certSIGN Autoritatea de Marcare Temporală 2

Codul de Politici, Practici și Proceduri

Versiunea 3.6

Data: 22 Iunie 2026

Nivel Securitate

Document Public

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 (ultima zi a lunii)	Motiv	Persoana care a făcut modificarea
1.0	Ianuarie 2017	Publicarea primei versiuni	Manager Servicii Electronice
2.0	Martie 2017	A doua versiune, după audit intermediar	Ofițer securitate informatică
2.1	Aprilie 2017	Actualizare minoră, pentru clarificare	Ofițer securitate informatică
2.2	Februarie 2018	Revizie anuala	Ofițer securitate informatică
2.3	Noiembrie 2018	Actualizare determinata de schimbarea sediului	Manager Politici PKI
2.4	Ianuarie 2019	Revizie anuala	Manager Politici PKI
2.5	Martie 2019	Actualizare minoră, pentru clarificare	Manager Politici PKI
2.6	Aprilie 2019	Actualizare minoră, pentru clarificare	Manager Politici PKI
2.7	Ianuarie 2020	Revizuire anuala	Manager Politici PKI
2.8	Ianuarie 2021	Revizuire anuala	Manager Politici PKI
2.9	Ianuarie 2022	Revizuire anuala	Manager Politici PKI
3.0	Ianuarie 2023	Revizuire anuala	Manager Politici PKI
3.0a	Aprilie 2023	Actualizare link-uri	Manager Politici PKI
3.1	Ianuarie 2024	Revizuire anuala	Manager Politici PKI
3.2	15 Ianuarie 2025	Revizuire anuala	Manager Politici PKI
3.3	18 Iulie 2025	Adaugare Ciclul de viata TSU	Manager Politici PKI
3.4	15 Ianuarie 2026	Revizuire anuala	Manager Politici PKI
3.5	31 Martie 2026	Actualizari pt conformitate eIDAS2	Manager Politici PKI
3.6	22 Iunie 2026	Adaugare SHA512	Manager Politici PKI

Acest document a fost creat de către și este proprietatea:

Proprietar	Autor	Data creării
Ofițer Securitate Informatică	Ofițer Securitate Informatică	Decembrie 2016

Lista de distribuție

Destinație	Data distribuirii
Public-Internet	Ianuarie 2017
Public-Internet	Martie 2017
Public-Internet	Aprilie 2017
Public-Internet	Februarie 2018
Public-Internet	Noiembrie 2018
Public-Internet	Ianuarie 2019
Public-Internet	Martie 2019
Public-Internet	Aprilie 2019
Public-Internet	Ianuarie 2020
Public-Internet	Ianuarie 2021
Public-Internet	Ianuarie 2022
Public-Internet	Ianuarie 2023
Public-Internet	Aprilie 2023
Public-Internet	Ianuarie 2024
Public-Internet	Ianuarie 2025
Public-Internet	Iulie 2025
Public-Internet	Ianuarie 2026
Public-Internet	Martie 2026
Public-Internet	Iunie 2026

Acest document a fost aprobat de:

Versiune	Nume	Data
1.0	Comitet de Management al Politicilor și Procedurilor	Ianuarie 2017
2.0	Comitet de Management al Politicilor și Procedurilor	Martie 2017
2.1	Comitet de Management al Politicilor și Procedurilor	Aprilie 2017
2.2	Comitet de Management al Politicilor și Procedurilor	Februarie 2018
2.3	Comitet de Management al Politicilor și Procedurilor	Noiembrie 2018
2.4	Comitet de Management al Politicilor și Procedurilor	Ianuarie 2019
2.5	Comitet de Management al Politicilor și Procedurilor	Martie 2019
2.6	Comitet de Management al Politicilor și Procedurilor	Aprilie 2019
2.7	Comitet de Management al Politicilor și Procedurilor	Ianuarie 2020
2.8	Comitet de Management al Politicilor și Procedurilor	Ianuarie 2021
2.9	Comitet de Management al Politicilor și Procedurilor	Ianuarie 2022
3.0	Comitet de Management al Politicilor și Procedurilor	Ianuarie 2023
3.0a	Comitet de Management al Politicilor și Procedurilor	Aprilie 2023
3.1	Comitet de Management al Politicilor și Procedurilor	Ianuarie 2024
3.2	Comitet de Management al Politicilor și Procedurilor	Ianuarie 2025
3.3	Comitet de Management al Politicilor și Procedurilor	Iulie 2025
3.4	Comitet de Management al Politicilor și Procedurilor	Ianuarie 2026
3.5	Comitet de Management al Politicilor și Procedurilor	Martie 2026
3.6	Comitet de Management al Politicilor și Procedurilor	Iunie 2026

Cuprins

1 Scop 6
2 Referinte 6
2.1 Referinte Normative 6
2.2 Referinte Informative 6
3 Definitii si abreviatii 7
3.1 Definitii 7
3.2 Abreviatii 8
4 Concepte generale 9
4.1 Concepte și condiții generale 9
4.2 Servicii de marcare temporala 9
4.3 Parti ale serviciilor de marcare temporala 9
4.3.1 Autoritatea de marcare temporala (TSA) 9
4.3.2 Beneficiar 9
4.3.3 Entitate parteneră TSA 10
4.4 Ciclul de viață al TSU 10
5 Politici de marcare temporală 11
5.1 Generale 11
5.2 Identificarea 11
5.3 Comunitate utilizatori și aplicabilitate 11
6 Politici si Practici 12
6.1 Evaluarea riscurilor 12
6.2 Codul de practici și proceduri pentru serviciile de încredere 12
6.2.1 Formatul mărcilor temporale 12
6.2.2 Acuratețea timpului 12
6.2.3 Limitele serviciului 12
6.2.4 Obligațiile beneficiarilor 13
6.2.5 Obligațiile entităților partenere 13
6.2.6 Verificarea mărcii temporale 13
6.2.7 Legea aplicabilă 13
6.2.8 Disponibilitatea serviciului 13
6.2.9 Procedurile de aprobare a CPP 13
6.3 Termeni si conditii 14
6.3.1 Implementarea politicii serviciului de încredere 14
6.3.2 Perioada de păstrare a jurnalelor 14
6.4 Politica de securitate informatică 14
6.5 Obligațiile TSA 14
6.5.1 Obligațiile TSA față de beneficiari 14
6.6 Informații pentru entitățile partenere 14
7 Managementul TSA și Operațiuni 15
7.1 Introducere 15
7.2 Organizarea internă 15
7.3 Personal de încredere 15
7.4 Controlul gestiunii 17
7.5 Controlul accesului 17
7.6 Controale criptografice 18
7.6.1 Generarea cheii TSU 18
7.6.2 Protejarea cheii private a TSU 19
7.6.3 Certificat cheie publică TSU 21
7.6.4 Reînnoire cheii TSU 21
7.6.5 Managementul ciclului de viață al hardware-ului criptografic 21
7.6.6 Sfârșitul ciclului de viață al cheii TSU 22

7.7 Marcarea temporală 22
7.7.1 Emitentul mărcilor temporale 22
7.7.2 Sincronizarea ceasului cu UTC 22
7.8 Securitatea fizică și a mediului 22
7.9 Security of operations 24
7.10 Securitatea rețelei 25
7.11 Managementul incidentelor 26
7.12 Colectarea dovezilor 27
7.13 Managementul continuității afacerii 27
7.14 Încetarea activității TSA și planurile încetării activității 28
7.15 Conformitatea 28

1 Scop

Acest document este Politica de marcare temporala si Codul de Practici si Proceduri al Autorității Marcare Temporala certSIGN (TSPS). Trebuie să citiți TSPS înainte de a solicita serviciul certSIGN Time Stamping 2. Scopul acestui document este de a specifica cerințele de politică și de securitate referitoare la practicile de operare și gestionare ale certSIGN ca Autoritate de Marcare Temporala în conformitate cu standardul ETSI EN 319 421 "Cerințe de politică și securitate pentru furnizorii de servicii de încredere care eliberează marci temporale" (denumita in continuare, certSIGN Time Stamping Authority 2 sau certSIGN TSA) pentru emiterea marcilor temporale calificate. Acestea pot fi utilizate în sprijinul semnăturilor electronice sau pentru orice aplicație care necesită dovada existenței unui datări înainte de o anumită perioadă de timp.
Această versiune a TSPS a fost aprobată pentru utilizarea de către Comitetul de Management al Politicilor și Procedurilor certSIGN și poate fi modificată în conformitate cu politicile și liniile directoare adoptate periodic de Comitetul de Management al Politicilor și Procedurilor certSIGN, Secțiunea 6.2.9. Data la care această versiune a TSPS devine efectivă este indicată în acest document.

