Coduri de practici
si proceduri al
Autoritatii de Marca Temporala
„CertDigital TimeStamping Authority”

Referinta: 1/2012

Versiune: 1.0.0

Pagini: 32

Nivel de distributie: Audienta generala

EMISA DE:			
DEPARTAMENT	**NUME**	**SEMNATURA**	**DATA**
CERTDIGITAL	SEF COMPARTIMENT		12/06/2016

APROBATA DE:			
DEPARTAMENT	**NUME**	**SEMNATURA**	**DATA**
CERTDIGITAL	SEF COMPARTIMENT		12/06/2016

ISTORICUL MODIFICARILOR:			
VERSIUNE	**AUTOR**	**DETALII MODIFICARI**	**DATA:**
1.0.0	SEF COMPARTIMENT	PUBLICARE PRIMA VERSIUNE	12/06/2016

Cuprins

Termeni si definitii

Acces	Posibilitatea utilizarii unei resurse informationale pe baza unui drept dobandit
Administrator	Utilizator care este autorizat de a folosi conturi administrative sau privilegiate pentru a-si indeplini sarcinile de serviciu. In general, administratorul are dreptul de gestiune asupra celorlalte tipuri de utilizatori.
Angajat	Orice persoana care are o relatie de angajament cu CertDigital in baza unui contract de munca semnat.
Audit de conformitate	Revizuire periodica efectuata asupra anumitor procese, in urma careia se stabileste gradul de conformitate cu standardele cerute
Autentificare	Validarea identitatii unui utilizator sau a unei entitati. Procesul autentificarii verifica daca entitatea este cea care pretinde a fi si in functie de rezultatul obtinut ofera sau nu acces catre resursele solicitate.
Autoritatea de Certificare	Institutie de incredere care emite certificate aferent cererilor eligibile. Pentru acest proces, Autoritatea de Certificare verifica informatiile specificate de solicitant in cererile de emitere a certificatului.
Autoritatea de Inregistrare	Institutie care este responsabila cu identificarea si autentificarea subiectului unui certificat
Cerere de emitere a unui certificat	Document electronic care contine detalii cu privire la certificatele care urmeaza sa fie create de catre Autoritatea de Certificare si inregistrate de catre Autoritatea de Inregistrare
Certificat	Colectie de date in forma electronica ce atesta legatura dintre datele de verificare a semnaturii electronice si o persoana, confirmând identitatea acelei persoane

Certificat calificat	Certificat eliberat de un furnizor de servicii de certificare in conditiile prevazute la art. 18 din Legea nr. 455/2001 privind semnatura electronica
Certificat digital	Reprezinta un act de identitate sub forma electronica folosit pentru autentificarea si certificarea identitatii unui utilizator in cazul accesarii de la distanta a unor resurse.
Certificat revocat	Certificat de cheie publica inclus in Lista Certificatelor Revocate
Certificat valid	Certificat de cheie publica emis de catre o Autoritate de Certificare, acceptat de solicitant si care nu a fost supus procesului de revocare
Cheie privata	Un cod digital cu caracter de unicitate, generat printr-un dispozitiv hardware si/ sau software specializat. In contextul semnaturii digitale, cheia privata reprezinta datele de creare a semnaturii electronice, asa cum apar ele definite in lege
Cheie publica	Cod digital, perechea cheii private necesara verificarii semnaturii electronice. In contextul semnaturii digitale cheia publica reprezinta datele de verificare a semnaturii electronice, asa cum apar ele definite in lege
Cod de Practici si Proceduri	Document ce reglementeaza activitatea de furnizare a serviciilor de certificare
Colaborator	Orice persoana care are o relatie de angajament cu CertDigital in baza unui contract de colaborare semnat intre persoana si CertDigital sau intre CertDigital si compania pentru care lucreaza persoana respectiva
Compromitere	O incalcare a unei politici de securitate care duce la pierderea controlului asupra unei informatii cu caracter sensibil

Confidentialitate	Reprezinta un principiu de securitate care restrange accesul datelor doar la persoanele autorizate.
Control al accesului	Limitarea si verificarea accesului la sistemele informatice cu scopul de a elimina utilizarea neautorizata a acestora
Criptare	Transformarea textului clar in text criptat cu scopul de a ascunde continutul informatiilor pentru a preveni modificarea si utilizarea neautorizata a acestora.
Date in forma electronica	Reprezentari ale informatiei intr-o forma conventionala adecvata crearii, prelucrarii, trimiterii, primirii sau stocarii acesteia prin mijloace electronice
Dispozitiv de creare a semnaturii electronice	Sisteme software si/sau hardwar configurate, utilizate pentru a implementa datele de creare a semnaturii electronice
Entitate	Termen folosit pentru a descrie un client. De exemplu, o entitate poate fi o companie, un trust, sau o persoana fizica
Extensii	Campuri de extensie in certificatele X.509 v.3
Firewall	Reprezinta un echipament sau o serie de echipamente configurate astfel incat sa asigure filtrarea, criptarea sau intermedierea traficului intre domenii diferite de securitate pe baza unor reguli predefinite
Furnizor de servicii de certificare	Autoritate de incredere ce furnizeaza servicii de creare, semnare si emitere de certificate
Generator de chei	Echipament criptografic folosit pentru generarea de chei criptografice
Hash-code	Funcţie care returneaza amprenta unui document electronic

HTTPS	Protocol de comunicare client-server similar HTTP, care permite vizualizarea de pagini web intr-un mod securizat bazat pe criptarea informaţiilor transmise de catre server şi decriptarea acesteia de catre client, folosind certificatul serverului, acceptat la iniţializarea conexiunii.
Incident de Securitate a Informatiei	Eveniment declansat accidental sau intentionat care altereaza informatiile si/sau echipamentele si care provoaca pierderea partiala sau completa a confidentialitatii/ integritatii informatiilor ori indisponibilitatea acestora.
Integritate	Principiu de securitate care asigura ca informatiile si sistemele informationale nu sunt modificate in mod accidental sau in mod voit.
Internet	Reprezinta o multitudine de calculatoare conectate intr-o retea globala care permite partajarea datelor (din institutii academice, institute de cercetare, companii private, agentii guvernamentale, indivizi, etc.) care pot fi accesate de la distanta
Lista Certificatelor Revocate	Document emis la anumite intervale de timp in care se specifica certificatele care au fost revocate sau suspendate inainte de expirarea perioadei de valabilitate. Informatiile specificate in aceasta lista includ numele emitentului, data publicarii, data urmatoarei actualizari, numerele de serie ale certificatelor revocate sau suspendate si motivele pentru care au fost revocate sau suspendate.
Modul de securitate hardware	Echipament hardware controlat printr-un software, care realizeaza operatii criptografice (inclusiv criptare si decriptare)
Nume distinct (ND)	Grup de informatii ale unei entitati ce alcatuiesc un nume distinctiv prin care se deosebeste de alte entitati similiare

