CERT DIGITAL – QPS
(SERVICIU DE CONSERVARE CALIFICAT)

POLITICA SERVICIULUI DE CONSERVARE PRACTICI ȘI DECLARAȚII (PSPPS)

VERSIUNEA 1.0 / 27.08.2025

[LIMBA: ROMÂNĂ]

Istoric versiuni

Data	Revizuire	Autor	Rezumat
27.08.2025	1.0	Adelin Cusman	Versiunea inițială a CERT DIGITAL QPS PSPPS

Creat de	Aprobat de

Orice întrebare sau solicitare de informații referitoare la conținutul acestui document trebuie adresată către office@certdigital.ro .

Cuprins

1. Introducere

1.1 Titlul documentului

CERT DIGITAL QPS – Politica și declarația privind practicile de conservare (PSPPS)

1.2 Versiunea çi controlul documentului

- **Versiune:** 1.0
- **Data:** 27.08.2025
- **Organizație autoare:** Centrul de Calcul S.A.
- **Stare (***proiect/aprobat***):** Proiect
- **Controlul documentului:** Acest document este supus controlului versiunilor. Toate reviziile sunt înregistrate în Istoricul versiunilor .

1.3 Scopul documentului

Scopul prezentei Politici și declarații privind serviciile de conservare (denumită în continuare *PSPPS*) este de a defini politicile și practicile aplicate de **CERT DIGITAL QPS** în furnizarea unui **serviciu de conservare calificat** pentru semnături electronice și sigilii electronice, în conformitate cu:

- **Regulamentul (UE) nr. 910/2014 (eIDAS)** și
- **Standardele ETSI** aplicabile, inclusiv, dar fără a se limita la ETSI EN 319 401, ETSI TS 119 511, ETSI TS 119 512, ETSI TS 119 312, ETSI EN 319 421/422, ETSI TS 119 441/442 și ETSI EN 319 102-1.

Acest document comunică autorităților de reglementare, auditorilor, abonaților, părților interesate și altor părți interesate cadrul în care CERT DIGITAL QPS își desfășoară serviciul de conservare, inclusiv:

- Obiectivele și domeniul de aplicare al serviciului;
- Rolurile și responsabilitățile participanților;
- Procesele de conservare și politicile privind probele;
- Obligațiile legale și de conformitate aplicabile.

1.4 Domeniul de aplicare al serviciului

Serviciul de conservare **CERT DIGITAL QPS** este conceput pentru a asigura **valabilitatea pe termen lung și valoarea probatorie** a:

- **Semnăturile electronice calificate (QES)**;
- **Sigiliilor electronice calificate (QSealS)**.

Serviciul oferă mecanisme de conservare a:

- Semnăturile și sigiliile digitale, inclusiv datele de validare asociate acestora (PDS – Conservarea semnăturilor digitale);
- Dovada existenței datelor digitale arbitrare (PGD – Dovada existenței datelor), acolo unde este cazul.

Serviciul acceptă unul sau mai multe **modele de stocare pentru păstrare,** astfel cum sunt definite în ETSI TS 119 511:

- **Cu stocare (WST);**
- **Cu stocare temporară (WTS);**
- **Fără stocare (WOS).**

1.5 Public

Acest document este destinat:

- **Auditorilor și organismelor de supraveghere** care evaluează conformitatea CERT DIGITAL QPS cu standardele eIDAS și ETSI;
- **Abonaților** (entități care utilizează serviciile de conservare CERT DIGITAL QPS);
- **Părțile** care se bazează pe dovezile păstrate emise de serviciu;
- **Personalul intern** al CERT DIGITAL QPS, pentru a asigura alinierea la practicile și politicile documentate.

1.6 Cadrul de politici

CERT DIGITAL QPS PSPPS este structurat în conformitate cu ETSI TS 119 511 §4.3 și ETSI EN 319 401. Acesta stabilește:

- **Politicile** care reglementează activitățile de conservare (algoritmi criptografici, marcarea temporală, reînnoirea probelor);

- **Practicile** aplicate în operațiunile de serviciu, inclusiv securitatea, generarea, stocarea, reînnoirea și recuperarea probelor.

Acest PSPPS este un **document disponibil public**, asigurând transparența și încrederea pentru toate părțile care interacționează cu serviciul de conservare.

Toate documentele publice legate de CERT DIGITAL QPS, inclusiv acest PSPPS, sunt publicate și puse la dispoziție la: **https://certdigital.ro/repository**.

1.7 Referințe

Acest PSPPS face referire la următoarele documente normative:

- Regulamentul (UE) nr. 910/2014 (eIDAS)
- ETSI EN 319 401 – Cerințe generale de politică pentru furnizorii de servicii de încredere
- ETSI TS 119 511 – Cerințe de politică și securitate pentru furnizorii de servicii de încredere care furnizează servicii de conservare
- ETSI TS 119 512 – Protocoale pentru furnizorii de servicii de încredere care furnizează servicii de conservare
- ETSI EN 319 421 – Cerințe de politică și securitate pentru furnizorii de servicii de încredere care emit marcaje temporale
- ETSI EN 319 422 – Protocol și profiluri de marcaj temporal
- ETSI TS 119 312 – Suite criptografice
- ETSI TS 119 441 – Cerințe de politică și securitate pentru furnizorii de servicii de încredere care oferă servicii de validare a semnăturilor
- ETSI TS 119 442 – Protocoale pentru furnizorii de servicii de încredere care oferă servicii de validare a semnăturilor
- ETSI EN 319 102-1 – Semnături electronice și infrastructuri (validare AdES)

1.8 Identificatori de obiecte (OID)

CERT DIGITAL QPS a stabilit un **arc OID** dedicat sub numărul său de întreprindere (1.3.6.1.4.1.47898) pentru serviciul de conservare calificat.

Următoarele OID-uri sunt rezervate și atribuite:

1.8.1 OID-uri de bază CERT DIGITAL QPS

OID	Descriere
1.3.6.1.4.1.47898.10	CERTDIGITAL Serviciu de conservare calificat (id-qps)
1.3.6.1.4.1.47898.10.1	CERTDIGITAL QPS Politica și declarația privind practicile serviciului de conservare (PSPPS)

1.8.2 Profiluri de conservare CERT DIGITAL QPS

OID	Descriere
1.3.6.1.4.1.47898.10.1.1	CERTDIGITAL QPS – Profil de conservare WOS
1.3.6.1.4.1.47898.10.1.2	CERTDIGITAL QPS – Profil de conservare WST
1.3.6.1.4.1.47898.10.1.3	CERTDIGITAL QPS – Profil de conservare WTS

1.8.3 Politici extinse CERT DIGITAL QPS (rezervate pentru utilizare viitoare)

OID	Descriere
1.3.6.1.4.1.47898.10.2	Politica de validare CERTDIGITAL QPS
1.3.6.1.4.1.47898.10.2.1	Politica de validare implicită CERTDIGITAL QPS (norme de bază ale UE)
1.3.6.1.4.1.47898.10.3	Politica criptografică CERTDIGITAL QPS
1.3.6.1.4.1.47898.10.4	Politica privind formatul probelor CERTDIGITAL QPS
1.3.6.1.4.1.47898.10.5	CERTDIGITAL QPS Profilul politicii API

Fiecare OID este utilizat pentru a identifica în mod unic **politicile, profilurile și configurațiile serviciilor**. Acești identificatori pot apărea în:

- Politici și contracte de servicii;
- Obiecte de conservare și containere de dovezi;
- Politici și rapoarte de validare;
- Intrări din lista de încredere.

1.9 Definiții çi acronime

În sensul prezentului document, se aplică definițiile din **Regulamentul eIDAS** și **standardele ETSI**. Definiții și acronime suplimentare sunt incluse în anexa A (Glosar).

2. Principii generale

2.1 Obiectivele serviciului de conservare

Obiectivul principal al **CERT DIGITAL QPS** este de a furniza un **serviciu de conservare calificat** care să asigure **valabilitatea, integritatea și valoarea probatorie pe termen lung** a:

- **semnăturilor electronice calificate (QES)**;
- **Sigiliilor electronice calificate (QSealS)**.

Serviciul este conceput pentru a:

- Păstreze valoarea juridică a semnăturilor și sigiliilor dincolo de durata de viață criptografică naturală a algoritmilor utilizați inițial;
- Permită părților interesate să verifice autenticitatea și validitatea semnăturilor și sigiliilor păstrate în orice moment în viitor;
- Furnizarea de **dovezi de păstrare** fiabile, verificabile independent, care pot fi utilizate în proceduri juridice sau administrative.

Serviciul este operat în deplină conformitate cu **Regulamentul (UE) 910/2014 (eIDAS)**, **standardele ETSI** relevante și cele mai bune practici recunoscute pentru conservarea digitală pe termen lung.

2.2 Domeniul de aplicare al serviciului

CERT DIGITAL QPS oferă servicii de conservare în următoarele domenii:

- **Păstrarea semnăturilor digitale (PDS):**
  Asigurarea faptului că semnăturile și sigiliile electronice, împreună cu datele de validare asociate acestora, rămân valabile și verificabile pe perioade îndelungate.
    - OID-uri de profil:

- Model WOS → **1.3.6.1.4.1.47898.10.1.1**
- Model WST → **1.3.6.1.4.1.47898.10.1.2**
- Model WTS → **1.3.6.1.4.1.47898.10.1.3**

- **Dovada existenței datelor (PGD) [opțional]:**
  Furnizarea unei dovezi criptografice că anumite date digitale au existat la un moment dat, fără a valida sau păstra neapărat semnăturile.
  - Un OID dedicat poate fi rezervat în conformitate cu **1.3.6.1.4.1.47898.10.6** dacă PGD este inclus în mod oficial în domeniul de aplicare.

