

Sistemul de Tahograf Digital pentru Republica Moldova
Codul de Practici si Proceduri pentru operarea MD-CP



CUPRINS

1 INTRODUCERE	4
1.1 Descriere generala	4
1.2 Numele si Identificarea Documentului	7
1.3 Participanți	7
1.3.1 Autoritatea de Certificare	7
1.3.2 Autoritatea de Înregistrare	7
1.3.3 Abonați	7
1.3.5 Destinatarii Cheilor pentru Senzorii de Mișcare	7
1.4 Utilizarea certificatului	7
1.5 Utilizarea Mesajului pentru Distribuirea Cheii (KDM)	7
1.6 Administrarea CPP	9
1.7 Definiții si Acronime	11
2 CONTROALE TEHNICE DE SECURITATE	11
2.1 Generarea si Instalarea Perechii de Chei pentru Carduri	11
2.1.1 Generarea perechii de chei	11
2.1.2 Distribuirea cheii private către entități	11
2.1.3 Trimiterea cheii publice către emițătorul certificatului (MD-CA)	11
2.1.4 Distribuirea cheilor publice ale cardurilor către entitățile partenere	11
2.1.5 Mărimile cheilor	12
2.1.6 Parametrii de generare ai cheilor publice	12
2.1.7 Verificarea calității parametrilor	12
2.1.8 Generarea Hardware/software a cheii	12
2.1.9 Utilizarea perechii de chei	12
2.2 Protecția Cheii Private	12
2.2.1 Standarde si controale pentru modulele criptografice	12
2.2.2 Controlul k din n al cheii private	12
2.2.3 Backup-ul cheii private	12
2.2.4 Arhivarea cheii private	12
2.2.5 Transferul cheii private din sau într-un modul HSM	13
2.2.6 Păstrarea cheii private într-un modul HSM	13
2.2.7 Metoda de activare a cheii private	13
2.2.10 Certificarea modulului HSM	13
2.3 Alte Aspecte ale Managementului Perechii de Chei	13
2.3.1 Arhivarea Cheii Publice	13
2.3.2 Perioadele de validitate pentru cheile publice si private emise de MD-CP	13
2.4 Datele de Activare	13
2.5 Controale de Securitate a Calculatoarelor	13
2.5.1 Cerințele tehnice specifice securității calculatoarelor	14
2.5.2 Evaluarea securității calculatoarelor	14
2.5.3 Controale tehnice specifice ciclului de viață	15
2.5.4 Controale de securitatea a rețelei	15
2.5.5 Controale specifice modulelor criptografice	15
2.5.6 Înregistrarea evenimentelor și procedurile de auditare	18
2.5.7 Arhivarea înregistrărilor	20
3 Controale de securitate fizică, organizațională și de personal	20
3.1 Controale de securitate fizică	20
3.1.1 Controale de securitate fizică în cadrul MD-CP	20
3.2 Controlul securității organizației	22
3.2.1 Roluri de încredere	22
3.2.2 Numărul de persoane necesare pentru îndeplinirea unei sarcini	23
3.2.3 Identificarea și autentificarea pentru fiecare rol	23
3.3 Controlul personalului	24



3.3.1	Experiența personală, calificările și clauzele de confidențialitate necesare	24
3.3.2	Cerințele de pregătire a personalului	24
3.3.3	Frecvența stagiilor de pregătire	24
3.3.4	Rotația funcțiilor	25
3.3.5	Sanționarea acțiunilor neautorizate	25
3.3.6	Personalul angajat pe baza de contract	25
3.3.7	Documentația oferită personalului	25
4	AUDITURILE PENTRU STABILIREA CONFORMITATII SI ALTE EVALUARI	26
4.1	Identitatea / calificările auditorului	26
4.2	Relația auditorilor cu entitatea auditată	26
4.3	Domeniile supuse auditării	26
4.4	Analiza vulnerabilităților	27
4.5	Măsurile întreprinse ca urmare a descoperirii unei deficiențe	27



1 INTRODUCERE

Agentia Nationala Transport Auto este responsabila pentru funcția de Autoritate Națională 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 mișcare);
- Chei de criptare pentru datele senzorilor de mișcare.

Scopul acestui document este acela de a descrie practicile implementate de MD-CP in lucrul cu cardurile de tahograf si cheile de criptare.

Documentul a fost creat pentru a asigura conformitatea cu cerințele enunțate in Politica de Certificare a MD-CA si se bazează pe cadrul creat prin IETF RFC 3647.

1.1 Descriere generala

Scopul principal al acestui document este acela de a fi folosit de către MD-A si de către cei care doresc sa evalueze gradul de încredere care poate fi acordat serviciilor oferite de MD-CP sau sa determine măsura in care acestea respecta cerințele sistemului pentru tahografe digitale.

Sistemul de management al cheilor criptografice (vezi figura următoare) 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.

MD-CA si MD-CP sunt operate sub responsabilitatea si autoritatea autorităților naționale sau a furnizorilor de servicii externi autorizați.

MD-CA are rolul de a certifica cheile RSA care sunt introduse in cardurile pentru tahografe de către MD-CP. Mai multe tipuri de carduri sunt emise următoarelor entități: șoferilor, atelierelor, organelor de control si firmelor de transport.



MD-CP primește cererile de cartele tahografice de la MD-CIA in format electronic securizat, generează perechile de chei RSA pentru cartele, generează cererile de certificat corespunzătoare, le transmite MD-CA, primește certificatele de la MD-CA, personalizează cartelele, ambalează cartelele si PIN-ul (pentru cartelele de atelier) si le trimite la MD-CIA pentru distribuție.

MD-CA își schimbă cheile la intervale regulate.

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

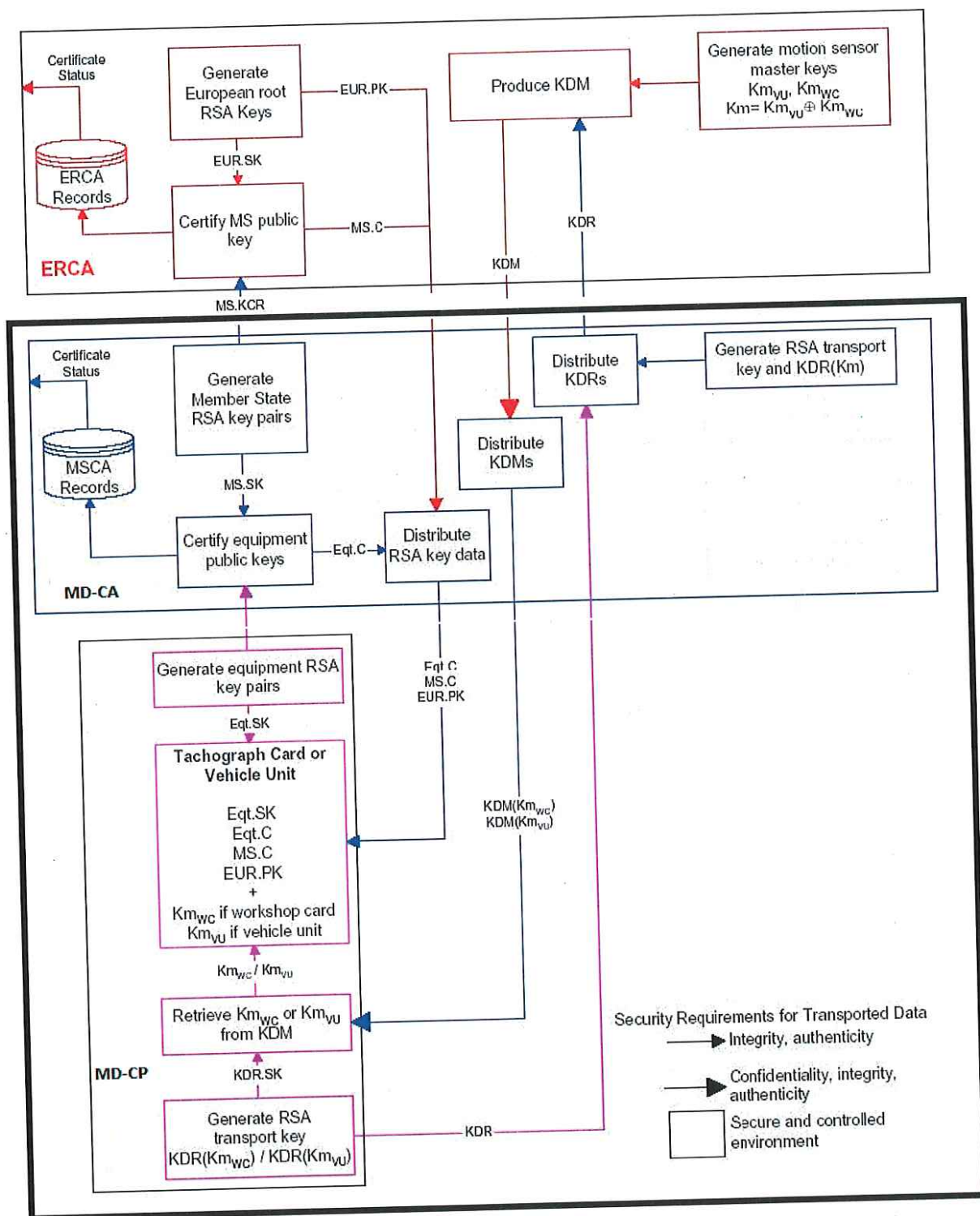
MD-CA generează, separa si distribuie o singura cheie criptografica simetrica, necesara pentru securizarea datelor de mișcare ale vehiculelor , in conformitate cu mecanismele definite de standardul ISO / IEC 16844-3.

Cheia master K_m este separata in doua părți , $K_{m_{VU}}$ si $K_{m_{WC}}$. $K_{m_{WC}}$ sunt inserate in cardurile de atelier de către personalizatorii de carduri.

Pentru a asigura confidențialitatea cheii $K_{m_{WC}}$ in timpul transportului de la ERCA la MD-CA, ERCA o criptează folosind o cheie publica de criptare RSA, pentru a produce un mesaj de distribuție a cheii (KDM). Același lucru este valabil si pentru transportul aceleiași cheii $K_{m_{WC}}$ de la MD-CA la MD-CP. Cheile RSA folosite la crearea mesajelor KDM sunt create de MD-CA sau MD-CP si trimise către ERCA sau respectiv MD-CA printr-o cerere de distribuție (KDR).

Necesitatea ca MD-CA sau MD-CP sa primească cheia $K_{m_{WC}}$ este definita intr-un acord semnat de ERCA si MD-A.





1.2 Numele si Identificarea Documentului

Acest document poarta denumirea de "Codul de Practici si Proceduri pentru Operarea MD-CP pentru Sistemul Tahografelor Digitale" si va fi referit in continuare simplu ca MD-CP CPP.

1.3 Participanți

Acest CPP este creat doar pentru a îndeplini cerințele sistemului pentru tahografe digitale.

1.3.1 Autoritatea de Certificare

MD-CA si MD-CP sunt operate sub autoritatea si responsabilitatea autorităților moldovene responsabile, sau a furnizorilor de servicii autorizați. MD-CA este certificat de ERCA.

1.3.2 Autoritatea de Înregistrare

Autoritatea Națională de Înregistrare implementează sisteme, produse si servicii necesare pentru emiterea de carduri de tahograf. RA-ul național este responsabil pentru a menține legătura între identificatorii subiecților certificatelor (cardurile) si persoanele fizice sau juridice care le folosesc. In Moldova, funcția RA pentru emiterea de certificate digitale pentru carduri de tahograf si cheii $K_{m_{wc}}$ este asigurata de MD-CIA.

1.3.3 Abonați

Abonații serviciilor de certificare oferite de MD-CA sunt cardurile de tahograf.

1.3.5 Destinatarii Cheilor pentru Senzorii de Mișcare

Destinatarii cheilor $K_{m_{wc}}$ sunt organizațiile care personalizează cardurile de atelier. Acestea sunt identificate in acordul semnat între ERCA si MD-CA.

