

Declarația practicilor de certificare a CERTDIGITAL ROOT CA G4

EMISA DE:			
DEPARTAMENT	**NUME**	**SEMNATURA**	**DATA**
MANGEMENTUL POLITICILOR SI PROCEDURILOR	Ofițer de Securitate IT		01/06/2023

APROBATA DE:			
DEPARTAMENT	**NUME**	**SEMNATURA**	**DATA**
MANGEMENTUL POLITICILOR SI PROCEDURILOR	Director Tehnic		05/06/2023

ISTORICUL MODIFICARILOR:			
VERSIUNE	**AUTOR**	**DETALII MODIFICARI**	**DATA:**
1.0	Ofițer de Securitate IT	Publicare primei versiuni a documentului	05/06/2023

Cuprins

1. Introducere 11
1.1. Elemente componente 11
1.2. Numele și identificarea documentului 11
1.3. Participanții la PKI 11
1.3.1. Autoritățile de certificare 12
1.3.2. Autoritățile de înregistrare 13
1.3.3. Abonații 13
1.3.4. Părțile 13
1.3.5. Alți participanți 13
1.4. Utilizarea certificatului 14
1.4.1 Utilizarea adecvată a certificatului 14
1.4.2 Utilizări interzise ale certificatelor 15
1.5 Administrarea politicilor 15
1.5.1 Organizația care administrează documentul 15
1.5.2 Persoana de contact 15
1.5.3 Persoana care determină adecvarea CPS pentru politică 15
1.5.4 Persoana care determină adecvarea CPS pentru politică 16
1.6 Definiții și acronime Definiții 16
2. Responsabilități de publicare și depozit 18
2.1. Depozit 18
2.2 Publicarea informațiilor de certificare 19
2.3 Timpul sau frecvența publicării 20
2.4 Controalele de acces pe depozite 20
3. Identificarea și autentificarea 21
3.1 Denumirea 21
3.1.1 Tipuri de nume 21
3.1.2 Necesitatea ca numele să aibă semnificație 21
3.1.3 Anonimitatea sau pseudonimitatea abonaților 22
3.1.4 Reguli pentru interpretarea diferitelor formulare de nume 22
3.1.5 Unicitatea numelor 22

3.1.6 Recunoașterea, autentificarea și rolul mărcilor comerciale 22
3.2 Validarea inițială a identității 22
3.2.1 Metoda de a dovedi posesia cheii private 22
3.2.2 Autentificarea identității organizației 23
3.3.1 Identificarea și autentificarea pentru re-cheie de rutină 23
3.3.2 Identificarea și autentificarea pentru re-cheie după revocare 23
3.4 Identificarea și autentificarea cererii de revocare 23
4 Cerințe operaționale ale ciclului de viață al certificatului 24
4.1 Aplicarea certificatului 24
4.1.1 Cine poate depune o cerere de certificat 24
4.1.2 Procesul de înscriere și responsabilitățile 24
4.2 Prelucrarea cererilor de certificate 25
4.2.1 Efectuarea funcțiilor de identificare și autentificare 25
4.2.2 Aprobarea sau respingerea cererilor de certificate 25
4.2.3 Timpul de procesare a cererilor de certificate 25
4.3 Eliberarea certificatului 25
4.3.1 Acțiunile CA în cursul emiterii certificatului 25
4.3.2 Notificarea către abonat de către CA a eliberării certificatului 25
4.4 Acceptarea certificatului 26
4.4.1 Desfășurarea acceptării certificatului 26
4.4.2 Publicarea certificatului de către CA 26
4.4.3 Notificarea eliberării certificatului de către CA altor entități 26
4.5 Utilizarea perechii de chei și a certificatului 26
4.5.1 Cheia privată a abonatului și utilizarea certificatului 26
4.5.2 Utilizarea cheii publice a părții publice și utilizarea certificatului 26
4.6 Reînnoirea certificatului 27
4.7 Recheierea certificatului 27
4.8 Modificarea certificatului 27
4.9 Revocarea și suspendarea certificatului 27
4.9.1 Circumstanțele pentru revocare 27
4.9.2 Cine poate cere revocarea 28
4.9.3 Procedura pentru cererea de revocare 28
4.9.4 Perioada de grație a cererii de revocare 28

4.9.5 Timpul în care CA trebuie să proceseze cererea de revocare 29
4.9.6 Cerințele de verificare a revocării pentru părțile implicate 29
4.9.7 Frecvența emiterii CRL 29
4.9.8 Latența maximă pentru CRL 29
4.9.9 Disponibilitate on-line de revocare / verificare stare 29
4.9.10 Cerințe de verificare on-line de revocare 30
4.9.11 Alte forme de anunțuri de revocare disponibile 30
4.9.12 Cerințe speciale privind compromisul cheie 30
4.9.13 Circumstanțe pentru suspendare 30
4.9.14 Cine poate solicita suspendarea 30
4.9.15 Procedura de suspendare a cererii 30
4.9.16 Limitele perioadei de suspendare 30
4.10 Servicii de stare a certificatului 31
4.10.1 Caracteristicile operaționale 31
4.10.2 Disponibilitatea serviciului 31
4.10.3 Caracteristici opționale 31
4.11 Încheierea abonamentului 31
4.12 Key escrow și recuperare 31
5. Facilități, management și controale operaționale 31
5.1 Controale fizice 32
5.1.1 Localizarea și construcția amplasamentului 32
5.1.2 Accesul fizic 33
5.1.3 Putere și aer condiționat 34
5.1.4 Expunerea la apă 34
5.1.5 Prevenirea și protecția împotriva incendiilor 34
5.1.6 Depozitare media 34
5.1.7 Eliminarea deșeurilor 35
5.1.8 Supravegherea în afara amplasamentului 35
5.2 Controale procedurale 35
5.2.1 Roluri de încredere 35
5.2.2 Numărul de persoane necesare pentru fiecare sarcină 37
5.2.3 Identificarea și autentificarea pentru fiecare rol 37
5.2.4 Roluri care necesită separarea sarcinilor 37

5.3 Controlul personalului 37
5.3.1 Cerințe privind calificările, experiența și cerințele de verificare 38
5.3.2 Proceduri de verificare de fond 38
5.3.3 Cerințe de instruire 38
5.3.4 Frecvența și cerințele de recalificare 39
5.3.5 Frecvența și secvența de rotație a lucrării 39
5.3.6 Sancțiuni pentru acțiuni neautorizate 39
5.3.7 Cerințele contractorului independent 39
5.3.8 Documentația furnizată personalului 40
5.4 Procedurile de înregistrare a auditului 40
5.4.1 Tipuri de evenimente înregistrate 40
5.4.2 Frecvența jurnalului de prelucrare 42
5.4.3 Perioada de păstrare pentru jurnalul de audit 43
5.4.4 Protecția jurnalului de audit 43
5.4.5 Proceduri de salvare a jurnalului de audit 43
5.4.6 Sistemul de colectare a auditului (intern/extern) 44
5.4.7 Notificarea subiectului care cauzează evenimente 44
5.4.8 Evaluări de vulnerabilitate 44
5.5 Arhivarea înregistrărilor 44
5.5.1 Tipuri de înregistrări arhivate 45
5.5.2 Perioada de păstrare pentru arhivă 45
5.5.3 Protecția arhivei 45
5.5.4 Proceduri de salvare a arhivelor 46
5.5.5 Cerințe pentru marcarea temporală a înregistrărilor 46
5.5.6 Sistemul de colectare a arhivelor (intern sau extern) 46
5.5.7 Proceduri de obținere și verificare a informațiilor de arhivă 46
5.6 Schimbarea cheilor 46
5.7 Recuperarea după compromiteri și dezastre 47
5.7.1 Procedurile de manipulare a incidentelor și compromisurilor 47
5.7.2 Resursele de calcul, software-ul și/sau datele sunt corupte 47
5.7.3 Procedura cheii private a entității compromisă 49
5.7.4 Capacitățile de continuitate a activității după un dezastru 50
5.8 Terminarea CA sau RA 50

6. Controalele tehnice de securitate 52
6.1 Generarea și instalarea perechilor de chei 52
6.1.1 Generarea perechii de chei 53
6.1.2 Livrarea cheii private către abonat 55
6.1.3 Livrarea cheii publice către emitentul certificatului 55
6.1.4 Furnizarea de chei publice CA către părțile implicate 55
6.1.5 Dimensiunile cheilor 56
6.1.6 Generarea și verificarea parametrilor cheilor publice 56
6.1.7 Obiectivele cheie de utilizare (conform câmpului de utilizare al cheii X.509 v3) 56
6.2 Protecția cheilor private și controlul ingineriei modulului criptografic 57
6.2.1 Standardele și comenzile modulului criptografic 58
6.2.2 Controlul multi-personal al cheii private 58
6.2.3 Private Key escrow 59
6.2.4 Backup-ul cheii private 60
6.2.5 Arhivarea cheii private 60
6.2.6 Transferul cheii private în sau din modulul criptografic 60
6.2.7 Depozitarea cheii private pe modulul criptografic 61
6.2.8 Metoda de activare a cheii private 61
6.2.9 Metoda de dezactivare a cheii private 61
6.2.10 Metoda de distrugere a cheii private 62
6.2.11 Evaluarea modulului criptografic 62
6.3 Alte aspecte ale gestionării perechii de chei 62
6.3.1 Arhivarea cheilor publice 63
6.3.2 Perioadele de funcționare a certificatului și perioadele de utilizare a perechilor de chei 63
6.4 Datele de activare 64
6.4.1 Generarea și instalarea de date de activare 64
6.4.2 Protecția datelor de activare 65
6.4.3 Alte aspecte ale datelor de activare 65
6.5 Controalele de securitate ale calculatoarelor 65
6.5.1 Cerințe tehnice specifice privind securitatea calculatoarelor 65
6.5.2 Evaluarea securității calculatorului 67
6.6. Controale tehnice pentru ciclul de viață 67
6.6.1 Controlul dezvoltării sistemului 67

6.6.2 Controalele de management al securității 67
6.6.3 Controalele de securitate a ciclului de viață 68
6.7 Controalele de securitate a rețelei 68
6.8 Timp-Stamping 70
7. Profiluri CER, CRL și OCSP 70
7.1 Profil certificat 70
7.1.1 Numărul (numerele) versiunii 73
7.1.2 Extensiile certificatelor 73
7.1.3 Identificatori de obiect al algoritmului 75
7.1.4 Formulare de nume 75
7.1.5 Constrângeri de nume 75
7.1.6 Identificatorul obiectului politicii certificatului 76
7.1.7 Utilizarea extensiei Constrângeri de politică 76
7.1.8 Sintaxa și semantica calificărilor de politică 76
7.1.9 Semantica de procesare a extinderii critice a Certificatelor de Certificare 76
7.2 Profilul CRL 77
7.2.1 Numărul (numerele) versiunii 77
7.2.2 Extensii de intrare pentru CRL și lista de certificate 77
7.3 Profil OCSP 78
7.3.1 Numărul (versiunile) versiuni 78
7.3.2 Extensii OCSP 78
8. Audit de conformitate și alte evaluări 79
8.1 Frecvența sau circumstanțele de evaluare 79
8.2 Identitatea / calificările evaluatorului 79
8.3 Relația evaluatorului cu entitatea evaluată 79
8.4 Subiectele acoperite de evaluare 79
8.5 Acțiuni întreprinse ca urmare a deficienței 80
8.6 Comunicarea rezultatelor 80
9 Alte probleme de afaceri și juridice 80
9.1 Taxe 80
9.1.1 Taxele de emitere și reînnoire a certificatului 81
9.1.2 Taxele de acces la certificat 81
9.1.3 Cheltuieli de revocare sau de acces la informații privind statutul 81

9.1.4 Taxe pentru alte servicii 81
9.1.5 Politica de rambursare 81
9.2 Responsabilitatea financiară 81
9.2.1 Acoperire de asigurare 81
9.2.2 Alte active 81
9.2.3 Asigurarea sau acoperirea garanției pentru entitățile finale 81
9.3 Confidențialitatea informațiilor despre afaceri 82
9.3.1 Domeniul de aplicare a informațiilor confidențiale 82
9.3.2 Informații care nu intră sub incidența informațiilor confidențiale 83
9.3.3 Responsabilitatea de a proteja informațiile confidențiale 84
9.4 Confidențialitatea informațiilor personale 84
9.5 Drepturi de proprietate intelectuală 84
9.6 Reprezentări și garanții 85
9.6.1 Reprezentări și garanții ale CA 85
9.6.2 Reprezentări și garanții ale RA 85
9.6.3 Reprezentări și garanții ale abonaților 85
9.6.4 Reprezentări și garanții ale partidelor invocate 85
9.6.5 Reprezentări și garanții ale altor participanți 85
9.7 Renunțarea la garanții 86
9.8 Limitarea răspunderii 86
9.9 Despăgubirile 86
9.10 Termen și reziliere 86
9.10.1 Termene 86
9.10.2 Rezilierea 86
9.10.3 Efectul terminării și al supraviețuirii 86
9.11 Observații individuale și comunicări cu participanții 87
9.12 Modificări 87
9.12.1 Procedura de modificare 87
9.12.2 Mecanismul de notificare și perioada 87
9.12.3 Circumstanțele în care OID trebuie schimbat 88
9.13 Dispoziții privind soluționarea litigiilor 88
9.14 Legea aplicabilă 88
9.15 Respectarea legislației în vigoare 88

9.16 Dispoziții diverse 88

1. Introducere

Declarația practicilor de certificare pentru CERTDIGITAL ROOT CA G4 (denumită în continuare CPS ROOT CA G4 sau CPS) detaliază politica de certificare și practicile pe care CERTDIGITAL le aplică pentru emiterea certificatelor digitale de către CA ROOT G4 pentru autoritățile de certificare subordonate.

Structura și conținutul CPS ROOT CA G4 respectă recomandările RFC 3647, ETSI EN 319 411-1 V1.1.1 (2016-02) și ETSI EN 319 411-2 V2.1.1 (2016-02).

1.1. Elemente componente

CERTDIGITAL, Autoritățile de Certificare și funcționarea asociate a partenerilor depind de CPS ROOT CA G4 pentru emiterea de certificate digitale către subordonații autorităților de certificare. De asemenea, acest document descrie regulile generale pentru furnizarea de servicii de certificare, cum ar fi: înregistrarea subiectului, certificarea cheii publice, recheierea cheilor și certificatelor și revocarea certificatelor.

1.2. Numele și identificarea documentului

Titlul acestui document este declarația de practici de certificare pentru CERTDIGITAL ROOT CA G4, denumită în continuare CPS ROOT CA G4 sau CPS.

Formularul electronic al acestui document este disponibil în Repository, la adresa https://www.certdigital.ro/repository.

1.3. Participanții la PKI

CPS ROOT CA G4 reglementează cele mai importante relații dintre entitățile care aparțin CERTDIGITAL, echipele de consultanță (inclusiv auditorii) și clienții (utilizatorii serviciilor furnizate):

- Autoritățile de certificare:
  - CERTDIGITAL ROOT CA G4
  - CERTDIGITAL QUALIFIED CA G4
- Autoritatea de Înregistrare,
- Repository,
- Autoritățile care emite confirmări electronice de non-repudiere,
- Subiectele,
- Abonații,
- Partenerii,

Furnizori relevanți pentru CERTDIGITAL în ceea ce privește emiterea și gestionarea certificatelor digitale CERTDIGITAL oferă servicii de certificare pentru fiecare persoană fizică sau juridică care acceptă regulamentul prezentului CPS. Scopul acestor practici (care includ procedurile de generare a cheilor, procedura de emitere a certificatelor și securitatea sistemului de informații) este de a asigura utilizatorilor serviciilor CERTDIGITAL că nivelurile de credibilitate declarate legate de certificatele emise respectă practicile autorităților de certificare.

1.3.1. Autoritățile de certificare

CERTDIGITAL ROOT CA G4 este Autoritatea Primară de Certificare pentru domeniul CERTDIGITAL. Celelalte Autorități de Certificare din acest domeniu sunt subordonate CERTDIGITAL ROOT CA G4 (Figura 1).

În prezent, următoarele autorități de certificare sunt subordonate CERTDIGITAL ROOT CA G4:

- CERTDIGITAL QUALIFIED CA G4 identificată de OID: 1.3.6.1.4.1.47898.4.2.2.1.2

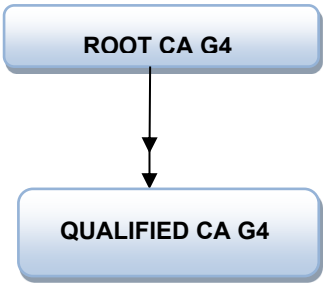


Figura 1 : Structura domeniului de certificare CERTDIGITAL

Autoritatea de certificare primară, CERTDIGITAL ROOT CA G4, poate înregistra și emite certificate numai autorităților de certificare și autorităților care emite confirmări electronice de non-repudiere care aparțin domeniului CERTDIGITAL. Înainte de începerea activității, fiecare autoritate de certificare subordonată va trimite o cerere autorității primare de certificare, CERTDIGITAL ROOT CA G4, pentru emiterea certificatului de înregistrare și a cheii publice (a se vedea și procedurile descrise în capitolul 6.1 al acestui document).

1.3.2. Autoritățile de înregistrare

Autoritatea de Înregistrare primește, verifică și aprobă sau respinge cererile de înregistrare și de emitere a certificatului, precum și cererile de revocare a certificatului. Verificarea cererilor intenționează să autentifice (pe baza documentelor anexate în cereri) atât solicitantul, cât și datele specificate în cerere. De asemenea, Autoritatea de Înregistrare poate depune cereri către Autoritatea de Certificare corespunzătoare pentru a anula cererea unui Subiect și pentru a-și retrage certificatul.

Autoritatea de Înregistrare este administrată de CERTDIGITAL.

1.3.3. Abonații

Abonatul este CERTDIGITAL, ca operator de autorități de certificare subordonat CERTDIGITAL ROOT CA G4.

Subiecții pot fi fie autorități de certificare, fie autorități care emite confirmări electronice de non-repudiere aparținând domeniului CERTDIGITAL.

1.3.4. Părțile

O parte bazată pe utilizarea serviciilor CERTDIGITAL poate fi orice entitate care ia decizii bazate pe corectitudinea legăturii dintre identitatea unui subiect și cheia publică.

O parte invocată este responsabilă pentru modul în care este verificată starea actuală a certificatului unui subiect. O astfel de decizie se ia de fiecare dată când o parte invocată este dispusă să utilizeze un certificat, să verifice o semnătură electronică, să verifice identitatea sursei sau autorul unui mesaj sau să creeze un canal de comunicare securizat cu Subiectul certificatului . O parte invocată va folosi informațiile dintr-un certificat pentru a decide dacă un certificat a fost utilizat în conformitate cu scopul declarat.

1.3.5. Alți participanți

Furnizorii de servicii CERTDIGITAL sunt: furnizori externi care sprijină activitățile CERTDIGITAL în baza unui acord contractual semnat.

Furnizori de dispozitiv de creare a semnăturilor calificate: furnizarea de module criptografice este asigurată de furnizori externi care susțin activitățile CERTDIGITAL în baza unui acord contractual semnat.

1.4. Utilizarea certificatului

Domeniul de aplicabilitate a certificatului stabilește scopul pentru care poate fi utilizat un certificat. Acest domeniu de aplicare este definit de două elemente:

- Unul care definește aplicabilitatea certificatului (de exemplu: semnătură electronică, confidențialitate)
- Un altul care implică o listă sau o descriere a aplicațiilor permise și interzise.

Partea invocată este responsabilă pentru stabilirea nivelului de credibilitate necesar pentru ca un certificat să poată fi utilizat într-un anumit scop. Partea invocată va decide, luând în considerare factorul de risc semnificativ, ce tip de certificat emis de CERTDIGITAL îndeplinește cererile formulate. Subiecții cunosc solicitările părților invocate (de exemplu, aceste cereri ar putea fi publicate ca o politică de semnătură sau ca politică de securitate a informațiilor) și apoi să ceară CERTDIGITAL să emită certificate corespunzătoare acestor solicitări.

1.4.1 Utilizarea adecvată a certificatului

CERTDIGITAL ROOT CA G4 poate înregistra și emite certificate doar autorităților de certificare și autorităților care emite confirmări electronice de non-repudiere aparținând domeniului CERTDIGITAL.

Certificatele pot fi utilizate în aplicații care îndeplinesc cel puțin următoarele condiții:

- Gestionarea corectă a cheilor publice și private,
- Certificatele și cheile publice asociate sunt utilizate în conformitate cu scopul declarat, confirmat de CERTDIGITAL,
- Au mecanisme integrate de verificare a statutului certificatului, de creare a căii de certificare și de control al validării (disponibilitatea semnăturii, data de expirare etc.)
- Oferă utilizatorilor informații relevante privind certificatele și statutul acestora.

Cererile pentru care Certificatul este considerat de încredere vor fi decise de către Părțile Întemeiate pe baza naturii și scopului (inclusiv utilizarea-cheie) a Certificatului, inclusiv orice limitare aplicabilă așa cum este ea înscrisă în Certificat.

