu se poate stabili dacă certificatul este valabil și, prin urmare, nu este posibil să se determine dacă semnătura este valabilă.

- În cazul unei semnături cu un nivel BASELINE-T, timpul de validare poate fi înlocuit cu *cel mai bun timp de semnătură* la verificarea constrângerii. Datele de revocare trebuie emise după cea mai bună semnătură, furnizată de un marcaj temporal al semnăturii.
- În cazul unui nivel BASELINE-B, nu există marcaj temporal printre atributele nesemnate. Dacă RFC este egal cu 0, atunci timpul de validare trebuie să fie mai mic decât *CRL.thisUpdate.* Aceasta înseamnă că datele de revocare trebuie să fi fost emise după încheierea procesului de validare , ceea ce nu este posibil.

Conform standardului ETSI TS 119 172-4, RFC se setează la 0 (zero). Dacă DSS ar fi avut un RFC egal cu 0, atunci ar invalida toate semnăturile de nivel B fără un marcaj temporal de semnătură. De aceea, prospețimea revocării nu este verificată în SVA în mod implicit. Nivelul de validare al verificării este setat la IGNORE, ceea ce înseamnă că utilizatorilor li se arată că verificarea există, dar nu este executată în procesul de validare.

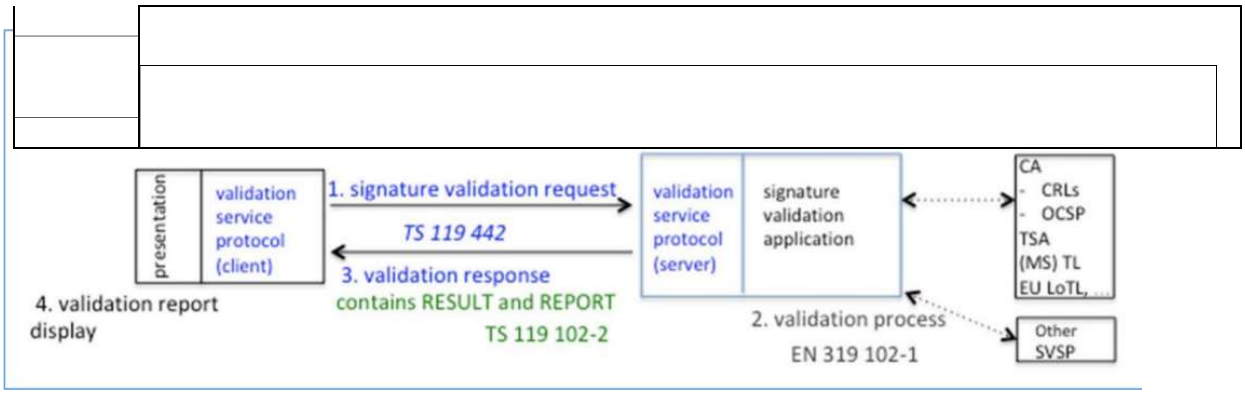
13.16.4 Accesare resurse externe

În cazul unei semnături cu nivel BASELINE-LT sau BASELINE-LTA, SVA va furniza următoarele surse de informații și parametri:

- sursa certificatelor de încredere [pe baza listei (listelor) sigure specifice contextului];
- sursa certificatelor intermediare utilizate pentru a construi lanțul de certificate până la ancora de încredere. Această sursă este necesară numai atunci când aceste certificate nu sunt incluse în semnătura propriu-zisă;
- sursa AIA;
- sursa OCSP;
- sursa LCR;