1.4 Utilizarea certificatului

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

Certificatele pentru tahografele digitale pot fi folosite in aplicații in legătura sistemul tahografelor digitale (de exemplu: Echipamente de calibrare utilizate in ateliere, echipamente pentru descărcarea de date folosite de organele de control, sisteme de management al flotelor auto si/sau mărfurilor 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 $K_{m_{wc}}$ între ERCA si MD-CA si între MD-CA si MD-CP.

1.6 Administrarea CPP

1 Acest CPP este creat, menținut si revizuit de către S.C. CERTSIGN S.A., care îndeplinește funcția de furnizor de servicii de personalizare pentru MD-CP, având ManufacturerCode 21₁₆ alocat de către "Digital Tachograph Laboratory" al Comisiei Europene, conform cerinței din Commission Regulation 1360/2002,

Annex I(B) Appendix 1, paragraph 2.67. De asemenea, S.C. CERTSIGN S.A. este declarat ca "service agency for MD-CA" conform politicii de securitate "Moldovian CA Policy", aprobata de către ERCA:

Organizația Moldoveana pentru Personalizarea Cardurilor de Tahograf

S.C. CERTSIGN S.A.

Sediu Social: Sos. Olteniței nr. 107 A, clădirea C1, parter

Sector 4, CP 041303, București, Romania

Sediu: Bulevardul Tudor Vladimirescu, nr. 29 A, AFI Tech Park 1,

Sector 5, București, România, CP 050881

Tel. (+4031)1011870

Fax: (+4021)3119905

Sediu de rezervă pentru situații de dezastru: Strada Gării 21, Cluj-Napoca, Cluj, România, 400394

2. Orice întrebare referitoare la prezentul CPP trebuie trimise către: S.C. CERTSIGN S.A.
3. Orice întrebare referitoare la operarea MD-CP trebuie trimise către S.C. CERTSIGN S.A.
4. Autoritatea Națională, MD-A, trebuie să stabilească dacă acest CPP este conform cu Politica de Certificare a MD-A.
5. Stabilirea conformității se bazează pe o evaluare de securitate realizată fie chiar de către MD-A, fie de un terț autorizat.



1.7 Definiții 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 către un agent de paza, sau a unei informatice de către un sistem care cuprinde un senzor, un mediu de transmisie si un panou de alarma unde se trimite alarma.

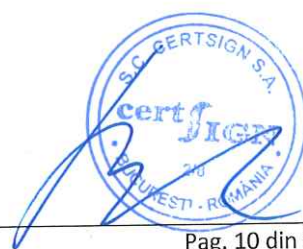
Escrow-ul cheii: trimiterea unei copii a cheii către o entitate autorizata sa folosească aceasta copie pentru alt scop decât acela de a-l returna entității care a generat cheia.

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

CAR	Certification Authority Reference
CHA	Certificate Holder Authorisation
CHR	Certificate Holder Reference
CIS	Center of Internet Security
CP	Component Personaliser
CPP	Codul de Practici si Proceduri
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
MD-A	Republic of Moldova Authority
MD-CA	Republic of Moldova Certification Authority



MD-CIA	Republic of Moldova Card Issuing Authority
MD-CP	Republic of Moldova Card Personalizing organization
NIST	National Institute of Standards and Technology
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 CONTROALE TEHNICE DE SECURITATE

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

2.1 *Generarea si Instalarea Perechii de Chei pentru Carduri*

2.1.1 Generarea perechii de chei

Procedurile de management a cheii se referă la păstrarea și folosirea în siguranță de către proprietar a cheilor sale.

Semnătura electronică este creată prin folosirea algoritmului RSA în combinație cu rezumatul criptografic SHA-1.

Generarea perechii de chei pentru carduri este realizată în serverele criptografice utilizând un HSM Cryptographic P3 data preparation module și a unui HSM nShield Connect. Modulele HSM ale serverelor criptografice sunt conforme cu cerințele FIPS 140-2 Nivel 3. Cheia privată este menținută în permanență criptată atât pe dispozitivul HSM, în baza de date CP și în tranzit către mașina de personalizat carduri.

Acțiunile întreprinse în momentul generării perechii de chei sunt înregistrate și datate. Înregistrările sunt păstrate din motive de audit sau pentru verificările obișnuite ale sistemului.

2.1.2 Distribuirea cheii private către entități

Transferul cheii private din modulul HSM în card se face în mod securizat cu ajutorul aplicației de personalizare. Nici o entitate nu poate interveni pentru a compromite cheia sau pentru a o copia.

2.1.3 Trimiterea cheii publice către emițătorul certificatului (MD-CA)

Conform politicii MD-CA.

2.1.4 Distribuirea cheilor publice ale cardurilor către entitățile partenere

Cheia publică a cardului este distribuită de MD-CP pe card sub forma de certificat emis de MD-CA, semnat cu cheia privată a MD-CA. Cheia publică a MD-CA este distribuită către MD-CP sub forma de certificat emis de ERCA. Cheia publică ERCA este distribuită către MD-CP ca atare. Distribuția certificatului MD-CA și a cheii publice a ERCA către MD-CP se face împreună cu certificatul cardului ca urmare a unei cereri KCR primite de MD-CA de la MD-CP.

2.1.5 Mărimile cheilor

Cheile RSA trebuie să aibă un modul de 1024 biți și un exponent public de 64 biți.



2.1.6 Parametrii de generare ai cheilor publice

Entitatea ca generează o cheie este responsabilă de verificarea calității parametrilor cheii generate. Aceasta trebuie să verifice:

- posibilitatea de a efectua operații de criptare și decriptare, inclusiv creare de semnături electronice și 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 și DSA).

2.1.7 Verificarea calității parametrilor

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

2.1.8 Generarea Hardware/software a cheii

Cheile pentru carduri sunt generate în module HSM certificate.

2.1.9 Utilizarea perechii de chei

Cheia privată RSA a cardului este utilizată doar pentru semnarea certificatelor cheilor cererii de certificat către MD-CA.

2.2 Protecția Cheii Private

2.2.1 Standarde și controale pentru modulele criptografice

MD-CP utilizează pentru generarea și stocarea cheilor private RSA ale cardurilor doar module HSM certificate. Operația modulului HSM este verificată periodic prin teste interne, iar upgrade-ul de firmware pentru HSM este realizat anual de administratorul HSM, dacă este cazul.

2.2.2 Controlul k din n al cheii private

Generarea cheii private este realizată de un HSM P3 data preparation pentru autorizarea căruia este necesară prezența a trei persoane autorizate și un HSM nShield Connect pentru autorizarea căruia este necesară prezența a două persoane autorizate.

2.2.3 Backup-ul cheii private

Nu se aplică.

2.2.4 Arhivarea cheii private

Nu se aplică.

2.2.5 Transferul cheii private din sau într-un modul HSM

Cheia privată RSA pentru carduri este generată în HSM și apoi transferată pe card în mod securizat.

2.2.6 Păstrarea cheii private într-un modul HSM

Cheile private ale cardurilor nu sunt păstrate în modulul HSM unde au fost generate.

2.2.7 Metoda de activare a cheii private

Activarea modului HSM pentru generarea cheilor private pentru cardurile tahograf se face folosind o schema 3/3 pentru HSM-ul P3 data preparation și o schema 2/6 pentru HSM-ul nShield Connect.

2.2.10 Certificarea modului HSM

MD-CP folosește module criptografice certificate cel puțin FIPS 140-2 Level 3.

2.3 Alte Aspecte ale Managementului Perechii de Chei

2.3.1 Arhivarea Cheii Publice

Perechile de chei a cardurilor tahograf sunt păstrate criptat în baza de date CP pentru o perioadă de 30 de zile.

2.3.2 Perioadele de validitate pentru cheile publice și private emise de MD-CP

Perioada de validitate a cheii private a cardului este de maximum: 5 ani (șoferi și companie), 2 controlor și 1 an (atelier).

Perioada de validitate a cheii publice a cardului este de maximum: 5 ani (șoferi și companie), 2 controlor și 1 an (atelier).

2.4 Datele de Activare

Singurul tip de card care folosește date de activare (PIN) este cardul de atelier.

2.5 Controale de Securitate a Calculatoarelor

Sarcinile operatorilor și administratorilor care lucrează în cadrul MD-CP sunt realizate prin intermediul unor dispozitive hardware și aplicații software de încredere.

2.5.1 Cerințele tehnice specifice securității calculatoarelor

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

Calculatoarele aparținând MD-CP dispun de următoarele mijloace de securitate:

- autentificarea obligatorie la nivelul sistemului de operare și 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 MD-CP,
- separarea sarcinilor, conform rolului în cadrul sistemului,



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

2.5.2 Evaluarea securității calculatoarelor

Sistemele de calcul ale MD-CP respectă cerințele descrise în procedura internă de hardening, dezvoltată pe baza standardelor National Institute of Standards and Technology (NIST) și Center for Internet Security (CIS).

2.5.3 Controale tehnice specifice ciclului de viață

Controale specifice dezvoltării sistemului

Fiecare aplicație, înainte de a fi folosită în producție de către MD-CP, este instalată astfel încât să se permită controlul versiunii curente și 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 așa fel încât să poată fi urmărită și 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 și de încredere.

Controale pentru managementul securității

Scopul controalelor pentru managementul securității este acela de a superviza funcționalitatea sistemelor MD-CP, garantând astfel că acestea operează corect și în concordanță cu configurarea acceptată și implementată.

Configurația curentă a sistemelor MD-CP, precum și orice modificare și actualizare a acestora, este înregistrată și controlată.

Controalele aplicate sistemelor MD-CP permit verificarea continuă a integrității aplicațiilor, versiunii și autentificarea și verificarea originii dispozitivelor hardware.



2.5.4 Controale de securitatea a rețelei

Serverele și stațiile de lucru de încredere aparținând MD-CP sunt conectate prin intermediul unei rețele locale (LAN), divizate în mai multe subrețele, cu acces controlat. Accesul dinspre alte rețele către orice segment, este protejat prin intermediul unui firewall inteligent.

Controalele de securitate sunt dezvoltate pe baza firewall-ului și a filtrelor de trafic aplicate la nivelul rutelor.

Mijloacele de asigurare a securității rețelei acceptă doar mesajele transmise prin protocoale securizate. Evenimentele (log-urile) sunt înregistrate în jurnalele de sistem și permit supravegherea folosirii corecte a serviciilor furnizate de MD-CP.

2.5.5 Controale specifice modulelor criptografice

Controalele modulelor criptografice includ cerințele impuse pentru dezvoltarea, producția și livrarea modulelor. MD-CP nu definește cerințe specifice în acest domeniu. Totuși, MD-CP acceptă și utilizează numai module criptografice care corespund cerințelor Politicii de Certificare a MD-A.

2.5.6 Înregistrarea evenimentelor și procedurile de auditare

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

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 păstrată și dezvăluită atunci când se desfășoară un audit.

Tipuri de evenimente înregistrate

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

Log-urile de evenimente MD-CP 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 și răspunsurile serverului (sau invers) la nivelul protocolului de rețea (de exemplu: https); datele concrete care se înregistrează sunt: adresa IP a stației sau a server-ului, operațiunile executate (de exemplu: căutare, editare, scriere etc.) și rezultatele lor (de exemplu introducerea cu succes a unei înregistrări în baza de date),

- **erori** – conține informații despre erori la nivelul protocoalelor de rețea și la nivelul modulelor aplicațiilor;
- **audit** – conțin informații specifice serviciilor de certificare, de exemplu: cererea de înregistrare și 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 și au o capacitate prestabilită. Atunci când se depășește această capacitate, este creată automat o nouă versiune de jurnal. Jurnalul anterior este arhivat și șters de pe disc.

