Politica de Certificare CertDigital

EMISA DE:		
DEPARTAMENT	**NUME**	**DATA**
Manager Servicii Electronice	Manager Servicii Electronice	01.01.2016

APROBATA DE:		
DEPARTAMENT	**NUME**	**DATA**
Director General	Director General	01.06.2016

ISTORICUL MODIFICARILOR:			
VERSIUNE	**AUTOR**	**DETALII MODIFICARI**	**DATA:**
1.0.0	Director Tehnic	Publicarea primei versiuni	19.03.2011
1.0.1	Director Tehnic	Adaugarea noilor autoritati de certificare CertDigital Qualified CA Class 3 G2 CertDigital Enterprise CA Class 3 G2 CertDigital NonRepudiation CA Class 4 G2	01.06.2016

LISTA DE DISTRIBUIRE:	
DESTINATAR	**DATA**
Public - Internet	29.03.2011

Cuprins

1. Introducere

Politica de Certificare a CertDigital (CP) descrie regulile şi principiile generale aplicate de CertDigital în procesul de certificare a cheilor publice şi folosire a autorităţii de marcare a timpului (TSA), precum şi a altor servicii de ne-repudiere. Politica de certificare defineşte:

- entităţile implicate în procesele de certificare,
- responsabilităţile şi obligaţiile fiecărei entităţi,
- tipurile de certificate,
- tipurile de confirmări,
- procedurile de verificare a identităţii şi
- aria de aplicabilitate.

Descrierea detaliata a regulilor de mai sus este prezentata în Codul de Practici şi Proceduri (CPP).

Cunoaşterea Politicii de Certificare, precum şi al Codului de Practici şi Proceduri prezintă importanţă în mod special pentru abonaţii şi entităţile partener ale CertDigital.

2. Certificatele

Certificatul este un şir de date (mesaj) care conţine cel puţin numele şi identificatorul autorităţii, identificatorul abonatului, cheia sa publică, perioada de validitate, numărul serial şi semnatura autorităţii emitente.

Certificatele sunt utilizate pentru a lega datele personale ale abonatului de cheile publice specifice. Proprietarul certificatului este, de asemenea, şi proprietarul cheii private, corespunzătoare cheii publice conţinută în certificat. Datele de identificare conţinute în certificat permit altor părţi să determine cu exactitate proprietarul certificatului. Dacă cheia privată este utilizată în timpul semnarii electronice a unui mesaj, destinatarul mesajului poate fi sigur că mesajul a fost creat folosind

cheia privată, corespunzătoare cheii publice conţinută în certificat (deci a fost creată de proprietarul certificatului) şi mesajul nu a fost modificat de către altcineva.

Autoritatea de Certificare CertDigital CA confirmă prin emiterea unui certificat pentru un abonat:

- Identitatea acestuia sau credibilitatea altor date, ca de exemplu adresa căsuţei de poştă electronică;
- Cheia publică conţinută de certificat aparţine abonatului respectiv.

Datorită celor de mai sus, entităţile partener, după recepţia unui mesaj semnat, pot determina cine este proprietarul certificatului care a semnat mesajul şi, opţional, îl pot trage pe acesta la răspundere pentru acţiunile sale sau angajamentele luate.

CertDigital furnizează servicii în concordanţă cu legislaţia şi practicile în domeniu. Cheile autorităţii de certificare sunt protejate folosind module hardware de securitate (Hardware Security Module - HSM), certificate conform FIPS 140-1 si FIPS 140-2 nivel 3. CertDigital implementează controalele fizice şi procedurale ale sistemului.

Autoritatea de Certificare CertDigital emite certificate de diferite Clase, având nivele de credibilitate diferite. Credibilitatea certificatului depinde de procedura de verificare a identităţii abonatului şi de efortul depus de operatorii CertDigital pentru a verifica datele trimise de către solicitant în cererea sa de înregistrare. Clasa certificatului poate, de asemenea, să depindă de Clasa de securitate a serverului sau dispozitivului de reţea pentru care se emite certificatul. Specialiştii CertDigital pot verifica starea tehnică şi Clasa de securitate a sistemului informatic al unui abonat înainte de a emite un certificat din cea mai înaltă Clasă de credibilitate.

