



CODUL DE PRACTICI ȘI PROCEDURI AL AUTORITĂȚII DE MARCARE TEMPORALĂ A ALFATRUST CERTIFICATION S.A.

Cuprins

1. Prezentare document	4
2. Managementul securității informației (InfoSEC)	4
2.1. Măsurile de securitate a personalului	5
2.1.1. Roluri de încredere	6
2.1.2. Numărul de persoane necesare pentru îndeplinirea unei sarcini	6
2.1.3. Identificarea și autentificarea pentru fiecare rol	7
2.1.4. Cerințele de pregătire a personalului	7
2.1.5. Sancționarea acțiunilor neautorizate	7
2.1.6. Personalul angajat pe baza de contract.....	8
2.2. Măsurile de securitate fizică.....	8
2.2.1. Accesul fizic.....	8
2.2.2. Energie și climatizare	9
2.2.3. Expunerea la apă.....	9
2.2.4. Prevenirea și protecția împotriva incendiilor	9
2.2.5. Mediile de stocare	9
2.2.6. Aruncarea lucrurilor nefolositoare	10
2.2.7. Depozitarea backup-urilor în afara locației	10
2.3. Măsurile de securitate CompuSEC.....	10
2.3.1. Cerințele de securitate specifice.....	10
2.3.2. Evaluarea securității calculatoarelor	11
2.3.3. Controale pentru managementul securității informației	11
2.3.4. Controale de securitate a rețelei	11
2.3.5. Sincronizarea bazei de timp.....	11
2.4. Măsurile de securitate criptografice.....	12
2.4.1. Generarea cheilor unităților de marcare temporală	12
2.4.2. Protecția cheilor private ale Autorităților de Marcare Temporală	12
2.4.2.1. Standarde pentru modulele criptografice	12
2.4.2.2. Controlul dual al accesului la cheia privată	12
2.4.2.2.1. Acceptarea păstrării secretului de către deținători.....	12
2.4.2.2.2. Protecția secretului partajat	13
2.4.2.3. Copia de siguranță a cheilor private	13

2.4.2.4. Introducerea cheii private în modulul criptografic.....	13
2.4.2.5. Activarea cheii private	14
2.4.2.6. Dezactivarea cheii private.....	14
2.4.3. Distribuirea cheilor publice ale Autorităților de Marcare Temporală	14
2.4.4. Schimbarea cheilor Autorităților de Marcare Temporală	14
2.4.5. Sfârșitul ciclului de viață al cheii private a Autorității de Marcare Temporală.....	14
2.4.6. Distrugerea cheilor Autorităților de Marcare Temporală.....	15
2.4.7. Managementul modulului hardware de securitate.....	15
2.5. Înregistrarea evenimentelor	15
2.5.1. Tipuri de evenimente înregistrate	15
2.5.2. Frecvența analizei jurnalelor de evenimente	16
2.5.2. Perioada de retenție a jurnalelor de evenimente	17
2.5.3. Protecția jurnalelor de evenimente.....	17
2.5.4. Procedurile de backup pentru jurnalele de evenimente	17
2.5.5. Notificarea entităților responsabile de tratarea evenimentelor	17
2.5.6. Arhivarea înregistrărilor.....	17
2.5.7. Perioada de păstrare a arhivelor	18
2.5.8. Procedurile de acces și verificarea informațiilor arhivate	18
3. Managementul Codului de Practici și Proceduri.....	18
3.1. Procedura de modificare a CPP	18
3.2. Publicarea CPP-ului	19
3.2.1. Documente ce nu se publică în CPP.....	19

1. Prezentare document

Codul de Practici si Proceduri este o descriere detaliată a termenilor și condițiilor în care se furnizează serviciile, ca și a practicilor manageriale si operaționale pe care le urmeaza Autoritatea de Marcare Temporală (AMT) operată de AlfaTrust Certification S.A. în furnizarea serviciilor de marcare temporală.

Codul de Practici si Proceduri descrie cum anume AlfaTrust Certification S.A. implementează cerințele tehnice, procedurale si organizaționale stabilite prin Politica de Marcare Temporală.

