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

Versiunea 4.3

Data intrării în vigoare: 20 iunie 2022

Informații generale	
Versiune	*4.3*
Clasificarea informației	*Public*
Aprobat de	*Comitet de Management al Politicilor si Procedurilor*
Data aprobării	*Mai 2022*
Data intrării în vigoare	*Iunie 2022*

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

CUPRINS

1. INTRODUCERE 5
1.1. Vedere de ansamblu 5
1.2. Identificare 6
1.3. Comunitatea și Aplicabilitatea 7
1.4. Detalii de contact 8
2. PREVEDERI GENERALE 9
2.1. Obligații 9
2.2. Răspundere 12
2.3. Responsabilitate financiară 12
2.4. Interpretare și Aplicare 13
2.5. Taxe 14
2.6. Publicarea și Depozitarul 14
2.7. Audit de Conformare 15
2.8. Confidențialitatea 15
2.9. Drepturile de Proprietate Intelectuală 15
3. IDENTIFICARE ȘI AUTENTIFICARE 16
3.1. Înregistrarea inițială 16
3.2. Rutina de acordare a unei chei noi 18
3.3. Acordarea unei alte chei după revocare 19
3.4. Reînnoirea certificatului 19
3.5. Cerere de revocare 19
4. CERINȚE OPERAȚIONALE 20
4.1. Solicitarea unui certificat 20
4.2. Emiterea unui certificat 20
4.3. Acceptarea certificatului 20
4.4. Diseminarea certificatului 21
4.5. Suspendarea,revocarea și reînnoirea unui certificat 21
5. CONTROALELE DE SECURITATE FIZICE, DE PROCEDURĂ ȘI DE PERSONAL 26
5.1. Controale fizice 26
5.2. Controale de procedură 27
5.3. Controale la nivel de personal 28
5.4. Procedurile de registre de audit 28

5.5. Arhivarea înregistrărilor 30
5.6. Schimbarea cheii 30
5.7. Compromiterea și recuperarea după dezastre 30
5.8. Terminarea AC 31
6. CONTROALE DE SECURITATE TEHNICĂ 32
6.1. Generarea și instalarea perechii de chei 32
6.2. Protecția cheii private 34
6.3. Alte aspecte legate de managementul perechii de chei 36
6.4. Datele de activare 37
6.5. Controalele de securitate ale calculatorului 37
6.6. Ciclul de viață al controalelor tehnice 37
6.7. Controalele de Securitate a Rețelei 38
6.8. Controale la nivelul modulului criptografic 38
7. PROFILELE CERTIFICATELOR, CRL ȘI OCSP 39
7.1. Profilul certificatului 39
7.2. Profilul CRL 41
7.3. Profilul OCSP 41
7.4. Procedurile de schimbare a specificațiilor 41
7.5. Politicile de publicare și notificare 42
7.6. Procedurile de aprobare a CPP 42
8. REFERINȚE 43
9. PROFILE CERTIFICATE 44
9.1. Trans Sped Root CA G2 44
9.2. Trans Sped Electronic Seal QCA G2 45
9.3. Trans Sped QCA G2 47
9.4. Trans Sped Mobile eIDAS QCA G2 48
9.5. End User QC 49
9.6. End User Mobile QC 50
9.7. OCSP responder certificate 51
9.8. Trans Sped QCA G2 CRL 53
10. GLOSAR 55

1. INTRODUCERE

Realizarea afacerii şi comunicarea prin reţele publice şi private devin din ce în ce mai importante în comerţul electronic. Una din cerinţele comunicării electronice este abilitatea de a identifica creatorul informaţiei electronice în acelaşi 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 sporeşte semnificativ dacă emiterea unei semnături electronice/sigiliu electronic de către un individ este efectuată de către o terţă parte independentă şi de încredere. Această terţă 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 criptografica publică de entitatea numită în certificat şi care posedă cheia criptografica 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 şi măsuri de protecţie pentru a minimiza ameninţările operaţionale şi financiare şi riscurile asociate cu emiterea de certificate digitale.

Acest document specifică practicile operării şi conducerii Trans Sped AC care emite certificate digitale calificate în conformitate cu Regulamentul (UE) nr. 910/2014 (eIDAS) şi în conformitate cu Specificaţiile tehnice 319 401 ale Institutului pentru Standardele Telecomunicaţiilor 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 si Proceduri (CPP) care descrie practicile pe care o AC le foloseşte în administrarea certificatelor digitale (solicitare, emitere, utilizare, şi revocare);
- o Politică de Certificare (PC) care descrie procesele de verificare şi permite o estimare a încrederii şi siguranţa bazate pe măsura etapelor de verificare întreprinse pentru a verifica conţinutul certificatelor.

Deoarece certificatele digitale calificate au la bază aceleaşi reglementări şi cerinţe definite în Regulamentul eIDAS ambele documente mai sus menţionate (CPP şi PC) au fuzionat într-un singur document, acest CPP/PC.

1.1. Vedere de ansamblu

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 şi trebuie ţinută secretă; cealaltă este publică şi poate fi pusă la dispoziţie pentru a fi disponibila 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 (şi vice versa). Această tehnică poate fi utilizată pentru a implementa semnături digitale sau sigilii electronice: expeditorul criptează datele folosind cheia lui privată, şi destinatarul poate verifica integritatea sa folosind cheia publică corespondentă dintr-un registru de chei publice.

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

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 semnatură electronică si sigilii electronice in conformitate cu Regulamentul eIDAS. Certificatele calificate pot fi folosite pentru a produce semnături electronice calificate si sigilii electronice calificate care sunt în mod legal considerate ca fiind echivalente cu semnăturile olografe. Ca o consecinţă naturală certificatele digitale calificate pentru semnături electronice pot fi emise doar către persoane fizice în nume propriu sau în beneficiul unei organizatii. 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 siguranţei certificatelor digitale calificate emise şi pentru a dovedi respectarea Regulamentului eIDAS şi în conformitate cu cerinţele ETSI EN 319 401, Trans Sped publică prezentul CPP/PC în care sunt descrise procedurile folosite pentru emiterea de certificate digitale calificate precum şi descrierea modului în care este efectuată verificarea datelor conţinute în certificat.

Prezentul CPP/PC descrie structura şi practicile Trans Sped. Nu constituie nici o declaraţie de self-escrow, nici nu declară garanţiile legale.

Prezentul CPP/PC se foloseşte în mare măsură de vocabularul legat de domeniul semnăturilor digitale, sigiliilor electronice şi a certificatelor, criptografie şi criptarea cheii publice, la care se face referire în GLOSAR (Capitolul 10). De asemenea, glosarul oferă definiţiile unor termeni importanţi care nu mai apar în altă parte în acest text şi care au legătură cu domeniile mai sus menţionate.

1.2. Identificare

Trans Sped S.A. cu sediul în strada Despot Vodă, nr. 38, 020656 Bucureşti, România (denumită “Trans Sped” sau “TSP” în aceast CPP/PC), este un Prestator de Servicii de Încredere Calificat, iar serviciile furnizate sunt calificate şi se regăsesc în Lista de Încredere (Trusted List) a statului membru UE, în cazul nostru România, in conformitate cu prevederile Regumanentului eIDAS.
https://esignature.ec.europa.eu/efda/tl-browser/#/screen/tl/RO/1
Prezentul CPP/PC este pus la dispoziţie 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

1.3. Comunitatea și Aplicabilitatea

Acest CPP/PC se aplica certificatelor digitale calificate pentru semnatura electronica si sigiliu electronic care:

a) întrunesc cerinţele prevăzute din Regulamentul eIDAS;

b) sunt emise de către TSP cu respectarea cerinţelor prevăzute în Regulamentul eIDAS;

c) sunt destinate pentru a fi utilizate doar cu dispozitive securizate de creare a semnăturii electronice (DSCS) care întrunesc condiţiile prevăzute in Regulamentul eIDAS;

d) sunt emise către public.

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 crează 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 acelaşi timp să folosească furnizori de servicii externi ca AI subsidiare responsabile pentru verificarea atât a informaţiilor de afaceri cât şi a datelor personale incluse în certificatul digital al utilizatorului.

