

TRANS SPED



Codul de Practici și Proceduri și Politică de Certificare pentru Certificate Calificate

Versiunea 4.1 / 05 Decembrie 2017

Istoricul versiunilor

Data	Versiunea	Descriere	Autor
29 Iulie 2017	4.0	Actualizare pentru cross-certificarea SAFE-BioPharma	Viky MANAILA
05 Decembrie 2017	4.1	Extinderea duratei de valabilitate a certificatelor pana la 3 ani	Viky MANAILA

Cuprins

1.	Introducere	8
1.1.	Vedere de ansamblu	8
1.2.	Identificare.....	9
1.3.	Comunitatea și Aplicabilitatea	9
1.3.1.	Autoritățile de Certificare	9
1.3.2.	Autoritățile de înregistrare.....	10
1.3.3.	Entitățile finale	10
1.3.4.	Aplicabilitatea.....	10
1.4.	Detalii de contact.....	10
1.4.1.	Specificarea organizării administrării	10
2.	Prevederi Generale	12
2.1.	Obligații	12
2.1.1.	Obligațiile AC.....	12
2.1.2.	Obligațiile AI.....	13
2.1.3.	Obligațiile Semnatarului	14
2.1.4.	Obligațiile părții de încredere.....	14
2.1.5.	Obligații privind depozitarul	14
2.2.	Răspundere.....	14
2.2.1.	Răspunderea AC.....	14
2.2.2.	Răspunderea AI.....	15
2.3.	Responsabilitate financiară.....	15
2.3.1.	Despăgubirea de către părțile de încredere.....	15
2.3.2.	Relațiile fiduciare	15
2.3.3.	Procesele Administrative	15
2.4.	Interpretare și Aplicare	15
2.4.1.	Legea care guvernează	15
2.4.2.	Separabilitate, supraviețuire, fuziune, notificare.....	15
2.4.2.1.	Separabilitate	15
2.4.2.2.	Supraviețuire	15
2.4.2.3.	Fuziune	16
2.4.2.4.	Notificare	16

2.4.3.	Procedurile de soluționare a disputelor	16
2.5.	Taxele	16
2.6.	Publicarea și Depozitarul	16
2.6.1.	Publicarea informațiilor AC	16
2.6.2.	Frecvența publicării	17
2.6.3.	Controlul accesului.....	17
2.6.4.	Depozitările	17
2.7.	Audit de Conformare.....	17
2.8.	Confidențialitatea	17
2.9.	Drepturile de Proprietate Intelectuală.....	18
3.	Identificare și Autentificare	19
3.1.	Înregistrarea inițială.....	19
3.1.1.	Tipuri de nume	19
3.1.2.	Necesitatea pentru ca numele să aibă înțeles	19
3.1.3.	Regulile pentru interpretarea unor diferite forme de nume	19
3.1.4.	Unicitatea numelor.....	20
3.1.5.	Procedura de soluționare a disputelor legate de nume.....	20
3.1.6.	Recunoașterea, autenticitatea și rolul mărcilor comerciale	20
3.1.7.	Metoda de a dovedi deținerea de cheie privată	20
3.1.8.	Autentificarea identității organizației.....	20
3.1.9.	Autentificarea identității individuale.....	21
3.1.10.	Informațiile abonatului neconfirmate	21
3.2.	Rutina de acordare a unei chei noi.....	21
3.3.	Acordarea de altă cheie după revocare	22
3.4.	Cerere de revocare	22
4.	Cerințe operaționale.....	23
4.1.	Solicitarea unui certificat.....	23
4.2.	Emiterea unui certificat	23
4.3.	Acceptarea certificatului	23
4.4.	Diseminarea certificatului.....	23
4.5.	Suspendarea și revocarea unui certificat.....	23
4.5.1.	Circumstanțele pentru revocare	24
4.5.2.	Cine poate solicita revocarea.....	24

4.5.3.	Procedura pentru cererea de revocare	24
4.5.4.	Perioada de grație a cererii de revocare	25
4.5.5.	Circumstanțele suspendării	25
4.5.6.	Cine poate solicita suspendarea	25
4.5.7.	Procedura pentru cererea de suspendare.....	25
4.5.8.	Limitele perioadei de suspendare	25
4.5.9.	Frecvența emiterii de CRL.....	26
4.5.10.	Cerințele de verificare ale CRL.....	26
4.5.11.	Verificare disponibilității stării/ revocării on-line.....	26
4.5.12.	Cerințele de verificare a revocării on-line.....	26
4.5.13.	Alte forme de înștiințare de revocare disponibile	26
4.5.14.	Cerințele de verificare pentru alte forme de înștiințare de revocare	26
4.5.15.	Cerințe speciale privind compromiterea cheii	26
5.	Controalele de securitate fizice, de procedură și de personal	27
5.1.	Controale fizice.....	27
5.2.	Controale de procedură	28
5.3.	Controale personale	29
5.4.	Procedurile de registre de audit.....	29
5.5.	Arhivarea înregistrărilor.....	30
5.6.	Schimbarea cheii	31
5.7.	Compromiterea și recuperarea după dezastre.....	31
5.8.	Terminarea AC.....	31
6.	Controale de securitate tehnică.....	32
6.1.	Generarea și instalarea perechii de chei	32
6.1.1.	Generarea perechii de chei.....	32
6.1.1.1.	Generarea perechii de chei AC	32
6.1.1.2.	Generarea de cheie privată a semnatarului	32
6.1.2.	Livrarea de cheie privată către entitate	32
6.1.3.	Livrarea de cheie privată către emițătorul de certificat	32
6.1.4.	Livrarea de cheie privată către utilizatori	33
6.1.5.	Dimensiunile cheii	33
6.1.6.	Parametrii de generare de chei publice	33
6.1.7.	Verificarea calității parametrului	33

6.1.8.	Generarea de cheie hardware/software	34
6.1.9.	Scopurile utilizării cheii (conform domeniului de utilizare a cheii X.509 v3)34	
6.2.	Protecția cheii private.....	34
6.2.1.	Standardele pentru modulul criptografic.....	34
6.2.2.	Controlul multi-persoane al cheii private (n din m)	34
6.2.3.	Cheia privată escrow.....	34
6.2.4.	Backup de cheie privată	34
6.2.5.	Arhivarea cheii private	35
6.2.6.	Intrarea cheii private în modulul criptografic.....	35
6.2.7.	Metoda de activare a cheii private.....	35
6.2.8.	Metoda de dezactivare a cheii private.....	35
6.2.9.	Metoda de distrugere a cheii private	35
6.3.	Alte aspecte legate de management-ul perechii de chei.....	36
6.3.1.	Arhivarea cheii publice	36
6.3.2.	Perioadele de utilizare pentru cheile private și publice	36
6.4.	Datele de activare	36
6.5.	Controalele de securitate ale calculatorului	36
6.6.	Ciclul de viață al controalelor tehnice	37
	<i>Controalele legate de dezvoltarea sistemului</i>	<i>37</i>
6.6.1.	Controalele management-ului de securitate.....	37
6.7.	Controalele de Securitate ale Rețelei	37
6.8.	Controale de Ingineria modulului criptografic.....	38
7.	Profilele certificatelor și CRL si OCSP	39
7.1.	Profilul certificatului.....	39
	<i>Numărul (numerele) versiunii</i>	<i>39</i>
7.1.1.	Extensiile certificatelor	39
7.1.2.	Identificatorii obiectului algoritm	39
7.1.3.	Formele numelui.....	39
7.1.4.	Constrângerile legate de nume.....	39
7.1.5.	Obiectul identicator al politicii de certificate	39
7.1.6.	Folosirea extensiilor constrângerilor politicii.....	40
7.1.7.	Sintaxa și semantica calificatelor politicii.....	40

7.1.8.	Procesarea semanticii pentru extensia critică a politicii de certificate 40	
7.2.	Profilul CRL.....	40
7.2.1.	Numărul (numerele) versiunii	40
7.2.2.	Extensiile de intrare CRL și CRL.....	40
7.3.	Profilul OCSP	40
Administrarea specifică.....		41
7.4	Procedurile de schimbare a specificației.....	41
7.5	Politicile de publicare și notificare.....	41
7.6	Procedurile de aprobare a CPP.....	41
8.	Referințe	42
9.	Profile certificate.....	43
9.1	Trans Sped Root CA G2	43
9.2	Trans Sped QCA G2	44
9.3	Trans Sped Mobile eIDAS QCA	45
9.4	End User QC.....	46
9.5	End User Mobile QC.....	47
9.6	OCSP responder certificate	48
9.7	Trans Sped QCA G2 CRL	49
GLOSAR.....		50

1. Introducere

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

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

Acest document specifică practicile operării și conducerii Trans Sped AC ce emite certificate calificate în conformitate cu Regulamentul eIDAS, în conformitate cu Legea Semnăturii Electronice din România (Legea Nr. 455/2001), și în conformitate cu Specificațiile tehnice 319 401 ale Institutului pentru Standardele Telecomunicațiilor Europene (ETSI EN 319 401): Cerințele privind politica generală a furnizorilor de servicii de încredere.