2. Managementul securității informației (InfoSEC)

AlfaTrust Certification S.A. a implementat un sistem de management al securității informației (în sensul standardului ISO 27001) pentru toate procesele implicate în furnizarea de servicii de încredere (servicii de certificare și de marcare temporală).

AlfaTrust Certification S.A. a implementat un proces permanent de identificare si contracarare a riscurilor operaționale și de securitate pentru toate serviciile pe care le furnizează în calitate de terță parte de încredere (servicii de certificare și servicii de marcare temporală).

Managementul riscului acoperă toate sistemele si aplicațiile informatice, rețelele de calculatoare, clădirile, camerele și personalul implicat în furnizarea acestor servicii, de-a lungul întregului lor ciclu de viață și identifică măsurile necesare pentru reducerea sau eliminarea completă a oricărui evenimente nedorite legate de confidențialitatea, integritatea și disponibilitatea informațiilor procesate și a serviciilor oferite.

Garantarea atingerii obiectivelor InfoSEC asumate se realizează prin implementarea următoarelor strategii de lucru:

- ✓ **Planificarea strategică** = Intreaga activitate a Autorității de Marcare Temporală operată de AlfaTrust Certification S.A. este planificată anual și multianual prin stabilirea unor obiective în acord cu cadrul legislativ și normativ și cu cerințele pieței și prin alocarea de resurse care să susțină atingerea acestor obiective.
- ✓ **Managementul arhitecturii platformelor tehnologice** = Sistemele tehnologice folosite pentru oferirea serviciilor de marcare temporală sunt realizate (eventual achiziționate) și actualizate printr-un proces care implică cooperarea dintre toate departamentele implicate (vânzări, dezvoltare, operare și suport).
- ✓ **Clasificarea și gestiunea resurselor** = Toate resursele Autorității de Marcare Temporală (informații, sisteme și aplicații) sunt inventariate periodic și clasificate din punct de vedere al securității și al importanței pentru business. Au fost puse la punct procese prin care gestiunea acestor resurse (intrare, ieșire, stocare, transfer, utilizare) este strict controlată prin măsuri direct proporționale cu clasificarea și importanța lor.
- ✓ **Managementul schimbării** = AlfaTrust Certification S.A. folosește un proces controlat pentru managementul schimbărilor. Fiecare aplicație, înainte de a fi folosită în producție este instalată astfel încât să se permită controlul versiunii curente și să se prevină instalarea neautorizată de programe sau falsificarea celor existente. Dezvoltarea, testarea si producția sunt zone distincte, iar transferul informațiilor și aplicațiilor dintr-o zonă în 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 resursă se face printr-un proces controlat la care iau parte managerii, administratorii de sistem și administratorul de securitate. Se respectă principiile necesității de a cunoaște (*need to know*) și a separării rolurilor (*segregation of duties*). Periodic se verifică că drepturile de acces existente sunt corespunzătoare.
- ✓ **Relațiile cu terții** = Procesul se referă în primul rând la relațiile cu furnizorii de servicii și presupune asigurarea securității informațiilor accesate de aceștia.
- ✓ **Managementul capacității** = Procesul prin care AlfaTrust Certification S.A. urmărește permanent încărcarea sistemelor care furnizează serviciile de încredere pentru a asigura calitatea și performanțele asumate prin politici și prin contracte. Personalul angajat în furnizarea serviciilor este pregătit atât la angajare, cât și ulterior, periodic, pentru a avea competențele profesionale necesare și pentru a cunoaște și aplica toate politicile, procedurile și măsurile tehnice operaționale și de securitate.
- ✓ **Monitorizarea** = Sistemele tehnologice, serviciile și personalul sunt permanent monitorizate pentru a asigura o calitate și o securitate a serviciilor care să mulțumească clienții și să asigure respectarea legilor, a normelor, precum și a propriilor standarde.
- ✓ **Securitatea fizică** = Accesul în incinta AlfaTrust Certification S.A. este controlat atât printr-un sistem de control al accesului cu carduri de proximitate cât și prin agenți de pază. Același sistem cu carduri de acces controlează accesul și în camerele cu resurse considerate critice. Există sisteme de detectare a intruziunii și un sistem de monitorizare video cu circuit închis.
- ✓ **Continuitatea afacerii** = AlfaTrust Certification S.A. a pregătit și testează anual un plan de asigurare a continuității afacerii care să permită restaurarea rapidă a tuturor serviciilor în cazul unor dezastre (incendii, cutremure etc). Există de asemenea un complex de măsuri preventive și corective care să permită asigurarea unei disponibilități maxime a serviciilor oferite (planuri de mentenanță, piese de schimb, redundanță a componentelor critice, copii de siguranță a datelor, ghiduri de tratare a erorilor și avariilor, etc.).
- ✓ **Tratarea incidentelor de securitate** = Toate sistemele critice și rețeaua sunt monitorizate permanent și administratorii de sistem, ca și cel de securitate sunt alertați în timp real la apariția oricărui incident. Există planuri de intervenție și de tratare a acestor incidente.