Pagina web	Document electronic, disponibil prin Internet
Pereche de chei	Pereche complementara de chei de criptare generate de Autoritatea de Certificare si formatate intr-o cheie privata şi o cheie publica. Cheia publica este distribuita intr-un certificat eliberat de catre Autoritatea de Certificare
Pereche de chei asimetrice	Pereche de chei in relatie unde cheia privata defineste transformarea privata si cheia publica defineste transformarea publica.
Parola	Sir de caractere unic asociat unui utilizator cu scopul de a valida identitatea acestuia.
Perioada de valabilitate	Perioada cuprinsa intre data intrarii in vigoare a certificatului si data de expirare a valabilitatii sau data la care este revocat
Persoana de incredere	Angajat permanent sau temporar al organizatiei ce detine drepturi de administrare a infrastructurii de incredere din cadrul organizatiei
PKI	Infrastructura de chei publice
PKCS (Public-Key Cryptography Standards)	Standard de criptografie a cheilor publice
PKCS#10	Sintaxa standard pentru cererile de certificat si standard de criptare a cheii publice #10, dezvoltat de catre RSA Security Inc.
Politica de Securitate a Informatiei	Politica ce sta la baza modului de abordare, de catre CertDigital, a problemelor referitoare la Managementul Securitatii Informatiilor.
Securitatea Informatiilor	Pastrarea confidentialitatii, integritatii si disponibilitatii informatiilor si asigurarea autenticitatii, responsabilitatii, nonrepudierii si acuratetii informatiei in scopul asigurarii continuitatii afacerii, minimizarii riscurilor si maximizarii profitului operational si a oportunitatilor de afaceri.

Semnatar	Persoana specificata ca subiect al certificatului ce detine cheia privata aferenta cheii publice din certificat.
Semnatura electronica	Grup de date in forma electronica atasate sau asociate logic cu alte date in forma electronica si care servesc ca metoda de identificare
SHA-1	Algoritm securizat de hash-code
Sistem de Detectie A Intruziunilor (IDS)	Sistem folosit pentru detectarea accesului neaprobat intr-o retea sau o statie de lucru.
Sistem de semnatura asimetrica	Sistem bazat pe tehnici asimetrice in care transformarea privata este folosita pentru semnare si transformarea publica este folosita pentru verificare.
SSL	Canal de comunicatie privat intre un server WEB si browser-ul client
Utilizator	Beneficiarul serviciilor de certificare, care, in baza unui contract incheiat cu un furnizor de servicii de certificare, denumit in continuare furnizor, deţine o pereche funcţionala cheie publica-cheie privata şi are o identitate probata printr-un certificat digital emis de acel furnizor
CDTSA	Cert Digital Timestamping Authority
TSS	TimeStampingService

1. Cadrul general

1.1. Marca CertDigital

CertDigital reprezinta marca inregistrata sub egida caruia S.C. Centrul de Calcul S.A. furnizeaza serviciile de certificare si marcare temporala. De fiecare data cand in continutul acestui document se fac referiri la CertDigital, acele referiri implica compania Centrul de Calcul S.A.

1.2. Continut

Documentul „Codul de Practici si Proceduri CDTSA" defineste practicile si procedurile de lucru implementate de S.C. Centrul de Calcul S.A. (de aici inainte referita ca „CertDigital") in procesul de furnizare a serviciilor de marcare temporala operate sub denumire "Cert Digital Timestamping Authority" (CDTSA) in conformitate cu prevederile legislative aplicabile .

1.3. Sponsorul procedurii

Documentul curent se afla sub sponsorizarea Conducerii CertDigital.

1.4. Audienta si aplicabilitate

In sfera de aplicabilitate a Codului de Practici si Proceduri TSA se include totalitatea participantilor la serviciile de certificare si marcare temporala CertDigital, respectiv abonati, distribuitori sau alte parti contractante.

2. Managementul cheilor private

2.1. Generarea perechii de chei CDTSA

2.1.1. Caracteristici cheie CDTSA

Perechea de chei CDTSA este generata folosind algoritmul RSA iar dimensiunea acesteia este 1024 biti, semnatura electronica fiind realizate in combinatie cu rezumatul criptografic SHA-1.

2.1.2. Procedura de generare a perechii de chei CDTSA

Perechea de chei CDTSA, este generata in cadrul locatie CertDigital, de catre Administratorul de sistem si in prezenta sefului de departament CertDigital ce va supraveghea intreaga procedura. Generarea cheii se face pe un dispozitiv hardware de securitate (HSM) conform cu cerintele FIPS 140-2. Cheia privata este stocata in permanenta pe acest dispozitiv si nu este disponibila in exteriorul dispozitivului in forma necriptata.

Atat seful de departmanet CertDigital cat si administratorul vor inregistra si semna operatiunile efectuate in timpul generarii perechii de chei. Inregistrarile sunt pastrate in scopul posibilitatii de auditare a acestora.

2.1.3. Protectia cheilor private CDTSA

Stocarea cheilor private CDTSA se realizeaza prin echipamente securizate conforme FIPS 140-2, ce sunt atestate sa indeplineasca reglementarile Legii nr. 455/2001 privind semnatura electronica si care nu pot fi falsificate. Pentru prevenirea oricarei tentative de acces neautorizat sau de falsificare a informatiilor sensibile, CertDigital implementeaza controale adecvate, revizuite periodic pentru a se asigura functionarea corespunzatoare.