[Notă: Dacă PGD nu face parte din domeniul de aplicare al serviciului, această subsecțiune va fi marcată cu „Nu se aplică” în versiunea finală aprobată.]

2.3 Modele de stocare pentru conservare

Serviciul acceptă unul sau mai multe modele de stocare, astfel cum sunt definite în **ETSI TS 119 511**, fiecare fiind identificat în mod unic printr-un **OID** înregistrat.

- **Cu stocare (WST):**
  - **OID:** 1.3.6.1.4.1.47898.10.1.2
  - Descriere: Obiectul de conservare (inclusiv semnăturile, datele de validare și dovezile) este stocat de CERT DIGITAL QPS pe întreaga durată a perioadei de păstrare definite în politica de servicii.
  - Avantaj: Simplifică verificarea de către părțile care se bazează pe acesta.
  - Responsabilitate: CERT DIGITAL QPS asigură stocarea sigură pe termen lung și reînnoirea probelor.
- **Cu stocare temporară (WTS):**
  - **OID:** 1.3.6.1.4.1.47898.10.1.3
  - Descriere: Obiectul de conservare este stocat de CERT DIGITAL QPS doar temporar, suficient pentru a finaliza procesarea conservării și pentru a permite abonaților să recupereze rezultatele. După această perioadă, obiectul de conservare este șters în mod securizat, dar dovezile de conservare pot fi păstrate.
- **Fără stocare (WOS):**

- **OID:** 1.3.6.1.4.1.47898.10.1.1
- Descriere: CERT DIGITAL QPS nu stochează obiectul de conservare. În schimb, dovezile de conservare sunt returnate imediat abonatului, care își asumă responsabilitatea pentru stocarea pe termen lung atât a datelor originale, cât și a dovezilor.

2.4 Asigurarea serviciului çi conformitatea

CERT DIGITAL QPS afirmă conformitatea cu următoarele:

- **Cadru de reglementare:**
  - Regulamentul (UE) nr. 910/2014 (eIDAS).
- **Standarde aplicabile:**
  - ETSI TS 119 511 – Cerințe de politică și securitate pentru serviciile de conservare.
  - ETSI TS 119 512 – Protocoale pentru servicii de conservare.
  - ETSI EN 319 401 – Cerințe generale de politică pentru furnizorii de servicii de încredere.
  - ETSI TS 119 312 – Suite criptografice.
  - ETSI EN 319 421/422 – Cerințe și protocoale pentru marcarea temporală.
  - ETSI TS 119 441/442 – Cerințe și protocoale pentru serviciile de validare.
- **Publicarea listei de încredere:**
  Serviciul va fi inclus în lista națională de încredere sub identificatorul tipului de serviciu:
  - **http://uri.etsi.org/TrstSvc/Svctype/PSES/Q** (Serviciu de conservare calificat).
    Cu calificative care indică domeniul de aplicare acceptat:
  - **ForSignatures**
  - **ForSeals**
- **Referință OID politică:**
  Toate operațiunile de conservare sunt executate în conformitate cu **CERT DIGITAL QPS PSPPS OID: 1.3.6.1.4.1.47898.10.1**, care face referire la acest document.

2.5 Transparență çi accesibilitate

Declarația privind politica și practicile serviciului de conservare (PSPPS) este un **document public**. Acesta este pus la dispoziția:

- Abonaților înainte de a încheia o relație contractuală cu CERT DIGITAL QPS;
- Părților interesate care doresc să verifice dovezile produse de CERT DIGITAL QPS;
- Auditorilor și organismelor de supraveghere pentru evaluări de conformitate.

OID-urile asociate sunt publicate în acest document și pot fi incluse și în:

- Obiecte de conservare și înregistrări ale dovezilor;
- Rapoarte de validare;
- Documentație accesibilă publicului (de exemplu, site-ul web al serviciului).

PSPPS și politicile de servicii de conservare conexe sunt disponibile pentru descărcare publică la adresa **https://certdigital.ro/repository**.

2.6 Limitări

Serviciul de conservare nu garantează validitatea semnăturilor sau ștampilelor care erau **invalide la momentul introducerii**. Conservarea se aplică numai:

- Semnăturile și ștampilele care erau valabile la momentul trimiterii inițiale către serviciu;
- Datele trimise în conformitate cu formatele tehnice și politicile criptografice definite în capitolul 11 (Specificații tehnice).

Serviciul nu se extinde dincolo de conservarea semnăturilor digitale, a sigiliilor și a dovezilor conexe. Serviciile suplimentare, cum ar fi arhivarea electronică a conținutului, serviciile de autoritate de certificare sau verificarea identității, nu intră în sfera de aplicare a CERT DIGITAL QPS.

3. Prezentare generală a serviciului

3.1 Descrierea serviciului

CERT DIGITAL QPS oferă un **serviciu de conservare calificat (QPS)** pentru semnături electronice și sigilii electronice, asigurând **valabilitatea, integritatea și valoarea probatorie pe termen lung** a acestora**,** în conformitate cu **Regulamentul (UE) nr. 910/2014 (eIDAS)** și **ETSI TS 119 511/512**.

Serviciul realizează acest lucru prin:

- Primirea obiectelor de conservare de la abonați;
- Validarea semnăturilor digitale și a sigiliilor în momentul preluării;
- Colectarea tuturor datelor de validare asociate (certificate, OCSP, CRL);
- Generarea **dovezilor de conservare** utilizând formate aprobate (ERS / AdES-LTA);
- Reînnoirea dovezilor de conservare înainte ca algoritmii criptografici să devină obsolet;
- Furnizarea de stocare sigură (WST / WTS) sau livrare imediată (WOS) a obiectelor de conservare;
- Facilitarea recuperării și verificării independente a dovezilor de către părțile interesate.

Toate operațiunile de conservare sunt efectuate în conformitate cu **CERT DIGITAL QPS PSPPS OID: 1.3.6.1.4.1.47898.10.1**.

3.2 Fluxuri de lucru ale serviciului

3.2.1 Flux de lucru de ingestie

1. **Trimitere:** Abonatul trimite o semnătură/sigiliu digital și, dacă este cazul, datele semnate sau rezumatele aprobate.
2. **Validare:** Serviciul validează semnătura/sigiliul în conformitate cu ETSI EN 319 102-1 și **CERT DIGITAL Default Validation Policy OID: 1.3.6.1.4.1.47898.10.2.1**.
3. **Colectarea datelor de validare:** Se colectează lanțurile de certificate, CRL-urile și/sau răspunsurile OCSP.
4. **Crearea probelor:**
    - Pentru profilurile ERS: probele sunt create utilizând **RFC 4998/6283** și sunt marcate cu data și ora (EN 319 422).

- Pentru profilurile AdES-LTA: marcajele temporale de arhivare sunt încorporate în containerul de semnături.

5. **Returnare/stocare:** În funcție de modelul de stocare selectat (WOS, WST, WTS), obiectul de conservare este returnat, stocat sau stocat temporar.

3.2.2 Fluxul de lucru pentru reînnoire

1. **Monitorizare:** CERT DIGITAL QPS monitorizează continuu durata de viață a algoritmilor în conformitate cu ETSI TS 119 312.
2. **Declanșator:** reînnoirea este inițiată atunci când o primitivă criptografică se apropie de data de expirare a securității.
3. **Acțiune de reînnoire:** Se generează noi dovezi cu algoritmi mai puternici și timestamp-uri actualizate.
4. **Actualizare:** Reînnoirile sunt adăugate la containerul obiectului de conservare (POC) și înregistrate.

3.2.3 Fluxul de lucru pentru recuperare

- **Solicitare:** Un abonat sau o parte de încredere emite o solicitare RetrievePO sau ValidateEvidence.
- **Prelucrare:** CERT DIGITAL QPS recuperează obiectul de conservare sau validează dovada.
- **Livrare:** Se returnează un container complet de obiecte de conservare (POC), cu rapoarte de validare și referințe la profilul OID aplicabil.

3.2.4 Fluxul de lucru pentru ștergere (dacă este cazul)

- Modele WST/WTS: Obiectele sunt șterse în siguranță după perioadele de păstrare contractuale.
- Evenimentele de ștergere sunt înregistrate și asociate cu profilul OID relevant.

3.3 Profiluri de conservare acceptate

CERT DIGITAL QPS acceptă următoarele profiluri de conservare, fiecare identificat printr-un **OID** dedicat:

- **Profil de conservare WOS – OID: 1.3.6.1.4.1.47898.10.1.1**
  - Descrierea profilului: Conservare fără stocare.

- Serviciul returnează imediat dovezile abonatului.
- Potrivit atunci când abonatul este responsabil pentru stocarea datelor și a dovezilor.

- **Profil de conservare WST – OID: 1.3.6.1.4.1.47898.10.1.2**
  - Descrierea profilului: Conservare cu stocare.
  - CERT DIGITAL QPS stochează obiectele de conservare și dovezile pentru perioada de păstrare convenită.
- **Profil de conservare WTS – OID: 1.3.6.1.4.1.47898.10.1.3**
  - Descrierea profilului: Conservare cu stocare temporară.
  - CERT DIGITAL QPS stochează obiectele de conservare numai până la finalizarea procesării și până când abonatul recuperează rezultatele.
- **Referință politică de validare – OID: 1.3.6.1.4.1.47898.10.2.1**
  - Politica de validare implicită aplicată tuturor semnăturilor/sigiliilor înainte de conservare.
- **Referință politică criptografică – OID: 1.3.6.1.4.1.47898.10.3**
  - Definește algoritmii aprobați, lungimile cheilor și regulile de reînnoire, în conformitate cu ETSI TS 119 312.

