# certSIGN Paperless Validation

# Politici, Practici și Proceduri

pentru

## Serviciul de Validare Semnături/Sigilii Calificate

**QSVS-PPS-RO**

**Versiune/ Data:v1.7 - 31 Mar.2026**

---

**Notă importantă**

Acest document este proprietatea CERTSIGN SA

Adresa: Bd.Tudor Vladimirescu, nr. 29 A,
AFI Tech Park 1, București 050881, România

Telefon: 004-021-31.19.901

Web: www.certsign.ro

**Istoric document**

| Versiune | Data efectivă *(ultima zi a lunii)* | Motiv | Persoana care a făcut schimbarea |
|---|---|---|---|
| 0.1 | Iulie 2021 | Publicarea primei versiuni | Manager Politici PKI |
| 1.0 | Iulie 2022 | Actualizări în conținut | Manager Politici PKI |
| 1.1 | August 2022 | Actualizari minore dupa audit | Manager Politici PKI |
| 1.2 | Ianuarie 2023 | Revizuire anuală | Manager Politici PKI |
| 1.3 | Ianuarie 2024 | Revizuire anuală | Manager Politici PKI |
| 1.4 | Martie 2024 | Appendix 3 completat | Manager Politici PKI |
| 1.5 | 15 Ianuarie 2025 | Revizuire anuală | Manager Politici PKI |
| 1.6 | 15 Ianuarie 2026 | Revizuire anuală | Manager Politici PKI |
| 1.7 | 31 Martie 2026 | Actualizari eIDAS2 | Manager Politici PKI |

**Acest document a fost creat și este proprietatea:**

| Proprietar | Autor | Data creării |
|---|---|---|
| BU eIDAS Trusted Services | Manager de politici PKI | iulie 2021 |

**Lista de distributie**

| Destinaţie | Data distribuirii |
|---|---|
| Public-Internet | iulie 2022 |
| Public-Internet | August 2022 |
| Public-Internet | Ianuarie 2023 |
| Public-Internet | Ianuarie 2024 |
| Public-Internet | Martie 2024 |
| Public-Internet | Ianuarie 2025 |
| Public-Internet | Ianuarie 2026 |
| Public-Internet | March 2026 |

**Acest document a fost aprobat de:**

| Versiune | Nume | Data |
|---|---|---|
| 1.0 | Comitet de Management al Politicilor și Procedurilor (CMPP) | iulie 2022 |
| 1.1 | Comitet de Management al Politicilor și Procedurilor (CMPP) | August 2022 |
| 1.2 | Comitet de Management al Politicilor și Procedurilor (CMPP) | Ianuarie 2023 |
| 1.3 | Comitet de Management al Politicilor și Procedurilor (CMPP) | Ianuarie 2024 |
| 1.4 | Comitet de Management al Politicilor și Procedurilor (CMPP) | Martie 2024 |
| 1.5 | Comitet de Management al Politicilor și Procedurilor (CMPP) | Ianuarie 2025 |
| 1.6 | Comitet de Management al Politicilor și Procedurilor (CMPP) | Ianuarie 2026 |
| 1.7 | Comitet de Management al Politicilor și Procedurilor (CMPP) | March 2026 |

**Conţinut**

# 1 Introducere

## 1.1 Prezentare generală

Acest document, **certSIGN Paperless Validation, Politici, Practici și Proceduri pentru Serviciul de Validare Semnături/Sigilii Calificate** (QSVS-PPS-RO), descrie politicile și practicile aplicate de Certsign SA (certSIGN) în furnizarea Serviciilor de Validare a Semnăturii/Sigiliilor Calificate în conformitate cu :

• 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 în piața internă și de abrogare a Directivei 1999/93/CE;
• Acte juridice ale României (cum ar fi Legea 214/2024, Ordinul 449/2017);
• Standardul UE ETSI EN 319 401 V2.3.1 (2021-05) Semnături și infrastructuri electronice (ESI); Cerințe generale ale politicii pentru furnizorii de servicii de încredere;
• ETSI TS 119 441 V1.2.1 (2023-10) Semnături și infrastructuri electronice (ESI); Cerințe de politică pentru TSP care furnizează servicii de validare a semnăturii.
Structura acestui document este conformă cu anexa A din ETSI TS 119 441.

### 1.1.1 Identificarea TSP

S.C. CERTSIGN S.A.
Adresa: B-dul Tudor Vladimirescu 29 A, AFI Tech Park 1, București, România
Număr Registrul Comerțului: J2006000484402
Cod de înregistrare fiscală: RO 18288250
Sediul social: str. Oltenitei 107A. Bloc C1, Et.1, camera 16, Sector 4, Bucuresti, Romania, PC 041303

### 1.1.2 Politici suportate de serviciul de validare a semnăturii

Politica Serviciului de Validare a Semnăturii/Sigiliilor Calificate (QSVS) este dedicată validării semnăturilor calificate și/sau a sigiliilor calificate conform Regulamentului UE.
Principala limitare a politicii se referă la validarea semnăturilor sau a sigiliilor plasate pe documentele pdf. Un singur document poate fi validat la un moment dat.
certSIGN ca QSVSP este conform cu cerințele ETSI TS 119 441 și utilizează următorul OID specific: **0.4.0.19441.1.2**
• itu-t(0) identified-organization(4) etsi(0) val-service-policies(19441) policy-identifiers(1) qualified (2)
Documentul este validat dacă nu a fost modificat de la ultima semnătură/sigiliu de pe acesta și dacă toate semnăturile/sigiliile sunt valabile și calificate conform Regulamentului UE nr. 910/2014.

**Conformitatea Semnătură-politică -** Indică faptul că procesarea pentru validarea semnăturii digitale și generarea raportului de verificare a regulilor de aplicabilitate corespunzătoare respectă cerințele ETSI TS 119 172-4.

- id-etsi-sars-SpCompliance - **0.4.0.191724.1.1**

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

- Semnătură 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

**Politica de validare a semnăturii certSIGN OID** : **1.3.6.1.4.1.25017.4.2.1.2**
• 1.3.6.1.4.1.25017 (certSIGN organization).4 (Validation).2 (Qualified Signature Validation Service).X (policy).Y (version)

- Default - PAdES validation policy - OID: 1.3.6.1.4.1.25017.4.2.1.2
- CAdES validation policy - OID: 1.3.6.1.4.1.25017.4.2.2.1

Rezumatul declarației specifice politicii de validare este prezentat în Anexa 2.

## 1.2 Componentele serviciului de validare a semnăturii

### 1.2.1 Actori SVS

QSVS-PPS reglementează cele mai importante relații dintre entitățile aparținând certSIGN, echipele de consultanță (inclusiv auditori) și clienții (utilizatorii serviciilor furnizate) acestuia:

- Autoritățile de certificare certSIGN (CAuri)
- Depozitar,
- Protocolul de stare a certificatului online (Autoritatea OCSP),
- Liste de revocare a certificatelor (autoritatea CRL)
- Servere de marcare temporală (Autorități TSA)
- Abonati,
- Părți terțe,
- Comitetul de management al politicilor si procedurilor
- Auditorii

### 1.2.2 Arhitectura serviciului

Diagrama de mai jos prezintă arhitectura simplificată certSIGN Qualified Validation Service și actorii implicați.

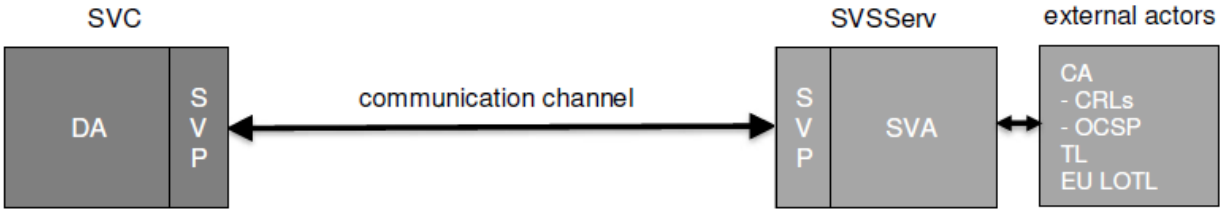



Figura 1 Arhitectura serviciului

**Clientul de validare a semnăturii** (SVC):

- execută **protocolul de validare a serviciului** (SVP) din partea utilizatorului
- construiește cererea de validare a semnăturii
- prezintă sau trimite raportul de validare

**Serverul serviciului de validare a semnăturilor** (SVSServ):

- execută SVP și procesează validarea semnăturii pe partea SVSS
- rulează aplicația de **validare a semnăturii** (SVA) care:
  - implementează algoritmul de validare
  - apelează actori externi pentru a-și îndeplini scopul
- creează **Raportul de validare a semnăturii** (SVR) aferent cererii
- construiește răspunsul de validare a semnăturii și îl întoarce la SVC

### 1.2.3 Cerințe esențiale ale politicii

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

Serviciul de validare certSIGN poate fi apelat în general de o aplicație într-un mod complet delegat, cu toate datele semnate (SD) trimise.

Datorită faptului că regulile specificate ulterior pot părea destul de complexe pentru cititorii/părțile interesate non-tehnice ale prezentului document de politică, partea rămasă a prezentului capitol oferă un rezumat informal, nenormativ al cerințelor esențiale ale politicii:

P1. Prezentul document de politică specifică regulile de validare pentru semnăturile și sigiliile electronice care sunt conforme cu standardele ETSI pentru semnăturile electronice calificate, în special cu PAdES.

P2. Deși poate fi definită o politică individuală pentru fiecare format de semnătură și mod de validare acceptat în scopul de a aborda în mod corespunzător detaliile specifice formatului de semnătură și responsabilitățile în funcție de actorii implicați, și anume CertSIGN și APP care are un contract de servicii de validare cu CertSIGN, setul general de reguli de validare este comun pentru toate politicile prezentului document. Formatele implicite acceptate sunt cele specificate în ETSI EN 319 142-1.

P3. În modul de validare completă, serviciul primește întreg documentul din aplicația de afaceri, în special un document PDF în cazul unei politici specifice PAdES și, prin urmare, este activat pentru a valida în mod specific dacă un hash calculat peste conținutul semnat se potrivește cu hash-ul corespunzător din obiectul de date semnat. Documentul de intrare este șters instantaneu după validare. Raportul de validare se păstrează 3 ani.

P4. În orice caz, aplicația de afaceri trebuie să permită utilizatorului final / părții de încredere să vizualizeze părți/versiuni semnate ale unui document pentru a verifica dacă conținutul semnat corespunde așteptărilor utilizatorului, astfel încât să poată fi luate deciziile corecte și prevenirea fraudei să fie mai bine abordată.

P5. Serviciul de validare validează toate semnăturile și sigiliile aferente aceluiași document de intrare și furnizează diagnosticele rezultate într-un singur raport. Cu toate acestea, nu face nici o interpretare a diagnosticelor furnizate sau a relațiilor reciproce dintre acele semnături și sigilii.

P6. Algoritmul de validare se conformează ETSI TS 119 102-1 – „Semnături și infrastructuri electronice (ESI); Proceduri de Creare și Validare a Semnăturilor Digitale AdES; Partea 1: Creare și validare”. Utilizează modelul shell pentru validarea certificatului, așa cum este specificat în secțiunea 5.2.6 din standardul respectiv. Algoritmul utilizează numai ancore de încredere care sunt publicate în listele de încredere ale UE.

P7. Algoritmul de validare acceptă doar marcaje temporale de încredere și calificate ca dovezi ale existenței datelor care sunt utilizate în timpul validării. În timpul acestui proces, orice elemente expirate sau învechite nu sunt luate în considerare. În special, expirarea poate viza și algoritmii criptografici atunci când aceștia nu sunt conform cerințelor specificate în ETSI TS 119 312 – „Electronic Signatures and Infrastructures (ESI); Suite criptografice”, pentru momentul în care li se cere să fie valabili.

Algoritmul de validare ia întotdeauna în considerare toate elementele eligibile conținute într-un obiect de date semnat pentru efectuarea unei *validări pentru semnături* pe baza profilului existent efectiv al unei semnături date, așa cum este specificat în secțiunea 5.1.2 din ETSI TS 119 102-1 – „Semnături electronice și infrastructuri (ESI); Proceduri de Creare și Validare a Semnăturilor Digitale AdES; Partea 1: Creare și validare".

P8. Algoritmul de validare verifică și determină atributele semnate conținute într-un obiect de date semnat, în special politica de semnătură și indicațiile tipului de angajament. Cu toate acestea, nu interpretează aceste elemente și lasă la latitudinea aplicațiilor comerciale dacă aceste elemente sunt utilizate pentru a lua decizii comerciale ulterioare.

P9. Serviciul de validare nu permite utilizatorului să selecteze certificatul (certificatele) care urmează să fie utilizat(e) pentru validare, de exemplu, în cazul în care atributele SDO nu conțin certificatul(ele) necesar(e). Permite folosirea doar a politicii implicite de validare a semnăturii dintre cele disponibile – pentru PaDES.

P10. Serviciul de validare permite utilizatorului să furnizeze unele intrări pentru procesul de validare (adică elemente pentru a parametriza politica de validare, cum ar fi clasa de semnătură, dar nu o ancora de încredere).

Conducerea certSIGN este responsabilă de implementarea celor mai bune practici necesare pentru îndeplinirea tuturor politicilor de validare din documentul curent.

În orice caz în care este asumată răspunderea certSIGN, aceasta va fi limitată la valoarea contractului la data producerii pagubei.
Jurnalele de evenimente ale serviciului certSIGN Paperless Validation sunt păstrate timp de 3 ani;
Litigiile legate de Serviciile de încredere furnizate de certSIGN vor fi soluționate inițial prin procedura de conciliere, (*https://www.certsign.ro/ro/procedura-primire-procesare-sesizari/*) în cursul căreia ambele părți vor negocia cu bună-credință soluții cu privire la orice dispute apărute. În cazul în care plângerea specifică nu este soluționată în termen de treizeci (30) de zile de la începerea procesului de conciliere, Părțile pot trimite litigiul instanțelor competente din București, România (sistemul juridic aplicabil).
Schema de evaluare a conformității serviciilor de încredere a TSP se bazează pe schema LSTI-Q055-v6.4, care face referire la ETSI EN 319 401 și ETSI TS 119 441.

Disponibilitatea depozitului de documente certSIGN și a depozitului CRL combinat este concepută pentru a depăși 99,8% din orele de lucru - definite ca 24 de ore pe zi, șapte zile pe săptămână, excluzând perioadele de întreținere planificate. Perioadele de întreținere planificate vor fi anunțate pe https://www.certsign.ro cu cel puțin 24 de ore înainte.

În caz de indisponibilitate din cauza unei catastrofe, defecțiuni a infrastructurii în afara controlului certSIGN sau orice alt motiv, certSIGN va depune toate eforturile pentru a restabili disponibilitatea serviciului în termen de 24 de ore.

## 1.3 Definiții și abrevieri

### 1.3.1 Definiții

**Autoritate de certificare** - Furnizor de servicii de încredere care emite certificate pentru semnături și/sau sigilii electronice.
**Regulamentul eIDAS** - Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacții pe piața internă și de abrogare a Directivei 1999/93/CE.
**Regulamentul general privind protecția datelor (GDPR)** - Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor).
**Furnizor de servicii de încredere (TSP)** - O entitate care oferă cel puțin un serviciu de încredere acordat de Organismul de supraveghere.
**Serviciu de validare a semnăturii calificat (QSVS)** – Un serviciu de încredere calificat pentru validarea semnăturilor și/sau a sigiliului
**Furnizor calificat de servicii de încredere** - O entitate care furnizează cel puțin un serviciu de încredere calificat acordat de Organismul de Supraveghere.
**Serviciu de validare calificat** - Un serviciu de încredere calificat pentru validarea semnăturii și/sau a sigiliului, atunci când este aplicat pe un document digital
**Parte de încredere** - O persoană fizică sau juridică care se bazează pe Serviciul de încredere
**Declarație de practici de validare a semnăturilor** - O declarație a practicilor pe care certSIGN le folosește în furnizarea serviciului său de încredere pentru validarea semnăturilor.
**Serviciu de validare a semnăturii** - Serviciu de încredere pentru validarea semnăturii și/sau a sigiliului
**Abonat** - O persoană juridică sau fizică legată printr-un acord cu certSIGN de obligații specifice Abonatului
**Organism de supraveghere** - Autoritatea desemnată de un stat membru pentru a desfășura activități de supraveghere asupra serviciilor de încredere și a furnizorilor de servicii de încredere în cadrul eIDAS pe teritoriul acelui stat membru.