Fiecare înregistrare, automată sau manuală, conține următoarele informații:

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

Conținutul înregistrărilor se referă la:

- alertele firewall-urilor și IDS-urilor,
- operațiile asociate înregistrării, certificării etc.,
- modificări ale structurii hard sau soft,
- modificări ale rețelei și conexiunilor,
- înregistrările fizice în zonele securizate și violările de securitate,
- schimbările de parole, drepturi asupra codurilor PIN, rolurile personalului,
- accesul reușit și nereușit la baza de date MD-CP și la aplicațiile serverului,
- generarea de chei pentru carduri, etc.,
- fiecare cerere primită și decizia emisă în format electronic,
- istoria creării copiilor de backup și a arhivelor cu înregistrări.

Accesul al jurnalele de evenimente (log-uri) este permis în exclusivitate administratorului de securitate și auditorilor.

Frecvența analizei jurnalelor de evenimente

Înregistrările din jurnalul de evenimente pot fi revizuite fie manual, la intervale periodice, fie prin intermediul unui sistem automatizat de monitorizare și analiză.

În cadrul organizației, jurnalele de evenimente sunt colectate și analizate în timp real de către un sistem SIEM, care corelează automat evenimentele, detectează anomaliile și generează alerte specifice.

Prin urmare, analiza manuală lunară detaliată a jurnalelor de evenimente nu este necesară, fiind înlocuită de mecanismele automate de detecție și raportare furnizate de sistemul SIEM.

Perioada de retenție a jurnalelor de evenimente

Înregistrările evenimentelor sunt stocate în fișiere pe discul sistem până când acestea ating capacitatea maximă permisă. După depășirea spațiului alocat, jurnalele sunt păstrate în arhive.

Pe lângă arhivarea tradițională, toate jurnalele sunt colectate și stocate în sistemul SIEM, asigurând astfel monitorizarea și analiza în timp real.

Jurnalele arhivate, inclusiv cele stocate în SIEM, sunt păstrate cel puțin 10 ani.

Protecția jurnalelor de evenimente

Săptămânal, fiecare înregistrare din jurnale este arhivată pe suport de stocare dedicat. După depășirea numărului maxim de înregistrări permis pentru un jurnal, conținutul acestuia este arhivat.

Arhivele pot fi semnate și criptate, iar cheia utilizată pentru criptarea acestora este plasată sub controlul administratorului de securitate.

Pe lângă arhivarea tradițională, jurnalele sunt colectate și stocate în sistemul SIEM, asigurând monitorizarea și analiza continuă a evenimentelor.

Un jurnal de evenimente poate fi revăzut numai de administratorului de securitate, sau de către un auditor.

Accesul la jurnalul de evenimente este configurat în așa fel încât:

- numai entitățile de mai sus au dreptul să citească înregistrările jurnalului,
- numai administratorul de securitate poate arhiva sau șterge fișiere (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 așa fel încât, chiar și după arhivarea jurnalului, este imposibil să ștergi înregistrări, sau să ștergi jurnalul înaintea expirării perioadei de retenție a jurnalului.



Procedurile de backup pentru jurnalele de evenimente

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

Notificarea entităților responsabile de tratarea evenimentelor

Modulul de analiză a jurnalului de evenimente implementat în sistem examinează evenimentele curente și 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. 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: telefon mobil, poștă 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 MD-CP. Pentru a realiza acest lucru, sunt copiate următoarele aplicații și fișiere:

- discurile de instalare a aplicațiilor sistem (de exemplu sistemul de operare),
- discurile de instalare a aplicațiilor pentru MD-CP,
- istoricul cheilor,
- datele privind personalul MD-CP,
- jurnalele de evenimente.

Metoda de creare a copiilor de backup are o influență deosebită asupra timpului și costului restaurării aplicațiilor după defectarea, sau distrugerea sistemului. MD-CP folosește atât backup-uri full (săptămânale), cât și backup-uri incrementale (zilnice), toate copiile sunt clonate și clonele sunt păstrate în altă locație, în aceleași condiții de securitate ca și cele din locația primară.

Procedura de restaurare va fi verificată cel puțin o dată la 12 luni, pentru a se verifica utilitatea backup-ului, în caz de dezastru. Concluziile testelor vor fi înregistrate.

2.5.7 Arhivarea înregistrărilor

Este necesar ca toate datele și fișierele referitoare la informațiile despre securitatea sistemului să fie arhivate.

Pe baza arhivelor se creează copii de siguranță care sunt ținute în afara locației MD-CP.

Tipurile de date arhivate

Următoarele date sunt incluse în procesul de arhivare:

- informațiile rezultate în urma examinării și evaluării (ca urmare a unui audit) măsurilor de protecție logica și fizica ale MD-CP,
- fișiere de audit,
- fișiere de configurare.

Frecvența arhivării datelor

Datele se arhivează cel puțin o dată pe săptămână.

Perioada de păstrare a arhivelor

Arhivele de păstrează cel puțin 10 ani.



3 Controale de securitate fizică, organizațională și de personal

Acest capitol descrie cerințele generale privind securitatea fizică și organizațională, precum și activitatea personalului MD-CP în activitatea de management al cheilor, personalizarea logica și optica a cardurilor, audit și crearea de copii de siguranță.

3.1 Controale de securitate fizică

3.1.1 Controale de securitate fizică în cadrul MD-CP

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

Amplasarea locației

MD-CP este localizată în București, la următoarea adresă:

Bulevardul Tudor Vladimirescu, nr. 29 A, AFI Tech Park 1,

Sector 5, București, România, CP 050881

MD-CP pentru sistemul de recuperare în caz de dezastru este localizat în Cluj-Napoca, la următoarea adresă:

Strada Gării 21, Cluj-Napoca, Cluj, 400394

Accesul fizic

Accesul fizic în cadrul MD-CP este controlat și monitorizat de un sistem de alarmă integrat. MD-CP dispune de sisteme de prevenire a incendiilor, sisteme de detectare a intrușilor și sisteme de alimentare cu energie electrică în caz de urgență.

Sediul MD-CP este accesibil numai persoanelor autorizate de către conducerea MD-CP. Vizitatorii locațiilor aparținând MD-CP trebuie să fie însoțiți permanent de persoane autorizate.

Zonele ocupate de MD-CP se împart în:

- zona serverelor,
- zona operatorilor CP
- zona de dezvoltare și testare.

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

Controlul accesului în *zona operatorilor* se face prin intermediul cardurilor și a cititoarelor de carduri. Deoarece toate informațiile sensitive sunt protejate prin folosirea unor seifuri, iar accesul la terminalele operatorilor și 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 MD-CP și persoanele autorizate; ultimilor nu le este permisă prezența în zonă neînsoțiți.

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

Sursa de alimentare cu electricitate și aerul condiționat

Zona operatorilor și administratorilor, precum și zona de dezvoltare și 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. Locația MD-CP dispune de sistem de prevenire a inundațiilor, fiind utilizați senzori amplasați la nivelul podelelor în conformitate cu standardele și reglementările în domeniu.

Prevenirea incendiilor

Locația MD-CP dispune de sistem de prevenire și protecție împotriva incendiilor în conformitate cu standardele și reglementările în domeniu.

Depozitarea mediilor de stocare a informațiilor

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

Aruncarea deșeurilor

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

Depozitarea backup-urilor în afara locației

Copiile parolelor, codurile PIN și cardurile criptografice pentru autorizarea accesului sunt stocate în containere speciale, situate în afara locației MD-CP.

Stocarea în afara locației se aplică și în cazul arhivelor, copiilor curente ale informațiilor procesate de sistem și kit-urilor de instalare ale aplicațiilor MD-CP. Acest lucru permite refacerea de urgență a oricărei funcții a MD-CP în 24 de ore, în locația principală a MD-CP, sau în locația auxiliară.

3.2 Controlul securității organizației

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

3.2.1 Roluri de încredere

Roluri de încredere în MD-CP

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

- **Responsabilul MD-CP**
 - Răspunzător pentru operarea sigură și continuă a funcției MD-CP,
 - Este reprezentantul organizației și este autorizat să ia decizii în cadrul organizației MD-CP,
 - Nu este direct implicat în implementarea proceselor de afaceri, dar este responsabil pentru respectarea și evaluarea măsurilor de securitate, ca și pentru managementul MD-CP,
 - Acceptă responsabilitatea pentru managementul schimbării.
- **Administrator de securitate** – Responsabilitate globală pentru implementarea politicilor și procedurilor de securitate.
 - Inițiază instalarea, configurarea și managementul aplicațiilor software și hardware (inclusiv resursele de rețea) ale MD-CP; inițiază și suspendă serviciile oferite de MD-CP; coordonează administratorii, inițiază și supraveghează generarea de chei și secrete partajate; atribuie drepturi din punct de vedere al securității și privilegiilor de acces ale utilizatorilor; atribuie parole pentru conturile utilizatorilor noi; verifică jurnalele de evenimente; supervizează auditurile interne și externe; primește și răspunde la rapoartele de audit; supervizează eliminarea deficiențelor constatate în urma auditului.
 - Supraveghează operatorii;
 - Configurează sistemele și rețeaua, activează și configurează mecanismele de protecție a rețelei; creează conturile pentru utilizatorii MD-CP; verifică log-urile de sistem; verifică respectarea Codului de Practici și Proceduri; generează secrete partajate și chei; creează copiile de siguranță de urgență; modifică numele și adresele serverelor.

- **Administratorul de sistem** – Autorizat să instaleze, configureze și să întrețină sistemele de încredere ale MD-CP pentru managementul cardurilor și al cheilor. Instalează dispozitivele hardware și sistemele de operare; instalează și configurează echipamentele de rețea.
- **Operator** – Responsabil de operarea zilnică a sistemelor de încredere ale MD-CP; ia parte în procesul de personalizare logică și optică a cardurilor.
- **HSM Administrator**
 - Autorizează accesul la HSM pentru procesul de management al cheilor,
- **Auditorul de sistem** – autorizat să acceseze arhivele și log-urile de audit ale sistemelor de încredere ale MD-CP. Responsabil de efectuarea de audituri interne pentru respectarea Codului de Practici și Proceduri de către personalul MD-CP;

*În cadrul MD-CP, 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.*

3.2.2 Numărul de persoane necesare pentru îndeplinirea unei sarcini

Procesul de generare de chei – pentru certificatele cardurilor de tahograf sau pentru generarea KDR și importul KDM este una din operațiile ce necesită o atenție deosebită. Generarea necesită prezența persoanelor care dețin următoarele roluri:

- I. Acțiunea de personalizare carduri: 3 operatori CP și un administrator de sistem,
- II. Acțiunea de generare KDR și import KDM: un administrator de securitate, 3 administratori de HSM și un administrator de sistem pentru utilizarea HSM-ului P3 gata preparation și un administrator de securitate, 2 administratori de HSM și un administrator de sistem pentru utilizarea HSM-ului nShield Connect.

3.2.3 Identificarea și autentificarea pentru fiecare rol

Personalul MD-CP este supus identificării și autentificării în următoarele situații:

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

Fiecare cont asignat:

- trebuie să fie unic și 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 MD-CP, a sistemului de operare și a controalelor de aplicații.

Operațiile efectuate în MD-CP care necesită acces la resurse de rețea comune sunt protejate prin mecanisme de autentificare sigură și de criptare a informațiilor transmise.

3.3 Controlul personalului

MD-CP trebuie să se asigure că persoana care îndeplinește responsabilitățile funcției, conform cu rolul atribuit în cadrul MD-CP:

- a absolvit cel puțin liceul,
- este cetățean român,
- a semnat un contract care descrie rolul și responsabilitățile sale în cadrul sistemului,
- a beneficiat de un stagiul de pregătire avansată în conformitate cu obligațiile și sarcinile asociate funcției sale,
- a fost instruit cu privire la protecția datelor personale și informațiilor confidențiale sau private,
- a semnat un contract ce conține clauze referitoare la protejarea datelor confidențiale (din punctul de vedere al securității MD-CP),

3.3.1 Experiența personală, calificările și clauzele de confidențialitate necesare

Personalul angajat al MD-CP care îndeplinește 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 permite accesul la informațiile clasificate. Dezvăluirea neautorizată a acestor informații poate cauza pierderea sau compromiterea intereselor, apărute de lege, ale unei persoane fizice sau ale unei organizații.

