CODUL DE PRACTICI ȘI PROCEDURI AL AUTORITĂȚII DE MARCARE TEMPORALĂ OPERATĂ DE CĂTRE SC COMTEC NET SRL

V 1.0 – Februarie 2011

CUPRINS

1. Aria de cuprindere

Codul de Practici şi Proceduri este o descriere detaliată a termenilor si condițiilor în care autoritatea de Marcare Temporală COMTEC NET furnizează serviciile de marcare temporală şi practicile manageriale şi operaționale pe care le urmează in furnizarea acestora. Codul de Practici şi Proceduri descrie modul de implementare a cerințelor stabilite prin politica de marcare temporală.

2. Managementul ciclului de viață al cheii

2.1. Generarea cheilor unităților de marcare temporală

2.1.1. Generarea perechii de chei pentru semnarea mărcilor temporale

Perechile de chei ale Autorității de Marcare Temporală COMTEC NET, sunt achiziționate de la un furnizor de servicii de certificare acreditat de MCSI conform reglementărilor legale în vigoare.

Cheia privata este menținuta în permanență criptată pe dispozitivul criptografic şi nu părăseşte niciodată dispozitivul intr-o formă necriptată.

După achiziționarea perechii de chei pentru semnarea de mărci temporale şi activarea cheii private în modulul hardware de securitate, aceasta poate fi folosita în operațiile criptografice până la expirarea perioadei de validitate sau până la o eventuala compromitere.

2.1.2. Dimensiunea cheilor

Dimensiunea cheilor RSA folosite pentru semnarea mărcilor temporale este 1024 biți.

2.2. Protejarea cheilor private ale unităților de marcare temporala

2.2.1. Standarde pentru modulele criptografice

Modulele hardware de securitate folosite de Autoritatea de Certificare respectă cerințele standardului FIPS 140-2. Semnătura electronica este creată prin folosirea algoritmului RSA în combinație cu rezumatul criptografic SHA-1.

2.2.2. Controlul accesului la cheia privata

Controlul accesului se realizează prin utilizarea cheilor private stocate pe carduri criptografice sau token-uri, protejate printr-un cod PIN achiziționate în mod autentificat de operatorii autorizați.

Deținătorii dispozitivului criptografic se angajează să îl protejeze declarând că nu va partaja cu nimeni utilizarea acestuia şi nu va dezvălui (direct sau indirect) codul PIN.

2.2.3. Responsabilitățile deținătorului de dispozitiv criptografic

Deținătorul de dispozitiv criptografic trebuie să-şi îndeplinească îndatoririle şi obligațiile conform cerințelor acestui Cod de Practici şi Proceduri, în mod responsabil în orice situație posibilă.

Un deținător de dispozitiv criptografic trebuie să anunțe emitentul acestuia în cazul furtului, pierderii, dezvăluirii neautorizate sau compromiterii securității, imediat după incident.

Un deținător de dispozitiv criptografic nu este responsabil pentru neîndeplinirea îndatoririlor /obligațiilor sale din cauza unor motive ce sunt imposibil de controlat de către acesta.

Deținătorul de dispozitiv criptografic este responsabil pentru neglijarea obligațiilor de a notifica emitentul despre dezvăluirea violarea securității ca urmare a greşelilor, neglijenței sau iresponsabilității sale.

2.2.4. Metoda de activare a cheii private

Metoda de activare a cheii private de semnare a mărcilor temporale se referă la activarea cheii înainte de orice folosire a sa.

La import, generare sau restaurare cheia privata a unei unități de marcare temporala este dezactivata. Cheia se activează prin pornirea serviciului.

O cheie odată activată poate fi folosită pe perioada in care serviciul funcționează. La oprirea serviciului cheia se dezactivează.

Activarea cheilor private este întotdeauna precedată de autentificarea operatorului.

Autentificarea este realizată pe baza dispozitivului criptografic deținut de operator; după introducerea acestuia în modulul criptografic şi folosirea codului PIN, cheia privată rămâne în stare activă până la scoaterea dispozitivului din modul.

2.2.5. Metoda de dezactivare a cheii private

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

În cazul cheii private a unui TSU, dezactivarea ei se face in momentul in care serviciul se oprește pentru orice operațiune.

Protecția hardware a cheii private înseamnă ca aceasta nu este in nici un moment disponibila in clar, nici măcar in memoria aplicației.

