S.C. DigiSign S.A.

Codul de Practici și Proceduri a Autorității de Marcare Temporală

Versiunea 2.0.0

Data: 23-03-2012

Cuprins

1 Aria de Cuprindere

Codul de Practici şi Proceduri este o descriere detaliată a termenilor si condiţiilor în care se furnizează serviciile, ca şi a practicilor manageriale şi operaţionale pe care le urmează Autoritatea de Marcare Temporală DigiSign in furnizarea serviciilor de marcare temporală. Codul de Practici şi Proceduri descrie cum anume aceasta implementează cerinţele tehnice, procedurale şi organizaţionale stabilite prin politică.

2 Managementul ciclului de viaţă al cheii

2.1 Generarea cheilor unităţilor de marcare temporală

2.1.1 Generarea perechii de chei pentru semnarea mărcilor temporale

Perechea de chei a unitaţilor de marcare temporală este generată prin control dual, în cadrul locaţiei DigiSign, în prezenţa unui grup de persoane de încredere (conform matricii de roluri pentru Autoritatea de Marcare Temporală DigiSign), intr-un modul hardware de securitate (HSM), conforme cu cerinţele FIPS 140-2 Nivel 3.

Cheia privata este menţinuta în permanenţă criptată pe acest dispozitiv şi nu părăseşte niciodată dispozitivul intr-o formă necriptată.

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

Mediul electronic în care se face generarea cheii şi în care aceasta există pe toată durata ei de viaţă este protejat fizic si electromagnetic.

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

2.1.2 Dimensiunea cheilor

Dimensiunea cheilor RSA folosite pentru semnarea marcilor temporale este de 1024, respectiv 2048 de biti.

2.2 Protejarea cheilor private ale unitatilor de marcare temporala

2.2.1 Standarde pentru modulele criptografice

Modulele hardware de securitate folosite de Autorităţile de Certificare respectă cerinţele standardului FIPS 140-2. Semnatura electronica este creată prin folosirea algoritmului RSA în combinaţie cu rezumatul criptografic SHA-1.

2.2.2 Controlul dual al accesului la cheia privata

Controlul dual al accesului se realizează prin distribuirea de secrete partajate operatorilor autorizaţi. Secretele sunt stocate pe carduri criptografice sau token-uri, protejate printr-un cod PIN şi transferate în mod autentificat deţinătorilor acestora.

Pentru operaţiuni de tipul iniţierea modulului criptografic hardware si transferul cheii private se implementează scheme prag de acces (de tip k din n) prin distribuire **de secrete partajate**.

Numărul total de secrete partajate este de 3, iar numărul necesar de secrete care permit accesul la cheia privata este de 2.

Procedura de transfer a secretului partajat implică prezenţa deţinătorului de secret pe timpul procesului de generare a cheii şi a distribuirii sale, acceptarea secretului dat şi a responsabilităţilor care reies din păstrarea sa.

2.2.2.1 Acceptarea păstrării secretului de către deținători

Fiecare deţinător de secret partajat, înainte de a primi partea sa de secret, trebuie să asiste personal la împărţirea secretului, să verifice corectitudinea secretului creat şi distribuirea sa.

Fiecare parte a secretului partajat trebuie transferată deţinătorului pe un card criptografic protejat de un cod PIN, ales de deţinător şi ştiut numai de el.

Primirea secretului partajat şi crearea sa sunt confirmate printr-o semnatura de mână pe un formular, a cărui copie este păstrată în arhivele Autorităţii de Certificare şi de către deţinătorul de secret.

2.2.2.2 Protecția secretului partajat

Deţinătorii secretului partajat trebuie să protejeze partea lor împotriva dezvăluirii.

Deţinătorul declară că:

i. nu va dezvălui, copia sau împărţi secretul cu nimeni şi că nu va folosi partea sa din secret într-un mod neautorizat,

ii. nu va dezvălui (direct sau indirect) că este deţinătorul secretului

2.2.2.3 Responsabilităţile deţinătorului de secret partajat

Deţinătorul de secret partajat trebuie să-şi îndeplinească îndatoririle şi obligaţiile conform cerinţelor acestui Cod de Practici şi Proceduri, în mod responsabil în orice situaţie posibilă.

Un deţinător de secret partajat trebuie să anunţe emitentul secretului în cazul furtului, pierderii, dezvăluirii neautorizate sau compromiterii securităţii secretului, imediat după incident.

Un deţinător de secret partajat nu este responsabil pentru neîndeplinirea îndatoririlor/obligaţiilor sale din cauza unor motive ce sunt imposibil de controlat de către acesta, dar este responsabil pentru dezvăluirea inoportună a secretului sau pentru neglijarea obligaţiilor de a notifica emitentul secretului despre dezvăluirea inoportună sau violarea securităţii secretului ca urmare a greşelilor, neglijenţei sau iresponsabilităţii deţinătorului.