2 Referinte

2.1 Referinte Normative

1. Regulamentul (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
2. Regulamentul (UE) 2024/1183 al Parlamentului European și al Consiliului din 11 aprilie 2024 de modificare a Regulamentului (UE) nr. 910/2014 în ceea ce privește instituirea cadrului european pentru identitatea digitală
3. IETF RFC 3161 "Internet X.509 Protocolul cu privire la infrastructura cheilor publice pentru Marci temporale"
4. ETSI EN 319 401: " Semnături electronice și infrastructuri (ESI); Cerințe generale de politică pentru furnizorii de servicii de încredere"
5. ETSI EN 319 421: " Semnături electronice și infrastructuri (ESI); Politică și securitate a. Cerințe pentru furnizorii de servicii de încredere care emit marci temporale"
6. ETSI EN 319 422: " Semnături electronice și infrastructuri (ESI); Protocolul de temporala și profilele token-urilor de timp ".
7. Legea nr.2014/2024 privind utilizarea semnăturii electronice, a mărcii temporale și prestarea serviciilor de încredere bazate pe acestea

2.2 Referinte Informative

1. recomandarile ITU-R TF.460-6 (2002): "Frecvență standard și emisii de timp ".
2. IETF RFC 5905: "Protocol de timp pentru rețea Versiunea 4: Specificații de protocol și algoritmi"
3. Termeni și condiții pentru clienții de marca temporala in www.anf.es
4. ISO/IEC 19790:2012: "Tehnologia informației - Tehnici de securitate - Cerințe de securitate pentru modulele criptografice".
5. ISO/IEC 15408 (parts 1 to 3): "Tehnologia informației - Tehnici de securitate - Criterii de evaluare pentru securitatea IT ".
6. FIPS PUB 140-3 (2019): "Cerințe de securitate pentru modulele criptografice ".

3 Definitii si abreviatii

3.1 Definitii

- **Ora universală coordonată (UTC)**: Scala de timp bazată pe secunda, așa cum este definită în Recomandarea ITU-R TF.460-6. Pentru toate scopurile practice, UTC este echivalent cu media timpului solar în meridianul principal (0°). Mai precis, UTC este un compromis între timpul atomic extrem de stabil (Temps Atomique International - TAI) si timpul solar derivat din rotația neregulată a Pământului. UTC este standardul principal al orei prin care lumea reglează ceasurile și timpul.
- **NTP**: "Network Time Protocol (NTP) este un protocol de rețea pentru sincronizarea ceasurilor sistemelor informatice prin rutarea pachetelor de rețea cu latență variabilă. Standardul de referință este IETF RFC 1305 (Network Time Protocol (NTP v3).
- **Ministerul Comunicațiilor și Societății Informaționale**: În scopuri juridice declarate ca standard național al acestei unități, precum și întreținerea și diseminarea oficială a scalei "Coordinated Universal Time"
- **Entitate Partenera**: Destinatarul unei marci temporale care se bazează pe acea marca temporala.
- **Autoritatea de Macrcare (TSA)**: Este TSP care oferă servicii de marcare temporala folosind una sau mai multe unități de marcare temporala.
- **Beneficiar**: Persoana juridical sau fizica pentru care se emite o marca temporala.
- **Marca temporala**: Datele în formă electronică care leagă alte date electronice de un moment dat, furnizând dovezi că aceste date au existat la un moment dat.
- **Politica de marcate temporala**: Un set de reguli care indică aplicabilitatea unei marci temporale pentru o comunitate și / sau o clasă de aplicatii a cerințelor comune de securitate. Acesta este un tip specific de politică privind serviciile de încredere, asa cum este definită în ETSI EN 319 421.
- **Serviciu de marcare temporala:** serviciu de incredere pentru emiterea de marci temporale.
- **Unitate de marca temporala (TSU)**: Setul de hardware și software care este gestionat ca unitate și are o singură cheie de semnare a unei marci temporale active.
- **Furnizor de servicii de incredere (TSP)**: Entitate care oferă unul sau mai multe servicii de încredere.
- **TSA Disclosure statement**: Set de declarații privind politicile și practicile unui TSA care necesită în mod special accentul în dezvăluirea către beneficiari și entitatile partenere, de exemplu, pentru a îndeplini cerințele de reglementare.
- **TSA Cod de practici**: Declarația privind practicile utilizate de TSA în emiterea marcilor temporale.
- **Sistem TSA**: Set de produse și componente IT utilizate pentru a oferi suport pentru furnizarea de servicii de marcare temporală.
- **UTC (k)**: Scală de timp dată de laboratorul "k" și care are o relație strânsă cu UTC, cu scopul de a atinge ± 100 ns.
- **certSIGN TSA:** Reprezintă "Autoritatea de marcare temporala certSIGN 2", care este Autoritatea de marcare temporala a certSIGN care funcționează în conformitate cu ETSI EN 319 421 "Cerințe de politică și securitate pentru furnizorii de servicii de încredere care emit marci temporale".

3.2 Abreviatii

Pentru scopurile prezentului document, abrevierile sunt după cum urmează:

BIPM Bureau International des Poids et Mesures
CA Autoritate de Certificare
IT Tehnologi informatiilor
PPMB Comitet de Management al Politicilor și Procedurilor
TAI Timpul International Atomic
TSA Marcare Temporala
TSP Furnizor de servicii de incredere
TST Token de marca temporala
TSU Unitate de marca temporala
UTC Timpul Universal Coordonat

4 Concepte generale

4.1 Concepte și condiții generale

TSPS Este o descriere detaliată a termenilor și condițiilor privind furnizarea serviciilor, a practicilor manageriale și operaționale pe care certSIGN Time Stamping Authority 2 le aplică în furnizarea serviciilor de marcare temporală.

4.2 Servicii de marcare temporala

Furnizarea serviciilor de marcare temporala este defalcată, în prezentul document, în următoarele servicii componente în scopul clasificării cerințelor:

- **Furnizarea de marci temporale**: Această componentă de serviciu generează TSTs.
- **Gestionarea marcilor temporale**: Componenta de serviciu care monitorizează și controlează funcționarea serviciilor de marcare a timpului pentru a se asigura că serviciul furnizat este conform specificațiilor din CPS și TSA CPS.

certSIGN TSA aderă la standardele și reglementările stabilite în secțiunea 2 a acestui document pentru a menține încrederea serviciilor de marcare a timpului pentru beneficiari și entitatile partenere.

4.3 Parti ale serviciilor de marcare temporala

4.3.1 Autoritatea de marcare temporala (TSA)

Un Furnizor de Servicii de Încredere (TSP) care furnizează publicului servicii de marcare temporală, este numit Autoritate de Marcare Temporală (TSA). TSA are responsabilitatea generală de furnizare a serviciilor de marcare temporală identificate în clauza 4.2. TSA este responsabil de operarea a una sau mai multe TSU-uri care creează și semnează în numele TSA. TSA-ul responsabil de emiterea mărcilor temporale este identificabil.
TSA certSIGN confirmă că TSA este auditat cel puțin o dată la 24 de luni de un organism de evaluare a conformității. Raportul de evaluare este trimis organismului național de supraveghere. Dacă organismul de supraveghere cere TSA să remedieze orice neîndeplinire a cerințelor, certSIGN in calitate de TSA va acționa în mod corespunzător și într-o manieră promptă.
Organismul de supraveghere va fi informat asupra oricărei modificări în furnizarea TSA-ului.
TSA certSIGN poate apela la alte părți pentru a furniza părți ale serviciilor de marcare temporală. Totuși, TSA-ul își asumă întotdeauna responsabilitatea globală (conform clauzei 6.5) și asigură că cerinețele politicii identificate în prezentul document sunt îndeplinite.
TSA certSIGN poate opera mai multe unități de marcare temporală identificabile.
TSA certSIGN este un prestator de servicii de încredere calificat, așa cum este descris în eIDAS, care emite mărci temporale calificate.
TSA certSIGN este identificată în certificatul TSU folosit pentru semnarea TST.

Date de contact:
certSIGN SA
Adresă: Bd. Tudor Vladimirescu, nr. 29 A, AFI Tech Park 1, București, România
Telefon: 004-021-31.19.901
Web: www.certsign.ro

4.3.2 Beneficiar

În cazul în care beneficiarul este un utilizator final, utilizatorul final va fi direct responsabil dacă nu își îndeplinește corect obligațiile.
În cazul în care beneficiarul este o organizație, ea cuprinde mai mulți utilizatori finali sau un utilizator final individual, iar unele dintre obligațiile care se aplică organizației trebuie să se aplice

și utilizatorilor finali. În orice caz, organizația va fi responsabilă dacă utilizatorii finali nu își îndeplinesc obligațiile corect; prin urmare, o astfel de organizație trebuie să își informeze în mod adecvat utilizatorii finali.

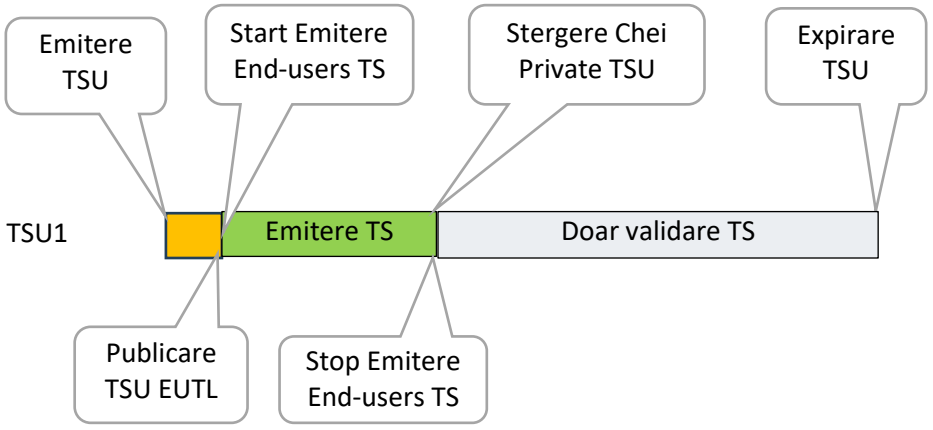
4.3.3 Entitate parteneră TSA

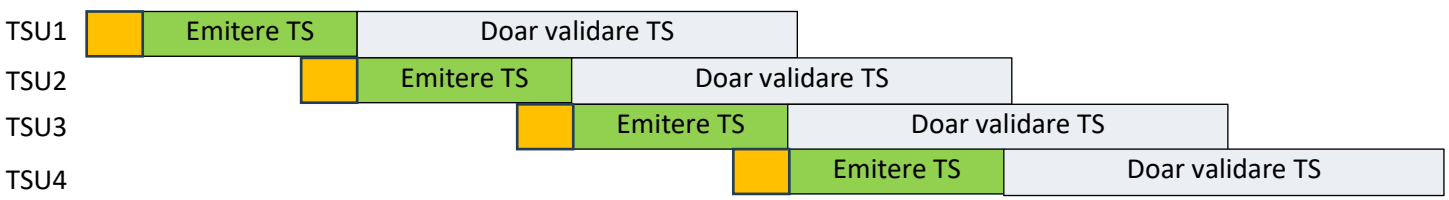
O entitate parteneră este un individ sau o entitate care acționează invocând un TST generat în cadrul politicii TSA certSIGN [ETSI EN 319 421]. O entitate parteneră poate sau nu poate fi și un beneficiar.