În cazul COMTEC NET, dezactivarea unei chei private se face de către persoanele cu roluri de încredere numai în cazul în care serviciul este oprit pentru actualizări, mentenanță, sau alte motive.

2.3. Distribuirea cheilor publice ale Autorității de Marcare Temporală COMTEC NET

Certificatele corespunzătoare cheilor private de semnare a mărcilor temporale emise de către unitățile de marcare temporală sunt publicate pe site https://www.comtec.ro

2.4. Schimbarea cheilor Autorității de Marcare Temporală COMTEC NET

Perioada de valabilitate a certificatului asociat cheii private de semnare a mărcilor temporale este de un an. Înainte cu o luna față de expirarea certificatului se va achiziționa o noua pereche de chei şi un nou certificat.

Cheia privata de semnare a mărcilor temporale va fi schimbata in situația in care a survenit revocarea certificatului corespunzător.

Aplicația care generează mărcile temporale este concepută în aşa fel încât orice încercare de emitere a unei mărci temporale după expirarea cheii private de semnare să fie respinsă.

2.5. Distrugerea cheilor TSU

Distrugerea cheii private a unui TSU al Autorității de Marcare Temporală COMTEC NET presupune ştergerea dispozitivului prin care este protejată cheia. După ştergere, cheia este pierdută pentru totdeauna. Fiecare distrugere de cheie privată este înregistrată în jurnalul de evenimente.

2.6. Managementul modulului hardware de securitate

Autoritatea de Marcare Temporală COMTEC NET se asigură că :

i. Integritatea modulelor criptografice de securitate nu a fost afectată în decursul transportului de la producător

ii. Integritatea modulelor criptografice de securitate nu a fost afectată în decursul stocării premergătoare instalării

iii. Instalarea, administrarea şi operarea acestora este efectuată doar de personal de încredere

iv. Modulele criptografice de securitate funcționează corect

v. Cheile private de semnare stocate pe modulele criptografice de securitate sunt distruse in momentul scoaterii din producție

3. Înregistrarea evenimentelor

3.1. Înregistrarea evenimentelor

Pentru a gestiona eficient sistemele COMTEC NET şi pentru a putea audita acțiunile utilizatorilor şi personalului COMTEC NET, 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 accesarea informațiilor necesare rezolvării disputelor şi detectarea tentativelor de compromitere a securității COMTEC NET, iar auditorilor şi autorității de supraveghere sa verifice conformitatea cu cadrul legal şi cu propriile politici şi proceduri. Evenimentele înregistrate fac obiectul procedurilor de arhivare.

Când este posibil, log-urile sunt create automat. Dacă înregistrările nu pot fi create automat, se vor folosi jurnalele de evenimente pe hârtie. În sistemele COMTEC NET, auditorul intern de securitate este obligat să realizeze anual un audit referitor la respectarea reglementărilor acestui Cod de Practici şi Proceduri şi să evalueze eficiența procedurilor de securitate existente.

3.2. Tipuri de evenimente înregistrate

Fiecare activitate critică din punctul de vedere al securității COMTEC NET 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.

Concret, se înregistrează următoarele informații:

- evenimentele apărute în sistemul informatic;
- sincronizările cu baza de timp;
- desincronizările cu baza de timp;
- schimbarea cheilor criptografice;
- opriri ale sistemului;
- incidente de securitate.

Jurnalele de evenimente 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 informații despre:

i. tipul evenimentului,

ii. identificatorul evenimentului,

iii. data şi ora apariției evenimentului,

iv. identificatorul persoanei responsabile de eveniment.

Conținutul înregistrărilor se refera la:

a) alertele firewall-urilor şi IDS-urilor,

b) operațiile asociate emiterilor sau verificărilor mărcilor temporale,

c) modificări ale structurii hard sau soft,

d) modificări ale rețelei şi conexiunilor,

e) înregistrările fizice în zonele securizate şi violările de securitate,

f) schimbările de parole, drepturi asupra codurilor PIN, rolurile personalului,

g) accesul reuşit şi nereuşit la baza de date şi la aplicațiile serverului,

h) activarea de chei,

i) schimbarea cheilor,

j) istoria creării copiilor de backup şi a arhivelor cu înregistrări,

k) fiecare cerere de marca temporala primită.