13.16.5 Procedura funcțională a serviciului de validare:

Pasul 1	(DA) generează și trimite o solicitare de validare a semnăturii către SVA. Protocoalele care susțin cererea și răspunsul corespund specificației ETSI TS 119 442. Cererea include: 1. documentul (documentele) semnat(e) (SD) și semnătura (semnăturile) [SDO (SDO)] care le semnează; sau 2. reprezentarea documentului (documentelor) semnat(e) [DST] și semnăturile care le semnează, pentru a evita expunerea conținutului documentului la serviciul de validare. Punerea în corespondență între documentele semnate și rezumatele acestora utilizate în cadrul semnăturilor este esențială atunci când se verifică o semnătură. În conformitate cu Regulamentul (UE) nr. 910/2014, legătura dintre documentul semnat și semnătură face parte din condițiile pentru o semnătură/sigiliu electronic avansat. Cu toate acestea, din motive de confidențialitate sau de performanță, există cazuri de utilizare în care este preferabil să se trimită numai rezumatele hash ale documentelor semnate. În acest caz, verificarea integrității
	SVAperfo rms procedura de validare (capitolul 5.2)
Pasul 2	Procesul de validare corespunde specificației ETSI TS 119 102-1. Validarea este efectuată de SVA în conformitate cu această politică de validare a semnăturii. Semnarea procesului de validare respectă prevederile ETSI TS 119 102-1.
	SVA pregătește și trimite răspunsul de validare
Pasul 3	Protocoalele care susțin cererea și răspunsul sunt cele specificate în ETSI TS 119 442. Răspunsul de validare include rapoartele de validare. Acesta include OID-ul politicii de servicii și OID-ul politicii de validare a semnăturii utilizate. Raportul de validare corespunde specificației
	Prezentarea raportului de validare
Pasul 4	DA poate oferi un modul de prezentare a validării semnăturii pentru a prezenta raportul de validare care specifică rezultatul și oferă un raport detaliat al fiecăruia dintre atributele semnate. DA,



13.16.6 Cerințe privind raportul de validare a semnăturii

- Raportul de validare poate fi furnizat automat beneficiarului în conformitate cu ETSI TS 119 442 și **ETSI TS 119 102-2**;

- Standardul **ETSI EN 319 102-1** specifică un model complet de validare și proceduri pentru validarea "semnăturilor digitale AdES/QC ". Raportul de validare va conține rezultatul unui proces de validare efectuat în conformitate cu aceste proceduri este un raport de validare și o indicație care poate fi:
  - ***TOTAL-TRECUT*** indicând faptul că semnătura a trecut verificarea și respectă politica de validare a semnăturii.
  - ***NEDETERMINAT***, indicând faptul că verificările formatului și semnăturii digitale nu au eșuat, dar nu există informații suficiente pentru a determina dacă semnătura electronică este validă.
  - ***TOTAL_FAILED*** indică faptul că fie formatul semnăturii este incorect, fie că valoarea semnăturii digitale nu trece verificarea.

- Raportul de validare trebuie prezentat utilizatorului printr-o pagină web în cadrul unei sesiuni TLS susținută de un certificat emis de autoritatea de certificare într-o formă convenabilă pentru acesta;

- Politica de validare a semnăturii (OID) este în conformitate cu ETSI TS 119 172-4 și prevede fără echivoc că semnătura este calificată în conformitate cu Regulamentul (UE) nr. 910/2014;

- Raportul de validare permite beneficiarului să aibă încredere în securitatea semnăturii/sigiliului. Există informații că:
  - certificatul a fost emis de un prestator de servicii de încredere calificat și că este valabil din momentul semnării
  - Datele despre validarea semnăturii corespund datelor furnizate de beneficiar.
  - Utilizarea oricărui pseudonim este indicată în mod clar beneficiarului dacă un pseudonim a fost utilizat la momentul semnării.
  - Sigiliul electronic este creat de undispozitiv de etanșare electronic.

- Integritatea datelor semnate nu este amenințată.