2.1. Măsuri de securitate a personalului

AlfaTrust Certification S.A. se asigură că persoana care îndeplinește responsabilitățile funcției, conform cu rolul atribuit în cadrul Autorității 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 și a datelor confidențiale și private ale abonaților,
- nu îndeplinește sarcini care pot genera conflicte de interese.

Personalul angajat al AlfaTrust Certification S.A. care îndeplinește un rol de încredere, trebuie să obțină avizul administratorului de securitate.

2.1.1. Roluri de încredere

În AlfaTrust Certification S.A. sunt definite următoarele roluri de încredere, care pot fi atribuite uneia sau mai multor persoane:

- A. **Administrator de securitate** – Responsabilitate globală pentru implementarea politicilor și procedurilor de securitate.
 - a. Inițiază instalarea, configurarea și managementul aplicațiilor software și hardware (inclusiv resursele de rețea) ale AlfaTrust;
 - b. Inițiază și suspendă serviciile oferite de AlfaTrust;
 - c. Coordonează administratorii,
 - d. Inițiază și supraveghează generarea de chei și secrete partajate;
 - e. Aprobă drepturi din punct de vedere al securității și privilegiilor de acces ale utilizatorilor;
 - f. Verifică jurnalele de evenimente;
 - g. Supervizează auditurile interne și externe;
 - h. Primește și răspunde la rapoartele de audit;
 - i. Supervizează eliminarea deficiențelor constatate în urma auditului;
 - j. Supraveghează operatorii;
 - k. Verifică respectarea Politicii de Marcare Temporală și a Codului de Practici și Proceduri a Autorității de Marcare Temporală;
- B. **Administratorul de sistem** – Autorizat să instaleze, configureze și să administreze sistemele și aplicațiile Autorității de Marcare Temporală.
- C. **Operatorul de sistem** – Responsabil cu operarea zilnică a sistemelor și aplicațiilor 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 AlfaTrust.
- D. **Administratorul HSM** – Administrează modulul de securitate și creează carduri operatori.
- E. **Operatorul HSM** – Pornește aplicația de marcarea temporală.
- F. **Administratorul registrului electronic** – se asigură că toate înregistrările sunt realizate și păstrate conform cu Politica de Marcare Temporală.
- G. **Auditorul de sistem** – autorizat să acceseze arhivele și log-urile de audit ale sistemelor de încredere ale Autorității de Marcare Temporală. Responsabil de efectuarea de audituri interne pentru respectarea Codului de Practici și Proceduri.

2.1.2. Numărul de persoane necesare pentru îndeplinirea unei sarcini

Procesul de generare de chei pentru semnarea mărcilor 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 unei Autorități de Marcare temporală participă 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 (HSM).

Activarea cheii private necesită cvorumul conform cu schema prag, asta înseamnă că prezența deținătorilor de secrete partajate este necesară și de fiecare dată când 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.