2.1.4. Backup-ul cheilor private CDTSA

Cert Digital Timestampig Authority se incadreaza in lantul de incredere CertDigital ca o subautoritate a Cert Digital Non-Repudiation CA Class 4. CertDigital mentine o copie a cheilor de root si a tuturor subautoritatilor, backup executat si mentinut conform specificatiilor din Codul de Practici si Proceduri. Prerechea de chei CDTSA nu este mentinuta in backup, in caz de aplicarea a procedurilor de urgenta aceasta va fi regenerata, certificatul aferent fiind revocat si publicat in crl.

2.2. Distribuirea chielor publice ale Cert Digital Timestamping Authority

Certificatele corespunzatoare cheilor private folosite in semnarea de catre CDTSA a marcilor temporale sunt disponibile pe site-ul www.certdigital.ro in sectiunea suport / lant de incredere.

2.3. Schimbare perechii de chei CDTSA

Perioada de valabilitate a certificatului aferent cheii private CDTSA, este de 2 ani. Cu cel putin 30 zile inainte de expirarea certificatului CDTSA, se va proceda la generarea unei noi perechi de chei si a unui nou certificat. Perechea de chei CDTSA va fi schimbata la orice revocare a certificatului aferent, indiferent de motivul revocarii.

3. Specificatii CDTSA

3.1. Standardele tehnice aplicabile

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

Profilul certificatului digital emis pentru Cert digital Timestamping Authority respectă recomandările IETF din RFC 3161 si RFC 2459, Internet X.509 Public Key Infrastructure Certificate.

Modulul hardware de securitate (HSM) utilizat in cadrul CDTSA respectă standardul NIST FIPS 140-2 Security Requirements for Cryptographic Modules.

In crearea semnaturii electronice a marcilor temporale se respecta standardul IETF RFC 2630 Cryptographic Message Syntax .

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

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

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

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

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

Managementul securitatii CDTSA este asigurat conform standardelor ISO 27001:2005, Information technology -- Security techniques --
Information security management systems – Requirements si ISO 27002, Information technology -- Security techniques -- Code of practice for information security management.

3.2. Timpul

Aplicatia ce deserveste CDTSA verifica in permanenta sincronizarea serverului local de timp cu baza de timp reprezentata de sistemul informatic destinat furnizarii orei oficiale a Romaniei.

Sincronizarea cu sursa de timp este monitorizata permanent si orice nesincronizare este semnalata imediat administratorilor.
Aplicatia software care emite marcile temporale este realizata astfel incat la orice desincronizare care depaseste precizia asumata sa opreasca emiterea de marci.
Daca totusi se constata ca s-au emis marci temporale care incalca precizia asumata, atat abonatii care au primit acele marci cat si autoritatea de supraveghere sunt notificati.

3.3. Procesul de marcare temporala

3.3.1. Structura marcii temporale

Structura marcii temporale este conforma normelor legale in vigoare la data publicarii versiunii curente a acestui document, respectiv Legea 451/2004 si Ordinul 492/2009 cu modificarile si completarile pana la data publicarii prezentului document.
In acest sens, marca temporala cuprinde:

- Amprenta imaginii electronice a documentului la data generarii marcii
- Informatii referitoare la furnizorul de servicii de marcare temporala precum si a autoritatii ce a emis marca temporala (ex: DN[C,O,OU,CN], SERIAL)
- Valoarea temporala a marcii

3.3.2. Aplicatie client pentru marcare temporala

CertDigital pune la dispozitia clientilor sai, in mod gratuit softul de marcare temporala CertDigitalSigner. Acest soft permite semnarea unui document folosind un certificate calificat, marcarea temporala a acestei semnaturi precum si verificarea unui fisier semnat pdf sau p7s.
Verificarea fisierului urmareste:

- Integritatea documentului
- Validitatea amprentei semnaturii calificate pentru documentul semnat
- Validitatea certificatului calificat cu care a fost semnat documentul
- Integritatea marcii temporale
- Validitatea amprentei din marca temporala pentru documentul semnat
- Validitatea certificatului cu care a fost semnata marca temporala

Aplicatia CertDigitalSigner creaza automat amprenta documentului, ce va fi folosita in procesul de generare a marcii temporale prin intermediul unui alogoritm ce

garanteaza unicitatea amprentei in raport cu documentul electronic si starea acestuia in momentul generarii amprentei. Amprenta este o reprezentare matematica a imaginii si starii documentului ce nu poate fi folosita pentru reconstructia documentului original.

3.3.3. Serviciul de marcare temporala

Generarea si furnizarea marcilor temporale se realizeaza in mod automat prin intermediul unui serviciu online. Acest serviciu denumit in continuare TSS (TimeStampingService) este responsabil cu procesarea cererilor de marcare temporala, verificarea structurii cererilor de marcare temporala, generarea marcii temporale si livrarea acesteia catre client.

TSS este un serviciu ce poate fi folosit doar in mod autentificat, pe baza de nume utilizator si parola.

4. Practici si proceduri operationale in domeniul IT

4.1. Procedura de control al accesului fizic

Regulile pe care se bazeaza masurile de control al accesului pornesc de la principiul ca toate drepturile sunt in general restrictionate in cazul in care nu exista o aprobare sau o autorizare explicita in conformitate cu politicile si procedurile CertDigital.

4.1.1. Amplasarea locatiei

Sediul CertDigital este localizat in str. Tudor Vladimirescu, nr. 17, Targu-Jiu, judetul Gorj.

4.1.2. Protectie impotriva accesului neautorizat

Sediul unde isi va desfasura activitatea Autoritatea de Certificare este dotat cu sistem de alarma si control acces (DVR stand-alone, camere de supraveghere, control acces, cititor de proximitate, senzori de miscare, fum, alarme).

CertDigital are incheiat un contract cu firma specializata de securitate care asigura intervenţia unui echipaj in maxim 6 minute de la receptionarea semnalelor antiefractie, antiincendiu sau panica.

Camera unde se gasesc echipamentele Autoritaţii de Certificare este protejata suplimentar cu o uşa metalica antiefractie, accesul realizându-se pe baza unei cartele magnetice, prin introducerea unui cod de securitate si actionarea unei chei, dispozitive pe care doar administratorul sistemului şi Directorul General le pot actiona.

4.1.3. Accesul fizic

Conducerea CertDigital indentifica drepturile de acces necesare angajatilor si comunica aceste drepturi personalului responsabil pentru a fi implementate in conformitate cu procedurile in vigoare.