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

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

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

1.1. Vedere de ansamblu

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

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

O Autoritate de Certificare acționează în calitate de terță parte de încredere care leagă certificatele 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 oferă certificate calificate emise în conformitate cu Regulamentul eIDAS și Legea Semnăturii Electronice din România. Certificatele calificate pot fi folosite pentru a produce semnături electronice care sunt în mod legal considerate ca fiind echivalente cu semnăturile olografe. Ca o consecință naturală certificatele calificate pot fi emise doar către persoane individuale. Certificatele calificate se eliberează pe dispozitive de creare a semnăturilor electronice certificate (dispozitive de creare a semnăturilor securizate sau HSM) care îndeplinesc cerințele regulamentului eIDAS

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

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

Prezentul CPP/PC se folosește în mare măsură de vocabularul legat de domeniul semnăturilor digitale și a certificatelor, criptografie și criptarea cheii publice, la care se face referire în

GLOSAR. De asemenea glosarul oferă definițiile unor termeni importanți care nu mai apar în altă parte în acest text și care au legătură cu domeniile mai sus menționate.

1.2. Identificare

SC Trans Sped SRL cu sediul în strada Despot Vodă, nr. 38, 020656 București, România (denumită "Trans Sped" în această CPP/PC), este un Furnizor de Servicii de Încredere (TSP) autorizat de către Autoritatea Română de Supraveghere [ARS] pentru a emite certificate calificate sub reglementările Legii referitoare la Semnătura Electronică din România [RESA].

Prezentul CPP/PC este pus la dispoziție la cerere prin e-mail sau poate fi preluat de la <http://www.transsped.ro/repository>.

1.3. Comunitatea și Aplicabilitatea

Acest CPP/PC este pentru certificatele calificate care:

- a) Întrunesc cerințele prevăzute în anexa I din Regulamentul eIDAS;
- b) Sunt emise de către TSP care respectă cerințele prevăzute în anexa II din Regulamentul eIDAS;
- c) Sunt pentru a fi utilizate doar cu dispozitive securizate de creare a semnăturii electronice (DSCRDCS) care întrunesc condițiile prevăzute în anexa II din Regulamentul eIDAS;
- d) sunt emise către public.

1.3.1. Autoritățile de Certificare

Trans Sped este un Furnizor de Servicii de Încredere care emite certificate calificate sub prezentul CPP/PC. Trans Sped operează una sau mai multe Autorități de Certificare (AC) care crează și semnează certificate 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, 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 este în concordanță cu facilitățile folosite pentru a găzdui informații sensibile, de mare valoare.

1.3.2. Autoritățile de înregistrare

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

Orice AI subsidiară este din punct de vedere contractual legată de Trans Sped. O AIR subsidiară este înregistrată ca furnizor de servicii de înregistrare. Ofițerii de Înregistrare ai unei asemenea AI subsidiare sunt identificați individual; aceștia sunt prevăzuți cu certificate speciale de Ofițer de Înregistrare (RO). Doar informațiile semnate de către RO vor fi acceptate de către AC.

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

Identificarea personală a utilizatorilor finali care aplică pentru un certificat se poate de asemenea desfășura de către ofițerii mobili de identificare care operează în numele Trans Sped.

1.3.3. Entitățile finale

În sensul prezentului document, entitatea finală (sau utilizatorul final) este un sinonim pentru semnatar (sau persoană). Se referă la persoanele fizice care folosesc certificate calificate emise de către Trans Sped.

1.3.4. Aplicabilitatea

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

Prezentul CPP/ PC sprijină certificatele:

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

1.4. Detalii de contact

1.4.1. Specificarea organizării 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

SC Trans Sped SRL

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

Versiunea 4.1

Strada Despot Vodă, nr. 38

020656 București

România

Tel: +40 21 210 87 02

Fax: +40 21 211 02 07

E-mail: office@transsped.ro

Persoana care determină conformitatea CPP

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

2. Prevederi Generale

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

2.1. Obligații

2.1.1. Obligațiile AC

Trans Sped furnizează servicii de certificare pentru certificate calificate în conformitate cu prezentul CPP/PC și în conformitate cu Legea referitoare la Semnătura Electronică din România și [eIDAS].

Trans Sped implementează măsuri și proceduri pentru furnizarea de servicii de certificare pentru certificate calificate după cum sunt descrise în § 1 și § 1 din prezentul CPP/PC.

Scopul primar al oricărei Autorități de Certificare este de a oferi servicii de management de certificate (generare, utilizare operațională, revocare și expirare) pentru clienți în cadrul respectivelor lor domeniu(ii) de politici.

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

Cheile AC Trans Sped pentru emiterea de certificate calificate sunt generate într-un Modul de Securitate Hardware certificat (HSM) FIPS 140-1 Nivel 3 într-o încălț securizată fizic.

AC Trans Sped pentru certificate calificate îndeplinește următoarele funcții:

1. generează propriile chei.
2. Operează într-o manieră eficientă și de încredere și în conformitate cu prezenta CPP/PC, Legea referitoare la Semnătura Electronică din România și [eIDAS].
3. Stabilește Autoritățile de Înregistrare subordonate, dacă e cazul.
4. la primirea cererii autentificate pentru certificat, emite certificate calificate care întrunesc standardul de certificate X.509, eIDAS și cerințele ETSI EN 319 401, și cerințele cererii.
5. Se asigură că certificatele sunt lipsite de orice erori de înregistrări de date și sunt corecte în baza informațiilor cunoscute de către AC la momentul emiterii.
6. Informează solicitantul cu privire la măsurile necesare pentru a spori securitatea semnăturilor electronice calificate și pentru a le testa în siguranță.
7. Informează solicitantul că o semnătură electronică calificată are același efect în tranzacțiile legale precum semnătura olografă, numai dacă legea prevede altceva.
8. Revocă certificatele la primirea cererilor de revocare autentificate, sau în conformitate cu § 3.4 sau § 4.5 din prezentul CPP/PC.
9. Transmite informațiile de revocare către registru și emite CRLs.
10. Notifică cu promptitudine deținătorul certificatului cu privire la revocare.

În plus, Trans Sped își rezervă dreptul de a investiga compromiterea și compromiterea suspectată a cheilor private, neconformarea sau neconformarea

suspectată a prevederilor prezentului CPP/PC în vederea protejării integrității comunității tuturor semnatarilor, și de a lua demersurile pe care le consideră potrivite în baza constatărilor sale.

Investigațiile pot include, dar fără a se limita la:

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

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

2.1.2. Obligațiile AI

O AI este asociată cu una sau mai multe AC și acționează în numele AC sale. O AI este responsabilă pentru înregistrarea solicitanților. Acesta efectuează verificarea identității și verificarea tuturor datelor certificatului.

În special sarcinile unei AI sunt:

- Înaintarea de date verificate și complete pentru emitere certificatului și revocarea certificatului către AC.
- Identificarea și autentificarea solicitanților și terțelor părți.
- Informarea semnatarilor referitor la utilizarea corespunzătoare a certificatelor calificate.
- Manipularea dispozitivului securizat de creare de semnături (DSCS) către solicitanți și activarea certificatelor.
- Urmărirea logisticii ciclului de viață a certificatului.
- Validarea cererilor de revocare.

