Sistemul de Tahografe Digitale pentru ROMANIA

Practicile si Procedurile pentru implementarea

Politicii de Certificare a RO-CA

CUPRINS

1 INTRODUCERE

Autoritatea Rutiera Romana este responsabila pentru functia de Autoritate Nationala de Certificare a infrastructurii de management a cheilor criptografice din cadrul sistemului de tahografe digitale introdus prin Reglementarea Consiliului UE nr. 3821/85, revizuita prin Reglementarea Comisiei CE nr. 1360/2002 si Reglementarea Comisiei CE nr. 432/2004.

Aceasta infrastructura de chei publice consta din sisteme, produse si servicii care asigura:

• Certificate pentru chei publice pentru componente de tahograf (carduri, unitati de vehicul si senzor de miscare);

• Chei de criptare pentru datele senzorilor de miscare.

Scopul acestui document este acela de a descrie practicile de certificare implementate de RO-CA.

Documentul a fost creat pentru a asigura conformitatea cu cerintele enuntate in Politica de

Certificare a RO-CA si se bazeaza pe cadrul creat prin IETF RFC 3647.

1.1 Descriere generala

Scopul principal al acestui document este acela de a fi folosit de catre RO-A si de catre cei care doresc sa evalueze gradul de incredere care poate fi acordat serviciilor oferite de RO-CA, sau sa determine masura in care acestea respecta cerintele sistemului pentru tahografe digitale.

Sistemul de management al cheilor criprografice (vezi figura urmatoare) este necesar pentru a implementa mecanismele de securitate definite in:

- Reglementarea Comisiei CE nr. 1360/2002, Anexa I(B), Appendix 11 Common Security Mechanisms
- ISO / IEC 16844-3 Road vehicles, Tachograph systems, Part 3: Motion sensor interface

RO-CA si RO-CP sunt operate sub responsabilitatea si autoritatea autoritatilor nationale sau a furnizorilor de servicii externi autorizati.

RO-CA are rolul de a certifica cheile RSA care sunt introduse in cardurile pt tahografe de catre RO-CP. Mai multe tipuri de carduri sunt emise soferilor, atelierelor, organelor de control si firmelor de transport.

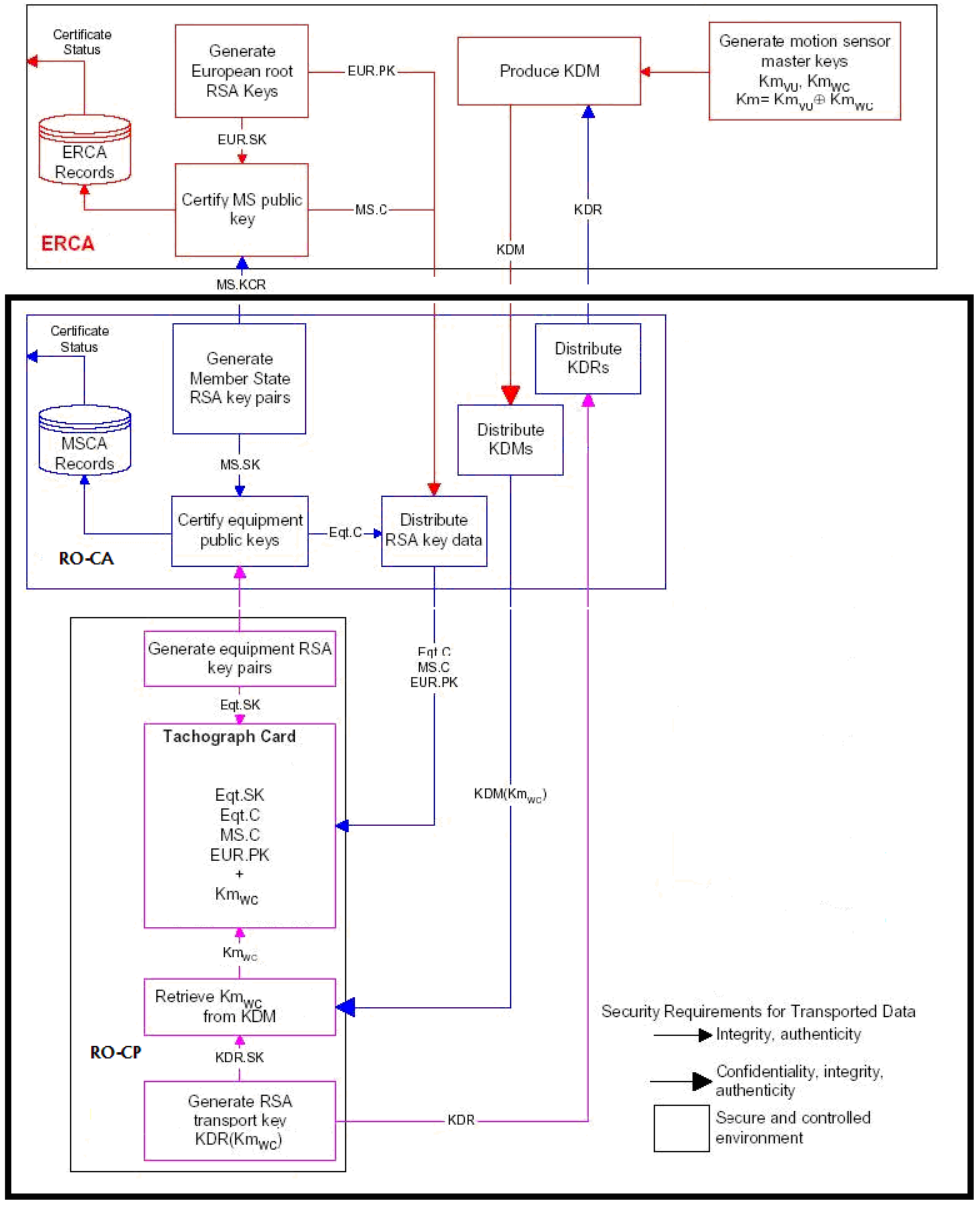
RO-CA isi schimba cheile la intervale regulate.

Formatul certificatelor digitale folosite este proprietar si incompatibil cu formatul X.509, al certificatelor digitale a caror utilizare este presupusa , dar nu ceruta obligatoriu de catre IETF RFC 3647.

RO-CA primeste de la ERCA si distribuie catre RO-CP o singura cheie criptografica simetrica, Km_{wc}, care va fi inserata de catre RO-CP in cardurile de atelier. Cheia este pastrata de RO-CP intr-un dispozitiv criptografic hardware de tip HSM

Pentru a asigura confidentialitatea cheii Km_{wc} in timpul transportului de la ERCA la RO-CP, ERCA o cripteaza folosind o cheie publica de criptare RSA de transport, pentru a produce un mesaj de distributie a cheii (KDM). Cheia de transport RSA folosita la crearea mesajelor KDM este creata la RO-CP si trimisa catre ERCA , printr-o cerere de distributie (KDR). Atat cererea KDR, cat si raspunsul KDM sunt transportate off-line intre ERCA si RO-CP prin intermediul RO-CA.

Necesitatea ca RO-CP sa primeasca cheia Km_{wc} este definita intr-un acord semnat de ERCA si RO-A.


Certificate Status
Generate European root RSA Keys
EUR.PK
Produce KDM
Generate motion sensor master keys
Km_{VU}, Km_{WC}
$Km = Km_{VU} \oplus Km_{WC}$
ERCA Records
EUR.SK
Certify MS public key
MS.C
KDR
ERCA
KDM
MS.KCR
Certificate Status
Generate Member State RSA key pairs
Distribute KDRs
Distribute KDMs
MSCA Records
MS.SK
Certify equipment public keys
Eqt.C
Distribute RSA key data
RO-CA
Generate equipment RSA key pairs
Eqt.C
MS.C
EUR.PK
Eqt.SK
Tachograph Card
Eqt.SK
Eqt.C
MS.C
EUR.PK
+
Km_{WC}
KDM(Km_{WC})
Km_{WC}
Retrieve Km_{WC} from KDM
RO-CP
KDR.SK
Generate RSA transport key KDR(Km_{WC})
KDR
Security Requirements for Transported Data
Integrity, authenticity
Confidentiality, integrity, authenticity
Secure and controlled environment

1.2 Numele si Identificarea Documentului

Acest document poarta denumirea de "Practicile si Procedurile de Certificare ale Autoritatii de Certificare Romane pentru Sistemul Tahografelor Digitale" si va fi referit in continuare simplu ca CPP.

1.3 Participanti

Acest CPP este creat doar pentru a indeplini cerintele sistemului pentru tahografe digitale din Romania.

1.3.1 Autoritati de Certificare

RO-CA si RO-CP sunt operate sub autoritatea si responsabilitatea autoritatilor romane responsabile, sau a furnizorilor de servicii autorizati. RO-CA este certificat de ERCA.

1.3.2 Autoritati de Inregistrare

Autoritatea Nationala de Inregistrare implementeaza sisteme, produse si servicii necesare pentru emiterea de carduri de tahograf. RA-ul national este responsabil pentru a mentine legatura intre identificatorii subiectilor certificatelor si persoanele fizice sau juridice care le folosesc. In Romania, functia RA pentru emiterea de certificate digitale pentru carduri de tahograf si a cheii Km_{wc} este asigurata de RO-CIA.

1.3.3 Abonati

Abonatii serviciilor de certificare oferite de RO-CA sunt utilizatorii cardurilor emise.

1.3.4 Entitatile partenere

Entitatile partenere sunt toate acele parti care solicita acces la informatiile despre certificatele emise de RO-CA.

1.3.5 Destinatarii Cheilor pentru Senzorii de Miscare

Destinatarii cheilor Km_{wc} sunt organizatiile care personalizeaza cardurile de atelier. Acestea sunt identificate in acordul semnat intre ERCA si RO-CA.

1.4 Utilizarea certificatului

Certificatele de cheie publica pentru tahografe trebuie inserate in componentele tahografelor digitale, asa cum se cere in procesul de autentificare mutuala descris in cerinta CSM_020 Reglementarea 1360/2002, Annex I(B) Appendix 11 Common Security Mechanism.

Certificatele pentru tahografele digitale pot fi folosite in aplicatii in legatura sistemul tahografelor digitale (de ex. Echipamente de calibrare utilizate in ateliere, echipamente pentru descarcarea de date folosite de organele de control, sisteme de management al flotelor auto si/sau marfurilor folosite de firmele de transport etc).

Certificatele pentru tahografe digitale nu pot fi folosite pentru nici un alt scop.

