

# **Sistemul de Tahografe Digitale pentru ROMANIA**

**Codul de Practici si Proceduri pentru operarea RO-CP**

# CUPRINS

<b>CUPRINS</b> .....	2
<b>1 INTRODUCERE</b> .....	4
1.1 Descriere generala .....	4
1.2 Numele si Identificarea Documentului .....	7
1.3 Participanti .....	7
1.3.1 Autoritati de Certificare .....	7
1.3.2 Autoritati de Inregistrare.....	7
1.3.3 Abonati.....	7
1.3.5 Destinatarii Cheilor pentru Senzorii de Miscare .....	7
1.4 Utilizarea certificatului.....	7
1.5 Utilizarea Mesajului pentru Distribuirea Cheii (KDM).....	7
1.6 Administrarea CPP .....	8
1.7 Definitii si Acronime .....	8
<b>2 CONTROALE TEHNICE DE SECURITATE</b> .....	10
2.1 Generarea si Instalarea Perechii de Chei pt Carduri.....	10
2.1.1 Generarea perechii de chei .....	10
2.1.2 Distribuirea cheii private catre entitati .....	10
2.1.3 Trimiterea cheii publice catre emitatorul certificatului (RO-CA) .....	10
2.1.4 Distribuirea cheilor publice ale cardurilor catre entitatile partenere.....	10
2.1.5 Marimile cheilor .....	11
2.1.6 Parametrii de generare ai cheilor publice.....	11
2.1.7 Verificarea calitatii parametrilor .....	11
2.1.8 Generarea Hardware/software a cheii .....	11
2.1.9 Utilizarea perechii de chei .....	11
2.2 Protectia Cheii Private .....	11
2.2.1 Standarde si controale pentru modulele criptografice .....	11
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 intr-un modul HSM .....	12
2.2.6 Pastrarea cheii private intr-un modul HSM.....	12
2.2.7 Metoda de activare a cheii private.....	12
2.2.10 Certificarea modulului HSM .....	12
2.3 Alte Aspecte ale Managementului Perechii de Chei.....	12
2.3.1 Arhivarea Cheii Publice .....	12
2.3.2 Perioadele de validitate pentru cheile publice si private ale RO-CA .....	12
2.4 Datele de Activare .....	12
2.5 Controale de Securitate a Calculatoarelor .....	12
2.5.1 Cerințele tehnice specifice securității calculatoarelor .....	13
2.5.2 Evaluarea securității calculatoarelor .....	14
2.5.3 Controale tehnice specifice ciclului de viata .....	14
2.5.4 Controale de securitatea a rețelei .....	14
2.5.5 Controale specifice modulelor criptografice .....	15
2.5.6 Înregistrarea evenimentelor și procedurile de auditare.....	15
2.5.7 Arhivarea înregistrărilor.....	19
<b>3 Controale de securitate fizică, organizațională și de personal</b> .....	21
3.1 Controale de securitate fizică .....	21
3.1.1 Controale de securitate fizică în cadrul RO-CP .....	21
3.2 Controlul securității organizației.....	23
3.2.1 Roluri de încredere.....	24
3.2.2 Numărul de persoane necesare pentru îndeplinirea unei sarcini .....	25
3.2.3 Identificarea și autentificarea pentru fiecare rol .....	25
3.3 Controlul personalului.....	26
3.3.1 Experiența personală, calificările și clauzele de confidențialitate necesare .....	26
3.3.2 Cerințele de pregătire a personalului .....	27

3.3.3 Frecvența stagiilor de pregătire.....	27
3.3.4 Rotația funcțiilor .....	27
3.3.5 Sancționarea acțiunilor neautorizate.....	27
3.3.6 Personalul angajat pe baza de contract.....	28
3.3.7 Documentația oferită personalului .....	28
4 AUDITURILE PENTRU STABILIREA CONFORMITATII SI ALTE EVALUARI .....	29
4.1 Identitatea / calificările auditorului .....	29
4.2 Relația auditorilor cu entitatea auditată .....	30
4.3 Domeniile supuse auditării.....	30
4.4 Analiza vulnerabilităților .....	30
4.5 Măsurile întreprinse ca urmare a descoperirii unei deficiențe .....	31
9.6 Comunicarea rezultatelor .....	31