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

Un Ofițer al AI nu trebuie să-și folosească cheile sale în alt scop în afară de cele asociate cu funcția sa fără permisiunea expresă a Trans Sped. AI trebuie să respecte prevederile din prezentul CPP/PC, cele din ETSI EN 319 401, și cele din Legea referitoare la Semnătura Electronică din România și eIDAS; acesta include, dar nu este limitat la asigurarea că cerințele specificate în § 1 CPP/PC sunt îndeplinite, și că sunt furnizate controalele definite în § 1 și § 6 CPP/PC; păstrarea informațiilor confidențiale ale semnatarului în conformitate cu § 2.8 CPP/PC și efectuarea procedurii de autentificare după cum este definită în § 3 CPP/PC.

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

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

2.1.3. Obligațiile Semnatarului

Obligațiile Semnatarului pot deriva din Regulamentul eIDAS sau din Legea referitoare la Semnătura Electronică din România.

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

- La ce date se referă semnătura,
- Dacă datele semnate sunt neschimbate,
- Cărui deținător de cod de semnătură îi este asociată semnătura,
- Conținutul certificatului calificat pe care se bazează semnătura, și
- Rezultatele verificării validității 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,
- Lua în calcul orice limitări legate de utilizarea certificatului indicate părții de încredere din certificat,
- Lua orice alte precauții prescrise în acorduri sau în altă parte.

2.1.5. Obligații privind depozitarul

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

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

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

2.2. Răspundere

2.2.1. Răspunderea AC

În calitate de Furnizor de Servicii de Încredere care emite certificate calificate către public Trans Sped este răspunzător după cum se specifică în Legea referitoare la Semnătura Electronică din România.

În calitate de Furnizor de Servicii de Încredere, conform Legii referitoare la Semnătura Electronică din România și eIDAS, Trans Sped are obligația de a face prevederi de acoperire corespunzătoare pentru a se asigura că poate să îndeplinească obligațiile statutare pentru rambursarea pagubelor cauzate de o încălcare a obligațiilor.

2.2.2. Răspunderea AI

Ca și Trans Sped, AI este răspunzător doar pentru aspectele care fac parte din sfera sa de influență și responsabilitate. Orice AI care operează în numele Trans Sped are un acord contractual cu Trans Sped. O entitate care intenționează să facă reclamații împotriva unei AI mai întâi ar trebui să apeleze la Trans Sped pentru că

(1) un semnatar are un acord contractual cu Trans Sped, nu cu AI, care acționează doar în numele Trans Sped.

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

Trans Sped va investiga faptele și, dacă Trans Sped ajunge la concluzia că nici o greșeală nu poate fi atribuită Trans Sped, trimite partea care face reclamațiile către AI relevantă.

2.3. Responsabilitate financiară

2.3.1. Despăgubirea de către părțile de încredere

Pentru ambele feluri de părți de încredere, părțile de încredere contractuale și non-contractuale, reglementările referitoare la despăgubirile din legislația română sunt obligatorii.

2.3.2. Relațiile fiduciare

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

2.3.3. Procesele Administrative

Un contabil autorizat public efectuează auditul bilanțului Trans Sped o dată pe an pentru a asigura integritatea financiară și management-ul corespunzător al afacerii.

2.4. Interpretare și Aplicare

2.4.1. Legea care guvernează

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

Reglementările pentru furnizarea de servicii de certificare pentru certificate calificate sunt în particular definite în [eIDAS] și în Legea referitoare la Semnătura Electronică în România (Legea nr. 455/2001).

2.4.2. Separabilitate, supraviețuire, fuziune, notificare

2.4.2.1. Separabilitate

Dacă părți din oricare din prevederile din prezentul CPP/PC sunt inoperative sau nule, acest lucru nu va afecta validitatea prevederilor care rămân.

2.4.2.2. Supraviețuire

În pofida faptului că prezentul CPP/PC poate în final să nu mai aibă efect, vor supraviețui următoarele obligații și limitări ale CPP/PC: § 2 (Obligații), § 14

(Răspundere), § 2.3.3 (Procesele Administrative), § 2.4 (Interpretare și Aplicare) și § 2.8 (Confidențialitate).

2.4.2.3. Fuziune

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

2.4.2.4. Notificare

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

SC Trans Sped SRL
Strada Despot Vodă, nr. 38
020656 București
România

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

2.4.3. Procedurile de soluționare a disputelor

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

Procedurile de soluționare a disputelor legate de disputele între Trans Sped și Clienți pot fi prevăzute în acordurile între părți. Procedurile de soluționare a disputelor legate de disputele între Trans Sped și Semnatari pot fi prevăzute în acordurile contractuale cu Semnatarii.

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

Disputele pot fi de asemenea raportate către:

SC Trans Sped SRL
Strada Despot Vodă, nr. 38
020656 București
România

2.5. Taxele

Trans Sped percepe taxe pentru utilizarea anumitor servicii pe care Trans Sped le oferă Semnatariilor săi. O listă actualizată a taxelor actuale poate fi găsită pe site-ul Trans Sped: <http://www.transsped.ro>.

2.6. Publicarea și Depozitarul

2.6.1. Publicarea informațiilor AC

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

Registrul tuturor certificatelor calificate accesibile și care pot fi descărcate, emise de către Trans Sped, poate fi găsit la <http://ca.transsped.ro>. Certificatele calificate sunt accesibile pentru a fi descărcate doar dacă deținătorul certificatului este de acord cu publicarea certificatului.

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

2.6.2. Frecvența publicării

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

CRL-urile sunt actualizate la fiecare douăzeci și patru (24) de ore. Baza de date care furnizează informațiile stării certificatelor calificate este actualizată de fiecare dată când un certificat este eliberat sau revocat. Orice alte informații prezentate în § 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 § 2.6.1.

2.6.4. Depozitarele

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

2.7. Audit de Conformare

Trans Sped este supusă auditurilor externe. Auditurile se efectuează o dată la doi ani, cu revizuirea conformității între auditurile de conformitate în conformitate cu Regulamentul eIDAS. Acestea includ audituri conform eIDAS, ETSI EN 319 401 și a Legii referitoare la Semnătura Electronică din România. Toate aceste audituri necesită demonstrarea unui nivel maxim de securitate și conformitate cu politicile și practicile documentate.

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

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

2.8. Confidențialitatea

Trans Sped păstrează informații confidențiale.

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

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

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

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

2.9. Drepturile de Proprietate Intelectuală

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

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

Prezentul CPP/PC reprezintă proprietatea intelectuală a Trans Sped.

3. Identificare și Autentificare

3.1. Înregistrarea inițială

În vederea obținerii unui certificat calificat, orice semnatar trebuie să aplice pentru un certificat, să se identifice și autentifice către Trans Sped.

Trans Sped se asigură că semnatarii sunt identificați și autentificați în mod corespunzător și că cererile legate de certificat sunt complete, corecte și legal autorizate.

Înainte ca un certificat calificat să fie emis, Trans Sped informează semnatarul referitor la termenii și condițiile privind folosirea certificatului după cum sunt reglementate în Regulamentul eIDAS și Legea referitoare la Semnătura Electronică din România.

Detaliile identificării sunt reglementate de Regulamentul eIDAS și de Legea referitoare la Semnătura Electronică din România. Documentele depuse pot fi pe suport de hârtie sau în format electronic.

Trans Sped verifică, la momentul înregistrării prin mijloace corespunzătoare și în conformitate cu eIDAS, ETSI EN 319 401 și legislația română, identitatea și, dacă e cazul, orice atribute specifice ale persoanei căreia îi este emis un certificat calificat.

Trans Sped înregistrează toate informațiile necesare pentru a verifica identitatea subiectului și, dacă este cazul, orice atribute specifice ale subiectului, 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 subiectul 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 și alte reglementări.

Numele trebuie să aibă semantică comun înțeleasă (prenume și nume, numele societății, adresa de e-mail) pentru ca partea de încredere să determine identitatea persoanei și / sau organizației.

În orice caz, solicitantul își poate alege un pseudonim în locul numelui în certificatul calificat. Trans Sped va emite asemenea certificate pseudonimizate; folosirea pseudonimului este indicată prin sufixul ":PN" în spațiul Nume Comun al certificatului.

3.1.3. Regulele pentru interpretarea unor diferite forme de nume

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

3.1.4. Unicitatea numelor

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

3.1.5. Procedura de soluționare a disputelor legate de nume

Trans Sped nu este responsabil pentru soluționarea disputelor legate de nume dintre semnatori. Trans Sped poate adăuga, la propria discreție, informații adiționale la un nume pentru a-l face unic printre 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 semnatar.