### 1.3.2 Abrevieri

| | |
|---|---|
| **AdES** | Semnătură electronică avansată |
| **AdES/QC** | Semnătură electronică avansată creată cu un certificat calificat |
| **CA** | Autoritate certificată |
| **CRL** | Lista de revocare a certificatelor |
| **CMS** | Sintaxa mesajelor criptografice |
| **DTBS** | Date care urmează să fie semnate sau date care au fost semnate. Cuprinde SD și atributele suplimentare pentru a fi semnate sau a fi validate |
| **ESI** | Semnături electronice și infrastructuri |
| **LOTL** | Lista listelor de încredere |
| **OCSP** | Protocolul de stare a certificatului online |
| **OID** | Identificator de obiect |
| **PoE** | Dovada Existenței |
| **QES** | Semnătură electronică calificată sau sigiliu electronic calificat |
| **(Q)SCD** | Dispozitiv de creare a semnăturii (calificat). |
| **QSVSP** | Furnizor calificat de servicii de validare a semnăturii |
| **SCA** | Aplicație de creare a semnăturii |
| **SD** | Documentul semnatarului |
| **SDO** | Obiect de date semnat |
| **SDR** | Reprezentare document semnat |

| | |
|---|---|
| **SVA** | Aplicatie(program) de validare a semnăturii |
| **SVP** | Protocolul de validare a semnăturii |
| **SVR** | Raport de validare a semnăturii |
| **SVS** | Serviciul de validare a semnăturii |
| **SVSP** | Furnizor de servicii de validare a semnăturii |
| **TSP** | Furnizor de servicii de încredere |
| **XML** | Limbajul de marcare extensibil |

## 1.4 Politici și practici

certSIGN TSP efectuează o evaluare a riscurilor actualizată anual pentru a identifica, analiza și evalua riscurile serviciilor de încredere, ținând cont de problemele de afaceri și tehnice. Apoi selectează măsurile adecvate de tratare a riscurilor, ținând cont de rezultatele evaluării riscului. Măsurile de tratare a riscurilor asigură că nivelul de securitate este proporțional cu gradul de risc.

certSIGN TSP a determinat toate cerințele de securitate și procedurile operaționale care sunt necesare pentru implementarea măsurilor de tratare a riscurilor alese, așa cum este documentat în Politica de securitate a informațiilor certSIGN și în documentele interne de management al riscului. Evaluarea riscurilor este revizuită, evaluată și aprobată în mod regulat de conducerea certSIGN, care acceptă riscul rezidual identificat.

Practicile prezentate în acest document sunt susținute de proceduri operaționale interne și/sau instrucțiuni pentru fiecare fază a managementului și operațiunilor TSP prezentate în Capitolul 2. certSIGN are un proces de revizuire pentru practici, inclusiv responsabilități pentru menținerea declarației de practică a TSP.

### 1.4.1 Organizația care administrează documentația TSP

Prezentul document este administrat de furnizorul de servicii de încredere (TSP) certSIGN prin Comitetul de management al politicilor și procedurilor (PPMB). PPMB include membri seniori ai managementului, precum și personal responsabil cu managementul operațional al mediului certSIGN TSP PKI.

| | |
|---|---|
| **Nume** | SC CERTSIGN SA<br>Birou: B-dul Tudor Vladimirescu 29 A, AFI Tech Park 1, București, România<br>Număr Registrul Comerțului: J2006000484402<br>Cod de înregistrare fiscală: RO 18288250<br>Sediul social: str. Oltenitei 107A. Bloc C1, Et.1, camera 16, Sector 4, Bucuresti, Romania, PC 041303 |
| **Telefon** | (+4021)3119901 |
| **e-mail** | office@certsign.ro |
| **Web** | www.certsign.ro |

Tabelul 1Organizația care administrează documentul

| | |
|---|---|
| **Nume** | Comitetul de management al politicilor si procedurilor |
| **Telefon** | (+4021)3119901 |
| **e-mail** | office@certsign.ro |
| **Web** | www.certsign.ro |

Tabelul 2Persoana care determină adecvarea pentru politici

### 1.4.2 Persoana de contact

Persoana de contact pentru actualizarea acestui document este Managerul de Politici PKI al certSIGN. Persoana de contact pentru gestionarea și aprobarea acestui document este PPMB:

| | |
|---|---|
| **Nume** | Comitetul de management al politicilor și procedurilor (PPMB) |
| **Telefon** | (+4021)3119901 |
| **e-mail** | office@certsign.ro |
| **Web** | www.certsign.ro |

Tabelul 3 Persoana de contact

### 1.4.3 Aplicabilitatea documentației TSP (publice).

**Declarația privind politicile și practicile serviciilor de validare a semnăturilor/sigiliilor calificate** (QSVS-PPS) descrie politicile și practicile aplicate de certSIGN în furnizarea serviciilor de validare pentru semnăturile/sigiliile calificate aplicate documentelor PDF.
Acest document este identificat prin: QSVS-PPS-ROși versiunea sa:v1.7 - 31 Mar.2026
certSIGN PPMB este responsabil pentru Declarația de Management al practicilor de servicii de validare certSIGN
Acest document este aprobat de Comitetul de Management al Politicilor și Procedurilor și este disponibil public pe site-ul certSIGN https://www.certsign.ro/ro/depozitar.
certSIGN va notifica Organismul de Supraveghere cu privire la orice modificări semnificative în furnizarea de servicii de încredere calificate fără întârzieri nejustificate, dar nu mai târziu de 3 zile lucrătoare.
certSIGN va notifica Organismul de Supraveghere despre încetarea planificată a serviciului de încredere calificat cu cel puțin 3 luni înainte de încetarea serviciului de încredere calificat.
Abonații și părțile terțe vor lua în considerare doar versiunea efectivă a certSIGN QSVS-PPS de la momentul utilizării serviciilor furnizate de certSIGN.
Cea mai recentă și anterioară versiune a acestei declarații de practică va fi întotdeauna prezentă la: https://www.certsign.ro/ro/document/politici-si-practici-pentru-serviciul-paperless-validation/ .

Documentul **Condițiile de utilizare a serviciului Paperless Validation** conține termenii și condițiile stabilite între certSIGN și beneficiarul final al serviciului de încredere.
Identificarea documentului este: T&C QVSA RO și versiunea sa din subsolul documentului.
Cea mai recentă versiune a Condițiilor de Utilizare a Serviciului de Validare va fi întotdeauna prezentă la: https://www.certsign.ro/ro/document/conditiile-de-utilizare-a-serviciului-paperless-validation/.
Versiunile mai vechi ale acestei declarații de practici și ale Condițiilor de Utilizare sunt stocate în arhive iar link-uri către acestea vor fi furnizate la cerere.
**Politica globală de securitate a informațiilor certSIGN** este un document intern, disponibil doar membrilor certSIGN. Politica de securitate a informațiilor se aplică tuturor liniilor de activitate ale companiei și acoperă informațiile, sistemele informaționale, rețelele, mediul fizic și persoanele relevante care susțin serviciile furnizate.
**certSIGN Risk Management** este un document confidențial, disponibil doar unui grup de distribuție certSIGN, care include analiza principalelor amenințări și vulnerabilități, o evaluare a riscurilor și soluția propusă pentru fiecare risc considerat.
certSIGN a implementat un Sistem de Management al Securității Informațiilor (ISMS) conform standardului ISO/IEC-27001:2013. certSIGN a obținut certificarea ISMS conform Standardul ISO/IEC-27001:2013.
certSIGN a implementat toate controalele necesare cerute de reglementările eIDAS și GDPR și standardele corespunzătoare (adică ETSI EN 319 401) în ISMS. Directorul executiv al certSIGN aprobă politicile și practicile legate de securitatea informațiilor.

## 2 Management și operare Servicii de Încredere

certSIGN a implementat un sistem de management al securității informațiilor conform ISO/IEC 27001:2013 și a obținut certificarea ISO/IEC 27001:2013 de la un organism de certificare internațional acreditat. Serviciile calificate de validare a semnăturilor și a sigiliului

intră în domeniul de aplicare al acestei certificări. Paragrafele de mai jos rezumă managementul și operațiunile serviciului de încredere, inclusiv controalele de securitate aplicate.

## 2.1 Organizare internă

### 2.1.1 Fiabilitatea organizației

certSIGN respectă toate obligațiile legale aplicabile furnizării serviciilor sale de încredere. Își desfășoară operațiunile în conformitate cu politicile și practicile adoptate.
certSIGN asigură că toate cerințele definite în Declarația de aplicabilitate ISO27001:2013 și această Declarație de practică sunt implementate și rămân aplicabile pentru serviciile de încredere furnizate.
certSIGN oferă serviciile sale de încredere conform practicilor nediscriminatorii.
certSIGN are stabilitatea financiară și resursele necesare pentru funcționarea în conformitate cu acest document. certSIGN menține asigurarea de răspundere civilă în conformitate cu legislația aplicabilă, pentru a acoperi obligațiile care decurg din operațiunile sale și în conformitate cu art 13 din regulamentul eIDAS. certSIGN poate oferi mai multe informații despre măsuri de fiabilitate la cererea specială legitimă a părților terțe.
certSIGN îndeplinește cerințele generale de securitate prevăzute la articolul 19 din Regulamentul eIDAS, astfel cum sunt dezvoltate în continuare în ETSI EN 319 401 Semnături și infrastructuri electronice (ESI); Cerințe generale ale politicii pentru furnizorii de servicii de încredere.
În legătură cu serviciile de încredere de validare, certSIGN oferă validarea semnăturilor și sigiliilor electronice (calificate) în conformitate cu articolul 32 din Regulamentul eIDAS și secțiunile relevante din ETSI TS 119 102-1 Semnături și infrastructuri electronice (ESI); Proceduri de Creare și Validare a Semnăturilor Digitale AdES; Partea 1: Creare și validare.
Serviciul de semnătură este furnizat în conformitate cu secțiunile aplicabile ale Regulamentului eIDAS, și anume considerentele (52, 55) și Anexa II.3.
Furnizarea Serviciilor de Încredere este supusă unui audit extern efectuat cel puțin o dată la 24 de luni de către un Organism de Evaluare a Conformității, iar statutul calificat este supravegheat de Organismul de Supraveghere.
Înregistrările privind funcționarea Serviciilor de încredere sunt puse la dispoziția părților terțe la cererea lor legitimă, pentru furnizarea de dovezi cu privire la funcționarea corectă a Serviciilor de încredere în scopul procedurilor judiciare.
Abonații sunt obligați să păstreze confidențialitatea parolelor și a acreditărilor aplicabile pentru a utiliza Serviciile de Validare și să comunice prompt certSIGN orice circumstanță care ridică suspiciuni sau riscul ca acestea să fie compromise.
certSIGN are aranjamente de asigurare adecvate pentru a acoperi furnizarea certSIGN de Servicii de încredere pentru a asigura despăgubiri pentru daune cauzate de o încălcare intenționată sau neglijentă a obligațiilor certSIGN conform Regulamentului eIDAS.
certSIGN nu este responsabil pentru:
• Orice prejudiciu care rezultă din nerespectarea unui semnatar sau a unui Abonat de a păstra secretul parolelor și credentialelor aplicabile pentru a utiliza Serviciul de semnătură sau serviciile de încredere
• Neexecutarea obligațiilor sale dacă o astfel de neexecutare se datorează unor erori sau probleme de securitate ale oricărei autorități publice
• Neîndeplinirea obligațiilor sale dacă o astfel de neîndeplinire este cauzată de un eveniment de Forță Majoră.
Litigiile legate de Serviciile de încredere furnizate de certSIGN vor fi soluționate inițial prin procedura de conciliere, în cursul căreia ambele părți vor negocia cu bună-credință soluții cu privire la orice diferende apărute. Consiliul TSP al certSIGN (PPMB) va fi responsabil pentru gestionarea acestei proceduri de conciliere. În cazul în care plângerea specifică nu este soluționată în termen de treizeci (30) de zile de la începerea procesului de conciliere, părțile pot trimite litigiul instanțelor competente din București, România.

Toate informațiile confidențiale și de proprietate dezvăluite către certSIGN în utilizarea Serviciilor de încredere vor fi informații confidențiale.
Informațiile confidențiale nu includ informații care:
• intră în domeniul public fără vina certSIGN;
• este comunicat de către un terț către certSIGN fără orice obligație de încredere;
• a fost dezvoltat independent de certSIGN fără referire la Informații Confidenţiale ale părții care dezvăluie;
• a fost în posesia legală a certSIGN înainte de dezvăluire și nici nu a fost obținut direct sau indirect de la partea care dezvăluie, sau
• este obligat să fie dezvăluit prin lege, cu condiția ca certSIGN să fi notificat prompt în scris dezvăluirea către partea afectată a unei astfel de cerințe și a acordat părții terțe un termen rezonabil pentru a se opune unei asemenea cerinţe.
Orice organizație externă care utilizează serviciile TSP va fi constrânsă prin contract să urmeze politicile și practicile aplicabile și să urmeze procedurile aprobate de certSIGN.
Toate versiunile implementate ale modulelor QSVS sunt testate anterior conform Planului de testare aprobat, în medii de testare, cu diferite cazuri de utilizare, pozitive și negative.

### 2.1.2 Separarea atribuțiilor

Se asigură organizațional și se implementează tehnic o segregare strictă a sarcinilor între dezvoltarea și operarea platformei. Rolurile de administrare și operare a securității sunt separate din punct de vedere organizațional și sunt strict limitate la personalul autorizat.
Sistem de management al securității informațiilor implementat și certificat conform ISO/IEC 27001:2013 asigură verificarea și menținerea separării sarcinilor. Mai precis: rolurile de manager de securitate a informațiilor (ISM) și de auditor intern sunt separate.
De asemenea, Comitetul de Management al Politicilor și Procedurilor este înființat pentru a se ocupa de problemele majore, inclusiv problemele de securitate a informațiilor.

## 2.2 Resurse umane

certSIGN, în calitate de furnizor de servicii de încredere, se asigură că verificările relevante sunt efectuate de personal de specialitate.
Obligațiile de bază în ceea ce privește securitatea sunt stabilite în contractul de muncă al fiecărei persoane: acesta include clauze de confidențialitate și de neconcurență în contract.
Fiecare potențial angajat este evaluat pentru dovezile necesare de calificare a pregătirii profesionale necesare pentru a îndeplini funcția în cauză într-o manieră competentă și calitativă. Dacă s-a dobândit suficientă experiență în mediul de lucru real și poate reprezenta echivalentul unui curs (sau cursuri) de formare profesională, cerințele relevante sunt clar stabilite în postul vacant și vor fi verificate prin referire la dovezile de experiență prezentate de către viitorul angajat.
Înainte de angajare:

- **Screening** - Politica de management al resurselor umane este o parte a ISMS. Dacă definește procesele de recrutare, angajare și încetare a angajării. Verificările și verificările înainte de angajare, inclusiv verificările privind condamnările penale, așa cum este necesar pentru furnizorii de servicii de încredere calificate, istoricul de angajare și referințele fac parte din procesul de recrutare certSIGN.
- **Termeni și condiții de angajare** - Fiecare angajat semnează o formă standardizată de contract de muncă și acord de confidențialitate înainte de angajare și de a presta activități efective. În plus, un angajat se familiarizează cu lista de secrete de afaceri care este aprobată de organul de conducere al organizației și toate informațiile și datele care se încadrează în categoriile definite că trebuie păstrate ca secrete de afaceri și protejate.

