TRANS SPED

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

Versiunea 4 / 29 Iulie 2017

Cuprins

1. Introducere 7
1.1. Vedere de ansamblu 7
1.2. Identificare 8
1.3. Comunitatea şi Aplicabilitatea 8
1.3.1. Autorităţile de Certificare 8
1.3.2. Autorităţile de înregistrare 9
1.3.3. Entităţile finale 9
1.3.4. Aplicabilitatea 9
1.4. Detalii de contact 9
1.4.1. Specificarea organizării administrării 9
2. Prevederi Generale 11
2.1. Obligaţii 11
2.1.1. Obligaţiile AC 11
2.1.2. Obligaţiile AI 12
2.1.3. Obligaţiile Semnatarului 13
2.1.4. Obligaţiile părţii de încredere 13
2.1.5. Obligaţii privind depozitarul 13
2.2. Răspundere 13
2.2.1. Răspunderea AC 13
2.2.2. Răspunderea AI 14
2.3. Responsabilitate financiară 14
2.3.1. Despăgubirea de către părţile de încredere 14
2.3.2. Relaţiile fiduciare 14
2.3.3. Procesele Administrative 14
2.4. Interpretare şi Aplicare 14
2.4.1. Legea care guvernează 14
2.4.2. Separabilitate, supravieţuire, fuziune, notificare 14
2.4.2.1. Separabilitate 14
2.4.2.2. Supravieţuire 14
2.4.2.3. Fuziune 15
2.4.2.4. Notificare 15

2.4.3. Procedurile de soluţionare a disputelor 15
2.5. Taxele 15
2.6. Publicarea şi Depozitarul 15
2.6.1. Publicarea informaţiilor AC 15
2.6.2. Frecvenţa publicării 16
2.6.3. Controlul accesului 16
2.6.4. Depozitarele 16
2.7. Audit de Conformare 16
2.8. Confidenţialitatea 16
2.9. Drepturile de Proprietate Intelectuală 17
3. Identificare şi Autentificare 18
3.1. Înregistrarea iniţială 18
3.1.1. Tipuri de nume 18
3.1.2. Necesitatea pentru ca numele să aibă înţeles 18
3.1.3. Regulile pentru interpretarea unor diferite forme de nume 18
3.1.4. Unicitatea numelor 19
3.1.5. Procedura de soluţionare a disputelor legate de nume 19
3.1.6. Recunoaşterea, autenticitatea şi rolul mărcilor comerciale 19
3.1.7. Metoda de a dovedi deţinerea de cheie privată 19
3.1.8. Autentificarea identităţii organizaţiei 19
3.1.9. Autentificarea identităţii individuale 20
3.1.10. Informațiile abonatului neconfirmate 20
3.2. Rutina de acordare a unei chei noi 20
3.3. Acordarea de altă cheie după revocare 21
3.4. Cerere de revocare 21
4. Cerinţe operaţionale 22
4.1. Solicitarea unui certificat 22
4.2. Emiterea unui certificat 22
4.3. Acceptarea certificatului 22
4.4. Diseminarea certificatului 22
4.5. Suspendarea şi revocarea unui certificat 22
4.5.1. Circumstanţele pentru revocare 23
4.5.2. Cine poate solicita revocarea 23

4.5.3. Procedura pentru cererea de revocare 23
4.5.4. Perioada de graţie a cererii de revocare 24
4.5.5. Circumstanţele suspendării 24
4.5.6. Cine poate solicita suspendarea 24
4.5.7. Procedura pentru cererea de suspendare 24
4.5.8. Limitele perioadei de suspendare 24
4.5.9. Frecvenţa emiterii de CRL 25
4.5.10. Cerinţele de verificare ale CRL 25
4.5.11. Verificare disponibilităţii stării/ revocării on-line 25
4.5.12. Cerinţele de verificare a revocării on-line 25
4.5.13. Alte forme de înştiinţare de revocare disponibile 25
4.5.14. Cerinţele de verificare pentru alte forme de înştiinţare de revocare 25
4.5.15. Cerinţe speciale privind compromiterea cheii 25
5. Controalele de securitate fizice, de procedură şi de personal 26
5.1. Controale fizice 26
5.2. Controale de procedură 27
5.3. Controale personale 28
5.4. Procedurile de registre de audit 28
5.5. Arhivarea înregistrărilor 29
5.6. Schimbarea cheii 30
5.7. Compromiterea şi recuperarea după dezastre 30
5.8. Terminarea AC 30
6. Controale de securitate tehnică 31
6.1. Generarea şi instalarea perechii de chei 31
6.1.1. Generarea perechii de chei 31
6.1.1.1. Generarea perechii de chei AC 31
6.1.1.2. Generarea de cheie privată a semnatarului 31
6.1.2. Livrarea de cheie privată către entitate 31
6.1.3. Livrarea de cheie privată către emiţătorul de certificat 31
6.1.4. Livrarea de cheie privată către utilizatori 32
6.1.5. Dimensiunile cheii 32
6.1.6. Parametrii de generare de chei publice 32
6.1.7. Verificarea calităţii parametrului 32

