

Codul de Practici si Proceduri al Autoritatii de Marcare Temporală operata de sc certSIGN srl certSAFE Time Stamping Authority

Cuprins:

1	Aria de Cuprindere.....	6
2	Managementul ciclului de viață al cheii.....	6
2.1	Generarea cheilor unitatilor de marcare temporala	6
2.1.1	Generarea perechii de chei pentru semnarea marcilor temporale.....	6
2.1.2	Dimensiunea cheilor	7
2.2	Protejarea cheilor private ale unitatilor de marcare temporala.....	7
2.2.1	Standarde pentru modulele criptografice.....	7
2.2.2	Controlul dual al accesului la cheia privata.....	7
2.2.3	Backup-ul cheilor private	9
2.2.4	Introducerea cheii private în modulul criptografic	9
2.2.5	Metoda de activare a cheii private.....	10
2.2.6	Metoda de dezactivare a cheii private	11
2.3	Distribuirea cheilor publice ale certSAFE Time Stamping Authority	11
2.4	Schimbarea cheilor certSAFE Time Stamping Authority	11
2.5	Sfarsitul ciclului de viata al cheii private a TSU	12
2.6	Distrugerea cheilor TSU	12
2.7	Managementul modulului hardware de securitate	12
3	Inregistrarea evenimentelor	13
3.1	Înregistrarea evenimentelor	13
3.2	Tipuri de evenimente înregistrate	14
3.3	Frecvența analizei jurnalelor de evenimente	15

CODUL DE PRACTICI SI PROCEDURI pt SERVICIILE DE MARCARE TEMPORALĂ

3.4	Perioada de retenție a jurnalelor de evenimente	16
3.5	Protecția jurnalelor de evenimente	16
3.6	Procedurile de backup pentru jurnalele de evenimente.....	17
3.7	Notificarea entităților responsabile de tratarea evenimentelor	17
3.8	Arhivarea înregistrărilor	18
3.9	Perioada de păstrare a arhivelor	18
3.10	Procedurile de acces și verificarea informațiilor arhivate.....	18
4	Managementul operational si al securitatii.....	19
4.1	Managementul Riscului	19
4.2	Controale de securitate fizică, organizațională și de personal	20
4.2.1	Masuri organizationale si procedurale	20
	Managementul schimbarii.....	21
	Controlul accesului	22
4.2.2	Controlul Personalului	24
	Masuri generale pentru controlul personalului	24
	Roluri de încredere	25
	Numărul de persoane necesare pentru îndeplinirea unei sarcini.....	26
	Identificarea și autentificarea pentru fiecare rol	27
	Cerințele de pregătire a personalului	28
	Sanționarea acțiunilor neautorizate.....	28
	Personalul angajat pe baza de contract.....	28
4.2.3	Controale de securitate fizică	29
4.3	Controalele tehnice.....	32
4.3.1	Controale de securitatea a rețelei.....	33
4.3.2	Standardele tehnice aplicabile.....	33
4.4	Timpul.....	35

CODUL DE PRACTICI SI PROCEDURI pt SERVICIILE DE MARCARE TEMPORALĂ

CODUL DE PRACTICI SI PROCEDURI pt SERVICIILE DE MARCARE TEMPORALĂ

4.5	Evaluarea securității sistemelor informatice.....	35
5	Managementul Codului de Practici și Proceduri	36
5.1	Procedura de schimbare a CPP	36
5.2	Procedurile de publicare și notificare	37
5.3	Procedurile de aprobare a CPP	37
	Anexa 1: Glosar.....	39

CODUL DE PRACTICI SI PROCEDURI pt SERVICIILE DE MARCARE TEMPORALĂ**Istoria documentului**

Versiune	Data	Motiv	Persoana care a facut modificarea
1.0	Ianuarie 2009	Publicarea primei versiuni	Manager Servicii Electronice
1.1	Iulie 2009	Modificarea adresei firmei	Manager Servicii Electronice

Acest document a fost creat si este proprietatea:

Proprietar	Autor	Data crearii
Manager Servicii Electronice	Manager Servicii Electronice	16 Ianuarie 2009

Lista de Distributie

Destinatar	Data distribuirii
Public-Internet	24 Iulie 2009

Acest document a fost aprobat de

Versiune	Nume	Data
1.0	Comitet de Management al Politicilor si Procedurilor pentru Serviciile de Incredere	Ianuarie 2009
1.1	Comitet de Management al Politicilor si Procedurilor pentru Serviciile de Incredere	Iulie 2009

CODUL DE PRACTICI SI PROCEDURI pt SERVICIILE DE MARCARE TEMPORALĂ

1 Aria de Cuprindere

Codul de Practici si Proceduri este o descriere detaliata a termenilor si conditiilor in care se furnizeaza serviciile, ca si a practicilor manageriale si operationale pe care le urmeaza certSAFE Time Stamping Authority in furnizarea serviciilor de marcarea temporala. Codul de Practici si Proceduri descrie cum anume aceasta implementeaza cerintele tehnice, procedurale si organizationale stabilite prin politica.