1.5 Utilizarea Mesajului pentru Distribuirea Cheii (KDM)

Mesajele KDM trebuie folosite doar in scopul transmiterii securizate a cheii Km_{wc} intre ERCA si RO-CP.

1.6 Administrarea CPP

1. Acest CPP este creat, mentinut si revizuit de catre ARR, care indeplineste functia de RO-CA:

   Autoritatea de Certificare pentru Sistemul Roman de Tahografe Digitale
   Autoritatea Rutiera Romana
   Strada ….

   Tel.+

   Fax +

2. Orice intrebare referitoare la prezentul CPP trebuie trimise catre:
   …..
3. Orice intrebare referitoare la operarea RO-CA trebuie trimisa catre responsabilul Ro-CA. Acesta este desemnat de catre Directorul General al ARR.
4. Autoritatea Nationala, RO-A, trebuie sa stabileasca daca acest CPP este conform cu Politica de Certificare a RO-CA.
5. Stabilirea conformitatii se bazeaza pe o evaluare de securitate realizata fie chiar de catre RO-A, fie de un tert autorizat.

1.7 Definitii si Acronime

Criptare Asimetrica: procesul de criptare in care o cheie este folosita pentru a cripta mesajul si o cheie diferita este utilizata pentru decriptarea mesajului.

Detectarea Intruziunii: detectarea unei intruziuni fizice de catre un agent de paza, sau a unei informatice de catre un sistem care cuprinde un senzor, un mediu de transmisie si un panou de alarma unde se trimite alarma.

Escrow-ul cheii: trimiterea unei copii a cheii catre o entitate autorizata sa foloseasca aceasta copie pentru alt scop decat acela de a-l returna entitatii care a generat cheia.

Criptare simetrica: procesul de criptare in care aceeasi chei este folosita si la criptarea mesajului si la decriptarea lui.

CAR	Certification Authority Reference
CHA	Certificate Holder Authorisation
CHR	Certificate Holder Reference
CP	Component Personaliser
CPI	Certificate Profile Identifier

CPS	Certification Practices Statement
CRL	Certificate Revocation List
CSP	Certification Service Provider
DES	Data Encryption Standard (symmetric encryption scheme)
EA	European Authority
ENI	ESSOR Nuclear Island
EOV	End Of Validity
ERCA	European Root Certification Authority
ETSI	European Telecommunications Standards Institute
KCR	Key Certification Request
KDR	Key Distribution Request
KDM	Key Distribution Message
Km	Motion sensor master key
Km_{wc}	Motion sensor master key inserted in workshop card
NCA	National Certification Authority
RO-MSA	Romanian Authority
RO-CA	Romanian Certification Authority
RO-CIA	Romanian Card Issuance Authority
OA	Operating Agent
OE	Operational Entity (used to refer to both a NCA and a CP)
OM	Operations Manager
PK	RSA public key
PKI	Public Key Infrastructure
PR	Permanent Representation of Member State
RSA	Rivest, Shamir, Adleman (asymmetric encryption scheme)
SAS	Single access system
SK	RSA secret key
TDES	Triple DES

2 PUBLICAREA INFORMATIEI RO-CA

2.1 Depozitele de inormatii

Responsabilul RO-CA are raspunderea fata de website-ul public http://www.certsign.ro, care este depozitul documentelor RO-CA.

2.2 Publicarea informatiei RO-CA

RO-CA publica urmatoarele informatii pe website-ul sau:

- Politica de Certificare RO-CA;
- Codul de Practici si Proceduri al RO-CA (acest document);
- Propunerile de modificare al CP si CPP RO-CA;
- RO-CA public key;

Conformitatea Politicii de Certificare a RO-CA este stabilita de catre ERCA la sfarsitul procesului de revizuire a politicii nationale, definit in Politica ERCA.

2.3 Frecventa publicarii

Informatiile referitoare la modificarile CP si CPS sunt publicate in conformitate cu planificarile facute in cadrul procedurilor de schimbare din fiecare document.

3 IDENTIFICAREA si AUTENTIFICAREA

3.1 Nume

Conceptul de nume ca un identificator al unei persoane fizice sau juridice nu se aplica in cazul certificatelor produse de RO-CA.

Emitentul certificatului si subiectul certificatului sunt identificati prin stringuri de lungime fixa de 8 octeti care contin informatia ceruta de protocolul mutual de autentificare dintre componenetele tahografice, definit in Reglementarea Commisie nr 1360/2002, Annex I(B) Appendix 11, cerinta CSM020.

3.1.1 Tipuri de Nume

Emitentul Certificatului si al KDM

Identificarea emitentului certificatului si al KDM se face prin referinta Certification Authority Reference (CAR), un string de 8 octeti definit in Reglementarea Comisiei nr. 1360/2002, Annex I(B) Appendix 1 - Data Dictionary, Section 2.36 CertificationAuthorityKID.

CAR este de asemenea folosita in timpul procedurii mutuale de autentificare dintre componentele tahografului pentru a identifica cheia publica folosita la verificarea certificatului.

Subiectul Certificatului

Acesta este format din:

- Certificate Holder Reference (CHR), un string de 8 octeti, string definit in Reglementarea Comisiei nr. 1360/2002 Annex I(B) Appendix 1, Section 2.36 CertificationAuthorityKID;
- Certificate Holder Authorisation (CHA), un string de 7 octeti, string definit in Reglementarea Comisiei nr. 1360/2002, Annnex I(B) Appendix 1, Section 2.34 si include EquipmentType, 1 octet as definit in Reglementarea Comisiei nr. 1360/2002 Annex I(B) Appendix 1, Section 2.52. Pentru certificatele de cheie publica emise de RO-CA, EquipmentType desemneaza o cartela de tahograf.

CHR apare in materialele printate si in datele descarcate din unitatea de vehicul. EquipmentType codificat in CHA este folosit in timpul procedurii mutuale de autentificare si selecteaza unul dintre cele patru moduri de operare ale unitatii de vehicul (operare, calibrare, control sau companie).

Key Distribution Message Recipient

Destinatarul final al cheii senzorului de miscare Km_{wc} este RO-CP. In scopul distributiei acesteia, fiecare cerere KDR este identificata astfel:

- Key Identifier (KID): un string de 8 octeti definit in Politica ERCA [3] Annex D. 1.
- Message Recipient Authorisation (MRA): un string de 7 octeti definit in Politica ERCA [3] AnnexD.1.

KID identifica unic cheia publica RSA folosita la criptarea cheii senzorului de miscare. MRA identifica cheia senzorului de miscare.

3.1.2 Necesitatea ca numele sa aiba inteles

Intelesul care il au:

- Emitentul certificatului
- Subiectul certificatului
- Destinatarul KDM

sunt definite in Reglementarea Comisiei nr. 1360/2002 Annex I(B) Appendix 1; si in Politica ERCA, Annex **D.**

3.1.3 Anonimatul sau folosirea pseudonimelor pentru abonati

Legatura dintre nume si persoanele fizice sau juridice este asigurata de RA (RO-CIA); ea nu poate fi stabilita din continutul certificatelor de cheie publica.

Ca urmare, numele utilizate de RO-CA pentru certificarea si distribuirea cheilor folosite in tahografele digitale sunt pseudonime pentru abonatii RO-CA.

Anonimatul abonatilor nu este permis.

3.1.4 Reguli pentru interpretarea diferitelior forme ale numelor

Nu se stipuleaza nimic.

3.1.5 Unicitatea numelor

Pentru ca procesul autentificarii mutuale sa functioneze corect, identificatorul emitentului certificatului trebuie sa identifice unic o pereche de chei RSA.

3.1.6 Recunoasterea, autentificare si rolul brandurilor

Nu se stipuleaza nimic.

3.2 Validarea Initiala a Identitatii

3.2.1 Metoda pentru a demonstra posesia cheii private

Cererile KCR pt certificarea cheilor publice asociate cheilor private care sunt introduse in carduri trebuie sa demonstreze posesia cheii private corespunzatoare.

Mesajele KCR constau din doua parti: o parte de text necodificat si semnatura digitala a acelui text. Intotdeauna textul include o cheie publica RSA. Semnatura digitala a textului

este creata cu cheia privata corespunzatoare.

Verificarea semnaturii digitale realizata cu cheia publica demonstreaza:

- Posesia cheii private;
- Integritatea textului.

Verificarea semnaturii este facuta la RO-CA. Daca verificarea esueaza, cererea de certificat este respinsa.

3.2.2 Autentificarea identitatii individuale

Legatura unica dintre aplicant (driver/firma de transport/atelier/politie), card, cheia privata si certificatul care se insereaza in card se realizeaza prin toate procesele care au loc la RO-CIA (inregistrarea aplicantului, emiterea cererii de carduri si transmiterea ei catre RO-CP), RO-CP (primirea cererii de card, inregistrarea ei, emiterea cererii de certificat si transmiterea ei catre RO-CA si ulterior inserarea certificatului in card) si RO-CA (primirea cererii de certificat, inregistrarea ei, emiterea certificatului si trimiterea acestuia inapoi catre RO-CP).

3.3 Identificarea si Autentificarea pentru Cererile de Re-key

3.3.1 Identificarea si autentificarea pentru cererile de re-key de rutina

Nu se aplica.

3.3.2 Identificarea si autentificarea pentru cerereile de re-key dupa revocare

Nu se aplica

3.4 Identificarea si Autentificarea pentru Cererile de Revocare

Certificatele pentru cardurile de tahograf nu se revoca. Pierderea cartelei trebuie raportata de catre posesorii acesteia la RO-CIA, care le publica intr-un blacklist.

4 CERINTELE OPERATIONALE PENTRU CICLUL DE VIATA AL CERTIFICATELOR

4.1 Cererea de Certificat

4.1.1 Cine poate face o cerere de certificat

Viitorii posesori de carduri nu fac cereri de certificate, ci certificatele sunt emise pe baza informatiile furnizate in cererea pentru cardurile de tahograf si preluate din registrul RO-CIA. Cheia publica care trebuie certificata este extrasa din cererea de certificat. RO-CA accepta doar cererile de certificat primite de la RO-CP. Aplicatiile software de la RO-CA si cele de la RO-CP asigura ca o cerere de certificat este generata doar pentru acele carduri pentru care exista o cerere si ca cel care a facut cererea este autentificat si autorizat.

4.1.2 Procesul de inregistrare si responsabilitatile asociate

Procesul de inregistrare este administrat la RO-CIA.