2.2.3 Backup-ul cheilor private

Autoritatea de Marcare Temporală DigiSign creează o copie de siguranţă a cheilor private folosita la semnarea marcilor temporale. Copiile sunt folosite în cazul punerii în aplicare a procedurilor de urgenţă (de exemplu, după dezastru) de recuperare a cheilor. Copiile cheilor private sunt protejate prin secretele partajate create la generarea cheiilor originale.

2.2.4 Introducerea cheii private în modulul criptografic

Operaţiunea de introducere a unei chei private într-un modul criptografic se aplică în următoarele cazuri:

i. în cazul creării copiilor de siguranţă a cheii private stocate într-un modul criptografic, poate fi necesară, ocazional, (ex. în cazul compromiterii sau defectării modulului) introducerea unei perechi de chei într-un modul de securitate diferit,

ii. când este necesară transferarea unei chei private din modulul operaţional folosit pentru operaţii standard ale entităţii, pe un alt modul; situaţia poate apărea în cazul invocarii planului de Disaster Recovery sau al necesităţii distrugerii modului operational.

Introducerea unei chei private într-un modul de securitate este o operaţiune critică şi de aceea trebuie implementate măsuri şi proceduri care să prevină dezvăluirea, modificarea sau falsificarea cheii private.

Introducerea unei chei private în modulul hardware de securitate al TSU al Autorităţii de Marcare Temporală DigiSign necesită restaurarea cheii de pe carduri în prezenţa unui număr corespunzător de deţinători de secrete partajate care protejează modulul ce conţine cheile private.

2.2.5 Metoda de activare a cheii private

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

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

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

Activarea cheilor private este întotdeauna precedată de autentificarea operatorului.

Autentificarea este realizată pe baza unui card criptografic deţinut de operator. După introducerea cardului în modulul criptografic şi folosirea codului PIN, cheia privată rămâne în stare activă până la scoaterea cardului din modul.

2.2.6 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 opreste pentru orice operatiune.

Protectia hardware a cheii private inseamna ca aceasta nu este in nici un moment disponibila in clar, nici macar in memoria aplicatiei.

În cazul DigiSign, dezactivarea unei chei private se face de către persoanele cu roluri de incredere numai în cazul în care serviciul este oprit pentru actualizari, mentenanţă, sau alte motive.

2.3 Distribuirea cheilor publice ale Autorității de Marcare Temporală DigiSign

Certificatele corespunzatoare cheilor private de semnare a mărcilor temporale emise de către unităţile de marcare temporală sunt publicate pe site la adresele: http://www.digisign.ro/TSA/CertificatTSA.cer , http://www.digisign.ro/TSA/CertificatTSA-0.cer, http://www.digisign.ro/TSA/CertificatTSA-1.cer, http://www.digisign.ro/TSA/CertificatTSA2016.cer .

2.4 Schimbarea cheilor Autorității de Marcare Temporală DigiSign

Perioada de valabilitate a certificatului asociat cheii private de semnare a mărcilor temporale este de 1 an. Inainte cu cel puţin 1 luna faţă de expirarea certificatului se va genera o noua pereche de chei şi un

nou certificat.

Cheia privata de semnare a marcilor temporale va fi schimbata in situatia in care a survenit revocarea certificatului corespunzator.

2.5 Sfarsitul ciclului de viata al cheii private a TSU

Autoritatea de Marcare Temporală DigiSign a implementat proceduri tehnice şi operaţionale pentru ca înainte de expirarea certificatului asociat cheii de semnare a unui TSU să se genereze o nouă pereche de chei şi un nou certificat.

In momentul înlocuirii perechilor de chei, vechea cheie privată şi orice secret partajat care ar permite recrearea ei sunt distruse.

Aplicaţia care generează marcile temporale este concepută în aşa fel incat orice incercare de emitere a unei marci temporale după expirarea cheii private de semnare sa fie respinsă.

2.6 Distrugerea cheilor TSU

Distrugerea cheii private a unui TSU al Autorităţii de Marcare Temporală DigiSign presupune ştergerea cardurilor care conţin secretele partajate prin care este protejată cheia. Dupa ştergerea lor, cheia este pierdută pentru totdeauna.