SV oferă un raport de validare în format PDF și/sau XML

Structura și semantica raportului de validare

Indicația principală	Sub-indicație	Raportați datele	Semantică
TOTAL-EȘUAT	FORMAT_FAILURE	Procesul de validare oferă faptele individuale care au condus la informații disponibile cu privire la prelucrarea nereușită a unei semnături/sigilii electronice.	Semnătura/sigiliul electronic nu este compatibil cu standardele suportate specificate în prezentul document la un nivel care împiedică verificarea criptografică să o proceseze.
	HASH_FAILURE	Procesul de validare a semnăturii oferă un identificator care identifică în mod unic elementul din obiectul/sigiliul de date semnatca utilizând defecțiunea sub forma certificatului pentru semnătură/sigiliu electronic.	Procesul de validare calificată a semnăturilor și sigiliilor electronice are ca rezultat TOTAL-EȘUAT, deoarece cel puțin un hash al unui obiect de date semnat care a fost inclus înprocesul de testare nu se potrivește cu valoarea hash corespunzătoare din semnătură/sigiliu.
	SIG_CRYPTO_FAILURE	Procesul de validare produce certificatul pentru semnătură/sigiliu electronic utilizat în procesul de validare. Valoarea semnăturii nu poate fi verificată cu ajutorul cheii publice a semnăturii/sigiliului.	Procesul de validare calificată a semnăturilor și sigiliilor electronice are ca rezultat TOTAL-EȘUAT, deoarece valoarea digitală a semnăturii nu a putut fi verificată utilizând cheia publică a semnatarului din certificatul de semnătură/sigiliu electronic.
	REVOCAT	Procesul de validare prevede următoarele: - Lanțul de certificate utilizat în procesul de validare; - Ora și, dacă este disponibil, motivul revocării certificatului de semnătură/sigiliu electronic. - LCR, dacă există, pentru care a fost stabilită revocarea	Procesul de validare calificată a semnăturilor și sigiliilor electronice are ca rezultat un TOTAL EȘUAT deoarece:- certificatul pentru semnătură/sigiliu electronic a fostrevocat; și - există dovada existenței (PoE) disponibilă că momentul semnăturii/sigiliului se află după

	SIG_CONSTRAINTS_FAILURE	Procesul de validare oferă mai multe motive care au dus la validarea nereușită.	Procesul de validare calificată a semnăturilor și sigiliilor electronice are ca rezultat NEDETERMINAT, deoarece unul sau mai multe atribute ale semnăturii/sigiliului electronic nu corespund constrângerilor de validare.
	CHAIN_CONSTRAINTS_FAILURE	Procesul de validare prevede următoarele: - Lanțul de certificate utilizat în procesul de validare. - Informații suplimentare despre cauza care a dus la acest rezultat.	Procesul de validare calificată a semnăturilor și sigiliilor electronice are ca rezultat NEDETERMINAT, deoarece lanțul de certificate utilizat în procesul de validare nu corespunde constrângerilor de validare legate de certificat. Informații suplimentare despre cauza care a dus la acest rezultat
	CERTIFICATE_CHAIN_GENERAL_FAILURE	Procesul de validare oferă informații suplimentare cu privire la motivul acestui rezultat.	Procesul de validare calificată a semnăturilor și sigiliilor electronice are ca rezultat NEDETERMINAT, deoarece validarea lanțului de certificate a produs o eroare dintr-un motiv nedeclarat/nespecificat .
	CRYPTO_CONSTRAINTS_FAILURE	Procesul de validare oferă identificarea unei semnături/a unui sigiliu electronic sau a unui certificat generat utilizând un algoritm sau o dimensiune a cheii sub nivelul de securitate criptografic necesar.	Cheile utilizate cu astfel de algoritmi sunt sub nivelul de securitate criptografic necesar și:• semnătura/sigiliul electronic și/ sau certificatele corespunzătoare au fost produse după perioada până la care acești algoritmi/chei au fost considerate sigure (dacă se cunoaște acest moment); și• semnătura/sigiliul electronic nu este protejat de o marcă temporală suficient de puternică aplicată înainte de momentul până la care algoritmul/cheia a fost luată în considerare sigur (dacă se cunoaște un astfel de moment). Algoritmii și cheile acceptate de-a lungul anilor sunt menționate în constrângeri.xml)
NEDETERMINAT	EXPIRAT	Procesul de validare oferă date despre lanțul de certificate validat.	Procesul de validare calificată a semnăturilor și sigiliilor electronice are ca rezultat NEDETERMINAT, deoarece momentul plasării semnăturii/sigiliului electronic este ulterior datei de expirare (notAfter) a certificatului.

