



Trans Sped
TSP
Your Trusted Service Provider

Codul de Practici și Proceduri și Politica de Certificare pentru *Certificate Calificate*

Versiunea 4.5

Data intrării în vigoare: 11 august 2023

Informații generale	
Versiune	4.5
Clasificarea informației	<i>Public</i>
Aprobat de	<i>Comitet de Management al Politicilor și Procedurilor</i>
Data aprobării	<i>Iulie 2023</i>
Data intrării în vigoare	<i>August 2023</i>

Istoricul Modificarilor			
Versiune	Descriere	Data	Autor(i)
4.0	Actualizare pentru cross-certificarea SAFE-BioPharme	Iulie 2017	Viky MANAILA
4.1	Extinderea duratei de valabilitate a certificatelor la 3 ani	Decembrie 2017	Viky MANAILA
4.2	Revizuire	Ianuarie 2020	Camelia IVAN
4.3	Actualizarea conținutului pentru sigilii electronice, certificate digitale calificate pentru semnatura electronica si metodele de identificare a persoanelor la distanta	Mai 2022	Camelia IVAN
4.5	Actualizarea conținutului pentru conformitate cu standardele în vigoare	Iunie 2023	Catalina GRIGORE



**Codul de Practici și Proceduri și Politica de Certificare
pentru Certificate Calificate
Versiune 4.5**

CUPRINS

CUPRINS	4
1. INTRODUCERE	7
1.1. Descriere generală.....	7
1.2. Denumirea documentului și identificare	8
1.3. Participanții PKI	9
1.4. Utilizarea certificatului	10
1.5. Administrarea politicii	11
1.6. Definiții și acronime	11
2. Publicare și Responsabilități Depozitar	21
2.1. Depozitar.....	21
2.2. Publicarea informațiilor din certificat	21
2.3. Frecvența publicării	21
2.4. Controlul accesului la Depozitare	21
3. Identificarea și autentificarea	21
3.1. Numele.....	21
3.2. Validarea inițială a identității.....	23
3.3. Identificarea și autentificarea pentru cererile de re-key	24
3.4. Identificarea și autentificarea pentru cererile de revocare	25
4. CERINȚE OPERAȚIONALE PRIVIND CICLUL DE VIAȚĂ AL CERTIFICATULUI.....	26
4.1. Aria de aplicabilitate a certificatelor.....	26
4.2. Procesarea cererilor de certificate	26
4.3. Emiterea unui certificat digital calificat.....	26
4.4. Acceptarea certificatului digital calificat	26
4.5. Utilizarea perechii de chei și a Certificatului.....	27
4.6. Reînnoirea unui certificat digital calificat.....	27
4.7. Revocarea și suspendarea Certificatului	28
4.8. Servicii privind starea certificatelor	31
5. CONTROALELE DE SECURITATE FIZICE, DE PROCEDURĂ ȘI DE PERSONAL	32
5.1. Controale fizice.....	32
5.2. Controale de procedură.....	33
5.3. Controale la nivel de personal	34
5.4. Procedurile de registre de audit	34
5.5. Arhivarea înregistrărilor	36

5.6.	Schimbarea cheii.....	36
5.7.	Compromiterea și recuperarea după dezastre	36
5.8.	Terminarea AC	37
6.	CONTROALE DE SECURITATE TEHNICĂ	38
6.1.	Generarea și instalarea perechii de chei.....	38
6.2.	Protecția cheii criptografice private	40
6.3.	Alte aspecte legate de managementul perechii de chei criptografice	42
6.4.	Datele de activare.....	43
6.5.	Controalele de securitate ale calculatorului	43
6.6.	Ciclul de viață al controalelor tehnice	43
6.7.	Controalele de Securitate a Rețelei.....	44
6.8.	Controale la nivelul modulului criptografic.....	44
6.9.	Marcare temporală	44
7.	PROFILELE CERTIFICATELOR, CRL ȘI OCSP.....	45
7.1.	Profilul certificatului.....	45
7.2.	Profilul CRL	61
7.3.	Profilul OCSP	62
7.4.	Procedurile de schimbare a specificațiilor	64
7.5.	Politicile de publicare și notificare	64
7.6.	Procedurile de aprobare a CPP	64
8.	AUDITUL DE CONFORMITATE ȘI ALTE EVALUĂRI	65
8.1.	Frecvența auditărilor	65
9.	ALTE ASPECTE LEGALE	66
9.1.	Taxe	66
9.2.	Responsabilitate financiară	66
9.3.	Confidențialitatea informațiilor de afaceri.....	66
9.4.	Confidențialitatea datelor personale	67
9.5.	Drepturile de proprietate Intelectuală	67
9.6.	Declarații și garanții.....	67
9.7.	Limitarea responsabilității	70
9.8.	Despăgubiri.....	71
9.9.	Termeni și încetarea.....	71
9.10.	Notificări individuale și comunicarea cu participanții	71
9.11.	Amendamente	72
9.12.	Procedurile de soluționare a litigiilor.....	72

9.13.	Legea aplicabilă	72
9.14.	Conformitate cu legislația aplicabilă	73

1. INTRODUCERE

Realizarea afacerii și comunicarea prin rețele publice și private devin din ce în ce mai importante în comerțul electronic. Una din cerințele comunicării electronice este abilitatea de a identifica creatorul informației electronice în același fel în care documentele sunt semnate folosind o semnătură olografă. Din punct de vedere tehnic acest lucru poate fi realizat prin semnăturile electronice sau sigiliile electronice. Valoarea semnăturilor electronice sporește semnificativ dacă emiterea unei semnături electronice/sigiliu electronic de către un individ este efectuată de către o terță parte independentă și de încredere. Această terță parte este denumită în mod comun Prestator de Servicii de Incredere sau Autoritate de Certificare (AC). O Autoritate de Certificare emite certificate digitale legând o cheie criptografică publică de entitatea numită în certificat și care posedă cheia criptografică privată corespondentă.

Pentru ca utilizatorii semnăturii electronice/sigiliilor electronice să aibă încredere în autenticitatea semnăturilor electronice au nevoie să aibă încredere că AC a stabilit în mod corespunzător proceduri și măsuri de protecție pentru a minimiza amenințările operaționale și financiare și riscurile asociate cu emiterea de certificate digitale.

Acest document specifică practicile operării și conducerii Trans Sped AC care emite certificate digitale calificate în conformitate cu Regulamentul (UE) nr. 910/2014 (eIDAS) și în conformitate cu Specificațiile tehnice 319 401 ale Institutului pentru Standardele Telecomunicațiilor Europene (ETSI EN 319 401): **Cerințele privind politica generală a Prestatorilor de Servicii de Incredere.**

Este o practică comună pentru o AC să emită două documente:

- un Cod de Practici și Proceduri (CPP) care descrie practicile pe care o AC le folosește în administrarea certificatelor digitale (solicitare, emitere, utilizare, și revocare);
- o Politică de Certificare (PC) care descrie procesele de verificare și permite o estimare a încrederii și siguranța bazate pe măsura etapelor de verificare întreprinse pentru a verifica conținutul certificatelor.

Deoarece certificatele digitale calificate au la bază aceleași reglementări și cerințe definite în Regulamentul eIDAS ambele documente mai sus menționate (CPP și PC) au fuzionat într-un singur document, acest CPP/PC.

1.1. Descriere generală

Certificatele digitale sunt utilizate folosind criptarea cheii criptografice publice, aceasta fiind o tehnică unde orice entitate care participă are o pereche de chei criptografice. Una din aceste chei criptografice este privată și trebuie ținută secretă; cealaltă este publică și poate fi pusă la dispoziție pentru a fi disponibilă în registrul de chei publice, cum ar fi numerele de telefon dintr-o carte de telefon publică. Orice este criptat cu cheie privată poate fi decriptat doar cu cheia publică corespondentă (și vice versa). Această tehnică poate fi utilizată pentru a implementa semnături digitale sau sigilii electronice: expeditorul criptează datele folosind cheia lui privată, și destinatarul poate verifica integritatea sa folosind cheia publică corespondentă dintr-un registru de chei publice.

Un certificat digital este, în esență, o cheie criptografică publică semnată digital. Acesta conține numele posesorului cheii criptografice private corespondente, care este denumit semnatar. Din moment ce oricine poate crea o cheie publică cu orice nume dat, este esențial să se verifice dacă un certificat luat dintr-un registru aparține semnatarului numit în acesta, pentru că altfel semnăturile ar putea fi falsificate.

O Autoritate de Certificare acționează în calitate de terță parte de încredere care leagă certificatele digitale de entitatea indicată. Un certificat eliberat de către o AC conține numele semnatarului, numele AC, cheia publică a semnatarului și este semnat de către AC.

Trans Sped emite certificate digitale calificate pentru semnătură electronică și sigilii electronice în conformitate cu Regulamentul eIDAS. Certificatele calificate pot fi folosite pentru a produce semnături electronice calificate și sigilii electronice calificate care sunt în mod legal considerate ca fiind echivalente cu semnăturile olografe. Ca o consecință naturală certificatele digitale calificate pentru semnături electronice pot fi emise doar către persoane fizice în nume propriu sau în beneficiul unei organizații. Certificatele digitale calificate pentru sigilii electronice pot fi emise doar pentru persoane juridice (organizații).

Certificatele digitale calificate se eliberează pe dispozitive de creare a semnăturilor electronice certificate (dispozitive de creare a semnăturilor securizate sau HSM) care îndeplinesc cerințele Regulamentului eIDAS.

Pentru a permite o estimare a siguranței certificatelor digitale calificate emise și pentru a dovedi respectarea Regulamentului eIDAS și în conformitate cu cerințele ETSI EN 319 401, Trans Sped publică prezentul CPP/PC în care sunt descrise procedurile folosite pentru emiterea de certificate digitale calificate precum și descrierea modului în care este efectuată verificarea datelor conținute în certificat.

Prezentul CPP/PC descrie structura și practicile Trans Sped. Nu constituie nici o declarație de self-escrow, nici nu declară garanțiile legale.

Prezentul CPP/PC se folosește în mare măsură de vocabularul legat de domeniul semnăturilor digitale, sigiliilor electronice și a certificatelor, criptografie și criptarea cheii publice, la care se face referire în Capitolul 1.6. De asemenea, capitolul 1.6 oferă definițiile unor termeni importanți care nu mai apar în altă parte în acest text și care au legătură cu domeniile mai sus menționate.

1.2. Denumirea documentului și identificare

Trans Sped S.A. cu sediul în strada Despot Vodă, nr. 38, 020656 București, România (denumită "Trans Sped" sau "TSP" în acest CPP/PC), este un Prestator de Servicii de Încredere Calificat, iar serviciile furnizate sunt calificate și se regăsesc în Lista de Încredere (Trusted List) a statului membru UE, în cazul nostru România, în conformitate cu prevederile Regulamentului eIDAS.

<https://esignature.ec.europa.eu/efda/tl-browser/#/screen/tl/RO/1>

Prezentul CPP/PC este pus la dispoziție la cerere prin e-mail sau poate fi preluat de pe site-ul Trans Sped <http://www.transsped.ro/repository> . respectiv <https://www.transsped.ro/certificari>
Structura și conținutul CPP/PC este în conformitate cu recomandările RFC 3647, ETSI EN 319 411-1 și ETSI EN 319 411-2.

1.3. Participanții PKI

Acest CPP/PC se aplică certificatelor digitale calificate pentru semnătură electronică și sigiliu electronic care:

- a) întrunesc cerințele prevăzute din Regulamentul eIDAS;
- b) sunt emise de către TSP cu respectarea cerințelor prevăzute în Regulamentul eIDAS;
- c) sunt destinate pentru a fi utilizate doar cu dispozitive securizate de creare a semnăturii electronice (DSCS) care întrunesc condițiile prevăzute în Regulamentul eIDAS;
- d) sunt emise către public.

Participanți ai Trans Sped PKI sunt acele entități care îndeplinesc un rol în Trans Sped PKI prin utilizarea și prin furnizarea serviciilor de certificare. Astfel sunt identificați următorii participanți:

- Autoritățile de certificare
- Autoritățile de Înregistrare
- Entitățile finale

1.3.1. Autoritățile de Certificare

Trans Sped este un Prestator Calificat de Servicii de Incredere care emite certificate digitale calificate sub prezentul CPP/PC. Trans Sped operează una sau mai multe Autorități de Certificare (AC) care creează și semnează certificate digitale calificate pentru entități finale. Trans Sped folosește diverse servicii PKI în care AC-urile sale sunt găzduite în centre de date securizate la nivel înalt.

Toate echipamentele pentru rularea serviciilor sale PKI incluzând dar fără a se limita la CA, OCSP, CRL, servere RA, Aplicație de Semnare a Serverului (ASS definită în [CEN / TS 419241]), HSM se bucură de aceleași controale descrise în secțiunile 5 și 6 pentru personalul fizic, securitatea procedurală și tehnică. Localizarea și construcția instalației care găzduiește CA-urile și echipamentele sunt în concordanță cu facilitățile folosite pentru a găzdui informații sensibile, de mare valoare.

1.3.2. Autoritățile de Înregistrare

O Autoritate de Înregistrare (AI) lucrează în numele unei AC. Trans Sped operează o Autoritate de Înregistrare internă dar poate în același timp să folosească furnizori de servicii externi ca AI subsidiare responsabile pentru verificarea atât a informațiilor de afaceri cât și a datelor personale incluse în certificatul digital al utilizatorului.

Orice AI subsidiară este din punct de vedere contractual legată de Trans Sped. Ofițerii de Înregistrare ai unei asemenea AI subsidiare sunt identificați individual; aceștia dețin certificate speciale de Ofițer de Înregistrare (RO). Doar informațiile semnate de către RO vor fi acceptate de către AC.

Identificarea personală a utilizatorilor finali care aplică pentru un certificat calificat poate avea loc la Trans Sped sau la oricare din AI subsidiare utilizate în acest scop.

De asemenea, identificarea personală a utilizatorilor finali care aplică pentru un certificat digital calificat se poate realiza prin mijloace video cu operator uman sau automat conform Norma ADR din 2021 privind reglementarea, recunoașterea, aprobarea sau acceptarea procedurii de identificare a persoanei la distanță utilizând mijloace video. TRANS SPED S.A. a primit aviz favorabil din partea Agenției pentru Digitalizarea României pentru furnizarea serviciilor de identificare la distanță prin mijloace video.

1.3.3. Entitățile finale

În prezentul document, entitatea finală (sau utilizatorul final) este un sinonim pentru semnatar (sau persoană). Se referă la persoanele fizice (pentru semnătura electronică) sau persoanele juridice (pentru sigiliu electronic) care folosesc certificate digitale calificate emise de către Trans Sped.

1.4. Utilizarea certificatului

Din punct de vedere tehnic, toate aplicațiile în domeniul semnăturilor electronice, sigiliilor electronice și comunicării sigure prin internet sunt potrivite pentru a fi folosite cu certificatele digitale emise în conformitate cu termenii prezentului CPP/PC.

Prezentul CPP/ PC definește certificatele digitale:

- a) Care întrunesc cerințele prevăzute în [eIDAS];
- b) Sunt emise de către Trans Sped în conformitate cu cerințele prevăzute în [eIDAS];
- c) Care sunt utilizate doar cu dispozitivele securizate de creare a semnăturii (DSCS) care respectă cerințele cuprinse în [eIDAS];
- d) sunt emise către public.

Aria de aplicabilitate a certificatelor stabilește scopul în care poate fi folosit un certificat. Acest scop este definit de două elemente:

- primul definește aplicabilitatea certificatului (de exemplu: semnătură electronică, confidențialitate).
- celălalt este o listă sau o descriere a aplicațiilor permise sau interzise.

Certificatele digitale emise în conformitate cu acest CPP pot fi utilizate pentru diferite scenarii, precum semnarea electronică, sigilierea electronică, marcarea temporală sau autentificare. Totuși, nivelul de importanță a unei informații procesate sau protejate de un certificat digital variază în funcție de anumiți factori. Prin urmare, orice Entitate Finală are obligația de a evalua în mod corespunzător un certificat digital, în funcție de mediul și aplicația în care se utilizează certificatul și riscurile asociate, luând o decizie informată și corectă în legătură cu utilizarea efectivă a unui anumit tip de certificat, emis în conformitate cu acest CPP.

Este interzisă utilizarea unui certificat digital emis de CA Trans Sped cu alt scop decât cel declarat în prezentul document. Indiferent de nivelul de încredere al unui certificat digital, acesta nu oferă nici o garanție referitoare la titularul certificatului precum ca acesta ar acționa cu bună credință, ca este cinstit sau onest în afacerile sale, ori că el sau afacerile sale sunt conforme cu legislația aplicabilă. Un certificat digital confirmă doar faptul că informațiile conținute în acesta au fost verificate în conformitate cu prevederile prezentului document în

momentul în care certificatul a fost emis (spre exemplu, certificatele pentru semnare de cod nu confirmă faptul că codul software semnat este sigur pentru instalare sau că nu conține viruși).

1.5. Administrarea politicii

Acest CPP/PC este administrat de Comitetul de Cod de Practici și Proceduri și Politici de Certificare al Trans Sped.

Persoană de contact:

Administrator CPP/PC
Trans Sped S.A.
Strada Despot Vodă, nr.38
020656 București
România
Tel: +40 21 210 87 02
Fax: +40 21 211 02 07
Email: office@transsped.ro

Persoana care determină conformitatea CPP

Conformitatea Politicilor Trans Sped și a CPP sunt determinate de Comitetul de CPP și PC al Trans Sped.

1.6. Definiții și acronime

A

AUTORITATE DE CERTIFICARE

O autoritate de certificare este o instituție de încredere care certifică cheile criptografice publice, și emite certificatele. În acest scop, informațiile conținute în cheia criptografică publică sunt verificate, în special identitatea deținătorului cheii.

ALGORITM ASIMETRIC

Spre deosebire de algoritmi simetrici, algoritmi de criptare asimetrici (sau cheia publică) folosesc două chei diferite pentru criptare și decriptare, unde cheia criptografică privată nu poate fi dedusă din cealaltă.

ALGORITMII CONVENTIONALI

A se vedea algoritmi simetrici.

ALGORITMUL DE CRIPTARE A CHEII PUBLICE

A se vedea algoritmul asimetric.

ALGORITMUL DE SCHIMB DE CHEIE PUBLICĂ

O metodă de chei publică pentru schimbul sesiunii cheilor. Majoritatea algoritmilor cheii criptografice publice sunt folosiți pentru schimbul de chei secrete pentru algoritmi de criptare

simetrică, nu pentru criptarea datelor. Diffie-Hellman este potrivit doar pentru schimbul de chei, în timp ce RSA este un algoritm de criptare a cheii publice.