2 Managementul ciclului de viață al cheii

2.1 Generarea cheilor unitatilor de marcarea temporala

2.1.1 Generarea perechii de chei pentru semnarea marcilor temporale

Perechea de chei a unitatilor de marcarea temporala este generata prin control dual, în cadrul locației certSIGN, în prezența unui grup de persoane de încredere (conform matricii de roluri pentru certSAFE Time Stamping Authority), într-un modul hardware de securitate (HSM), conforme cu cerințele FIPS 140-2 Nivel 3. Cheia privata este menținuta în permanență criptata pe acest dispozitiv si nu paraseste niciodata dispozitivul într-o forma necriptata.

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

Mediul electronic in care se face generarea cheii si in care aceasta exista pe toata durata ei de viata este protejat fizic si electromagnetic.

După generarea perechii de chei pentru semnarea de marci temporale si 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 marilor temporale este de 1024 biti.

2.2 Protejarea cheilor private ale unitatilor de marcare temporală

2.2.1 Standarde pentru modulele criptografice

Modulele hardware de securitate folosite de Autoritățile de Certificare respectă cerințele standardului FIPS 140-2. Semnatura electronica este creată prin folosirea algoritmului RSA în combinație 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 autorizați. Secretele sunt stocate pe carduri criptografice sau token-uri, protejate printr-un cod PIN și transferate în mod autentificat deținătorilor acestora.

Pentru operațiuni de tipul inițierea 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 prezența deținătorului de secret pe timpul procesului de generare a cheii și a distribuiri sale, acceptarea secretului dat și a responsabilităților care reies din păstrarea sa.

2.2.2.1 Acceptarea păstrării secretului de către deținători

Fiecare deținător de secret partajat, înainte de a primi partea sa de secret, trebuie să asiste personal la împărțirea secretului, să verifice corectitudinea secretului creat și distribuirea sa. Fiecare parte a secretului partajat trebuie transferată deținătorului pe un card criptografic protejat de un cod PIN, ales de deținător și știut numai de el. Primirea secretului partajat și crearea sa sunt confirmate printr-o semnatura de mână pe un formular, a cărui copie este păstrată în arhivele Autorității de Certificare și de către deținătorul de secret.

2.2.2.2 Protecția secretului partajat

Deținătorii secretului partajat trebuie să protejeze partea lor împotriva dezvăluirii.

Deținătorul declară că:

- nu va dezvălui, copia sau împărți secretul cu nimeni și că nu va folosi partea sa din secret într-un mod neautorizat,
- nu va dezvălui (direct sau indirect) că este deținătorul secretului

2.2.2.3 Responsabilitățile deținătorului de secret partajat

Deținătorul de secret partajat trebuie să-și îndeplinească îndatoririle și obligațiile conform cerințelor acestui Cod de Practici și Proceduri, în mod responsabil în orice situație posibilă. Un deținător de secret partajat trebuie să anunțe emitentul secretului în cazul furtului, pierderii, dezvăluirii neautorizate sau compromiterii

securității secretului, imediat după incident. Un deținător de secret partajat nu este responsabil pentru neîndeplinirea îndatoririlor/obligațiilor sale din cauza unor motive ce sunt imposibil de controlat de către acesta, dar este responsabil pentru dezvăluirea inoportună a secretului sau pentru neglijarea obligațiilor de a notifica emitentul secretului despre dezvăluirea inoportună sau violarea securității secretului ca urmare a greșelilor, neglijenței sau iresponsabilității deținătorului.

2.2.3 Backup-ul cheilor private

certSAFE Time Stamping Authority creează o copie de siguranță a cheilor private folosite la semnarea marcilor temporale. Copiile sunt folosite în cazul punerii în aplicare a procedurilor de urgență (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

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

- în cazul creării copiilor de siguranță 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,
- când este necesară transferarea unei chei private din modulul operațional folosit pentru operații standard ale entității, pe un alt modul; situația poate

apărea în cazul invocării planului de Disaster Recovery sau al necesității distrugerii modului operational.

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

Introducerea unei chei private în modulul hardware de securitate al TSU al certSAFE Time Stamping Authority necesită restaurarea cheii de pe carduri în prezența unui număr corespunzător de deținători de secrete partajate care protejează modulul ce conține cheile private.

2.2.5 Metoda de activare a cheii private

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

La import, generare sau restaurare cheia privata a unei unitati de marcare temporală este dezactivată. Cheia se activează prin pornirea serviciului.

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

Activarea cheilor private este întotdeauna precedată de autentificarea operatorului. Autentificarea este realizată pe baza unui card criptografic deținut de operator. După introducerea cardului în modulul criptografic și 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 certSIGN, dezactivarea unei chei private se face de către persoanele cu roluri de incredere numai în cazul în care serviciul este oprit pentru actualizari, mentenanta, sau alte motive.

2.3 Distribuirea cheilor publice ale certSAFE Time Stamping Authority

Certificatele corespunzatoare cheilor private de semnare a marcilor temporale emise de catre unitatile de marcare temporală (in prezent exista doar certSAFE Time Stamping Authority 1) sunt publicate pe site la adresa https://www.certsign.ro/certificate_digitale/lantul_de_incredere.htm.