# 1 INTRODUCERE

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

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

- Certificate pentru chei publice pentru componente de tahograf (carduri, unitati de vehicul si senzor de miscare);
- Chei de criptare pentru datele senzorilor de miscare motion sensor data encryption keys.

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

Documentul a fost creat pentru a asigura conformitatea cu cerintele enuntate in Politica de Certificare a RO-CA si se bazeaza pe cadrul creat prin IETF RFC 3647.

## 1.1 Descriere generala

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

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

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

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

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

RO-CP primeste cererile de cartele tahografice de la RO-CIA in format electronic securizat, genereaza perechile de chei RSA pentru cartele, genereaza cererile de certificat corespunzatoare, le transmite RO-CA, primeste certificatele de la RO-CA, personalizeaza

cartelele, ambaleaza cartelele si PIN-ul (pentru cartelele de atelier) si le trimite la RO-CIA pentru distributie.

RO-CA isi schimba cheile la intervale regulate.

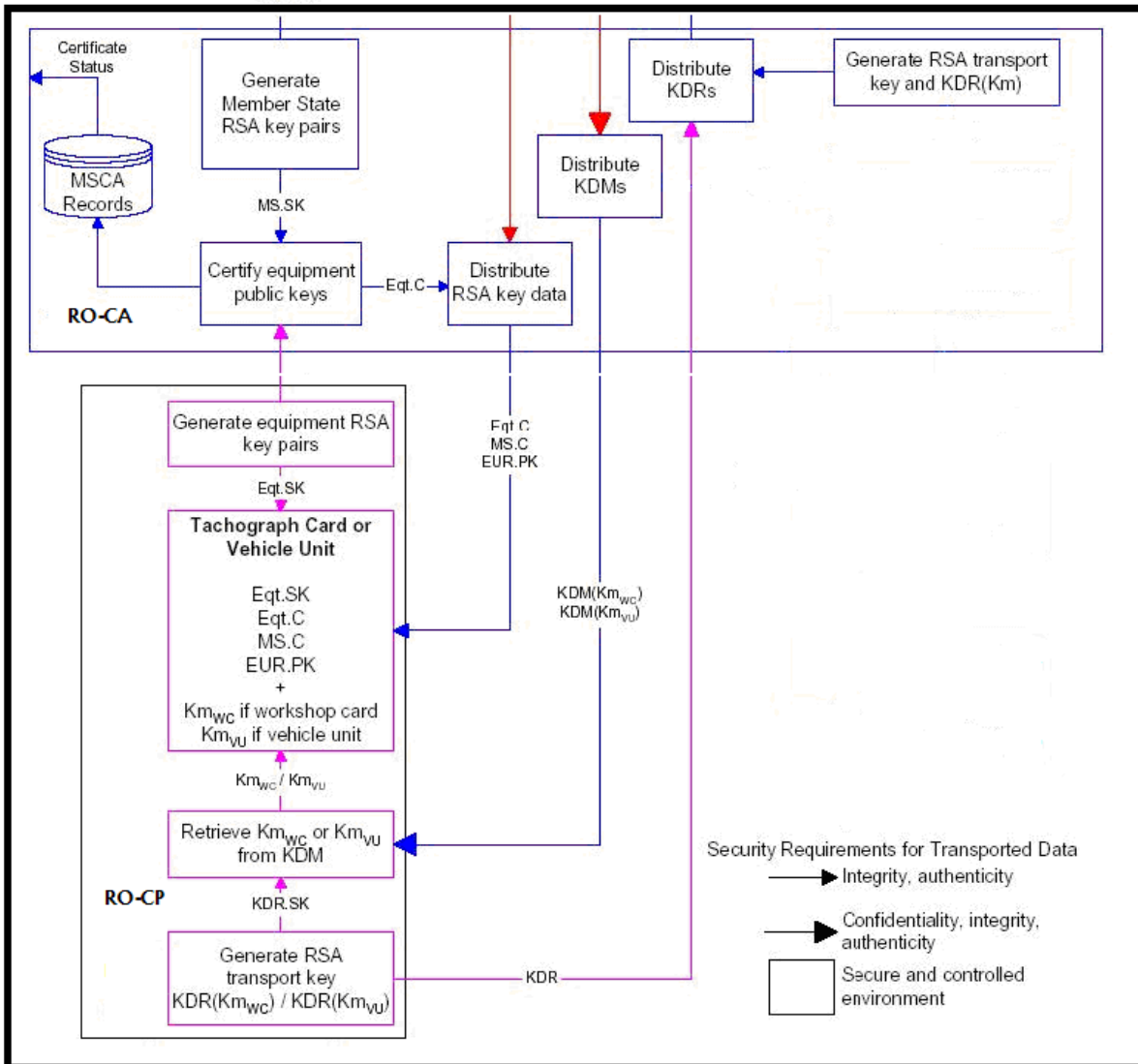
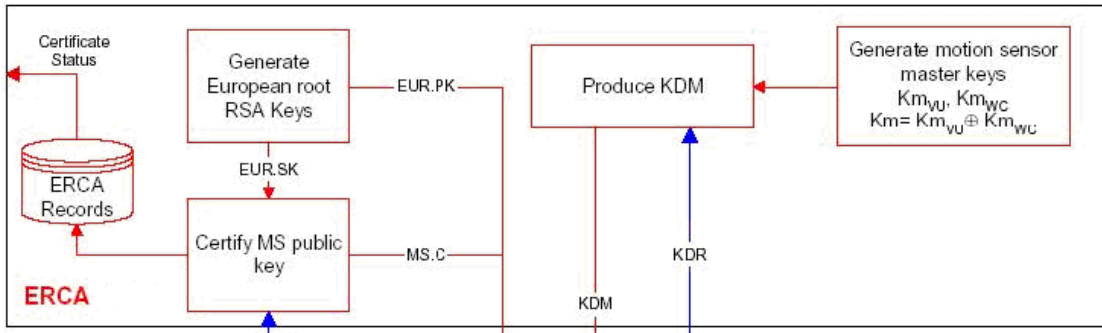