2.1.3. Identificarea și autentificarea pentru fiecare rol

Personalul AlfaTrust Certification S.A. este supus identificării și autentificării ori de câte ori accesează o cameră sau un sistem informatic prevăzute cu sisteme de control al accesului. Identificarea și autentificarea se fac prin una din următoarele metode, sau printr-o combinație a lor:

- Nume și parolă
- Cheie privată stocată electronic și PIN
- Cheie privată stocată hardware (pe un dispozitiv criptografic) și 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 persoană

respectivă) pe baza software-ului de sistem al AlfaTrust, a sistemului de operare și a controalelor de aplicații.

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

2.1.4. Cerințele de pregătire a personalului

Personalul care îndeplinește roluri și sarcini ca urmare a asumării unui rol din cadrul Autorității 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.

2.1.5. Sancționarea acțiunilor neautorizate

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

2.1.6. Personalul angajat pe baza de contract

Personalul angajat pe bază de contract (servicii externe, dezvoltatori de subsisteme sau aplicații etc.) respectă aceleași măsuri de securitate ca și personalul permanent.

În plus, personalul angajat pe bază de contract, pe timpul cât își desfășoară activitatea în locația AlfaTrust, trebuie permanent însoțit de către un angajat al AlfaTrust Certification S.A., cu excepția celor care au primit aviz din partea administratorului de securitate și care pot accesa informații clasificate intern sau în conformitate cu normele legale în vigoare.

2.2. Măsuri de securitate fizică

Sistemele de calcul, terminalele operatorilor și resursele informaționale ale AlfaTrust Certification sunt dispuse într-o zonă dedicată, protejată fizic împotriva accesului neautorizat, distrugerilor sau perturbării activității. Aceste locații sunt monitorizate. Fiecare intrare și ieșire este înregistrată în jurnalul de evenimente (log-urile sistemului); stabilitatea sursei de electricitate precum și temperatura sunt de asemenea monitorizate și controlate.

2.2.1. Accesul fizic

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

Sediul AlfaTrust Certification și Autoritatea de Marcare Temporală sunt accesibile publicului în fiecare zi lucrătoare între 10:00 și 16:00. În restul timpului (inclusiv în zilele nelucrătoare), accesul este permis numai persoanelor autorizate de către conducerea AlfaTrust Certification. Vizitatorii locațiilor aparținând AlfaTrust Certification trebuie să fie însoțiți permanent de persoane autorizate.

Zonele ocupate de AlfaTrust Certification se împart în:

- ❖ **Zona de securitate clasa I** – nu este permis accesul (nici măcar însoțit) al nici unei persoane (vizitator, client sau personal al AlfaTrust Certification) cu excepția administratorilor de securitate și administratorilor de sistem. Persoanele autorizate de a pătrunde în această zonă de securitate nu vor intra niciodată singure ci vor respecta condiția de acces de minim 2 persoane (“four eyes or two men rule”). Această zonă de securitate este compusă din:

- zona serverelor și a echipamentelor de comunicații,
- zona administratorilor Autorităților de Marcare temporală.

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 Autorității de Marcare Temporală și administratorul de sistem. Monitorizarea drepturilor de acces se face folosind carduri și cititoare, montate lângă punctul de acces. Fiecare intrare și ieșire din zonă este înregistrată automat în jurnalul de evenimente.

- ❖ **Zona de securitate clasa a II-a** – în aceste zone este permis accesul numai persoanelor autorizate de conducerea AlfaTrust Certification, accesul și activitatea în aceste zone conformându-se principiului compartimentării muncii și a principiului nevoii de a cunoaște “need to know”. Această zonă este compusă din:

- zona operatorilor Autorității de Marcare Temporală și administratorilor,

- zona de dezvoltare și testare,
- zona de depozitare a echipamentelor informatice, de comunicații sau criptografice.