Cererile înregistrate, asociate serviciilor oferite, trimise de către un Abonat, în afara utilizării lor în rezolvarea disputelor şi a detectării abuzurilor, permit calcularea taxelor serviciilor.

Accesul la jurnalele de evenimente (log-uri) este permis în exclusivitate administratorului de securitate şi administratorilor de sistem.

3.3. 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 loguri.

Orice acțiune executată ca rezultat al funcționării defectuoase detectate trebuie înregistrată în jurnal.

3.4. 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 online, la cererile autorizate. După depăşirea spațiului alocat, jurnalele sunt păstrate în arhive şi pot fi accesate numai off-line.

Jurnalele arhivate sunt păstrate cel puțin 10 ani.

3.5. Protecția jurnalelor de evenimente

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.

După arhivare, un jurnal de evenimente poate fi revăzut numai cu aprobarea administratorului de securitate. Accesul la jurnalul de evenimente este configurat în aşa fel încât:

- este posibilă detectarea oricărei violări de integritate deci înregistrările nu conțin goluri sau falsuri,
- nici o entitate nu are dreptul să modifice conținutul unui jurnal.

Procedurile de securitate COMTEC NET solicită ca jurnalul de evenimente să facă obiectul backup-ului periodic, conform procedurii de backup aprobate.

3.6. Notificarea entităților responsabile de tratarea evenimentelor

Modulul de analiză a jurnalului de evenimente implementat în sistem examinează evenimentele curente şi sesizează automat activitățile suspecte sau pe cele care au ca scop compromiterea securității. În cazul activităților care au influență asupra securității sistemului, sunt notificați automat administratorul de securitate şi administratorii de sistem. În celelalte cazuri, notificarea este direcționată numai către administratorii de sistem.

Transmiterea informațiilor către persoanele autorizate despre situațiile critice – din punctul de vedere al securității sistemului – se face prin mijloace de comunicare, protejate corespunzător (de exemplu, telefon mobil sau poştă electronica). Entitățile notificate iau măsurile corespunzătoare pentru a proteja sistemul față de amenințarea detectată.

3.7. Arhivarea înregistrărilor

Toate înregistrările din Registrul Electronic Operativ al mărcilor temporale sunt arhivate.

Registrul on-line conține toate mărcile temporale emise precum şi date referitoare la marca şi la certificatul folosit şi poate fi accesat permanent pentru efectuarea unor servicii externe ale Autorității de Marcare Temporală COMTEC NET, de exemplu verificarea unei mărci temporale.

Arhivele off-line conțin înregistrările cu până la 10 ani înainte de data curentă. Arhiva este folosită pentru rezolvarea eventualelor dispute, referitoare la documente electronice vechi. După expirarea perioadei de păstrare declarate, datele arhivate sunt distruse.

3.8. Procedurile de acces şi verificarea informațiilor arhivate

Pentru a verifica integritatea informațiilor arhivate, datele sunt periodic testate.

Această activitate poate fi realizată numai in prezența administratorului 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.

4. Managementul operațional si al securității

SC COMTEC NET SA a implementat şi certificat un sistem de management al securității informatice (SMSI, in sensul standardului ISO 27001) pentru toate serviciile furnizate.

4.1. Managementul Riscului

SC COMTEC NET SRL a implementat un proces permanent de identificare si contracarare a riscurilor operaționale si de securitate pentru toate serviciile pe care le furnizează în calitate de terță parte de încredere (servicii de certificare digitală şi servicii de marcare temporală la data prezentei). Managementul riscului acoperă toate sistemele şi aplicațiile informatice, rețelele de calculatoare, clădirile, camerele şi personalul implicat in furnizarea acestor servicii, de-a lungul întregului lor ciclu de viață şi identifică masurile necesare pentru reducerea sau eliminarea completă a oricăror evenimente nedorite legate confidențialitatea, integritatea şi disponibilitatea informațiilor procesate şi a serviciilor oferite.

4.2. Controale de securitate fizică, organizațională şi de personal

Acest capitol descrie cerințele generale referitoare la organizarea activităților, la personal, cat şi pe cele privind procesele de asigurare a securității fizice.

4.2.1. Masuri organizaționale si procedurale

COMTEC NET a implementat si certificat un proces de management al securității informațiilor conform ISO 27001. In companie exista un administrator de securitate şi un Comitet pentru Managementul Securității. De asemenea, fiecare anagajat este responsabilizat prin asumarea scrisa a fişei postului.