NOT_YET_VALID	Procesul de validare oferă date despre lanțul de certificate validat.	Procesul de validare calificată a semnăturilor și sigiliilor electronice are ca rezultat NEDETERMINAT, deoarece momentul plasării semnăturii/sigiliului electronic este înainte de data expirării (nu înainte) a certificatului.
POLICY_PROCESSING_ERROR	Procesul de validare oferă informații suplimentare cu privire la motiv.	Procesul de validare calificată a semnăturilor și sigiliilor electronice are ca rezultat NEDETERMINAT, deoarece fișierul formal de politică dat nu a putut fi prelucrat din niciun motiv (de exemplu, nu este accesibil, nu poate fi urmărit, digeră neconcordanța etc.) .
SIGNATURE_POLICY_NOT_AVAILABLE	-	Procesul de validare calificată a semnăturilor și sigiliilor electronice are ca rezultat NEDETERMINAT, deoarece documentul care conține detaliile politicii nu este disponibil.
TIMESTAMP_ORDER_FAILURE	Procesul de validare produce o listă de marcaje temporale care nu respectă constrângerile de ordonare.	Procesul de validare calificată a semnăturilor și sigiliilor electronice are ca rezultat NEDETERMINAT lista furnizată de mărci temporale și / sau obiecte de date semnate nu respectă constrângerile asupra comenzii.
NO_SIGNING_CERTIFICATE_FOUND	-	Procesul de validare calificată a semnăturilor și sigiliilor electronice are ca rezultat NEDETERMINAT, deoarece certificatul pentru semnătură/sigiliu electronic nu poate fi identificat.
NO_CERTIFICATE_CHAIN_FOUND		Procesul de validare calificată a semnăturilor și sigiliilor electronice are ca rezultat NEDETERMINAT, deoarece nu a fost găsit niciun lanț de certificate pentru certificatul identificat pentru semnătură/sigiliu electronic.
REVOKED_NO_POE	Procesul de validare prevede următoarele: •Lanțul de certificate utilizat în procesul de validare. • Ora și motivul revocării certificatului de semnătură/sigiliu electronic.	Procesul de validare calificată a semnăturilor și sigiliilor electronice are ca rezultat NEDETERMINAT, deoarece certificatele corespunzătoare au fost revocate în timpul validării. Cu toate acestea, nu se poate stabili dacă momentul semnării este înainte sau după momentul revocării.

REVOKED_CA_NO_POE	Procesul de validare prevede următoarele: •Lanțul de certificate care include certificatul autorității de certificare revocat; • Ora și motivul revocării certificatului.	Procesul de validare calificată a semnăturilor și sigiliilor electronice rezultă dinNEDETERMINARE, deoarece a fost găsit cel puțin un lanț de certificate, dar o autoritate de certificare intermediară este revocată.
OUT_OF_BOUNDS_NO_POE		Procesul de validare calificată a semnăturilor și sigiliilor electronice are ca rezultat NEDETERMINAT, deoarece certificatul este expirat sau nu este încă valabil la data/ora validării, iar SVA nu poate constata că timpul semnării se încadrează în intervalul de valabilitate al certificatului.
CRYPTO_CONSTRAINTS_FAILURE_NO_POE	Procesul de validare prevede următoarele: Identificarea semnăturii/sigiliului electronic sau a certificatului respectiv care este produs utilizând o dimensiune inacceptabilă a cheii sau un algoritm care nu îndeplinește nivelul de securitate criptografic necesar.	Procesul de validare calificată asemnăturilor și sigiliilor electronice are ca rezultat NEDETERMINAT, deoarece cel puțin unul dintre algoritmii care au fost utilizați în semnătura/sigiliul electronic sau în certificatele respective implicate în validarea acestora sau dimensiunea unei chei utilizate cu un astfel de algoritm este sub nivelul de securitate criptografic necesar și nu există nicio dovadă că semnătura/sigiliul sau aceste certificate au fost produse înainte de momentul până la care Acest algoritm/cheie a fost considerat sigur.
NO_POE	Procesul de validare identifică doar semnăturile/sigiliile pentru care lipsește dovada existenței (PoE). Procesul de validare ar trebui să furnizeze informații suplimentare despre problemă.	Procesul de validare calificată a semnăturilor și sigiliilor electronice are ca rezultat NEDETERMINAT, deoarece nu există nicio dovadă a existenței (PoE) care să stabilească faptul că semnătura/sigiliul a fost produsă înainte de un eveniment compromițător cunoscut (de exemplu, algoritm defect).