6.1.8. Generarea de cheie hardware/software 33
6.1.9. Scopurile utilizării cheii (conform domeniului de utilizare a cheii X.509 v3) 33
6.2. Protecţia cheii private 33
6.2.1. Standardele pentru modulul criptografic 33
6.2.2. Controlul multi-persoane al cheii private (n din m) 33
6.2.3. Cheia privată escrow 33
6.2.4. Backup de cheie privată 33
6.2.5. Arhivarea cheii private 34
6.2.6. Intrarea cheii private în modulul criptografic 34
6.2.7. Metoda de activare a cheii private 34
6.2.8. Metoda de dezactivare a cheii private 34
6.2.9. Metoda de distrugere a cheii private 34
6.3. Alte aspecte legate de management-ul perechii de chei 35
6.3.1. Arhivarea cheii publice 35
6.3.2. Perioadele de utilizare pentru cheile private şi publice 35
6.4. Datele de activare 35
6.5. Controalele de securitate ale calculatorului 35
6.6. Ciclul de viaţă al controalelor tehnice 36
Controalele legate de dezvoltarea sistemului 36
6.6.1. Controalele management-ului de securitate 36
6.7. Controalele de Securitate ale Reţelei 36
6.8. Controale de Ingineria modulului criptografic 37
7. Profilele certificatelor şi CRL si OCSP 38
7.1. Profilul certificatului 38
Numărul (numerele) versiunii 38
7.1.1. Extensiile certificatelor 38
7.1.2. Identificatorii obiectului algoritm 38
7.1.3. Formele numelui 38
7.1.4. Constrângerile legate de nume 38
7.1.5. Obiectul identificator al politicii de certificate 38
7.1.6. Folosirea extensiilor constrângerilor politicii 39
7.1.7. Sintaxa şi semantica calificatorilor politicii 39

7.1.8. Procesarea semanticii pentru extensia critică a politicii de certificate 39
7.2. Profilul CRL 39
7.2.1. Numărul (numerele) versiunii 39
7.2.2. Extensiile de intrare CRL şi CRL 39
7.3. Profilul OCSP 39
Administrarea specifică 40
7.4 Procedurile de schimbare a specificaţiei 40
7.5 Politicile de publicare şi notificare 40
7.6 Procedurile de aprobare a CPP 40
8. Referinţe 41
9. Profile certificate 42
9.1 Trans Sped Root CA G2 42
9.2 Trans Sped QCA G2 43
9.3 Trans Sped Mobile eIDAS QCA 44
9.4 End User QC 45
9.5 End User Mobile QC 46
9.6 OCSP responder certificate 47
9.7 Trans Sped QCA G2 CRL 48
GLOSAR 49

1. Introducere

Realizarea de afaceri şi comunicarea prin reţele publice şi private devin din ce în ce mai importante în comerţul electronic. Una din cerinţele comunicării electronice este abilitatea de a identifica creatorul informaţiei electronice în acelaşi fel în care documentele sunt semnate folosind o semnătură olografă. Din punct de vedere tehnic acest lucru poate fi realizat prin semnăturile electronice. Valoarea semnăturilor electronice sporeşte semnificativ dacă emiterea unei semnături electronice către un individ este efectuată de către o terţă parte independentă şi de încredere. Această terţă 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 şi 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 şi măsuri de protecţie pentru a minimiza ameninţările operaţionale şi financiare şi riscurile asociate cu emiterea de certificate.

Acest document specifică practicile operării şi 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), şi în conformitate cu Specificaţiile tehnice 319 401 ale Institutului pentru Standardele Telecomunicaţiilor Europene (ETSI EN 319 401): Cerinţele privind politica generală a furnizorilor de servicii de încredere.

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

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

Deoarece certificatele calificate au la bază aceleaşi reglementări şi cerinţe definite în Regulamentul eIDAS şi în Legea Semnăturii Electronice din România ambele documente mai sus menţionate (CPP şi 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 şi trebuie ţinută secretă; cealaltă este publică şi poate fi pusă la dispoziţie pentru a fi regasită în registrul de chei publice, cum ar fi numerele de telefon dintr-o carte de telefon publică. Orice este criptat cu cheie privată poate fi decriptat doar cu cheia publică corespondentă (şi vice versa). Această tehnică poate fi utilizată pentru a implementa semnături digitale: expeditorul criptează datele folosind cheia lui privată, şi destinatarul poate verifica integritatea sa folosind cheia publică corespondentă dintr-un registru de chei publice.

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

O Autoritate de Certificare acţionează în calitate de terţă parte de încredere care leagă certificatele de entitatea indicată. Un certificat eliberat de către o AC conţine

numele semnatarului, numele AC, cheia publică a semnatarului, şi este semnat de către AC.

Trans Sped oferă certificate calificate emise în conformitate cu Regulamentul eIDAS şi 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 consecinţă 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 siguranţei certificatelor calificate emise şi pentru a dovedi respectarea Regulamentului eIDAS în combinaţie cu Legea de Semnătură Electronică din România, şi în conformitate cu cerinţele ETSI EN 319 401, Trans Sped publică prezentul CPP/PC în care sunt descrise procedurile folosite pentru emiterea de certificate calificate precum şi descrierea modului în care este efectuată verificarea datelor conţinute în certificat.

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

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

GLOSAR. De asemenea glosarul oferă definiţiile unor termeni importanţi care nu mai apar în altă parte în acest text şi care au legătură cu domeniile mai sus menţionate.

1.2. Identificare

SC Trans Sped SRL cu sediul în strada Despot Vodă, nr. 38, 020656 Bucureşti, România (denumită "Trans Sped" în aceast 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].

Prezentula CPP/PC este pus la dispoziţie la cerere prin e-mail sau poate fi preluat de la http://www.transsped.ro/repository .

1.3. Comunitatea şi Aplicabilitatea

Acest CPP/PC este pentru certificatele calificate care:

a) Întrunesc cerinţele prevăzute în anexa I din Regulamentul eIDAS;

b) Sunt emise de către TSP care respectă cerinţele prevăzute în anexa II din Regulamentul eIDAS;

c) Sunt pentru a fi utilizate doar cu dispozitive securizate de creare a semnăturii electronice (DSCRDSCS) care întrunesc condiţiile prevăzute în anexa II din Regulamentul eIDAS;

d) sunt emise către public.