ALGORITMUL CHEII SECRETE

A se vedea algoritmul simetric.

ALGORITMUL SIMETRIC

În contrast cu algoritmii asimetrice, cheia utilizată pentru decriptare (sau criptare) poate fi calculată de cealaltă cheie într-un algoritm simetric (sau convențional) de criptare. În majoritatea timpului ambele chei sunt la fel.

APLICAREA PENTRU CERTIFICAT

În contextul prezentului document, termenul “aplicare pentru certificat” se referă la toate informațiile pe care un utilizator le transmite către Autoritatea de Certificare atunci când solicita emiterea unui certificat digital calificat. Aceste informații cuprind, dar nu sunt limitate la, cererea pentru certificat (digital), date cu caracter personal, o fotocopie a cardului său de identitate etc. A se vedea de asemenea cererea pentru certificat.

AMPRENTA DIGITALĂ

Amprenta digitală este un extras din cheia publică (de obicei 128 sau 160 bits în dimensiune) care este utilizată pentru a verifica citind că cineva are cheia corectă, mai precis că cheia aparține entității numite în certificat, fără a trebui să verifice dacă întreaga cheie se potrivește cu exactitate (de obicei 1024 bits și mai mult). Aceasta se realizează prin aplicarea funcției hash la cheia publică.

AUTENTIFICARE

Autentificarea se referă la procesul de confirmare fie a identității unei persoane sau a integrității informației (sau ambele).

AUTO-SEMENAT

O cheie publică este numită auto-semnată dacă este semnată digital folosind cheia privată corespondentă.

AUTORITATEA DE CERTIFICARE

O Autoritate de Certificare este o instituție de încredere care certifică cheile publice, adică emite certificate digitale calificate. În acest scop, sunt verificate informațiile conținute în cheia criptografică publică, în special identitatea deținătorului cheii.

AUTORITATEA DE ÎNREGISTRARE

O entitate care este responsabilă pentru identificarea și autentificarea utilizatorilor certificatului, dar nu semnează sau emite certificate, adică unei AI îi sunt delegate anumite sarcini în numele unei AC.

B

C

CERTIFICAT

Un certificat este o cheie criptografică publică, care este semnat de către o Autoritate de Certificare. El leagă o cheie publică de entitatea numită în certificat (subiect) care deține cheia criptografică privată corespondentă. Un certificat poate fi gândit ca un card electronic ID. Acesta identifică de asemenea Autoritatea de Certificare care a emis certificatul. Formatele certificatelor cele mai folosite în prezent sunt PGP și X.509.

CERTIFICAT DIGITAL CALIFICAT

Un certificat digital calificat este un certificat emis în conformitate cu Regulamentul (UE) nr. 910/2014 (eIDAS). O semnătură realizată folosind un certificat calificat este considerată a fi legal egală cu semnătura olografă.

CIFRU BLOC

Un bloc cifru este un algoritm simetric care încrăpțează blocuri mai mari de text de dimensiune fixată, de obicei 64 bits (egal cu cinci caractere). Exemple de cifre bloc sunt IDEA, DES și Triple-DES. A se vedea de asemenea cifrul stream.

CEREREA PENTRU CERTIFICAT

În contextul prezentului document, termenul “cerere pentru certificat” se referă la cheia publică auto-semnată digital a semnatarului, care poate fi codificată sub formă de binar sau text. Informațiile precum cheia publică ND și cheia publică din cererea de certificat sunt pentru a crea și a semna certificatul. A se vedea de asemenea aplicarea pentru certificat.

CALEA DE CERTIFICARE

Un lanț comandat de certificate care împreună cu cheia publică a obiectului inițial din cale, poate fi procesat pentru a obține obiectul final din cale.

CERTIFICA

A semna digital cheia criptografică publică a altei entități prin utilizarea propriei chei private.

CERTIFICAT DIGITAL

A se vedea certificat.

CHEIE

Un cod digital utilizat pentru a cripta, decripta, crea și verifica semnăturile digitale. Cheile utilizate pentru algoritmi asimetrici sunt în perechi unde cheia privată este folosită pentru a semna datele iar cheia publică este folosită pentru a le verifica. Algoritmi simetrici, în orice caz, utilizează aceeași cheie pentru criptare și decriptare, și nu există conceptul de semnătură digitală.

CHEIA CRIPTOGRAFICĂ PRIVATĂ

Din perechea de chei utilizată în algoritmi asimetrici, cheia privată este cea care trebuie păstrată în siguranță de către deținătorul său. Nimeni altcineva nu mai trebuie să aibă acces la această cheie. De obicei, cheia privată este protejată de o parolă sau parolă frază. Este utilizată pentru decriptarea mesajelor trimise către deținătorul cheii publice corespondente și pentru generarea de semnături digitale.

CHEIA CRIPTOGRAFICĂ PUBLICĂ

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

CHEIA SESIUNII

În algoritmi hibrid, cheia utilizată pentru algoritmul de criptare simetric și schimbat prin algoritmul cheii publice. Cheia sesiunii este generată la întâmplare pentru fiecare schimb de

date, adică pentru fiecare sesiune, în timp ce cheia publică rămâne aceeași pe o perioadă mai lungă de timp.

CHEIA SECRETĂ

A se vedea cheia privată.

CIFRU

Un cifru este un algoritm criptografic folosit pentru criptare.

CIFRU STREAM

Un cifru stream este un algoritm simetric care încrîpțează mesajul caracter cu caracter. A se vedea de asemenea cifru bloc.

CONFIRMA

A stabili prin anchetă și investigație adecvată.

CORESPUNDE

A aparține aceleiași perechi de chei.

CPD

A se vedea Definițiile Politicii de Certificare.

CRL

A se vedea Lista Certificatelor Revocate.

CRIPATANALIZA

Criptanaliza tratează distrugerea algoritmilor de criptare, adică decriptarea mesajelor codificate.

CRIPTARE

Procesul de codificare și acordare de date inutile pentru oricine altcineva decât primitorul menit pentru aceasta.

CRIPTOGRAFIE

Criptografia este știința păstrării secretului unor mesaje.

CRIPTOLOGIE

Criptologia este zona din matematică care combină criptografia și criptanaliza.

CODUL DE PRACTICI ȘI PROCEDURI

O declarație de practici pe care o Autoritate de Certificare le folosește în emiterea de certificate. A se vedea de asemenea Politica de Certificare.

D

DATELE DE ACTIVARE

Valorile datelor, altele decât cheile, care sunt solicitate pentru operarea modulelor criptografice și care trebuie să fie protejate (de ex., un PIN sau o parolă).

DECRIPARE

Procesul de descifrarea al datelor încrîpțate.

DEPOZITAR

O colecție de baze de date pentru depozitarea și retragerea certificatelor, CRL și orice alte informații legate de certificate și semnături digitale, de exemplu prezenta DPC.

DES

DES (Standardul de încriptare al datelor) este un cifru bloc dezvoltat de către IBM la începutul anilor 1970. Inițial dimensiunea cheii utilizate în algoritm a fost de 128 bits, dar NSA a redus-o la 56 bits, care este considerată a fi prea slabă în zilele noastre. O variantă DES cunoscută ca Triple DES oferă o securitate mai bună.

DH

A se vedea Diffie-Hellman.

DIFFIE-HELLMAN

Diffie-Hellman este un algoritm de schimb de cheie publică securizat inventat de către Whitfield Diffie și Martin Hellman în anul 1976. Patentul Diffie-Hellman a expirat în anul 1997.

DPC

A se vedea Codul de Practici și Proceduri.

DN

A se vedea Nume distinct.

DSA

Un algoritm de semnătură de cheie publică propus de către NIST pentru folosirea în DSS care utilizează o cheie variabilă cu mărimea de la 1024 până la 3072 bits.

DSS

DSS (Standardul Semnăturii Digitale) este un standard de semnătură digitală propus de către NIST. DSS este utilizat, de exemplu, de către PGP versiunea 5.0 și mai sus.

E

EMITE UN CERTIFICAT

Procesul unei AC care semnează cheia publică a utilizatorului final, astfel creând certificatul, și notificând semnatarul conținuturilor lor.

ENTITATE

A se vedea persoană.

F FSC

A se vedea Furnizorul de Servicii de Certificare.

FUNCTIA UN SINGUR SENS

A se vedea funcția hash.

PRESTATORUL DE SERVICII DE ÎNCREDERE CALIFICAT

Un Prestator de Servicii de Încredere care prestează unul sau mai multe servicii de încredere calificate și căruia i se acordă statutul de calificat de către organismul de supraveghere.

G

GTC

A se vedea Termenii și Condițiile Generale.

H

FUNCTIA HASH

O funcție hash generează un extras scurt de lungime fixă (MD5: 128 bits = 16 caractere, SHA-2: 256 bits = 64 caractere), valoarea hash, din orice date acordate într-un asemenea mod încât datele originale să nu poată deriva din extras, și că este nefezabil să se construiască alte date care produc aceeași valoare hash. De exemplu, valoarea hash derivată prin aplicarea funcției hash la conținutul (mesajul text) unui e-mail este apoi folosită alături de cheia privată pentru a semna digital e-mail-ul.

I-J

ID UTILIZATORULUI

O structură de date PGP conținând identitatea deținătorului cheii. Formatul comun utilizat este "Numele complet <adresa e-mail >", de ex: "John Doe <jdoe@company.com>".

IDEA

IDEA (Algoritmul de criptare a datelor cu caracter internațional) este un bloc cifru de 64 bit care utilizează o cheie de 128 bit. IDEA este considerat a fi unul dintre algoritmi de criptare cei mai siguri. Este utilizat (printre altele) de către PGP. Utilizatorii comerciali ai PGP care folosesc IDEA ca cifru simetric trebuie să plătească o taxă de licență către compania elvețiană ASCOM; utilizarea non-comercială este gratuită.

Identificarea persoanei la distanță prin mijloace video

procesul de identificare și verificare a identității persoanei fizice, în baza documentelor prezentate, a imaginilor capturate și/sau a informațiilor comunicate de persoana fizică, utilizând mijloace video

IETF

The Internet Engineering Task Force (IETF) este o comunitate internațională deschisă de proiectanți de rețea, operatori, vânzători și cercetători preocupați de evoluția arhitecturii Internetului și de operarea fără probleme a internetului. Este deschisă oricărei persoane interesate.

INELUL CHEII

Un inel al cheii este fișierul PGP care păstrează cheile publice (sau private) în el.

K-L LAN

Rețeaua Locală.

LDAP

Un protocol pentru accesarea serviciilor directorului on-line. LDAP a fost definit de către IETF pentru a încuraja adoptarea de directoare X.500. Un Protocol de Acces la Director (DAP) a fost perceput drept prea complex pentru ca clienții de pe internet să-l poată folosi. O intrare în director LDAP este o colecție de atribute cu un nume, denumit nume distinct (ND). ND se referă la intrarea fără ambiguități. Fiecare din atributele intrării are un tip și una sau mai multe valori. Tipurile sunt arcuri mnemonice tipice, precum "CN" pentru nume comun, sau "mail" pentru adresa de e-mail. Valorile depind de tip. De exemplu, un atribut mail poate conține valoarea "john.doe@company.com". Intrările în directorul LDAP sunt aranjate într-o structură ierarhică care reflectă limitările politice, geografice și / sau organizaționale.

LISTA CERTIFICATELOR REVOCATE

O listă care conține certificate revocate pe care AC le-a emis. În cazul în care o AC emite certificate în cadrul diferitelor politici de certificate, cu o cheie diferită de semnare

utilizată pentru fiecare politică, multiple CRL-uri vor fi generate. Cu toate acestea, lista certificatelor revocate va fi identică pentru toate CRL-urile.

M

MD5

MD5 este o funcție hash 128 bit dezvoltată de către Ron Rivest. Este folosită la scară largă, iar PGP o folosește în legătură cu algoritmul RSA.

Mijloace video

Mijloace de identificare la distanță ce utilizează tehnologii care presupun fie transmiterea audiovideo de succesiuni de imagini în mișcare, în timp real, în cadrul unei videoconferințe cu prezența unui operator uman, fie transmiterea de succesiuni de imagini în mișcare reprezentând capturi video cu persoana fizică, fără prezența unui operator uman, cu verificarea ulterioară a acestora de către furnizorul de servicii de identificare (cu sau fără implicarea unui operator uman)

Mijloace digitale

Mijloace care utilizează tehnologii digitale inovatoare care folosesc, printre altele, inteligența artificială și/sau procese de învățare automată (machine learning), cum ar fi aplicațiile care realizează identificarea unei persoane și/sau verificări ale actelor de identitate (prin capturi de imagini digitale, măsurători ale semnelor biometrice faciale, comparare de imagini), tehnologia NFC (comunicare în câmp apropiat) încorporată în documentele electronice de identitate;

N

NIST

The NIST (Institutul Național pentru Standarde și Tehnologie) este o filială a departamentului comercial din Statele Unite care propune standarde de interoperabilitate deschise.

NSA

The NSA (Agenția de Securitate Națională) este o organizație criptologică a guvernului Statelor Unite care se ocupă cu dezvoltarea și criptanaliza algoritmilor de încriptare.

NUME DISTINCT

Strict vorbind, un Nume Distinct (ND) este o cale printr-un copac registru de informații X.500 care identifică în mod unic o entitate. Un copac registru X.500 este o structură ierarhică, dar pentru că informațiile precum o adresă de e-mail nu urmează o astfel de ierarhie, n-ar trebui să fie o parte dintr-un ND. Majoritatea DN, în orice caz, conțin o adresă e-mail, iar un ND este în mod comun înțeles a cuprinde colectarea câmpurilor de date care alcătuiesc standardul X.509, adică, Țara (T), Statul / Provincia (SP), Localitatea (L), Organizația (O), Organizational Unit (OU), Common Name (CN) and Email. Un DN arată în felul următor: /C=US/SP=Washington/L=Seattle/O=My Company, Inc. /OU=Internet Services/CN=John Doe/Email=jdoe@mycompany.com.

O-P

PAROLA FRAZĂ

O frază de trecere, la fel ca și un cuvânt de trecere, este utilizată pentru a nu permite accesul neautorizat la datele confidențiale. O frază de trecere constă din câteva cuvinte, semne de punctuație și numere pentru a furniza o securitate mai bună decât un simplu cuvânt de trecere. O frază de trecere este utilizată, de exemplu, pentru a proteja cheia privată.

PARTE DE ÎNCREDERE

Primitorul unui certificat care acționează bazându-se pe acel certificat și / sau semnături digitale/sigilii electronice verificate folosind acel certificat.

PERECHEA DE CHEI

Setul de chei utilizat pentru algoritmi asimetrici. A se vedea de asemenea cheie.

PERSOANĂ

O ființă sau orice organizație capabilă de semnarea unui document, fie legal sau ca un aspect de fapt.

PGP

PGP (Pretty Good Privacy), dezvoltat de către Phillip Zimmermann, este o aplicație foarte răspândită utilizată și populară pentru schimbul de e-mail și fișiere de încryptare sigur. Folosirea non-comercială este gratuită, utilizatorii comerciali vor trebui să obțină o licență de la PGP Inc.,.

PIN

Număr de Identificare Personală.

POLITICA DE CERTIFICARE

Un set numit de reguli care indică aplicabilitatea unui certificat la o comunitate particulară și / sau clasă de aplicații cu cerințe de securitate comune. În timp ce un CPP este pregătit de o Autoritate de Certificare, orice organizație poate defini o Politică de Certificare.

Q-R

RA

A se vedea Autoritatea de Înregistrare.

REVOCAREA

Revocarea este procesul prin care se declară o cheie publică a cuiva ca nu mai fiind valabilă. Acest lucru se face în mod normal pentru că deținătorul său nu mai poate garanta că el are unicul acces, și că cheia sa privată nu a fost compromisă. Prin revocarea cheii publice a certificatului se țintește împiedicarea unor terte persoane de a aduce prejudicii prin pretinderea că sunt deținătorul cheii. Revocarea cheii publice a certificatului informează publicul că cheia publică nu va mai trebui utilizată pentru a cripta orice mesaje sau fișiere, și că semnăturile digitale realizate folosind această cheie nu vor mai trebui acceptate. Cheia publică revocată a numărului serial al certificatului este inclusă apoi pe o CRL (Listă a Certificatelor Revocate) de către o Autoritate de Certificare astfel că oricine poate verifica dacă o cheie publică a certificatului este încă validă.

RSA

RSA este numele algoritmului asimetric dezvoltat de către o companie cu baza în Statele Unite cu același nume, RSA Data Security Inc. Securitatea acesteia se bazează pe faptul că este ușor să se multiplice două prime mari (cu câteva sute de zecimale fiecare) dar foarte greu de a le scoate din produs. Abrevierea RSA se referă la trei inventatori ai algoritmului: Ron Rivest, Adi Shamir și Leonard Adleman.

S

SEMNATAR

O persoană care este subiectul numit într-un certificat și care deține cheia privată corespondentă cheii publice prezentate în certificat.

SEMĂNĂTURĂ DIGITALĂ (folosind algoritmul RSA)

O semnătură digitală este un bloc mic de date (valoare hash) care este încriptat folosind cheia privată a trimițătorului și anexată datelor semnate pentru a furniza autenticitate și integritate. Semnătura digitală este verificată folosind cheia publică a trimițătorului.

SERVER-UL CHEII PUBLICE

Un server de cheie publică este un registru de chei publice, ca o carte de telefon publică, care cuprinde numele utilizatorului și cheile lor publice pentru un acces facil.

SET DE PREVEDERI

O colecție de declarații de practici și / sau politici, care prezintă o serie de subiecte standard, pentru utilizarea în exprimarea unei definiții de politică de certificare sau CPP.

SHA-2

SHA-2 este o funcție hash dezvoltată de NIST care este utilizată în DSS.

SHA-256

SHA-256 este o funcție hash pe 32 bit.

SIGILIU ELECTRONIC

Date în format electronic, care sunt atașate sau asociate logic cu alte date în format electronic pentru a asigura originea și integritatea celor din urmă.

Sistem informatic pentru identificarea persoanei la distanță prin mijloace video

Reprezintă ansamblul de elemente implicate în procesul de identificare a persoanei la distanță prin mijloace video, prin care se transmit datele, imaginile capturate/încărcate și/sau informațiile comunicate de persoana fizică, denumit în continuare *sistem*;

S/MIME

S/MIME (Secure Multipurpose Internet Mail Extension) este un standard sugerat de către un grup de dezvoltatori de software condus de RSADSI care furnizează criptare și semnături digitale pentru schimbul sigur de e-mail. Certificatele S/MIME se bazează pe formatul X.509.

