Serviciul calificat pentru păstrarea și garantarea pe termen lung a semnăturilor electronice

(Qualified Preservation Service - QPS)

Declarație de Politici, Practici și Proceduri

Versiunea 1.4

Data: 15 Ianuarie 2026

Notă importantă

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

Telefon: 004-021-31.19.901

Web: www.certsign.ro

Istoric document

Versiune	Data efectivă[1]	Motiv	Persoana care a făcut modificarea
1.0	Septembrie 2024	Prima versiune	Manager Politici PKI
1.1	10 Octombrie 2024	Actualizari minore	Manager Politici PKI
1.2	30 Octombrie 2024	Corectii dupa audit	Manager Politici PKI
1.3	15 Ianuarie 2025	Revizie anuala	Manager Politici PKI
1.4	15 Ianuarie 2026	Revizie anuala	Manager Politici PKI

Acest document a fost creat de către și este proprietatea:

Proprietar	Autor	Data creării
certSIGN	Manager Politici PKI	Septembrie 2024

Lista de distribuție

Destinație	Data distribuirii
Public-Internet	Octombrie 2024
Public-Internet	Ianuarie 2025
Public-Internet	Ianuarie 2026

Acest document a fost aprobat de:

Versiune	Nume	Data
1.1	Comitet de Management al Politicilor și Procedurilor (CMMP)	Octombrie 2024
1.2	Comitet de Management al Politicilor și Procedurilor (CMMP)	Octombrie 2024
1.3	Comitet de Management al Politicilor și Procedurilor (CMMP)	Ianuarie 2025
1.4	Comitet de Management al Politicilor și Procedurilor (CMMP)	Ianuarie 2026

[1] *Data efectivă = ultima zi a lunii , dacă nu este specificată*

Cuprins

1 Introducere

Declarația privind **Politicile, practicile și procedurile** referitoare la **Serviciul calificat de păstrare și garantare pe termen lung a semnăturilor electronice** (QPS) - (denumit în continuare **PPPS-QPS** sau **PPPS**) detaliază politicile, practicile și procedurile pe care certSIGN le aplică în ceea ce privește serviciul calificat de păstrare pe termen lung a semnăturilor calificate.
Conținutul **PPPS-QPS** este în conformitate cu cerințele ultimei versiuni ETSI TS 119 511 și ETSI TS 119 512.
certSIGN respectă Legea Română nr.214/2024 - privind utilizarea semnăturii electronice, a mărcii temporale și prestarea serviciilor de încredere bazate pe acestea.

1.1 Descriere generală

certSIGN, ca Furnizor de Servicii de Încredere (TSP), beneficiarii și părțile terțe afiliate trebuie să adere la **PPPS-QPS** în vigoare pentru utilizarea serviciului calificat de păstrare pe termen lung a semnăturilor electronice calificate și a sigiliilor calificate. Prezentul document descrie normele generale pentru furnizarea serviciilor calificate de păstrare.

1.2 Denumirea documentului și identificarea

Titlul acestui document este Serviciul calificat pentru păstrarea și garantarea pe termen lung a semnăturilor electronice (QPS) - Declarație de Politici, Practici și Proceduri, denumit în continuare PPPS-QPS sau PPPS.
Documentul este disponibil în format electronic în Depozitar, la adresa https://www.certsign.ro/depozitar.

1.3 Participanții PKI

certSIGN TSP reglementează cele mai importante relații dintre: entitățile certSIGN, echipele de consultanți (inclusiv auditorii) și clienții (utilizatorii serviciilor furnizate) acesteia:

- certSIGN Furnizor de Servicii de Încredere (TSP) pentru QPS,
- Autoritatea de Înregistrare,
- Depozitar,
- Beneficiarii,
- Entitățile Terțe/Partenere,
- Furnizori ai certSIGN - păstrare și management semnături digitale,
- Comitetul de Management al Politicilor și Procedurilor
- Auditorii.

certSIGN oferă servicii pentru orice persoană fizică sau entitate juridică care este de acord cu prevederile prezentului PPPS. Scopul prezentului PPPS (care include procedurile de validare a certificatelor și semnăturilor digitale, procedurile de păstrare a semnăturilor şi securitatea sistemului informaţional) este acela de a garanta utilizatorilor serviciilor certSIGN că nivelele de credibilitate declarate ale semnăturilor administrate corespund practicilor certSIGN, Furnizor de Servicii de Încredere (TSP).

1.3.1 certSIGN TSP pentru QPS

certSIGN Trust Services Provider este autoritatea care furnizează servicii de păstrare pe termen lung care se ocupă de verificarea valabilității și păstrării semnăturilor electronice, a sigiliilor electronice, a ștampilelor temporale și a certificatelor acestora, incluzând opțional păstrarea documentelor electronice semnate și sigilate.
Serviciul de prezervare al certSIGN este identificat prin următorul OID: 1.3.6.1.4.1.25017.5.

Serviciul calificat de prezervare al certSIGN este identificat prin: 1.3.6.1.4.1.25017.5.2

1.3.2 Autoritățile de Înregistrare

Autoritatea de înregistrare primește, verifică și aprobă sau respinge înregistrarea cererilor beneficiarilor de utilizare a serviciilor de păstrare/prezervare. Verificarea cererilor are ca scop autentificarea (pe baza documentelor anexate la cereri) atât a beneficiarului, cât și a datelor specificate în cerere. Autoritatea de înregistrare poate, de asemenea, să transmită cereri către TSP certSIGN pentru a anula un abonament.
Autoritatea de Înregistrare este operată de certSIGN sau de către o terță parte delegată.
RA-urile externe trebuie sa respecte aceleasi cerinte de securitate pe care le respecta TSP. in ceea ce priveste resursele umane, securitatea operationala, a retelei si a datelor personale asa cum este specificat in acest document.

1.3.3 Beneficiarii

Beneficiarii sunt persoanele fizice sau juridice care solicită Certsign un abonament pentru utilizarea serviciilor de păstrare și cu care semnează un Contract de abonament.
Beneficiarii pot solicita validarea și/sau păstrarea semnăturilor digitale calificate cu sau fără documentele corespunzătoare. Un beneficiar este, de asemenea, responsabil pentru notificarea imediată a certSIGN în cazul în care există o (suspiciune de) compromitere a cheii private a oricărui certificat utilizat pentru semnăturile în păstrare.

1.3.4 Entitățile Partenere

O entitate parteneră (terță parte) poate fi orice entitate care utilizează serviciile certSIGN și care ia decizii pe baza validității semnăturilor digitale aplicate sau a marcilor temporale.
O entitate parteneră este responsabilă pentru modul în care verifică starea curentă a unei semnături/marca temporala. Entitatea parteneră ia o astfel de decizie de fiecare dată când este necesar să se bazeze pe o semnătură electronică. O entitate parteneră utilizează informațiile dintr-un document semnat digital numai după ce se adresează unui serviciu de validare de încredere pentru a decide dacă o semnătură a fost utilizată în conformitate cu scopul declarat.

1.3.5 Alți participanți

Comitetul de Management al Politicilor și Procedurilor (CMMP) este un Comitet creat în cadrul certSIGN de către Consiliul de administrație pentru a supraveghea întreaga activitate a Autorităților certSIGN. Rolurile și responsabilitățile CMMP sunt descrise în documentația internă certSIGN.
Furnizorii de servicii ai certSIGN: furnizori externi care sprijină activitățile certSIGN pe baza unui acord contractual semnat.
Notarii publici sau avocații: pot efectua identificarea și garanta pentru identitatea reală a Beneficiarilor, în conformitate cu legile din România.
Furnizorii de Dispozitive de Creare a Semnăturilor Electronice Calificate: furnizorii externi care sprijină activitățile certSIGN în cadrul unui acord contractual semnat ce asigură furnizarea dispozitivelor criptografice fizice utilizate de către Beneficiari.

1.4 Utilizarea serviciului QPS

Aria de aplicabilitate a serviciului stabileşte scopul în care poate fi folosit acesta. Acest scop este definit de două elemente:

- Unul care defineşte aplicabilitatea serviciului (de exemplu, validitate semnătura sau sigiliu, păstrare semnătura/sigiliu sau/și document, integritate),
- Și unul care presupune o listă sau o descriere a aplicaţiilor permise sau interzise.

Entitatea Parteneră este responsabilă de stabilirea nivelului de credibilitate necesar pentru o semnătură/marcă temporală utilizată într-un anume scop. Luând în considerare factorii de risc semnificativi, Entitatea Parteneră trebuie să stabilească ce tip de semnătură întrunește cerinţele formulate.
Serviciul QPS oferă:
1) furnizarea de dovezi ale existenței pe perioade lungi de timp a datelor generale, indiferent dacă aceste date sunt semnate sau nu;
2) păstrarea pe perioade lungi de timp a capacității de a valida o semnătură digitală, de a-și menține valabilitatea, statutul și pentru a obține o dovadă a existenței datelor semnate asociate; și/sau
3) augmentarea/menținerea probelor de păstrare depuse la serviciul QPS.

1.4.1 Utilizări admise ale serviciului QPS

Serviciul QPS poate fi utilizat în aplicații care gestionează în mod corespunzător semnăturile digitale/mărcile temporale și cheile publice/private.
Aplicațiile pentru care se consideră că semnătura este de încredere vor fi decise chiar de către Entitățile Partenere, pe baza naturii și scopului semnăturii, inclusiv orice limitare aplicabilă înscrisă în Semnătură/Certificat.
Este responsabilitatea Beneficiarului să utilizeze serviciul QPS în conformitate cu acest PPPS.
Este responsabilitatea Beneficiarului de a utiliza aplicații software care interpretează corect, afișează și utilizează informațiile și restricțiile codificate în semnături/certificate, cum ar fi, dar fără a se limita la: utilizarea cheilor, răspundere limitată pentru fiecare tranzacție etc.
Este responsabilitatea Beneficiarului și a Entității Partenere să decidă pentru ce scop vor fi considerate semnăturile/ mărcile temporale ca fiind de încredere. O Entitate Parteneră trebuie să ia întotdeauna în considerare nivelul de asigurare și alte informații din PPPS înainte de a decide în privința aplicabilității semnăturii.

1.4.2 Utilizări interzise ale serviciului QPS

Orice utilizare a serviciului care diferă de utilizarea permisă în mod explicit în PPPS este interzisă.

1.5 Administrarea politicii

1.5.1 Organizația care administrează documentul

Prezentul document este administrat de către Prestatorul de servicii de încredere certSIGN (”TSP”) prin Comitetul de Management al Politicilor și Procedurilor (CMMP). CMMP include membri seniori din conducere, precum și personalul responsabil pentru gestionarea operațională a infrastructurii PKI a certSIGN.

Nume	S.C. certSIGN S.A. Punct de lucru: Bd. Tudor Vladimirescu, nr. 29 A, AFI Tech Park 1, București, România Registrul comerțului: J40/484/2006 CUI: RO 18288250 Sediul social: Șos. Olteniței 107A, clădirea C1, etaj 1, camera 16, Sector 4, București, România, Cod postal 041303
Telefon	(+4021)3119901

e-mail	office@certsign.ro
Web	www.certsign.ro

Tabel: 1.5.1 Organizația ce administrează documentul

1.5.2 Persoana de contact

Nume	Comitetul de Management al Politicilor și Procedurilor (CMMP)
Telefon	(+4021)3119901
e-mail	office@certsign.ro
Web	www.certsign.ro

Tabel: 1.5.2 Persoana de contact

1.5.3 Persoana care decide conformitatea PPPS cu politica

Nume	Comitetul de Management al Politicilor și Procedurilor (CMMP)
Telefon	(+4021)3119901
e-mail	office@certsign.ro
Web	www.certsign.ro

Tabel: 1.5.3 Persoana ce decide conformitatea PPPS cu politica

1.5.4 Procedurile de aprobare a PPPS

Comitetul de Management al Politicilor și Procedurilor este responsabil de aprobarea PPPS.
Beneficiarii trebuie să respecte PPPS-ul în vigoare publicat la adresa http://www.certsign.ro/repository.
Beneficiarii care nu acceptă noii termenii și reglementările modificate ale PPPS, sunt obligaţi să depună, în termen de 15 zile de la data la care noua versiune a PPPS a fost publicat, o declaraţie în acest sens. Acest lucru va duce la încetarea contractului de prestări servicii QPS.

1.6 Definiții și acronime

1.6.1 Definiții

Auditor – persoană care evaluează conformitatea cu cerințele specificate în documentele relevante
Autentificare – proces electronic ce permite identificarea electronică a unei persoane fizice sau juridice sau originea și integritatea datelor electronice care trebuie confirmate
Certificat – cheia publică a unui Subiect, împreună cu alte informații, ce sunt protejate împotriva falsificării prin criptarea cu cheia privată emisă de o autoritate de certificare
Lista de Certificate Revocate (CRL) – o listă semnată ce indică un set de certificate ce nu mai sunt considerate valide de către TSP
Autoritate de Certificare – autoritate considerată de încredere de unul sau mai mulți utilizatori, pentru crearea și atribuirea certificatelor
Lista de Revocare a Autorității de Certificare –o listă de revocare ce conține o listă de certificate de CA emise autorităților de certificare care nu mai sunt considerate valide de către TSP
Codul de Practici și Proceduri (CPP) – un cod de practici pe care o Autoritate de Certificare le utilizează în emiterea, gestionarea, revocarea și reînnoire sau re-key-ul certificatelor.
Declarație privind politicile, practicile și procedurile (PPPS) - o declarație a politicilor, practicilor și procedurilor pe care un TSP le utilizează pentru a furniza un serviciu de încredere.
Cross-certificare – un certificat care este emis pentru a stabili o relație de încredere între două autorități de certificare

Obiect de date - date binare/octeți, care sunt prelucrate (de exemplu, transformate, digerate sau semnate) de către o aplicație și care pot fi asociate cu informații suplimentare precum un identificator, codificarea, dimensiunea sau tipul.
Semnătură electronică – date în format electronic care sunt atașate sau asociate logic cu alte date în format electronic și care sunt utilizate de către semnatar pentru semnare.
Serviciu de păstrare calificat UE - serviciu de păstrare care îndeplinește cerințele pentru un serviciu de păstrare calificat pentru semnături electronice calificate și/sau pentru sigilii electronice calificate, astfel cum se prevede în Regulamentul (UE) 910/2014
Pachet de export-import - informații extrase din serviciul de păstrare, inclusiv obiectul de date de transmitere (SubDO), probele de păstrare și metadatele legate de păstrare, care permit unui alt serviciu de păstrare să le importe pentru a continua să realizeze obiectivul de păstrare pe baza acestor informații.
Termen lung - perioadă de timp în care schimbările tehnologice pot fi o preocupare
EXEMPLU: Schimbările tehnologice posibile sunt obsolescența tehnologiei criptografice, cum ar fi algoritmii criptografici, dimensiunile cheilor sau funcțiile hash, compromiterea cheilor.
Păstrarea pe termen lung - Prelungirea stării de valabilitate a unei semnături digitale pe perioade lungi de timp și/sau prelungirea furnizării dovezilor de existență a datelor pe perioade lungi de timp, în ciuda obsolescenței tehnologiei criptografice, cum ar fi algoritmii criptografici, dimensiunile cheilor sau funcțiile hash, a compromiterii cheilor sau a pierderii capacității de a verifica starea de valabilitate a certificatelor de cheie publică.
Meta-date – date despre alte date. NOTĂ: vezi ISO 14721:2012
Identificator de obiect (OID) – identificator alfanumeric / numeric înregistrat în concordanţă cu standardul ISO/IEC 9834 şi care descrie în mod unic un obiect specificat sau clasa sa
Dovezi de păstrare - dovezi produse de serviciul de păstrare care pot fi utilizate pentru a demonstra că unul sau mai multe obiective de păstrare sunt îndeplinite pentru un anumit obiect de păstrare.
Augmentarea dovezilor de păstrare - adăugarea de date la o dovadă de păstrare existentă pentru a prelungi perioada de valabilitate a acelei dovezi.
EXEMPLU: Adăugarea unei noi ștampile de timp care protejează datele de validare suplimentare care pot fi utilizate pentru a valida o semnătură și/sau o ștampilă de timp anterioare și/sau hash-ul datelor protejate utilizând un algoritm hash mai puternic.
Politica privind probele de păstrare - set de reguli care specifică cerințele și procesul intern de generare sau modul de validare a unei probe de păstrare.
Obiectiv de păstrare - unul dintre următoarele obiective atinse pe parcursul perioadei de păstrare: extinderea pe perioade lungi de timp a statutului de valabilitate a semnăturilor digitale, furnizarea de dovezi ale existenței datelor pe perioade lungi de timp sau sporirea dovezilor de păstrare furnizate din exterior.
NOTĂ: Un serviciu de păstrare poate atinge unul sau mai multe obiective de păstrare.
Interfață de păstrare - componentă care implementează protocolul de păstrare pe partea serviciului de păstrare.
Obiect de păstrare - obiect de date tipizat care este prezentat, prelucrat sau recuperat de la un serviciu de păstrare.
Identificatorul obiectului de păstrare - identificatorul unic al unui (set de) obiect(e) de păstrare transmis(e) unui serviciu de păstrare.
Perioada de păstrare - pentru un serviciu de păstrare cu stocare, durata pe parcursul căreia serviciul de păstrare conservă obiectele de păstrare transmise și dovezile asociate.