1.3.1. Autorităţile 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. Autorităţile de înregistrare

O Autoritate de Înregistrare (AI) lucrează în numele unei AC. Trans Sped operează o Autoritate de Înregistrare internă dar poate în acelaşi timp să folosească furnizori de servicii externi ca AI subsidiare responsabile pentru verificarea atât a informaţiilor de afaceri cât şi a datelor personale incluse în certificatul 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. Ofiţerii de Înregistrare ai unei asemenea AI subsidiare sunt identificaţi individual; aceştia sunt prevăzuţi cu certificate speciale de Ofiţer de Înregistrare (RO). Doar informaţiile semnate de către RO vor fi acceptate de către AC.

Identificarea personală a utilizatorilor finali care aplică pentru un certificat 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 desfăşura de către ofiţerii mobili de identificare care operează în numele Trans Sped.

1.3.3. Entităţile 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 aplicaţiile în domeniul semnăturilor electronice şi 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 cerinţele prevăzute în [eIDAS];

b) Sunt emise de către Trans Sped în conformitate cu cerinţele prevăzute în [eIDAS];

c) Care sunt spre utilizare doar cu dispozitivele securizate de creare a semnăturii (DSCS) care respectă cerinţele cuprinse în [eIDAS];

d) sunt emise către public.

1.4. Detalii de contact

1.4.1. Specificarea organizării administrării

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

Persoană de contact

Administrator CPP/PC

SC Trans Sped SRL

Strada Despot Vodă, nr. 38

020656 Bucureşti

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 şi a CPP sunt determinate de Comitetul de CPP si PC al Trans Sped.

2. Prevederi Generale

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

2.1. Obligaţii

2.1.1. Obligaţiile AC

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

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

Scopul primar al oricărei Autorităţi de Certificare este de a oferi servicii de management de certificate (generare, utilizare operaţională, revocare şi expirare) pentru clienţi în cadrul respectivelor lor domeniu(ii) de politici.

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

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 incintă securizată fizic.

AC Trans Sped pentru certificate calificate îndeplineşte următoarele funcţii:

1. generează propriile chei.
2. Operează într-o manieră eficace şi de încredere şi în conformitate cu prezenta CPP/PC, Legea referitoare la Semnătura Electronică din România și [eIDAS].
3. Stabileşte Autorităţile 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 cerinţele ETSI EN 319 401, şi cerinţele cererii.
5. Se asigură că certificatele sunt lipsite de orice erori de înregistrări de date şi sunt corecte în baza informaţiilor cunoscute de către AC la momentul emiterii.
6. Informează solicitantul cu privire la măsurile necesare pentru a spori securitatea semnăturilor electronice calificate şi pentru a le testa în siguranţă.
7. Informează solicitantul că o semnătură electronică calificată are acelaşi efect în tranzacţiile legale precum semnătura olografă, 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 informaţiile de revocare către registru şi emite CRLs.
10. Notifică cu promptitudine deţinătorul certificatului cu privire la revocare.

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

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

Investigaţiile pot include, dar fără a se limita la:

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

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

2.1.2. Obligaţiile AI

O AI este asociată cu una sau mai multe AC şi acţionează în numele AC sale. O AI este responsabilă pentru înregistrarea solicitanţilor. Acesta efectuează verificarea identităţii şi verificarea tuturor datelor certificatului.

În special sarcinile unei AI sunt:

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

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

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

Orice AI trebuie să aibă angajaţi calificaţi corespunzător şi de încredere care să fie autorizaţi pentru a îndeplini îndatoririle AI. Staţia de lucru utilizată pentru depunerea informaţiilor de înregistrare către Trans Sped nu trebuie să fie public accesibilă, iar comunicarea prin canalele nesecurizate trebuie să fie protejate în mod adecvat.

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

2.1.3. Obligaţiile Semnatarului

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

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

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

2.1.4. Obligaţiile părţii de încredere

O parte de încredere va:

- Verifica validitatea sau revocarea certificatului folosind informaţiile stării de revocare actuale,
- Lua în calcul orice limitări legate de utilizarea certificatului indicate părţii de încredere din certificat,
- Lua orice alte precauţii prescrise în acorduri sau în altă parte.

2.1.5. Obligaţii privind depozitarul

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

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

Trans Sped protejează integritatea şi autenticitatea tuturor sistemelor care furnizează informaţii legate de starea certificatului.

2.2. Răspundere

2.2.1. Răspunderea AC

În calitate de 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 obligaţia de a face prevederi de acoperire corespunzătoare pentru a se asigura că poate să îndeplinească obligaţiile statutare pentru rambursarea pagubelor cauzate de o incalcare a obligatiilor.

2.2.2. Răspunderea AI

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

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

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

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

2.3. Responsabilitate financiară

2.3.1. Despăgubirea de către părţile de încredere

Pentru ambele feluri de părţi de încredere, părţile de încredere contractuale şi non-contractuale, reglementările referitoare la despăgubirile din legislaţia română sunt obligatorii.

2.3.2. Relaţiile fiduciare

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

2.3.3. Procesele Administrative

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

2.4. Interpretare şi Aplicare

2.4.1. Legea care guvernează

Legile din România și Regulamentul eIDAS vor guverna aplicabilitatea, construcţia, interpretarea şi valabilitatea prezentului CPP/PC şi 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, supravieţuire, fuziune, notificare

2.4.2.1. Separabilitate

Dacă părţi 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. Supravieţuire

În pofida faptului că prezentul CPP/PC poate în final să nu mai aibă efect, vor supravieţui următoarele obligaţii şi limitări ale CPP/PC: § 2 (Obligaţii), § 13

(Răspundere), § 2.3.3 (Procesele Administrative), § 2.4 (Interpretare şi Aplicare) şi § 2.8 (Confidenţialitate).