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

2.7 Managementul modulului hardware de securitate

Autoritatea de Marcare Temporală DigiSign se asigură că :

i. Integritatea modulelor criptografice de securitate nu a fost afectată în decursul transportului de la producator
ii. Integritatea modulelor criptografice de securitate nu a fost afectată în decursul stocării premergatoare instalării
iii. Instalarea, administrarea şi operarea acestora este efctuată doar de personal de incredere
iv. Modulele criptografice de securitate funcţionează corect
v. Cheile private de semnare stocate pe modulele criptografice de securitate sunt distruse in momentul scoaterii acestuiă din producţie

3 Inregistrarea evenimentelor

3.1 Înregistrarea evenimentelor

Pentru a gestiona eficient sistemele DigiSign şi pentru a putea audita acţiunile utilizatorilor şi personalului DigiSign, toate evenimentele care apar în sistem sunt înregistrate. Informaţiile înregistrate alcătuiesc jurnalele (log-urile) de evenimente şi trebuie păstrate în aşa fel încât să permită Entităţilor Partenere să acceseze informaţiile corespunzătoare şi necesare rezolvării disputelor şi să detecteze tentativele de compromitere a securităţii DigiSign, iar auditorilor şi autorităţii de supraveghere sa verifice conformitatea cu cadrul legal şi cu propriile politici şi proceduri. Evenimentele înregistrate fac obiectul procedurilor de arhivare. Arhivele sunt păstrate în afara incintei DigiSign.

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 DigiSign, auditorul intern de securitate este obligat să realizeze anual un audit referitor la respectarea reglementărilor acestui Cod de Practici şi Proceduri şi să evalueze eficienţa procedurilor de securitate existente.

3.2 Tipuri de evenimente înregistrate

Fiecare activitate critică din punctul de vedere al securităţii DigiSign 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 inregistreaza următoarele informaţii:

evenimentele apărute în sistemul informatic;

- sincronizările cu baza de timp;
- desincronizarile 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, conţine informaţii despre:

i. tipul evenimentului,
ii. identificatorul evenimentului,
iii. data şi ora apariţiei evenimentului,
iv. identificatorul persoanei responsabile de eveniment.

Conţinutul înregistrărilor se refera la:

a) alertele firewall-urilor şi IDS-urilor,
b) operaţiile asociate emiterilor sau verificarilor marcilor temporale,
c) modificări ale structurii hard sau soft,
d) modificări ale reţelei 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 aplicaţiile serverului,
h) generarea 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 puţin o dată pe lună. Orice eveniment având o importanţă 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 acţiune executată ca rezultat al funcţionării 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 spaţiului alocat, jurnalele sunt păstrate în arhive şi pot fi accesate numai off-line. Jurnalele arhivate sunt păstrate cel puţin 10 ani.

3.5 Protecția jurnalelor de evenimente

Periodic, fiecare înregistrare din jurnale face obiectul copierii pe bandă magnetică.

După depăşirea numărului acceptat de înregistrări pentru un jurnal, conţinutul 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.

Dupa copiere sau 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; acest lucru asigură faptul că înregistrările nu conţin goluri sau falsuri,
- nici o entitate nu are dreptul să modifice conţinutul unui jurnal.

3.6 Procedurile de backup pentru jurnalele de evenimente

Procedurile de securitate DigiSign solicită ca jurnalul de evenimente să facă obiectul backup-ului periodic, conform procedurii de backup aprobate. Aceste copii sunt stocate în locaţii auxiliare ale DigiSign.

3.7 Notificarea entităților responsabile de tratarea evenimentelor

Modulul de analiză a jurnalului de evenimente implementat în sistem examinează evenimentele curente şi sesizează automat activităţile suspecte sau pe cele care au ca scop compromiterea securităţii. În cazul activităţilor care au influenţă asupra securităţii sistemului, sunt notificaţi automat administratorul de securitate şi administratorii de sistem. În celelalte cazuri, notificarea este direcţionată numai către administratorii de sistem.

Transmiterea informaţiilor către persoanele autorizate despre situaţiile critice – din punctul de vedere al securităţii sistemului – se face prin mijloace de comunicare, protejate corespunzător (de exemplu, telefon mobil sau poştă electronica). Entităţile notificate iau măsurile corespunzătoare pentru a proteja sistemul faţă de ameninţarea detectată.

3.8 Arhivarea înregistrărilor

Toate inregistrarile din Registrul Electronic Operativ al marcilor temporale sunt arhivate.

Registrul on-line conţine toate marcile temporale emise precum şi date referitoare la marca şi la certificatul folosit şi poate fi accesat permanent pentru efectuarea unor servicii externe ale Autorităţii de Marcare Temporală DigiSign, de exemplu verificarea unei marci temporale.

Arhivele off-line conţin inregistrarile cu până la 10 ani înainte de data curentă. Arhiva este folosită pentru rezolvarea eventualelor dispute, referitoare la documente electronice vechi. Tehnologia folosită permite arhivarea inregistrarilor si restaurarea lor in siguranţă pe perioade de timp de minim 50 de ani.