1.4.2 Utilizări interzise ale certificatelor

Este interzisă utilizarea certificatelor CERTDIGITAL în alte scopuri decât cele menționate și în aplicațiile care nu îndeplinesc condițiile minime specificate în Capitolul 1.4.1.

1.5 Administrarea politicilor

1.5.1 Organizația care administrează documentul

Nume	S.C. CENTRUL DE CALCUL S.A. Sediul: Str. Tudor Vladimirescu , Nr. 17, Targu Jiu, Gorj, Romania, Cod poștal : 210132 Nr. Registrul Comerțului: J18/103/1991 Codul de înregistrare fiscală: RO2163993 Sediu social: : Str. Tudor Vladimirescu , Nr. 17 , Targu Jiu, Gorj, Romania, Cod poștal : 210132
Telefon	(+40253)214767
Fax	(+40253)213409
e-mail	office@certdigital.ro
Web	www.certdigital.ro

Tabelul 1.5.1 Organizația care administrează documentul

1.5.2 Persoana de contact

Nume	Compartimentul de management al politicilor și procedurilor (CMPP)
Phone	(+40253)214767
Fax	(+40253)213409
e-mail	office@certdigital.ro
Web	www.certdigital.ro

Tabelul 1.5.2 Persoana de contact

1.5.3 Persoana care determină adecvarea CPS pentru politică

Nume	Compartimentul de management al politicilor și procedurilor (CMPP)
Phone	(+40253)214767
Fax	(+40253)213409
e-mail	office@certdigital.ro
Web	www.certdigital.ro

Table 1.5.3 Persoana care determină adecvarea CPS pentru politică

1.5.4 Persoana care determină adecvarea CPS pentru politică

Departamentul de gestionare a politicilor și procedurilor este responsabil de aprobarea CPS.

Subiecții trebuie să respecte numai cerințele CPS aplicabile în prezent.

Subiecții / abonații care nu acceptă termenii și regulamentele noi modificate ale CPS fac o declarație adecvată în termen de 15 zile de la data aprobării noului versiune CPS. Acesta va duce la rezilierea contractului privind serviciile de certificare furnizate și la revocarea certificatului eliberat pe teren.

1.6 Definiții și acronime Definiții

Auditor - persoană care evaluează conformitatea cu cerințele specificate în documentele de cerințe date
Autentificare - proces electronic care permite identificarea electronică a unei persoane fizice sau juridice sau originea și integritatea datelor în formă electronică să fie confirmată

Certificat - cheia publică a unui utilizator, împreună cu alte informații, care au fost făcute imposibile prin chestionare cu cheia privată a autorității de certificare care a emis-o

Lista de certificate de revocare (CRL) - lista semnată care indică un set de certificate care nu mai sunt considerate valabile de către emitentul de certificare

Autoritatea de certificare - (CARL) - lista de revocări care conține o listă de certificări CA emise autorităților de certificare care nu mai sunt considerate valabile de către declarația de

Practici de certificare (CPS) a emitentului certificatului Practici pe care o Autoritate de Certificare utilizata în procesul de gestionare se angajează să emită certificate de revocare, reînnoire sau reînnoire a certificatului

Certificare încrucișată - certificat utilizat pentru stabilirea unei relații de încredere între două autorități de certificare

Semnătura electronică - date în format electronic care sunt atașate sau asociate logic cu alte date din Electronică și care este utilizat de semnatar pentru a semna

Identificatorul de obiect (OID) - identificator alfanumeric / numeric înregistrat în conformitate cu standardul ISO / IEC 9834 și descriind în mod unic un obiect specificat sau clasa sa.

Cheia privată - una dintre cheile asimetrice aparținând unui subiect și utilizată numai de acel subiect. În cazul sistemului cheie asimetric, o cheie privată descrie transformarea unei semnături. În cazul sistemului de criptare asimetric, o cheie privată descrie transformarea decriptare. Cheia privată este (1) cheia a cărei scop este decriptarea sau crearea de semnături, pentru utilizarea exclusivă a proprietarului; (2) acea cheie dintr-o pereche de chei care este cunoscută numai proprietarului.

Cheie publică - una dintre cheile de pe perechea de chei asimetrice a unui subiect, care poate fi accesibilă publicului. În cazul sistemului de criptografie asimetrică, cheia publică definește transformarea verificării semnăturii. În cazul criptării asimetrice, o cheie publică definește transformarea de criptare a mesajelor.

Infrastructura cu chei publice (PKI) - arhitectură, tehnici, practici și proceduri care sprijină în mod colectiv implementarea și funcționarea sistemelor de criptografie bazate pe certificat public; PKI este alcătuit din hardware, software, baze de date, resurse de rețea, proceduri de securitate și obligații legale legate împreună, care colaborează pentru a furniza și implementa servicii de certificare, precum și alte servicii asociate infrastructurii (de exemplu, timbru de timp).

Dispozitiv de creare a semnăturilor electronice calificate înseamnă un dispozitiv de creare a semnăturii electronice care îndeplinește cerințele stabilite în anexa II la Regulamentul (UE) nr. 910/2014 **Consiliul (UE) nr. 910/2014** AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93 / CE

Rădăcina CA se află la cel mai înalt nivel din domeniul TSP și care se utilizează pentru a semna CA (sub) subordonat

Subiect: entitate identificată într-un certificat ca deținător al cheii private asociate cu cheia publică prezentată în certificatul

Subordonat CA - Este semnat de autoritatea de bază sau de un alt abonat CA

Subordonat - persoană juridică sau fizică legată de un furnizor de servicii de asigurare a încrederii față de orice obligație a abonatului

Furnizor de servicii de încredere - o persoană fizică sau juridică care oferă unul sau mai multe servicii de încredere Sau ca furnizor de servicii de încredere necalificat;

Acronime

CA Autoritatea de certificare

CPS Procedura de certificare

CRL Lista certificatelor de revocare

CARL Lista autorităților de certificare revocate

DN Nume distincte

NIMB Institutul Național de Metrologie București

OCSP Protocolul de stare certificat on-line

PKI Infrastructura cheii publice

CMPP Compartimentul de management al politicilor și procedurilor

QSCD Dispozitiv de creare a semnăturilor electronice calificate

RSA Algoritmul criptografic asimetric Adleman, Rivest, Shamir

TSP Furnizor de servicii de încredere

UTC Ora universală coordonată

2. Responsabilități de publicare și depozit

2.1. Depozit

Depozitul este disponibil on-line: https://www.certdigital.ro/repository si conține:

- Declarația privind practica certificatului pentru CA-urile operate de CERTDIGITAL
- Autoritățile de baza (Root CA) și autoritățile de certificare subordonare
- Certificate ale subiecților
- Liste certificatelor revocate
- Termeni și condiții pentru utilizarea certificatelor digitale
- Șabloane pentru contracte cu subiecți și abonați

Depozitul este gestionat și controlat de CERTDIGITAL si drept urmare CERTDIGITAL se angajează:

- Asigure toate eforturile necesare pentru a se asigura că toate certificatele publicate în Depozit aparținând Subiecților înregistrați în certificate și că toți Subiecții și-au dat acordul cu privire la aceste certificate,
- Să se asigure că certificatele autorităților de certificare, autoritatea de înregistrare aparținând domeniului CERTDIGITAL, precum și certificatele subiectului sunt publicate și arhivate la timp,
- Asigurarea publicării și arhivării CPS, a listelor de aplicații și a dispozitivelor recomandate,
- Oferiți acces la informații despre starea certificatului prin publicarea listelor de revocare a certificatului (CRL), prin intermediul serverelor OCSP sau al solicitărilor HTTP,
- Asigurarea accesului permanent la informații în Depozit pentru Autoritățile de Certificare, Autoritatea de Înregistrare, Subiecții și Părțile învinuite,
- Publicarea CRL sau a altor informații în timp util și în conformitate cu termenele limită menționate în CPS,
- Asigurați accesul sigur și controlat la informațiile din Depozit.

2.2 Publicarea informațiilor de certificare

La emitere, în cadrul repozitorului se publică un certificat digital.

Pentru toate certificatele emise, informațiile despre starea certificatului sunt disponibile prin CRL-uri, iar serviciile de validare a certificatelor sunt furnizate de CERTDIGITAL.

Disponibilitate

Disponibilitatea depozitului de documente și a repozitorului CRL combinat este proiectat să depășească 99,8% din programul de lucru - definit ca 24 de ore pe zi, șapte zile pe săptămână, cu excepția perioadelor de întreținere planificate.

Perioadele planificate de întreținere vor fi anunțate pe https://www.certdigital.ro cu cel puțin 24 de ore în avans.

In caz de indisponibilitate datorata unei catastrofe, defecțiuni ale infrastructurii aflate in afara controlului CERTDIGITAL sau din orice alt motiv, CERTDIGITAL va depune toate eforturile pentru a restabili serviciul in termen de 5 zile lucrătoare.

Certificatele expirate care au fost revocate înainte de expirarea lor nu sunt eliminate din listele de revocare

2.3 Timpul sau frecvența publicării

Informațiile publicate de CERTDIGITAL sunt actualizate cu următoarea frecvență:

- CPS - vezi capitolul 1.5,
- Certificatul autorităților de certificare - după emiterea unui nou certificat;
- Lista de revocare a certificatelor este creată fie la fiecare 12 luni, fie când un certificat CA este revocat;
- Informații suplimentare - după fiecare actualizare.

2.4 Controalele de acces pe depozite

Toate informațiile publicate de CERTDIGITAL în Depozit la adresa https://www.certdigital.ro/repository sunt disponibile pentru public.

CERTDIGITAL a implementat mecanisme de protecție logică și fizică împotriva adăugărilor, ștergerilor sau modificărilor neautorizate ale informațiilor publicate în Depozit.

Abonații, subiecții și părțile învestite au acces numai în citire prin Internet la toate depozitele menționate în secțiunea 2.1.

CERTDIGITAL poate lua măsuri rezonabile pentru a proteja și a preveni utilizarea abuzivă a depozitului, a serviciilor OCSP și a descărcării CRL.

La descoperirea încălcării integrității informației în Depozit, CERTDIGITAL va întreprinde acțiunile necesare pentru a restabili integritatea informației, va impune acțiuni în justiție pentru cei vinovați și va notifica imediat entitățile afectate.

3. Identificarea și autentificarea

3.1 Denumirea

3.1.1 Tipuri de nume

Certificatele emise de CERTDIGITAL sunt în conformitate cu standardul X.509 v3. Aceasta înseamnă că emitentul certificatului și autoritatea de înregistrare care acționează în numele emitentului aprobă numele Subiectului în conformitate cu standardul X.509 (cu referire la recomandările seriei X.500). Numele de bază ale subiecților și ale emitenților de certificate plasați în certificatele CERTDIGITAL respectă denumirile distinctive - DN - (cunoscute și sub numele de director), create după recomandările X.500 și X.520. În cadrul DN, este posibil să se definească atributele Serviciului de nume de domeniu (DNS). Aceasta permite Subiecților să utilizeze simultan două tipuri de nume: DN și DNS. Aceasta este o opțiune foarte importantă în cazul emiterii de certificate pentru servere administrate de subiect.

3.1.2 Necesitatea ca numele să aibă semnificație

Numele utilizate în certificate sunt alese astfel încât:

- Este clar că certificatul este un certificat CA,
- Scopul CA este clar,
- Include o identificare clară a persoanei juridice a Abonatului.

Numele certificatelor CA emise vor include următoarele informații despre nume:

CN = CERTDIGITAL ROOT CA G4

2.5.4.97 = VATRO-2163993

OU = CERTDIGITAL

O = CENTRUL DE CALCUL S.A.

C = RO

Multe aplicații software utilizează câmpul commonName pentru a afișa o alegere de certificate pentru utilizatorul final. Pentru a ajuta utilizatorul final să aleagă certificatul adecvat, câmpul commonName poate conține, de asemenea, formularea simplă care descrie utilizarea intenționată a certificatului (adică " Qualified CA ").

commonName Numele semnificativ al CA subordonat

organizationName	Denumirea oficială înregistrată a CA de abonament ca corporație sau organizație
OrganizationIdentifier	Un identificator oficial unic al Abonatului ca corporație sau organizație (formatat în ETSI EN 319 412-1)

Numele Subiectului va fi confirmat de CMPB și aprobat de ROOT CA.

CERTDIGITAL asigură (în domeniul său) unicitatea DN-urilor.

3.1.3 Anonimitatea sau pseudonimitatea abonaților

Nu se aplica.

3.1.4 Reguli pentru interpretarea diferitelor formulare de nume

Interpretarea câmpurilor din cadrul certificatelor emise de CERTDIGITAL se face în conformitate cu profilurile certificatelor descrise în Certificatele și Profilurile CRL prezentate in capitolul 7 al acestui document. Crearea și interpretarea DN se efectuează în conformitate cu recomandările din capitolul 3.1.2 al acestui document.

3.1.5 Unicitatea numelor

Identificarea fiecărui deținător al certificatelor emise de CERTDIGITAL se realizează pe baza DN. CERTDIGITAL asigură unicitatea DN atribuită fiecărui subiect.

3.1.6 Recunoașterea, autentificarea și rolul mărcilor comerciale

Nu se aplică.

3.2 Validarea inițială a identității

3.2.1 Metoda de a dovedi posesia cheii private

Posesia cheii private, corespunzătoare cheii publice pentru care se solicită generarea unui certificat, va fi dovedită prin trimiterea cererii de semnare a certificatului (CSR), conform standardului RSA PKCS # 10, care va include cheia publică semnată de Cheia privată asociată.

3.2.2 Autentificarea identității organizației

CertDigital ROOT CA G4 este o autoritate de certificare primară pentru domeniul CERTDIGITAL. Orice altă autoritate de certificare din acest domeniu va fi subordonată CertDigital ROOT CA G4 și operată de aceeași entitate juridică.

Prin urmare, nu este necesară autentificarea identității entității juridice.

Solicitările de certificate sunt realizate prin roluri de încredere asociate CertDigital ROOT CA G4, sub supravegherea Compartimentului de Management al Politicii și Procedurilor (CMPP).

3.2.3 Autentificarea identității individuale

Nu se aplică.

3.2.4 Informațiile abonatului neconfirmate

Nu se aplică.

3.2.5 Validarea autorității

Nu se aplică.

3.3 Identificarea și autentificarea pentru solicitările de re-cheie

3.3.1 Identificarea și autentificarea pentru re-cheie de rutină

Capitolul 4.7 din prezentul document descrie procesul.

3.3.2 Identificarea și autentificarea pentru re-cheie după revocare

Se folosește același proces ca și validarea inițială a identității.

3.4 Identificarea și autentificarea cererii de revocare

CertDigital ROOT CA G4 este o autoritate de certificare primară pentru domeniul CERTDIGITAL. Orice altă autoritate de certificare din acest domeniu este subordonată CertDigital ROOT CA G4 și operată de aceeași entitate juridică.

Prin urmare, solicitările de revocare se efectuează prin roluri de încredere asociate cu CertDigital ROOT CA G4, sub supravegherea compartimentului de management a politicilor și procedurilor (CMPP).

4 Cerințe operaționale ale ciclului de viață al certificatului

Acest capitol descrie procedurile de bază care se aplică tuturor tipurilor de certificate de tip emise de CertDigital ROOT CA G4.

Procedurile detaliate referitoare la serviciile componente ale PKI (CA, semnările CRL urilor, răspunsurile OCSP) și persoanele / rolurile implicate în procesul operațional al acestor componente sunt descrise în documentația internă confidențială.

Următoarea secțiune oferă o descriere a acestor documente care pot fi dezvăluite în mod public.

CertDigital ROOT CA G4 oferă acces la următoarele servicii de bază:

A. Înregistrare și certificare;

B. Revocarea certificatului;

C. Verificarea valabilității certificatelor CA ale subautoritatilor.

4.1 Aplicarea certificatului

4.1.1 Cine poate depune o cerere de certificat

Solicitările de certificate sunt realizate prin roluri de încredere asociate CertDigital ROOT CA G4, sub supravegherea Compartimentului de Management al Politicii și Procedurilor (CMPP).

4.1.2 Procesul de înscriere și responsabilitățile

Procesul de înscriere este gestionat de roluri de încredere asociate cu CertDigital ROOT CA G4, sub supravegherea Compartimentul de Management al Politicii și Procedurilor (CMPP).

CERTDIGITAL furnizează infrastructura și resursele pentru funcționarea CertDigital ROOT CA G4. CERTDIGITAL oferă, de asemenea, supraveghere, suport și audit pentru toate procesele și serviciile CERTDIGITAL ROOT CA G4.

CERTDIGITAL asigură o segregare a proceselor de livrare pentru un QSCD și datele de activare asociate acestuia.

4.2 Prelucrarea cererilor de certificate

4.2.1 Efectuarea funcțiilor de identificare și autentificare

CertDigital ROOT CA G4 este o autoritate de certificare primară pentru domeniul CERTDIGITAL. Orice altă autoritate de certificare din acest domeniu va fi subordonată CertDigital ROOT CA G4 și operată de aceeași entitate juridică.

Prin urmare, funcțiile de identificare și autentificare se realizează prin roluri de încredere asociate cu CertDigital ROOT CA G4, sub supravegherea Compartimentului de Management al Politicii și Procedurilor (CMPP).

4.2.2 Aprobarea sau respingerea cererilor de certificate

Aprobarea sau respingerea unei cereri de certificat se face prin roluri de încredere asociate CertDigital ROOT CA G4, sub supravegherea Compartimentului de Management al Politicii și Procedurilor (CMPP).

4.2.3 Timpul de procesare a cererilor de certificate

Procesul de livrare a certificatelor poate dura câteva ore, în funcție de punerea în aplicare a procedurilor de lucru.

4.3 Eliberarea certificatului

4.3.1 Acțiunile CA în cursul emiterii certificatului

După primirea și procesarea unei cereri, Autoritatea de Certificare emite un certificat. După eliberarea certificatului, CERTDIGITAL îl va publica în depozitele corespunzătoare. Perioada de valabilitate a certificatelor eliberate depinde de tipul certificatului și de categoria Subiectului și este compatibilă cu intervalele de timp listate în Tabelul 6.3.2.1.

4.3.2 Notificarea către abonat de către CA a eliberării certificatului

Notificarea privind emiterea unui certificat de către CertDigital ROOT CA G4 pentru o componentă internă a PKI este implicită și este specificată în documentația internă.

4.4 Acceptarea certificatului

4.4.1 Desfășurarea acceptării certificatului

Acceptarea unui certificat se face prin roluri de încredere asociate cu CertDigital ROOT CA G4, sub supravegherea Compartimentului de Management al Politicii și Procedurilor (CMPP).

4.4.2 Publicarea certificatului de către CA

A se vedea capitolul 2 al prezentului document.

4.4.3 Notificarea eliberării certificatului de către CA altor entități

Fiecare certificat eliberat este publicat în depozitul CERTDIGITAL. Publicarea certificatului este echivalentă cu notificarea altor entități (adică a unor părți dependente) cu privire la faptul că a fost emis un certificat pentru o CA subordonată.

4.5 Utilizarea perechii de chei și a certificatului

4.5.1 Cheia privată a abonatului și utilizarea certificatului

CERTDIGITAL protejează accesul cheilor private de către personal neautorizat sau alte terțe părți.

CERTDIGITAL utilizează chei private numai în conformitate cu utilizările specificate în extensia de folosire a cheilor.

Vezi secțiunile 1.4.1, 6.1.7 și 7.1.

4.5.2 Utilizarea cheii publice a părții publice și utilizarea certificatului

CERTDIGITAL presupune că toate software-urile utilizatorilor vor fi conforme cu X.509 v.3, protocolul SSL / TLS și alte standarde aplicabile care aplică cerințele și cerințele stabilite în acest CPS. CERTDIGITAL nu garantează că software-ul unei terțe părți va sprijini sau impune astfel de controale sau cerințe și toate părțile interesate sunt sfătuite să solicite consultanță tehnică sau juridică adecvată.

Părțile implicate vor folosi cheile private și certificatele:

- În conformitate cu scopul declarat în prezentul CPS și în conformitate cu conținutul certificatului (câmpurile *keyUsage* și *extendedKeyUsage*),
- În conformitate cu prevederile acordului dintre Subiect / Abonat și CERTDIGITAL,
- Numai după verificarea statutului și a semnăturii autorității de certificare emitente.

Bazându-se pe o semnătură digitală nesigură sau o sesiune SSL / TLS, este posibil să existe riscuri pe care partea de bază își asumă în întregime și care CERTDIGITAL nu își asumă în nici un fel.

4.6 Reînnoirea certificatului

Nu se aplică.

4.7 Recheierea certificatului

Nu se aplică.

4.8 Modificarea certificatului

Nu se aplică.

4.9 Revocarea și suspendarea certificatului

Certificatele emise de CertDigital ROOT CA G4 pot fi revocate, dar nu sunt suspendate. Revocarea certificatului este ireversibilă.

Revocarea certificatului implică și retragerea drepturilor de emitere a certificatului pentru proprietarul său și revocarea tuturor certificatelor emise pentru el.