	TRY_LATER		Procesul de validare calificată a semnăturilor și sigiliilor electronice are ca rezultat NEDETERMINAT, deoarece nu toate constrângerile pot fi îndeplinite utilizând informațiile disponibile. Cu toate acestea, procesul poate fi posibil dacă validarea utilizează informații suplimentare de revocare care vor fi disponibile ulterior.
	SIGNED_DATA_ NOT_FOUND	Procesul de validare prevede următoarele: Identificatorul (de exemplu, un URI) al datelor de semnătură/sigiliu care au cauzat defecțiunea.	Procesul de validare calificată Procesul de validare calificată a semnăturilor și sigiliilor electronice devineNEDETERMINAT deoarece datele despre semnătură/sigiliu nu pot fi obținute.
	GENERIC	Procesul de validare oferă informații suplimentare care arată de ce indicația de validare este NEDETERMINATĂ	Procesul de validare calificată are ca rezultat NEDETERMINAT din alte motive.

Raportul de validare este o reprezentare a etapelor efectuate în timpul procesului de validare, astfel cum sunt definite în standardul ETSI EN 319 102-1 și structurate utilizând procesele și blocurile definite în standardul respectiv:

- Blocuri de bază;
  - **FC** - verificarea formatului;
  - **ISC** - identificarea certificatului de semnare;
  - **VCI** - inițializarea contextului de validare;
  - **RFC** - Verificator de prospețime revocare;
  - Validare certificat XCV - X.509;
  - **CV** - verificare criptografică ;
  - **SAV** - Validarea acceptării semnăturii.
- Procesul de validare a semnăturilor de bază;
- Bloc constitutiv de validare a mărcilor temporale;
- Procesul de validare a semnăturilor cu timp și a semnăturilor cu materiale de validare pe termen lung;
- Proces de validare pentru semnături care oferă disponibilitate pe termen lung și integritatea validării.
- De exemplu, blocurile de bază sunt împărțite în șapte elemente:

Următoarele elemente suplimentare pot fi, de asemenea, executate în cazul validării în trecut:

- PCV - **validarea certificatelor anterioare**;
- VTS **- Proces de alunecare a timpului de validare;**
- Extragere POE **- Extragere Dovada Existentei;**
- PSV **- validarea semnăturii anterioare.**

Pentru a procesa datele de revocare, SVA efectuează următoarele verificări suplimentare:

- **CRS** (CertificateRevocationSelector) - validates un set de date de revocare pentru un anumit certificat și returnează cea mai recentă intrare valabilă cunoscută ca conținând informații despre certificatul în cauză;
- **RAC** (RevocationAcceptanceCheck) - verifică dacă se știe că o singură dată de revocare conține informațiidespre certificatul respectiv.

13.17 Constrângerile algoritmului criptografic

13.17.1 Constrângeri de validare X.509

- Câmpul Utilizare cheie al certificatului semnatarului trebuie să aibă setul de biți nonRepudiation (denumit și contentCommitment).

13.17.2 Constrângeri ale algoritmului hash:

- În cazul formatului BDOC: la validarea unei semnături în care a fost utilizată funcția SHA-1, se returnează un avertisment de validare cu privire la metoda de digerare slabă.