NOTĂ: Obiectele de păstrare transmise pot fi actualizate în timpul perioadei de păstrare.
Profil de păstrare - set identificat în mod unic de detalii de punere în aplicare pertinente pentru un model de stocare de păstrare și unul sau mai multe obiective de păstrare, care specifică modul în care sunt generate și validate dovezile de păstrare.
Protocol de păstrare - protocol de comunicare între serviciul de păstrare și un client de păstrare.
Schemă de păstrare - set generic de proceduri și reguli relevante pentru un model de stocare de păstrare și pentru unul sau mai multe obiective de păstrare, care prezintă modul în care sunt create și validate dovezile de păstrare.
Serviciu de păstrare - serviciu capabil să extindă statutul de valabilitate al unei semnături digitale pe perioade lungi de timp și/sau să furnizeze dovezi de existență a datelor pe perioade lungi de timp.
Furnizor de servicii de păstrare - furnizor de servicii de încredere care furnizează un serviciu de păstrare.
Politica serviciului de păstrare - politica serviciului de încredere pentru un serviciu de păstrare.
Declarație privind practica serviciului de păstrare - declarație privind practica serviciului de încredere pentru un serviciu de păstrare.
Model de stocare pentru păstrare - una dintre următoarele modalități de implementare a unui serviciu de păstrare - cu stocare, cu stocare temporară, fără stocare.
Abonat serviciu păstrare - persoană fizică sau juridică obligată prin acord cu un furnizor de servicii fiduciare de păstrare la orice obligații de abonat
Dovada de existență - dovada care dovedește că un obiect a existat la o anumită dată/timp
Dovada de integritate - dovada că datele nu au fost modificate de când au fost protejate
NOTĂ: O dovadă a existenței necesită și implică o dovadă a integrității.
Cheie privată – una dintre cheile asimetrice care aparţin unui Subiect şi care este folosită numai de acel Subiect. În cazul sistemelor cu chei asimetrice, o cheie privată descrie transformarea unei semnături. În cazul sistemului asimetric de criptare, o cheie privată descrie transformarea care are loc la decriptare. Cheia privată este (1) cheia al cărei scop este decriptarea sau crearea de semnătură pentru uzul exclusiv al proprietarului; (2) acea cheie dintr-o pereche de chei care este cunoscută numai proprietarului
Cheie publică – una dintre cheile perechii de chei asimetrice ale unui Subiect, care poate fi disponibilă publicului. În cazul sistemelor de criptare asimetrică, cheia publică defineşte transformarea de verificare a semnăturii. În cazul criptării asimetrice, cheia publică defineşte transformarea mesajelor la criptare.
Infrastructura cu Cheie Publică (PKI) – arhitectura, tehnicile, practicile și procedurile care contribuie în mod colectiv la implementarea și funcţionarea sistemelor criptografice cu chei publice, bazate pe certificate; PKI constă în hardware, software, baze de date, resurse de reţea, proceduri de securitate și obligaţii legale, legate împreună și care colaborează pentru a furniza și implementa atât serviciile de certificare, cât şi alte servicii asociate infrastructurii (de ex. marcă temporală).
Certificat Calificat pentru Semnătura Electronică – un certificat pentru semnăturile electronice care este emis de un prestator de servicii de încredere calificat și care îndeplinește cerințele prevăzute în Anexa I a Regulamentului (UE) 910/2014;
Certificat Calificat pentru Sigiliul Electronic – certificat pentru un sigiliu electronic care este emis de un prestator de servicii de încredere calificat și care îndeplinește cerințele prevăzute în Anexa III a Regulamentului (UE) 910/2014;

Dispozitiv de Creare a Semnăturilor Electronice Calificate un dispozitiv de creare a semnăturilor electronice care îndeplinește cerințele prevăzute în Anexa II a Regulamentului (UE) 910/2014.
Regulamentul (UE) nr. 910/2014 – REGULAMENTUL (UE) NR. 910/2014 AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE.
Autoritate de Înregistrare – entitate responsabilă în special de identificarea și autentificarea Subiecților certificatelor
Root CA – autoritate de certificare care se află la cel mai înalt nivel în cadrul domeniului TSP și care este utilizată pentru semnarea CA-ului (-urilor) subordonat(e).
Subiect: entitate identificată într-un certificat ca fiind deținătorul cheii private asociate cheii publice din certificat
CA subordonat - autoritate de certificare al cărei certificat este semnat de Root CA sau de un alt CA subordonat.
Beneficiar – persoană juridică sau fizică legată prin contractul cu un furnizor de servicii de încredere de toate obligațiile Beneficiarului
Marcă temporară - date în formă electronică care leagă alte date electronice de un anumit moment, demonstrând că aceste date au existat la acel moment
Autoritate de marcare temporală - furnizor de servicii de încredere care emite mărci temporale utilizând una sau mai multe unități de marcare temporală
Serviciu de marcare temporală - serviciu de încredere pentru emiterea de mărci temporale
Unitate de marcare temporală - set de hardware și software care este gestionat ca o unitate și are o singură cheie de semnare a mărcii temporale activă la un moment dat
Prestator de servicii de încredere – o persoană fizică sau juridică ce furnizează unul sau mai multe servicii de încredere, fie ca furnizor de servicii de încredere calificate, fie ca furnizor de servicii de încredere ne-calificate;
Listă de încredere - listă care furnizează informații cu privire la statutul și istoricul statutului serviciilor de încredere din partea prestatorilor de servicii de încredere în ceea ce privește conformitatea cu cerințele aplicabile și cu dispozițiile relevante ale legislației aplicabile.
NOTĂ: În contextul statelor membre ale Uniunii Europene, astfel cum se specifică în Regulamentul (UE) nr. 910/2014, se referă la o listă a unui stat membru al UE care include informații referitoare la furnizorii de servicii de încredere calificați pentru care este responsabil, împreună cu informații referitoare la serviciile de încredere calificate furnizate de aceștia.
Date de validare - date care sunt utilizate pentru validarea unei semnături digitale

1.6.2 Acronime

AUG Obiectiv de augmentare
CA Autoritatea de certificare
CARL Lista de revocare a autorității de certificare
CRL Listă de revocare a certificatelor
DN Nume distinct
EUMS Statul membru al Uniunii Europene
NIMB Institutul Național de Metrologie București
OCSP Protocolul privind starea certificatelor on-line
OVR Global
PDS Păstrarea semnăturilor digitale
PGD Păstrarea datelor generale
PKI Infrastructură de chei publice
PO Obiect de conservare
POC Container de obiecte de conservare
PPMB Organism de gestionare a politicilor și procedurilor
PPPS Declarație privind politicile, practicile și procedurile
PSP Furnizor de servicii de conservare
QES Semnătură electronică calificată sau sigiliu electronic calificat
QPS Serviciu Calificat de Păstrare (Qualified Preservation Service)
QSCD Dispozitiv de creare a semnăturii electronice calificate
RA Autoritate de înregistrare
RSA Algoritm criptografic asimetric Rivest, Shamir, Adleman
SCVP Protocol de validare a certificatelor bazat pe server
SigS Serviciul de creare a semnăturii digitale
SubDO Submission Data Object
TS Serviciu de încredere
TSA Autoritate de ștampilare a timpului
TSP Furnizor de servicii de încredere
UTC Timp universal coordonat
ValS Serviciul de validare
WOS fără stocare
WST cu stocare
WTS cu stocare temporară

2 Publicare și responsabilități Depozitar

certSIGN publică PPPS-urile cel puțin anual, chiar dacă nu sunt schimbări.
Toate procedurile sunt planificate annual pentru revizuire si actualizare.

2.1 Depozitar

Depozitarul este disponibil on-line: https://www.certsign.ro/depozitar. Acesta conține:

- Declaratia de Politici, Practici și Proceduri pentru serviciul QPS al certSIGN
- Termenii și condițiile privind utilizarea serviciului QPS

Depozitarul este gestionat și controlat de certSIGN. certSIGN se angajează:

- Să asigure publicarea şi arhivarea PPPS,
- Să asigure accesul permanent la informaţiile din Depozitar pentru Autorităţile certSIGN, Beneficiari și Entităţile Partenere,
- Să asigure accesul sigur și controlat la informațiile din Depozitar.

2.2 Publicarea informațiilor despre serviciul QPS

Disponibilitatea

Disponibilitatea depozitarului de documente este proiectată să depășească 99,8% din programul de lucru - definit ca 24 de ore pe zi, șapte zile pe săptămână, cu excepția perioadelor planificate de întreținere.

Perioadele planificate de întreținere vor fi anunțate pe https://www.certsign.ro cu cel puțin 24 de ore în avans.

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

2.3 Timpul sau frecvența publicării

Informațiile publicate de certSIGN sunt actualizate anual sau la următoarele evenimente:

- Actualizări PPPS,
- Rapoartele auditurilor realizate de instituții autorizate – când le primește certSIGN;
- Informațiile suplimentare – după fiecare actualizare.

2.4 Controlul accesului la Depozitare

Toate informațiile publicate de certSIGN în Depozitar la adresa https://www.certsign.ro/depozitar/ sunt accesibile publicului.
certSIGN a implementat mecanisme logice și fizice de protecţie împotriva adăugării, ştergerii și modificării neautorizate a informaţiilor publicate în Depozitar.
Beneficiarii și Entitățile Partenere au acces doar read-only prin intermediul Internetului la toate depozitarele menționate în secțiunea 2.1.
certSIGN poate lua măsuri rezonabile de protecție împotriva și pentru prevenirea utilizării abuzive a depozitarului, a OCSP sau serviciilor de descărcare a CRL.

La descoperirea unor breşe ce afectează integritatea informaţiilor din Depozitar, certSIGN va lua măsurile corespunzătoare pentru a restabili integritatea informaţiilor, va trage la răspundere pe cei vinovaţi și va notifica imediat entităţile afectate.

3 Serviciul de Păstrare pe Termen Lung - QPS

Sarcina principală a serviciului de păstrare pe termen lung este păstrarea valabilității documentelor semnate digital sau a sigiliilor aplicate pe un document electronic.
Prezentul PPPS definește cerințele pentru asigurarea valabilității pe termen lung a semnăturilor și sigiliilor electronice.
certSIGN poate specifica și restricționa formatul semnăturilor sau sigiliilor electronice acceptate, autoritățile de certificare acceptate și orice alt parametru.

3.1 Obiective pentru păstrare

Serviciul de Păstrare a Semnăturilor Electronice pe Termen Lung urmărește diferite obiective de păstrare, care au influență asupra sarcinilor operaționale suportate, și care pot fi utilizate separat sau în combinație:

- **Păstrarea datelor generale (PGD)** oferă o dovadă a existenței pe perioade lungi de timp a obiectului de date prezentat serviciului de păstrare.
- **Păstrarea semnăturilor digitale (PDS)** extinde pe perioade lungi de timp capacitatea de a valida o semnătură digitală, de a-și menține starea de valabilitate și de a obține o dovadă a existenței datelor semnate asociate.
- **Augmentare (AUG)** indică faptul că serviciul de păstrare sprijină îmbunătățirea dovezilor de păstrare prezentate. Augmentarea se face numai în combinație cu celelalte două obiective (PGD sau PDS).

Toate aceste obiective necesită:
- Dovada integrității unui document electronic sau a unei semnături/sigiliu;
- Dovada existenței unui document electronic sau a unei semnături/sigiliu la un moment dat/în trecut;
- Menținerea valabilității semnăturilor/sigiliilor electronice pe perioade lungi de timp;
- Disponibilitatea datelor.

Integritatea datelor este verificată pe parcursul perioadei de păstrare prin intermediul unei dovezi de integritate (hash, semnătură/sigiliu).
Dovada de existență indică faptul că obiectul digital a existat la un anumit moment și este pusă în aplicare prin combinarea unei dovezi de integritate și a unei indicații temporale de încredere (ștampilă calificată de timp).
Pentru a menține statutul de valabilitate al semnăturii/sigiliului electronic, trebuie păstrate și toate elementele necesare pentru a verifica validitatea și a căror disponibilitate nu poate fi garantată în viitor. Acestea pot include certificate, informații de revocare (CRL, răspunsuri OCSP), liste de încredere etc.
Disponibilitatea datelor este asigurată prin utilizarea unor dispozitive de stocare dedicate în două locații diferite, într-o configurație de înaltă disponibilitate, folosind un backend clusterizat care oferă copii în oglindă ale tuturor documentelor și ale meta-datelor asociate.

3.2 Modele de stocare

Păstrarea cu depozitare (WST)
În acest model de stocare, Serviciul QPS stochează obiectele de date, precum și dovezile de păstrare care sunt produse pentru acestea de către serviciul de păstrare. În acest model, Serviciul QPS sprijină exportul și importul de obiecte de păstrare și de dovezi produse de el însuși și de alte servicii de păstrare, cu condiția ca obiectele și dovezile de păstrare să fie compatibile cu formatele acceptate de QPS.
Acest model de stocare este specificat de valoarea ***WithStorage (WST)*** din *PreservationStorageModelType.*

Păstrarea cu depozitare temporară (WTS)
În acest model de stocare, Serviciul QPS nu stochează permanent obiectele de date, dar le stochează numai atâta timp cât este necesar pentru a crea dovezile corespunzătoare. Dovezile de păstrare sunt produse asincron și sunt stocate o perioadă de timp de maxim 5 zile pentru a permite clientului să le recupereze.
Pentru acest model de stocare, clientul trimite Serviciului QPS obiectul de date complet.
Acest model de stocare este specificat de valoarea *WithTemporaryStorage (WTS)* în cadrul *PreservationStorageModelType*.

Păstrarea fără depozitare (WOS)
În acest model de stocare de păstrare, Serviciul QPS nu stochează obiectele de date și dovezile de păstrare sunt produse sincron.
Acest model de stocare este specificat de valoarea *WithoutStorage (WOS)* din *PreservationStorageModelType*.

3.3 Scheme de păstrare

O schemă de păstrare suportă cel puțin un obiectiv de păstrare și funcționează doar cu un model de stocare.
O schemă de păstrare este o descriere destul de abstractă și poate fi implementată de unul sau mai multe profiluri de păstrare, care sunt descrise de elemente de profil care pot fi citite automat. Elementul *Profil* descrie aspectele tehnice ale unui *Profil de păstrare*, care permit unui client să utilizeze interfața de păstrare pentru a comunica cu Serviciul QPS. Setul de profiluri de păstrare acceptate de Serviciul QPS poate fi regăsit utilizând funcția *RetrieveInfo*, expusă de serviciul de păstrare.
Un profil de păstrare conține (trimite la) informații legate de *politici*, care abordează aspecte ale creării și validării dovezilor și validării semnăturii, în cazul în care obiectivul de păstrare este *PDS*. În cazul în care obiectivul de păstrare este *PGD*, datele primite de la client vor fi semnate de către Serviciul QPS (prin intermediul clientului conectat la un serviciu de semnături electronice calificate), urmând apoi aplicarea elementelor definite în profilele de păstrare echivalente, definite pentru obiectivul de păstrare *PDS*.

Schema de păstrare	Obiectivul păstrării	Modelul de stocare	Evidențe/Dovezi de păstrare
pds+wst+aug	PDS & AUG	WST	PAdES Document Time-Stamp[2]
pgd+wst+aug	PGD & AUG	WST	PAdES Document Time-Stamp[2]
pds+wts+aug	PDS & AUG	WTS	PAdES Document Time-Stamp[2]
pgd+wts+aug	PGD & AUG	WTS	PAdES Document Time-Stamp[2]
pds+wos+aug	PDS & AUG	WOS	PAdES Document Time-Stamp[2]
pgd+wos+aug	PGD & AUG	WOS	PAdES Document Time-Stamp[2]

3.4 Politici de păstrare pe termen lung
Serviciul de păstrare al certSIGN este identificat prin următorul OID: 1.3.6.1.4.1.25017.5.
Serviciul de păstrare al certSIGN suportă următoarele politici de bază:

- **OID 0.4.0.19511.1.2** – **Calificate** este politica aplicată atunci când cerința explicită este pentru păstrarea semnăturilor/sigillilor calificate, așa cum este definită în Regulamentul EU Nr.910/2014 - *itu-t(0) identified-organization(4) etsi(0) pres-service-policies(19511) policy-identifiers(1) qualified (2).*

[2] *Conform ETSI EN 319 142-1*

Fiecare politică este aplicată în cadrul unui profil de păstrare, cu obiective de păstrare specificate, în cadrul unui model de stocare, care aplica un set specific de operații pe formate specificate (cu detaliere la capitolul 7):
- 1.3.6.1.4.1.25017.5.2.1 Cu semnătură digitală și stocare
- 1.3.6.1.4.1.25017.5.2.2 Cu semnătură digitală și stocare temporară
- 1.3.6.1.4.1.25017.5.2.3 Cu semnătură digitală și fără stocare
- 1.3.6.1.4.1.25017.5.2.4 Schema generală de păstrare cu stocare a datelor
- 1.3.6.1.4.1.25017.5.2.5 Schemă generală de păstrare a datelor cu stocare temporară
- 1.3.6.1.4.1.25017.5.2.6 Schema generală de păstrare a datelor fără stocare

Politica de creare a dovezilor de păstrare aplicate și o politică recomandată de validare a probelor de păstrare este anunțată în elementul profil/politică aplicabil, cu tipul egal cu următoarele URI:
- http://uri.etsi.org/19512/policy/preservation-evidence - general aplicabil
- http://uri.etsi.org/19512/policy/signature-validation - aplicabil doar la păstrarea semnăturilor/sigillior digitale (PDS) când datele de validare nu sunt furnizate de Beneficiar.