Controlul accesului în zona operatorilor și administratorilor se face prin intermediul cardurilor și a cititoarelor de carduri. Deoarece toate informațiile sensitive sunt protejate prin folosirea unor seifuri, iar accesul la terminalele operatorilor și administratorilor necesită în prealabil autorizarea acestora, securitatea fizică în această zonă este considerată ca fiind adecvată. Cheile de acces pot fi ridicate numai de personalul autorizat. În această zonă au acces numai angajații AlfaTrust Certification 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. Dacă este necesar un altfel de acces, atunci el se poate face numai în prezența administratorului de securitate. Proiectele în curs de implementare și software-ul aferent este testat în mediul de dezvoltare al AlfaTrust Certification.

- ❖ **Zone administrative** – în această categorie intră orice alte zone din locația Furnizorului de Servicii de Marcare Temporală AlfaTrust Certification ce nu se încadrează în primele două clase de zone de securitate. În zonele administrative nu este permis accesul vizitatorilor sau a clienților decât dacă sunt însoțiți de personal al AlfaTrust Certification. Aceste zone se compun din:
 - birourile personalului,
 - zonele de primire a clienților AlfaTrust Certification.

2.2.2. Energie și climatizare

Zona operatorilor și administratorilor, precum și zona de dezvoltare și testare sunt prevăzute cu surse de climatizare a mediului ambiental. Din momentul întreruperii alimentării cu energie, sursele de electricitate de urgență (UPS) permit continuarea neperturbată a activității până la intervenția automată a grupului electrogen ce deservește toate facilitățile AlfaTrust Certification.

2.2.3. Expunerea la apă

AlfaTrust Certification și-a luat precauții deosebite pentru a minimiza impactul expunerii la apă a sistemelor AlfaTrust Certification.

2.2.4. Prevenirea și protecția împotriva incendiilor

AlfaTrust Certification și-a luat precauții deosebite pentru a preveni și a stinge focul sau alte expuneri la flacără sau fum. Măsurile AlfaTrust Certification de prevenire și protecție împotriva focului au fost stabilite pentru a respecta reglementările cu privire la prevenirea și stingerea incendiilor și siguranța la foc.

2.2.5. Mediile de stocare

Toate mediile în care există software de producție și date, verificare, arhivă sau informații salvate se află în locațiile AlfaTrust Certification sau într-o locație off-site de înmagazinare securizată cu controale de acces fizic și logic, pentru a limita accesul numai pentru personalul autorizat și pentru a proteja aceste medii împotriva pagubelor accidentale (cauzate de apă, foc sau câmp electromagnetic).

2.2.6. Aruncarea lucrurilor nefolositoare

Documentele și materialele sensibile sunt distruse (tocate) înainte de a fi aruncate. Mijloacele folosite pentru a strânge sau a transmite informațiile sensibile nu mai pot fi citite, înainte de a fi aruncate. Înainte de a fi aruncate, dispozitivele criptografice sunt distruse fizic sau șterse într-o manieră sigură, în concordanță cu îndrumările anterioare ale producătorului. Alte lucruri nefolositoare sunt aruncate, ținând cont de cerințele AlfaTrust Certification.

2.2.7. Depozitarea backup-urilor în afara locației

Copiile parolelor, codurile PIN și cardurile criptografice sunt stocate în containere speciale, situate în afara locației AlfaTrust Certification.

Stocarea în afara locației se aplică și în cazul arhivelor, copiilor curente ale informațiilor procesate de sistem și kit-urilor de instalare ale aplicațiilor AlfaTrust Certification. Acest lucru permite refacerea de urgență a oricărei funcții a AlfaTrust Certification în 48 de ore, în locația principală a AlfaTrust Certification, sau în locația auxiliară.

2.3. Măsurile de securitate CompuSEC

Sarcinile angajaților, colaboratorilor sau entităților partenere Furnizorului de Servicii de Marcare Temporală care lucrează în mediul AlfaTrust Certification sunt realizate prin intermediul unor dispozitive hardware (sisteme informatice și de comunicații, dispozitive criptografice, etc.) și aplicații software de încredere.