SSL

SSL (Secure Socket Layer) este un protocol dezvoltat de către Netscape care dorește să furnizeze un schimb de date securizat prin Internet. SSL este sprijinit și folosit de către toate browser-ele moderne de Internet pentru a se proteja comunicarea și transferul de date delicate prin web în toată lumea prin încriptare. Din păcate, versiunile de export ale acestor aplicații care se găsesc în afara Statelor Unite sunt limitate la o criptare fragilă de 40 bit (în loc de 128 bit) din cauza restricțiilor de export. Certificatele SSL se bazează pe formatul X.509.

SUSPENDARE

Suspendarea este un proces de punere a unui certificat în așteptare, adică declarându-l temporar invalid. Acest lucru este în mod normal efectuat pentru că semnatarul suspectează că cheia sa privată a fost pierdută sau compromisă. Prin suspendarea cheii publice a certificatului se țintește împiedicarea tertelor parti de a aduce prejudicii prin pretinderea de a fi deținătorul cheii. Suspendarea cheii publice a certificatului anunță publicul că, pentru moment, cheia publică nu poate fi folosită pentru a cripta mesaje sau fișiere, și că semnăturile digitale efectuate folosind cheia privată corespunzătoare nu trebuie acceptate pentru moment. Un certificat bazat pe chei publice suspendat trebuie să fie revocat la confirmarea că cheia privată a fost într-adevăr pierdută sau compromisă, atunci când este

inclusă pe CRL (Lista certificatelor revocate) de către Autoritatea de Certificare care emite, sau susendarea poate fi ridicată, dacă, de exemplu, cheia privată a fost recuperată (adică nu este pierdută).

T

TERMENI SI CONDITII GENERALE

Serviciile și ofertele Autorității de Certificare sunt furnizate pe baza Termenilor și Condițiilor Generale. Acestea pot fi găsite în depozitar.

TIME-STAMP

O indicare a (cel puțin) data și momentul în care documentul a fost semnat și de către cine.

TRIPLE-DES

O variantă a algoritmului DES unde DES (dimensiunea cheii 56 bits) este utilizată de trei ori cu trei chei diferite. Dimensiunea cheii efective este de doar 112 bits (și nu 168 bits, după cum s-a putea imagina).

U

Utilizator

O persoană care este subiectul numit într-un certificat și care deține cheia privată corespondentă cheii publice prezentate în certificat.

V W-Z

WAN

Rețea pe arie largă.

X.509

X.509 este un format standard de certificat al ITU-T (International Telecommunication Union-Telecommunication). Acesta conține numele emitentului, de obicei o Autoritate de Certificare, informații referitoare la identitatea deținătorului cheii și semnătura digitală a emitentului. Atât SSL cât și S/MIME folosesc formatul de certificat X.509.

2. Publicare și Responsabilități Depozitar

2.1. Depozitar

Trans Sped va publica prezentul CPP/PC la <https://www.transsped.ro/repository> și <https://www.transsped.ro/certificari>. Certificatele autorităților Trans Sped sunt de asemenea accesibile în depozitar.

2.2. Publicarea informațiilor din certificat

Registrul tuturor certificatelor digitale calificate accesibile și care pot fi descărcate, emise de către Trans Sped, poate fi găsit la https://www.transsped.ro/applications/search_qc/search_qc.aspx

Certificatele digitale calificate sunt accesibile pentru a fi descărcate doar dacă deținătorul certificatului este de acord cu publicarea certificatului.

Listele Certificatelor Revocate (CRL) pentru certificatele digitale calificate pot fi găsite la <https://www.transsped.ro/repository/>

2.3. Frecvența publicării

Prezentul CPP/PC și orice modificări ulterioare sunt puse la dispoziția publicului după aprobarea de către Comitetul de Politici și Practici al Trans Sped.

CRL-urile sunt actualizate la fiecare douăzeci și patru (24) de ore. Baza de date care furnizează informațiile stării certificatelor digitale calificate este actualizată de fiecare dată când un certificat este eliberat sau revocat. Orice alte informații prevăzute în art. 2.1 sunt actualizate de fiecare dată când sunt modificate.

2.4. Controlul accesului la Depozitare

Doar personalul autorizat poate publica sau modifica orice informații la care se face referire în art. 2.1.

3. Identificarea și autentificarea

3.1. Numele

Trans Sped emite certificate X.509 versiunea 3 în conformitate cu RFC 5280, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

3.1.1. Tipuri de nume

Câmpurile subiectului și emitentului din certificat trebuie să fie populate cu un Nume Distinctiv unic (ND), în conformitate cu standardul X.500, cu tipul atributului cum este limitat în continuare

de RFC 5280. Atunci când există mai multe valori pentru un atribut dintr-un ND, ND trebuie să fie codificat astfel încât fiecare valoare a atributului să fie codificată într-un nume distinctiv separat.

3.1.2. Necesitatea pentru ca numele să aibă înțeles

Trans Sped va determina ND al semnatarului să fie conform cu standardele, practicile și alte reglementări. Numele trebuie să aibă semantică comun înțeleasă (prenume și nume, numele societății, adresa de e-mail) pentru ca partea de încredere să determine identitatea persoanei și / sau organizației. În orice caz, solicitantul își poate alege un pseudonim în locul numelui în certificatul digital calificat. Trans Sped va emite asemenea certificate pseudonizate; folosirea pseudonimului este indicată prin sufixul “:PN” în spațiul Nume Comun al certificatului

Acest capitol descrie obligațiile și răspunderea AC Trans Sped, a AI, semnatarilor și ale părților de încredere. Obligațiile și răspunderea sunt guvernate de Regulamentul eIDAS și de acordurile mutuale efectuate de către părțile mai sus menționate.

3.1.3. Reguli pentru interpretarea unor diferite forme de nume

Orice certificat X.509 emis pentru uzul privat va avea câmpurile Organizația și Unitatea Organizațională goale. Dacă unul (sau ambele) din aceste câmpuri sunt prezente, certificatul este fie menit pentru scopuri comerciale sau sponsorizat de către organizație.

3.1.4. Unicitatea numelor

Orice ND dintr-un certificat digital calificat emis de Trans Sped trebuie să identifice în mod unic o singură entitate dintre toți utilizatorii Trans Sped de certificate digitale calificate. Dacă e cazul, Trans Sped poate atașa numere sau litere adiționale la numele real pentru a asigura unicitatea numelui. Aceeași entitate poate avea certificate diferite toate purtând același ND subiect dar două entități separate nu pot împărți un ND comun (și să fie emis de aceeași AC). În orice caz, nu trebuie să existe două certificate X.509 care au același emitent ND și număr serial.

Trans Sped nu este responsabil pentru soluționarea disputelor legate de nume dintre utilizatori. Trans Sped poate adăuga, la propria discreție, informații adiționale la un nume pentru a face unic numele certificatelor emise de Trans Sped.

3.1.5. Procedura de soluționare a disputelor legate de nume

Trans Sped nu este responsabil pentru soluționarea disputelor legate de nume dintre utilizatori. Trans Sped poate adăuga, la propria discreție, informații adiționale la un nume pentru a face unic numele certificatelor emise de Trans Sped.

3.1.6. Recunoașterea, autentificarea și rolul mărcilor comerciale

Trans Sped va onora reclamațiile legate de mărcile comerciale care sunt prezentate documentat de către un utilizator.

3.2. Validarea inițială a identității

În vederea obținerii unui certificat digital calificat, orice utilizator trebuie să solicite, să se identifice și autentifice la Trans Sped.

Trans Sped se asigură că utilizatorii sunt identificați și autentificați în mod corespunzător și că solicitările de certificat sunt complete, corecte și legal autorizate. Înainte ca un certificat digital calificat să fie emis, Trans Sped informează semnatarul referitor la termenii și condițiile privind folosirea certificatului după cum sunt reglementate în Regulamentul eIDAS și a legislației privind semnăturile electronice din România. Detaliile identificării sunt reglementate de Regulamentul eIDAS și de legislația privind semnăturile electronice din România. Documentele depuse pot fi pe suport de hârtie sau în format electronic.

Trans Sped verifică, la momentul înregistrării prin mijloace corespunzătoare și în conformitate cu eIDAS și a Standardelor ETSI EN 319 401, identitatea și, dacă e cazul, orice atribute specifice ale persoanei căreia îi este emis un certificat digital calificat. Trans Sped înregistrează toate informațiile necesare pentru a verifica identitatea utilizatorului și, dacă este cazul, orice atribute specifice ale acestuia, inclusiv orice număr de referință cu privire la documentația utilizată pentru verificare, precum și orice limitări privind valabilitatea acestuia, dar și acordul semnat cu informațiile solicitate. Trans Sped colectează o adresă fizică sau alte atribute care descriu modul în care utilizatorul poate fi contactat.

3.2.1. Metoda de a dovedi deținerea cheii criptografice private

Înainte de emiterea unui certificat digital calificat, AC trebuie să asigure și să se asigure că utilizatorul deține și are sub controlul său cheia criptografică privată aparținând cheii criptografice publice a certificatului.

Dacă utilizatorul (clientul), numit într-un certificat digital calificat, generează propriile sale chei criptografice, acesta trebuie să utilizeze cheia criptografică privată pentru a semna o valoare și pentru a furniza respectiva valoare AC-ului care emite certificatul. AC trebuie apoi să valideze semnătura/sigiliul utilizând cheia criptografică publică a subiectului.

Dacă Trans Sped generează în incinta sa cheia criptografică privată aparținând certificatului digital calificat al utilizatorului - de regulă pe dispozitivul de creare a semnăturii electronice calificate sau pe modulul hardware de securitate, atunci nu este necesară dovada posesiei.

3.2.2. Autentificarea identității organizației

Dacă solicitantul este o persoană care este identificată în legătură cu o persoană juridică sau altă entitate organizațională, pe lângă datele din art. 3.2.3 va fi dovedita existența persoanei juridice sau entității organizaționale. Această verificare poate fi efectuată prin prezentarea unei

copii a unui document, care dovedește existența organizației (extrasul actual al unui registru oficial competent în care organizația este listată sau un document comparabil).

Autoritățile guvernamentale sau administrative trebuie să furnizeze documentele care reflectă relația lor cu următoarea entitate superioară ierarhică (de ex: autoritate superioară) cu antet oficial, semnată de către un funcționar autorizat.

Documentația trebuie să cuprindă:

- Numele complet și statutul legal al persoanei juridice asociate sau altă entitate organizațională,
- Informații de înregistrare existente relevante (de ex: înregistrarea societății) a persoanei juridice asociate sau altă entitate organizațională.

3.2.3. Autentificarea identității individuale

Autentificarea unei persoane fizice (solicitant) este realizată în conformitate cu prevederile Regulamentului eIDAS, standardul ETSI EN 319 401, ETSI EN 319 411-1 și ETSI EN 319 411-2. Dovada identității solicitantului este verificată printr-un document oficial (carte de identitate sau pasaport) cu fotografia personală a acestuia. Trans Sped poate folosi, cu acordul utilizatorului, datele cu caracter personal colectate anterior. Documentul oficial trebuie să cuprindă:

- Numele complet (inclusiv numele de familie și prenumele),
- Data și locul nașterii,
- Un număr de serie sau alte atribute care pot fi folosite pentru a distinge persoana din alte persoane cu același nume
- Un număr de telefon mobil

De asemenea, este permisă verificarea identității utilizatorului în mod indirect folosind mijloace care oferă o asigurare echivalentă a prezenței fizice (de exemplu dacă utilizatorul deja deține un certificat digital calificat, care implică faptul că acesta a fost identificat cu prezența personală).

Dacă utilizatorul este o persoană care este identificată în legătură cu o persoană juridică sau altă entitate organizațională în completarea datelor din art. 3.2.2 dovezile următoare vor fi furnizate:

- Dovada că utilizatorul este asociat cu persoana juridică sau entitatea organizațională,
- Acordul de la persoana juridică sau entitatea organizațională.

3.2.4. Informațiile neverificate ale abonatului

Informațiile care nu sunt verificate nu vor fi incluse în Certificate.

3.3. Identificarea și autentificarea pentru cererile de re-key

Acordarea unei chei criptografice noi presupune schimbarea cheii criptografice publice pentru un certificat existent prin emiterea unui nou certificat cu o cheie criptografică publică diferită. Numele certificatului rămâne același. Acest proces este diferit de cel de reînnoire care

presupune emiterea unui nou certificat, cu o perioadă de valabilitate prelungită, pentru aceeași cheie criptografică publică. (A se vedea [RFC4949].)

În momentul în care cheile criptografice trebuie schimbate, utilizatorii sunt notificați prin e-mail. Schimbarea cheii criptografice în cazul certificatelor care nu au expirat încă, poate fi solicitată folosind procedura on-line care verifică validitatea certificatului utilizatorului. Noul certificat este emis după ce solicitarea este aprobată de către Trans Sped. Reinnoirea certificatului SSCD necesită demonstrarea posesiei cheii criptografice private curente prin trimiterea unui e-mail S/MIME semnat sau prin efectuarea unei conexiuni TLS autentificată de client. Reinnoirea certificatului bazat pe server necesită autentificare pentru dispozitivul de creare a semnăturii (consultați definiția [CEN / TS 419241]) utilizând aceleași credențiale folosite pentru a activa utilizarea cheii criptografice private.

Obținerea unei noi chei criptografice în cazul în care certificatul a expirat se face folosind aceleași reguli ca și la înregistrarea inițială.

Dacă noul certificat va conține date despre o organizație, trebuie prezentate din nou documentele specificate în art. 3.1, înainte de a avea loc schimbarea cheii criptografice.

3.4. Identificarea și autentificarea pentru cererile de revocare

După ce un certificat a fost revocat, utilizatorul trebuie să solicite un nou certificat conform prevederilor art. 3.3. având în vedere ca perechea de cheie criptografice revocată nu este eligibilă pentru a semna și autentifica o cerere de acordare a unei noi chei criptografice (a se vedea art. 3.3).

Reînnoirea online a certificatului digital calificat presupune generarea unei perechi noi de chei criptografice direct către titularul vechiului certificat digital calificat.

Condițiile care trebuie să fie îndeplinite pentru reînnoirea online:

- Certificatul curent nu este revocat și se află în perioada de valabilitate;
- Datele înscrise în certificat nu s-au schimbat (Nume, Prenume, Funcție, Departament, Organizație, email și număr de telefon).

Cererile pentru suspendarea sau revocarea unui certificat digital calificat emis de către Trans Sped sunt autentificate de către posesorul certificatului în conformitate cu una din următoarele metode:

- Prezența personală a posesorului certificatului digital calificat la AI;
- Semnarea olografa a formularului de suspendare / revocare;
- Prin dovedirea posesiei cheii criptografice private;

4. CERINȚE OPERAȚIONALE PRIVIND CICLUL DE VIAȚĂ AL CERTIFICATULUI

4.1. Aria de aplicabilitate a certificatelor

Pentru obținerea unui certificat digital calificat un utilizator solicită către Trans Sped emiterea certificatului și urmează procedura descrisă în prezentul CPP/PC sau în descrierile Trans Sped pentru solicitarea unui certificat digital calificat.

4.2. Procesarea cererilor de certificate

Trans Sped poate aproba sau respinge aceste solicitari. Perechea de chei criptografice poate fi generată într-un mediu securizat de către AC, AI sau semnatar. Cheile criptografice pentru semnăturile electronice/sigiliile electronice calificate sunt întotdeauna create în dispozitivele securizate de creare a semnăturii care sunt aprobate a fi utilizate în astfel de scopuri. Cheile criptografice private nu vor fi exportabile din aceste dispozitive.

Utilizatorul (Abonatul) va semna cu Trans Sped următoarele:

- Declarația că informațiile furnizate sunt corecte;
- Acordul la obligațiile utilizatorului;
- Acordul la publicarea certificatului în depozitar.
- Acordul GDPR
- Termeni si Conditii Trans Sped

4.3. Emiterea unui certificat digital calificat

Trans Sped verifică corectitudinea și valabilitatea tuturor datelor necesare pentru emiterea unui certificat digital calificat conform prevederilor Regulamentului eIDAS. La finalul procesului Trans Sped fie va emite utilizatorului certificatul digital calificat, fie îl va informa referitor la orice probleme sau inadvertențe.

Trans Sped generează certificate digitale calificate folosind formatul de certificat corespunzător și stabilește perioadele de valabilitate și domeniile de extindere în conformitate cu standardele relevante și reglementările legale.

Perioada de valabilitate a unui certificat calificate este de maxim trei ani de la data emiterii acestuia.

4.4. Acceptarea certificatului digital calificat

La primirea unui certificat digital calificat, utilizatorul trebuie să verifice datele înregistrate în certificat. Dacă certificatul conține greșeli care nu pot fi acceptate de către utilizator, acesta trebuie să informeze Trans Sped fără întârziere. Trans Sped va revoca certificatul și va lua măsurile care se impun fie de a restitui prețul certificatului fie de a emite un certificat nou cu informațiile corecte.

Dacă un certificat nu este respins în termen de 7 zile de la primirea acestuia, certificatul este considerat acceptat.

4.5. Utilizarea perechii de chei și a Certificatului

Trans Sped protejează cheia privată de accesul neautorizat. Certificatele digitale calificate sunt publicate în depozitarul Trans Sped pentru a fi puse la dispoziția terțelor părți, doar cu acordul utilizatorului.

Beneficiarul este responsabil personal pentru:

- utilizarea cheilor numai pentru uzul prevăzut, așa cum este definit în acest CPP și codat în certificate;
- cheile private care corespund certificatelor calificate emise în baza acestui CPP și vor fi utilizate pentru a crea semnături electronice sau sigilii electronice
- să păstreze confidențialitatea acestor informații.

4.6. Reînnoirea unui certificat digital calificat

4.6.1. Reînnoirea on-line a certificatelor digitale calificate cu cheile criptografice stocate în cloud

1. Solicitarea reînnoirii certificatului digital calificat în cloud este efectuată de către posesor din portalul de administrare al certificatului:
<https://msign.transsped.ro/serverbku/protected/index.jsf>
2. Trans Sped primește solicitarea și o aprobă după verificarea tuturor informațiilor din solicitare.

Pentru reînnoirea online a certificatului digital calificat trebuie să fie respectate următoarele condiții:

- Posesorul deține un certificat digital calificat activ;
- Autentificarea în portalul Trans Sped de administrare al certificatului este realizată folosind credențialele certificatului activ;
- Informațiile care au fost utilizate pentru emiterea certificatului inițial: nume, prenume, număr de telefon mobil, adresă de email, funcție, organizație (funcția și organizația sunt obligatorii doar pentru certificatele emise în numele unei organizații) sunt neschimbate;
- Certificatul reînnoit va conține aceleași informații ca și certificatul anterior. Orice solicitare de modificare a datelor din certificatul care urmează să expire invalidează procedura de reînnoire online.