Formatele datelor de intrare, acceptate de serviciul QPS sunt: pdf, PAdES.
Formatele datelor de ieșire, suportate de serviciul QPS sunt: PAdES-LTA (cu dovadă de păstrare de tip PAdES Document Timestamp, conform cu ETSI EN 319 142-1).
Politicile de validare a semnăturii utilizate sunt descrise în "certSIGN Paperless Validation Politici, Practici și Proceduri pentru Serviciul de Validare Semnături/Sigilii Calificate": https://www.certsign.ro/ro/document/politici-si-practici-pentru-serviciul-paperless-validation/

3.5 Procesul de generare a dovezilor de păstrare

Autoritatea de păstrare permite arhivarea semnăturilor electronice și implementează tehnologii capabile să extindă rezistența semnăturilor electronice pe termen lung, dincolo de perioada de validitate tehnologică a acestora. Autoritatea de păstrare se integrează cu Autoritatea de Validare, pentru obținerea elementelor de validare necesare garantării pe termen lung a semnăturilor electronice și asigurării procesului de validare a acestora.
Autoritatea de păstrare permite gestiunea semnăturilor aflate în formatele PAdES PDF/A. Pentru garantarea securității și rezistentei în timp a algoritmilor criptografici folositi, Autoritatea de păstrare realizează procesări asupra semnăturilor pentru a genera formate PAdES-B-LT care includ informații de validare (Signatures with Long-Term Validation Material), iar apoi realizează mentenanța semnăturiilor folosind formate mai puternice, precum PAdES-B-LTA (Signatures providing Long-Term Availability and Integrity of Validation Material).
Aceste procesări implică aplicarea unor mărci temporale calificate sau a unor sigilii calificate peste ansamblul dovezilor de păstrare.
Detaliile procesului, procedurilor și algoritmilor de creare și operare a TimeStamp sunt detaliate în „certSIGN Autoritatea de Marcare Temporală 2 Codul de Politici, Practici și Proceduri" : https://www.certsign.ro/ro/document/certsafe-tsa-2-cod-practici-si-proceduri/

3.6 Procesul de validare a dovezilor de păstrare

Autoritatea de Validare a semnăturilor electronice este o componentă centralizată de tip server având capabilități avansate de validare a semnăturilor digitale primite. Pe lângă validarea semnăturii, componenta realizează de asemenea colectarea informațiilor necesare pentru validare, verificarea și adăugarea acestora la nivelul semnăturii în scopul asigurării informațiilor necesare păstrării și validării semnăturilor pe termen lung. Formatele obținute sunt transmise înapoi utilizatorului sau pot fi procesate mai departe la nivelul serviciului de prezervare în scopul arhivarii și garantării pe termen lung. Pentru validarea unei semnături

sunt avute în vedere mai multe aspecte cum ar fi integritatea datelor semnate, disponibilitatea și valabilitatea informațiilor necesare pentru validare, armonizarea cu politicile autorităților de certificare operate la nivelul furnizorilor de certificate, generarea unor formate de semnătura care să asigure materialul necesar validării pe termen lung.
Politicile de validare utilizate sunt descrise în "certSIGN Paperless Validation Politici, Practici și Proceduri pentru Serviciul de Validare Semnături/Sigilii Calificate": https://www.certsign.ro/ro/document/politici-si-practici-pentru-serviciul-paperless-validation/

3.7 Procesul de re-auditare a dovezilor de păstrare

În conformitate cu contractul de servicii semnat cu Beneficiarul, certSIGN poate asigura re-augmentarea periodică a dovezilor de păstrare, prin aplicarea unor mărci temporale calificate sau a unor sigilii calificate peste ansamblul dovezilor de păstrare.
Serviciul de Păstrare utilizează autoritatea certSIGN de marcare temporală (TSA), care emite marcaje temporale (conform ETSI EN 319 422) și serviciul certSIGN de creare a semnăturilor sau sigiliilor (SigS), care emite semnături digitale calificate. Acesta va utiliza și un serviciu de validare (ValS) (conform ETSI TS 119 441 și ETSI TS 119 442), pentru a colecta informații despre calea de certificare și informații de revocare.
Serviciul de Păstrare a Semnăturilor Electronice pe Termen Lung poate utiliza atât un spațiu de stocare intern, cât și un spațiu de stocare extern, aflat sub controlul său, pentru păstrarea pe termen lung a semnăturilor electronice.
În plus, serviciul de păstrare poate apela clientul prin interfața de notificare pentru a-l informa cu privire la evenimentele relevante. Un tip important de eveniment este că un algoritm criptografic aplicat anterior este de așteptat să devină slab (conform cu ETSI TS 119 312) și, prin urmare, clientul și/sau serviciul de păstrare trebuie să efectueze măsuri suplimentare.

3.8 Procesul de export-import set de documente

QPS permite Beneficiarului să solicite pachetul de export-import, care conține datele păstrate, dovezile și toate informațiile necesare pentru validarea dovezilor;
Cererile de pachete de export-import vor fi acceptate după cum urmează:

- prin e-mail: cererea trebuie depusă de la o adresă de e-mail cunoscută și aprobată anterior;
- prin prezență fizică: orice persoană care are o împuternicire formală de a reprezenta

Beneficiarul poate depune o cerere la sediul certSIGN.
Pentru fiecare cerere primita se va deschide un ticket cu toate detaliile, pentru monitorizare.
Importul unor cantități mari de documente de pe diferite platforme necesită o abordare diferită. Formatul documentelor este conform cu Anexa G din ETSI TS 119 512.
Documentele trebuie să fie prezente în forma lor originală împreună cu dovezile de păstrare.
Serviciul de import trebuie să revalideze datele și să verifice dovezile de păstrare pentru acuratețe, după care marchează din nou dovezile cu marca temporală a certSIGN.
QPS poate exporta toate documentele unui Beneficiar și poate furniza atât documentele originale cât și care dovezile de păstrare asociate cu acestea.

4 Cerințe operaționale privind ciclul de viață QPS

Acest capitol descrie procedurile de bază care se aplică tuturor activităților operaționale necesare operării și menținerii serviciilor de păstrare QPS furnizate de certSIGN.

O descriere detaliată a procedurilor referitoare la serviciile componentelor PKI (CA-uri, RA-uri, CRL Signers, Responder OCSP etc.) și persoanele/rolurile implicate în procesul operațional al acestor componente este inclusă în documentația internă confidențială.

certSIGN QPS include următoarele activități operaționale generice:

a) Înregistrare Beneficiar QPS - contractare serviciu;
b) Încărcare semnături/sigilii sau documente în vederea păstrării pe termen lung;
c) Verificarea situației curente a semnăturilor/sigiliilor sau documentelor;
d) Menținerea valabilității pe termen lung a semnăturilor/sigiliilor sau documentelor;
e) Actualizarea semnăturilor/sigiliilor sau documentelor păstrate
f) Descărcarea/Afișarea semnăturilor/sigiliilor sau documentelor păstrate;
g) Ștergerea de semnături/sigilii sau documente păstrate;
h) Încetarea contractului de păstrare.

Serviciul QPS oferă următoarele:

1. Beneficiarul poate încărca documente electronice în arhiva QPS operată de certSIGN.
2. certSIGN QPS păstrează în siguranță semnăturile digitale acceptate și/sau documentele electronice asociate și materialul de validare pe termen lung - și asigură pe întreaga perioadă de păstrare că:
   - numai persoanele autorizate au acces la datele păstrate;
   - beneficiarul îndreptățit are acces continuu la datele păstrate;
   - datele păstrate nu pot fi modificate sau șterse fără autorizație.
3. certSIGN QPS asigură menținerea valabilității pe termen lung a semnăturilor și sigiliilor electronice, de sine stătătoare sau plasate pe documentele păstrate.
4. QPS asigură lizibilitatea pe termen lung a semnăturilor din documente, în timpul perioadei de păstrare. Perioada de păstrare este de obicei de 30 de ani, cu excepția cazului în care valabilitatea contractului de servicii încetează înainte de sfârșitul acestei perioade.
5. Beneficiarul are acces permanent la documentele, semnăturile și sigiliile plasate de acesta în arhiva QPS și la materialul de validare pe termen lung corespunzător și le poate descărca.
6. După primirea datelor de intrare de la Beneficiar, pe baza unui acord individual, QPS verifică semnăturile sau sigiliile digitale furnizate separat sau pe documentele furnizate, validează și/sau completează materialul de validare pe termen lung, plasează ștampile electronice de timp pe materialul de validare pe termen lung și salvează totul.
7. La cererea Beneficiarului, QPS șterge semnăturile/ștampilele și/sau documentele din depozitul său de stocare.

Implementarea de către certSIGN a serviciului de păstrare respectă „Protocoalele operaționale și de notificare" descrise în capitolul 8 din ETSI TS 119 511 și detaliate în ETSI TS 119 512. certSIGN este în conformitate cu cerințele „Procesului de păstrare" din capitolul 9 din ETSI TS 119 511.
Ca QTSP, certSIGN respectă cerințele din anexa A la ETSI TS 119 511 pentru un serviciu de păstrare calificat al UE.

4.1 Procesul de înregistrare și contractare serviciu QPS

Întreg procesul este gestionat de o entitate specifică numită Autoritatea de Înregistrare sau RA, care este operată de certSIGN în mod direct sau bazându-se pe un terț, în conformitate cu legislația națională.

certSIGN poate delega atributiile de identificare și înregistrare a beneficiarilor către terțe părți care pot asigura metode/proceduri ce oferă un nivel de asigurare echivalent Autorității de Înregistrare. În orice situație, certSIGN, în calitate de furnizor de servicii de incredere, își asumă răspunderea pentru actele sau omisiunile tuturor agenților terți.

Identificarea Beneficiarului

RA este responsabilă de verificarea următoarelor elemente:
- Identitatea Beneficiarului, pe baza unui act de identitate
- Atribute ale Beneficiarului, ca persoană fizică sau persoană juridică,
- Cererea Beneficiarului pentru serviciul solicitat.

Procesul de identificare și înregistrare este realizat în conformitate cu regulile și metodele descrise în PPPS, în procedurile RA și în legislația aplicabilă.

Beneficiarului i se pun la dispoziție următoarele informații și documente:
- Acord contractual (sau adresa online a acestora)
- Termeni și Condiții (sau adresa online a acestora)
- Adresa online a PPPS, notificări sau alte documente necesar a fi furnizate de/către Beneficiar (definite în Acordul contractual cu Beneficiarul).

Semnarea Acordului contractual

După verificarea identității Beneficiarului, RA îl informează pe acesta cu privire la drepturile și obligațiile sale, precum și la opțiunile și detaliile acordului de furnizare a serviciilor de păstrare pe termen lung.
Responsabilitatea entității RA este de a colecta informațiile necesare pentru validarea necesităților Beneficiarului și pentru ghidarea acestuia în vederea alegerii configurațiilor dorite ale serviciului QPS. Totodată RA prezintă Beneficiarului modul de utilizare al serviciului QPS.
Operatorul RA efectuează o verificare a documentelor și verifică dacă informațiile înscrise sunt complete și corecte.

Prin semnarea Acordului contractual și acceptarea Termenilor și Condițiilor, Beneficiarul înțelege și acceptă următoarele:
- responsabilitatea sa ca informațiile furnizate către RA sunt corecte, complete, valabile și actualizate,
- că certSIGN păstreaza pe perioada derulării contractului, dar și pentru 3 ani de la data încheierii acestuia, toate informațiile referitoare la înregistrare și înscriere, la cererea de păstrare și la toate activitățile legate de actualizarea și mentenanța datelor păstrate,
- că, în cazul în care certSIGN (în calitate de TSP pentru servicii de păstrare) își încetează activitatea, aceste date pot fi transferate către o terță parte, cu acordul părților,
- recunoaște drepturile, obligațiile și responsabilitățile certSIGN și ale altor participanți la PKI, astfel cum sunt definite în Acordul cu Beneficiarul și în legislațiile naționale,

- că Beneficiarul are obligația de a informa certSIGN cu privire la orice schimbare sau eveniment care poate afecta validitatea datelor păstrate.

Procesul de înregistrare
Procesul de înregistrare se desfășoară în cadrul RA.
RA verifică contractul semnat și completează datele de înregistrare în sistemul de păstrare certSIGN. RA este responsabilă de înregistrarea corectă a opțiunilor Beneficiarilor în vederea configurării corecte a serviciului QPS.

După finalizarea procesului de înregistrare Beneficiarul este înștiințat (prin telefon sau email) că poate începe utilizarea serviciilor QPS și primește atât linkul de acces la QPS cât și credențialele contului său (acces multifactor).

4.2 Încărcarea și validarea documentelor (PreservePo)

QPS acceptă încărcarea semnăturilor/sigiliilor și/sau a documentelor care urmează să fie păstrate numai după autentificarea Beneficiarului în cadrul unei proceduri securizate.
Procedura de încărcare asigură integritatea și confidențialitatea semnăturilor/sigiliilor și a documentelor încărcate, și specifică opțiunile disponibile pe parcursul procesului.
Contractul de servicii semnat specifică în mod clar ce tip de semnătură/sigiliu și ce format de fișier este acceptat de QPS, modul în care se verifică semnăturile și sigiliile electronice și în ce condiții se acceptă documentele electronice.
Documentele fără semnătură/sigiliu, sunt securizate prin sigilare cu un sigiliu certSIGN.
Valabilitatea semnăturilor electronice sau a sigiliilor de pe documentele primite este verificată cu ajutorul serviciului de validare certSIGN (QVSA). Verificarea se poate baza pe materialul de validare parțială sau completă (pe termen lung) atașat semnăturilor sau sigiliilor electronice. Orice informație necesară pentru validare este colectată de QPS și păstrată.
După procesarea materialelor de validare, QPS aplică un sigiliu temporal calificat pe fiecare material de validare. Conectarea cu orice serviciu extern se face prin autentificare mutuală.
QPS verifică semnăturile/sigiliile și documentele primite cât mai curând posibil, dar cel târziu în termen de 24 ore de la primire și trimite o confirmare către Beneficiar că materialul de validare a fost verificat cu succes și că a acceptat documentele.
În cazul în care procesul este întrerupt undeva, QPS notifică beneficiarul printr-un mesaj de eroare. Pe baza mesajului de eroare trebuie să se poată identifica în mod clar care semnătură/sigiliu sau document este implicat și care a fost motivul respingerii.
În cazul în care verificarea privind acceptarea semnăturii/sigiliului sau a documentului nu ajunge la Beneficiar în termenul stabilit, acesta trebuie să considere că QPS NU a acceptat semnătura/sigiliul sau documentul pentru care nu există confirmarea acceptării.
certSIGN este singurul responsabil pentru păstrarea semnăturii/sigiliului sau a documentului și pentru asigurarea credibilității pe termen lung a semnăturilor și sigiliilor electronice incluse în cazul trimiterii unei confirmări pozitive.

4.3 Raportare informații (RetriveTrace)

La cererea Beneficiarului, QPS emite un raport în legătură cu informații despre semnăturile/ sigiliile sau documentele încărcate. In funcție de solicitare raportul poate include:

1. Confirmarea că semnăturile/sigiliile sau documentele date au hash-ul neschimbat, deci sunt identice cu semnăturile/sigiliile sau documentele cu același hash prezentate de Beneficiar.
2. Momentul acceptării semnăturilor/sigiliilor sau documentelor în QPS.
3. Dimensiunea fișierului
4. Numărul de versiuni ale documentelor

QPS eliberează raportul la cerere.
Nu este necesară cunoașterea semnăturilor/sigiliilor sau a documentelor stocate pentru emiterea raportului, acesta fiind emis pe baza identificatorului de obiect păstrat (POID).

4.4 Menținerea valabilității pe termen lung

Pentru semnăturile/sigiliile și documentele transmise pentru păstrare pe termen lung în arhiva QPS, certSIGN asigură menținerea valabilității acestora, conform contractului, prin augmentare periodică a materialelor de validare – cu aplicarea unei ștampile de marcă temporală calificată pe ultima versiune a obiectului păstrat, utilizând algoritmi actualizați.
În urma fiecărei operațiuni de augmentare efectuată conform planificării certSIGN va informa Beneficiarul printr-un raport de stare.

4.5 Disponibilitatea documentelor (RetrivePO & RetriveTrace)

certSIGN se asigură că Beneficiarul poate descărca semnăturile/sigiliile sau documentele sale păstrate în arhivă și materialul de validare pe termen lung corespunzător în perioada de valabilitate a contractului de servicii. De asemenea, Beneficiarul poate solicita un istoric al operațiunilor care au fost executate asupra documentelor sale.
Beneficiarul are acces la rapoarte, semnături/sigilii sau documente și la materialul de validare pe termen lung păstrat în arhiva QPS doar prin intermediul unui canal securizat.
certSIGN se asigură că fiecare Beneficiar are acces doar la semnăturile/sigiliile sau documentele sale și la materialul de validare pe termen lung la care are dreptul real de acces.

4.6 Descărcarea documentelor (RetrivePO)

certSIGN QPS pune la dispoziția Beneficiarului, în funcție de acordurile încheiate, ca, prin utilizarea dispozitivelor software și hardware ale QPS, să poată descărca documentele păstrate, stocate de QPS.

4.7 Ștergerea documentelor (DeletePO)

certSIGN QPS pune la dispoziție ștergerea selectivă a semnăturilor/sigiliilor sau a documentelor și a tuturor materialelor de validare corespunzătoare păstrate în arhivă, la cererea beneficiarului. Prin ștergere se înțelege ștergerea fizică a semnăturilor/sigiliilor sau documentelor păstrate și suprascrierea acestora astfel încât să nu poată fi restaurate ulterior (sau doar cu cheltuieli financiare nerealiste) de pe suportul de date. Ștergerea se efectuează în întregul sistem al certSIGN QPS, iar în timpul ștergerii se va distruge fiecare copie păstrată a semnăturilor/sigiliilor sau documentelor.
certSIGN specifică în Contractul de beneficiar modalitatea și condițiile de admitere și prelucrare a cererii de ștergere.

4.8 Încetarea contractului de servicii

În cazul rezilierii contractului, certSIGN pune la dispoziția Beneficiarului sau a altei persoane îndreptățite semnăturile/sigiliile sau documentele și materialele de validare pe termen lung comandate de Beneficiar pentru a fi păstrate pentru descărcare.
După rezilierea contractului, certSIGN șterge semnăturile/ sigiliile sau documentele și materialul de validare pe termen lung care corespund Beneficiarului.

5 Facilitate, Management și Controale Operaționale

În calitate de furnizor de servicii de încredere, certSIGN pune securitatea în centrul activităților sale. Pentru ca toate activele, activitățile și serviciile sale să fie sigure, certSIGN a implementat, menține și îmbunătățește continuu un sistem informatic de management al securității certificat ISO 27001:2022. În acord cu cerințele acestui cadru de securitate, toate activitățile de securitate încep cu o evaluare a riscului, pentru a identifica și clasifica toate activele informaționale, pentru a evalua riscurile la care sunt expuse și pentru a determina controalele tehnice, manageriale, organizatorice și procedurale necesare. certSIGN menține un inventar al tuturor activelor informaționale și le atribuie o clasificare în concordanță cu evaluarea riscurilor.

Toate acele controale aferente activelor și activităților TSP sunt conforme cu cerințele aplicabile din următoarele standarde:

- ETSI EN 319 401, Cerințele generale privind politicile Furnizorilor de Servicii de Încredere,
- ETSI TS 119 511, Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques
- ETSI TS 119 512, Protocols for trust service providers providing long-term data preservation servicesPhysical Controls

5.1 Controale fizice

Rețeaua de sisteme de calcul, terminalele operatorilor şi resursele informaţionale ale certSIGN se află într-o zonă dedicată, protejată fizic împotriva accesului neautorizat, distrugerilor sau perturbării activităţii. Aceste locaţii sunt monitorizate. Fiecare intrare și ieşire este înregistrată în jurnalul de evenimente (log-urile sistemului); stabilitatea sursei de electricitate precum şi temperatura și umiditatea sunt de asemenea monitorizate și controlate.