Pentru asigurarea securității informațiilor au fost identificate, implementate şi sunt controlate prin SMSI următoarele procese:

- Planificarea strategică
- Managementul arhitecturii platformelor tehnologice
- Inventarul resurselor

- Clasificarea informației
- Utilizarea resurselor
- Managementul schimbării
- Controlul accesului
- Relațiile cu terții
- Managementul resurselor umane
- Continuitatea afacerii
- Tratarea incidentelor

Toate procesele identificate şi implementate pentru asigurarea securității sunt controlate prin politici şi proceduri specifice.

4.2.2. Controlul Personalului

COMTEC NET trebuie să se asigure că persoana care îndeplineşte responsabilitățile funcției, conform cu rolul atribuit în cadrul Autorității de Marcare Temporală:

i. a absolvit cel puțin liceul,

ii. este cetățean român,

iii. a semnat un contract care descrie rolul şi responsabilitățile sale în cadrul sistemului,

iv. a beneficiat de un stagiu de pregătire în conformitate cu obligațiile şi sarcinile asociate funcției sale,

v. a fost instruit cu privire la protecția datelor personale şi informațiilor confidențiale sau private,

vi. a semnat un contract ce conține clauze referitoare la protejarea informațiilor senzitive (din punctul de vedere al securității COMTEC NET) şi a datelor confidențiale şi private ale Abonaților,

vii. nu îndeplineşte sarcini care pot genera conflicte de interese,

Personalul angajat al COMTEC NET care îndeplineşte un rol de încredere, trebuie să obțină avizul administratorului de securitate.

4.2.2.1. Roluri de încredere

În COMTEC NET sunt definite următoarele roluri de încredere, care pot fi atribuite uneia sau mai multor persoane:

i. **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 COMTEC NET;
- inițiază şi suspendă serviciile oferite de COMTEC NET;

- coordonează administratorii, inițiază şi supraveghează generarea de chei şi secrete partajate;
- aproba drepturi din punct de vedere al securității şi privilegiilor de acces ale utilizatorilor;
- 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;
- Verifică respectarea Politicii de Marcare Temporală şi a Codului de Practici şi Proceduri;

ii. **Administratorul de sistem** – Autorizat să instaleze, configureze şi să administreze sistemele si aplicațiile Autorității de Marcare Temporală.

iii. **Operatorul de sistem** – Responsabil cu operarea zilnică a sistemelor şi aplicațiilor Autorității de Marcare Temporală. Autorizat să execute operațiile de backup şi restaurare a sistemului; transferă copiile de siguranță ale arhivei şi ale datelor curente în afara locației COMTEC NET.

iv. **Administratorul HSM** – Administrează modulul de securitate.

v. **Operatorul HSM** – Porneşte aplicația de marcare temporală.

vi. **Administratorul registrului electronic** – se asigură că toate înregistrările sunt realizate şi păstrate conform cu Politica de Marcare Temporală.

vii. **Auditorul de sistem** – autorizat să acceseze arhivele şi log-urile de audit ale sistemelor de încredere ale Autorității de Certificare. Responsabil de efectuarea de audituri interne pentru respectarea Codului de Practici şi Proceduri de către Autoritatea de Certificare; această responsabilitate se extinde şi asupra Autorității de Înregistrare care operează în cadrul COMTEC NET.

4.2.2.2. Identificarea şi autentificarea pentru fiecare rol

Personalul COMTEC NET este supus identificării şi autentificării ori de cate ori accesează o camera sau un sistem informatic prevăzute cu sisteme de control al accesului. Identificarea şi autentificarea se fac prin una din următoarele metode, sau printr-o combinație a lor:

- Nume şi parolă,
- Cheie privată stocată electronic şi PIN,
- Cheie privată stocată hardware (pe un dispozitiv criptografic) şi PIN.

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 COMTEC NET, a sistemului de operare şi a controalelor de aplicații.

Fiecare dispozitiv criptografic este înmânat utilizatorului de către administratorul de securitate pe baza unui proces verbal.