Orice AI subsidiară este din punct de vedere contractual legată de Trans Sped. Ofiţerii de Înregistrare ai unei asemenea AI subsidiare sunt identificaţi individual; aceştia detin certificate speciale de Ofiţer de Înregistrare (RO). Doar informaţiile 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 miloace video cu operator uman sau automat conform Norma ADR din 2021 privind reglementarea, recunoaşterea, aprobarea sau acceptarea procedurii de identificare a persoanei la distanţă 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.

1.3.4. Aplicabilitatea

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

Prezentul CPP/ PC defineste certificatele digitale:

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

1.4. Detalii de contact

1.4.1. Specificarea organizării si administrării

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.

2. PREVEDERI GENERALE

Acest capitol descrie obligaţiile şi răspunderea AC Trans Sped, a AI, semnatarilor şi ale părţilor de încredere. Obligaţiile şi răspunderea sunt guvernate de Regulamentul eIDAS şi de acordurile mutuale efectuate de către părţile mai sus menţionate.

2.1. Obligații

2.1.1. Obligațiile AC

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

Trans Sped implementează măsuri şi 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 Autorităţi de Certificare este de a oferi servicii de management de certificate (generare, utilizare operaţională, suspendare, revocare şi expirare) pentru clienţi în cadrul respectivelor lor domeniu(ii) de politici.

AC Trans Sped foloseşte propriile perechi de chei criptografice. Cheia criptografica privată a AC este utilizată pentru a semna certificatele digitale către semnatari.

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 îndeplineşte următoarele funcţii:

1. Generează propriile chei criptografice.
2. Operează într-o manieră eficace şi de încredere şi în conformitate cu prezentul CPP/PC și Regulamentul eIDAS.
3. Stabileşte Autorităţile 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, cerinţele ETSI EN 319 401 şi cerinţele solicitarii.
5. Se asigură că datele inregistrate in certificatele digitale sunt corecte, lipsite de orice erori şi sunt inregistrate corect în baza informaţiilor cunoscute de către AC la momentul emiterii.
6. Informează solicitantul cu privire la măsurile necesare pentru a spori securitatea semnăturilor/sigiliilor electronice calificate şi pentru a le testa în siguranţă.
7. Informează solicitantul că o semnătură electronică calificată are acelaşi efect în tranzacţiile legale precum semnătura olografă si este non-repudiabila.
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 informaţiile de revocare către registru şi emite CRLs.
10. Notifică cu promptitudine deţinătorul certificatului cu privire la revocare.

În plus, Trans Sped îşi rezervă dreptul de a investiga compromiterea şi compromiterea suspectată a cheilor private, neconformarea sau neconformarea suspectată a prevederilor prezentului CPP/PC în vederea protejării integrităţii comunităţii tuturor semnatarilor, şi de a lua masurile pe care le consideră potrivite în baza constatărilor sale.

Investigaţiile pot include, fără a se limita:

1. Interviuri cu personalul operaţional al AI;
2. O revizuire a înregistrărilor sistemului aplicabil, înregistrări operaţionale şi alte fişiere asociate sau documente, inclusiv e-mail-uri;
3. Un audit al procedurilor operaţionale;
4. Un audit al controalelor de securitate, proceduri, şi măsuri;
5. Solicitarea de informaţii.

Aceste drepturi şi obligaţii pot fi adresate în detaliu în acordurile contractuale cu utilizatorii.

2.1.2. Obligațiile AI

O AI este asociată cu una sau mai multe AC şi acţionează în numele AC. O AI este responsabilă pentru identificarea si înregistrarea utilizatorilor. Acesta efectuează verificarea identităţii şi verificarea tuturor datelor inregistrate in certificatul digital calificat.

Sarcinile unei AI sunt, în special:

- Identificarea şi autentificarea solicitanţilor şi terţelor părţi.
- Transmiterea de date verificate şi complete pentru emitere certificatului calificat şi revocarea certificatului calificat căte AC.
- Informarea utilizatorilor referitor la utilizarea corespunzătoare a certificatelor digitale calificate.
- Manipularea dispozitivului securizat de creare de semnături (DSCS) către solicitanţi şi activarea certificatelor digitale calificate.
- Urmărirea logisticii ciclului de viaţă al certificatului digital calificat.
- Validarea cererilor de revocare.

Identificarea personală a solicitanţilor pentru un certificat digital calificat poate avea loc în oricare din AI. Ofiţerii mobili ai AI pot identifica şi autentifica persoanele la locaţiile clientului.

Un Ofiţer al AI nu trebuie să-şi folosească cheile sale în alt scop în afară de cele asociate cu funcţia sa fără permisiunea expresă a Trans Sped. AI trebuie să respecte prevederile din prezentul CPP/PC, cele din ETSI EN 319 401, şi cele ale Reulamentului eIDAS; acesta include, dar nu este limitat la asigurarea că cerinţele specificate în cap. 1 CPP/PC sunt îndeplinite, şi că sunt furnizate controalele definite în art. 1 şi art. 6 din prezentul CPP/PC; păstrarea informaţiilor

confidenţiale ale semnatarului în conformitate cu prevederile art. 2.8 din prezentul CPP/PC şi efectuarea procedurii de autentificare după cum este definită în art. 3 din prezentul CPP/PC.

Orice AI trebuie să aibă angajaţi calificaţi corespunzător şi de încredere care să fie autorizaţi pentru a îndeplini îndatoririle AI. Staţia de lucru utilizată pentru depunerea informaţiilor 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 îşi rezervă dreptul de a interzice îndeplinirea serviciilor AI în numele Trans Sped, dacă o AI nu se conformează prevederilor stabilite de către Trans Sped.

2.1.3. Obligațiile Semnatarului

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

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

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

2.1.4. Obligațiile părții de încredere

O parte de încredere va:

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

2.1.5. Obligațiile privind depozitarul

Trans Sped îşi va actualiza depozitarul, constând in politicile relevante, registrul de certificate care pot fi descărcate, şi serviciul de verificare a stării certificatului, într-un termen rezonabil de timp, cel puţin o dată în 24 ore, pentru a reflecta noile informaţii care privesc valabilitatea şi siguranţa certificatelor emise.

Informaţia referitoare la revocare este disponibilă public 24 de ore pe zi, 7 zile pe săptămână. La intreruperea sistemului, serviciului sau alţi 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 şi autenticitatea tuturor sistemelor care furnizează informaţii legate de starea certificatului.

2.2. Răspundere

2.2.1. Răspunderea AC

În calitate de Prestator de Servicii de Încredere Calificat care emite certificate digitale calificate către public, Trans Sped isi asuma raspunderea prevazuta de catre Regulamentul eIDAS si are obligaţia de lua masurile necesare pentru a se asigura că poate să îndeplinească obligaţiile statutare pentru rambursarea pagubelor cauzate de o încălcare a obligațiilor.

2.2.2. 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 intenţionează să facă reclamaţii 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 acţionează doar în numele Trans Sped.

(2) o parte de încredere, în general, nu va cunoaşte AI care a comis actul care a condus la reclamaţia făcută de către partea de încredere.

Trans Sped va investiga faptele şi, dacă ajunge la concluzia că nicio greşeală nu poate fi atribuită TSP, trimite reclamatia va fi indreptata către AI relevantă.

2.3. Responsabilitate financiară

2.3.1. Despăgubirea de către părțile de încredere

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

2.3.2. Relații fiduciare

Nicio relaţie fiduciară între AI, AC, utilizator sau parte de încredere nu este reprezentată de către Trans Sped. Trans Sped nu reprezintă, sau acţionează ca agent, fiduciar, sau persoană de încredere a utilizatorului. Trans Sped nu poate fi legat prin nicio obligaţie în niciun fel de către utilizatori sau părţi de încredere si nu va face nicio declaraţie contradictorie în niciun fel.

2.3.3. Procesele Administrative

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

2.4. Interpretare și Aplicare

2.4.1. Legea care guvernează

Regulamentul eIDAS și legislația din România vor guverna 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.

2.4.2. Separabilitate, supraviețuire, fuziune, notificare

2.4.2.1. Separabilitate

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

2.4.2.2. 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 in vigoare: art. 2 (Obligații), art. 14 (Răspundere), art. 2.3.3. (Procesele Administrative), art. 2.4. (Interpretare și Aplicare) și art. 2.8. (Confidențialitate).