4.6.2. Reînnoirea on-line a certificatelor digitale calificate cu cheile criptografice stocate pe dispozitiv criptografic (token)

Reînnoirea on-line a certificatelor digitale calificate cu cheile criptografice stocate pe token se poate realiza doar dacă informațiile din certificatul inițial: nume, prenume, număr de telefon, adresa de email, funcția și organizația (funcția și organizația sunt obligatorii doar pentru certificatele emise în numele unei organizații) sunt neschimbate. Certificatul reînnoit va conține

aceleași informații ca și certificatul anterior. Orice solicitare de modificare a datelor din certificatul care urmează să expire invalidează procedura de reînnoire online.

Condiții pentru reînnoirea online a certificatelor digitale calificate cu cheile criptografice stocate pe token :

- Posesorul trebuie să dețină un certificat digital calificat activ emis de catre Trans Sped;
- Datele din certificatul digital reînnoit trebuie să fie valabile și să nu necesite modificări;
- Datele de identificare ale titularului certificatului reînnoit sunt identice cu cele ale certificatului care urmează să expire și pentru care se realizează reînnoirea;
- Codul PIN asociat dispozitivului criptografic trebuie să fie cunoscut de catre titular, iar dispozitivul criptografic trebuie să nu fie blocat;
- PC/laptop utilizat în procesul de reînnoire trebuie să aibă acces la internet;
- Clientul trebuie detina driverele dispozitivului pe care este instalat dispozitivul;
- Clientul trebuie să aibă cea mai recentă versiune a aplicației EasySign.

Dacă una sau mai multe dintre condițiile enumerate mai sus nu sunt îndeplinite, este necesar ca reînnoirea să se realizeze utilizând procedura standard, care este similar procesului descris în art. 3.2.3. și 4.2.

Un certificat digital calificat poate fi suspendat sau revocat. Suspendarea certificatului digital calificat se realizeaza in situatia in care posesorul certificatului are suspiciuni privind pierderea sau compromiterea cheii criptografice private, până la clarificarea situației. Dacă posesorul certificatului digital calificat are certitudini privind pierderea sau compromiterea cheii criptografice private, sau dacă datele înregistrate în certificat s-au schimbat în mod substanțial, certificatul trebuie să fie revocat.

Dacă un certificat este revocat, el devine invalid de îndată ce Trans Sped a operat cererea de revocare. Numărul de serie al certificatului și data revocării vor fi incluse în Lista Certificatelor Revocate, iar investigații legate de starea ulterioara la depozitarul certificatelor vor conduce la citarea certificatului drept invalid.

Dacă un certificat este suspendat, acesta va fi inclus în Lista Certificatelor Revocate, iar orice investigații legate de stare la depozitarul de certificate în timp ce suspendarea este activa vor conduce la citarea certificatului drept invalid.

Trans Sped furnizează informații legate de starea de revocare prin distribuirea de Liste ale Certificatelor Revocate (CRLs) prin depozitar sau folosind serviciul on-line al stării certificatului (OCSP).

4.7. Revocarea și suspendarea Certificatului

4.7.1. Circumstanțe pentru revocarea certificatului digital calificat

Un certificat digital calificat este revocat în următoarele situații:

1. Posesorul sau o terță parte autorizată a depus o cerere de revocare;

2. Trans Sped a aflat că au fost furnizate informații false în solicitarea de certificat, fapt pentru care invalidează certificatul;
3. Organismul de supraveghere solicită Trans Sped să revoce un certificat în conformitate cu prevederile eIDAS;
4. Trans Sped încetează operarea și niciun alt furnizor de servicii de certificare nu mai poate continua serviciile de certificare ale Trans Sped;

Ori de câte ori apare una din situațiile de mai sus, certificatul asociat trebuie revocat și plasat într-un CRL. Certificatele revocate trebuie să fie incluse în toate publicațiile noi ale informațiilor privind statutul certificatului până la expirarea acestuia. Certificatele revocate trebuie să apară pe cel puțin un CRL.

4.7.2. Cine poate solicita revocarea unui certificat digital calificat

Posesorul certificatului sau înlocuitorul său pot solicita revocarea.

Dacă un certificat digital prevede că deținătorul lui poate acționa în numele unei terțe părți, această parte poate de asemenea solicita revocarea certificatului. Orice entitate sau terță parte care au confirmat orice informații cuprinse în certificat are dreptul să revoce certificatul respectiv.

Oricine poate informa Trans Sped referitor la faptul că informațiile dintr-un certificat nu sunt, sau nu mai sunt corecte. După primirea informațiilor Trans Sped va verifica dacă o revocare este corespunzătoare conform art. 4.7.1, 2.

4.7.3. Procedura pentru cererea de revocare a certificatelor digitale

Revocarea certificatului digital calificat se poate realiza în următoarele modalități:

1. Posesorul sau o terță parte autorizată solicită revocarea unui certificat digital calificat prin completarea și semnarea unui formular de revocare în fața Ofițerului de Înregistrare. Autentificarea este furnizată de semnătura olografa.
2. Posesorul sau o terță parte autorizată solicită revocarea unui certificat digital calificat prin trimiterea unei cereri de revocare în format electronic către Trans Sped. Autentificarea este furnizată printr-o semnătură electronică calificată.
3. Posesorul revocă certificatul digital calificat din portalul de administrare al certificatului <https://msign.transsped.ro/serverbku/protected/index.jsf>

Trans Sped confirmă o cerere pentru revocare prin e-mail sau trimite o confirmare scrisă, în termen de timp rezonabil, nu mai târziu de douăzeci și patru (24) de ore după primirea cererii.

4.7.4. Perioada de revocare a certificatului digital calificat

Trans Sped operează cererea de revocare după confirmarea faptului că provine de la o entitate autorizată, cât mai prompt și eficient. Perioada maximă pentru revocarea unui certificat digital calificat este douăzeci și patru (24) de ore.

4.7.5. Circumstanțele suspendării certificatului digital calificat

Un certificat digital calificat este suspendat în următoarele situații:

1. Posesorul sau o terță parte autorizată au depus o cerere de suspendare;
2. Trans Sped suspectează că în solicitarea pentru certificat au fost furnizate informații false pentru care ar putea invalida certificatul;
3. Posesorul nu a efectuat plata pentru certificatul digital conform prevederilor contractuale.

4.7.6. Cine poate solicita suspendarea certificatului digital calificat

Posesorul sau reprezentantul său pot solicita suspendarea certificatului digital calificat.

Dacă un certificat prevede că posesorul lui poate acționa în numele unei terțe părți, această terță parte poate solicita suspendarea certificatului. Orice entitate sau terță parte care au confirmat orice informații cuprinse în certificat are dreptul să solicite suspendarea certificatului respectiv.

Oricine poate informa Trans Sped referitor la faptul că informațiile dintr-un certificat s-ar putea să nu fie corecte. Trans Sped va verifica dacă este necesar o suspendare conform art. 4.7.5, 6.

4.7.7. Procedura pentru suspendarea certificatului digital calificat

Solicitarea pentru suspendarea unui certificat digital calificat se poate realiza în următoarele modalități:

1. Posesorul sau o terță parte autorizată poate solicita suspendarea unui certificat digital calificat prin completarea și semnarea unui formular de suspendare în fața Ofițerului de Înregistrare. Autentificarea este furnizată de semnătura olografa.
2. Posesorul sau o terță parte autorizată poate solicita suspendarea unui certificat digital calificat prin transmiterea unei cereri de suspendare în format electronic către Trans Sped. Autentificarea este furnizată printr-o semnătură electronică calificată.
3. Posesorul certificatului digital calificat poate realiza suspendarea în portalul de administrare al certificatului:

<https://msign.transsped.ro/serverbku/protected/icarus/welcome.jsf>

Trans Sped confirmă o cerere pentru suspendare prin e-mail sau trimite o confirmare scrisă, într-un termen rezonabil de timp, nu mai târziu de douăzeci și patru (24) de ore după primirea solicitării.

4.7.8. Limitele perioadei de suspendare a certificatului digital calificat

Un certificat digital calificat poate fi suspendat pentru maxim șapte (7) zile. Posesorul unui certificat digital poate solicita suspendarea acestuia maxim de 2 ori în perioada de valabilitate a certificatului. Depășirea numărului de suspendări sau a perioadei atrag după sine revocarea certificatului.

4.7.9. Frecvența emiterii de CRL

Frecvența emiterii de CRL va fi cel puțin la fiecare douăzeci și patru (24) de ore. AC Trans Sped semnează CRL-uri la fiecare 18 ore, cu următoarea actualizare la 24 de ore. AC-urile offline (de exemplu, AC root) prezintă CRL-uri care au o actualizare ulterioară de 60 de zile sau mai puțin.

4.7.10. Cerințele de verificare ale CRL

Părțile de încredere, atunci când lucrează cu certificate digitale calificate emise de către Trans Sped, trebuie să poată verifica aceste certificate în orice moment. Aceasta include folosirea de CRL, conform cu procedura de validare a căii de certificare specificată în RFC 5280.

4.7.11. Verificarea disponibilității stării/revocării on-line

Statutul certificatului digital calificat poate fi verificat on-line la sistemul de informare a stării certificatului. Orice modificări efectuate în sistemul de informare referitor la stare sunt imediat disponibile oricărui semnatar și / sau parte de încredere.

4.7.12. Cerințele de verificare a revocării on-line

Este responsabilitatea părții de încredere de a verifica starea de revocare on-line.

4.7.13. Alte forme de înștiințare de revocare disponibile

Nu există prevederi.

4.7.14. Cerințele de verificare pentru alte forme de înștiințare de revocare

Nu există prevederi.

4.7.15. Cerințe speciale privind compromiterea cheii criptografice private

În cazul în care posesorul suspectează sau are certitudini că cheia sa criptografică privată a fost compromisă, acesta este obligat să solicite revocarea certificatului cât mai curând posibil. Posesorul certificatului este responsabil de obligațiile sale de semnatar până când este notificat de către Trans Sped în legătură cu revocarea certificatului.

4.8. Servicii privind starea certificatelor

4.8.1. Caracteristici operaționale

Serviciile Trans Sped de verificare a stării certificatelor sunt CRL și OCSP. Serviciile de verificare a stării certificatelor oferă informații despre starea certificatelor valide.

4.8.2. Disponibilitatea serviciului

Serviciile de stare a certificatului sunt disponibile 24 de ore pe zi, 7 zile pe săptămână.

5. CONTROALELE DE SECURITATE FIZICE, DE PROCEDURĂ ȘI DE PERSONAL

Trans Sped are obligativitatea de a stabili și menține starea controalelor de securitate solicitate de către AC și AI. Acest capitol oferă o descriere a cadrului de controale de securitate, care reflectă prevederile cuprinse în legislația privind semnătura electronică din România, Regulamentul eIDAS și Standardele ETSI EN 319 401. Prevederile respective se completează unele pe celelalte și au menirea de a spori controalele de securitate în ansamblu. Toate acestea necesită cele mai înalte standarde de controale de securitate.

Din motive de securitate, Trans Sped nu va dezvălui niciun detaliu specific legat de măsurile specifice luate. Documentele care descriu implementarea controalelor de securitate Trans Sped sunt considerate a fi confidențiale.

5.1. Controale fizice

Nivelul controalelor de securitate fizică restricționează accesul la sistemele sensibile, hardware și software, utilizate pentru efectuarea operațiunilor critice ale AC, care au loc în cadrul unei locații sigure din punct de vedere fizic. Aceste sisteme sunt separate din punct de vedere fizic de alte sisteme ale organizației astfel încât numai angajații autorizați să poată avea acces la acestea.

Accesul fizic la sistemele AC este strict controlat, doar persoanele de încredere cu un motiv valid au drept de acces. Sistemul de control al accesului este întotdeauna funcțional și utilizează carduri de acces în combinație cu parole pentru acces. Se păstrează un registru în care sunt înregistrate toate intrările fizice în zonele restricționate.

Cheile critografice private folosite pentru emiterea de certificate sau semnarea răspunsurilor legate de starea certificatului nu sunt vulnerabile la penetrarea fizică. Aceste chei sunt depozitate în dispozitive securizate de creare a semnăturii ce nu pot fi falsificate, sunt atestate să îndeplinească cerințele prevăzute în legislația privind semnătura electronică din România și Regulamentul eIDAS. Orice acces neautorizat la informația depozitată, posibil provenind din pierderea, falsificarea, sau utilizarea greșită a acestora este împiedicată prin mijloace corespunzătoare. Verificările de securitate regulate sunt efectuate pentru a se asigura că aceste controale funcționează corespunzător.

Accesul la orice zonă fizică unde sunt amplasate informații sau echipament sensibil la operațiunile AC necesită ca cel puțin două persoane autorizate să aibă acces la respectivele locații. Intrarea în zonele restricționate folosind același dispozitiv token de două ori (pentru a sustrage cerința a două persoane diferite care au acces la respectiva locație) este împiedicată prin mijloace tehnice. De asemenea, zonele sensibile sunt monitorizate prin camere video.

Orice sistem computerizat sensibil cu privire la emiterea de certificate operează un sistem de operare sigur B1 și nu poate fi operat prin LAN sau WAN, ci doar de la consolă. Sistemele computerizate care furnizează registrul și serviciile depozitare pot fi administrate doar de la consolă sau printr-un protocol de rețea sigur. Accesul la sistemele sensibile necesită prezența a două persoane (sau log on) în același timp.

Toate sistemele AC au energie electrică de industrie standard și sisteme de aer condiționat care să ofere un mediu de operare corespunzător. Toate sistemele AC au precauții rezonabile luate

pentru a minimiza impactul expunerii la apă și au mecanisme standard de prevenire a incendiilor și de protecție în locație.

Rezervele din afara locației sunt depozitate într-o manieră sigură din punct de vedere fizic de către o societate de depozitare terță parte legală.

Orice AI care confirmă informațiile semnatarului și care înaintează aceste informații către Trans Sped trebuie să ofere o facilitate sigură din punct de vedere fizic pentru depozitarea înregistrărilor legate de cereri și token necesare pentru a avea acces la componentele AI. Dacă o AI păstrează informațiile confidențiale ale semnatarului controalele de securitate din punct de vedere fizic trebuie să se potrivească cu cele ale Trans Sped.

AI nu stochează niciodată informațiile legate de cheia semnatarului.

5.2. Controale de procedură

Controalele de procedură asigură că nicio persoană care acționează singur(ă) nu va putea înșela măsura de securitate luată prin procedurile operationale.

Responsabilitățile de management formale și proceduri existente au scopul de a controla toate modificările la echipamentul AC, software, și proceduri de operare. Responsabilitățile și ariile de răspundere sunt segregate pentru a reduce oportunitățile pentru modificarea neautorizată sau utilizarea greșită a informațiilor sau serviciilor. Acest lucru se realizează, de exemplu, prin definirea diferitelor roluri astfel încât efectuarea anumitor sarcini esențiale să necesite mai multe persoane. Acest “control dual” împiedică falsificarea unui certificat de către o singură persoană.

AC a implementat următoarele sunt rolurile de încredere:

- Manager - persoană cu responsabilitate generală pentru sistemele AC;
- Ofițer de securitate - persoane cu responsabilitate generală pentru securitatea serviciului. Aceste persoane gestionează și monitorizează jurnalele de evenimente și arhivele discutate în secțiunile 5.4 și 5.5. Ei nu dețin alte roluri;
- Administrator de sistem - persoane autorizate să instaleze, să configureze și să mențină AC; Crearea și întreținerea de conturi de utilizator; Configura profilele și parametrii de audit; Și să genereze chei de componente;
- Operator de sistem - persoană autorizată să efectueze backup și recuperare de sistem;
- Responsabil de înregistrare - persoană autorizată să solicite sau să aprobe solicitări pentru emiterea, suspendarea sau revocarea certificatelor. Aceste persoane nu dețin alte roluri;
- Auditor - persoană autorizată să vizualizeze și să mențină jurnalele de audit ale AC

Facilitățile de dezvoltare și testare sunt din punct de vedere fizic separate de facilitățile operationale. Procedurile există și sunt urmate pentru raportarea defectărilor software-ului, pentru a se asigura că neregulile sunt raportate și sunt luate acțiunile corective. Utilizatorii de sisteme de AC trebuie să observe și să raporteze slăbiciunile observate sau suspectate și amenințările la sisteme sau servicii. Documentația sistemului este protejată împotriva accesului neautorizat.

Cererile de capacitate sunt monitorizate precum și proiecțiile cerințelor de capacitate viitoare sunt menite să asigure că puterea de procesare necesară și de depozitare sunt întotdeauna disponibile.

Sunt implementate controale de detectare și prevenire pentru a proteja împotriva virușilor și software rău voitor și proceduri de informare a utilizatorului adecvate.

Există o procedură de raportare formală și este urmată, împreună cu o procedură de răspuns în caz de incident, prezentând acțiunea ce va fi luată la primirea unui raport legat de existența unui incident. Responsabilitățile și procedurile de management ale unui incident există și sunt urmate pentru a asigura un răspuns rapid, eficace și ordonat ca răspuns la incidentele de securitate.

5.3. Controale la nivel de personal

Trans Sped se asigură că întregul personal implicat în emiterea, administrarea, suspendarea și revocarea certificatelor digitale calificate, precum și datele și informațiile legate de administrare sunt integre, de încredere și loiale. Acest lucru include, dar fără a se limita la solicitarea unui certificat emis de către poliție, declararea că persoana în cauză nu are cazier de niciun fel. Întregul personal trebuie să aibă cunoștințele și experiența necesare legate de operațiunile AC și trebuie să fi demonstrat seriozitate și cunoașterea legată de securitate referitoare la îndatoririle sale la Trans Sped. Au loc evaluări periodice pentru a verifica încrederea întregului personal.

Niciun utilizator neautorizat nu are acces la sistemele care stochează datele sensibile. Toate sistemele care stochează asemenea informații sunt amplasate în interiorul zonei protejate. De asemenea, accesul la camerele din interiorul zonei protejate este controlat de către un sistem de control al accesului, iar accesul la sisteme este permis doar persoanelor autorizate.

Angajații semnează un contract de confidențialitate (nedivulgare) ca parte din termenii și condițiile inițiale de angajare. Toți angajații organizației și, unde este cazul, utilizatorii terțe părți primesc pregătire profesională adecvată în politicile și procedurile organizaționale.

Există și este urmat un proces disciplinar formal pentru angajații care au încălcat politicile și procedurile de securitate organizaționale. Politicile și procedurile Trans Sped specifică sancțiunile împotriva personalului pentru acțiunile neautorizate, folosirea neautorizată de autoritate și folosirea neautorizată a sistemelor.

Acțiunile adecvate și la timp sunt luate atunci când un angajat este concediat, astfel încât controalele și securitatea să nu fie impactate de un asemenea eveniment.