Revocarea nu afectează nici tranzacțiile efectuate înainte de revocare, nici obligațiile care decurg din respectarea prezentei CPS.

Acest capitol precizează condițiile necesare pentru revocarea certificatului de către o autoritate de certificare.

4.9.1 Circumstanțele pentru revocare

Un motiv de bază pentru revocarea unui certificat îl constituie pierderea controlului (sau suspiciunea unei astfel de pierderi) asupra cheii private sau încălcarea obligațiilor / solicitărilor incluse în CPS.

Certificatul este revocat atunci când:

- Informațiile din certificat s-au modificat,
- Autoritatea de Certificare își încetează activitatea; În acest caz, toate certificatele emise de această autoritate de certificare înainte de termenul stabilit pentru terminarea serviciilor vor fi revocate împreună cu certificatul autorității de certificare,

- Cheia privată sau securitatea unei autorități de certificare au fost compromise într-un mod care pune în pericol credibilitatea certificatelor,
- Conținutul sau formatul tehnic al certificatului prezintă un risc inacceptabil pentru furnizorii de aplicații software sau pentru părți dependente.
- În alte cazuri, la decizia CMPP.

O cheie privată compromisă se referă la : (1) acces neautorizat la cheia privată sau un motiv puternic pentru a suspecta un astfel de lucru; (2) pierderea cheii private sau apariția unui motiv pentru a suspecta o asemenea pierdere; (3) Apariția unui motiv pentru a suspecta un astfel de jaf, (4) ștergerea accidentală a cheii private.

Cererea de revocare se face prin roluri de încredere asociate cu CertDigital ROOT CA G4, sub supravegherea Compartimentului de Management al Politicii și Procedurilor (CMPP).

4.9.2 Cine poate cere revocarea

Compartimentul de Management al Politicii și Procedurilor (CMPP) este singura entitate autorizată să solicite revocarea unui certificat emis de CertDigital ROOT CA G4.

4.9.3 Procedura pentru cererea de revocare

Revocarea certificatului se face prin roluri de încredere asociate CertDigital ROOT CA G4, sub supravegherea Compartimentului de Management al Politicii și Procedurilor (CMPP).

Înainte de revocarea certificatului unui CA subordonat, toate certificatele valide semnate de acest certificat sunt revocate. Informațiile despre certificatele revocate sunt plasate în lista de revocare a certificatelor eliberată de autoritățile de certificare corespunzătoare.

4.9.4 Perioada de grație a cererii de revocare

CERTDIGITAL efectuează revocarea pe baza celor mai bune eforturi, pentru a se asigura că timpul necesar procesării cererii de revocare și publicării notificării de revocare (CRL actualizat) este cât mai redus.

4.9.5 Timpul în care CA trebuie să proceseze cererea de revocare

CERTDIGITAL garantează revocarea certificatelor digitale emise de CertDigital ROOT CA G4 în maxim 8 ore.

Informațiile despre revocarea certificatului sunt stocate în baza de date a CERTDIGITAL. Certificatele revocate sunt plasate pe Lista de revocare a certificatului (CRL), în conformitate cu termenele de publicare ale CRL.

În momentul revocării certificatului, operatorii, subiecții și abonații autorității de înregistrare implicați sunt informați automat despre această revocare. Informații despre starea actuală a certificatului sunt disponibile prin intermediul serviciului de verificare a statusului certificatului imediat după perioada de grație declarată. Acest serviciu poate fi solicitat, de exemplu, de o parte invocată care verifică disponibilitatea unei semnături electronice aplicată unui document primit de la subiect.

4.9.6 Cerințele de verificare a revocării pentru părțile implicate

Părțile implicate vor folosi toate resursele puse la dispoziție de CERTDIGITAL prin depozitul său pentru a verifica stadiul unui certificat în orice moment înainte de a se baza pe acesta. CERTDIGITAL actualizează OCSP, CRL în consecință.

4.9.7 Frecvența emiterii CRL

Lista de revocare a certificatelor (CRL) pentru CertDigital ROOT CA G4 este emisă cel puțin o dată pe an, cu condiția să nu existe revocări de certificate ale uneia dintre autoritățile din subordinea CA.

În cazul revocării certificatului unei autorități afiliate la CERTDIGITAL, acest certificat este publicat imediat în Lista de Revocare a Certificatelor.

4.9.8 Latența maximă pentru CRL

CRL-ul Autorității de Certificare (CA) și toate certificatele sale emisie de autoritățile subordonate se eliberează în conformitate cu capitolul 4.9.7 și se publică fără întârziere.

4.9.9 Disponibilitate on-line de revocare / verificare stare

Pentru statutul certificatelor CERTDIGITAL CA actualizează informațiile furnizate cel puțin printr-un protocol de stare de certificat online

- La fiecare douăsprezece luni și

- În decurs de 24 de ore de la revocarea unui certificat de certificat secundar.

Dacă răspunsul OCSP primește o solicitare de statutul unui certificat care nu a fost emis, atunci respondentul nu răspunde cu o stare "bună" pentru aceste certificate.

Răspunsurile OCSP sunt semnate de un Responsabil OCSP al cărui certificat este semnat de CA care a emis certificatul a cărui stare de revocare este verificată.

Certificatul de semnare OCSP conține o extensie de tip id-pkix-ocsp-nocheck, așa cum este definită de RFC6960.

4.9.10 Cerințe de verificare on-line de revocare

Vezi capitolul 4.9.6 al documentului curent.

4.9.11 Alte forme de anunțuri de revocare disponibile

Nu se aplică.

4.9.12 Cerințe speciale privind compromisul cheie

Nu se aplică.

4.9.13 Circumstanțe pentru suspendare

Nu se aplică

4.9.14 Cine poate solicita suspendarea

Nu se aplică

4.9.15 Procedura de suspendare a cererii

Nu se aplică

4.9.16 Limitele perioadei de suspendare

Nu se aplică

4.10 Servicii de stare a certificatului

4.10.1 Caracteristicile operaționale

Serviciile de stare a certificatului CERTDIGITAL sunt CRL și OCSP. Accesul la aceste servicii se face prin intermediul site-ului web www.certdigital.ro sau "crl.certdigital.ro" și "ocsp.certdigital.ro". Serviciile de stare a certificatului furnizează informații despre starea certificatelor valide. Integritatea și autenticitatea informațiilor referitoare la statut sunt protejate de o semnătură digitală a CA-ului respectiv.

4.10.2 Disponibilitatea serviciului

Serviciile de stare a certificatului sunt disponibile 24 de ore pe zi, 7 zile pe săptămână.

4.10.3 Caracteristici opționale

Serviciile de stare a certificatului CERTDIGITAL nu includ sau nu necesită funcții suplimentare.

4.11 Încheierea abonamentului

Nu se aplică.

4.12 Key escrow și recuperare

Nu se aplică

5. Facilități, management și controale operaționale

În calitate de furnizor de servicii de certificare, CERTDIGITAL plasează securitatea în centrul activităților sale. Pentru a se asigura că toate activele, activitățile și serviciile sale sunt sigure, CERTDIGITAL a implementat, menține și îmbunătățește continuu sistemul de management al securității informațiilor ISO 27001: 2013. În conformitate cu cerințele acestui cadru de securitate, toate activitățile de securitate încep cu o evaluare a riscurilor pentru a identifica și a clasifica toate activele informaționale, pentru a evalua riscurile la care sunt expuse și pentru a determina controalele tehnice, manageriale, organizaționale și procedurale necesare. CERTDIGITAL menține un inventar al tuturor activelor informaționale și le atribuie o clasificare compatibilă cu evaluarea riscurilor.

Toate aceste controale referitoare la activele și activitățile CA si RA sunt conforme cu cerințele aplicabile din următoarele standarde:

- ETSI EN 319 401, Cerințe generale de politică pentru furnizorii de servicii de încredere

- ETSI EN 319 411-1, cerințe privind politica și securitatea pentru furnizorii de servicii de asigurare care eliberează certificate; Partea 1: Cerințe generale
- ETSI EN 319 411-2, Cerințe de politică și de securitate pentru furnizorii de servicii de trust care eliberează certificate; Partea 2: Cerințe pentru furnizorii de servicii de încredere care eliberează certificate calificate UE
- ETSI EN 319 421, Cerințe privind politica și securitatea pentru furnizorii de servicii de încredere care emite timbre

5.1 Controale fizice

Sistemul informatic de rețea, terminalele operatorului și resursele informaționale ale CERTDIGITAL sunt situate în zone dedicate, protejate fizic împotriva accesului neautorizat, distrugerii sau întreruperii funcționării lor. Aceste locații sunt monitorizate. Fiecare intrare și ieșire, precum și fluctuațiile de putere, sunt înregistrate în jurnalul de evenimente (jurnale de sistem). Temperatura și umiditatea sunt monitorizate și controlate.

5.1.1 Localizarea și construcția amplasamentului

Toate operațiunile CA și RA ale CERTDIGITAL se desfășoară într-un mediu protejat fizic, cu controale bazate pe evaluarea riscurilor, menite să descurajeze, să prevină, să detecteze și să contracareze materializarea riscurilor asupra activelor sale. De asemenea, susținem instalațiile de recuperare în caz de dezastru pentru operațiunile noastre CA și RA, facilități care sunt protejate de controalele de securitate fizică similare cu cele implementate în instalația noastră principală. Toate controalele de securitate fizică implementate de CERTDIGITAL sunt în conformitate cu standardele ISO 27001 și sunt descrise în detaliu în politicile și procedurile de securitate. Unele dintre cele mai importante controale de securitate sunt:

- Un perimetru clar definit și protejat prin care sunt monitorizate toate intrările și ieșirile;
- Componentele critice sunt protejate cu mai multe perimetre;
- Un sistem de control al accesului configurat să permită accesul numai la acele persoane care au fost examinate în mod corespunzător și au fost autorizate în mod specific să intre în zonă;
- Monitorizarea în permanență a personalului și monitorizarea electronică a intruziunii neautorizate;
- Personalul care nu este pe lista de acces este escortat și supravegheat în mod corespunzător;
- Un jurnal de acces la site este menținut și inspectat periodic;

- Toate echipamentele sunt întreținute corect pentru a asigura disponibilitatea și integritatea lor continuă.

5.1.2 Accesul fizic

Accesul fizic este controlat și monitorizat de un sistem de alarmă integrat. Sistemul de prevenire a incendiilor, sistemul de detecție a intruziunilor și sistemul de alimentare de urgență sunt instalate.

Programul de lucru CERTDIGITAL este de luni până vineri între orele 8.00 și 18.00. În afara acestui interval de timp, inclusiv sărbătorile legale, accesul la sediul CERTDIGITAL este permis numai persoanelor autorizate de către conducerea CERTDIGITAL.

Vizitatorii sunt escortați permanent de către personalul autorizat.

Sediile CERTDIGITAL sunt împărțite în:

- Zone de birouri,
- Zone IT,
- Zona operatorilor CA
- Operatorii și administratorii RA,
- Dezvoltarea și testarea zonei.

Zonele IT sunt echipate cu sistem de securitate monitorizat construit pe baza mișcării, a intruziunii și a incendiului. Accesul în acest domeniu este permis numai personalului autorizat. Monitorizarea drepturilor de acces se realizează pe baza cardurilor electronice și a cititoarelor corespunzătoare, montate lângă zona de intrare. Fiecare intrare și ieșire din zonă este înregistrată automat în jurnalul de evenimente.

Accesul la zona operatorilor este permis numai pe baza unei cartele electronice și a cititorului corespunzător. Întrucât toate informațiile sensibile sunt protejate prin utilizarea de dulapuri încuiate, în timp ce accesul la terminalul operatorului sau al administratorului necesită o autorizare prealabilă, securitatea fizică implementată este considerată adecvată. Cheile către zonă sunt accesibile numai personalului autorizat. Zona poate fi ocupată numai de personalul CERTDIGITAL și persoanele autorizate, acesta din urmă fiind acordat accesului numai dacă este însoțit.

Persoanele nesupravegheate nu sunt permise în acest domeniu. Programatorii și dezvoltatorii nu au acces la informații sensibile. Dacă este necesar un astfel de acces, este necesară prezența administratorului de

securitate. Proiectele care sunt implementate și software-ul lor sunt testate pe mediul de dezvoltare al CERTDIGITAL.

5.1.3 Putere și aer condiționat

Sistemul de ventilație este disponibil în toate zonele. În zonele serverului, unitățile de aer condiționat sunt redundante și temperatura este monitorizată. Când apar defecțiuni de alimentare, sursele de energie de urgență (UPS) permit continuarea activităților până la intervenția automată a generatorului de rezervă în clădire. Infrastructura de energie electrică este proiectată astfel încât, dacă puterea principală a clădirii este pierdută, toate activitățile pot continua timp de cel puțin 24 de ore folosind generatorul de energie de rezervă. Fiecare server, echipamente de rețea și toate computerele angajaților care desfășoară activități importante pentru operațiunile CA și RA sunt de asemenea conectate la UPS-uri. Componentele principale ale sistemului de protecție fizică sunt, de asemenea, conectate la UPS-uri și la generatorul de energie de rezervă.

5.1.4 Expunerea la apă

Riscul de inundații în zona serverelor este atenuat prin plasarea tuturor pieselor de echipament în rafturi la cel puțin 15 cm de la nivelul podelei. În plus, toate camerele de date sunt monitorizate cu ajutorul senzorilor de umiditate.

5.1.5 Prevenirea și protecția împotriva incendiilor

Locația CERTDIGITAL beneficiază de un sistem de prevenire și stingere a incendiilor, în conformitate cu standardele și reglementările corespunzătoare din acest domeniu. Ușile camerelor de date sunt certificate cu rezistență la foc și toate pasajele din pereți sunt sigilate cu substanțe rezistente la foc.

5.1.6 Depozitare media

În conformitate cu cerințele politicii de clasificare a informației, materialele care conțin date sau informații de rezervă sunt manipulate și stocate în siguranță în cadrul unității principale. Mediile de rezervă sunt, de asemenea, stocate în siguranță într-o locație separată de locația originală, cu aceeași securitate ca și locația primară. Unitățile de stocare care conține date sensibile sunt dezafectate cu siguranță doar atunci când nu mai sunt necesare.

5.1.7 Eliminarea deșeurilor

După expirarea perioadei de păstrare, hârtia și suporturile electronice care conțin informații semnificative pentru securitatea CERTDIGITAL sunt distruse. Modulele hardware de securitate sunt distruse în conformitate cu recomandările producătorului.

Când nu mai este necesar, HSM-urile vor fi zeroizate pentru a preveni orice posibilitate de reutilizare a cheilor private CA și returnate la inventarul criptografic.

După încetarea operațiunii, dispozitivele și cardurile de roluri de încredere vor fi distruse. Ștergerea securizată se face în conformitate cu politica de securitate a informațiilor de la CERTDIGITAL.

5.1.8 Supravegherea în afara amplasamentului

Copiile cardurilor criptografice sunt stocate în cutia de depozitare în afara locației primare CERTDIGITAL.

Depozitul în afara spațiului cuprinde și arhive, copii actuale ale informațiilor prelucrate de sistem și kituri de instalare a aplicațiilor CERTDIGITAL. Permite recuperarea de urgență a fiecărei funcții CERTDIGITAL în termen de 48 de ore în locația de recuperare în caz de dezastru a CERTDIGITAL.

5.2 Controale procedurale

5.2.1 Roluri de încredere

Toate rolurile implicate în furnizarea serviciilor de certificare ale CERTDIGITAL sunt atribuite angajaților CERTDIGITAL.

Toți angajații CERTDIGITAL sunt angajați prin semnătură pentru a nu avea interese conflictuale cu CERTDIGITAL, pentru a păstra confidențialitatea informațiilor și pentru a proteja datele personale.

CERTDIGITAL asigură o separare a sarcinilor pentru funcțiile critice pentru a împiedica o persoană să utilizeze în mod necorespunzător sistemele CA fără detectare.

Securitatea informațiilor prelucrate de CERTDIGITAL și de serviciile sale este asigurată prin controale procedurale legate de controlul accesului. Astfel, accesul la informațiile și funcțiile sistemului de aplicații este restricționat în conformitate cu Politica de control al accesului. CERTDIGITAL gestionează drepturile de acces ale operatorilor, administratorilor și auditorilor de sistem. Administrația include gestionarea contului de utilizator și modificarea în timp util sau eliminarea accesului. Au fost furnizate suficiente controale de securitate a calculatorului pentru separarea rolurilor de încredere identificate,

inclusiv separarea funcțiilor de administrare a securității și a funcțiilor de operare. În mod special, utilizarea programelor de utilitate a sistemului este restricționată și controlată.

CERTDIGITAL poate atribui următoarele roluri de încredere uneia sau mai multor persoane:

- *Responsabil de securitate* - Responsabilitatea generală pentru implementarea practicilor și politicilor de securitate.
- *Administrator de sistem* - autorizat să instaleze, să configureze și să mențină sistemele de încredere ale Autorității de Certificare pentru înregistrare, generare de certificate, furnizarea de dispozitive și gestionarea revocărilor. Instalează sisteme hardware și de operare; Instalează și configurează echipamentul de rețea.
- *Operator de sistem* - Responsabil pentru funcționarea sistemelor de încredere ale Autorității de Certificare pe o bază zilnică. Autorizat să efectueze backup și recuperare de sistem. Are acces la certificatele pentru subiecți; Revocă certificatele de subiecți; Asigură continuitatea copiilor și arhivelor de rezervă ale creării de jurnale de date și de sistem; Gestionează baze de date; Are acces la informații confidențiale despre Subiecți / Abonați, dar nu are voie să acceseze fizic orice alte resurse de sistem; Transferă copii de arhivă și copiile de rezervă actuale la sediul desemnat.
- *Responsabilii de înregistrare* - Responsabil de verificarea informațiilor necesare eliberării și aprobării certificatelor de solicitare de certificare;
- *Ofițeri de revocare* - Responsabili cu modificarea statusului certificatului;
- *Auditorul sistemului* - autorizat să acceseze arhivele și jurnalele de audit ale sistemelor de încredere ale Autorității de Certificare. Responsabil de efectuarea auditului intern, conformitatea unei autorități de certificare cu acest CPS; Această responsabilitate se extinde și la Autoritatea de Înregistrare, care operează în cadrul CERTDIGITAL.

Rolul auditorului nu poate fi combinat cu niciun alt rol în cadrul CERTDIGITAL. Nici o entitate care nu a atribuit niciun alt rol diferit decât un auditor poate lua responsabilitățile auditorului.

Angajații sunt numiți în mod oficial pentru roluri de încredere de către Compartimentul Managementul Politicilor si Procedurilor (CMPP). Principiul "cel mai puțin privilegiat" se aplică atunci când se atribuie drepturi de acces la roluri de încredere.

5.2.2 Numărul de persoane necesare pentru fiecare sarcină

În cazul în care este necesar un control dublu sau multiplu, cel puțin două persoane distincte, cu roluri de încredere relevante, sunt prezente pentru a putea efectua operația.

Circumstanțele care necesită control dublu sau multiplu sunt descrise în documentația internă confidențială.

5.2.3 Identificarea și autentificarea pentru fiecare rol

Fiecare angajat al CERTDIGITAL care acționează într-un rol de încredere este identificat și autentificat pentru a accesa infrastructura pentru a-și îndeplini rolul prin intermediul a cel puțin doi factori de autentificare.

- Fiecare cont alocat:
- Este unic și atribuit direct unei anumite persoane,
- Nu este împărtășită cu nicio altă persoană,

Este restricționată în acord cu funcția (rezultată din rolul unei anumite persoane) bazată pe sistemul software CERTDIGITAL, pe sistemul de operare și pe controalele aplicației.

Toate acțiunile angajaților în roluri de încredere sunt urmărite și se asigură o responsabilitate deplină.

5.2.4 Roluri care necesită separarea sarcinilor

CERTDIGITAL implementează și impune o separare a rolurilor și atribuțiilor pentru rolurile Administratorului, Operatorului și Auditorului pentru a se asigura că aceeași persoană nu poate deține mai multe roluri. Toate aceste roluri au descrieri de posturi, cu cerințe specifice de competență și experiență, definite din punctul de vedere al rolurilor îndeplinite. Împărțirea sarcinilor și principiile celor mai puțin privilegiate sunt în vigoare. Sensibilitatea poziției bazată pe atribuții determină nivelurile de acces, screening-ul de fundal și instruirea și conștientizarea angajaților.

Se stabilesc și se pun în aplicare proceduri pentru toate rolurile de încredere și administrative care au un impact asupra furnizării de servicii.

5.3 Controlul personalului

CERTDIGITAL se asigură că persoana care își îndeplinește responsabilitățile de serviciu, care decurg din rolul acționat într-o Autoritate de Certificare sau într-o Autoritate de Înregistrare:

- a absolvit cel puțin școala secundară,
- a înțeles și a semnat un acord care descrie rolul său în sistem și responsabilitățile acestuia,
- a fost supus unei pregătiri avansate cu privire la gama de obligații și sarcini asociate poziției sale,
- a fost instruit în domeniul protecției datelor cu caracter personal și a protecției confidențiale și a informațiilor private,
- a semnat un acord care conține clauze referitoare la protecția informațiilor sensibile ale CERTDIGITAL și a confidențialității și confidențialității datelor abonatului,
- Nu îndeplinește sarcini care pot conduce la un conflict de interese între o autoritate de certificare și o autoritate de înregistrare care acționează în numele acesteia.