3.4 Formate çi standarde acceptate

Formate de semnături/sigilii:

- CAdES (CMS Advanced Electronic Signatures) – ETSI EN 319 122-1
- XAdES (semnături electronice avansate XML) – ETSI EN 319 132-1
- PAdES (semnături electronice avansate PDF) – ETSI EN 319 142-1
- ASiC (Containere de semnături asociate) – ETSI EN 319 162-1

Dovezi de conservare:

- RFC 4998 Sintaxa înregistrării dovezilor (ERS)
- RFC 6283 XMLERS (Sintaxa înregistrării dovezilor XML)

- Augmentare AdES-LTA (ETSI EN 319 122-1, 319 132-1, 319 142-1)

Protocoale:

- Legături de protocol de conservare conform ETSI TS 119 512 (SOAP/XML și REST/JSON).

3.5 Limitări ale serviciului

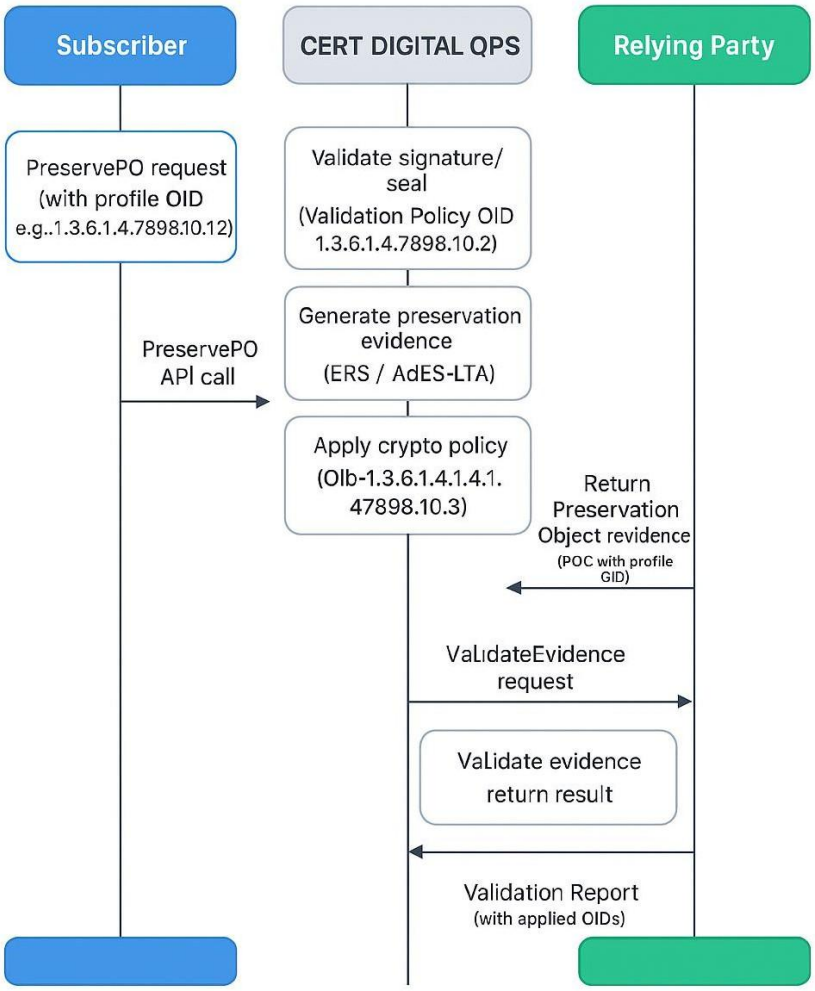
- Numai semnăturile/sigiliile **valabile la momentul introducerii** pot fi conservate.
- Obiectele de conservare trebuie să respecte **formatele acceptate** și **politica de criptare OID: 1.3.6.1.4.1.47898.10.3**.
- Dimensiunea datelor poate fi limitată în funcție de constrângerile tehnice (specificate în capitolul 11).
- Reînnoirea este legată de pragurile politicii de criptare (OID 1.3.6.1.4.1.47898.10.3).

3.6 Interfețe de serviciu

CERT DIGITAL QPS expune următoarele interfețe (conform ETSI TS 119 512):

- PreservePO → Trimite obiect de conservare (face referire la profilul aplicat OID).
- RetrievePO / RetrievePOC → Recuperare obiecte stocate (include OID-ul modelului de stocare).
- UpdatePOC → Reînnoire dovezi (cu referire la OID politica de criptare).
- ValidateEvidence → Validarea dovezilor și returnarea rezultatelor cu OID-ul politicii de validare aplicate.
- DeletePO → Ștergere sigură (acolo unde este cazul).
- RetrieveInfo → Recuperare metadate, inclusiv OID-uri acceptate.
- RetrieveTrace → Recuperarea jurnalelor, cu referințe OID pentru trasabilitatea ciclului de viață.

3.7 Diagrama fluxului de lucru la nivel înalt



4. Mediul de servicii

4.1 Prezentare generală

Serviciul de conservare **CERT DIGITAL QPS** funcționează într-un **mediu sigur, redundant și controlat,** conceput pentru a asigura:

- Disponibilitatea continuă a serviciului de conservare;
- Protecția materialelor criptografice sensibile;
- Integritatea și confidențialitatea datelor abonaților;
- Conformitatea cu **politica criptografică OID: 1.3.6.1.4.1.47898.10.3**;
- Alinierea la **ETSI EN 319 401**, **TS 119 511** și reglementările aplicabile în materie de protecție a datelor (de exemplu, GDPR).

4.2 Controale de securitate fizică

- **Centre de date:**
  - Operate în facilități de nivel III+ sau echivalente din UE.
  - Sisteme redundante de alimentare cu energie, răcire și stingere a incendiilor.
  - Acces fizic restricționat la personalul autorizat, aplicat prin autentificare multifactorială (ecuson + date biometrice).
- **Controlul accesului:**
  - Toate accesele fizice sunt înregistrate și monitorizate prin CCTV.
  - Control dublu necesar pentru intrarea în încăperile critice (de exemplu, seifurile HSM).
  - Vizitatorii și contractorii sunt supuși unor politici stricte de escortă.
- **Monitorizarea mediului:**
  - Monitorizarea continuă a temperaturii, umidității și riscurilor de incendiu.
  - Alerte automate și proceduri de incident în caz de abateri.

4.3 Securitatea logică çi a rețelei

- **Segmentarea rețelei:**

- Separarea rețelelor interne de servicii de încredere de zonele cu acces public (DMZ).
- VLAN-uri dedicate de gestionare, inaccesibile de pe Internet.

- **Firewall-uri și IDS/IPS:**
  - Firewall-uri multi-strat la perimetru și nucleu.
  - Sisteme de detectare și prevenire a intruziunilor care monitorizează toate intrările/ieșirile.
- **Comunicații sigure:**
  - Toate interacțiunile externe (de exemplu, PreservePO, ValidateEvidence) prin TLS 1.2+ cu suite de criptare puternice (aliniate la politica de criptare OID: 1.3.6.1.4.1.47898.10.3).
  - Autentificare reciprocă pentru conexiunile abonaților și părților de încredere, acolo unde este cazul.
- **Consolidarea sistemului:**
  - Servere consolidate în conformitate cu standardele CIS/NIST.
  - Patch-uri de securitate aplicate în conformitate cu politica de gestionare a vulnerabilităților.
  - Sisteme critice protejate de SELinux/AppArmor și monitorizarea integrității.

4.4 Mediul modulului criptografic

- **Module de securitate hardware (HSM):**
  - Toate cheile private utilizate de CERT DIGITAL QPS (de exemplu, pentru semnarea dovezilor de conservare, emiterea de declarații de serviciu) sunt stocate în **HSM-uri certificate FIPS 140-2 Nivel 3 sau Common Criteria EAL4**+.
  - Operațiuni HSM legate de **politica de criptare OID: 1.3.6.1.4.1.47898.10.3**.
- **Gestionarea cheilor:**
  - Control dublu necesar pentru activarea cheilor de semnare.
  - Ceremonii de chei efectuate în conformitate cu proceduri documentate.

- Cheile sunt supuse gestionării ciclului de viață (generare, utilizare, reînnoire, distrugere).

- **Sincronizarea timpului:**
  - Toate operațiunile criptografice sunt sincronizate cu surse de timp UTC sigure și redundante.
  - Marcajele temporale utilizate în dovezile de conservare sunt obținute de la o **autoritate calificată de marcare temporală (QTSA)** conformă cu **EN 319 421/422**.

4.5 Redundanța çi continuitatea serviciului

- **Redundanță:**
  - Toate componentele critice (servere de aplicații, HSM-uri, baze de date) sunt implementate în clustere de înaltă disponibilitate.
  - Echilibrarea sarcinii asigură continuitatea serviciului în timpul întreținerii sau în cazul defectării unui nod.
- **Backup și recuperare:**
  - Backupuri criptate zilnice ale obiectelor și dovezilor de conservare (profiluri WST/WTS).
  - Replicare off-site cu facilități separate geografic.
  - Plan de recuperare în caz de dezastru testat, care asigură un obiectiv de punct de recuperare (RPO) ≤ 24 ore și un obiectiv de timp de recuperare (RTO) ≤ 4 ore.
- **Continuitatea activității:**
  - Plan documentat de continuitate a activității (BCP) și plan de recuperare în caz de dezastru (DRP).
  - Testări periodice de failover și exerciții de răspuns la incidente.

4.6 Monitorizare çi înregistrare

- **Monitorizarea serviciilor:**
  - Monitorizarea continuă a disponibilității, performanței și latenței API-urilor (PreservePO, RetrievePO, ValidateEvidence).

- Alerte generate în cazul anomaliilor și defecțiunilor.