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

3.3.2 Cerințele de pregătire a personalului

Personalul care îndeplinește roluri și sarcini ca urmare a angajării la MD-CP, trebuie să fie instruit cu privire la:

- reglementările Codului de Practici și Proceduri al MD-CP,
- reglementările Politicii de certificare a MD-CA,
- procedurile și controalele de securitate folosite de MD-CA,
- aplicațiile software ale MD-CP,
- responsabilitățile ce decurg din rolurile și sarcinile executate în sistem,
- procedurile ce trebuie executate ca urmare a apariției unei defecțiuni în funcționarea sistemului.

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

3.3.3 Frecvența stagiilor de pregătire

Pregătirea descrisă în paragraful 3.3.2 trebuie repetată de fiecare dată când apar modificări semnificative în MD-CP.

3.3.4 Rotația funcțiilor

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

3.3.5 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 MD-CP. Măsurile disciplinare pentru astfel de incidente trebuie descrise în regulamente corespunzătoare și trebuie să fie conforme cu prevederile legale.

3.3.6 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 și în cazul angajaților MD-CP. În plus, personalul angajat pe bază de contract, pe timpul cât își desfășoară activitatea în locația MD-CP, trebuie permanent însoțit de către un angajat al MD-CP, cu excepția celor care au primit avizare din partea administratorului de securitate și care poate accesa informații clasificate intern sau în conformitate cu normele legale în vigoare.

3.3.7 Documentația oferită personalului

MD-CP trebuie să ofere personalului său accesul la următoarele documente:

- Politica de certificare a MD-A,
- Codul de Practici și Proceduri al MD-CP,
- Responsabilitățile și obligațiile asociate rolului deținut în sistem,
- Manuale ale aplicațiilor,
- Manuale de operare,
- Proceduri operaționale.



4 AUDITURILE PENTRU STABILIREA CONFORMITATII SI ALTE EVALUARI

Auditurile au ca obiectiv verificarea consistenței acțiunilor MD-CP sau a entităților delegate de aceasta cu declarațiile și procedurile acestora (inclusiv cu prezentul Cod de Practici și Proceduri).

Auditurile desfășurate la MD-CP urmăresc în principal centrele de procesare a datelor, gestiunea cardurilor și a PIN-urilor, procedurile de gestiune a cheilor.

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

Frecvența auditării

Auditul extern pentru verificarea conformității cu reglementările legale și procedurale (Codul de Practici și Proceduri) se desfășoară la interval de doi ani. În cazul în care, în urma auditului, sunt identificate neconformități semnificative, se poate decide organizarea unui audit suplimentar la un interval de un an. Auditul intern este efectuat ori de câte ori administratorul de securitate consideră necesar, în funcție de rezultate și riscurile identificate.

4.1 Identitatea / calificările auditorului

Auditul extern trebuie realizat de personal având cunoștințe și experiență tehnică corespunzătoare (să dispună de documente care să certifice acest lucru) în domeniul infrastructurilor de chei publice, tehnologiilor și dispozitivelor de securitate informatică și de auditare a securității sistemelor. De asemenea auditorul trebuie să posede cunoștințe solide ale reglementărilor UE, CE și MD-A referitoare la sistemul tahografelor digitale.

Auditul intern este realizat de către departamentul de calitate și audit al MD-CP.

4.2 Relația auditorilor cu entitatea auditată

Vezi paragraful anterior. Auditorul nu trebuie să depindă în nici un fel de entitatea auditată și nici să nu fi fost în vreun fel implicat în activitățile de planificare și operare ale sistemelor ITC ale entității auditate.

4.3 Domeniile supuse auditării

Auditurile interne și externe se desfășoară conform regulilor și procedurilor acceptate pe plan internațional și vizează:

- securitatea fizică a MD-CP,
- procedurile de furnizare a serviciilor,
- securitatea aplicațiilor software și a accesului la rețea,
- securitatea personalului MD-CP,
- securitatea gestiunii cardurilor,



- jurnalele de evenimente și procedurile de monitorizare a sistemului,
- arhivarea și restaurarea datelor,
- procedurile de arhivare,
- înregistrările referitoare la modificarea parametrilor de configurare pentru MD-CP,
- înregistrările referitoare la analizele și verificările efectuate pentru aplicațiile software și dispozitivele hardware.

4.4 Analiza vulnerabilităților

MD-CP face anual o analiză a vulnerabilităților pentru fiecare procedură internă, aplicație și sistem informatic. Cerințele de analiză pot, de asemenea, să fie stabilite de către o instituție externă, autorizată să auditeze MD-CP. 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 și conformitatea cu Codul de Practici și Proceduri.

Instituția externă care efectuează auditul de securitate, trebuie să desfășoare această activitate respectând recomandările ISO/IEC 27001:2022.

4.5 Măsurile întreprinse ca urmare a descoperirii unei deficiențe

În cazul descoperirii unor deficiențe se pot lua trei tipuri de măsuri:

1. continuarea operațiilor,
2. continuarea limitată a operațiilor,
3. suspendarea operațiilor.

Auditorul, împreună cu MD-A, decide ce acțiuni trebuie întreprinse. Decizia se bazează pe gravitatea deficiențelor și a posibilului impact.

În cazul în care se decide acțiunea de tipul 1, managementul MD-CP este responsabil pentru implementarea măsurilor corective specificate în raportul de audit, în limitele de timp din același raport.

În cazul în care se decide acțiunea de tipul 2, MD-CP continuă operațiile în modul restrâns indicat în raportul de audit.

În cazul în care se decide acțiunea de tipul 3, toate cardurile afectate trebuie trecute pe un blacklist. Managementul MD-CP trebuie să raporteze săptămânal stadiul măsurilor de remediere către auditor. MD-A și auditorul determină când trebuie făcută o nouă evaluare de securitate. Dacă deficiențele sunt considerate ca remediate după reevaluare, atunci MD-CP își poate relua operațiile.



9.6 Comunicarea rezultatelor

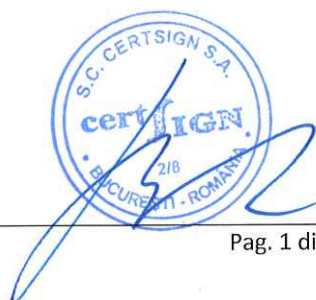
Rezultatele auditului sunt comunicate către MD-A. În cazul acțiunilor de tipul 1 sau 2, MD-A se asigură de faptul că toate entitățile care trebuie notificate primesc informațiile în conformitate cu prezentul document.



FINALUL DOCUMENTULUI



Sistemul de Tahograf Digital pentru Republica Moldova
Codul de Practici și Proceduri pentru implementarea
Politicii de Certificare a MD-CA si operarea MD-CA



CUPRINS

1 INTRODUCERE	5
1.1 Descriere generala	5
1.2 Numele si Identificarea Documentului	8
1.3 Participanti	8
1.3.1 Autoritatea de Certificare	8
1.3.2 Autoritatea de Înregistrare	8
1.3.3 Abonați	8
1.3.4 Entitățile partenere	8
1.3.5 Destinatarii Cheilor pentru Senzorii de Miscare	8
1.4 Utilizarea certificatului	8
1.5 Utilizarea Mesajului pentru Distribuirea Cheii (KDM)	8
1.6 Administrarea CPP	8
1.7 Definiții si Acronime	10
2 PUBLICAREA INFORMATIEI MD-CA	12
2.1 Depozitele de informații	12
2.2 Publicarea informației MD-CA	12
2.3 Frecvența publicării	12
3 IDENTIFICAREA SI AUTENTIFICAREA	13
3.1 Nume	13
3.1.1 Tipuri de Nume	13
3.1.2 Necesitatea ca numele sa aibă inteles	14
3.1.3 Anonimatul sau folosirea pseudonimelor pentru abonati	14
3.1.4 Reguli pentru interpretarea diferitelor forme ale numelor	14
3.1.5 Unicitatea numelor	14
3.1.6 Recunoașterea, autentificare si rolul brandurilor	14
3.2 Validarea Inițiala a Identității	14
3.2.1 Metoda pentru a demonstra posesia cheii private	14
3.2.2 Autentificarea identității individuale	15
3.3 Identificarea si Autentificarea pentru Cererile de Re-key	15
3.3.1 Identificarea si autentificarea pentru cererile de re-key de rutina	15
3.3.2 Identificarea si autentificarea pentru cererile de re-key după revocare	15
3.4 Identificarea si Autentificarea pentru Cererile de Revocare	15
4 CERINTELE OPERATIONALE PENTRU CICLUL DE VIATA AL CERTIFICATELOR	16
4.1 Cererea de Certificat	16
4.1.1 Cine poate face o cerere de certificat	16
4.1.2 Procesul de înregistrare si responsabilitățile asociate	16
4.2 Procesarea Cererilor de Certificat	16
4.2.1 Identificarea si autentificarea	16
4.2.2 Aprobarea sau respingerea cererilor de certificate	16
4.2.3 Timpul necesar pentru prelucrarea cererilor de certificate	16
4.3 Emiterea Certificatului	17
4.3.1 Acțiunile MD-CA in timpul emiterii certificatului	17
4.4 Acceptarea certificatului	17
4.4.1 Comportament care semnifica acceptarea certificatului	17
4.4.2 Distribuirea certificatelor de carduri si a informației aferente	17
4.5 Folosirea Perechii de Chei si a Certificatului	18
4.5.1 Folosirea Perechii de Chei si a Certificatului	18
4.5.2 Folosirea cheii publice si a certificatului de catre entitățile partenere	18
4.6 Reînnoirea Certificatului	18
4.7 Re-key	18
4.8 Modificarea Certificatului	18
4.9 Revocarea Certificatului	18
4.9.1 Cerințe speciale referitoare la compromiterea cheii	18



4.9.2 Suspendarea certificatului.....	19
4.10 Servicii de Verificare a Stării Certificatului	19
4.11 Escrow-ul si Recuperarea Cheii.....	19
5 CERINTELE CICLULUI DE VIATA AL CHEII SENZORULUI DE MISCARE	20
5.1 Cererile pentru Serviciile de Distribuie a Cheii Senzorului de Miscare	20
5.1.1 Cine poate trimite o cerere de distribuie a cheii senzorului de miscare	20
5.1.2 Procesul de înregistrare si responsabilitățile asociate	20
5.2 Procesarea cererilor KDR pentru cheia senzorului de miscare	20
5.2.1 Identificarea si autentificarea	20
5.2.2 Timpul in care se procesează cererile de distribuție KDR.....	21
5.3 Distribuiea KDM a cheii senzorului de miscare.....	21
5.3.1 Acțiunile MD-CA in timpul emiterii mesajului de distribuie a cheii senzorului de miscare	21
5.4 Folosirea Cheii Senzorului de Miscare	21
5.4.1 Folosirea cheii de catre destinatar	21
5.4.2 Responsabilitățile Entităților Partenere.....	21
5.5 Cerințe speciale referitoare la compromiterea cheii	21
6 Controale de securitate fizică, organizațională și de personal	22
6.1 Controale de securitate fizică	22
6.1.1 Controale de securitate fizică în cadrul MD-CA.....	22
6.2 Controlul securității organizației	24
6.2.1 Roluri de încredere	24
6.2.2 Numărul de persoane necesare pentru îndeplinirea unei sarcini	25
6.2.3 Identificarea și autentificarea pentru fiecare rol	25
6.3 Controlul personalului	26
6.3.1 Experiența personală, calificările și clauzele de confidențialitate necesare	26
6.3.2 Cerințele de pregătire a personalului	27
6.3.3 Frecvența stagiilor de pregătire.....	27
6.3.4 Rotația funcțiilor	27
6.3.5 Sancționarea acțiunilor neautorizate	27
6.3.6 Personalul angajat pe baza de contract.....	27
6.3.7 Documentația oferită personalului	28
7 CONTROALE TEHNICE DE SECURITATE	29
7.1 Generarea si Instalarea Perechii de Chei a MD-CA.....	29
7.1.1 Generarea perechii de chei a MD-CA.....	29
7.1.2 Distribuiea cheii private catre entități.....	29
7.1.3 Trimiterea cheii publice catre emițătorul certificatului (ERCA)	29
7.1.4 Distribuiea cheilor publice ale MD-CA si ERCA catre entitățile partenere.....	29
7.1.5 Mărimile cheilor	29
7.1.6 Parametrii de generare ai cheilor publice	29
7.1.7 Verificarea calității parametrilor	30
7.1.8 Generarea Hardware/software a cheii.....	30
7.1.9 Utilizarea perechii de chei a MD-CA	30
7.2 Protecția Cheii Private	30
7.2.1 Standarde si controale pentru modulele criptografice	30
7.2.2 Controlul k din n al cheii private	30
7.2.3 Escrow-ul cheii private.....	31
7.2.4 Backup-ul cheii private.....	31
7.2.5 Arhivarea cheii private	31
7.2.6 Transferul cheii private din sau intr-un modul HSM.....	31
7.2.7 Păstrarea cheii private intr-un modul HSM	31
7.2.8 Metoda de activare a cheii private	31
7.2.9 Metoda dezactivării cheii private	31
7.2.10 Metoda distrugerii cheii private	31
7.2.11 Certificarea modulului HSM	31
7.3 Alte Aspecte ale Managementului Perechii de Chei	32
7.3.1 Arhivarea Cheii Publice	32
7.3.2 Perioadele de validitate pentru cheile publice si private ale MD-CA.....	32



