



Trans Sped

TSP

Your Trusted Service Provider

Codul de Practici și Proceduri și Politica de Marcare Temporală

Versiune 2.1

Data intrării în vigoare: 16 august 2021

Informații generale	
Versiune	2.1
Clasificarea informației	Public
Aprobat de	Comitet de Management al Politicilor si Procedurilor
Data aprobării	August 2021
Data intrării în vigoare	August 2021

Istoricul Modificarilor			
Versiune	Descriere	Data	Autor(i)
1.0	Versiune inițială	Ianuarie 2017	Mario STOICA
2.0	Revizuire internă	Februarie 2020	Camelia IVAN
2.1	Conținut revizuit și actualizat conform standardelor ETSI	August 2021	Camelia IVAN

CUPRINS

1. INTRODUCERE.....	4
2. SCOP	4
3. REFERINȚE.....	5
4. DEFINIȚII ȘI ABREVIERI	6
4.1. Definiții	6
4.2. Abrevieri.....	6
5. CONCEPTE GENERALE	8
5.1. Serviciile de marcă temporală	8
5.2. Autoritatea de Marcă Temporală	8
5.3. Abonat	8
5.4. Politica de marcă temporală și Codul de practici și proceduri al TSA	9
6. POLITICA DE MARCARE TEMPORALĂ	10
6.1. Generalități	10
6.2. Identificarea politicii	10
6.3. Aplicabilitatea politicii	10
6.4. Conformitatea	10
7. OBLIGAȚII ȘI RESPONSABILITĂȚI.....	11
7.1. Obligațiile TSA	11
7.2. Obligațiile abonaților	12
7.3. Obligațiile terțelor părți.....	12
7.4. Răspunderi	12
7.5. Publicarea și notificarea politicilor.....	12
7.6. Aprobarea Codului de Practici și Proceduri	12
8. CERINȚE PRIVIND PRACTICILE TSA	13
8.1. Declarații.....	13
8.2. Managementul ciclului de viață a cheilor criptografice.....	14
8.3. Marcarea temporală.....	16
8.4. Managementul și operarea TSA	18
8.5. Măsuri organizaționale.....	24

1. INTRODUCERE

Acest document descrie practicile, procedurile și politicile aferente serviciului de marcă temporală furnizate de Trans Sped S.A.

Trans Sped S.A. cu adresa în str. Despot Vodă nr. 38, 020656, București, România (denumit în continuare "Trans Sped") este un furnizor de servicii de încredere care emite certificate digitale calificate care pot fi folosite pentru crearea de semnături electronice sau sigilii electronice cu valoare juridică, conform Regulamentului eIDAS (910/2014).

Trans Sped oferă serviciul de marcă temporală ca parte a serviciilor sale de încredere, în conformitate cu Legea nr. 451/2004 și regulamentul eIDAS. Mărcile temporale au rolul de a determina cu exactitate momentul la care a fost creat sau semnat un document electronic. Mărcile temporale permit implementarea unor scheme avansate de semnături necesare în contextul dezvoltării pe scară largă a serviciilor electronice.

Pentru furnizarea serviciului de marcă temporală, Trans Sped a implementat o Autoritate de Marcă Temporală (Time Stamping Authority) – Trans Sped TSA.

Acest document conține **politica de marcă temporală** ce descrie regulile generale ce sunt respectate de Trans Sped TSA și **codul de practici și proceduri** ce descrie procesele și procedurile prin intermediul cărora sunt implementate aceste reguli.

Structura și conținutul acestui document sunt în conformitate cu standardul EN 319 421 v1.1.1 (2016-3) Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.

Acest document este disponibil publicului pe site-ul Trans Sped:

www.transspoed.ro/repository.

2. SCOP

Prezentul document specifică cerințele privind funcționarea Trans Sped TSA și definește practicile de operare și management a Trans Sped TSA astfel încât utilizatorii și terțele părți să poată avea încredere în serviciile furnizate de către Trans Sped TSA.

Soluția implementată respectă cerințele regulamentului eIDAS, Legii nr. 451/2004 privind marca temporală și Ordinul MCSI nr. 492/2009 privind normele tehnice și metodologice pentru aplicarea Legii nr. 451/2004 privind marca temporală.

Soluția implementată se bazează pe folosirea criptografiei cu chei publice, a certificatelor digitale, a funcțiilor hash criptografice și a unei surse de timp de încredere.

Prezentul document, împreună cu modul de organizare, procesele și procedurile interne ale Trans Sped, poate fi folosit de către un organism independent pentru a evalua încrederea în serviciile de marcă temporală oferite de Trans Sped.

3. REFERINȚE

- [LEGE-ES] Legea nr. 455/2001 privind semnăturile electronice
- [LEGE-TS] Legea nr. 451/2004 privind marca temporală
- [ORDIN-TS] Ordinul MCSI nr. 492/2009 privind normele tehnice și metodologice pentru aplicarea Legii nr. 451/2004 privind marca temporală
- [EU-REG] REGULAMENTUL (UE) NR. 910/2014 AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI din 23 iulie 2014
- [ORDIN-eIDAS] Ordinul nr. 449/2017 privind procedura de acordare, suspendare și retragere a statutului de prestator de servicii de încredere calificat în conformitate cu Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014
- [ETS1] EN 319 401 v2.2.1 (2018-04) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
- [ETS2] EN 319 421 v1.1.1 (2016-03) Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time- Stamps
- [RFC3161] Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)
- [FIPS] FIPS PUB 140-2: Security Requirements for Cryptographic Modules

4. DEFINIȚII ȘI ABREVIERI

4.1. Definiții

Abonat: o persoană juridică cu mai mulți utilizatori sau o persoană fizică, utilizator individual ce folosește serviciile de marcă temporală ale Trans Sped TSA și care în mod explicit sau implicit a agreat termenii și condițiile Trans Sped.