2.4.2.3. Fuziune

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

2.4.2.4. Notificare

Ori de către ori o parte doreşte 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, şi trebuie să fie adresată la:

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

E-mail-ul trebuie să fie confirmat de către destinatar în termen de o săptămână prin e-mail semnat digital. Dacă expeditorul nu primeşte 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 soluţionare a disputelor

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

Procedurile de soluţionare a disputelor legate de disputele între Trans Sped şi Clienţi pot fi prevăzute în acordurile între părţi. Procedurile de soluţionare a disputelor legate de disputele între Trans Sped şi Semnatari pot fi prevăzute în acordurile contractuale cu Semnatarii.

În cazul unei dispute, reclamaţie 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 Bucureşti
România

2.5. Taxele

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

2.6. Publicarea şi Depozitarul

2.6.1. Publicarea informaţiilor 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 şi 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 deţinătorul 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. Frecvenţa publicării

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

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

2.6.4. Depozitarele

Pentru locaţia depozitarului de certificate şi 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 si a Legii referitoare la Semnătura Electronică din România. Toate aceste audituri necesită demonstrarea unui nivel maxim de securitate şi conformitate cu politicile şi practicile documentate.

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

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

2.8. Confidenţialitatea

Trans Sped păstrează informaţii confidenţiale.

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

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

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

Trans Sped protejează toate datele personale şi legate de organizaţie care nu sunt incluse în certificat împotriva accesului neautorizat. Trans Sped îşi rezervă dreptul de a menţiona o organizaţie 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 numiţi în aceste certificate.

Prezentul CPP/PC reprezintă proprietatea intelectuală a Trans Sped.

3. Identificare şi Autentificare

3.1. Înregistrarea iniţială

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

Trans Sped se asigură că semnatarii sunt identificaţi şi autentificaţi în mod corespunzător şi că cererile legate de certificat sunt complete, corecte şi legal autorizate.

Înainte ca un certificat calificat să fie emis, Trans Sped informează semnatarul referitor la termenele şi condiţiile privind folosirea certificatului după cum sunt reglementate în Regulamentul eIDAS şi 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 şi în conformitate cu eIDAS, ETSI EN 319 401 și legislaţia română, identitatea şi, 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 înţeles

Trans Sped va determina ND al semnatarului să fie conform cu standardele, practicile şi alte reglementări.

Numele trebuie să aibă semantică comun înţeleasă (prenume şi nume, numele societăţii, adresa de e-mail) pentru ca partea de încredere să determine identitatea persoanei şi / sau organizaţiei.

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

3.1.3. Regulile pentru interpretarea unor diferite forme de nume

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

3.1.4. Unicitatea numelor

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

3.1.5. Procedura de soluţionare a disputelor legate de nume

Trans Sped nu este responsabil pentru soluţionarea disputelor legate de nume dintre semnatari. Trans Sped poate adăuga, la propria discreţie, informaţii adiţionale la un nume pentru a-l face unic printre numele certificatelor emise de Trans Sped.

3.1.6. Recunoaşterea, autenticitatea şi rolul mărcilor comerciale

Trans Sped va onora reclamaţiile legate de mărcile comerciale care sunt prezentate documentat de către un semnatar.

3.1.7. Metoda de a dovedi deţinerea 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. Autentificarea identităţii organizaţiei

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

Autorităţile guvernamentale sau administrative trebuie să furnizeze documentele care reflectă relaţia lor cu următoarea entitate mai înaltă (de ex: autoritate superioară) cu antet oficial, ştampilată cu ştampila oficială şi semnată de un funcţionar autorizat.

Documentaţia trebuie să cuprindă:

- Numele întreg şi statutul legal al persoanei juridice asociate sau altă entitate organizaţională,
- Informaţii de înregistrare existente relevante (de ex: înregistrarea societăţii) al persoanei juridice asociate sau altă entitate organizaţională.

3.1.9. Autentificarea identităţii individuale

Autentificarea unei entităţi 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 si ETSI EN 319 411-2.

Dovada identităţii 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 şi prenumele),
- Data şi locul naşterii,
- Un număr de serie sau alte atribute care pot fi folosite pentru a distinge persoana din altele cu acelaşi nume.

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

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

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

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 acelaşi. Acest proces este diferit de cel de reînnoire care presupune emiterea unui nou certificat, cu o perioadă de valabilitate prelungită, pentru aceeaşi cheie publică. (A se vedea [RFC4949].) Reînnoirea certificatelor calificate nu este suportată.

În momentul în care cheile trebuie schimbate, abonaţii sunt notificaţi 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. Reinnoirea 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. Reinnoirea 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.

Obţinerea unei noi cheii în cazul în care certificatul a expirat se face folosind aceleaşi reguli ca şi la înregistrarea iniţială. Întregul proces de înregistrare trebuie repetat.

Dacă noul certificat va conţine date despre o organizaţie, 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 şi 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:

- Prezenţa 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. Cerinţe operaţionale

4.1. Solicitarea unui certificat

Un semnatar depune o solicitare pentru certificat către Trans Sped şi 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 desfăşura 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:

- Declaraţia că informaţiile furnizate sunt corecte;
- Acordul la obligaţiile semnatarului;
- Acordul la publicarea certificatului în depozitar.

4.2. Emiterea unui certificat

Trans Sped verifică corectitudinea şi valabilitatea tuturor datelor necesare pentru emiterea unui certificat calificat (a se compara § 3.1.8 şi § 3.1.9). Trans Sped va verifica datele conţinute 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 inadvertenţe.