5.4. Procedurile de registre de audit

Trans Sped păstrează rapoarte de audit și fișiere ale sistemului de înregistrare care documentează acțiunile întreprinse ca parte din serviciile de încredere calificate ale Trans Sped. Cel puțin, fiecare înregistrare de audit include următoarele:

- timpul evenimentului;
- tipul evenimentului;
- un indicator de succes sau de defecțiune pentru eveniment și identitatea entității care a provocat evenimentul.

Trans Sped înregistrează manual sau în mod automat următoarele evenimente semnificative:

- modificări ale parametrilor de audit (de exemplu, frecvența auditului, tipul de eveniment auditat);
- încercarea de a șterge sau modifica jurnalele de audit;
- conectări reușite, încercări de conectare nereușite pentru roluri de încredere;
- schimbarea numărului de încercări nereușite permise;
- atingerea limitei numărului permis de încercări de conectare nereușite;
- readmisia unui utilizator blocat din cauza încercărilor de conectare nereușite;
- toate evenimentele pentru întregul ciclu de viață al cheilor AC (generare, încărcare, salvare, etc.);
- evenimente legate de generarea și gestionarea cheilor de utilizator;
- fiecare cerere legată de emiterea, re-cheie, suspendarea și revocarea certificatului;
- evenimente legate de procesarea cererilor;
- eliberarea certificatului sau schimbarea statutului;
- generarea unui nou CRL;
- generarea unui răspuns OCSP;
- schimbarea setărilor oricărei componente a AC;
- modificarea rolurilor utilizatorilor;
- modificarea profilului certificatului;
- modificarea profilului CRL;
- modificările setărilor politicii de securitate
- instalarea, ștergerea (resetarea), eliminarea, eliminarea, a unui HSM;
- încărcarea cheilor, certificatelor către HSM;
- accesul la o componentă a sistemului AC;
- fișiere sau înregistrări sensibile la securitate citite, scrise sau șterse;
- accidente de sistem, defecțiuni hardware și alte anomalii;
- activitatea firewall-ului și a ruterului;
- intrarea / ieșirea vizitatorului instalației AC;

Evenimentele din jurnalele de audit sunt marcate temporal și semnate digital. Trans Sped utilizează semnalul de timp GPS și un set de servere NTP ca sursă de timp.

Registrele de audit și jurnalele de evenimente sunt revizuite periodic și arhivate pentru a ajuta la viitoarele investigații privind incidentele legate de securitate. În plus, rezumatele recenziilor sunt, de asemenea, arhivate.

Ca parte din procedurile periodice de salvare de sistem, fișierele raportului de audit sunt salvate pe medii de tip WORM. Fișierele raportului de audit sunt arhivate de către un administrator de sistem săptămânal (cel puțin). Jurnalul de evenimente sunt revizuite cel puțin săptămânal de către auditorii interni.

Nicio persoană nu poate modifica sau șterge fișierele rapoartelor de audit sau de registru de sistem de una singură, iar accesul la acestea este strict restricționat. Aceste prevederi sunt implementate folosind trăsăturile unui sistem de operare sigur B1 care necesită login-ul simultan a două persoane.

Pentru informații suplimentare legate de cerințele și procedurile de audit extern și intern, vezi art. 8.1.

5.5. Arhivarea înregistrărilor

Fișierele rapoartelor de audit și ale sistemului de înregistrare (a se vedea art. 5.4) sunt salvate periodic pe medii WORM (scriere o dată, citire multiplă) și arhivate într-o locație sigură. Datele de audit arhivate referitoare la certificatele digitale calificate sunt pastrate conform Regulamentului eIDAS.

Trans Sped utilizează arhivarea internă și externă pentru a împiedica pierderea documentelor importante sau a datelor digitale. Arhivele sunt amplasate în locații diferite (interne sau externe) și protejate de sistemele de control ale accesului. În general, rapoartele privind certificatele digitale calificate sunt reținute cel puțin zece (10) ani și 6 (șase) luni conform prevederilor legislației naționale și a Regulamentului eIDAS. Nicio persoană singură nu poate modifica sau distruge materialul arhivat, iar accesul la acesta este strict restricționat.

5.6. Schimbarea cheii

Root AC este valabil timp de 10 ani (până în 2031). Certificatele de autorizare sunt valabile timp de 5 ani (până în 2026). Atunci când se generează un certificat AC nou, se modifică și denumirea AC. Același lucru este și cu CDP de certificate de utilizator final.

Certificatul AC mai vechi, dar încă valabil, va fi disponibil pentru a verifica semnăturile vechi până când toate certificatele semnate utilizând cheia privată asociată vor expira. Vechea cheie privată este, de asemenea, utilizată pentru a semna certificatele CRL și OCSP Responder. Prin urmare, datorită reluării o AC poate crea CRL-uri multiple, lista tuturor acestor CRL-uri fiind identică.

Schimbarea cheilor AC permite Trans Sped să modifice parametrii cheii și algoritmi criptografici, ținând cont de potrivirea algoritmilor și parametrilor pentru a compensa noile descoperiri în știință și/sau tehnologie. Orice AC nouă poate fi pusă la dispoziție la cerere prin e-mail sau de la depozitarul Trans Sped la www.transsped.ro/repository.

5.7. Compromiterea și recuperarea după dezastre

Pentru a restaura operațiunile într-un termen rezonabil de timp ca urmare a întreruperii proceselor critice, au fost dezvoltate planuri de continuitate de afaceri. Planul de continuitate al afacerii definește perioada de timp, adică o perioadă de întrerupere a sistemului acceptabilă în

cazul unui dezastru natural de amploare sau compromitere a cheii private AC. Această perioadă de întrerupere tolerată depinde de cerințele de valabilitate ale serviciului specific și poate dura de la o oră la 12 ore.

O locație de recuperare în caz de dezastru a fost stabilită pentru a asigura continuitatea operațională în cazul în care locația principală este indisponibilă temporar.

Rezervele unor informații esențiale și sistemul software al AC sunt operate în fiecare zi. Procedurile de recuperare în caz de dezastre sunt testate cu regularitate. Documentația referitoare la aceste proceduri este considerată confidențială.

5.8. Terminarea AC

Activitatea AC poate fi terminată de către Organismul Român de Supraveghere (OS) sau de către Consiliul de Administrație al Trans Sped. Trans Sped va informa posesorii de certificate valide (adică nici revocate nici expirate) cât de mult permit circumstanțele și încearcă să furnizeze surse alternative de interoperare.

Trans Sped va depune toate eforturile pentru a transfera înregistrările AC și depozitarul de certificate către un alt emitent de certificate digitale calificate. Trans Sped, de asemenea, va încerca să stabilească o procedură acceptabilă pentru posesori și părțile de încredere pentru a se transfera la un alt furnizor de servicii de încredere, pentru ca Trans Sped să minimizeze efectele încercând să furnizeze el singur aceste servicii.

Dacă niciun furnizor de servicii de încredere nu continuă serviciile Trans Sped toate certificatele care nu au expirat sau nu au fost revocate de către respectivii posesori vor fi revocate de către Trans Sped. Toată documentația relevantă va fi transferată către Organismul Român de Supraveghere (OS) după cum prevede legislația privind semnătura electronică din România și Regulamentul (UE) nr. 910/2014.

Posesorii de certificate digitale calificate vor fi notificați dacă Trans Sped întreprinde o asemenea acțiune.

6. CONTROALE DE SECURITATE TEHNICĂ

6.1. Generarea și instalarea perechii de chei

6.1.1. Generarea perechii de chei

1.1.1.1. Generarea perechii de chei AC

Cheia criptografică privată AC folosită pentru emiterea de certificate digitale calificate este generată într-un HSM certificat FIPS 140-1/2 Nivel 3. Cheile de semnare ale AC sunt utilizate pentru generarea certificatelor și/sau doar pentru emiterea informațiilor privind starea revocărilor; acestea nefiind utilizate pentru alte scopuri.

Întreaga procedură de generare de chei criptografice este efectuată sub un control dual. În plus, generarea de cheie se face în prezența și semnată de o terță parte neimplicată în generarea de cheie propriu-zisă.

În niciun moment pe parcursul procesului de generare cheia criptografică privată nu părăsește HSM-ul sub formă necriptată, și niciun material privind cheie criptografică privată necriptat nu este eliberat.

Generarea de software și / sau utilizarea de chei criptografice nu sunt suportate în legătură cu emiterea de certificate digitale calificate.

Nicio copie a niciunei chei criptografice private nu este păstrată permanent pe suport magnetic media în format necriptat. Niciun material nu va stoca cheie criptografică privată temporar pe suport magnetic media pentru că cheile pentru certificate digitale calificate sunt generate în interiorul HSM.

1.1.1.2. Generarea cheii criptografice private a semnatarului

Dacă generarea cheii criptografice private către posesor este efectuată de către AC sau AI cheile sunt depozitate pe dispozitiv securizat de creare a semnăturii protejat cu PIN (DSCS) sau HSM. Acest proces are loc în locații securitate. Nicio copie a cheilor criptografice private ale posesorului nu este păstrată de către AC sau AI astfel că utilizarea lor greșită nu este posibilă.

Dacă generarea cheii criptografice private este realizată de către Posesor iar solicitarea de emitere certificat trimisă către AC, atunci Trans Sped nu oferă nicio garanție legată de generarea cheii. Perechile de chei criptografice trebuie să fie generate pe dispozitiv securizat de creare a semnăturii protejat cu PIN (DSCS) aprobat de Trans Sped. PIN-ul de protejare al DSCS este strict personal.

6.1.2. Livrarea cheii criptografice private către entitate

Cheile criptografice private generate de AC sau AI pe DSCS sunt livrate către posesor prin serviciul de curierat. Codurile PIN sunt distribuite separat de DSCS-uri.

Alternativ, semnatarul poate colecta DSCS cu cheia criptografică privată la birourile AC sau AI. La cererea posesorului de certificat digital calificat DSCS poate fi livrat prin altă formă acceptabilă de livrare securizată.

6.1.3. Livrarea cheilor criptografice private către posesorii de certificate digitale calificate

Posesorii de certificate digitale calificate transmit cheia criptografică publică generată ca pe o cerere electronică al cărei format trebuie să respecte PKCS#10 Sintaxa Cererii de Certificare. Solicitățile posesorilor trebuie să fie semnate utilizând cheia criptografică privată corespunzătoare cheii publice care va fi indicată în certificat.

Legătura între solicitarea de emiteră a certificatului și verificarea identității posesorului este aprobată după cum urmează:

- Pentru verificarea identității inițiale a posesorului pentru SSCD, posesorul se prezintă fizic la AC sau AI și crearea certificatului digital calificat și verificarea identității se face în același timp.
- Pentru reînnoire online, sesiunea TLS sau mesajul S/MIME utilizează cheia criptografică privată curentă pentru autentificarea posesorului și include cererea PKCS # 10.
- Pentru dovedirea inițială a identității, precum și reînnoire posesorul trebuie să se autentifice în contul său de administrare al certificatului utilizând același credențiale ale certificatului.

6.1.4. Livrarea cheilor criptografice private către utilizatori

Metodele de livrare a certificatelor AC includ:

- publicarea certificatelor AC pe o listă națională de încredere a prestatorilor de servicii de încredere calificată;
- publicarea certificatelor AC pe depozitul Trans Sped și prin livrarea unui hash a certificatului printr-un canal de încredere la cerere.

Cheia criptografică publică a utilizatorului este livrată pe același DSCS folosit pentru depozitarea cheii criptografice private a utilizatorului dacă perechea de chei criptografice este generată de către AC sau AI.

De asemenea, dacă utilizatorul certificatului digital calificat este de acord ca certificatul său să fie publicat în depozitarul de certificate Trans Sped, acesta este disponibil pentru descărcare.

6.1.5. Dimensiunile cheii criptografice

Perechile de chei criptografice trebuie să aibe o lungime suficientă astfel încât să prevină deducerea cheii private de către alții folosind cryptoanaliza în timpul perioadei de utilizare a acestor perechi de chei criptografice.

Perechile de chei criptografice ale AC-urilor Trans Sped au lungimea de 2048 biti. Orice cheie generată pe un DSCS și folosită pentru un certificat digital calificat are dimensiunea de cel puțin 2048 biti.

Nu se semnează certificate, CRL sau răspunsuri OCSP utilizând un algoritm RSA 2048 care se extinde peste data de 31.03.2030. De asemenea, toate certificatele emise pentru chei RSA de 2048 de biți vor expira la 12/31/2030, altfel vor fi revocate.

6.1.6. Parametrii de generare a cheii criptografice publice

Algoritmii permisi și parametrii cheii criptografice pentru perechile de chei utilizate pentru certificate digitale calificate sunt publicați de către eIDAS și ETSI. Trans Sped utilizează doar

astfel de algoritmi și parametri de cheie criptografică publică pentru certificate digitale calificate care sunt definiți a fi corespunzători.

Toate cheile criptografice publice ale AC pentru emiterea de certificate digitale calificate sunt chei RSA pe 2048 bit și utilizează algoritmul hash SHA-256.

6.1.7. Verificarea calității parametrilor

Perechile de chei criptografice ar trebui generate doar pe carduri inteligente aprobate sau HSM-uri. Cardurile inteligente ce sunt folosite de către Trans Sped sunt formate pentru a permite doar dimensiuni de cheie de 2048 bit. Aplicația online și/sau mecanismele de certificare vor verifica cererile de certificat corespunzător generate și formatul lor corect.

6.1.8. Generarea de chei hardware/software

Cheile pentru certificatele digitale calificate vor fi generate doar pe dispozitiv securizat de creare a semnăturii (DSCS).

6.1.9. Scopurile utilizării cheii (conform domeniului de utilizare a cheii X.509 v3)

Certificatele digitale calificate emise de către Trans Sped trebuie să fie folosite în conformitate cu domeniul de utilizare a cheii X.509 v3 stabilit de către Trans Sped (a se vedea de asemenea art. 7.1). Certificatele digitale calificate pot fi utilizate pentru semnături electronice sau sigilii electronice.

6.2. Protecția cheii criptografice private

Trans Sped asigură gestionarea sigură a cheilor criptografice private AC utilizate pentru emiterea de certificate digitale calificate și cheile criptografice private utilizate pentru semnarea informațiilor privind statutul de revocare (CRL, OCSP) și împiedică dezvăluirea, copierea, ștergerea, modificarea și utilizarea neautorizată a cheilor criptografice private. Cheile criptografice private AC sunt stocate într-o locație sigură din punct de vedere fizic, într-un Modul de securitate hardware (HSM) securizat.

Accesul la cheia publică și la cheile private este protejat de mecanismele de control al accesului. Cheile criptografice private pot fi activate numai de două persoane și sunt stocate într-un sistem HSM certificat FIPS 140-1/2 nivel 3. Nu este scris niciodată pe niciun suport de stocare permanent sau magnetic.

6.2.1. Standardele pentru modulul criptografic

Pentru emiterea de certificate digitale calificate este utilizat un HSM certificat FIPS 140-1/2 Nivel 3.

De asemenea, pentru stocarea altor tipuri de chei sunt utilizate Hardware Security Module (HSM). Aceste module sunt certificate FIPS 140-1/2 Nivel 3. Accesul fizic la HSM este restricționat printr-un sistem de control al accesului. HSM sunt utilizate în modul FIPS 140-1/2 Nivel 3.

HSM pot fi activate doar de două persoane simultan (login dual).

Cheile private necriptate nu pot fi extrase din modulul de securitate hardware în niciun moment.

6.2.2. Controlul multi-pesoane al unei chei criptografice private (n din m)

Cheile criptografice private AC sunt stocate într-un HSM certificat FIPS 140-1/2 Nivel 3 (sau echivalent). Pentru a activa cheile criptografice private ale AC, sunt necesare două persoane (a se vedea art. 6.2.1). Nicio persoană singură nu are toate datele de activare necesare pentru accesarea oricăror chei private AC.

6.2.3. Cheia privată escrow

Trans Sped nu va păstra cheile de semnătură privată ale utilizatorilor finali pentru certificate digitale calificate.

Pentru certificatele emise conform prevederilor Regulamentului eIDAS, orice formă de cheie escrow este în mod explicit interzisă.

6.2.4. Backup de cheie criptografica privată

Cheile criptografice private ale AC sunt generate într-un HSM certificat FIPS 140-1/2 Nivel 3. Trans Sped realizează copii de siguranță înainte de a pune cheile CA în funcțiune. În timpul copierii de rezervă, cheia criptografica privată părăsește modulul într-o formă criptată și această cheie criptată poate fi restabilită numai într-un alt modul. Cheile criptate au copii de rezervă pe medii WORM și pot fi activate doar sub controlul dual într-o locație securizată din punct de vedere fizic.

Cheile criptografice pentru utilizatorii finali sunt generate și stocate pe un DSCS. Aceste chei nu pot fi scoase de pe cardul inteligent și de aceea nu au copii de rezervă.

6.2.5. Arhivarea cheii criptografice private

Cheia de rezervă (a se vedea art. 6.2.4) este utilizată în scopuri de arhivare. Se aplică prevederile legate de rezerve de chei private.

Cheile AC arhivate sunt distruse la finalul perioadei de arhivare folosind controlul dual într-o locație securizată din punct de vedere fizic. Cheile arhivate nu sunt niciodată puse în producție.

6.2.6. Intrarea cheii criptografice private în modulul criptografic

Cheile criptografice private AC sunt generate și depozitate într-un HSM certificat FIPS 140-1/2 Nivel 3. Cheile private AC nu sunt stocate în clar în afara modulului criptografic. Trans Sped exportă numai cheia privată de la HSM în scopul realizării unei copii de siguranță. Exportul și încărcarea cheilor private AC se efectuează în conformitate cu art. 6.2.4.

HSM-urile sunt protejate și manipulate în timpul transportului, depozitării și utilizării.

6.2.7. Metoda de activare a cheii criptografice private

Activarea cheilor criptografice private AC utilizate pentru emiterea de certificate digitale calificate necesită autentificarea prin parole și/sau PIN și poate fi realizată doar sub controlul dual, din moment ce secretul autentificării este împărțit în două sau mai multe părți.

6.2.8. Metoda de dezactivare a cheii criptografice private

Cheia criptografică privată AC este în mod automat dezactivată după ce emiterea de certificate a fost finalizată iar cererile pentru certificat ies din sau închid conectarea la HSM. Înainte de a mai putea fi folosit din nou, HSM-ul trebuie să fie reactivat.

6.2.9. Metoda de distrugere a cheii criptografice private

Distrugerea oricărei chei private ale AC trebuie să fie autorizată de către conducere. Aceasta se realizează sub control dual, și este în prezența și semnată de o terță parte care nu este implicată în distrugerea propriu-zisă a cheii. Toate copiile și fragmentele cheii private sunt distruse la finalul ciclului de viață al perechii de chei.