4.2 Procesarea Cererilor de Certificat

4.2.1 Identificarea si autentificarea

Functiile de identificare si autentificare sunt implementate la RO-CIA. RO-CP asigura prin aplicatiile sale software ca datele de intrare contin informatii care fac Certificate Holder Reference (CHR) unic.Si RO-CA asigura emiterea unui certificat unic pt un CHR dat.

4.2.2 Aprobarea sau respingerea cererilor de certificate

Daca cererile sunt semnate cu cheia privata asociata cheii publice care trebuie certificata, atunci cererea este acceptata. In caz contrar, ea este respinsa.

4.2.3 Timpul necesar pentru prelucrarea cererilor de certificate

Dupa primirea unei cereri valide de certificat, acesta este emis in maxim 24 de ore.

4.3 Emiterea Certificatului

4.3.1 Actiunile RO-CA in timpul emiterii certificatului

Structura certificatelor emise de RO-CA prin intermediul aplicatiei tachoSAFE CA este conforma cu cerintele specificate de Reglementarea Comisiei Europene (EC) 1360/2002, Anexa IB, Appendix 11, cerintele CSM_016, CSM_017, CSM_018. Astfel, certificatele emise pentru cartelele tahografice contin identificarea tipului de echipament pentru care sunt emise (cartele tahografica de sofer, de companie, de control, sau de atelier). De asemenea, certificatele contin identificatorul autoritatii emitente (prin intermediul campului CAR – Certification Authority Reference), identificandu-se astfel inclusiv statul membru emitent (Romania) precum si tipul autoritatii emitente (operationala sau de test).

Urmatoarele informatii sunt inregistrate in baza de date a RO-CA pentru fiecare operatie de certificare de cheie:

- certificatul complet;
- modulul RSA (n) si exponentul public (e) ale cheii publice
- perioada de validitate a certificatului;
- Certificate Holder Reference (pentru identificarea cheii publice RSA);
- timestamp.

4.4 Acceptarea certificatului

4.4.1 Comportament care semnifica acceptarea certificatului

Acceptarea cardului inseamna si acceptarea certificatului asociat.

4.4.2 Distribuirea certificatelor de carduri si a informatiei aferente

Toate certificatele emise de catre tahcoSAFE CA pentru cartelele tahografice sunt stocate in baza de date interna a autoritatii de certificare. Pentru fiecare certificat emis, se pastreaza de asemenea cererea de certificat corespunzatoare (cu toate detaliile sale) primita de la RO-CP, pe baza careia s-a cerut emiterea acelui certificat. In felul acesta, autoritatea de certificare va pastra inregistrari cu toate cheile publice certificate precum si tipul de echipamente pentru care s-au facut acele certificari, asigurandu-se cerinta CSM_008, din Reglementarea Comisiei Europene (CE) 1360/2002, Anexa IB, Appendix 11.

4.5 Folosirea Perechii de Chei si a Certificatului

4.5.1 Folosirea Perechii de Chei si a Certificatului

Certificatele pentru componenentele sistemului de tahografe digitale sunt destinate numai in cadrul acestuia.

Key-pair usage	Key-pair usage period	Component service life	Key-pair certificate validity
Driver card issuing	2 years	5 years	7 years
Workshop card issuing	6 years	1 year	7 years

Usage periods for RO-CA key-pairs

4.5.2 Folosirea cheii publice si a certificatului de catre entitatile partenere

Vezi 4.4.2.

4.6 Reinnoirea Certificatului

Nu se aplica.

4.7 Re-key

Nu se aplica.

4.8 Modificarea Certificatului

Nu se aplica.

4.9 Revocarea Certificatului

Nu se aplica.

4.9.1 Cerinte speciale referitoare la compromiterea cheii

Compromiterea cheii este un incident de securitate care cere o serie de actiuni.

Daca cheia RO-CA este compromisa, sau se suspecteaza ca este compromisa, atunci RO-CA trebuie sa raporteze incidentul la RO-A. Investigatiile care urmeaza si eventualele actiuni sunt descrise in Politica de certificare nationala.

4.9.2 Suspendarea certificatului

Nu se aplica.

4.10 Servicii de Verificare a Starii Certificatului

Nu se aplica.

4.11 Escrow-ul si Recuperarea Cheii

Escrow-ul cheii este strict interzisa de Politica ERCA.

5 CERINTELE CICLULUI DE VIATA AL CHEII SENZORULUI DE MISCARE

Mecanismele de securitate referitoare la senzorul de miscare al tahografului digital sunt descrise in ISO / IEC 16844-3. Cheile senzorului de miscare sunt generate de ERCA si trebuie distribuite in mod sigur catre RO-CA. Mai departe RO-CA le va distribui catre RO-CP.

Cheile de transport RSA transport trebuie sa aiba modul de 1024 biti. Generarea cheilor de transport este realizata intr-un mediu controlat si sigur de catre RO-CP, in conformitate cu Politica de Certificare RO-CA si cu Codul de Practici si Proceduri al RO-CP. Nu exista si nici nu se intrevad pe viitor servicii similare cu suspendarea, revocarea sau verificarea starii pentru mesajele KDM.

5.1 Cererile pentru Serviciile de Distribuire a Cheii Senzorului de Miscare

5.1.1 Cine poate trimite o cerere de distribuire a cheii senzorului de miscare

RO-CA accepta cereri de distributie doar de la RO-CP.

5.1.2 Procesul de inregistrare si responsabilitatile asociate

Procedura de inregistrare pentru destinatarii cheilor master ale senzorului de miscare este aceeasi ca cea pentru serviciile de certificare ale RO-CA, descrise la sectiunea 4.1.2.

5.2 Procesarea cererilor KDR pentru cheia senzorului de miscare

Prin trimiterea de cererri KDR, destinatarii cheii senzorului de miscare adera la termenii prezentului CPP.

5.3 Distribuirea KDM a cheii senzorului de miscare

RO-CA primeste KDM de la ERCA pe CD si il transmite mai departe catre RO-CP.

5.4 Folosirea Cheii Senzorului de Miscare

5.4.1 Folosirea cheii de catre destinatar

Folosirea cheii senzorului de miscare este restrictionata la acele scopuri autorizate de Politicile ERCA si RO-CA pentru sistemul tahografelor digitale si in conformitate cu prezentul CPP.

Destinatarii folosesc cheia de transport RSA doar pentru a crea o cerere KDR si pentru a recupera cheia senzorului de miscare din KDM.

Nu exista nici o prevedere referitoare la perioadele de folosire a cheii senzorului de miscare.

5.4.2 Responsabilitatile Entitatilor Partenere

Nu exista nici o prevedere.

5.5 Cerinte speciale referitoare la compromiterea cheii

Compromiterea cheii este un incident de securitate care reclama o serie de actiuni.

Daca o copie a unei chei a senzorului de miscare a fost compromisa sau se suspecteaza ca este compromisa, atunci RO-CP trebuie sa raporteze incidentul catre RO-A pentru investigatii si pentru actiuni in conformitate cu politica nationala.Rezultatul acestor investigatii se raporteaza catre ERCA.

6 CONTROALE DE SECURITATE FIZICĂ, ORGANIZAȚIONALĂ ŞI DE PERSONAL

Acest capitol descrie cerințele generale privind securitatea fizică şi organizațională, precum şi activitatea personalului RO-CA în activitatea de generare de chei, verificarea autenticității entităților, emiterea şi publicarea certificatelor, revocarea certificatelor, audit şi crearea de copii de siguranță.

6.1 Controale de securitate fizică

6.1.1 Controale de securitate fizică în cadrul RO-CA

Sistemele de calcul, terminalele operatorilor şi resursele informaționale ale RO-CA sunt dispuse într-o zonă dedicată, protejată fizic împotriva accesului neautorizat, distrugerilor sau perturbării activității. Aceste locații sunt monitorizate. Fiecare intrare şi ieşire este înregistrată în jurnalul de evenimente (log-urile sistemului); stabilitatea sursei de electricitate precum şi temperatura sunt de asemenea monitorizate şi controlate.

Amplasarea locației

RO-CA este localizată în Bucureşti, la următoarea adresă:

SC certSIGN srl, Sos Oltenitei nr. 107A, Corp C1, parter, CP 041303, Bucuresti, Romania

Accesul fizic

Accesul fizic în cadrul RO-CA este controlat şi monitorizat de un sistem de alarmă integrat. RO-CA dispune de sisteme de prevenire a incendiilor, sisteme de detectare a intruşilor şi sisteme de alimentare cu energie electrică în caz de urgență.

Sediul RO-CA şi Autoritatea de Certificare sunt accesibile publicului în fiecare zi lucrătoare între 10:00 şi 16:00. În restul timpului (inclusiv în zilele nelucrătoare), accesul este permis numai persoanelor autorizate de către conducerea RO-CA. Vizitatorii locațiilor aparținând RO-CA trebuie să fie însoțiți permanent de persoane autorizate.

Zonele ocupate de RO-CA se împart în:

- zona serverelor,

- zona administratorilor CA
- zona administratorilor de sistem,
- zona de dezvoltare şi testare.

Zona serverelor este echipată cu un sistem de securitate monitorizat continuu, alcătuit din senzori de mişcare, efracție şi incendiu. Accesul în această zonă este permis numai personalului autorizat, de exemplu, ofiterului de securitate, administratorul Autorității de Certificare şi administratorul de sistem. Monitorizarea drepturilor de acces se face folosind carduri şi cititoare, montate lângă punctul de acces. Fiecare intrare şi ieşire din zonă este înregistrată automat în jurnalul de evenimente.

Controlul accesului în *zona administratorilor* se face prin intermediul cardurilor şi a cititoarelor de carduri. Deoarece toate informațiile senzitive sunt protejate prin folosirea unor seifuri, iar accesul la terminalele administratorilor necesită în prealabil autorizarea acestora, securitatea fizică în această zonă este considerată ca fiind adecvată. Cheile de acces pot fi ridicate numai de personalul autorizat. În această zonă au acces numai angajații RO-CA şi persoanele autorizate; ultimilor nu le este permisă prezența în zonă neînsoțiți.

Zona de dezvoltare şi testare este protejată într-o manieră similară cu zona operatorilor şi administratorilor. În această zonă este permisă şi prezența persoanelor neînsoțite. Programatorii şi dezvoltatorii nu au acces la informații senzitive. Dacă este necesar un astfel de acces, atunci el se poate face numai în prezența administratorul de securitate. Proiectele în curs de implementare şi software-ul aferent este testat în mediul de dezvoltare al RO-CA.

