Sistemul de Tahografe Digitale pentru ROMANIA

Codul de Practici si Proceduri pentru operarea RO-CP

CUPRINS

1 INTRODUCERE

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

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

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

• Chei de criptare pentru datele senzorilor de miscare 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 criprografice (vezi figura urmatoare) este necesar pentru a implementa mecanismele de securitate definite in:

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

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

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

RO-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.

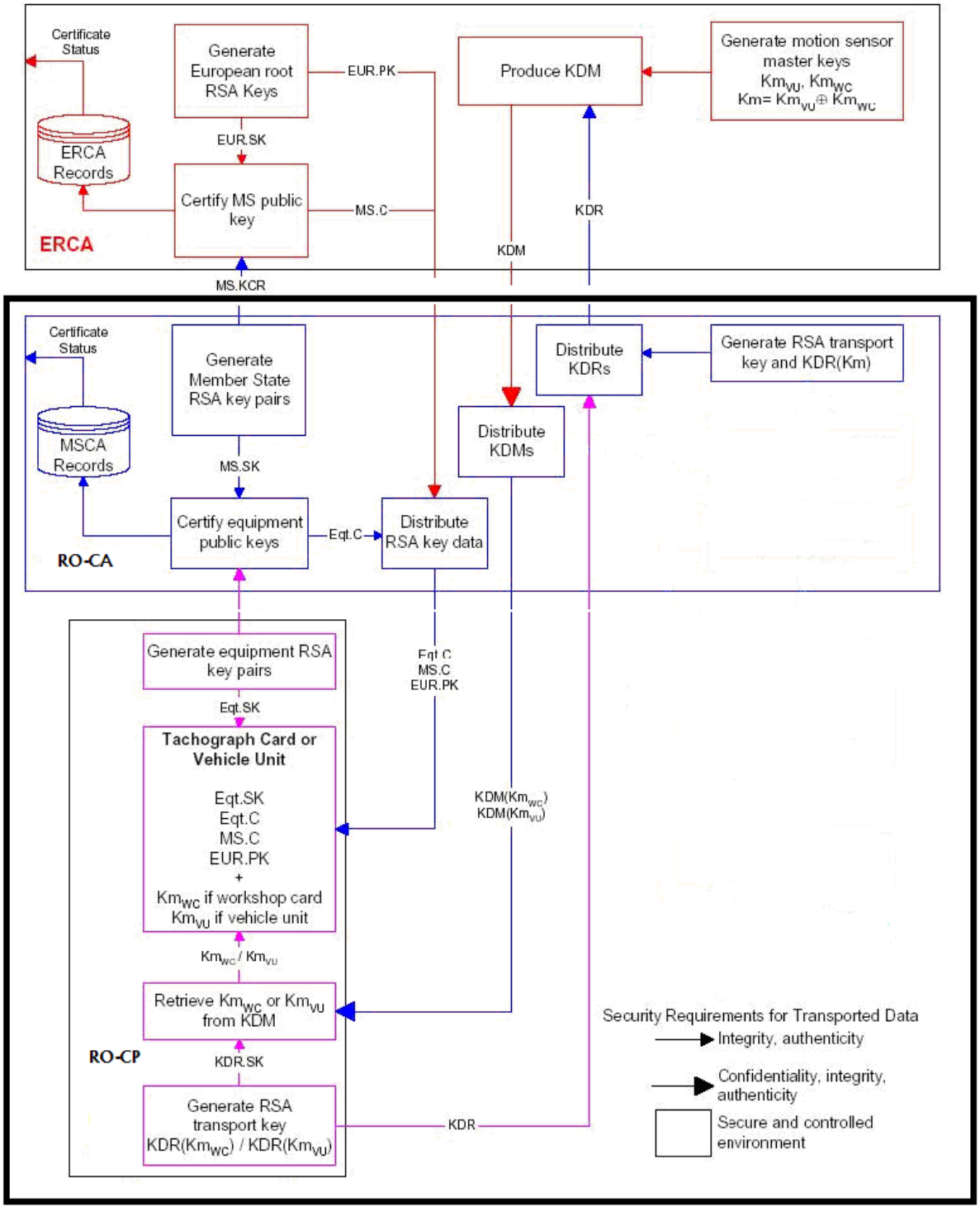
Formatul certificatelor digitale folosite este proprietar si incompatibil cu formatul X.509, al certificatelor digitale a caror utilizare este presupusa , dar nu ceruta obligatoriu de catre IETF RFC 3647.