5.1.1 Amplasarea și construcția sediului

Toate operațiunile TSP certSIGN sunt realizate într-un mediu fizic protejat cu controale bazate pe evaluarea riscurilor care anticipează, previn, detectează și contracarează materializarea riscurilor pentru activele sale. De asemenea, menținem facilități de recuperare în caz de dezastru pentru operațiunile noastre, facilități care sunt protejate prin măsuri de securitate fizică similare celor implementate la facilitatea noastră primară. Toate controalele de securitate fizică puse în aplicare de certSIGN sunt în conformitate cu standardele ISO 27001 și 27002 și sunt descrise în detaliu în politicile și procedurile de securitate. Printre cele mai importante controale de securitate sunt:

- Un perimetru clar definit și protejat, prin care sunt controlate toate intrările și ieșirile;
- Componentele critice sunt protejate cu mai multe perimetre;
- Un sistem de control de intrare, care admite numai acele persoane autorizate în mod corespunzător să intre în zonă;
- Monitorizare cu echipaj uman și electronic a intruziunilor neautorizate, în orice moment;
- Personalul care nu se regăsește pe lista de acces este însoțit și supravegheat în mod corespunzător;
- Un jurnal de acces este întreținut și controlat periodic;
- Echipamentul este întreținut în mod corect pentru a-i asigura disponibilitatea continuă și integritatea.

5.1.2 Accesul fizic

Accesul fizic în cadrul certSIGN este controlat și monitorizat de un sistem de alarmă integrat. certSIGN dispune de sisteme de prevenire a incendiilor, sisteme de detectare a intruşilor şi sisteme de alimentare cu energie electrică în caz de urgenţă.

Sediul certSIGN este accesibil publicului în fiecare zi lucrătoare între 09:00 şi 18:00. În restul timpului (inclusiv în zilele nelucrătoare), accesul este permis numai persoanelor autorizate de către conducerea certSIGN.

Vizitatorii locaţiilor aparţinând certSIGN trebuie să fie însoţiţi permanent de personal autorizat.

Zonele ocupate de certSIGN se împart în:

- Zona de birouri,
- Zonele IT,
- Zona operatorilor
- Zona administratorilor,
- Zona de dezvoltare și testare.

Zonele IT sunt echipate cu un sistem de securitate monitorizat, compus din senzori de mişcare, efracţie şi incendiu. Accesul în această zonă este permis numai personalului autorizat. Monitorizarea drepturilor de acces se face folosind carduri de identitate și cititoare, montate lângă punctul de acces. Fiecare intrare și ieşire în și din zonă este înregistrată automat în jurnalul de evenimente.

Accesul în **zona operatorilor** se face pe baza unui card electronic și a unui cititor de card. Deoarece toate informaţiile sensibile sunt protejate prin folosirea unor seifuri, iar accesul la terminalele operatorilor şi administratorilor necesită autorizarea prealabilă a acestora, securitatea fizică în această zonă este considerată ca fiind adecvată. Cheile de acces pot fi ridicate numai de personalul autorizat. Zona este accesibilă exclusiv personalului certSIGN şi persoanelor autorizate; prezenţa în zonă a celor din urmă le este permisă doar dacă sunt însoțiți de un angajat certSIGN.

În această zonă nu este permisă prezenţa persoanelor neînsoţite. Programatorii și dezvoltatorii nu au acces la informaţii sensibile. Dacă este necesar accesul la astfel de informații, el este permis doar în prezenţa administratorului de securitate. Proiectele în curs de implementare şi software-ul aferent sunt testate în mediul de dezvoltare al certSIGN.

5.1.3 Alimentarea cu curent și aerul condiționat

Toate zonele sunt prevăzute cu aer condiționat. În zona serverelor, echipamentele de aer condiționat sunt redundante, iar temperatura este monitorizată atât automat (cu o alertă când un anumit nivel este atins) cât și manual. Din momentul întreruperii alimentării cu energie, sursele de electricitate de urgenţă (UPS) permit continuarea neperturbată a activităţii până la intervenţia automată a grupului electrogen al clădirii. Infrastructura de curent electric este concepută astfel încât la o întrerupere a curentului în clădire toate activitățile să fie disponibile pentru cel puțin 24 de ore cu ajutorul generatorului diesel. Fiecare server, echipament de rețea și toate calculatoarele angajaților care desfășoară activități importante pentru activitățile TSP sunt conectate la UPS-uri. Principalele componente ale securității fizice sunt de asemenea conectate la UPS-uri și la generatorul diesel.

5.1.4 Expunerea la apă

Riscul de inundație în zona serverelor este controlat prin rack-uri. Toate echipamentele sunt plasate în rack-uri la o distanță de minim 15 cm de la sol. În plus, toate camerele serverelor sunt monitorizate cu senzori de umiditate.

5.1.5 Prevenirea și protecția împotriva incendiilor

Locaţia certSIGN dispune de sistem de prevenire și protecţie împotriva incendiilor în conformitate cu standardele și reglementările în domeniu. Ușile camerelor serverelor sunt certificate ca ignifuge și toate culoarele de acces sunt protejate cu substanțe rezistente la foc.

5.1.6 Depozitarea mediilor de stocare a informaţiilor

În conformitate cu cerințele politicii de clasificare a informațiilor, mediile care conțin date sau informații de rezervă sunt manipulate și stocate în siguranță în interiorul facilității primare. Mediile de backup sunt stocate în siguranță, într-o locație separată de locația principală, cu același nivel de securitate ca locația principală. Mediile care conțin date sensibile sunt distruse securizat atunci când nu mai sunt necesare.

5.1.7 Aruncarea deșeurilor

După expirarea perioadei de păstrare, hârtia și suporturile electronice care conțin informații semnificative pentru securitatea certSIGN sunt distruse.

Ștergerea securizată se face în conformitate cu politica de securitate a informațiilor a certSIGN.

5.1.8 Stocarea copiilor de siguranță în afara locației

Stocarea în afara locației cuprinde, de asemenea, arhive, copii curente ale informațiilor procesate de sistem și kit-urile de instalare ale aplicațiilor certSIGN. Aceasta permite recuperarea de urgență a fiecărei activități certSIGN în termen de 24 de ore în sediul certSIGN sau într-un sediu auxiliar.

5.2 Controale procedurale

5.2.1 Roluri de încredere

Toate rolurile implicate în furnizarea serviciilor certSIGN sunt atribuite către angajați certSIGN.

Toți angajații certSIGN se angajează, sub semnătură, să nu aibă conflicte de interese cu certSIGN, să păstreze confidențialitatea informațiilor și să protejeze datele cu caracter personal.

certSIGN asigură o separare a sarcinilor pentru funcțiile critice pentru a împiedica o persoană rău intenționată, să folosească sistemele TSP fără a fi detectată.

Securitatea informațiilor prelucrate de certSIGN și a serviciilor sale este pusă în aplicare prin controale procedurale legate de controlul accesului. Astfel, accesul la informații și la funcțiile de sistem ale aplicațiilor este restricționat în conformitate cu Politica de Control al Accesului. certSIGN administrează drepturile de acces ale operatorilor, administratorilor și auditorilor de sistem, iar administrarea include managementul conturilor utilizatorilor și modificarea la timp sau eliminarea accesului. Sunt furnizate suficiente controale de securitate a calculatoarelor pentru separarea rolurilor de încredere identificate, inclusiv separarea funcțiilor de administrare de securitate și de funcționare. În special, utilizarea de programe utilitare de sistem este limitată și controlată.

certSIGN poate aloca cel puțin următoarele roluri de încredere la una sau mai multe persoane:

- **Ofițer de securitate** – Responsabilitate globală pentru implementarea politicilor şi procedurilor de securitate.
- **Administratorul de sistem (System/Network Administrator)** – Autorizat să instaleze, configureze și să întreţină sistemele de încredere ale TSP. Instalează dispozitivele hardware şi sistemele de operare; instalează şi configurează echipamentele de reţea.
- **System operator (Application Operator/DB Administrator) -** Responsabil de operarea zilnică a sistemelor de încredere ale TSP. Autorizat să execute operaţiile de backup și restaurare a sistemului. Asigură continuitatea copiilor de siguranţă şi a arhivelor bazelor de date şi crearea log-urilor de sistem; administrează bazele de date; are acces la informaţii confidenţiale despre Beneficiari, dar nu are dreptul de a accesa

fizic nici o altă resursă a sistemului; transferă copiile de siguranţă ale arhivei și ale datelor curente către locaţiile desemnate.

- **Ofițer înregistrare** (**Processing Operator**): Responsabil de verificarea informațiilor care sunt necesare pentru înregistrarea în utilizarea serviciilor TSP;
- **Auditor de sistem** – autorizat să acceseze arhivele și log-urile de audit ale sistemelor de încredere ale TSP. Responsabil de efectuarea de audituri interne pentru respectarea PPPS de către TSP.

În cadrul certSIGN, rolul de auditor nu poate fi combinat cu nici un alt rol. Nicio entitate care are un rol diferit de cel de auditor nu poate prelua responsabilităţile auditorului.

Angajaților li se alocă în mod oficial roluri de încredere de către CMMP. Principiul "cel mai mic privilegiu" este aplicat atunci când se configurează privilegiile de acces către rolurile de încredere.

5.2.2 Numărul de persoane necesare pentru fiecare sarcină

Acolo unde controlul dual sau controlul multiplu este necesar, cel putin două persoane distincte, cu roluri de încredere relevante sunt prezente pentru a putea îndeplini operațiunea.

Circumstanțele ce necesită control dual sau multiplu sunt descrise în documentația internă confidențială.

5.2.3 Identificarea și autentificarea pentru fiecare rol

Fiecare angajat certSIGN ce are un rol de încredere este identificat și autentificat la accesarea infrastructurii pentru îndeplinirea rolului său prin mijloace de autentificare cu cel puțin doi factori.

Fiecare cont alocat:

- este unic şi alocat direct unei anumite persoane,
- nu este folosit în comun cu nici o altă persoană,
- este restricţionat conform funcţiei (ce reiese din rolul îndeplinit de persoana respectivă) pe baza software-ului de sistem al certSIGN, a sistemului de operare şi a controalelor de aplicaţii.

Toate acțiunile angajaților care au roluri de încredere sunt urmărite și este asigurată răspunderea deplină.

5.2.4 Rolurile care necesită separarea sarcinilor

certSIGN implementează și impune o separare a rolurilor și a sarcinilor pentru rolurile de Administrator, Operator și Auditor pentru a se asigura că aceeași persoană nu poate deține mai multe roluri. Toate aceste roluri au fișe de post, cu solicitări de abilități și experiențe specifice, definite din punctul de vedere al rolurilor îndeplinite. Se implementează următoarele principii: segregearea rolurilor ți atribuirea de drepturi minim necesare în sisteme. În funcție de cât de sensibile sunt pozițiile ca urmare a atribuțiilor asociate acestora, se stabilesc: nivelele de acces, precum și procedura de verificare a activității precedente ale persoanelor care urmează sa ocupe respectivele poziții, precum și nivelul de instruire și constientizare necesar pentru ele.

Procedurile sunt stabilite și implementate pentru toate rolurile de încredere și administrative care au impact asupra furnizării de servicii.

5.3 Controlul personalului

certSIGN se asigură că persoana care îndeplineşte responsabilităţile funcţiei, conform cu rolul atribuit în cadrul TSP:

- A absolvit cel puţin liceul,

- A inteles și a semnat un contract ce descrie rolul şi responsabilităţile sale în cadrul sistemului,
- A beneficiat de un stagiu de pregătire avansată în conformitate cu obligaţiile și sarcinile asociate funcţiei sale,
- A fost instruit cu privire la protecţia datelor personale şi informaţiilor confidenţiale sau private,
- A semnat un contract ce conţine clauze referitoare la protejarea informaţiilor senzitive ale certSIGN și a datelor confidenţiale şi private ale Beneficiarilor,
- Nu îndeplineşte sarcini care pot genera conflicte de interese.

Rolurile și responsabilitățile de securitate, așa cum sunt specificate în politica certSIGN privind securitatea informațiilor, sunt documentate în fișa postului sau în documentele aflate la dispoziția personalului în cauză.

5.3.1 Calificări, experință și aprobări necesare

certSIGN se asigură că toți angajații care acționează pentru furnizarea de servicii TSP sunt verificați înainte de angajare în ceea ce privește identitatea, încrederea, calificările, cunoștințele de specialitate, experiențe și autorizare necesare și, după caz, pentru a îndeplini roluri de încredere și pentru a îndeplini funcția specifică postului ocupat. Personalul de conducere posedă expertiză și experiență în domeniul tehnologiei PKI și suficientă experiență de management al securității informațiilor și de gestionare a riscurilor pentru a-și îndeplini funcțiile de conducere.

5.3.2 Proceduri de verificare a antecedentelor

certSIGN asigură efectuarea controalelor relevante personalului potențial prin intermediul rapoartelor de stare emise de o autoritate competentă, al declarațiilor de la terți sau al declarațiilor auto-semnate.

5.3.3 Cerinţele de pregătire a personalului

Personalul care îndeplinește roluri și sarcini ca urmare a angajării în cadrul certSIGN trebuie să fie instruit cu privire la:

- Cerințele PPPS,
- Procedurile și controalele de securitate folosite de TSP
- Responsabilităţile ce decurg din rolurile și sarcinile executate în sistem,

După încheierea pregătirii, participanţii semnează un document prin care confirmă familiarizarea lor cu PPPS și acceptă restricţiile și obligaţiile impuse.

5.3.4 Frecvența și cerințele stagiilor de pregătire

Pregătirea descrisă în Capitolul 5.3.3 trebuie repetată sau suplimentată de fiecare dată când apar modificări semnificative în modul de funcționare al TSP certSIGN.

5.3.5 Frecvența și secvența rotației posturilor

Nu se aplică.

5.3.6 Sancțiunile pentru acțiunile neautorizate

certSIGN va lua masuri împotriva celor ce incalcă politicile sau procedurile, realizează acțiuni neautorizate, folosirea neautorizată a autorității și utilizarea neautorizată a sistemelor. Acestea pot include, printre altele, revocarea de privilegii, disciplinare administrativă, sancțiuni reglementate de legislația muncii din România și / sau urmărirea penală.

5.3.7 Cerințele pentru contractanții independenți

Personalul angajat pe baza de contract (servicii externe, dezvoltatori de subsisteme sau aplicaţii etc.) face obiectul unor verificări similare celor efectuate în cazul angajaţilor certSIGN (vezi Capitolul 5.3.1, 5.3.2 și 5.3.3). În plus, personalul angajat pe bază de contract, pe

timpul cât îşi desfăşoară activitatea în locaţia certSIGN, trebuie să fie însoţit permanent de un angajat al certSIGN, cu excepţia celor care au primit avizare din partea administratorului de securitate și care pot accesa informaţii clasificate intern sau în conformitate cu normele legale în vigoare.

5.3.8 Documentația oferită personalului

certSIGN oferă personalului său accesul la următoarele documente:

- PPPS,
- Lista Responsabilităţilor şi obligaţiilor asociate rolului deţinut în sistem
- Politicile și procedurile de securitate

Alte documente relevante (proceduri operaționale, instrucțiuni de lucru, manuale) necesare personalului pentru a-și îndeplini funcțiile specifice legate de furnizarea de servicii de prezervare certSIGN, sunt distribuite în timpul formării inițiale, training-urilor anuale și ori de câte ori este cazul.

5.4 Procedurile de înregistrare a datelor de audit

Pentru gestionarea eficientă a sistemelor și aplicațiilor folosite de certSIGN în activitatea sa în calitate de furnizor de servicii TSP, dar și pentru a permite auditarea acțiunilor angajaților și clienților, toate informațiile cu privire la evenimente importante, generate de sisteme și aplicații sunt înregistrate. Aceste informații, cunoscute în mod colectiv sub numele de log-uri trebuie să fie păstrate în așa fel încât să poată fi accesate de către Entitățile Partenere, auditori și autoritățile de stat oricând au nevoie de ea, pentru a furniza dovezi ale funcționării corecte a serviciilor în scopul procedurilor legale sau pentru a detecta încercările de a compromite securitatea certSIGN. Evenimentele înregistrate sunt arhivate și păstrate într-o locație secundară.

Când este posibil, log-urile sunt create automat. Dacă înregistrările nu pot fi create automat, se vor folosi jurnalele de evenimente pe hârtie. Fiecare înregistrarea în log, electronic sau de mână, este păstrată şi dezvăluită atunci când se desfăşoară un audit, dacă este necesar. Acuratețea temporală a log-urilor este asigurată de un server de timp care este sincronizat cu cel puțin două surse de timp care pot fi sateliți GPS sau UTC (NIMB).

5.4.1 Evenimente Înregistrate

Fiecare activitate critică din punctul de vedere al securităţii certSIGN este înregistrată în log-urile de evenimente şi arhivată. Arhivele sunt depozitate pe medii de stocare ce nu pot fi suprascrise sau distruse cu ușurință (cu excepția cazului în cazul în care sunt transferate pe un suport de păstrare pe termen lung) în perioada de timp în care acestea sunt obligate să fie păstrate. Log-urile de evenimente certSIGN conţin înregistrări ale tuturor activităţilor generate de componentele software din cadrul sistemului. Aceste înregistrări sunt împărţite în trei categorii separate:

- **Loguri de sistem** – conţin informaţii despre cererile clienţilor şi răspunsurile server-ului (sau invers) la nivelul protocolului de reţea (de exemplu http, https); datele concrete care se înregistrează sunt: adresa IP a staţiei sau a server-ului, operaţiunile executate (de exemplu: căutare, editare, scriere etc.) şi rezultatele lor (de exemplu introducerea cu succes a unei înregistrări în baza de date),
- **Erori** – conţin informaţii despre erori la nivelul protocoalelor de reţea și la nivelul modulelor aplicaţiilor;
- **Audit logs**– conţin informaţii specifice serviciilor TSP, de exemplu: cererea de înregistrare, acceptarea documentelor, păstrarea și augmentarea, etc.