7.4	Datele de Activare	32
7.5	Controale de Securitate a Calculatoarelor	33
7.5.1	Cerințele tehnice specifice securității calculatoarelor	33
7.5.2	Evaluarea securității calculatoarelor	34
7.5.3	Controale tehnice specifice ciclului de viața	34
7.5.4	Controale de securitatea a rețelei	34
7.5.5	Controale specifice modulelor criptografice	35
7.5.6	Înregistrarea evenimentelor și procedurile de auditare	35
7.5.7	Arhivarea înregistrărilor	38
7.6	Compromiterea cheilor și Recuperarea în Caz de Dezastru	39
7.6.1	Procedurile de tratare a incidentelor de securitate și a cazurilor de compromitere a cheilor	39
7.6.2	Defecțiuni ale echipamentelor, software-ului sau pierderea integrității datelor	39
7.6.3	Procedurile în cazul compromiterii cheii private	39
7.6.4	Continuarea afacerii în caz de dezastru	39
7.7	Scoaterea din uz a MD-CA	40
8	AUDITURILE PENTRU STABILIREA CONFORMITĂȚII ȘI ALTE EVALUARI	41
9.1	Identitatea / calificările auditorului	41
9.2	Relația auditorilor cu entitatea auditată	41
9.3	Domeniile supuse auditării	41
9.4	Analiza vulnerabilităților	42
9.5	Măsurile întreprinse ca urmare a descoperirii unei deficiențe	42
9.6	Comunicarea rezultatelor	43

1 INTRODUCERE

Agentia Nationala Transport Auto este responsabila pentru funcția de Autoritate Națională 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 mișcare);
- Chei de criptare pentru datele senzorilor de mișcare.

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

Documentul a fost creat pentru a asigura conformitatea cu cerințele enunțate in Politica de Certificare a MD-A si se bazează pe cadrul creat prin IETF RFC 3647.

1.1 Descriere generala

Scopul principal al acestui document este acela de a fi folosit de către MD-A si de către cei care doresc sa evalueze gradul de încredere care poate fi acordat serviciilor oferite de MD-CA, sau sa determine măsura in care acestea respecta cerințele sistemului pentru tahografe digitale.

Sistemul de management al cheilor criptografice (vezi figura următoare) 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.

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

MD-CA are rolul de a certifica cheile RSA care sunt introduse in cardurile pentru tahografe de către MD-CP.

Mai multe tipuri de carduri sunt emise șoferilor, atelierelor, organelor de control si firmelor de transport.

MD-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.

MD-CA genereaza, separa si distribuie o singura cheie criptografica simetrica, necesara pentru securizarea datelor de miscare ale vehiculelor, in conformitate cu mecanismele definite de standardul ISO / IEC 16844-3.

Cheia master Km este separata in doua parti , Km_{VU} si Km_{WC} . Km_{WC} sunt inserate in cardurile de atelier de catre personalizatorii de carduri.

Pentru a asigura confidentialitatea cheii Km_{WC} in timpul transportului de la ERCA la MD-CA, ERCA o criptează folosind o cheie publica de criptare RSA, pentru a produce un mesaj de distribuție a cheii (KDM). Același lucru este valabil si pentru transportul aceleiași cheii Km_{WC} de la MD-CA la MD-CP. Cheile RSA folosite la crearea mesajelor KDM sunt create de MD-CA sau MD-CP si trimise catre ERCA sau respectiv MD-CA printr-o cerere de distribuție (KDR).

Necesitatea ca MD-CA sau MD-CP sa primească cheia Km_{WC} este definita intr-un acord semnat de ERCA si MD-A.

1.2 Numele si Identificarea Documentului

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

1.3 Participanti

Acest CPP este creat doar pentru a îndeplini cerințele sistemului pentru tahografe digitale.

1.3.1 Autoritatea de Certificare

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

1.3.2 Autoritatea de Înregistrare

Autoritatea Nationala de Înregistrare implementează sisteme, produse si servicii necesare pentru emiterea de carduri de tahograf. RA-ul național este responsabil pentru a menține legătura între identificatorii subiecților certificatelor (cardurile) si persoanele fizice sau juridice care le folosesc. In Moldova, funcția RA pentru emiterea de certificate digitale pentru carduri de tahograf si cheii Km_{wc} este asigurata de MD-CIA.

1.3.3 Abonați

Abonații serviciilor de certificare oferite de MD-CA sunt cardurile de tahograf.

1.3.4 Entitățile partenere

1.3.5 Destinatarii Cheilor pentru Senzorii de Miscare

Destinatarii cheilor Km_{wc} sunt organizațiile care personalizează cardurile de atelier. Acestea sunt identificate in acordul semnat între ERCA si MD-CA.

1.4 Utilizarea certificatului

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

Certificatele pentru tahografele digitale pot fi folosite in aplicații in legătura sistemul tahografelor digitale (de exemplu: Echipamente de calibrare utilizate in ateliere, echipamente pentru descărcarea de date folosite de organele de control, sisteme de management al flotelor auto si/sau mărfurilor 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} între ERCA si MD-CA si între MD-CA si MD-CP.

1.6 Administrarea CPP

1 Acest CPP este creat, menținut si revizuit de catre S.C. CERTSIGN S.A., care îndeplinește funcția de furnizor de servicii de certificare pentru MD-CA, fiind declarat ca "service agency for MD-CA" conform



politicii de securitate "MD CA Policy", aprobată de către ERCA:

Autoritatea de Certificare pentru Sistemul Moldovean de Tahografe Digitale
S.C. CERTSIGN S.A.

Sediu Social: Sos. Oltenitei nr. 107 A, clădirea C1, parter

Sector 4, CP 041303, București, România

Sediu: Bulevardul Tudor Vladimirescu, nr. 29 A, AFI Tech Park 1,

Sector 5, București, România, CP 050881

Tel. (+4031)1011870

Fax: (+4021)3119905

Sediu de rezervă pentru situații de dezastru: Strada Gării 21, Cluj-Napoca, Cluj, România, 400394

2. Orice întrebare referitoare la prezentul CPP trebuie trimisă către S.C. CERTSIGN S.A.
3. Orice întrebare referitoare la operarea MD-CA trebuie trimisă către S.C. CERTSIGN S.A.
4. Autoritatea Națională, MD-A, trebuie să stabilească dacă acest CPP este conform cu Politica de Certificare a MD-A.
5. Stabilirea conformității se bazează pe o evaluare de securitate realizată fie chiar de către MD-A, fie de un terț autorizat.



1.7 Definiții și Acronime

Criptare Asimetrică: procesul de criptare în care o cheie este folosită pentru a cripta mesajul și o cheie diferită este utilizată pentru decriptarea mesajului.

Detectarea Intruziunii: detectarea unei intruziuni fizice de către un agent de pază, sau a unei informații de către un sistem care cuprinde un senzor, un mediu de transmisie și un panou de alarmă unde se trimite alarma.

Escrow-ul cheii: trimiterea unei copii a cheii către o entitate autorizată să folosească această copie pentru alt scop decât acela de a-l returna entității care a generat cheia.

Criptare simetrică: procesul de criptare în care aceeași cheie este folosită și la criptarea mesajului și la decriptarea lui.

CAR	Certification Authority Reference
CHA	Certificate Holder Authorisation
CHR	Certificate Holder Reference
CIS	Center of Internet Security
CP	Component Personaliser
CPI	Certificate Profile Identifier
CPP	Codul de Practici și Proceduri
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
MD-A	Republic of Moldova Authority



MD-CA	Republic of Moldova Certification Authority
MD-CIA	Republic of Moldova Card Issuing Authority
MD-CP	Republic of Moldova Card Personalizing organization
NIST	National Institute of Standards and Technology
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 MD-CA

2.1 *Depozitele de informații*

Informații publice cu privire la acest CPP se găsesc în depozitele electronice ale MD-CA.

2.2 *Publicarea informației MD-CA*

MD-CA publica următoarele informații în depozitele electronice:

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

2.3 *Frecventa publicării*

Informațiile referitoare la modificările CPP sunt publicate în conformitate cu planificările făcute în 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 MD-CA.

Emitentul certificatului si subiectul certificatului sunt identificați prin stringuri de lungime fixa de 8 octeti care conțin informația ceruta de protocolul mutual de autentificare dintre componentele tahografice, definit in Reglementarea Comisie nr 1360/2002, Annex I(B) Appendix 11, cerința CSM020.

3.1.1 Tipuri de Nume

Emitentul Certificatului si al KDM

Identificarea emitentului certificatului si al KDM se face prin referința 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 octetistring definit in Reglementarea Comisiei nr. 1360/2002, Annex 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 MD-CA, EquipmentType desemnează o cartela de tahograf.

CHR apare in materialele printate si in datele descărcate din unitatea de vehicul. EquipmentType codificat in CHA este folosit in timpul procedurii mutuale de autentificare si selectează 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 MD-CP. In scopul distribuției 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 aibă inteles

Intelesul pe 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; ea nu poate fi stabilita din continutul certificatelor de cheie publica.

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

Anonimatul abonatilor nu este permis.

3.1.4 Reguli pentru interpretarea diferitelor forme ale numelor

Nu se stipulează nimic.

3.1.5 Unicitatea numelor

Pentru ca procesul autentificării mutuale sa funcționeze corect, identificatorul emitentului certificatului trebuie sa ide notifice unic o pereche de chei RSA.

3.1.6 Recunoașterea, autentificare si rolul brandurilor

Nu se stipulează nimic.

3.2 Validarea Inițiala a Identității

3.2.1 Metoda pentru a demonstra posesia cheii private

Abonatii care trimit cereri KCR trebuie sa demonstreze posesia cheii private corespunzătoare.

Protocolul KCR este definit in Politica ERCA.

Mesajele KCR constau din doua parti: o parte de text necodificat si semnătura digitala a acelu text.

Întotdeauna textul include o cheie publica RSA. Semnătura digitala a textului este creata cu cheia privata

corespunzătoare.

Verificarea semnăturii digitale realizată cu cheia publică demonstrează:

- Posesia cheii private;
- Integritatea textului.

Verificarea semnăturii este făcută la MD-CA. Dacă verificarea eșuează, cererea de certificat este respinsă.

3.2.2 Autentificarea identității individuale

Subiecții la care se referă MD-CA nu sunt persoane fizice. Această secțiune se referă doar la cerințele de identificare și autentificare pentru cererile de certificate de cheie pentru carduri și pentru certificatele de cheie publică schimbate între MD-CP și MD-CA.