Formatul certificatelor digitale folosite este proprietar si incompatibil cu formatul X.509, al certificatelor digitale a caror utilizare este presupusa , dar nu ceruta obligatoriu de catre IETF RFC 3647.

RO-CA 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  $K_m$  este separata in doua parti ,  $K_{m_{VU}}$  si  $K_{m_{WC}}$ .  $K_{m_{WC}}$  sunt inserate in cardurile de atelier de catre personalizatorii de carduri.

Pentru a asigura confidentialitatea cheii  $K_{m_{WC}}$  in timpul transportului de la ERCA la RO-CA, ERCA o cripteaza folosind o cheie publica de criptare RSA, pentru a produce un mesaj de distributie a cheii (KDM). Acelasi lucru este valabil si pentru transportul aceleiasi cheii  $K_{m_{WC}}$  de la RO-CA la RO-CP. Cheile RSA folosite la crearea mesajelor KDM sunt create de RO-CA sau RO-CP si trimise catre ERCA sau respectiv RO-CA printr-o cerere de distributie (KDR).

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



## **1.2 Numele si Identificarea Documentului**

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

## **1.3 Participanti**

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

### **1.3.1 Autoritati de Certificare**

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

### **1.3.2 Autoritati de Inregistrare**

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

### **1.3.3 Abonati**

Abonatii serviciilor de certificare oferite de RO-CA sunt cardurile de tahograf.