Accesul in incinta sediului se face pe baza urmatoarelor reguli:

- Fiecare angajat CertDigital are implicit acces deplin la biroul sau;
- Pe toata durata de desfasurare a programului, fiecare angajat are acces in toate zonele, cu exceptia zonelor pe care managerul responsabil le-a marcat ca zone cu acces limitat;
- Dreptul de acces pentru colaboratori, consultanti, personal responsabil de curatenie etc. este permis numai in zonele in care isi desfasoara

activitatea. Accesul se va face prin specificarea locului si a timpului necesar si va fi aprobat de catre managerul responsabil;

- Vizitatorilor le este permis accesul doar in spatiile de receptie, iar accesul in zonele securizate se va face numai in baza unei nevoi definite clar pentru desfasurarea activitatii si in permanenta supraveghere a unui angajat CertDigital;
- Personalul IT emite recomandari privind regulile de acces pentru consultantii si colaboratorii fiecarui departament care au o relatie de afaceri cu tertii.

4.1.4. Controale de mediu in zonele IT critice

Pentru stabilirea conditiilor optime in zonele IT critice au fost implementate urmatoarele masuri:

- Sisteme de aer conditionat si ventilatoare montate pe rack-uri care asigura o temperatura optima de functionare a echipamentelor IT;
- Echipament de tip UPS ce deserveste totate dispozitivele hardware cu rol critic in furnizarea serviciilor de marcare temporala :servere, HSM-ul, router-ul, firewall-ul, switch-urile şi modem-urile de internet;
- Conexiune la o retea electrica separata pentru a asigura protectia impotriva supratensiunii;
- Pentru evitarea unor posibile amenintari (precum inundatiile), echipamentele sunt aşezate intr-un rack inaltat, care este protejat printr-o incuietoare cu cheie.

Sisteme de detectie a fumului si sisteme de stingere a incendiilor.

4.2. Politica de securitate

Masurile de securitate implementate de CertDigital care asigura desfasurarea activitatii de marcare temporala in conditii optime se impart in:

- masuri de asigurare a redundantei pentru datele critice;
- masuri de asigurare a continuitatii serviciilor oferite;
- masuri de protectie fata de greselile personalului angajat;

4.2.1. Masuri de asigurare a redundantei pentru datele critice

Sistem de mirroring pentru hard-disk-urile serverelor :siguranţa datelor este asigurata de sisteme ce se bazeaza pe matrici RAID Mirroring forma duplicarea datelor asigurand protecţie impotriva pierderii fizice a informaţiilor.

Sistem de clustering pentru serviciul de marcare temporala :server-ul ce gazduieste serviciul de marcare temporala este setat sa lucreze in clustering cu alt server de rezerva, asigurându-se astfel un nivel ridicat de disponibilitate a serviciilor.

Proces de backup sistematic: datele aferente serviciului de marcare temporala sunt salvate şi arhivate periodic in conformitate cu prevederile procedurii de salvare si restaure a datelor.

4.2.2. Masuri de asigurare a continuitatii serviciilor oferite

In vederea asigurarii unei continuitati a serviciilor oferite, CDTSA dispune de conexiune la Internet prin doua linii oferite de furnizori diferiti, dupa cum urmeaza:

- RDS – linie principala fibra optica de 2 MB garantat;
- Romtelecom – linie back-up de 20 MB ADSL.

4.2.3. Masuri de protectie fata de greselile personalului angajat

Personal calificat in activitaţile de certificare

Personalul angajat al CDTSA este format din oameni calificaţi cu o bogata experienţa profesionala şi care poseda certificari şi diplome.

Personalul implicat in procesele CDTSA trebuie sa prezinte dovada indeplinirii cerinţelor legate de trecut, calificari şi experienţa, necesare pentru a indeplini in mod competent şi satisfacator responsabilitaţile postului respectiv.

- Activitaţile sunt imparţite pe baza de roluri conform fişei de responsabilitaţi, astfel incât o activitate mai complexa sa poata fi dusa la capat numai cu acordul mai multor persoane. Un exemplu ar fi aici crearea de noi perechi de chei şi certificate pentru autoritaţile de certificare, unde administratorul sistemului şi responsabilul cu gestiunea autoritaţii de certificare trebuie sa colaboreze aşa cum este specificat in cadrul procedurii operaţionale ce reglementeaza aceasta activitate. Mai mult decat atât, pentru activitaţi critice este necesar acordul scris al Directorului General.

4.3. Procedura de salvare si restaurare a datelor

Programul de salvare a datelor este dezvoltat in baza unei evaluari a riscului efectuate de catre personalul IT din cadrul CertDigital.

Administratorul de sistem este responsabil de intregul proces de back-up si restaurare, care trebuie sa se desfaşoare conform curentei proceduri. Pentru procedura de restuarare este necesara, insa, o imputernicire scrisa, semnata de Conducerea CertDigital.

4.3.1. Procesul de salvare

La nivelul CDTSA sunt identificate doua seturi de date critice.

- baza de date SQL Server, unde se pastreaza toate marcile temporale emise;
- perechile de chei aferente CDTSA, stocate pe echipamentul Hardware Security Module (HSM).

Procesul de backup se face de catre adminsitratorul de sistem, care include ambele puncte de la paragraful de mai sus.

Procesul de back-up al bazei de date SQL Server se executa automat, programatic, folosind programe (scripturi de back-up) native SQL Server in urmatoarele etape:

1. **Full Back-up (Salvare Totala)** - se executa saptamânal in fiecare zi de duminica la ora 00.00. Backup-ul consta in salvarea in intregime a bazei de date: tabele, structura, vederi, proceduri stocate si functii, indecsi, rezultand o copie exacta a bazei de date initiale la momentul salvarii. Salvare se efectueaza pe Network Storage intr-un fisier denumit “ca_full_backup.bak”.
2. **Differential Back-up (Salvare Diferentiala)** se executa automat zilnic, o singura data, la orele 1.00 si consta in salvarea tuturor modificarilor din baza de date care au avut loc de la ultimul Full Backup. Salvare se efectueaza pe Network Storage intr-un fisier denumit ca_diff_backup.bak.
3. **Transaction Log Back-up (Salvarea Jurnalului de Tranzactii)** se executa automat zilnic, incepând cu ora 8:00 pâna la ora 18:00, din doua in doua ore, incluzând intervalele orare. Prin aceasta procedura se salveaza jurnalul operatiunilor efectuate asupra bazei de date de SQL. Salvare se efectueaza pe Network Storage intr-un fisier denumit “ca_log_backup.bak”.