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

Perioada de valabilitate a certificatelor calificate este de un an de la data emiterii în conformitate cu Legea referitoare la Semnătura Electronică din România.

4.3. Acceptarea certificatului

La primirea unui certificat, semnatarul trebuie să verifice conţinutul acestuia. Dacă certificatul conţine greşeli care nu pot fi acceptate de către semnatar, semnatarul trebuie să informeze Trans Sped fără întârziere. Trans Sped atunci va revoca certificatul şi va lua măsurile care se impun fie de a restitui preţul 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 dispoziţie pentru a fi luate din depozitarul de certificate al Trans Sped de către terţe părţi doar cu acordul semnatarului.

4.5. Suspendarea şi 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 situaţiei. Dacă cheia privată a fost compromisă sau pierdută cu siguranţă, sau dacă datele semnatarului reprezentate în certificat s-au

schimbat în mod substanţial, 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 şi data revocării vor fi incluse în Lista Certificatelor Revocate, iar investigaţii legate de starea ulterioare la depozitarul certificatelor vor conducere la citarea certificatului drept invalid.

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

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

4.5.1. Circumstanţele pentru revocare

Un certificat este revocat în cazul în care:

1. Semnatarul sau o terţă parte autorizată au depus o cerere de revocare;
2. Trans Sped a aflat că au fost furnizate informaţii 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 şi 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 intr-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 deţinătorul lui poate acţiona în numele unei terţe părţi, această parte poate de asemenea solicita revocarea certificatului.

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

Oricine poate informa Trans Sped referitor la faptul că informaţiile 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 terţă parte autorizată poate solicita revocarea unui certificat prin completarea şi semnarea unui formular de revocare în faţa Ofiţerului de Înregistrare. Autentificarea este furnizată apoi de semnătura scrisă de mână.
2. Semnatarul sau o terţă 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 şi patru (24) de ore după primirea cererii.

4.5.4. Perioada de graţie a cererii de revocare

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

4.5.5. Circumstanţele suspendării

Un certificat este suspendat în cazul în care:

1. Semnatarul sau o terţă parte autorizată au depus o cerere de suspendare;
2. Trans Sped suspectează că au fost furnizate informaţii 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 deţinătorul lui poate acţiona în numele unei terţe părţi, această parte poate de asemenea solicita suspendarea certificatului.

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

Oricine poate informa Trans Sped referitor la faptul că informaţiile 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 terţă parte autorizată poate solicita suspendarea unui certificat pentru completarea şi semnarea unui formular de suspendare în faţa Ofiţerului de Înregistrare. Autentificarea este furnizată apoi de semnătura scrisă de mână.
2. Semnatarul sau o terţă 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 şi patru (24) de ore după primirea cererii.

4.5.8. Limitele perioadei de suspendare

Un certificat este suspendat pentru maximum şapte (7) zile după cererea de suspendare. Un certificat poate fi suspendat de două ori; o a treia suspendare şi depăşirea 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. Frecvenţa emiterii de CRL

Frecvenţa emiterii de CRL se va face la fiecare douăzeci şi patru (24) de ore, cel puţin. 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. Cerinţele de verificare ale CRL

Părţile 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 disponibilităţii 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 şi / sau parte de încredere.

4.5.12. Cerinţele de verificare a revocării on-line

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

4.5.13. Alte forme de înştiinţare de revocare disponibile

Nu există prevederi.

4.5.14. Cerinţele de verificare pentru alte forme de înştiinţare de revocare

Nu există prevederi.

4.5.15. Cerinţe speciale privind compromiterea cheii

În cazul în care semnatarul suspectează sau ştie cu siguranţă că cheia sa privată a fost compromisă, acesta este obligat să solicite revocarea cât mai curând posibil. Un semnatar nu este eliberat de obligaţiile sale de semnatar până ce nu este notificat de către Trans Sped în legătură cu revocarea certificatului.

5. Controalele de securitate fizice, de procedură şi de personal

Trans Sped are obligativitatea de a stabili şi menţine starea controalelor de securitate solicitate de către AC şi AI. Acest capitol oferă o descriere a cadrului de controale de securitate, care reflectă prevederile cuprinse în Legea referitoare la Semnătura Electronică din România, eIDAS şi ETSI EN 319 401. Prevederile respective se completează unele pe celelalte şi au menirea de a spori controalele de securitate în ansamblu. Toate acestea necesită cele mai înalte standarde de controale de securitate.

Din motive de securitate, 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-publice.

5.1. Controale fizice

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

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 cerinţele Legii referitoare la Semnătura Electronică din România și eIDAS. Orice acces neautorizat la informaţia depozitată, posibil provenind din pierderea, falsificarea, sau utilizarea greşită a acestora este împiedicată prin mijloace corespunzătoare. Verificările de securitate regulate sunt efectuate pentru a se asigura că aceste controale funcţionează corespunzător.

Accesul la orice zonă fizică unde sunt amplasate informaţiile sau echipamentul sensibil la operaţiunile AC necesită ca cel puţin două persoane autorizate să aibă acces la respectivele locaţii. Intrarea în zonele restricţionate folosind același dispozitiv token de două ori (pentru a sustrage cerinţa a două persoane diferite care au acces la respectiva locaţie) este împiedicată prin mijloace tehnice. De asemenea, zonele sensibile sunt monitorizate prin camere video.

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

Toate sistemele AC au energie electrică de industrie standard şi sisteme de aer condiţionat care să ofere un mediu de operare corespunzător. Toate sistemele AC au precauţii rezonabile luate pentru a minimiza impactul expunerii la apă. Toate sistemele AC au mecanisme standard de prevenire a incendiilor şi de protecţie în locaţie.