Sursa de alimentare cu electricitate şi aerul condiționat

Zona operatorilor şi administratorilor, precum şi zona de dezvoltare şi testare sunt prevăzute cu aer condiționat. Din momentul întreruperii alimentării cu energie, sursele de electricitate de urgență (UPS) permit continuarea neperturbată a activității până la intervenția automată a grupului electrogen al clădirii.

Expunerea la apă

Riscul de inundație în zona serverelor este foarte mic, deoarece distanța față de conductele de apă este mare, iar locația RO-CA este la ultimul etaj. În plus, personalul

de pază este localizat chiar lângă zona serverelor şi este instruit să anunțe imediat administratorul RO-CA şi administratorul clădirii.

Prevenirea incendiilor

Locația RO-CA dispune de sistem de prevenire şi protecție împotriva incendiilor în conformitate cu standardele şi reglementările în domeniu.

Depozitarea mediilor de stocare a informațiilor

În funcție de sensibilitatea informațiilor, mediile electronice care conțin arhivele şi copiile de siguranță ale datelor curente sunt stocate în seifuri metalice, localizate într-o camera cu grad ridicat de securitate. Accesul la camera şi seifuri este permis numai persoanelor autorizate.

Aruncarea deşeurilor

Hârtiile şi mediile electronice care conțin informații importante din punct de vedere al securității RO-CA sunt distruse după expirarea perioadei de păstrare. Modulele de securitate hardware sunt resetate şi şterse conform recomandărilor producătorului. Aceste dispozitive sunt, de asemenea, resetate şi şterse atunci când sunt trimise în service sau reparate.

Depozitarea backup-urilor în afara locației

Copiile parolelor, codurile PIN şi cardurile criptografice sunt stocate în containere speciale, situate în afara locației RO-CA.

Stocarea în afara locației se aplică şi în cazul arhivelor, copiilor curente ale informațiilor procesate de sistem şi kit-urilor de instalare ale aplicațiilor RO-CA. Acest lucru permite refacerea de urgență a oricărei funcții a RO-CA în 48 de ore, în locația principală a RO-CA, sau în locația auxiliară.

6.2 Controlul securității organizației

Acest capitol prezintă rolurile ce pot fi atribuite personalului aparținând RO-CA. De asemenea, tot în acest capitol sunt descrise responsabilitățile şi sarcinile specifice fiecărui rol.

6.2.1 Roluri de încredere

Roluri de încredere în RO-CA

În RO-CA sunt definite următoarele roluri de încredere, care pot fi atribuite uneia sau mai multor persoane:

- **Responsabilul RO-CA**

    - Este responsabil pt operarea sigura si fara probleme a RO-CA ca organizatie .
    - Este reprezentantul organizatiei si este autorizat sa dea instructiuni in cadrul ei
    - Nu este direct implicat in implementarea proceselor de business, dar este responsabil pt respectarea si evaluarea masurilor de securitate
    - Accepta responsabilitatea pt managementul schimbarii

- **Administrator de securitate (Ofiterul de securitate informatica)**

    - Atribuirea privilegiilor de securitate si controlul accesului pt administratorul CA
    - Crearea parolelor pt toate conturile noi
    - Arhivarea inregistrarilor
    - Revizuirea logurilor de audit pt a verifica respectarea de catre administratorii CA a politicilor de securitate a sistemelor. Revizuirea se va face saptamanal.
    - Conducerea sau supravegherea unui inventar anual al inregistrarilor RO-CA
    - Participarea la generarea cheii RO-CA

- **Administratorul de sistem**

    - Configurarea initiala a sistemelor , inclusiv pt pornirea si oprirea sigura
    - Administrarea sistemelor
    - Crearea si configurarea conturilor;

- Administrarea conturilor
- Crearea configuratiei initiale a retelei;
- Administrarea retelei
- Crearea de CD-uri pt repornirea de urgenta a sistemelor
- Crearea de copii de siguranta, updatarea softului

- CA Administrator
  - Generarea cheilor;
  - Generarea certificatelor;
  - Functii administrative asociate cu intretinerea bazei de date a RO-CA si participarea la investigarea incidentelor.

- **Key Administrator (HSM Operator)**
  - CA key container authorization for CA key/KCR generation
  - - CA key container authorization for CA certificate importing
  - - CA key container authorization for CA key usage (signing certificates)
- **HSM Administrator**
  - Initializarea si administrarea dispozitivului hardware de protectie a cheilor (HSM)

  The function of the HSMA can be implemented only on the basis of the 'four-eyes-principle'.
- **Auditorul de sistem** – autorizat să acceseze arhivele şi log-urile de audit ale sistemelor de încredere ale Autorității de Certificare. Responsabil de efectuarea de audituri interne pentru respectarea Codului de Practici şi Proceduri de către Autoritatea de Certificare; această responsabilitate se extinde şi asupra fiecărei Autorități de Înregistrare care operează în cadrul RO-CA.

*În cadrul RO-CA, rolul de **auditor** nu poate fi combinat cu nici un alt rol. O entitate care are un rol diferit de cel de auditor nu poate prelua responsabilitățile auditorului.*

6.2.2 Numărul de persoane necesare pentru îndeplinirea unei sarcini

Procesul de generare de chei – pentru semnarea certificatelor – este una din operațiile ce necesită o atenție deosebită. Generarea necesită prezența a cel puțin trei persoane: CA Admin, 2 Key Admin

Prezența Administratorului Autorității de Certificare şi a unui număr corespunzător de Key Admin este necesară şi la importul certificatului corespunzator cheii criptografice a Autorității de Certificare în modulul hardware de securitate. Orice altă operațiune sau rol, descris în cadrul CPP poate fi efectuată de o singură persoană, special desemnată în acest sens.

6.2.3 Identificarea şi autentificarea pentru fiecare rol

Personalul RO-CA este supus identificării şi autentificării în următoarele situații:

- plasarea pe lista de persoane care au dreptul de a accesa locațiile RO-CA ,
- plasarea pe lista de persoane care au acces fizic la sisteme şi resurse de rețea aparținând RO-CA,
- emiterea confirmării care autorizează îndeplinirea rolului asignat,
- asignarea unui cont şi a unei parole în sistemul informatic al RO-CA,

Fiecare cont asignat:

- trebuie să fie unic şi asignat direct unei anumite persoane,
- nu poate fi folosit în comun cu nici o altă persoană,
- trebuie restricționat conform funcției (ce reiese din rolul îndeplinit de persoana respectivă) pe baza software-ului de sistem al RO-CA, a sistemului de operare şi a controalelor de aplicații.

Operațiile efectuate în RO-CA care necesită acces la resurse de rețea comune sunt protejate prin mecanisme de autentificare sigură şi de criptare a informațiilor transmise.

6.3 Controlul personalului

RO-CA trebuie să se asigure că persoana care îndeplineşte responsabilitățile funcției, conform cu rolul atribuit în cadrul unei Autorități de Certificare:

- a absolvit cel puțin liceul,
- este cetățean român,
- a semnat un contract care descrie rolul şi responsabilitățile sale în cadrul sistemului,

- a beneficiat de un stagiu de pregătire avansată în conformitate cu obligațiile şi sarcinile asociate funcției sale,
- a fost instruit cu privire la protecția datelor personale şi informațiilor confidențiale sau private,
- a semnat un contract ce conține clauze referitoare la protejarea informațiilor senzitive (din punctul de vedere al securității RO-CA) şi a datelor confidențiale şi private ale Abonaților,
- nu îndeplineşte sarcini care pot genera conflicte de interese între Autoritatea de Certificare şi Autoritatea de Înregistrare care acționează în numele acesteia.

6.3.1 Experiența personală, calificările şi clauzele de confidențialitate necesare

Personalul angajat al RO-CA care îndeplineşte un rol de încredere, trebuie să obțină avizul responsabilului de securitate. Avizul nu este necesar în cazul persoanelor care nu exercită un rol de încredere.

Îndeplinirea unei funcții de încredere ca administrator(ofiter) de securitate, administrator al Autorității de Certificare şi administrator HSM permite accesul la informațiile clasificate. Dezvăluirea neautorizată a acestor informații poate cauza pierderea sau compromiterea intereselor, apărate de lege, ale unei persoane fizice sau ale unei organizații.

Procedurile de acces la informațiile clasificate şi de verificare a încrederii în personal sunt în conformitate cu Legea Protecției Datelor cu Caracter Personal.

6.3.2 Cerințele de pregătire a personalului

Personalul care îndeplineşte roluri şi sarcini ca urmare a angajării la RO-CA sau la o Autoritatea de Înregistrare, trebuie să fie instruit cu privire la:

- reglementările Codului de Practici şi Proceduri,
- reglementările Politicii de certificare,
- procedurile şi controalele de securitate folosite de Autoritatea de Certificare şi Autoritatea de Înregistrare,
- aplicațiile software ale Autorității de Certificare şi Autorității de Înregistrare,
- responsabilitățile ce decurg din rolurile şi sarcinile executate în sistem,

- procedurile ce trebuie executate ca urmare a apariției unei defecțiuni în funcționarea sistemului Autorității de Certificare.

După încheierea pregătirii, participanții semnează un document prin care confirmă familiarizarea lor cu Codul de Practici şi Proceduri, Politica de certificare şi acceptă restricțiile şi obligațiile impuse.

6.3.3 Frecvența stagiilor de pregătire

Pregătirea descrisă în paragraful 6.3.2 trebuie repetată de fiecare dată când apar modificări semnificative în RO-CA.

6.3.4 Rotația funcțiilor

Acest Cod de Practici şi Proceduri nu specifică nici un fel de cerințe în această privință.

6.3.5 Sancționarea acțiunilor neautorizate

În cazul descoperirii sau existenței suspiciunii unui acces neautorizat, administratorul de sistem împreună cu administratorul de securitate poate suspenda accesul persoanei respective la sistemul RO-CA. Măsurile disciplinare pentru astfel de incidente trebuie descrise în regulamente corespunzătoare şi trebuie să fie conforme cu prevederile legale.

6.3.6 Personalul angajat pe baza de contract

Personalul angajat pe baza de contract (servicii externe, dezvoltatori de subsisteme sau aplicații etc.) fac obiectul unor verificări similare ca şi în cazul angajaților RO-CA . În plus, personalul angajat pe bază de contract, pe timpul cât îşi desfăşoară activitatea în locația RO-CA, trebuie permanent însoțit de către un angajat al RO-CA , cu excepția celor care au primit avizare din partea administratorului de securitate şi care poate accesa informații clasificate intern sau în conformitate cu normele legale în vigoare.