Terță parte: o entitate care are încredere în mărcile temporale emise de Trans Sped TSA.

Marcă temporală: obiect ce certifică faptul că anumite date au fost prezentate la un moment de timp determinat furnizorului de servicii de marcă temporală;

NTP (Network Time Protocol): protocol de rețea pentru sincronizarea ceasului unui sistem informatic în rețea cu latență variabilă

Cheie criptografică publică: Din perechea de chei utilizată în algoritmi asimetrici, cheia criptografică publică este cea pusă la dispoziția publicului, de ex. pe un server de cheie criptografică publică. Scopul său este de a cripta mesajele trimise către deținătorul cheii și de a verifica semnăturile digitale pe care cel de-al doilea le-a realizat folosind cheia privată corespondentă. O cheie criptografică publică certificată de o Autoritate de Certificare este denumită certificat.

Autoritate de Marcare Temporală (TSA): terț de încredere care emite mărci temporale.

Unitate de Marcare Temporală (TSU): hardware sau software folosit pentru generarea mărcilor temporale.

Timpul Universal Coordonat (UTC): Scală de timp bazată pe secunde, definită prin recomandarea ITU-R Recommendation TF.460-5. UTC este echivalent cu timpul solar la primul meridian (00).

4.2. Abrevieri

ETSI European Telecommunications Standards Institute

FIPS Federal Information Processing Standards

HTTP Hypertext Transfer Protocol NTP Network Time Protocol

OID Object Identifier

RFC Request for Comments

RSA Rivest Shamir Adleman Algorithm SHA Secure Hash Algorithm



Codul de Practici și Proceduri și Politica de Marcare Temporală Versiune 2.1

TSA Time Stamping Authority

TSPS Time Stamping Practice Statement

TSU Time Stamping Unit

HSM Hardware Security Module

UTC Coordinated Universal Time

5. CONCEPTE GENERALE

5.1. Serviciile de marcare temporală

Prezentul document respectă standardul ETSI EN 319 401, ETSI 319 421 V1.1.1 (2016 0 -3), ETSI 319 422 V1.1.1 (2016 0 -3) referitoare la cerințele ce trebuie îndeplinite de furnizorii de servicii de încredere.

Serviciile de marcare temporală sunt compuse din:

- Furnizarea mărcilor temporale: Componenta care se ocupă cu generarea mărcilor temporale.
- Managementul mărcilor temporale: Componenta care monitorizează și controlează modul de operare al serviciilor de marcare temporală. De exemplu, această componentă asigură faptul că ceasul folosit în procesul de marcare temporală este sincronizat corect cu UTC.

Această descompunere a serviciilor de marcare temporală are scopul doar de a clarifica cerințele specificate în acest document și nu impune nicio restricție cu privire la modul efectiv de implementare a serviciilor de marcare temporală.

5.2. Autoritatea de Marcare Temporală

Autoritatea în care utilizatorii (abonați sau terțe părți) au încredere în a emite mărci temporale poartă denumirea de Autoritate de Marcare Temporală (TSA). TSA poartă întreaga responsabilitate pentru furnizarea serviciilor de marcare temporală identificate în capitolul 5.1.

O Autoritate de Marcare Temporală (TSA) poate dispune de una sau mai multe Unități de Marcare Temporală (TSU) ce generează și semnează mărci temporale în numele TSA. Fiecare TSU trebuie să poată fi identificată în mod unic și trebuie să aibă o cheie de semnare proprie.

O Autoritate de Marcare Temporală (TSA) este furnizor de servicii de certificare în accepțiunea Regulamentului (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.

Trans Sped confirmă faptul că Autoritate de Marcare Temporală (TSA) este auditată cel puțin o dată la 24 de luni de către un organism de verificare și raportul de audit este adus la cunoștința organismului de supraveghere național, în 3 zile lucrătoare.

5.3. Abonat

Abonatul poate fi o persoană juridică cu mai mulți utilizatori sau o persoană fizică, utilizator individual.

Atunci când abonatul este o persoană juridică, o parte din obligațiile care se aplică persoanei

juridice respective se vor aplica și utilizatorilor proprii. În orice caz, persoana juridică respectivă este responsabilă dacă utilizatorii proprii nu-și îndeplinesc obligațiile în mod corect. Este de așteptat ca persoana juridică respectivă să informeze în mod corespunzător utilizatorii proprii.

În cazul în care abonatul este o persoană fizică, aceasta este responsabil în mod direct în cazul în care obligațiile sale nu sunt îndeplinite în mod corect.

5.4. Politica de marcare temporală și Codul de practici și proceduri al TSA

Aceast capitol explică rolul pe care îl au Politica de Marcare Temporală și Codul de Practici și Proceduri pentru un TSA.

Politica de marcare temporală și Codul de practici și proceduri al TSA respectă cerințele specificate în ETSI EN 319 401 aplicabile pentru furnizorii de servicii de încredere.

5.4.1. Rol

În general, Politica de Marcare Temporală a TSA declară „care sunt cerințele ce trebuie respectate” pe când Codul de Practici și Proceduri al TSA stabilește „cum trebuie respectate aceste cerințe”. Relația dintre Politica de Marcare Temporală și Codul de Practici și Proceduri al TSA este similară cu relația dintre politica unei firme care declară cerințele de business pe când unitățile operaționale definesc practicile și procedurile prin intermediul cărora cerințele de business urmează a fi realizate.

Acest document conține atât politica de marcare temporală cât și codul de practici și proceduri al Trans Sped TSA.

Politica de Marcare Temporală a Trans Sped TSA descrie cerințele generale pe care le îndeplinesc serviciile de marcare temporală.

Codul de Practici și Proceduri al Trans Sped TSA descrie modul în care aceste cerințe sunt îndeplinite.