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

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

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

O AI nu stochează niciodată informaţiile legate de cheia semnatarului.

5.2. Controale de procedură

Procedurile operaţionale sunt documentate şi menţinute. Controalele de procedură asigură că nici o singură persoană care acţionează singur(ă) nu va putea înşela măsura de securitate luată.

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

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

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

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

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

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

5.3. Controale personale

Trans Sped se asigură că întregul personal implicat în emiterea, administrarea, suspendarea şi revocarea certificatelor calificate, precum şi datele şi informaţiile legate de administrare sunt integre, de încredere şi loiale. Acest lucru include, dar fără a se limita la solicitarea unui certificat emis de către poliţie, declararea că persoana în cauză nu are cazier de niciun fel. Întregul personal trebuie să aibă cunoştinţele şi experienţa necesare legate de operaţiunile AC şi trebuie să fi demonstrat conştiinciozitate şi cunoaşterea legată de securitate referitoare la îndatoririle sale la Trans Sped. Au loc revizuiri periodice pentru a verifica încrederea întregului personal.

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

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

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

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

5.4. Procedurile de registre de audit

Trans Sped păstrează rapoarte de audit şi fişiere ale sistemului de înregistrare care documentează acţiunile întreprinse ca parte din serviciile de 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 uneui nou CRL;
- generarea unui răspuns OCSP;
- schimbarea setărilor oricărei componente a AC;
- modificarea rolurilor utilizatorilor;
- modificarea profilului certificatului;
- modificarea profilului CRL;
- modificările setărilor politicii de securitate
- instalarea, ștergerea (resetarea), eliminarea, eliminarea, a unui HSM;
- încărcarea cheilor, certificatelor către HSM.
- accesul la o componentă a sistemului AC;
- fișiere sau înregistrări sensibile la securitate citite, scrise sau șterse
- accidente de sistem, defecțiuni hardware și alte anomalii
- activitatea firewall-ului și a ruterului
- intrarea / ieșirea vizitatorului instalației AC

Evenimentele din jurnalele de audit sunt 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, fişierele raportului de audit sunt salvate pe medii de tip WORM. Fişierele raportului de audit sunt arhivate de către un administrator de sistem săptămânal (cel puţin). Jurnalele de evenimente sunt revizuite cel puţin săptămânal de către auditorii interni.

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

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

5.5. Arhivarea înregistrărilor

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

Trans Sped utilizează arhivarea internă şi externă pentru a împiedica pierderea documentelor importante sau a datelor digitale. Arhivele sunt amplasate în locaţii diferite (interne sau externe) şi protejate de sistemele de control asupra accesului. In general, rapoartele privind certificatele calificate sunt reţinute cel puţin 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 restricţionat.

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. Acelaşi lucru este și cu CDP de certificate de utilizator final.

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

Schimbarea cheilor AC permite Trans Sped să modifice parametrii cheii şi algoritmii criptografici, ţinând cont de potrivirea algoritmilor şi parametrilor pentru a compensa noile descoperiri în ştiinţă şi/sau tehnologie. Orice AC nouă poate fi pusă la dispoziţie la cerere prin e-mail sau de la depozitarul Trans Sped la http://www.transsped.ro/repository .

5.7. Compromiterea şi recuperarea după dezastre

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

Rezervele unor informaţii de afaceri esenţiale şi sistemul software al AC sunt operate în fiecare zi. Procedurile de recuperare în caz de dezastre sunt testate cu regularitate. Documentaţia referitoare la aceste proceduri este considerată confidenţială.

5.8. Terminarea AC

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

Trans Sped va depune toate eforturile pentru a transfera înregistrările AC şi depozitarul de certificate către un alt emitent de certificate calificate. Trans Sped de asemenea va încerca să stabilească o procedură acceptabilă pentru semnatari şi părţile 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 semnatari vor fi revocate de către Trans Sped. Toată documentaţia relevantă va fi transferată către Organismul Român de Supraveghere (OS) după cum prevede Legea referitoare la Semnătura Electronică din România.

Semnatarii vor fi notificaţi dacă Trans Sped întreprinde o asemenea acţiune.

6. Controale de securitate tehnică

6.1. Generarea şi 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 prezenţa şi semnată de o terţă parte neimplicată în generarea de cheie propriu-zisă.

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

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

Nicio copie a niciunei chei private nu este păstrată în permanenţă 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 locaţii securitate. Nicio copie a cheilor private ale semnatarului nu este păstrată de către AC sau AI astfel că utilizarea lor greşită 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 garanţie 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 emiţătorul de certificat

Semnatarii transmit cheia publică generată ca pe o cerere electronică al cărei format trebuie să respecte PKCS#10 Sintaxa Cererii de Certificare. Solicitările 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 inițiala 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 acelaşi 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 periodei 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 permişi şi parametrii cheii pentru perechile de chei utilizate pentru certificate calificate sunt publicaţi de către eIDAS și ETSI. Trans Sped utilizează doar astfel de algoritmi şi parametri de cheie pentru certificate calificate care sunt definiţi a fi corespunzători.

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

6.1.7. Verificarea calităţii parametrului

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

6.1.8. Generarea de 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 § 38). Certificatele calificate pot fi utilizate pentru semnături electronice.

6.2. Protecţia 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 restricţionat 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 şi pot fi activate doar sub controlul dual într-o locaţie securizată din punct de vedere fizic.

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

6.2.5. Arhivarea cheii 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 locaţie securizată din punct de vedere fizic. Cheile arhivate nu sunt niciodată puse în producţie.