Salvarea datelor de pe HSM este efectuata pe SmarCard-urile producatorului, informatia este criptata si distribuita intr-o schema care sa asigure redundanta. Smart-cardurile sunt tinute in siguranta intr-o locatie externa, autorizata pentru depozitarea valorilor .

In fiecare saptamâna in ziua de Vineri, salvarile efectuate pe Network Storage, sunt scrise pe suport magnetic CD/DVD, pe care se va nota data si ora la care au fost salvate. Ulterior unitatile de tip CD/DVD sunt pastrare intr-un loc sigur, in fisete de metal protejate de cheie si de sistemul de securitate dedicat, din incinta CertDigital.

4.3.2. Procedura de restaurare

Implementarea procedurilor de restaurare se desfasoara dupa cum urmeaza:

- Departamentul IT realizeaza cel putin trimestrial testarea mediului de back-up pentru a verifica faptul ca acesta poate fi folosit pentru restaurarea datelor.
- Testarea restaurarii – se realizeaza pe mediul de test si are ca scop verificarea functionarii corecte a datelor restaurate.

In cazul identificarii unor defecţiuni hardware (defectare a placii de baza, defectare a unităţii de stocare sau altele) se trece la remedierea problemei prin inlocuirea componentelor defecte cu alte componente noi compatibile având caracteristicile tehnice identice cu cele ale componentelor iniţiale.

Dupa instalarea noilor componente in sistem, daca este necesar, se va trece la repopularea cu datele existente salvate inainte de apariţia problemei. Pentru executarea procedurii de restaurare a datelor de pe suportul de back-up (CD sau DVD) este necesar acordul scris al Directorului General.

Procesul de restaurare se va realiza de catre administratorul de sistem sub supravegherea Directorului Tehnic, care va raspunde de acest proces.

4.3.3. Procedura de continuare a activitatii in cazul compromiterii cheii private a CDTSA

In cazul compromiterii cheii private a CDTSA, sau în cazul suspiciunii unei astfel de compromiteri, trebuie luate urmatoarele masuri:

- Se va genera o noua pereche de chei si un nou certificat.
- Vechilul certificat va fi revocat si publicat in Lista de Certificare Revocate.
- Clientii activi vor fi instiintati prin intermediul postei electronice de acest eveniment.

4.4. Procedura de administrare a conturilor in sistemele CertDigital

Toate conturile de utilizator ale angajatilor CertDigital sunt identificate in mod unic printr-un nume de utilizator (care se va constitui pe baza numelui angajatului care foloseste contul) si o parola (care va fi stabilita pe baza regulilor si procedeelor mentionate in Procedura de Administrare a Parolelor).

Numele de utilizator al unui angajat se emite pe durata de desfasurare a activitatilor acestuia sub contract cu CertDigital si nu poate fi modificat decat in baza unor nevoi bine justificate (angajatul isi schimba in mod legal numele, in cadrul CertDigital isi desfasoara activitatea un alt angajat cu nume similar sau asemanator care poate crea confuzie etc.).

Aplicatiile informatice si de posta electronica din cadrul CertDigital permit definirea unor grupuri de utilizatori care specifica drepturile pe care utilizatorii care fac parte dintr-un grup le detin in utilizarea unui sistem informatic. Grupurile de utilizatori vor fi definite in conformitate cu responsabilitatile si necesitatile stricte pe care categoria de utilizatori careia i se asociaza le are.

Utilizatorii au obligatia de a-si folosi drepturile de acces in sistemele informatice care le-au fost acordate doar in vederea indeplinirii sarcinilor si responsabilitatilor alocate si se interzice folosirea informatiilor catre care au acces in alte scopuri decat cele precizate.

De asemenea, se interzice cu desavarsire angajatilor instrainarea sau “imprumutul” conturilor de acces proprii in reteaua de calculatoare, aplicatiile informatice sau sistemele de posta electronica catre alti angajati.

Contul unui utilizator poate avea mai multe stari, dupa cum urmeaza:

- *Activ* – contul este pe deplin operational;
- *Expirat* – parola corespunzatoare contului este expirata si pentru reactivarea sa este necesara generarea unei noi parole;
- *Dezactivat* – utilizarea contului de utilizator a fost oprita pe motivul incheierii contractului de munca intre angajatul posesor si Companie sau in cazul in care titularul de cont nu mai indeplineste criteriile de utilizare a contului.

4.4.1. Crearea conturilor de utilizatori

Definirea conturilor de utilizatori pentru reteaua de calculatoare, sistemele informatice sau sistemele de posta electronica din cadrul CertDigital se realizeaza de catre personalul de administrare a aplicatiilor din cadrul Departamentului IT.

La angajarea unei persoane noi in cadrul CertDigital care are nevoie de acces intr-unul sau mai multe dintre sistemele informatice, se va solicita de catre seful direct crearea conturilor de utilizator necesare prin completarea unui formular pentru crearea unui cont de utilizator. In cadrul formularului se vor detalia aplicatiile si sistemele pentru care se solicita contul de acces precum si drepturile si profilele de utilizator de care respectiva persoana are nevoie pentru indeplinirea responsabilitatilor care i-au fost alocate.

Formularul completat trebuie semnat atat de catre utilizator cat si de catre superiorul direct si trebuie transmis Departamentului IT pentru implementare.

Pe baza formularului completat si a aprobarii sale, Departamentul IT va crea conturile solicitate intocmai cu drepturile si profilele specificate.

4.4.2. Modificarea conturilor de utilizatori

In cazul in care este nevoie de a modifica un cont de acces in sistemele informatice CertDigital, utilizatorul solicitant va completa un formular de modificare a unui cont de utilizator prin specificarea in detaliu a noilor drepturi pe care le solicita (aplicatii si sisteme informatice, profil de utilizator etc.) dar si a drepturilor pe care le detine si care trebuie anulate odata cu modificarea pozitiei in cadrul CertDigital.