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 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 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 trasnportul aceleiasi cheii Km_{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 Km_{wc} este definita intr-un acord semnat de ERCA si RO-MSA.


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

1.2 Numele si Identificarea Documentului

Acest document poarta denumirea de "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 Km_{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 Km_{wc} sunt organizatiile care personalizeaza cardurile de atelier. Acestea sunt identificate in acordul semnat intre ERCA si RO-CA.

1.4 Utilizarea certificatului

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

Certificatele pentru tahografele digitale pot fi folosite in aplicatii in legatura sistemul tahografelor digitale (de ex. Echipamente de calibrare utilizate in ateliere, echipamente pentru descarcarea de date folosite de 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 Km_{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 chei este folosita si la criptarea mesajului si la decriptarea lui.

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

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

2 CONTROALE TEHNICE DE SECURITATE

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

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

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 certificateleor 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 annual 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>=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 acre 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 şi 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 şi aplicațiilor, folosite în cadrul RO-CP. Măsurile de securitate care protejează sistemele de calcul sunt aplicate la nivelul sistemului de operare, al aplicațiilor precum şi din punct de vedere fizic.

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

- autentificarea obligatorie la nivelul sistemului de operare şi al aplicațiilor,
- control discreționar al accesului,
- posibilitatea de a fi auditate din punct de vedere al securității,
- calculatorul este accesibil doar personalului autorizat, cu roluri de încredere în RO-CP
- separarea sarcinilor, conform rolului în cadrul sistemului,
- identificarea şi autentificarea rolurilor şi a personalului care îndeplineşte aceste roluri,
- prevenirea refolosirii unui obiect de către un alt proces după eliberarea acestuia de către procesul autorizat,
- protecția criptografică a schimburilor de informații şi protecția bazelor de date,
- arhivarea istoricului operațiunilor executate pe un calculator şi a datelor necesare auditării,
- o cale sigură ce permite identificarea şi autentificarea rolurilor şi a personalului care îndeplineşte aceste roluri,
- metode de restaurare a cheilor (numai în cazul modulelor hardware de securitate), a aplicaților şi a sistemului de operare,
- mijloace de monitorizare şi alertare în cazul accesului neautorizat la resursele de calcul.

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) şi 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 viata

Controale specifice dezvoltării sistemului

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

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

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

Controale pentru managementul securității

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

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

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

2.5.4 Controale de securitatea a rețelei

Serverele şi stațiile de lucru de încredere aparținând RO-CP sunt conectate prin intermediul unei rețele locale (LAN), divizate în mai multe subretele, cu acces controlat.

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

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

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

2.5.5 Controale specifice modulelor criptografice

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

2.5.6 Înregistrarea evenimentelor şi procedurile de auditare

Pentru a gestiona eficient sistemele RO-CP şi pentru a putea audita acțiunile utilizatorilor şi personalului RO-CP, toate evenimentele care apar în sistem sunt înregistrate. Informațiile înregistrate alcătuiesc jurnalele (log-urile) de evenimente şi trebuie păstrate în aşa fel încât să permită, daca este cazul, să se acceseze informațiile corespunzătoare şi necesare rezolvării disputelor, sau să detecteze tentativele de compromitere a securității RO-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 păstrata şi dezvăluita atunci când se desfăşoară un audit.

Tipuri de evenimente înregistrate

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

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

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

Fiecare înregistrare, automată sau manuală, conține următoarele informații:

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

Conținutul înregistrărilor se refera la:

- alertele firewall-urilor şi IDS-urilor,
- operațiile asociate înregistrării, certificării etc.,
- modificări ale structurii hard sau soft,
- modificări ale rețelei şi conexiunilor,
- înregistrările fizice în zonele securizate şi violările de securitate,

- schimbările de parole, drepturi asupra codurilor PIN, rolurile personalului,
- accesul reuşit şi nereuşit la baza de date RO-CP şi la aplicațiile serverului,
- generarea de chei pentru carduri, etc.,
- fiecare cerere primită şi decizia emisă în format electronic,
- istoria creării copiilor de backup şi a arhivelor cu înregistrări.