2.4 Schimbarea cheilor certSAFE Time Stamping Authority

Perioada de valabilitate a certificatului asociat cheii private de semnare a marilor temporale este de 3 ani. Inainte cu cel putin 1 luna fata de expirarea certificatului se va genera o noua pereche de chei si un nou certificat.

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

2.5 Sfarsitul ciclului de viata al cheii private a TSU

certSAFE Time Stamping Authority a implementat proceduri tehnice si operationale pentru ca inainte de expirarea certificatului asociat cheii de semnare a unui TSU sa se genereze o noua pereche de chei si un nou certificat.

In momentul inlocuirii perechilor de chei, vechea cheie privata si orice secret partajat care ar permite recrearea ei sunt distruse.

Aplicatia care genereaza marcile temporale este conceputa in asa fel incat orice incercare de emitere a unei marci temporale dupa expirarea cheii private de semnare sa fie respinsa.

2.6 Distrugerea cheilor TSU

Distrugerea cheii private a unui TSU al certSAFE Time Stamping Authority presupune stergerea cardurilor care contin secretele partajate prin care este protejata cheia. Dupa stergerea lor, cheia este pierduta pentru totdeauna.

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

2.7 Managementul modulului hardware de securitate

certSAFE Time Stamping Authority se asigura ca :

- a) Integritatea modulelor criptografice de securitate nu a fost afectata in decursul transportului de la producator
- b) Integritatea modulelor criptografice de securitate nu a fost afectata in decursul stocarii premergatoare instalarii
- c) Instalarea, administrarea si operarea acestora este efectuata doar de personal de incredere
- d) Modulele criptografice de securitate functioneaza corect
- e) Cheile private de semnare stocate pe modulele criptografice de securitate sunt distruse in momentul scoaterii acestuia din productie

3 Inregistrarea evenimentelor

3.1 Înregistrarea evenimentelor

Pentru a gestiona eficient sistemele certSIGN și pentru a putea audita acțiunile utilizatorilor și personalului certSIGN, toate evenimentele care apar în sistem sunt înregistrate. Informațiile înregistrate alcătuiesc jurnalele (log-urile) de evenimente și trebuie păstrate în așa fel încât să permită Entităților Partenerere să acceseze informațiile corespunzătoare și necesare rezolvării disputelor și să detecteze tentativele de compromitere a securității certSIGN, iar auditorilor și autorității de supraveghere să verifice conformitatea cu cadrul legal și cu propriile politici și proceduri. Evenimentele înregistrate fac obiectul procedurilor de arhivare. Arhivele sunt păstrate în afara incintei certSIGN.

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

3.2 Tipuri de evenimente înregistrate

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

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 depășește această capacitate, este creată automat o nouă versiune de jurnal. Jurnalul anterior este arhivat și șters de pe disc.

Fiecare înregistrare, automată sau manuală, conține informații despre:

- tipul evenimentului,
- identificatorul evenimentului,
- data și ora apariției evenimentului,

- identificatorul persoanei responsabile de eveniment.

Conținutul înregistrărilor se refera la:

- alertele firewall-urilor și IDS-urilor,
- operațiile asociate emiterilor sau verficarilor marcilor temporale,
- modificări ale structurii hard sau soft,
- modificări ale rețelei și conexiunilor,
- înregistrările fizice în zonele securizate și violările de securitate,
- schimbările de parole, drepturi asupra codurilor PIN, rolurile personalului,
- accesul reușit și nereușit la baza de date și la aplicațiile serverului,
- generarea de chei
- schimbarea cheilor
- istoria creării copiilor de backup și a arhivelor cu înregistrări.
- fiecare cerere de marca temporală primită

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

Accesul la jurnalele de evenimente (log-uri) este permis în exclusivitate administratorului de securitate și 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 și descris

într-un jurnal. Procesul de verificare a jurnalului include verificarea unor eventuale falsificări, sau modificări și verificarea fiecărei alerte sau anomalii consemnată în log-uri. Orice acțiune executată ca rezultat al funcționării defectuoase detectate trebuie înregistrată în jurnal.

3.4 Perioada de retenție a jurnalelor de evenimente

Înregistrările evenimentelor sunt stocate în fișiere pe discul sistem până când acestea ajung la capacitatea maximă permisă. În tot acest timp sunt disponibile online, la cererile autorizate. După depășirea spațiului alocat, jurnalele sunt păstrate în arhive și pot fi accesate numai off-line.

Jurnalele arhivate sunt păstrate cel puțin 10 ani.

3.5 Protecția jurnalelor de evenimente

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

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 așa fel încât:

- este posibilă detectarea oricărei violări de integritate; acest lucru asigură faptul că înregistrările nu conțin goluri sau falsuri,

- nici o entitate nu are dreptul să modifice conținutul unui jurnal.