4.4 Ciclul de viață al TSU

certSIGN emite în fiecare an un nou certificat de ștampilă de timp, o TSU, cu o valabilitate de maxim 3 ani.
Cea mai nouă unitate (TSU1) va emite marci de timp pentru utilizatorii finali pentru o durată de un an de la publicarea sa în EU TL. Între emiterea certificatului TSU și publicarea acestuia în EU TL poate exista o diferență de 1-2 luni.
După un an, când noul certificat de unitate de marcă temporală (TSU2) va fi emis și apoi publicat în EU TL, cheile private ale certificatului anterior de unitate de marcă temporală (TSU1) vor expira sau vor fi șterse pentru a fi utilizate numai pentru validarea certificatelor de marcă temporală pentru utilizatorii finali deja emise.
Noua unitate TSU2 va deveni TSU activă care va emite mărci de timp pentru utilizatorii finali.
După încă un an, va fi emis un nou certificat de unitate de marcare temporală, TSU3, care va fi publicat în TL UE. Cheile private ale certificatului anterior (TSU2) vor expira sau vor fi șterse pentru a putea fi utilizate numai pentru validarea certificatelor de marcă temporală pentru utilizatorii finali deja emise.

După încă un an, va fi emis un nou certificat de unitate de marcă temporală, TSU4, care va fi publicat în TL UE. Cheile private ale certificatului anterior (TSU3) vor expira sau vor fi fi șterse pentru a putea fi utilizate numai pentru validarea certificatelor deja emise de utilizatorii finali.
Iar ciclul de viață continuă an de an, conform imaginii de mai jos.





5 Politici de marcare temporală

5.1 Generale

TSA certSIGN generează TST-uri în conformitate cu ETSI EN 319 421 și Politica de Marcare Temporală. TST-urile sunt emise cu o acuratețe de o secundă față de UTC sau mai bine.

5.2 Identificarea

Identificatorul politicii de marcare temporală specificat în prezentul document este OID:

1.3.6.1.4.1.25017.2.2.1

{iso(1) identified-organization(3) dod(6) internet (1) private(4) enterprise(1) certSIGN (25017) TSA(2) CPS-PC-EU Regulation 910/2014(2)}

- 1 is the number of the TS Unit

Prin includerea acestui identificator de obiect în mărcile temporale generate, TSA certSIGN își afirmă conformitatea cu această politică de marcare temporală.

Marcile teporale pot include si OID **0.4.0.2023.1.1**, dacă acest lucru este specificat în conținutul cererii de marca temporala.

5.3 Comunitate utilizatori și aplicabilitate

Această politică are ca scop satisfacerea cerințelor de marcare temporală pentru valabilitatea pe termen lung (de exemplu, așa cum este definit în ETSI EN 319 122), dar este, în general, aplicabilă oricărei utilizări care are o cerință de calitate echivalentă. Această politică poate fi folosită pentru servicii publice de marcare temporală sau pentru servicii de marcare temporală utilizate într-o comunitate închisă.

6 Politici si Practici

6.1 Evaluarea riscurilor

certSIGN TSA efectuează evaluări de risc în mod regulat pentru a asigura calitatea și fiabilitatea serviciilor de marcare temporala. Controalele de securitate definite într-un cadru de securitate pentru serviciile de marcare temporala sunt controlate la fiecare șase luni pentru a asigura eficiența acestora.
Procesul de management al riscului al certSIGN acoperă în detaliu acest subiect.

6.2 Codul de practici și proceduri pentru serviciile de încredere

Asigurarea Calității este una dintre cele mai importante calități ale TSA certSIGN. Prin urmare, au fost implementate o varietate de controale de securitate pentru a asigura calitatea, performanța și funcționarea serviciului de marcare temporală.
Controalele de securitate sunt documentate și sunt verificate în mod regulat de o entitate independentă, de încredere și capabilă să verifice respectarea controalelor de securitate.
În plus, pentru conformitatea cu ETSI EN 319 421, următoarele măsuri au fost aplicate , respectiv, următoarelor servicii:

6.2.1 Formatul mărcilor temporale

Token-ul de marcă temporală emis de TSA certSIGN este conform cu standardul RFC 3161 privind mărcile temporale. Serviciul emite mărci temporale cu un algoritm RSA și o lungime a cheilor de 4096[1] biți, care acceptă algoritmul de hash SHA512, SHA384 si SHA256.

6.2.2 Acuratețea timpului

TST-urile sunt emise cu o acuratețe de 1 secundă de UTC sau mai bine.

6.2.3 Limitele serviciului

Serviciul de marcare temporală al TSA certSIGN poate fi utilizat pentru orice tranzacție legală, fără limitări. În limitele stabilite de lege, certSIGN nu va fi responsabilă în nici un caz (cu excepția fraudelor sau a faptelor ilicite săvârșite cu intenție) pentru:

- Orice pierdere de profit;
- Orice pierdere de date;
- Orice daune indirecte, subsecvente sau punitive ce decurg din sau în legătură cu utilizarea, livrarea, licența, și performanța sau non-performanța certificatelor sau a semnăturilor digitale;
- Orice alte daune.

certSIGN nu își asumă responsabilitatea financiară pentru mărcile temporale folosite necorespunzător.

certSIGN va acoperi prejudiciile pe care le-ar putea cauza datorita furnizarii serviciilor de marcare temporala persoanelor care si-au construit conduita morala pe efectele legale ale certificatelor calificate până la echivalentul în lei al sumei de 10.000 de euro pentru fiecare risc asigurat.

certSIGN va acoperi prejudiciile pe care le-ar putea cauza datorita furnizarii serviciilor de marcare temporala persoanelor care si-au construit conduita morala pe efectele legale ale certificatelor calificate până la echivalentul în lei al sumei de 10.000 de euro pentru fiecare risc asigurat. Riscul asigurat reprezintă fiecare prejudiciu cauzat, chiar și în cazul în care există mai multe astfel de prejudicii ca urmare a neîndeplinirii de către furnizor a obligațiilor menționate de lege.

[1] *TSU-ul activ emite chei cu 2048 biti. Urmatorul TSU, din Q4 2026 va emite chei cu 4096 biti.*

6.2.4 Obligațiile beneficiarilor

Pentru informații detaliate, a se vedea "Termeni și condiții pentru serviciile de marcare temporală".

6.2.5 Obligațiile entităților partenere

Pentru informații detaliate, a se vedea "Termeni și condiții pentru serviciile de marcare temporală".

6.2.6 Verificarea mărcii temporale

Verificarea mărcii temporale include următoarele:

Verificarea emitentului mărcii temporale

Emitentul este o autoritate de marcare temporală care utilizează certificate digitale adecvate pentru emiterea mărcii temporale. Cheile publice ale certificatelor utilizate sunt incluse în TSU și în certificatele CA și sunt publicate pentru a putea verifica dacă marca temporală a fost semnată de către TSA.

Verificarea stării de revocare a mărcii temporale

Verificarea revocării certificatului TSU se face utilizând serviciul OCSP disponibil la http://ocsp.certsign.ro sau CRL disponibil la http://crl.certsign.ro/certsign-qualifiedca.crl sau la https://crl.certsign.ro/certsign-qualifiedca2023rsa.crl.

Verificarea integrității mărcii temporale

Integritatea criptografică a mărcii temporale, de exemplu structura ASN.1 este corectă, și un set de date (datele au fost marcate temporal) aparțin aplicației. Acest lucru poate fi verificat prin serviciul web al TSA certSIGN, care este oferit gratuit.

6.2.7 Legea aplicabilă

Pentru informații detaliate, a se vedea "Termeni și condiții pentru serviciile de marcare temporală".

6.2.8 Disponibilitatea serviciului

TSA certSIGN a implementat următoarele măsuri pentru a asigura disponibilitatea serviciului:

- Configurarea redundantă a sistemelor informatice, pentru a evita un punct unic de avarie.
- Conexiuni Internet de mare viteză redundante, pentru a evita pierderea serviciului,
- Utilizarea de surse de curent electric neîntreruptibile și generator electric.