În timpul angajării:

- **Responsabilități de management** - Managementul guvernează și sprijină activitățile ISMS, iar angajații sunt una dintre părțile esențiale ale ISMS. Procesul de guvernare și responsabilitățile de management sunt descrise în Politica de securitate a informațiilor și documentul privind practicile de management
- **Conștientizarea securității informațiilor, educație și formare** - Activitățile de formare și conștientizare internă sunt esențiale pentru ca personalul să înțeleagă importanța managementului securității informațiilor și propria contribuție la ISMS, să accepte politici și planuri și să înțeleagă consecințele încălcării regulilor de securitate a informațiilor. Ca urmare, planul de instruire și conștientizare este pregătit și coordonat de ISM si include actualizari periodice (anuale) pentru amenintari noi si practici curente de securitate. Executarea acestuia are ca rezultat înregistrări tangibile asociate. Toți angajații care ocupă funcții de încredere îndeplinesc cerința privind „cunoștințele de specialitate, experiența și calificările" prin formare profesională și diplome, prin experiență practică sau printr-o combinație a celor două.
- **Proces disciplinar** - Conform Politicii de management al resurselor umane, acțiunile disciplinare fac parte din:
  - Codul Muncii din Romania;
  - Contractul de muncă;
  - Clauze speciale NDA semnate de angajat.
- **Încetarea sau schimbarea responsabilităților în muncă** - Conform NDA-urilor cu angajații, declarațiile de confidențialitate rămân valabile după încetarea raportului de muncă. Revizuirea drepturilor de acces ar trebui efectuată conform Politicii de control al accesului atunci când apar modificări în responsabilitățile angajării.

## 2.3 Gestionarea activelor

### 2.3.1 Practici generale

certSIGN menține liste actualizate de active, inclusiv active de informații. Managementul riscului se bazează pe identificarea activelor. Cerințele generale includ:
**Inventarul activelor** – certSIGN menține liste actualizate cu toate activele (atât virtuale, cât și fizice) și proprietarii acestora. Evaluarea riscurilor organizației este aliniată cu identificarea activelor și amenințările sunt identificate ca fiind legate de active folosind o mapare a acestora.
**Proprietatea activelor** - menține liste actualizate cu toate activele (atât virtuale, cât și fizice) și ale proprietarilor acestora.
**Utilizarea acceptabilă a activelor** - Politica de utilizare acceptabilă definește reguli clare pentru utilizarea de sisteme informatice și alte active informaționale la certSIGN. De asemenea, definește responsabilitățile, activitățile interzise, preluarea activelor în afara site-ului, returnările de active, backup-urile, utilizarea internetului în cadrul activelor, computerul mobil, lucrul la distanță.
**Returnarea activelor** – certSIGN se asigură că toate echipamentele, software-ul și informațiile în formă electronică și hârtie sunt returnate, acolo unde este cazul.

### 2.3.2 Manipularea media

Suporturile care conțin informații sensibile sunt gestionate în siguranță și în conformitate cu Politica de clasificare a informațiilor certSIGN și Procedurile de operare certSIGN. Specific:
**Gestionarea suporturilor amovibile** - Politica de clasificare a informațiilor definește modul de gestionare a informațiilor în formate tipărite, electronice, electronice în sistemele informatice și e-mail, inclusiv mediile amovibile (și de stocare). Include accesul, utilizarea parolelor și criptarea.

**Eliminarea mediilor** - Procedurile de operare oferă controale pentru eliminarea și distrugerea echipamentelor și a mediilor. În general, toate echipamentele care conțin medii de stocare (de exemplu, computere, telefoane mobile etc.) trebuie să fie șterse înainte de a fi reutilizate sau mediile distruse înainte de a fi aruncate.
**Transfer fizic** - Politica de clasificare a informațiilor definește controalele tehnice de securitate pentru securizarea informațiilor în media, inclusiv pentru transfer, în funcție de nivelul de clasificare. Procedurile de operare prevăd cerința de a șterge orice tip de suport înainte de a fi reutilizat.

## 2.4 Controlul accesului

certSIGN operează o rețea segmentată (utilizatori, dezvoltare și producție) în care sunt instalate firewall-uri.
Accesul la operațiunile privilegiate este restricționat prin intermediul controalelor de acces, unde au fost definite și atribuite o serie de grupuri și profiluri în funcție de responsabilitățile postului: acestea sunt concepute pentru a impune segregarea sarcinilor și principiul cel mai mic privilegiu.
Drepturile de acces sunt alocate după autorizarea managementului.

Cerințe de business pentru controlul accesului:
**Politica de control al accesului** - Principiul de bază este că accesul la toate sistemele, rețelele, serviciile și informațiile este interzis („interzis implicit”), cu excepția cazului în care este permis în mod expres („trebuie să știe”) utilizatorilor individuali sau grupurilor de utilizatori. Politica de control al accesului oferă un cadru cuprinzător pentru furnizarea de acces (electronic), cerințe pentru setările de securitate a contului corporativ, gestionarea privilegiilor și revizuirea regulată a drepturilor de acces. Conform politicii, trebuie asigurate și păstrate înregistrările de control ale accesulu, cu trasabilitate.
**Accesul la rețele și serviciile de rețea** – Principiul de bază este că accesul la toate sistemele, rețelele, serviciile și informațiile este interzis („interzis implicit”), cu excepția cazului în care este permis în mod expres („trebuie să știe”) utilizatorilor individuali sau grupurilor de utilizatori. Accesul la distanță este acceptat numai într-un mod criptat (proceduri de operare) și face obiectul Politicii de utilizare acceptabilă de la certSIGN.

Gestionarea accesului utilizatorilor:
**Înregistrarea și anularea utilizatorilor** – Politica de control al accesului certSIGN oferă un cadru pentru înregistrarea unui utilizator în directorul corporativ, rețeaua internă și sistemele informaționale. Politica de control al accesului oferă, de asemenea, un proces de anulare a înregistrării utilizatorilor, inclusiv cerințe pentru eliminarea conturilor.
**Asigurarea accesului utilizatorilor** - Principiul de bază este că accesul la toate sistemele, rețelele, serviciile și informațiile sunt interzise („interzise în mod implicit”), cu excepția cazului în care sunt permise în mod expres („trebuie să știe”) utilizatorilor individuali sau grupurilor de utilizatori. Accesul de la distanță este acceptat numai în mod criptat (Proceduri de operare) și face obiectul Politicii de utilizare acceptabilă.
**Gestionarea drepturilor de acces privilegiate** - privilegiile pentru fiecare sistem (activ) pot fi acordate numai de proprietarii respectivi sau de PPMB.
**Gestionarea informațiilor secrete de autentificare ale utilizatorilor** - Politica de utilizare acceptabilă oferă cerințe complete pentru ca utilizatorii să gestioneze și să utilizeze informațiile secrete de autentificare.
**Revizuirea drepturilor de acces utilizator** - Revizuirea regulată a drepturilor de acces este definită în Politica de control al accesului.
**Eliminarea sau ajustarea drepturilor de acces** - Drepturile de acces sunt eliminate sau ajustate prin respectarea Politicii de control al accesului. În afara modificărilor imediate ale drepturilor de acces la solicitările de business, managerul responsabil garantează și asigură că drepturile de acces pentru fiecare sistem/subsistem/componentă sunt revizuite cel puțin o dată pe an.

Responsabilitatile utilizatorului:
**Utilizarea informațiilor secrete de autentificare** - Politica de utilizare acceptabilă oferă cerințe complete pentru ca utilizatorii să gestioneze și să utilizeze informațiile secrete de autentificare. Aplica cele mai bune practici din industrie, cum ar fi utilizarea instrumentelor criptate de gestionare a parolelor.

Control acces la sistem și aplicație:
**Restricționarea accesului la informații** - Politica de clasificare a informațiilor definește procedurile de restricție și furnizare a accesului la informații. În plus, Politica de control al accesului definește principiul de bază conform căruia accesul la toate sistemele, rețelele, serviciile și informațiile este interzis („interzis implicit”), cu excepția cazului în care este permis în mod expres („trebuie să cunosc”) către utilizatori individuali sau grupuri de utilizatori.
**Proceduri securizate de conectare** - regulile de furnizare a accesului (electronic) în Politica de control al accesului necesită ca accesul la serviciul/aplicația internă, externă sau terță parte să fie furnizat prin utilizarea serviciului de autentificare a contului corporativ.
**Sistem de gestionare a parolelor** - Cerințele detaliate pentru setările de securitate a contului corporativ sunt enumerate în Politica de control al accesului, care reflectă cele mai bune practici din industrie.
**Utilizarea programelor utilitare privilegiate** - Există o limitare în Politica de utilizare acceptabilă conform căreia utilizatorii nu trebuie să ia parte la activități care pot fi utilizate pentru a ocoli controalele de securitate ale sistemului informatic.
**Controlul accesului la codul sursă al software-ului** - Codul sursă al programului este proprietate intelectuală și este accesibil doar pe bază de necesitate. Politica de clasificare a informațiilor definește persoanele autorizate și restricțiile de acces la secretele de afaceri (codul sursă al programului face parte din secretele de afaceri). Codul sursă fizic este stocat în sistemul de versiune a codului sursă, unde ISM oferă acces bazat pe chei la sursele necesare.

## 2.5 Controale criptografice

Datele în repaus și în tranzit sunt criptate folosind standarde din industrie.
Controale criptografice:
**Politica privind utilizarea controalelor criptografice** - Politica privind utilizarea controalelor criptografice definește reguli (regulament) pentru utilizarea controalelor criptografice, precum și regulile de utilizare a cheilor criptografice, în scopul protejării confidențialității, integrității, autenticității și nerepudierea informațiilor.
**Managementul cheilor** - Politica privind utilizarea controalelor criptografice definește gestionarea cheilor, inclusiv practicile de distribuire a acestora.
certSIGN CA folosesc protecția cheii hardware care respectă cel puțin standardele FIPS 140-2 nivel 3 sau Common Criteria EAL 4. Generarea perechilor de chei CA trebuie efectuată într-un dispozitiv criptografic securizat care este un sistem de încredere care respectă cel puțin standardele FIPS 140-2 nivel 3 sau Common Criteria EAL 4.
În cadrul certSIGN, în calitate de QSVSP, implementarea serviciului respectă mecanismele criptografice convenite, aprobate de Grupul european de certificare în domeniul securității cibernetice și publicate de ENISA, privind utilizarea tehnicilor criptografice adecvate la furnizarea serviciilor de validare calificate pentru QES.[GP1.1]
Cheile private de semnare ale certSIGN sunt exportate și importate într-un alt dispozitiv criptografic securizat, numai cu aprobarea PPMB, cum ar fi la sediul DR, unde aceste operațiuni de export și import sunt implementate în condiții de securitate și în conformitate cu certificarea dispozitivelor HSM.

## 2.6 Securitate fizică și de mediu

Accesul fizic la birouri și centrele de date este limitat în mod corespunzător personalului autorizat. Sunt în vigoare măsuri de salvgardare pentru a proteja activele critice și pentru a asigura continuitatea.
Accesul fizic este controlat și monitorizat de un sistem de alarmă integrat. Sistemul de prevenire a incendiilor, sistemul de detectare a intruziunilor și sistemul de alimentare de urgență sunt în vigoare.
Programul de lucru CERTSIGN este de luni până vineri între orele 9.00 și 18.00. În afara acestui interval orar, inclusiv de sărbătorile legale, accesul în incinta CERTSIGN este permis numai persoanelor autorizate de către Conducerea CERTSIGN.
Vizitatorii sunt însoțiți permanent de personalul autorizat.
Spațiile CERTSIGN sunt împărțite în:

- zone de birouri,
- domenii IT,
- Zona operatori CA
- Zona operatori și administratori RA,
- Zona de dezvoltare și testare.

Zonele IT sunt dotate cu sistem de securitate monitorizat construit pe baza mișcării, intruziunii și incendiului. Accesul în această zonă este permis numai personalului autorizat. Monitorizarea drepturilor de acces se realizează pe baza de carduri electronice și cititoare adecvate, montate lângă zona de intrare. Fiecare intrare și ieșire din zonă este înregistrată automat în jurnalul de evenimente.

Accesul în zona operatorilor este permis numai pe baza unui card electronic și a cititorului corespunzător acestuia. Întrucât toate informațiile sensibile sunt protejate prin utilizarea dulapurilor încuiate, în timp ce accesul la terminalul operatorului sau al administratorului necesită o autorizare prealabilă, securitatea fizică implementată este considerată adecvată. Cheile din zonă sunt accesibile numai personalului autorizat. Zona poate fi ocupata exclusiv de personalul CERTSIGN si persoane autorizate, acestora din urma li se acorda acces numai daca sunt insotite.

Persoanele nesupravegheate nu sunt permise în această zonă. Programatorii și dezvoltatorii nu au acces la informații sensibile. Dacă un astfel de acces este necesar, este necesară prezența administratorului de securitate. Proiectele în curs de implementare și software-ul lor sunt testate în mediul de dezvoltare al CERTSIGN.

## 2.7 Securitatea operațiunii

În ceea ce privește Controlul schimbărilor, pentru fiecare modificare sau proiect pe platformele certSIGN, se efectuează analize funcționale și tehnice care includ identificarea măsurilor de securitate adecvate necesare. Schimbările sunt controlate prin intermediul unui proces formal de management al incidentelor și al schimbărilor.
Protecția anti-malware este activată, iar utilizarea suporturilor amovibile este limitată și nu acceptă activități critice pentru afaceri.
Serverele Windows și bazele de date SQL sunt actualizate periodic, utilizând platforma implicită de actualizare. Este definit formal un proces de gestionare a patch-urilor. certSIGN utilizează un mediu de aplicație care este actualizat constant cu cele mai recente remedieri de securitate, pentru a se asigura că sistemele pe care este dezvoltată aplicația aplică măsurile de securitate adecvate și se adaptează la mediile specifice de aplicație.
CERTSIGN utilizează sisteme și produse de încredere care sunt protejate împotriva modificărilor și asigură securitatea tehnică și fiabilitatea proceselor susținute de acestea.

certSIGN utilizează implementări bine testate și verificate ale protocoalelor și bibliotecilor standardizate în toate implementările și configurațiile aplicațiilor utilizate.

### 2.7.1 Cerințe tehnice specifice de securitate informatică

Mecanismele de securitate care protejează sistemele informatice sunt executate la nivelul sistemelor de operare, aplicațiilor și protecțiilor fizice.

Calculatoarele sunt configurate cu următoarele mecanisme de securitate:

- Înregistrare autentificată obligatorie la nivel de sistem de operare și aplicații,
- Control al accesului discreționar,
- Posibilitatea de a efectua audit de securitate,
- Computerul este accesibil numai personalului autorizat, care îndeplinește roluri de încredere în CERTSIGN,
- Aplicarea separării sarcinilor, care decurge din rolul îndeplinit în sistem,
- Identificarea și autentificarea rolurilor și a personalului care îndeplinește aceste roluri,
- Prevenirea reutilizarii unui obiect de către un alt proces după ce obiectul a fost eliberat printr-un proces autorizat,
- Protecția criptografică a schimbului de informații și protecția bazelor de date,
- Arhivarea istoricului operațiunilor pe computer și a datelor solicitate de audituri,
- O cale sigură care permite identificarea și autentificarea fiabilă a rolurilor și a personalului care îndeplinește aceste roluri,
- Metode de restaurare a cheilor (numai pentru modulele de securitate hardware),
- Monitorizare si alertare in caz de acces neautorizat.

Integritatea sistemelor și informațiilor CERTSIGN este protejată împotriva virușilor, a software-ului rău intenționat și neautorizat.

Suporturile utilizate în sistemele CERTSIGN sunt gestionate în siguranță pentru a proteja mediile de deteriorare, furt, acces neautorizat și uzură.

Procedurile de gestionare a media sunt implementate pentru a proteja împotriva învechirii și deteriorării suporturilor pentru perioada de timp pentru care trebuie păstrate înregistrările.

Datele sensibile sunt protejate împotriva dezvăluirii prin intermediul obiectelor stocate reutilizate (de exemplu, fișiere șterse) care nu sunt accesibile utilizatorilor neautorizați. În acest scop, se utilizează software special cu algoritmi de ștergere securizată pentru mediile de stocare, HSM-urile vor fi setate la zero, dispozitivele criptografice securizate (jetoane/carduri) vor fi formatate înainte de reutilizare/sau distruse fizic la sfârșitul ciclului lor de viață.

### 2.7.2 Controale de dezvoltare a sistemului

O analiză a cerințelor de securitate este efectuată în etapa de proiectare și specificare a cerințelor proiectelor de dezvoltare a sistemelor preluate de CERTSIGN sau în numele CERTSIGN pentru a se asigura că securitatea este integrată în sistemele IT.

Fiecare aplicație, înainte de a fi utilizată pentru producție în cadrul CERTSIGN, este instalată astfel încât să permită controlul versiunii curente și să prevină instalarea neautorizată a programelor sau falsificarea celor existente.