3.6 Procedurile de backup pentru jurnalele de evenimente

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

3.7 Notificarea entităților responsabile de tratarea evenimentelor

Modulul de analiză a jurnalului de evenimente implementat în sistem examinează evenimentele curente și sesizează automat activitățile suspecte sau pe cele care au ca scop compromiterea securității. În cazul activităților care au influență asupra securității sistemului, sunt notificați automat administratorul de securitate și 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 poștă electronică). Entitățile notificate iau măsurile corespunzătoare pentru a proteja sistemul față de amenințarea detectată.

3.8 Arhivarea înregistrărilor

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

Registrul on-line conține toate marcile temporale emise precum și date referitoare la marca și la certificatul folosit și poate fi accesat permanent pentru efectuarea unor servicii externe ale TSA certSIGN, de exemplu verificarea unei marci 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. Tehnologia folosită permite arhivarea înregistrărilor și restaurarea lor în siguranță pe perioade de timp de minim 50 de ani.

3.9 Perioada de păstrare a arhivelor

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

3.10 Procedurile de acces și verificarea informațiilor arhivate

Pentru a verifica integritatea informațiilor arhivate, datele sunt periodic testate. Această activitate poate fi realizată numai în prezența administratorului de securitate

și trebuie înregistrată în jurnalul de evenimente. Dacă sunt detectate deteriorări sau modificări ale datelor originale, acestea trebuie corectate cât mai repede posibil.

4 Managementul operational si al securitatii

SC certSIGN a implementat un sistem de management al securitatii informatice (SMSI, in sensul standardului ISO 27001) pentru toate procesele implicate in furnizarea de servicii de incredere (servicii de certificare si de marcare temporala la data prezentei).

4.1 Managementul Riscului

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

sc certSIGN srl a implementat un proces permanent de identificare si contracarare a riscurilor operationale si de securitate pentru toate serviciile pe care le furnizeaza in calitate de terta parte de incredere (servicii de certificare digitala si servicii de marcare temporala la data prezentei). Managementul riscului acopera toate sistemele si aplicatiile informatice, retelele de calculatoare, cladirile, camerele si personalul implicat in furnizarea acestor servicii, de-a lungul intregului lor ciclu de viata si identifica masurile necesare pentru reducerea sau eliminarea completa a oricaror evenimente nedorite legate confidentialitatea, integritatea si disponibilitatea informatiilor procesate si a serviciilor oferite.

4.2 Controale de securitate fizică, organizațională și de personal

Acest capitol descrie cerințele generale referitoare la organizarea activitatilor, la personal, cat si pe cele privind procesele de asigurare a securitatii fizice.

4.2.1 Masuri organizationale si procedurale

In firma a fost creata o structura de departamente si una de roluri care respecta principiul „separation of duties” si impiedica preluarea controlului unui intreg proces sau al unei activitati critice de catre o singura persoana. Exista un administrator de securitate si un Comitet pentru Managementul Securitatii. Fiecare anagajat este responsabilizat prin asumarea scrisa a fisei postului.

Pentru asigurarea securitatii informatiilor au fost identificate, implementate si sunt controlate prin SMSI urmatoarele procese:

- Planificarea strategica
- Managementul arhitecturii platformelor tehnologice
- Inventarul resurselor (informatii, software, echipamente, camere, cladiri)
- Clasificarea si gestiunea informatiei
- Utilizarea resurselor
- Managementul schimbarii
- Controlul accesului
- Relatiile cu tertii
- Managementul capacitatii
- Instruirea personalului
- Monitorizarea
- Securitatea fizica
- Continuitatea afacerii
- Tratarea incidentelor de securitate

Toate procesele identificate si implementate pentru asigurarea securitatii sunt controlate prin politici si proceduri specifice.

Planificarea strategica

Intreaga activitate a Autoritatii de Marcare Temporală este planificata anual si multianual prin stabilirea unor obiective in acord cu cadrul legislativ si normativ si cu cerintele pietei si prin alocarea de resurse care sa sustina atingerea acestor obiective.

Managementul arhitecturii platformelor tehnologice

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

Clasificarea si gestiunea resurselor

Toate resursele Autoritatii de Marcăre Temporală (informatii, sisteme si aplicatii) sunt inventariate periodic si clasificate din punct de vedere al securitatii si al importantei pentru business. Au fost puse la punct procese prin care gestiunea acestor resurse (intrare, iesire, stocare, transfer, utilizare) este strict controlata prin masuri direct proportionale cu clasificarea si importanta lor.

Managementul schimbarii

certSIGN foloseste un proces controlat pentru managementul schimbarilor. Fiecare aplicatie, înainte de a fi folosita în productie de certSIGN, este instalata astfel încât să se permită controlul versiunii curente și să se prevină instalarea neautorizată de programe sau falsificarea celor existente. Dezvoltarea, testarea si productia sunt

zone distincte, iar transferul informatiilor si aplicatiilor dintr-o zona in alta se face controlat.

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

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

Controlul accesului

Orice acces la o resursa se face printr-un proces controlat la care iau parte managerii, administratorii de sistem si administratorul de securitate. Se respecta principiile necesitatii de a cunoaste si a separarii rolurilor. Periodic se verifica ca drepturile de acces existente sunt corespunzatoare.