Autoritatea de Certificare CertDigital CA emite certificate pentru publicul larg şi furnizează servicii specifice unei infrastructuri de chei publice. Printre cele mai importante aplicaţii ale certificatelor emise de CertDigital CA, se numără (fără a se limita la):

- Semnarea documentelor electronice,
- Securizarea mesajelor de e-mail (poştă electronică),
- Securizarea tranzacţiilor Web,

- Securizarea comunicaţiilor de reţea,
- Semnarea codului pentru aplicaţii,
- Marcarea timpului.

2.1 Certificate de Clasă 1

Certificatele de Clasă 1 sunt emise de Autoritatea de Certificare **Cert Digital Simple CA** si **CertDigital Simple CA G2**. Aceste certificate sunt folosite numai pentru scopuri si utilizari interne şi nu oferă nici o garanţie asupra identităţii subiectului. Certificatele simple sunt destinate în principal pentru testarea performanţei aplicaţiilor sau dispozitivelor înainte de cumpărarea certificatelor finale. Autoritatea de **Certificare Cert Digital Simple CA** si **CertDigital Simple CA G2** emite certificate pentru aproape toate scopurile. În majoritatea cazurilor, în timpul procesului de înregistrare se verifică adresa căsuţei de mesagerie electronică şi/sau numele şi prenumele persoanei fizice sau al reprezentantului persoanei juridice.

Certificatele de Clasa 1 conţin următorul identificator de politică:

{CertDigital}*id-policy(1) id-cp(1)id-Class-1(1)

CertDigital nu îşi asumă nici o obligaţie financiară şi nu oferă nici o garanţie pentru certificatele (şi conţinutul acestora) emise în cadrul politicii de mai sus.

* {CertDigital}=1.3.6.1.4.1.47898= iso(1). identified-organization(3). dod(6). internet(1). private(4). enterprise(1). CertDigital's IANNA assigned number (47898)

2.2 Certificate de Clasă 2

Certificatele de Clasă 2 sunt emise de Autoritatile de Certificare **Cert Digital Organization CA Class 2** si **CertDigital Organization CA Class 2 G2**. Acestea sunt certificate personale şi sunt destinate în principal pentru securizarea corespondenţei electronice sau autentificarea clienţilor în timpul sesiunilor online. Operatorii Autorităţilor de Certificare Cert Digital Organization CA Class 2 si CertDigital Organization CA Class 2 G2 verifică datele furnizate de clienţi în timpul procesului de certificare. Identitatea persoanei fizice solicitante sau a reprezentantului persoanei juridice este supusă unei verificări detaliate. Autenticitatea adresei căsuţei de mesagerie electronică inclusă în certificat este de asemenea verificată.

Certificatele de Clasa 2 conţin următorul identificator de politică:

{CertDigital}.id-policy(1).id-cp(1).id-Class-2(2)

Certificatele emise în cadrul acestei politici oferă garanţii şi responsabilităţi limitate.

2.3 Certificate de Clasă 3

Certificatele de Clasă 3 sunt emise de catre 4 Autoritati de Certificare: **Cert Digital Enterprise CA Class 3, CertDigital Enterprise CA Class 3 G2, Cert Digital Qualified CA Class 3, CertDigital Qualified CA Class 3 G2**.

Certificatele emise în această clasă pot fi certificate calificate sau certificate pentru securizarea obiectelor binare şi protecţia transmisiilor de date utilizând protocoalele IPSec, SSL şi TLS. Operatorii CertDigital verifică datele furnizate de clienţi (organizaţii sau instituţii) în timpul procesului de înregistrare. Toate datele ce urmează a fi incluse în certificat sunt verificate.

Pe baza unui certificat emis de Cert Digital Enterprise CA Class 3, CertDigital Enterprise CA Class 3 G2, Cert Digital Qualified CA Class 3, CertDigital Qualified CA Class 3 G2 se poate determina cu exactitate identitatea unui subiect sau autenticitatea unei organizaţii.

Certificatele calificate emise de Cert Digital Qualified CA Class 3, CertDigital Qualified CA Class 3 G2 pot fi utilizate pentru crearea de semnaturi electronice care să înlocuiască semnaturile olografe.