3.9 Perioada de păstrare a arhivelor

Datele arhivate sunt păstrate pentru o perioada de timp de 10 ani. După expirarea perioadei de păstrare declarate, datele arhivate sunt distruse.

3.10 Procedurile de acces şi verificarea informațiilor arhivate

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

Această activitate poate fi realizată numai in prezenţa 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 operational si al securitatii

SC DigiSign SA a implementat un sistem de management al securităţii informatice (SMSI, in sensul standardului ISO 27001) pentru toate procesele implicate în furnizarea de servicii de încredere (servicii de certificare şi de marcare temporală la data prezentei).

4.1 Managementul Riscului

Dintre toate procesele de asigurare a securitatii informatiei cel mai important, de care depind toate celelate, este managementul riscului.

SC DigiSign SA a implementat un proces permanent de identificare si contracarare a riscurilor operationale si de securitate pentru toate serviciile pe care le furnizeaza în calitate de terţă parte de incredere (servicii de certificare digitală şi servicii de marcare temporală la data prezentei). Managementul riscului acoperă toate sistemele şi aplicaţiile informatice, reţelele de calculatoare, cladirile, camerele şi personalul implicat in furnizarea acestor servicii, de-a lungul intregului lor ciclu de viaţă şi identifică masurile necesare pentru reducerea sau eliminarea completă a oricaror evenimente nedorite legate confidentialitatea, integritatea şi disponibilitatea informaţiilor procesate şi a serviciilor oferite.

4.2 Controale de securitate fizică, organizațională şi de personal

Acest capitol descrie cerinţele generale referitoare la organizarea activitatilor, la personal, cat şi pe cele privind procesele de asigurare a securităţii fizice.

4.2.1 Masuri organizationale si procedural

In firma a fost creata o structură de departamente şi una de roluri care respectă principiul „separation of duties" şi impiedică preluarea controlului unui intreg proces sau al unei activităţi critice de catre o singură persoană.

Exista un administrator de securitate şi un Comitet pentru Managementul Securităţii. Fiecare anagajat este responsabilizat prin asumarea scrisa a fişei postului.

Pentru asigurarea securităţii informaţiilor au fost identificate, implementate şi sunt controlate prin SMSI urmatoarele procese:

- Planificarea strategică
- Managementul arhitecturii platformelor tehnologice
- Inventarul resurselor (informaţii, software, echipamente, camere, cladiri)
- Clasificarea şi gestiunea informaţiei
- Utilizarea resurselor
- Managementul schimbării
- Controlul accesului
- Relaţiile cu terţii
- Managementul capacităţii
- Instruirea personalului
- Monitorizarea
- Securitatea fizică
- Continuitatea afacerii
- Tratarea incidentelor de securitate

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

4.2.1.1 Planificarea strategica

Intreaga activitate a Autorităţii de Marcare Temporală este planificată anual şi multianual prin stabilirea unor obiective în acord cu cadrul legislativ şi normativ şi cu cerinţele pieţei şi prin alocarea de resurse care să susţina atingerea acestor obiective.

4.2.1.2 Managementul arhitecturii platformelor tehnologice

Sistemele tehnologice folosite pentru oferirea serviciilor de marcare temporala sunt realizate (eventual achizitionate) şi actualizate printr-un proces care implica cooperarea dintre toate departamentele implicate (vanzari, dezvoltare, operare şi suport).

4.2.1.3 Clasificarea si gestiunea resurselor

Toate resursele Autorităţii de Marcare Temporală (informaţii, sisteme şi aplicaţii) sunt inventariate periodic şi clasificate din punct de vedere al securităţii şi al importanţei pentru business. Au fost puse la punct procese prin care gestiunea acestor resurse (intrare, ieşire, stocare, transfer, utilizare) este strict controlată prin masuri direct proporţionale cu clasificarea şi importanţa lor.

4.2.1.4 Managementul schimbarii

DigiSign foloseşte un proces controlat pentru managementul schimbărilor. Fiecare aplicaţie, înainte de a fi folosită în producţie de DigiSign, este instalată astfel încât să se permită controlul versiunii curente şi să se prevină instalarea neautorizată de programe sau falsificarea celor existente.

Dezvoltarea, testarea şi producţia sunt zone distincte, iar transferul informaţiilor şi aplicaţiilor dintr-o zonă in alta se face controlat.

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

- dispozitivele fizice sunt furnizate în aşa fel încât să poată fi urmărită 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.