4.2.2.3. Cerințele de pregătire a personalului

Personalul care îndeplineşte roluri şi sarcini ca urmare a asumării unui rol din cadrul Autorității de Marcare Temporala, trebuie să fie instruit cu privire la:

- reglementările Codului de Practici şi Proceduri,
- reglementările Politicii de Marcare Temporală,
- masurile de securitate folosite,
- aplicațiile software ale Autorității de Marcare Temporală,
- responsabilitățile ce decurg din rolurile şi sarcinile executate în sistem.

4.2.2.4. Sancționarea acțiunilor neautorizate

În cazul descoperirii sau existenței suspiciunii unui acces neautorizat, administratorul de securitate va investiga incidentul şi poate suspenda accesul persoanei respective la sistemul COMTEC NET. Măsurile disciplinare pentru astfel de incidente sunt descrise în politicile şi procedurile corespunzătoare şi sunt conforme cu prevederile legale.

4.2.2.5. Personalul angajat pe baza de contract

Personalul angajat pe baza de contract (servicii externe, dezvoltatori de subsisteme sau aplicații etc.) respectă aceleaşi masuri de securitate ca şi personalul permanent.

În plus, personalul angajat pe bază de contract, pe timpul cât îşi desfăşoară activitatea în locația COMTEC NET, trebuie permanent însoțit de către un angajat al COMTEC NET , 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.

4.2.3. Controale de securitate fizică

Sistemele de calcul, terminalele operatorilor şi resursele informaționale ale COMTEC NET sunt dispuse în zone dedicate, protejate 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 surselor de electricitate precum şi temperatura sunt de asemenea monitorizate şi controlate.

4.2.3.1. Amplasarea locației

COMTEC NET are sediul la următoarea adresă: Str. Mexic, nr. 13, Sector 1, Bucureşti.

4.2.3.2. Accesul fizic

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

Sediul COMTEC NET este deschis publicului în fiecare zi lucrătoare între 09:00 şi 17:00.

În restul timpului, accesul este permis numai persoanelor autorizate de către conducerea COMTEC NET. Vizitatorii spațiilor aparținând COMTEC NET trebuie să fie însoțiți permanent de persoane autorizate.

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 de sistem.

Sediul societății este monitorizat permanent, inclusiv video, de către o societate de protecție si paza.

4.2.3.3. Sursa de alimentare cu electricitate şi aerul condiționat

Întreg sediul societății este prevăzut cu aer condiționat. Din momentul întreruperii alimentării cu energie, sursele de electricitate de urgență (UPS) permit continuarea neperturbată a activității. Generatorul de curent al clădirii intra automat in funcțiune in cazul oricărei întreruperi a alimentarii cu energie din sistemul public.

4.2.3.4. Expunerea la apă

Riscul de inundație în zona serverelor este foarte mic, deoarece distanța față de conductele de apă este mare, iar locația COMTEC NET este proiectate in asa fel încât se asigură un drenaj corespunzător al apei în surplus.

4.2.3.5. Prevenirea incendiilor

Locația COMTEC NET dispune de sistem de prevenire şi protecție împotriva incendiilor în conformitate cu standardele şi reglementările în domeniu.

4.2.3.6. 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 cameră şi seifuri este permis numai persoanelor autorizate.

4.2.3.7. Aruncarea deşeurilor

Hârtiile şi mediile electronice care conțin informații importante din punct de vedere al securității COMTEC NET 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.

4.2.3.8. Backup-ul în afara locației

COMTEC NET dispune de un centru de date de back-up situat in Brașov. Stocarea în afara locației se aplică în cazul arhivelor, copiilor curente ale informațiilor procesate de sistem şi kit-urilor de instalare ale aplicațiilor COMTEC NET. Aceasta organizare permite refacerea de urgență a oricărei funcții a COMTEC NET în termenele stabilite prin planul de asigurare a continuității afacerii.

4.3. Controalele tehnice

Cerințele tehnice prezentate în acest capitol se referă la controalele de securitate specifice calculatoarelor şi aplicațiilor, folosite în cadrul COMTEC NET.

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 Autorității de Marcare Temporală 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 COMTEC NET,
- 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.

4.3.1. Controale de securitatea a rețelei

Serverele şi stațiile de lucru de încredere aparținând COMTEC NET 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 şi a filtrelor de trafic aplicate la nivelul ruterelor şi serviciilor proxy.