Certificatele calificate sunt emise de Autoritatile de Certificare **Cert Digital Qualified CA Class 3, CertDigital Qualified CA Class 3 G2**. Aceste certificate sunt conforme cu Directiva 1999/93/EC a Parlamentului European referitoare la Cadrul Comunitar privind Semnatura Electronica, Legea Semnaturii Electronice 455/2001 din România şi Hotărârea de Guvern 1259/Decembrie 2001 privind Normele de Aplicare ale Legii Semnaturii Electronice.

Autoritatile de certificare Cert Digital Enterprise CA Class 3 si Cert Digital Qualified CA Class 3 folosesc un certificat emis cu algoritmul sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) iar CertDigital Enterprise CA Class 3 G2, CertDigital Qualified CA Class 3 G2 folosesc un certificat emis cu algoritmul sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11).

Certificatele de Clasa 3 conţin următorul identificator de politică:

{CertDigital} id-policy(1) id-cp(1)id-Class-3(3)

În plus, pentru certificatele calificate se adaugă identificatorul de politică

itu-t(0).identified-organization(4).etsi(0).qualified-certificate-policies(1456).policy-identifiers(1). qcp-public-with-sscd (1),

pentru certificatele emise de **CertDigital Enterprise CA Class 3 G2** se adauga identificatorul de politica

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline- requirements(2) subject-identity-validated(2)} (2.23.140.1.2.2)

Responsabilitatea financiară a CertDigital pentru datele din certificatele emise în cadrul politicii de mai sus este prezentată în Codul de Practici şi Proceduri (CPP) (a se vedea

http://www.certdigital.ro/repository). Certificatele emise în cadrul acestei politici oferă garanţii şi responsabilităţi complete.

2.4 Certificate de Clasă 4

Certificatele de Clasă 4 sunt emise de Autoritatile de Cert Digital Non-Repudiation CA Class 4 si

CertDigital NonRepudiation CA Class 4 G2. Aceste certificate sunt destinate în principal Autorităţilor de Certificare subordonate sau altor furnizori de servicii de încredere (OCSP sau Autorităţi de Marcare Temporală). Operatorii Cert Digital Non-Repudiation CA Class 4 si CertDigital NonRepudiation CA Class 4 G2 verifică identitatea clienţilor care trebuie să se prezinte personal la unul din ghişeele CertDigital. Se vor verifica împuternicirea din partea firmei, autenticitatea şi corectitudinea documentelor de identitate furnizate precum şi actele organizaţiei. Cert Digital Non-Repudiation CA Class 4 si CertDigital NonRepudiation CA Class 4 G2 acceptă şi documente autentificate de către un notar. Pe baza unui certificat emis de Cert Digital Non-Repudiation CA Class 4 si CertDigital NonRepudiation CA Class 4 G2 se poate determina cu exactitate identitatea unui subiect, autenticitatea unei organizaţii sau credibilitatea unei Autorităţi de Certificare externe. Cheile abonatului ce deţine un certificat de Clasă 4 trebuie protejate utilizând module hardware de securitate (HSM).

Certificatele de Clasă 4 conţin următorul identificator de politică:

{CertDigital} id-policy(1) id-cp(1)id-Class-4(4)

Certificatele emise în cadrul acestei politici oferă garanţii şi responsabilităţi complete.

Abonatul CertDigital poate alege tipul de certificat potrivit nevoilor sale. Tipurile de certificate sunt descrise pe larg în Codul de Practici şi Proceduri (CPP) care poate fi consultat pe site-ul Web al CertDigital. De asemenea, aceste informaţii pot fi primite şi prin poştă electronica trimiţând un mesaj la adresa: office@certdigital.ro.

3. Jetoane de ne-repudiere

Jetoanele de ne-repudiere sunt structuri de date (mesaje) conţinând cel puţin:

- informaţiile furnizate de către client (de exemplu, valoare hash, numărul serial al certificatului, numărul cererii etc.) unei autorităţi de ne-repudiere şi
- semnatura electronica a autorităţii respective.

Autorităţile de ne-repudiere care oferă servicii clienţilor sunt afiliate la CertDigital.