Pentru cheile private utilizate în legătură cu un HSM, spațiul de depozitare magnetic care a purtat cheia privată este șters de mai multe ori pentru a elimina orice urmă rămasă iar token-ul hardware (smart cardul) necesar pentru a activa cheia este șters în totalitate sau distrus din punct de vedere fizic, numai dacă nu este nevoie de activarea altor chei private. Dacă mediul de stocare este înlocuit (de exemplu, din cauza erorilor hardware), acesta este distrus din punct de vedere fizic.

Dacă un dispozitiv securizat criptografic este accesibil și cunoscut a fi permanent scos din serviciu, toate cheile private stocate în dispozitiv care au fost vreodată sau potențial ar putea fi folosite pentru orice scop criptografic sunt distruse.

Dacă un dispozitiv criptografic AC este în permanență scos din serviciu, atunci orice cheie conținută în dispozitivul care a fost folosit în orice scop criptografic este ștearsă din dispozitiv. În cazul unui dispozitiv criptografic AC menit să furnizeze protecție fizică la atacuri dacă dispozitivul este scos din serviciu definitiv, atunci acesta este distrus.

Dacă o cheie privată este depozitată pe un DSCS, acesta este distrus prin distrugerea fizică a cardului inteligent. Nu există fragmente de material de cheie sau copiate care trebuie să fie distruse în acest caz pentru că folosirea unui DSCS garantează că cheile private nu pot fi niciodată exportate din DSCS.

6.3. Alte aspecte legate de managementul perechii de chei criptografice

6.3.1. Arhivarea cheii criptografice publice

Orice certificat digital calificat emis de către Trans Sped este stocat în depozitarul de certificate și pe mediul de rezervă al sistemelor care găzduiesc depozitarul de certificate. De asemenea, orice certificat digital calificat emis de către Trans Sped este depozitat pe sisteme AC și în fișierele de audit create pentru sistemul AC.

6.3.2. Perioadele de utilizare pentru cheile criptografice private și publice

Cheile criptografice private și publice pot fi utilizat atâta timp cât indică perioada de valabilitate a certificatului și/sau depozitarul. De îndată ce expiră această perioadă, cheile nu mai sunt valabile. Folosirea cheilor criptografice private ale AC este limitată la perioada de timp în care

algoritmii utilizați sunt considerați ca fiind adecvați pentru utilizare; întrebuițarea acestora va fi oprită după acel moment.

6.4. Datele de activare

Cerințele pentru controlul accesului sunt definite și documentate într-o politică referitoare la controlul accesului care cuprinde procesul de identificare și autentificare pentru fiecare utilizator, segregarea îndatoririlor, și numărul de persoane necesare pentru a desfășura operațiuni specifice AC (însemnând, regula m din n). Datele de activare (și acces) pentru cheile și activele sensibile sunt sub control dual și/sau împărțite între cel puțin două grupuri distincte de angajați.

O procedură formală de înregistrare și de înregistrare a utilizatorului pentru acordarea accesului la datele de activare pentru sistemele de informare AC și servicii este urmată, iar alocarea și utilizarea datelor de activare și privilegiile este restricționată și controlată. Drepturile de acces ale utilizatorilor sunt revizuite la intervale regulate și sunt necesare pentru a urma politicile și procedurile definite în selectarea și utilizarea parolelor.

6.5. Controalele de securitate ale calculatorului

Un document de politică a securității informației generale (politică de securitate) este aprobat de către conducere, publicat și comunicat, drept corespunzător către toți angajații. Această politică este suplimentată de politicile și procedurile detaliate pentru personalul implicat în management-ul certificatului digital și cheii criptografice.

Politică de securitate a informației conține o definiție a securității informației, obiectivele ei complete și aria, și importanța securității ca un mecanism care permite partajarea de informații. Acesta conține o declarație a intenției conducerii, sprijinind obiectivele și principiile securității informației și oferă o explicație a politicilor de securitate, principii, standarde, și cerințele de conformare de o importanță specială pentru organizație.

Politică de securitate a informației prezintă responsabilitățile generale și specifice pentru management-ul de securitate a informației, inclusiv raportarea incidentelor legate de securitate, și conține referiri la documentația care sprijină politica. Responsabilitățile pentru protecția activelor individuale și pentru desfășurarea proceselor de securitate specifice sunt clar definite.

Codul de Politici și Practici (a se vedea art. 8.1) asigură că există o direcție clară și un sprijin de conducere vizibil pentru inițiativele de securitate. Acesta este responsabil cu menținerea politicii de securitate și coordonează implementarea măsurilor legate de securitatea informației.

6.6. Ciclul de viață al controalelor tehnice

Dezvoltarea este realizată în conformitate cu standardele de dezvoltarea ale sistemelor și management-ul de schimbare.

Trans Sped utilizează numai aplicații și dispozitive care:

- sunt echipamente hardware și software comerciale, concepute și dezvoltate printr-o metodologie de proiectare documentată; sau
- hardware și software personalizat dezvoltat de către o entitate sigură într-un mediu controlat utilizând metode structurate de dezvoltare sau;

- software open source care respectă cerințele de securitate, iar caracterul adecvat al acestora este asigurat prin verificarea și validarea software-ului.

Noile componente sunt mai întâi testate în mediul de testare înainte de a fi utilizate în mediul de producție. Mediile de testare și de producție sunt total decuplate.

Hardware-ul este achiziționat și expediat într-o manieră pentru a reduce probabilitatea de manipulare frauduloasă. Hardware-ul este dedicat soluțiilor și operațiunilor PKI.

6.6.1. Controalele managementului de securitate

Trans Sped are mecanisme și politici menite să controleze și monitorizeze configurația și integritatea sistemelor sale.

6.7. Controalele de Securitate a Rețelei

Trans Sped a instalat protecție corespunzătoare atât împotriva atacurilor interne cât și externe (firewall, mecanisme de detectare de intruziune, etc.). Controalele de rutare sunt menite să asigure că conexiunile de calculator și fluxurile de informații nu încalcă politica de control al accesului a aplicațiilor de afaceri ale organizației.

Accesul la toate serverele este supusă autentificării. Utilizatorilor li se acordă acces direct doar la serviciile pentru care au fost în mod specific autorizați spre a le folosi.

Trans Sped utilizează semnalul de timp GPS și un set de servere NTP ca sursă de timp pentru toate componentele AC. Timpul derivat din sursele de timp de încredere este folosit pentru a stabili timpul pentru:

- perioada de valabilitate inițială a certificatului unui client
- revocarea certificatului unui client
- postarea actualizărilor CRL
- răspunsurile OCSP

6.8. Controale la nivelul modulului criptografic

Echipamentele (DSCS-urile) utilizate pentru stocarea cheilor sunt certificate în conformitate cu ITSEC Nivel "E4 high" (sau echivalent).

Modulele de Securitate Hardware folosite pentru depozitarea altor materiale cheie AC sunt certificate a fi conforme FIPS 140-1/2 Nivelul 3 (a se vedea art. 6.2.1).

6.9. Marcare temporală

Serviciul de marcă temporală este disponibil în cadrul PKI-Trans Sped.

7. PROFILELE CERTIFICATELOR, CRL ȘI OCSP

7.1. Profilul certificatului

7.1.1. Numărul (numerele) versiunii

Trans Sped emite certificate X.509 versiunea 3 în conformitate cu RFC 5280, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

7.1.2. Extensiile certificatelor

Trans Sped utilizează extensii standard X.509v3. Certificatele digitale calificate emise de către Trans Sped includ următoarele câmpuri de extensie:

- basicConstraints este o extensie critică și are valoarea fals.
- keyUsage este o extensie critică și are valoarea digitalSignature, nonRepudiation.
- subjectAltName este o extensie non critică care permite identități adiționale ce vor fi legate de subiectul certificatului cum ar fi adresa de e-mail sau UPN.
- authorityKeyId este o extensie non critică care identifică certificatul AC care trebuie utilizat pentru a verifica certificatul semnatarului.
- qcStatements este o extensie non critică și are valorile:
 - id-etsi-qcs-QcCompliance
 - id-etsi-qcs-QcSSCD
 - id-etsi-qcs-QcPDS indicând indicand Declarația de dezvăluire a PKI

7.1.3. Identificatorii obiectului algoritmului

Pentru certificatele digitale calificate Trans Sped sprijină doar asemenea combinație a algoritmului semnăturii digitale/funcție hash care sunt permise pentru utilizarea certificatelor digitale calificate.

Cheile actuale ale AC pentru emiterea de certificate calificate sunt cheile RSA cu 2048 bit și folosesc algoritmul hash SHA-2.

7.1.4. Formele numelui

A se vedea art. 3.1.

7.1.5. Constrângerile legate de nume

Nu se aplică.

7.1.6. Obiectul identificator al politicii de certificate

În funcție de Root-ul Autorității de Certificare emitente, Trans Sped are mai multe politici OID, după cum urmează:

Trans Sped QCA G2 OID

0.4.0.194112.1.2

itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1)
qcp-natural-qscd (2)

1.3.6.1.4.1.39965.1.1.1

Trans Sped QCA G3 OID

0.4.0.194112.1.2

itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1)
qcp-natural-qscd (2)

1.3.6.1.4.1.39965.1.1.1

Trans Sped Mobile eIDAS QCA G2 OID

0.4.0.194112.1.2

itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1)
qcp-natural-qscd (2)

1.3.6.1.4.1.39965.4.1.1

Trans Sped Mobile eIDAS QCA G3 OID

0.4.0.194112.1.2

itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1)
qcp-natural-qscd (2)

1.3.6.1.4.1.39965.4.1.1

Trans Sped Electronic Seal QCA G2 OID

0.4.0.194112.1.3

itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1)
qcp-legal-qscd (2)

1.3.6.1.4.1.39965.5.1.1

Trans Sped Electronic Seal QCA G3 OID

0.4.0.194112.1.3

itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1)
qcp-legal-qscd (2)

1.3.6.1.4.1.39965.5.1.1

Trans Sped Advanced eIDAS CA G2 OID

0.4.0.2042.1.1

itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1)
ncp(1)

1.3.6.1.4.1.39965.6.1.1

Trans Sped Advanced eIDAS CA G3 OID

0.4.0.2042.1.1

itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1)
ncp(1)

1.3.6.1.4.1.39965.6.1.1

Trans Sped TSA G2 OID

0.4.0.2023.1.1

itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(2023) policy-identifiers(1) baseline-ts-policy(1)

1.3.6.1.4.1.39965.1.2.1

Trans Sped TSA G3 OID

0.4.0.2023.1.1

SAFE CA OID

1.3.6.1.4.1.39965.2.1.1 mediumAssuranceHardware

trans sped (1.3.6.1.4.1.39965) safe (2) policies (1) mediumAssuranceHardware (1)

1.3.6.1.4.1.39965.2.1.3 mediumAssuranceHardwareRoaming

trans sped (1.3.6.1.4.1.39965) safe (2) policies (1) mediumAssuranceHardwareRoaming (3)

7.1.7. Folosirea extensiilor constrângerilor politicii

Nu există prevederi.

7.1.8. Sintaxa și semantica calificatorilor politicii

Certificatele digitale calificate emise de Trans Sped pot conține calificate de politică, cum ar fi anunțul utilizatorului, numele politicii și indicatorii CPS.

7.1.9. Procesarea semanticii pentru extensia critică a politicii de certificate

Dacă această extensie este critică, software-ul de validarea căii de certificare trebuie să poată interpreta această extensie (inclusiv calificatorul opțional), sau trebuie să respingă certificatul.

7.1.10. Trans Sped Root CA G2

Câmpul de date	Valoare	
Versiune	v3	
Număr serial	automatic	
Algoritm de semnare	sha256withRSAEncryption	
Emitent	Atribut	Valoare
	CN	Trans Sped Root CA G2
	OU	Trans Sped CA
	O	Trans Sped SRL

	C	RO
Valabilitate	2016 – 2031	
Subiect	Atribut	Valoare
	CN	Trans Sped Root CA G2
	OU	Trans Sped CA
	O	Trans Sped SRL
	C	RO
Cheia publică subiectului	a30 82 01 0a 02 82 01 01 00 be e3 c9 f2 35 e1 c2 f6 75 0e 22 b8 20 bb e1 97 23 a4 ae b9 a6 cc c3 f5 18 77 74 29 2f d2 9f 8a e7 77 ba 39 f3 21 d0 c2 fa 4f 06 74 68 33 b0 31 f7 29 ad 64 85 a6 1d e3 e7 07 77 03 bf 0d be 3f fd d7 e9 93 ba a0 64 01 36 17 a4 20 95 55 a3 54 9e 4a c6 4c 1e eb e3 f7 2b 84 3a ae 9e 1d b2 39 e5 6f a1 24 32 1e 1e cf cb bc 54 7f 5a ce 86 fe e8 39 dd 3c 5b e6 de 15 f2 50 c7 6d 5a 02 36 fc 1a 86 23 3a e7 13 f1 73 8b c3 88 c5 c4 90 d7 cc 9a c5 65 f4 6d 7e 9f b2 be 38 e9 3a c0 c0 3e 55 b3 8d 6d 84 f3 8a 14 62 e4 99 d8 30 b8 aa 10 14 0d f4 63 af 6d e1 cd 9d 38 52 42 25 5e 44 aa f7 9e 71 06 d5 d3 8c 65 3b 3d c0 83 2e 8e e2 30 b0 c5 0e 2f e5 a0 d1 a2 73 f6 fc 14 42 bb ee a6 7a 3d 27 3e c8 7a fe fa c8 50 78 77 8b c4 44 21 c5 03 30 8f 88 91 19 7f 16 fe 12 9d f5 c6 eb 49 a7 02 03 01 00 01	
Extensie	Critic	Valoare
basicConstraints	yes	cA: TRUE pathLenConstraint: none
keyUsage	yes	keyCertSign cRLSign
subjectKeyIdentifier	no	automatic

7.1.11. Trans Sped Electronic Seal QCA G2

Câmpul de date	Valoare	
Versiune	v3	
Număr serial	automatic	
Algoritm de semnare	sha256withRSAEncryption	
Emitent	Atribut	Valoare
	= Subject of Trans Sped Root CA G2	
Valabilitate	2020 - 2029	

	Atribut	Valoare
Subiect	CN	Trans Sped Electronic Seal QCA G2
	OU	LEGAL PERSON CA
	O	Trans Sped SRL
	C	RO
	Cheia publică a subiectului	
Extensie	Critic	Valoare
basicConstraints	yes	cA: TRUE pathLenConstraint: 0
keyUsage	yes	keyCertSign cRLSign
certificatePolicies	no	[1]Certificate Policy: Policy Identifier=0.4.0.194112.1.3 [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.39965.5.1.1 [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.transsped.ro/repository
subjectKeyIdentifier	no	automatic
authorityKeyIdentifier	no	= subjectKeyIdentifier of Trans Sped Root CA G2
authorityInfoAccess	no	Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)

		Alternative Name: URL=http://www.transsped.ro/cacerts/ts_root_g2.crt [2]Authority Information Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.transsped.ro/
cRLDistributionPoints	no	http://www.transsped.ro/crl/ts_root_g2.crl
Thumbprint algorithm	no	sha1

7.1.12. Trans Sped QCA G2

Câmpul de date	Valoare	
Versiune	v3	
Număr serial	automatic	
Algoritm de semnare	sha256withRSAEncryption	
Emitent	Atribut	Valoare
	= Subject of Trans Sped Root CA G2	
Valabilitate	2016 - 2026	
Subiect	Atribut	Valoare
	CN	Trans Sped QCA G2
	OU	Individual Subscriber CA
	O	Trans Sped SRL
	C	RO
Cheia publică subiectului	a30 82 01 0a 02 82 01 01 00 b0 f7 8c 42 1e d0 3f 4f 2c 8e eb cf fb 19 dc 3b 39 eb a7 d0 3f 49 83 44 4a b2 18 fc 92 74 06 04 0c 1a 9b 65 14 5d 11 64 1e 4d 40 48 83 6e fa af f8 0b 69 43 05 51 56 04 bd 99 72 70 79 d9 d2 69 b4 87 14 bd 25 43 55 97 44 ff 60 6f af c6 69 59 3d d8 e1 ba e5 55 e1 8e ec 0c b8 b7 05 09 81 b9 bb 9e 9d 22 7e b3 86 99 51 75 d5 14 b2 c1 c9 d3 7a fc 4a 2d b1 be 20 02 12 cb 0f 35 66 c9 53 49 6d c9 4d 43 97 e2 ba 87 7e d4 76 f6 86 94 71 e2 b8 8e e6 28 e0 37 63 a0 e2 16 45 ab 04 bc f9 cf d8 4f 4c 6d f1 c4 49 b7 e1 7f db 62 0c ea 42 4b 0a 9a f1 e4 65 4d 33 4b b9 0c a0 6b 1a 8f 54 ac 56 65 43 a5 79 58 b2 f6 88 08 e5 58 14 c4 20 c7 13 e1 55 cc 92 1a bc 4f c1 22 1d 05 b6 ff df 61 c3	

	91 fa 37 b4 f1 a6 51 e7 22 2e 13 ca c6 f8 89 7a 9b 52 ae 7c a9 e5 db c6 13 1e d7 36 42 f1 6d 02 03 01 00 01	
Extensie	Critic	Valoare
basicConstraints	yes	cA: TRUE pathLenConstraint: 0
keyUsage	yes	keyCertSign cRLSign
certificatePolicies	no	[1] 0.4.0.194112.1.2 [2] 1.3.6.1.4.1.39965.1.1.1 cPSuri = http://www.transsped.ro/repository
subjectKeyIdentifier	no	automatic
authorityKeyIdentifier	no	= subjectKeyIdentifier of Trans Sped Root CA G2
authorityInfoAccess	no	[1]accessMethod: calssuers accessLocation: URL= http://www.transsped.ro/cacerts/ts_root_g2.crt [2]accessMethod: OCSP accessLocation: URI: http://ocsp.transsped.ro/
cRLDistributionPoints	no	http://www.transsped.ro/crl/ts_root_g2.crl

7.1.13. Trans Sped Mobile eIDAS QCA G2

Câmpul de date	Valoare	
Versiune	V3	
Număr serial	automatic	
Algoritm de semnare	sha256withRSAEncryption	
Emitent	Atribut	Valoare
		= Subject of Trans Sped Root CA G2
Valabilitate	2017 - 2027	
	Atribut	Valoare
	CN	Trans Sped Mobile eIDAS QCA G2
	OU	Individual Subscriber CA