6.3.7 Documentația oferită personalului

RO-CA trebuie să ofere personalului său accesul la următoarele documente:

- Politica de certificare,
- Codul de Practici şi Proceduri,
- Responsabilitățile şi obligațiile asociate rolului deținut în sistem.

7 CONTROALE TEHNICE DE SECURITATE

Acest capitol descrie procedurile de generare şi management a perechii de chei criptografice a Autorității de Certificare şi Abonatului, inclusiv cerințele tehnice asociate.

7.1 Generarea si Instalarea Perechii de Chei a RO-CA

7.1.1 Generarea perechii de chei a RO-CA

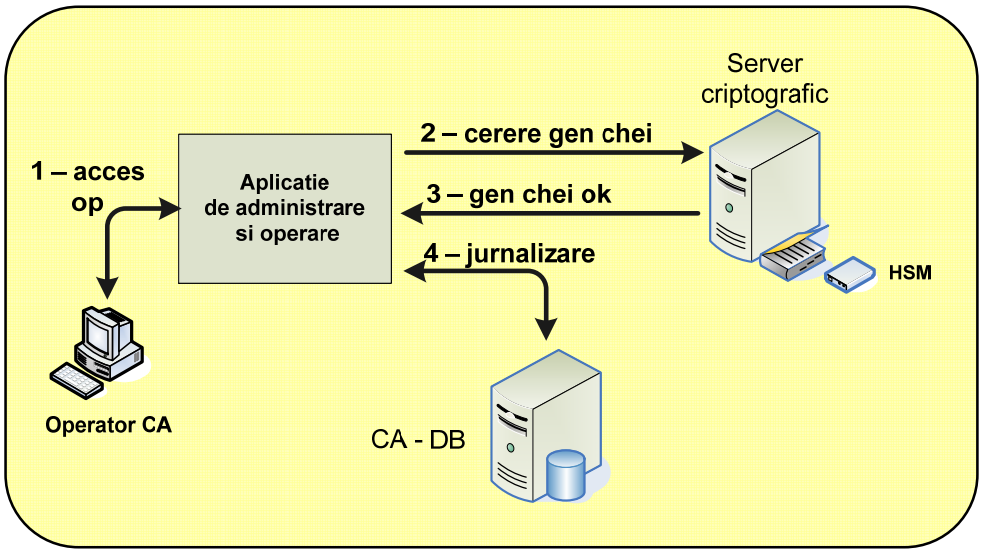
Procedurile de management a cheii se referă la păstrarea şi folosirea în siguranță de către proprietar a cheilor sale. O atenție deosebită se acordă generării şi protecției cheii private a RO-CA, care influențează funcționarea în siguranță a întregului sistem de certificare a cheilor publice din cadrul RO-CA.

Autoritatea de Certificare **RO-CA** deține mai multe certificate semnate de catre ERCA. Cheia privată corespunzătoare cheii publice conținută de aceste certificate este folosită exclusiv în scopul semnarii certificatelor pentru carduri si pentru crearea cererii de certificare a cheii publice RO.PK, adresata ERCA.

Generarea perechilor de chei ale autoritatii de certificare se face in faza de creare a CA - urilor folosindu-se aplicatia web-based de administrare si operare a tachoSAFE CA. Accesul la aplicatia de administrare si operare se obtine folosindu-se autentificarea bazata pe certificate X.509 si token criptografic. Aplicatia de administrare si operare ofera doar interfata de operare, necesara pentru aceasta operatie. Generarea efectiva a cheilor se face prin intermediul serverului criptografic (componenta tachoSAFE-cryptoServer).

Generarea perechilor de chei de semnare a autoritatii de certificare se va face pe un dispozitiv hardware criptografic tamper-proof, acreditat FIPS 140-2 level 3, de tip HSM marca nCipher. Generarea perechilor de chei se face pe principiul K/N (“four eyes principle”). Astfel, autorizarea operatiei de generare de chei se face in prezenta a K (K>= 2) operatori cu roluri de administratori de chei fiind conforma cu specificatiile din Politica de Certificare si Codul de Practici si Proceduri propuse. Fiecare dintre acesti administratori de chei detine cate un smartcard special protejat pe baza de PIN pe care se afla chei criptografice speciale de acces la HSM. Autorizarea procesului de generare de chei pe HSM se face utilizand aceste smartcard-uri.

Fluxul de operatii pentru procedura de generare chei este descris in schema urmatoare:



Asadar,

- administratorul de CA acceseaza aplicatia de operare si administrare pentru operatia de generare de CA –uri. Autentificarea la aceasta aplicatie se face prin certificat digital X.509 stocat pe token criptografic
- se face autentificarea la HSM prin intermediul a K (K >=2) administratori de chei autorizandu-se accesul pentru generarea de chei RSA pe HSM
- se genereaza perechile de chei de semnare pentru CA –uri

Asadar, conform procedurii explicate mai sus, generarea perechii de chei de semnare RO.SK si RO.PK (cheie de tip RSA pe 1024 biti) se face pe un dispozitiv tamper-proof FIPS 140-2 level 3 iar procesul de generare necesita participarea activa a cel putin 3 persoane dintre care una cu rol de administrator de CA.

Dupa generarea perechilor de chei ale CA –urilor, partea publica a acestor chei (cheile publice ale CA -urilor) sunt extrase de pe HSM si sunt stocate in baza de date a autoritatii de certificare. Aceste chei publice vor fi certificate prin intermediul cheilor private (secrete) ale ERCA, obtinandu-se certificatele corespunzatoare.

Dupa generarea perechilor de chei ale CA –urilor, cheile private (secrete) ale CA –urilor, nu parasesc niciodata dispozitivul HSM fiind imposibila extragerea lor in afara acestuia. Operatia de semnare a certificatelor se face exclusiv in interiorul HSM –ului si poate avea loc numai prin autorizarea cu smartcard -urile administratorilor de chei. Aceasta autorizare se poate face numai in prezenta activa a acestor administratori de chei (K administratori, cu K >=2) utilizand smartcardurile speciale de acces la HSM.

Cheile private (secrete) ale CA – urilor, generate si stocate pe dispozitivul hardware de tip HSM prin procedura de mai sus, reprezinta cheile de semnare a certificatelor digitale

dedicate cartelelor tahografice fiind folosite exclusiv numai pentru acest scop.

Cheile publice ale CA –urilor, generate pe dispozitvul hardware de tip HSM prin procedura de mai sus, sunt cheile de verificare a certificatelor digitale dedicate cartelelor tahografice si emise de aceste CA –uri, fiind folosite exclusiv in acest sens.

Asadar, stocarea cheii secrete RO.SK de semnarea a certificatelor dedicate cartelelor tahografice se face pe un dispozitiv tamper-proof FIPS 140-2 level 3, indeplinind cele mai riguroase cerinte de securitate. Accesul la cheia privata de semnare se face prin participarea activa a cel putin 2 persoane.

Cheia privata (RO.SK) va fi emisa pe o perioada limitata de 2 ani. Cheia publica (RO.PK) va fi emisa pe o perioada nelimitata. Aplicatia tachoSAFE CA, permite schimbarea (reinoirea) cheilor de semnare a certificatelor (RO.SK), in mod regulat, la o anumita perioada asigurandu-se astfel cerintele din specificatiile Comisiei Europene (cerinta CSM_008 din Reglementarea Comisiei Europene (EC) 1360/2002, Anexa IB, Appendix 11). Dupa generarea unei noi perechi de chei, utilizand procedura descrisa in acest capitol, vechea cheie privata va fi distrusa, iar perechea sa publica va fi mentinuta in continuare in sistem putand fi folosita la verificarea certificatelor emise cu cheia privata pereche.

Cheile publice ale CA –urilor (operational si de test) vor fi utilizate pentru a obtine certificatele corespunzatoare semnate cu cheile private (secrete) corespunzatoare, ale autoritatii de certificare root de la nivel european (ERCA).
Astfel, prin intermediul aplicatiei de administrare si operare, cheia publica a RO-CA (RO.PK) poate fi exportata intr-o cerere de certificare - Key Certification Request (RO.KCR) - in formatul specificat in Anexa A din Politica de Certificare a ERCA, versiunea 2.0 (SPI04131). Aceasta cerere de certificare va fi transmisa catre ERCA pentru a fi semnata cu cheia privata de la nivel european in cadrul unui certificat pentru Romania (RO.C). Aplicatia de administrare si operare permite importarea in sistem a certificatului RO.C emis de ERCA precum si a cheii publice EUR.PK a ERCA, verificand corectitudinea certificatului in raport cu cheia privata RO.SK.
Transportul cererii de certificare RO.KCR, respectiv a certificatului RO.C si a cheii publice ERCA, EUR.PK se va face conform specificatiilor din Anexa C a Politicii de Certificare a ERCA, versiunea 2.0 (SPI04131).

Toate operatiile implicate in cadrul procesului de generare de chei si cereri de certificate vor fi jurnalizate in loguri speciale care pot fi apoi auditate.

7.1.2 Distribuirea cheii private catre entitati

RO-CA nu genereaza cheile private RSA pentru carduri. Acestea sunt generate la RO-CP.

7.1.3 Trimiterea cererii KCR pentru certificarea cheii publice RO.PK si a cererii KDR pentru cheia senzorului de miscare Km_{wc} catre emitatorul certificatului (ERCA)

Cele doua cereri se vor face conform politicii ERCA. RO-A va nominaliza o persoana care va transporta mediul de stocare continand mesajele intre RO-CA si ERCA.

7.1.4 Distribuirea cheilor publice ale RO-CA si ERCA catre entitatile partenere

Cheia publica a RO-CA este distribuita catre RO-CP sub forma de certificat semnat cu cheia privata a ERCA. Cheia publica a ERCA este distribuita catre RO-CP ca atare. Distribuirea lor se face impreuna cu certificatul care va fi scris pe card ca urmare a unei cerereri KCR primite de RO-CA de la RO-CP.

Una dintre functiile importante ale entitatii RO-CA este aceea de interfatare cu centrul de personalizare a cartelelor tahografice, RO-CP.

Aplicatia de la RO-CA, de interfatare si comunicare cu RO-CP, comunica cu aplicatia similara de la RO-CP folosind un canal securizat. Securizarea se face astfel utilizand o legatura criptata si autentificata prin certificate digitale X.509
Astfel toate informatiile vehiculate intre RO-CP si RO-CA si invers (inclusiv cererile de certificate) sunt criptate si semnate, asigurandu-se astfel confidentialitatea, autenticitatea si integritatea datelor.