- **Jurnalizare de securitate:**
  - Înregistrarea detaliată a accesului, apelurilor API, generării de dovezi și acțiunilor de reînnoire.
  - Jurnalele sunt protejate împotriva modificărilor și păstrate timp de cel puțin 10 ani.
- **Trasabilitate:**
  - API-ul RetrieveTrace permite abonaților și auditorilor să obțină informații de trasabilitate pe durata ciclului de viață, inclusiv OID-urile profilurilor și politicilor aplicate.

4.7 Controale ale personalului çi organizaționale

- **Roluri de încredere:**
  - Roluri definite pentru administratorii de sistem, ofițerii de securitate și personalul operațional.
  - Separarea sarcinilor pentru a preveni conflictele de interese.
- **Verificări ale antecedentelor:**
  - Tot personalul de încredere este supus unei verificări înainte de angajare și unei revalidări periodice.
- **Instruire:**
  - Formare anuală în materie de securitate și conformitate cu cerințele ETSI/eIDAS, răspunsul la incidente și gestionarea sigură a cheilor.
- **Politici de acces:**
  - Se aplică principiul privilegiului minim.
  - Controlul accesului bazat pe roluri implementat în toate sistemele.

5. Politica de servicii

5.1 Politica privind dovezile de conservare

Serviciul de păstrare **CERT DIGITAL QPS** asigură că toate dovezile de păstrare generate sunt:

- **Complete:** conțin toate datele necesare pentru a dovedi validitatea la momentul conservării (semnături, certificate, date de revocare, marcaje temporale).
- **Verificabile:** verificabile în mod independent de către părțile interesate, utilizând instrumente și politici standard.
- **Imutabile:** odată generate, dovezile sunt legate criptografic pentru a împiedica modificarea.
- **Urmăribile:** dovezile includ referințe la profilul specific de conservare OID aplicat (de exemplu, WOS/WST/WTS).

Dovezile de conservare pot fi implementate într-una dintre următoarele forme:

- **Sintaxa înregistrării dovezilor (ERS)** – **RFC 4998/6283**, utilizând arbori hash ancorați cu timbre temporale.
- **Augmentare AdES-LTA** – Adăugarea de timbre temporale de arhivare și date de validare în semnăturile electronice avansate (PAdES-LTA, XAdES-A, CAdES-A).

Alegerea formatului dovezilor este reglementată de **Politica privind formatul dovezilor OID: 1.3.6.1.4.1.47898.10.4**.

5.2 Politica privind probele temporale

- **Marcare temporală:**
  - Toate probele de conservare includ **timbre temporale de încredere** conforme cu profilurile **RFC 3161** și ETSI EN 319 422.
  - Ștampilele temporale sunt obținute de la o **autoritate calificată de ștampilare temporală (QTSA)** în conformitate cu **EN 319 421**.
- **Asigurare:**
  - Serviciul garantează că fiecare lanț de dovezi include cel puțin o marcă temporală de la o QTSA.

- Marcajele temporale sunt reînnoite periodic pentru a menține puterea criptografică pe termen lung.

- **Referință politică:**
  - Politica privind probele temporale este definită în **PSPPS OID: 1.3.6.1.4.1.47898.10.1** și menționată în continuare în **Politica privind formatul probelor OID: 1.3.6.1.4.1.47898.10.4**.

5.3 Politica criptografică

CERT DIGITAL QPS aplică o politică criptografică strictă, aliniată la **ETSI TS 119 312 (Suite criptografice)**.

- **Identificator de politică: OID: 1.3.6.1.4.1.47898.10.3**
- **Funcții hash acceptate:**
  - SHA-256 (minim) – implicit în prezent
  - SHA-384, SHA-512 – acceptate pentru utilizare cu grad ridicat de siguranță
- **Algoritmi de semnătură acceptați:**
  - RSA ≥ 3072 biți
  - ECDSA cu curbe P-256, P-384, P-521
  - EdDSA (Ed25519, Ed448) acolo unde este acceptat
- **Algoritmi de semnătură cu marcaj temporal:**
  - La fel ca mai sus, limitat la algoritmii acceptați de QTSA selectat.
- **Praguri de reînnoire criptografică:**
  - Algoritmi hash reînnoiți cu cel puțin 5 ani înainte de data cunoscută a coliziunii/slăbiciunii.
  - Algoritmi de semnătură reînnoiți cu cel puțin 3 ani înainte de sfârșitul duratei de viață recomandate.

Toate operațiunile criptografice din cadrul serviciului (inclusiv semnarea probelor și operațiunile HSM) fac referire la acest **OID al politicii criptografice** în înregistrările de audit și metadatele probelor.

5.4 Politica de reînnoire

Serviciul de conservare implementează o **strategie de reînnoire proactivă** pentru a asigura securitatea pe termen lung a semnăturilor și sigiliilor conservate.

- **Monitorizare:** Algoritmii sunt monitorizați continuu în raport cu actualizările ETSI TS 119 312, recomandările NIST și orientările ENISA.
- **Intervale de reînnoire:**
    - Lanțurile de dovezi (ERS) sunt reînnoite la fiecare **X ani** [de definit contractual] sau mai devreme, dacă sunt identificate vulnerabilități criptografice.
    - Timestamp-urile de arhivare AdES-LTA sunt reînnoite periodic pentru a menține valabilitatea.
- **Proces:**

1. Se verifică validitatea lanțului de dovezi.
2. Se construiește un nou arbore hash utilizând algoritmi actualizați.
3. Obținerea de noi timestamp-uri de la QTSA.
4. Dovezile actualizate sunt atașate la Containerul de obiecte de conservare (POC).

- **Referință politică:** Fiecare acțiune de reînnoire este înregistrată cu referire la **OID-ul politicii de criptare (1.3.6.1.4.1.47898.10.3)**.

5.5 Politica de validare

- **Identificator de politică: OID: 1.3.6.1.4.1.47898.10.2.1**
- **Domeniu de aplicare:** Se aplică tuturor semnăturilor și sigiliilor la momentul introducerii.
- **Bază:** Derivată din ETSI EN 319 102-1 (validarea semnăturilor AdES) și ETSI TS 119 441/442.
- **Aplicare:** Asigură că numai semnăturile/ștampilele **valabile la momentul preluării** sunt păstrate. Semnăturile nevalide sunt respinse cu un raport de validare detaliat.

5.6 Publicarea politicii

- **PSPPS (OID: 1.3.6.1.4.1.47898.10.1)** și toate OID-urile politicilor subordonate sunt publicate:
    - În acest document (disponibil public).
    - Pe site-ul oficial CERT DIGITAL QPS.
    - În rapoartele de audit, acolo unde este cazul.
- Politicile sunt actualizate periodic, modificările fiind înregistrate în **Istoricul modificărilor (Anexa C)**.

PSPPS și toate OID-urile de politică sunt publicate în depozitul CERT DIGITAL QPS: **https://certdigital.ro/repository**

6. Practici de serviciu

6.1 Prezentare generală

Practicile operaționale ale **CERT DIGITAL QPS** sunt concepute pentru a se asigura că toate activitățile de conservare sunt:

- efectuate în mod sigur și consecvent,
- Ușor de urmărit și verificat,
- În conformitate cu **PSPPS (OID: 1.3.6.1.4.1.47898.10.1)**,
- Executate în conformitate cu **profilurile de conservare** definite **(WOS/WST/WTS)**.

Aceste practici se aplică tuturor fazelor operaționale, de la ingestie la reînnoirea probelor, recuperare și eventuală ștergere.

6.2 Introducerea obiectelor de conservare

- **Trimitere:**
    - Abonații trimit obiecte de conservare (semnături, sigilii sau date cu metadate asociate) prin intermediul interfeței PreservePO.
    - Fiecare trimitere specifică OID-ul profilului dorit (de exemplu, WST → 1.3.6.1.4.1.47898.10.1.2).

- **Validare:**
    - Obiectele trimise sunt validate în conformitate cu **OID-ul politicii de validare: 1.3.6.1.4.1.47898.10.2.1**.
    - Obiectele nevalide sunt respinse cu un raport de validare detaliat.
- **Prelucrare:**
    - Dacă este valid, sistemul colectează toate datele de validare necesare (certificate, CRL-uri, OCSP).
    - Dovezile de conservare sunt generate în conformitate cu **politica privind formatul dovezilor OID: 1.3.6.1.4.1.47898.10.4**.
- **Confirmare:**
    - Se creează un container de obiecte de conservare (POC).
    - Returnat abonatului (WOS/WTS) sau stocat în siguranță (WST).

6.3 Generarea dovezilor

- **Dovezi bazate pe ERS (RFC 4998/6283):**
    - Arborii hash sunt calculați pe baza obiectului de conservare și a datelor de validare asociate.
    - Ancorate de timestamp-uri calificate (EN 319 421/422).
- **Augmentare AdES-LTA:**
    - Marcaje temporale de arhivare și date de validare încorporate în containerul de semnături original (de exemplu, PAdES-LTA).
- **Semnarea dovezilor:**
    - Toate dovezile sunt legate criptografic și semnate folosind chei protejate HSM.
    - Operațiunile sunt conforme cu **politica de criptare OID: 1.3.6.1.4.1.47898.10.3**.

6.4 Reînnoirea dovezilor

- **Declanșare:**

- Reînnoirea este programată în mod proactiv înainte de sfârșitul duratei de viață a algoritmilor, conform **Politicii de criptare OID**.
- Reînnoirea poate fi declanșată și de alerte de supraveghere (de exemplu, actualizări criptografice ENISA).

- **Proces**

1. Dovezile existente sunt validate.
2. Se generează noi arbori hash sau timestamp-uri de arhivare utilizând algoritmi actualizați.
3. Se adaugă o nouă marcă temporală calificată.
4. Dovezile reînnoite sunt stocate în POC actualizat.