5.4.2. Nivel de detaliere

Politica de Marcare Temporală este un document mai puțin detaliat decât Codul de Practici și Proceduri al TSA. Codul de Practici și Proceduri al Trans Sped TSA descrie în detaliu termenii și condițiile, precum și procedurile operaționale folosite pentru generarea și managementul mărcilor temporale. Codul de Practici și Proceduri al Trans Sped TSA implementează regulile generale definite de Politica de Marcare Temporală a Trans Sped TSA. Codul de Practici și Proceduri al Trans Sped TSA demonstrează cum Trans Sped TSA satisface cerințele tehnice, organizatorice și procedurale definite prin Politica de Marcare Temporală a Trans Sped TSA.

5.4.3. Mod de abordare

Modul de abordare al Politicii de Marcare Temporală diferă semnificativ de cel al Codului de Practici și Proceduri.

Politica de Marcare Temporală este definită independent de detaliile specifice modului de operare al TSA, pe când Codul de Practici și Proceduri reflectă structura organizațională, procedurile de operare, facilitățile și sistemele informatice ale TSA.

6. POLITICA DE MARCARE TEMPORALĂ

6.1. Generalități

Acest capitol definește cerințele pe care Trans Sped TSA se angajează să le respecte atunci când generează mărci temporale.

Trans Sped TSA emite mărcile temporale în conformitate cu cerințele Regulamentului eIDAS, Legii nr. 451/2004 privind marca temporală, Ordinului MCSI nr. 492/2009 privind normele tehnice și metodologice pentru aplicarea Legii nr. 451/2004 privind marca temporală și specificațiile standardului EN 319 421 v1.1.1 (2016-03) ETSI 319 421 V1.1.1 (2016 0 -3), ETSI 319 422 V1.1.1 (2016 0 -3).

6.2. Identificarea politicii

Identificatorul politicii Trans Sped TSA este următorul:

OID = 1.3.6.1.4.1.39965.1.2.1

Identificatorul politicii ETSI de bază respectate este următorul: 0.4.0.2023.1.1

itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(02023) policy-identifiers(1)
baseline-ts-policy (1)

Identificatorul politicii Trans Sped TSA este inclus în fiecare marcă temporală emisă.

6.3. Aplicabilitatea politicii

Acest document nu stabilește nici o limitare privind aplicabilitatea mărcilor temporale emise în concordanță cu această politică. Trans Sped furnizează servicii de încredere, de marcă temporală în conformitate cu legislația în vigoare.

6.4. Conformitatea

Trans Sped include identificatorul de politică (OID) stabilit la capitolul 6.2 în toate mărcile temporale emise.

Pentru a demonstra conformitatea, Trans Sped se angajează să:

1. îndeplinească obligațiile definite în capitolul 7.1;
2. implementeze măsurile de control specificate în capitolul 8.

Conformitatea cu Politica de Marcare Temporală este verificată periodic prin audituri independente, interne sau externe.

7. OBLIGAȚII ȘI RESPONSABILITĂȚI

7.1. Obligațiile TSA

7.1.1. Obligații general valabile

Trans Sped se obligă să asigure conformitatea cu cerințele stabilite prin Politica de Marcare Temporală și cu următoarele reglementări:

- Regulamentul European 910/2014 eIDAS
- Legea nr. 451/2004 privind marca temporală;
- Ordinul MCSI nr. 492/2009 privind normele tehnice și metodologice pentru aplicarea Legii nr. 451/2004 privind marca temporală;
- Specificațiile standardului EN 319 421 v1.1.1 (2016-03).

Trans Sped se angajează să implementeze măsurile de control stabilite prin Codul de Practici și Proceduri descris în acest document.

7.1.2. Obligațiile TSA față de abonați

Trans Sped asigură accesul permanent la serviciul de marcare temporală cu excepția perioadelor de mentenanță, a momentelor în care sursa de timp nu este disponibilă sau în cazul evenimentelor de forta majora care nu depind de Trans Sped (de exemplu, război, grevă, restricții legale, etc).

Perioadele de mentenanță trebuie agreate în prealabil cu abonații sau anunțate din timp pe site-ul Trans Sped.

În plus, Trans Sped se obligă să:

- implementeze o infrastructură de comunicații și aplicații informatice fiabile și de încredere;
- ofere serviciul de marcare temporală în conformitate cu standardele în domeniu, agreate pe scară largă;
- emită numai mărci temporale corecte și să nu permită antedatarea documentelor.

Sursa de timp a serviciului de marcare temporală al Trans Sped folosește semnalul GPS împreună cu un set de servere Network Time Protocol (NTP) ca sursă de timp. Folosind această configurație abaterea este de +/- 1 secundă sau mai precisă folosind UTC.

7.2. Obligațiile abonaților

Abonații trebuie să folosească serviciul de marcă temporală al Trans Sped TSA în conformitate cu specificațiile din capitolul 4 (Requirements for a time-stamping client) al standardului EN 319 422 v1.1.1 (2016-03) Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles.

Abonații trebuie să verifice că mărcile temporale au fost semnate corect și că cheia privată a TSU folosită pentru semnarea mărcilor temporale nu a fost revocată.

Trans Sped poate include în contractele încheiate cu fiecare abonat în parte, cerințe suplimentare pe care aceștia trebuie să le respecte.

Pentru mai multe informații vă rugăm să consultați Termenii și condițiile disponibile la www.transsped.ro

7.3. Obligațiile terțelor părți

Terțele părți care au încredere în mărcile temporale emise de Trans Sped TSA, trebuie să verifice că mărcile temporale au fost semnate corect și că cheia privată a TSU folosită pentru semnarea mărcilor temporale nu a fost revocată.