Deși aceste măsuri asigură disponibilitatea serviciului TSA certSIGN, o disponibilitate anuală de 100% nu poate fi garantată. TSA certSIGN își propune să ofere o disponibilitate a serviciului de 99% pe an.

6.2.9 Procedurile de aprobare a CPP

certSIGN este responsabil prin intermediul Comitetul de Management al Politicilor si Procedurilor pentru aprobarea și modificarea TSPS. TSPS este revizuită cel puțin o dată pe an.

Singurele modificări pe care PPMB le poate face specificațiilor TSPS fără notificare sunt modificări minore care nu afectează nivelul de asigurare al TSPS, de ex.: corecții editoriale sau tipografice sau modificări ale detaliilor de contact.

Sunt comunicate erori, actualizări sau sugestii de modificari ale acestui document, inclusiv o descriere a modificării, o justificare a modificării și informații de contact ale persoanei care solicită modificarea.

PPMB acceptă, modifică sau respinge modificarea propusă după finalizarea unei faze de revizuire.

Orice modificări ale CPP sunt aprobate de PPMB și, dacă este necesar, sunt anunțate clienților certSIGN. Subiectii/Beneficiarii trebuie să respecte numai cerințele CPP aplicabile în prezent.

Beneficiarii trebuie să respecte numai documentul aplicabil în prezent. Beneficiarii care nu acceptă termenii și regulamentele noi modificate ale TSPS fac o declarație adecvată în termen de 15 zile de la data efectivă a noii versiuni publicate a TSPS. Aceasta va conduce la rezilierea contractului privind serviciile de marcare temporala furnizate.

6.3 Termeni si conditii

Documentul publicat "Termeni și condiții de utilizare a serviciilor de marcare temporală ", conține informații despre, de exemplu, limitele serviciului, obligațiile beneficiarului, informațiile pentru entitățile partenere sau limitări de responsabilitate. În plus, următoarele informații se aplică:

6.3.1 Implementarea politicii serviciului de încredere

Prezentul document informează despre politica aplicabilă serviciului de încredere. Pentru detalii suplimentare, a se vedea capitolul 5.

6.3.2 Perioada de păstrare a jurnalelor

Jurnalele de evenimente ale TSP sunt stocate în fișiere de pe discul de system, până când acestea ating limita maximă admisă. După depășirea spațiului alocat, jurnalele sunt stocate în arhive și sunt disponibile doar off-line. Jurnalele arhivate sunt păstrate pentru cel puțin 10 ani.

6.4 Politica de securitate informatică

TSA certSIGN a implementat o politică de Securitate informatică în întreaga companie. Toți angajații trebuie să adere la reglementările prevăzute în această politică și la conceptele de securitate derivate. Politica de securitate informatică este revizuită în mod regulat, în special atunci când au loc modificări semnificative. Consiliul director al certSIGN aprobă modificările politicii de securitate informatică.

6.5 Obligațiile TSA

6.5.1 Obligațiile TSA față de beneficiari

Conformitatea cu procedurile prevăzute în prezentul document este asigurată de TSA certSIGN. Un organism independent de supraveghere verifică eficiența procedurilor în mod regulat.

Prezentul document nu plasează nicio obligație specială asupra beneficiarului, dincolo de orice alte cerințe specifice TSA menționate în clauza 11 din **Termeni si conditii** pentru utilizarea serviciului de marcare temporala oferit de **certSIGN Time Stamping Authority 2.**

6.6 Informații pentru entitățile partenere

- Entitățile partenere verifică dacă TST-ul a fost semnat corec, cu cheia corespunzătoare a certificatului TSU și se asigură că cheia private folosită la semnarea TST nu a fost revocată.
- Entitățile partenere sunt obligate să ia toate măsurile necesare pentru a asigura validitatea TST dincolo de durata de viață a certificatelor TSA certSIGN.
- Trebuie să ia în considerare orice limitări privind utilizarea mărcii temporale indicate de politica de marcare temporală.
- Trebuie să ia în considerare orice alte măsuri de precauție prevăzute în acorduri sau în orice altă parte.

7 Managementul TSA și Operațiuni

7.1 Introducere

TSA certSIGN a implementat un system de management al securității infromatice pentru menține securitatea serviciului.
Furnizarea unui TST ca răspuns la o cerere este la discreția TSA certSIGN, în funcție de acordul beneficiarului.

7.2 Organizarea internă

Structura oganizatorică a companiei certSIGN, politicile, procedurile și controalele se aplică și TSA certSIGN.
Procedurile organizaționale respectă regulile și reglementările definite în secțiunea 2.1 a acestui document.

a) Entitate legală
Autoritatea de Marcare Temporală este furnizată de certSIGN SA.
certSIGN SA este o companie de tehnologie specializată în dezvoltarea și producerea de produse, soluții și servicii de securitate informatică:

certSIGN SA
Adresa: Bd. Tudor Vladimirescu, nr. 29 A, AFI Tech Park 1, București, România
Telefon: 004-021-31.19.901
Web: www.certsign.ro

b) Managementul securității informatice și managementul calității serviciului sunt realizate în cadrul conceptului de securitate al serviciului.

7.3 Personal de încredere

certSIGN asigură că persoana care își îndeplinește responsabilitățile de serviciu, în accord cu rolul alocat în cadrul Autorității de Marcare Temporală:

- A absolvit cel puțin liceul,
- Este cetățean român,
- A semnat un contract care descrie rolul și responsabilitățile sale în cadrul sistemului,
- A urmat un program de formare, în acord cu obligațiile sale și sarcinile asociate postului său, sau a furnizat evidente de cunostinte, experienta si calificari de specialist/expert.
- A fost instruit/ă cu privire la protecția datelor cu caracter personal și a informațiilor confidențiale sau private,
- A semnat un contract ce conține clauze privind protecția informațiilor sensibile (din punctul de vedere al securității certSIGN) și datele private și confidențiale ale Beneficiarilor,
- Nu îndeplinește activități care pot genera conflicte de interes.

Personalul angajat al certSIGN care îndeplinește un rol de încredere trebuie să obțină avizul administratorului de securitate.
În cadrul certSIGN, următoarele roluri de încredere sunt definite, roluri ce pot fi atrbuite uneia sau mai multor persoane:

- **Administrator de securitate** – Responsabilitate globală de implementare a politicilor și procedurilor de securitate.
- Inițiază instalarea, configurarea și managementul aplicațiilor software și hardware ale certSIGN (inclusiv resurse de rețea); inițiază și suspendă serviciile furnizate de certSIGN; coordonează administratorii, inițiază și supraveghează generarea cheilor și generarea secretelor partajate; aprobă drepturile în ceea ce privește securitatea și privilegiile de acces ale utilizatorilor; verifică jurnalele de evenimente; supraveghează auditurile interne și

externe; primește și răspunde la rapoartele de audit; supraveghează eliminarea deficiențelor constatate în urma auditului.
- Supraveghează operatorii;
- Verifică conformitatea cu Politica de Marcare Temporală și cu Codul de Practici și Proceduri;
- **Administrator de sistem** – Autorizat să instaleze, configureze și să gestioneze sistemele și aplicațiile Autorității de Marcare Temporală.
- **Operator de sistem** – Responsabil cu operarea zilnică a sistemelor și aplicațiilor TSA. Autorizat să execute operațiile de back-up și repornire a sistemului; transferă copiile de back-up ale arhivei și ale datelor curente în afara locației certSIGN.
- **Administrator HSM** – Gestionează modulul de securitate și creează carduri de operatori.
- **Operator HSM** – Pornește aplicația de marcare temporală.
- **Administrator registru electronic** – se asigură că toate înregistrările sunt făcute și păstrate în conformitate cu Politica de Marcare Temporală.
- **Auditor de sistem** – autorizat să acceseze arhivele, jurnalele de audit ale sistemelor de încredere ale Autorității de Certificare. Responsabil cu realizarea auditurilor interne de conformitate cu Codul de Practici și Proceduri al Autorității de Certificare; această responsabilitate se extinde și asupra Autorității de Înregistrare care operează în cadrul certSIGN.

Numărul de persoane necesare pentru efectuarea unei sarcini

Procesul de generare a cheilor – pentru semnarea mărcilor temporale – este unul dintre operațiunile care necesită atenție specială. El necesită prezența a cel puțin două persoane: un administrator de securitate și un administrator de sistem. Deținătorii secretului partajat – care păstrează partea lor de cheie într-o locație sigură – participă de asemenea la procesul de generare a cheii unui TSU.

Prezența administratorului de securitate și a unui număr adecvat de deținători ai secretului partajat este de asemenea necesară la încărcarea cheii criptografice în modulul hardware de securitate.

Activarea cheii private necesită cvorumul conform schemei de prag; acest lucru înseamnă că prezența deținătorilor secretului partajat este de asemenea necesară de fiecare dată când serviciul este repornit.

Orice altă operațiune sau rol, descris în acest Cod de Practici poate fi realizat/ă de către o singură persoană, desemnată în mod special în acest scop.

Identificarea și autentificarea pentru fiecare rol

Personalul certSIGN este supus identificării și autentificării de fiecare dată când accesează camera un sistem informatic echipat cu sisteme de control al accesului. Identificarea și autentificarea se face prin una dintre următoarele metode sau o combinație a acestora:

- Nume și parolă
- Cheie privată stocată electronic și PIN
- Cheie privată stocată pe o componentă hardware (pe un dispozitiv criptografic) și PIN
- Card de acces cu fotografia deținătorului
- Fiecare cont alocat:
- Trebuie să fie unic și să fie alocat unei anumite persoane,
- Nu poate fi partajat cu nicio altă persoană,
- Este restricționat, în conformitate cu poziția (care decurge din rolul îndeplinit de persoana în cauză) pe baza software-ului de sistem al certSIGN, a sistemului de operare și a controalelor de aplicații.