- **Auditabilitate:**
  - Fiecare acțiune de reînnoire este înregistrată și legată de OID-urile aplicate.
  - Urmărirea reînnoirii este disponibilă prin intermediul interfeței RetrieveTrace.

6.5 Recuperarea dovezilor

- **RetrievePO/RetrievePOC:**
  - Abonații și părțile interesate pot solicita recuperarea obiectelor de conservare complete sau a containerelor de dovezi.
  - Obiectul returnat include referințe la OID-urile profilului și politicii.
- **ValidateEvidence:**
  - Permite verificarea la cerere a probelor.
  - Returnează starea de validare (TOTAL-PASSED, FAILED, INDETERMINATE) în conformitate cu ETSI EN 319 102-1.
  - Rapoartele de validare fac referire explicită la OID-ul politicii de validare aplicate.

6.6 Ștergerea obiectelor de conservare

- **WST:**

- Obiectele de conservare sunt șterse numai după expirarea perioadei de păstrare contractuale sau la cererea abonatului.
- Ștergerea se efectuează în condiții de siguranță (ștergere în mai multe etape sau ștergere criptografică).

- **WTS:**
  - Obiectele sunt șterse automat după livrarea cu succes a probelor.
- **WOS:**
  - Nu este necesară ștergerea, deoarece datele nu sunt niciodată stocate de CERT DIGITAL QPS.

Toate ștergerile sunt înregistrate, inclusiv referințele la OID-urile afectate.

6.7 Înregistrarea çi urmele de audit

- **Înregistrarea evenimentelor:**
  - Toate evenimentele cheie (preluare, validare, generare de dovezi, reînnoire, ștergere) sunt înregistrate.
  - Jurnalele includ OID-ul profilului și politicile aplicate.
- **Piste de audit:**
  - Jurnalele sunt protejate împotriva modificărilor (stocare WORM).
  - Sunt păstrate timp de minimum 10 ani, cu posibilitate de prelungire în conformitate cu legislația națională.
- **Accesul la jurnale:**
  - Auditorii autorizați și organismele de supraveghere pot solicita jurnalele ciclului de viață prin intermediul API-ului RetrieveTrace.

6.8 Gestionarea incidentelor

- **Detectare și răspuns:**
  - Sistemele de monitorizare a securității detectează anomalii în funcționarea serviciului.

- Incidentele sunt clasificate (minore/majore/critice) și escaladate în consecință.

- **Raportare:**
  - Incidentele cu impact potențial asupra dovezilor de conservare sunt raportate organismului de supraveghere în conformitate cu obligațiile eIDAS.
  - Abonații sunt notificați dacă obiectele lor de conservare pot fi afectate.
- **Acțiuni post-incident:**
  - Analiza cauzelor principale efectuată.
  - Se implementează măsuri de atenuare.
  - Înregistrările din jurnalul de audit sunt păstrate pentru verificare independentă.

6.9 Continuitatea activității în operațiuni

- **Recuperare în caz de dezastru:**
  - Serviciile de generare a probelor pot fi restabilite în termen de 4 ore (RTO).
  - Integritatea probelor este garantată prin stocarea replicată în afara amplasamentului (WST/WTS).
- **QTSA de rezervă:**
  - Dacă QTSA-ul principal nu este disponibil, se utilizează un QTSA secundar conform cu EN 319 421/422.
- **Testare periodică:**
  - Planurile de continuitate a activității sunt testate cel puțin o dată pe an.
  - Rezultatele testelor sunt documentate și revizuite de către conducere.

7. Roluri çi responsabilități

7.1 Prezentare generală

Serviciul de conservare **CERT DIGITAL QPS** implică multiple roluri și părți interesate, fiecare cu responsabilități distincte. Definirea clară a rolurilor asigură transparența, responsabilitatea și conformitatea cu **eIDAS** și **ETSI TS 119 511**.

Rolurile principale sunt:

- **Furnizor calificat de servicii de încredere (QTSP): CERT DIGITAL QPS**
- **Abonați** (entități care utilizează serviciul)
- **Părți care se bazează pe servicii** (verificatori de dovezi)
- **Furnizori externi** (de exemplu, autorități de marcare temporală)

7.2 Furnizor calificat de servicii de încredere (QTSP)

QTSP, care operează sub identitatea **CERT DIGITAL QPS**, este responsabil din punct de vedere legal pentru serviciul de conservare calificat.

Responsabilități

- Operarea serviciului de conservare în conformitate cu:
    - **PSPPS OID: 1.3.6.1.4.1.47898.10.1**
    - OID-urile profilului aplicabil (WOS/WST/WTS)
- Asigurarea conformității cu standardele eIDAS și ETSI.
- Menținerea securității fizice, logice și organizaționale, astfel cum este descris în capitolul 4.
- Gestionați cheile criptografice în HSM, urmând **politica de criptare OID: 1.3.6.1.4.1.47898.10.3**.
- Oferiți acces la dovezile de conservare și la rezultatele validării prin intermediul API-urilor definite.
- Monitorizați algoritmii și declanșați reînnoirea la timp a dovezilor.
- Păstrați jurnalele de audit și asigurați trasabilitatea ciclului de viață prin API-ul RetrieveTrace.

- Notificați autoritățile de supraveghere și abonații afectați în cazul incidentelor care afectează integritatea dovezilor.
- Publicați toate politicile de servicii relevante la **https://certdigital.ro/repository**.

7.3 Abonați

Abonații sunt persoane fizice sau juridice care transmit semnături, sigilii sau date către serviciul de conservare CERT DIGITAL QPS.

Responsabilități

- Utilizarea serviciului în conformitate cu contractele, politicile și standardele aplicabile.
- Trimiteți obiectele de conservare în formate acceptate și aliniate cu **OID-ul politicii de criptare**.
- Asigurarea faptului că semnăturile/ștampilele trimise erau **valabile la momentul introducerii**.
- Protejarea dovezilor de conservare returnate în conformitate cu profilurile WOS/WTS.
- Notificați QTSP în cazul în care există suspiciuni de compromitere a datelor trimise sau a credențialelor aferente.
- Acceptați faptul că semnăturile/ștampilele nevalide nu pot fi „reparate” prin conservare.

7.4 Părți de încredere

Părțile care se bazează sunt persoane fizice sau juridice care se bazează pe dovezile de conservare furnizate de CERT DIGITAL QPS pentru a verifica validitatea pe termen lung a semnăturilor și sigiliilor.

Responsabilități

- Verificarea dovezilor utilizând proceduri standard de validare (ETSI EN 319 102-1).
- Asigurați-vă că utilizează instrumente de validare actualizate, capabile să interpreteze formatele dovezilor de conservare.
- Să ia în considerare **OID-ul politicii de validare** aplicate în evaluările lor.
- Acceptarea faptului că răspunderea CERT DIGITAL QPS este limitată la domeniul de aplicare definit în capitolul 9 (Răspundere și aspecte juridice).

7.5 Furnizori externi

CERT DIGITAL QPS poate apela la furnizori externi pentru servicii de încredere specifice, în special:

- **Autorități calificate de marcare temporală (QTSA):**
  - Furnizează marcaje temporale calificate (RFC 3161, EN 319 422).
  - Trebuie să fie incluse în Lista de încredere a UE.
  - Marcajele temporale constituie piatra de temelie a dovezilor de conservare.
- **Furnizori de servicii de validare (opțional):**
  - Dacă se utilizează servicii de validare externe (conforme cu ETSI TS 119 441/442), rezultatele acestora sunt integrate în dovezile de conservare.

Responsabilitățile furnizorilor externi:

- Să funcționeze în conformitate cu eIDAS și standardele ETSI relevante.
- Garantarea integrității și disponibilității serviciilor lor.
- Oferă garanții contractuale către CERT DIGITAL QPS în ceea ce privește răspunderea și continuitatea.

7.6 Autoritatea de supraveghere

Autoritatea de supraveghere este organismul național desemnat în temeiul eIDAS pentru a supraveghea furnizorii de servicii de încredere calificați.

Responsabilități

- Evaluează conformitatea CERT DIGITAL QPS prin audituri periodice (EN 319 403).
- Asigurarea că CERT DIGITAL QPS este corect inclus în Lista de încredere a UE ca furnizor de servicii de conservare calificate.
- Luarea de măsuri corective în caz de neconformitate.

7.7 Rezumatul rolurilor çi asocierilor OID

Rol	Responsabilități cheie	OID-uri relevante
QTSP (CERT DIGITAL QPS)	Operarea serviciului, gestionarea politicii de criptare, generarea și reînnoirea dovezilor, asigurarea conformității, publicarea politicilor	PSPPS OID: 1.3.6.1.4.1.47898.10.1 Politica de criptare OID: 1.3.6.1.4.1.47898.10.3 Politica privind formatul dovezilor OID: 1.3.6.1.4.1.47898.10.4
Abonat	Trimiteți semnături/sigilii valide, protejați dovezile (WOS/WTS), respectați formatele și regulile de criptare	OID-uri profiluri de conservare: .1.1 (WOS), .1.2 (WST), .1.3 (WTS)
Partea care se bazează	Verificați dovezile, interpretați politicile de validare, acceptați domeniul de aplicare/limitări	Politica de validare OID: 1.3.6.1.4.1.47898.10.2.1
Furnizori externi	Furnizează servicii QTSA și servicii opționale de validare	Conectați indirect prin timestamp-uri (EN 319 421/422)
Autoritatea de supraveghere	Auditează și supraveghează conformitatea	Înregistrare în lista de încredere a UE (PSES/Q)

8. Obligații

8.1 Prezentare generală

Această secțiune definește obligațiile tuturor părților implicate în serviciul de conservare **CERT DIGITAL QPS**.
Obligațiile asigură funcționarea fiabilă a serviciului și distribuirea clară a responsabilităților între:

- **QTSP (CERT DIGITAL QPS)**
- **Abonați**

- **Părțile care se bazează pe serviciu**
- **Furnizori externi**

8.2 Obligațiile QTSP (CERT DIGITAL QPS)

Furnizorul de servicii de încredere calificat, care operează sub **CERT DIGITAL QPS**, are următoarele obligații:

- **Conformitate și funcționare**
  - Să opereze serviciul de conservare în conformitate cu:
    - **PSPPS OID: 1.3.6.1.4.1.47898.10.1**
    - OID-uri profil de conservare: WOS (.1.1), WST (.1.2), WTS (.1.3)
    - OID pentru politica de criptare: 1.3.6.1.4.1.47898.10.3
    - OID pentru politica de validare: 1.3.6.1.4.1.47898.10.2.1
  - Menținerea conformității cu Regulamentul eIDAS și standardele ETSI.
- **Securitate**
  - Protejarea tuturor materialelor criptografice sensibile în HSM-uri certificate.
  - Menținerea securității fizice, logice și organizaționale, astfel cum se prevede în capitolul 4.
  - Asigurarea integrității și confidențialității datelor abonaților.
- **Disponibilitatea serviciilor**
  - Asigurați accesul continuu și fiabil la serviciile de conservare (24/7).
  - Mențineți o disponibilitate ridicată prin măsuri de redundanță și continuitate.
- **Conservare și reînnoire**
  - Validați toate semnăturile/ștampilele la preluare în conformitate cu politica de validare declarată.
  - Asigurarea reînnoirii la timp a dovezilor pe baza politicii criptografice.
- **Transparență și publicare**
  - Publicați PSPPS și politicile de servicii conexe la **https://certdigital.ro/repository**.
  - Faceți publică lista OID-urilor și politicilor acceptate.
- **Notificare și gestionarea incidentelor**

- Notificați abonații și autoritățile de supraveghere cu privire la orice incident care afectează dovezile de conservare.
- Furnizați măsuri de atenuare și recuperare.

8.3 Obligațiile abonaților

Abonații care utilizează serviciul CERT DIGITAL QPS au următoarele obligații:

- **Utilizare corectă**
  - Să trimită obiectele de conservare în formate acceptate și conforme cu **OID-ul politicii de criptare**.
  - Să specifice în mod clar profilul de conservare (WOS/WST/WTS) care trebuie aplicat.
  - Asigurarea că semnăturile/ștampilele erau **valabile la momentul introducerii**.
- **Gestionarea probelor**
  - În profilurile WOS și WTS, păstrați probele de conservare și datele asociate după recuperare.
  - Păstrați probele pe durata necesității legale sau comerciale.
- **Acuratețe și integritate**
  - Furnizați metadate și informații corecte în momentul trimiterii.
  - Abțineți-vă de la trimiterea de date frauduloase, corupte sau rău intenționate.
- **Notificare**
  - Informați imediat QTSP dacă există suspiciuni că probele sau acreditările aferente au fost compromise.
- **Respectarea contractului**
  - Respectați termenii contractuali ai serviciului, inclusiv limitările de răspundere și cerințele tehnice.

8.4 Obligațiile părților care se bazează pe certificat

Părțile care se bazează pe dovezile de conservare generate de CERT DIGITAL QPS sunt obligate să:

- **Verificarea dovezilor**
  - Validați dovezile de conservare utilizând instrumente conforme cu ETSI EN 319 102-1.
  - Verifice politica de validare OID aplicată (de exemplu, 1.3.6.1.4.1.47898.10.2.1).
- **Interpretare**
  - Interpreteze rapoartele de validare în contextul politicilor și OID-urilor declarate.
  - Acceptați faptul că răspunderea CERT DIGITAL QPS este limitată, astfel cum se descrie în capitolul 9.
- **Limitări**
  - Recunoașteți că serviciul de conservare garantează valabilitatea pe termen lung numai pentru semnăturile/ștampilele care erau valabile la momentul introducerii.

8.5 Obligațiile furnizorilor externi

Furnizorii externi care susțin CERT DIGITAL QPS (de exemplu, QTSA, servicii de validare externe) sunt obligați să:

- **Autoritatea de marcare temporală (QTSA):**
  - Furnizeze marcaje temporale calificate în conformitate cu EN 319 421/422.
  - Asigure disponibilitatea și fiabilitatea continuă a serviciilor de marcare temporală.
  - Menținerea înscrierii pe lista de încredere a UE.
- **Furnizori de servicii de validare (dacă este cazul):**
  - Furnizează rezultate de validare în conformitate cu ETSI TS 119 441/442.
  - Garantați integritatea și autenticitatea răspunsurilor de validare.
- **Angajamente contractuale:**

- Menținerea acordurilor privind nivelul serviciilor cu CERT DIGITAL QPS, care acoperă fiabilitatea, securitatea și răspunderea.

8.6 Rezumatul obligațiilor

Rol	Obligații	Referințe OID
QTSP (CERT DIGITAL QPS)	Operarea serviciului în condiții de siguranță, asigurarea conformității, reînnoirea dovezilor, publicarea politicilor, notificarea incidentelor	PSPPS OID .10.1, Profil OID .10.1.1–.1.3, Politica de criptare OID .10.3, Politica de validare OID .10.2.1
Abonați	Trimiteți semnături valide, utilizați profiluri corecte, protejați dovezile (WOS/WTS), notificați compromiterile	OID-uri profil .10.1.1–.1.3, OID politică de criptare .10.3
Părți de încredere	Verifică dovezile, interpretează rezultatele validării, acceptă limitele de răspundere	OID pentru politica de validare .10.2.1
Furnizori externi	Furnizează marcaje temporale calificate și rezultate opționale de validare, mențin conformitatea cu standardele ETSI	Referință indirectă la politicile privind marcajele temporale (EN 319 421/422)

9. Răspundere çi aspecte juridice

9.1 Prezentare generală

Scopul acestei secțiuni este de a stabili **întinderea răspunderii** furnizorului de servicii de încredere calificate (QTSP), precum și limitările aplicabile abonaților, părților care se bazează pe servicii și furnizorilor externi.
Cadrul de răspundere este aliniat la **Regulamentul (UE) 910/2014 (eIDAS)**, în special la articolele **13, 19 și 34**, și la cerințele **ETSI TS 119 511**.

9.2 Răspunderea QTSP (CERT DIGITAL QPS)

În calitate de **furnizor calificat de servicii de încredere**, CERT DIGITAL QPS își recunoaște răspunderea astfel cum este definită la **articolul 13 din eIDAS**:

- **Obligații privind serviciile de conservare:**
  - CERT DIGITAL QPS este responsabil pentru asigurarea faptului că dovezile de conservare sunt generate, stocate (dacă este cazul), reînnoite și livrate în conformitate cu prezentul PSPPS (OID: 1.3.6.1.4.1.47898.10.1).
  - Răspunderea se aplică numai în cazul în care abonații au respectat obligațiile definite în capitolul 8.
- **Integritatea dovezilor:**
  - CERT DIGITAL QPS garantează că dovezile emise în conformitate cu profilurile sale de servicii (WOS/WST/WTS) sunt intacte și corect legate de obiectul conservat.
  - Dovezile de păstrare includ referințe explicite la OID-urile profilului aplicat pentru trasabilitate.
- **Disponibilitate:**
  - CERT DIGITAL QPS este responsabil pentru asigurarea disponibilității serviciului în conformitate cu acordurile contractuale privind nivelul de servicii (SLA).
- **Reînnoire:**
  - CERT DIGITAL QPS este responsabil pentru efectuarea reînnoirilor în timp util, în conformitate cu **OID-ul politicii de criptare: 1.3.6.1.4.1.47898.10.3**.
- **Publicare:**
  - CERT DIGITAL QPS se asigură că PSPPS, politicile de conservare și informațiile privind starea serviciilor sunt publicate pe **https://certdigital.ro/repository**.

9.3 Limitarea răspunderii

CERT DIGITAL QPS își limitează răspunderea în următoarele condiții:

- **Semnături nevalide la preluare:**
  - Răspunderea nu se extinde la semnăturile sau sigiliile care erau nevalide la momentul preluării, chiar dacă au fost conservate ulterior.

- **Utilizarea necorespunzătoare a dovezilor:**
    - Răspunderea nu acoperă utilizarea necorespunzătoare a probelor de păstrare, inclusiv interpretarea eronată de către părțile care se bazează pe acestea sau modificarea de către abonați.
- **Dependențe externe:**
    - Răspunderea este limitată pentru defecțiunile cauzate de furnizori externi (de exemplu, întreruperea funcționării QTSA), cu condiția ca furnizorii redundanți să fi fost disponibili.
- **Forță majoră:**
    - CERT DIGITAL QPS nu este răspunzător pentru defecțiunile serviciului cauzate de evenimente care nu pot fi controlate în mod rezonabil (de exemplu, dezastre naturale, atacuri cibernetice la scară largă).
- **Limitări ale profilului WOS:**
    - În conformitate cu **profilul WOS (OID: 1.3.6.1.4.1.47898.10.1.1)**, CERT DIGITAL QPS nu este răspunzător pentru păstrarea pe termen lung a probelor, deoarece acestea sunt livrate și gestionate de abonat.

9.4 Răspunderea abonaților

Abonații sunt responsabili pentru:

- Trimiterea numai a semnăturilor/ștampilelor valide în momentul introducerii.
- Păstrarea dovezilor de conservare atunci când se utilizează profiluri WOS/WTS.
- Furnizarea de informații exacte în momentul depunerii.
- Utilizarea abuzivă sau pierderea dovezilor de conservare aflate sub controlul lor.

9.5 Răspunderea părților care se bazează pe informații

Părțile care se bazează sunt responsabile pentru:

- Validarea corespunzătoare a dovezilor în conformitate cu ETSI EN 319 102-1.
- Interpretarea corectă a OID-urilor aplicate și a politicilor de validare.