2.3.1. Cerințele de securitate specifice

Cerințele tehnice prezentate în acest capitol se referă la controalele de securitate specifice calculatoarelor, rețelelor de calculatoare și aplicațiilor folosite în mediul AlfaTrust Certification. 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 AlfaTrust Certification S.A. și componentele asociate acestora au implementate următoarele măsuri (controale) 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 AlfaTrust Certification,
- separarea sarcinilor, conform rolului în cadrul sistemului,
- identificarea și autentificarea rolurilor și a personalului care îndeplinește aceste roluri,
- prevenirea refolosirii unui obiect de către un alt proces după eliberarea acestuia de către procesul autorizat,
- protecția criptografică a schimburilor de informații și protecția bazelor de date,
- arhivarea istoricului operațiunilor executate pe un calculator și a datelor necesare auditării,
- o cale sigură ce permite identificarea și autentificarea rolurilor și a personalului care îndeplinește aceste roluri,

- metode de restaurare a cheilor (numai în cazul modulelor hardware de securitate), a aplicațiilor și a sistemului de operare,
- mijloace de monitorizare și alertare în cazul accesului neautorizat la resursele de calcul.

2.3.2. Evaluarea securității calculatoarelor

Sistemele de calcul AlfaTrust Certification respectă cerințele descrise în standardele ETSI: ETSI TS 101 456 (Cerințele de Politică pentru Autoritățile de Certificare care emit certificate calificate), ETSI TS 102 023 (Cerințele de Politică pentru Autoritățile de Marcare Temporală), CEN CWA 14167 (Cerințele de Securitate pentru Sistemele de Încredere care asigură Managementul certificatelor pentru Semnatura Electronica) și ISO 27001.

2.3.3. Controale pentru managementul securității informației

Scopul controalelor pentru managementului securității este acela de a superviza funcționalitatea sistemelor AlfaTrust Certification, garantând astfel că acestea operează corect și în concordanță cu configurarea acceptată și implementată.

Configurația curentă a sistemelor AlfaTrust Certification, precum și orice modificare și actualizare a acestora, este înregistrată și controlată.

Controalele aplicate sistemelor AlfaTrust Certification permit verificarea continuă a integrității aplicațiilor, versiunii și autentificarea și verificarea originii dispozitivelor hardware.

Fiecare aplicație, înainte de a fi folosită în producție de AlfaTrust Certification, este instalată astfel încât să se permită controlul versiunii curente și să se prevină instalarea neautorizată de programe sau falsificarea celor existente.

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

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

2.3.4. Controale de securitate a rețelei

Serverele și stațiile de lucru de încredere aparținând AlfaTrust Certification 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.

2.3.5. Sincronizarea bazei de timp

Platforma AlfaTrust 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.

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

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

2.4. Măsurile de securitate criptografice

2.4.1. Generarea cheilor unităților de marcare temporală

Perechea de chei a unităților de marcare temporală este generată prin control dual, în cadrul locației AlfaTrust, în prezența unui grup de persoane de încredere, într-un modul hardware de securitate (HSM), conform cu cerințele FIPS 140-2 Nivel 3.

Cheia privată este menținută în permanență criptată pe acest dispozitiv și nu părăsește niciodată dispozitivul într-o formă necriptată.

Acțiunile 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 în care se face generarea cheii și în care aceasta există pe toată durata ei de viață este protejat fizic și electromagnetic.

După generarea perechii de chei pentru semnarea de mărci temporale și activarea cheii private în modulul hardware de securitate (HSM), aceasta poate fi folosită în operațiile criptografice până la expirarea perioadei de validitate sau până la o eventuală compromitere.

Dimensiunea cheilor RSA folosite pentru semnarea mărcilor temporale este de 1024 biti.

2.4.2. Protejarea cheilor private ale Autorităților de Marcare Temporală

2.4.2.1. Standarde pentru modulele criptografice

Modulele hardware de securitate (HSM) folosite de Autoritățile de Marcare Temporală respectă cerințele standardului FIPS 140-2. Semnătura electronică este creată prin folosirea algoritmului RSA în combinație cu rezumatul criptografic SHA-1.

2.4.2.2. Controlul dual al accesului la cheia privată

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 (HSM) și 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 privată este de 2.