Rolul și responsabilitățile de securitate, așa cum sunt specificate în politica de securitate a informației a CERTDIGITAL, sunt documentate în fișele de post sau în documentele disponibile tuturor personalului implicat.

5.3.1 Cerințe privind calificările, experiența și cerințele de verificare

CERTDIGITAL se asigură că toți angajații implicați în furnizarea serviciilor de certificare ale CERTDIGITAL sunt verificați înainte de angajare în ceea ce privește calificările, cunoștințele de specialitate, experiența și autorizarea necesară și că sunt adecvate să li se atribuie roluri de încredere și să îndeplinească funcția specifică de post aferent. Personalul de conducere deține expertiza și instruirea în domeniul tehnologiei PKI și experiența în managementul securității informațiilor și gestionarea riscurilor, suficientă pentru îndeplinirea funcțiilor de management.

5.3.2 Proceduri de verificare de fond

CERTDIGITAL asigură efectuarea verificărilor relevante pentru personalul potențial prin intermediul rapoartelor de stare emise de o autoritate competentă, al declarațiilor de la terți sau al declarațiilor autodeclarate.

5.3.3 Cerințe de instruire

Personalul care îndeplinește rolurile și sarcinile care decurg din angajarea în CERTDIGITAL trebuie să completeze următoarele cursuri de instruire privind:

- cerințele Declarației de practici de certificare,

- procedurile și controalele de securitate utilizate de Autoritatea de Certificare și de Autoritatea de Înregistrare
- responsabilitățile care decurg din rolurile și sarcinile executate în sistem,

După finalizarea instruirii, participanții semnează un document care confirmă familiarizarea lor cu declarația de practici de certificare, alte documente relevante și acceptarea restricțiilor și obligațiilor asociate.

5.3.4 Frecvența și cerințele de recalificare

Formările descrise în Capitolul 5.3.3 trebuie repetate sau completate întotdeauna în situațiile în care se fac modificări semnificative ale operațiunilor CERTDIGITAL.

5.3.5 Frecvența și secvența de rotație a lucrării

Nu se aplică.

5.3.6 Sancțiuni pentru acțiuni neautorizate

CERTDIGITAL va lua măsuri împotriva celor responsabili de încălcarea politicilor sau a procedurilor, acțiunile neautorizate, utilizarea neautorizată a autorității și utilizarea neautorizată a sistemelor. Aceasta poate include, printre altele, revocarea privilegiilor, acțiuni disciplinare, sancțiuni reglementate de legislația muncii din România, proceduri civile sau penale.

5.3.7 Cerințele contractorului independent

Personalul contractual (serviciu extern, dezvoltatori de subsisteme sau aplicații etc.) este supus aceleiași proceduri de verificare ca și angajații CERTDIGITAL (a se vedea capitolele 5.3.1, 5.3.2 și 5.3.3). În plus, atunci când își îndeplinesc sarcinile la sediul CERTDIGITAL, personalul contractual trebuie să fie escortat de un angajat al CERTDIGITAL, cu excepția celor care au fost autorizați de către ofițerul de securitate și care au acces la informații clasificate interne sau în conformitate cu legile în vigoare.

5.3.8 Documentația furnizată personalului

CERTDIGITAL oferă personalului următoarele documente:

- CPS,
- Lista responsabilităților și obligațiilor asociate cu rolul atribuit în sistem
- Politici și proceduri de securitate

Alte documente relevante (proceduri operaționale, instrucțiuni de lucru, manuale) necesare personalului pentru a-și îndeplini funcțiile specifice de serviciu legate de furnizarea serviciilor de certificare ale CERTDIGITAL sunt distribuite pe parcursul instruirii inițiale, antrenamentelor anuale și ori de câte ori este cazul.

5.4 Procedurile de înregistrare a auditului

Pentru a gestiona eficient sistemele și aplicațiile utilizate de CERTDIGITAL în activitatea sa de furnizor de servicii de certificare, dar și pentru a controla acțiunile angajaților și clienților, sunt înregistrate toate informațiile despre evenimentele importante, specifice generate de sisteme și aplicații. Aceste informații, denumite în mod colectiv "jurnal", sunt păstrate în așa fel încât să poată fi accesate de către Părțile asociate, auditorii și autoritățile de stat în orice moment de care au nevoie, pentru a dovedi funcționarea corectă a serviciilor în scopul legal sau pentru a detecta încercările de a compromite securitatea CERTDIGITAL. Evenimentele înregistrate sunt susținute și păstrate într-o locație secundară.

Ori de câte ori este posibil, jurnalele sunt create automat. Dacă acest lucru nu este posibil, vor fi utilizate jurnalele de hârtie. Fiecare înregistrare dintr-un jurnal creat fie automat, fie manual, este păstrată sau dezvăluită în timpul unui audit, dacă este necesar. Precizia de timp a jurnalelor este asigurată de un server de timp care este sincronizat cu cel puțin două surse de timp care pot fi sateliți GPS sau UTC (NIMB).

5.4.1 Tipuri de evenimente înregistrate

Fiecare activitate critică din punctul de vedere al securității CERTDIGITAL este înregistrată în jurnale de evenimente și arhivată. Arhivele sunt stocate pe suporturi de stocare care nu pot fi șterse sau distruse cu ușurință (cu excepția cazului în care sunt transferate în mod fiabil pe suporturi pe termen lung) în perioada în care acestea trebuie să fie ținute. Jurnalele de evenimente CERTDIGITAL conțin înregistrări ale tuturor activităților generate de componentele software din cadrul sistemului.

Aceste înregistrări sunt împărțite în trei categorii distincte:

- Jurnale de sistem - conțin informații despre solicitările clienților și despre răspunsurile serverului (sau invers) la nivelul protocolului de rețea (de exemplu http, https); datele înregistrate sunt: adresa IP a postului sau a serverului, operațiile efectuate (de exemplu: căutarea, editarea, scrierea etc.) și rezultatele acestora (de exemplu intrarea cu succes a unei înregistrări în baza de date);
- Erori - conțin informații despre erori la nivelul protocoalelor de rețea și la nivelul modulelor aplicațiilor;
- Jurnale de audit - conțin informații specifice pentru serviciile de certificare, de exemplu: cererea de înregistrare și de certificare, solicitarea de rekey, acceptarea certificatului, emiterea certificatului și CRL etc.

Jurnalele de mai sus sunt comune fiecărei componente instalate pe un server sau într-o stație de lucru și au o capacitate predefinită. Când această capacitate este depășită, se va crea automat o versiune a jurnalului. Jurnalul anterior este arhivat și șters de pe disc.

Fiecare înregistrare automată sau manuală conține următoarele informații:

- Tip de eveniment,
- Identificator de eveniment,
- Data și ora producerii evenimentului,
- Identificatorul persoanei responsabile cu evenimentul.

Sunt înregistrate toate evenimentele legate de ciclul de viață al cheilor CA.

Sunt înregistrate toate evenimentele legate de ciclul de viață al certificatelor.

Toate evenimentele legate de ciclul de viață al cheilor gestionate de CA, inclusiv cheile de subiecte generate de CA sunt înregistrate.

Toate solicitările și rapoartele privind revocarea, precum și acțiunea care rezultă sunt înregistrate.

Toate evenimentele legate de înregistrare, inclusiv cererile de re-cheiere a certificatelor, sunt înregistrate.

Toate informațiile de înregistrare, inclusiv următoarele, sunt înregistrate:

- tipul de document (documente) prezentat de solicitant pentru a susține înregistrarea;
- înregistrarea de date de identificare unice, numere sau o combinație a acestora (de exemplu, carte de identitate a solicitantului sau pașaport) a documentelor de identificare, dacă este cazul;

- locația de depozitare a copiilor aplicațiilor și a documentelor de identificare, inclusiv acordul semnat de subiect/abonat;
- orice opțiuni specifice din acordul subiect/abonat (de exemplu, aprobarea publicării certificatului);
- identitatea entității care acceptă cererea;
- metoda utilizată pentru validarea documentelor de identificare,

În plus, CERTDIGITAL menține jurnalele interne ale tuturor evenimentelor de securitate și ale tuturor evenimentelor operaționale relevante din întreaga infrastructură, indiferent de serviciul component, inclusiv, dar fără a se limita la:

- Modificări ale politicii de securitate;
- Pornirea și oprirea sistemelor;
- Întreruperea funcționării;
- Accidente de sistem și defecțiuni hardware;
- Activități firewall și router;
- Încercări de acces la sistemul PKI;
- Accesul fizic al personalului și al altor persoane la părțile sensibile ale oricărui loc sau zonă securizată;
- Back-up și restaurare;
- Raport de teste de recuperare în caz de catastrofe;
- Inspecții de audit;
- Actualizarea și modificarea sistemelor, software-ului și infrastructurii;
- Intruziuni de securitate și încercări de intruziune.

Accesul la jurnale este permis exclusiv pentru ofițerul de securitate, personalul special desemnat și auditorii. Se păstrează confidențialitatea informațiilor despre subiect.

5.4.2 Frecvența jurnalului de prelucrare

Înregistrările sunt procesate în mod continuu și/sau după orice alarmă sau eveniment anormal. Înregistrările sunt arhivate în mod regulat și susținute.

5.4.3 Perioada de păstrare pentru jurnalul de audit

Înregistrările evenimentelor sunt stocate în fișiere de pe discul sistemului până când acestea ating capacitatea maximă permisă. În acest moment sunt disponibile on-line, la fiecare persoană autorizată sau cerere de proces. După depășirea capacității permise, jurnalele sunt păstrate ca arhive și pot fi accesate exclusiv off-line, de la o anumită stație de lucru.

Jurnalul arhivat al înregistrărilor este păstrat cel puțin 10 ani.

5.4.4 Protecția jurnalului de audit

Fișierele jurnal sunt protejate corespunzător de un mecanism de control al accesului. Protecția adecvată împotriva modificării și ștergerii jurnalelor de audit este pusă în aplicare astfel încât nimeni să nu poată modifica sau șterge înregistrările de audit decât după transferul pe suporturi pe termen lung pentru arhivare. Numai ofițerul de securitate, personalul special desemnat sau un auditor pot examina un jurnal de evenimente. Accesul la jurnalul evenimentelor este configurat astfel :

- Numai entitățile de mai sus au dreptul să citească înregistrările jurnalului,
- Platforma de jurnal central arhivează sau șterge automat fișiere (după arhivare) care conțin evenimente înregistrate,
- Este posibil să se identifice orice încălcare a integrității; Acest lucru asigură că înregistrările nu conțin lacune sau falsuri,
- Nici o entitate nu are dreptul să modifice conținutul unui jurnal.

Mai mult, comenzile de protecție a jurnalului sunt implementate astfel încât, chiar și după arhivarea jurnalului, este imposibil să se șteargă înregistrările sau jurnalul înainte de expirarea timpului de retenție global al jurnalului.

5.4.5 Proceduri de salvare a jurnalului de audit

Politicile de securitate CERTDIGITAL impun ca jurnalul de evenimente să aibă o copie de rezervă periodică. Aceste copii de siguranță sunt stocate în locațiile auxiliare ale CERTDIGITAL. Fișierele de înregistrări și traseele de audit sunt susținute în conformitate cu procedurile interne.

5.4.6 Sistemul de colectare a auditului (intern/extern)

Toate jurnalele generate de servere, dispozitive de rețea, echipamente de securitate, aplicații sunt trimise continuu la o platformă centrală, al cărei scop este:

- Colectarea
- Depozitarea
- Analiza
- Corelarea
- Arhivarea
- Back-up pe termen lung

5.4.7 Notificarea subiectului care cauzează evenimente

Nu se aplică.

5.4.8 Evaluări de vulnerabilitate

Întreaga infrastructură face obiectul evaluării vulnerabilității ca parte a procedurilor de evaluare internă a riscurilor și de gestionare a riscurilor de către CERTDIGITAL.

Pentru a se asigura că toate activele, activitățile și serviciile sale sunt sigure, CERTDIGITAL a implementat, menține și îmbunătățește continuu sistemul de management al securității informațiilor ISO 27001. În conformitate cu cerințele acestui cadru de securitate, toate activitățile de securitate încep cu o evaluare a riscurilor pentru a identifica și a clasifica toate activele informaționale, pentru a evalua riscurile la care sunt expuse și pentru a determina controalele tehnice, manageriale, organizaționale și procedurale necesare. CERTDIGITAL menține un inventar al tuturor activelor informaționale și le atribuie o clasificare compatibilă cu evaluarea riscurilor.

5.5 Arhivarea înregistrărilor

Se solicită ca toate datele și fișierele legate de înregistrarea informațiilor asociate cu securitatea sistemului, cererile transmise de subiecți/abonați, informații despre subiecți/abonați, certificate emise și CRL-uri, cheile utilizate de Autoritățile de Certificare și Înregistrare, întreaga corespondență între CERTDIGITAL și subiecții/abonații, să fie arhivate.

Depozitul on-line conține certificatele active și poate fi utilizat pentru a efectua anumite servicii externe ale Autorității de Certificare, cum ar fi verificarea valabilității unui certificat, publicarea certificatelor pentru proprietarii acestora (restabilirea certificatelor) și a entităților autorizate.

Arhiva conține certificate expirate, inclusiv certificate revocate. Arhivă certificatului revocat conține informații despre un certificat, motivul de revocare, data la care certificatul a fost plasat pe CRL. Arhiva este utilizată pentru soluționarea litigiilor referitoare la documente vechi, semnate electronic de un subiect.

Copiile de rezervă sunt create și păstrate în afara locației CERTDIGITAL.

5.5.1 Tipuri de înregistrări arhivate

Următoarele date sunt supuse unei arhive demne de încredere:

- Toate certificatele pentru o perioadă de cel puțin 10 ani de la expirarea lor.
- Jurnalul arhivat al informațiilor este păstrat cel puțin 10 ani.
- Buletine de emitere și revocare a certificatelor pentru o perioadă de minimum 10 ani de la emitere / revocare.
- CRL-uri pentru cel puțin 10 ani de la publicare.
- Următoarele, cel puțin 10 ani după ce orice certificat bazat pe aceste înregistrări nu mai este valabil:
    - jurnalele tuturor evenimentelor legate de ciclul de viață al cheilor gestionate de CA, inclusiv orice perechi de chei generate de CA ale subiecților
    - Termeni și condiții semnate privind utilizarea certificatului

5.5.2 Perioada de păstrare pentru arhivă

Vezi secțiunea 5.5.1 de mai sus. După expirarea perioadei de reținere declarate, datele arhivate sunt distruse.

5.5.3 Protecția arhivei

CERTDIGITAL asigură:

- implementarea controalelor pentru prevenirea pierderilor de date arhive
- arhivarea confidențialității datelor și a integrității în timpul perioadei de păstrare a acestora, Arhivele sunt accesibile numai personalului autorizat.

5.5.4 Proceduri de salvare a arhivelor

Copierea de rezervă a datelor de arhivă se face în conformitate cu politicile și procedurile interne de rezervă.

5.5.5 Cerințe pentru marcarea temporală a înregistrărilor

CERTDIGITAL asigură înregistrarea exactă a timpului de arhivare a tuturor evenimentelor, înregistrărilor și documentelor menționate mai sus. Acest lucru se realizează prin sincronizarea tuturor sistemelor cu serverele de timp. Precizia timpului este asigurată de un server de timp care este sincronizat cu cel puțin două surse de timp care pot fi sateliți GPS sau UTC (NIMB).

5.5.6 Sistemul de colectare a arhivelor (intern sau extern)

Sistemele de colectare a arhivelor CERTDIGITAL sunt interne.

5.5.7 Proceduri de obținere și verificare a informațiilor de arhivă

Arhivele sunt accesibile angajaților autorizați ai CERTDIGITAL și auditorilor desemnați. Înregistrările sunt păstrate în format electronic sau pe suport de hârtie.

Abonatul/subiectul poate avea acces la înregistrările de înregistrare aferente și alte informații referitoare la subiectul certificatului.

5.6 Schimbarea cheilor

Procedurile de schimbare a cheilor permite trecerea ușoară de la expirarea certificatelor CA la certificatele CA noi. Spre sfârșitul vieții Cheilor Private CA, CERTDIGITAL încetează să utilizeze Cheia Privată CA care expiră pentru a semna Certificate (cu cel puțin un an înainte de expirare) și utilizează vechea cheie privată doar pentru a semna CRL-uri. O nouă pereche de chei CA de semnare este comandată și toate certificatele emise ulterior și CRL-urile sunt semnate cu noua cheie privată de semnare. Atât vechile, cât și noile perechi de chei pot fi active simultan. Acest proces de schimbare a cheilor ajută la minimizarea oricăror efecte negative ale expirării certificatului CA. Noua cheie publică a certificatului este furnizată abonaților și partenerilor prin metodele de difuzare detaliate în capitolul 6.1.4.

5.7 Recuperarea după compromiteri și dezastre

Acest capitol descrie procedurile efectuate de CERTDIGITAL în situații anormale (inclusiv dezastre naturale) pentru a restabili un nivel de servicii garantat. Astfel de proceduri sunt executate în conformitate cu planul acceptat pentru continuitatea afacerii și pentru recuperarea în caz de dezastru.

5.7.1 Procedurile de manipulare a incidentelor și compromisurilor

CERTDIGITAL a implementat o procedură de gestionare a incidentelor de securitate pentru a răspunde rapid și coordonat la incidente și pentru a limita impactul încălcărilor de securitate. Angajații sunt încredințați unor roluri de încredere pentru a urmări alertele cu privire la eventualele evenimente critice de securitate și pentru a se asigura că incidentele relevante sunt raportate în conformitate cu procedura. Defectele critice se fac pe baza aceleiași proceduri.

Procedura de gestionare a incidentelor de securitate specifică și modalitatea de notificare a părților corespunzătoare, în conformitate cu normele de reglementare aplicabile, cu privire la orice încălcare a securității sau a pierderii integrității care are un impact semnificativ asupra serviciului de încredere furnizat și asupra datelor personale menținute în termen de 24 de ore de la încălcare fiind identificată.

În cazul unui incident de securitate, se utilizează proceduri interne. Procedurile includ notificarea organului de supraveghere.

În cazul în care încălcarea securității sau pierderea integrității poate afecta negativ o persoană fizică sau juridică căreia i-a fost furnizat serviciul de certificare, vom notifica, de asemenea, persoanei fizice sau juridice încălcarea securității sau pierderea integrității fără întârzieri nejustificate.

Toate jurnalele evenimentelor de securitate sunt analizate în mod continuu prin mecanisme automate, pentru a identifica dovezi ale activității rău intenționate și a alerta personalul desemnat de posibile evenimente de securitate critice.

Toate incidentele sunt documentate și toate înregistrările asociate sunt arhivate conform descrierii din secțiunea 5.5 a CPS.

5.7.2 Resursele de calcul, software-ul și/sau datele sunt corupte

Politica de Securitate a CERTDIGITAL ia în considerare următoarele amenințări care influențează disponibilitatea și continuitatea serviciilor furnizate:

- Corupția fizică la sistemul informatic al CERTDIGITAL, incluzând corupția resurselor de rețea - această amenințare abordează corupțiile generate de situații de urgență,
- Disfuncționalitatea software-ului și a aplicațiilor, care face ca datele să fie inaccesibile - astfel de corupții abordează sistemul de operare, aplicațiile utilizatorilor și executarea de software rău intenționat, de exemplu viruși, viermi, troieni,
- Pierderea serviciilor de rețea, importantă pentru activitatea CERTDIGITAL. Pierderea sistemului de alimentare cu energie și deteriorarea conexiunilor de rețea,
- Corupția unei părți a infrastructurii interne de rețea, utilizată de CERTDIGITAL pentru a furniza servicii - corupția poate implica obstrucționarea clienților și blocarea (neintenționată) a serviciilor.

Pentru a preveni sau a limita rezultatele amenințărilor de mai sus:

- Politica de securitate a CERTDIGITAL include un plan de continuitate a afacerii și de recuperare în caz de catastrofe,
- În caz de corupție care restrânge funcționalitatea CERTDIGITAL, în termen de 48 de ore va fi activată o facilitate de urgență, care ar trebui să înlocuiască toate funcțiile semnificative ale Autorității de Certificare până la restabilirea serviciilor instalației primare. Distanța dintre instalațiile primare și cele de urgență este suficient de mare pentru a evita ca potențialele catastrofe care apar la locul primar să poată afecta și locul de urgență.
- Instalarea unei versiuni software actualizate în producție este posibilă numai după efectuarea testelor intensive pe un mediu de testare, efectuată în strictă conformitate cu procedurile descrise. Orice modificare a sistemului necesită acceptarea administratorului de securitate CERTDIGITAL.
- Sistemele CERTDIGITAL utilizează aplicații pentru crearea de copii de siguranță a datelor, permițând recuperarea sistemului în orice moment și efectuarea auditului. Copiile de rezervă includ toate datele relevante din punct de vedere al securității.