Formularul completat este aprobat de catre superiorul direct al angajatului care isi va exprima acordul si va revizui unde este cazul detaliile privind conturile de utilizator solicitate, dar si a celor care vor fi anulate.

Pe baza formularului completat si a aprobarii sale, Departamentul IT va executa operatiile de modificare a conturile in conformitate cu detaliile specificate.

De asemenea, in cazul intreruperii activitatii pentru o perioada mai lunga de 60 de zile (de exemplu in cazul unui concediu de maternitate), angajatul respectiv are obligatia de a solicita prin formularul pentru modificarea unui cont de utilizator dezactivarea temporara a contului de utilizator. Formularul trebuie semnat de catre superiorul direct si trimis Departamentului IT care va actiona in consecinta.

4.4.3. Dezactivarea conturilor de utilizatori

Procesul de dezactivare a unui cont de utilizator se realizeaza pe baza fisei de lichidare emise de catre Departamentul de Resurse Umane. Astfel, in momentul terminarii contractului de munca cu CertDigital, angajatul respectiv va prezenta Departamentului IT fisa de lichidare care va contine o referire la dezactivarea conturilor sale de utilizator.

Departamentul IT va dezactiva conturile imediat sau in cel mai scurt timp posibil in vederea diminuarii riscului de mentinere a unui cont activ in mod necorespunzator si va confirma acest lucru prin semnarea fisei de lichidare.

Pentru a facilita trasabilitatea activitatilor efectuate cu ajutorul conturilor de utilizator, aceastea vor fi dezactivate si nu sterse. Dupa trecerea unei perioade de minim 24 de luni de la dezactivare, Departamentul IT poate decide stergerea definitiva a conturilor.

4.5. Procedura de administrare a utilizatorilor cu drepturi privilegiate

Un drept privilegiat reprezinta accesul nerestrictionat de controalele implementate al unui utilizator la una sau mai multe functionalitati din cadrul unui sistem informatic.

Aceste drepturi includ, dar nu se limiteaza la:

- Un utilizator cu drepturi de administrator;
- Dreptul de accesa direct bazele de date ale aplicaţiilor;
- Drept de acces pe facilitati de sistem specifice (aplicaţii, utilitare).

Alocarea drepturilor privilegiate pentru utilizatori in aplicatiile informatice din cadrul Companiei este permis decât in baza unei autorizatii si a unei nevoi justificate in fişa postului in cazul angajatilor, respectiv in contractele de servicii/ colaborare in cazul terţelor parţi.

Beneficiarii drepturilor privilegiate sunt, in general, administratorii de sisteme, administratorii de reţea, inginerii de sistem sau consultanţii din partea unor terţe parţi care necesita acces in aplicatiile informatice din cadrul CertDigital pentru a intreprinde actiuni specifice (precum intreţinere, mentenanţa, debugging etc.).

Drepturile privilegiate sunt identificate pentru fiecare element al infrastructurii (de ezemplu sistem de operare, baza de date, etc.) şi pentru fiecare aplicatie. De asemenea, sunt identificate si categoriile de utilizatori pentru care vor fi alocate aceste drepturi.

Anumite situatii de urgenta pot justifica folosirea conturilor privilegiate. Astfel, este efectuata o configurare prealabila a accesului cu drepturi privilegiate si impunerea unui control

adecvat. Spre exemplu, datele de acces ale conturilor de utilizatori pot fi pastrate intr-un plic sigilat intr-o locaţie sigura, alaturi de o lista cu persoane autorizate sa foloseasca in caz de necesitate aceste conturi. De asemenea, in plicul sigilat sunt incluse si datele de contact ale administratorului de sistem care trebuie contactat atunci când este necesara deschiderea plicului.

4.5.1. Administrarea conturilor de utilizatori cu drepturi privilegiate

Personalul de administrare a aplicatiilor are in responsabilitate crearea, modificarea si ştergerea conturilor de utilizatori cu drepturi privilegiate. Procesul de creare a unui cont cu drepturi privilegiate pe baza unei cereri emise implica, in plus fata de procesul obisnuit si descris in procedura de administrare a conturilor in sistemele CertDigital.

Conturile de utilizatori privilegiate trebuie permanent revizuite de catre Responsabilul de Securitate pentru a preintâmpina situatia in care ar putea exista in sistem conturi active nefolosite sau drepturi de acces acordate necorespunzator.

Personalul de administrare a sistemului, daca este posibil, nu trebuie sa foloseasca conturile cu drepturi privilegiate pentru desfasurarea activitatilor zilnice de nivel scazut. Pentru aceste activitati, fiecare administrator trebuie sa detina in paralel un cont cu drepturi normale de acces.

4.5.2. Monitorizarea conturilor de utilizatori cu drepturi privilegiate

Toate activitaţile desfaşurate prin intermediul unor conturi de utilizator cu drepturi privilegiate vor fi monitorizate si inregistrate. Conform politicii de retentie, aceste fisiere vor fi salvate şi pastrate pentru o perioada determinata de timp şi vor fi revizuite periodic sau ori de câte ori este nevoie de catre Responsabilul de Securitate. Acesta va intocmi rapoarte regulate conţinând rezultatele procesului de revizuire.

4.6. Procedura de management al parolelor pentru personalul CertDigital

Scopul acestei proceduri este de a stabili standarde de creare a parolelor, de protectie si de schimbare frecventa a acestora, astfel incat sistemul informatic CertDigital sa fie protejat impotriva accesului neautorizat.

Parolele sunt asociate cu conturile de utilizator si sunt folosite in cadrul aplicatiilor sau diverselor sisteme CertDigital (de ex. pentru acces la retea, e-mail etc.). De aceea, este necesar ca toti angajatii sa cunoasca recomandarile cu privire la alegerea unor parole adecvate.

4.6.1. Reguli privind alegerea parolelor

Parolele **adecvate** au urmatoarele caracteristici:

- Contin atat majuscule cat si litere mici (a-z, A-Z);
- Contin cifre si cel putin un caracter alfanumeric (0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./);
- Nu sunt cuvinte intalnite in nicio limba, dialect, argou, jargon etc;
- Nu se bazeaza pe informatii personale precum nume, numere de telefon etc;
- Nu coincid si nu contin numele de utilizator;
- Au lungimea minima de opt caractere.