Reguli similare se aplică pentru înlocuirea componentelor hardware, după cum urmează:

- Hardware-ul este furnizat într-o manieră care să permită trasabilitatea și monitorizarea traseului componentelor până la locul de instalare a acestora,

- Livrarea hardware-ului de rezervă se realizează într-un mod similar cu livrarea hardware-ului original; înlocuirea este efectuată de personal de încredere și instruit.

### 2.7.3 Controale de management al securității

Scopul controlului managementului securității este de a supraveghea funcționalitatea sistemelor CERTSIGN, oferind asigurarea că sistemul funcționează corect și în conformitate cu configurațiile acceptate și implementate.

Controalele aplicate sistemului CERTSIGN permit verificarea continuă a integrității aplicației, a versiunii acestora, precum și autentificarea și verificarea originii hardware.

### 2.7.4 Controale de securitate a ciclului de viață

Politicile și procedurile de control al modificărilor sunt aplicate pentru lansări, modificări și remedieri software de urgență ale oricărui software operațional și modificări ale configurațiilor care aplică politica de securitate a CERTSIGN.

Configurația curentă a sistemelor CERTSIGN, orice modificare sau lansare nouă, modificare și remedieri software de urgență ale oricărui software operațional sunt documentate.

Configurațiile sistemelor de producție, ale sistemelor de management, ale sistemelor de asistență de securitate și ale sistemelor de asistență front-end /interne sunt revizuite periodic pentru a determina dacă vreo modificare a încălcat politicile de securitate ale CA.

CERTSIGN implementează proceduri de securitate internă pentru a se asigura că:

- Patch-urile de securitate sunt aplicate într-un timp rezonabil după ce sunt disponibile;
- Patch-urile de securitate nu sunt aplicate dacă introduc vulnerabilități sau instabilități suplimentare care depășesc beneficiile aplicării lor;

Motivele pentru care nu se aplică un patch de securitate sunt documentate.

CERTSIGN implementează o procedură internă de management al capacității care asigură monitorizarea capacității infrastructurii TIC pentru serviciile de producție și că sunt făcute estimări ale cerințelor de capacitate pentru a asigura disponibilitatea unei puteri de procesare și stocare adecvate.

## 2.8 Securitatea retelei

CERTSIGN își protejează rețeaua și sistemele împotriva atacurilor. În acest scop și pe baza evaluărilor de risc și a celor mai bune practici, implementăm un set integrat de controale de securitate:

a) Sistemele sunt segmentate în rețele sau zone pe baza relației funcționale, logice și fizice (inclusiv locația) dintre sisteme și servicii de încredere. CERTSIGN aplică aceleași controale de securitate tuturor sistemelor amplasate în aceeași zonă.
b) Accesul și comunicațiile între zone sunt limitate la cele necesare pentru funcționarea serviciilor de productie. Conexiunile și serviciile inutile sunt în mod explicit interzise sau dezactivate. Setul de reguli stabilit este revizuit în mod regulat.
c) Toate sistemele care sunt critice pentru funcționarea serviciilor de productie sunt păstrate într-una sau mai multe zone securizate
d) Rețeaua dedicată pentru administrarea sistemelor IT și rețeaua operațională sunt separate. Sistemele utilizate pentru administrarea implementării politicii de securitate nu sunt utilizate în alte scopuri. Sistemele / serviciile de producție sunt separate de sistemele utilizate în dezvoltare și testare (de exemplu sisteme de dezvoltare, testare și punere în pas).
e) Comunicarea între sisteme de încredere distincte se stabilește numai prin canale de încredere care sunt distincte din punct de vedere logic de alte canale de comunicație

și oferă o identificare securizată a punctelor finale și protecția datelor canalului împotriva modificărilor sau dezvăluirii.

f) Dacă este necesar un nivel ridicat de disponibilitate a accesului extern la un anumit serviciu de producție, conexiunea la rețeaua externă este redundantă pentru a asigura disponibilitatea serviciilor în cazul unei singure defecțiuni.

g) Se efectuează o scanare regulată a vulnerabilităților pe adresele IP publice și private identificate de CERTSIGN și se înregistrează dovezi că fiecare scanare a vulnerabilităților a fost efectuată de o persoană sau entitate cu abilitățile, instrumentele, competența, codul de etică și independența necesare pentru a furniza un raport de încredere.

h) Serviciile de producție CERTSIGN sunt supuse unui test de penetrare a sistemelor aferente la instalare și după upgrade-uri sau modificări ale infrastructurii sau aplicațiilor pe care CERTSIGN le consideră semnificative. Se înregistrează dovezi că fiecare test de penetrare a fost efectuat de o persoană sau entitate cu abilitățile, instrumentele, competența, codul de etică și independența necesare pentru a furniza un raport de încredere.

Serverele și stațiile de lucru de încredere ale sistemului CERTSIGN sunt conectate printr-o rețea locală (LAN), împărțită în subrețele prevăzute cu acces controlat. Accesul de pe Internet la orice segment este protejat prin firewall inteligent.

Controalele de securitate sunt dezvoltate pe baza firewall-ului și filtrarea traficului pe routere și servicii Proxy care protejează domeniile rețelei interne ale CERTSIGN de accesul neautorizat, inclusiv accesul de către Subiecți/Abonați și terți. Firewall-urile sunt configurate pentru a preveni toate protocoalele și accesele care nu sunt necesare pentru funcționarea CERTSIGN CA.

Mijloacele de protecție a securității rețelei acceptă numai mesaje trimise cu utilizarea protocoalelor http, https, NTP, POP3 și SMTP. Evenimentele (jurnalele) sunt înregistrate în jurnalele de sistem și permit supravegherea utilizării serviciilor furnizate de CERTSIGN.

CERTSIGN menține și protejează toate sistemele critice în cel puțin o zonă securizată și are în vigoare o procedură de securitate care protejează sistemele și comunicațiile dintre sistemele din zonele de securitate și zonele de înaltă securitate.

CERTSIGN configurează toate sistemele critice eliminând sau dezactivând toate conturile, aplicațiile, serviciile, protocoalele și porturile care nu sunt utilizate în operațiunile efective.

CERTSIGN oferă acces la zonele securizate și zonele de înaltă securitate numai rolurilor de încredere.

## 2.9 Gestionarea incidentelor

Logging-ul folosește funcționalitățile implicite ale platformei, atât la nivel de gazdă, cât și la nivel de cont. Monitorizarea jurnalului se realizează în mod reactiv, pentru a asigura analiza comportamentului anormal. Este definit un proces formal de gestionare a incidentelor și un proces dedicat de gestionare a incidentelor de securitate a informațiilor.

## 2.10 Culegere de probe

certSIGN păstrează înregistrări cu privire la funcționarea Serviciilor de încredere în scopul de a furniza dovezi ale funcționării corecte a Serviciilor de încredere. Aceste înregistrări vor fi dezvăluite autorităților de aplicare a legii numai prin hotărâre judecătorească și persoanelor cu drept de acces la ele la cererea legitimă. Aceste înregistrări sunt păstrate în

mod confidențial în facilități pentru a asigura disponibilitatea pe toată perioada în care sunt păstrate.
Pentru a gestiona eficient sistemele si aplicatiile utilizate de CERTSIGN in activitatea sa de prestator de servicii de încredere dar si pentru auditarea actiunilor angajatilor si clientilor, se inregistreaza toate informatiile despre evenimente importante, specifice, generate de sisteme si aplicatii. Aceste informații, cunoscute în mod colectiv sub denumirea de jurnal, sunt păstrate în așa fel încât să poată fi accesate de către Părțile terțe, auditori și autoritățile de stat oricând au nevoie de ele, pentru a oferi dovezi ale funcționării corecte a serviciilor în scopuri legale. proceduri sau pentru a detecta încercări de a compromite securitatea CERTSIGN. Evenimentele înregistrate sunt copiate de rezervă și păstrate într-o locație secundară.

Ori de câte ori este posibil, jurnalele sunt create automat. Dacă acest lucru nu este posibil, se vor folosi jurnalele pe hârtie. Fiecare înregistrare dintr-un jurnal creat fie automat, fie manual este păstrată sau dezvăluită în timpul unui audit, dacă este necesar. Precizia timpului a jurnalelor este asigurată de un server de timp care este sincronizat cu cel puțin două surse diferite care pot fi sateliți GPS sau UTC (NIMB).

### 2.10.1 Tipuri de evenimente înregistrate

Fiecare activitate critică din punct de vedere al securității CERTSIGN este înregistrată în jurnalele de evenimente și arhivată. Arhivele sunt stocate pe medii de stocare care nu pot fi șterse sau distruse cu ușurință (cu excepția cazului în care sunt transferate în mod fiabil pe medii pe termen lung) în perioada de timp în care trebuie să fie păstrate. Jurnalele de evenimente CERTSIGN conțin înregistrări ale tuturor activităților generate de componentele software din sistem. Aceste înregistrări sunt împărțite în trei categorii distincte:

- **Jurnalele de sistem** – conțin informații despre solicitările clienților și răspunsurile serverului (sau invers) la nivelul protocolului de rețea (de exemplu http, https); datele înregistrate sunt: adresa IP a stației sau serverului, operațiunile efectuate (de exemplu: căutare, editare, scriere etc.) și rezultatele acestora (de exemplu introducerea cu succes a unei înregistrări în baza de date),
- **Erori** – conțin informații despre erori la nivelul protocoalelor de rețea și la nivelul modulelor aplicațiilor;
- **Jurnalele de Audit** – conțin informații specifice serviciilor de producție, de exemplu: cerere de validare, cerere de verificare document, acceptare semnătură/sigiliu etc.

Jurnalele de mai sus sunt comune pentru fiecare componentă instalată pe un server sau pe o stație de lucru și au o capacitate predefinită. Când această capacitate este depășită, o versiune de jurnal este creată automat. Jurnalul anterior este arhivat și șters de pe disc.

Fiecare înregistrare automată sau manuală conține următoarele informații:

- Tip de eveniment,
- identificator de eveniment,
- Descrierea evenimentului,
- Data și ora producerii evenimentului,
- Identificatorul persoanei responsabile cu evenimentul.

Toate evenimentele legate de ciclul de viață al certificatelor utilizate în semnaturi/sigilii sunt înregistrate.

CERTSIGN menține jurnalele interne ale tuturor evenimentelor de securitate și ale tuturor evenimentelor operaționale relevante din întreaga infrastructură, indiferent de serviciul component, inclusiv, dar fără a se limita la:

- Modificări ale politicii de securitate
- Pornirea și oprirea sistemelor;
- Întreruperi;
- Blocări de sistem și defecțiuni hardware
- Activități de firewall și router
- Încercări de acces la sistemul PKI
- Accesul fizic al personalului și al altor persoane la părțile sensibile ale oricărui site sau zonă securizată;
- Backup și restaurare;
- Raportul testelor de recuperare în caz de dezastru;
- Inspecții de audit;
- Actualizări și modificări ale sistemelor, software-ului și infrastructurii;
- Intruziuni în securitate și încercări de intruziune.

Accesul la jurnalele este permis exclusiv ofițerului de securitate, personalului special desemnat și auditorilor.

Confidențialitatea informațiilor abonatului este menținută.

### 2.10.2 Frecvența procesării jurnalului

Jurnalele sunt procesate continuu și/sau în urma oricărei alarme sau evenimente anormale. Jurnalele sunt arhivate și copiate în mod regulat.

### 2.10.3 Perioada de păstrare a jurnalului de audit

Înregistrările evenimentelor sunt stocate în fișiere de pe discul de sistem până când ating capacitatea maximă permisă. În tot acest timp, acestea sunt disponibile on-line, la cererea fiecărei persoane autorizate sau a procesului. După depășirea capacității admise, jurnalele sunt păstrate ca arhive și pot fi accesate exclusiv off-line, de la o anumită stație de lucru.

Arhivele jurnalelor se păstrează 3 ani.

### 2.10.4 Protecția jurnalului de audit

Fișierele jurnal sunt protejate corespunzător de un mecanism de control al accesului. Protecția corespunzătoare împotriva modificării și ștergerii jurnalelor de audit este implementată astfel încât nimeni să nu poată modifica sau șterge înregistrările de audit decât după transferul pe un mediu de stocare pe termen lung în scopuri de arhivare. Doar ofițerul de securitate, personalul special desemnat sau un auditor pot revizui un jurnal de evenimente. Accesul la jurnalul de evenimente este configurat astfel încât:

- Numai entitățile de mai sus au dreptul de a citi înregistrările revistei,
- Platforma centrală de jurnal arhivează sau șterge automat fișierele (după arhivarea lor) care conțin evenimente înregistrate,
- Este posibil să se identifice orice încălcare a integrității; acest lucru asigură că înregistrările nu conțin lacune sau falsuri,
- Nicio entitate nu are dreptul de a modifica conținutul unui jurnal.

Mai mult, controalele de protecție a jurnalelor sunt implementate în așa fel încât, chiar și după arhivarea jurnalului, este imposibil să ștergeți înregistrările sau jurnalul în ansamblu înainte de expirarea timpului de păstrare globală a jurnalului.

### 2.10.5 Proceduri de copiere a jurnalului de audit

Politicile de securitate CERTSIGN necesită ca jurnalul de evenimente să aibă o copie de rezervă periodică. Aceste copii de siguranță sunt stocate în locații auxiliare ale CERTSIGN. Fișierele jurnal și traseele de audit sunt copiate de siguranță conform procedurilor interne.

### 2.10.6 Sistem de colectare a auditului (intern vs. extern)

Toate jurnalele generate de servere, dispozitive de rețea, echipamente de securitate, aplicații sunt trimise continuu către o platformă centrală, al cărei scop este:

- Colectarea
- Stocarea
- Analiza
- Corelarea
- Arhivarea
- Back-up pe termen lung

## 2.11 Managementul continuității activității

Există un plan de continuitate a activității și de recuperare în caz de dezastru.
CERTSIGN a stabilit într-un Plan de Continuitate a Afacerii și de Recuperare în caz de dezastru toate măsurile necesare pentru a asigura recuperarea completă a serviciilor sale în caz de dezastru, sau de întrerupere a oricărei componente sau serviciu IT&C importantă mai mult decât timpul de nefuncționare maxim tolerabil stabilit. Orice astfel de măsuri sunt conforme cu standardele ISO/IEC 27001 și 27002. Pentru fiecare componentă sau serviciu, operațiunile vor fi restabilite în limitele de timp maxim tolerabil stabilit în planul de continuitate.

Toate datele din sistemele necesare reluării operațiunilor de producție sunt copiate și stocate într-un loc îndepărtat și sigur, potrivit pentru a permite serviciilor de încredere să revină în timp util la operațiuni în caz de incident/dezastre.

Copii de rezervă ale informațiilor esențiale și ale software-ului sunt realizate în mod regulat. Sunt furnizate facilități de backup adecvate pentru a se asigura că toate informațiile și software-ul esențial pot fi recuperate în urma unui dezastru sau a unei defecțiuni media. Aranjamentele de rezervă sunt testate în mod regulat pentru a se asigura că îndeplinesc cerințele planurilor de continuitate a activității.

Funcțiile de backup și restaurare sunt realizate de rolurile de încredere relevante.

Planurile BCP și DRP abordează, de asemenea, compromisul, pierderea sau presupusul compromis al cheii private a unei CA sau compromisul algoritmilor PKI ca un dezastru și procesele planificate sunt în vigoare.

În urma unui dezastru, acolo unde este practic, se vor lua măsuri pentru a evita repetarea activităților greșite.

## 2.12 Planuri de terminare și de terminare a TSP

CERTSIGN are un plan de reziliere actualizat pentru a minimiza întreruperile abonaților și părților terțe, care ar putea apărea dintr-o decizie de a înceta o activitate/serviciu. Planul include obligații de a notifica în prealabil toți Abonații Serviciului TSP supus rezilierii (dacă există) și tranziției responsabilităților, în conformitate cu reglementarile in vigoare catre un alt Furnizor de Servicii de Încredere (TSP).

**Cerințe asociate tranziției sarcinilor**

Înainte ca un TSP să își înceteze activitatea, acesta va:

- Informa (cu cel puțin 30 de zile înainte) despre decizia de încetare a serviciilor: toți Abonații cu care CERTSIGN are acorduri sau altă formă de relații, printre care părțile care se bazează, alți furnizori de servicii de încredere și autorități relevante, cum ar fi organismele de supraveghere. În plus, aceste informații vor fi puse la dispoziția și a altor părți terțe;
- Transfera obligațiile sale unei părți de încredere pentru păstrarea tuturor informațiilor necesare pentru a furniza dovezi ale funcționării serviciilor de încredere pentru o perioadă rezonabilă, cu excepția cazului în care se poate demonstra că CERTSIGN nu deține astfel de informații. Informațiile se referă la informațiile de validare, și arhivele jurnalului de evenimente pentru perioada respectivă, așa cum este indicată Abonatului și părților terțe implicate;
- Acolo unde este posibil, va face aranjamente pentru a transfera furnizarea de servicii de validare pentru clienții existenți către un alt furnizor de servicii de încredere.