### **1.3.5 Destinatarii Cheilor pentru Senzorii de Miscare**

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

## **1.4 Utilizarea certificatului**

Certificatele de cheie publica pentru tahografe trebuie inserate in componentele tahografelor digitale, asa cum se cere in procesul de autentificare mutuala descris in cerinta CSM\_020 Reglementarea 1360/2002, Annex I(B) Appendix 11 Common Security Mechanism.

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

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

## **1.5 Utilizarea Mesajului pentru Distribuirea Cheii (KDM)**

Mesajele KDM trebuie folosite doar in scopul transmiterii securizate a cheii  $K_{m_{wc}}$  intre ERCA si RO-CA si intre RO-CA si RO-CP

## 1.6 Administrarea CPP

1. Acest CPP este creat, mentinut si revizuit de catre UTI Systems, care indeplineste functia de RO-CP:  
Organizatia Romana pt Personalizarea Cardurilor de Tahograf  
Firma UTI Systems  
Sos Oltenitei, Nr 107A
2. Orice intrebare referitoare la prezentul CPP trebuie trimise catre: UTI Systems
3. Orice intrebare referitoare la operarea RO-CP trebuie trimise catre responsabilul Ro-CP. Acesta este desemnat de catre Directorul General al ARR.
4. Autoritatea Nationala, RO-MSA, trebuie sa stabileasca daca acest CPP este conform cu Politica de Certificare a RO-CA.
5. Stabilirea conformitatii se bazeaza pe o evaluare de securitate realizata fie chiar de catre RO-MSA, fie de un tert autorizat.

## 1.7 Definitii si Acronime

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

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

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

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

CAR	Certification Authority Reference
CHA	Certificate Holder Authorisation
CHR	Certificate Holder Reference
CP	Component Personaliser
CPI	Certificate Profile Identifier
CPS	Certification Practices Statement
CRL	Certificate Revocation List
CSP	Certification Service Provider
DES	Data Encryption Standard (symmetric encryption scheme)
EA	European Authority
ENI	ESSOR Nuclear Island
EOV	End Of Validity
ERCA	European Root Certification Authority

ETSI	European Telecommunications Standards Institute
KCR	Key Certification Request
KDR	Key Distribution Request
KDM	Key Distribution Message
Km	Motion sensor master key
Km <sub>wc</sub>	Motion sensor master key inserted in workshop card
NCA	National Certification Authority
RO-MSA	Romanian Authority
RO-CA	Romanian Certification Authority
RO-CIA	Romanian Card Issuance Authority
OA	Operating Agent
OE	Operational Entity (used to refer to both a NCA and a CP)
OM	Operations Manager
PK	RSA public key
PKI	Public Key Infrastructure
PR	Permanent Representation of Member State
RSA	Rivest, Shamir, Adleman (asymmetric encryption scheme)
SAS	Single access system
SK	RSA secret key
TDES	Triple DES

## **2 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 pt 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 realizata in serverul criptografic cu participarea activa a cel puțin 3 persoane. Modulul HSM al serverului criptografic este conform cu cerintele FIPS 140-2 Nivel 3. Cheia privata este menținuta în permanență criptata pe dispozitivul HSM.

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

#### **2.1.2 Distribuirea cheii private catre entitati**

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

#### **2.1.3 Trimiterea cheii publice catre emitatorul certificatului (RO-CA)**

Conform politicii RO-CA.

#### **2.1.4 Distribuirea cheilor publice ale cardurilor catre entitatile partenere**

Cheia publica a cardului este distribuita de RO-CP pe card sub forma de certificat emis de RO-CA, semnat cu cheia privata a RO-CA. Cheia publica a RO-CA este distribuita catre RO-CP sub forma de certificat emis de ERCA. Cheia publica ERCA este distribuita catre RO-CP ca atare. Distribuirea certificatului RO-CA si a cheii publice a

ERCA catre RO-CP se face impreuna cu certificatul cardului ca urmare a unei cereri KCR primite de RO-CA de la RO-CP.