Parolele **neadecvate** reprezinta parole cu grad scazut de complexitate ce sunt deseori caracterizate de una dintre urmatoarele specificatii:

- Reprezinta un cuvant folosit in mod uzual, cum ar fi:
    - Cuvintele „CertDigital", "Bucuresti", "parola" sau alte derivate;
    - Numele utilizatorului familie, al copiilor, colegilor de serviciu, animalelor de companie, etc.;
    - Zile de nastere, adrese, numere de telefon, numarul de la masina sau alte informatii personale;
    - Cuvinte sau succesiuni de litere sau cifre de genul: abcdef, 123456, zyxwvuts, 123321 etc.;
    - Oricare dintre cuvintele de mai sus scrise in ordine inversa;
- Au in alcatuire cuvinte ce se regasesc intr-un dictionar (Roman, Englez etc);
- Coincid sau contin numele de utilizator;
- Au lungimea mai mica de opt caractere.

4.6.2. Protejarea parolelor de catre utilizatori

Parolele asociate conturilor de utilizatori nu sunt folosite pentru autentificarea in sisteme externe CertDigital (de exemplu, conturi personale de e-mail, conturi pe site-uri comerciale etc.). De asemnea, parolele sunt alese in mod distinct pentru fiecare tip de aplicatie care necesita autentificare prin parola.

Toate parolele sunt clasificate ca informatii confidentiale si nu este permisa stocarea acestora in sistemele informatice sau pe un alt suport.

In cazul in care controalele referitoare la folosirea parolelor nu sunt respectate, CertDigital adopta masurile adecvate in acest sens pentru a se ajunge la conformitatea cu acestea.

4.7. Procedura de securitate a informatiilor

Pentru manipularea optima a informatiei, pentru simplificarea deciziilor privind securitatea informatiilor si pentru minimizarea costurilor legate de securitatea informatiilor CertDigital are implementata o ierarhizare a informatiei pe baza confidentialitatii. Principalul scop al acestei ierarhizari este de a furniza un proces consistent de manipulare a informatiilor, indiferent de modul in care se prezinta informatia, cui ii este adresata sau cine o are in custodie.

Fiecare angajat trebuie sa aiba acces doar la informatia necesara pentru a-si indeplini sarcinile de serviciu. Informatiile sensibile trebuie accesate doar de catre angajatii carora proprietarul aplicatiei respective le-a acordat drept de acces.

Informatiile CertDigital nu trebuie folosite in alte scopuri decat cele de business aprobate in mod oficial de catre Conducere. Folosirea neaprobata a informatiilor restrictionate este interzisa. Politica se aplica tuturor tipurilor de informatii cadrul CertDigital. Politica se aplica tuturor partilor care intra in contact cu informatiile CertDigital, inclusiv colaboratorilor externi.

Utilizatorilor nu le este permis sa efectueze nicio activitate in sistemele informatice interne ce ar putea conduce la deteriorarea imaginii CertDigital.

CertDigital foloseste trei categorii de clasificare a informatiilor detaliate in continuare.

4.7.1. Informatie Publica

Aceasta informatie este aprobata de catre Conducerea CertDigital ca fiind publica. Dezvaluirea neautorizata a informatiilor publice este admisa intrucat nu poate cauza probleme companiei CertDigital, clientilor sau partenerilor de afaceri. (exemplu de informatie publica brosurile si materialele de pe pagina de internet oficiala). Pentru ca informatia sa fie clasificata ca publica trebuie sa fie etichetata ca atare sub permisiunea Proprietarului Informatiei.

4.7.2. Informatie cu utilizare Interna

Utilizarea acestor informatii este permisa in cadrul CertDigital, iar in unele situatii si in cadrul organizatiilor afiliate (partenerilor CertDigital). Dezvaluirea neautorizata a acestui tip de

informatii catre persoane din afara CertDigital nu este admisa si poate cauza probleme in cadrul organizatiei, clientilor sau partenerilor de afaceri. Acest tip de informatie poate fi raspandita in interiorul CertDigital fara aprobarea in avans a Proprietarului informatiei. (exemple de informatie cu utilizare interna: numerele de telefon cadrul CertDigital si adresele casutelor de e-mail).

4.7.3. Informatie restrictionata

Reprezinta informatia cea mai sensibila si necesita monitorizare permanenta. Se incadreaza la cel mai ridicat nivel de confidentialitate. Divulgarea neautorizata a acestui tip de informatie catre angajatii carora nu le este necesara poate constitui o incalcare a legislatiei si a reglementarilor in vigoare, si poate cauza probleme organizatiei, clientilor sau partenerilor de afaceri. Proprietarul informatiei poate aproba accesul la acest tip de informatii. (exemple de informatie restrictionata: planurile de fuziune si achizitie si informatiile legale protejate de confidentialitatea avocat-client).

4.8. Procedura de personal

4.8.1. Cerinţe privind trecutul, calificarile, experienţa şi acceptarea

Personalul care este nominalizat pentru a face parte din echipa care se ocupa cu emiterea/revocarea certificatelor calificate si a marcilor temporare trebuie sa prezinte dovada indeplinirii cerinţelor legate de trecut, calificari şi experienţa, necesare pentru a indeplini in mod competent şi satisfacator responsabilitaţile postului respectiv.

4.8.2. Proceduri de verificare a trecutului

CertDigital face urmatoarele verificari asupra trecutului personalului care se va ocupa cu emiterea/revocarea certificatelor calificate si a marcilor temporare:

- Confirmarea locului de munca anterior;
- Verificarea referinţelor profesionale;
- Confirmarea celei mai inalte sau relevante instituţii de invaţamânt urmate;
- Studierea cazierului judiciar
- Cautarea rapoartelor financiare;
- Cautarea rapoartelor privind permisul de conducere;
- Cautarea rapoartelor privind asistenţa sociala;

In masura in care, oricare dintre cerinţele impuse nu poate fi satisfacuta, CertDigital va folosi o tehnica de investigaţie care este permisa de lege şi care furnizeaza informaţii asemanatoare.