Subiect	O	Trans Sped SRL
	C	RO
Cheia publică subiectului	a30 82 01 0a 02 82 01 01 00 dc 11 d8 dc 23 7e 52 ca 8c 5f a3 96 77 7e 7e d0 0c d2 ed b0 55 b1 25 87 8d 2f 7c b1 18 f8 91 10 09 ee db 79 1e 4c 60 99 20 49 1b fc 8d 9a 16 6a 6b b2 b9 54 06 f7 b2 37 db 1f 8c 7e 35 62 b1 cc 75 03 fb ca 4a 49 a7 89 42 99 5a 21 b9 cf 6e 8a 98 5c 7c 0f f3 ca 67 f8 1d d0 2f ba 3c 64 26 c9 5c c1 a0 42 d5 85 bc 4e a0 d0 68 29 6c 83 95 35 7c 3e 9d 2c 71 85 26 72 ea be fa d2 7c 5c 59 cd b8 ab ae 7b 04 6b 64 89 c4 75 bd ed 85 ac 96 c5 b1 a7 d1 1c a7 99 cc c7 2e 61 09 bc e7 61 1f f6 62 ef 43 70 db 54 a1 f0 7c 4e dd ce bf 01 9e fb d7 f2 00 30 61 5d 07 5c c1 dd 3c 01 95 85 b9 d4 dd e1 f4 05 3b 64 cb b9 c4 40 2c 5f ec 45 0b 18 19 48 52 7e ac a6 0c bd b9 1c 82 bc dc 9e 49 07 97 d6 7e 41 30 26 7b 6d 81 d9 5a 59 51 36 7c 63 58 63 3d 7e 10 04 8b 63 0c 18 33 d6 d0 28 0a 95 02 03 01 00 01	
Extensie	Critic	Valoare
basicConstraints	yes	cA: TRUE pathLenConstraint: 0
keyUsage	yes	keyCertSign cRLSign
certificatePolicies	no	[1] 0.4.0.194112.1.2 [2] 1.3.6.1.4.1.39965.4.1.1 cPSuri = http://www.transsped.ro/repository
subjectKeyIdentifier	no	automatic
authorityKeyIdentifier	no	= subjectKeyIdentifier of Trans Sped Root CA G2
authorityInfoAccess	no	[1]accessMethod: calssuers accessLocation: URL= http://www.transsped.ro/cacerts/ts_root_g2.crt [2]accessMethod: OCSP accessLocation: URI: http://ocsp.transsped.ro/
cRLDistributionPoints	no	http://www.transsped.ro/crl/ts_root_g2.crl

7.1.14. End User QC

Câmpul de date	Valoare
Versiune	v3

Număr serial	automatic	
Algoritm de semnare	sha256withRSAEncryption	
Emitent	Atribut	Valoare
	= Subject of Trans Sped QCA G2	
Valabilitate	Up to 3 years	
Subiect	Atribut	Valoare
	CN	<Common Name = First name + Last name>
	G	<First name>
	SN	<Last name>
	SERIALNUMBER	<Personal Identification Code>
	OU	<Organizational Unit> optional
	O	<Organization> optional
C	<Country Code>	
Cheia publică subiectului	a[RSA Key, 2048 Bit]	
Extensie	Critic	Valoare
basicConstraints	yes	cA: FLASE
keyUsage	yes	digitalSignature nonRepudiation
extKeyUsage	no	clientAuth (1.3.6.1.5.5.7.3.2) emailProtection (1.3.6.1.5.5.7.3.4)
certificatePolicies	no	[1] 0.4.0.194112.1.2 [2] 1.3.6.1.4.1.39965.1.1.1 cPSuri = http://www.transsped.ro/repository
qcStatement	no	Qualified Certificate Statements: id-etsi-qcs-QcCompliance id-etsi-qcs-QcSSCD id-etsi-qcs-QcPDS (location of PKI Disclosure Statements = http://www.transsped.ro/repository)
subjectAltName	no	Other Name / rfc822-Name = <Email Address>
subjectKeyIdentifier	no	automatic
authorityKeyIdentifier	no	= subjectKeyIdentifier of Trans Sped QCA G2

authorityInfoAccess	no	[1]accessMethod: calssuers accessLocation:
---------------------	----	--

7.1.15. End User Mobile QC

Câmpul de date	Valoare	
Versiune	v3	
Număr serial	automatic	
Algoritm de semnare	sha256withRSAEncryption	
Emitent	Atribut	Valoare
	= Subject of Trans Sped Mobile eIDAS QCA G2	
Valabilitate	Up to 3 years	
Subiect	Atribut	Valoare
	CN	<Common Name = First name + Last name>
	G	<First name>
	SN	<Last name>
	SERIALNUMBER	<Personal Identification Code>
	OU	<Organizational Unit> optional
	O	<Organization> optional
Cheia publică subiectului	C	<Country Code>
	a[RSA Key, 2048 Bit]	
Extensie	Critic	Valoare
basicConstraints	yes	cA: FLASE
keyUsage	yes	digitalSignature nonRepudiation
extKeyUsage	no	clientAuth (1.3.6.1.5.5.7.3.2) emailProtection (1.3.6.1.5.5.7.3.4)
certificatePolicies	no	[1] 0.4.0.194112.1.2 [2] 1.3.6.1.4.1.39965.4.1.1 cPSuri = http://www.transsped.ro/repository

qcStatement	no	Qualified Certificate Statements: id-etsi-qcs-QcCompliance id-etsi-qcs-QcSSCD id-etsi-qcs-QcPDS (location of PKI Disclosure Statements = http://www.transsped.ro/repository)
-------------	----	---

7.1.16. Trans Sped Root CA G3

Data Field	Value		
Version	v3		
Serial Number	automatic		
Signature Algorithm	sha256withRSAEncryption		
Issuer	Attribute	Value	Coding
	CN	Trans Sped Root CA G3	PrintableString
	OU	Trans Sped Trust Services	PrintableString
	2.5.4.97	VATRO-12458924	PrintableString
	O	Trans Sped S.A.	PrintableString
	C	RO	PrintableString
Validity	2023 – 2048 (25 years)		
Subject	Attribute	Value	Coding
	CN	Trans Sped Root CA G3	PrintableString
	OU	Trans Sped Trust Services	PrintableString
	2.5.4.97	VATRO-12458924	PrintableString
	O	Trans Sped S.A.	PrintableString
	C	RO	PrintableString
Subject Public Key	[RSA Key, 4096 Bit]		
Extension	Critical	Value	
basicConstraints	yes	cA: TRUE pathLenConstraint: None	
keyUsage	yes	keyCertSign cRLSign	
subjectKeyIdentifier	no	automatic	

7.1.17. Trans Sped Electronic Seal QCA G3

Data Field	Value		
Version	v3		
Serial Number	automatic		
Signature Algorithm	sha256withRSAEncryption		
Issuer	Attribute	Value	Coding
	= Subject of Trans Sped Root CA G3		
Validity	2023 – 2038 (15 years)		
Subject	Attribute	Value	Coding
	CN	Trans Sped Electronic Seal QCA G3	PrintableString
	OU	Trans Sped Trust Services	PrintableString
	2.5.4.97	VATRO-12458924	PrintableString
	O	Trans Sped S.A.	PrintableString
	C	RO	PrintableString
Subject Public Key	[RSA Key, 4096 Bit]		
Extension	Critical	Value	
basicConstraints	yes	cA: TRUE pathLenConstraint: 0	
keyUsage	yes	keyCertSign cRLSign	
certificatePolicies	no	[1] 0.4.0.194112.1.3 (qcp-l-qscd) [2] 1.3.6.1.4.1.39965.5.1.1 cPSuri = http://www.transsped.ro/repository	
subjectKeyIdentifier	no	automatic	
authorityKeyIdentifier	no	= subjectKeyIdentifier of Trans Sped Root CA G3	
authorityInfoAccess	no	[1]accessMethod: calssuers accessLocation: URL= http://www.transsped.ro/cacerts/ts_root_g3.p7c	
cRLDistributionPoints	no	http://www.transsped.ro/crl/ts_root_g3.crl	

7.1.18. Trans Sped QCA G3

Data Field	Value
Version	v3
Serial Number	automatic

Signature Algorithm	sha256withRSAEncryption		
Issuer	Attribute	Value	Coding
	= Subject of Trans Sped Root CA G3		
Validity	2023 – 2038 (15 years)		
Subject	Attribute	Value	Coding
	CN	Trans Sped QCA G3	PrintableString
	OU	Trans Sped Trust Services	PrintableString
	2.5.4.97	VATRO-12458924	PrintableString
	O	Trans Sped S.A.	PrintableString
	C	RO	PrintableString
Subject Public Key	[RSA Key, 4096 Bit]		
Extension	Critical	Value	
basicConstraints	yes	cA: TRUE pathLenConstraint: 0	
keyUsage	yes	keyCertSign cRLSign	
certificatePolicies	no	[1] 0.4.0.194112.1.2 (qcp-n-qscd) [2] 1.3.6.1.4.1.39965.1.1.1 cPSuri = http://www.transsped.ro/repository	
subjectKeyIdentifier	no	automatic	
authorityKeyIdentifier	no	= subjectKeyIdentifier of Trans Sped Root CA G3	
authorityInfoAccess	no	[1]accessMethod: calssuers accessLocation: URL=http://www.transsped.ro/cacerts/ts_root_g3.p7c	
cRLDistributionPoints	no	http://www.transsped.ro/crl/ts_root_g3.crl	

7.1.19. Trans Sped Mobile eIDAS QCA G3

Data Field	Value		
Version	v3		
Serial Number	automatic		
Signature Algorithm	sha256withRSAEncryption		
Issuer	Attribute	Value	Coding
	= Subject of Trans Sped Root CA G3		
Validity	2023 – 2038 (15 years)		

Subject	Attribute	Value	Coding
	CN	Trans Sped Mobile eIDAS QCA G3	PrintableString
	OU	Trans Sped Trust Services	PrintableString
	2.5.4.97	VATRO-12458924	PrintableString
	O	Trans Sped S.A.	PrintableString
	C	RO	PrintableString
Subject Public Key	[RSA Key, 4096 Bit]		
Extension	Critical	Value	
basicConstraints	yes	cA: TRUE pathLenConstraint: 0	
keyUsage	yes	keyCertSign cRLSign	
certificatePolicies	no	[1] 0.4.0.194112.1.2 (qcp-n-qscd) [2] 1.3.6.1.4.1.39965.4.1.1 cPSuri = http://www.transsped.ro/repository	
subjectKeyIdentifier	no	automatic	
authorityKeyIdentifier	no	= subjectKeyIdentifier of Trans Sped Root CA G3	
authorityInfoAccess	no	[1]accessMethod: calssuers accessLocation: URL=http://www.transsped.ro/cacerts/ts_root_g3.p7c	
cRLDistributionPoints	no	http://www.transsped.ro/crl/ts_root_g3.crl	

7.1.20. End User QCA G3

Data Field	Value		
Version	v3		
Serial Number	automatic		
Signature Algorithm	sha256withRSAEncryption		
Issuer	Attribute	Value	Coding
	= Subject of Trans Sped QCA G3		
Validity	1 year		
Subject	Attribute	Value	Coding
	CN	<Common Name = First name + Last name>	PrintableString
	G	<First name>	PrintableString
	SN	<Last name>	PrintableString

	SER	<Personal Identification Code>	PrintableString
	Title	<Title> optional	PrintableString
	OU	<Organizational Unit> optional	PrintableString
	O	<Organization> optional	PrintableString
	C	<Country Code>	PrintableString
Subject Public Key	[RSA Key, 2048 Bit]		
Extension	Critical	Value	
basicConstraints	yes	cA: FLASE	
keyUsage	yes	digitalSignature nonRepudiation	
extKeyUsage	no	clientAuth (1.3.6.1.5.5.7.3.2) emailProtection (1.3.6.1.5.5.7.3.4) Document Signing (1.3.6.1.4.1.311.10.3.12)	
certificatePolicies	no	[1] 0.4.0.194112.1.2 (qcp-n-qscd) [2] 1.3.6.1.4.1.39965.1.1.1 cPSuri = http://www.transsped.ro/repository	
Private CertExtensions	no	Qualified Certificate Statements: id-etsi-qcs-QcCompliance (0.4.0.1862.1.1) id-etsi-qcs-QcSSCD (0.4.0.1862.1.4) id-etsi-qcs-QcType (0.4.0.1862.1.6) id-etsi-qct-esign (0.4.0.1862.1.6.1) id-etsi-qcs-QcPDS (0.4.0.1862.1.5) https://www.transsped.ro/repository EN	
subjectAltNames	no	Other Name / rfc822-Name = <Email Address>	
subjectKeyIdentifier	no	automatic	
authorityKeyIdentifier	no	= subjectKeyIdentifier of Trans Sped QCA G3	
authorityInfoAccess	no	[1]accessMethod: caIssuers accessLocation: URL= http://www.transsped.ro/cacerts/ts_qca_g3.p7c [2]accessMethod: OCSP accessLocation: URI: http://ocsp.transsped.ro/	
cRLDistributionPoints	no	http://www.transsped.ro/crl/ts_qca_g3.crl	

7.1.21. End User Mobile eIDAS QCA G3

Data Field	Value		
Version	v3		
Serial Number	automatic		
Signature Algorithm	sha256withRSAEncryption		
Issuer	Attribute	Value	Coding
	= Subject of Trans Sped Mobile eIDAS QCA G3		
Validity	1 year		
Subject	Attribute	Value	Coding
	CN	<Common Name = First name + Last name>	PrintableString
	G	<First name>	PrintableString
	SN	<Last name>	PrintableString
	SER	<Personal Identification Code>	PrintableString
	Title	<Title> optional	PrintableString
	OU	<Organizational Unit> optional	PrintableString
	O	<Organization> optional	PrintableString
	C	<Country Code>	PrintableString
Subject Public Key	[RSA Key, 2048 Bit]		
Extension	Critical	Value	
basicConstraints	yes	cA: FLASE	
keyUsage	yes	digitalSignature nonRepudiation	
extKeyUsage	no	clientAuth (1.3.6.1.5.5.7.3.2) emailProtection (1.3.6.1.5.5.7.3.4) Document Signing (1.3.6.1.4.1.311.10.3.12)	
certificatePolicies	no	[1] 0.4.0.194112.1.2 (qcp-n-qscd) [2] 1.3.6.1.4.1.39965.4.1.1 cPSuri = http://www.transsped.ro/repository	
Private CertExtensions	no	Qualified Certificate Statements: id-etsi-qcs-QcCompliance (0.4.0.1862.1.1) id-etsi-qcs-QcSSCD (0.4.0.1862.1.4) id-etsi-qcs-QcType (0.4.0.1862.1.6) id-etsi-qct-esign (0.4.0.1862.1.6.1) id-etsi-qcs-QcPDS (0.4.0.1862.1.5) https://www.transsped.ro/repository EN	

subjectAltNames	no	Other Name / rfc822-Name = <Email Address>
subjectKeyIdentifier	no	automatic
authorityKeyIdentifier	no	= subjectKeyIdentifier of Trans Sped Mobile eIDAS QCA G3
authorityInfoAccess	no	[1]accessMethod: calssuers accessLocation: URL=http://www.transsped.ro/cacerts/ts_mqca_g3.p7c [2]accessMethod: OCSP accessLocation: URI: http://ocsp.transsped.ro/
cRLDistributionPoints	no	http://www.transsped.ro/crl/ts_mqca_g3.crl

7.2. Profilul CRL

7.2.1. Numărul (numerele) versiunii

Trans Sped emite CRL X.509 versiunea 2 în conformitate cu RFC 5280, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile". Starea certificatelor este, de asemenea, furnizată prin mecanismul de validare online OCSP.

7.2.2. Extensiile de intrare CRL

Nu există prevederi.

7.2.3. Trans Sped QCA G2 CRL

Parametrii de emitere CRL sunt:

Customer Root PCA	Value
Perioada de emitere CRL	6 hours
Perioada de grație CRL (secunde)	86400 (24 hours)
Generarea automata a unui nou CRL la revocarea certificatelor (5.2) or Generarea CRL în baza motivului de revocare(5.3)	Checked

Include codul ID al Autorității în CRL	Checked (http://www.transsped.ro/crl/ts_qca_g2.crl)
Emiterea extensiei punctului de distribuție (când este necesar – introdusă într-un CDP) CRL, dar nu CRL complet) este critic	Unchecked
Eliminarea emiterea punctului de distribuție din CRL (doar 5.3)	Checked
Include extinderea motivului revocării atunci când motivul nu este specificat	Unchecked
Include codul de instrucțiuni de reținere a intrărilor CRL	Checked

CRL-urile vor avea următoarele câmpuri:

Câmp	Conținut
x.509 Fields	
Versiune	V2
Număr CRL	Allocated automatically
Numele distinct al emitentului	Trans Sped QCA G2
Acest Update	Allocated automatically
Următorul Update	Allocated automatically

7.3. Profilul OCSP

Cererile și răspunsurile OCSP trebuie să fie în conformitate cu RFC 6960.

Administrarea specifică
Informații de contact

TRANS SPED S.A.

Strada Despot Vodă, nr. 38
020656 București
România
Tel: +40 21 210 87 02
Fax: +40 21 211 02 07
www: www.transsped.ro
E-Mail: office@transsped.ro

7.3.1. OCSP responder certificate

Trans Sped QCA G2 OCSP Semnatar

Câmpul de date	Valoare	
Versiune	v3	
Număr serial	Allocated automatically	
Algoritm de semnare	sha256withRSAEncryption	
Emitent	Atribut	Valoare
	CN	Trans Sped QCA G2
	OU	Individual Subscriber CA
	O	Trans Sped SRL
	C	RO
Valabilitate	No longer than 60 days from date of issue	
Subiect	Atribut	Valoare
	CN	Trans Sped QCA G2 OCSP Signer
	OU	Individual Subscriber CA
	O	Trans Sped SRL
	C	RO
Cheia publică subiectului	a[RSA Key, 2048 Bit]	
Extensie	Critic	Valoare
	basicConstraints	yes
keyUsage	yes	Digital Signature (80)
subjectKeyIdentifier	no	Allocated automatically

Authority Info Access	yes	Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://www.transsped.ro/cacerts/ts_gca_g2.crt
OCSP no revocation checking	no	05 00
Enhanced Key Usage	yes	OCSP Signing (1.3.6.1.5.5.7.3.9)
Thumbprint algorithm	no	Sha1
Thumbprint	no	Allocated automatically

7.4. Procedurile de schimbare a specificațiilor

Comitetul de Politici și Practici Trans Sped are autoritatea finală și responsabilitatea pentru specificarea și aprobarea Politicii de Certificare și Codul de Practici și Proceduri. Este responsabil pentru efectuarea unei evaluări (continue) pentru a evalua riscurile de afaceri și determina cerințele de securitate și procedurile operaționale ce vor fi incluse în Politica de Certificare și Codul de Practici și Proceduri.