### **2.1.5 Marimile cheilor**

Cheile RSA trebuie sa aiba un modul de 1024 biti si un exponent public de 64 biti.

### **2.1.6 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 crearea de semnături electronice și verificarea 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 calitatii parametrilor**

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

### **2.1.8 Generarea Hardware/software a cheii**

Cheile pentru carduri sunt generate in module HSM certificate.

### **2.1.9 Utilizarea perechii de chei**

Cheia privata RSA a cardului este utilizata doar pentru semnarea certificatelor cheilor cererii de certificat catre RO-CA.

## **2.2 Protectia Cheii Private**

### **2.2.1 Standarde si controale pentru modulele criptografice**

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

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

### **2.2.2 Controlul k din n al cheii private**

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

### **2.2.3 Backup-ul cheii private**

Nu se aplica.

### **2.2.4 Arhivarea cheii private**

Nu se aplica.

### **2.2.5 Transferul cheii private din sau intr-un modul HSM**

Cheia privata RSA este generata in HSM si apoi transferat pe card in mod securizat.

### **2.2.6 Pastrarea cheii private intr-un modul HSM**

Cheile private ale cardurilor nu sunt pastrate in modulul HSM unde au fost generate.

### **2.2.7 Metoda de activare a cheii private**

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

### **2.2.10 Certificarea modulului HSM**

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

## ***2.3 Alte Aspecte ale Managementului Perechii de Chei***

### **2.3.1 Arhivarea Cheii Publice**

Cheia publica a RO-CA este pastrata in baza de date a RO-CA in certificatul emis de acesta.

### **2.3.2 Perioadele de validitate pentru cheile publice si private ale RO-CA**

Perioada de validitate a cheii private a cardului este de maximum 5 ani.

Perioada de validitate a cheii publice a cardului este de maximum 5 ani.

## ***2.4 Datele de Activare***

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

## ***2.5 Controale de Securitate a Calculatoarelor***

Sarcinile operatorilor si administratorilor care lucrează în cadrul RO-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 RO-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 RO-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 RO-CP
- 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.

## **2.5.2 Evaluarea securității calculatoarelor**

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

## **2.5.3 Controale tehnice specifice ciclului de viața**

### **Controale specifice dezvoltării sistemului**

Fiecare aplicație, înainte de a fi folosită în producție de către RO-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 RO-CP, garantând astfel că acestea operează corect și în concordanță cu configurarea acceptată și implementată.

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

Controalele aplicate sistemelor RO-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 RO-CP sunt conectate prin intermediul unei rețele locale (LAN), divizate în mai multe subrețele, cu acces controlat.

Accesul dinspre Internet către orice segment, este protejat prin intermediul unui firewall inteligent.

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

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

### **2.5.5 Controale specifice modulelor criptografice**

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

### **2.5.6 Înregistrarea evenimentelor și procedurile de auditare**

Pentru a gestiona eficient sistemele RO-CP și pentru a putea audita acțiunile utilizatorilor și personalului RO-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 RO-CP. Evenimentele înregistrate fac obiectul procedurilor de arhivare. Arhivele sunt păstrate în afara incintei RO-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 RO-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 RO-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 server-ului (sau invers) la nivelul protocolului de rețea (de exemplu http, https); datele concrete care se înregistrează sunt: adresa IP a stației sau a server-ului, operațiunile executate (de exemplu: căutare, editare, scriere etc.) 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 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 RO-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 trebuie revăzute în detaliu cel puțin o dată pe lună. Orice eveniment având o importanță semnificativă trebuie explicat și descris într-un jurnal. Procesul de verificare a jurnalului include verificarea unor eventuale falsificări, sau modificări și verificarea fiecărei alerte sau anomalii consemnată în log-uri. Orice acțiune executată ca rezultat al funcționării defectuoase detectate trebuie înregistrată în jurnal.