6.2.6. Intrarea cheii private în modulul criptografic

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

6.2.8. Metoda de dezactivare a cheii 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, şi este în prezenţa şi semnată de o terţă parte care nu este implicată în distrugerea propriu-zisă a cheii.

Toate copiile şi fragmentele cheii private sunt distruse la finalul ciclului de viaţă al perechii de chei.

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

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

Dacă un dispozitiv criptografic AC este în permanenţă scos din serviciu, atunci orice cheie conţinută în dispozitivul care a fost folosit în orice scop criptografic este ştearsă din

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

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

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

6.3. Alte aspecte legate de 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 şi 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 şi în fişierele de audit create pentru sistemul AC.

6.3.2. Perioadele de utilizare pentru cheile private şi publice

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

Pentru certificatele calificate perioada de valabilitate este de un an în conformitate cu Legea referitoare la Semnătura Electronică din România.

Folosirea cheilor private ale AC este limitată la peroada de timp in care algoritmii utilizați sunt considerați ca fiind adecvați pentru utilizare; întrebuințarea acestora va fi oprită după acel moment.

6.4. Datele de activare

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

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

6.5. Controalele de securitate ale calculatorului

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

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

securitate, principii, standarde, şi cerinţele de conformare de o importanţă specială pentru organizaţie.

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

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

6.6. Ciclul de viaţă al controalelor tehnice

Controalele legate de dezvoltarea sistemului

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

Trans Sped utilizează numai aplicații și dispozitive care:

- sunt echipamente 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 producţie. Mediile de testare şi de producţie sunt total necuplate.

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

6.6.1. Controalele management-ului de securitate

Trans Sped are mecanisme şi politici menite să controleze şi monitorizeze configuraţia şi integritatea sistemelor sale.

6.7. Controalele de Securitate ale Reţelei

Trans Sped a instalat protecţie corespunzătoare atât împotriva atacurilor interne cât şi externe (firewall, mecanisme de detectare de intruziune, etc.). Controalele de rutare sunt menite să asigure că conexiunile de calculator şi fluxurile de informaţii nu încalcă politica de control al accesului a aplicaţiilor de afaceri ale organizaţiei.

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

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

- perioada de valabilitate inițială a certificatului unui abonat

- revocarea certificatului unui abonat

- postarea actualizărilor CRL

- răspunsurile OCSP

6.8. Controale de Ingineria modulului 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 şi CRL si 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 şi 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 şi are valoarea `fals`.
- `keyUsage` este o extensie critică şi are valoarea `digitalSignature`, `nonRepudiation`.
- `subjectAltName` este o extensie non critică care permite identităţi adiţionale ce vor fi legate de subiectul certificatului cum ar fi adresa de e-mail sau UPN.
- `authorityKeyIdentifier` este o extensie non critică care identifică certificatul AC care trebuie utilizat pentru a verifica certificatul semnatarului.
- `qcStatements` este o extensie non critică şi are 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 combinaţie a algoritmului semnăturii digitale/funcţie hash care sunt permise pentru utilizarea certificatelor calificate.

Cheile actuale ale AC pentru emiterea de certificate calificate sunt cheile RSA cu 2048 bit şi 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 şi 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 opţional), sau trebuie să respingă certificatul.

7.2. Profilul CRL

7.2.1. Numărul (numerele) versiunii

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

7.2.2. Extensiile de intrare CRL şi CRL

Nu există prevederi.

7.3. Profilul OCSP

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

Administrarea specifică

Informaţii de contact:

TRANS SPED SRL
Strada Despot Vodă, nr. 38
020656 Bucureşti
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 specificaţiei

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

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

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

Această versiune a CPP/PC este datată februarie 2013.

7.5 Politicile de publicare şi notificare

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

7.6 Procedurile de aprobare a CPP

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

8. Referinţe

CEN/TS 419241 Cerințe de securitate pentru sisteme de încredere care susțin semnareaunui server.

[ETSI] ETSI EN 319 401: Semnăturile electronice şi infrastructuri (ESI); Cerințele privind politica generală a furnizorilor de servicii de încredere

ETSI EN 319 411-1: Semnături electronice și infrastructuri (ESI); Cerințe privind politica și securitatea pentru Furnizori de Servicii de Încredere care emit certificate, Partea 1: Cerințe generale

ETSI EN 319 411-2: Semnăturile electronice şi infrastructuri (ESI); Cerințele de Securitate și Politicile Furnizorilor de Servicii de Încredere pentru emiterea certificatelor;

Partea a 2-a: Cerințe pentru Furnizorii de Servicii de Încredere care emit certificate calificate în UE;

ETSI EN 319 412-2 Semnături electronice și infrastructuri (ESI);

Certificate de profil; Partea 2: Profil certificat pentru certificate eliberate persoanelor fizice

ETSI EN 319 412 -5 Semnături electronice și infrastructuri (ESI);

Certificate de profil; Partea 5: Situațiile QC

[eIDAS] REGULAMENTUL (UE) NR. 910/2014 AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE

[OS] Organismul de supraveghere

[RESA] Legea referitoare la Semnătura Electronică din România (Legea nr. 455/2001)

[RFC2828] Glosarul de Securitate Internet

[RFC5280] Internet X.509 Public Key Infrastructure

Profilul certificatului și a listei certificatelor revocate (CRL)

[X509] ISO/IEC 9594-8, Tehnologia informaţiei – Interconectare sisteme deschise – Registru: Cadrul de Autentificare. De asemenea publicat ca Recomandarea ITU-T X.509. A se vedea ediţia ITU-T Rec. X.509 (1993 E) sau ISO/IEC 9594-8:1995 cu Corrigendum Tehnic 1 şi Amendamentul 1 (Extensiile Certificatului) aplicate pentru certificatele X.509v3

9. Profile certificate

Această secțiune conține formatele pentru diferitele obiecte PKI, cum ar fi certificatele, 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: caIssuers accessLocation: URL=http://www.transsped.ro/cacerts/ts_root_g2.crt [2]accessMethod: OCSP accessLocation: URI: http://ocsp.transsped.ro	
cRLDistributionPoints	no	http://www.transsped.ro/crl/ts_root_g2.crl	

9.4 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	1 year		
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	1 year		
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.transsped.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 cheiei, sunt verificate

ALGORITM ASIMETRIC

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

ALGORITMII CONVENŢIONALI

A se vedea algoritmii simetrici.