Evenimentele (log-urile) sunt înregistrate în jurnalele de sistem şi permit supravegherea folosirii corecte a serviciilor furnizate de COMTEC NET.

4.3.2. Standardele tehnice aplicabile

Structura mărcii temporale este conform SR ETSI TS 101 861 V1.2.1:2005 Profil de marcare temporală si Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP): IETF RFC 3161.

Politica de marcare temporala a fost creată plecând de la standardul SR ETSI TS 102 023 V1.2.1:2005 Semnături electronice şi infrastructuri (ESI). Cerințe privind politica pentru autoritățile de marcare temporală.

Profilul certificatului digital emis pentru Autoritatea de Marcare Temporală COMTEC NET respectă recomandările IETF din RFC 3161 si RFC 2459, Internet X.509 Public Key Infrastructure Certificate.

Modulul hardware de securitate (HSM) utilizat în cadrul TSU al Autorității de Marcare Temporală COMTEC NET respectă standardul NIST FIPS 140-2 Security Requirements for Cryptographic Modules.

In crearea semnăturii electronice a mărcilor temporale se respecta standardul IETF RFC 2630 Cryptographic Message Syntax.

Formatul timpului din mărcile temporale este conform IETF RFC 3339, Date and Time on the Internet: Timestamps.

Algoritmul SHA-1 este definit in FIPS Pub 180-2, Secure Hash Standard.

Algoritmul MD5 este definit in RFC 1321, The MD5 Message-Digest Algorithm.

Algoritmul RIPEMD-160 este definit in ISO/IEC 10118-3, Security techniques -- Hash-functions -- Part 3: Dedicated hash-functions.

Algoritmul sha1WithRSAEncryption este definit in IETF RFC2437 - PKCS #1: RSA Cryptography Specifications Version 2.0.

Managementul securității Autorității de Marcare Temporală COMTEC NET este asigurat conform standardelor ISO 27001:2005, Information technology -- Security

techniques -- Information security management systems – Requirements si ISO 27002, Information technology -- Security techniques -- Code of practice for information security management.

4.4. Timpul

Platforma COMTEC NET de furnizare a serviciilor de marcare temporală conține un server de timp care este sincronizat cu timpul UTC prin conectarea permanentă şi securizată la baza de timp reprezentată de sistemul informatic destinat furnizării orei oficiale a României.

Sincronizarea cu sursa de timp este monitorizată permanent şi orice desincronizare este semnalată imediat administratorilor.

Aplicația software care emite mărcile temporale este realizată astfel ca la orice desincronizare care depăşeşte precizia asumată să oprească emiterea de mărci.

Dacă totuși se constată că s-au emis mărci temporale care încalcă precizia asumată, atât abonații care au primit acele mărci cât şi autoritatea de supraveghere sunt notificați.

4.5. Evaluarea securității sistemelor informatice

Sistemele de calcul COMTEC NET respectă cerințele descrise în standardele ETSI TS 101456 (Cerințele de Politică pentru Autoritățile de Certificare care emit certificate calificate), ETSI TS 102023 (Cerințele de Politică pentru Autoritățile de Marcare temporală), si este certificata ISO 27002.

5. Managementul Codului de Practici şi Proceduri

Fiecare versiune a Codului de Practici şi Proceduri este în vigoare (starea sa este **validă**) până în momentul publicării şi aprobării noii sale versiuni. O nouă versiune este dezvoltată de către COMTEC NET şi publicata pentru comentarii cu mențiunea **spre aprobare** (daca este cazul). După primirea şi includerea comentariilor, Codul de Practici şi Proceduri intra în procedura de aprobare internă.

Responsabil de aprobarea formei finale a Codului de Practici si Proceduri este un comitet format din directorul general, managerii departamentelor tehnice şi managerul departamentului de dezvoltare a afacerii.

Responsabil pentru întreținerea Codului de Practici şi Proceduri este managerul departamentului care asigură furnizarea serviciilor de marcare temporală.

După terminarea procedurii de aprobare, noua versiune a CPP este transmisă Autorității de Reglementare şi Supraveghere şi apoi, în termen de 10 zile, este publicată şi marcată ca fiind în starea **validă**.

Regulile şi cerinţele descrise mai jos, cu privire la managementul Codului de Practici şi Proceduri guvernează şi managementul Politicii de certificare.