Fiecare dispozitiv criptografic sau card de acces al utilizatorului este înmânat de administratorul de securitate, pe baza unei declarații.

Cerințele de pregătire a personalului

Personalul care îndeplinește roluri și activități în urma asumării unui rol în cadrul Autorității de Marcare temporală trebuie instruit cu privire la:

- Reglementările Codului de Practici și Proceduri,
- Politicile de marcare temporală,
- Măsurile active de securitate,
- Aplicațiile software ale Autorității de Marcare Temporală,
- Actualizari anuale privind noi amenintari si practici de securitate
- Responsabilitățile care decurg din rolurile și activități întreprinse în cadrul sistemului.

Sancțiuni pentru acțiunile neautorizate

În cazul care este descoperit sau există suspiciunea asupra accesului neautorizat, administratorul de securitate va investiga incidentul și poate supenda accesul unei persoane la sistemul certSIGN. Măsurile disciplinare pentru astfel de incidente sunt descrise în politicile și procedurile corespunzătoare și sunt conforme cu prevederile legale.

Personalul angajat pe bază de contract

Personalul angajat pe bază de contract (servicii externe, dezvoltatori de subsisteme sau aplicații etc.) respectă aceleași măsuri de securitate ca și angajații permanenți.
În plus, pe timpul cât îşi desfăşoară activitatea în locaţia certSIGN, personalul angajat pe bază de contract trebuie însoţit permanent de către un angajat al certSIGN, cu excepţia celor care au primit avizul administratorului de securitate şi care pot accesa informaţii clasificate intern sau în conformitate cu regulile în vigoare.

7.4 Controlul gestiunii

Toate resursele Autorității de Marcare Temporală (informații, ssteme și aplicații) sunt inventariate în mod regulat și clasificate din punct de vedere al securității și importanței pentru business. Au fost puse în aplicare procese prin care managementul acelor resurse (intrare, ieșire, stocare, transfer, utilizare) este strict controlat prin măsuri direct proporționale importanței și clasificării lor.
certSIGN utilizează un proces controlat de management al schimbării. Înainte de a fi utilizat în producție de certSIGN, fiecare aplicație este instalată astfel încât să permit controlul versiunii curente și să prevină instalarea neautorizată de software sau falsificarea celor existente. Dezvoltarea, testarea și producția sunt zone distincte, iar transferul de informații și aplicații dintr-o zonă în alta este controlat.
Reguli similare se aplică la înlocuirea componentelor hardware, precum:

- Dispozitivele fizice sunt furnizate într-un mod care să permită monitorizarea și evaluarea traseului fiecărui dispozitiv, la locul de instalare,
- Livrarea unui dispozitiv fizic de schimb este similară cu livrarea dispozitivului original; înlocuirea este efectuată de personal calificat și de încredere.

7.5 Controlul accesului

Accesul la o resursă este realizat printr-un proces controlat, care presupune participarea managerilor, administratorilor de sistem și a administratorului de securitate. Principiul need-to-know și principiul separării atribuțiilor sunt respectate. Periodic, drepturile existente de acces sunt verificate pentru a determina dacă sunt adecvate.

Niveluri diferite de securitate în raport cu accesul fizic și logic asigură operarea sigură a serviciului de marcare temporară. De exemplu:

- Mediu fizic securizat
- Segregarea segmentelor de rețea
- Segregarea atribuțiilor
- Firewall-uri
- Monitorizarea rețelei și a serviciului
- Întărirea sistemelor IT

Dacă o persoană care efectuează operații pentru serviciile de marcare temporală primește un alt rol sau pleacă din organizație, toate token-urile ei de securitate sunt retrase.

Relațiile cu terții

Procesul se referă în primul rând la relațiile cu furnizorii de servicii și controlul acestuia implică asigurarea securității informațiilor accesate de către acești furnizori de servicii.

Management capacității

Procesul prin care certSIGN monitorizează în permanență încărcarea sistemelor care furnizează serviciile de încredere, pentru a asigura calitiatea și performanțele asumate prin politici și contracte.

Monitorizarea

Sistemele tehnologice, serviciile și personalul sunt monitorizați în permanență pentru a garanta că siguranța și calitatea serviciilor satisfac clienții și asigură conformitatea cu prevederile legale, regulamentele și propriile lor standard.

Securitatea fizică

Accesul fizic în cadrul certSIGN este controlat atât printr-un sistem de control al accesului cu carduri de proximitate, cât și prin agenți de securitate prezenți permanent. Același sistem cu carduri de acces controlează accesul în încăperile în care se află resursele considerate critice. Sunt instalate, de asemenea, sisteme de detecție a intruziunii precum și un sistem de supraveghere video cu circuit închis.

7.6 Controale criptografice

În cadrul certSIGN, implementarea serviciului de marcare temporală respectă „Agreed Cryptographic Mechanisms”, aprobate de European Cybersecurity Certification Group și publicate de ENISA, în vederea utilizării unor tehnici criptografice adecvate la furnizarea serviciilor de marcare temporală calificate.

7.6.1 Generarea cheii TSU

Perechea de chei a TSU este generată prin control dual, în locația certSIGN, în prezența unui grup de administrator (conform matricei de roluri pentru Autoritatea de Marcare Temporală certSAFE) într-un modul hardware de securitate (HSM) conform FIPS PUB 140-3, level 3, sau ISO 15408 Common Criteria EAL 4+. Cheia privată este păstrată în permanență în formă criptată pe acest dispozitiv și nu părăsește niciodată dispozitivul în formă necriptată.

Acțiunile luate atunci când este generate perechea de chei sunt înregistrate, datate și semnate de fiecare persoană prezentă în tipmul generării perechei de chei. Înregistrările sunt păstrate pentru audit sau pentru verificări regulate ale sistemului.

Cheia este generate și există pe întreg ciclul său de viață într-un mediu electronic protejat fizic și electromagnetic.

După generarea perechii de chei pentru semnarea mărcilor temporale și activarea cheii private în modulul hardware de securitate, ea poate fi folosită pentru operații criptografice, conform cu #4.4, până la expirarea valabilității sale sau până la compromiterea ei.

TSU folosește o pereche de chei RSA cu o lungime de 4096[2] de biți. Această pereche de chei este utilizată doar pentru semnarea TST-urilor.

7.6.2 Protejarea cheii private a TSU

Modulul hardware de securitate utilizat de Autoritățile de Certificare respectă standardele FIPS PUB 140-3, level 3, sau ISO 15408 Common Criteria EAL 4+. Semnătura electronica este creata utilizând algoritmul RSA în combinație cu rezumatul criptografic SHA512, SHA384 sau SHA256.

Controlul dual al accesului se realizează prin distribuirea de secrete operatorilor autorizaţi. Secretele sunt stocate pe carduri criptografice sau token-uri, protejate printr-un cod PIN şi transferate în mod autentificat deţinătorilor acestora.

Pentru operaţiuni precum iniţierea modulului criptografic hardware și transferul cheilor private se implementează o schemă prag de acces (de tip k din n) prin distribuire de secrete partajate.

Numărul total de de secrete partajate este 3, iar numărul necesar de secrete care permit acceul la cheia privată este 2.

Procedura de transfer a secretului partajat implică prezenţa deţinătorului secretului pe toată durata procesului de generare a cheii şi în timpul distribuirii sale, acceptarea secretului dat şi a responsabilităţilor care decurg din păstrarea sa.
Înainte de a primi partea sa de secret, fiecare deţinător al secretului partajat trebuie să fie prezent personal la partajarea secretului, să verifice corectitudinea secretului creat şi distribuirea sa. Fiecare parte a secretului partajat trebuie transferată deţinătorului pe un card criptografic protejat de un cod PIN, ales de deţinător şi ştiut numai de el.

Crearea și primirea secretului partajat sunt confirmate printr-o semnătură de mână pe un formular, a cărui copie este păstrată în arhivele Autorităţii de Certificare şi de către deţinătorul de secret.

Deţinătorii secretului partajat trebuie să protejeze partea lor împotriva dezvăluirii. Deţinătorul declară că:

- nu va dezvălui, copia sau partaja secretul cu nimeni şi că nu va folosi partea sa din secret într-un mod neautorizat,
- nu va dezvălui (direct sau indirect) că este deţinătorul secretului

Deţinătorul secretului partajat trebuie să-şi îndeplinească îndatoririle şi obligaţiile conform cerinţelor acestui Cod de Practici şi Proceduri, în mod responsabil, în orice situaţie posibilă. Un deţinător de secret partajat trebuie să anunţe emitentul secretului în cazul furtului, pierderii, dezvăluirii neautorizate sau compromiterii securităţii secretului, imediat după incident. Un deţinător de secret partajat nu este responsabil pentru neîndeplinirea îndatoririlor/obligaţiilor sale din cauza

[2] *TSU-ul activ emite chei cu 2048 biti. Urmatorul TSU, din Q4 2026 va emite chei cu 4096 biti.*

unor motive ce sunt imposibil de controlat de către acesta, dar este responsabil pentru dezvăluirea inoportună a secretului sau pentru neglijarea obligaţiilor de a notifica emitentul secretului despre dezvăluirea inoportună sau violarea securităţii secretului ca urmare a greşelilor, neglijenţei sau iresponsabilităţii deţinătorului.