Procedura de transfer a secretului partajat implică prezența deținătorului de secret pe timpul procesului de generare a cheii și a distribuirii sale, acceptarea secretului dat și a responsabilităților care reies din păstrarea sa.

2.4.2.2.1. 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 semnătură de mână pe un formular, a cărui copie este păstrată în arhivele Autorității de Marcare Temporală și de către deținătorul de secret.

2.4.2.2.2. 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

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.

2.4.2.3. Copia de siguranță a cheilor private

AlfaTrust Certification S.A. creează o copie de siguranță a cheilor private folosite la semnarea mărcilor 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.

2.4.2.4. 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 modulului operațional.

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 (HSM) al Autorității de Marcare Temporală operată de AlfaTrust Certification S.A. necesită restaurarea cheii de pe carduri în prezența unui număr corespunzător de deținători de secrete partajate care protejează modulul ce conține cheile private.

2.4.2.5. Activarea cheii private

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

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

O cheie odată activată poate fi folosită pe perioada în care serviciul funcționează. 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.

2.4.2.6. Dezactivarea 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 unei Autorități de Marcare Temporală, dezactivarea ei se face în momentul în care serviciul se oprește pentru orice operațiune.

Protecția hardware a cheii private înseamnă că aceasta nu este în nici un moment disponibilă în clar, nici măcar în memoria aplicației.

În cazul autorităților de marcare temporală operate de AlfaTrust Certification S.A., dezactivarea unei cheii private se face de către persoanele cu roluri de încredere numai în cazul în care serviciul este oprit pentru actualizări, mentenanță sau alte motive.

2.4.3. Distribuirea cheilor publice ale Autorităților de Marcare Temporală

CertIFICATELE autorităților de marcare temporală sunt publicate pe site la adresa:

<http://www.alfastamp.ro/uploads/LantAlfaTrust.exe>

2.4.4. Schimbarea cheilor Autorităților de Marcare Temporală

Perioada de valabilitate a certificatului asociat cheii private de semnare a mărcilor temporale este de 3 ani.

Înainte de cel puțin 1 lună față de expirarea certificatului se va genera o nouă pereche de chei și un nou certificat.

Cheia privată de semnare a mărcilor temporale va fi schimbată în situația în care a survenit revocarea certificatului corespunzător.

2.4.5. Sfârșitul ciclului de viață al cheii private a Autorității de Marcare Temporală

AlfaTrust Certification S.A. a implementat proceduri tehnice și operationale pentru ca înainte de expirarea certificatului asociat cheii de semnare a unei autorități de marcare temporală să se genereze o nouă pereche de chei și un nou certificat.

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

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

2.4.6. Distrugerea cheilor Autorităților de Marcare Temporală

Distrugerea cheii private a unei autorități de marcă temporală presupune ștergerea cardurilor care conțin secretele partajate prin care este protejată cheia. După ștergerea lor, cheia este pierdută pentru totdeauna.

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

2.4.7. Managementul modului hardware de securitate

AlfaTrust Certification S.A. se asigură că:

- i. Integritatea modulelor criptografice de securitate nu a fost afectată în decursul transportului de la producător
- ii. Integritatea modulelor criptografice de securitate nu a fost afectată în decursul stocării premergătoare instalării
- iii. Instalarea, administrarea și operarea acestora este efectuată doar de personal de încredere
- iv. Modulele criptografice de securitate funcționează corect
- v. Cheile private de semnare stocate pe modulele criptografice de securitate sunt distruse în momentul scoaterii acestuia din producție.

2.5. Înregistrarea evenimentelor

Pentru a gestiona eficient sistemele autorităților de marcă temporală operate de AlfaTrust Certification S.A. și pentru a putea audita acțiunile utilizatorilor și personalului AlfaTrust, toate evenimentele care apar în sistem sunt înregistrate.

Informațiile înregistrate alcătuiesc jurnalele (log-urile) de evenimente și sunt păstrate în așa fel încât să permită Entităților Partenere să acceseze informațiile corespunzătoare și necesare rezolvării disputelor și să detecteze tentativele de compromitere a securității autorităților de marcă temporală, 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 AlfaTrust Certification.