Trebuie creată o legătură între aplicat (driver/firma de transport/atelier/politie), card cheie privată și certificat.

Dacă generarea cheii are loc în afara cardului, atunci MD-CA creează certificatul cerut dacă cel care face solicitarea demonstrează printr-o procedură agreeată că este în posesia cheii private.

3.3 Identificarea și Autentificarea pentru Cererile de Re-key

3.3.1 Identificarea și autentificarea pentru cererile de re-key de rutină

La fel ca la secțiunea 3.2 Validarea Inițială a Identității.

3.3.2 Identificarea și autentificarea pentru cererile de re-key după revocare

Nu se aplică.

3.4 Identificarea și Autentificarea pentru Cererile de Revocare

Certificatele pentru cardurile de tahograf nu se revocă. Pierderea cartei trebuie raportată de către posesorii acesteia la MD-CIA.

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 informațiile furnizate în cererea pentru cardurile de tahograf și preluate din registrul MD-CIA. Cheia publică care trebuie certificată este extrasă din cererea de certificat. MD-CA accepta doar cererile de certificat primite de la MD-CP. Aplicațiile software de la MD-CA și cele de la MD-CP asigură ca o cerere de certificat este generată doar pentru acele carduri pentru care există o cerere și ca cel care a făcut cererea este autentificat și autorizat.

4.1.2 Procesul de înregistrare și responsabilitățile asociate

Procesul de înregistrare este administrat la MD-CIA.

4.2 Procesarea Cererilor de Certificat

4.2.1 Identificarea și autentificarea

Funcțiile de identificare și autentificare sunt implementate la MD-CIA. MD-CP asigură prin aplicațiile sale software ca datele de intrare conțin informații care fac Certificate Holder Reference (CHR) unic.

4.2.2 Aprobarea sau respingerea cererilor de certificate

Dacă cererile sunt semnate cu cheia privată asociată cheii publice care trebuie certificată, atunci cererea este acceptată. În caz contrar, ea este respinsă.

4.2.3 Timpul necesar pentru prelucrarea cererilor de certificate

După primirea unei cereri valide de certificat, acesta este emis în maxim 24 de ore.



4.3 Emiterea Certificatului

4.3.1 Acțiunile MD-CA în timpul emiterii certificatului

Următoarele informații sunt înregistrate în baza de date a MD-CA pentru fiecare operație de certificare de cheie:

- certificatul complet;
- modulul RSA (n) și exponentul public (e) ale cheii publice;
- perioada de validitate a certificatului;
- Certificate Holder Reference (pentru identificarea cheii publice RSA);
- Hashul SHA-1 pentru datele certificatului în format binar;
- Hashul SHA-1 pentru datele mesajului KCR în format binar;
- timestamp.

4.4 Acceptarea certificatului

4.4.1 Comportament care semnifică acceptarea certificatului

Acceptarea cardului înseamnă și acceptarea certificatului asociat.

4.4.2 Distribuirea certificatelor de carduri și a informației aferente

MD-CA trebuie să exporte toate datele referitoare la certificat către registrul MD-CIA în așa fel încât certificatele, cardurile și utilizatorii acestora să fie asociați. MD-CIA se asigură că informația aferentă devine disponibilă celor care au nevoie de ea.



4.5 Folosirea Perechii de Chei si a Certificatului

4.5.1 Folosirea Perechii de Chei si a Certificatului

CertIFICATELE pentru componentele sistemului de tahografe digitale sunt destinate numai in cadrul acestuia.

Utilizarea perechilor de chei	Ciclu de viața	Validitate certificat
Șofer	5 ani	5 ani
Companie	5 ani	5 ani
Controlor	2 ani	2 ani
Atelier	1 an	1 an

Utilizarea cheilor pentru cardurile de tahograf

4.5.2 Folosirea cheii publice si a certificatului de catre entitățile partenere

Vezi 4.4.2.

4.6 Reînnoirea 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 Cerințe speciale referitoare la compromiterea cheii

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

Daca cheia MD-CA este compromisa, sau se suspectează ca este compromisa, atunci MD-CA trebuie sa raporteze incidentul la MD-A. Investigatiile care urmează si eventualele acțiuni sunt descrise in planul si procedurile de raspuns la incidente al organizatiei MD-CA.

4.9.2 Suspendarea certificatului

Nu se aplica.

4.10 Servicii de Verificare a Stării Certificatului

Nu se aplica.

4.11 Escrow-ul si Recuperarea Cheii

Escrow-ul cheii este strict interzisa de catre 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 MD-CA. Mai departe MD-CA le va distribui la cerere catre MD-CP.

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

5.1 Cererile pentru Serviciile de Distribuie a Cheii Senzorului de Miscare

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

MD-CA accepta cereri de distribuție doar de la MD-CP.

5.1.2 Procesul de înregistrare si responsabilitățile asociate

Procedura de înregistrare pentru destinatarii cheilor master ale senzorului de miscare este aceeași ca cea pentru serviciile de certificare ale MD-CA, descrise la secțiunea 4.1.2.

5.2 Procesarea cererilor KDR pentru cheia senzorului de miscare

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

5.2.1 Identificarea si autentificarea

Aplicațiile de interfațare MD-CA cu MD-CP de la MD-CA si MD-CP cu MD-CA de la MD-CP creează un canal securizat (autentificarea sursei si criptarea mesajului) prin care circula cererile KDR de la MD-CP si răspunsurile KDM de la MD-CA. In plus cheia publica RSA de transport a cheii senzorului de miscare K_{wc} generata la MD-CP este distribuita in mod sigur in mod offline catre MD-CA apoi încredințata curierului de încredere al MD-A. La primirea cererii KDR, MD-CP răspunde cu un KDM in care cheia K_{wc} este criptata cu cheia RSA de transport.



5.2.2 Timpul in care se procesează cererile de distribuție KDR

5.3 Distribuirea KDM a cheii senzorului de miscare

5.3.1 Acțiunile MD-CA in timpul emiterii mesajului de distribuire a cheii senzorului de miscare

Următoarele informații sunt înregistrate in baza de date MD-CA pentru fiecare operație KDM:

- modulul RSA (n) si exponentul public (e) pentru cheia publica a mesajului KDM;
- Key Identifier (pentru identificarea cheii publice RSA);
- Hashul SHA-1 pentru mesajul KDM in format binar;
- Hashul SHA-1 pentru mesajul KDR;
- KDM status "Pending acceptance";
- timestamp;
- un flag de distribuție one-time pentru cheia senzorului de miscare.

5.4 Folosirea Cheii Senzorului de Miscare

5.4.1 Folosirea cheii de catre destinatar

Folosirea cheii senzorului de miscare este restricționata la acele scopuri autorizate de Politicile ERCA si MD-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 master a senzorului de miscare.

5.4.2 Responsabilitățile Entităților Partenere

Nu exista nici o prevedere.

5.5 Cerințe speciale referitoare la compromiterea cheii

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

Daca o copie a unei chei a senzorului de miscare a fost compromisa sau se suspectează ca este compromisa, atunci MD-CP trebuie sa raporteze incidentul catre MD-A pentru investigații si pentru acțiuni in conformitate cu politica naționala. Investigațiile care urmează si eventualele acțiuni sunt descrise in planul si procedurile de raspuns la incidente al organizatiei MD-CA. Rezultatul acestor investigații se raportează catre ERCA.



6 Controale de securitate fizică, organizațională și de personal

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

6.1 Controale de securitate fizică

6.1.1 Controale de securitate fizică în cadrul MD-CA

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

Amplasarea locației

MD-CA este localizată în București, la următoarea adresă:

S.C. CERTSIGN S.A.

Bulevardul Tudor Vladimirescu, nr. 29 A, AFI Tech Park 1,
Sector 5, București, România, CP 050881

MD-CA pentru sistemul de recuperare în caz de dezastru este localizat în Cluj-Napoca, la următoarea adresă:

Strada Gării 21, Cluj-Napoca, Cluj, 400394

Accesul fizic

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

Accesul în sediul MD-CA este permis numai persoanelor autorizate de către conducerea MD-CA. Vizitatorii locațiilor aparținând MD-CA trebuie să fie însoțiți permanent de persoane autorizate.

Zonele ocupate de MD-CA se împart în:

- zona serverelor,
- zona operatorilor CA,
- zona administratorilor,
- zona de dezvoltare și testare.

Zona serverelor este echipată cu un sistem de securitate monitorizat continuu, alcătuit din senzori de mișcare, efracție și incendiu. Accesul în această zonă este permis numai personalului autorizat, de exemplu, administratorul de securitate, administratorul MD-CA și administratorul de sistem. Monitorizarea drepturilor de acces se face folosind carduri și cititoare, montate lângă punctul de acces. Fiecare intrare și ieșire din zonă este înregistrată automat în jurnalul de evenimente.

Controlul accesului în *zona operatorilor și administratorilor* se face prin intermediul cârdurilor și a cititoarelor de carduri. Deoarece toate informațiile sensitive sunt protejate prin folosirea unor seifuri, iar accesul la terminalele operatorilor și 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 MD-CA și persoanele autorizate.

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

Sursa de alimentare cu electricitate și aerul condiționat

Zona operatorilor și administratorilor, precum și zona de dezvoltare și 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. Locația MD-CA dispune de sistem de prevenire a inundațiilor, fiind utilizați senzori amplasați la nivelul podelelor în conformitate cu standardele și reglementările în domeniu.

Prevenirea incendiilor

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

Depozitarea mediilor de stocare a informațiilor

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

Aruncarea deșeurilor

Hârtiile și mediile electronice care conțin informații importante din punct de vedere al securității MD-CA sunt distruse după expirarea perioadei de păstrare. Modulele de securitate hardware sunt resetate și șterse.



conform recomandărilor producătorului. Aceste dispozitive sunt, de asemenea, resetate și șterse atunci când sunt trimise în service sau reparate.

Depozitarea backup-urilor în afara locației

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

Stocarea în afara locației se aplică și în cazul arhivelor, copiilor curente ale informațiilor procesate de sistem și kit-urilor de instalare ale aplicațiilor MD-CA. Acest lucru permite refacerea de urgență a oricărei funcții a MD-CA în 24 de ore, în locația principală a MD-CA, sau în locația auxiliară.

6.2 Controlul securității organizației

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

6.2.1 Roluri de încredere

Roluri de încredere în MD-CA

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

- **Responsabil MD-CA**
 - responsabil pentru operarea în siguranță și în parametrii ai MD-CA ca organizație.
 - este un reprezentant al organizației și este autorizat să dea instrucțiuni în cadrul organizației MD-CA.
 - direct implicat în punerea în aplicare a proceselor de afaceri, dar este responsabil pentru respectarea și evaluarea măsurilor de securitate, împreună cu conducerea MD-CA.
 - Își asuma responsabilitatea pentru Managementul schimbării.
- **Administrator de securitate** – Responsabilitate globală pentru implementarea politicilor și procedurilor de securitate. În plus poate aproba/revoca/suspenda certificate.
 - Inițiază instalarea, configurarea și managementul aplicațiilor software și hardware (inclusiv resursele de rețea) ale MD-CA; inițiază și suspendă serviciile oferite de MD-CA; coordonează administratorii, inițiază și supraveghează generarea de chei și secrete partajate; atribuie drepturi din punct de vedere al securității și privilegiilor de acces ale utilizatorilor; atribuie parole pentru conturile utilizatorilor noi; verifică jurnalele de evenimente; supervizează auditurile interne și externe; primește și răspunde la rapoartele de audit; supervizează eliminarea deficiențelor constatate în urma auditului.
 - Supraveghează operatorii Autorității de Certificare; configurează sistemele și rețeaua, activează și configurează mecanismele de protecție a rețelei; creează conturile pentru utilizatorii MD-CA; verifică log-urile de sistem; verifică respectarea Politicii de certificare și a



Codului de Practici și Proceduri; generează secrete partajate și chei; creează copii de siguranță de urgență; modifică numele și adresele serverelor.