Prin emiterea unui jeton, o autoritate de ne-repudiere confirmă apariţia unui eveniment în momentul creării acestuia sau la un moment de timp anterior. Acest eveniment poate fi: transmiterea unui document, data creării semnaturii etc.

Entitatea parteneră poate verifica, pe baza datelor recepţionate, corectitudinea semnaturii bazându-se pe încrederea în CertDigital CA.

3.1 Mărcile Temporale

Mărcile temporale sunt emise de catre Autoritatile Cert Digital Time Stamping Authority si CertDigital Timestamping Authority G2. Mărcile temporale, ca element de bază în asigurarea ne-repudierii, sunt emise atât persoanelor private cât şi celor aparţinând unei organizaţii. Mărcile temporale pot fi încorporate în:

- semnaturi electronice,
- acceptarea tranzacţiilor electronice,
- arhivarea datelor,
- notarizarea documentelor electronice etc.

Regulile ce stabilesc modul de operare al Autorităţii de Marcare Temporală precum şi alte informaţii suplimentare legate de acest sistem sunt descrise într-un document separat (a se vedea Politica Generala de Marcare Temporala).

Jetonul de marcare temporală conţine următorul identificator de politică:

{CertDigital}*.id-Time-Stamping(2).Id-Policy(1)

---

* {CertDigital}=1.3.6.1.4.1.47898= iso(1). identified-organization(3). dod(6). internet(1). private(4). enterprise(1). CertDigital’s IANNA assigned number (47898)

Responsabilitatea financiară a CertDigital pentru timpul, data şi alte informaţii suplimentare incluse în mărcile temporale emise în cadrul politicii de mai sus este prezentată în Politica Generala de Marcare Temporala CertDigital (a se vedea http://www.certdigital.ro/repository). Cert Digital Time Stamping Authority si CertDigital Timestamping Authority G2 oferă garanţii pentru mărcile temporale emise în limitele specificate în Politica generala de marcare temporala.

3.2 Răspunsul de confirmare OCSP

Răspunsurile OCSP (Online Certificate Status Protocol) sunt emise de Autoritatea **CertDigital Validation Authority G2**. Răspunsurile OCSP sunt utilizate în principal pentru determinarea stării certificatelor. Aceste servicii sunt disponibile public şi reprezintă o alternativă la Listele de Certificate Revocate (Certificate Revocation List – CRL). CertDigital Validation Authority G2 oferă garanţii pentru răspunsurile OCSP emise, în limitele descrise în CPP. Modul de funcţionare al autorităţii OCSP şi informaţii suplimentare privind acest serviciu sunt prezentate pe pagina web (a se vedea http://www.certdigital.ro) şi în CPP.

4. Garantiile oferite de CertDigital

În funcţie de tipul de certificat emis, CertDigital garantează că va depune efortul necesar pentru a verifica în mod corespunzător informaţiile incluse în cadrul certificatelor (a se vedea Codul de Practici şi Proceduri - Capitolul 2.1.1: Obligaţii). Verificarea informaţiilor este importantă în primul rând pentru entităţile partenere ce primesc mesaje de la un abonat care se identifică printr-un certificat digital calificat emis de CertDigital. În consecinţă, CertDigital este responsabilă din punct de vedere financiar pentru pagubele rezultate ca urmare a neglijenţei sau erorilor comise de CertDigital în ceea ce priveşte aceste tipuri de certificate. Responsabilităţile CertDigital depind de clasa certificatului abonatului, iar responsabilitatea este atât faţă de abonat cât şi faţă de entităţile partenere care au încredere în informaţiile din certificat (a se vedea Codul de Practici şi Proceduri).

Garanţiile CertDigital pot fi limitate de anumite restricţii. Aceste restricţii sunt aduse la cunoştinţă abonatului care confirmă acest lucru în cadrul unei declaraţii (a se vedea declaraţia de Acceptare a Certificatului). CertDigital garantează unicitatea semnaturilor electronice pentru abonaţii săi.