4.2.1.5 Controlul accesului

Orice acces la o resursa se face printr-un proces controlat la care iau parte managerii, administratorii de sistem şi administratorul de securitate. Se respectă principiile necesităţii de a cunoaşte şi a separarii rolurilor. Periodic se verifică că drepturile de acces existente sunt corespunzatoare.

4.2.1.6 Relatiile cu tertii

Procesul se referă în primul rând la relaţiile cu furnizorii de servicii şi controlul său presupune asigurarea securităţii informaţiilor accesate de acestia.

4.2.1.7 Managementul capacitatii

Procesul prin care DigiSign urmareşte permanent încarcarea sistemelor care furnizează serviciile de încredere pentru a asigura calitatea şi performanţele asumate prin politici si prin contracte.

4.2.1.8 Instruirea personalului

Personalul angajat în furnizarea serviciilor este pregatit atat la angajare, cât şi ulterior, periodic, pentru a avea competenţele profesionale necesare şi pentru a cunoaşte şi aplica toate politicile, procedurile şi masurile tehnice operaţionale şi de securitate.

4.2.1.9 Monitorizarea

Sistemele tehnologice, serviciile şi personalul sunt permanent monitorizate pentru a asigura o calitate şi o securitate a serviciilor care sa mulţumească clienţii şi să asigure respectarea legilor, a normelor precum şi a propriilor standarde.

4.2.1.10 Securitatea fizica

Accesul în incinta DigiSign este controlat atat printr-un sistem de control al accesului cu carduri de proximitate cât şi, permanent, prin agenţi de pază. Acelaşi sistem cu carduri de acces controlează accesul şi în camerele cu resurse considerate critice. Există sisteme de detectare

4.2.1.11 Continuitatea afacerii

DigiSign a pregatit şi testează anual un plan de asigurare a continuităţii afacerii care să permita restaurarea rapida a tuturor serviciilor în cazul unor dezastre (incendii, cutremure etc). Există de asemenea un complex de masuri preventive şi corective care să permită asigurarea unei disponibilităţi maxime a serviciilor oferite (planuri de mentenanţă, piese de schimb, redundanţă a componenetelor critice, copii de siguranţă a datelor, ghiduri de tratare a erorilor si avariilor etc).

4.2.1.12 Tratarea incidentelor de securitate

Toate sistemele critice şi reteaua sunt monitorizate permanent şi administratorii de sistem, ca şi cel de securitate sunt alertaţi in timp real la apariţia oricarui incident.

Exista planuri de intervenţie şi de tratare a acestor incidente.

4.2.2 Controlul Personalului

4.2.2.1 Masuri generale pentru controlul personalului

DigiSign trebuie să se asigure că persoana care îndeplineşte responsabilităţile funcţiei, conform cu rolul atribuit în cadrul Autorităţii de Marcare Temporală:

i. a absolvit cel puţin liceul,

ii. este cetăţean român,

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

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

v. a fost instruit cu privire la protecţia datelor personale şi informaţiilor confidenţiale sau private,

vi. a semnat un contract ce conţine clauze referitoare la protejarea informaţiilor senzitive (din punctul de vedere al securităţii DigiSign) şi a datelor confidenţiale şi private ale Abonaţilor,

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

Personalul angajat al DigiSign care îndeplineşte un rol de încredere, trebuie să obţină avizul administratorului de securitate.

4.2.2.2 Roluri de încredere

În DigiSign 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.

   a) Iniţiază instalarea, configurarea şi managementul aplicaţiilor software şi hardware (inclusiv resursele de reţea) ale DigiSign; iniţiază şi suspendă serviciile oferite de DigiSign; coordonează administratorii, iniţiază şi supraveghează generarea de chei şi secrete partajate; aproba drepturi din punct de vedere al securităţii şi privilegiilor de acces ale utilizatorilor; verifică jurnalele de evenimente; supervizează auditurile interne şi externe; primeşte şi răspunde la rapoartele de audit; supervizează eliminarea deficienţelor constatate în urma auditului.

   b) Supraveghează operatorii;

   c) 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 aplicatiile Autorităţii de Marcare Temporală.

iii. **Operatorul de sistem** – Responsabil cu operarea zilnică a sistemelor şi aplicaţiilor Autorităţii de Marcare Temporală. Autorizat să execute operaţiile de backup şi restaurare a sistemului; transferă copiile de siguranţă ale arhivei şi ale datelor curente în afara locaţiei DigiSign.

iv. **Administratorul HSM** – Administrează modulul de securitate şi creează carduri operatori.

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

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

vii. **Auditorul de sistem** – autorizat să acceseze arhivele şi log-urile de audit ale sistemelor de încredere ale Autorităţii 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 Autorităţii de Înregistrare care operează în cadrul DigiSign.