Factorii implicaţi in verificarea trecutului, ce pot duce la respingerea persoanelor candidate a face parte din echipa sau la luarea de masuri impotriva celor care fac parte din echipa, includ:

- Prezentarea greşita facuta de catre candidat;
- Referinţe personale nefavorabile sau care nu inspira incredere;
- Condamnari;
- Indicii ale lipsei de responsabilitate financiara.

Rapoartele care conţin astfel de informaţii sunt evaluate de personalul de la resurse umane şi securitate, care determina cursul potrivit al acţiunii, in funcţie de tipul, importanţa şi frecvenţa comportamentului dezvaluit de verificarea trecutului. Aceste acţiuni pot include masuri care pot ajunge la incheierea rapoartelor contractuale cu persoana respectiva. Folosirea informaţiilor gasite prin verificarea trecutului pentru a intreprinde astfel de acţiuni este supusa legilor aflate in vigoare.

4.8.3. Cerinţe de pregatire

CertDigital asigura personalului pregatirea necesara pentru a indeplini in mod competent şi satisfacator responsabilitaţile funcţiei. Programele de pregatire ale CertDigital sunt realizate ţinând cont de responsabilitaţile individuale şi includ urmatoarele:

- Concepte de baza despre infrastructura cheii publice;
- Responsabilitaţile funcţiei;
- Politicile şi procedurile de securitate şi operaţionale CertDigital;
- Folosirea şi funcţionarea hardware-ului şi software-ului existent;
- Raportarea şi tratarea cazurilor de incident şi compromis;
- Procedurile de recuperare in caz de dezastru şi de continuare a activitaţii.

4.8.4. Cerinţele şi frecvenţa cursurilor de perfecţionare

CertDigital furnizeaza cursuri de perfecţionare şi de actualizare pentru personal, in masura şi cu frecvenţa care permit asigurarea menţinerii nivelului necesar pentru indeplinirea

competenta şi satisfacatoare a responsabilităţilor de serviciu. Se asigura periodic pregatire de securitate.

4.8.5. Sancţiuni pentru acţiuni neautorizate

Se iau masuri disciplinare adecvate pentru acțiunile neautorizate sau pentru alte violari ale politicilor şi procedurilor CertDigital. Acțiunile disciplinare pot include masuri care duc pâna la incheiere contractului şi sunt luate in funcție de frecvența şi severitatea acțiunilor.

4.8.6. Cerinţe pentru contractarea personalului

In circumstanțe limitate, se pot folosi contractanți sau consultanți independenți pentru a ocupa funcții de incredere. Orice astfel de contractant sau consultant este menținut dupa aceleaşi criterii funcționale şi de securitate care se aplica şi in cazul CertDigital, care se afla intr-o poziție asemanatoare. Contractanții şi consultanții independenți care nu au desavârşit procedurile de verificare a trecutului specificate la punctul 1.2 pot accesa locațiile securizate ale CertDigital numai daca sunt escortați şi supravegheați direct de persoane de incredere.

4.8.7. Documentaţie furnizata personalului

Personalul CertDigital implicat in funcționarea serviciilor infrastructurii cheii publice ale CertDigital trebuie sa citeasca codul de practici şi proceduri şi politica de securitate interna. CertDigital ofera angajaților sai pregatirea necesara şi alta documentație necesara pentru a indeplini competent şi satisfacator responsabilitățile funcției.

5. Administrarea documentului

5.1. Mecanismul de schimbare

Modificarile care pot surveni in continutul acestui document sunt determinate fie de obtinerea unor neconformitati in urma unor revizuiri ale proceselor fie din imbunatatiri periodice ale fluxurilor operationale in cadrul CertDigital.

Implementarea modificarilor actualizeaza numarul de versiune al documentului si data de emitere a Codului de Practici si Proceduri TSA in functie de data la care au fost efectuate modificarile.

CertDigital isi aloca dreptul de a efecta modificari de continut (corectarea erorilor de tipar, modificarea legaturilor URL publicate, schimbari in informatiile de contact etc.) asupra reglementarilor Codului de Practici si Proceduri TSA.

Revizuirile Codului de Proceduri si Practici TSA fara impact sau cu un impact nesemnificativ asupra semnatarilor si partilor de incredere care utilizeaza certificatele emise de CertDigital si informatiile corespunzatoare legate de starea certificatului se pot realiza si inregistra fara a notifica utilizatorii si partile de incredere si nu implica modificarea numarului de versiune a documentului sau data de intrare in vigoare.

Odata cu sintetizarea modificarilor de implementat, Codul de Practici si Proceduri TSA intra in procedura de aprobare interna care se desfasoara pe baza unui comitet format din directorul general, directorul general adjunct si managerii departamentelor tehnice.

Responsabilitatea intretinerii Codului de Practici si Proceduri TSA este alocata catre managerul departamentului care asigura furnizarea serviciilor de certificare. Aferent aprobarii, Codul de Practici si Proceduri TSA este transmis Autoritatii de Reglementare si Supraveghere urmand ca in termen de 10 zile, sa fie publicat si marcat ca fiind valid.

Versiunea curenta a Codului de Practici si Proceduri TSA este datata iunie 2012.

5.2. Mecanismul de publicare si notificare

Documentul Codului de Practici şi Proceduri TSA este disponibil in forma electronica pe site-ul CertDigital la adresa: www.certdigital.ro sau poate fi solicitat prin posta electronica la adresa sediu@centruldecalcul.ro.

Prin interfata online de afisare a informatiilor public, CertDigital pune la dispozitie doua versiuni ale documentului:

- Versiunea curenta;
- Versiunea anterioara;

Documentele de securitate considerate confidenţiale de catre CertDigital sunt inaccesibile publicului.

5.3. Procedura de aprobare a Codului de Practici si Proceduri TSA

Codul de practici si proceduri actualizat este considerat a fi valid din momentul publicarii sale pe site-ul CertDigital.

Utilizatorii care nu agreaza varianta actualizata a Codului de Practici si Proceduri TSA si a modificarilor aferente sunt obligati ca in termen de 15 zile de la data validarii noii versiuni, sa intocmeasca o declaratie in acest sens. In acest caz, CertDigital isi atribuie dreptul de a rezilia contractul de furnizare a serviciilor de de certificare si la revocarea certificatului emis in baza acestuia. Ulterior intervalului de 15 zile de la punerea in vigoare a noii versiuni, CertDigital considera ca implicit acceptul utilizatorilor.