2.4.2.3. Fuziune

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

2.4.2.4. Notificare

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

Trans Sped S.A.
Strada Despot Vodă, nr. 38
020656 Bucureşti
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 primeşte o confirmare în cadrul perioadei de timp specificate notificarea trebuie re-trimisă în scris după cum s-a menţionat mai sus.

2.4.3. Procedurile de soluționare a disputelor

Este în interesul Trans Sped în calitate de Prestator de Servicii de Încredere Calificat şi terţă parte de încredere să soluţioneze orice dispută cu promptitudine şi în mod eficient. De aceea, orice parte care intenţionează să facă reclamaţii ar trebui să contacteze Trans Sped mai întâi, indiferent de natura reclamaţiei.

Procedurile de soluţionare a reclamatilor si disputelor între Trans Sped şi Clienţi pot fi prevăzute în acordurile între părţi sau în acordurile contractuale cu Semnatarii.

În cazul unei dispute, reclamaţie 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 Bucureşti
România

2.5. 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 solicitata prin email la vanzari@transsped.ro .

2.6. Publicarea și Depozitarul

2.6.1. Publicarea informațiilor AC

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

Registrul tuturor certificatelor digitale calificate accesibile şi 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 deţinătorul certificatului este de acord cu publicarea certificatului.

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

2.6.2. Frecvența publicării

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

CRL-urile sunt actualizate la fiecare douăzeci şi patru (24) de ore. Baza de date care furnizează informaţiile stării certificatelor digitale calificate este actualizată de fiecare dată când un certificat este eliberat sau revocat. Orice alte informaţii prevazute în art 2.6.1 sunt actualizate de fiecare dată când sunt modificate.

2.6.3. Controlul accesului

Doar personalul autorizat poate publica sau modifica orice informații la care se face referire în art. 2.6.1.

2.6.4. Depozitarele

Pentru locația depozitarului de certificate și CPP/PC a se consulta art. 2.6.1.

2.7. Audit de Conformitate

Trans Sped este supusă auditurilor externe care se efectuează o dată la doi ani, cu revizuirea conformității între aceste audituri conform prevederilor Regulamentului eIDAS si a Standardelor ETSI EN 319 401. Toate aceste audituri necesită demonstrarea unui nivel maxim de securitate şi conformitate cu politicile şi 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 şi verificări extinse asupra politicilor management-ului cheilor criptografice, controalelor de securitate, politica operațională şi verificări cuprinzătoare asupra profilurilor certificatului.

Trans Sped îşi rezervă dreptul de a efectua inspecţii periodice şi audituri ale oricăror locaţii AI pentru a valida că AI operează în conformitate cu practicile de securitate şi procedurile prevăzute în prezenta CPP/PC şi în documentele interne.

2.8. Confidențialitatea

Trans Sped păstrează informaţii confidenţiale, 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 entităţile care le solicită. Certificatele digitale calificate pot fi obţinute doar dacă deţinătorul certificatului a fost de acord cu publicarea certificatului.

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

Trans Sped nu va transmite datele conţinute în certificate către terţe părţi în scopuri publicitare si nu va folosi în mod comercial datele obţinute în legătură cu o solicitare pentru un certificat.

Trans Sped protejează toate datele personale şi legate de organizaţie care nu sunt incluse în certificat împotriva accesului neautorizat si îşi rezervă dreptul de a menţiona o organizaţie drept client al său.

2.9. 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 numiţi în aceste certificate.

Prezentul CPP/PC reprezintă proprietatea intelectuală a Trans Sped.

3. IDENTIFICARE ȘI AUTENTIFICARE

3.1. Înregistrarea inițială

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

Trans Sped se asigură că utilizatorii sunt identificaţi şi autentificaţi în mod corespunzător şi că solicitarile de certificat sunt complete, corecte şi legal autorizate. Înainte ca un certificat digital calificat să fie emis, Trans Sped informează semnatarul referitor la termenele şi condiţiile 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 şi în conformitate cu eIDAS si a Standardelor ETSI EN 319 401, identitatea şi, 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.

3.1.1. 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 şi alte reglementări. Numele trebuie să aibă semantică comun înţeleasă (prenume şi nume, numele societăţii, adresa de e-mail) pentru ca partea de încredere să determine identitatea persoanei şi / sau organizaţiei. În orice caz, solicitantul îşi poate alege un pseudonim în locul numelui în certificatul digital calificat. Trans Sped va emite asemenea certificate pseudomizate; folosirea pseudonimului este indicată prin sufixul “:PN” în spaţiul Nume Comun al certificatului.

3.1.3. Regulile pentru interpretarea unor diferite forme de nume

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

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 toţi utilizatorii Trans Sped de certificate digitale calificate. Dacă e cazul, Trans Sped poate ataşa numere sau litere adiţionale la numele real pentru a asigura unicitatea numelui. Aceeaşi entitate poate avea certificate diferite toate purtând acelaşi ND subiect dar două entităţi separate nu pot împărţi un ND comun (şi să fie emis de aceeaşi AC). În orice caz, nu trebuie să existe două certificate X.509 care au acelaşi emitent ND şi număr serial.

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, autenticitatea și rolul mărcilor comerciale

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

3.1.7. 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 criptografica 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 criptografica 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 criptografica publică a subiectului.

Dacă Trans Sped generează în incinta sa cheia criptografica 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.

3.1.8. Autentificarea identității organizației

Dacă solicitantul este o persoană care este identificată în legătură cu o persoană juridică sau altă entitate organizaţională, pe lângă datele din art. 3.1.9 va fi dovedita existenta persoanei juridice sau entitatii organizationale. Această verificare poate fi efectuată prin prezentarea unei copii a unui document, care dovedeşte existenţa organizaţiei (extrasul actual al unui registru oficial competent în care organizaţia este listată sau un document comparabil).

Autorităţile guvernamentale sau administrative trebuie să furnizeze documentele care reflectă relaţia lor cu următoarea entitate superioar ierarhica (de ex: autoritate superioară) cu antet oficial, semnată de catre un funcţionar autorizat.

Documentaţia trebuie să cuprindă:

- Numele complet şi statutul legal al persoanei juridice asociate sau altă entitate organizaţională,

- Informaţii de înregistrare existente relevante (de ex: înregistrarea societăţii) a persoanei juridice asociate sau altă entitate organizaţională.

3.1.9. 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 si ETSI EN 319 411-2. Dovada identităţii 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 şi prenumele),
- Data şi locul naşterii,
- Un număr de serie sau alte atribute care pot fi folosite pentru a distinge persoana din alte persoane cu acelaşi nume
- Un numar de telefon mobil

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

Dacă utilizatorul este o persoană care este identificată în legătură cu o persoană juridică sau altă entitate organizaţională în completarea datelor din art. 3.1.8 dovezile următoare vor fi furnizate:

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

3.1.10. Informațiile neverificate ale abonatului

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

3.2. Rutina de acordare a unei chei criptografice noi

Acordarea unei chei criptografice noi presupune schimbarea cheii criptografice publice pentru un certificat existent prin emiterea unui nou certificat cu o cheie criptografica publică diferită. Numele certificatului rămâne acelaşi. Acest proces este diferit de cel de reînnoire care presupune emiterea unui nou certificat, cu o perioadă de valabilitate prelungită, pentru aceeaşi cheie criptografica publică. (A se vedea [RFC4949].)

În momentul în care cheile criptografice trebuie schimbate, utilizatorii sunt notificaţi prin e-mail. Schimbarea cheii criptografice în cazul certificatelor care nu au expirat încă, poate fi solicitata 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 aceleasi credentiale folosite pentru a activa utilizarea cheii criptografice private.

Obţinerea unei noi chei criptografice în cazul în care certificatul a expirat se face folosind aceleaşi reguli ca şi la înregistrarea iniţială.

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

3.3. Acordarea unei alte chei criptografice după revocare

După ce un certificat a fost revocat, utilizatorul trebuie să solicite un nou certificat conform prevederilor art. 3.1. avand in vedere ca perechea de cheie criptografice revocată nu este eligibilă pentru a semna şi autentifica o cerere de acordare a unei noi chei criptografice (a se vedea art. 3.2).