Astfel,singura cale de comunicare va fi numai prin intermediul aplicatiei de interfatare si comunicare RO-CA – RO-CP, care, in plus, va asigura si confidentialitatea, autenticitatea si integritatea datelor transmise.

7.1.5 Marimile cheilor

Perechile de chei generate pentru semnarea certificatelor (operationale si de test) sunt chei RSA de 1024 de biti conforme cu cerintele specifice din Reglementarea Comisiei Europene (EC) 1360/2002 avand:

- modulul n pe 1024 biti
- exponentul public e pe 64 biti, avand valoarea mai mare sau egal cu 3 si
- exponentul privat d pe 1024 biti

(cerintele CSM_003, CSM_014 din Reglementarea Comisiei Europene (EC) 1360/2002, Anexa IB, Appendix 11).

7.1.6 Parametrii de generare ai cheilor publice

Cel care generează o cheie este responsabil de verificarea calității parametrilor cheii generate. Acesta trebuie să verifice:

- posibilitatea de a efectua operații de criptare şi decriptare, inclusiv creare de semnături electronice şi verificare a acestora,
- procesul de generare a cheii trebuie să se bazeze pe generatoare puternice de numere aleatoare – surse fizice de zgomot alb, dacă este posibil,
- imunitatea la atacuri cunoscute (în cazul algoritmilor RSA şi DSA).

7.1.7 Verificarea calitatii parametrilor

Se folosesc module HSM certificate, configurate pentru a genera chei RSA cu modulul de 1024-bit.

7.1.8 Generarea Hardware/software a cheii

Cheile RO-CA sunt generate in module HSM certificate FIPS 140-2 Level 3

7.1.9 Utilizarea perechii de chei a RO-CA

Cheia privata RSA a RO-CA este utilizata doar pentru semnarea certificatelor cheilor publice pentru tahografe si pentru crearea cererii de certificat catre ERCA.

7.2 Protectia Cheii Private

7.2.1 Standarde si controale pentru modulele criptografice

RO-CA utilizeaza pentru generarea si stocarea cheilor sale private RSA doar module HSM certificate.

Operatia modulului HSM este verificata periodic prin teste interne, iar upgrade-ul de firmware pentru HSM este realizat annual de administratorul HSM, daca este cazul.

7.2.2 Controlul k din n al cheii private

Generarea cheii private este realizata de cel putin trei persoane autorizate.

7.2.3 Escrow-ul cheii private

Escrow-ul cheii este interzis de politica de certificare a RO-CA.

7.2.4 Backup-ul cheii private

RO-CA creează o copie de siguranță a cheiilor sale private. Copiile sunt folosite în cazul punerii în aplicare a procedurilor standard, sau de urgență (de exemplu, după dezastru) de recuperare a cheii. Copiile cheilor private sunt protejate prin secrete partajate. Secretele partajate sunt criptate si stocate in cardurile modulului HSM.

Copiile cheilor sunt verificate o data pe an prin incercarea de restaurare a lor intr-un HSM identic. Verificarea se face intr-o incinta cu acelasi grad de siguranta ca si mediul de productie in prezenta unui administrator si a unui auditor.
Daca verificarea nu reuseste, noi copii sunt create in cel mai scurt timp.

7.2.5 Arhivarea cheii private

Ca la 7.2.4

7.2.6 Transferul cheii private din sau intr-un modul HSM

Pe baza copiilor cheilor criptate protejate si a secretelor partajate de pe cardurile modulului HSM, cheile private pot fi transferate intr-un alt modul HSM.

7.2.7 Pastrarea cheii private intr-un modul HSM

Cheile private ale RO-CA sunt pastrate in modulul HSM in care au fost generate.

7.2.8 Metoda de activare a cheii private

Activarea cheii se face dupa principiul K din N, cu K>=2. La operatie participa doi operatori HSM.

7.2.9 Metoda dezactivarii cheii private

Metoda de dezactivare a cheii private se referă la dezactivarea cheii după folosirea acesteia sau ca urmare a terminării unei sesiuni în timpul căreia a fost folosită cheia.

În cazul RO-CA, dezactivarea unei chei private se face de către ofițerul de securitate numai în cazul în care o sesiune de lucru a fost încheiată, perioada de validitate a cheii a expirat, cheia a fost revocată sau este necesar să se suspende imediat activitățile sistemului. Dezactivarea se face prin intermediul aplicatiei de administrarea a CA-ului. Dupa dezactivare, accesul la cheile private nu mai este posibil decat prin procedura standard de login descrisa in acest document.

7.2.10 Metoda distrugerii cheii private

Distrugerea cheii se face simuland o fortare a modulului HSM.
Fiecare distrugere de cheie privată este înregistrată în jurnalul de evenimente.

7.2.11 Certificarea modulului HSM

RO-CA foloseste module criptografice certificate cel putin FIPS 140-2 Level 3.

7.3 Cheia senzorului de miscare pentru cardurile de atelier Km_{wc}

Cheia senzorului de miscare nu este gestionata de aplicatiile RO-CA, ci de cele de la RO-CP.

7.4 Cheile asimetrice inserate in carduri

Atat la autoritatea romana de certificare, RO-CA, cat si la organizatia care personalizeaza cardurile, RO-CP exista doua aplicatii similare intre care se realizeaza un canal de comunicatie cu un grad ridicat de securitate care sa asigure transmiterea datelor in ambele sensuri: de la CA catre CP si de la CP catre CA.Cele doua aplicatii vor avea cite un certificat digital X.509 prin intermediul carora va face securizarea schimbului de informatii.

Astfel, la RO-CA va opera aplicatia de interfatare si comunicatie intre RO-CA si RO-CP care este responsabila de comunicarea automata cu o componenta speciala, similara de la RO-CP.

Fluxul operatiilor aplicației de intefațare şi comunicare cu RO-CP la aplicatia de la RO-CA este urmatorul:

- Receptioneaza cererile, in forma de structuri de date XML, semnate si criptate care vin de la RO-CP. Aceste structurile de date contin cereri de certificate pentru cartele tahografice;
- Extrage si reasambleaza datele receptionate de la RO_CP;
- Verifica structura si consistenta datelor continute in structurile XML receptionate;
- Daca toate verificarile au fost realizate cu success datele (cererile) receptionate, sunt inserate in baza de date a RO-CA si sunt furnizate modulelor de procesare ale RO-CA.

- Obtine certificatele emise pentru cartelele tahografice si le exporta în structuri de date XML. Aceste structuri de date XML vor contine pe langa certificate si id-urile cererilor pentru care s-au emis certificatele respective;
- Impacheteaza structurile de date XML semnate si criptate intr-un format acceptat de canalul de comunicatie;

Pentru toate transferurile de date intre RO-CA si RO-CP se vor genera jurnalizari in fisierele speciale de audit folosind modulul de logare si notificare. Vor fi logate momentul de timp al evenimentului, id-uri de cereri pentru care s-a realizat transferul, rezultatul transferului (success sau fail), eventualele probleme legate de operatiile criptografice (criptare, semnare, verificare semnatura), erorile de comunicație, de integritate a datelor.

7.5 Alte Aspecte ale Managementului Perechii de Chei

7.5.1 Arhivarea Cheii Publice

Scopul arhivării cheilor publice este acela de a crea posibilitatea verificării semnăturii electronice după eliminarea unui certificat din baza de date.

Arhivarea cheilor publice presupune arhivarea certificatelor care conțin aceste chei.

Fiecare autoritate care emite certificate arhivează cheile publice ale Abonaților către care au fost emise certificatele.

Arhivele cheilor publice trebuie protejate în aşa fel încât să se prevină adăugarea, inserarea, modificarea şi ştergerea neautorizată de chei din arhivă. Protecția este realizată prin autentificarea entității care face arhivarea şi autorizarea cererilor.

Ofiterul de securitate verifică periodic integritatea arhivelor de chei publice. Scopul acestei verificări este de a asigura faptul că nu sunt goluri în arhive şi că certificatele din arhive nu au fost modificate. Mecanismul de verificare a integrității arhivelor ține cont de faptul că perioada de păstrare poate fi mai lungă decât cea a mecanismelor de securitate folosite la crearea arhivelor.

Cheile publice sunt păstrate în arhivele cu certificate digitale 15 ani după momentul expirării.

Comment [CG1]: ??

7.5.2 Perioadele de validitate pentru cheile publice si private ale RO-CA

Perioada de validitate a cheii private RO-CA este stabilita la 2 ani prin Politica de Certificare a RO-CA.

Perioada de validitate a cheii publice RO-CA si a cheilor master ale senzorului de miscare este nelimitata.

7.6 Datele de Activare

Metodele de activare a cheii private se referă la activarea cheii înainte de orice folosire a sa, sau de începerea unei sesiunii de lucru ce necesită folosirea cheii respective. O cheie odată activată poate fi folosită până la dezactivare.

Executarea procedurilor de activare (şi dezactivare) a unei chei private depinde de de intervalul de timp în care cheia trebuie să rămână activă (pe timpul unei singure operațiuni, sesiuni sau pentru o perioadă nelimitată).

Cheia privata a RO-CA rămâne în stare activă până la ştergerea ei fizică de pe modul sau până la scoaterea ei din serviciile RO-CA . Activarea cheii private este întotdeauna precedată de autentificarea operatorului. Autentificarea este realizată pe baza unui card criptografic deținut de operator. După introducerea cardului în modulul criptografic şi folosirea codului PIN, cheia privată rămâne în stare activă până la scoaterea cardului din modul.

7.7 Controale de Securitate a Calculatoarelor

Sarcinile operatorilor si administratorilor care lucrează în cadrul RO-CA sunt realizate prin intermediul unor dispozitive hardware şi aplicații software de încredere.

7.8.1 Cerințele tehnice specifice securității calculatoarelor

Cerințele tehnice prezentate în acest capitol se referă la controalele de securitate specifice calculatoarelor şi aplicațiilor, folosite în cadrul RO-CA. Măsurile de securitate care protejează sistemele de calcul sunt aplicate la nivelul sistemului de operare, al aplicațiilor precum şi din punct de vedere fizic.