Toate sistemele din infrastructura IT utilizată pentru a furniza servicii de certificare și semnarea temporară sunt monitorizate continuu și toate evenimentele de securitate sunt înregistrate și analizate. Activitățile anormale ale sistemului care indică o posibilă încălcare a securității, inclusiv intruziunea în sisteme și rețea, sunt detectate și raportate ca alarme pentru a permite CERTDIGITAL să detecteze, să se înregistreze și să reacționeze în timp util la încercările neautorizate și / sau neregulate de a accesa resursele sale.

Sensibilitatea informațiilor colectate sau analizate este luată în considerare prin protejarea acestora de accesul neautorizat.

Pentru a detecta orice discontinuitate în operațiunile de monitorizare, este de asemenea monitorizată pornirea și oprirea funcțiilor de înregistrare

Se monitorizează, de asemenea, disponibilitatea tuturor componentelor importante ale infrastructurii ICT utilizate pentru furnizarea serviciilor de certificare, precum și disponibilitatea serviciilor critice.

CERTDIGITAL abordează orice vulnerabilitate critică care nu a fost abordată anterior, într-o perioadă de 48 de ore după descoperirea sa. CERTDIGITAL pregătește și implementează un plan de atenuare a noilor vulnerabilități, dacă aceasta este eficientă din punct de vedere al costurilor în comparație cu impactul acestora, sau documentează decizia că vulnerabilitatea nu necesită remediere.

5.7.3 Procedura cheii private a entității compromisă

Compromiterea cheii private a CA sau al datelor de activare asociate implică revocarea imediată a certificatului cheii sau cheilor compromise.

În cazul în care cheile private ale Autorității de Certificare (afiliate cu CERTDIGITAL) sunt compromise sau există suspiciunea de compromitere, vor fi luate și următoarele acțiuni:

- Notificarea compromisului tuturor subiecților/abonaților și a altor entități cu care CERTDIGITAL are acorduri sau alte forme de relații stabilite, printre care se bazează părțile și alți furnizori de servicii de încredere. În plus, aceste informații vor fi puse la dispoziția altor părți interesate prin mijloace de informare în masă și poștă electronică.
- Notificarea publicului larg prin intermediul mai multor canale, inclusiv un mesaj pe depozitul CA CERTDIGITAL și site, un comunicat de presă în mass-media.
- Un certificat corespunzător cheii compromise este plasat pe Lista de Revocări a Certificatelor.
- Toate certificatele semnate de CA-ul corupt sunt revocate și un motiv potrivit pentru revocare este depus.
- Autoritatea de Certificare generează o nouă pereche de chei și un certificat nou .
- Se creează certificate noi pentru Subiect.
- Noile certificate pentru subiecți le sunt trimise gratuit.

5.7.4 Capacitățile de continuitate a activității după un dezastru

CERTDIGITAL a stabilit într-un Plan de Continuitate în Afaceri și Recuperare în caz de Dezastre, toate măsurile necesare pentru a asigura recuperarea completă a serviciilor sale în caz de dezastru sau o întrerupere a oricărei componente sau servicii ICT importante mai mult decât perioada de timp maximă tolerabilă stabilită. Toate aceste măsuri sunt conforme cu standardele ISO / IEC 27001. Pentru fiecare componentă sau serviciu, operațiunile vor fi restabilite în intervalul maxim de toleranță stabilit în planul de continuitate.

Toate datele de la sistemele necesare pentru a relua operațiunile CA sunt susținute și stocate într-un loc îndepărtat și sigur, adecvate pentru a permite certificarea pentru a reveni în timp util la operațiuni în caz de incident/dezastru.

Copiile de siguranță ale informațiilor esențiale și ale software-ului sunt realizate în mod regulat. Sunt furnizate facilități adecvate de rezervă pentru a se asigura că toate informațiile esențiale și software-ul pot fi recuperate în urma unui dezastru sau a unei erori media. Aranjamentele de rezervă sunt testate în mod regulat pentru a se asigura că îndeplinesc cerințele planurilor de continuitate a afacerii.

Funcțiile de backup și restaurare sunt realizate de rolurile de încredere relevante.

Planurile BCP & DRP se referă și la compromiterea, pierderea sau presupusa compromitere a cheii private a CA, în caz de dezastru, iar procesele planificate sunt în vigoare.

După un dezastru, acolo unde este posibil, se vor lua măsuri pentru a evita repetarea unui dezastru.

5.8 Terminarea CA sau RA

CERTDIGITAL are o terminare actualizată pentru a reduce la minimum întreruperile pentru subiecți/abonați și Părți asociate care ar putea rezulta dintr-o decizie a unei Autorități de Certificare de a înceta funcționarea. Planul include obligația de a notifica în prealabil toți subiecții/abonații autorității care a certificat Autoritatea de Certificare despre terminare (dacă există) și trecerea responsabilităților (servicii furnizate subiecților/abonaților, baze de date etc.), în conformitate cu Reglementările în vigoare către o altă autoritate de certificare.

Cerințe asociate tranziției de serviciu

Înainte ca o autoritate de certificare să își înceteze activitatea, va :

- Informa (cu cel puțin 30 de zile în avans) despre decizia de încetare a serviciilor sale: toți Subiecții/Abonații care dețin certificate active (neexpuse și nerevocate) emise de această autoritate și alte entități cu care CERTDIGITAL are acorduri sau alte forme de relații stabilite, printre care părțile asociate, alți furnizori de servicii de încredere și autoritățile relevante, cum ar fi organele de supraveghere. În plus, aceste informații vor fi puse la dispoziția altor părți interesate;
- Revoca certificatele neexecutate care au fost emise.
- Transfera obligațiile sale către o parte sigură pentru păstrarea tuturor informațiilor necesare pentru a furniza dovezi privind funcționarea serviciilor de certificare pe o perioadă rezonabilă, cu excepția cazului în care se poate demonstra că CERTDIGITAL nu deține astfel de informații. Informațiile se referă la înregistrări, statutul de revocare a certificatelor neexpirate care au fost emise și arhivele jurnalului de evenimente pentru perioada respectivă de timp indicată subiecților/abonatului și părții care se bazează;
- Distruge cheile private CA, inclusiv copiile de rezervă, sau le retrage din utilizare, astfel încât cheile private să nu poată fi preluate;
- Lua măsuri pentru a transfera furnizarea de servicii de certificare pentru clienții existenți unui alt furnizor de servicii de certificare, dacă este posibil.

CERTDIGITAL va menține sau va transfera către o parte asociată obligațiile de a-și pune la dispoziție cheia publică pentru o perioadă rezonabilă de timp.

În cazul în care CERTDIGITAL își va înceta activitatea fără transferul parțial sau total al activităților sale, va revoca certificatele afectate la o lună de la notificarea abonaților și/sau a subiecților.

CERTDIGITAL are un aranjament care să acopere costurile pentru a îndeplini aceste cerințe minime în cazul în care acesta se află în stare de faliment sau din alte motive nu este în măsură să acopere costurile în sine, în măsura posibilului, în limitele impuse de legislația aplicabilă privind falimentul.

Eliberarea certificatului de către succesorul autorității de certificare desființate

Pentru a asigura continuitatea serviciilor de emitere a certificatelor pentru Subiecți, o Autoritate de Certificare reziliată poate semna un acord cu o altă Autoritate de Certificare care oferă servicii similare legate de emiterea de certificate de înlocuire pentru certificatele valabile ale autorității de certificare terminată.

Prin emiterea unui certificat de înlocuire, succesorul autorității de certificare desființate preia drepturile și obligațiile autorității de certificare desființate legate de gestionarea certificatelor care rămân în uz.

Arhiva Autorității de Certificare care își încetează activitatea trebuie să fie predată autorității de certificare primare - CertDigital ROOT CA G4 (în cazul terminării serviciilor următoarei autorități CertDigital QUALIFIED CA G4) sau la instituția cu care a fost semnat contractul (în cazul rezilierii serviciilor CertDigital ROOT CA G4).

6. Controalele tehnice de securitate

6.1 Generarea și instalarea perechilor de chei

Acest capitol descrie procedurile de generare și gestionare a unei perechi de chei criptografice a unei Autorități de Certificare, inclusiv cerințele tehnice asociate. Există controale de securitate adecvate pentru gestionarea oricăror chei criptografice și a oricăror dispozitive criptografice de-a lungul ciclului lor de viață. Aceste măsuri de securitate protejează și datele de activare a cheilor criptografice, a depozitelor, a cheilor private și a datelor de activare pentru cheile private ale CA-urilor și a altor participanți la PKI și alți parametri critici de securitate.

Procedurile pentru gestionarea cheilor se aplică pentru stocarea sigură și utilizarea cheilor deținute de proprietar. O atenție deosebită este acordată generării și protejării cheilor private ale CERTDIGITAL, influențând funcționarea sigură a întregului sistem de certificare a cheilor publice.

Autoritatea de certificare CertDigital ROOT CA G4 deține cel puțin un certificat auto-semnat. Cheia privată corespunzătoare cheii publice conținută în certificatul auto-semnat este folosită exclusiv pentru a semna cheile publice ale Autorităților de Certificare : CertDigital QUALIFIED CA G4 prin semnarea certificatelor operaționale și a Listei de revocare a certificatelor pentru funcționarea autorităților. Un scop similar este destinat cheilor private deținute de fiecare autoritate: CertDigital QUALIFIED CA G4, corespunzătoare cheilor publice incluse în certificatele emise de CertDigital ROOT CA G4 pentru fiecare autoritate.

Perechea de chei deținute de fiecare Autoritate de Certificare ar trebui să permită semnarea certificatului și a CRL - o cheie publică asociată cu o cheie privată autentificată cu un certificat auto-semnat (în cazul CertDigital ROOT CA G4) sau certificat (în cazul CertDigital QUALIFIED CA G4).

O semnătură electronică este creată prin intermediul algoritmului RSA în combinație cu criptarea SHA-512.

6.1.1 Generarea perechii de chei

CERTDIGITAL are o procedură documentată pentru efectuarea generării de perechi de chei CA pentru toate CA-urile, indiferent dacă acestea sunt Root CA sau CA-uri subordonate, inclusiv CA care emite certificate către utilizatorii finali. Această procedură indică următoarele:

- Rolurile care participă la generare (internă și externă din partea organizației);
- Funcțiile care trebuie îndeplinite de fiecare rol și în ce faze;
- Responsabilități în timpul și după generare;
- Dovezi care trebuie colectate în timpul ceremoniei.

După generarea cheilor CERTDIGITAL va prezenta un raport de generare a cheilor care să dovedească faptul că a fost efectuată în conformitate cu procedura stabilită și că integritatea și confidențialitatea perechii de chei au fost asigurate. Acest raport este semnat:

- Pentru CertDigital ROOT CA G4: prin rolul de încredere responsabil pentru securitatea de gestionare a generării cheilor CERTDIGITAL (ofițer de securitate) și a unei persoane de încredere independente de managementul (auditorul) CERTDIGITAL ca martor că raportul înregistrează corect gestionarea de generare a cheilor în timp ce se desfășoară.
- Pentru CA-urile subordonate: prin rolul de încredere responsabil pentru securitatea de gestionare a generării cheilor CERTDIGITAL (de exemplu, ofițer de securitate) ca martor că raportul înregistrează corect ceremonia de gestionare a cheilor în timp ce este efectuată.

În toate cazurile, CA:

- Generează cheile CA în cadrul modulelor criptografice care îndeplinesc cerințele tehnice și de afaceri aplicabile, astfel cum sunt prezentate în Procedura de certificare;
- Înregistrează activitățile de generare a cheilor CA;
- Menține controale eficiente pentru a oferi o asigurare rezonabilă că Cheia Privată a fost generată și protejată în conformitate cu procedurile descrise în Procedura de certificare și, dacă este cazul, în scriptul generării cheii.

Cheile CertDigital QUALIFIED CA G4 precum și cheile altor autorități subordonate și certificarea ulterioară a cheilor publice sunt efectuate într-un mediu fizic securizat de către personal în roluri de încredere, de cel puțin, control dublu:

- Cel puțin trei angajați în roluri de încredere
- Agentul de securitate
- Cel puțin un reprezentant al Compartimentul Managementul Politicilor si Procedurilor (CMPP)
- Un maestru al generării cheii
- Cel puțin un auditor independent și extern

Perechile de chei ale Autorităților de Certificare care funcționează în cadrul CERTDIGITAL sunt generate pe stații de lucru desemnate și autentificate și conectate la module de securitate hardware care respectă cerințele FIPS 140-2 Level 3 sau ISO / IEC 15408 EAL 4. Acestea sunt reținute permanent pe aceste dispozitive criptate.

Procesul de generare a perechilor de chei ale Autorităților de Certificare este similar cu procedura acceptată pentru generarea de perechi de chei în CERTDIGITAL, așa cum este descris mai sus. Acțiunile executate în timpul generării perechii de chei sunt înregistrate, datate și semnate de fiecare persoană prezentă în timpul generării. Înregistrările sunt păstrate pentru necesitățile auditurilor și revizuirilor comune ale sistemului.

Operatorii Autorității de Înregistrare au doar cheile pentru autentificarea tuturor acțiunilor lor. Aceste chei sunt generate de operator (în prezența ofițerului de securitate) prin intermediul unui software autentificat furnizat de o Autoritate de Certificare și pe un QSCD.

Generarea de perechi de chei CA este efectuată într-un dispozitiv criptografic securizat, care este un sistem de încredere care este asigurat la EAL 4 sau superior conform ISO / IEC 15408 sau FIPS PUB 140-2 nivel 3.

Generarea de perechi de chei CA este realizată utilizând algoritmul RSA cu lungimea cheii de 4096 biți.

Înainte de expirarea certificatului CA utilizat pentru semnarea cheilor subiectului, CA va genera un nou certificat pentru semnarea perechilor cheilor subiectului și va aplica toate acțiunile necesare pentru a evita perturbarea operațiunilor oricărei entități care se poate baza pe certificatul CA. Noul certificat CA va fi, de asemenea, generat și distribuit în conformitate cu acest CPS. Aceste operațiuni trebuie efectuate cu intervalul de timp adecvat între data de expirare a certificatului și ultimul certificat semnat, pentru a

permite tuturor părților care au relații cu CERTDIGITAL (subiecți, abonați, părțile implicate, CA mai mari în ierarhia CA etc.) să confirme schimbarea de chei și punerea în aplicare a operațiunilor necesare pentru a evita orice inconvenient și funcționare defectuoasă. Acest lucru nu se aplică în cazul în care ar înceta operațiunile înainte de data de expirare a certificatului de semnătură sau de certificat.

6.1.2 Livrarea cheii private către abonat

Nu se aplică

6.1.3 Livrarea cheii publice către emitentul certificatului

Nu se aplică

6.1.4 Furnizarea de chei publice CA către părțile implicate

Cheile de verificare a semnăturii CA sunt puse la dispoziția părților asociate într-o manieră care asigură integritatea cheii publice CA și autentifică originea acesteia.

Cheile publice ale Autorității de Certificare care eliberează certificate pentru subiecți sunt distribuite numai sub forma certificatelor care respectă recomandările ITU-T X.509 v.3. În cazul autorității de certificare CertDigital ROOT CA G4, certificatele sunt semnate automat.

Autoritățile de certificare CERTDIGITAL își publică certificatele prin plasarea lor în depozitul public al CERTDIGITAL: https://www.certdigital.ro/repository .

Certificatele Autorității de Certificare CERTDIGITAL pot fi transmise părților asociate împreună cu software-ul (sisteme de operare, browsere web, clienți de e-mail etc.), care permit utilizarea serviciilor oferite de CERTDIGITAL.

Depozitul de certificate impune controlul accesării după adăugarea, ștergerea certificatelor sau modificarea informațiilor aferente.

6.1.5 Dimensiunile cheilor

Dimensiunile cheilor eliberate de Autoritățile de Certificare, de operatorii Autorității de Înregistrare și de subiecți sunt prezentate în Tabelul 6.1.

Proprietar cheie	Utilizarea cheii primare		
	RSA pentru semnarea certificatului si CRL-ului	RSA pentru semnarea mesajului	RSA pentru schimbul de chei
CERTDIGITAL ROOT CA G4	4096 bits	-	-
CERTDIGITAL QUALIFIED CA G4	4096 bits	-	-

Tabelul 6.1. Dimensiunea cheilor folosite

6.1.6 Generarea și verificarea parametrilor cheilor publice

Un creator de chei este responsabil pentru verificarea calității parametrilor cheii generate. Este obligat să verifice:

- Abilitatea de a executa operațiuni de criptare și decriptare, inclusiv crearea de semnături electronice și verificarea acesteia,
- Procesul de generare a cheilor, care ar trebui să se bazeze pe generatoare de numere criptografice puternice aleatorii - surse fizice de zgomot alb, dacă este posibil,
- Rezistența la atacuri cunoscute (se aplică algoritmilor RSA și DSA).

6.1.7 Obiectivele cheie de utilizare (conform câmpului de utilizare al cheii X.509 v3)

Scopurile de utilizare a cheilor permise sunt descrise în câmpul KeyUsage (vezi Capitolul 7.1.1.2) din extensia standard a unui certificat care respectă X.509 v3. Acest câmp trebuie să fie verificat de aplicația Subiecților care gestionează certificatele.

Utilizarea biților din câmpul KeyUsage trebuie să respecte următoarele reguli:

a) digitalSignature: certificat destinat verificării semnăturii electronice,

b) nonRepudiation: certificat destinat furnizării unui serviciu de non-repudiere de către persoane fizice, precum și în alte scopuri decât cele descrise la punctele f) și g). Nota de repetare nu poate fi stabilită decât într-un certificat de cheie publică destinat să verifice semnăturile

electronice și nu trebuie combinat cu scopurile descrise la punctele c) -e) și legate de asigurarea confidențialității,

c) keyEncipherment: destinat să cripteze cheile algoritmului simetric, furnizând confidențialitatea datelor,

d) dataEncipherment:destinate criptării datelor Subiectului, altele decât cele descrise în c) și e)

e) keyAgreement: destinat pentru protocoale de schimb de cheie,

f) keyCertDigital: cheia publică este folosită pentru verificarea semnăturii electronice în certificatele emise de entitățile care furnizează servicii de certificare,

g) cRLSign: cheia publică este folosită pentru verificarea semnăturilor electronice pe listele revocate și suspendate eliberate de entitățile care furnizează servicii de certificare,

h) encipherOnly: poate fi folosit exclusiv cu un bit keyAgreement pentru a indica scopul său de criptare a datelor în protocoalele de schimb de chei,

i) decipherOnly: poate fi folosit exclusiv cu bit keyAgreement pentru a indica scopul său de decriptare a datelor în protocoalele de schimb cheie.

6.2 Protecția cheilor private și controlul ingineriei modulului criptografic

Fiecare subiect, operator al Autorității de Certificare și Autoritatea de Certificare generează și stochează cheia privată folosind un sistem fiabil care împiedică pierderea, dezvăluirea, modificarea sau accesul neautorizat al cheii private. În cazul în care o Autoritate de Certificare generează o pereche cheie pe baza unei solicitări a subiectului/abonatului autorizat, trebuie să o livreze în mod sigur subiectului și să impună subiectul să-și protejeze cheia privată.

CERTDIGITAL utilizează dispozitive criptografice sigure adecvate pentru a efectua sarcini de gestionare a cheilor CA. Aceste dispozitive criptografice sunt de asemenea cunoscute ca Module de Securitate Hardware (HSM).

Mecanismele hardware și software care protejează cheile private CA sunt documentate corespunzător. HSM-urile sunt pregătite, distribuite și gestionate în conformitate cu următoarele standarde tehnice:

- ETSI EN 319 401
- ETSI EN 319 411-1
- ETSI EN 319 411-2

Măsurile sunt luate astfel încât dispozitivele criptografice sigure să nu fie manipulate în timpul transportului și depozitării în incinta CERTDIGITAL.

HSM-urile nu părăsesc mediul securizat al spațiilor securizate ale CA. În cazul în care HSM necesită întreținere sau reparații care nu pot fi efectuate în incinta securizată a CA (sub controlul dublu al mai multor angajați într-un rol de încredere), acestea sunt dezafectate în siguranță.

Între sesiunile de utilizare, HSM-urile sunt păstrate în siguranță în incinta securizată a CA.

Cheile private CA rămân sub un control multiplu. Administratorilor CA li se atribuie sarcina de a activa și dezactiva cheile private ale CA. Cheile CA sunt active pentru perioade de timp definite.

Cheile private de semnare ale CA stocate pe dispozitivul criptografic securizat al CA vor fi distruse la retragerea dispozitivului.

6.2.1 Standardele și comenzile modulului criptografic

Subiectul utilizează o protecție hardware cheie care respectă cel puțin standardele FIPS 140-2 nivel 3 sau Common Criteria EAL 4. Generarea de perechi de chei generate de CA va fi efectuată într-un dispozitiv criptografic securizat, care este un sistem de încredere care respectă cel puțin standardele FIPS 140-2 de nivel 3 sau Common Criteria EAL 4.