Jurnalele de evenimente de mai sus sunt comune fiecărei componente instalate pe un server sau staţie de lucru și au o capacitate prestabilită. Atunci când se depăşeşte această capacitate,

este creată automat o nouă versiune de jurnal. Jurnalul anterior este arhivat şi şters de pe disc.

Fiecare înregistrare, automată sau manuală, conţine următoarele informaţii:

- Tipul evenimentului,
- Identificatorul evenimentului,
- Descrierea evenimentului,
- Data și ora apariţiei evenimentului,
- Identificatorul persoanei responsabile de eveniment.

Toate evenimentele legate de ciclul de viață QPS sunt înregistrate.

Toate cererile și rapoartele referitoare la actualizările de date, precum și acțiunea rezultată sunt înregistrate.

Toate informațiile de înregistrare, inclusiv următoarele sunt înregistrate:

- tipul de document(e) prezentat de către solicitant la înregistrare;
- înregistrarea datelor de identificare unice, numere, sau o combinație a acestora (de exemplu, cartea de identitate a solicitantului sau pașaport) a documentelor de identificare, dacă este cazul;
- locul de depozitare al copiilor cererilor și a documentelor de identificare, inclusiv contractul semnat de Beneficiar;
- orice opțiuni specifice din contract (de exemplu, acceptarea serviciilor)
- Identitatea entității care acceptă cererea;
- Metoda utilizată pentru validarea documentelor de identificare,

În plus, certSIGN păstrează jurnalele interne ale tuturor evenimentelor de securitate și toate evenimentele operaționale relevante din întreaga infrastructură, oricare ar fi elementul tehnic, dar fără a se limita la:

- Modificări ale politicii de securitate;
- Pornirea și oprirea sistemelor;
- Întreruperile;
- Erorile de sistem și de hardware;
- Activitățile firewall-urilor și ale routerelor;
- Încercările de acces în sistemul PKI;
- Accesul fizic al personalului și al altor persoane la părțile sensibile ale oricărui site securizat sau zonă;
- Back-up și restaurare;
- Raportul testelor de recuperare în caz de dezastru;
- Inspecții de audit;
- Actualizări și modificări ale sistemelor, software-ului și infrastructurii;
- Intruziuni de securitate și tentative de intruziune.

Accesul la log-uri este permis exclusiv pentru ofițerul de securitate, personal special nominalizat și auditori, prin cerere adresata pe email sau in format hartie catre ofiterul de securitate.

Confidențialitatea informațiilor Beneficiarului este menținută.

5.4.2 Frecvența procesării jurnalelor de evenimente

Jurnalele de audit sunt prelucrate în mod continuu și/sau ca urmare a unei alarme sau eveniment anormal. Jurnalele de audit sunt arhivate și copii de siguranță sunt făcute în mod continuu.

5.4.3 Perioada de păstrare a log-urilor de audit

Înregistrările evenimentelor sunt stocate în fişiere pe discul sistem până când ajung la capacitatea maximă permisă. În tot acest timp sunt disponibile on-line, la cererea fiecărei

persoane sau proces autorizat. După depăşirea spaţiului alocat, jurnalele sunt păstrate în arhive și pot fi accesate numai off-line, de la o anumită stație de lucru.

Jurnalele arhivate sunt păstrate cel puțin 3 ani.

5.4.4 Protecția jurnalelor de evenimente

Fișierele jurnalelor sunt protejate în mod corespunzător printr-un mecanism de control al accesului. Un sistem de protecție adecvată împotriva modificărilor și ștergerii jurnalelor de audit este pus în aplicare astfel încât nimeni nu poate modifica sau șterge înregistrări de audit, cu excepția transferului pe un mediu de păstrare pe termen lung, în scopuri de arhivare. Doar ofițerul de securitate, administratorii sau un auditor poate revizui un jurnal de evenimente. Accesul la jurnalul de evenimente este configurat în așa fel încât:

- Doar entităţile de mai sus au dreptul să citească înregistrările jurnalului,
- Platforma centrală de jurnale arhivează sau șterge automat fișierele (după arhivarea lor) care conțin evenimentele înregistrate,
- Este posibilă detectarea oricărei violări de integritate; acest lucru asigură faptul că înregistrările nu conţin lacune sau falsuri,
- Nici o entitate nu are dreptul să modifice conţinutul unui jurnal.

În plus, procedurile de protecţie a jurnalului sunt implementate în aşa fel încât, chiar și după arhivarea jurnalului, este imposibil să ştergi înregistrări, sau să ştergi jurnalul înaintea expirării perioadei de retenţie a jurnalului.

5.4.5 Procedura de backup a log-urilor de Audit

Politicile de securitate ale certSIGN cer ca jurnalul de evenimente să fie salvat periodic într-o copie de rezervă. Aceste copii de rezervă sunt păstrate în locațiile auxiliare ale certSIGN. Copiile de rezervă ale fișierelor-jurnal și ale pistelor de audit sunt salvate în conformitate cu procedurile interne.

5.4.6 Sistemul de colectare a datelor pentru audit (intern vs extern)

Toate log-urile generate de servere, dispozitive de rețea, echipamente de Securitate, aplicații sunt trimise periodic la o platforma centrală, al cărei scop este să:

- Colecteze
- Depoziteze
- Analizeze
- Coreleze
- Arhiveze
- Genereze copii de siguranță pe termen lung

5.4.7 Notificarea sursei care a generat

Nu se aplică.

5.4.8 Evaluări de vulnerabilitate

Întreaga infrastructură face obiectul evaluării vulnerabilității ca parte a procedurilor de evaluare internă a riscurilor și de gestionare a riscurilor de către certSIGN .

Pentru a se asigura că toate activele, activitățile și serviciile sale sunt sigure, certSIGN a implementat, menține și îmbunătățește continuu sistemul de management al securității informațiilor certificat ISO 27001: 2022. În conformitate cu cerințele prezentului cadru de securitate, toate activitățile de securitate încep cu o evaluare a riscurilor pentru a identifica și a clasifica toate activele informaționale, pentru a evalua riscurile la care sunt expuse și pentru a determina controalele tehnice, manageriale, organizaționale și procedurale necesare. certSIGN menține un inventar al tuturor activelor informaționale și le atribuie o clasificare compatibilă cu evaluarea riscurilor.

5.5 Arhivarea înregistrărilor

Este necesar ca toate datele și fişierele referitoare la înregistarea informaţiior asociate securității sistemului, cererile trimise de Beneficiari, informaţiile despre Beneficiari, metadatele utilizate, și toată corespondenţa dintre certSIGN și Beneficiari să fie arhivate.

Arhiva QPS conţine metadate active și expirate, inclusiv cele anulate. Arhiva QPS conţine informaţii despre Beneficiar, contract, momentul când a fost activat serviciul și toate operațiunile efectuate. Arhiva este folosită pentru rezolvarea eventualelor dispute, referitoare la documente depuse pentru păstrare, semnate electronic sau sigilate.

Copiile de siguranţă sunt ţinute în afara locaţiei certSIGN.

5.5.1 Tipuri de date arhivate

Următoarele date sunt incluse într-o arhivă de încredere, timp de cel puțin 3 ani după încheierea contractului pe care se bazează pe aceste înregistrări:

- Toate metadatele aferente operațiunilor QPS efectuate pe perioada derulării contractului
- Jurnalele de log-uri arhivate
- Log-rile tuturor evenimentelor legate de ciclul de viață al documentelor prezervate de certSIGN pe perioada derulării contractului
- Contract de prestare servicii QPS – aceste evidențe vor fi păstrate conform legii
- Termeni și condiții (acceptați) privind utilizarea serviciului QPS

5.5.2 Perioada de retenție a arhivei

Vezi secțiunea 5.5.1 de mai sus. După expirarea perioadei de păstrare declarate, datele arhivate sunt distruse.

5.5.3 Protecția arhivei

certSIGN asigură:

- implementarea controalelor pentru prevenirea pierderilor de date din arhivă
- confidențialitatea datelor arhivate și menținerea integrității în timpul perioadei sale de reținere,

Arhivele sunt accesibile exclusiv personalului autorizat.

5.5.4 Procedurile de back-up al arhivei

Backup-ul datelor arhivate se face în conformitate cu politicile și procedurile interne privind back-up-ul.

5.5.5 Cerințe privind marcarea temporală a înregistrărilor

certSIGN garantează că ora exactă de arhivare a tuturor evenimentelor, înregistrările și documentelor menționate mai sus este înregistrată. Acest lucru este realizat prin sincronizarea tuturor sistemelor cu serverele de timp. Acuratețea timpului este asigurată de un server de timp care este sincronizat cu cel puțin două surse de timp care pot fi sateliți GPS sau UTC (NIMB).

5.5.6 Sistemul de colectare al arhivei (intern sau extern)

Sistemele de colectare ale arhivei certSIGN sunt interne.

5.5.7 Proceduri de obținere și verificare a informațiilor arhivate

Arhivele sunt accesibile angajaților autorizați ai certSIGN și auditorilor desemnați. Înregistrările sunt păstrate în format electronic, sau în format pe suport de hârtie.

Beneficiarul/Subiectul poate primi acces la înregistrări și alte informații referitoare la Subiectul Certificatului.

5.6 Compromiterea și recuperare în caz de dezastru

Acest capitol descrie procedurile folosite de certSIGN în situaţii anormale (inclusiv dezastrele naturale) pentru restaurarea serviciilor la nivelul garantat. Aceste proceduri sunt executate în concordanţă cu Planul certSIGN de Continuitate a afacerii și de Recuperare în caz de Dezastru.

5.6.1 Procedurile de administrare a a incidentelor și compromiterilor

certSIGN are un proces pentru Managementul Crizelor, pus în aplicare printr-o procedură de gestionare a incidentelor de securitate, în scopul de a răspunde rapid și coordonat la incidente și pentru a limita impactul breșelor de securitate. Angajaților le sunt atribuite roluri de încredere pentru a urmări alertele evenimentelor de securitate potențiale critice și pentru a se asigura că incidentele relevante sunt raportate în conformitate cu procedura. În cazul defecțiunilor critice se acționează pe baza aceleiași proceduri.

Procedura de administrare a incidentelor de securitate specifică de asemenea modul în care se face notificarea părților corespunzătoare în conformitate cu normele de reglementare aplicabile oricărei breșe de securitate sau pierderii integrității care are un impact semnificativ asupra serviciului de încredere furnizat și asupra datelor cu caracter personal păstrate de acesta în termen de 24 de ore de la identificarea breșei.

În caz de incidente de Securitate, se utilizează procedurile interne. Aceste proceduri includ și notificarea Organismului National de Supraveghere, CSIRT sau alte autorități competente.

În cazul în care breșa de securitate sau pierderea integrității poate afecta în mod negativ o persoană fizică sau juridică căreia i-a fost prestat serviciul de prezervare, vom notifica de asemenea, persoana fizică sau juridică imediat.

Toate jurnalele evenimentelor de securitate sunt analizate în mod continuu prin mecanisme automate, pentru a identifica dovezi de activitate rău intenționată și pentru a alerta personalul asupra posibilelor evenimente critice de securitate.

Toate incidentele și/sau compromiterile sunt documentate și toate înregistrările asociate sunt arhivate așa cum este descris în secțiunea 5.5 a PPPS.

certSIGN are un Plan de răspuns la incidente și un Plan de recuperare în caz de dezastru, care includ Planul de Management în situații de Criză, precum și proceduri documentate de continuitatea afacerii și recuperare în caz de dezastre, proiectate astfel încât să notifice și să protejeze în mod rezonabil furnizorii de aplicații software, beneficiarii și entitățile partenere, în eventualitatea unui dezastru, compromitere a securității sau eșec al afacerii. certSIGN pune la dispoziția auditorilor, la cerere, planurile de continuitate a afacerii și de securitate. Toate procedurile sunt anual testate, revizuite și actualizate.

5.6.2 Proceduri la compromiterea resurselor de calcul, a aplicațiilor software și/sau datelor

Politica de Securitate certSIGN ia în considerate următoarele amenințări care pot influența disponibilitatea și continuitatea serviciilor furnizate:

- distrugerea fizică a sistemului de calcul al certSIGN, inclusiv alterarea resurselor de reţea – această amenințare se referă la distrugerile provocate de situaţiile de urgenţă,
- funcţionarea defectuoasă a aplicaţiilor, având ca efect imposibilitatea accesării datelor - aceste deteriorări se referă la sistemul de operare, aplicaţiile utilizatorilor şi executarea de aplicaţii periculoase, cum ar fi viruşii, viermii, caii troieni,
- pierderea unor servicii de reţea importante pentru activitatea certSIGN. Acestea se referă în primul rând la căderile de tensiune şi distrugerea legăturilor de reţea.

- distrugerea unei părţi din Intranetul folosit de certSIGN pentru a furniza servicii – acest lucru poate duce la obstrucţionarea clienţilor şi refuzul (neintenţionat) serviciilor.

Pentru a preveni sau limita rezultatele ameninţărilor de mai sus:

- Politica de securitate a certSIGN include un Plan de continuitate a afacerii și recuperare în caz de dezastru,
- În cazul apariţiei unui eveniment ce blochează funcţionarea certSIGN, în maxim 48 de ore, va fi activată locaţia auxiliară ce poate substitui toate funcţiile importante ale unui TSP până la restaurarea locaţiei principale. Distanța dintre locația primară și cea secundară este suficient de mare pentru ca potențialul dezastru care afectează locația primară să nu afecteze și locația secundară.
- Instalarea de versiuni noi ale aplicaţiilor software în producţie se poate face numai după testarea intensivă a acestora într-un mediu de test, în conformitate cu procedurile descrise. Orice modificare a sistemului necesită aprobarea administratorului de securitate al certSIGN.
- Sistemele certSIGN utilizează aplicaţii pentru crearea copiilor de rezervă a datelor pe baza cărora se poate face în orice moment restaurarea sistemului și auditarea acestuia. Copiile de siguranţă includ toate datele relevante din punct de vedere al securităţii.
- Toate sistemele din care este compusă infrastructura IT pentru furnizarea de servicii de încredere sunt monitorizate în mod continuu și toate evenimentele de securitate sunt înregistrate și analizate. Activitățile de sistem anormale care indică o potențială încălcare a securității, inclusiv intruziune în sistemele de rețea sunt detectate și raportate ca alarme pentru a permite certSIGN să detecteze, înregistreze și reacționeze în timp util la orice tentativă neautorizată și/sau neobișnuite de a accesa resursele sale.
- Sensibilitatea oricăror informații colectate sau analizate este luată în considerare, protejându-le împotriva accesului neautorizat.
- Pentru a detecta orice discontinuitate în operațiunile de monitorizare, pornirea și oprirea funcțiilor de logare este, de asemenea, monitorizată.
- Disponibilitatea tuturor componentelor importante ale infrastructurii ICT utilizate pentru furnizarea serviciilor de încredere, precum și disponibilitatea serviciilor critice sunt, de asemenea, monitorizate.
- certSIGN va aborda orice vulnerabilitate critică care anterior nu a fost adresată, într-o perioadă de 96 de ore de la descoperirea sa. Dacă acest lucru este rentabil, având în vedere impactul, va fi creat și pus în aplicare un plan pentru a reduce vulnerabilitatea sau va fi documentată decizia că vulnerabilitatea nu necesită remediere.

5.6.3 Capacități de Continuitate a afacerii în caz de dezastru

certSIGN a stabilit într-un Plan de Continuitate a afacerii și de recuperare în caz de dezastru (BC&DRP) toate măsurile necesare pentru a asigura recuperarea integrală a serviciilor noastre de încredere în caz de dezastru, sau în cazul unei discontinuități a oricărei componente ICT ori a unui serviciu important, mai mare decât Downtime-ul Maxim Tolerabil. Orice astfel de măsuri sunt conforme cu standardele ISO/IEC 27001 și 27002. Funcționarea fiecărei componente sau serviciu va fi restaurată în timpul Maxim Tolerabil de Downtime stabilit în planul de continuitate.

Toate datele sistemelor necesare pentru reluarea operațiunilor TSP sunt salvate și stocate într-un loc la distanță și în condiții de siguranță, pentru a permite serviciilor să își reia activitatea în timp util în cazul unui incident / dezastru.

Copiile de siguranță ale informațiilor și software-ului esențial sunt realizate în mod regulat. Se oferă facilități de back-up adecvate pentru a se asigura că toate informațiile și software-urile esențiale pot fi recuperate în urma unui dezastru sau unei defectiuni a mediilor de stocare. Activitățile de back-up sunt testate în mod regulat pentru a se asigura că acestea îndeplinesc cerințele planurilor de continuitate a afacerii.

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

În urma unui dezastru, acolo unde este posibil, vor fi luate măsuri pentru a evita repetarea unui dezastru.

5.7 Încetarea serviciului QPS

certSIGN are un plan actualizat de încetare a activității utilizat pentru a minimiza efectele negative asupra Beneficiarilor şi Entităţilor Partenere ce pot apărea ca urmare a deciziei TSP de a-şi înceta activitatea QPS. Planul include obligativitatea notificării Beneficiarilor în legatură cu serviciile ce urmează să își înceteze activitatea și transferarea responsabilităților (servicii furnizate către Beneficiari, baze de date, etc) în conformitate cu reglementarile aplicabile către alt TSP.

Cerințe asociate transferului responsabilității

Înainte ca serviciile QPS să își înceteze activitatea, certSIGN TSP va:

- Informa (cu cel puțin 30 de zile înainte) despre decizia de încetare a serviciilor pe următorii: toți Beneficiarii care dețin contracte active (neexpirate și neîncheiate) încheiate cu certSIGN TSP și alte entități cu care certSIGN are înțelegeri sau alte forme de colaborare, printre care terțe părți și alți furnizori de servicii de încredere și autorități relevante, cum ar fi organismele de supraveghere. În plus, această informație va fi facută disponibilă și altor Entități Partenere;
- Transferă obligațiile sale unei părți de încredere pentru a menține toate informațiile necesare pentru funcționarea serviciilor QPS pentru o perioadă rezonabilă;
- Dacă este posibil, se vor realiza înțelegeri pentru a transfera furnizarea serviciilor QPS pentru clienții existenți către un alt furnizor de servicii de încredere.

certSIGN va păstra sau va trasfera unei părți de încredere obligațiile sale, astfel încât să asigure disponibilitatea serviciilor QPS pentru o perioadă rezonabilă de timp.