3.4. Reînnoirea certificatului digital calificat

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 numar de telefon).

3.5. Cerere de revocare si suspendare a certificatului digital calificat

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

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

4. CERINȚE OPERAȚIONALE

4.1. Solicitarea unui certificat digital calificat

Pentru obtinerea unui certificat digital calificat un utilizator solicita către Trans Sped emiterea certificatului si urmează procedura descrisă în prezentul CPP/PC sau în descrierile Trans Sped pentru solicitarea unui certificat digital calificat. Trans Sped poate aproba sau respinge aceste solicitari.

Perechea de chei criptografice poate fi generată într-un mediu securizat de catre 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 urmatoarele:

- Declaraţia că informaţiile furnizate sunt corecte;
- Acordul la obligaţiile utilizatorului;
- Acordul la publicarea certificatului în depozitar.
- Acordul GDPR
- Termeni si Conditii Trans Sped

4.2. Emiterea unui certificat digital calificat

Trans Sped verifică corectitudinea şi valabilitatea tuturor datelor necesare pentru emiterea unui certificat digital calificat (a se compara art. 3.1.8 şi art. 3.1.9) conform prevederilor Regulamentului eIDAS. La finalul procesului Trans Sped fie va emite utilizatorului certificatul digital calificat, fie il va informa referitor la orice probleme sau inadvertenţe.

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

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

4.3. Acceptarea certificatului digital calificat

La primirea unui certificat digital calificat, utilizatorul trebuie să verifice datele inregistrate in certificat. Dacă certificatul conţine greşeli care nu pot fi acceptate de către utilizator, acesta trebuie să informeze Trans Sped fără întârziere. Trans Sped va revoca certificatul şi va lua măsurile care se impun fie de a restitui preţul certificatului fie de a emite un certificat nou cu informatiile corecte.

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

4.4. Diseminarea certificatului digital calificat

Certificatele digitale calificate sunt publicate in depozitarul Trans Sped pentru a fi puse la dispoziția terțelor părți, doar cu acordul utilizatorului.

4.5. Suspendarea, revocarea și reînnoirea unui certificat digital calificat

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 situaţiei. Dacă posesorul certificatului digital calificat are certitudini privind pierderea sau compromiterea cheii criptografice private, sau dacă datele inregistrate în certificat s-au schimbat în mod substanţial, 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 şi data revocării vor fi incluse în Lista Certificatelor Revocate, iar investigaţii legate de starea ulterioara la depozitarul certificatelor vor conducere la citarea certificatului drept invalid.

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

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

4.5.1. Circumstanțe pentru revocarea certifiactului digital calificat

Un certificat digital calificat este revocat în urmatoarele situatii:

1. Posesorul sau o terţă parte autorizată a depus o cerere de revocare;
2. Trans Sped a aflat că au fost furnizate informaţii 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 şi niciun alt furnizor de servicii de certificare nu mai poate continua serviciile de certificare ale Trans Sped;

Ori de câte ori apare una din situatiile de mai sus, certificatul asociat trebuie revocat și plasat intr-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.

4.5.2. Cine poate solicita revocarea unui certificat digital calificat

Posesorul certificatului sau înlocuitorul său pot solicita revocarea.

Dacă un certificat digital prevede că deţinătorul lui poate acţiona în numele unei terţe părţi, această parte poate de asemenea solicita revocarea certificatului. Orice entitate sau terţă parte care au confirmat orice informaţii cuprinse în certificat are dreptul să revoce certificatul respectiv.

Oricine poate informa Trans Sped referitor la faptul că informaţiile dintr-un certificat nu sunt, sau nu mai sunt corecte. Dupa primirea informatiilor Trans Sped va verifica dacă o revocare este corespunzătoare conform art. 4.5.1. 2.

4.5.3. Procedura pentru cererea de revocare a certificatelor digitale

Revocarea certificatului digital calificat se poate realiza in urmatoarele modalitati:

1. Posesorul sau o terţă parte autorizată solicita revocarea unui certificat digital calificat prin completarea şi semnarea unui formular de revocare în faţa Ofiţerului de Înregistrare. Autentificarea este furnizată de semnătura olografa.
2. Posesorul sau o terţă parte autorizată solicita 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 revoca 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 şi patru (24) de ore după primirea cererii.

4.5.4. Perioada de revocare a certificatului digital calificat

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

4.5.5. Circumstanțele suspendării certificatului digital calificat

Un certificat digital calificat este suspendat în urmatoarele situatii:

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

4.5.6. 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 acţiona în numele unei terţe părţi, această terta parte poate solicita suspendarea certificatului. Orice entitate sau terţă parte care au confirmat orice informaţii cuprinse în certificat are dreptul să solicite suspendarea certificatului respectiv.

Oricine poate informa Trans Sped referitor la faptul că informaţiile dintr-un certificat s-ar putea să nu fie corecte. Trans Sped va verifica dacă este necesar o suspendare conform art. 4.5.5, 6.

4.5.7. Procedura pentru suspendarea certificatului digital calificat

Solicitarea pentru suspendarea unui certificat digital calificat se poate realiza in urmatoarele modalitati:

1. Posesorul sau o terţă parte autorizată poate solicita suspendarea unui certificat digital calificat prin completarea şi semnarea unui formular de suspendare în faţa Ofiţerului de Înregistrare. Autentificarea este furnizată de semnătura olografa.
2. Posesorul sau o terţă 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 in 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 şi patru (24) de ore după primirea solicitarii.

4.5.8. Limitele perioadei de suspendare a certificatului digital calificat

Un certificat digital calificat poate fi suspendat pentru maxim şapte (7) zile. Posesorul unui certificat digital poate solicita suspendarea acestuia maxim de 2 ori in perioada de valabilitate a certificatului. Depasirea numarului de suspendari sau a perioadei atrag după sine revocarea certificatului.

4.5.9. Procedura de reînnoire a certificatului digital calificat

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

1. Solicitarea reînnoirii certificatului digital calificat în cloud este efectuata 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 reinnoirea online a certificatului digital calificat trebuie sa fie respectate urmatoarele conditii:

- Posesorul detine un certificat digital calificat activ;
- Autentificarea in portalul Trans Sped de administrare al certificatului este realizata folosind credentialele certificatului activ;

- Informațiile care au fost utilizate pentru emiterea certificatului initial: nume, prenume, numar 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.

4.5.9.2. 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 daca informațiile din certificatul initial: nume, prenume, numar 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 certifcatului care urmează să expire și pentru care se realizează reînnoirea;
- Codul PIN asociat dispozitiviului criptografic trebuie să fie cunoscut de catre titular, iar dispozivitul 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 descries în art. 3.1.9. și 4.2.

4.5.10. Frecvența emiterii de CRL

Frecvenţa emiterii de CRL va ficel putin la fiecare douăzeci şi 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.

4.5.11. Cerințele de verificare ale CRL

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

4.5.12. 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 şi / sau parte de încredere.

4.5.13. Cerințele de verificare a revocării on-line

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

4.5.14. Alte forme de înștiințare de revocare disponibile

Nu există prevederi.

4.5.15. Cerințele de verificare pentu alte forme de înștiințare de revocare

Nu există prevederi.

4.5.16. Cerințe speciale privind compromiterea cheii criptografice private

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

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

Trans Sped are obligativitatea de a stabili şi menţine starea controalelor de securitate solicitate de către AC şi 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 şi Standardele ETSI EN 319 401. Prevederile respective se completează unele pe celelalte şi 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 confidentiale.

5.1. Controale fizice

Nivelul controalelor de securitate fizică restricţionează accesul la sistemele sensibile, hardware şi software, utilizate pentru efectuarea operaţiunilor critice ale AC, care au loc în cadrul unei locaţii sigure din punct de vedere fizic. Aceste sisteme sunt separate din punct de vedere fizic de alte sisteme ale organizaţiei astfel incat numai angajaţii autorizaţi 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 funcţional şi utilizează carduri de acces în combinaţie cu parole pentru acces. Se păstrează un registru în care sunt înregistrate toate intrările fizice in zonele restricţionate.