În cazul în care CERTSIGN își va înceta activitățile fără un transfer parțial sau total al activităților sale, va iniția procedura de reziliere a contractelor semnate cu partenerii implicați și/sau furnizorii.

CERTSIGN are un aranjament pentru a acoperi costurile pentru îndeplinirea acestor cerințe minime în cazul în care intră în faliment sau, din alte motive, este în imposibilitatea de a acoperi costurile de la sine, în măsura posibilului, în limita constrângerilor legislației aplicabile privind falimentul.

## 2.13 Conformitate

Procedurile operaționale definesc procesul de validare a semnăturilor pentru părțile interesate, precum și cerințele și responsabilitățile legale, de reglementare, contractuale și de altă natură pentru îndeplinirea acestora.
**Identificarea legislației aplicabile și a cerințelor contractuale** - O procedură operațională include procesul de validare a semnăturilor pentru părțile interesate, precum și cerințele legale, de reglementare, contractuale și de altă natură legate de securitatea informațiilor și resposabilitățile pentru îndeplinirea acestora. Activitățile au ca rezultat Lista menținută și actuală a cerințelor legale, de reglementare, contractuale și de altă natură.
**Drepturi de proprietate intelectuală** - Drepturile de proprietate intelectuală fac parte din Secretele de afaceri definite de PPMB. Este reglementat conform legislației UE și locale. Protecția drepturilor de proprietate intelectuală are ca rezultat NDA, obligații și responsabilități contractuale și termeni ai serviciilor certSIGN.
**Protecția înregistrărilor** - O procedură operațională asigură controlul asupra creării, aprobării, distribuției, utilizării și actualizărilor documentelor și înregistrărilor utilizate în ISMS. În general, angajații organizației pot accesa înregistrările stocate doar urmând principiul „trebuie să știi”.
**Confidențialitate și protecție a informațiilor de identificare personală** – activitățile certSIGN TSP sunt supuse reglementărilor UE GDPR, ale căror cerințe sunt încorporate în mod corespunzător în organizație, inclusiv documentația ISMS. Din perspectiva proprietarilor de servicii/procese/active, proprietarii de servicii/procese/active sunt responsabili pentru identificarea fiecărei cerințe individuale (inclusiv contractuale) și conformitatea în cadrul activului.
**Reglementarea controalelor criptografice** –Politicile certSIGN definesc reguli (reglementări) pentru utilizarea controalelor criptografice, precum și regulile de utilizare a cheilor criptografice, pentru a proteja confidențialitatea, integritatea, autenticitatea și nerepudierea informațiilor.

**Prevederi diverse** - certSIGN oferă acces nelimitat la servicii pentru persoanele cu dizabilități în conformitate cu legislația și standardele în vigoare.

## 2.14 Lantul de aprovizionare

certSIGN a documentat și implementat procese și proceduri pentru gestionarea riscurilor de securitate a informațiilor asociate utilizării produselor sau serviciilor furnizorilor. Acestea sunt detaliate în politica internă a certSIGN privind gestionarea furnizorilor terți („Politica de Management al Serviciilor Furnizate de Terti").
Procesul și procedurile implementate gestionează riscurile de securitate a informațiilor asociate cu lanțul de aprovizionare al produselor și serviciilor din domeniul tehnologiilor informației și comunicațiilor, conform cerințelor din ETSI EN 319 401 #7.14.
Atunci când certSIGN apelează la alte părți, inclusiv furnizori de componente de servicii de încredere, pentru a furniza părți ale serviciului său prin subcontractare, externalizare sau alte acorduri cu terți, își păstrează responsabilitatea generală pentru conformitatea cu politica lanțului de aprovizionare, politica sa de securitate a informațiilor și cerințele definite în politica serviciilor de încredere.
certSIGN revizuiește politica privind lanțul de aprovizionare și monitorizează, revizuiește, evaluează și gestionează modificările practicilor de securitate cibernetică ale furnizorilor direcți sau ale furnizorilor de servicii la intervale planificate sau după un incident legat de furnizarea de servicii de către furnizorii direcți sau furnizorii de servicii.

# 3 Proiectarea serviciului de validare a semnăturii

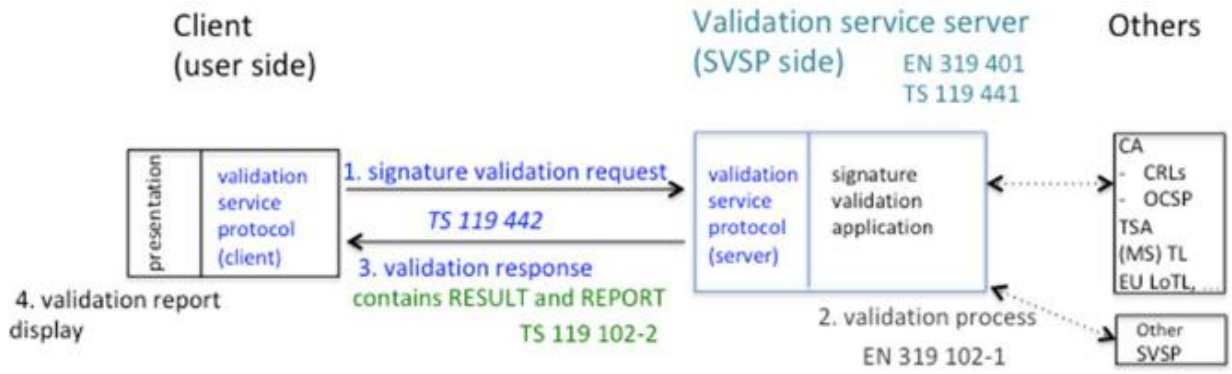
Serviciul poate fi utilizat numai de clienții contractuali certSIGN. Serviciul poate fi accesat doar folosind interfețe definite și publicate de certSIGN.
Abonatul Serviciului este obligat să protejeze interfața Serviciului de utilizarea neautorizată și să ofere securitate adecvată atunci când utilizează Serviciile. Aceasta se aplică la orice interfață utilizată pentru a accesa acest Serviciu.
Interfață înseamnă, în special, aplicația web pentru utilizarea Serviciului sau oricare aplicație sau interfață de integrare furnizată exclusiv de certSIGN sau de un integrator specificat de certSIGN.

## 3.1 Procesul de validare a semnăturii

Atunci când cerințe și reguli specifice sunt stabilite în prezenta specificație, acestea prevalează asupra cerințelor corespunzătoare din ETSI TS 119 102 sau ETSI TS 119 441. În cazul unor discrepanțe între prezentele specificații și specificațiile din ETSI TS 119 102 sau ETSI TS 119 441, prezentele specificații vor prevala.

### 3.1.1 Fluxul procesului de validare a semnăturii

Procesul este conform ETSI TS 119 441 V1.2.1 (2023-10) Electronic Signatures and Infrastructures (ESI); Cerințe de politică pentru TSP care furnizează servicii de validare a semnăturii.




În funcție de modul de validare ales, Clientul trimite o cerere de validare către certSIGN SVSP care conține documentul(ele) de validat, împreună cu semnăturile și parametrii tranzacționali complementari.
Serviciul certSIGN analizează cererea și

- când are succes
  - efectuează validarea intrării
  - creează un raport de validare
  - sigilează raportul creat și
  - returnează un răspuns care cuprinde raportul sigilat
- in caz contrar
  - returnează un mesaj de eroare

În acest sens, serviciul de validare certSIGN operează independent de contextul aplicației.

În scopul potrivirii unei valori digest (hash) cu date semnate, este important:

- A aplica algoritmul de digest (hash) care a fost specificat în timpul creării semnăturii,

- Că algoritmul de digest (hash) aplicat este considerat sigur în momentul semnării și nu a devenit slab până la momentul validării sau a fost protejat prin mijloace de conservare complementare;
- Că implementarea pentru (re)calcularea algoritmului de digest (hash) aplicat este corectă și de încredere și
- Că orice transformare explicită sau implicită a octeților de intrare pentru calcularea valorii de digest (hash) corespunzătoare este corectă în raport cu tipul de suport al documentului de intrare dat. De exemplu, în cazul unui document PDF, intervalele de octeți indicate în dicționarul de semnături specifică direct octeții de intrare pentru calculul digest, în timp ce în cazul unui document generic pot fi necesare transformări de conținut definite în mod explicit sau implicit pentru a obține octeți de intrare pentru calculul digest.

În conformitate cu ETSI EN 319 102-1 V1.3.1 (2021-11) *„ Semnături și infrastructuri electronice (ESI); Proceduri de Creare și Validare a Semnăturilor Digitale AdES; Partea 1: Creare și Validare ”*, procesul de validare prevede, pentru fiecare semnătură, una dintre următoarele trei indicații de stare:

- TOTAL-PASSED: indică faptul că semnătura a trecut verificarea și că respectă politica de validare a semnăturii
- TOTAL-FAILED: indică fie că formatul semnăturii este incorect, fie că valoarea semnăturii digitale nu trece verificarea
- INDETERMINAT: indică faptul că formatul și verificările semnăturii digitale nu au eșuat, dar nu există suficiente informații pentru a determina dacă semnătura electronică este validă

### 3.1.2 Validarea semnăturii și verificarea conformității

Modelul conceptual al validării semnăturii și al verificării conformității:

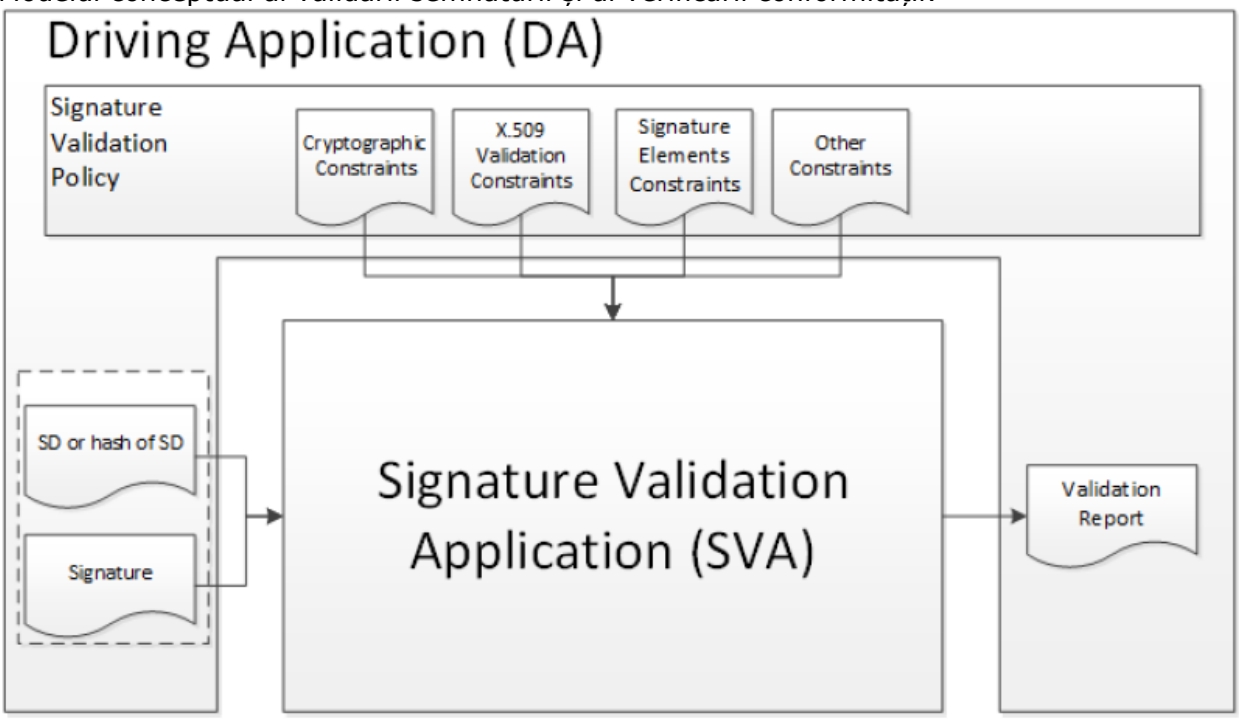



Figura 2 Model de validare a semnăturii cu verificarea conformității inclusă în SVA

În timp ce validarea semnăturii este procesul de verificare și confirmare a validității tehnice a unei semnături, verificarea conformității determină dacă o semnătură respectă cerințele unei specificații sau reglementări. Astfel, validarea semnăturilor și verificarea conformității semnăturilor sunt procese independente:

- O semnătură poate fi validă, dar nu și conformă cu un anumit nivel de semnătură necesar.
- O semnătură poate fi conformă cu un anumit nivel de semnătură, dar validarea acesteia poate să întoarcă o indicație de stare INDETERMINATĂ sau TOTAL-FAILED.

În timp ce verificarea conformității este în principiu ortogonală cu validarea semnăturii (o semnătură poate fi validă, dar nu și conformă), verificarea conformității poate fi cerută de o politică de validare a semnăturii pentru anumite contexte de afaceri.

Pentru fiecare dintre verificările de validare, procesul de validare oferă informații care justifică motivele pentru indicarea stării rezultată ca urmare a verificării față de constrângerile aplicabile. În plus, standardul ETSI definește o modalitate consecventă și precisă de justificare a stărilor sub un set de subindicații.

Procesul de validare este condus de politica de validare și permite validarea semnăturii pe termen lung. Verificarea semnăturii se face urmând blocurile de bază ale algoritmului de validare.
Pe diagrama simplificată de mai jos, care arată procesul de validare de bază a semnăturii, puteți urmări relațiile dintre fiecare modul care reprezintă un set logic de verificări utilizate în procesul de validare.

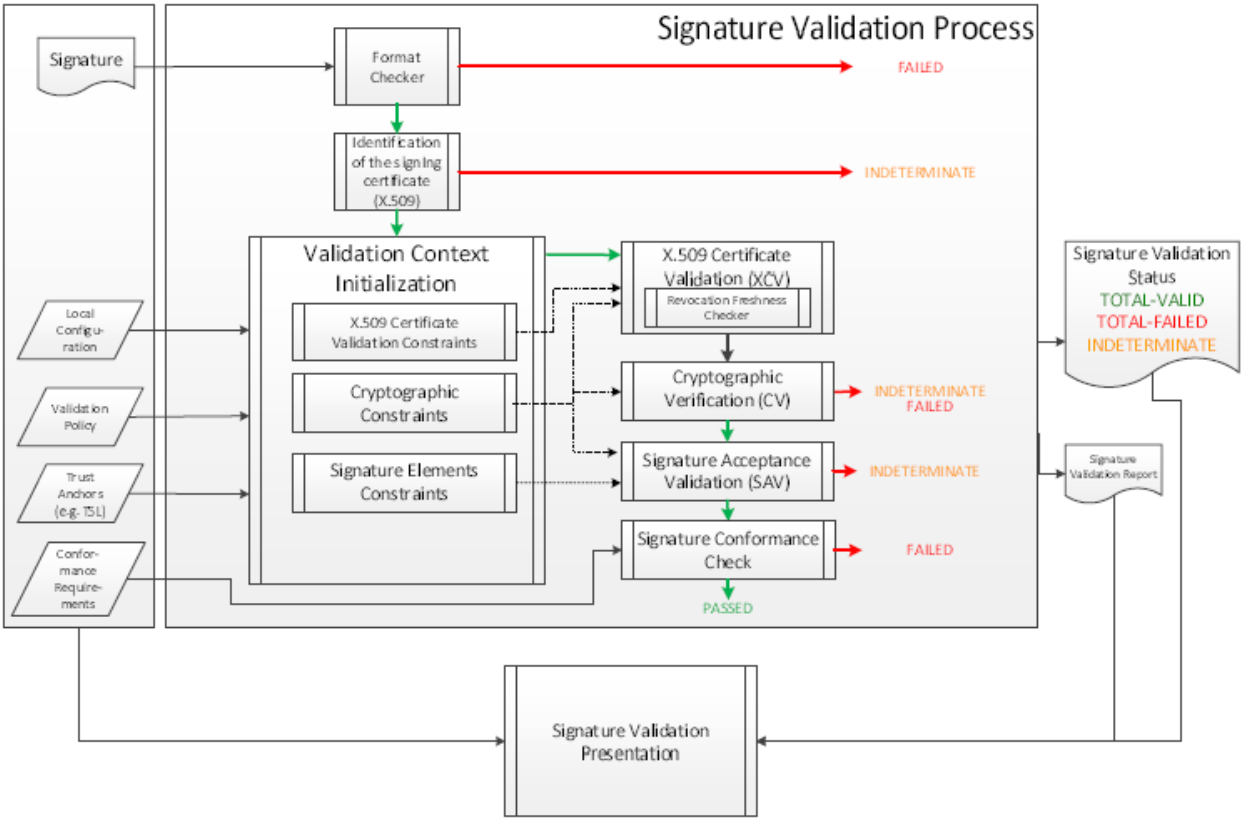



*Figura 3 Verificarea conformității ca parte a validării semnăturii*

certSIGN validează semnătura în raport cu o politică de validare a semnăturii, constând dintr-un set de constrângeri de validare, și emite o indicație de stare și un raport de validare care oferă detalii despre validarea tehnică a fiecăreia dintre constrângerile aplicabile (de exemplu, certificate sau marcaje temporale expirate, certificate revocate, perioada de utilizare algoritmi criptografici depașită).

certSIGN QSVS este conform ETSI TS 119 172-4 Constrângeri de validare și proceduri de validare (capitolul 4.2), acceptă cerințele privind validarea semnăturii și practicile de verificare a regulilor de aplicabilitate (capitolul 4.3) și a implementat procesul de verificare a aplicabilității tehnice (reguli) (capitolul 4.4). ). Raportul este implementat în conformitate cu Cerințe privind raportul de verificare a regulilor de aplicabilitate (capitolul 4.5).