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

Frecvența analizei jurnalelor de evenimente

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

Perioada de retenție a jurnalelor de evenimente

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

Jurnalele arhivate sunt păstrate cel puțin 10 ani.

Protecția jurnalelor de evenimente

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

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

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

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

Procedurile de backup pentru jurnalele de evenimente

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

Procedura de backup si restaurare

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

- discurile de instalare a aplicațiilor sistem (de exemplu sistemul de operare),
- discurile de instalare a aplicațiilor pentru 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 şi costului restaurării aplicatiilor după defectarea, sau distrugerea sistemului. RO-CP foloseşte atât backup-uri full (săptămânale), cat şi backup-uri incrementale (zilnice), toate copiile sunt clonate şi clonele sunt păstrate în altă locație, în aceleaşi condiții de securitate ca şi cele din locația primară.

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

2.5.7 Arhivarea înregistrărilor

Este necesar ca toate datele şi fişierele 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 şi evaluării (ca urmare a unui audit) măsurilor de protecție logica şi fizica ale RO-CP,
- baza de date cu date despre carduri,

Frecvența arhivării datelor

Datele se arhiveaza cel putin o data pe saptamana.

Perioada de păstrare a arhivelor

Arhivele de pastreaza cel putin 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 marcare temporală este disponibil în cadrul RO-CA .

Procedurile de acces şi verificarea informațiilor arhivate

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

3 Controale de securitate fizică, organizațională şi de personal

Acest capitol descrie cerințele generale privind securitatea fizică şi organizațională, precum şi activitatea personalului RO-CP în activitatea de management al cheilor, personalizarea optica a cardurilor, audit şi 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 şi 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 şi ieşire este înregistrată în jurnalul de evenimente (log-urile sistemului); stabilitatea sursei de electricitate precum şi temperatura sunt de asemenea monitorizate şi controlate.

Amplasarea locației

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

Accesul fizic

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

Sediul RO-CP este accesibil în fiecare zi lucrătoare între 10:00 şi 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 şi testare.

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

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

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

Sursa de alimentare cu electricitate şi aerul condiționat

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

Expunerea la apă

Riscul de inundație în zona serverelor este foarte mic, deoarece distanța față de conductele de apă este mare, iar locația RO-CP este la ultimul etaj. În plus, personalul de pază este localizat chiar lângă zona serverelor şi este instruit să anunțe imediat administratorul RO-CP şi administratorul clădirii.

Prevenirea incendiilor

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

Depozitarea mediilor de stocare a informațiilor

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

Aruncarea deşeurilor

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

Depozitarea backup-urilor în afara locației

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

Stocarea în afara locației se aplică şi în cazul arhivelor, copiilor curente ale informațiilor procesate de sistem şi kit-urilor de instalare ale aplicațiilor RO-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 şi 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 şi procedurilor de securitate.
  - Inițiază instalarea, configurarea şi managementul aplicațiilor software şi hardware (inclusiv resursele de rețea) ale RO-CP; inițiază şi suspendă serviciile oferite de RO-CP; coordonează administratorii, inițiază şi supraveghează generarea de chei şi secrete partajate; atribuie drepturi din punct de vedere al securității şi privilegiilor de acces ale utilizatorilor; atribuie parole pentru conturile utilizatorilor noi; verifică jurnalele de evenimente; supervizează auditurile interne şi externe; primeşte şi răspunde la rapoartele de audit; supervizează eliminarea deficiențelor constatate în urma auditului.
  - Supraveghează operatorii;
  - Configurează sistemele şi rețeaua, activează şi configurează mecanismele de protecție a rețelei; creează conturile pentru utilizatorii RO-CP; verifică log-urile de sistem; verifică respectarea Codului de Practici şi Proceduri; generează secrete partajate şi chei; creează copiile de siguranță de urgență; modifică numele şi adresele serverelor.