În cazul verificării unei mărci temporale după expirarea validității certificatului TSU, terțele părți trebuie să se asigure că funcția hash, algoritmi criptografici și lungimile de chei folosite pot fi considerate în continuare ca fiind sigure.

Pentru mai multe informații vă rugăm să consultați Termenii și condițiile disponibile la www.transsped.ro

7.4. Răspunderi

Trans Sped răspunde pentru prejudiciul dovedit adus oricărei persoane care își întemeiază conduita pe efectele juridice ale mărcilor temporale emise, în conformitate cu prevederile legale în vigoare.

Trans Sped nu răspunde în cazurile în care probează că, deși a depus diligența necesară, nu a putut împiedica producerea prejudiciului. De asemenea, Trans Sped nu răspunde pentru daunele cauzate de forța majoră și / sau cazul fortuit.

Trans Sped nu răspunde pentru daunele produse abonaților sau terțelor părți cauzate de neglijență sau de nerespectarea obligațiilor prezentate în capitolele 7.2 și 7.3.

7.5. Publicarea și notificarea politicilor

Ori de câte ori Codul de Practici și Proceduri este modificat și versiunea modificată este aprobată de managementul Trans Sped, aceasta va fi publicată în depozitarul disponibil pe website.

7.6. Aprobarea Codului de Practici și Proceduri

Codul de Practici și Proceduri este revizuit și aprobat de către managementul Trans Sped înainte

de publicarea în depozitar.

8. CERINȚE PRIVIND PRACTICILE TSA

Trans Sped se obligă să implementeze măsuri de control în conformitate cu cerințele prezentate în continuare. Cerințele sunt descrise sub formă de obiective de securitate.

8.1. Declarații

8.1.1. Declarația privind practicile TSA

Trans Sped TSA se obligă să demonstreze încrederea necesară cu privire la furnizarea serviciilor de marcă temporală. În acest sens:

- a) Trans Sped TSA a efectuat o analiză de risc pentru de a evalua resursele și amenințările la care sunt expuse acestea cu scopul de a determina măsurile de securitate necesare;
- b) Trans Sped TSA dispune de un set de practici și proceduri folosite pentru a implementa cerințele identificate prin prezenta politică;
- c) Practicile și procedurile stabilite includ obligațiile tuturor entităților ce asigură suportul pentru serviciile de marcă temporală;
- d) Trans Sped TSA pune la dispoziția abonaților și terțelor părți, practicile și procedurile precum și alte documente relevante, pentru ca aceștia să poată evalua conformitatea cu Politica de Marcare Temporală;
- e) Trans Sped TSA aduce la cunoștința abonaților și terțelor părți, termenii și condițiile privind utilizarea serviciilor de marcă temporală;
- f) Trans Sped TSA dispune de o procedură de aprobare a practicilor și procedurilor de către managementul companiei;
- g) Managementul companiei asigură că practicile și procedurile sunt implementate corect;
- h) Trans Sped TSA are stabilit un proces de revizuire a practicilor și procedurilor și de actualizare a acestora.

8.1.2. Declarația privind aducerea la cunoștință

Trans Sped TSA aduce la cunoștința tuturor abonaților și terțelor părți termenii și condițiile privind utilizarea serviciilor de marcă temporală. Mai exact, utilizatorii sunt informați cu privire la:

- a) Datele de contact ale TSA;
- b) Politica de Marcare Temporală aplicată;
- c) Algoritmii de hash acceptați pentru calculul rezumatului datelor asupra cărora urmează să se aplice marca temporală;
- d) Durata de viață estimată a semnăturii folosită pentru semnarea mărcilor temporale (care depinde de algoritmul de hash utilizat, de algoritmul de semnare utilizat și de lungimea cheii private);

- e) Precizia timpului din mărcile temporale în raport cu UTC;
- f) Orice limitări cu privire la utilizarea serviciului de marcă temporală;
- g) Obligațiile abonaților, în conformitate cu capitolul 7.2;
- h) Obligațiile terțelor părți, în conformitate cu capitolul 7.3;
- i) Informații cu privire la modul de verificare a mărcilor temporale;
- j) Perioada de timp pentru care TSA păstrează logurile;
- k) Legislația aplicabilă;
- l) Orice limitare a răspunderii;
- m) Modalitatea de soluționare a litigiilor;
- n) Dacă TSA a fost auditată și de către ce organism.

8.2. Managementul ciclului de viață a cheilor criptografice

8.2.1. Generarea cheii TSU

Trans Sped TSA se obligă să asigure că cheile criptografice sunt generate în condiții strict controlate. În acest sens:

- a) Generarea cheii de semnare a TSU se face într-un mediu fizic securizat, de către personal de încredere, sub control dual;
- b) Generarea cheii de semnare a TSU se face în interiorul unui modul criptografic (HSM – Hardware Security Module), certificat FIPS 140-2 Level 3;
- c) Algoritmii de generare a cheilor, algoritmul de semnare și lungimea cheilor de semnare respectă recomandările naționale și internaționale în domeniul criptografiei.

8.2.2. Protecția cheii private a TSU

Trans Sped TSA se obligă să asigure confidențialitatea și integritatea cheilor private de semnare ale TSU. În acest sens:

- a) Cheia privată de semnare a TSU este păstrată și utilizată prin intermediul unui modul criptografic (HSM – Hardware Security Module), certificat FIPS 140-2 Level 3;
- b) Dacă cheia privată de semnare a TSU este salvată, atunci operațiile de copiere, stocare și restaurare se vor face de către personal de încredere, sub control dual, într-un mediu fizic securizat;
- c) Orice copie de rezervă a cheii private de semnare a TSU este protejată în vederea asigurării confidențialității de către modulul criptografic înainte de a fi stocată în afara acestui dispozitiv.