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 cerinţele prevazute in legislația privind semnătura electronică din România și Regulamentul eIDAS. Orice acces neautorizat la informaţia depozitată, posibil provenind din pierderea, falsificarea, sau utilizarea greşită a acestora este împiedicată prin mijloace corespunzătoare. Verificările de securitate regulate sunt efectuate pentru a se asigura că aceste controale funcţionează corespunzător.

Accesul la orice zonă fizică unde sunt amplasate informaţii sau echipament sensibil la operaţiunile AC necesită ca cel puţin două persoane autorizate să aibă acces la respectivele locaţii. Intrarea în zonele restricţionate folosind același dispozitiv token de două ori (pentru a sustrage cerinţa a două persoane diferite care au acces la respectiva locaţie) 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 şi nu poate fi operat prin LAN sau WAN, ci doar de la consolă. Sistemele computerizate care furnizează registrul şi serviciile depozitare pot fi administrate doar de la consolă sau printr-un protocol de reţea sigur. Accesul la sistemele sensibile necesită prezenţa a două persoane (sau log on) în acelaşi timp.

Toate sistemele AC au energie electrică de industrie standard şi sisteme de aer condiţionat care să ofere un mediu de operare corespunzător. Toate sistemele AC au precauţii rezonabile luate

pentru a minimiza impactul expunerii la apă si au mecanisme standard de prevenire a incendiilor şi de protecţie în locaţie.

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

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

AI nu stochează niciodată informaţiile legate de cheia semnatarului.

5.2. Controale de procedură

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

Responsabilităţile de management formale şi proceduri existente au scopul de a controla toate modificările la echipamentul AC, software, şi proceduri de operare. Responsabilitatile şi ariile de răspundere sunt segregate pentru a reduce oportunităţile pentru modificarea neautorizată sau utilizarea greşită a informaţiilor sau serviciilor. Acest lucru se realizează, de exemplu, prin definirea diferitelor roluri astfel încât efectuarea anumitor sarcini esenţiale 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 solicitari 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

Facilităţile de dezvoltare şi testare sunt din punct de vedere fizic separate de facilităţile operaţionale. Procedurile există şi sunt urmate pentru raportarea defectărilor software-ului, pentru a se asigura că neregulile sunt raportate şi sunt luate acţiunile corective. Utilizatorii de sisteme de AC trebuie să observe şi să raporteze slăbiciunile observate sau suspectate şi ameninţările la sisteme sau servicii. Documentaţia sistemului este protejată împotriva accesului neautorizat.

Cererile de capacitate sunt monitorizate precum si proiecţiile cerinţelor de capacitate viitoare sunt menite să asigure că puterea de procesare necesară şi de depozitare sunt întotdeauna disponibile.

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

Există o procedură de raportare formală şi este urmată, împreună cu o procedură de răspuns în caz de incident, prezentând acţiunea ce va fi luată la primirea unui raport legat de existenţa unui incident. Responsabilităţile şi procedurile de management ale unui incident există şi sunt urmate pentru a asigura un răspuns rapid, eficace şi 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 şi revocarea certificatelor digitale calificate, precum şi datele şi informaţiile legate de administrare sunt integre, de încredere şi loiale. Acest lucru include, dar fără a se limita la solicitarea unui certificat emis de către poliţie, declararea că persoana în cauză nu are cazier de niciun fel. Întregul personal trebuie să aibă cunoştinţele şi experienţa necesare legate de operaţiunile AC şi trebuie să fi demonstrat seriozitate şi cunoaşterea legată de securitate referitoare la îndatoririle sale la Trans Sped. Au loc evaluari periodice pentru a verifica încrederea întregului personal.

Niciun utilizator neautorizat nu are acces la sistemele care stochează datele sensibile. Toate sistemele care stochează asemenea informaţii 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.

Angajaţii semnează un contract de confidenţialitate (nedivulgare) ca parte din termenii şi condiţiile iniţiale de angajare. Toţi angajaţii organizaţiei şi, unde este cazul, utilizatorii terţe părţi primesc pregătire profesională adecvată în politicile şi procedurile organizaţionale.

Există şi este urmat un proces disciplinar formal pentru angajaţii care au încălcat politicile şi procedurile de securitate organizaţionale. Politicile şi procedurile Trans Sped specifică sancţiunile împotriva personalului pentru acţiunile neautorizate, folosirea neautorizată de autoritate şi folosirea neautorizată a sistemelor.

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

5.4. Procedurile de registre de audit

Trans Sped păstrează rapoarte de audit şi fişiere ale sistemului de înregistrare care documentează acţiunile întreprinse ca parte din serviciile de incredere 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, fişierele raportului de audit sunt salvate pe medii de tip WORM. Fişierele raportului de audit sunt arhivate de către un administrator de sistem săptămânal (cel puţin). Jurnalele de evenimente sunt revizuite cel puţin săptămânal de către auditorii interni.

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

Pentru informaţii suplimentare legate de cerinţele şi procedurile de audit extern şi intern, vezi art. 2.7.

5.5. Arhivarea înregistrărilor

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

Trans Sped utilizează arhivarea internă şi externă pentru a împiedica pierderea documentelor importante sau a datelor digitale. Arhivele sunt amplasate în locaţii diferite (interne sau externe) şi protejate de sistemele de control ale accesului. In general, rapoartele privind certificatele digitale calificate sunt reţinute cel puţin zece (10) ani si 6 (sase) luni conform prevederilor legislatiei nationale si a Regulamentului eIDAS. Nicio persoană singură nu poate modifica sau distruge materialul arhivat, iar accesul la acesta este strict restricţionat.

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 şi algoritmii criptografici, ţinând cont de potrivirea algoritmilor şi parametrilor pentru a compensa noile descoperiri în ştiinţă şi/sau tehnologie. Orice AC nouă poate fi pusă la dispoziţie 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 operaţiunile 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 defineşte 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 cerinţele de valabilitate ale serviciului specific şi 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 informaţii esenţiale şi sistemul software al AC sunt operate în fiecare zi. Procedurile de recuperare în caz de dezastre sunt testate cu regularitate. Documentaţia referitoare la aceste proceduri este considerată confidenţială.

5.8. Terminarea AC

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

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

Dacă niciun furnizor de servicii de incredere 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 documentaţia 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 notificaţi dacă Trans Sped întreprinde o asemenea acţiune.

6. CONTROALE DE SECURITATE TEHNICĂ

6.1. Generarea și instalarea perechii de chei

6.1.1. Generarea perechii de chei

6.1.1.1. Generarea perechii de chei AC

Cheia criptografica 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 prezenţa şi semnată de o terţă parte neimplicată în generarea de cheie propriu-zisă.

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

Generarea de software şi / 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 criptografica privată temporar pe suport magnetic media pentru că cheile pentru certificate digitale calificate sunt generate în interiorul HSM.

6.1.1.2. 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 locaţii securitate. Nicio copie a cheilor criptografice private ale posesorului nu este păstrată de către AC sau AI astfel că utilizarea lor greşită 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 garanţie 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 criptografica 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 criptografica publică generată ca pe o cerere electronică al cărei format trebuie să respecte PKCS#10 Sintaxa Cererii de Certificare. Solicitările posesorilor trebuie să fie semnate utilizând cheia criptografica privată corespunzătoare cheii publice care va fi indicată în certificat.

Legatura între solicitarea de emitere a certificatului și verificarea identității posesorului este aprobată după cum urmează:

- Pentru verificarea identității inițiale a posesorului pentru SSCD, posesorul se prezinta fizic la AC sau AI și crearea certificatului digital calificat și verificarea identității se face în același timp.
- Pentru reinnoire online, sesiunea TLS sau mesajul S/MIME utilizează cheia criptografica privată curentă pentru autentificarea posesorului și include cererea PKCS # 10.
- Pentru dovedirea inițială a identității, precum și reinnoire posesorul trebuie să se autentifice în contul său de administrare al certificatului utilizând același credentiale 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 criptografica publică a utilizatorului este livrată pe acelaşi 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 certifictaului 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 periodei 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 permişi şi parametrii cheii criptografice pentru perechile de chei utilizate pentru certificate digitale calificate sunt publicaţi de către eIDAS și ETSI. Trans Sped utilizează doar astfel de algoritmi şi parametri de cheie criptografica publica pentru certificate digitale calificate care sunt definiţi a fi corespunzători.