4.2.2.3 Numărul de persoane necesare pentru îndeplinirea unei sarcini

Procesul de generare de chei – pentru semnarea marcilor temporale – este una din operaţiile ce necesită o atenţie deosebită. Generarea necesită prezenţa a cel puţin două persoane: un administrator de securitate şi un administrator de sistem. La procesul de generare a cheii unui TSU participă de asemenea posesorii de secrete partajate care păstrează partea lor de cheie în locaţii sigure.

Prezenţa administratorului de securitate şi a unui număr corespunzător de posesori de secrete partajate este necesară şi la încărcarea cheii criptografice în modulul hardware de securitate.

Activarea cheii private necesită cvorumul conform cu schema prag, asta înseamnă că prezenta deţinatorilor de secrete partajate este necesară şi de fiecare dată cand e repornit serviciul. Orice altă operaţiune sau rol, descris în cadrul CPP-ului poate fi efectuată de o singură persoană, special desemnată în acest sens.

4.2.2.4 Identificarea şi autentificarea pentru fiecare rol

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

- Nume şi parolă,
- Cheie privată stocată electronic şi PIN,
- Cheie privată stocată hardware (pe un dispozitiv criptografic) şi PIN,
- Card de acces cu poză.

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 restricţionat conform funcţiei (ce reiese din rolul îndeplinit de persoana respectivă) pe baza software-ului de sistem al DigiSign, a sistemului de operare şi a controalelor de aplicaţii.

Fiecare dispozitiv criptografic sau card de acces este înmanat utilizatorului de către administratorul de securitate pe baza unui proces verbal.

4.2.2.5 Cerințele de pregătire a personalului

Personalul care îndeplineşte roluri şi sarcini ca urmare a asumarii unui rol din cadrul Autoritatii 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,
- aplicaţiile software ale Autorităţii de Marcare Temporală,
- responsabilităţile ce decurg din rolurile şi sarcinile executate în sistem.

4.2.2.6 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 DigiSign. Măsurile disciplinare pentru astfel de incidente sunt descrise în politicile şi procedurile corespunzătoare şi sunt conforme cu prevederile legale.

4.2.2.7 Personalul angajat pe baza de contract

Personalul angajat pe baza de contract (servicii externe, dezvoltatori de subsisteme sau aplicaţii 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 locaţia DigiSign, trebuie permanent însoţit de către un angajat al DigiSign , cu excepţia celor care au primit avizare din partea administratorului de securitate şi care poate accesa informaţii clasificate intern sau în conformitate cu normele legale în vigoare.

4.2.3 Controale de securitate fizică

Sistemele de calcul, terminalele operatorilor şi resursele informaţionale ale DigiSign sunt dispuse în zone dedicate, protejate fizic împotriva accesului neautorizat, distrugerilor sau perturbării activităţii. Aceste locaţii 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*

DigiSign este localizată în Bucureşti, la următoarea adresă: Str. Virgil Madgearu, nr. 2-6, sector 1, Bucureşti.

4.2.3.2 *Accesul fizic*

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

Sediul DigiSign este deschis publicului în fiecare zi lucrătoare între 09:30 şi 17:00.

În restul timpului, accesul este permis numai persoanelor autorizate de către conducerea DigiSign. Vizitatorii spaţiilor aparţinând DigiSign trebuie să fie însoţiţi permanent de persoane autorizate.

Zonele ocupate de DigiSign se împart în:

- zona serverelor,
- zona operatorilor,
- zona administratorilor,
- zona de dezvoltare şi testare,
- zona office.

Zona serverelor este echipată cu un sistem de securitate monitorizat continuu, alcătuit din senzori de mişcare, efracţie şi incendiu. Accesul în această zonă este permis numai personalului autorizat, de exemplu, administratorul de securitate, 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 *zonele operatorilor şi administratorilor* se face prin intermediul cardurilor şi a cititoarelor de carduri. Deoarece toate informaţiile 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. În această zonă au acces numai angajaţii DigiSign şi persoanele autorizate; ultimilor nu le este permisă prezenţa în zonă neînsoţiţi.

Zona de dezvoltare şi testare este protejată într-o manieră similară cu zona operatorilor şi administratorilor. Proiectele în curs de implementare şi software-ul aferent este testat în mediul de dezvoltare al DigiSign.

4.2.3.3 *Sursa de alimentare cu electricitate şi aerul condiționat*

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

4.2.3.4 *Expunerea la apă*

Riscul de inundaţie în zona serverelor este foarte mic, deoarece distanţa faţă de conductele de apă este mare, iar locaţia DigiSign este proiectate in asa fel incât se asigură un drenaj corespunzător al apei în surplus. În plus, personalul de pază este localizat chiar lângă zona serverelor şi este instruit să anunţe imediat administratorul DigiSign şi administratorul clădirii in caz de incident.