8.2.3. Distribuirea cheii publice a TSU

Trans Sped TSA se obligă să asigure integritatea și autenticitatea cheilor publice de semnare ale TSU pe parcursul distribuirii acestora către terțele părți. În acest sens:

- a) Cheia publică de semnare a TSU este pusă la dispoziția terțelor părți sub formă de certificat de cheie publică;
- b) Certificatul cheii publice de semnare a TSU este emis de către o autoritate de certificare de încredere.

8.2.4. Schimbarea cheii TSU

Cheile private de semnare ale TSU au o durată de viață în acord cu rezistența algoritmului folosit și cu lungimea cheilor. Cheile private expirate nu sunt arhivate și sunt distruse imediat la expirare. Certificatele de cheii publice ale TSU sunt stocate pentru 15 ani pentru a permite verificarea mărcilor de timp emise în trecut.

8.2.5. Distrugerea cheii TSU

Trans Sped TSA se obligă să asigure că cheile private de semnare ale TSU nu mai sunt folosite după expirarea perioadei de viață. În acest sens:

- a) Au fost stabilite proceduri operaționale și tehnice ce permit instalarea unei noi chei atunci când cea veche expiră;
- b) Cheia privată de semnare a TSU care a expirat, inclusiv copiile de rezervă sunt distruse astfel încât să nu mai poată fi refăcute.
- c) TSU nu permite generarea de noi mărci temporale dacă cheia sa privată de semnare a expirat.

8.2.6. Managementul modulului criptografic folosit pentru a semna mărcile temporale

Trans Sped TSA se obligă să asigure securitatea modulului criptografic pe tot parcursul ciclului de viață, de la producător până la scoaterea acestuia din producție. În acest sens, Trans Sped TSA verifică că:

- a) Modulul criptografic nu a fost deschis pe parcursul livrării;
- b) Modulul criptografic nu a fost deschis pe timpul depozitării;
- c) Instalarea, activarea și duplicarea cheilor de semnare ale TSU în cadrul modulului criptografic se face numai de către personal de încredere, sub control dual, într-un mediu fizic securizat;
- d) Modulul criptografic funcționează corect;
- e) Cheile private de semnare ale TSU stocate pe modulul criptografic sunt șterse după scoaterea acestuia din funcțiune.

8.3. Marcarea temporală

8.3.1. Marca temporală

Trans Sped TSA se obligă să asigure că mărcile temporale sunt emise în mod securizat și conțin timpul corect. În acest sens:

- a) Mărcile temporale emise includ un identificator al politicii sub care sunt emise;
- b) Fiecare marcă temporală are un număr de identificare unic;
- c) Sursa de timp a serviciului de marcă temporală al Trans Sped folosește semnalul GPS împreună cu un set de servere Network Time Protocol (NTP) ca sursă de timp. Folosind această configurație abaterea este de +/- 1 secundă sau mai precisă folosind UTC.
- d) Dacă ceasul Trans Sped își pierde sincronizarea, atunci TSU nu va mai emite mărci temporale;
- e) Marca temporală include rezumatul datelor (valoarea hash) ce se doresc a fi marcate temporal;
- f) Marca temporală este semnată folosind o cheie generată exclusiv pentru acest scop.

8.3.2. Acuratețea timpului

Sursa de timp a serviciului de marcă temporală al Trans Sped folosește semnalul GPS împreună cu un set de servere Network Time Protocol (NTP) ca sursă de timp. Folosind această configurație abaterea este de +/- 1 secundă sau mai precisă folosind UTC.

Trans Sped TSA se obligă să conceapă și să implementeze măsurile necesare pentru a detecta schimbările în calibrarea ceasului intern și problemele de sincronizare care pot compromite precizia stabilită prin prezenta politică.

8.3.3. Formatul mărcii temporale

Marca temporală furnizată de Trans Sped TSA este în conformitate cu RFC 3161. Serviciul furnizează mărci temporale cu algoritm RSA și o lungime a cheii de 2048 ce acceptă algoritmul hash SHA 256.

8.3.4. Limitări ale serviciului

În contextul în care abonatul deține o relație contractuală pentru furnizarea mărcilor temporale cu Trans Sped TSA, serviciul de mărci temporale furnizat de Trans Sped TSA poate fi utilizat în scopul oricărei tranzacții legale, fără limitări, atât timp cât nu sunt precizate alte condiții specifice la nivel de contract.

În limitele stabilite de legislația din România, în nicio circumstanță (exceptând fraudă sau conduita incorectă) Trans Sped nu va fi responsabil pentru:

- Orice pierdere financiară;

- Orice pierdere de date
- Oricare consecință negativă determinată direct sau indirect de utilizarea, furnizarea, licențierea, performanța sau neperformanța certificatelor sau a semnăturilor electronice;
- Oricare alte consecințe negative.

Trans Sped nu are nicio responsabilitate financiară pentru utilizarea improprie a mărcilor temporale.

8.3.5. Verificarea mărcilor temporale

Pentru a verifica o marcă temporală emisă de către Trans Sped TSA, următoarele aspecte vor fi avute în vedere:

- **Verificarea emitentului mărcii temporale:** Emitentul unei mărci temporale este un TSA care trebuie să utilizeze certificate adecvate pentru emiterea acelei mărci temporale. Cheile publice ale certificatelor de marcă temporală sunt incluse în TSU și certificatele AC sunt publicate pentru a permite verificarea faptului că marca temporală a fost semnată corect de către TSA. Certificate TSU din cadrul Trans Sped sunt disponibile pentru verificare la adresa: www.transsped.ro
- **Verificarea statusului revocării mărcii temporale:** Trans Sped pune la dispoziția entităților interesate un serviciu OCSP pentru verificarea statusului de revocare a certificatelor utilizate de TSU pentru semnarea mărcii temporale. Adresa pentru accesarea serviciului OCSĂ este inclusă în certificatul TSU, utilizat pentru semnarea mărcii temporale
- **Verificarea integrității mărcii temporale:** Pentru a verifica integritatea unei mărci temporale, se are în vedere verificarea integrității criptografice a mărcii (de exemplu, dacă structura ASN.1 este corectă și datele aparțin aplicației). Această informație poate fi verificată prin serviciul web Trans Sped TSA furnizat gratuit de către Trans Sped.