În cazul în care certSIGN își încetează activitatea, fără a transfera o parte sau toate activitățile sale, va iniția procedura de terminare a contractelor încheiate cu partenerii și/sau furnizorii implicați.

certSIGN are un aranjament care să acopere costurile îndeplinirii acestor cerințe minime, în cazul în care intră în faliment sau dacă din orice alt motiv nu poate acoperi aceste costuri de una singură, în măsura în care este posibil, în limitele legislației aplicabile privind falimentul.

Preluarea QPS de către succesorul TSP care își încetează activitatea

Pentru a asigura continuitatea serviciilor QPS pentru Beneficiari, TSP care îşi încetează activitatea poate semna un contract cu alt TSP ce oferă servicii similare, pentru a prelua, în condiții prestabilite, datele și activitățile specifice QPS.

Prin preluarea QPS, succesorul TSP care îşi încetează activitatea preia drepturile și obligaţiile acestei autorităţi în ceea ce priveşte managementul documentelor care rămân în prezervare.

După notificarea terminării de către TSP certSIGN a serviciilor QPS Beneficiarul are decizia acceptării continuării serviciilor cu noul TSP sau a retragerii din acordul încheiat cu certSIGN.

Arhiva QPS a TSP care-şi încetează activitatea trebuie predată noului TSP în cazul încetării activităţii TSP certSIGN.

5.8 Lanțul de aprovizionare

certSIGN a documentat și implementat procese și proceduri pentru gestionarea riscurilor de securitate a informațiilor asociate cu utilizarea produselor sau serviciilor furnizorilor. Acestea sunt detaliate în politica internă certSIGN de gestionare a furnizorilor terți („ Politica de Management al Serviciilor Furnizate de Terți").

Procesul și procedurile implementate gestionează riscurile de securitate a informațiilor asociate lanțului de aprovizionare cu produse și servicii din domeniul tehnologiilor informației și comunicațiilor, astfel cum se solicită în ETSI EN 319 401 #7.14.

Atunci când certSIGN apelează la alte părți, inclusiv la furnizorii de componente ale serviciilor de încredere, pentru a furniza părți ale serviciului său prin subcontractare, externalizare sau alte acorduri cu terți, acesta păstrează responsabilitatea generală pentru conformitatea cu politica privind lanțul de aprovizionare, cu politica sa privind securitatea informațiilor și cu cerințele definite în politica privind serviciile de încredere.

certSIGN revizuiește politica privind lanțul de aprovizionare și monitorizează, revizuiește, evaluează și gestionează schimbările în practicile de securitate cibernetică ale furnizorilor direcți sau ale prestatorilor de servicii la intervale planificate sau după un incident legat de furnizarea de servicii de către furnizorii direcți sau prestatorii de servicii.

6 Controale tehnice de securitate

certSIGN QPS utilizează sisteme și echipamente fiabile și protejate împotriva modificărilor pentru gestionarea întregului ciclu de viață al documentelor electronice.

Cererințele de capacitate sunt monitorizate în permanență, iar cererințele viitoare de capacitate sunt estimate, astfel încât astfel încât să se asigure disponibilitatea necesară pentru necesitățile de procesare și stocare.

6.1 Datele de activare

6.1.1 Generarea și instalarea datelor de activare

Datele de activare sunt folosite în două situații principale:

- Ca element al unei proceduri de autentificare bazate pe unul sau mai mulți factori (așa-numitele fraza de autentificare, de ex. parolă, cod PIN etc),
- Ca parte a secretului partajat.

Operatorii și administratorul TSP, precum și alte persoane care îndeplinesc rolurile descrise în Capitolul 5.2, trebuie să folosească parole rezistente (token-uri/carduri) ca să se autentifice la rolurile lor. Cheile lor private care sunt generate pe dispozitive de semnătură electronică calificate sau smartcard-HSM de către certSIGN sunt asociate cu datele de activare ale utilizatorului (cod PIN) fiind personalizate și distribuite în siguranță. certSIGN garantează că datele de activare ale operatorilor și administratorilor și sunt gestionate și protejate de participanți, prin proceduri interne aplicabile puse la dispoziția acestor participanți.

Secretele partajate folosite pentru protejarea cheii private a TSP sunt generate în concordanţă cu cerinţele prezentate în Capitolul 6.2 şi păstrate pe carduri criptografice. Cardurile sunt protejate printr-un cod PIN. Secretele partajate devin date de activare după activarea acestora, de exemplu, prin introducerea corectă a codului PIN care protejează cardul. certSIGN asigură faptul că datele de activare a cheilor și a operațiunilor de activare a cheilor private ale CA, sunt generate, gestionate, stocate și arhivate așa cum s-a descris în subsecțiunea relevantă a secțiunilor 6.1 și 6.2. Instalarea și recuperarea perechilor de chei

ale TSP într-un dispozitiv criptografic securizat necesită controlul simultan a cel puțin doi angajați cu roluri de încredere.

Atunci când cheile sunt generate pe QSCD de către certSIGN, QSCD unde se stochează cheia privată și certificatul digital este fie livrat personal Beneficiarului, fie trimis prin intermediul serviciilor poștale sau de curierat către acesta. Datele de activare secretă (adică codul PIN) necesare pentru a accesa QSCD sunt trimise utilizând un plic securizat.

6.1.2 Protejarea datelor de activare

Protejarea datelor de activare include metode de control al datelor de activare prin care se previne dezvăluirea lor. Metodele de control al datelor de activare depind de natura acestora: dacă sunt fraze de autentificare sau dacă acest control se bazează pe cheia privată sau pe distribuirea informaţiilor de activare în secrete partajate.

Datele de activare folosite pentru activarea cheii private trebuie să fie protejate prin intermediul unor controale criptografice și printr-un control al accesului fizic. Datele de activare trebuie să fie memorate (nu scrise) de către entitatea autentificată. În cazul în care datele de activare sunt scrise, nivelul lor de protecție ar trebui să fie aceleași ca al datelor protejate prin utilizarea unui card criptografic. Mai multe încercări nereușite de a accesa modulul criptografic trebuie să ducă la blocarea acestuia. Datele de activare stocate nu trebuie să fie păstrate împreună cu cardul criptografic.

Beneficiarii sunt responsabili pentru gestionarea și protejarea sigură a datelor de activare (de exemplu codul PIN).

Datele de activare secretă (de exemplu codul PIN) primite de la certSIGN vor fi imediat modificate de Beneficiar după primirea acestuia.

6.1.3 Alte aspect ale datelor de activare

Nu se aplică.

6.2 Controale de Securitate ale computerelor

Acest capitol descrie controalele de securitate ale computerelor certSIGN.

Subiectul este responsabil pentru propriile controale de securitate ale computerului. Aceste aspecte nu sunt acoperite în subcapitolele de mai jos.

6.2.1 Cerințe tehnice specifice ale securității calculatoarelor

Măsurile de securitate care protejează sistemele de calcul sunt aplicate la nivelul sistemului de operare, al aplicaţiilor precum și din punct de vedere fizic.

Computerele sunt configurate cu următoarele mecanisme de securitate:

- autentificarea obligatorie la nivelul sistemului de operare şi al aplicaţiilor,
- control discreţionar al accesului,
- posibilitatea de a efectua un audit de securitate,
- calculatorul este accesibil doar personalului autorizat, cu roluri de încredere în certSIGN,
- separarea sarcinilor, conform rolului în cadrul sistemului,
- identificarea şi autentificarea rolurilor şi a personalului care îndeplineşte aceste roluri,
- prevenirea refolosirii unui obiect de către un alt proces după eliberarea acestuia de către un proces autorizat,
- protecţia criptografică a schimburilor de informaţii și protecţia bazelor de date,

- arhivarea istoricului operaţiunilor executate pe un calculator și a datelor necesare auditării,
- o cale sigură ce permite identificarea şi autentificarea rolurilor şi a personalului care îndeplineşte aceste roluri,
- metode de restaurare a cheilor (numai în cazul modulelor hardware de securitate), a aplicaţiilor şi a sistemului de operare,

- mijloace de monitorizare și alertare în cazul accesului neautorizat la resursele de calcul.

Integritatea sistemelor și informațiilor certSIGN este protejată împotriva virușilor, software-urilor rău intenționate și neautorizate.

Mediile utilizate în cadrul sistemelor certSIGN sunt manipulate în siguranță, pentru a proteja mediile împotriva deteriorării, furtului, accesul neautorizat și uzurii morale.

Procedurile de gestionare a mediilor sunt puse în aplicare pentru a proteja împotriva uzurii morale și deteriorării mediilor în perioada de timp în care este obligatorie păstrarea înregistrărilor.

Datele sensibile sunt protejate împotriva relevării prin obiecte de stocare re-utilizate (de exemplu, fișiere șterse), fiind accesibile utilizatorilor neautorizați. În acest scop, trebuie utilizat un software special, cu algoritmi de ștergere siguri pentru mediile de stocare, HSM-urile se resetează, dispozitivele criptografice securizate (token-uri / carduri) trebuie formatate înainte de reutilizare / sau distruse fizic la sfârșitul ciclului lor de viață.

Pentru toate conturile capabile să producă în mod direct emiterea de certificate, este pusă în aplicare autentificarea multi-factor.

6.2.2 Evaluarea securității calculatoarelor

Sistemul informatic certSIGN îndeplinește cerințele descrise în standardele ETSI și CEN CWA 14167 (Cerințe de securitate pentru sisteme de încredere care gestionează certificate pentru semnături electronice).

6.3 Controale de securitate specifice ciclului de viață

certSIGN utilizează sisteme și produse de încredere care sunt protejate împotriva modificărilor și asigură securitatea tehnică și fiabilitatea proceselor susținute de acestea.

6.3.1 Controale specifice dezvoltării sistemului

O analiză a cerințelor de securitate se realizează în etapa de proiectare precum și o definire a cerințelor a oricărui proiect de dezvoltare a sistemelor întreprinse de certSIGN sau în numele certSIGN, pentru a se asigura că securitatea este construită în sistemele informatice.

Înainte de a fi folosită în producţie in cadrul certSIGN, fiecare aplicaţie este instalată astfel încât să se permită controlul versiunii curente și să se prevină instalarea neautorizată de programe sau falsificarea celor existente.

Reguli similare se aplică în cazul înlocuirii componentelor hardware, cum ar fi:

- dispozitivele fizice sunt furnizate în aşa fel încât să poată fi urmărită și evaluată ruta fiecăruia, până la locul său de instalare,
- livrarea unui dispozitiv fizic pentru înlocuire se realizează într-un mod similar celui de livrare al dispozitivului original; înlocuirea se realizează de către personal calificat şi de încredere.

6.3.2 Controale specifice managementului securității

Scopul controalelor specifice managementului securităţii este de a superviza funcţionalitatea sistemelor certSIGN, garantând astfel că acestea operează corect şi în concordanţă cu configurarea acceptată şi implementată.

Controalele aplicate sistemelor certSIGN permit verificarea continuă a integrităţii aplicaţiilor, versiunii și autentificarea şi verificarea originii dispozitivelor hardware.

6.3.3 Controale de securitate specifice ciclului de viață

Politicile și procedurile de control al modificărilor sunt aplicate lansărilor, modificărilor și remedierilor de urgență ale oricărui software operațional, precum și modificărilor de configurație care se aplică prin politica de securitate certSIGN.

Configurarea actuală a sistemului certSIGN, orice modificare a lor, precum și a oricărei lansări, modificări și remedieri de urgență ale oricărui software operațional sunt documentate.

Configuratiile Sistemelor de suport al Serviciilor, a Sistemelor de Management al Certificatelor, a Sistemelor Suport de Securitate si a Sistemelor Front-End/ Sistemelor de Suport Intern sunt verificate cel putin saptamanal pentru a determina orice schimbari care ar viola politicile de securitate ale CA-ului.

certSIGN pune în aplicare procedurile de securitate internă pentru a asigura că:

- patch-urile de securitate sunt aplicate într-un termen rezonabil după ce au venit disponibile;
- patch-urile de securitate nu se aplică dacă ele aduc vulnerabilități sau instabilități suplimentare care depășesc beneficiile aplicării acestora;

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

certSIGN implementează o procedură de gestionare a capacității interne care să garanteze că pentru infrastructura TIC dedicată serviciilor de încredere, cererile de capacitate sunt monitorizate și proiecțiile cerințelor de capacitate viitoare sunt făcute pentru a se asigura că puterea de procesare și de stocare adecvate sunt disponibile.

6.4 Controale de securitate a rețelei

certSIGN își protejează rețeaua și sistemele de atacuri. 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 luând în considerare relația funcțională, logică și fizică (inclusiv de locație) dintre sistemele și servicii de încredere. certSIGN aplică aceleași controale de securitate pentru toate sistemele co-localizate în aceeași zonă.
b) Accesul și comunicarea între zone sunt permise doar persoanelor necesare funcționării serviciilor de încredere. Conexiunile și serviciile care nu sunt necesare sunt interzise în mod explicit sau dezactivate. Setul de reguli stabilite sunt reviziuite periodic.
c) Toate sistemele critice pentru funcționarea serviciilor de încredere sunt păstrate într-una sau mai multe zone securizate)
d) Rețeaua dedicată administrării sistemelor IT și rețeaua operațională sunt separate. Sistemele utilizate pentru administrarea implementării politicii de securitate nu sunt utilizate în alte scopuri. Sistemele de producție ale serviciilor de încredere sunt separate de sistemele utilizate în dezvoltare și testare (de exemplu, sistemele de dezvoltare, testare și planificare).
e) Comunicarea între sisteme de încredere distincte se realizează doar prin intermediul unor canaluri de încredere care sunt distincte logic de alte canale de comunicații și

oferă identificarea sigură a punctelor terminale și protecția datelor canalului de modificare sau divulgare.

f) Dacă este necesar un nivel înalt de disponibilitate a accesului extern la un anumit serviciu de încredere, conexiunea externă la rețea este redundantă, pentru a asigura disponibilitatea serviciilor, în cazul unui singur eșec.

g) Se realizează o scanare periodică a vulnerabilității adreselor IP publice și private identificate de certSIGN și se înregistrează dovezi că fiecare scanare a vulnerabilității a fost realizată de către o persoană sau o entitate cu abilitățile, instrumentele, competența, codul de etică, și independența necesare pentru a oferi un raport de încredere.

h) Serviciile de încredere ale certSIGN sunt supuse unui test de penentrare pe sistemele aferente la inițiere și după upgrade-uri de infastructură sau de aplicații sau după modificări pe care certSIGN le consideră importante. Se înregistrează dovezi că fiecare test de penetrare a fost realizat de către o persoană sau o entitate cu abilitățile, instrumentele, competența, codul de etică, și independența necesare pentru a oferi un raport de încredere.

Serverele și stațiile de lucru de încredere ale sistemului certSIGN sunt conectate printr-o rețea locală (LAN) și împărțite în mai multe sub-rețele, cu control al accesului. Accesul din Internet la oricare dintre segmente este protejat printr-un firewall inteligent.

Controalele de securitate sunt dezvoltate pe baza firewall-ului și a filtrelor de trafic aplicate la nivelul routerelor și serviciilor Proxy care protejează domeniile rețelei interne ale certSIGN împotriva accesului neautorizat, inclusiv împotriva accesării de către Beneficiari și terți. Firewall-urile sunt configurate pentru a împiedica toate protocoalele și porturile care nu sunt necesare operării certSIGN CA.

Mijloacele de protecție a securității rețelei acceptă doar mesajele transmise utilizând protocoalele http, https, NTP, POP3 și SMTP. Evenimentele (log-uri) sunt înregistrate în jurnalele de system și permit supervizarea corectitudinii utilizării serviciilor furnizate de certSIGN.

certSIGN menține și protejează toate sistemele TSP cel puțin într-o zonă sigură și are implementată o procedură de securitate care protejează sistemele și comunicațiile dintre sistemele din zonele sigure și cele din zonele de înaltă securitate.

certSIGN configurează toate sistemele TSP prin eliminarea sau dezactivarea tuturor conturilor, aplicațiilor, serviciilor, protocoalelor și a porturilor care nu sunt utilizate în operațiunile TSP-ului.

certSIGN oferă acces la zonele sigure și la cele de înaltă securitate exclusiv rolurilor de încredere.

Sistemul suport **QPS** se află într-o zonă de înaltă securitate.

6.5 Marcare temporală

Precizia de timp a jurnalelor este asigurată de un server de timp care este sincronizat cu cel puțin două surse de timp care pot fi sateliți GPS sau UTC (NIMB).

7 Profile, Formate și Scheme de păstrare

O schemă de păstrare (profil) trebuie să îndeplinească următoarele cerințe generale:

1. Este documentat suficient de detaliat, astfel încât să fie posibilă interoperabilitatea între implementări independente.
2. Este identificată printr-un URI în conformitate cu *IETF RFC 3986*.
3. Specifică modelul aplicabil de depozitare din sistemul de păstrare.
4. Specifică setul de obiective de păstrare susținute de schema de păstrare.
5. Specifică setul de operațiuni obligatorii și opționale suportate.
6. Descrie procesul de generare și validare a dovezilor de păstrare – detaliat in #3.6.
7. Pentru păstrarea WOS sau WTS, durata așteptată a dovezilor (*Expected Evidence Duration*) se bazează pe estimarea adecvării algoritmului criptografic RSA în conformitate cu ETSI TS 119 312 V1.4.3 #8 și #9.
8. Descrie modul în care are loc menținerea dovezilor de păstrare– detaliat in #3.7.
9. Specifica formatele necesare sau recomandate ale parametrilor de intrare și ieșire și transformările aferente ale datelor, dacă este cazul, pentru punerea în aplicare a sistemului de păstrare.