Autoritatea de Marcare Temporală certSAFE creează o copie de siguranță a cheilor private folosite pentru semnarea mărcilor temporale. Copiile sunt folosite în cazul punerii în aplicare a procedurilor de urgenţă (de exemplu, în caz de dezastru) de recuperare a cheii. Copiile cheilor private sunt protejate prin secretul partajat creat la generarea cheilor inițiale.

Operaţiunea de introducere a unei chei private într-un modul criptografic se aplică în următoarele cazuri:

- Ocazional, la crearea copiilor de siguranţă ale cheilor private stocate într-un modul criptografic (de ex. în cazul compromiterii sau defectării modulului), poate fi necesară introducerea unei perechi de chei într-un modul de securitate diferit,
- Când este necesară transferarea unei chei private din modulul operaţional folosit pentru operaţiile standard ale entităţii, pe un alt modul; situaţia poate apărea în cazul invocării Planului de Recuperare în caz de Dezastru sau atunci când modulul operațional trebuie distrus.

Introducerea unei chei private într-un modul de securitate este o operaţiune critică; de aceea, trebuie implementate măsuri şi proceduri care să prevină dezvăluirea, modificarea sau falsificarea cheii private.

Introducerea unei chei private în modulul hardware de securitate al TSU-ului Autorității de Marcare Temporală certSAFE necesită restaurarea cheii de pe carduri în prezenţa unui număr adecvat de deţinători ai secretului partajat care protejează modulul ce conţine cheile privat.

Metoda de activare a cheii private folosită la semnarea mărcilor temporale se referă la activarea cheii înainte de orice folosire a sa.

În timpul importării, generării sau restaurării, cheia private a TSU este dezactivată. Cheia este activate când serviciul este pornit.

Odată activată, o cheie poate fi folosită cât timp serviciul este pornit. Când serviciul este oprit, cheia este dezactivată.

Activarea cheilor private este întotdeauna precedată de autentificarea operatorului. Autentificarea se realizează pe baza unui card criptografic deţinut de operator. După introducerea cardului în modulul criptografic şi folosirea codului PIN, cheia privată rămâne în stare activă până la scoaterea cardului din modul.

Metoda de dezactivare a cheii private se referă la dezactivarea cheii după folosirea ei sau la sfârșitul unei sesiuni în care a fost folosită cheia.

Pentru cheia private a TSU, dezactivarea se realizează atunci când serviciul este oprit pentru orice operație.

Protecția hardware a cheii private se referă la faptul că cheia nu este niciodată disponibilă în clar, nici măcar în memoria aplicației.

În cazul certSIGN, dezactivarea unei chei private este realizată de persoane cu roluri de încredere, însă numai în cazurile în care serviciul este oprit pentru actualizări, mentenanță sau din alte motive.

7.6.3 Certificat cheie publică TSU

TSA garantează integritatea și authenticitatea cheilor (publice) de verificare a semnăturii TSU, astfel:

a) (Cheile publice pentru) Verificare semnăturii TSU sunt disponibile entităților partenere care au încredere într-un certificate de cheie publică. Certificatele sunt publicate la următoarea adresă: https://www.certsign.ro/ro/resurse/lantul-de-incredere-g2/
b) TSU nu emite o marcă temporală înainte de verificare semnăturii sale (cheie publică). Când un certificate este încărcat în TSU, TSA verifică dacă certificatul a fost semnat în mod corespunzător (inclusiv verificarea căii de certificare a unei autorități de certificare de încredere).
c) Este emis doar un certificat TSU, cu cheia sa privată.
d) Certificatele TSU nu sunt reînnoite.
e) Validitatea informațiilor despre certificatele TSU este actualizată periodic iar CRL-urile sau serviciile OCSP sunt disponibile cu referințele localizate în certificate.

Mărcile temporale emise de TSA certSIGN TSA sunt mărci temporale electronice calificate conform Regulamentului (EU) Nr 910/2014 [i.4] iar certificatul de verificare a semnăturii TSU (cheie publică) este emis de certSIGN Qualified 2023 RSA CA în conformitate cu politica de certificare ETSI EN 319 411-2. Certificatul cu marcaj temporal conține o singură instanță a extensiei qcStatements în câmpul de extensii al certificatului, cu sintaxa definită în IETF RFC 3739, clauza 3.2.6.

7.6.4 Reînnoire cheii TSU

Durata de viață a certificatului TSU corespunde perioadei algoritmului ales și lungimii cheii. Cheile TSU vor avea o viață maximă de operare de 3 ani. Un certificat poate fi emis pentru toată durata de viață așteptată. Durata clasei TSU este limitată de:

- Perioada de valabilitate a certificatului root al entității emitente.
- O dată pe an sau când au loc modificări semnificative, persoana care îndeplinește funcția de "Cryptography Supervisor" verifică toți algoritmii criptografici folosiți în cadrul TSA, verificând dacă fiecare algoritm este recuncoscut ca fiind adecvat
- În cazul în care un algoritm poate cauza o situație de risc, acesta nu va mai fi considerat ca fiind adecvat; managerul de securitate va da TSA instrucțiuni de încetare a utilizării cheilor afectate și încărcarea unor chei noi.

7.6.5 Managementul ciclului de viață al hardware-ului criptografic

certSIGN TSA assures that:

a) Integritatea modulelor criptografice de securitate nu a fost afectată în timpul transportului de la producător,
b) Integritatea modulelor criptografice de securitate nu a fost afectată în timpul stocării premergătoare instalării,
c) Instalarea, administrarea și operarea lor este efectuată doar de personal de încredere,
d) Modulele criptografice de securitate funcționează corect,
e) Cheile private de semnare stocate pe modulele criptografice de securitate sunt distruse în momentul scoaterii lui din producție.

Inspecția respectă protocoale.

În plus, se aplică următoarele:

a) Instalarea și activarea cheilor de semnare ale TSU în hardware criptografic sunt realizate doar de personal cu roluri de încredere care utilizează, cel puțin, controlul dual într-un mediu securizat fizic.
b) Cheile private de semnare stocate intr-un modul criptografic al TSU sunt sterse după scoatere dispozitivului din producție într-un mod care face practice imposibilă recuperarea

lor.

7.6.6 Sfârșitul ciclului de viață al cheii TSU

După expirarea cheilor private, cheile private din modulul criptografic sunt distruse într-un mod care face imposibilă recuperarea lor.

7.7 Marcarea temporală

7.7.1 Emitentul mărcilor temporale

TSA certSIGN oferă servicii de marcare temporală utilizând RFC 3161 "Protocol Marcare Temporală (TSP)". URL-ul serviciului este specificat în contractul cu beneficiarul. Fiecare TST contine identificatorul Politicii de Marcare Temporală, un număr serial unic și un certificat ce conține informațiile de identificare a TSU-ului TSA certSIGN.
TSU-ul din cererile de marcă temporală acceptă algoritmi de hash SHA512, SHA384 sau SHA256 și utililizează funcția hash criptografică SHA512, SHA384 sau SHA256 pentru semnarea TST.
Cheile TSU sunt chei RSA de 4096[3] biți. Cheia este folosită numai pentru semnarea TST-urilor.
TSA înregistrează în jurnale toate TST-urile emise. Înregistrările TST-urilor sunt păstrate pentru o perioadă nedefinită. TSA certSIGN poate dovedi existența unui TST la cererea unei entități partenere. TSA certSIGN poate solicita entității partenere să acopere costurile unui astfel de serviciu.
TSU nu mai emite niciun TST când cheia privată a TSU ajunge la sfârșitul perioadei de valabilitate.

7.7.2 Sincronizarea ceasului cu UTC

certSIGN garantează că ceasul său este singronizat cu timpul UTC cu o precizie de o secundă sau mai bine, utilizând protocolul NTP.
certSIGN își monitorizează sincronizarea ceasului și garantează că, dacă timpul indicat într-un TST se abate sau își pierde sincronizarea cu timpul UTC, acest lucru este detectat. În cazul în care ceasul TSA își pierde acuratețea, nicio marcă temporală nu este emisă până când ceasul este sincronizat.

Mai exact, următoarele subiecte sunt acoperite:

- Calibrarea continua a ceasului TSU,
- Monitorizarea preciziei ceasului TSU,
- Analiza thread-uri împotriva atacurilor asupra semnalelor de timp
- Comportamentul în cazul când sunt sărite/adăugate secunde bisecte
- Comportamentul în cazul când se abate cu mai mult de 1s de la timpul UTC

7.8 Securitatea fizică și a mediului

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

Amplasarea locației

certSIGN este localizată în Bucureşti, la următoarea adresă: Bd. Tudor Vladimirescu, nr. 29 A, AFI Tech Park 1, București, România

[3] *TSU-ul activ emite chei cu 2048 biti. Urmatorul TSU, din Q4 2026 va emite chei cu 4096 biti.*

Accesul fizic

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

Sediul certSIGN este accesibil publicului în fiecare zi lucrătoare, între 10:00 și 18:00.
În restul timpului, accesul este permis exclusiv perosanelor autorizate de conducerea certSIGN. Vizitatorii spațiilor care aparțin certSIGN trebuie să fie însoțiți în permanență de persoane autorizate.