### 3.1.3 Liste de încredere din UE ale furnizorilor de servicii de certificare

Pentru a permite accesul la listele de încredere ale tuturor statelor membre într-un mod ușor, Comisia Europeană a publicat o listă centrală cu link-uri către „listele de încredere” naționale (LOTL).
LOTL este publicat de UE la următorul URL:
https://eidas.ec.europa.eu/efda/tl-browser/#/screen/home
https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml.
Acest fișier XML conține lista listelor de încredere. Acest fișier trebuie să fie semnat de un certificat valid. Pentru a ști cine are permisiunea de a semna/publica LOTL, trebuie să ne referim la Jurnalul Oficial al Uniunii ( https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv: OJ.C_.2016.233.01.0001.01.RO).
Dacă semnătura LOTL este validă, conținutul poate fi, de asemenea, de încredere. Conține câteva informații pentru fiecare țară: URL-urile fișierelor XML / PDF, certificatele valide pentru semnătută, … Când avem încredere în LOTL, putem procesa fiecare TL. Dacă TL este valid, putem avea încredere în furnizorii de servicii și în certificatele acestuia.

Acest LOTL este apoi utilizat pentru a efectua validările de certificat care sunt necesare în contextul unei validări a semnăturii. SVS construiește calea certificatului până la o ancoră de încredere cunoscută, validează fiecare certificat găsit (folosind OCSP atunci când este posibil, în caz contrar CRL) și determină „calificarea" europeană.
Pentru a determina calificarea certificatului, SVA urmează standardul Semnături și infrastructuri electronice (ESI); Politici de semnătură; Partea 4: Politica de validare a semnăturilor pentru semnăturile/sigiliile electronice calificate europene folosind liste de încredere (ETSI TS 119 172-4). Acesta analizează proprietățile certificatului și aplică posibile anulări din lista de încredere aferentă.
SVA va calcula întotdeauna starea certificatului pentru două momente diferite: eliberarea certificatului și timpul de semnare/validare. Aceasta este o necesitate, deoarece calificarea certificatului poate evolua în timp.

## 3.2 Cerințe pentru protocolul de validare a semnăturii

Protocolul de validare a semnăturii este următorul:
1. SVC trimite SD-ul care conține semnătura (semnăturile) digitală pentru validare către SVS
2. SVS trimite răspunsul de validare a semnăturii care conține SVR către SVC

## 3.3 Interfețe

### 3.3.1 Canal de comunicare

Comunicarea între DA și SVS are loc printr-o conexiune TLS securizată. Acest lucru asigură confidențialitatea datelor transmise și oferă o modalitate pentru ambele părți de a se autentifica reciproc.

### 3.3.2 SVSP - alt TSP

Comunicarea dintre SVSP și alți TSP depinde de interfața care este definită și de cerințele TSP-ului care trebuie apelat.
SVS setează conexiuni TLS sau alte mijloace de autentificare pentru a comunica cu actori externi.

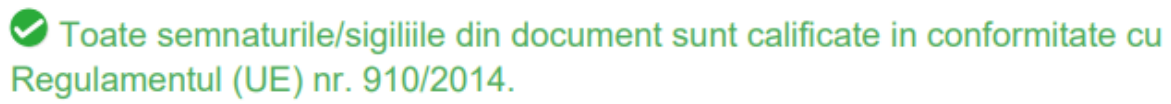
## 3.4 Raportul de validare a semnăturii

Raportul care poate fi citit de mașină este conform ETSI TS 119 102-2 V1.3.1 Semnături și infrastructuri electronice (ESI); Proceduri pentru crearea și validarea semnăturilor digitale AdES Partea 2: Raport de validare a semnăturii. certSIGN utilizează schema cerută în ETSI: https://forge.etsi.org/rep/esi/x19_10202_validation_report/raw/v1.3.1/1910202xmlSchema.xsd .
Raportul serviciului de validare a semnăturii conține:

- Numele documentului validat;
- Hash-ul documentului și algoritmul utilizat;
- Data și ora validării;
- O stare care indică rezultatul global al validării semnăturii pe document;
- Lista semnăturilor digitale incluse în document;
- Pentru fiecare semnătură digitală:
  - Starea validării semnăturii și a verificării conformității
  - Numele semnatarului din certificat
  - Emitentul certificatului de semnătură/sigiliu cu numele comun și identificatorul organizației
  - Data și ora UTC ale semnării
  - Emitentul certificatului de marcare temporală cu numele comun și identificatorul organizației
  - Starea validării ștampilei de timp și a verificării conformității

- Identificarea QSVS și versiunea acestuia;
- Sigiliul calificat certSIGN TSP cu ștampilă de timp pentru nerepudiere

Verificarea conformității efectuată de certSIGN se aplică Regulamentului UE Art.32 „Cerințe pentru validarea semnăturilor electronice calificate”. Prin urmare, doar un document PDF cu toate semnăturile validate ca TOTAL-PASSED și toate semnăturile conforme cu Regulamentul UE va avea o rezoluție la nivel de document care marchează că toate semnăturile/sigiliile sunt calificate UE:




Raportul de validare este semnat.

# 4 Anexa 1 - Parametrii de business

Descrierea politicilor de validare a parametrilor generali de acoperire a afacerii (BSP) este aplicabilă tuturor cazurilor și este independentă de formatul de semnătură utilizat.

## 4.1 BSP-uri legate în principal de aplicația/procesul de business

### BSP (a): FLUXUL DE LUCRU (SECVENȚIEREA ȘI TIMINGUL) AL SEMNATURĂRILOR

Politicile prezente de validare abordează validarea semnăturilor electronice avansate și calificate cuprinzând posibile marcaje temporale și extensii de date de probă privind o singură instanță sau mai multe instanțe de DTBS în timpul unei singure tranzacții, în timp ce un singur raport este returnat de către serviciu după o validare efectuată cu succes. Un DTBS poate consta din orice date binare care reprezintă în mod specific un document PDF. În cazul în care mai multe semnături sunt încorporate în același document PDF, semnăturile trebuie să fie seriale. Ordinea de validare este irelevantă.

Serviciul de validare certSIGN poate fi utilizat de către un Client/APP pentru a implementa fluxuri de lucru de afaceri care cuprind tranzacții multiple; într-un astfel de caz, fiecare tranzacție în cadrul fluxului de lucru Client/APP va fi efectuată conform politicii prezente în funcție de modul de validare ales.

### BSP (b): DATE DE VALIDAT

Clientul/APP este responsabil pentru conținutul și formatarea corectă a datelor care urmează să fie validate în conformitate cu standardele aplicabile. În special, trebuie să se asigure că datele de validat nu conțin coduri rău intenționate sau scripturi care ar putea altera datele de validat sau ar putea deteriora serviciile certSIGN.
În special, formatul unui SD poate fi doar PDF.
Serviciul de validare certSIGN garantează confidențialitatea unui SD în conformitate cu legile aplicabile privind confidențialitatea și legile românești privind sectorul financiar. certSIGN șterge în mod special și imediat, de pe serverele sale, toate copiile unui SD primit, dacă există, după ce a efectuat o tranzacție solicitată.

### BSP (c): RELAȚIA DINTRE DATELE SEMNATE ȘI SEMNATURĂ(E)

Relația dintre datele semnate și semnătura (semnăturile) depinde în mod specific de formatul semnăturii. Serviciul de validare certSIGN acceptă formatul PAdES, ceea ce înseamnă că semnătura este inclusă în documentul PDF.
Profilurile/Nivelurile de semnătură acceptate sunt:
1. B-B (semnătură de bază)
2. B-T (semnătură cu timp)
3. B-LT (semnătură cu material de validare pe termen lung)
4. B-LTA (Semnături care asigură disponibilitatea și integritatea pe termen lung a materialului de validare)

### BSP (d): COMUNITATEA ȚINTĂ

Dacă nu se specifică altfel într-o politică de validare a Clientului/APP derivată, serviciul de validare certSIGN validează semnăturile pe baza listelor europene de încredere și respectă Regulamentul eIDAS.

### BSP (e): ALOCAREA RESPONSABILITĂȚII PENTRU VALIDAREA ȘI EXTINDEREA SEMNĂTURII

Pe lângă ceasul mașinii serviciului, care este sincronizat cu o sursă de timp precisă de

încredere, serviciul de validare certSIGN folosește marcaje temporale de încredere și calificate conform profilului de solicitare (B-T, B-LT sau B-LTA) ca dovadă a existenței. în ceea ce privește elementele DTBS care sunt acoperite criptografic de marcajele de timp date.
Serviciul de validare certSIGN validează semnăturile existente pe DTBS. În cazul în care DTBS conține o semnătură nevalidă, informațiile respective sunt indicate în rezultatul furnizat de serviciu. certSIGN NU va anula procesul de validare din cauza unei semnături nevalide care este conținută în DTBS.
Un singur raport de validare furnizat de serviciul de validare certSIGN poate conține rezultate cu privire la semnăturile multiple aferente unui SD, în timp ce orice interpretare a acestor rezultate sau o diagnosticare generală a rezultatului, în special orice interrelație semantică a semnăturilor validate independent, este lăsată complet la latitudinea aplicației de afaceri. Serviciul de validare certSIGN nu realizează nicio interpretare semantică; furnizează numai diagnostice privind semnăturile validate individual, în conformitate cu standardele aplicabile.

## 4.2 BSP influențate în principal de prevederile legale/de reglementare asociate cererii/procesului de afaceri în cauză

### BSP (f): TIPUL LEGAL AL SEMNATURII

Serviciul de validare certSIGN acceptă validarea pentru toate tipurile legale de semnături electronice calificate pentru persoane juridice sau pentru persoane fizice care acționează în nume propriu sau în numele unei persoane juridice:

- Semnături electronice calificate acceptate de un certificat calificat X.509 v3;

Tipul legal al unei semnături este indicat în raportul de validare atunci când aceasta poate fi validată cu succes.

### BSP (g): ANGAJAMENT ASUMAT DE SEMNATAR

Serviciul de validare certSIGN poate dezvălui tipul de angajament atunci când este asociat cu o anumită semnătură pentru a fi luată în considerare de aplicația de afaceri.
Serviciul de validare nu interpretează un tip de angajament care este asociat cu o semnătură.

**Tipuri de angajament**

Următoarele tipuri de angajamente generice sunt definite în ETSI TS 119 172-1:

1) **Dovada originii**

- Descriere: indică faptul că semnatarul recunoaște că a creat, aprobat și trimis datele semnate.
- Identificator obiect: id-cti-ets-proofOfOrigin OBJECT IDENTIFIER ::= { iso(1) member-body(2)us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) cti (6) 1}
- URI: URI-ul pentru acest angajament este http://uri.etsi.org/01903/v1.2.2#ProofOfOrigin.

2) **Dovada de primire**

- Descriere: indică faptul că semnatarul recunoaște că a primit conținutul datelor semnate.
- Identificator obiect: id-cti-ets-proofOfReceipt OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) cti (6) 2}
- URI: URI-ul pentru acest angajament este http://uri.etsi.org/01903/v1.2.2#ProofOfReceipt.

3) **Dovada livrării**

- Descriere: indică faptul că TSP-ul care furnizează această indicație a livrat date semnate într-un magazin local accesibil destinatarului datelor semnate.

- Identificator de obiect: id-cti-ets-proofOfDelivery IDENTIFICATOR DE OBIECT ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) cti (6) 3}
- URI: URI-ul pentru acest angajament este http://uri.etsi.org/01903/v1.2.2#ProofOfDelivery.

4) **Dovada expeditorului**

- Descriere: indică faptul că entitatea care furnizează acea indicație a trimis datele semnate (dar nu neapărat le-a creat).
- Identificator de obiect: id-cti-ets-proofOfDelivery IDENTIFICATOR DE OBIECT ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) cti (6) 3}
- URI: URI-ul pentru acest angajament este http://uri.etsi.org/01903/v1.2.2#ProofOfSender.

5) **Dovada de aprobare**

- Descriere: indică faptul că semnatarul a aprobat conținutul datelor semnate.
- Identificator obiect: id-cti-ets-proofOfApproval OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) cti (6) 5}
- URI: URI-ul pentru acest angajament este http://uri.etsi.org/01903/v1.2.2#ProofOfApproval.

6) **Dovada creației**

- Descriere: indică faptul că semnatarul a creat datele semnate (dar nu neapărat aprobate, nici trimise).
- Identificator obiect: id-cti-ets-proofOfCreation OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) cti (6) 6}
- URI: URI-ul pentru acest angajament este http://uri.etsi.org/01903/v1.2.2#ProofOfCreation.

### BSP (h): NIVEL DE ASIGURARE PRIVIND EVIDENȚE LEGATE DE TIMP

Pentru a stabili ora semnăturii, serviciul de validare certSIGN utilizează următoarele tipuri de dovezi temporale:

- Un timp de semnare revendicat și
- Marcaje temporale de încredere sau calificate bazate pe ancore de încredere care sunt verificabile în conformitate cu lista de încredere a statelor membre.

Orice astfel de indicație, cu excepția timpului de semnare revendicat, poate servi nu numai ca o dovadă a existenței utilizată de serviciu pentru a efectua validarea semnăturilor dincolo de perioada de valabilitate a certificatelor implicate, dar poate reprezenta și un indicator de timp de încredere pentru aplicația de afaceri. pentru a lua decizii privind fluxul de lucru la propria discreție.
Serviciul de validare certSIGN poate procesa numai ștampilele de timp/mărcile temporale care sunt conforme cu RFC 3161. Serviciul de validare certSIGN nu interpretează dovezile de sincronizare dincolo de faptul că le utilizează pentru efectuarea validării semnăturii.
Serviciul de validare certSIGN va include toate dovezile temporale găsite în semnăturile procesate.

### BSP (i): FORMALITATI DE SEMNARE

Serviciul de validare certSIGN aplică procedurile de validare documentului PDF furnizat ca intrare de către utilizator.
Serviciul de validare certSIGN dezvăluie în raportul final de stare atributele de semnătură asociate.

## BSP (j): LONGEVITATE ȘI REZISTENTĂ LA SCHIMBARE

Longevitatea așteptată a unei semnături electronice depinde de profilul acesteia.

**Semnătura B-B** : longevitatea semnăturii este cea a certificatului de semnare în momentul semnării, cu excepția cazului în care certificatul de semnatar sau orice certificat de părinte din lanțul emitentului până la ancora de încredere a fost revocat după semnare, ceea ce în acest caz ar reda instantaneu semnătura ca fiind neverificabilă.