3.1.7. Metoda de a dovedi deținerea de cheie privată

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

Dacă Abonatul, numit într-un certificat calificat, generează propriile sale chei, Abonatul trebuie să utilizeze cheia privată pentru a semna o valoare și pentru a furniza respectiva valoare AC-ului care emite certificatul. AC trebuie apoi să valideze semnătura utilizând cheia publică a subiectului.

Dacă Trans Sped generează în incinta sa cheia privată aparținând certificatului calificat al subiectului - 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. Autenticarea identității organizației

Dacă solicitantul este o persoană care este identificată în legătură cu o persoană juridică sau altă entitate organizațională, pe lângă datele din § 3.1.9 dovada va fi dată de existența sa. Această verificare poate fi efectuată prin prezentarea unei copii al unui document, care dovedește existența organizației (extrasul actual al unui registru oficial competent în care organizația este listată sau un document comparabil).

Autoritățile guvernamentale sau administrative trebuie să furnizeze documentele care reflectă relația lor cu următoarea entitate mai înaltă (de ex: autoritate superioară) cu antet oficial, ștampilată cu ștampila oficială și semnată de un funcționar autorizat.

Documentația trebuie să cuprindă:

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

3.1.9. Autentificarea identității individuale

Autentificarea unei entități individuale este realizată în conformitate cu Regulamentul eIDAS, Legea referitoare la Semnătura Electronică din România, standardul ETSI EN 319 401, ETSI EN 319 411-1 și ETSI EN 319 411-2.

Dovada identității solicitantului este verificată printr-un document oficial (carte de identitate sau CI) cu fotografia personală a solicitantului. Trans Sped poate folosi, cu acordul solicitantului, datele cu caracter personal luate anterior. Documentul oficial trebuie să cuprindă:

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

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

Dacă solicitantul este o persoană care este identificată în legătură cu o persoană juridică sau altă entitate organizațională în completarea datelor din § 3.1.8 dovezile următoare vor fi furnizate:

- Dovada că subiectul este asociat o persoană juridică sau altă entitate organizațională,
- Autorizația de la persoana juridică sau altă entitate organizațională.

3.1.10. Informațiile abonatului neconfirmate

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

3.2. Rutina de acordare a unei chei noi

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

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

Obținerea unei noi cheii în cazul în care certificatul a expirat se face folosind aceleași reguli ca și la înregistrarea inițială. Întregul proces de înregistrare trebuie repetat.

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

3.3. Acordarea de altă cheie după revocare

După ce un certificat a fost revocat, semnatarul trebuie să reaplice pentru unui nou certificat în conformitate cu § 3.1. devreme ce perechea de cheie revocată este ineligibilă pentru a semna și autentifica o cerere de acordare a unei alte chei (a se vedea § 3.2).

3.4. Cerere de revocare

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

- Prezența personală la AI;
- Cu o semnătură scrisă de mână pe un formular de suspendare / revocare;
- prin dovedirea posesiei cheii private;
- Login-ul cu succes la serviciile de certificare on-line furnizate de către Trans Sped.

4. Cerințe operaționale

4.1. Solicitarea unui certificat

Un semnatar depune o solicitare pentru certificat către Trans Sped și urmează procedura descrisă în prezentul CPP/PC sau în descrierile Trans Sped pentru cererea unui certificat.

Solicitările unui certificat sunt depuse la Trans Sped pentru a fi operate, rezultatul putând fi o aprobare sau un refuz.

Perechea de chei poate fi generată de AC, AI sau semnatar. În orice caz, generarea de cheie se va desfășura într-un mediu securizat. Cheile pentru semnăturile electronice calificate sunt întotdeauna create în dispozitivele securizate de creare a semnăturii care sunt aprobate a fi utilizate în astfel de scopuri. Cheile private nu vor fi exportabile din asemenea dispozitive.

Semnatarul va semna un acord cu Trans Sped care cuprinde:

- Declarația că informațiile furnizate sunt corecte;
- Acordul la obligațiile semnatarului;
- Acordul la publicarea certificatului în depozitar.

4.2. Emiterea unui certificat

Trans Sped verifică corectitudinea și valabilitatea tuturor datelor necesare pentru emiterea unui certificat calificat (a se compara § 3.1.8 și § 3.1.9). Trans Sped va verifica datele conținute în cerere în conformitate cu Legea semnăturii electronice și eIDAS. Trans Sped fie va emite certificatul semnatarului la completarea cu succes a acestui proces fie va informa semnatarul referitor la orice probleme sau inadvertențe.

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

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

4.3. Acceptarea certificatului

La primirea unui certificat, semnatarul trebuie să verifice conținutul acestuia. Dacă certificatul conține greșeli care nu pot fi acceptate de către semnatar, semnatarul trebuie să informeze Trans Sped fără întârziere. Trans Sped atunci va revoca certificatul și va lua măsurile care se impun fie de a restitui prețul certificatului sau de a emite un certificat nou.

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

4.4. Diseminarea certificatului

Certificatele calificate sunt puse la dispoziție pentru a fi luate din depozitarul de certificate al Trans Sped de către terțe părți doar cu acordul semnatarului.

4.5. Suspendarea și revocarea unui certificat

Un certificat poate fi suspendat sau revocat. Dacă nu este sigur dacă cheia privată corespondentă a fost pierdută sau compromisă, semnatarul trebuie să suspende certificatul până la clarificarea situației. Dacă cheia privată a fost compromisă sau pierdută cu siguranță, sau dacă datele semnatarului reprezentate în certificat s-au

schimbat în mod substanțial, certificatul trebuie să fie revocat iar semnatarul trebuie să facă din nou o solicitare.

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

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

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

4.5.1. Circumstanțele pentru revocare

Un certificat este revocat în cazul în care:

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

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

4.5.2. Cine poate solicita revocarea

Semnatarul sau înlocuitorul său pot solicita revocarea.

Dacă un certificat prevede că deținătorul lui poate acționa în numele unei terțe părți, această parte poate de asemenea solicita revocarea certificatului.

Orice entitate sau terță parte care au confirmat orice informații cuprinse în certificat are dreptul să revoce certificatul afectat.

Oricine poate informa Trans Sped referitor la faptul că informațiile dintr-un certificat nu sunt sau nu mai sunt corecte. Trans Sped va verifica apoi dacă o revocare este corespunzătoare în conformitate cu § 4.5.1, 2.

4.5.3. Procedura pentru cererea de revocare

Există câteva feluri în care se poate depune o cerere de revocare:

1. Semnatarul sau o terță parte autorizată poate solicita revocarea unui certificat prin completarea și semnarea unui formular de revocare în fața Ofițerului de Înregistrare. Autentificarea este furnizată apoi de semnătura scrisă de mână.
2. Semnatarul sau o terță parte autorizată poate solicita revocarea unui certificat prin trimiterea unei cereri de revocare în format electronic către Trans Sped. Autentificarea este apoi furnizată printr-o semnătură electronică calificată.
3. Folosirea de servicii on-line furnizate de către Trans Sped.

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

4.5.4. Perioada de grație a cererii de revocare

Trans Sped operează cererea de revocare, la confirmarea faptului că provine de la o entitate autorizată, cât mai prompt și eficient posibil. Perioada necesară pentru a revoca un certificat nu depășește douăzeci și patru (24) de ore.

4.5.5. Circumstanțele suspendării

Un certificat este suspendat în cazul în care:

1. Semnatarul sau o terță parte autorizată au depus o cerere de suspendare;
2. Trans Sped suspectează că au fost furnizate informații false în aplicarea pentru certificat lucra care ar putea invalida certificatul;
3. Certificatul nu a fost plătit în conformitate cu prevederile contractuale.

4.5.6. Cine poate solicita suspendarea

Semnatarul sau înlocuitorul său pot solicita suspendarea.

Dacă un certificat prevede că deținătorul lui poate acționa în numele unei terțe părți, această parte poate de asemenea solicita suspendarea certificatului.

Orice entitate sau terță parte care au confirmat orice informații cuprinse în certificat are dreptul să suspende certificatul afectat.

Oricine poate informa Trans Sped referitor la faptul că informațiile dintr-un certificat s-ar putea să nu fie corecte. Trans Sped va verifica apoi dacă o suspendare în conformitate cu § 4.5.5, 6 este corespunzătoare.