8.3.6. Disponibilitatea serviciului

Trans Sped TSA a implementat următoarele măsuri pentru a asigura disponibilitatea serviciului:

- Dispunere redundantă a sistemelor IT pentru a evita “single point of failures”
- Conexiuni internet de mare viteză redundante
- Utilizarea surselor de alimentare fără întreruperi (UPS-uri) și a generatoarelor electrice

Deși aceste măsuri asigură disponibilitatea serviciilor Trans Sped TSA, o disponibilitate anuală de 100% nu poate fi garantată. Trans Sped TSA urmărește să asigure o disponibilitate a serviciului de 99% pe an.

8.4. Managementul și operarea TSA

8.4.1. Managementul securității

Trans Sped se asigură că procedurile administrative și manageriale sunt aplicate în cadrul companiei și că acestea sunt în concordanță cu practicile în domeniu. În particular:

- a) Trans Sped poartă întreaga responsabilitate pentru furnizarea serviciului de marcă temporală în conformitate cu această politică;
- b) Trans Sped dispune de o politică privind securitatea informațiilor care este cunoscută și respectată de către toți angajații și colaboratorii companiei;
- c) Infrastructura necesară pentru managementul securității informațiilor în cadrul Trans Sped este menținută și îmbunătățită. Orice modificare care are implicații asupra nivelului de securitate asigurat este aprobată de managementul Trans Sped.
- d) Controalele de securitate și procedurile de operare aferente Trans Sped TSA sunt documentate, implementate și menținute.

8.4.2. Clasificarea și managementul bunurilor

Trans Sped se asigură că informațiile, precum și celelalte bunuri, sunt protejate în mod corespunzător. În particular, Trans Sped menține un inventar al bunurilor de valoare și să le clasifice din punct de vedere al cerințelor de protecție, în concordanță cu rezultatele analizei de risc.

8.4.3. Securitatea personalului

Trans Sped se asigură că personalul selectat contribuie la sporirea încrederii în modul de operare al TSA. În particular:

- a) Trans Sped folosește pentru operarea TSA numai personal cu cunoștințe și experiență în domeniul semnăturilor electronice și mărcilor temporale;
- b) Rolurile și responsabilitățile pe linia asigurării securității sunt incluse în fișele posturilor. Rolurile de încredere, de care depinde securitatea Trans Sped TSA, sunt clar identificate;
- c) Trans Sped asigură separarea responsabilităților și respectarea principiului celui mai mic privilegiu, instruirea și conștientizarea angajaților;
- d) Personalul își exercită atribuțiunile în conformitate cu politicile și procedurile de securitate.

Rolurile de încredere pentru Trans Sped TSA, presupun următoarele responsabilități:

- *Administrator de securitate:* Responsabilitate globală pentru implementarea politicilor și procedurilor de securitate;
- *Administrator de sistem:* Autorizat să instaleze, configureze și să administreze sistemele și aplicațiile TSA;

- *Operator*: Responsabil cu operarea zilnică a sistemelor și aplicațiilor TSA. Autorizat să execute operațiile de salvare și de restaurare a sistemului;
- *Auditor intern*: Autorizat să acceseze arhivele și log-urile de audit ale sistemelor de încredere ale TSA.

Desemnarea persoanelor care vor ocupa roluri de încredere se face de către managementul companiei care efectuează verificări detaliate cu privire la background-ul acestora.

8.4.4. Securitatea fizică și de mediu

Trans Sped se asigură că accesul fizic la sistemele critice este controlat și că riscurile de natură fizică la adresa bunurilor de valoare ale companiei sunt minimizate și respectă cerințele standardului ETSI EN 319 401. În particular:

- a) Pentru serviciul de furnizare a mărcilor temporale cât și pentru cel de management al mărcilor temporale:
 - accesul fizic în locațiile în care sunt dispuse serviciile de marcă temporală este permis numai personalului autorizat;
 - sunt implementate măsuri de control care să preîntâmpine pierderea, distrugerea sau compromiterea bunurilor sau întreruperea activităților companiei;
 - sunt implementate măsuri de control care să preîntâmpine compromiterea sau furtul de informații sau de sisteme de procesare a informațiilor.
 - sunt implementate măsuri de control al accesului la modulele criptografice folosite pentru a semna mărcile temporale;
- b) Pentru serviciul de management al mărcilor temporale sunt asigurate în plus următoarele măsuri:
 - Serviciile de management al mărcilor temporale sunt operate într-un mediu care să asigure protecția fizică împotriva compromiterii prin accesul neautorizat la sisteme și date;
 - Protecția fizică este asigurată prin crearea de perimetre de securitate clar definite;
 - Sunt implementate măsuri de control fizic și de mediu pentru a proteja locațiile care găduiesc sistemele și facilitățile folosite pentru implementarea acestor servicii. Aceste măsuri asigură, cel puțin, controlul fizic al accesului, protecția împotriva dezastrelor naturale, protecția împotriva incendiilor, protecția împotriva penelor de curent, protecția împotriva efracțiilor și restaurarea în caz de dezastru;
 - Sunt implementate măsuri de control care să asigure protecție împotriva scoaterii fără autorizație în afara companiei a echipamentelor, informațiilor, mediilor de stocare și software-ului aferent serviciilor de marcă temporală.