5.1. Procedura de schimbare a CPP

Modificarea Codului de Practici şi Proceduri poate fi rezultatul depistării unor erori, actualizării sale sau a sugestiilor primite din partea entităţilor interesate.

Propunerile de modificare pot fi trimise prin poştă sau e-mail pe adresa COMTEC NET. Propunerile de modificare trebuie să descrie modificările necesare, motivele acestor modificări şi să ofere mijloace de contact ale persoanei care solicită modificarea.

După introducerea unei modificări, este actualizată data emiterii Codului de Practici şi Proceduri sau a Politicii de certificare şi este modificat numărul versiunii documentului.

Modificările introduse pot fi în general împărţite în două categorii: una care nu necesită consultarea Abonaţilor şi una care cere (de obicei în avans) consultarea Abonaţilor. Prima categorie include modificări de urgenţă sau modificări neesenţiale.

5.2. Procedurile de publicare şi notificare

O copie a Codului de Practici şi Proceduri este disponibilă în formă electronică pe site-ul de Web http://www.comtec.ro sau prin e-mail la adresa office@tecnet.ro.

5.3. Procedurile de aprobare a CPP

Dacă în timp de 30 de zile de la data publicării propunerilor de modificare ale Codului de Practici şi Proceduri, COMTEC NET nu primeşte remarci semnificative cu privire la aceste schimbări, noua versiune a Codului de Practici şi Proceduri, aflată în starea **spre aprobare,** devine documentul care guvernează politica de certificare şi trebuie respectat de toţi Abonaţii COMTEC NET iar starea acestei versiuni va fi schimbată în **validă**.

Abonaţii care nu acceptă noul Cod de Practici şi Proceduri, conţinând termenii şi reglementările modificate, sunt obligaţi să depună, în termen de 15 zile de la data la care noua versiune a Codului de Practici şi Proceduri a fost aprobată, o declaraţie în acest sens. Acest lucru duce la încetarea contractului de presari servicii de certificare şi la revocarea certificatului emis în baza acestuia.

6. Glosar

Abonat - o persoană juridică cu mai mulţi utilizatori sau o persoana fizică, utilizator individual.

Acces – abilitatea de a folosi o resursă informaţionala din sistem.

Audit – executarea unor proceduri independente de verificare şi evaluare cu scopul de a testa măsura în care este suficient şi adecvat managementul implementat pentru controlul sistemului, de a verifica dacă managementul şi operaţiile sistemului sunt îndeplinite în conformitate cu Politica serviciului şi cu celelalte reglementări care decurg din ea, de a descoperi posibilele breşe de securitate şi de a recomanda modificarea corespunzătoare a măsurilor de control, a politicii de certificare şi a procedurilor aferente.

A autentifica – a confirma identitatea declarată a unei entităţi.

Autentificare – controlul de securitate cu scopul de a oferi siguranţă şi încredere datelor transferate, mesajelor sau emitenţilor lor; controalele de verificare a autenticităţii unei persoane, înainte de a-i livra un tip de informaţii secreta

Autoritatea de Marcare Temporala – vezi TSA.

Certificatul de cheie publică – o structură de date care conţine cel puţin numele sau identificatorul unei Autorităţi de Certificare , identificatorul unui Abonat, cheia sa publică, perioada de validitate, numărul serial şi cel asignat de către Autoritatea de Certificare. Un certificat poate fi în una din trei stări fundamentale: în aşteptarea activării, activ şi inactiv.

Certificat Valid – un certificat de cheie publică este valid numai atunci când (1) a fost emis de o Autoritate de Certificare (2) a fost acceptat de Abonat (subiectul certificatului) şi (3) nu a fost revocat.

Certificat revocat – certificat de cheie publică plasat pe Lista certificatelor Revocate.

Cheie secretă - cheie folosită în tehnicile criptografice simetrice, cunoscută doar de un grup de Abonaţi autorizaţi.

Cheie privată – una dintre cheile asimetrice aparţinând unui Abonat şi folosită numai de acel abonat.

În cazul sistemelor cu chei asimetrice, o cheie privată descrie transformarea de semnare. În cazul sistemului asimetric de criptare, o cheie privată descrie transformarea de decriptare. Cheia privată este (1) cheia al cărei scop este decriptarea sau crearea de semnătură pentru uzul exclusiv al proprietarului; (2) acea cheie din perechea de chei care este cunoscută numai proprietarului.