4.5.7. Procedura pentru cererea de suspendare

Există câteva feluri în care se poate depune o cerere de suspendare:

1. Semnatarul sau o terță parte autorizată poate solicita suspendarea unui certificat pentru completarea și semnarea unui formular de suspendare în fața Ofițerului de Înregistrare. Autentificarea este furnizată apoi de semnătura scrisă de mână.
2. Semnatarul sau o terță parte autorizată poate solicita suspendarea unui certificat prin trimiterea unei cereri de suspendare în format electronic către Trans Sped. Autentificarea este apoi furnizată printr-o semnătură electronică calificată.
3. Folosirea de servicii on-line furnizate de către Trans Sped.

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

4.5.8. Limitele perioadei de suspendare

Un certificat este suspendat pentru maximum șapte (7) zile după cererea de suspendare. Un certificat poate fi suspendat de două ori; o a treia suspendare și depășirea perioadei de suspendare atrag după sine revocarea certificatului.

Cererea de restabilire a certificatului nu trebuie autentificată utilizând certificatul care este suspendat, revocat, expirat sau nevalidat.

4.5.9. Frecvența emiterii de CRL

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

4.5.10. Cerințele de verificare ale CRL

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

4.5.11. Verificare disponibilității stării/ revocării on-line

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

4.5.12. Cerințele de verificare a revocării on-line

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

4.5.13. Alte forme de înștiințare de revocare disponibile

Nu există prevederi.

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

Nu există prevederi.

4.5.15. Cerințe speciale privind compromiterea cheii

În cazul în care semnatarul suspectează sau știe cu siguranță că cheia sa privată a fost compromisă, acesta este obligat să solicite revocarea cât mai curând posibil. Un semnatar nu este eliberat de obligațiile sale de semnatar până ce nu 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 și menține starea controalelor de securitate solicitate de către AC și AI. Acest capitol oferă o descriere a cadrului de controale de securitate, care reflectă prevederile cuprinse în Legea referitoare la Semnătura Electronică din România, eIDAS și ETSI EN 319 401. Prevederile respective se completează unele pe celelalte și au menirea de a spori controalele de securitate în ansamblu. Toate acestea necesită cele mai înalte standarde de securitate.

Din motive de securitate, în orice caz, 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 non-publique.

5.1. Controale fizice

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

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

Cheile 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, care sunt atestate să îndeplinească cerințele Legii referitoare la Semnătura Electronică din România și eIDAS. Orice acces neautorizat la informația depozitată, posibil provenind din pierderea, falsificarea, sau utilizarea greșită a acestora este împiedicată prin mijloace corespunzătoare. Verificările de securitate regulate sunt efectuate pentru a se asigura că aceste controale funcționează corespunzător.

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

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

Toate sistemele AC au energie electrică de industrie standard și sisteme de aer condiționat care să ofere un mediu de operare corespunzător. Toate sistemele AC au precauții rezonabile luate pentru a minimiza impactul expunerii la apă. Toate sistemele AC au mecanisme standard de prevenire a incendiilor și de protecție în locație.

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

Orice AI care confirmă informațiile semnatarului și care înaintează aceste informații către Trans Sped trebuie să ofere o facilitate sigură din punct de vedere fizic pentru depozitarea înregistrărilor legate de cereri și token necesare pentru a avea acces la

componentele AI. Dacă o AI păstrează informațiile confidențiale ale semnatarului controalele de securitate din punct de vedere fizic trebuie să se potrivească cu cele ale Trans Sped.

O AI nu stochează niciodată informațiile legate de cheia semnatarului.

5.2. Controale de procedură

Procedurile operaționale sunt documentate și menținute. Controalele de procedură asigură că nici o singură persoană care acționează singur(ă) nu va putea înșela măsura de securitate luată.

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

Următoarele sunt rolurile de încredere implementate de AC:

- Manager - persoană cu responsabilitate generală pentru sistemele AC;
- Ofițer de securitate - persoană 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 - persoană autorizată 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 certificate sau revocări de certificate. Aceste persoane nu dețin alte roluri;
- Auditor - persoană autorizată să vizualizeze și să mențină jurnalele de audit ale AC

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

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

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

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

5.3. Controale personale

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

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

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

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

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

5.4. Procedurile de registre de audit

Trans Sped păstrează rapoarte de audit și fișiere ale sistemului de înregistrare care documentează acțiunile întreprinse ca parte din serviciile de certificare 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 unei noi 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 semnate cu timp și semnate digital. Trans Sped utilizează semnalul de timp GPS și un set de servere NTP ca sursă de timp.

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

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

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

Pentru informații suplimentare legate de cerințele și procedurile de audit extern și intern, vezi § 2.7.

5.5. Arhivarea înregistrărilor

Fișierele rapoartelor de audit și ale sistemului de înregistrare (a se vedea § 5.4) sunt salvate periodic pe medii WORM (scriere o dată, citire multiplă) și arhivate într-o locație sigură. Datele de audit arhivate referitoare la certificatele calificate sunt reținute după cum prevede Legea referitoare la Semnătura Electronică din România.

Trans Sped utilizează arhivarea internă și externă pentru a împiedica pierderea documentelor importante sau a datelor digitale. Arhivele sunt amplasate în locații diferite (interne sau externe) și protejate de sistemele de control asupra accesului. În general, rapoartele privind certificatele calificate sunt reținute cel puțin zece (10) ani după cum prevede Legea referitoare la Semnătura Electronică din România. Nicio persoană singură nu poate modifica sau chiar distruge materialul arhivat, iar accesul la acesta este strict restricționat.

5.6. Schimbarea cheii

Root AC este valabil timp de 15 ani (până în 2031). Certificatele de autorizare sunt valabile timp de 10 ani (până în 2026). Atunci când se generează un certificat CA nou, se modifică și denumirea AC. Același lucru este și cu CDP de certificate de utilizator final.

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

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

5.7. Compromiterea și recuperarea după dezastre

Pentru a restaura operațiunile de afaceri într-un termen rezonabil de timp ca urmare a întreruperii sau a nereușitei proceselor de afaceri critice, au fost dezvoltate planuri de continuitate de afaceri. Planul de continuitate al afacerii definește perioada de timp, adică o perioadă de întrerupere a sistemului acceptabilă în cazul unui dezastru natural de amploare sau compromis al cheii private AC. Această perioadă de întrerupere tolerată depinde de cerințele de valabilitate ale serviciului specific și poate dura de la o oră la 12 ore.

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

5.8. Terminarea AC

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

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

Dacă niciun furnizor de certificate alternativ nu continuă serviciile Trans Sped toate certificatele care nu au expirat sau nu au fost revocate de către respectivii semnatori vor fi revocate de către Trans Sped. Toată documentația relevantă va fi transferată către Organismul Român de Supraveghere (OS) după cum prevede Legea referitoare la Semnătura Electronică din România.

Semnatarii vor fi notificați dacă Trans Sped întreprinde o asemenea acțiune.

6. Controale de securitate tehnică

6.1. Generarea și instalarea perechii de chei

6.1.1. Generarea perechii de chei

6.1.1.1. Generarea perechii de chei AC

Cheia privată AC folosită pentru emiterea de certificate calificate este generată într-un HSM certificat FIPS 140-1 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 este efectuată sub un control dual. În plus, generarea de cheie se face în prezența și semnată de o terță parte neimplicată în generarea de cheie propriu-zisă.

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

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

Nicio copie a niciunei chei private nu este păstrată în permanență pe suport magnetic media în format necriptat. Niciun material de cheie privată nu este stocat temporar pe suport magnetic media pentru că cheile pentru certificate calificate sunt generate în interiorul HSM.

6.1.1.2. Generarea de cheie privată a semnatarului

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

Dacă generarea de cheie este realizată de către Semnatar iar cererea de certificat trimisă către AC, atunci Trans Sped nu oferă nicio garanție legată de generarea de cheie. Perechile de chei 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 de cheie privată către entitate

Cheile private generate de AC sau AI pe DSCS sunt livrate către semnatar prin scrisoare recomandată cu confirmare de primire. Codurile PIN sunt distribuite separat de DSCS-uri.

Alternativ, semnatarul poate colecta DSCS cu cheia privată la birourile AC sau AI.