4.2.3.5 *Prevenirea incendiilor*

Locaţia DigiSign dispune de sistem de prevenire şi protecţie împotriva incendiilor în conformitate cu standardele şi reglementările în domeniu.

4.2.3.6 *Depozitarea mediilor de stocare a informațiilor*

În funcţie de sensibilitatea informaţiilor, mediile electronice care conţin arhivele şi copiile de siguranţă 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 conţin informaţii importante din punct de vedere al securităţii DigiSign 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 *Depozitarea backup-urilor în afara locației*

Cardurile criptografice necesare pentru restaurarea serviciilor în caz de dezastru sunt stocate în containere speciale, situate în afara locaţiei DigiSign.

Stocarea în afara locaţiei se aplică şi în cazul arhivelor, copiilor curente ale informaţiilor procesate de sistem şi kit-urilor de instalare ale aplicaţiilor DigiSign. Acest lucru permite refacerea de urgenţă a oricărei funcţii a DigiSign în termenele stabilite prin planul de asigurare a continuităţii afacerii.

4.3 Controalele tehnice

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

Calculatoarele aparţinând Autorităţii de Marcare Temporală dispun de următoarele mijloace de securitate:

- autentificarea obligatorie la nivelul sistemului de operare şi al aplicaţiilor,
- control discreţionar al accesului,
- posibilitatea de a fi auditate din punct de vedere al securităţii,
- calculatorul este accesibil doar personalului autorizat, cu roluri de încredere în DigiSign,
- 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,
- protecţia criptografică a schimburilor de informaţii şi protecţia bazelor de date,
- arhivarea istoricului operaţiunilor 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 aplicaţilor 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 reţelei

Serverele şi staţiile de lucru de încredere aparţinând DigiSign sunt conectate prin intermediul unei reţele locale (LAN), divizate în mai multe subreţele, 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 DigiSign.

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 plecand de la standardul SR ETSI TS 102 023 V1.2.1:2005 Semnături electronice şi infrastructuri (ESI). Cerinţe privind politica pentru autorităţile de marcare temporală.

Profilul certificatului digital emis pentru Autoritatea de Marcare Temporală DigiSign 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 Autorităţii de Marcare Temporală DigiSign 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 securităţii Autorităţii de Marcare Temporală DigiSign 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 DigiSign de furnizare a serviciilor de marcare temporală conţine un server de timp care este sincronizat cu timpul UTC prin conectarea permanentă si 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.

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

Dacă totusi se constată că s-au emis mărci temporale care incalcă precizia asumată, atat abonaţii care au primit acele marci cât şi autoritatea de supraveghere sunt notificaţi.

4.5 Evaluarea securității sistemelor informatice

Sistemele de calcul DigiSign respectă cerinţele descrise în standardele ETSI TS 101456 (Cerinţele de Politică pentru Autorităţile de Certificare care emit certificate calificate), ETSI TS 102023 (Cerinţele de Politică pentru Autorităţile de Marcare temporală), CEN CWA 14167 (Cerinţele de Securitate pentru Sistemele de Încredere care asigură Managementul certificatelor pentru Semnatura Electronică) si 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 DigiSign şi publicata pentru comentarii cu menţiunea **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, directorul general adjunct, managerii departamentelor tehnice şi managerul departamentului de dezvoltare a afacerii.

Responsabil pentru intreţinerea 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 Autorităţii 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.

Abonaţii trebuie să respecte numai Politica de certificare şi Codul de Practici şi Proceduri în vigoare în momentul respectiv.

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 DigiSign. 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 modificari de urgenţă sau modificari 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.digisign.ro/repository sau prin e-mail la adresa office@digisign.ro.

Trei versiuni ale Codului de Practici şi Proceduri sunt întotdeauna disponibile în Depozit şi prin e-mail: versiunea în vigoare, versiunea anterioară şi versiunea în curs de aprobare (dacă este cazul).

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, DigiSign 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 DigiSign 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.

Actualizarea de certificat – înainte de expirarea unui certificat, CA îl poate actualiza (sau înnoi) confirmând validitatea aceleiaşi perechi de chei pentru următoarea perioadă de validitate (în concordanţă cu Politica de certificare).

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.

Calea de certificare – calea ordonată a certificatelor, pornind de la un certificat considerat punct de încredere (ales de verificator) până la certificatul de verificat. O cale de certificare îndeplineşte următoarele condiţii:

- *pentru toate certificatele cert(x) incluse în calea de certificare {cert(1),*cert(2), ……., cert(n-1)} subiectul certificatului cert(x) este emitentul certificatului cert(x+1),
- certificatul cert(1) este emis de o Autoritate de Certificare (punct de încredere) considerată de încredere de către verificator,
- cert(n) este certificatul de verificat.