Calculatoarele aparținând RO-CA dispun de următoarele mijloace de securitate:

- autentificarea obligatorie la nivelul sistemului de operare şi al aplicațiilor,
- control discreționar al accesului,
- posibilitatea de a fi auditate din punct de vedere al securității,
- calculatorul este accesibil doar personalului autorizat, cu roluri de încredere în RO-CA ,

- separarea sarcinilor, conform rolului în cadrul sistemului,
- identificarea şi autentificarea rolurilor şi a personalului care îndeplineşte aceste roluri,
- prevenirea refolosirii unui obiect de către un alt proces după eliberarea acestuia de către procesul autorizat,
- protecția criptografică a schimburilor de informații şi protecția bazelor de date,
- arhivarea istoricului operațiunilor executate pe un calculator şi a datelor necesare auditării,
- o cale sigură ce permite identificarea şi autentificarea rolurilor şi a personalului care îndeplineşte aceste roluri,
- metode de restaurare a cheilor (numai în cazul modulelor hardware de securitate), a aplicaților şi a sistemului de operare,
- mijloace de monitorizare şi alertare în cazul accesului neautorizat la resursele de calcul.

7.7.2 Evaluarea securității calculatoarelor

Sistemele de calcul ale RO-CA respectă cerințele descrise în standardele ETSI: ETSI TS 101456 (Cerințele de Politică pentru Autoritățile de Certificare care emit certificate calificate) şi CEN CWA 14167 (Cerințele de Securitate pentru Sistemele de Încredere care asigură Managementul certificatelor pentru Semnătură Electronică).

7.7.3 Controale tehnice specifice ciclului de viata

Controale specifice dezvoltării sistemului

Fiecare aplicație, înainte de a fi folosita în producție de catre RO-CA, este instalata astfel încât să se permită controlul versiunii curente şi să se prevină instalarea neautorizată de programe sau falsificarea celor existente.

Reguli similare se aplică în cazul înlocuirii componentelor hardware, cum ar fi:

- dispozitivele fizice sunt furnizate în aşa fel încât să poată fi urmărita şi evaluată ruta fiecăruia, până la locul său de instalare,
- livrarea unui dispozitiv fizic pentru înlocuire se realizează într-un mod similar celui de livrare al dispozitivului original; înlocuirea se realizează de către personal calificat şi de încredere.

Controale pentru managementul securității

Scopul controalelor pentru managementului securității este acela de a superviza funcționalitatea sistemelor RO-CA, garantând astfel că acestea operează corect şi în concordanță cu configurarea acceptată şi implementată.

Configurația curentă a sistemelor RO-CA, precum şi orice modificare şi actualizare a acestora, este înregistrată şi controlată.

Controalele aplicate sistemelor RO-CA permit verificarea continuă a integrității aplicațiilor, versiunii şi autentificarea şi verificarea originii dispozitivelor hardware.

7.7.4 Controale de securitatea a rețelei

Serverele şi stațiile de lucru de încredere aparținând RO-CA sunt conectate prin intermediul unei rețele locale (LAN), divizate în mai multe subretele, cu acces controlat. Accesul dinspre Internet către orice segment, este protejat prin intermediul unui firewall inteligent.

Controalele de securitate sunt dezvoltate pe baza firewall-ului şi a filtrelor de trafic aplicate la nivelul ruterelor şi serviciilor Proxy.

Mijloacele de asigurare a securității rețelei acceptă doar mesajele transmise prin protocoalele http, https, NTP, POP3 şi SMTP. Evenimentele (log-urile) sunt înregistrate în jurnalele de sistem şi permit supravegherea folosirii corecte a serviciilor furnizate de RO-CA.

7.7.5 Controale specifice modulelor criptografice

Controalele modulelor criptografice includ cerințele impuse pentru dezvoltarea, producția şi livrarea modulelor. RO-CA nu defineşte cerințe specifice în acest domeniu. Totuşi, RO-CA acceptă şi utilizează numai module criptografice care corespund cerințelor din Capitolul 6 din Politica de Certificare a RO-CA.

7.7.6 Înregistrarea evenimentelor şi procedurile de auditare

Pentru a gestiona eficient sistemele RO-CA şi pentru a putea audita acțiunile utilizatorilor şi personalului RO-CA, toate evenimentele care apar în sistem sunt înregistrate. Informațiile înregistrate alcătuiesc jurnalele (log-urile) de evenimente şi trebuie păstrate în aşa fel încât să permită, daca este cazul, să se acceseze informațiile corespunzătoare şi necesare rezolvării disputelor, sau să detecteze tentativele de compromitere a securității RO-CA. Evenimentele înregistrate fac obiectul procedurilor de arhivare. Arhivele sunt păstrate în afara incintei RO-CA.

Când este posibil, log-urile sunt create automat. Dacă înregistrările nu pot fi create automat, se vor folosi jurnalele de evenimente pe hârtie. Fiecare înregistrarea în log, electronic sau de mână, este păstrata şi dezvăluita atunci când se desfăşoară un audit.

Tipuri de evenimente înregistrate

Fiecare activitate critică din punctul de vedere al securității RO-CA este înregistrată în log-urile de evenimente şi arhivată. Arhivele sunt depozitate pe medii de stocare ce nu pot fi suprascrise pentru a preveni modificarea sau falsificarea lor.

Log-urile de evenimente RO-CA conțin înregistrări ale tuturor activităților generate de componentele software din cadrul sistemului. Aceste înregistrări sunt împărțite în trei categorii separate:

- **înregistrări de sistem** – conțin informații despre cererile clienților software şi răspunsurile server-ului (sau invers) la nivelul protocolului de rețea (de exemplu http, https); datele concrete care se înregistrează sunt: adresa IP a stației sau a server-ului, operațiunile executate (de exemplu: căutare, editare, scriere etc.) şi rezultatele lor (de exemplu introducerea cu succes a unei înregistrări în baza de date),
- **erori** – conține informații despre erori la nivelul protocoalelor de rețea şi la nivelul modulelor aplicațiilor;
- **audit** – conțin informații specifice serviciilor de certificare, de exemplu: cererea de înregistrarea şi de certificare, cererea de schimbare a cheii, acceptarea certificatului, emiterea de certificat etc.

Jurnalele de evenimente de mai sus sunt comune fiecărei componente instalate pe un server sau stație de lucru şi au o capacitate prestabilită. Atunci când se depăşeşte această capacitate, este creată automat o nouă versiune de jurnal. Jurnalul anterior este arhivat şi şters de pe disc.

Fiecare înregistrare, automată sau manuală, conține următoarele informații:

- tipul evenimentului,
- identificatorul evenimentului,
- data şi ora apariției evenimentului,
- identificatorul persoanei responsabile de eveniment.

Conținutul înregistrărilor se refera la:

- alertele firewall-urilor şi IDS-urilor,
- operațiile asociate înregistrării, certificării etc.,
- oprirea si pornirea sistemelor
- modificări ale structurii hard sau soft,
- modificări ale rețelei şi conexiunilor,
- înregistrările fizice în zonele securizate şi violările de securitate,
- creari si modificari de conturi
- schimbările de parole, drepturi asupra codurilor PIN, rolurile personalului,
- accesul reuşit şi nereuşit la baza de date RO-CA şi la aplicațiile serverului,
- generarea de chei pentru CA, etc.,
- fiecare cerere primită şi decizia emisă în format electronic,
- istoria creării copiilor de backup şi a arhivelor cu înregistrări.

Accesul al jurnalele de evenimente (log-uri) este permis în exclusivitate administratorului de securitate, operatorilor Autorităților de Certificare şi auditorilor.

Frecvența analizei jurnalelor de evenimente

Înregistrările din jurnalul de evenimente trebuie revăzute în detaliu cel puțin o dată pe lună. Orice eveniment având o importanță semnificativă trebuie explicat şi descris într-un jurnal. Procesul de verificare a jurnalului include verificarea unor eventuale falsificări, sau modificări şi verificarea fiecărei alerte sau anomalii consemnată în log-uri. Orice acțiune executată ca rezultat al funcționări defectuoase detectate trebuie înregistrată în jurnal.

Perioada de retenție a jurnalelor de evenimente

Înregistrările evenimentelor sunt stocate în fişiere pe discul sistem până când acestea ajung la capacitatea maximă permisă. În tot acest timp sunt disponibile on-line, la cererea fiecărei persoane, sau proces autorizat. După depăşirea spațiului alocat, jurnalele sunt păstrate în arhive şi pot fi accesate numai off-line, de la o anumită stație de lucru.

Jurnalele arhivate sunt păstrate cel puțin 7 ani.

Protecția jurnalelor de evenimente

Săptămânal, fiecare înregistrare din jurnale face obiectul arhivării pe bandă magnetică. După depăşirea numărului acceptat de înregistrări pentru un jurnal, conținutul acestuia este arhivat. Arhivele pot fi criptate folosind algoritmul Triple DES sau AES. O cheie folosită pentru criptarea arhivelor este plasată sub controlul administratorului de securitate.

Un jurnal de evenimente poate fi revăzut numai de administratorului de securitate, administratorul Autorității de Certificare, sau de către un auditor. Accesul la jurnalul de evenimente este configurat în aşa fel încât:

- numai entitățile de mai sus au dreptul să citească înregistrările jurnalului,
- numai administratorul de securitate poate arhiva sau şterge fişiere (după arhivarea acestora) care conțin evenimentele înregistrate,
- este posibilă detectarea oricărei violări de integritate; acest lucru asigură faptul că înregistrările nu conțin goluri sau falsuri,
- nici o entitate nu are dreptul să modifice conținutul unui jurnal.

În plus, procedurile de protecție a jurnalului sunt implementate în aşa fel încât, chiar şi după arhivarea jurnalului, este imposibil să ştergi înregistrări, sau să ştergi jurnalul înaintea expirării perioadei de retenție a jurnalului.

Procedurile de backup pentru jurnalele de evenimente

Procedurile de securitate RO-CA solicita ca jurnalul de evenimente să facă obiectul backup-ului lunar. Aceste backup-uri sunt stocate în locații auxiliare ale RO-CA.

Notificarea entităților responsabile de tratarea evenimentelor

Modulul de analiză a jurnalului de evenimente implementat în sistem examinează evenimentele curente şi sesizează automat activitățile suspecte sau pe cele care au ca scop compromiterea securității. În cazul activităților care au influență asupra securității sistemului, sunt notificați automat administratorul de securitate şi administratorul Autorității de Certificare. În celelalte cazuri, notificarea este direcționată numai către administratorul de sistem. Transmiterea informațiilor către persoanele autorizate despre situațiile critice – din punctul de vedere al securității sistemului – se face prin alte mijloace de comunicare, protejate corespunzător, de exemplu, pager, telefon mobil, poştă electronică. Entitățile notificate iau măsurile corespunzătoare pentru a proteja sistemul față de amenințarea detectată.