La cererea semnatarului DSCS poate fi de asemenea livrat prin altă formă acceptabilă de livrare securizată.

6.1.3. Livrarea de cheie privată către emițătorul de certificat

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

Legarea între cererea de certificat și verificarea identității este aprobată după cum urmează:

- Pentru verificarea identității inițiale pentru SSCD, abonatul apare în persoană și crearea de certificat și verificarea identității se face în același timp.
- Pentru recheierea pentru SSCD, sesiunea TLS sau mesajul S / MIME utilizează cheia privată curentă pentru autentificarea abonatului și include cererea PKCS # 10.
- Pentru probarea inițială a identității, precum și recheierea aplicației Secure Server, abonatul trebuie să se autentifice în contul său utilizând același factor multiplu folosit pentru a invoca cheia privată.

6.1.4. Livrarea de cheie privată către utilizatori

Metodele de livrare a certificatelor AC către părțile de bază includ:

- publicarea certificatelor AC pe o listă națională de încredere a furnizorilor 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 publică a semnatarului este livrată pe același DSCS folosit pentru depozitarea cheii private a semnatarului dacă perechea de chei este generată de către AC sau AI.

Dacă semnatarul este de acord ca certificatul său de cheie publică să fie publicat în depozitarul de certificate Trans Sped, acesta este disponibil pentru descărcare de asemenea.

6.1.5. Dimensiunile cheii

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

Perechile de chei ale AC-urilor Trans Sped au lungimea de 2048 biti. Orice cheie generată pe un DSCS și folosită pentru un certificat calificat are dimensiunea de cel puțin 2048 biti. Certificatele calificate emise după 01 ianuarie 2013 trebuie să folosească perechi de chei de 2048 biti.

Nu se semnează certificate, CRL sau răspunsuri OCSP utilizând un algoritm RSA 2048 care se extinde dincolo de data 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 de chei publice

Algoritmii permiși și parametrii cheii pentru perechile de chei utilizate pentru certificate calificate sunt publicați de către eIDAS și ETSI. Trans Sped utilizează doar astfel de algoritmi și parametri de cheie pentru certificate calificate care sunt definiți a fi corespunzători.

Toate cheile actuale AC pentru emiterea de certificate calificate sunt chei RSA pe 2048 bit și utilizează algoritm hash SHA-256.

6.1.7. Verificarea calității parametrului

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

6.1.8. Generarea de cheie hardware/software

Cheile pentru certificatele 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 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 § 39). Certificatele calificate pot fi utilizate pentru semnături electronice.

6.2. Protecția cheii private

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

Accesul la cheia facilității și la cheile private este protejat de mecanismele de control al accesului. Cheile 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 nici un suport de stocare permanent sau magnetic.

6.2.1. Standardele pentru modulul criptografic

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

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

6.2.2. Controlul multi-persoane al cheii private (n din m)

Cheile private AC sunt stocate într-un HSM certificat FIPS 140-1 Nivel 3 (sau echivalent). Pentru a activa cheile private ale AC, sunt necesare două persoane (a se vedea § 6.2.1). Nicio persoană singură nu are toate datele de activate 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 calificate.

Pentru certificatele emise în conformitate cu Legea Semnăturii Electronice din România, orice formă de cheie escrow este în mod explicit interzisă.

6.2.4. Backup de cheie privată

Cheile private ale AC sunt generate într-un HSM certificat FIPS 140-1 Nivel 3. Trans Sped face copii sigure înainte de a pune cheile CA în funcțiune. În timpul copierii de rezervă, cheia privată părăsește modulul într-o formă criptată și această cheie criptată

poate fi restabilită numai într-un alt modul. Cheile criptate au copii de rezervă pe medii WORM și pot fi activate doar sub controlul dual într-o locație securizată din punct de vedere fizic.

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

6.2.5. Arhivarea cheii private

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

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

6.2.6. Intrarea cheii private în modulul criptografic

Cheile private AC sunt generate și depozitate într-un HSM certificat FIPS 140-1 Nivel 3. Cheile private AC nu există în text simplu în afara modulului criptografic. Trans Sped exportă numai cheia privată de la HSM în scopul realizării unei copii securizate. Exportul și încărcarea cheilor private AC se efectuează în conformitate cu secțiunea § 6.2.4.

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

6.2.7. Metoda de activare a cheii private

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

6.2.8. Metoda de dezactivare a cheii private

Cheia 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 private

Distrugerea oricărei chei private ale AC trebuie să fie autorizată de către conducere. Aceasta se realizează sub control dual, și este în prezența și semnată de o terță parte care nu este implicată în distrugerea propriu-zisă a cheii.

Toate copiile și fragmentele cheii private sunt distruse la finalul ciclului de viață al perechii de chei.

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

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

Dacă un dispozitiv criptografic AC este în permanență scos din serviciu, atunci orice cheie conținută în dispozitivul care a fost folosit în orice scop criptografic este ștersă din

dispozitiv. În cazul unui dispozitiv criptografic AC menit să furnizeze protecție fizică la atacuri dacă dispozitivul este scos din serviciu definitiv, atunci acesta este distrus.

Dacă o cheie privată este depozitată pe un DSCS, acesta este distrus prin distrugerea fizică a cardului inteligent.

Nu există fragmente de material de cheie sau copiate care trebuie să fie distruse în acest caz pentru că folosirea unui DSCS garantează că cheile private nu pot fi niciodată exportate din DSCS.

6.3. Alte aspecte legate de management-ul perechii de chei

6.3.1. Arhivarea cheii publice

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

6.3.2. Perioadele de utilizare pentru cheile private și publice

Cheile private și publice pot fi utilizat atâta timp cât indică perioada de valabilitate a certificatului și/sau depozitarul. De îndată ce expiră această perioadă, cheile nu mai sunt valabile.

Folosirea cheilor private ale AC este limitată la perioada de timp în care algoritmiile utilizați sunt considerați ca fiind adecvați pentru utilizare; întrebunțarea acestora va fi oprită după acel moment.

6.4. Datele de activare

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

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

6.5. Controalele de securitate ale calculatorului

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

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

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

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

6.6. Ciclul de viață al controalelor tehnice

Controalele legate de dezvoltarea sistemului

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

Trans Sped utilizează numai aplicații și dispozitive care:

- sunt echipamente și software comercializate la distanță, concepute și dezvoltate printr-o metodologie de proiectare documentată;

- hardware și software personalizat dezvoltate de o parte sigură într-un mediu controlat utilizând metode structurate de dezvoltare sau;

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

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

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

6.6.1. Controalele management-ului de securitate

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

6.7. Controalele de Securitate ale Rețelei

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

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

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

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

6.8. Controale de Ingineria modului criptografic

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 Nivelul 3 (a se vedea § 6.2.1).

7. Profilele certificatelor și CRL și OCSP

7.1. Profilul certificatului

Numărul (numerele) versiunii

Trans Sped emite certificate X.509 versiunea 3 în conformitate cu RFC 5280, "Profilul certificatului infrastructurii cheii publice Internet X.509 și lista certificatelor revocate (CRLs)".

7.1.1. Extensiile certificatelor

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

- `basicConstraints` este o extensie critică și are valoarea `false`.
- `keyUsage` este o extensie critică și are valoarea `digitalSignature, nonRepudiation`.
- `subjectAltName` este o extensie non critică care permite identități adiționale ce vor fi legate de subiectul certificatului cum ar fi adresa de e-mail sau UPN.
- `authorityKeyIdentifier` este o extensie non critică care identifică certificatul AC care trebuie utilizat pentru a verifica certificatul semnatarului.
- `qcStatements` este o extensie non critică și are valoarea:

`id-etsi-qcs-QcCompliance`

`id-etsi-qcs-QcSSCD`

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

7.1.2. Identificatorii obiectului algoritm

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

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

7.1.3. Formele numelui

A se vedea § 3.1

7.1.4. Constrângerile legate de nume

Nu se aplica.

7.1.5. 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

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)

MOBILE QCA (Issued by CT-CSSP-CA-A1 / Cybertrust)

1.3.6.1.4.1.39965.3.1.1

1.3.6.1.4.1.39965.3.1.3

MOBILE eIDAS QCA

1.3.6.1.4.1.39965.4.1.1

7.1.6. Folosirea extensiilor constrângerilor politicii

Nu există prevederi.