8.4.5. Managementul operațional

Trans Sped se asigură că componentele sistemului TSA sunt securizate și operate corect astfel încât să se minimizeze riscul întreruperii serviciului de marcă temporală. În particular:

- a) Integritatea componentelor sistemului TSA și a informațiilor sunt protejate împotriva virușilor, codului malițios sau neautorizat;
- b) Procedurile de raportare și răspuns la incidente sunt gândite astfel încât pierderile rezultate în urma incidentelor de securitate să fie minimizezate;
- c) Mediile de stocare folosite în cadrul sistemelor de încredere ale TSA să fie administrate în siguranță pentru a preveni distrugerea, furtul sau accesul neautorizat;
- d) Sunt elaborate și implementate proceduri de operare pentru rolurile de încredere sau administrative care au impact asupra furnizării serviciilor de marcă temporală;
- e) Mediile de stocare sunt administrate în siguranță, în conformitate cu cerințele impuse prin schema de clasificare a informațiilor. Mediile de stocare ce conțin date sensibile sunt distruse atunci când nu mai sunt necesare;
- f) Capacitatea echipamentelor este monitorizată. De asemenea, sunt făcute previziuni cu privire la nevoile viitoare de capacitate pentru a asigura că există întotdeauna suficientă putere de procesare și spațiu de stocare disponibil;
- g) TSA se asigură că poate acționa în timp util și de o manieră coordonată pentru a răspunde rapid la incidente și pentru a limita impactul breșelor de securitate. Toate incidentele sunt raportate cât mai repede posibil.

8.4.6. Managementul accesului la sisteme

Trans Sped se asigură că accesul la sistemele TSA este permis numai personalului autorizat. În particular:

- a) Sunt implementate măsuri de control (de exemplu, firewall) pentru a proteja rețeaua internă a TSA împotriva accesului neautorizat;
- b) Asigură managementul corespunzător al conturilor utilizatorilor pentru a menține securitatea sistemelor;
- c) Se asigură că accesul la informații și aplicații este restricționat în conformitate cu politica de control al accesului și că sistemele TSA permit separarea rolurilor de încredere, în special a celor de administrator și operator. Folosirea utilităților de sistem este restricționată și controlată strict.
- d) Personalul TSA este identificat și autentificat în mod corespunzător înainte de a putea folosi aplicațiile specifice serviciului de marcă temporală.
- e) Acțiunile personalului TSA sunt jurnalizate;

Pentru serviciul de management al mărcilor temporale sunt asigurate în plus următoarele măsuri:

- a) Componentele de rețea (de exemplu, ruterele) sunt păstrate într-un mediu fizic securizat iar configurația acestora este auditată periodic;

- b) Sunt implementate soluții de monitorizare continuă și alarmare care să permită detectarea, înregistrarea și reacționarea în timp util în cazul oricărui acces neautorizat la o resursă.

8.4.7. Instalarea și mentenanța sistemelor de încredere

Trans Sped utilizează sisteme și produse de încredere care să fie protejate împotriva modificărilor. În particular:

- a) În faza de proiectare și elaborare a cerințelor pentru orice proiect de dezvoltare de sistem derulat de Trans Sped, sunt analizate cerințele de securitate;
- b) Sunt aplicate proceduri de control al schimbării pentru darea în exploatare, modificarea, actualizarea aplicațiilor software operaționale.

8.4.8. Compromiterea serviciilor TSA

În cazul unui eveniment care afectează securitatea serviciilor TSA, cum ar fi compromiterea cheilor private ale TSU sau decalibrarea ceasului folosit în procesul de marcă temporală, Trans Sped va informa în mod corespunzător abonații și terțele părți.

Procesul de emitere al mărcilor temporale este întrerupt până la remedierea cauzei care a produs evenimentul respectiv.

8.4.9. Încetarea activității TSA

În eventualitatea în care Trans Sped TSA își încetează operațiunile, indiferent de motiv, va notifica autoritatea națională de supraveghere înainte de încetarea propriu-zisă.

În cazul în care Trans Sped TSA încetează a mai furniza servicii de marcă temporală minimizează potențialele disfuncționalități cauzate abonaților și terțelor părți și să permită în continuare accesul la informațiile necesare validării mărcilor temporale emise anterior. În particular:

- a) Trans Sped TSA informează abonații și terțele părți cu privire la decizia de a înceta furnizarea serviciilor de marcă temporală;
- b) Trans Sped TSA transferă unui alt TSA sau, după caz, Autorității de Reglementare și Supraveghere, registrul electronic operativ de evidență a mărcilor temporale emise, documentația aferentă algoritmilor și procedurilor de generare a mărcilor temporale, certificatul digital al cheii publice de semnare a mărcilor temporale, precum și alte informații necesare demonstrării corectitudinii și validării mărcilor temporale emise anterior;
- c) Cheile private ale TSU, inclusiv copiile de rezervă, sunt distruse astfel încât să nu mai poată fi refăcute.
- d) Certificatele TSU sunt revocate.

8.4.10. Conformitatea cu cerințele legale

Trans Sped va lua toate măsurile pentru a asigura conformitatea cu cerințele legale în vigoare, în special cu:

- Regulamentul European 910/2014 eIDAS
- Legea nr. 455/2001 privind semnăturile electronice;
- Legea nr. 451/2004 privind marca temporală;
- Ordinul MCSI nr. 492/2009 privind normele tehnice și metodologice pentru aplicarea Legii nr. 451/2004 privind marca temporală;
- Regulamentul (UE) 679/2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (GDPR)
- Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679

8.4.11. Înregistrarea operațiilor cu privire la operarea serviciului de marcă temporală

Trans Sped se asigură că toate informațiile relevante cu privire la operarea serviciului de marcă temporală sunt înregistrate și păstrate pentru a permite rezolvarea disputelor, detectarea tentativelor de compromitere a securității TSA și auditarea TSA. În particular:

- a) Este asigurată confidențialitatea și integritatea înregistrărilor curente și arhivate;
- b) Înregistrările cu privire la operarea serviciului de marcă temporală sunt arhivate în siguranță;
- c) Evenimentele importante cu privire la TSA, cum ar fi cele legate de managementul cheilor sau sincronizarea ceasului, sunt înregistrate;
- d) Înregistrările sunt păstrate în conformitate cu prevederile legale în vigoare.