13.17.3 Constrangeri ale Algoritmului criptografic asimetric:

- Algoritmii criptografici RSA și ECC sunt susținuți
- În cazul formatelor PAdES/XAdES (de asemenea, BDOC)/CAdES, lungimea cheii RSA trebuie să fie de cel puțin 1024 biți, iar lungimea cheii ECC de cel puțin 192 biți.
  - <Algo Size="160">DSA</Algo>
  - <Algo Size="1024">RSA</Algo>
  - <Algo Size="160">ECDSA</Algo>
  - <Algo Size="160">PLAIN-ECDSA</Algo>

13.17.4 Constrângerile ancorei de încredere

1. Semnătura trebuie să conțină certificatul ancorei de încredere și toate certificatele necesare validatorului de semnături pentru a construi o cale de certificare până la ancora de autentificare. Acest lucru se aplică certificatului semnatarului și certificatelor prestatorilor de servicii de încredere care au emis simbolul privind marca temporală și datele de revocare care sunt încorporate în semnătură.
2. Ancorele de încredere sunt:
   - În cazul formatelor XAdES/CAdES/PAdES: listele sigure ale statelor membre ale UE.

13.17.5 Constrângeri privind datele de revocare

1. Semnătura trebuie să conțină dovezi înregistrate pentru a confirma că certificatul era valabil la momentul semnării.
2. Înregistrarea dovezilor certificatului semnatarului trebuie să fie sub forma unei confirmări OCSP sau sub forma unei liste de revocare a certificatului.
3. În timpul validării nu se solicită alte date de revocare decât datele care au fost încorporate inițial în semnătură.
4. Verificarea revocării certificatelor considerate ancore de încredere:
   - În cazul formatelor XAdES/CAdES/PAdES: revocarea certificatelor ancoră de încredere este verificată pe baza datelor din listele sigure.

13.17.6 Constrângeri privind noutatea revocării certificatului de semnatar

1. În cazul semnăturilor XAdES/CAdES/PAdES BASELINE_LT și BASELINE_LTA cu marca temporală a semnăturii: prospețimea datelor de revocare este verificată în conformitate cu următoarele reguli:
   - În cazul răspunsului OCSP, dacă diferența dintre timpul de producție al mărcii temporale a semnăturii (câmpul genTime) și timpul de producție al confirmării OCSP a semnatarului (câmpul productAt) este mai mare de 24 de ore, atunci semnătura este considerată nevalidă. Dacă diferența este mai mare de 15 minute și mai mică de 24 de ore, atunci se returnează un avertisment de validare.
   - Înconformitate cu lista de certificate revocate, ora de producție a mărcii temporale a semnăturii (câmpul genTime) trebuie să se încadreze în intervalul de valabilitate al CRL (între această actualizare și următoareaactualizare)

13.17.7 Constrângeri de timp ale semnaturii de încredere

1. Timpul de semnare de încredere, care indică cel mai timpuriu moment în care se poate avea încredere (deoarece dovedit de unele dovezi de existență prezente în semnătură) că o semnătură a existat, este determinat după cum urmează:
   - În cazul semnăturii cu marcă temporală (nivel BASELINE_T, BASELINE_LT sau BASELINE_LTA) - valoarea genTime a celui mai vechi simbol valabil al mărcii temporale a semnăturii din semnătură.
   - În cazul semnăturii de bază (BASELINE_B) - valoarea timpului de semnare de încredere nu poate fi determinată, deoarece nu există nicio dovadă a existenței semnăturii.

13.17.8 Cerințe specifice containerului ASICE

Containerul ASICE trebuie să fie conform cu standardul ETSI EN 319 162-1. 1. Avertismentul este returnat atunci când semnăturile din container nu semnează toate fișierele de date. 2. Fișierul manifest trebuie să fie prezent.

13.17.9 Cerințe specifice containerului ASICS

Serviciul acceptă atât containere ASIC-S bazate pe semnătură, cât și pe Time Stamp Token (TST). Containerele bazate pe înregistrări de dovezi nu sunt acceptate. Containerul ASIC-S trebuie să respecte standardele ETSI EN 319 162-1 și ETSI EN 319 162-2.

1. Fișierul manifest nu poate fi prezent în cazul containerelor ASIC-S bazate pe semnătură.
2. Este acceptat un singur TimeStampToken per container. Fără suport AsicArchiveManifest.xml.
3. Nu se face nicio verificare bazată pe TSL a certificatelor în cazul containerelor bazate pe TimeStampToken.