- **Administratorul de sistem** – Autorizat să instaleze, configureze și să întrețină sistemele de încredere ale Autorității de Certificare pentru înregistrarea, generarea de certificate, inițializarea dispozitivelor. Instalează dispozitivele hardware și sistemele de operare; instalează și configurează echipamentele de rețea.
- **Ofițer de Securitate CA (CAO)** – Responsabil de operarea zilnică a sistemelor de încredere ale Autorității de Certificare.
- **Administrator CA (CAA)** – Autorizat să execute operațiile de backup și restaurare a sistemului. Are acces la certificatele Abonaților; asigură continuitatea copiilor de siguranță și arhivelor bazelor de date și a creării log-urilor de sistem; administrează bazele de date; are acces la informații confidențiale despre Abonați, dar nu poate accesa fizic nici o altă resursă a sistemului; transferă copiile de siguranță ale arhivei și ale datelor curente în afara locației MD-CA.
- **HSM Operator (HSMO)** – ia parte la procesul de semnare a certificatelor MD-CA.
- **HSM Administrator (HSMA)**
 - Execuția în condiții de siguranță a proceselor de gestionare a cheilor,
 - Generarea certificatelor, administrarea și ștergerea de chei asimetrice ale MD-CA.

Funcția HSMA poate fi pusă în aplicare numai pe baza principiului 'four-eyes-principle'.

- **Auditorul de sistem** – autorizat să acceseze arhivele și log-urile de audit ale sistemelor de încredere ale MD-CA. Responsabil de efectuarea de audituri interne pentru respectarea Codului de Practici și Proceduri de către MD-CA; această responsabilitate se extinde și asupra fiecărei Autorități de Înregistrare care operează în cadrul MD-CA.

*În cadrul MD-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 sau pentru transportul K_{mc} – este una din operațiile ce necesită o atenție deosebită. Generarea necesită prezența a cel puțin trei persoane: un administrator de securitate, doi administrator de HSM și un Operator CA.

Prezența Operatorului Autorității de Certificare și a unui număr corespunzător de operatori HSM este necesară și la încărcarea 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 și autentificarea pentru fiecare rol

Personalul MD-CA este supus identificării și autentificării în următoarele situații:



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

Fiecare cont asignat:

- trebuie să fie unic și 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 MD-CA, a sistemului de operare și a controalelor de aplicații.

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

6.3 Controlul personalului

MD-CA trebuie să se asigure că persoana care îndeplinește responsabilitățile funcției, conform cu rolul atribuit în cadrul MD-CA:

- a absolvit cel puțin liceul,
- este cetățean român,
- a semnat un contract care descrie rolul și responsabilitățile sale în cadrul sistemului,
- a beneficiat de un stagiu de pregătire avansată în conformitate cu obligațiile și sarcinile asociate funcției sale,
- a fost instruit cu privire la protecția datelor personale și informațiilor confidențiale sau private,
- a semnat un contract ce conține clauze referitoare la protejarea informațiilor sensitive (din punctul de vedere al securității MD-CA) și a datelor confidențiale și private ale Abonaților,
- nu îndeplinește sarcini care pot genera conflicte de interese între Autoritatea de Certificare MD-CA și Autoritatea de Înregistrare MD-CIA, care acționează în numele acesteia.

6.3.1 Experiența personală, calificările și clauzele de confidențialitate necesare

Personalul angajat al MD-CA care îndeplinește 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 de securitate, administrator al Autorității de Certificare și administrator HSM permite accesul la informațiile clasificate. Dezvăluirea neautorizată a acestor informații poate cauza pierderea sau compromiterea intereselor, apărute de lege, ale unei persoane fizice sau ale unei organizații.

Procedurile de acces la informațiile nepublice și 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 îndeplinește roluri și sarcini ca urmare a angajării la MD-CA, trebuie să fie instruit cu privire la:

- reglementările Codului de Practici și Proceduri,
- reglementările Politicii MSA,
- procedurile și controalele de securitate folosite de Autoritatea de Certificare,
- aplicațiile software ale Autorității de Certificare,
- responsabilitățile ce decurg din rolurile și 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 și Proceduri, Politica MD-A și acceptă restricțiile și 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 MD-CA.

6.3.4 Rotația funcțiilor

Acest Cod de Practici și 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 MD-CA. Măsurile disciplinare pentru astfel de incidente trebuie descrise în regulamente corespunzătoare și 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 și în cazul angajaților MD-CA. În plus, personalul angajat pe bază de contract, pe timpul cât își desfășoară activitatea în locația MD-CA, trebuie permanent însoțit de către un angajat al MD-CA, cu excepția celor care au primit avizare din partea administratorului de securitate și care poate accesa informații clasificate intern sau în conformitate cu normele legale în vigoare.

6.3.7 Documentația oferită personalului

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

- Politica MD-A,
- Codul de Practici și Proceduri,
- Responsabilitățile și obligațiile asociate rolului deținut în sistem,
- Manuale ale aplicațiilor,
- Proceduri operaționale.

7 CONTROALE TEHNICE DE SECURITATE

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

7.1 Generarea și Instalarea Perechii de Chei a MD-CA

7.1.1 Generarea perechii de chei a MD-CA

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

Autoritatea de Certificare **MD-CA** deține mai multe certificate semnate de către ERCA. Cheia privată corespunzătoare cheii publice conținută de aceste certificate este folosită exclusiv în scopul semnării certificatelor pentru cardurile tahograf și pentru generarea cererii criptografice a MD-CA adresate ERCA.

Generarea perechii de chei MD-CA (MD.SK și MD.PK) este realizată într-un server criptografic cu participarea activă a cel puțin trei persoane. Modulul HSM al serverului criptografic este conform cu cerințele FIPS 140-2 Nivel 3. Cheia privată este menținută în permanență criptată pe dispozitivul HSM.

Acțiunile întreprinse în momentul generării perechii de chei sunt înregistrate, datate și semnate de fiecare persoană prezentă în timpul generării. Înregistrările sunt păstrate din motive de audit sau pentru verificările obișnuite ale sistemului.

7.1.2 Distribuirea cheii private către entități

MD-CA nu generează cheile private RSA pentru carduri. Acestea sunt generate la MD-CP.

7.1.3 Trimiterea cheii publice către emițătorul certificatului (ERCA)

Conform politicii ERCA.

7.1.4 Distribuirea cheilor publice ale MD-CA și ERCA către entitățile partenere

Cheia publică a MD-CA este distribuită către MD-CP sub forma de certificat semnat cu cheia privată a ERCA. Cheia publică a ERCA este distribuită către MD-CP ca atare. Distribuirea lor se face împreună cu certificatul care va fi scris pe card ca urmare a unei cererii KCR primite de MD-CA de la MD-CP.

7.1.5 Mărimile cheilor

Cheile RSA au lungimea modulului de 1024 de biți, iar lungimea exponentului cheii publice de 64-biți.

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 și decriptare, inclusiv creare de semnături electronice și 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 și DSA).

7.1.7 Verificarea calității parametrilor

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

7.1.8 Generarea Hardware/software a cheii

Cheile MD-CA sunt generate în module HSM certificate.

7.1.9 Utilizarea perechii de chei a MD-CA

Cheia privată RSA a MD-CA este utilizată doar pentru semnarea certificatelor cheilor publice pentru tahografe și pentru crearea cererii de certificat a MD-CA către ERCA.

7.2 Protecția Cheii Private

7.2.1 Standarde și controale pentru modulele criptografice

MD-CA utilizează pentru generarea și stocarea cheilor sale private RSA și a cheilor $K_{m_{wc}}$ doar module HSM certificate.

Operarea modulului HSM este verificată periodic prin teste interne, iar upgrade-ul de firmware pentru HSM este realizat anual de administratorul HSM, dacă este cazul.

7.2.2 Controlul k din n al cheii private

MD-CA dispune de perechi de chei și certificate asociate pentru fiecare din sistemele sale, producție, backup, și recuperare în caz de dezastru. Generarea acestor chei este realizată de cel puțin trei persoane autorizate. Operațiile de certificare a cheii publice și de distribuire a cheii master a senzorului de mișcare necesită participarea a doi operatori HSM și a unui operator CA.

7.2.3 Escrow-ul cheii private

Escrow-ul cheii este interzis de politica de certificare a MD-A.

7.2.4 Backup-ul cheii private

MD-CA nu creează o copie de siguranță a cheilor sale private. MD-CA dispune de perechi de chei si certificate asociate pentru fiecare din sistemele sale, productie, backup, si recuperare in caz de dezastru.

7.2.5 Arhivarea cheii private

Ca la 7.2.4

7.2.6 Transferul cheii private din sau intr-un modul HSM

7.2.7 Păstrarea cheii private într-un modul HSM

Cheile private ale MD-CA sunt păstrate in modulul HSM in care au fost generate. Cheile pot fi importate in modulul HSM găzduit de sistemul din centrul de recuperare in caz de dezastru doar in mod securizat, respectând procedura de restaurare a sistemului si in prezenta unui administrator de sistem, a doi administratori de HSM si a unui auditor, daca este cazul.

7.2.8 Metoda de activare a cheii private

Activarea cheii se face după principiul K din N, cu $K \geq 2$. La operație participa doi operatori HSM.

7.2.9 Metoda dezactivării 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 MD-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 unei chei private se face conform procedurii de inactivare a unei CA si a ștergerii securizate a cheilor acesteia. Acțiunile întreprinse în acest proces sunt înregistrate, datate și semnate de fiecare persoană prezentă în timpul inactivării si ștergerii securizate. Înregistrările sunt păstrate din motive de audit sau pentru verificările obișnuite ale sistemului.

7.2.10 Metoda distrugerii cheii private

Ștergerea cheii private se face respectând procedura de ștergere securizata a cheilor de pe modulul HSM, conform metodelor recomandate de producătorul dispozitivului.

Fiecare distrugere de cheie privată este înregistrată în jurnalul de evenimente.

7.2.11 Certificarea modulului HSM

MD-CA folosește module criptografice certificate FIPS 140-2 Level 3.

7.3 Alte Aspecte ale Managementului Perechii de Chei

7.3.1 Arhivarea Cheii Publice

7.3.2 Perioadele de validitate pentru cheile publice si private ale MD-CA

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

Perioada de validitate a cheii publice MD-CA este de 7 ani, iar a cheilor master ale senzorului de miscare este nelimitata.

7.4 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 (și dezactivare) a unei chei private depinde de intervalul de timp în care cheia trebuie să rămână activă (pe timpul unei singure operațiuni, sesiuni sau pentru o perioadă mai lungă). Cheia privata a MD-CA rămâne în stare activă până la ștergerea ei fizică de pe modul sau până la scoaterea ei din serviciile MD-CA. Activarea cheii private este întotdeauna precedată de autentificarea operatorilor. Autentificarea este realizată pe baza cardurilor criptografice deținute de operatori. După introducerea cardurilor în modulul criptografic și folosirea codurilor PIN, cheia privată rămâne în stare activă până la dezactivarea acesteia.

7.5 Controale de Securitate a Calculatoarelor

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

7.5.1 Cerințele tehnice specifice securității calculatoarelor

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

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

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

7.5.2 Evaluarea securității calculatoarelor

Sistemele de calcul ale MD-CP respectă cerințele descrise în procedura internă de hardening, dezvoltată pe baza standardelor National Institute of Standards and Technology (NIST) și Center for Internet Security (CIS).

7.5.3 Controale tehnice specifice ciclului de viață

Controale specifice dezvoltării sistemului

Fiecare aplicație, înainte de a fi folosită în producție de către MD-CA, este instalată astfel încât să se permită controlul versiunii curente și 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 așa fel încât să poată fi urmărită și 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 și de încredere.

Controale pentru managementul securității

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

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

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

7.5.4 Controale de securitatea a rețelei

Serverele și stațiile de lucru de încredere aparținând MD-CA sunt conectate prin intermediul unei rețele locale (LAN), divizate în mai multe subrețele, cu acces controlat. Accesul dinspre alte rețele este protejat prin intermediul unui firewall inteligent.