Toate cheile criptografice publice ale AC pentru emiterea de certificate digitale calificate sunt chei RSA pe 2048 bit şi utilizează algoritm 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 catre Trans Sped sunt formatate pentru a permite doar dimensiuni de cheie de 2048 bit. Aplicaţia online şi/sau mecanismele de certificare vor verifica cererile de certificat corespunzător generate şi 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 publica 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 restricţionat 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 şi pot fi activate doar sub controlul dual într-o locaţie securizată din punct de vedere fizic.

Cheile criptografice pentru utilizatorii finali sunt generate şi stocate pe un DSCS. Aceste chei nu pot fi scoase de pe cardul inteligent şi 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 locaţie securizată din punct de vedere fizic. Cheile arhivate nu sunt niciodată puse în producţie.

6.2.6. Intrarea cheii criptografice private în modulul criptografic

Cheile criptografice private AC sunt generate şi 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 şi/sau PIN şi poate fi realizată doar sub controlul dual, din moment ce secretul autentificării este împărţit în două sau mai multe părţi.

6.2.8. Metoda de dezactivare a cheii criptografice private

Cheia criptografica 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, şi este în prezenţa şi semnată de o terţă parte care nu este implicată în distrugerea propriu-zisă a cheii. Toate copiile şi fragmentele cheii private sunt distruse la finalul ciclului de viaţă al perechii de chei.

Pentru cheile private utilizate în legătură cu un HSM, spaţiul de depozitare magnetic care a purtat cheia privată este şters de mai multe ori pentru a elimina orice urmă rămasă iar token-ul hardware (smart cardul) necesar pentru a activa cheia este şters 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 şi cunoscut a fi permanent scos din serviciu, toate cheile private stocate în dispozitiv care au fost vreodată sau potenţial ar putea fi folosite pentru orice scop criptografic sunt distruse.

Dacă un dispozitiv criptografic AC este în permanenţă scos din serviciu, atunci orice cheie conţinută în dispozitivul care a fost folosit în orice scop criptografic este ştearsă din dispozitiv. În cazul unui dispozitiv criptografic AC menit să furnizeze protecţie 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 şi 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 şi în fişierele de audit create pentru sistemul AC.

6.3.2. Perioadele de utilizare pentru cheile criptografice private și publice

Cheile criptografice private şi publice pot fi utilizat atâta timp cât indică perioada de valabilitate a certificatului şi/sau depozitarul. De îndată ce expiră această perioadă, cheile nu mai sunt valabile. Folosirea cheilor criptografice private ale AC este limitată la peroada de timp in care algoritmii utilizați sunt considerați ca fiind adecvați pentru utilizare; întrebuințarea acestora va fi oprită după acel moment.

6.4. Datele de activare

Cerinţele pentru controlul accesului sunt definite şi documentate într-o politică referitoare la controlul accesului care cuprinde procesul de identificare şi autentificare pentru fiecare utilizator, segregarea îndatoririlor, şi numărul de persoane necesare pentru a desfăşura operaţiuni specifice AC (însemnând, regula m din n). Datele de activare (şi acces) pentru cheile şi activele sensibile sunt sub control dual şi/sau împărţite între cel puţin două grupuri distincte de angajaţi.

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

6.5. Controalele de securitate ale calculatorului

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

Politica de securitate a informaţiei conţine o definiţie a securităţii informaţiei, obiectivele ei complete şi aria, şi importanţa securităţii ca un mecanism care permite partajarea de informaţii. Acesta conţine o declaraţie a intenţiei conducerii, sprijinind obiectivele şi principiile securităţii informaţiei şi oferă o explicaţie a politicilor de securitate, principii, standarde, şi cerinţele de conformare de o importanţă specială pentru organizaţie.

Politica de securitate a informaţiei prezintă responsabilităţile generale şi specifice pentru management-ul de securitate a informaţiei, inclusiv raportarea incidentelor legate de securitate, şi conţine referiri la documentaţia care sprijină politica. Responsabilităţile pentru protecţia activelor individuale şi pentru desfăşurarea proceselor de securitate specifice sunt clar definite.

Codul de Politici şi Practici (a se vedea art. 8.1) asigură că există o direcţie clară şi un sprijin de conducere vizibil pentru iniţiativele de securitate. Acesta este responsabil cu menţinerea politicii de securitate şi coordonează implementarea măsurilor legate de securitatea informaţiei.

6.6. Ciclul de viață al controalelor tehnice

Dezvoltarea este realizată în conformitate cu standardele de dezvoltarea ale sistemelor şi 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 producţie. Mediile de testare şi de producţie sunt total decuplate.

Hardware-ul este achiziționat și expediat într-o manieră pentru a reduce probabilitatea de manipulare frauduloasă. Hardware-ul este dedicat solutiilor 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 protecţie corespunzătoare atât împotriva atacurilor interne cât şi externe (firewall, mecanisme de detectare de intruziune, etc.). Controalele de rutare sunt menite să asigure că conexiunile de calculator şi fluxurile de informaţii nu încalcă politica de control al accesului a aplicaţiilor de afaceri ale organizaţiei.

Accesul la toate serverele este supusă autentificării. Utilizatorilor li se acordă acces direct doar la serviciile pentru care au fost în mod specific autorizaţi 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).

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 şi are valoarea fals.
- keyUsage este o extensie critică şi are valoarea digitalSignature, nonRepudiation.
- subjectAltName este o extensie non critică care permite identităţi adiţionale ce vor fi legate de subiectul certificatului cum ar fi adresa de e-mail sau UPN.
- authorityKeyIdentifier este o extensie non critică care identifică certificatul AC care trebuie utilizat pentru a verifica certificatul semnatarului.
- qcStatements este o extensie non critică şi are valoarile:

  id-etsi-qcs-QcCompliance
  id-etsi-qcs-QcSSCD
  id-etsi-qcs-QcPDS indicând indicand Declarația de dezvăluire a PKI

7.1.3. Identificatorii obiectului algoritm

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

Cheile actuale ale AC pentru emiterea de certificate calificate sunt cheile RSA cu 2048 bit şi 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 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 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 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 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

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 calificative 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 opţional), sau trebuie să respingă certificatul.

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.

7.3. 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 Bucureşti
România
Tel: +40 21 210 87 02
Fax:+40 21 211 02 07
www: www.transsped.ro
E-Mail: office@ transsped.ro

7.4. Procedurile de schimbare a specificațiilor

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

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

Revizuirile la prezentul CPP/PC care sunt considerate a avea impact minimal sau deloc asupra semnatarilor şi părţile de încredere care utilizează certificatele şi informaţiile legate de starea certificatului emise de Trans Sped pot fi efectuate şi înregistrate în depozitar fără a

notifica utilizatorii referitor la CPP/PC şi 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 şi Practici, acesta va fi publicat în depozitar.

7.6. Procedurile de aprobare a CPP

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

8. REFERINȚE

CEN/TS 419241	Cerințe de securitate pentru sisteme de încredere care susțin semnarea unui server.
[ETSI]	ETSI EN 319 401: Semnăturile electronice şi infrastructuri (ESI); Cerințele privind politica generală a furnizorilor de servicii de încredere
	ETSI EN 319 411-1: Semnături electronice și infrastructuri (ESI); Cerințe privind politica și securitatea pentru Furnizori de Servicii de Încredere care emit certificate, Partea 1: Cerințe generale
	ETSI EN 319 411-2: Semnăturile electronice şi infrastructuri (ESI); Cerințele de Securitate și Politicile Furnizorilor de Servicii de Încredere pentru emiterea certificatelor;
	Partea a 2-a: Cerințe pentru Furnizorii de Servicii de Încredere care emit certificate calificate în UE;
	ETSI EN 319 412-2 Semnături electronice și infrastructuri (ESI); Certificate de profil; Partea 2: Profil certificat pentru certificate eliberate persoanelor fizice
	ETSI EN 319 412 -5 Semnături electronice și infrastructuri (ESI); Certificate de profil; Partea 5: QCStatements
[eIDAS]	REGULAMENTUL (UE) NR. 910/2014 AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE
[OS]	Organismul de supraveghere
[LSE]	Legea semnaturii electronice (Legea 455/2001)
[RFC4949]	Internet Security Glossary
[RFC5280]	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
[RFC6960]	Internet X.509 Public Key Infrastructure Online Certificate Status Protocol – OCSP, 2013
[X509]	ISO/IEC 9594-8, Tehnologia informaţiei – Interconectare sisteme deschise – Registru: Cadrul de Autentificare. De asemenea, publicat ca Recomandarea ITU-T X.509. A se vedea ediţia ITU-T Rec. X.509 (1993 E) sau ISO/IEC 9594-8:1995 cu Corrigendum Tehnic 1 şi Amendamentul 1 (Extensiile Certificatului) aplicate pentru certificatele X.509v3

9. PROFILE CERTIFICATE

Această secțiune conține formatele pentru diferitele obiecte PKI, cum ar fi certificatele digitale calificate, CRL-urile și cererile și răspunsurile OCSP.