### **Perioada de retenție a jurnalelor de evenimente**

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

Jurnalele arhivate sunt păstrate cel puțin 10 ani.

### **Protecția jurnalelor de evenimente**

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

Un jurnal de evenimente poate fi revăzut numai de administratorului de securitate, 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 RO-CP solicita ca jurnalul de evenimente să facă obiectul backup-ului lunar. Aceste backup-uri sunt stocate în locații auxiliare ale RO-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, pager, 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 RO-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 RO-CP,
- istoricul cheilor,

- datele privind personalul RO-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. RO-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 3 luni, pentru a se verifica utilitatea backup-ului, în caz de crash. Va trebui să se verifice dacă datele salvate pe bandă sunt suficiente pentru restaurarea sistemului în cel mai scurt timp posibil. 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 copiile de siguranță care sunt ținute în afara locației RO-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 logică și fizică ale RO-CP,
- baza de date cu date despre carduri,

#### **Frecvența arhivării datelor**

Datele se arhivează cel puțin o dată pe săptămână.

#### **Perioada de păstrare a arhivelor**

Arhivele de păstrează cel puțin 10 ani.

#### **Cerințele pentru marcarea temporală a înregistrărilor**

Se recomandă ca datele arhivate să fie semnate cu o marcă temporală, creată de Autoritatea de Marcare Temporală (TSA) autorizată, având certificatul emis de Autoritatea de Certificare operațională afiliată la RO-CA. Serviciul de marcă temporală este disponibil în cadrul RO-CA .

### **Procedurile de acces și verificarea informațiilor arhivate**

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

## **3 Controale de securitate fizică, organizațională și de personal**

Acest capitol descrie cerințele generale privind securitatea fizică și organizațională, precum și activitatea personalului RO-CP în activitatea de management al cheilor, personalizarea 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 RO-CP**

Sistemele de calcul, terminalele operatorilor și resursele informaționale ale RO-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**

RO-CP este localizată în București, la următoarea adresă: Central Bussiness Park, Strada Serban Voda, Nr. 133, Cladirea C1.

#### **Accesul fizic**

Accesul fizic în cadrul RO-CP este controlat și monitorizat de un sistem de alarmă integrat. RO-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 RO-CP este accesibil în fiecare zi lucrătoare între 10:00 și 16:00. numai persoanelor autorizate de către conducerea RO-CP. Vizitatorii locațiilor aparținând RO-CP trebuie să fie însoțiți permanent de persoane autorizate.

Zonele ocupate de RO-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 senzitive 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 RO-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 senzitive. 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 RO-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, iar locația RO-CP este la ultimul etaj. În plus, personalul de pază este localizat chiar lângă zona serverelor și este instruit să anunțe imediat administratorul RO-CP și administratorul clădirii.

### **Prevenirea incendiilor**

Locația RO-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 RO-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 sunt stocate în containere speciale, situate în afara locației RO-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 RO-CP. Acest lucru permite refacerea de urgență a oricărei funcții a RO-CP în 48 de ore, în locația principală a RO-CP, sau în locația auxiliară.

### **3.2 Controlul securității organizației**

Acest capitol prezintă rolurile ce pot fi atribuite personalului aparținând RO-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 RO-CP

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

- **Responsabilul RO-CP**
  - Raspunzator pentru operarea sigura si continua a functiei RO-CP
  - Este reprezentantul organizatiei si este autorizat sa ia decizii in cadrul organizatiei RO-CP
  - Nu este direct implicat in implementarea proceselor de afaceri, dar este responsabil pentru respectarea si evaluarea masurilor de securitate, ca si pentru managementul RO-CP
  - Accepta responsabilitatea pentru managementul schimbarii.
- **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 RO-CP; inițiază și suspendă serviciile oferite de RO-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 RO-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 RO-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 RO-CP; ia parte în procesul de personalizare logică și optică a cardurilor
- **HSM Administrator**
  - Execută în siguranță Procesul de Management al Cheilor,
  - Generează, administrează și distruge cheile asimetrice pentru carduri
- **Auditorul de sistem** – autorizat să acceseze arhivele și log-urile de audit ale sistemelor de încredere ale RO-CP. Responsabil de efectuarea de audituri interne pentru respectarea Codului de Practici și Proceduri de către personalul RO-CP;