6.2.2 Controlul multi-personal al cheii private

Controlul multi-personal al unei chei private se aplică cheilor private de la CertDigital ROOT CA G4 utilizate pentru certificarea și semnarea CRL.

Controlul dual al accesului este realizat prin furnizarea de secrete operatorilor autorizați. Secretele sunt stocate pe carduri sau dispozitive criptografice, protejate de un cod PIN și transferate autentificate proprietarului lor.

Procedura comună de transfer secret trebuie să includă: procesul de generare și distribuire a cheilor, acceptarea secretului eliberat și responsabilitățile care rezultă din păstrarea acestuia.

Acceptarea secretului împărtășit de deținătorii săi

Fiecare deținător de secrete comune, înainte de a-și primi secretul, ar trebui să verifice corectitudinea unui secret creat și distribuirea sa. Fiecare parte a secretului partajat trebuie să fie transferată titularului său pe un card criptografic sau un jeton protejat de un număr PIN atribuit de titular și cunoscut doar de acesta.

Recepția secretului comun și crearea sa adecvată este confirmată prin semnătura pe o formă corespunzătoare, a cărei copie este păstrată în arhivele Autorității de Certificare și de către deținătorul secretului.

Protecția secretului comun

Titularii de secrete partajate trebuie să-și protejeze partea de a fi divulgate. Titularul declară că:

- nu va dezvălui, nu va copia sau nu va împărți secretul cu nici o altă parte și că nu va folosi acțiunea în mod neautorizat,
- nu va dezvălui (direct sau indirect) că este titularul secretului,

Disponibilitatea și ștergerea (transferul) secretului partajat

Titularul unui secret comun ar trebui să permită accesul părții sale la entitățile juridice autorizate (într-o formă adecvată, semnată de titular la livrarea acțiunii) numai după autorizarea transmiterii secrete. Această situație ar trebui înregistrată în sistemul de securitate ca un jurnal de tranzacții adecvat.

În cazul catastrofelor naturale, deținătorul secretului trebuie să se prezinte pe site-ul de recuperare de urgență al CERTDIGITAL, conform instrucțiunilor emise de emitentul de acțiuni. Secretul comun ar trebui să fie transmis de către deținător la site-ul de recuperare de urgență.

Personal de către deținător într-o manieră care permite utilizarea partajată pentru restaurarea activității CERTDIGITAL în starea sa normală.

Responsabilitățile titularului secretului comun

Titularul secretului comun trebuie să își îndeplinească îndatoririle și obligațiile în conformitate cu cerințele prezentei Declarații de practici de certificare și într-un mod deliberat și responsabil în orice situație posibilă. Un deținător secret comun ar trebui să notifice emitentului secretul partajat în caz de furt, pierdere, dezvăluire neautorizată sau încălcare a securității imediat după producerea incidentului. Un deținător de secret comun nu poate fi acuzat de neglijarea sarcinilor sale din motive care îi depășesc controlul. Pe de altă parte, el este responsabil pentru divulgarea necorespunzătoare a secretului sau pentru omisiunea de a notifica emitentului secretul despre încălcarea securității secretului, care rezultă din greșeala, neglijența sau iresponsabilitatea titularului.

6.2.3 Private Key escrow

Cheile private ale Autorităților de Certificare nu sunt supuse custodiei.

6.2.4 Backup-ul cheii private

Autoritățile de certificare care funcționează în cadrul CERTDIGITAL creează o copie de siguranță a cheii private. Copiile sunt utilizate în cazul executării procedurii de recuperare standard sau de urgență a cheii (de exemplu după dezastru). Când este în afara dispozitivului criptografic securizat, cheia privată CA este protejată într-un mod care asigură același nivel de protecție ca cel furnizat de dispozitivul criptografic securizat. Copiile cheilor private sunt protejate de secrete comune.

CERTDIGITAL nu păstrează copii ale cheilor private ale operatorului de certificare.

Cheia privată de semnare CA este copiată (backup), stocată și recuperată numai de către personalul cu roluri de încredere, utilizând cel puțin controlul dublu într-un mediu fizic securizat. Numărul personalului autorizat să efectueze această funcție este menținut la un nivel minim și în concordanță cu practicile CA.

Copiile cheilor private de semnare ale CA sunt supuse aceluiași nivel sau unor niveluri mai mari de controale de securitate ca și cheile utilizate în prezent.

6.2.5 Arhivarea cheii private

Cheile private ale Autorităților de Certificare utilizate pentru crearea semnăturii electronice nu sunt arhivate - acestea sunt distruse imediat după terminarea executării operațiunii criptografice care utilizează aceste chei sau după expirarea certificatului asociat sau după revocarea acesteia.

6.2.6 Transferul cheii private în sau din modulul criptografic

Funcționarea introducerii unei chei private într-un modul criptografic se efectuează în următoarele cazuri:

- La crearea copiilor de rezervă pentru cheile private stocate într-un modul criptografic, poate fi ocazional necesar (de exemplu, în caz de corupere sau defecțiune a modulului) să introducă o pereche de chei într-un alt modul de securitate,
- Când este necesar să se transfere o cheie privată din modulul operațional, utilizat de entitate pentru operații standard, la un alt modul; situația poate apărea în cazul defectării sau dezafectării modulului.

Introducerea unei chei private în modulul de securitate este o operație critică, prin urmare măsurile și procedurile care împiedică dezvăluirea, modificarea sau falsificarea cheie sunt puse în aplicare în timpul executării operației.

Introducerea unei chei private într-un modul hardware de securitate al Autorității de Certificare CertDigital ROOT CA G4 necesită restaurarea cheii de pe HSM în prezența unui număr corespunzător de proprietari ai secretului comun care protejează modulul care conține cheile private. Datorită faptului că Autoritatea de Certificare poate păstra o copie criptată a cheii private, cheile pot fi, de asemenea, transferate între module.

6.2.7 Depozitarea cheii private pe modulul criptografic

CERTDIGITAL utilizează module de securitate hardware (HSM) pentru a efectua sarcini de gestionare a cheilor CA. Sunt luate măsuri pentru ca dispozitivele criptografice sigure să nu fie manipulate în timpul expedierii și în timp ce sunt depozitate în incinta CERTDIGITAL.

Trebuie să existe controale de acces pentru a se asigura că cheile nu sunt accesibile în afara dispozitivelor criptografice securizate dedicate unde sunt stocate cheile private de copiere și copii ale CA.

HSM-urile nu părăsesc mediul securizat al spațiilor securizate ale CA.

Între sesiunile de utilizare, HSM-urile sunt păstrate în siguranță în incinta securizată a CA.

Cheile private CA rămân sub un control multiplu. Administratorilor CA li se atribuie sarcina de a activa și dezactiva cheile private ale CA. Cheile CA sunt active pentru perioade de timp definite.

Operatorii utilizează dispozitive de creare a semnelor electronice calificate (dispozitive / carduri). Cheile sunt întotdeauna generate pe dispozitive și nu se copiază niciodată de pe dispozitiv. Dispozitivele securizate sunt protejate de producători pentru CERTDIGITAL, în timpul depozitării la CERTDIGITAL și în timp ce sunt distribuite.

6.2.8 Metoda de activare a cheii private

Toate cheile private ale CertDigital ROOT CA G4 sunt introduse în modul după generare, importate într-o formă criptată dintr-un alt modul sau după restaurarea din secrete comune. Activarea cheilor private este întotdeauna precedată de autentificarea operatorului. Autentificarea se efectuează pe baza unui card criptografic deținut de operator. După introducerea cardului în modulul criptografic și după introducerea numărului PIN, cheia privată rămâne activă până când cardul este scos din modul.

6.2.9 Metoda de dezactivare a cheii private

Metoda de dezactivare a cheii private se aplică dezactivării cheie după folosirea acesteia sau la terminarea fiecărei sesiuni în care a fost utilizată cheia.

Dezactivarea unei chei private se efectuează atunci când cardul este scos din modul.

6.2.10 Metoda de distrugere a cheii private

La sfârșitul vieții, cheile private ale CA sunt distruse de roluri de încredere ale CA în prezența a mai mult de un reprezentant al Compartimentul de Management al Politicii și Procedurilor (CMPP), pentru a se asigura că aceste chei private nu pot fi recuperate sau folosite din nou .

Cheia privată CA poate fi distrusă prin ștergerea tuturor cardurilor HSM (Operator și Administrator). În plus, HSM permit zeroirea dispozitivului prin acces fizic și setările de pe dispozitiv. Aceasta reinitializează dispozitivul și suprascrie toate datele din acesta cu zerouri binare. În cazurile în care această procedură de zeroiziere sau reinițializarea nu reușește, CERTDIGITAL va zdrobi, arunca și / sau arde aparatul într-o manieră care distruge capacitatea de a extrage orice secret.

Aceste module hardware sunt tratate într-un mod sigur, așa cum este descris în procedurile interne de distrugere a documentelor cheie documentate. Dosarele asociate sunt arhivate în siguranță. Compartimentul de Management al Politicii și Procedurilor (CMPP) autorizează distrugerea cheii private a CA și atribuie personalului sarcina.

Fiecare distrugere a cheii private este înregistrată în jurnalul evenimentului.

6.2.11 Evaluarea modulului criptografic

Vezi deasupra.

6.3 Alte aspecte ale gestionării perechii de chei

CERTDIGITAL va folosi în mod corespunzător cheile de semnătură private ale CA și nu le va folosi după sfârșitul ciclului lor de viață.

Cheile de semnare ale CA utilizate pentru generarea certificatelor și listele de revocare a certificatelor nu vor fi utilizate în alte scopuri.

Cheile de semnare a certificatelor se utilizează numai în spații protejate fizic.

Utilizarea cheii private a CA este compatibilă cu algoritmul hash, algoritmul de semnătură și lungimea cheii de semnătură utilizate pentru generarea de certificate, în conformitate cu practicile curente (lungimea și algoritmul cheie selectat pentru cheia de semnare CA sunt RSA 4096 biți în acord Cu cerințele din ETSI TS 119 312 pentru scopurile de semnare ale CA)

Toate copiile cheilor private de semnare ale CA vor fi distruse la sfârșitul ciclului lor de viață.

Atributele certificatului CertDigital ROOT CA G4 (certificat auto-semnat) trebuie să fie compatibile cu utilizarea cheie definită conform recomandării ITU-T X.

6.3.1 Arhivarea cheilor publice

CERTDIGITAL își arhivează propriile chei publice CA. Vezi secțiunea 5.5 a CPS pentru condițiile de arhivare.

Scopul arhivei cheilor publice este de a crea posibilitatea de a verifica o semnătură electronică după ce un certificat este scos din depozit. Este extrem de important în furnizarea de servicii non-repudiere, cum ar fi serviciile de timestamp sau serviciile de verificare a statutului certificatului.

Arhivarea cheilor publice implică arhivarea certificatelor care conțin aceste chei.

Fiecare autoritate care emite certificate arhivează cheile publice ale subiecților cărora le-au fost eliberate certificatele. Autoritățile de certificare cheile publice sunt arhivate împreună cu cheile private, în modul descris în Capitolul 6.2.5.

Arhivele de chei publice ar trebui să fie protejate împotriva adăugării neautorizate, introducerii, modificării sau ștergerii neautorizate a cheii către sau din arhivă. Protecția este pusă în aplicare prin autentificarea entității de arhivare și prin autorizarea cererilor acestora.

Administratorul de securitate efectuează examinarea integrității arhivei cheilor publice de două ori pe an. Scopul acestei verificări este de a se asigura că nu există lacune în arhivă, iar certificatele stocate în arhivă nu au fost modificate. Mecanismele care verifică integritatea arhivei iau în considerare faptul că perioada de păstrare a arhivelor poate fi mai lungă decât mijloacele de securitate utilizate pentru crearea arhivelor.

Cheile publice sunt păstrate în arhiva certificatelor digitale pentru o perioadă de cel puțin 10 ani.

6.3.2 Perioadele de funcționare a certificatului și perioadele de utilizare a perechilor de chei

Perioada de utilizare a cheilor publice este definită de valoarea valabilității câmpului fiecărui certificat menționat mai jos.

Valorile standard ale perioadei maxime de utilizare a certificatelor autorității de certificare sunt enumerate în tabelul 6.3.2.1

Perioadele de utilizare a certificatelor și cheile private corespunzătoare pot fi reduse în cazul revocării certificatelor.

În general, data de începere a valabilității unui certificat corespunde datei emiterii acestuia. Nu este permisă setarea acestei date în viitor sau în trecut.de cheie publică. Este, de asemenea, perioada de valabilitate aplicată cheii private. Perioada maximă de utilizare a cheilor de la Subiect nu poate depăși dublul duratei de valabilitate a unui certificat, care este

Proprietar cheie	Scopul principal al folosirii cheie
	RSA pentru semnarea certificatului și CRL
CertDigital ROOT CA G4	30 ani
CertDigital QUALIFIED CA G4	15 ani

Tabelul 6.3.2.1 Perioada maximă de utilizare a certificatelor CA

6.4 Datele de activare

6.4.1 Generarea și instalarea de date de activare

Datele de activare sunt utilizate în două cazuri de bază:

- Ca element al procedurii de autentificare cu una sau mai multe factori (așa-numita expresie de autentificare, de exemplu, parolă, număr PIN etc.)
- Ca parte a secretului comun.

Autoritățile și administratorii Autorității de Înregistrare și Autorității de Certificare, precum și alte persoane care îndeplinesc rolurile descrise în Capitolul 5.2 utilizează acreditări securizate (dispozitive / carduri) pentru a identifica și autentifica pentru rolurile lor. Cheile lor private care sunt generate de dispozitive de semnătură electronică calificată sau de carduri inteligente HSM de către CERTDIGITAL sunt asociate cu activarea și distribuirea sigură a datelor de activare a utilizatorului (codul PIN). CERTDIGITAL se asigură că datele de activare a operatorilor și administratorilor RA și CA sunt gestionate și protejate în siguranță de acești participanți prin proceduri interne aplicabile acestor participanți.

Secretele comune utilizate pentru protecția cheii private a Autorității de Certificare sunt generate în conformitate cu cerințele prezentate în Capitolul 6.2 și păstrate în interiorul cartelelor criptografice. Cardurile sunt protejate de un număr PIN. Secretele partajate devin date de activare după activarea

acestora, adică punerea codului PIN corect protejând cardul. CERTDIGITAL asigură că datele de activare asociate cheilor private și operațiunilor CA.

Sunt generate, gestionate, stocate și arhivate în siguranță, după cum se descrie în subsecțiunea relevantă din secțiunile 6.1 și 6.2. Instalarea și recuperarea perechilor cheie ale CA într-un dispozitiv criptografic securizat necesită un control simultan al cel puțin doi angajați în roluri de încredere.

6.4.2 Protecția datelor de activare

Protecția datelor privind activarea include metode de control al activării datelor care împiedică dezvăluirea acestora. Metodele de control al protecției datelor de activare sunt selectate în funcție de faptul dacă acestea sunt fraze de autentificare sau dacă controlul este pus în aplicare pe baza cheii private sau pe distribuirea datelor sale de activare în secrete partajate.

Datele de activare utilizate pentru activarea cheii private trebuie să fie protejate prin intermediul controalelor criptografice și a controalelor de acces fizic. Datele de activare trebuie memorate (nu sunt scrise în jos) de entitatea care este autentificată. Dacă datele de activare sunt scrise, nivelul protecției lor ar trebui să fie același cu datele protejate prin utilizarea unei cărți criptografice. Mai multe încercări nereușite de a accesa modulul criptografic ar trebui să ducă la blocarea acestuia. Datele de activare stocate nu vor fi reținute niciodată împreună cu cardul criptografic.

6.4.3 Alte aspecte ale datelor de activare

Nu se aplică

6.5 Controalele de securitate ale calculatoarelor

Sarcinile autorităților de înregistrare și ale autorităților de certificare care operează în cadrul CERTDIGITAL se desfășoară prin hardware și software de încredere.

6.5.1 Cerințe tehnice specifice privind securitatea calculatoarelor

Mecanismele de securitate care protejează sistemele informatice sunt executate la nivelul sistemelor de operare, al aplicațiilor și al protecției fizice.

Computerele sunt configurate cu următoarele mecanisme de securitate:

- Înregistrarea obligatorie autentificată la nivelul sistemului de operare și al aplicațiilor,
- Controlul accesului discreționar,

- Posibilitatea efectuării auditului de securitate,
- Calculatorul este accesibil numai personalului autorizat, executând roluri de încredere în CERTDIGITAL,
- Punerea în aplicare a segregării sarcinilor, care decurge din rolul jucat în sistem,
- Identificarea și autentificarea rolurilor și a personalului care efectuează aceste roluri,
- Prevenirea unei reutilizări a unui obiect prin alt proces după ce obiectul a fost eliberat printr-un proces autorizat,
- Protecția criptografică a schimbului de informații și protecția bazelor de date,
- Arhivarea istoricului operațiunilor pe computer și a datelor solicitate de audituri,
- cale sigură care să permită identificarea și autentificarea fiabilă a rolurilor și a personalului care efectuează aceste roluri,
- Metode de restaurare a cheilor (numai pentru module de securitate hardware)
- Monitorizarea și alertarea în caz de acces neautorizat.

Integritatea sistemelor și informațiilor CERTDIGITAL este protejată împotriva virușilor, software-urilor rău intenționate și neautorizate.

Mijloacele folosite în cadrul sistemelor CERTDIGITAL sunt manipulate în siguranță pentru a proteja mediile de deteriorare, furt, acces neautorizat și uzură morală.

Procedurile de gestionare media sunt puse în aplicare pentru a proteja împotriva uzurii și deteriorării suporturilor media pentru perioada de timp pentru care trebuie păstrate înregistrările.

Datele sensibile sunt protejate împotriva dezvăluirii prin obiecte stocate reutilizate (de ex., Fișiere șterse) care sunt accesibile utilizatorilor neautorizați. În acest scop se utilizează software special cu algoritmi de ștergere sigure pentru mediile de stocare, HSM-urile sunt zero, dispozitivele criptografice securizate (dispozitive / carduri) trebuie formatate înainte de reutilizare / sau distruse fizic la sfârșitul ciclului lor de viață.

Pentru toate conturile capabile să provoace în mod direct emiterea certificatelor, este aplicată autentificarea multifactorială.

6.5.2 Evaluarea securității calculatorului

Sistemul informatic CERTDIGITAL îndeplinește cerințele descrise în standardele ETSI: ETSI EN 319 411-2 (Cerințe de politică și de securitate pentru furnizorii de servicii de asigurare care eliberează certificate, Partea 2: Cerințe pentru furnizorii de servicii de încredere care eliberează certificate calificate UE) Și CEN CWA 14167 (Cerințe de securitate pentru sisteme de încredere care gestionează certificate pentru semnături electronice).

6.6. Controale tehnice pentru ciclul de viață

CERTDIGITAL utilizează sisteme și produse de încredere care sunt protejate împotriva modificărilor și asigură securitatea tehnică și fiabilitatea proceselor suportate de acestea.

6.6.1 Controlul dezvoltării sistemului

O analiză a cerințelor de securitate se realizează în etapa de proiectare și cerințe a proiectelor de dezvoltare a sistemelor întreprinse de CERTDIGITAL sau în numele CERTDIGITAL pentru a se asigura că securitatea este integrată în sistemele informatice.

Fiecare aplicație, înainte de a fi utilizată pentru producție în cadrul CERTDIGITAL, este instalată astfel încât să permită controlul versiunii curente și să prevină instalarea neautorizată de programe sau falsificarea celor existente.

Reguli similare se aplică înlocuirii componentelor hardware, după cum urmează:

- Hardware-ul este furnizat într-o manieră care permite trasabilitatea și monitorizarea rutei componentelor la locul de instalare,
- Livrarea hardware-ului de rezervă se realizează într-un mod similar cu livrarea hardware-ului original; Înlocuirea este efectuată de personal de încredere și instruit.

6.6.2 Controalele de management al securității

Scopul controlului de management al securității este de a supraveghea funcționalitatea sistemelor CERTDIGITAL asigurând că sistemul funcționează corect și în conformitate cu configurațiile acceptate și implementate.

Controalele aplicate sistemului CERTDIGITAL permit verificarea continuă a integrității aplicației, a versiunii sale, precum și autentificarea și verificarea originii hardware.

6.6.3 Controalele de securitate a ciclului de viață

Politicile și procedurile de control al schimbării sunt aplicate pentru eliberările, modificările și remedierile de software de urgență ale oricărui software operațional și modificările configurațiilor care aplică politica de securitate a CERTDIGITAL.

Configurarea actuală a sistemelor CERTDIGITAL, orice modificări sau soluții de lansare, modificări și software de urgență pentru orice software operațional sunt documentate.