9.1. 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 a subiectului	30 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

9.2. 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	
Subiect	Atribut	Valoare
	CN	Trans Sped Electronic Seal QCA G2
	OU	LEGAL PERSON CA
	O	Trans Sped SRL
	C	RO
Cheia publică a subiectului	30 82 01 0a 02 82 01 01 00 81 82 9f 43 41 f4 92 e3 9c 59 65 70 53 a1 7d cd f0 3e 2f 47 2a 4e 4f d1 43 a3 79 f6 e2 6f 56 0d 21 f3 49 53 3f 0a b8 e0 74 61 89 23 39 c8 e0 0c 09 ce b6 61 18 a1 0b 2b da d0 a0 37 e6 47 6e 4c 6c 93 50 fa 7a be 24 b6 88 56 1b f6 c4 59 bb ce 5b 9b d0 cf d7 d5 61 b5 6e 9a ab 81 85 81 35 b6 87 49 50 e6 27 73 05 ac 5a 15 80 a3 aa 27 2a 2e 14 bc 64 60 33 5a fc 68 47 7a 68 d6 bb b6 10 f4 a2 4e 60 46 1d 78 fc b8 7c 8a 65 a1 85 b5 e8 95 86 41 14 04 47 3c e9 0f 3d 44 1b 98 75 55 3c 4d 82 68 42 47 52 8d f7 09 26 12 7d 79 0f 6d be 3c 5c c0 4b 27 46 eb fe 73 e8 e2 05 e5 ee a3 e8 b8 17 f3 43 28 19 8c 0c ad 12 3f 2f dd b8 4f 71 20 b6 0f 9b 39 ff 97 d8 5b ba 9b dc f0 d6 5a 0f 6e eb 68 fc 70 cd f3 bf f8 10 c5 2f b4 2c c2 1e 28 a9 12 6b f6 8f 5f f4 cc 81 27 86 da 16 a4 f5 df 02 03 01 00 01	
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

9.3. 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 a subiectului	[RSA Key, 2048 Bit]	
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: caIssuers 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

9.4. Trans Sped Mobile eIDAS QCA G2

Câmpul de date	Valoare	
Versiune	v4	
Număr serial	automatic	
Algoritm de semnare	sha256withRSAEncryption	
Emitent	Atribut	Valoare
	= Subject of Trans Sped Root CA G2	
Valabilitate	2017 - 2027	
Subiect	Atribut	Valoare
	CN	Trans Sped Mobile eIDAS QCA G2
	OU	Individual Subscriber CA
	O	Trans Sped SRL
	C	RO
Cheia publică a subiectului	[RSA Key, 2048 Bit]	
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: caIssuers 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

9.5. 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 a subiectului	[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: caIssuers accessLocation:

9.6. 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**
	C	<Country Code>

Cheia publică a subiectului	[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)

9.7. 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	
	Atribut	Valoare
	CN	Trans Sped QCA G2 OCSP Signer

Subiect	OU	Individual Subscriber CA
	O	Trans Sped SRL
	C	RO
Cheia publică a subiectului	[RSA Key, 2048 Bit]	
Extensie	Critic	Valoare
basicConstraints	yes	Subject Type=End Entity Path Length Constraint=None

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_qca_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

9.8. 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 moivul 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

10. GLOSAR

A

AUTORITATE DE CERTIFICARE

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

ALGORITM ASIMETRIC

Spre deosebire de algoritmii simetrici, algoritmii de criptare asimetrici (sau cheia publică) folosesc două chei diferite pentru criptare şi decriptare, unde cheia criptografica privata nu poate fi dedusă din cealaltă.

ALGORITMII CONVENȚIONALI

A se vedea algoritmii 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 folosiţi 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 asimetrici, cheia utilizată pentru decriptare (sau criptare) poate fi calculată de cealaltă cheie într-un algoritm simetric (sau convenţional) 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 informaţiile pe care un utilizator le transmite către Autoritatea de Certificare atunci când solicita emiterea unui certificat figital califica. Aceste informaţii 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 aparţine entităţii numite în certificat, fără a trebui să verifice dacă întreaga cheie se potriveşte cu exactitate (de obicei 1024 bits şi mai mult). Aceasta se realizează prin aplicarea funcţiei hash la cheia publică.

AUTENTIFICARE

Autentificarea se referă la procesul de confirmare fie a identităţii unei persoane sau a integrităţii informaţiei (sau ambele).

AUTO-SEMNAT

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

AUTORITATEA DE CERTIFICARE

O Autoritate de Certificare este o instituţie de încredere care certifică cheile publice, adică emite certificate digitale calificate. În acest scop, sunt verificate informaţiile conţinute în cheia criptografica publică, în special identitatea deţinătorului cheii.

AUTORITATEA DE ÎNREGISTRARE

O entitate care este responsabilă pentru identificarea şi 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 criptografica publică, care este semnat de către o Autoritate de Certificare. El leagă o cheie publică de entitatea numită în certificat (subiect) care deţine cheia criptografica 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 şi X.509.

CERTIFICAT DIGITAL CALIFICAT

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

CIFRU BLOC

Un bloc cifru este un algoritm simetric care încriptează blocuri mai mari de text de dimensiune fixată, de obicei 64 bits (egal cu cinci caractere). Exemple de cifre bloc sunt IDEA, DES şi 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 lanţ comandat de certificate care împreună cu cheia publică a obiectului iniţial din cale, poate fi procesat pentru a obţine obiectul final din cale.

CERTIFICA

A semna digital cheia criptografica publică a altei entităţi prin utilizarea propriei chei private.

CERTIFICAT DIGITAL

A se vedea certificat.

CHEIE

Un cod digital utilizat pentru a cripta, decripta, crea şi verifica semnăturile digitale.

Cheile utilizate pentru algoritmii asimetrici sunt în perechi unde cheia privata este folosita pentru a semna datele iar cheia publica este folosita pentru a le verifica
Algoritmii simetrici, în orice caz, utilizează aceeaşi cheie pentru criptare şi decriptare, şi nu există conceptul de semnătură digitală.

CHEIA CRIPTOGRAFICA PRIVATĂ

Din perechea de chei utilizată în algoritmii asimetrici, cheia privată este cea care trebuie păstrată în siguranţă de către deţinătorul 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 deţinătorul cheii publice corespondente şi pentru generarea de semnături digitale.

CHEIA CRIPTOGRAFICA PUBLICĂ

Din perechea de chei utilizată în algoritmii asimetrici, cheia publică este cea care este pusă la dispoziţia publicului, de ex. pe un server de cheie publică. Scopul său este de a cripta mesajele trimise către deţinătorul cheii şi 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 algoritmii hibrid, cheia utilizată pentru algoritmul de criptare simetric şi 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 aceeaşi 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 încriptează mesajul caracter cu caracter. A se vedea de asemenea cifru bloc.

CONFIRMA

A stabili prin anchetă şi investigaţie adecvată.

CORESPUNDE

A aparţine aceleiaşi perechi de chei.

CPD

A se vedea Definiţiile Politicii de Certificare.

CRL

A se vedea Lista Certificatelor Revocate.