7.1 Schema de păstrare cu semnătură digitală și stocare

- ***ProfileIdentifier:***
  Profil de bază:
  - Calificate - pds+wst (OID: 1.3.6.1.4.1.25017.5.2.1
  Profilul este identificat prin profilul de bază la care se adaugă durata de păstrare în ani. (De exemplu, 1.3.6.1.4.1.25017.5.2.1.40 = pds+wst calificat pentru 40 de ani).
- ***Operation:***
  - **Operațiuni obligatorii**
    - PreservePO
    - RetrievePO
    - DeletePO
  - **Operațiuni opționale**
    - RetrieveTrace
- ***Policy:***
  - Politica de creare a dovezilor de păstrare aplicate și o politică recomandată de validare a probelor de păstrare pot fi anunțate în elementul profil/politică aplicabil, cu tipul egal cu următorul URI:
    - http://uri.etsi.org/19512/policy/preservation-evidence
- ***ProfileValidityPeriod:***
  - conform contractului
- ***PreservationStorageModel:***
  - modelul de stocare de păstrare "cu stocare", care corespunde valorii WithStorage în cadrul elementului PreservationStorageModel.
- ***PreservationGoal:***
  - prelungirea pe perioade lungi de timp a stării de valabilitate a semnăturilor digitale, care este indicată de URI:http://uri.etsi.org/19512/goal/pds
  - completare/augmentarea dovezilor prezentate, care este indicată de URI: http://uri.etsi.org/19512/goal/aug
- ***EvidenceFormat***:
  - completează semnătura corespunzătoare formatului semnăturii, care este anunțată în elementul Profil/EvidenceFormat cu următoarele URI:
    - http://uri.etsi.org/ades/PAdES/document-time-stamp
- ***Specification***:
  - https://www.certsign.ro/depozitar/
- ***Description:***

- funcția PreservePO a actualului sistem de păstrare distinge un singur tip de caz de utilizare, anume: semnătura și datele semnate sunt în același obiect.
- Serviciul de păstrare verifică dacă toate datele de validare necesare pentru validarea semnăturii sunt disponibile, le adaugă semnăturii și le protejează cu o marcă de timp corespunzătoare formatului specific al semnăturii. Serviciul de păstrare alege un algoritm hash pentru a proteja datele de validare, semnătura și datele semnate corespunzătoare stadiului actual al tehnolgiei.
- Dovezile sunt incluse în semnătură.
- Standardul specific formatului de semnătură specifică modul de validare a dovezilor corespunzătoare
- Pe baza monitorizării caracteristicilor algoritmilor criptografici conform unei politici criptografice adecvate, cum ar fi ETSI TS 119 312, de exemplu, serviciul de păstrare efectuează o completare/augmentare a semnăturilor în conformitate cu formatul specific al dovezilor de păstrare.

- ***SchemeIdentifier***:
  - http://uri.etsi.org/19512/scheme/pds+wst+aug
- ***ExpectedEvidenceDuration:***
  - N/A
- ***PreservationEvidenceRetentionPeriod***:
  - *N/A*
- ***Extension***:
  - N/A

7.2 Schema de păstrare cu semnătură digitală și stocare temporară

- ***ProfileIdentifier:***
  Profil de bază:
  - Calificate - pds+wts (OID: 1.3.6.1.4.1.25017.5.2.2)

Profilul este identificat prin profilul de bază la care se adaugă durata de păstrare în ani. (De exemplu, 1.3.6.1.4.1.25017.5.2.2.40 = pds+wts calificat pentru 40 de ani).

- ***Operation:***
  - **Operațiuni obligatorii**
    - PreservePO
    - RetrievePO
  - **Operațiuni opționale**
    - RetrieveTrace
- ***Policy:***
  - Politica de creare a dovezilor de păstrare aplicate și o politică recomandată de validare a probelor de păstrare pot fi anunțate în elementul profil/politică aplicabil, cu tipul egal cu următorul URI:
    - http://uri.etsi.org/19512/policy/preservation-evidence
- ***ProfileValidityPeriod:***
  - conform contractului
- ***PreservationStorageModel:***
  - modelul de stocare de păstrare "cu stocare temporară", care corespunde valorii *WithTemporaryStorage* în cadrul elementului *PreservationStorageModel*.
- ***PreservationGoal:***
  - prelungirea pe perioade lungi de timp a stării de valabilitate a semnăturilor digitale, care este indicată de URI:http://uri.etsi.org/19512/goal/pds
  - completare/augmentarea dovezilor prezentate, care este indicată de URI: http://uri.etsi.org/19512/goal/aug
- ***EvidenceFormat***:
  - completează semnătura corespunzătoare formatului semnăturii, care este anunțată în elementul Profil/EvidenceFormat cu următoarele URI:

        - http://uri.etsi.org/ades/PAdES/document-time-stamp
- ***Specification***:
    - https://www.certsign.ro/depozitar/
- ***Description:***
    - funcția PreservePO a actualului sistem de păstrare distinge un singur tip de caz de utilizare, anume: semnătura și datele semnate sunt în același obiect.
    - Serviciul de păstrare verifică dacă toate datele de validare necesare pentru validarea semnăturii sunt disponibile, le adaugă semnăturii și le protejează cu o marcă de timp corespunzătoare formatului specific al semnăturii. Serviciul de păstrare alege un algoritm hash pentru a proteja datele de validare, semnătura și datele semnate corespunzătoare stadiului actual al tehnolgiei.
    - Dovezile sunt incluse în semnătură.
    - Standardul specific formatului de semnătură specifică modul de validare a dovezilor corespunzătoare.
    - Pe baza monitorizării caracteristicilor algoritmilor criptografici conform unei politici criptografice adecvate, cum ar fi ETSI TS 119 312, de exemplu, serviciul de păstrare efectuează o completare/augmentare a semnăturilor în conformitate cu formatul specific al dovezilor de păstrare.
- ***SchemeIdentifier***:
    - http://uri.etsi.org/19512/scheme/pds+wts+aug
- ***ExpectedEvidenceDuration:***
    - conform contractului
- ***PreservationEvidenceRetentionPeriod***:
    - *96 ore*
- ***Extension***:
    - N/A

7.3 Schema de păstrare cu semnătură digitală și fără stocare

- ***ProfileIdentifier:***
  Profil de bază:
    - Calificate - pds+wos (OID: 1.3.6.1.4.1.25017.5.2.3)

Profilul este identificat prin profilul de bază la care se adaugă durata de păstrare în ani. (De exemplu, 1.3.6.1.4.1.25017.5.2.3.40 = pds+wos calificat pentru 40 de ani).

- ***Operation:***
    - **Operațiuni obligatorii**
        - PreservePO
    - **Operațiuni opționale**
        - RetrieveTrace
- ***Policy:***
    - Politica de creare a dovezilor de păstrare aplicate și o politică recomandată de validare a probelor de păstrare pot fi anunțate în elementul profil/politică aplicabil, cu tipul egal cu următorul URI:
        - http://uri.etsi.org/19512/policy/preservation-evidence
- ***ProfileValidityPeriod:***
    - conform contractului
- ***PreservationStorageModel:***
    - modelul de stocare de păstrare "fără stocare", care corespunde valorii *WithoutStorage* în cadrul elementului *PreservationStorageModel*.
- ***PreservationGoal:***
    - prelungirea pe perioade lungi de timp a stării de valabilitate a semnăturilor digitale, care este indicată de URI:http://uri.etsi.org/19512/goal/pds

- completare/augmentarea dovezilor prezentate, care este indicată de URI: http://uri.etsi.org/19512/goal/aug

- ***EvidenceFormat***:
  - completează semnătura corespunzătoare formatului semnăturii, care este anunțată în elementul Profil/EvidenceFormat cu următoarele URI:
    - http://uri.etsi.org/ades/PAdES/document-time-stamp
- ***Specification***:
  - https://www.certsign.ro/depozitar/
- ***Description:***
  - funcția PreservePO a actualului sistem de păstrare distinge un singur tip de caz de utilizare, anume: semnătura și datele semnate sunt în același obiect.
  - Serviciul de păstrare verifică dacă toate datele de validare necesare pentru validarea semnăturii sunt disponibile, le adaugă semnăturii și le protejează cu o marcă de timp corespunzătoare formatului specific al semnăturii. Serviciul de păstrare alege un algoritm hash pentru a proteja datele de validare, semnătura și datele semnate corespunzătoare stadiului actual al tehnolgiei.
  - Dovezile sunt incluse în semnătură.
  - Standardul specific formatului de semnătură specifică modul de validare a dovezilor corespunzătoare.
  - Pe baza monitorizării caracteristicilor algoritmilor criptografici conform unei politici criptografice adecvate, cum ar fi ETSI TS 119 312, de exemplu, serviciul de păstrare efectuează o completare/augmentare a semnăturilor în conformitate cu formatul specific al dovezilor de păstrare.
- ***SchemeIdentifier***:
  - http://uri.etsi.org/19512/scheme/pds+wos+aug
- ***ExpectedEvidenceDuration:***
  - conform contractului
- ***PreservationEvidenceRetentionPeriod***:
  - *N/A*
- ***Extension***:
  - N/A

7.4 Schema generală de păstrare cu stocare a datelor

- ***ProfileIdentifier***

Profil de bază:

- Calificate - pgd+wst (OID: 1.3.6.1.4.1.25017.5.2.4)

Profilul este identificat prin profilul de bază la care se adaugă durata de păstrare în ani. (De exemplu, 1.3.6.1.4.1.25017.5.2.4.40 = pgd+wst calificat pentru 40 de ani).

- ***Operation:***
  - **Operațiuni obligatorii**
    - PreservePO
    - RetrievePO
    - DeletePO
  - **Operațiuni opționale**
    - RetrieveTrace
- ***Policy:***
  - Politica de creare a dovezilor de păstrare aplicate și o politică recomandată de validare a probelor de păstrare pot fi anunțate în elementul profil/politică aplicabil, cu tipul egal cu următorul URI:
    - http://uri.etsi.org/19512/policy/preservation-evidence
- ***ProfileValidityPeriod:***
  - conform contractului

- ***PreservationStorageModel:***
  - modelul de stocare de păstrare "cu stocare", care corespunde valorii ***WithStorage*** în cadrul elementului *PreservationStorageModel*.
- ***PreservationGoal:***
  - o dovadă a existenței pe perioade lungi de timp a obiectului de date prezentat serviciului de păstrare, indicată de URI: http://uri.etsi.org/19512/goal/pgd
  - completarea/augmentarea dovezilor prezentate, care este indicată de URI: http://uri.etsi.org/19512/goal/aug
- ***EvidenceFormat***:
  - completează semnătura corespunzătoare formatului semnăturii, care este anunțată în elementul Profil/EvidenceFormat cu următoarele URI:
    - http://uri.etsi.org/ades/PAdES/document-time-stamp
- ***Specification***:
  - https://www.certsign.ro/depozitar/
- ***Description:***
  - Schema de păstrare actuală asigură dovada existenței pe perioade lungi de timp a obiectului de date, prin semnarea obiectului de date și apoi completarea semnăturii corespunzătoare formatului semnăturii
  - funcția PreservePO a actualului sistem de păstrare distinge un singur tip de caz de utilizare, anume: semnătura și datele semnate sunt în același obiect.
  - Serviciul de păstrare verifică dacă toate datele de validare necesare pentru validarea semnăturii sunt disponibile, le adaugă semnăturii și le protejează cu o marcă de timp corespunzătoare formatului specific al semnăturii. Serviciul de păstrare alege un algoritm hash pentru a proteja datele de validare, semnătura și datele semnate corespunzătoare stadiului actual al tehnolgiei.
  - Dovezile sunt incluse în semnătură.
  - Standardul specific formatului de semnătură specifică modul de validare a dovezilor corespunzătoare
  - Pe baza monitorizării caracteristicilor algoritmilor criptografici conform unei politici criptografice adecvate, cum ar fi ETSI TS 119 312, de exemplu, serviciul de păstrare efectuează o completare/augmentare a semnăturilor în conformitate cu formatul specific al dovezilor de păstrare.
- ***SchemeIdentifier***:
  - http://uri.etsi.org/19512/scheme/pgd+wst+aug
- ***ExpectedEvidenceDuration:***
  - N/A
- ***PreservationEvidenceRetentionPeriod***:
  - *N/A*
- ***Extension***:
  - N/A

7.5 Schema generală de păstrare a datelor cu stocare temporară

- ***ProfileIdentifier***

  Profil de bază:
  - Calificate - pgd+wts (OID: 1.3.6.1.4.1.25017.5.2.5)

Profilul este identificat prin profilul de bază la care se adaugă durata de păstrare în ani. (De exemplu, 1.3.6.1.4.1.25017.5.2.5.40 = pds+wst calificat pentru 40 de ani).

- ***Operation:***
  - **Operațiuni obligatorii**
    - PreservePO
    - RetrievePO
  - **Operațiuni opționale**
    - RetrieveTrace

- ***Policy:***
  - Politica de creare a dovezilor de păstrare aplicate și o politică recomandată de validare a probelor de păstrare pot fi anunțate în elementul profil/politică aplicabil, cu tipul egal cu următorul URI:
    - http://uri.etsi.org/19512/policy/preservation-evidence
- ***ProfileValidityPeriod:***
  - conform contractului
- ***PreservationStorageModel:***
  - modelul de stocare de păstrare "cu stocare temporară", care corespunde valorii ***WithTemporaryStorage*** în cadrul elementului *PreservationStorageModel*.
- ***PreservationGoal:***
  - o dovadă a existenței pe perioade lungi de timp a obiectului de date prezentat serviciului de păstrare, indicată de URI URI: http://uri.etsi.org/19512/goal/pgd
  - completare/augmentarea dovezilor prezentate, care este indicată de URI: http://uri.etsi.org/19512/goal/aug
- ***EvidenceFormat***:
  - completează semnătura corespunzătoare formatului semnăturii, care este anunțată în elementul Profil/EvidenceFormat cu următoarele URI:
    - http://uri.etsi.org/ades/PAdES/document-time-stamp
- ***Specification***:
  - https://www.certsign.ro/depozitar/
- ***Description:***
  - Schema de păstrare actuală asigură dovada existenței pe perioade lungi de timp a obiectului de date, prin semnarea obiectului de date și apoi completarea semnăturii corespunzătoare formatului semnăturii
  - funcția PreservePO a actualului sistem de păstrare distinge un singur tip de caz de utilizare, anume: semnătura și datele semnate sunt în același obiect.
  - Serviciul de păstrare verifică dacă toate datele de validare necesare pentru validarea semnăturii sunt disponibile, le adaugă semnăturii și le protejează cu o marcă de timp corespunzătoare formatului specific al semnăturii. Serviciul de păstrare alege un algoritm hash pentru a proteja datele de validare, semnătura și datele semnate corespunzătoare stadiului actual al tehnolgiei.
  - Dovezile sunt incluse în semnătură.
  - Standardul specific formatului de semnătură specifică modul de validare a dovezilor corespunzătoare.
  - Pe baza monitorizării caracteristicilor algoritmilor criptografici conform unei politici criptografice adecvate, cum ar fi ETSI TS 119 312, de exemplu, serviciul de păstrare efectuează o completare/augmentare a semnăturilor în conformitate cu formatul specific al dovezilor de păstrare.
- ***SchemeIdentifier***:
  - http://uri.etsi.org/19512/scheme/pgd+wts+aug
- ***ExpectedEvidenceDuration:***
  - conform contractului
- ***PreservationEvidenceRetentionPeriod***:
  - *96 ore*
- ***Extension***:
  - N/A

7.6 Schema generală de păstrare a datelor fără stocare

- ***ProfileIdentifier***

  Profil de bază:
  - Calificate - pgd+wos (OID: 1.3.6.1.4.1.25017.5.2.6)

Profilul este identificat prin profilul de bază la care se adaugă durata de păstrare în ani. (De exemplu, 1.3.6.1.4.1.25017.5.2.6.40 = pds+wst calificat pentru 40 de ani).

- ***Operation:***
  - **Operațiuni obligatorii**
    - PreservePO
  - **Operațiuni opționale**
    - RetrieveTrace
- ***Policy:***
  - Politica de creare a dovezilor de păstrare aplicate și o politică recomandată de validare a probelor de păstrare pot fi anunțate în elementul profil/politică aplicabil, cu tipul egal cu următorul URI:
    - http://uri.etsi.org/19512/policy/preservation-evidence
- ***ProfileValidityPeriod:***
  - conform contractului
- ***PreservationStorageModel:***
  - modelul de stocare de păstrare "fără stocare", care corespunde valorii ***WithoutStorage*** în cadrul elementului *PreservationStorageModel*.
- ***PreservationGoal:***
  - o dovadă a existenței pe perioade lungi de timp a obiectului de date prezentat serviciului de păstrare, indicată de URI: http://uri.etsi.org/19512/goal/pgd
  - completare/augmentarea dovezilor prezentate, care este indicată de URI: http://uri.etsi.org/19512/goal/aug
- ***EvidenceFormat***:
  - completează semnătura corespunzătoare formatului semnăturii, care este anunțată în elementul Profil/EvidenceFormat cu următoarele URI:
    - http://uri.etsi.org/ades/PAdES/document-time-stamp
- ***Specification***:
  - https://www.certsign.ro/depozitar/
- ***Description:***
  - Schema de păstrare actuală asigură dovada existenței pe perioade lungi de timp a obiectului de date, prin semnarea obiectului de date și apoi completarea semnăturii corespunzătoare formatului semnăturii
  - funcția PreservePO a actualului sistem de păstrare distinge un singur tip de caz de utilizare, anume: semnătura și datele semnate sunt în același obiect.
  - Serviciul de păstrare verifică dacă toate datele de validare necesare pentru validarea semnăturii sunt disponibile, le adaugă semnăturii și le protejează cu o marcă de timp corespunzătoare formatului specific al semnăturii. Serviciul de păstrare alege un algoritm hash pentru a proteja datele de validare, semnătura și datele semnate corespunzătoare stadiului actual al tehnolgiei.
  - Dovezile sunt incluse în semnătură.
  - Standardul specific formatului de semnătură specifică modul de validare a dovezilor corespunzătoare.
  - Pe baza monitorizării caracteristicilor algoritmilor criptografici conform unei politici criptografice adecvate, cum ar fi ETSI TS 119 312, de exemplu, serviciul de păstrare efectuează o completare/augmentare a semnăturilor în conformitate cu formatul specific al dovezilor de păstrare.
- ***SchemeIdentifier***:
  - http://uri.etsi.org/19512/scheme/pgd+wos+aug
- ***ExpectedEvidenceDuration:***
  - conform contractului
- ***PreservationEvidenceRetentionPeriod***:
  - *N/A*
- ***Extension***:
  - N/A

8 Auditul de conformitate și alte evaluări

certSIGN este furnizor de servicii de încredere in conformitate cu Regulamentul UE 910/2014. În ceea ce privește auditurile de conformitate și competența, funcționarea consecventă și imparțialitatea conformității organismelor de evaluare care evaluează și certifică conformitatea noastră ca furnizor de servicii de încredere și conformitatea serviciilor noastre cu criteriile din Regulamentul 910/2014 și al actelor de punere în aplicare, urmărim cerințele din standardul ETSI EN 319 401.