**Semnătura B-T** : longevitatea semnăturii este cea a certificatului de semnare în momentul semnării și este posibil extinsă dincolo de durata sa de viață atunci când sunt disponibile dovezi online adecvate privind starea certificatului. Momentul semnării este în acest caz confirmat prin intermediul unui marcaj temporal al semnăturii, marca temporală a semnăturii fiind o condiție prealabilă pentru o astfel de longevitate extinsă dincolo de durata de viață a certificatului de semnare. Longevitatea extinsă poate fi acceptată în acest caz până la longevitatea certificatului de marcare temporală la momentul creării mărcii temporale a semnăturii. Spre deosebire de o semnătură B-B, revocarea certificatului de semnătură sau revocarea oricărui părinte al acestuia după crearea ștampilei temporale a semnăturii nu are niciun impact asupra longevității unei semnături B-T. În schimb, longevitatea extinsă a unei semnături B-T poate fi afectată atunci când un algoritm criptografic, care a fost implicat în crearea ștampilei de timp a semnăturii, a devenit slab în timp.

**Semnătura B-LT** : longevitatea semnăturii este cea a semnăturii B-T citate mai sus. Acesta este completat de elemente de probă adăugate la obiectul de date semnate pentru a permite parțial validarea offline a semnăturii, în funcție de longevitatea și eligibilitatea datelor de probă adăugate. Este important de reținut că longevitatea unei semnături nu este extinsă dincolo de cea a creșterii B-T menționată mai sus, doar datorită utilizării dovezilor suplimentare de stare offline. Cu toate acestea, augmentarea B-LT poate facilita procesul general de validare și poate servi ca pas pregătitor pentru augmentarea B-LTA.

**Semnătura B-LTA** : longevitatea semnăturii este cea a semnăturii B-T sau B-LT menționate mai sus. Acesta este completată cu elemente de probă complete privind elementele preexistente ale obiectului de date semnat care sunt necesare pentru validarea semnăturii semnatarului, întreaga structură fiind acoperită de un marcaj de timp al documentului/arhivă. Acest lucru permite extinderea longevității semnăturii până la longevitatea certificatului de marcare temporală a acelui document/arhivă de timp marcată la momentul creării sale. Această extindere maximă a longevității semnăturii necesită, de asemenea, ca toate dovezile adăugate de dragul măririi să fie eligibile și să rămână în perioada dorită evaluabile ca fiind valabile la momentul creării documentului/marcajului de timp al arhivei, în timp ce o astfel de evaluare se bazează, de asemenea, pe disponibilitatea dovezilor de stare online adecvate. O longevitate extinsă a unei semnături B-LTA poate fi afectată atunci când un algoritm criptografic, care a fost implicat în crearea ștampilei de timp a documentului/arhivei, a devenit slab în timp.

O semnătură B-LTA poate fi extinsă în mod repetat prin adăugarea unei structuri B-LTA învăluitoare, ori de câte ori este necesar din cauza riscului de expirare a oricărui element de probă implicat sau, în mod excepțional, din cauza slăbiciunii premature a unui algoritm criptografic folosit de oricare dintre dovezile implicate. elemente care au fost adăugate de la extinderea B-LTA precedentă. Trebuie avut în vedere faptul că crearea unui nou tip de timp pentru document/arhivă protejează algoritmii criptografici ai tuturor structurilor acoperite să nu devină slabi, cu condiția ca algoritmii utilizați pentru crearea noului marcaj temporal să rămână rezistenți sau să fie acoperiți în alt mod de un alt marcaj temporal rezistent înainte de a deveni slabi..

O semnătură B-LTA poate fi extinsă în mod repetat ori de câte ori este necesar pentru a acoperi întreaga perioadă necesară de longevitate a semnăturii semnatarului inițial. Ca o alternativă la extinderea repetată a B-LTA, poate fi utilizat un serviciu centralizat de păstrare a semnăturii electronice pentru a asigura o perioadă echivalentă de longevitate.

În orice caz, algoritmii și parametrii criptografici sunt verificați în raport cu standardele criptografice aplicabile pentru a se asigura că rezistența semnăturii electronice poate fi

confirmată pentru un anumit artefact semnat în raport cu cea mai apropiată dovadă a existenței care poate fi detectată prin procesul de validare .
Pentru a preveni expirarea elementelor înainte de a ajunge la sfârșitul perioadei de valabilitate necesare, așa cum este definită de aplicația de afaceri, se recomandă insistent Clientului/APP-urilor să ia prevederi pentru creșterea în timp util a semnăturilor și a sigiliilor.
Independent de prevederile menționate mai sus, serviciul de validare certSIGN încearcă să obțină online date doveditoare după cum este necesar, în special atunci când elementele stocate lipsesc sau au expirat în obiectul de date semnat în momentul validării, în scopul determinării diagnosticului general al semnăturii.
Cu toate acestea, trebuie reținut că datele de probă online pot să nu fie potrivite pentru a face față situațiilor în care algoritmii criptografici pentru elementele cruciale ale unui obiect de date semnat nu mai sunt eligibili. În acele cazuri particulare, creșterea în timp util devine inevitabilă pentru a asigura o rezistență suficientă în ceea ce privește valabilitatea necesară pe termen lung a semnăturilor și a sigiliilor.

#### BSP (k): ARHIVARE

Prezenta politică nu impune cerințe specifice de arhivare pentru semnături. Longevitatea acestuia din urmă trebuie adaptată de Client/APP astfel încât să fie suficientă pentru cazul de utilizare considerat.
Dacă este necesar, arhivarea semnăturii trebuie luată în considerare de către Client/APP, care o poate delega semnatarului în ceea ce privește propria politică de semnătură sau termenii de utilizare. Serviciul de validare certSIGN poate lua în considerare doar dovezile care sunt furnizate într-o cerere de validare. În consecință, Clientul/APP trebuie să prevadă o longevitate adecvată a semnăturilor care urmează să fie validate în timp util, pentru a asigura rezistența și disponibilitatea acestuia la momentul validării.
Cu toate acestea, jurnalele de tranzacții ale serviciului de validare certSIGN sunt susținute pentru a oferi dovezi complementare referitoare la serviciul furnizat, arhivate timp de 10 (zece) ani și accesibile pentru utilizare în cadrul procedurilor judiciare.
Următoarele tipuri de dovezi pot fi dezvăluite de jurnalul de tranzacții certSIGN:

- Timpul de creare a înregistrărilor care este sincronizat cu o sursă de timp precisă de încredere
- Identificatorul unic al Clientului/APP-ului solicitant
- Întregul raport de validare cuprinzând informațiile tranzacționale relevante
- Dacă cererea a avut succes

### 4.3 BSP-uri legate în principal de actorii implicați în crearea / extinderea / validarea semnăturilor

#### BSP (l): IDENTITATEA (ȘI ROLILE/ATRIBUȚIILE) SEMNATARILOR

Serviciul de validare dezvăluie identitatea semnatarului, care poate fi luată în considerare de aplicația de business pentru luarea deciziilor de flux de lucru la propria discreție.
Prezenta politică de validare nu conține nicio cerință privind rolul semnatarului.

#### BSP (m): NIVEL DE ASIGURARE NECESAR PENTRU AUTENTIFICAREA SEMNATARULUI

Nivelul de asigurare semnatar este implicat prin efectuarea validării pe baza ancorelor de încredere publicate în listele de încredere ale UE.
Serviciul de validare certSIGN dezvăluie tipul legal al unei semnături, ceea ce asigură nivelul minim de asigurare corespunzător.

### BSP (n): DISPOZITIVE DE CREARE A SEMNĂTURII

La validarea cu succes a unei semnături, serviciul de validare certSIGN dezvăluie implicit, prin detectarea tipului legal al unei semnături, dacă un **Dispozitiv Calificat de Creare a Semnăturii** (QSCD) a fost utilizat de către semnatar. Aplicația de afaceri poate folosi aceste informații pentru a lua decizii privind fluxul de lucru la propria discreție.

## 4.4 Alte BSP-uri

### BSP (o): ALTE INFORMAȚII TREBUIE ASOCIATE CU SEMNATURA

Nicio cerință specifică

### BSP (p): SUITE CRYPTOGRAFICE

Dacă nu se specifică altfel în configurarea serviciului pentru Client/APP, suitele criptografice eligibile pentru validarea semnăturii sunt preluate din ETSI TS 119 312 – „Electronic Signatures and Infrastructures (ESI); Suite criptografice”. Totuși, raportul de validare a semnăturii nu va indica dacă algoritmul și lungimile cheilor erau încă de încredere în momentul utilizării.

### BSP (q): MEDIU TEHNOLOGIC

Nicio cerință specifică.

# 5 Anexa 2 –Politici calificate de validare - Parametrii de validare QSigSeal

Conform ETSI TS 119 172-1 Capitolul 4 Politicile de semnătură și documentul de politică de semnătură: *„ politica de semnătură va fi exprimată sub forma unui rezumat al declarației de politică de semnătură stabilit pe baza tabelului A.1 din anexa A ”*.

Numele și identificatorul autorității de politică de validare: **Comitetul de management al politicilor și procedurilor** (a se vedea capitolul 1.4.1 de mai sus)

## 5.1 Politica de validare implicită PAdES

Numele și identificatorul politicii de validare: **certSIGN QVal** – „certSIGN QVAL default policy” - OID: **1.3.6.1.4.1.25017.4.2.1.2**
Identificatorul validării(lor) în cauză în fluxul de lucru de validare în cauză: **Validarea semnăturii/sigiliului calificat**

| BSP | Titlul BSP | Rezumatul declarației de afaceri | Omologul declarației tehnice |
|---|---|---|---|
| **BSP(a)** | **Fluxul de lucru (secvențiere și sincronizare) al semnăturilor** | | |
| | Prezenta politică de validare abordează validarea semnăturilor electronice avansate și calificate, cuprinzând posibile marcaje temporale și extensii de date de probă privind o singură instanță sau mai multe instanțe de DTBS în timpul unei singure tranzacții, în timp ce un singur raport este returnat de către serviciu după o validare efectuată cu succes.<br>Serviciul de validare certSIGN poate fi utilizat de către un Client/APP pentru a implementa fluxuri de lucru de afaceri care cuprind tranzacții multiple; într-un astfel de caz, fiecare tranzacție în cadrul fluxului de lucru Client/APP va fi efectuată conform uneia dintre politicile prezente în funcție de modul de validare ales. Fluxul de lucru implicit este secvențial conform ETSI TS 119 102-1 V1.2.1. | Flux la momentul semnăturii = irelevant |
| | | | Semnături multiple = serie |
| | | | Sincronizează totul cu un moment fix = nu |
| | | | Sincronizare moment validare cu moment semnare = da |
| | | | Cu marca temporală = specific per nivel semnătură |
| | | | Nivel de încredere (LoA) = specific per nivel semnătură |
| **BSP(b)** | **Date care trebuie semnate (DTBS)** | | |
| | Clientul/APP este responsabil pentru conținutul și formatarea corectă a datelor care urmează să fie validate în conformitate cu standardele aplicabile. În special, trebuie să se asigure că datele de validat nu conțin coduri rău intenționate sau scripturi care ar putea altera datele de validat sau ar putea deteriora serviciile certSIGN.<br>În special, formatul unui SD poate fi doar PDF. Serviciul de validare certSIGN garantează confidențialitatea unui SD în conformitate cu legile aplicabile privind confidențialitatea și legile românești. certSIGN șterge în mod special și imediat toate copiile unui SD primit, dacă există, de pe serverele sale după ce a efectuat o tranzacție solicitată.<br>Serviciul de validare certSIGN aplică proceduri de scanare antivirus/malware înainte de a aplica procesul de validare a semnăturii. | Formatul și structura datelor = cf. ETSI EN 319 142-1 |
| | | | MimeType = application/pdf |
| | | | Obiecte structurate = nu |

| BSP | Titlul BSP | Rezumatul declarației de afaceri | Omologul declarației tehnice |
|---|---|---|---|
| **BSP(c)** | **Relația dintre datele semnate și semnătura (semnăturile)** | | |
| | Relația dintre datele semnate și semnătura (semnăturile) depinde în mod specific de profilul semnăturii. Profilurile/nivelurile de semnătură acceptate sunt:<br>1. B-B (semnătură de bază)<br>2. B-T (semnătură cu timp)<br>3. B-LT (semnătură cu material de validare pe termen lung)<br>4. B-LTA (Semnături care asigură disponibilitatea și integritatea pe termen lung a materialului de validare)<br>Raportul de validare va indica profilul/nivelul corespunzător pentru semnăturile examinate și marcajele de timp implicate în cazul în care acestea pot fi validate cu succes. | DTBSCardinality = 1 |
| | | | Validarea semnăturii multiple = integral – totul ok |
| | | | SigDTBSRelativePosition = EnvelopedSig |
| | | | SigLevels:<br>http://uri.etsi.org/ades/191x2/level/baseline/B-B<br>http://uri.etsi.org/ades/191x2/level/baseline/B-T<br>http://uri.etsi.org/ades/191x2/level/baseline/B-LT<br>http://uri.etsi.org/ades/191x2/level/baseline/B-LTA |
| | | | SigFormats: http://www.etsi.org/19142/v.1.1.1 |
| **BSP(d)** | **Comunitate vizată** | | |
| | Nu există o comunitate specifică vizată care să fie adresată in afara de cele menționate în secțiunea BSP (d). | | grup țintă specific = nu |
| | | | Excluderi = nu |
| **BSP(e)** | **Alocarea responsabilității pentru validarea și augmentarea semnăturii** | | |
| | Serviciul de validare certSIGN are responsabilitatea procesului de validare, validând semnăturile existente pe DTBS și nu este responsabil pentru augmentarea semnăturii. În cazul în care DTBS conține o semnătură nevalidă, informațiile respective sunt indicate în rezultatul furnizat de serviciu. certSIGN NU va anula procesul de validare din cauza unei semnături nevalide care este conținută în DTBS. | | |
| **BSP(f)** | **Tipul juridic al semnăturilor** | | |
| | In plus față de semnăturile electronice avansate, serviciul de validare certSIGN acceptă validarea pentru toate tipurile legale de semnături electronice calificate pentru persoane juridice (sigilii calificate) sau pentru persoane fizice (semnături calificate) care acționează în nume propriu sau în numele unei persoane juridice:<br>• Semnături electronice calificate acceptate de un certificat calificat X.509 v3;<br>Tipul legal al unei semnături este indicat în raportul de validare atunci când aceasta poate fi validată cu succes. | Nivel dispozitive SCD = SCD/QSCD |
| | | | Ancore de încredere = Liste de încredere UE (EUTL) |
| | | | Nivel de tip certificat = ESig/ESeal/QESig/QESeal |
| **BSP(g)** | **Angajamentul asumat de semnatar** | | |
| | Serviciul de validare certSIGN procesează orice tip de angajament găsit în cadrul semnăturii dacă acesta este în conformitate cu secțiunea 5.2.3 din ETSI EN 319 122-1.<br>Serviciul de validare certSIGN poate dezvălui tipul de angajament atunci când este asociat cu o | | Tipul de angajament -sintaxa = cf. ETSI EN 319 122-1. |