Procedura de backup si restaurare

Copiile de siguranță permit restaurarea completă (dacă este necesar, de exemplu, după distrugerea sistemului) a datelor esențiale pentru activitatea RO-CA. Pentru a realiza acest lucru, sunt copiate următoarele aplicații şi fişiere:

- discurile de instalare a aplicațiilor sistem (de exemplu sistemul de operare),
- discurile de instalare a aplicațiilor pentru Autoritatea de Certificare,
- istoricul cheilor si certificatelor,
- datele privind personalul RO-CA,
- jurnalele de evenimente.

Metoda de creare a copiilor de backup are o influență deosebită asupra timpului şi costului restaurării Autorității de Certificare după defectarea, sau distrugerea sistemului. RO-CA foloseşte atât backup-uri full (săptămânale), cat şi backup-uri incrementale (zilnice), toate copiile sunt clonate şi clonele sunt păstrate în altă locație, în aceleaşi condiții de securitate ca şi cele din locația primară.

Procedura de restaurare va fi verificata cel puțin o data la 3 luni, pentru a se verifica utilitatea backup-ului, in caz de crash. Va trebui sa se verifice daca datele salvate pe banda sunt suficiente pentru restaurarea sistemului in cel mai scurt timp posibil. Concluziile testelor vor fi inregistrate.

7.7.7 Arhivarea înregistrărilor

Este necesar ca toate datele şi fişierele referitoare la informațiile despre securitatea sistemului, cererile de certificate, certificatele emise, cheile folosite de Autoritatea de Certificare să fie arhivate.

Pe baza arhivelor se creează copiile de siguranță care sunt ținute în afara locației RO-CA.

Tipurile de date arhivate

Următoarele date sunt incluse în procesul de arhivare:

- informațiile rezultate în urma examinării şi evaluării (ca urmare a unui audit) măsurilor de protecție logica şi fizica ale Autorității de Certificare,

- cererile de certificate primite si toate mesajele legate de acestea, schimbate cu RO-CP
- continutul certificatelor emise
- baza de date cu certificate (sau evenimente legate de emiterea de certificate)
- istoria cheii Autorității de Certificare, de la generare până la distrugere,
- toate versiunile anterioare ale CP si CPS

Cerințele pentru marcarea temporală a înregistrărilor

Se recomandă ca datele arhivate să fie semnate cu o marcă temporală, creată de Autoritatea de Marcare Temporală (TSA). Serviciul de marcare temporală este disponibil în cadrul RO-CA .

Procedurile de acces şi verificarea informațiilor arhivate

Pentru a verifica integritatea informațiilor arhivate, datele sunt periodic testate şi verificate prin comparație cu datele originale (dacă mai sunt încă accesibile în sistem). Această activitate poate fi realizată numai de către administratorul de securitate şi trebuie înregistrată în jurnalul de evenimente. Dacă sunt detectate deteriorări sau modificări ale datelor originale, acestea trebuie corectate cât mai repede posibil.

7.8 Compromiterea cheilor si Recuperarea in Caz de Dezastru

7.8.1 Procedurile de tratare a incidentelor de securitate si a cazurilor de compromitere a cheilor

Procedurile sunt descrise in manualul de tratare a incidentelor care este distribuit doar administratorilor si auditorilor.

La detectarea unui incident, CA-ul RO-CA poate fi trecut in carantina si operatiile sale suspendate pana la stabilirea gradului de compromitere.

7.8.2 Defectiuni ale echipamentelor, software-ului sau pierderea integritatii datelor

In functie de natura dezastrului, pasii de recuperare sunt urmatorii:

1. Se inlocuieste imedita CA-ul cu sistemele de rezerva
2. Se restaureaza aplicatiile software folosinf copiile de siguranta
3. Se restaureaza datele folosind copiile de siguranta
4. Se restaureaza cheile RSA folosind HSM-ul de rezerva si cardurile de HSM de rezerva

7.8.3 Procedurile in cazul compromiterii cheii private

In cazul in care cheia privata a RO-CA sau cheia senzorului demiscare au fost compromise, sau se suspecteaza ca au fost compromise, se notifica imediat RO-A.

7.8.4 Continuarea afacerii in caz de dezastru

Folosind copiile de siguranta se restaureaza datele si aplicatiile si se recreeaza un mediu de lucru securizat intr-o locatie alternativa.

7.9 Scoaterea din uz a RO-CA

Incheierea serviciului RO-CA service se realizeaza astfel:

1. Toate datele sunt distruse in mod securizat prin stergerea securizata a discurilor folosind programe specializate si prin fortarea modulului HSM;
2. Toate copiile cheilor RO-CA sunt distruse
3. Arhiva RO-CA si inregistrarile auditurilor sunt predate catre RO-MSA.

Procedura de scoatere din uz se desfasoara sub controlul dual al RO-CA si al RO-MSA.

8 PROFILELE CERTIFICATELOR, CRL-URILOR SI CELE OCSP

8.1 Profilul Certificatelor

8.1.1 Versionarea

This CPS supports the digital tachograph certificate profile identifier 1.

8.1.2 Extensiile certificatelor

Nu exista nici o prevedere.

8.1.3 Algorithm object identifiers

Nu exista nici o prevedere.

8.1.4 Formele Numelor

Nu exista nici o prevedere.

8.1.5 Constrangerile numelor

Nu exista nici o prevedere.

8.1.6 Certificate policy object identifier

Nu exista nici o prevedere.

8.1.7 Usage of Policy Constraints extension

Nu exista nici o prevedere.

8.1.8 Policy qualifiers syntax and semantics

Nu exista nici o prevedere.

8.1.9 Processing semantics for the critical Certificate Policies extension

Nu exista nici o prevedere.

8.2 Profilele CRL si OCSP

Nu se aplica.

9 AUDITURILE PENTRU STABILIREA CONFORMITATII SI ALTE EVALUARI

Auditurile au ca obiectiv verificarea consistenței acțiunilor RO-CA sau a entităților delegate de aceasta cu declarațiile şi procedurile acestora (inclusiv Politica de certificare şi Codul de Practici şi Proceduri).

Auditurile desfăşurate la RO-CA urmăresc în principal centrele de procesare a datelor şi procedurile de gestiune a cheilor. De asemenea, aceste audituri au în vedere şi Autoritatea de Certificare RO-CA.

Auditurile desfăşurate la RO-CA pot fi efectuate de echipe interne (audit intern) sau de RO-A sau organizații independente (audit extern) angajate de aceasta. În toate aceste cazuri, auditul se desfăşoară sub supravegherea administratorului de securitate

Frecvența auditării.

Auditul extern prin care se verifică compatibilitatea cu reglementările legale şi procedurale (în special cu Politica de certificare şi Codul de Practici şi Proceduri) se desfăşoară anual, în timp ce un audit intern este efectuat ori de cate ori administratorul de securitate considera necesar.

9.1 Identitatea / calificările auditorului

Auditul extern trebuie realizat de personal având cunoştințe şi experiență tehnică corespunzătoare (să dispună de documente care să certifice acest lucru) în domeniul infrastructurilor de chei publice, tehnologiilor şi dispozitivelor de securitate informatică şi de auditare a securității sistemelor. De asemnea auditorul trebuie sa posede cunostinte solide ale reglementarilor UE, CE si RO-A referitoare la sistemul tahografelor digitale.

Auditul intern este realizat de către departamentul de calitate şi audit al RO-CA.

9.2 Relația auditorilor cu entitatea auditată

Vezi paragraful anterior. Auditorul nu trebuie sa depinda in nici un fel de entitatea auditata si nici sa nu fi fost in vre-un fel implicat in activitatile de planificare si operare ale sistemelor ITC ale entitatii auditate.

9.3 Domeniile supuse auditării

Auditurile interne şi externe se desfăşoară conform regulilor şi procedurilor acceptate pe plan internațional şi vizează:

- securitatea fizică a RO-CA,
- procedurile de verificare a identității aplicantilor,
- serviciile de certificare şi procedurile de furnizare a serviciilor,
- securitatea aplicațiilor software şi a accesului la rețea,
- securitatea personalului RO-CA,
- jurnalele de evenimente şi procedurile de monitorizare a sistemului,
- arhivarea şi restaurarea datelor,
- procedurile de arhivare,
- înregistrările referitoare la modificarea parametrilor de configurare pentru RO-CA,
- înregistrările referitoare la analizele şi verificările efectuate pentru aplicațiile software şi dispozitivele hardware.

9.4 Analiza vulnerabilităților

Autoritatea de Certificare face anual o analiză a vulnerabilităților pentru fiecare procedură internă, aplicație şi sistem informatic. Cerințele de analiză pot, de asemenea, să fie stabilite de către o instituție externă, autorizată să auditeze certSIGN. Administratorul de securitate are sarcina de a solicita audituri interne prin care să verifice conformitatea

înregistrărilor din jurnalul de securitate, corectitudinea copiilor de backup, activitățile executate în cazul apariției unei amenințări şi conformitatea cu Codul de Practici şi Proceduri.

Instituția externă care efectuează auditul de securitate, trebuie să desfăşoare această activitate respectând recomandările ISO/IEC 13335 (Guidelines for Management of IT Security) şi ISO/IEC 17799 (Code of Practice for Information Security Management).

9.5 Măsurile întreprinse ca urmare a descoperirii unei deficiențe

In cazul descoperirii unor deficiente se pot lua trei tipuri de masuri:

1. continuarea operatiilor
2. continuarea limitata a operatiilor;
3. suspendarea operatiilor.

Auditorul, impreuna cu RO-A, decide ce actiune trebuie intreprinsa. Decizia se bazeaza pe gravitatea deficientelor si a posibilului impact.

In cazul in care se decide actiunea de tipul 1, managementul RO-CA este raspunzator pentru implementarea masurilor corective specificate in raportul de audit, in limitele de timp din acelasi raport.

In cazul in care se decide actiunea de tipul 2, RO-CA continua operatiile in modul restrans indicat in raportul de audit.

The level of service may include or exclude any of the following activities:

- RO-CA policy approval or maintenance;
- RO-CA maintenance operations;
- public key certification operations;
- motion sensor key distribution operations.

In cazul in care se decide actiunea de tipul 3, toate cardurile afectate trebuie trecute pe un backlist. Managementul RO-CA trebuie sa raporteze saptamanal stadiul masurilor de remediere catre auditor. RO-A si auditorul determina cand trebuie facuta o noua evaluare de securitate. Daca deficientele sunt considerate ca remediate dupa reevaluare, atunci RO-CA isi poate relua operatiile.

9.6 Comunicarea rezultatelor

Rezultatele auditului annual sunt communicate catre RO-A. In cazul actiunilor de tipul 1 sau 2, RO-A se asigura ca toti cei care trebuie informati sunt informati.