Relatiile cu tertii

Procesul se refera in primul rand la relatiile cu furnizorii de servicii si controlul sau presupune asigurarea securitatii informatiilor accesate de acestia.

Managementul capacitatii

Procesul prin care certSIGN urmareste permanent incarcarea sistemelor care furnizeaza serviciile de incredere pentru a asigura calitatea si performanetele asumate prin politici si prin contracte.

Instruirea personalului

Personalul angajat in furnizarea serviciilor este pregatit atat la angajare, cat si ulterior, periodic, pentru a avea competentele profesionale necesare si pentru a cunoaste si aplica toate politicile, procedurile si masurile tehnice operationale si de securitate.

Monitorizarea

Sistemele tehnologice, serviciile si personalul sunt permanent monitorizate pentru a asigura o calitate si o securitate a serviciilor care sa multumeasca clientii si sa asigure respectarea legilor, a normelor precum si a propriilor standarde.

Securitatea fizica

Accesul in incinta certSIGN este controlat atat printr-un sistem de control al accesului cu carduri de proximitate cat si, permanent, prin agenti de paza. Acelasi sistem cu carduri de acces controleaza accesul si in camerele cu resurse considerate critice. Exista sisteme de detectare a intruziunii si un sistem de monitorizare video cu circuit inchis.

Continuitatea afacerii

certSIGN a pregatit si testeaza anual un plan de asigurare a continuitatii afacerii care sa permita restaurarea rapida a tuturor serviciilor in cazul unor dezastre (incendii, cutremure etc). Exista de asemenea un complex de masuri preventive si corective care sa permita asigurarea unei disponibilitati maxime a serviciilor oferite (planuri de mentenanta, piese de schimb, redundanta a componentetelor critice, copii de siguranta a datelor, ghiduri de tratare a erorilor si avariilor etc)

Tratarea incidentelor de securitate

Toate sistemele critice si reseaua sunt monitorizate permanent si administratorii de sistem, ca si cel de securitate sunt alertati in timp real la aparitia oricarui incident. Exista planuri de interventie si de tratare a acestor incidente.

4.2.2 Controlul Personalului

Masuri generale pentru controlul personalului

certSIGN trebuie să se asigure că persoana care îndeplinește responsabilitățile funcției, conform cu rolul atribuit în cadrul Autoritatii de Marcare Temporală:

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

Personalul angajat al certSIGN care îndeplinește un rol de încredere, trebuie să obțină avizul administratorului de securitate.

Roluri de încredere

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

- **Administrator de securitate** – Responsabilitate globală pentru implementarea politicilor și procedurilor de securitate.
 - Inițiază instalarea, configurarea și managementul aplicațiilor software și hardware (inclusiv resursele de rețea) ale certSIGN; inițiază și suspendă serviciile oferite de certSIGN; coordonează administratorii, inițiază și supraveghează generarea de chei și secrete partajate; aproba drepturi din punct de vedere al securității și privilegiilor de acces ale utilizatorilor; verifică jurnalele de evenimente; supervizează auditurile interne și externe; primește și răspunde la rapoartele de audit; supervizează eliminarea deficiențelor constatate în urma auditului.
 - Supraveghează operatorii;
 - Verifică respectarea Politicii de Marcare Temporală și a Codului de Practici și Proceduri;
- **Administratorul de sistem** – Autorizat să instaleze, configureze și să administreze sistemele și aplicațiile Autorității de Marcare Temporală.

- **Operatorul de sistem** – Responsabil cu operarea zilnică a sistemelor si aplicatiilor Autorității de Marcare Temporală. Autorizat să execute operațiile de backup și restaurare a sistemului; transferă copiile de siguranță ale arhivei și ale datelor curente în afara locației certSIGN.
- **Administratorul HSM** – Administreaza modulul de securitate si creeaza carduri operatori
- **Operatorul HSM** – Porneste aplicatia de marcarea temporală
- **Administratorul registrului electronic** – se asigura ca toate inregistrarile sunt realizate si pastrate conform cu Politica de Marcare Temporală
- **Auditorul de sistem** – autorizat să acceseze arhivele și log-urile de audit ale sistemelor de încredere ale Autorității de Certificare. Responsabil de efectuarea de audituri interne pentru respectarea Codului de Practici și Proceduri de către Autoritatea de Certificare; această responsabilitate se extinde și asupra Autorității de Înregistrare care operează în cadrul certSIGN.

Numărul de persoane necesare pentru îndeplinirea unei sarcini

Procesul de generare de chei – pentru semnarea marilor temporale – este una din operațiile ce necesită o atenție deosebită. Generarea necesită prezența a cel puțin două persoane: un administrator de securitate și un administrator de sistem. La procesul de generare a cheii unui TSU participa de asemenea posesorii de secrete partajate care păstrează partea lor de cheie în locații sigure.

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

Activarea cheii private necesita cvorumul conform cu schema prag, asta inseamna ca prezenta detinatorilor de secrete partajate este necesara si de fiecare data cand e repornit serviciul.

Orice altă operațiune sau rol, descris în cadrul CPP-ului poate fi efectuată de o singură persoană, special desemnată în acest sens.