Zonele care aparțin certSIGN se impart în:

- Zona serverelor,
- Zona operatorilor,
- Zona administratorilor,
- Zona de dezvoltare și testare
- Zona de birou.

Zona serverelor este echipată cu un sistem de securitate monitorizat continuu, alcătuit din senzori de mişcare, efracţie şi incendiu. Accesul în această zonă este permis numai personalului autorizat, de exemplu, administratorul de securitate, administratorul de sistem. Monitorizarea drepturilor de acces se face folosind carduri şi cititoare, montate lângă punctul de acces. Fiecare intrare şi ieşire din zonă este înregistrată automat în jurnalul de evenimente.

Controlul accesului în **zona operatorilor** şi în **zona administratorilor** se face prin intermediul cardurilor şi a cititoarelor de carduri. 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. În această zonă au acces numai angajaţii certSIGN şi persoanele autorizate; ultimilor nu le este permisă prezenţa în zonă neînsoţiţi.

Zona de dezvoltare este protejată într-o manieră similară cu zona operatorilor şi administratorilor. Proiectele în curs de implementare şi software-ul aferent sunt testate în mediul de dezvoltare al certSIGN

Sursa de alimentare cu electricitate şi aerul condiţionat

Zona operatorilor şi administratorilor, precum şi zona de dezvoltare şi testare sunt prevăzute cu aer condiţionat. Din momentul întreruperii alimentării cu energie, sursele de electricitate de urgenţă (UPS) permit continuarea neperturbată a activităţii până la intervenţia automată a generatorului clădirii.

Expunerea la apă

Riscul inundării serverelor este scăzut, întrucât distanța față de țevile de apă este mare. În plus, în data room-uri sunt instalați senzori de inundație care sunt monitorizați non-stop de personalul de securitate localizat în imediata apropiere a serverelor și care este instruit să anunțe imediat administratorul certSIGN sau administratorul clădirii în cazul unui incident.

Prevenirea incendiilor

Locaţia certSIGN dispune de un sistem de prevenire şi protecţie împotriva incendiilor în conformitate cu standardele şi reglementările în domeniu.

Depozitarea mediilor de stocare a informaţiilor

În funcţie de sensibilitatea informaţiilor, mediile electronice care conţin arhivele şi copiile de siguranţă ale datelor curente sunt stocate în seifuri metalice, localizate într-o camera cu grad ridicat de securitate. Accesul la camera şi seifuri este permis numai persoanelor autorizate.

Aruncarea deşeurilor

Hârtiile şi mediile electronice care conţin informaţii importante din punctul de vedere al securităţii certSIGN sunt distruse după expirarea perioadei de păstrare. Modulele de securitate hardware sunt resetate şi şterse conform recomandărilor producătorului.

Aceste dispozitive sunt, de asemenea, resetate şi şterse atunci când sunt trimise în service sau reparate.

Depozitarea backup-urilor în afara locaţiei

Cardurile criptografice necesare pentru recuperaera în caz de dezastru a serviciilor sunt stocate în containere speciale, situate în afara locaţiei certSIGN.

Stocarea în afara locaţiei se aplică şi în cazul arhivelor, copiilor curente ale informaţiilor procesate de sistem şi kit-urilor de instalare ale aplicaţiilor certSIGN. Acest lucru permite refacerea de urgenţă a oricărei funcţii a certSIGN în termenele limită stabilite de planul de asigurare a continuităţii afacerii.

7.9 Security of operations

Cerințele tehnice prezentate în acest capitol se referă la controalele de securitate specifice computerelor și aplicațiilor utilizate în cadrul certSIGN. Măsurile de securitate au fost luate la toate nivelurile, începând de la nivelul fizic până la nivelul aplicațiilor.

Controalele care aparțin TSA certSIGN au următoarele mijloace de securitate:

- autentificarea obligatorie la nivelul sistemului de operare şi al aplicaţiilor,
- control discreţionar al accesului,
- posibilitatea de a fi auditate din punct de vedere al securităţii,
- 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 procesul autorizat,
- protecţia criptografică a schimburilor de informaţii şi protecţia bazelor de date,
- arhivarea istoricului operaţiunilor executate pe un calculator şi 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 aplicaţilor şi a sistemului de operare,
- mijloace de monitorizare şi alertare în cazul accesului neautorizat la resursele de calcul.
- Integritatea sistemelor și a informațiilor TSA trebuie să fie protejată împotriva virușilor, software-urilor rău intenționate și neautorizate.
- Mediile utilizate în cadrul sistemelor TSA trebuie să fie manipulate în siguranță pentru a mediile împotriva deteriorării, furtului, accesului neautorizat și uzurii morale.

- Procedurile de gestionare a mediilor trebuie să protejeze împotriva uzurii și a deteriorării suportului media în perioada în care trebuie păstrate înregistrările.

certSIGN utilizează sisteme și produse de încredere care sunt protejate împotriva modificărilor și asigură securitatea și fiabilitatea tehnică a proceselor pe care le suportă.
O analiză a cerințelor de securitate se realizează in etapa de proiectare și de specificare a cerințelor oricărui proiect de dezvoltare a sistemelor întreprinse de certSIGN sau în numele certSIGN pentru a se asigura că securitatea este integrată în sistemele informatice.
Fiecare aplicație, înainte de a fi utilizată pentru producerea în cadrul certSIGN, este instalată astfel încât să permită controlul versiunii curente și să prevină instalarea neautorizată a programelor sau falsificarea celor existente.
Reguli similare se aplică la înlocuirea componentelor hardware, cum ar fi:

- Hardware-ul este furnizat într-o manieră care permite urmărirea și evaluarea rutei componentei catre locul instalării,
- Livrarea hardware-ului de înlocuire se efectuează într-un mod similar cu livrarea hardware-ului original; Înlocuirea este efectuată de personal de încredere și instruit.

Scopul controlului de management al securității este de a supraveghea funcționalitatea sistemelor certSIGN asigurând că sistemul funcționează corect și în conformitate cu configurația acceptată și implementată.
Controalele aplicate sistemului certSIGN permit verificarea continuă a integrității aplicației, a versiunii precum și autentificarea și verificarea originii hardware-ului.
Politicile și procedurile de control al schimbării sunt aplicate pentru lansarile, modificările și remedierile de software de urgență ale oricărui software operațional și modificările aduse configurației care aplică politica de securitate a certSIGN.
Configurarea actuală a sistemului certSIGN, orice modificare a acestora, precum și orice lansari, modificări și soluții software de urgență ale oricărui software operațional sunt documentate.
Configuratiile Sistemelor de Emitere a Marcilor Temporale, 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 implementează proceduri interne de securitate pentru a asigura acest lucru:

- Patch-urile de securitate sunt aplicate într-un timp rezonabil după ce acestea sunt disponibile;
- Patch-urile de securitate nu se aplică dacă introduc vulnerabilități sau instabilități suplimentare care depășesc beneficiile aplicării acestora;
- Motivele pentru neaplicarea unor patch-uri de securitate sunt documentate.

certSIGN implementează o procedură internă de gestionare a capacității care asigură monitorizarea cerințelor de capacitate pentru infrastructura TIC pentru serviciile TSA și proiecții ale viitoarelor cerințe de capacitate, pentru a se asigura că există o putere și o capacitate de stocare adecvată.

7.10 Securitatea rețelei

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

a) Sistemele noastre sunt segmentate în rețele sau zone bazate pe relația funcțională, logică și fizică (inclusiv locația) dintre sistemele și serviciile de încredere. certSIGN aplică aceleași controale de securitate tuturor sistemelor co-localizate în aceeași zonă.

b) Accesul și comunicațiile între zone sunt limitate la persoanele necesare pentru funcționarea serviciilor de certificare. Conexiunile și serviciile necesare nu sunt strict interzise sau dezactivate. Setul stabilit de reguli este revizuit în mod regulat.

c) Toate sistemele critice pentru funcționarea serviciilor de certificare sunt păstrate într-una sau mai multe zone securizate.

d) Rețeaua dedicată pentru administrarea sistemelor informatice și reteaua operaționala sunt separată. Sistemele folosite pentru administrarea implementării politicii de securitate nu sunt utilizate în alte scopuri. Sistemele de producție pentru serviciile de certificare sunt separate de sistemele utilizate în dezvoltare și testare (de exemplu, sisteme de dezvoltare, testare și staționare).

e) Comunicarea între sisteme distincte de încredere se stabilește numai prin intermediul unor canale de încredere care sunt distincte logic de alte canale de comunicare și oferă o identificare sigură a punctelor sale finale și protecția datelor canalului de la modificare sau dezvăluire.

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

g) Se realizează o scanare trimestriala a vulnerabilității pe adresele IP publice și private identificate de certSIGN și se înregistrează dovezi că fiecare scanare de vulnerabilitate a fost efectuată de o persoană sau entitate cu abilități, instrumente, competențe, cod etic și independența necesară pentru a furniza un raport de încredere.

h) Serviciile de certificare certSIGN se supun unui test anual de penetrare a sistemelor aferente la instalare și după actualizarea infrastructurii sau a aplicațiilor sau a modificărilor pe care certSIGN le determină ca fiind semnificative. Se inregistreaza dovezi că fiecare test de penetrare a fost efectuat de o persoană sau entitate cu abilitățile, instrumentele, competența, codul de etică și independența necesară pentru a furniza un raport de încredere.