- Acceptarea limitărilor serviciului de conservare, astfel cum sunt definite în prezentul PSPPS.

9.6 Răspunderea furnizorilor externi

Furnizorii externi (de exemplu, QTSA, furnizorii de servicii de validare) sunt responsabili pentru integritatea și disponibilitatea serviciilor lor respective, în conformitate cu acordurile contractuale încheiate cu CERT DIGITAL QPS.
CERT DIGITAL QPS poate transfera anumite riscuri către furnizorii externi prin contracte și SLA-uri cu caracter juridic obligatoriu.

9.7 Soluționarea litigiilor

- **Procedură:**
    - Litigiile dintre CERT DIGITAL QPS și abonați sau părțile care se bazează pe servicii trebuie soluționate prin negocieri de bună credință.
    - Dacă nu se rezolvă, litigiile vor fi supuse arbitrajului sau medierii, astfel cum se definește în acordurile contractuale.
- **Escaladare:**
    - În cazul litigiilor de natură reglementară, autoritatea de supraveghere poate interveni în conformitate cu legislația națională de punere în aplicare a eIDAS.

9.8 Legislația aplicabilă çi jurisdicția

- Prezentul PSPPS și toate acordurile contractuale reglementate de acesta vor fi supuse legislației din **România**, ca țară de stabilire a CERT DIGITAL QPS.
- Instanțele competente din **București, România**, vor avea jurisdicție asupra litigiilor, cu excepția cazului în care legislația UE prevede altfel.
- Recunoașterea transfrontalieră respectă **recunoașterea reciprocă eIDAS** a serviciilor de încredere calificate în toate statele membre ale UE.

9.9 Matricea rezumativă a răspunderii

Parte	Acoperirea răspunderii	Excluderi	Referințe OID
QTSP (CERT DIGITAL QPS)	Integritatea probelor, generarea corectă, reînnoirea, publicarea	Semnături nevalide la introducere, utilizare necorespunzătoare de către abonat, forță majoră	PSPPS OID .10.1, Profiluri OID .10.1.1–.1.3, Politica de criptare OID .10.3
Abonat	Trimitere validă a datelor, protejarea dovezilor	Intrare nevalidă, pierderea/utilizarea abuzivă a dovezilor	OID-uri profil .10.1.1–.1.3
Partea de încredere	Validarea corectă a dovezilor	Interpretare eronată, ignorarea politicilor OID	Politica de validare OID .10.2.1
Furnizori externi	Acuratețea marcajelor temporale, rezultatele validării	Timpul de nefuncționare a serviciului peste SLA	Legat de EN 319 421/422, 441/442

10. Audit çi conformitate

10.1 Prezentare generală

Serviciul **CERT DIGITAL QPS** este supus unor **evaluări** periodice **de conformitate** pentru a demonstra conformitatea cu:

- **Regulamentul (UE) nr. 910/2014 (eIDAS)**
- **ETSI EN 319 401** (Cerințe generale de politică)
- **ETSI TS 119 511** (Politica de conservare și cerințe de securitate)
- **ETSI TS 119 512** (Protocoale de conservare)
- **ETSI TS 119 312** (Suite criptografice)

- **ETSI EN 319 421/422** (Marcare temporală calificată)
- **ETSI TS 119 441/442** (Servicii de validare)

Conformitatea este evaluată în mod independent de un **organism de evaluare a conformității (CAB)** în conformitate cu **ETSI EN 319 403-1**.

10.2 Procesul de evaluare a conformității

- **Frecvență:**
  - Evaluările complete ale conformității sunt efectuate cel puțin o dată la **24 de luni**, în conformitate cu cerințele eIDAS.
  - Auditurile de supraveghere interimare pot fi efectuate anual sau conform mandatului autorității de supraveghere.
- **Domeniu de aplicare**
  - Verificarea conformității cu PSPPS OID **1.3.6.1.4.1.47898.10.1**.
  - Evaluarea practicilor operaționale (capitolele 6-8).
  - Inspecția controalelor criptografice în conformitate cu politica criptografică OID **1.3.6.1.4.1.47898.10.3**.
  - Confirmarea utilizării serviciilor de marcare temporală calificate (EN 319 421/422).
  - Verificarea referințelor OID în dovezi, rapoarte și jurnale.
- **Rezultate:**
  - Un **raport** oficial **de evaluare a conformității (CAR)** emis de CAB.
  - Transmiterea CAR către autoritatea de supraveghere.

10.3 Supravegherea autorității de supraveghere

- Autoritatea națională de supraveghere desemnată în temeiul eIDAS supraveghează CERT DIGITAL QPS.
- Autoritatea de supraveghere:
  - Examinează rapoartele de evaluare a conformității.
  - Menține CERT DIGITAL QPS pe **lista de încredere a UE (TL)** ca **serviciu de conservare calificat**.

- Poate efectua **audituri extraordinare** în cazul incidentelor, reclamațiilor sau modificărilor legislative.

- **Intrare în lista de încredere:**
  - Identificator tip serviciu: **http://uri.etsi.org/TrstSvc/Svctype/PSES/Q**
  - Calificatori:
    - **ForSignatures**
    - **Pentru sigilii**

10.4 Monitorizarea conformității interne

CERT DIGITAL QPS menține un program intern de conformitate care include:

- **Audituri interne periodice:**
  - Cel puțin o dată pe an, acoperind securitatea operațională, fluxurile de lucru de conservare și reînnoirea probelor.
- **Gestionarea vulnerabilităților:**
  - Monitorizarea continuă a stării algoritmului criptografic (conform ETSI TS 119 312).
  - Actualizări prompte ale **politicii de criptare OID: 1.3.6.1.4.1.47898.10.3** atunci când sunt necesare modificări.
- **Gestionarea politicilor:**
  - Toate actualizările PSPPS și ale politicilor subordonate sunt urmărite în istoricul versiunilor (anexa).
  - Politicile revizuite sunt publicate la adresa **https://certdigital.ro/repository**.
- **Instruire și conștientizare:**
  - Toate rolurile de încredere beneficiază de instruire anuală în materie de conformitate și securitate.

10.5 Raportarea incidentelor Conformitate

- **Obligații eIDAS:**

- CERT DIGITAL QPS respectă **articolul 19 alineatul (2)** din eIDAS, care impune notificarea incidentelor către autoritățile de supraveghere fără întârzieri nejustificate.

- **Notificarea abonaților:**
  - Abonații sunt notificați cu privire la orice incident care poate afecta validitatea sau disponibilitatea dovezilor lor.
- **Comunicarea către părțile care se bazează pe dovezi:**
  - În cazul incidentelor cu impact sistemic, pot fi publicate declarații publice la adresa URL a depozitului.

10.6 Îmbunătățire continuă

- CERT DIGITAL QPS adoptă o **abordare bazată pe riscuri** în ceea ce privește conformitatea.
- Lecțiile învățate din incidente, audituri și feedback-ul de supraveghere sunt utilizate pentru a îmbunătăți:
  - Controalele de securitate
  - Practicilor operaționale
  - Politicile și procedurile

10.7 Rezumatul conformității

Audit / Supraveghere Actor	**Domeniu**	**Frecvență**	**Referință**
Organismul de evaluare a conformității (CAB)	Audit extern de conformitate vs. ETSI/eIDAS	La fiecare 24 de luni	ETSI EN 319 403-1
Autoritatea de supraveghere	Includerea în lista de încredere, supravegherea reglementară, audituri extraordinare	Continuu + după necesități	eIDAS Art. 17, 19, 20

Audit / Supraveghere Actor	Domeniu	Frecvență	Referință
conformitate	operaționale, actualizări criptografice, instruire	anuală + continuă	Politica de criptare OID .10.3

11. Specificații tehnice

11.1 Prezentare generală

Această secțiune descrie specificațiile tehnice aplicate de **CERT DIGITAL QPS** în furnizarea serviciului său de conservare calificată. Aceasta include:

- Formate de semnătură și sigiliu acceptate,
- Formate de dovezi acceptate,
- Algoritmi criptografici acceptați,
- Formate de containere pentru obiecte de conservare,
- Legături de protocol de serviciu,
- Utilizarea OID-urilor în fluxurile de lucru tehnice.

11.2 Formate de semnătură çi sigiliu acceptate

CERT DIGITAL QPS acceptă păstrarea următoarelor formate de semnături electronice avansate (AdES), astfel cum sunt definite de standardele ETSI:

- **CAdES (CMS Advanced Electronic Signatures)** – ETSI EN 319 122-1
- **XAdES (semnături electronice avansate XML)** – ETSI EN 319 132-1
- **PAdES (semnături electronice avansate PDF)** – ETSI EN 319 142-1
- **ASiC (Containere de semnături asociate)** – ETSI EN 319 162-1

Conservarea se aplică atât **semnăturilor,** cât și **sigiliilor** create în conformitate cu cerințele eIDAS.

11.3 Formate de dovezi acceptate

Probele de conservare generate de CERT DIGITAL QPS sunt conforme cu:

- **Sintaxa înregistrării probelor (ERS)** – RFC 4998
- **XMLERS (Sintaxa înregistrării probelor XML)** – RFC 6283
- **AdES-LTA Augmentation:**
    - PAdES-LTA (PDF)
    - XAdES-A (XML)
    - CAdES-A (CMS)

Alegerea formatului probelor este reglementată de **Politica privind formatul probelor OID: 1.3.6.1.4.1.47898.10.4**.

11.4 Algoritmi criptografici și lungimi ale cheilor

Toate primitivele criptografice sunt conforme cu **ETSI TS 119 312 (Suite criptografice)**.