Identificarea și autentificarea pentru fiecare rol

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

- Nume si parola
- Cheie privata stocata electronic si PIN
- Cheie privata stocata hardware (pe un dispozitiv criptografic) si PIN
- Card de acces cu poza

Fiecare cont asignat:

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

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

Cerințele de pregătire a personalului

Personalul care îndeplinește roluri și sarcini ca urmare a asumarii unui rol din cadrul Autoritatii de Marcare Temporală, trebuie să fie instruit cu privire la:

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

Sanționarea acțiunilor neautorizate

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

Personalul angajat pe baza de contract

Personalul angajat pe baza de contract (servicii externe, dezvoltatori de subsisteme sau aplicații etc.) respecta aceleași măsuri de securitate ca și personalul permanent. În plus, personalul angajat pe bază de contract, pe timpul cât își desfășoară activitatea în locația certSIGN, trebuie permanent însoțit de către un angajat al certSIGN , cu excepția celor care au primit avizare din partea administratorului de

securitate și care poate accesa informații clasificate intern sau în conformitate cu normele legale în vigoare.

4.2.3 Controale de securitate fizică

Sistemele de calcul, terminalele operatorilor și resursele informaționale ale certSIGN sunt dispuse în zone dedicate, protejate fizic împotriva accesului neautorizat, distrugerilor sau perturbării activității. Aceste locații sunt monitorizate. Fiecare intrare și ieșire este înregistrată în jurnalul de evenimente (log-urile sistemului); stabilitatea surselor de electricitate precum și temperatura sunt de asemenea monitorizate și controlate.

Amplasarea locației

certSIGN este localizată în București, la următoarea adresă: Sos Oltenitei nr. 107A, C1, parter.

Accesul fizic

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

Sediul certSIGN este deschis publicului în fiecare zi lucrătoare între 10:00 și 18:00. În restul timpului, accesul este permis numai persoanelor autorizate de către conducerea certSIGN. Vizitatorii spațiilor aparținând certSIGN trebuie să fie însoțiți permanent de persoane autorizate.

Zonele ocupate de certSIGN se împart în:

- zona serverelor,
- zona operatorilor

- zona administratorilor,
- zona de dezvoltare și testare
- zona office.

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

Controlul accesului în *zonele operatorilor si administratorilor* se face prin intermediul cardurilor și a cititoarelor de carduri. Deoarece toate informațiile senzitive sunt protejate prin folosirea unor seifuri, iar accesul la terminalele operatorilor și administratorilor necesită în prealabil autorizarea acestora, securitatea fizică în această zonă este considerată ca fiind adecvată. În această zonă au acces numai angajații certSIGN și persoanele autorizate; ultimilor nu le este permisă prezența în zonă neînsoțiți.

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

Sursa de alimentare cu electricitate și aerul condiționat

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

Expunerea la apă

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

Prevenirea incendiilor

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

Depozitarea mediilor de stocare a informațiilor

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

Aruncarea deșeurilor

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

Depozitarea backup-urilor în afara locației

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

Stocarea în afara locației se aplică și în cazul arhivelor, copiilor curente ale informațiilor procesate de sistem și kit-urilor de instalare ale aplicațiilor certSIGN. Acest lucru permite refacerea de urgență a oricărei funcții a certSIGN în termenele stabilite prin planul de asigurare a continuitatii afacerii.

4.3 Controalele tehnice

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

Calculatoarele aparținând Autorității de Marcare Temporală dispun de următoarele mijloace de securitate:

- autentificarea obligatorie la nivelul sistemului de operare și al aplicațiilor,
- control discreționar al accesului,
- posibilitatea de a fi auditate din punct de vedere al securității,
- calculatorul este accesibil doar personalului autorizat, cu roluri de încredere în certSIGN ,
- separarea sarcinilor, conform rolului în cadrul sistemului,
- identificarea și autentificarea rolurilor și a personalului care îndeplinește aceste roluri,
- prevenirea refolosirii unui obiect de către un alt proces după eliberarea acestuia de către procesul autorizat,
- protecția criptografică a schimburilor de informații și protecția bazelor de date,

- arhivarea istoricului operațiunilor executate pe un calculator și a datelor necesare auditării,
- o cale sigură ce permite identificarea și autentificarea rolurilor și a personalului care îndeplinește aceste roluri,
- metode de restaurare a cheilor (numai în cazul modulelor hardware de securitate), a aplicațiilor și a sistemului de operare,
- mijloace de monitorizare și alertare în cazul accesului neautorizat la resursele de calcul.

4.3.1 Controale de securitatea a rețelei

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

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

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

4.3.2 Standardele tehnice aplicabile

Solicitarile de marcare temporală se realizează conform....

Răspunsurile la solicitările de marcare temporală se formează conform..

CODUL DE PRACTICI SI PROCEDURI pt SERVICIILE DE MARCARE TEMPORALĂ

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

Profilul certificatului digital emis pentru certSAFE Time Stamping Authority respectă recomandările IETF din RFC 3161 și RFC 2459, Internet X.509 Public Key Infrastructure Certificate

Modulul hardware de securitate (HSM) utilizat în cadrul TSU al certSAFE Time Stamping Authority respectă standardul NIST FIPS 140-2 Security Requirements for Cryptographic Modules.