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

Mijloacele de asigurare a securității rețelei acceptă doar mesaje transmise prin protocoale securizate. Evenimentele (log-urile) sunt înregistrate în jurnalele de sistem și permit supravegherea folosirii corecte a serviciilor furnizate de MD-CA.

7.5.5 Controale specifice modulelor criptografice

Controalele modulelor criptografice includ cerințele impuse pentru dezvoltarea, producția și livrarea modulelor. MD-CA nu definește cerințe specifice în acest domeniu. Totuși, MD-CA acceptă și utilizează numai module criptografice care corespund cerințelor din Capitolul 6 din Politica de Certificare a MD-A.

7.5.6 Înregistrarea evenimentelor și procedurile de auditare

Pentru a gestiona eficient sistemele MD-CA și pentru a putea audita acțiunile utilizatorilor și personalului MD-CA, toate evenimentele care apar în sistem sunt înregistrate. Informațiile înregistrate alcătuiesc jurnalele (log-urile) de evenimente și trebuie păstrate în așa fel încât să permită, dacă este cazul, să se acceseze informațiile corespunzătoare și necesare rezolvării disputelor, sau să detecteze tentativele de compromitere a securității MD-CA. Evenimentele înregistrate fac obiectul procedurilor de arhivare. Arhivele sunt păstrate în afara incintei MD-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 înregistrare în log, electronic sau de mână, este păstrată și dezvăluită atunci când se desfășoară un audit.

Tipuri de evenimente înregistrate

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

Log-urile de evenimente MD-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 și răspunsurile serverului (sau invers) la nivelul protocolului de rețea (de exemplu https); datele concrete care se înregistrează sunt: adresa IP a stației sau a server-ului, operațiunile executate (de exemplu: căutare, editare, scriere etc.) și rezultatele lor (de exemplu introducerea cu succes a unei înregistrări în baza de date),
- **erori** – conține informații despre erori la nivelul protocolelor de rețea și la nivelul modulelor aplicațiilor;
- **audit** – conțin informații specifice serviciilor de certificare, de exemplu: cererea de certificat, emiterea de certificat etc.

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

Fiecare înregistrare, automată sau manuală, conține următoarele informații:

- tipul evenimentului,

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

Conținutul înregistrărilor se refera la:

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

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

Frecvența analizei jurnalelor de evenimente

Înregistrările din jurnalul de evenimente pot fi revizuite fie manual, la intervale periodice, fie prin intermediul unui sistem automatizat de monitorizare și analiză.

În cadrul organizației, jurnalele de evenimente sunt colectate și analizate în timp real de către un sistem SIEM, care corelează automat evenimentele, detectează anomaliile și generează alerte specifice.

Prin urmare, analiza manuală lunară detaliată a jurnalelor de evenimente nu este necesară, fiind înlocuită de mecanismele automate de detecție și raportare furnizate de sistemul SIEM

Perioada de retenție a jurnalelor de evenimente

Înregistrările evenimentelor sunt stocate în fișiere pe discul sistem până când acestea ating capacitatea maximă permisă. După depășirea spațiului alocat, jurnalele sunt păstrate în arhive.

Pe lângă arhivarea tradițională, toate jurnalele sunt colectate și stocate în sistemul SIEM, asigurând astfel monitorizarea și analiza în timp real.

Jurnalele arhivate, inclusiv cele stocate în SIEM, sunt păstrate cel puțin 10 ani.

Protecția jurnalelor de evenimente

Fiecare înregistrare din jurnale face obiectul arhivării pe un server de log centralizat. După depășirea numărului acceptat de înregistrări pentru un jurnal, conținutul acestuia este arhivat. Arhivele pot fi semnate criptate. O cheie folosită pentru criptarea arhivelor este plasată sub controlul administratorului de securitate.

Pe lângă arhivarea tradițională, jurnalele sunt colectate și stocate în sistemul SIEM, asigurând monitorizarea și analiza continuă a evenimentelor.

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 așa fel încât:

- numai entitățile de mai sus au dreptul să citească înregistrările jurnalului,
- numai administratorul de securitate poate arhiva sau șterge fișiere (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 așa fel încât, chiar și după arhivarea jurnalului, este imposibil să ștergi înregistrări, sau să ștergi jurnalul înaintea expirării perioadei de retenție a jurnalului.

Procedurile de backup pentru jurnalele de evenimente

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

Notificarea entităților responsabile de tratarea evenimentelor

Modulul de analiză a jurnalului de evenimente implementat în sistem examinează evenimentele curente și 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 și 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: telefon mobil, poștă 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 MD-CA. Pentru a realiza acest lucru, sunt copiate următoarele aplicații și fișiere:

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

Metoda de creare a copiilor de backup are o influență deosebită asupra timpului și costului restaurării Autorității de Certificare după defectarea, sau distrugerea sistemului. MD-CA folosește atât backup-uri full (zilnice) toate copiile sunt clonate și clonele sunt păstrate în altă locație secundară, în aceleași condiții de securitate ca și cele din locația primară.

Procedura de restaurare va fi verificată cel puțin o dată la 12 luni, pentru a se verifica utilitatea backup-ului, în caz de dezastru. Va trebui să se verifice dacă datele salvate sunt suficiente pentru restaurarea sistemului în cel mai scurt timp posibil. Concluziile testelor vor fi înregistrate.

7.5.7 Arhivarea înregistrărilor

Este necesar ca toate datele și fișierele 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 MD-CA.

Tipurile de date arhivate

Următoarele date sunt incluse în procesul de arhivare:

- informațiile rezultate în urma examinării și evaluării (ca urmare a unui audit) măsurilor de protecție logică și fizică ale Autorității de Certificare,
- cererile de certificate primite și certificatele emise,
- baza de date cu certificate, (sau evenimente legate de emiterea de certificate),
- evenimente legate de distribuirea cheii K_{mc} ,
- istoria cheii Autorității de Certificare, de la generare până la distrugere.

7.6 Compromiterea cheilor si Recuperarea in Caz de Dezastru

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

Procedurile sunt descrise in planul si procedurile de raspuns la incidente ale organizatiei MD-CA.

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

7.6.2 Defecțiuni ale echipamentelor, software-ului sau pierderea integrității datelor

In funcție de natura dezastrului, pașii de recuperare sunt următorii:

1. Se înlocuiește imediat CA-ul cu sistemele de rezerva,
2. Se restaurează aplicațiile software folosind mediile de instalare,
3. Se restaurează datele folosind copiile de siguranță,
4. Se restaurează cheile RSA folosind HSM-ul de rezerva si cardurile de HSM de rezerva.

7.6.3 Procedurile in cazul compromiterii cheii private

In cazul in care cheia privata a MD-CA sau cheia senzorului de miscare au fost compromise, sau se suspectează ca au fost compromise, se notifica imediat MD-A si ERCA.

7.6.4 Continuarea afacerii in caz de dezastru

Folosind copiile de siguranță se restaurează datele si aplicațiile si se recreează un mediu de lucru securizat intr-o locație alternativa.

7.7 Scoaterea din uz a MD-CA

Încheierea serviciului MD-CA service se realizează astfel:

1. Toate datele sunt distruse în mod securizat prin ștergerea securizată a discurilor folosind programe specializate și prin ștergerea securizată a datelor modulului HSM.
2. Toate copiile cheilor MD-CA sunt distruse.
3. Arhiva MD-CA și înregistrările auditurilor sunt predate către MD-A.

Procedura de scoatere din uz se desfășoară sub controlul dual al MD-CA și al MD-A.

8 AUDITURILE PENTRU STABILIREA CONFORMITATII SI ALTE EVALUARI

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

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

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

Frecvența auditării

Auditul extern pentru verificarea conformității cu reglementările legale și procedurale (Codul de Practici și Proceduri) se desfășoară la interval de doi ani. În cazul în care, în urma auditului, sunt identificate neconformități semnificative, se poate decide organizarea unui audit suplimentar la un interval de un an. Auditul intern este efectuat ori de câte ori administratorul de securitate consideră necesar, în funcție de rezultate și riscurile identificate.

9.1 Identitatea / calificările auditorului

Auditul extern trebuie realizat de personal având cunoștințe și experiență tehnică corespunzătoare (să dispună de documente care să certifice acest lucru) în domeniul infrastructurilor de chei publice, tehnologiilor și dispozitivelor de securitate informatică și de auditare a securității sistemelor. De asemenea auditorul trebuie să posede cunoștințe solide ale reglementărilor UE, CE și MD-A referitoare la sistemul tahografelor digitale.

Auditul intern este realizat de către departamentul de calitate și audit al MD-CA.

9.2 Relația auditorilor cu entitatea auditată

Vezi paragraful anterior. Auditorul nu trebuie să depindă în nici un fel de entitatea auditată și nici să nu fi fost în vreun fel implicat în activitățile de planificare și operare ale sistemelor ITC ale entității auditate.

9.3 Domeniile supuse auditării

Auditurile interne și externe se desfășoară conform regulilor și procedurilor acceptate pe plan internațional și vizează:

- securitatea fizică a MD-CA,
- procedurile de verificare a identității aplicanților,
- serviciile de certificare și procedurile de furnizare a serviciilor,
- securitatea aplicațiilor software și a accesului la rețea,
- securitatea personalului MD-CA,
- jurnalele de evenimente și procedurile de monitorizare a sistemului,

- arhivarea și restaurarea datelor,
- procedurile de arhivare,
- înregistrările referitoare la modificarea parametrilor de configurare pentru MD-CA,
- înregistrările referitoare la analizele și verificările efectuate pentru aplicațiile software și dispozitivele hardware.

9.4 Analiza vulnerabilităților

Autoritatea de Certificare face anual o analiză a vulnerabilităților pentru fiecare procedură internă, aplicație și sistem informatic. Cerințele de analiză pot, de asemenea, să fie stabilite de către o instituție externă, autorizată să auditeze MD-CA. 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 și conformitatea cu Codul de Practici și Proceduri. Instituția externă care efectuează auditul de securitate, trebuie să desfășoare această activitate respectând recomandările ISO/IEC 27001:2022.

9.5 Măsurile întreprinse ca urmare a descoperirii unei deficiențe

În cazul descoperirii unor deficiențe se pot lua trei tipuri de măsuri:

1. continuarea operațiilor,
2. continuarea limitată a operațiilor,
3. suspendarea operațiilor.

Auditorul, împreună cu MD-A, decide ce acțiuni trebuie întreprinse. Decizia se bazează pe gravitatea deficiențelor și a posibilului impact.

În cazul în care se decide acțiunea de tipul 1, managementul MD-CA este răspunzător pentru implementarea măsurilor corective specificate în raportul de audit, în limitele de timp din același raport.

În cazul în care se decide acțiunea de tipul 2, MD-CA continuă operațiile în modul restrâns indicat în raportul de audit.

Nivelul de servicii poate include sau exclude oricare dintre următoarele activități:

- aprobarea și întreținerea politicii MD-CA;
- operații de întreținere a MD-CA;
- certificarea cheilor publice pentru cardurile de tahograf;
- operațiuni de distribuție a cheilor pentru senzorul de mișcare.

În cazul în care se decide acțiunea de tipul 3, toate cardurile afectate trebuie trecute pe un blacklist. Managementul MD-CA trebuie să raporteze săptămânal stadiul măsurilor de remediere către auditor. MD-A și auditorul determină când trebuie făcută o nouă evaluare de securitate. Dacă deficiențele sunt considerate ca remediate după reevaluare, atunci MD-CA își poate relua operațiile.

9.6 Comunicarea rezultatelor

Rezultatele auditului sunt comunicate catre MD-A. In cazul acțiunilor de tipul 1 sau 2, MD-A se asigura de faptul ca toate entitățile care trebuie notificate primesc informațiile in conformitate cu prezentul document.



FINALUL DOCUMENTULUI