Fiecare cale de certificare poate fi legată de una sau mai multe politici de certificare sau o astfel de politică poate fi inexistentă. Politicile atribuite unei căi de certificare sunt intersecţia politicilor a căror identificatori sunt incluşi în fiecare certificat, încorporate în calea de certificare şi definite în extensia Certificate Policies.

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 semnatură 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 semnaturii. 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.

Deţinător de secret partajat – deţinător autorizat al unui card electronic folosit pentru păstrarea secretului partajat.

Entitate parteneră – utilizatori de marci 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 concordanţă 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 funcţionarea sistemelor criptografice cu chei publice, bazate pe certificate; PKI constă în hardware şi software, baze de date, resurse de reţea, proceduri de securitate şi

obligaţii 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, permiţând identificarea certificatelor care au fost revocate sau suspendate înainte de expirarea perioadei de validitate. CRL conţine 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 combinaţie a lor şi care execută operaţiile criptografice (inclusiv criptare şi decriptare) în interiorul zonei acestui modul criptografic.

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

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

Politica de certificare – document sub forma unui set de reguli care sunt respectate strict de către o autoritate emitentă în timpul prestării serviciilor de certificare.

Procedura de aplicat în situaţiile de urgenţă - procedura alternativă la cea standard, care se execută la apariţia unei situaţii de urgenţă.

Publicarea certificatelor şi a Listei de certificate Revocate – procedurile de distribuire a certificatelor emise şi a certificatelor revocate.

Revocarea unui certificat – defineşte procedurile privind revocarea unei perechi de chei valide (revocarea de certificat) în cazul în care accesul la perechea de chei trebuie restricţionat pentru a preveni posibila utilizare a sa în criptarea sau crearea de semnatură electronică. Un certificat revocat este plasat pe Lista de certificate Revocate (CRL).

Secret partajat – parte a unui secret criptografic, de ex. o cheie distribuită între n persoane de încredere (jetoane criptografice, de ex. carduri electronice) în aşa fel încât este nevoie de m părţi ale secretului (unde m<n) pentru a restaura cheia distribuită.

Semnatura electronica – transformarea criptografică a datelor pentru a permite atât verificarea originii şi integrităţii datelor de către destinatarul acestora cât şi protejarea expeditorului şi a destinatarului împotriva falsificării de către primitor; semnaturile 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 informaţiei.

Stările unei chei private – o cheie privată poate fi în una din următoarele trei stări fundamentale (conform standardului ISO/IEC 11770-1):

- ***în aşteptarea activării (pregătită)*** – cheia a fost deja generată dar nu este încă disponibilă pentru folosire;
- ***activă*** – cheia poate fi folosită în operaţiuni criptografice (de ex. Pentru crearea de semnaturi electronice);
- ***inactivă*** – cheia poate fi folosită exclusiv pentru decriptare sau perechea ei publică pentru

verificarea de semnaturi electronice.

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

Transformarea stării cheii – starea unei chei poate fi schimbată numai când apare una dintre următoarele transformări (în conformitatea cu ISO/IEC 11770-1):

- ***generarea*** – procesul de generare de chei; generarea de cheie trebuie să se realizeze în concordanţă cu procedurile acceptate; procesul poate include proceduri de testare cu scopul de a îmbunătăţi calitatea cheii;
- ***activarea*** – are ca rezultat devenirea validă a unei chei şi disponibilă pentru executarea de operaţii criptografice;
- ***dezactivarea*** – restrângerea unei chei; poate să apară la expirarea perioadei de validitate a cheii;
- ***reactivarea*** – permite folosirea în continuarea a unei chei aflată în starea de indisponibilitate pentru executarea de operaţii criptografice;
- ***distrugerea*** – are ca rezultat terminarea ciclului de viaţă al cheii; această noţiune se referă la distrugerea logică a cheii dar poate fi aplicată şi la distrugerea ei fizică.

Terţi de încredere (TTP) – instituţie sau reprezentantul său în care are încredere o entitate autentificată, o entitate care execută verificări sau alte entităţi din zona operaţiilor asociate cu securitatea şi autentificarea.

TSA – Autoritatea de Marcare Temporală - In cazul unei persoane juridice este acea parte a sa, formată din personal de incredere, care opereaza un sistem informatic (inclusiv unul sau mai multe TSU) in condiţii 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 aplicaţia care creează mărcile temporale, sistemul de calcul pe care aceasta este instalată şi modulul hardware criptografic cu ajutorul căruia se semneaza 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.