| BSP | Titlul BSP | Rezumatul declarației de afaceri | Omologul declarației tehnice |
|---|---|---|---|
| | anumită semnătură pentru a fi luată în considerare de aplicația de afaceri.<br>Serviciul de validare nu interpretează un tip de angajament care este asociat cu o semnătură. | | |
| **BSP(h)** | **Nivelul de asigurare a dovezilor de timp** | | |
| | Astfel cum se specifică în secțiunea BSP(h) din apendicele 1. Revendicat de semnatar pentru nivelul de bază, ștampilă temporală pentru nivelurile superioare. | | Dovezi de timp dovedesc = marca temporală TSP – conform RFC 3161 |
| | | | Nivelul marcajului de timp = Necalificat/Calificat |
| | | | SemnareaCertTrustConditions: EUTL |
| **BSP(i)** | **Formalitati de semnare** | | |
| | Serviciul de validare certSIGN aplică procedurile de validare documentului PDF furnizat ca intrare de către utilizator. Serviciul de validare certSIGN dezvăluie în raportul final de stare atributele de semnătură asociate. | | |
| **BSP(j)** | **Longevitatea și rezistența la schimbare** | | |
| | În conformitate cu nivelul de semnătură descris în secțiunea BSP(j) | | |
| **BSP(k)** | **De arhivă** | | |
| | Prezenta politică nu impune cerințe specifice de arhivare pentru semnături. Longevitatea acestuia din urmă trebuie adaptată de Client/APP astfel încât să fie suficientă pentru cazul de utilizare considerat. | | |
| **BSP(l)** | **Identitatea (și rolurile/atributele) semnatarilor** | | |
| | Serviciul de validare poate să identifice și să dezvăluie identitatea și tipul semnatarului folosind proprietățile certificatului acestuia. Prezenta politică de validare nu conține nicio cerință privind rolul semnatarului. | | |
| **BSP(m)** | **Nivelul de asigurare necesar pentru autentificarea semnatarului** | | |
| | Nivelul de asigurare semnatar este implicat prin efectuarea validării pe baza ancorelor de încredere publicate în listele de încredere EUTL<br>Serviciul de validare certSIGN va indica în raportul final de stare tipul de certificat al semnatarului (calificat sau necalificat) și lista informațiilor de revocare utilizate de serviciu pentru validarea certificatului. | | TrustAnchors = EU Trusted Lists |
| | | | ServiceTypes = qualified/not-qualified<br>ServiceStatuses = granted/ recognisedatnationallevel/ recognisedatnationallevel/ setbynationallaw<br>RevocationCheckingConstraints = eitherCheck |
| **BSP(n)** | **Dispozitive de creare a semnăturilor** | | |
| | La validarea cu succes a unei semnături, serviciul de validare certSIGN dezvăluie implicit, prin detectarea tipului legal al unei semnături, dacă un Dispozitiv Calificat de Creare a Semnăturii (QSCD) a fost utilizat de către semnatar. Aplicația de afaceri poate folosi aceste informații pentru a lua decizii privind fluxul de lucru la propria discreție. | | |
| **BSP(o)** | **Alte informații care trebuie asociate cu semnătura** | | |

| BSP | Titlul BSP | Rezumatul declarației de afaceri | Omologul declarației tehnice |
|---|---|---|---|
| | Nu sunt cerințe specifice. | | Localizare geografică = nu |
| | | | Ora semnării = marca temporală/ timpul solicitat de semnatar |
| **BSP(p)** | **Suite criptografice** | | |
| | Cu excepția cazului în care se specifică altfel în configurarea serviciului pentru Client/APP, suitele criptografice eligibile pentru validarea semnăturii sunt preluate din ETSI TS 119 312 – „Electronic Signatures and Infrastructures (ESI); Suite criptografice”. Totuși, raportul de validare a semnăturii nu va indica dacă algoritmul și lungimile cheilor erau încă de încredere în momentul utilizării. | | Suite criptografice = conform. ETSI TS 119 312 |
| **BSP(q)** | **Mediul tehnologic** | | |
| | Fără cerințe specifice | | Tip mediu = în Centrul de date |

„Politica_default” nu aplică alte constrângeri specifice.

## 5.2 Politica de validare CAdES

Numele și identificatorul politicii de validare: **certSIGN QVal CAdES** – „certSIGN QVAL CAdES policy" - OID: **1.3.6.1.4.1.25017.4.2.2.1**
Identificatorul validării(lor) în cauză în fluxul de lucru de validare în cauză: **Validarea semnăturii/sigiliului calificat**

| BSP | Titlul BSP | Rezumatul declarației de afaceri | Omologul declarației tehnice |
|---|---|---|---|
| **BSP(a)** | **Fluxul de lucru (secvențiere și sincronizare) al semnăturilor** | | |
| | Prezenta politică de validare abordează validarea semnăturilor electronice avansate și calificate, cuprinzând posibile marcaje temporale și extensii de date de probă privind o singură instanță sau mai multe instanțe de DTBS în timpul unei singure tranzacții, în timp ce un singur raport este returnat de către serviciu după o validare efectuată cu succes.<br>Serviciul de validare certSIGN poate fi utilizat de către un Client/APP pentru a implementa fluxuri de lucru de afaceri care cuprind tranzacții multiple; într-un astfel de caz, fiecare tranzacție în cadrul fluxului de lucru Client/APP va fi efectuată conform uneia dintre politicile prezente în funcție de modul de validare ales. Fluxul de lucru implicit este secvențial conform ETSI TS 119 102-1 V1.2.1. | Flux la momentul semnăturii = irelevant |
| | | | Semnături multiple = serie |
| | | | Sincronizează totul cu un moment fix = nu |
| | | | Sincronizare moment validare cu moment semnare = da |
| | | | Cu marca temporală = specific per nivel semnătură |
| | | | Nivel de încredere (LoA) = specific per nivel semnătură |
| **BSP(b)** | **Date care trebuie semnate (DTBS)** | | |
| | Clientul/APP este responsabil pentru conținutul și formatarea corectă a datelor care urmează să fie validate în conformitate cu standardele aplicabile. În special, trebuie să se asigure că datele de validat nu conțin coduri rău intenționate sau scripturi care ar putea altera datele de validat sau ar putea deteriora serviciile certSIGN.<br>Serviciul de validare certSIGN garantează confidențialitatea unui SD în conformitate cu legile aplicabile privind confidențialitatea și legile românești. certSIGN șterge în mod special și imediat toate copiile unui SD primit, dacă există, de pe serverele sale după ce a efectuat o tranzacție solicitată.<br>Serviciul de validare certSIGN aplică proceduri de scanare antivirus/malware înainte de a aplica procesul de validare a semnăturii. | Formatul și structura datelor = cf. ETSI EN 319 122-1 |
| | | | MimeType = application/pdf |
| | | | Obiecte structurate = nu |
| **BSP(c)** | **Relația dintre datele semnate și semnătura (semnăturile)** | | |
| | Relația dintre datele semnate și semnătura (semnăturile) depinde în mod specific de profilul semnăturii. Profilurile/nivelurile de semnătură acceptate sunt:<br>1. B-B (semnătură de bază)<br>2. B-T (semnătură cu timp)<br>3. B-LT (semnătură cu material de validare pe termen lung)<br>4. B-LTA (Semnături care asigură disponibilitatea și integritatea pe termen lung a materialului de validare)<br>Raportul de validare va indica profilul/nivelul corespunzător pentru semnăturile examinate și | DTBSCardinality = 1 |
| | | | Validarea semnăturii multiple = nu |
| | | | SigDTBSRelativePosition = EnvelopedSig |
| | | | SigLevels:<br>http://uri.etsi.org/ades/191x2/level/baseline/B-B<br>http://uri.etsi.org/ades/191x2/level/baseline/B-T<br>http://uri.etsi.org/ades/191x2/level/baseline/B-LT |

| BSP | Titlul BSP | Rezumatul declarației de afaceri | Omologul declarației tehnice |
|---|---|---|---|
| | marcajele de timp implicate în cazul în care acestea pot fi validate cu succes. | | http://uri.etsi.org/ades/191x2/level/baseline/B-LTA |
| | | | SigFormats: http://www.etsi.org/19122/v.1.1.1 |
| **BSP(d)** | **Comunitate vizată** | | |
| | Nu există o comunitate specifică vizată care să fie adresată in afara de cele menționate în secțiunea BSP (d). | | grup țintă specific = nu |
| | | | Excluderi = nu |
| **BSP(e)** | **Alocarea responsabilității pentru validarea și augmentarea semnăturii** | | |
| | Serviciul de validare certSIGN are responsabilitatea procesului de validare, validând semnăturile existente pe DTBS și nu este responsabil pentru augmentarea semnăturii. În cazul în care DTBS conține o semnătură nevalidă, informațiile respective sunt indicate în rezultatul furnizat de serviciu. certSIGN NU va anula procesul de validare din cauza unei semnături nevalide care este conținută în DTBS. | | |
| **BSP(f)** | **Tipul juridic al semnăturilor** | | |
| | In plus față de semnăturile electronice avansate, serviciul de validare certSIGN acceptă validarea pentru toate tipurile legale de semnături electronice calificate pentru persoane juridice (sigilii calificate) sau pentru persoane fizice (semnături calificate) care acționează în nume propriu sau în numele unei persoane juridice:<br>• Semnături electronice calificate acceptate de un certificat calificat X.509 v3;<br>Tipul legal al unei semnături este indicat în raportul de validare atunci când aceasta poate fi validată cu succes. | | Nivel dispozitive SCD = SCD/QSCD |
| | | | Ancore de încredere = Liste de încredere UE (EUTL) |
| | | | Nivel de tip certificat = ESig/ESeal/QESig/QESeal |
| **BSP(g)** | **Angajamentul asumat de semnatar** | | |
| | Serviciul de validare certSIGN procesează orice tip de angajament găsit în cadrul semnăturii dacă acesta este în conformitate cu secțiunea 5.2.3 din ETSI EN 319 122-1.<br>Serviciul de validare certSIGN poate dezvălui tipul de angajament atunci când este asociat cu o anumită semnătură pentru a fi luată în considerare de aplicația de afaceri.<br>Serviciul de validare nu interpretează un tip de angajament care este asociat cu o semnătură. | | Tipul de angajament -sintaxa = cf. ETSI EN 319 122-1. |
| **BSP(h)** | **Nivelul de asigurare a dovezilor de timp** | | |
| | Astfel cum se specifică în secțiunea BSP(h) din apendicele 1. Revendicat de semnatar pentru nivelul de bază, ștampilă temporală pentru nivelurile superioare. | | Dovezi de timp dovedesc = marca temporală TSP – conform RFC 3161 si indicarea timpului de semnare data de semnatar |
| | | | Nivelul marcajului de timp = Necalificat/Calificat |
| | | | SemnareaCertTrustConditions: EUTL |

| BSP | Titlul BSP | Rezumatul declarației de afaceri | Omologul declarației tehnice |
|---|---|---|---|
| **BSP(i)** | **Formalitati de semnare** | | |
| | Serviciul de validare certSIGN aplică procedurile de validare SD furnizat ca intrare de către utilizator. Serviciul de validare certSIGN dezvăluie în raportul final de stare atributele de semnătură asociate. | | |
| **BSP(j)** | **Longevitatea și rezistența la schimbare** | | |
| | În conformitate cu nivelul de semnătură descris în secțiunea BSP(j) | | |
| **BSP(k)** | **De arhivă** | | |
| | Prezenta politică nu impune cerințe specifice de arhivare pentru semnături. Longevitatea acestuia din urmă trebuie adaptată de Client/APP astfel încât să fie suficientă pentru cazul de utilizare considerat. | | |
| **BSP(l)** | **Identitatea (și rolurile/atributele) semnatarilor** | | |
| | Serviciul de validare poate să identifice și să dezvăluie identitatea și tipul semnatarului folosind proprietățile certificatului acestuia. Prezenta politică de validare nu conține nicio cerință privind rolul semnatarului. | | |
| **BSP(m)** | **Nivelul de asigurare necesar pentru autentificarea semnatarului** | | |
| | Nivelul de asigurare semnatar este implicat prin efectuarea validării pe baza ancorelor de încredere publicate în listele de încredere EUTL<br>Serviciul de validare certSIGN va indica în raportul final de stare tipul de certificat al semnatarului (calificat sau necalificat) și lista informațiilor de revocare utilizate de serviciu pentru validarea certificatului. | TrustAnchors = EU Trusted Lists |
| | | | ServiceTypes = qualified/not-qualified<br>ServiceStatuses = granted/ recognisedatnationallevel/ recognisedatnationallevel/ setbynationallaw<br>RevocationCheckingConstraints = eitherCheck |
| **BSP(n)** | **Dispozitive de creare a semnăturilor** | | |
| | La validarea cu succes a unei semnături, serviciul de validare certSIGN dezvăluie implicit, prin detectarea tipului legal al unei semnături, dacă un Dispozitiv Calificat de Creare a Semnăturii (QSCD) a fost utilizat de către semnatar. Aplicația de afaceri poate folosi aceste informații pentru a lua decizii privind fluxul de lucru la propria discreție. | | |
| **BSP(o)** | **Alte informații care trebuie asociate cu semnătura** | | |
| | Nu sunt cerințe specifice. | | Localizare geografică = nu |
| | | | Ora semnării = marca temporală/ timpul solicitat de semnatar |
| **BSP(p)** | **Suite criptografice** | | |
| | Cu excepția cazului în care se specifică altfel în configurarea serviciului pentru Client/APP, suitele criptografice eligibile pentru validarea semnăturii sunt preluate din ETSI TS 119 312 – „Electronic Signatures and Infrastructures (ESI); Suite criptografice”. Totuși, raportul de validare a | | Suite criptografice = conform. ETSI TS 119 312 |

| BSP | Titlul BSP | Rezumatul declarației de afaceri | Omologul declarației tehnice |
|---|---|---|---|
| | semnăturii nu va indica dacă algoritmul și lungimile cheilor erau încă de încredere în momentul utilizării. | | |
| **BSP(q)** | **Mediul tehnologic** | | |
| | Fără cerințe specifice | | Tip mediu = în Centrul de date |

„Politica CAdES" nu aplică alte constrângeri specifice.

# 6 Anexa 3 – Descriere testare

## 6.1 Introducere

Prezentul apendix descrie o serie de teste aplicate de Certsign SA (certSIGN) pentru a valida funcționalitatea furnizată de serviciul de validare a semnăturii calificate/semnăturii.
În total, există peste 500 de teste, atât pozitive, cât și negative, concepute pentru a acoperi o gamă cât mai largă de cazuri. certSIGN a participat, de asemenea, la evenimentul regulat ETSI Plugtests desfășurat la sfârșitul anului 2023. Astfel, a fost generată o mare varietate de teste cu ajutorul fișierelor generate de actori externi, respectiv alte companii TSP, prin care am validat interoperabilitatea serviciului de validare a semnăturii calificate/semnăturii în toate țările membre ale UE

## 6.2 Teste

În continuare este prezentată o listă rezumativă a principalelor teste utilizate pentru a demonstra implementarea corectă a serviciului de validare.

| Test name | Description | Expected Result | Achieved Result | Observations |
|---|---|---|---|---|
| 1_1_Adobe_B | B-B profile validation testing | TOTAL-PASSED | TOTAL-PASSED | |
| 1_2_Adobe_BT | B-T profile validation testing | TOTAL-PASSED | TOTAL-PASSED | |
| 1_3_1_Adobe_LT_Partial_ByteRange | Validation testing of a valid signature not covering the whole document | TOTAL-PASSED | TOTAL-PASSED | |
| 2_Adobe_OnlyTimestamp | Testing document signed only with a Document Timestamp. | TOTAL-PASSED | TOTAL-PASSED | |
| 4_1_FlowSign_LT | B-LT profile validation testing | TOTAL-PASSED | TOTAL-PASSED | |
| 4_2_FlowSign_LTA | B-LTA profile validation testing | TOTAL-PASSED | TOTAL-PASSED | |

| Test name | Description | Expected Result | Achieved Result | Observations |
|---|---|---|---|---|
| 5_1_FlowSign_LT_LT | Validation testing of signed document with two valid LT level signatures | TOTAL-PASSED | TOTAL-PASSED | |
| 11_OneSignature_OneEmptyField | Validation testing of a signed document containing one signature and one blank signature field | TOTAL-PASSED | TOTAL-PASSED | |
| 7_6_Adobe_LTA_LTA | Validation testing of a signed document with two valid LTA-level signatures | TOTAL-PASSED | TOTAL-PASSED | |
| 8_1_Adobe_BT_B | Validation testing of a document with two signatures, the first of which is of level B-T and the second of level B-B. | TOTAL-PASSED | TOTAL-PASSED | |
| 2_Unsigned | Document validation test without signature. | TOTAL-FAILED FORMAT_FAILURE | TOTAL-FAILED FORMAT_FAILURE | |
| 3_SelfSigned | Validation testing signed document with self-signed certificate that is not trusted. | INDETERMINATE NO_CERTIFICATE_CHAIN_FOUND | INDETERMINATE NO_CERTIFICATE_CHAIN_FOUND | |
| MissingAttrs_3 | Validation testing signed document with B-B level signature whose certificate was valid for 1 year. In addition, the 'signing-certificate' attribute is missing. | INDETERMINATE NO_POE | INDETERMINATE NO_POE | |
| MissingAttrs_7 | Validation test signed document whose signature is missing the 'message-digest' and 'signed-certificate' attributes. | INDETERMINATE SIG_CONSTRAINTS_FAILURE | INDETERMINATE SIG_CONSTRAINTS_FAILURE | |