7.1.7. Sintaxa și semantica calificatorilor politicii

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

7.1.8. Procesarea semanticii pentru extensia critică a politicii de certificate

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

7.2. Profilul CRL

7.2.1. Numărul (numerele) versiunii

Trans Sped emite CRL X.509 versiunea 2 în conformitate cu RFC 5280, "Profilul certificatului infrastructurii cheii publice Internet X.509 și lista certificatelor revocate (CRL)". Starea certificatelor este de asemenea furnizată prin mecanismul de validare online OCSP

7.2.2. Extensiile de intrare CRL și 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 SRL
Strada Despot Vodă, nr. 38
020656 București
România
Tel: +40 21 210 87 02
Fax: +40 21 211 02 07
WWW: <http://www.transsped.ro>
E-Mail: office@transsped.ro

7.4 Procedurile de schimbare a specificației

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

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

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

Această versiune a CPP/PC este datată februarie 2013.

7.5 Politicile de publicare și notificare

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

7.6 Procedurile de aprobare a CPP

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

8. Referințe

CEN/TS 419241 [ETSI]	<p>Cerințe de securitate pentru sisteme de încredere care susțin semnarea unui server.</p> <p>ETSI EN 319 401: Semnăturile electronice și infrastructuri (ESI); Cerințele privind politica generală a furnizorilor de servicii de încredere</p> <p>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</p> <p>ETSI EN 319 411-2: Semnăturile electronice și infrastructuri (ESI); Cerințele de Securitate și Politicile Furnizorilor de Servicii de Încredere pentru emiterea certificatelor;</p> <p>Partea a 2-a: Cerințe pentru Furnizorii de Servicii de Încredere care emit certificate calificate în UE;</p> <p>ETSI EN 319 412-2 Semnături electronice și infrastructuri (ESI);</p> <p>Certificate de profil; Partea 2: Profil certificat pentru certificate eliberate persoanelor fizice</p> <p>ETSI EN 319 412 -5 Semnături electronice și infrastructuri (ESI);</p> <p>Certificate de profil; Partea 5: Situațiile QC</p>
[eIDAS]	<p>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</p>
[OS]	<p>Organismul de supraveghere</p>
[RESA]	<p>Legea referitoare la Semnătura Electronică din România (Legea nr. 455/2001)</p>
[RFC2828]	<p>Glosarul de Securitate Internet</p>
[RFC5280]	<p>Internet X.509 Public Key Infrastructure</p> <p>Profilul certificatului și a listei certificatelor revocate (CRL)</p>
[X509]	<p>ISO/IEC 9594-8, Tehnologia informației – Interconectare sisteme deschise – Registru: Cadrul de Autentificare. De asemenea publicat ca Recomandarea ITU-T X.509. A se vedea ediția ITU-T Rec. X.509 (1993 E) sau ISO/IEC 9594-8:1995 cu Corrigendum Tehnic 1 și Amendamentul 1 (Extensiile Certificatului) aplicate pentru certificatele X.509v3</p>

9. Profile certificate

Această secțiune conține formatele pentru diferitele obiecte PKI, cum ar fi certificatele, 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	Codificare
	CN	Trans Sped Root CA G2	PrintableString
	OU	Trans Sped CA	PrintableString
	O	Trans Sped SRL	PrintableString
	C	RO	PrintableString
Valabilitate	2016 – 2031		
Subiect	Atribut	Valoare	Codificare
	CN	Trans Sped Root CA G2	PrintableString
	OU	Trans Sped CA	PrintableString
	O	Trans Sped SRL	PrintableString
	C	RO	PrintableString
Cheia publică a subiectului	[RSA Key, 2048 Bit]		
Extensie	Critic	Valoare	
basicConstraints	yes	cA: TRUE pathLenConstraint: none	
keyUsage	yes	keyCertSign cRLSign	
subjectKeyIdentifier	no	automatic	

9.2 Trans Sped QCA G2

Câmpul de date	Valoare		
Versiune	v3		
Număr Serial	automatic		
Algoritm de semnare	sha256withRSAEncryption		
Emitent	Atribut	Valoare	Codificare
	= Subject of Trans Sped Root CA G2		
Valabilitate	2016 - 2026		
Subiect	Atribut	Valoare	Codificare
	CN	Trans Sped QCA G2	PrintableString
	OU	Individual Subscriber CA	PrintableString
	O	Trans Sped SRL	PrintableString
	C	RO	PrintableString
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	

9.3 Trans Sped Mobile eIDAS QCA

Câmpul de date	Valoare		
Versiune	v3		
Număr Serial	automatic		
Algoritm de semnare	sha256withRSAEncryption		
Emitent	Atribut	Valoare	Codificare
	= Subject of Trans Sped Root CA G2		
Valabilitate	2016 - 2026		
Subiect	Atribut	Valoare	Codificare
	CN	Trans Sped Mobile eIDAS QCA G2	PrintableString
	OU	Individual Subscriber CA	PrintableString
	O	Trans Sped SRL	PrintableString
	C	RO	PrintableString
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: calssuers accessLocation: URL= http://www.transsped.ro/cacerts/ts_root_g2.crt [2]accessMethod: OCSP accessLocation: URI: http://ocsp.transsped.ro	
cRLDistributionPoints	no	http://www.transsped.ro/crl/ts_root_g2.crl	

9.4 End User QC

Câmpul de date	Valoare		
Versiune	v3		
Număr Serial	automatic		
Algoritm de semnare	sha256withRSAEncryption		
Emitent	Atribut	Valoare	Codificare
	= Subject of Trans Sped QCA G2		
Valabilitate	No more than 3 years		
Subiect	Atribut	Valoare	Codificare
	CN	<Common Name = First name + Last name>	PrintableString
	G	<First name>	PrintableString
	SN	<Last name>	PrintableString
	SER	<Personal Identification Code>	PrintableString
	OU	<Organizational Unit> optional	PrintableString
	O	<Organization> optional	PrintableString
	C	<Country Code>	PrintableString
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	
Private CertExtensions	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)	
subjectAltNames	no	Other Name / rfc822-Name = <Email Address>	
subjectKeyIdentifier	no	automatic	
authorityKeyIdentifier	no	= subjectKeyIdentifier of Trans Sped QCA G2	
authorityInfoAccess	no	[1]accessMethod: caIssuers accessLocation: URL= http://www.transsped.ro/cacerts/ts_qca_g2.crt	
		[2]accessMethod: OCSP accessLocation: URI: http://ocsp.transsped.ro	
cRLDistributionPoints	no	http://www.transsped.ro/crl/ts_qca_g2.crl	

9.5 End User Mobile QC

Câmpul de date	Valoare		
Versiune	v3		
Număr Serial	automatic		
Algoritm de semnare	sha256withRSAEncryption		
Emitent	Atribut	Valoare	Codificare
	= Subject of Trans Sped Mobile eIDAS QCA G2		
Valabilitate	No more than 3 years		
Subiect	Atribut	Valoare	Codificare
	CN	<Common Name = First name + Last name>	PrintableString
	G	<First name>	PrintableString
	SN	<Last name>	PrintableString
	SER	<Personal Identification Code>	PrintableString
	OU	<Organizational Unit> optional	PrintableString
	O	<Organization> optional	PrintableString
	C	<Country Code>	PrintableString
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	
Private CertExtensions	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)	
subjectAltNames	no	Other Name / rfc822-Name = <Email Address>	
subjectKeyIdentifier	no	automatic	
authorityKeyIdentifier	no	= subjectKeyIdentifier of Trans Sped Mobile eIDAS QCA	
authorityInfoAccess	no	[1]accessMethod: caIssuers accessLocation: URL= http://www.transsped.ro/cacerts/ts_mobile_eidas_qca_g2.crt [2]accessMethod: OCSP accessLocation: URI: http://ocsp.transsped.ro	
cRLDistributionPoints	no	http://www.transsped.ro/crl/ts_mobile_eidas_qca_g2.crl	

9.6 OCSP responder certificate

Trans Sped QCA G2 OCSP Signer

Data Field	Value	
Version	v3	
Serial Number	Allocated automatically	
Signature Algorithm	sha256withRSAEncryption	
Issuer	Attribute	Value
	CN	Trans Sped QCA G2
	OU	Individual Subscriber CA
	O	Trans Sped SRL
	C	RO
Validity	No longer than 60 days from date of issue	
Subject	Attribute	Value
	CN	Trans Sped QCA G2 OCSP Signer
	OU	Individual Subscriber CA
	O	Trans Sped SRL
	C	RO
Subject Public Key	[RSA Key, 2048 Bit]	
Extension	Critical	Value
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