CERTDIGITAL implementează proceduri interne de securitate pentru a se asigura că:

- patch-uri de securitate sunt aplicate într-un timp rezonabil după ce acestea sunt disponibile;
- patch-urile de securitate nu sunt aplicate dacă introduc vulnerabilități sau instabilități suplimentare care depășesc beneficiile aplicării acestora;

Motivele pentru neaplicarea unor patch-uri de securitate sunt documentate.

CERTDIGITAL implementează o procedură internă de gestionare a capacității care să asigure monitorizarea capacității infrastructurii TIC pentru serviciile de certificare și realizarea de estimări ale cerințelor de capacitate pentru a se asigura disponibilitatea și stocarea adecvată a procesării.

6.7 Controalele de securitate a rețelei

CERTDIGITAL își protejează rețeaua și sistemele de atac.

În acest scop și pe baza evaluărilor de risc și a celor mai bune practici, implementăm un set integrat de controale de securitate:

a) Sistemele sunt segmentate în rețele sau zone bazate pe relația funcțională, logică și fizică (inclusiv locația) dintre sistemele și serviciile de încredere. CERTDIGITAL aplică aceleași controale de securitate tuturor sistemelor co-localizate în aceeași zonă.

b) Accesul și comunicațiile între zone sunt limitate la cele necesare pentru funcționarea serviciilor de certificare. Conexiunile și serviciile inutile sunt explicit interzise sau dezactivate. Setul stabilit de reguli este revizuit în mod regulat.

c) Toate sistemele critice pentru funcționarea serviciilor de certificare sunt păstrate într-una sau mai multe zone securizate,

d) Rețele dedicate pentru administrarea sistemelor informatice și a rețelei operaționale sunt separate. Sistemele utilizate pentru administrarea implementării politicii de securitate nu sunt

utilizate în alte scopuri. Sistemele de producție pentru serviciile de certificare sunt separate de sistemele utilizate în dezvoltarea și testare (de exemplu, sisteme de dezvoltare, testare și staționare).

e) Comunicarea între sisteme distincte de încredere se stabilește numai prin intermediul unor canale de încredere care sunt distincte în mod logic de alte canale de comunicare și oferă o identificare securizată a punctelor sale de final și protecția datelor canalelor de la modificare sau dezvăluire.

f) În cazul în care este necesar un nivel ridicat de disponibilitate a accesului extern la un anumit serviciu de certificare, conexiunea la rețeaua externă este redundantă pentru a asigura disponibilitatea serviciilor în cazul unei singure defecțiuni.

g) S-a efectuat scanarea obișnuită a vulnerabilității pe adresele IP publice și private identificate de CERTDIGITAL și se înregistrează dovezi că fiecare scanare de vulnerabilitate a fost efectuată de o persoană sau o entitate cu abilitățile, instrumentele, competența, codul de etică și independența necesară pentru a furniza un raport de încredere.

h) Serviciile de certificare CERTDIGITAL se supun unui test de penetrare a sistemelor aferente la înființare și după upgrade-uri sau modificări de infrastructură sau aplicații pe care CERTDIGITAL le consideră semnificative. Se evidențiază că fiecare test de penetrare a fost efectuat de o persoană sau entitate cu abilitățile, instrumentele, competența, codul de etică și independența necesară pentru a furniza un raport de încredere.

Serverele și stațiile de lucru de încredere ale sistemului CERTDIGITAL sunt conectate printr-o rețea locală (LAN), împărțită în sub-rețele cu acces controlat. Accesul de pe Internet către orice segment este protejat prin intermediul unui firewall inteligent.

Comenzile de securitate sunt dezvoltate pe baza firewall-ului și a filtrării traficului pe router-ele și serviciile Proxy care protejează domeniile rețelei interne ale CERTDIGITAL de acces neautorizat, inclusiv accesul de la subiecți / abonați și terți. Firewall-urile sunt configurate pentru a preveni toate protocoalele și accesările care nu sunt necesare pentru funcționarea CERTDIGITAL CA.

Mijloacele de protecție a securității rețelei acceptă numai mesajele transmise cu ajutorul protocoalelor http, https, NTP, POP3 și SMTP. Evenimentele (jurnalele) sunt înregistrate în jurnalele de sistem și permit supravegherea utilizării serviciilor furnizate de CERTDIGITAL. Componentele de rețea locală (de ex.,

Router-ele) sunt păstrate într-un mediu fizic și logic securizat, iar configurațiile lor trebuie verificate periodic pentru a se conforma cerințelor specificate de CERTDIGITAL.

CERTDIGITAL menține și protejează toate sistemele CA în cel puțin o zonă securizată și dispune de o procedură de securitate care protejează sistemele și comunicațiile dintre sistemele din zonele securizate și zonele de securitate ridicate.

CERTDIGITAL configurează toate sistemele CA eliminând sau dezactivând toate conturile, aplicațiile, serviciile, protocoalele și porturile care nu sunt utilizate în operațiunile CA.

CERTDIGITAL acordă acces la zonele securizate și zonele de securitate ridicate numai pentru roluri de încredere. Sistemul Root CA se află într-o zonă de securitate ridicată.

6.8 Timp-Stamping

Precizia de timp a jurnalelor este asigurată de un server de timp care este sincronizat cu cel puțin două surse de timp care pot fi sateliți GPS sau UTC (NIMB).

7. Profiluri CER, CRL și OCSP

Profilurile certificatelor și profilul listei de revocare a certificatelor (CRL) respectă formatul descris în standardul ITU-T X.509 v.3, în timp ce profilul OCSP respectă cerințele RFC 6960. Informațiile prezentate mai jos descriu semnificația Respectivele câmpuri de certificate, CRL și OCSP, ale standardelor aplicate și ale extensiilor private utilizate de CERTDIGITAL.

7.1 Profil certificat

Profilul câmpurilor de bază pentru certificatul CERTDIGITAL ROOT CA G4 descris în Tabelul 7.1.

Field name	Value or value's constraint	
Version	3	
Serial Number	201104209402	
Signature Algorithm	Sha512WithRSAEncryption (OID: 1.2.840.113549.1.1.13)	
Issuer (Distinguished Name)	Common Name (CN)=	CERTDIGITAL ROOT CA G4
	Organization Identifier (2.5.4.97) =	VATRO-2163993
	Organization Unit Name (OU) =	CERTDIGITAL
	Organization (O) =	CENTRUL DE CALCUL S.A.
	Country (C) =	RO

Not before (validity period beginning date)	July 07 03:00:00 2023 GMT	
Not after (validity period end date)	July 07 03:00:00 2053 GMT	
Subject (Distinguished Name)	Common Name (CN)=	CERTDIGITAL ROOT CA G4
	Organization Identifier (2.5.4.97) =	VATRO-2163993
	Organization Unit Name (OU) =	CERTDIGITAL
	Organization (O) =	CENTRUL DE CALCUL S.A.
	Country (C) =	RO
Subject Public Key Info	4096 bits RSA key	
Signature	Sha512WithRSAEncryption (OID: 1.2.840.113549.1.1.13)	

Tabelul 7.1. Profilul câmpurilor de bază pentru CertDigital ROOT CA G4

Profilul câmpurilor de bază pentru certificatele emise de CertDigital ROOT CA G4 este descris în Tabelul 7.2.

Field name	**Value or value's constraint**	
Version	Version 3	
Serial Number	Unique value greater than zero (0) for all certificate issued by Certification Authorities within CertDigital. It contains a random value of 8 bytes. A hardware cryptographic module is used for generating this value.	
Signature Algorithm	Sha512WithRSAEncryption (OID: 1.2.840.113549.1.1.13)	
Issuer (Distinguished Name)	Common Name (CN)=	CERTDIGITAL ROOT CA G4
	Organization Identifier (2.5.4.97) =	VATRO-2163993
	Organization Unit Name (OU) =	CERTDIGITAL
	Organization (O) =	CENTRUL DE CALCUL S.A.
	Country (C) =	RO
Not before (validity period beginning date)	Universal Time Coordinated based	
Not after (validity period end date)	Universal Time Coordinated based	
Subject (Distinguished Name)	Common Name (CN)=	Common Name of the CA
	Organization Identifier (2.5.4.97) =	Organization Identifier
	Organization Unit Name (OU) =	Organization Unit Name

	Organization (O) =	Organization
	Country (C) =	CA country
Subject Public Key Info	Encoded in accordance with RFC 5280, may contain information about RSA, DSA or ECDSA public keys (key identifier, key size in bits and value of the public key); RSA key size is presented in Chapter 6.1.5.	
Signature	Certificate signature, generated and encoded in accordance with the requirements described in RFC 5280.	

Tabelul 2. Profilul câmpurilor de bază ale certificatelor emise la nivelul ROOT CA

7.1.1 Numărul (numerele) versiunii

Toate certificatele emise de CERTDIGITAL sunt X.509 versiunea 3.

7.1.2 Extensiile certificatelor

Extensiile de certificate pentru CERTDIGITAL ROOT CA G4 sunt descrise în Tabelul 7.3.

Extension	Value or Value constraint	Extension status
Basic Constraints	Subject type=CA, Path length constraint=none	Critical
Key Usage	Certificate Signing, Off-line CRL Signing, CRL Signing (06)	Critical
Subject Key Identifier	eae713a1ea9dac9b90fb3d43188b39763fefb0e4	Non-critical
Thumbprint	1d2e6247728accdfe925782975b328e49450f200	Non-critical

Public key	30 82 02 0a 02 82 02 01 00 cc 4a 0e c7 90 e3 4a 24 bd 47 8e 20 70 9b 43 8a 5f b1 b9 ae e9 fe ff a4 f4 ee f8 db 42 22 9b 61 e5 cc 65 42 f2 e2 f2 d8 04 6e ae d8 5d 8d 55 32 c4 71 3f 44 ee 06 50 da 9b 17 53 a5 fb c5 bd 0c d6 48 29 58 64 f4 ea 82 c7 3b 5a 9b 07 62 a0 38 ff cc a5 cd 80 3c 25 e3 ff 4e 7a 44 73 90 31 73 3c ee ef 63 d3 f2 8a 12 4b d8 9b 66 81 d4 b2 d3 83 71 69 0e 9a 3c d2 f0 6a e4 90 86 09 d2 9f be 74 2d 0d a3 27 f4 c4 20 4e e6 07 9c 32 e8 ab 62 4e 1a 77 35 65 77 bd b1 9a 2a e3 44 5e b0 a1 bb 56 cd c8 88 9d df 88 74 55 30 b4 d9 91 e8 12 99 0f 2d 3e a4 68 11 aa 03 41 e5 65 2a 14 07 c3 b6 4a c8 e6 5a 95 a7 11 83 c7 5b c7 b2 30 6d de dc de 41 23 33 47 4e 70 18 63 d9 07 c1 5a e6 fc be 41 69 e4 f8 68 6c 64 ec 36 3e 23 4d 97 bf a0 cb dc 87 3c 58 15 5b da 91 1f a7 46 7c 2d 94 bf ec f7 b2 78 c0 0a e8 f8 79 ac 59 75 92 29 7b 43 63 0a 30 f6 2b 1f c1 7b 82 dc fb 47 e5 52 a5 ab 94 76 88 6c 00 b5 68 1b ff 8c 11 51 ae c5 b6 87 bb c4 d4 31 3e 6e ad d9 f9 e2 5f 5f 39 49 c3 e3 8b 9e 83 8b a9 cf a0 cf 5e 92 cb 30 22 b6 27 ef ef b1 fd 34 d7 f7 bd 93 08 d5 03 ce 12 d6 f0 a3 2c 33 0d 73 07 13 8d 6f 51 67 de a5 0f 9a 64 d5 31 7f 0e 31 7f c9 cc 2b 4c 7c 41 56 e1 35 1c 6d 7a 50 da 8a 1e 9a 3f 0b 13 9b 27 75 7b f4 09 49 b6 e9 11 1b 61 39 a4 12 17 de 21 82 6d f0 c3 be 6f 4e da f0 53 5e 50 7c f1 47 14 fc 52 5c f6 b9 62 e8 ee e6 4d 10 02 e8 40 df 1f 03 ee 23 57 4b c8 f9 5f 51 03 36 73 e9 3d 6f c4 ae 59 db 2a 14 42 70 0f d5 cd 86 a3 5d 7c 15 ad bc 7e d5 72 47 67 a7 b2 9b 56 79 46 ac 53 51 fc 12 6c 0e 47 54 d0 43 aa 88 85 71 1c 8e f5 94 27 69 d7 47 13 9e 25 02 03 00 f0 a5
ROOT CA G4 – Base64 Certificate	-----BEGIN CERTIFICATE----- MIIFvjCCA6agAwIBAgIGIBEEIJQCMA0GCSqGSIb3DQEBDQUAMH0xCzAJBgNVBAYT AlJPMR8wHQYDVQQKDBZDRU5UUlVMIERFIENBTENVTCBTLkEuMRQwEgYDVQQLDAtD RVJUREIHSVRBTDEWMBQGA1UEYQwNVkFUUk8tMjE2Mzk5MzEfMB0GA1UEAwwWQ0VS VERJR0IUQUwgUk9PVCBDQSBHNDAgFw0yMzA3MDcwMDAwMDBaGA8yMDUzMDcwNzAw MDAwMFowfTELMAkGA1UEBhMCUk8xHzAdBgNVBAoMFkNFTIRSVUwgREUgQ0FMQ1VM IFMuQS4xFDASBgNVBAsMC0NFUIRESUdJVEFMMRYwFAYDVQRhDA1WQVRSTy0yMTYz OTkzMR8wHQYDVQQDDBZDRVJUREIHSVRBTCBST09UIENBIEc0MIICIjANBgkqhkiG

	9w0BAQEFAAOCAg8AMIICCgKCAgEAzEoOx5DjSiS9R44gcJtDil+xua7p/v+k9O74 20Iim2HlzGVC8uLy2ARurthdjVUyxHE/RO4GUNqbF1OI+8W9DNZIKVhk9OqCxzta mwdioDj/zKXNgDwl4/9OekRzkDFzPO7vY9PyihJL2JtmgdSy04NxaQ6aPNLwauSQ hgnSn750LQ2jJ/TEIE7mB5wy6KtiThp3NWV3vbGaKuNEXrChu1bNyIid34h0VTC0 2ZHoEpkPLT6kaBGqA0HlZSoUB8O2SsjmWpWnEYPHW8eyMG3e3N5BIzNHTnAYY9kH wVrm/L5BaeT4aGxk7DY+I02Xv6DL3Ic8WBVb2pEfp0Z8LZS/7PeyeMAK6Ph5rFI1 kiI7Q2MKMPYrH8F7gtz7R+VSpauUdohsALVoG/+MEVGuxbaHu8TUMT5urdn54l9f OUnD44ueg4upz6DPXpLLMCK2J+/vsf001/e9kwjVA84S1vCjLDMNcwcTjW9RZ96l D5pk1TF/DjF/ycwrTHxBVuE1HG16UNqKHpo/CxObJ3V79AlJtukRG2E5pBIX3iGC bfDDvm9O2vBTXlB88UcU/FJc9rli6O7mTRAC6EDfHwPuI1dLyPlfUQM2c+k9b8Su WdsqFEJwD9XNhqNdfBWtvH7Vckdnp7KbVnlGrFNR/BJsDkdU0EOqiIVxHI71ICdp 10cTniUCAwDwpaNCMEAwHQYDVR0OBBYEFOrnE6HqnaybkPs9QxiLOXY/77DkMA8G A1UdEwEB/wQFMAMBAf8wDgYDVR0PAQH/BAQDAgEGMA0GCSqGSIb3DQEBDQUAA4IC AQCNZ3sP+Qo/w909Y5kjrcLt+ydDDwk5uojxevbl/WMJGIy3IOIGSpPmftNWi+5f E6PGbEzzNWRpQm97Nxbd1n0dmtGmCqJpwyKxBcqIhMTO9taZPsrOE6Pwg3i0KIwg GUqPrV7dZOYcuChThjQqiTIGeC3CE0QsWn3gR+QyfMaaV8qpmWA8t5a1ul3kPZLj UsSmjygPKkbAe/f9NRDJREfIMeve4kPuxRm76L1jD1jATRMzM7TWzAJwWebSrTyk ajTKr/SdLDITqLT/E0xKOTS6YOKIPhcDONnoQYvSFDwWgsom34SPHpt0EBHU8INa 8lqWJ39to8tPk1Z9HYnD82ijXwoxX2pCWxGLq8oSjWp6YM2sdOEcmneAR2oloPS6 owglCrwlmiTfpi3gppyquzOpSChmgFjzgfq2DhDa1pkUg6C0HPQj110Ansxs62vW uY3y9UQ5gN4DrDB7GKP6hHHPQCHe+/ZR6bOFZJ3Ksf6Zq/rD7ya6P4ceH1tnU+aK lAettX/lgznNOLYA54ug8a/sAdr+A49BqUz8HGkadu3Skwf+wTQLi8lsPEKY/zOc eP3AlhFm2jCm2+YbFw+FkoateWPcECQseauTwhueoVljRgPeLPnIJOGbgDqjNDxe 7T+tLZ1e2NZspzqdYD10F6Cxz3NCerBujYJqzjoo/8yW8Q== -----END CERTIFICATE-----

Table 7.3. Extensiile certificatului CertDigital ROOT CA G4.

Extensiile de certificate pentru Autoritățile subordonate CERTDIGITAL ROOT CA G4 sunt descrise în Tabelul 7.4.

Extension	Value or Value constraint	Extension status
Authority Key Identifier	KeyID=eae713a1ea9dac9b90fb3d43188b39763fefb0e4	Non-critical
Subject Key Identifier	KeyIdentifier este compus din SHA-1 hash pe 160 biți a valorii BIT STRING subjectPublicKey (cu excepția etichetei, lungimii și numărului de biți neutilizate).	Non-critical
Basic Constraints	Subject type=CA, Path length constraint=0	Critical
Key Usage	Certificate Signing, Off-line CRL Signing, CRL Signing (06)	Critical
CRL Distribution Points	http://crl.certdigital.ro/certdigital_root_g4.crl	Non-critical

Certificate Policies	Certificate Policies [1]Certificate Policy: Policy Identifier = All issuance policies [1,1]Policy Qualifier Info: Policy Qualifier Id = CPS Qualifier: https://www.certdigital.ro/repository	Non-critical
Authority Info Access	[1] Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.g4.certdigital.ro [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= https://certs.certdigital.ro/certdigital_root_g4.crt	Non-critical

Tabelul 7.4. Extensiile certificatelor pentru certificatele autorităților subordonate

7.1.3 Identificatori de obiect al algoritmului

Câmpul algoritmului de semnătură conține un identificator algoritm criptografic utilizat pentru semnătură electronică creat de o autoritate de certificare pe certificat. În cazul CERTDIGITAL, algoritmul utilizat este Sha512WithRSAEncryption (OID: 1.2.840.113549.1.1.13)

7.1.4 Formulare de nume

Vezi secțiunea 3.1 Denumirea.

7.1.5 Constrângeri de nume

Nu se aplică.

7.1.6 Identificatorul obiectului politicii certificatului

Certificatele de identificare a obiectelor de politică utilizate la nivel de CA Root sunt descrise în Tabelul 7.6.

Root CA Level	Type	OID
CERTDIGITAL ROOT CA G4	CA certificates	2.5.29.32.0
	OCSP certificate	1.3.6.1.4.1.47898.4.2.2.1.2

Tabel 7.6 Elementele de identificare a obiectelor de politică de certificare

7.1.7 Utilizarea extensiei Constrângeri de politică

Nu se aplică.

7.1.8 Sintaxa și semantica calificărilor de politică

Certificatele de emisiune CERTDIGITAL conțin un calificativ de politică în cadrul extensiei Politicile certificatului. Această extensie conține un calificativ CPS pointer care indică CPS.

7.1.9 Semantica de procesare a extinderii critice a Certificatelor de Certificare

Nu se aplică.

7.2 Profilul CRL

Profilul CRL este descris în Tabelul 7.7.

Field name	Value or value's constraint	
Version	V2	
Signature Algorithm	Sha512WithRSAEncryption (OID: 1.2.840.113549.1.1.13)	
Issuer	Common Name (CN)=	Common Name (CN)=
	Organization Identifier (2.5.4.97) =	VATRO-2163993
	Organization Unit Name (OU) =	CERTDIGITAL
	Organization (O) =	CENTRUL DE CALCUL S.A.
	Country (C) =	RO
ThisUpdate	Date of CRL issuance	
NextUpdate	Date of next expected CRL update	
Revoked Certificates	List of revoked certificates	

Tabel 7.7 Profil CRL pentru CERTDIGITAL ROOT CA G4

7.2.1 Numărul (numerele) versiunii

Toate CRL emise de CERTDIGITAL sunt X.509 versiunea 3.

7.2.2 Extensii de intrare pentru CRL și lista de certificate

Extensiile CRL pentru CERTDIGITAL ROOT CA G4 sunt descrise în Tabelul 7.8.

Extension	Value or Value constraint	Extension status
Authority Key Identifier	KeyID=eae713a1ea9dac9b90fb3d43188b39763fefb0e4	Non-critical
CRL Number	monotonically increasing sequence number	Non-critical

Tabelul 7.8. Extensiile CRL pentru CertDigital ROOT CA G4.