- **Identificator de politică: Politica de criptare OID: 1.3.6.1.4.1.47898.10.3**
- **Funcții hash acceptate:**
    - SHA-256 (implicit)
    - SHA-384
    - SHA-512
- **Algoritmi de semnătură digitală acceptați:**
    - RSA ≥ 2048 biți
    - ECDSA (P-256, P-384, P-521)
    - EdDSA (Ed25519, Ed448)
- **Algoritmi simetrici acceptați (utilizare internă):**
    - AES-256 (criptare în repaus, suite de cifrare TLS)
- **Algoritmi de semnătură cu marcaj temporal:**

- RSA/ECDSA/EdDSA pentru funcțiile hash acceptate

- **Reînnoire criptografică:**
  - Dovezi reînnoite cu cel puțin 3 ani înainte de sfârșitul duratei de viață a algoritmului.

11.5 Format obiect de conservare çi container

CERT DIGITAL QPS implementează containere de obiecte de conservare (POC) în conformitate cu **ETSI TS 119 511 Anexa G**.

Fiecare POC conține:

- Obiectul de date conservat (sau rezumate aprobate în profilurile WOS),
- Date de validare (certificate, CRL-uri, răspunsuri OCSP),
- Dovezi de conservare (ERS sau AdES-LTA),
- Metadate care fac referire la politica aplicată și la OID-urile profilului.

Referințe OID în POC:

- **PSPPS OID:** 1.3.6.1.4.1.47898.10.1
- **OID profil:** unul dintre 1.3.6.1.4.1.47898.10.1.1 (WOS), .1.2 (WST), .1.3 (WTS)
- **OID pentru politica de validare:** 1.3.6.1.4.1.47898.10.2.1
- **OID pentru politica de criptare:** 1.3.6.1.4.1.47898.10.3
- **Politica privind formatul probelor OID:** 1.3.6.1.4.1.47898.10.4

11.6 Protocoale de servicii

Interfețele de servicii sunt conforme cu **ETSI TS 119 512 (Protocoale de servicii de conservare)**.

- **Legături acceptate:**
  - SOAP/XML (pentru sisteme vechi)
  - REST/JSON (pentru integrări moderne)
- **Operațiuni API de bază:**

- RetrieveInfo → Returnează metadatele serviciului, profilurile acceptate și OID-urile
- PreservePO → Trimite obiectul pentru conservare (include referința OID a profilului)
- RetrievePO / RetrievePOC → Recuperează obiectul conservat/containerul de dovezi
- UpdatePOC → Declanșează reînnoirea probelor
- ValidateEvidence → Validează probele conservate (returnează raportul cu OID-ul politicii de validare aplicate)
- DeletePO → Ștergerea sigură a obiectelor (numai WST/WTS)
- RetrieveTrace → Recuperare jurnale de trasabilitate

11.7 Utilizarea OID-urilor în fluxurile de lucru tehnice

OID-urile sunt încorporate în toate fluxurile tehnice relevante pentru trasabilitate:

- **Ingestie:** Abonatul specifică profilul de conservare OID (.1.1 / .1.2 / .1.3).
- **Validare:** Referință rezultate Politica de validare OID (1.3.6.1.4.1.47898.10.2.1).
- **Crearea probelor:** Referințe metadate Politica privind formatul probelor OID (1.3.6.1.4.1.47898.10.4).
- **Aplicarea criptării:** Referințe la operațiuni HSM și de semnare Politica de criptare OID (1.3.6.1.4.1.47898.10.3).
- **Publicare:** Toate OID-urile politicilor sunt documentate la **https://certdigital.ro/repository**.

11.8 Constrângeri privind dimensiunea datelor çi performanța

- **Dimensiunea maximă a obiectului de conservare (WST/WTS):** [de definit; de exemplu, 500 MB]
- **Dimensiunea maximă aprobată de WOS pentru rezumat:** până la 512 octeți per valoare hash.
- **Obiective de latență:**

- PreservePO → Dovezi returnate în ≤ 5 secunde (95% din cazuri).
- ValidateEvidence → Raport returnat în ≤ 3 secunde (95% din cazuri).

11.9 Interoperabilitate çi conformitate cu standardele

- Dovezile de conservare și POC-urile pot fi validate cu instrumente standard conforme cu ETSI EN 319 102-1.
- Toate marcajele de timp sunt emise de TSA-uri calificate incluse în Lista de încredere a UE.
- Obiectele de conservare pot fi exportate pentru migrarea între sisteme.

11.10 Rezumatul specificațiilor tehnice

Domeniu	Standard / Referință	OID Mapare
Formate de semnătură	CAdES, XAdES, PAdES, ASiC	–
Formate de dovezi	RFC 4998 (ERS), RFC 6283 (XMLERS), AdES-LTA	Politica privind formatele de dovezi OID .10.4
Criptografie	ETSI TS 119 312	Politica de criptare OID .10.3
Validare	EN 319 102-1, TS 119 441/442	Politica de validare OID .10.2.1
Protocoale	ETSI TS 119 512	–
Profiluri de conservare	TS 119 511 (WOS/WST/WTS)	OID-uri profil .10.1.1–.1.3
Referință PSPPS	TS 119 511 §4.3	OID PSPPS .10.1

12. Anexe

12.1 Glosar

AdES (Semnătură electronică avansată): Un tip de semnătură electronică care respectă cerințele Regulamentului UE 910/2014 (eIDAS) și standardele ETSI, asigurând autenticitatea și integritatea.

ASiC (Container de semnături asociate): Un format pentru gruparea datelor semnate și a semnăturilor digitale asociate într-un singur container.

CAdES (CMS Advanced Electronic Signatures): Un standard AdES pentru semnături bazate pe CMS (Cryptographic Message Syntax).

CERT DIGITAL QPS: Furnizorul de servicii de încredere calificate (QTSP) care operează serviciul de conservare calificat descris în prezentul PSPPS.

Crypto Policy OID: Un identificator de obiect care face referire la setul de algoritmi criptografici și lungimi de chei acceptate de serviciu.

eIDAS: Regulamentul (UE) nr. 910/2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă.

ERS (Evidence Record Syntax): un format definit în RFC 4998 pentru păstrarea semnăturilor digitale prin înregistrări criptografice.

LTA (Long-Term Archival): Un profil al AdES care încorporează marcaje temporale și date de validare pentru a asigura valabilitatea pe termen lung.

OID (Identificator de obiect): Un identificator unic la nivel global utilizat pentru a face referire la politici, profiluri și specificații tehnice.

PAdES (PDF Advanced Electronic Signatures): Un standard AdES pentru semnături bazate pe PDF.

PO (Preservation Object): Obiectul de date original, semnătura sau sigiliul trimis pentru conservare.

POC (Container obiect de conservare): Structura care încapsulează obiectul conservat, dovezile și metadatele, inclusiv referințele la OID-uri.

PGD (Proof of Existence of Data): Un profil de conservare opțional care dovedește că un anumit obiect de date a existat la un moment dat.

PSPPS (Declarație privind politica și practicile serviciului de conservare): Prezentul document care definește politicile și practicile CERT DIGITAL QPS.

QTSA (Autoritate de marcare temporală calificată): Un furnizor de servicii de încredere care emite marcaje temporale electronice calificate în conformitate cu eIDAS.

QES (Semnătură electronică calificată): O semnătură electronică avansată creată de un dispozitiv calificat de creare a semnăturilor și bazată pe un certificat calificat.

QSealS (sigiliu electronic calificat): un sigiliu electronic avansat creat de un dispozitiv calificat de creare a sigiliilor și bazat pe un certificat calificat.

TSL (listă de încredere): lista oficială menținută de fiecare stat membru al UE, care conține informații despre QTSP-urile recunoscute și serviciile acestora.

WOS/WST/WTS: Modele de stocare pentru conservare definite de ETSI: fără stocare, cu stocare, cu stocare temporară.

12.2 Referințe

Legislație primară:

- Regulamentul (UE) nr. 910/2014 (Regulamentul eIDAS)

Standarde ETSI:

- ETSI EN 319 401 – Cerințe generale de politică pentru furnizorii de servicii de încredere
- ETSI EN 319 403-1 – Cerințe de evaluare a conformității
- ETSI TS 119 511 – Cerințe de politică și securitate pentru serviciile de conservare
- ETSI TS 119 512 – Protocoale pentru servicii de conservare
- ETSI TS 119 312 – Suite criptografice
- ETSI EN 319 421 – Cerințe de politică și securitate pentru autoritățile de marcare temporală
- ETSI EN 319 422 – Protocoale și profiluri de marcare temporală
- ETSI TS 119 441 – Cerințe de politică și securitate pentru serviciile de validare a semnăturilor
- ETSI TS 119 442 – Protocoale pentru servicii de validare a semnăturilor

- ETSI EN 319 102-1 – Proceduri pentru validarea semnăturilor AdES

RFC:

- RFC 4998 – Sintaxa înregistrărilor probatorii (ERS)
- RFC 6283 – Sintaxa înregistrării probelor XML (XMLERS)
- RFC 3161 – Protocol de marcare temporală

Îndrumări suplimentare:

- Ghiduri criptografice ENISA
- NIST SP 800-131A – Orientări privind gestionarea cheilor criptografice

12.3 Informații de contact

Organizație: Centrul de Calcul S.A.
Formă juridică: Furnizor de servicii de încredere calificat în conformitate cu Regulamentul (UE) 910/2014
Adresă: Strada Tudor Vladimirescu, nr. 17, Târgu Jiu, Gorj România
URL-ul depozitului: https://certdigital.ro/repository
E-mail: office@certdigital.ro
sediu@centruldecalcul.ro
Telefon: +40 31 94 66
+40 253 214 767

Toate întrebările referitoare la acest PSPPS trebuie adresate echipei de conformitate la datele de contact de mai sus.