9.7 Trans Sped QCA G2 CRL

Parametrii emitenți ai CRL sunt:

Customer Root PCA	Value
CRL Issuance Period	6 hours
CRL Grace Period (seconds)	86400 (24 hours)
Automatically generate a new CRL when certificates are revoked (5.2) or Generate CRL based on revocation reason (5.3)	Checked
Include Authority Key ID extension in CRL	Checked (http://www.transped.ro/crl/ts_qca_g2.crl)
Issuing Distribution Point Extension (when required - inserted in a "CDP" CRL but not in full CRL) is critical	Unchecked
Remove Issuing Distribution Point from CRL (5.3 only)	Checked
Include Revocation Reason Extension when the reason is Unspecified	Unchecked
Include Hold Instruction Code in CRL entries	Checked

CRL-urile vor avea, prin urmare, următoarele câmpuri:

Field	Content
x.509 Fields	
Version	V2
CRL Number	Allocated automatically
Issuer Distinguished Name	Trans Sped QCA G2
This Update	Allocated automatically
Next Update	Allocated automatically
Signing Algorithm	SHA-256 with RSA encryption (1.2.840.113549.1.1.11)
x.509 Extensions	
Authority Key ID	KeyID=62 b5 7d f9 68 21 a6 0b b4 b6 5a 20 45 4b 4a 70 e0 53 e2 e9
Revoked Certificate List Entries:	
Certificate Serial Number	
Revocation date	
Revocation Reason Code	

GLOSAR

A

AC

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

ALGORITM ASIMETRIC

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

ALGORITMI CONVENȚIONALI

A se vedea algoritmi simetrici.

ALGORITMUL DE CRIPTARE A CHEII PUBLICE

A se vedea algoritmul asimetric.

ALGORITMUL DE SCHIMB DE CHEIE PUBLICĂ

O metodă de chei publică pentru schimbul sesiunii cheilor. Majoritatea algoritmilor cheii publice sunt folosiți pentru schimbul de chei secrete pentru algoritmi de criptare simetrică, nu pentru criptarea datelor. Diffie-Hellman este potrivit doar pentru schimbul de chei, în timp ce RSA este un algoritm de criptare a cheii publice.

ALGORITMUL CHEII SECRETE

A se vedea algoritmul simetric.

ALGORITMUL SIMETRIC

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

APLICAREA PENTRU CERTIFICAT

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

AMPRENTA DIGITALĂ

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

AUTENTIFICARE

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

AUTO-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 instituție de încredere care certifică cheile publice, adică emite certificate. În acest scop, sunt verificate informațiile conținute în cheia publică, în special identitatea deținătorului cheii.

AUTORITATEA DE ÎNREGISTRARE

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

CERTIFICAT CALIFICAT

Un certificat calificat este un certificat emis în conformitate cu Regulamentul eIDAS și în conformitate cu Legea semnăturii electronice din România. O semnătură produsă folosind un certificat calificat este considerată a fi legal egală cu semnătura olografă.

CIFRU BLOC

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

CEREREA PENTRU CERTIFICAT

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

CALEA DE CERTIFICARE

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

CERTIFICA

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

CERTIFICAT DIGITAL

A se vedea certificat.

CHEIE

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

CHEIA PRIVATĂ

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

CHEIA PUBLICĂ

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

CHEIA SESIUNII

În algoritmi hibrid, cheia utilizată pentru algoritmul de criptare simetric și schimbat prin algoritmul cheii publice. Cheia sesiunii este generată la întâmplare pentru fiecare schimb de date, adică pentru fiecare sesiune, în timp ce cheia publică rămâne aceeași pe o perioadă mai lungă de timp.

CHEIA SECRETĂ

A se vedea cheia privată.

CIFRU

Un cifru este un algoritm criptografic folosit pentru criptare.

CIFRU STREAM

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

CONFIRMA

A stabili prin anchetă și investigație adecvată.

CORESPUNDE

A aparține aceleiași perechi de chei.

CPD

A se vedea Definițiile Politicii de Certificare.

CRL

A se vedea Lista Certificatelor Revocate.

CRIPATANALIZA

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

CRIPTARE

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

CRIPTOGRAFIE

Criptografia este știința păstrării secretului unor mesaje.

CRIPTOLOGIE

Criptologia este zona din matematică care combină criptografia și criptanaliza.

CODUL DE PRACTICI SI PROCEDURI

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

D

DATELE DE ACTIVARE

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

DECRIPARE

Procesul de descifrarea al datelor înciptate.

DEPOZITAR

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

DES

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

DH

A se vedea Diffie-Hellman.

DIFFIE-HELLMAN

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

DPC

A se vedea Codul de Practici și Proceduri.

DN

A se vedea Nume distinct.

Dsa

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

Dss

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

E

EMITE UN CERTIFICAT

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

ENTITATE

A se vedea persoană.

F

Fsc

A se vedea Furnizorul de Servicii de Certificare.

FUNCTIA UN SINGUR SENS

A se vedea funcția hash.

FURNIZORUL DE SERVICII DE CERTIFICARE

Un Furnizor de Servicii de Certificare este o terță parte care conduce oricare din serviciile pe care o Autoritate de Certificare în general le furnizează, cum ar fi emiterea de certificate, un serviciu director, un respondent al statului certificatului online sau înregistrare entității.

G

GTC

A se vedea Termenii și Condițiile Generale.

H

FUNCTIA HASH

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

I-J

ID UTILIZATORULUI

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

IDEA

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

IETF

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

INELUL CHEII

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

K-L

LAN

Rețeaua Locală.

LDAP

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

LISTA CERTIFICATELOR REVOCATE

O listă care conține certificate revocate pe care AC le-a emis. În cazul în care o AC emite certificate în cadrul diferitelor politici de certificate, cu o cheie diferită de semnare utilizată pentru fiecare politică, multiple CRL-uri vor fi generate. Cu toate acestea, lista certificatelor revocate va fi identică pentru toate CRL-urile.

M

MD5

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

N

NIST

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

NSA

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

NUME DISTINCT

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

O-P

PAROLA FRAZĂ

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

PARTE DE ÎNCREDERE

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

PERECHEA DE CHEI

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

PERSOANĂ

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

PGP

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

PIN

Număr de Identificare Personală.

POLITICA DE CERTIFICARE

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

Q-R

RA

A se vedea Autoritatea de Înregistrare.

REVOCAREA

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

RSA

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

S

SEMNATAR

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

SEMNĂTURĂ DIGITALĂ (folosind algoritmul RSA)

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

SERVER-UL CHEII PUBLICE

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

SET DE PREVEDERI

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

SHA-2

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

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 și semnături digitale pentru schimbul sigur de e-mail. Certificatele S/MIME se bazează pe formatul X.509.

SSL

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

SUSPENDARE

Suspendarea este un proces de punere a unui certificat în așteptare, adică declarându-l temporar invalid. Acest lucru este în mod normal efectuat pentru că semnatarul suspectează că cheia sa privată a fost pierdută sau compromisă. Prin suspendarea cheii publice a certificatului se țintește împiedicarea altora de a aduce prejudicii prin pretinderea de a fi deținătorul cheii. Suspendarea cheii publice a certificatului îi anunță pe oameni că, pentru moment, cheia publică nu poate fi folosită pentru a cripta mesaje sau fișiere, și că semnăturile digitale efectuate folosind cheia privată corespunzătoare nu trebuie acceptate pentru moment. Un certificat bazat pe chei publice suspendat trebuie să fie revocat la confirmarea că cheia privată a fost într-adevăr pierdută sau compromisă, atunci când este inclusă pe CRL (Lista certificatelor revocate) de către Autoritatea de Certificare care emite, sau suspendarea poate fi ridicată, dacă, de exemplu, cheia privată a fost recuperată (adică nu este pierdută).

T

TERMENI ȘI CONDIȚII GENERALE

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

TIME-STAMP

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

TRIPLE-DES

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

U-V

W-Z

WAN

Rețea pe arie largă.

X.509

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