Cheie publică – una dintre cheile perechii asimetrice ale unui Abonat, care este disponibilă publicului. În cazul sistemelor de criptare asimetrică, cheia publică defineşte transformarea de verificare a semnăturii. În cazul criptării asimetrice, cheia publică defineşte transformarea de criptare a mesajelor.

Control al accesului – procesul de acordare a accesului la resursele informaţionale de sistem numai utilizatorilor autorizaţi, aplicaţiilor, proceselor şi altor sisteme.

Entitate parteneră – utilizatori de mărci temporale.

Furnizor de servicii de certificare – instituţie de încredere (inclusiv dispozitivele hardware aflate sub controlul sau) care face parte dintre terţii de încredere şi care furnizează servicii capabile să creeze, să semneze şi să emită certificate sau servicii de ne-repudiere.

Identificator de obiect (OID) – identificator alfanumeric / numeric înregistrat în concordanță cu standardul ISO/IEC 9834 şi oferind unicitate unui obiect specificat sau clasei sale.

Infrastructura de cheie publică (PKI) – arhitectura, tehnicile, practicile şi procedurile care contribuie în mod colectiv la implementarea şi funcționarea sistemelor criptografice cu chei publice, bazate pe certificate; PKI constă în hardware şi software, baze de date, resurse de rețea, proceduri de securitate şi obligații legale, legate împreună şi care colaborează pentru a furniza şi implementa atât serviciile de certificare cât şi alte servicii asociate infrastructurii (de ex. furnizarea de marcă temporală).

Lista de certificate Revocate (CRL) – listă emisă periodic sau imediat, semnată electronic de către o autoritate, permițând identificarea certificatelor care au fost revocate sau suspendate înainte de expirarea perioadei de validitate. CRL conține numele emitentului său, data publicării, data următoarei actualizări, numerele seriale ale certificatelor revocate sau suspendate şi datele şi motivele revocării sau suspendării lor.

Modul criptografic (HSM) – un dispozitiv care constă în hardware, software, microcod sau o combinație a lor şi care execută operațiile criptografice (inclusive criptare şi decriptare) în interiorul zonei acestui modul criptografic.

Obiect – obiect la care accesul este controlat, de exemplu un fişier, o aplicație, o zonă de memorie principală unde se face asamblarea şi păstrarea datelor personale.

Perioada de activitate a certificatului – perioada dintre începutul şi sfârşitul validității unui certificat sau perioada dintre data de începere a validității certificatului şi momentul revocării sau suspendării lui.

Procedura de aplicat în situațiile de urgență - procedura alternativă la cea standard, care se execută la apariția unei situații de urgență.

Semnătura electronica – transformarea criptografică a datelor pentru a permite atât verificarea originii şi integrității datelor de către destinatarul acestora cât şi protejarea expeditorului şi a destinatarului împotriva falsificării de către primitor; semnăturile electronice asimetrice pot fi generate de către o entitate prin folosirea unei chei private şi a unui algoritm asimetric, ex. RSA;

Sistem informatic – întreaga infrastructură, personal şi componente folosite pentru asamblarea, procesarea, depozitarea, transmiterea, publicarea, distribuirea şi managementul informației.

Marca temporală - Structura de date care leagă reprezentarea unor date electronice de un anumit timp, stabilind astfel dovada că acele date existau înainte de acel moment de timp.

Terți de încredere (TTP) – instituție sau reprezentantul său în care are încredere o entitate autentificată, o entitate care execută verificări sau alte entități din zona operațiilor asociate cu securitatea şi autentificarea.

TSA – Autoritatea de Marcare Temporală - In cazul unei persoane juridice este acea parte a sa, formată din personal de încredere, care operează un sistem informatic

(inclusiv unul sau mai multe TSU) in condiții stabilite prin Politica de Marcare temporală şi Codul de Practici şi Proceduri, pentru a furniza serviciile de marcare temporală.

TSU – Unitate de Marcare Temporală - Sistemul format din aplicația care creează mărcile temporale, sistemul de calcul pe care aceasta este instalată şi modulul hardware criptografic cu ajutorul căruia se semnează marca. La un moment dat, o singura cheie privată este activă.

Validarea certificatelor de cheie publică – verificarea stării unui certificat, care permite stabilirea dacă certificatul este revocat sau nu.