ALGORITMUL DE CRIPTARE A CHEII PUBLICE

A se vedea algoritmul asimetric.

ALGORITMUL DE SCHIMB DE CHEIE PUBLICĂ

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

ALGORITMUL CHEII SECRETE

A se vedea algoritmul simetric.

ALGORITMUL SIMETRIC

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

APLICAREA PENTRU CERTIFICAT

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

AMPRENTA DIGITALĂ

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

AUTENTIFICARE

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

AUTO-SEMNAT

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

AUTORITATEA DE CERTIFICARE

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

AUTORITATEA DE ÎNREGISTRARE

O entitate care este responsabilă pentru identificarea şi autentificarea subiecţilor 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 deţine 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 şi X.509.

CERTIFICAT CALIFICAT

Un certificat calificat este un certificat emis în conformitate cu Regulamentul eIDAS şi 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 încriptează blocuri mai mari de text de dimensiune fixată, de obicei 64 bits (egal cu cinci caractere). Exemple de cifre bloc sunt IDEA, DES şi Triple-DES. A se vedea de asemenea cifrul stream.

CEREREA PENTRU CERTIFICAT

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

CALEA DE CERTIFICARE

Un lanţ comandat de certificate care împreună cu cheia publică a obiectului iniţial din cale, poate fi procesat pentru a obţine obiectul final din cale.

CERTIFICA

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

CERTIFICAT DIGITAL

A se vedea certificat.

CHEIE

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

CHEIA PRIVATĂ

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

CHEIA PUBLICĂ

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

CHEIA SESIUNII

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

CHEIA SECRETĂ

A se vedea cheia privată.

CIFRU

Un cifru este un algoritm criptografic folosit pentru criptare.

CIFRU STREAM

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

CONFIRMA

A stabili prin anchetă şi investigaţie adecvată.

CORESPUNDE

A aparţine aceleiaşi perechi de chei.

CPD

A se vedea Definiţiile Politicii de Certificare.

CRL

A se vedea Lista Certificatelor Revocate.

CRIPTANALIZA

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

CRIPTARE

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

CRIPTOGRAFIE

Criptografia este ştiinţa păstrării secretului unor mesaje.

CRIPTOLOGIE

Criptologia este zona din matematică care combină criptografia şi criptanaliza.

CODUL DE PRACTICI ŞI PROCEDURI

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

D

DATELE DE ACTIVARE

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

DECRIPTARE

Procesul de descifrarea al datelor încriptate.

DEPOZITAR

O colecţie de baze de date pentru depozitarea şi retragerea certificatelor, CRL şi orice alte informaţii legate de certificate şi semnături digitale, de exemplu prezenta DPC.

DES

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

DH

A se vedea Diffie-Hellman.

DIFFIE-HELLMAN

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

DPC

A se vedea Codul de Practici și Proceduri.

DN

A se vedea Nume distinct.

DSA

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

DSS

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

E

EMITE UN CERTIFICAT

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

ENTITATE

A se vedea persoană.

F

FSC

A se vedea Furnizorul de Servicii de Certificare.

FUNCŢIA UN SINGUR SENS

A se vedea funcţia hash.

FURNIZORUL DE SERVICII DE CERTIFICARE

Un Furnizor de Servicii de Certificare este o terţă 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 entităţii.

G

GTC

A se vedea Termenii şi Condiţiile Generale.

H

FUNCŢIA HASH

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

I-J

ID UTILIZATORULUI

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

IDEA

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

IETF

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

INELUL CHEII

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

K-L

LAN

Reţeaua Locală.

LDAP

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

LISTA CERTIFICATELOR REVOCATE

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

M

MD5

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

N

NIST

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

NSA

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

NUME DISTINCT

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

O-P

PAROLA FRAZĂ

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

PARTE DE ÎNCREDERE

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

PERECHEA DE CHEI

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

PERSOANĂ

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

PGP

PGP (Pretty Good Privacy), dezvoltat de către Phillip Zimmermann, este o aplicaţie foarte răspândit utilizată şi populară pentru schimbul de e-mail şi fişiere de încriptare sigur. Folosirea non-comercială este gratuită, utilizatorii comerciali vor trebui să obţină o licenţă de la PGP Inc.,.

PIN

Număr de Identificare Personală.

POLITICA DE CERTIFICARE

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

Q-R

RA

A se vedea Autoritatea de Înregistrare.

REVOCAREA

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

RSA

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

S

SEMNATAR

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

SEMNĂTURĂ DIGITALĂ (folosind algoritmul RSA)

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

SERVER-UL CHEII PUBLICE

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

SET DE PREVEDERI

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

SHA-2

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

S/MIME

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

SSL

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

SUSPENDARE

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

T

TERMENI ŞI CONDIŢII GENERALE

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

TIME-STAMP

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

TRIPLE-DES

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

U-V

W-Z

WAN

Reţea pe arie largă.

X.509

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