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 AlfaTrust, 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.

2.5.1. Tipuri de evenimente înregistrate

Fiecare activitate critică din punctul de vedere al securității AlfaTrust 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 referă la:

- ❖ alertele firewall-urilor și IDS-urilor,
- ❖ operațiile asociate emiterilor sau verficarilor mărcilor 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 siguranță și a arhivelor cu înregistrări.
- ❖ fiecare cerere de marcă 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.

2.5.2. Frecvența analizei jurnalelor de evenimente

Înregistrările din jurnalul de evenimente sunt revăzute în detaliu cel puțin o dată pe lună. Orice eveniment având o importanță semnificativă este 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 loguri.

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

2.5.2. 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.

2.5.3. 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.

2.5.4. Procedurile de backup pentru jurnalele de evenimente

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

2.5.5. 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.

2.5.6. Arhivarea înregistrărilor

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

Registrul on-line conține toate mărcile temporale emise precum și date referitoare la marca și la certificatul folosit și poate fi accesat permanent pentru efectuarea unor servicii externe ale autorității de marcă temporală operată de AlfaTrust Certification S.A., de exemplu verificarea unei mărci temporale.

Arhivele off-line conțin înregistrările cu până la 10 ani înainte de data curentă. Arhiva este folosită pentru rezolvarea eventualelor dispute, referitoare la documente electronice vechi. Tehnologia folosită permite arhivarea înregistrărilor și restaurarea lor în siguranță pe perioade de timp de minim 50 de ani.

2.5.7. 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.

2.5.8. 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 sunt corectate cât mai repede posibil.

3. Managementul Codului de Practici și Proceduri

Fiecare versiune a Codului de Practici și Proceduri este în vigoare până în momentul aprobării și publicării noii sale versiuni. O nouă versiune este dezvoltată de către AlfaTrust Certification și publicată pentru comentarii cu mențiunea spre aprobare (dacă este cazul).

După primirea și includerea comentariilor, Codul de Practici și Proceduri intră în procedura de aprobare internă. Responsabil de aprobarea formei finale a Codului de Practici și Proceduri este un comitet format din directorul general și managerii departamentelor din AlfaTrust Certification. Responsabil pentru întreținerea Codului de Practici și Proceduri este managerul departamentului care asigură furnizarea serviciilor de marcare temporală.

După terminarea procedurii de aprobare, noua versiune a CPP este transmisă Autorității de Reglementare 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 Marcare Temporală.

Utilizatorii finali și entitățile partenere trebuie să respecte numai Politica de Marcare Temporală și Codul de Practici și Proceduri în vigoare în momentul respectiv.

3.1. Procedura de modificare 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 AlfaTrust Certification S.A. 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 utilizatorilor și entităților partenere și una care cere (de obicei în avans) consultarea acestora. Prima categorie include modificări de urgență sau modificări neesențiale.

Identificatorii politicilor de certificare folosite de autoritățile emitente de certificate pot fi, de asemenea, modificați ca urmare a implementării următoarelor schimbări:



- schimbarea extensiei pentru un grup de utilizatori de marcă temporală în domenii precum sistemele electronice de plăți, schimburile de informații dintre bănci etc.;
- introducerea unor noi tipuri de servicii;
- permiterea cross-certificării între autoritățile emitente de certificate din cadrul sistemului;
- modificări semnificative ale conținutului și modului de interpretare a câmpurilor certificatului și ale CRL-ului, de ex. modificarea caracterului critic/necritic al unui câmp.

3.2. Publicarea CPP-ului

O copie a Codului de Practici și Proceduri este disponibilă în formă electronică pe site-ul de web <http://www.alfastamp.ro/depozit> sau prin e-mail la adresa office@alfastamp.ro.

3.2.1. Documente ce nu se publică în CPP

Documentația de securitate (proceduri și instrucțiuni detaliate de lucru), care sunt considerate confidențiale de AlfaTrust Certification, nu se dezvăluie publicului. În această categorie intră și regulamentele interne, ce nu vor fi făcute publice.