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

### **3.2.2 Numărul de persoane necesare pentru îndeplinirea unei sarcini**

Procesul de generare de chei – pentru semnarea certificatelor sau pentru transportul  $K_{m_{wc}}$  – este una din operațiile ce necesită o atenție deosebită. Generarea necesită prezența a cel puțin trei persoane: un administrator de securitate, un 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.

### **3.2.3 Identificarea și autentificarea pentru fiecare rol**

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

- plasarea pe lista de persoane care au dreptul de a accesa locațiile RO-CP ,
- plasarea pe lista de persoane care au acces fizic la sisteme și resurse de rețea aparținând RO-CP,

- emiterea confirmării care autorizează îndeplinirea rolului asignat,
- asignarea unui cont și a unei parole în sistemul informatic al RO-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 RO-CP, a sistemului de operare și a controalelor de aplicații.

Operațiile efectuate în RO-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**

RO-CP trebuie să se asigure că persoana care îndeplinește responsabilitățile funcției, conform cu rolul atribuit în cadrul RO-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 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 datelor confidențiale (din punctul de vedere al securității RO-CP) ,

#### **3.3.1 Experiența personală, calificările și clauzele de confidențialitate necesare**

Personalul angajat al RO-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 RO-CP, trebuie să fie instruit cu privire la:

- reglementările Codului de Practici și Proceduri al RO-CP,
- reglementările Politicii de certificare a RO-CA,
- procedurile și controalele de securitate folosite de RO-CA,
- aplicațiile software ale RO-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 RO-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 RO-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 RO-CP . În plus, personalul angajat pe bază de contract, pe timpul cât își desfășoară activitatea în locația RO-CP, trebuie permanent însoțit de către un angajat al RO-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**

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

- Politica de certificare a RO-CA,
- Codul de Practici și Proceduri al RO-CP,
- Responsabilitățile și obligațiile asociate rolului deținut în sistem.

## **4 AUDITURILE PENTRU STABILIREA CONFORMITATII SI ALTE EVALUARI**

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

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

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

### **Frecvența auditării**

Auditul extern prin care se verifică compatibilitatea cu reglementările legale și procedurale (Codul de Practici și Proceduri) se desfășoară anual, în timp ce un audit intern este efectuat ori de câte ori administratorul de securitate considera necesar.

### ***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 aibă cunoștințe solide ale reglementărilor UE, CE și RO-MSA referitoare la sistemul tahografelor digitale.

Auditul intern este realizat de către departamentul de calitate și audit al RO-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 vre-un 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 RO-CP,
- procedurile de furnizare a serviciilor,
- securitatea aplicațiilor software și a accesului la rețea,
- securitatea personalului RO-CP,
- jurnalele de evenimente și procedurile de monitorizare a sistemului,
- arhivarea și restaurarea datelor,
- procedurile de arhivare,
- înregistrările referitoare la modificarea parametrilor de configurare pentru RO-CP,
- înregistrările referitoare la analizele și verificările efectuate pentru aplicațiile software și dispozitivele hardware.

## **4.4 Analiza vulnerabilităților**

RO-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 RO-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 13335 (Guidelines for Management of IT Security) și ISO/IEC 17799 (Code of Practice for Information Security Management).

#### **4.5 Măsurile întreprinse ca urmare a descoperirii unei deficiențe**

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

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

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

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

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

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

#### **9.6 Comunicarea rezultatelor**

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