8.1 Frecvența sau circumstanțele de evaluare

Activitățile certSIGN care sprijină furnizarea serviciilor prezentate de PPPS sunt auditate cel puțin o dată la 24 de luni.

Auditul verifică conformitatea cu PPPS, standardele tehnice ETSI 319 401 și ETSI 119 511.

Auditurile la cerere pot fi realizate la discreția certSIGN, la cererea organismului de supraveghere, astfel cum este definit în Regulamentul UE 910/2014, sau pentru a demonstra conformitatea cu cerințele specifice industriei, juridice sau de afaceri.

8.2 Identitatea / calificările evaluatorului

Evaluarea va fi efectuată de un organism de evaluare a conformității, astfel cum este definit în Regulamentul UE 910/2014.

8.3 Relația evaluatorului cu entitatea evaluată

Organismul de evaluare a conformității este un auditor independent, care nu este afiliat direct sau indirect cu certSIGN.

8.4 Subiectele acoperite de evaluare

Auditurile planificate cuprind, dar nu se limitează la, toate aspectele operațiunilor QPS și serviciilor certSIGN specificate în PPPS.

8.5 Acțiuni întreprinse ca urmare a deficienței

Organismul de evaluare a conformității raportează deficiențele și neconformitățile detectate către PPMP. certSIGN și organismul de evaluare a conformității analizează concomitent rezultatele raportului și aprobă un plan de corecție și un interval de timp pentru punerea în aplicare a acestuia.

Este posibil să se efectueze un audit ulterior, pentru a verifica acțiunile de remediere.

8.6 Comunicarea rezultatelor

Organismul de evaluare a conformității comunică raportul de audit conducerii certSIGN și către CMMP.

9 Alte elemente de afaceri și legale

9.1 Tarife

Tarifele serviciilor de încredere și ale categoriilor de servicii sunt publicate în lista de preţuri disponibilă la adresa https://www.certsign.ro . Prețurile sunt formate conform politici interne de preț.

Plăţile se vor face în numerar, prin ordin de plată, și prin carduri bancare, conform reglementărilor legale în vigoare.

9.2 Răspunderea financiară

certSIGN își asumă responsabilitatea financiară pentru a-și îndeplini toate obligațiile definite în prezentul document și în contractul de servicii încheiat cu Clientul. Pentru a acoperi costurile asociate cu încetarea activității de servicii și pentru a susține fiabilitatea certSIGN îndeplinește cerințele legale pentru prestatorii de servicii de încredere calificați.

9.2.1 Asigurarea sau acoperirea garanției

certSIGN beneficiază de asigurare care acoperă garanțiile profesionale.

9.3 Confidențialitatea informațiilor de afaceri

9.3.1 Scopul informațiilor confidențiale

Toate informaţiile referitoare la Beneficiar/Entități Partenere pe care le prelucrează certSIGN sunt obţinute, păstrate şi procesate în concordanţă cu prevederile Regulamentului (UE) nr. 910/2014. Relaţiile dintre un Beneficiar, o Entitate Parteneră și certSIGN se bazează pe încredere.

Datele furnizate de certSIGN nu vor fi dezvăluite în nicio circumstanţă vreunei terţe părţi, în mod voluntar (cu excepţia situaţiilor prevăzute de lege).

Dezvăluirea oricărei informaţii entităților implicate în îndeplinirea obligaţiilor se va face confidenţial și se va extinde doar asupra informaţiilor necesare pentru îndeplinirea obligaţiilor.

Tipuri de informații considerate a fi confidențiale și private

certSIGN, angajații săi precum și entitățile care desfăşoară activităţi de încredere sunt obligate să păstreze secretul informaţiilor, atât pe durata, cât și după încetarea contractului de muncă, în cazul angajaţilor. Sunt catalogate drept informaţii private sau confidenţiale:

- informaţiile furnizate de Beneficiari, în plus faţă de informaţiile care apar in Depozitar; dezvăluirea acestor informaţii se face doar cu aprobare scrisă, în prealabil, din partea proprietarului informaţiei sau în alte condiţii prevăzute de lege;
- conţinutul contractelor încheiate cu Beneficiarii sau Entităţile Partenere, conturi bancare, aplicaţii; aceste informații pot fi dezvăluite doar cu aprobarea și în scopul menţionat de proprietarul informaţiilor (de exemplu, Beneficiarul), cu excepţia informaţiilor din Depozitar, conform prezentului PPPS;
- înregistrările corespunzătoare tranzacţiilor din sistem (toate tipurile de tranzacţii, precum și datele pentru controlul tranzacţiilor, aşa numitele loguri ale tranzacţiilor din sistem);
- înregistrările corespunzătoare evenimentelor (log-uri) ce ţin de serviciile de prezervare, păstrate de certSIGN;

- rezultatele auditurilor interne și externe, dacă acestea reprezintă o amenințare pentru securitatea certSIGN;
- planurile în caz de urgenţă;
- informaţiile referitoare la măsurile luate pentru protecţia dispozitivelor hardware și aplicaţiilor software, informaţiile referitoare la administrarea serviciilor de încredere și la regulile de înregistrare planificate.

Divulgarea de informații nepublice către autorități

Informaţiile confidenţiale pot fi dezvăluite reprezentanţilor autorităţilor legale numai după îndeplinirea tuturor formalităţilor cerute de legislaţia în vigoare în România.

9.3.2 Informații care nu sunt considerate a fi confidențiale

certSIGN will be exonerated from the liability of disclosing confidential data if:
a) the information is known to certSIGN before it was received by the Subscriber;or
b) the information is disclosed after obtaining the written consent of the Subscriber;or
c) certSIGN is legally obliged to disclose the information.

9.3.3 Responsibilitatea de a proteja informațiile confidențiale

certSIGN si angajații săi, păstrează confidențialitatea informațiilor atât în timpul prestării serviciilor de încredere, cât și după încetarea valabilității contractelor.

9.4 Confidențialitatea informațiilor personale

În prestarea serviciilor de încredere certSIGN prelucrează date cu caracter personal ale Beneficiarului în conformitate cu cerințele Regulamentului (UE) nr. 910/2014 și cu respectarea dispozițiile de drept intern, a Regulamentului nr. 679/2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date și al altor dispoziții de drept al Uniunii referitoare la protecția datelor.
Scopul prelucrării datelor cu caracter personal este acela de a presta servicii de încredere.

9.4.1 Planul de asigurare a protectiei datelor cu caracter personal

În prestarea serviciilor de prezervare, certSIGN proceseaza date cu caracter personal conform cu Regulamentul nr. 679/2016 si alte prevederi legale legate de protectia datelor, la nivel UE sau internationale.
Măsurile de securitate cerute de Regulamentului (UE) nr. 910/2014 și Regulamentul nr. 679/2016 sunt puse în aplicare de certSIGN pentru a garanta că:

- sunt luate măsuri tehnice și organizatorice adecvate pentru asigurarea securității datelor prelucrate, pentru protejarea drepturilor persoanelor fizice și respectarea principiilor prevăzute de Regulamentul nr. 679/2016 și a prevederilor Regulamentului (UE) nr. 910/2014.
- accesul la serviciile certSIGN se referă la prelucrarea doar a acelor date de identificare, care sunt adecvate, pertinente și care nu sunt excesive pentru a acorda acces la serviciul respectiv
- este asigurată confidențialitatea și integritatea datelor de înregistrare: atunci când sunt schimbate cu beneficiarul, atunci când sunt schimbate între componentele sistemului certSIGN, precum și atunci când sunt depozitate.

9.4.2 Informatii considerate ca fiind cu caracter personal

Toate informatiile directe sau indirecte care conduc la identificarea unei persoane fizice sunt considerate ca fiind cu caracter personal.

9.4.3 Informații care nu sunt considerate private

Informatiile accesibile prin Depozitar sunt informații publice.

9.4.4 Responsabilitatea de a proteja informațiile private

certSIGN se angajează să păstreze confidențialitatea informațiilor cu caracter personal atât în timpul prestării serviciilor de încredere, cat și după încetarea acestora.
certSIGN nu va divulga informatii cu carcater personal niciunui tert, pentru niciun motiv, cu exceptia situatiilor in care va fi obligata sa o faca prin lege sau de catre autoritatile competente.

9.4.5 Notificarea persoanelor vizate pentru utilizarea datelor cu caracter personal

In procesul QPS Beneficiarii sunt informati despre necesitatea utilizarii datelor cu caracter personal care le apartin, in vederea prestarii serviciului.
Utilizarea datelor cu caracter personal poate fi facuta si pentru alte scopuri comunicate în mod expres de certSIGN prin contract sau în alt mod.
Beneficiarul este responsabil pentru natura datelor cu caracter personal conținute în documentele păstrate și pentru prelucrarea acestora în conformitate cu legislația aplicabilă protecției datelor cu caracter personal.

9.4.6 Divulgare ca urmare a unui process administrativ sau juridic

certSIGN este exonerat de răspundere pentru dezvăluirea datelor cu caracter personal în următoarele situații:

- dezvăluirea informațiilor personale față de Organismul de supraveghere conform legislației aplicabile;
- față de instituțiile și organismele abilitate, în baza obligațiilor de drept public pe care certSIGN le are, în conformitate cu prevederile legale;

9.4.7 Alte circumstante pentru divulgare

De asemenea, constituie excepții de la obligația de păstrare a confidențialității datelor cu caracter personal care exonerează certSIGN de răspundere, următoarele situații:

- ✓ dezvăluirea informațiilor personale ale Beneficiarilor față de:
  - auditori în cadrul auditurilor la care certSIGN este supus conform prevederilor Regulamentului (UE) nr. 910/2014 în condiții de confidențialitate;
  - terți care-și bazează conduita pe serviciile de încredere furnizate de certSIGN în relația cu care Beneficiarul folosește aceste servicii
  - împuterniciți către care certSIGN a externalizat anumite servicii;
  - firmele afiliate certSIGN
- ✓ în orice alte situații, cu înștiințarea în prealabil a Beneficiarului.

9.5 Drepturile de Proprietate Intelectuală

Toate mărcile, denumirile, patentele, siglele, licenţele, aplicatiile, programele software, imaginile grafice etc. folosite de certSIGN sunt şi vor rămâne proprietatea intelectuală a deţinătorilor legali ai acestora. certSIGN se obligă să specifice acest lucru conform cerinţelor impuse de deţinători.

Toate mărcile, denumirile, patentele, siglele, licenţele, aplicatiile, programele software, imaginile grafice etc., aparţinând certSIGN sunt şi rămân proprietatea acesteia, indiferent dacă sunt însoţite sau nu de patente, modele de utilitate, copyright sau altele asemenea și nu pot fi reproduse sau furnizate unei terţe părţi fără acordul prealabil în scris al certSIGN.

9.6 Reprezentări și garanții

9.6.1 Reprezentările și garanțiile certSIGN

certSIGN garantează că toate cerințele prevăzute în PPPS sunt respectate. De asemenea, își asumă responsabilitatea de a asigura o astfel de conformitate și furnizarea acestor servicii în conformitate cu PPPS.

Singura garanție oferită de certSIGN este că procedurile sale sunt puse în aplicare în conformitate cu PPPS și cu procedurile de verificare în vigoare.

9.6.2 Reprezentările și garanțiile Beneficiarului

Beneficiarul acceptă Termenii și Condițiile relevante pentru serviciul furnizat de certSIGN.

Beneficiarul este de acord cu PPPS-ul și cu responsabilitățile, îndatoririle și obligațiile sale relevante, așa cum sunt prevăzute în secțiunile relevante ale PPPS aplicabil.

9.6.3 Reprezentările și garanțiile Entităților Partenere

Entitățile partenere decid pe baza politicilor lor cu privire la modul de acceptare și utilizare a documentelor, semnăturilor și/sau ștampilelor temporale păstrate prin QPS. În timpul verificării valabilității pentru menținerea nivelului de securitate garantat de furnizorul QPS este necesar ca entitățile partenere să acționeze cu prudență, deci se recomandă în special:
• să respecte cerințele, reglementările definite în PPPS;
• utilizarea unui mediu și a unor aplicații IT fiabile;
• să ia în considerare fiecare restricție în legătură cu utilizarea care este inclusă în PPPS.

9.6.4 Reprezentările și garanțiile altor participanți

Nu se aplică.

9.7 Renunțarea la garanții

Cu excepția celor prevăzute în mod expres în PPPS aplicabil și în legislația aplicabilă, certSIGN neagă toate garanțiile și obligațiile de orice tip, inclusiv orice garanție de comercializare, orice garanție de adecvare pentru un anumit scop, precum și orice garanție a exactității informațiilor (cu excepția faptului că a venit dintr-o sursă autorizată) și nu își asumă nici o răspundere pentru neglijența și neatenția Beneficiarilor și Entităților Partenere.

9.8 Limitarea răspunderii

In limitele stabilite de legea română, în orice caz (cu excepția fraudelor sau a faptelor ilicite săvârșite cu intenție) certSIGN nu va fi răspunzător in fata Beneficiarului, partilor interesate sau terte parti, pentru:

- Orice pierderi de profit, de venituri, sau de afaceri;
- Orice pierderi de date;
- Orice daune indirecte, subsecvente sau punitive ce decurg din sau în legătură cu utilizarea, livrarea, licența, și performanța sau non-performanța serviciilor QPS;
- Orice alte daune.

În orice caz, răspunderea certSIGN va fi limitată la valoarea serviciilor de păstrare pentru fiecare cerere de păstrare și nu va depăși valoarea serviciilor pentru ultimele 6 luni înainte de apariția prejudiciului în cazul unei cereri de despăgubire, indiferent de numărul de documente păstrate sau de cereri de păstrare.

9.9 Despăgubiri

certSIGN nu își asumă nicio responsabilitate financiară pentru datele păstrate în QPS, utilizate în mod necorespunzător. certSIGN răspunde și compensează numai în limitele stabilite mai sus în art. #9.8.

9.10 Termeni și încetarea

9.10.1 Termenii

Prezentul PPPS și orice modificări ale acestuia vor intra în vigoare după publicare în Depozitar și în conformitate cu secțiunea 9.12.2 și vor rămâne în vigoare perpetuu până la încetarea lor în conformitate cu prezenta secțiune 9.10.

9.10.2 Încetarea

PPPS rămâne în vigoare până la înlocuirea cu o nouă versiune.

9.10.3 Efectul terminării și supraviețuirii

Condițiile și efectul care rezultă din incetarea acestui PPPS vor fi comunicate prin intermediul site-ului web certSIGN. Această comunicare va evidenția dispozițiile care pot supraviețui incetarii acestui PPPS și vor rămâne în vigoare. Responsabilitățile de protejare a informațiilor confidențiale și a informațiilor personale trebuie să supraviețuiască încetării, iar termenii și condițiile pentru toate serviciile existente vor rămâne valabile pentru restul perioadelor de valabilitate ale acestora.

9.11 Notificări individuale și comunicarea cu participanții

Toate notificările și alte comunicări care pot sau trebuie date sau trimise în mod obligatoriu în temeiul PPPS se vor face în scris și se vor transmite, cu excepția celor prevăzute în mod expres în PPPS, fie prin

(i) adresa poștală înregistrată, confirmare de primire, poșta preplătită,
(ii) un serviciu de curierat "în 24 de ore" sau expres recunoscut international,
(iii) livrarea în mână
(iv) transmiterea prin fax, considerată a fi primită la livrarea efectivă sau la finalizarea fax-ului, sau
(v) în format electronic, semnat cu o semnătură electronică calificată și să fie adresată certSIGN, folosind datele de contact furnizate în capitolul 1.5.1 din prezentul document.

9.12 Amendamente

9.12.1 Procedura pentru amendamente

certSIGN este responsabilă, prin Comitetul de Management al Politicilor și Procedurilor (CMMP), de aprobarea și modificarea prezentului PPPS. PPPS se revizuiește cel puțin odată pe an.

Singurele modificări pe care le poate face CMMP acestor specificații PPPS fără notificare sunt modificări minore care nu afectează nivelul de încredere al acestui PPPS, de exemplu, corecturi editoriale sau tipografice sau modificări ale detaliilor de contact.

Erorile, actualizările sau sugestiile de modificare a acestui document vor fi comunicate așa cum este menționat în prezentul PPPS, secțiunea 1.5.4. O astfel de comunicare va include o descriere a schimbării, o justificare a schimbării, precum și informațiile de contact ale persoanei care solicită modificarea.

CMMP va accepta, modifică sau respinge modificarea propusă după finalizarea unei faze de revizuire.

Orice modificări la PPPS sunt aprobate de CMMP și sunt anunțate clienților certSIGN. Beneficiarii trebuie să respecte numai cerințele PPPS aplicabile în prezent.

9.12.2 Mecanismul de notificare și perioada

Toate modificările aduse prezentului PPPS aflate în analiza CMMP vor fi distribuite părților interesate pentru o perioadă de minimum 2 zile. Data emiterii și data intrării în vigoare sunt indicate pe pagina titlului prezentului PPPS.

9.13 Procedurile de soluționare a litigiilor

Toate disputele asociate prezentului PPPS vor fi rezolvate în conformitate cu legile din România, de către tribunale românești și în limba română.

9.14 Legea aplicabilă

Legea română guvernează aplicabilitatea, construirea, interpretarea, și validitatea prezentului PPPS (cu excluderea oricarui conflict de legii care ar determina aplicarea altor legi nationale sau internationale).

9.15 Conformitatea cu legea aplicabilă

Prezentul PPPS și furnizarea serviciilor certSIGN sunt conforme cu legile române relevante și aplicabile și regulamentul EU 910/2014.

9.16 Prevederi diverse

certSIGN asigura accesul nerestrictionat la serviciile furnizate pentru persoanele cu disabilitati in conformitate cu legislatia si standardele in vigoare.