În crearea semnăturii electronice a marilor temporale se respectă standardul IETF RFC 2630 Cryptographic Message Syntax .

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

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

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

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

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

Managementul securității certSAFE Time Stamping Authority este asigurat conform standardelor ISO 27001:2005, Information technology -- Security techniques -- Information security management systems – Requirements și ISO 27002,

CODUL DE PRACTICI SI PROCEDURI pt SERVICIILE DE MARCARE TEMPORALĂ

Information technology -- Security techniques -- Code of practice for information security management.

4.4 Timpul

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

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

Aplicatia software care emite marcile temporale este realizată astfel ca la orice desincronizare care depășește precizia asumată să oprească emiterea de marci. Dacă totuși se constată că s-au emis marci temporale care încălcă precizia asumată, atât abonatii care au primit acele marci cât și autoritatea de supraveghere sunt notificați.

4.5 Evaluarea securității sistemelor informatice

Sistemele de calcul certSIGN 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), CEN CWA 14167 (Cerințele de Securitate pentru Sistemele de Încredere care asigură Managementul certificatelor pentru Semnatura Electronică) și ISO 27002.

5 Managementul Codului de Practici și Proceduri

Fiecare versiune a Codului de Practici și Proceduri este în vigoare (starea sa este **valida**) până în momentul publicării și aprobării noii sale versiuni. O nouă versiune este dezvoltată de către certSIGN și publicată pentru comentarii cu mențiunea **spre aprobare** (daca este cazul). După primirea și includerea comentariilor, Codul de Practici și Proceduri intra în procedura de aprobare internă. Responsabil de aprobarea formei finale a Codului de Practici și Proceduri este un comitet format din directorul general, directorul general adjunct, managerii departamentelor tehnice și managerul departamentului de dezvoltare a afacerii. Responsabil pentru întreținerea Codului de Practici și Proceduri este managerul departamentului care asigură furnizarea serviciilor de marcă temporală. După terminarea procedurii de aprobare, noua versiune a CPP este transmisă Autorității de Reglementare și Supraveghere și apoi, în termen de 10 zile, este publicată și marcată ca fiind în starea **validă**. Regulile și cerințele descrise mai jos, cu privire la managementul Codului de Practici și Proceduri guvernează și managementul Politicii de certificare.

Abonații trebuie să respecte numai Politica de certificare și Codul de Practici și Proceduri în vigoare în momentul respectiv.

5.1 Procedura de schimbare a CPP

Modificarea Codului de Practici și Proceduri poate fi rezultatul depistării unor erori, actualizării sale sau a sugestiilor primite din partea entităților interesate. Propunerile de modificare pot fi trimise prin poștă sau e-mail pe adresa certSIGN. Propunerile de

modificare trebuie să descrie modificările necesare, motivele acestor modificări și să ofere mijloace de contact ale persoanei care solicită modificarea.

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

Modificările introduse pot fi în general împărțite în două categorii: una care nu necesită consultarea Abonaților și una care cere (de obicei în avans) consultarea Abonaților. Prima categorie include modificari de urgenta sau modificari neesentiale.

5.2 Procedurile de publicare și notificare

O copie a Codului de Practici și Proceduri este disponibilă în formă electronică pe site-ul de Web <http://www.certSIGN.ro/repository> sau prin e-mail la adresa office@certSIGN.ro. Trei versiuni ale Codului de Practici și Proceduri sunt întotdeauna disponibile în Depozit și prin e-mail: versiunea în vigoare, versiunea anterioară și 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 și Proceduri, certSIGN nu primește remarci semnificative cu privire la aceste schimbări, noua versiune a Codului de Practici și Proceduri, aflata în starea **spre aprobare**, devine documentul care guvernează politica de certificare și trebuie respectat de toți Abonații certSIGN iar starea acestei versiuni va fi schimbată în **validă**.

Abonații care nu acceptă noul Cod de Practici și Proceduri, conținând termenii și reglementările modificate, sunt obligați să depună, în termen de 15 zile de la data la

CODUL DE PRACTICI SI PROCEDURI pt SERVICIILE DE MARCARE TEMPORALĂ

care noua versiune a Codului de Practici și Proceduri a fost aprobată, o declarație în acest sens. Acest lucru duce la încetarea contractului de presari servicii de certificare și la revocarea certificatului emis în baza acestuia.

Anexa 1: Glosar

Abonat - o persoana juridica cu mai multi utilizatori sau o persoana fizica, utilizator individual;

Acces – abilitatea de a folosi o resursă informaționala din sistem

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

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

A autentifica – a confirma identitatea declarată a unei entități

Autentificare – controlul de securitate cu scopul de a oferi siguranță și încredere datelor transferate, mesajelor sau emitenților lor; controalele de verificare a autenticității unei persoane, înainte de a-i livra un tip de informații secreta

Autoritatea de Marcare Temporală – 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 îndeplinește următoarele condiții:

- 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 intersecția politicilor a căror identificatori sunt incluși în fiecare certificat, încorporate în calea de certificare și definite în extensia certificatePolicies.