Serverele și stațiile de lucru de încredere ale sistemului certSIGN sunt conectate printr-o rețea locală (LAN), concepută în mai multe sub-rețele cu acces controlat. Accesul de pe Internet către orice segment este protejat prin intermediul unui firewall inteligent.

Controalele de securitate sunt dezvoltate pe baza firewall-ului și a filtrării traficului pe routerele și serviciile Proxy care protejează domeniile rețelei interne ale certSIGN de acces neautorizat, inclusiv accesul de către Subiecți / Beneficiari și terți. Firewall-urile sunt configurate pentru a preveni toate protocoalele și accesările care nu sunt necesare pentru funcționarea certSIGN TSA.

Mijloacele de protecție a securității rețelei acceptă numai mesajele transmise cu ajutorul protocoalelor http, https, NTP, POP3 și SMTP. Evenimentele (logs) sunt înregistrate în jurnalele de sistem și permit supravegherea corectitudinii utilizării serviciilor furnizate de certSIGN.

Clientul de marcare temporală și serverul de marcare temporală acceptă protocolul de marcare temporală prin HTTPS, conform definiției din clauza 3.4 a documentului IETF RFC 3161.

certSIGN menține și protejează toate sistemele TSA în cel puțin o zonă securizată și dispune de o procedură de securitate care protejează sistemele și comunicațiile dintre sistemele din zonele securizate și zonele de securitate ridicata.

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

certSIGN acordă acces la zonele securizate și zonele de securitate ridicata numai pentru roluri de încredere.

7.11 Managementul incidentelor

Activitățile sistemului privind accesul la sistemele IT, sistemele sale de utilizatori si cererile

serviciilor sunt monitorizate. În special:
a) Activitățile de monitorizare țin cont de sensibilitatea oricărei informații colectate sau analizate.
b) Activitățile anormale ale sistemului care indică o potențială violare a securității, inclusiv intruziunea în rețeaua TSP, sunt detectate și raportate ca alarme.
c) Sistemele IT TSP monitorizează următoarele evenimente: Pornirea și oprirea funcților de logare; disponibilitatea și utilizarea serviciilor necesare cu rețeaua TSP.

d) TSP-ul acționează în mod oportun și coordonat pentru a răspunde rapid la incidente și pentru a limita impactul breșelor de Securitate. TSP-ul numește personalul cu roluri de încredere care urmărește alertele evenimentelor de securitate potential critice și se asigură că incidentele relevante sunt raportate în linie cu procedurile TSP.
e) TSP-ul notifică entitățile corespunzătoare, în linie cu normele de reglementare aplicabile, despre orice breșă de securitate sau pierdere a integrității care are un impact semnificativ asupra servicului de încredere furnizat și asupra datelor cu caracter personal păstrate de acesta.
f) Organismul national de supraveghere este informat în termen de 24 de ore de la descoperirea unei breșe critice de securitate.
g) Log-urile auditurilor sunt monitorizate sau revizuite în mod regulat pentru a identifica dovezile activităților malițioase.
h) TSP-ul va rezolva vulnerabilitățile critice într-un timp rezonabil de la descoperirea lor. Dacă acest lucru nu este posibil, TSP-ul va crea și va implementa un plan de diminuare a vulnerabilității critice sau TSP-ul va documenta baza factuală în sprijinul deciziei că vulnerabilitatea nu necesită remediere.
i) Procedurile de raportare și răspuns la incidente sunt utilizate astfel încât daunele incidentelor de securitate și defecțiunilor să fie minimizate.

7.12 Colectarea dovezilor

Înregistrările TSP sunt accesibile pentru o perioadă adecvată, inclusive după încetarea activităților TSP. Toate informațiile relevante cu privire la datele emise sau primate de TSP sunt păzite, pentru a oferi dovezi în procesele legale și pentru a asigura continuitatea serviciului. Mai ales:
a) Este păstrată confidențialitatea și integritatea înregistrărilor curente și a celor arhivate cu privire la operarea serviciilor.
b) Înregistrările cu privire la gestiunea serviciilor sunt confidențiale și clasifcate în conformitate cu practicile de afaceri descrise.
c) Dacă este necesar, înregistrările privind gestiunea serviciilor sunt puse la dispoziție în scopul dovedirii funcționării corecte a serviciilor în procesele judiciare.
d) TSP-ul înregistrează la momentul exact evenimentele semnificative ale mediului, managementul cheilor și sincronizarea ceasului. Timpul folosit pentru înregistrarea evenimentelor, așa cum se solicit în log-ul de audit, este sincronizat în mod continuu cu UTC.
e) Înregistrările privind serviciile sunt păstrate pentru o perioadă după expirarea valabilității cheilor de semnare sau a oricărui token al serviciului pentru a asigura încredere pentru dovezile legale necesare, în conformitate cu prezentul document.
f) Evenimentele sunt înregistrate astfel încât să nu poată fi șterse sau distruse (cu excepția cazului în care ele pot fi transferate în mod fiabil pe un suport pe termen lung).

7.13 Managementul continuității afacerii

Copiile de siguranță ale bazelor de date ale tuturor TST-urilor emise de TSA certSIGN sunt păstrate în afara locației. În cazul în care cheia private a TSU este compromisă sau există suspiciunea compromiterii ei, TSA certSIGN va informa Beneficiarii și Entitățile Partenere și va înceta să mai utilizeze cheia compromisă.
În cazul revocării certificatului TSU, acțiunile necesare vor fi luate în accord cu Planul de Recuperare.
În cazul desincronizării ceasului, TSA certSIGN își suspendă operațiile, pentru a nu cauza daune suplimentare. Planul de Recuperare este activat pentru a restabili sincronizarea și serviciul.

Serviciul de marcare temporală în sine se află într-un mediu securizat fizic care minimizează riscul dezastrelor naturale (de exemplu, incendiu).
Cheile private ale TSU sunt stocate într-un modul de securitate criptografică.
În cazul în care cheile private sunt compromise, arhiva mărcilor temporale salvate ajută la diferențierea între mărcile temporale corecte și cele false într-un audit trail.
HSM-ul este izolat din rețeaua publică și, dacă este necesar, se vor lua următoarele măsuri:

- Va fi anunțat managerul de securitate, ca să coordoneze măsurile care trebuie luate.
- Va fi demarat un audit de securitate a cheilor private rămase (controale de integritate, jurnal de analiză a fișierelor).
- Entitățile partenere vor fi notificate cu privire la incident.
- În cazul unor dezastre naturale (de exemplu incendii, cutremur, furtună), dacă se produce o pierdere a serviciului, serviciul de marcare temporală ar putea fi suspendat până la activarea recuperării serviciului în caz de dezastru.

7.14 Încetarea activității TSA și planurile încetării activității

În cazul în care TSA își încetează activitatea din orice motiv, va notifica organismul național de supraveghere înaintea încetării activității.

- O notificare va fi trimisă în timp util tuturor entităților partenere pentru a minimiza orice întreruperi cauzate de încetarea activității serviciului.
- În plus, în colaborare cu entitatea de supraveghere, TSP-ul va coordona măsurile necesare pentru a asigura retenția tuturor înregistrărilor arhivate relevante înainte de încetarea activității serviciului.
- De asemenea, se aplică următoarele:
    a) TSP mențione un plan de încetare a activității actualizat.
    b) Înainte ca TSP să înceteze activității serviciului, cel puțin următoarele procedure se aplică:
        i. TSP va informa despre încetarea serviciului pe: toți Beneficiarii și alte entități cu care TSP are înțelegeri sau altă formă de relații stabilite. Această informație va fi pusă la dispoziția altor entități partenere;
        ii. TSP va înceta autorizarea tuturor subcontractorilor de a acționa în numele TSP în îndeplinirea oricăror funcții legate de procesele de emitere a token-urilor serviciilor de încredere;
        iii. TSP va transfera unei entități de încredere, pentru o perioadă rezonabilă de timp, obligațiile sale de a păstra toate informațiile necesare pentru a oferi dovada operațiunilor TSP, cu excepția cazului în care se paote dovedi că TSP nu este deținătorul unor astfel de informații;
        iv. Cheile private ale TSP, inclusive copiile de rezervă, vor fi distruse, sau retrase din uz, într-o manieră care face imposibilă recuperarea cheilor private.
        v. TSA certSIGN ia măsurile necesare pentru revocarea certificatelor TSU.
        vi. Când este posibil, TSP va utiliza un sistem care permite transferul serviciilor pe care le furnizează clientului său către un alt TSP.
    c) TSP-ul are o înțelegere pentru acoperirea costurilor de îndeplinire a acestor cerințe minime în cazul în care TSP intră în faliment sau din alte motive care împiedică TSP să acopere singur costurile, în măsura posibilităților, în limitele legislației în vigoare referitoare la faliment.
    d) TSP-ul va mențione și va transfera către o entitate de încredere obligațiile sale de a pune la dispoziția entităților partenere cheia sa publică sau token-urile serviciului de încredere pentru o perioadă rezonabilă de timp

7.15 Conformitatea

certSIGN TSA asigură conformitatea cu legislația aplicabilă în orice moment. Mai exact, asigură

conformitatea cu:

a. Regulamentul (EU) Nr. 910/2014, cu modificarile aduse de Regulamentul (UE) 1183/2024
b. Legea română nr. 214/2024
c. ETSI TS 119 421
d. IETF (RFC 3161)

Validarea respectării acestor reglementări se realizează în cadrul evaluării conformității.