Trans Sped menține un registru electronic operativ de evidență al mărcilor temporale emise, disponibil permanent pentru consultare online. Structura și condițiile de exploatare ale registrului electronic sunt cele stabilite prin Ordinul MCSI nr. 492/2009 privind normele tehnice și metodologice pentru aplicarea Legii nr. 451/2004 privind marca temporală.

8.4.12. Accesul la rețea

Trans Sped asigură protecția rețelei și a sistemelor de atacuri malițioase. În particular:

- a) Rețeaua Trans Sped este segmentată și construită astfel în urma analizei de risc. Această analiză a ținut cont de relația funcțională, logică și fizică dintre sistemele de încredere și servicii
- b) Trans Sped restricționează accesul și comunicațiile între zonele folosite de serviciile de încredere. Serviciile ce nu sunt necesare, sunt dezactivate și conexiunile ce nu sunt

- necesare sunt interzise printr-un set de reguli revizuite periodic.
- c) Toate elementele critice folosite de Trans Sped sunt ținute într-un mediu sigur și securizat.
 - d) Sunt stabilite rețele dedicate folosite pentru administrarea sistemului IT ce sunt separate de celelalte rețele. Sistemul utilizat pentru administrare nu va fi folosit în alte scopuri decât cel prestabilit.
 - e) Trans Sped dispune de un mediu de test folosit de dezvoltatori și care este separat de mediul de producție.
 - f) Comunicarea între sistemele de încredere distincte pot fi stabilite numai prin canale de încredere, care sunt în mod logic, distincte de celelalte canale de comunicare și asigură identificarea sigură și protecția părților implicate și a modificarea datelor sau divulgarea acestora.
 - g) Conexiune la internet este redundantă, asigurând funcționalitatea în cazul în care semnalul nu este corespunzător.
 - h) Trans Sped efectuează periodic teste de penetrare și scanări ale sistemului pentru a identifica vulnerabilitățile acestuia. Testele de penetrare și scanarea vulnerabilităților sunt efectuate de personal calificat ce respecta codul de etică și care furnizează periodic rapoarte exacte.

8.4.13. Gestionarea incidentelor

Activitățile sistemului, userii și serviciile folosite de Trans Sped sunt monitorizate. În special:

- a) Monitorizarea activității ține cont de informațiile colectate și analizate
- b) Activitățile care nu se încadrează în normele impuse ale sistemului și indică o posibilă încălcare de securitate, inclusiv intruziune în rețea, sunt detectate și raportate ca alarme persoanelor abilitate numite de Trans Sped.
- c) Sistemele Trans Sped monitorizează următoarele evenimente.
 - conectarea și deconectarea de la rețea
 - disponibilitatea și activitatea serviciilor necesare, utilizate în rețea
- d) Managementul a atribuit personal care acționează în timp util și coordonat, în scopul de a răspunde rapid la incidente și pentru a limita impactul eventualelor încălcări ale securității. Personalul atribuit are rolul de a urmări evenimentele critice de securitate și să se asigure că incidentele relevante sunt raportate în conformitate cu procedurile interne.
- e) Trans Sped notifică părțile implicate cu privire la orice încălcare a securității sau pierderea integrității, care are un impact semnificativ asupra serviciului de încredere furnizat și a datele cu caracter personal. Organismele de supraveghere sunt anunțate în termen de 24 de ore după descoperirea încălcării critice de securitate.
- f) Log-urile generate în urma monitorizării sunt verificate periodic pentru a identifica posibilele activități malițioase.

- g) Trans Sped va remedia vulnerabilitățile critice descoperite într-o perioadă corespunzătoare. În cazul în care vulnerabilitatea nu poate fi remediată se încearcă să se scadă impactul, până când va dispune de resursele (echipamente, update-uri, etc) necesare. Dacă o vulnerabilitate critică nu va fi remediată se va întocmi un document ce va specifica motivul pentru care nu este necesară nicio acțiune în acest sens.
- h) Procedurile de raportare și răspuns sunt concepute astfel încât să diminueze impactul pe care un incident îl poate produce.

8.4.14. Managementul continuității afacerii

Toate sisteme IT implicate în serviciul de marcare temporală oferă redundanță de minim N + 1 și sunt fizic localizate într-un mediu securizat care diminuează riscul dezastrelor naturale.

Cheile private ale serviciului de marcare temporală sunt stocate în siguranță, într-un echipament HSM FIPS 140-2 Level 3, care oferă, de asemenea, o redundanță N + 1.

În cazul în care cheile private devin compromise, back-ul efectuat periodic ajută la diferențierea între marcajele de timp corecte și false, într-un proces de auditare.

În urma unui dezastru natural care cauzează pierderea sediului central, serviciul de marcare temporală va funcționa folosind echipamentele destinate acestui tip de incident, iar activitatea va fi redirecționată către un punct de lucru prestabilit în procedura de Managementul continuității afacerii.

8.5. Măsurile organizaționale

Trans Sped demonstrează că este o companie de încredere. Pentru aceasta, Trans Sped a implementat și certificată următoarele sisteme de management: Sistem de management al calității conform ISO 9001:2015, Sistem de management al securității informațiilor conform ISO/IEC 27001: 2013, Sistem de management de mediu conform SR EN ISO 14001:2005, Sistem de management al sănătății și securității ocupaționale conform OHSAS 18001:2008.