- **Administratorul de sistem** – Autorizat să instaleze, configureze şi să întreţină sistemele de încredere ale RO-CP pentru managementul cardurilor si al cheilor. Instalează dispozitivele hardware şi sistemele de operare; instalează şi configurează echipamentele de reţea.
- **Operator –** Responsabil de operarea zilnică a sistemelor de încredere ale RO-CP; ia parte in procesul de personalizare logica si optica a cardurilor
- **HSM Administrator**
    - Executa in siguranta Procesul de Management al Cheilor,
    - Genereaza, administreaza si distruge cheile asimetrice pentru carduri
- **Auditorul de sistem** – autorizat să acceseze arhivele şi log-urile de audit ale sistemelor de incredere ale RO-CP. Responsabil de efectuarea de audituri interne pentru respectarea Codului de Practici şi 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 responsabilităţile auditorului.*

3.2.2 Numărul de persoane necesare pentru îndeplinirea unei sarcini

Procesul de generare de chei – pentru semnarea certificatelor sau pentru transportul Km_{wc}– este una din operaţiile ce necesită o atenţie deosebită. Generarea necesită prezenţa a cel puţin trei persoane: un administrator de securitate, un administrator de HSM si un Operator CA.

Prezenţa Operatorului Autorităţii de Certificare şi a unui număr corespunzător de operatori HSM este necesară şi la încărcarea cheii criptografice a Autorităţii de Certificare în modulul hardware de securitate. Orice altă operaţiune sau rol, descris în cadrul CPP poate fi efectuată de o singură persoană, special desemnată în acest sens.

3.2.3 Identificarea şi autentificarea pentru fiecare rol

Personalul RO-CP este supus identificării şi autentificării în următoarele situaţii:

- plasarea pe lista de persoane care au dreptul de a accesa locaţiile RO-CP ,
- plasarea pe lista de persoane care au acces fizic la sisteme şi resurse de reţea aparţinând RO-CP,

- emiterea confirmării care autorizează îndeplinirea rolului asignat,
- asignarea unui cont şi a unei parole în sistemul informatic al RO-CP,

Fiecare cont asignat:

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

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

3.3 Controlul personalului

RO-CP trebuie să se asigure că persoana care îndeplineşte 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 şi responsabilitățile sale în cadrul sistemului,
- a beneficiat de un stagiu de pregătire avansată în conformitate cu obligațiile şi sarcinile asociate funcției sale,
- a fost instruit cu privire la protecția datelor personale şi informațiilor confidențiale sau private,
- a semnat un contract ce conține clauze referitoare la protejarea datelor confidențiale (din punctul de vedere al securității RO-CP) ,

3.3.1 Experiența personală, calificările şi clauzele de confidențialitate necesare

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

Îndeplinirea unei funcții de încredere permite accesul la informațiile clasificate. Dezvăluirea neautorizată a acestor informații poate cauza pierderea sau compromiterea intereselor, apărate de lege, ale unei persoane fizice sau ale unei organizații.

Procedurile de acces la informațiile nepublice şi 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 îndeplineşte roluri şi sarcini ca urmare a angajării la RO-CP, trebuie să fie instruit cu privire la:

- reglementările Codului de Practici şi Proceduri al RO-CP,
- reglementările Politicii de certificare a RO-CA,
- procedurile şi controalele de securitate folosite de RO-CA,
- aplicațiile software ale RO-CP,
- responsabilitățile ce decurg din rolurile şi 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 şi Proceduri, Politica de certificare şi acceptă restricțiile şi 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 şi 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 şi 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 şi în cazul angajaților RO-CP . În plus, personalul angajat pe bază de contract, pe timpul cât îşi desfăşoară 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 şi 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 şi Proceduri al RO-CP,
- Responsabilitățile şi 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 şi procedurile acestora (inclusiv cu prezentul Cod de Practici şi Proceduri).

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

Auditurile desfăşurate 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 desfăşoară sub supravegherea administratorului de securitate

Frecvența auditării

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

4.1 Identitatea / calificările auditorului

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

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

4.2 Relația auditorilor cu entitatea auditată

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

4.3 Domeniile supuse auditării

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

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

4.4 Analiza vulnerabilităților

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

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

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