5. Acceptarea certificatului

Responsabilităţile şi garanţiile CertDigital se aplică din momentul acceptării certificatului de către abonat. Modalitatea de furnizare a certificatului şi acceptanţa certificatului sunt descrise în Codul de Practici şi Proceduri (a se vedea capitolul 3.5 Acceptarea Certificatului) şi sunt detaliate în acordurile încheiate cu abonaţii.

6. Serviciul de certificare

CertDigital furnizează patru servicii de bază:

I. înregistrarea,

II. emiterea unui certificat digital,

III. reînnoirea unui certificat,

IV. revocarea unui certificat şi

V. verificarea stării unui certificat.

CertDigital oferă şi următoarele servicii de ne-repudiere:

VI. Autoritate de Marcare Temporală,

VII. Serviciu de validare on-line a stării certificatelor digitale.

Înregistrarea are ca scop verificarea identităţii unui abonat şi precedă operaţiunea de emitere a certificatului (a se vedea Codul de Practici şi Proceduri, capitolul 3.1 Cererea unui certificat şi Capitolul 3.2 Emiterea certificatului digital).

Reînnoirea unui certificat are loc atunci când un abonat înregistrat deja doreşte să obţină un certificat pentru o aceeaşi cheie publică cu modificarea perioadei de valabilitate (a se vedea Codul de Practici şi Proceduri, Capitolul 3.7 Prelungirea perioadei de valabilitate pentru un certificate valid).

Revocarea unui certificat are loc atunci când cheia privată corespunzătoare cheii publice din certificatul digital a fost compromisă sau este susceptibilă că ar putea fi compromisă (a se vedea Codul de Practici şi Proceduri, Capitolul 3.6 Revocarea unui certificat).

Verific area stării unui c ertificat este un serviciu prin care CertDigital confirmă validitatea unui certificat digital, folosind Listele de Certificate Revocate (CRL) emise de autorităţile afiliate. Verificarea stării unui certificat se poate realiza şi prin intermediul serviciului de validare on-line a stării certificatelor (a se vedea Codul de Practici şi Proceduri).

CertDigital permite ca fiecare pereche de chei (privată-publică) să fie generată de către abonat. CertDigital poate face recomandări cu privire la dispozitivele pentru generarea cheilor. În anumite condiţii specifice, CertDigital poate genera perechi de chei unice şi livra aceste chei abonaţilor.

7. Entitatea Partener

Entitatea partener este obligată să verifice în mod corespunzător fiecare semnatură electronică de pe documentele recepţionate (inclusiv certificatul digital). Pe timpul procesului de verificare, entitatea partener trebuie să utilizeze procedurile şi resursele puse la dispoziţie de CertDigital. Acestea specifică, printre altele, faptul că trebuie verificată lista de certificate revocate publicată de CertDigital şi căile de certificare permise (a se vedea Codul de Practici şi Proceduri, Capitolul 1.4.2 Autoritatea de inregistrare).

Fiecare document pentru care există probleme la verificarea semnaturii digitale trebuie să fie respins şi trebuie să fie verificat prin alte modalităţi sau proceduri, de exemplu verificarea documentului la un notar.

8. Abonatul

Abonatul este obligat să păstreze în siguranţă cheia sa privată, pentru a preveni accesul neautorizat la aceasta al unei terţe părţi. În cazul în care există bănuiala că a fost accesată de o terţă parte, abonatul este obligat să anunţe imediat autoritatea care a emis certificatul sau digital. Informaţiile furnizate autorităţii trebuie să fie suficiente pentru a determina cu exactitate identitatea persoanei căreia i se va revoca certificatul digital.

9. Actualizarea politicii de certificare

Politica de certificare a CertDigital se poate modifica periodic. Aceste modificări vor fi disponibile tuturor abonaţilor prin intermediul site-lui Web al CertDigital. Abonaţii care nu acceptă modificările aduse politicii de certificare trebuie să trimită către CertDigital o declaraţie în acest sens şi să renunţe la serviciile oferite de CertDigital.

10. Taxe

Serviciile de certificare furnizate de CertDigital sunt disponibile comercial. Tarifele pentru aceste servicii depind de clasa certificatelor emise sau deţinute de un abonat şi de tipul de serviciu cerut. Tarifele sunt prezentate în listele de preţuri, disponibile pe site-ul CertDigital (http://www.certdigital.ro).