Trans Sped pune la dispoziția publicului său Codul de Practici și Proceduri/Politica de Certificare (CPP/PC) către toți utilizatorii și părțile de încredere adecvate. Revizuirile la prezentul CPP/PC care au un impact semnificativ asupra utilizatorilor prezentului CPP/PC nu trebuie efectuate retroactiv și vor fi publicate cu cel puțin două săptămâni înainte de intrarea în vigoare.

Revizuirile la prezentul CPP/PC care sunt considerate a avea impact minimal sau deloc asupra semnatarilor și părților de încredere care utilizează certificatele și informațiile legate de starea certificatului emise de Trans Sped pot fi efectuate și înregistrate în depozitar fără a notifica utilizatorii referitor la CPP/PC și fără a schimba numărul versiunii sau data prezentului CPP/PC.

Această versiune a CPP/PC este datată august 2021.

7.5. Politicile de publicare și notificare

În momentul în care prezentul CPP/PC este modificat, iar versiunea modificată este aprobată de către Comitetul de Politici și Practici, acesta va fi publicat în depozitar.

7.6. Procedurile de aprobare a CPP

Documentul CPP/PC este revizuit de și acreditat de Comitetul de Politici și Practici al Trans Sped înainte de a fi publicat în depozitar.

8. AUDITUL DE CONFORMITATE ȘI ALTE EVALUĂRI

Auditul este procesul prin care personal calificat, colectează și evaluează probe pentru a determina gradul de conformitate între măsurile implementate și anumite criterii prestabilite în planul de audit.

Obiectivele auditului sunt:

- evaluarea implementării corespunzătoare a politicilor de certificare;
- verificări extinse asupra politicilor de management al cheilor, controalelor de securitate, politica operațională și profilul certificatului.

8.1. Frecvența auditărilor

Trans Sped este supusă auditurilor externe care se efectuează o dată la doi ani, cu revizuirea conformității între aceste audituri conform prevederilor Regulamentului eIDAS și a Standardelor ETSI EN 319 401. Toate aceste audituri necesită demonstrarea unui nivel maxim de securitate și conformitate cu politicile și practicile documentate.

De asemenea, Trans Sped efectuează propriile audituri interne. Aspectele acoperite de aceste audituri includ verificări ale implementării corespunzătoare a politicilor de certificare Trans Sped și verificări extinse asupra politicilor management-ului cheilor criptografice, controalelor de securitate, politica operațională și verificări cuprinzătoare asupra profilurilor certificatului.

Trans Sped își rezervă dreptul de a efectua inspecții periodice și audituri ale oricăror locații AI pentru a valida că AI operează în conformitate cu practicile de securitate și procedurile prevăzute în prezenta CPP/PC și în documentele interne.

9. ALTE ASPECTE LEGALE

9.1. Taxe

Trans Sped percepe taxe pentru utilizarea anumitor servicii pe care Trans Sped le oferă Semnatarilor săi. O listă actualizată a taxelor poate fi găsită pe site-ul Trans Sped: www.transsped.ro sau solicitată prin email la vanzari@transsped.ro.

9.2. Responsabilitate financiară

9.2.1. Despăgubirea de către părțile de încredere

Pentru ambele tipuri de părți de încredere, contractuale și non-contractuale, reglementările privind despăgubirile din legislația românească și Regulamentul eIDAS sunt obligatorii.

9.2.2. Relații fiduciare

Nicio relație fiduciară între AI, AC, utilizator sau parte de încredere nu este reprezentată de către Trans Sped. Trans Sped nu reprezintă, sau acționează ca agent, fiduciar, sau persoană de încredere a utilizatorului. Trans Sped nu poate fi legat prin nicio obligație în niciun fel de către utilizatori sau părți de încredere și nu va face nicio declarație contradictorie în niciun fel.

9.2.3. Procesele Administrative

Un auditor financiar independent efectuează auditul bilanțului Trans Sped o dată pe an pentru a asigura integritatea financiară și managementul corespunzător al afacerii.

9.3. Confidențialitatea informațiilor de afaceri

Trans Sped păstrează informații confidențiale, colectează, procesează și utilizează datele cu caracter personal conform prevederilor GDPR (Regulamentul 679/2016).

Registrul cu certificate al Trans Sped transmite datele declarate în certificat către toate entitățile care le solicită. Certificatele digitale calificate pot fi obținute doar dacă deținătorul certificatului a fost de acord cu publicarea certificatului.

Trans Sped colectează, prelucrează și utilizează datele personale și legate de organizație doar în măsura în care este necesar și adecvat pentru emiterea unui certificat digital calificat.

Trans Sped nu va transmite datele conținute în certificate către terțe părți în scopuri publicitare și nu va folosi în mod comercial datele obținute în legătură cu o solicitare pentru un certificat.

Trans Sped protejează toate datele personale și legate de organizație care nu sunt incluse în certificat împotriva accesului neautorizat și își rezervă dreptul de a menționa o organizație drept client al său.

9.4. Confidențialitatea datelor personale

În prestarea serviciilor de încredere Trans Sped prelucrează date cu caracter personal ale Subiectului/Beneficiarului în conformitate cu cerințele Regulamentului (UE) nr. 910/2014 și cu respectarea dispozițiilor de drept intern, a Regulamentului nr. 679/2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și al altor dispoziții de drept al Uniunii referitoare la protecția datelor.

Scopul prelucrării datelor cu caracter personal este acela de a presta servicii de certificare.

9.5. Drepturile de proprietate Intelectuală

Perechile de chei criptografice care corespund certificatelor AC Trans Sped sunt proprietatea Trans Sped.

Perechile de chei care corespund certificatelor utilizatorilor sunt proprietatea utilizatorilor care sunt numiți în aceste certificate.

Prezentul CPP/PC reprezintă proprietatea intelectuală a Trans Sped.

9.6. Declarații și garanții

9.6.1. Obligațiile AC

Trans Sped furnizează servicii de încredere pentru certificate digitale calificate în conformitate cu prezentul CPP/PC și în conformitate cu legislația națională, respectiv cu Regulamentul eIDAS.

Trans Sped implementează măsuri și proceduri pentru furnizarea serviciilor de încredere pentru certificate digitale calificate după cum sunt descrise în secțiunile 4 și 5 din prezentul CPP/PC.

Principalul scop al oricărei Autorități de Certificare este de a oferi servicii de management de certificate (generare, utilizare operațională, suspendare, revocare și expirare) pentru clienți în cadrul respectivelor lor domenii de politici.

AC Trans Sped folosește propriile perechi de chei criptografice. Cheia criptografică privată a AC este utilizată pentru a semna certificatele digitale către semnatori.

Cheile criptografice AC Trans Sped pentru emitere de certificate digitale calificate sunt generate într-un Modul de Securitate Hardware certificat (HSM) FIPS 140-1/2 Nivel 3 într-o incintă securizată fizic.

AC Trans Sped pentru certificate digitale calificate îndeplinește următoarele funcții:

1. Generează propriile chei criptografice.
2. Operează într-o manieră eficientă și de încredere și în conformitate cu prezentul CPP/PC și Regulamentul eIDAS.
3. Stabilește Autoritățile de Înregistrare subordonate, dacă e cazul.

4. La primirea cererii autentificate pentru certificat digital emite certificate digitale calificate care întrunesc standardul de certificate X.509, eIDAS, cerințele ETSI EN 319 401 și cerințele solicitării.
5. Se asigură că datele înregistrate în certificatele digitale sunt corecte, lipsite de orice erori și sunt înregistrate corect în baza informațiilor cunoscute de către AC la momentul emiterii.
6. Informează solicitantul cu privire la măsurile necesare pentru a spori securitatea semnăturilor/sigiliilor electronice calificate și pentru a le testa în siguranță.
7. Informează solicitantul că o semnătură electronică calificată are același efect în tranzacțiile legale precum semnătura olografă și este non-repudiabilă.
8. Revocă certificatele la primirea cererilor de revocare autentificate, sau în conformitate cu art. 3.4 sau 4.5 din prezentul CPP/PC.
9. Transmite informațiile de revocare către registru și emite CRLs.
10. Notifică cu promptitudine deținătorul certificatului cu privire la revocare.

În plus, Trans Sped își rezervă dreptul de a investiga compromiterea și compromiterea suspectată a cheilor private, neconformarea sau neconformarea suspectată a prevederilor prezentului CPP/PC în vederea protejării integrității comunității tuturor semnatarilor, și de a lua măsurile pe care le consideră potrivite în baza constatărilor sale.

Investigațiile pot include, fără a se limita:

1. Interviu cu personalul operațional al AI;
2. O revizuire a înregistrărilor sistemului aplicabil, înregistrări operaționale și alte fișiere asociate sau documente, inclusiv e-mail-uri;
3. Un audit al procedurilor operaționale;
4. Un audit al controalelor de securitate, proceduri, și măsuri;
5. Solicitarea de informații.

Aceste drepturi și obligații pot fi adresate în detaliu în acordurile contractuale cu utilizatorii.

9.6.2. Obligațiile AI

O AI este asociată cu una sau mai multe AC și acționează în numele AC. O AI este responsabilă pentru identificarea și înregistrarea utilizatorilor. Acesta efectuează verificarea identității și verificarea tuturor datelor înregistrate în certificatul digital calificat.

Sarcinile unei AI sunt, în special:

- Identificarea și autentificarea solicitanților și terțelor părți.
- Transmiterea de date verificate și complete pentru emiteri certificatele calificate și revocarea certificatului calificat către AC.

- Informarea utilizatorilor referitor la utilizarea corespunzătoare a certificatelor digitale calificate.
- Manipularea dispozitivului securizat de creare de semnături (DSCS) către solicitanți și activarea certificatelor digitale calificate.
- Urmărirea logisticii ciclului de viață al certificatului digital calificat.
- Validarea cererilor de revocare.

Identificarea personală a solicitanților pentru un certificat digital calificat poate avea loc în oricare din AI. Ofițerii mobili ai AI pot identifica și autentifica persoanele la locațiile clientului.

Un Ofițer al AI nu trebuie să-și folosească cheile sale în alt scop în afară de cele asociate cu funcția sa fără permisiunea expresă a Trans Sped. AI trebuie să respecte prevederile din prezentul CPP/PC, cele din ETSI EN 319 401, și cele ale Regulamentului eIDAS; acesta include, dar nu este limitat la asigurarea că cerințele specificate în cap. 4 CPP/PC sunt îndeplinite, și că sunt furnizate controalele definite în art. 5 și art. 6 din prezentul CPP/PC; păstrarea informațiilor confidențiale ale semnatarului în conformitate cu prevederile art. 9.3,4 din prezentul CPP/PC și efectuarea procedurii de autentificare după cum este definită în art. 3 din prezentul CPP/PC.

Orice AI trebuie să aibă angajați calificați corespunzător și de încredere care să fie autorizați pentru a îndeplini îndatoririle AI. Stația de lucru utilizată pentru depunerea informațiilor de înregistrare către Trans Sped nu trebuie să fie public accesibilă, iar comunicarea prin canalele nesecurizate trebuie să fie protejate în mod adecvat.

Trans Sped își rezervă dreptul de a interzice îndeplinirea serviciilor AI în numele Trans Sped, dacă o AI nu se conformează prevederilor stabilite de către Trans Sped.

9.6.3. Obligațiile Semnatarului

Obligațiile Utilizatorului derivă din prevederile Regulamentului eIDAS și/sau din legislația națională.

Se recomandă ca utilizatorii să folosească componentele aplicației pentru semnătură care indică în mod clar producerea unei semnături electronice calificate/sigiliu electronic calificat și permit utilizatorului să identifice datele la care se referă semnătura. Pentru a verifica datele semnate sunt necesare componente sau aplicații de semnare care să arate:

- La ce date se referă semnătura/sigiliul,
- Dacă datele semnate sunt neschimbate,
- Cărui deținător de cod de semnătură/sigiliu îi este asociată semnătura,
- Conținutul certificatului calificat pe care se bazează semnătura/sigiliul, și
- Rezultatele verificării validității ulterioare a certificatelor.

9.6.4. Obligațiile părții de încredere

O parte de încredere va:

- Verifica validitatea sau revocarea certificatului folosind informațiile stării de revocare actuale,

- la în considerare orice limitări legate de utilizarea certificatului indicate părții de încredere din certificat,
- Retine orice alte precauții înscrise în acorduri sau în alt document.

9.6.5. Obligațiile privind depozitarul

Trans Sped își va actualiza depozitarul, constând în politicile relevante, registrul de certificate care pot fi descărcate, și serviciul de verificare a stării certificatului, într-un termen rezonabil de timp, cel puțin o dată în 24 ore, pentru a reflecta noile informații care privesc valabilitatea și siguranța certificatelor emise.

Informația referitoare la revocare este disponibilă public 24 de ore pe zi, 7 zile pe săptămână. La intreruperea sistemului, serviciului sau alți factori care nu se află sub controlul Trans Sped, Trans Sped depune toate eforturile pentru a se asigura că serviciul referitor la starea de revocare nu este indisponibil pentru mai mult decât inevitabil.

Trans Sped protejează integritatea și autenticitatea tuturor sistemelor care furnizează informații legate de starea certificatului.

9.6.6. Răspunderea AC

În calitate de Prestator de Servicii de Încredere Calificat care emite certificate digitale calificate către public, Trans Sped își asumă răspunderea prevăzută de către Regulamentul eIDAS și are obligația de lua măsurile necesare pentru a se asigura că poate să îndeplinească obligațiile statutare pentru rambursarea pagubelor cauzate de o încălcare a obligațiilor.

9.6.7. Răspunderea AI

Asemenea Trans Sped, AI este răspunzătoare doar pentru aspectele care fac parte din sfera sa de responsabilitate. Orice AI care operează în numele Trans Sped are un acord contractual cu Trans Sped. O entitate care intenționează să facă reclamații împotriva unei AI mai întâi trebuie să se adreseze către Trans Sped pentru că:

- (1) un utilizator are un acord contractual cu Trans Sped, nu cu AI, care acționează doar în numele Trans Sped.
- (2) o parte de încredere, în general, nu va cunoaște AI care a comis actul care a condus la reclamația făcută de către partea de încredere.

Trans Sped va investiga faptele și, dacă ajunge la concluzia că nicio greșeală nu poate fi atribuită TSP, trimite reclamația va fi îndreptată către AI relevantă.

9.7. Limitarea responsabilității

Trans Sped nu este responsabil pentru:

- daunele cauzate de forța majoră și/sau cazul fortuit
- utilizarea necorespunzătoare a serviciilor de încredere calificate
- stocarea de date eronate în bazele de date ale STS CA și includerea acestora în certificate digitale emise Utilizatorului în cazul în care Utilizatorul a declarat ca aceste date sunt corecte

- prejudiciile cauzate de furtul sau deteriorarea dispozitivelor criptografice securizate care stochează certificatele digitale
- folosirea neautorizată a acestora sau pentru orice fel de neglijență a Utilizatorului în păstrarea și utilizarea acestora.

De asemenea, Trans Sped nu va fi răspunzător pentru:

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

9.8. Despăgubiri

Trans Sped nu își asumă nicio responsabilitate financiară pentru Certificatele, CRL-urile etc. utilizate în mod necorespunzător sau în scopuri ilicite.

Trans Sped nu răspunde față de nicio persoană (beneficiar, subiect, terț, entitate parteneră etc.) în cazul în care datele prezentate la emiterea certificatelor sunt false, inexacte, incomplete sau expirate sau sunt prezentate acte de identitate false.

9.9. Termeni și încetarea

9.9.1. Termeni

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

9.9.2. Încetarea

CPP rămâne în vigoare până la înlocuirea cu o nouă versiune

9.9.3. Efectul încetării și supraviețurii

Condițiile și efectul care rezultă din încetarea acestui CPP/PC vor fi comunicate prin intermediul siteului web: transsped.ro.

9.10. Notificări individuale și comunicarea cu participanții

Ori de câte ori o parte dorește sau trebuie să notifice orice altă parte cu privire la prezentul CPP/PC, o astfel de notificare va fi transmisă prin e-mail semnat digital sau în scris. Notificarea în scris trebuie să fie livrată fie prin scrisoare recomandată (inclusiv confirmare de primire), sau printr-un serviciu de curierat care confirmă livrarea în scris, și trebuie să fie adresată la:

Trans Sped S.A.
Strada Despot Vodă, nr. 38
020656 București
România

Email: office@transsped.ro

E-mail-ul trebuie să fie confirmat de către destinatar în termen de o săptămână prin e-mail. Dacă expeditorul nu primește o confirmare în cadrul perioadei de timp specificate notificarea trebuie re-trimisă în scris după cum s-a menționat mai sus.

9.11. Amendamente

9.11.1. Separabilitate

Dacă părți din prevederile prezentului CPP/PC sunt inoperative sau nule, acest lucru nu va afecta validitatea celorlalte prevederi.

9.11.2. Supraviețuire

În pofida faptului că prezentul CPP/PC poate în final să nu mai aibă efect, următoarele obligații și limitări ale CPP/PC vor ramane în vigoare: art. 9.6 (Obligații), art. 9.6 (Răspundere), art. 9.2.3. (Procesele Administrative), art. 9.11 (Amendamente) și art. 9.3. (Confidențialitate).

9.11.3. Fuziune

În cazul unei fuziuni, Trans Sped va asigura continuitatea și stabilitatea operării AC cu toate mijloacele rezonabile

9.12. Procedurile de soluționare a litigiilor

Este în interesul Trans Sped în calitate de Prestator de Servicii de Încredere Calificat și terță parte de încredere să soluționeze orice dispută cu promptitudine și în mod eficient. De aceea, orice parte care intenționează să facă reclamații ar trebui să contacteze Trans Sped mai întâi, indiferent de natura reclamației.

Procedurile de soluționare a reclamatilor si disputelor între Trans Sped și Clienți pot fi prevăzute în acordurile între părți sau în acordurile contractuale cu Semnatarii.

În cazul unei dispute, reclamație sau controversă cu privire la prezentul CPP/PC sau orice certificat digital calificat emis de Trans Sped, comunicarea poate fi realizata prin e-mail la: office@transsped.ro. sau la:

Trans Sped S.A.
Strada Despot Vodă, nr. 38
020656 București
România

9.13. Legea aplicabilă

Prezentul CPP se supune legislației naționale aplicabile.

9.14. Conformitate cu legislația aplicabilă

Regulamentul eIDAS și legislația din România vor governa aplicabilitatea, construcția, interpretarea și valabilitatea prezentului CPP/PC și a contractelor asociate.

Reglementările pentru furnizarea de servicii de încredere pentru certificate digitale calificate sunt în particular definite în Regulamentul eIDAS și în legislația din România