CODUL DE PRACTICI SI PROCEDURI pt SERVICIILE DE MARCARE TEMPORALĂ

certificatul de cheie publică – o structura de date care conține cel puțin numele sau identificatorul unei Autorități de Certificare , identificatorul unui Abonat, cheia sa publică, perioada de validitate, numărul serial și cel asignat de către Autoritatea de Certificare. Un certificat poate fi în una din trei stări fundamentale: în așteptarea activării, activ și 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) și (3) nu a fost revocat.

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

Cheie secretă - cheie folosită în tehnicile criptografice simetrice, cunoscuta doar de un grup de Abonați autorizați.

Cheie privată – una dintre cheile asimetrice aparținând unui Abonat și 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 semnatura pentru uzul exclusiv al proprietarului; (2) acea cheie din pereche 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 definește transformarea de verificare a semnăturii. În cazul criptării asimetrice, cheia publică definește transformarea de criptare a mesajelor.

Control al accesului – procesul de acordare a accesului la resursele informaționale de sistem numai utilizatorilor autorizați, aplicațiilor, proceselor și altor sisteme.

Deținător de secret partajat – deținător autorizat al unui card electronic folosit pentru păstrarea secretului partajat.

Entitate partenera – utilizatori de marci temporale

Furnizor de servicii de certificare – instituție de încredere (inclusiv dispozitivele hardware aflate sub controlul sau) care face parte dintre terții de încredere și care furnizează servicii capabile să creeze, să semneze și să emită certificate sau servicii de ne-repudiare.

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

Infrastructura de cheie publică (PKI) – arhitectura, tehnicile, practicile și procedurile care contribuie în mod colectiv la implementarea și funcționarea sistemelor criptografice cu chei publice, bazate pe certificate; PKI constă în hardware și software, baze de date, resurse de rețea, proceduri de securitate și obligații legale, legate împreună și care colaborează pentru a furniza și implementa atât

CODUL DE PRACTICI SI PROCEDURI pt SERVICIILE DE MARCARE TEMPORALĂ

CODUL DE PRACTICI SI PROCEDURI pt SERVICIILE DE MARCARE TEMPORALĂ

serviciile de certificare cât și 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 și datele și motivele revocării sau suspendării lor.

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

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

Perioada de activitate a certificatului – perioada dintre începutul și sfârșitul validității unui certificat sau perioada dintre data de începere a validității certificatului și 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 situațiile de urgență - procedura alternativă la cea standard, care se execută la apariția unei situații de urgență.

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

Revocarea unui certificat – definește procedurile privind revocarea unei perechi de chei valide (revocarea de certificat) în cazul în care accesul la perechea de chei trebuie restricționat pentru a preveni posibila utilizare a sa în criptarea sau crearea de semnatura electronica. 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 așa fel încât este nevoie de m părți ale secretului (unde $m < n$) pentru a restaura cheia distribuită.

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

CODUL DE PRACTICI SI PROCEDURI pt SERVICIILE DE MARCARE TEMPORALĂ

CODUL DE PRACTICI SI PROCEDURI pt SERVICIILE DE MARCARE TEMPORALĂ

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

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

- **în așteptarea activării (pregătită)** – cheia a fost deja generată dar nu est încă disponibilă pentru folosire;
- **activă** – cheia poate fi folosită în operațiuni criptografice (de ex. pentru crearea de semnături electronice);
- **inactivă** – cheia poate fi folosită exclusiv pentru decriptare sau perechea ei publica pentru verificarea de semnături electronice.

Marca temporală. Structura de date care leaga reprezentarea unor date electronice de un anumit timp, stabilind astfel dovada ca 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 concordanță cu procedurile acceptate; procesul poate include proceduri de testare cu scopul de a îmbunătăți calitatea cheii;
- activarea – are ca rezultat devenirea validă a unei chei și disponibilă pentru executarea de operații criptografice;
- dezactivarea – restrângerea unei chei; poate să apară la expirarea perioadei de validitate a cheii;
- reactivarea – permite folosirea în continuarea a unei chei aflata în starea de indisponibilitate pentru executarea de operații criptografice;
- distrugerea – are ca rezultat terminarea ciclului de viață al cheii; această noțiune se referă la distrugerea logică a cheii dar poate fi aplicată și la distrugerea ei fizică.

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 și autentificarea.

TSA – Autoritatea de Marcare Temporală. În 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) în condiții stabilite prin Politica de Marcare temporală și Codul de Practici și Proceduri, pentru a furniza serviciile de marcă temporală.

CODUL DE PRACTICI SI PROCEDURI pt SERVICIILE DE MARCARE TEMPORALĂ

CODUL DE PRACTICI SI PROCEDURI pt SERVICIILE DE MARCARE TEMPORALĂ

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

Validarea certificatelor de cheie publică – verificarea stării unui certificat, care permite stabilirea dacă certificatul este revocat sau nu. Această problemă poate fi rezolvată pe baza CRL-ului sau printr-o cerere trimisă direct serverului OCSP.