CRIPTANALIZA

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

CRIPTARE

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

CRIPTOGRAFIE

Criptografia este ştiinţa păstrării secretului unor mesaje.

CRIPTOLOGIE

Criptologia este zona din matematică care combină criptografia şi criptanaliza.

CODUL DE PRACTICI ȘI PROCEDURI

O declaraţie de practici pe care o Autoritate de Certificare le foloseşte 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 şi care trebuie să fie protejate (de ex., un PIN sau o parolă).

DECRIPTARE

Procesul de descifrarea al datelor încriptate.

DEPOZITAR

O colecţie de baze de date pentru depozitarea şi retragerea certificatelor, CRL şi orice alte informaţii legate de certificate şi 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. Iniţial 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 şi 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 şi mai sus.

E

EMITE UN CERTIFICAT

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

ENTITATE

A se vedea persoană.

F FSC

A se vedea Furnizorul de Servicii de Certificare.

FUNCŢIA UN SINGUR SENS

A se vedea funcţia hash.

PRESTATORUL DE SERVICII DE ÎNCREDERE CALIFICAT

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

G

GTC

A se vedea Termenii şi Condiţiile Generale.

H

FUNCŢIA HASH

O funcţie 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, şi că este nefezabil să se construiască alte date care produc aceeaşi valoare hash. De exemplu, valoarea hash derivată prin aplicarea funcţiei hash la conţinutul (mesajul text) unui e- mail este apoi folosita alaturi de cheia privată pentru a semna digital e-mail-ul.

I-J

ID UTILIZATORULUI

O structură de date PGP conţinând identitatea deţinătorului 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 internaţional) este un bloc cifru de 64 bit care utilizează o cheie de 128 bit. IDEA este considerat a fi unul dintre algoritmii 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 licenţă către compania elveţiană ASCOM; utilizarea non-comercială este gratuită.

Identificarea persoanei la distanţă prin mijloace video

procesul de identificare şi verificare a identităţii persoanei fizice, în baza documentelor prezentate, a imaginilor capturate şi/sau a informaţiilor comunicate de persoana fizică, utilizând mijloace video

IETF

The Internet Engineering Task Force (IETF) este o comunitate internaţională deschisă de proiectanţi de reţea, operatori, vânzători şi cercetători preocupaţi de evoluţia arhitecturii Internetului şi de operarea fără probleme a internetului. Este deschisă oricărei persoane interesate.

INELUL CHEII

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

K-L LAN

Reţeaua 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 clienţii de pe internet să-l poată folosi. O intrare în director LDAP este o colecţie de atribute cu un nume, denumit nume distinct (ND). ND se referă la intrarea fără ambiguităţi. Fiecare din atributele intrării are un tip şi 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 conţine valoarea "john.doe@company.com". Intrările în directorul LDAP sunt aranjate într-o structură ierarhică care reflectă limitările politice, geografice şi / sau organizaţionale.

LISTA CERTIFICATELOR REVOCATE

O listă care conţine 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 funcţie hash 128 bit dezvoltată de către Ron Rivest. Este folosită la scară largă, iar PGP o foloseşte în legătură cu algoritmul RSA.

Mijloace video

Mijloace de identificare la distanţă ce utilizează tehnologii care presupun fie transmiterea audiovideo de succesiuni de imagini în mişcare, în timp real, în cadrul unei videoconferinţe cu prezenţa unui operator uman, fie transmiterea de succesiuni de imagini în mişcare reprezentând capturi video cu persoana fizică, fără prezenţa 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, inteligenţa artificială şi/sau procese de învăţare automată (machine learning), cum ar fi aplicaţiile care realizează identificarea unei persoane şi/sau verificări ale actelor de identitate (prin capturi de imagini digitale, măsurători ale semnalmentelor biometrice faciale, comparare de imagini), tehnologia NFC (comunicare în câmp apropiat) încorporată în documentele electronice de identitate;

N

NIST

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

NSA

The NSA (Agenţia de Securitate Naţională) este o organizaţie criptologică a guvernului Statelor Unite care se ocupă cu dezvoltarea şi criptanaliza algoritmilor de încriptare.

NUME DISTINCT

Strict vorbind, un Nume Distinct (ND) este o cale printr-un copac registru de informaţii X.500 care identifică în mod unic o entitate. Un copac registru X.500 este o structură ierarhică, dar pentru că informaţiile 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, conţin o adresă e-mail, iar un ND este în mod comun înţeles a cuprinde colactarea câmpurilor de date care alcătuiesc standardul X.509, adică, Ţara (Ţ), Statul / Provincia (SP), Localitatea (L), Organizaţia (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 şi un cuvânt de trecere, este utilizată pentru a nu permite accesul neautorizat la datele confidenţiale. O frază de trecere constă din câteva cuvinte, semne de punctuaţie şi 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 acţionează bazându-se pe acel certificat şi / 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 fiinţă sau orice organizaţie 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 aplicaţie foarte răspândit utilizată şi populară pentru schimbul de e-mail şi fişiere de încriptare sigur. Folosirea non-comercială este gratuită, utilizatorii comerciali vor trebui să obţină o licenţă 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 şi / sau clasă de aplicaţii cu cerinţe de securitate comune. În timp ce un CPP este pregătit de o Autoritate de Certificare, orice organizaţie 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 deţinătorul său nu mai poate garanta că el are unicul acces, şi că cheia sa privată nu a fost compromisă. Prin revocarea cheii publice a certificatului se ţinteşte împiedicarea unor terte persoane de a aduce prejudicii prin pretinderea că sunt deţinătorul cheii. Revocarea cheii publice a certificatului informează publicul că cheia publică nu va mai trebui utilizată pentru a cripta orice mesaje sau fişiere, şi că semnăturile digitale realizate folosind această cheie nu vor mai trebui acceptate. Cheia publica revocată a numarului 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 ceritificatului este încă validă.

RSA

RSA este numele algoritmului asimetric dezvoltat de către o companie cu baza în Statele Unite cu acelaşi nume, RSA Data Security Inc. Securitatea acesteia se bazează pe faptul că este uşor 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 şi Leonard Adleman.

S

SEMNATAR

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

SEMNĂTURĂ DIGITALĂ (folosind algoritmul RSA)

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

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 şi cheile lor publice pentru un acces facil.

SET DE PREVEDERI

O colecţie de declaraţii de practici şi / sau politici, care prezintă o serie de subiecte standard, pentru utilizarea în exprimarea unei definiţii de politică de certificare sau CPP.

SHA-2

SHA-2 este o funcţie 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 data în format electronic pentru a asigura originea si integritatea celor din urmă.

Sistem informatic pentru identificarea persoanei la distanţă prin mijloace video

Reprezintă ansamblul de elemente implicate în procesul de identificare a persoanei la distanţă prin mijloace video, prin care se transmit datele, imaginile capturate/încărcate şi/sau informaţiile 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 dezvoltători de software condus de RSADSI care furnizează criptare şi 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 doreşte să furnizeze un schimb de date securizat prin Internet. SSL este sprijinit şi folosit de către toate browser-ele moderne de Internet pentru a se proteja comunicarea şi transferul de date delicate prin web în toată lumea prin încriptare. Din păcate, versiunile de export ale acestor aplicaţii care se găsesc în afara Statelor Unite sunt limitate la o criptare fragilă de 40 bit (în loc de 128 bit) din cauza restricţiilor de export. Certificatele SSL se bazează pe formatul X.509.

SUSPENDARE

Suspendarea este un proces de punere a unui certificat în aşteptare, 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 ţinteşte împiedicarea tertelor parti de a aduce prejudicii prin pretinderea de a fi deţinătorul cheii. Suspendarea cheii publice a certificatului anunţă publicul că, pentru moment, cheia publică nu poate fi folosită pentru a cripta mesaje sau fişiere, şi că semnăturile digitale efectuate folosind cheia privata corespunzatoare 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 ŞI CONDIŢII GENERALE

Serviciile şi ofertele Autorităţii de Certificare sunt furnizate pe baza Termenilor şi Condiţiilor Generale. Acestea pot fi găsite în depozitar.

TIME-STAMP

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

TRIPLE-DES

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

U

Utilizator

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

V W-Z

WAN

Reţea pe arie largă.

X.509

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