7.3 Profil OCSP

Protocolul de verificare a statutului certificatului on-line (OCSP) permite evaluarea statutului certificatului.

Serviciul OCSP este furnizat de CERTDIGITAL în numele tuturor autorităților de certificare afiliate. Serverul OCSP, care emite confirmări de stare a certificatului, utilizează o pereche de chei speciale pentru fiecare CA subordonat și CA Root, generate exclusiv în acest scop.

Certificatul de server OCSP trebuie să conțină extensia extKeyUsage, descrisă în RFC 5280.

Această extensie ar trebui să fie stabilită ca necritică și înseamnă că o autoritate de certificare care emite certificatul pentru serverul OCSP confirmă prin delegarea sa autorizația de a emite conformarea statutului certificatului (de la abonații acestei autorități).
De asemenea, certificatul de server OCSP conține extensia *OCSPNoCheck*, descrisă de RFC 6960. Această extensie trebuie declarată non-critică, ceea ce înseamnă că un client OCSP care primește un răspuns semnat cu cheia privată asociată acestui certificat poate avea încredere în certificatul serverului OCSP fără a fi necesară verificarea statutului său de revocare.

Entitatea care primește o confirmare emisă de serverul OCSP trebuie să accepte formatul de răspuns standard cu identificatorul **id-pkix-ocsp-basic.**

Informații despre starea certificatului sunt incluse în câmpul **certStatus** al câmpului structura **singleResponse**. Aceasta poate avea una din următoarele trei valori principale:

- GOOD - indică statutul valabil al unui certificate
- REVOKED - indică faptul că certificatul a fost emis și revocat sau că certificatul nu a fost emis în conformitate cu RFC 6960
- UNKNOWN - indică faptul că nu există suficiente informații pentru a determina starea certificatului

Când răspunsul OCSP conține un cod de eroare (mesaj), răspunsul nu este semnat digital (RCF 6960).

7.3.1 Numărul (versiunile) versiuni

Serverul OCSP care funcționează în cadrul CERTDIGITAL emite confirmări de stare a certificatului în conformitate cu RFC 6960. Singura valoare admisibilă a numărului de versiune este 0 (este echivalentul versiunii v1).

7.3.2 Extensii OCSP

În conformitate cu RFC 6960, serverul OCSP CERTDIGITAL acceptă următoarea extensie:
Obligativitatea unei cereri și a unui răspuns pentru a preveni atacurile de răspuns**.** **Nonce** este inclus în **requestExtension** a **OCSPRequest** și repetată în răspunsul câmpului Extension al **OCSPResponse.**

8. Audit de conformitate și alte evaluări

În prezent, CERTDIGITAL este un furnizor calificat de servicii de certificare în conformitate cu articolul 51 alineatul 3 (măsură tranzitorie) din Regulamentul UE 910/2014. CERTDIGITAL intenționează să-și păstreze statutul de furnizor de servicii de certificare calificat și este în curs de a efectua un audit și să transmită organismului național de supraveghere un raport de evaluare a conformității cât mai curând posibil, dar nu mai târziu de 1 iulie 2017.
În ceea ce privește auditurile de conformitate și competența, funcționarea consecventă și imparțialitatea conformității organismelor de evaluare care evaluează și certifică conformitatea noastră ca furnizor de servicii de certificare și conformitatea serviciilor noastre de certificare cu criteriile din Regulamentul 910/2014 și actele de punere în aplicare a acestuia, Cerințele din standardul ETSI EN 319 403.

8.1 Frecvența sau circumstanțele de evaluare

Activitățile CERTDIGITAL care sprijină furnizarea serviciilor prezentate de CPS ROOT CA sunt auditate cel puțin o dată la 24 de luni.
Auditul verifică conformitatea cu standardele tehnice CPS și ETSI 319401 și ETSI 319411.
Auditul la cerere poate fi realizat la discreția CERTDIGITAL, la cererea organismului de supraveghere, astfel cum este definit în Regulamentul UE 910/2014, sau pentru a demonstra conformitatea cu cerințele specifice industriei, legale sau de afaceri.

8.2 Identitatea / calificările evaluatorului

Evaluarea va fi efectuată de un organism de evaluare a conformității, astfel cum este definit în Regulamentul UE 910/2014.

8.3 Relația evaluatorului cu entitatea evaluată

Organismul de evaluare a conformității este un auditor independent, care nu este afiliat direct sau indirect cu CERTDIGITAL.

8.4 Subiectele acoperite de evaluare

Auditurile planificate acoperă, dar nu se limitează la, toate aspectele operațiunilor și serviciilor CERTDIGITAL specificate în CPS ROOT CA.

8.5 Acțiuni întreprinse ca urmare a deficienței

Organismul de evaluare a conformității raportează deficiențele și neconformitățile detectate către CMPP. CERTDIGITAL și organismul de evaluare a conformității analizează concomitent rezultatele raportului și aprobă un plan de corecție și un interval de timp pentru punerea în aplicare a acestuia.
Este posibil să se efectueze un audit ulterior, pentru a verifica acțiunile de remediere.

8.6 Comunicarea rezultatelor

Organismul de evaluare a conformității comunică raportul de audit Administrației CERTDIGITAL și CMPP.

9 Alte probleme de afaceri și juridice

9.1 Taxe

Taxele de servicii de certificare și tipurile de servicii facturate sunt publicate în lista de taxe disponibile la adresa https://www.certdigital.ro. Prețurile sunt stabilite în funcție de politica internă a prețurilor.
Serviciile oferite de CERTDIGITAL sunt stabilite după cum urmează:

- ***Servicii de certificare individuală*** - prețul este stabilit pentru fiecare serviciu în parte, de exemplu pentru un certificat individual vândut sau un număr mai mic de certificate,
- pachete de servicii de certificare - prețul este stabilit pentru pachetele de servicii prestate unei singure entități,
- ***Servicii de abonament*** - prețul este stabilit pentru serviciile prestate lunar; Valoarea sumelor plătite depinde de tipul și numărul de servicii accesate și este utilizată în principal pentru servicii de verificare a timpului și de verificare a statusului certificatului prin intermediul protocoalelor OCSP,
- ***Servicii indirecte*** - prețul este stabilit pentru fiecare serviciu oferit clienților săi de către un partener CERTDIGITAL a cărui activitate se bazează pe infrastructura CERTDIGITAL; De exemplu, dacă o autoritate de certificare comercială este certificată de CERTDIGITAL, atunci CERTDIGITAL va percepe o taxă pentru fiecare certificat eliberat de respectiva autoritate de certificare.

Plățile se vor efectua în numerar, prin ordin de plată sau prin carduri bancare în conformitate cu prevederile legale în vigoare.

9.1.1 Taxele de emitere și reînnoire a certificatului

Prețurile sunt stabilite în funcție de politica internă a prețurilor.

9.1.2 Taxele de acces la certificat

Serviciu gratuit.

9.1.3 Cheltuieli de revocare sau de acces la informații privind statutul

Prețurile sunt stabilite în funcție de politica internă a prețurilor.

9.1.4 Taxe pentru alte servicii

Prețurile sunt stabilite în funcție de politica internă a prețurilor.

9.1.5 Politica de rambursare

Politica de rambursare este definită în cadrul politicii interne de prețuri.

9.2 Responsabilitatea financiară

9.2.1 Acoperire de asigurare

Nu se aplică.

9.2.2 Alte active

Nu se aplică.

9.2.3 Asigurarea sau acoperirea garanției pentru entitățile finale

Nu se aplică

9.3 Confidențialitatea informațiilor despre afaceri

9.3.1 Domeniul de aplicare a informațiilor confidențiale

Toate informațiile furnizate de CERTDIGITAL au fost colectate, stocate și prelucrate în conformitate cu legile aplicabile, în special cu legislația română privind protecția datelor cu caracter personal (Legea 677/2001) și Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice. Relațiile dintre un subiect, un abonat, o parte învestită și CERTDIGITAL se bazează pe încredere.
În prestarea serviciilor de încredere CERTDIGITAL prelucrează date cu caracter personal ale Subiectului/Beneficiarului în conformitate cu cerințele Regulamentului (UE) nr. 910/2014 și cu respectarea dispozițiile de drept intern, a Regulamentului nr. 679/2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și al altor dispoziții de drept al Uniunii referitoare la protecția datelor. Scopul prelucrării datelor cu caracter personal este acela de a presta servicii de certificare.
O terță parte poate avea acces numai la informațiile publice disponibile în certificate. Alte date furnizate în cererile trimise către CERTDIGITAL nu vor fi divulgate de bunăvoie unei terțe părți în niciun caz (cu excepția situațiilor juridice).
O parte va fi exonerată de răspunderea de divulgare a datelor confidențiale dacă:
a) informația a fost cunoscută părții contractante înainte de a fi primit de către cealaltă parte contractantă;
sau
b) informația a fost dezvăluită după obținerea consimțământului scris al celeilalte părți;
sau
c) Partidul a fost obligat din punct de vedere legal să dezvăluie informațiile.

Dezvăluirea informațiilor părților implicate în îndeplinirea obligațiilor lor se va face în mod confidențial și va acoperi doar informațiile necesare îndeplinirii obligațiilor.

Tipuri de informații considerate confidențiale și private

CERTDIGITAL, angajații săi și alte entități care desfășoară activități de certificare se angajează să păstreze secretul informațiilor atât în timpul cât și după angajare. Sunt considerate informații private și confidențiale:

- Informațiile furnizate de către Subiecți / Abonați în plus față de informațiile care vor fi trimise pentru a efectua serviciile de certificare; În acele situații care dezvăluie informațiile primite necesită consimțământul prealabil scris al proprietarului de informații sau în alte condiții conform legii.
- Informațiile furnizate de / către subiecți / abonați (de exemplu, conținutul contractelor încheiate cu subiecți / abonați sau părți invocate, conturi bancare, cereri de înregistrare, emitere, rechetare, revocarea certificatelor - cu excepția informațiilor incluse în certificate sau din depozit , În conformitate cu prezentul CPS); O parte din informațiile

menționate mai sus pot fi dezvăluite numai cu aprobarea și în scopul specificat de proprietarul informațiilor (de exemplu, Subiectul),

- Înregistrări ale tranzacțiilor de sistem (toate tipurile de tranzacții, precum și date pentru controlul tranzacțiilor, așa-numitele jurnale de tranzacții de sistem)
- Înregistrarea evenimentelor (jurnalelor) legate de serviciile de certificare, păstrate de CERTDIGITAL,
- Rezultatele auditurilor interne și externe, dacă acestea reprezintă o amenințare pentru securitatea CERTDIGITAL,
- Planurile de urgență,
- Informații despre măsurile luate pentru a proteja dispozitivele hardware și aplicațiile software, informații despre gestionarea serviciilor de certificare și regulile planificate de înregistrare

Obligația de confidențialitate nu se aplică CERTDIGITAL pentru furnizarea de servicii de certificare unei terțe părți. Persoanele responsabile de păstrarea confidențialității informațiilor și care respectă regulile privind gestionarea informațiilor poartă răspunderea conform legilor în vigoare.

Dezvăluirea motivului de revocare a certificatului
Dacă un certificat a fost revocat la cererea unei părți autorizate, alta decât subiectul sau subiectul, informațiile despre revocare și motivele aferente sunt comunicate ambelor părți.

Dezvăluirea informațiilor fără caracter public către funcționarii responsabili cu aplicarea legii
Informațiile confidențiale pot fi divulgate oficialilor de aplicare a legii numai după îndeplinirea tuturor formalităților cerute de legislația română în vigoare.

9.3.2 Informații care nu intră sub incidența informațiilor confidențiale

Toate informațiile necesare pentru buna funcționare a serviciilor de certificare nu sunt considerate confidențiale sau private. Aceasta se referă în special la informațiile incluse într-un certificat de către autoritatea de certificare emitentă, în conformitate cu specificațiile din capitolul 7.
Un subiect / abonat care solicită obținerea unui certificat este conștient de tipul de informație inclus în certificat și este de acord cu publicarea acestuia.
O parte din informațiile furnizate de către sau către Subiect / Abonat pot fi puse la dispoziția altor entități numai cu acordul scris al Subiectului / Abonatului și în scopul declarat în contractul încheiat cu Subiectul / Abonatul.

9.3.3 Responsabilitatea de a proteja informațiile confidențiale

CERTDIGITAL, angajații săi și de asemenea entitățile care desfășoară activități de certificare se angajează să păstreze secretul atât în timpul cât și după angajare.

9.4 Confidențialitatea informațiilor personale

CERTDIGITAL este înregistrată în registrul de protecție a datelor din România sub numărul de înregistrare ***19791***.

Toate informațiile CERTDIGITAL au fost colectate, stocate și prelucrate în conformitate cu legile aplicabile, în special cu legislația română privind protecția datelor cu caracter personal (Legea 677/2001) și Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice.
Măsurile de securitate cerute de Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal sunt implementate pentru a garanta că:

- Sunt luate măsuri tehnice și organizatorice adecvate împotriva prelucrării neautorizate sau ilegale a datelor cu caracter personal și împotriva pierderii accidentale sau a distrugerii sau deteriorării datelor cu caracter personal.
- Accesul la serviciile CERTDIGITAL se referă numai la prelucrarea acelor date de identificare care sunt adecvate, relevante și nu excesive pentru a permite accesul la serviciul respectiv.
- Protecția confidențialității și integritatea datelor de înregistrare: atunci când sunt schimbate cu abonatul / subiectul, atunci când sunt schimbate între componentele sistemului CERTDIGITAL, precum și atunci când sunt stocate.

9.5 Drepturi de proprietate intelectuală

Toate mărcile comerciale, brevetele, marcajele, licențele, imaginile grafice etc. utilizate de CERTDIGITAL sunt și vor fi proprietatea intelectuală a proprietarilor lor legali. CERTDIGITAL se angajează să menționeze acest lucru conform cererilor impuse de proprietari.
Toate mărcile comerciale, brevetele, marcajele, licențele, imaginile grafice etc. aparținând CERTDIGITAL sunt și rămân proprietatea sa, indiferent dacă sunt împreună cu brevete, modele de utilitate, drepturi de autor sau nu și nu pot fi reproduse sau livrate unui terț fără Consimțământul scris prealabil al CERTDIGITAL.

9.6 Reprezentări și garanții

9.6.1 Reprezentări și garanții ale CA

CERTDIGITAL emite certificate compatibile X509 v3.
CERTDIGITAL garantează că toate cerințele stabilite în CPS aplicabile (și indicate în certificat în conformitate cu capitolul 7) sunt respectate. De asemenea, aceasta își asumă responsabilitatea de a asigura conformitatea și de a furniza aceste servicii în conformitate cu CPS.
Singura garanție oferită de CERTDIGITAL este că procedurile sale sunt implementate în conformitate cu CPS și procedurile de verificare existente și că toate Certificate emise cu un identificator de obiect (OID) au fost emise în conformitate cu procedurile relevante, iar CPS as Aplicabile în momentul emiterii.

9.6.2 Reprezentări și garanții ale RA

RA are obligația să respecte cu scrupulozitate CPS și procedurile interne relevante ale CERTDIGITAL.

9.6.3 Reprezentări și garanții ale abonaților

Subiectul acceptă Termenii și condițiile relevante pentru serviciul furnizat de CERTDIGITAL.
Subiectul este de acord cu CPS și cu responsabilitățile, obligațiile și obligațiile sale relevante, astfel cum se prevede în secțiunile relevante ale CPS.
În special, Subiectul este răspunzător față de Părțile învinuite pentru orice utilizare a QSCD, inclusiv cheile sau certificatele, cu excepția cazului în care poate dovedi că a luat măsurile necesare pentru O revocare în timp util a Certificatului (lor), atunci când este necesar.

9.6.4 Reprezentări și garanții ale partidelor invocate

Exemplele de obligații și responsabilități ale părților încrezătoare includ (fără limitare):

- Performanța cu succes a operațiunilor cu chei publice ca o condiție prealabilă pentru utilizarea unui certificat CERTDIGITAL
- Validarea unui certificat CERTDIGITAL prin utilizarea serviciilor de validare (CRL) sau a certificatelor furnizate de CERTDIGITAL
- Terminarea imediată a oricărei dependențe de un certificat CERTDIGITAL dacă a fost revocată sau expirată.

9.6.5 Reprezentări și garanții ale altor participanți

Nu se aplică.

9.7 Renunțarea la garanții

Cu excepția cazului în care se prevede altfel în CPS și în legislația aplicabilă, CERTDIGITAL renunță la toate garanțiile și obligațiile de orice tip, inclusiv orice garanție de vandabilitate, orice garanție de adecvare pentru un anumit scop și orice garanție de exactitate a informațiilor furnizate A provenit dintr-o sursă autorizată) și, în plus, își declină orice răspundere pentru neglijență și lipsă de atenție rezonabilă din partea Subiectului, a abonaților și a părților invocate.

9.8 Limitarea răspunderii

În limita stabilită de legea română, CERTDIGITAL nu va fi răspunzător în nici un caz (cu excepția fraudei sau abaterilor intenționate) pentru:

- Orice pierdere a profitului;
- Orice pierdere de date;
- Orice daune indirecte, consecvente sau punitive rezultate din sau în legătură cu utilizarea, livrarea, licența și performanța sau neexecutarea certificatelor sau semnăturilor digitale;
- Orice alte daune.

9.9 Despăgubirile

CERTDIGITAL nu își asumă nicio responsabilitate financiară pentru certificatele, LRD-urile utilizate în mod necorespunzător.

9.10 Termen și reziliere

9.10.1 Termene

Acest CPS și orice modificări ale acestuia vor intra în vigoare după publicare în Depozit și în conformitate cu secțiunea 9.12.2 și vor rămâne în vigoare perpetual până când vor fi reziliate în conformitate cu prezenta secțiune 9.10.

9.10.2 Rezilierea

CPS rămâne în vigoare până la înlocuirea cu o nouă versiune.

9.10.3 Efectul terminării și al supraviețuirii

Condițiile și efectul care rezultă din terminarea acestui CPS vor fi comunicate prin intermediul site-ului web CERTDIGITAL la terminarea acestuia. Această comunicare va evidenția dispozițiile care pot supraviețui rezilierii acestei CPC și vor rămâne în vigoare. Responsabilitățile de protejare a informațiilor confidențiale și a informațiilor personale vor

supraviețui încetării, iar termenii și condițiile pentru toate certificatele existente vor rămâne valabile pentru restul perioadelor de valabilitate ale acestor certificate.

9.11 Observații individuale și comunicări cu participanții

Toate notificările și alte comunicări care pot fi sau trebuie să fie furnizate, comunicate sau trimise conform CPS vor fi în scris și vor fi trimise, cu excepția cazului în care se prevede în mod explicit în CPS, fie prin :

- e-mail sau scrisoare recomandată cu chitanța de returnare sau plata anticipată,
- un serviciu de curierat "rapid" sau de curierat recunoscut la nivel internațional,
- livrare manuala,
- transferul prin fax sau reproducere a documentului, considerat recepționat la livrarea reală sau la finalizarea procesului de trimitere/recepție,
- in format electronic, semnată cu o semnătură electronică calificată și adresată CERTDIGITAL folosind datele de contact prevăzute în capitolul 1.5.1 din prezentul document

9.12 Modificări

9.12.1 Procedura de modificare

CERTDIGITAL este responsabil prin intermediul Organului său de gestionare a politicilor și procedurilor pentru aprobarea și modificarea prezentului CPS.

Singurele modificări pe care CMPP le poate face acestor specificații CPS fără notificare sunt modificări minore care nu afectează nivelul de asigurare al acestei CPS, de exemplu, corecții editoriale sau tipografice sau modificări ale detaliilor de contact.

Erori, actualizări sau modificări sugerate ale acestui document vor fi comunicate după cum este identificat în prezentul CPS, secțiunea 1.5.4. O astfel de comunicare va include o descriere a schimbării, o justificare a schimbării și informații de contact ale persoanei care solicită modificarea.

CMPP acceptă, modifică sau respinge modificarea propusă după finalizarea unei etape de revizuire.

9.12.2 Mecanismul de notificare și perioada

Toate modificările aduse prezentei CPS examinate de CMPP vor fi diseminate părților interesate pentru o perioadă de minimum 10 zile. Data emiterii și data efectivă sunt indicate pe

pagina de titlu a prezentului CPS. Data intrării în vigoare va fi de cel puțin 2 zile de la data publicării.

9.12.3 Circumstanțele în care OID trebuie schimbat

Nu se aplică

9.13 Dispoziții privind soluționarea litigiilor

Toate disputele asociate cu prezentul CPS vor fi soluționate în conformitate cu legile din România.

9.14 Legea aplicabilă

Legile române vor reglementa executarea, construirea, interpretarea și validitatea prezentului CPS (fără a aduce atingere oricărei prevederi privind conflictul de legi care ar determina aplicarea altor legi).

9.15 Respectarea legislației în vigoare

Prezenta CPS și furnizarea serviciilor CERTDIGITAL respectă legile românești relevante și aplicabile și Regulamentul UE 910/2014.

9.16 Dispoziții diverse

Nu se aplică.