

Declarația practicilor de certificare a CertDigital QUALIFIED CA G3

EMISA DE:			
DEPARTAMENT	**NUME**	**SEMNATURA**	**DATA**
MANGEMENTUL POLITICILOR SI PROCEDURILOR	Ofițer de Securitate IT		07/06/2017

APROBATA DE:			
DEPARTAMENT	**NUME**	**SEMNATURA**	**DATA**
MANGEMENTUL POLITICILOR SI PROCEDURILOR	Director Tehnic		07/06/2017

ISTORICUL MODIFICARILOR:			
VERSIUNE	**AUTOR**	**DETALII MODIFICARI**	**DATA:**
1.0	Ofițer de Securitate IT	Publicare primei versiuni a documentului	07/06/2017
1.1	Director Tehnic	Revizuire anuala	31/01/2019
1.2	Director Tehnic	Revizie document	31/01/2021

Cuprins

2.1. Depozit....17
2.2. Publicarea informațiilor de certificare....18
2.3. Timpul sau frecvența publicării....19
2.4. Controalele de acces în depozite....19
3. Identificarea și autentificarea....20
3.1. Denumirea....20
3.1.1. Tipuri de nume....20
3.2.2. Autentificarea identității organizației....23
3.2.3. Autentificarea identității individuale....24
3.2.4. Informațiile neverificate ale abonaților....24
3.2.5. Validarea autorității....25
3.2.6. Criterii de interoperare....25
3.3.1. Identificarea și autentificarea pentru re-cheia de rutină....25
3.3.2. Identificarea și autentificarea pentru re-cheie după revocare....25
3.4. Identificarea și autentificarea cererii de revocare....25
4. Cerințe operaționale ale ciclului de viață al certificatului....27
4.1. Cererea de certificat....27
4.1.1. Cine poate depune o cerere de certificat....27
4.1.2. Procesul de înscriere și responsabilitățile....28
4.2. Prelucrarea cererilor de certificate....29
4.2.1. Efectuarea funcțiilor de identificare și autentificare....30
4.2.2. Aprobarea sau respingerea cererilor de certificate....31
4.2.3. Timpul de procesare a cererilor de certificate....31
4.3. Eliberarea certificatului....31
4.3.1. Acțiunile CA în cursul emiterii certificatului....31
4.3.2. Notificarea către abonat de către CA a eliberării certificatului....31
4.4. Acceptarea certificatelor....32
4.4.2. Publicarea certificatului de către CA....33
4.4.3. Notificarea eliberării certificatului de către CA altor entități....33
4.5. Utilizarea perechii de chei și a certificatului....33

4.5.1. Cheia privată a abonatului și utilizarea certificatului 33
4.5.2. Utilizarea cheii publice a părții publice și utilizarea certificatului 34
4.6. Reînnoirea certificatului 35
4.7. Certificate Re - key 35
4.7.1. Circumstanța pentru Re-key certificat 35
4.7.2. Cine poate solicita certificarea unei noi chei publice 36
4.7.3. Prelucrarea cererilor de re-cheiere a certificatului 36
4.7.4. Notificarea emiterii noului certificat către abonat 36
4.7.5. Desfășurarea acceptării unui certificat reîncadrat 36
4.7.6. Publicarea certificatului reîncadrat de către CA 36
4.7.7. Notificarea eliberării certificatului de către CA altor entități 37
4.8. Modificarea certificatului 37
4.9. Revocarea și suspendarea certificatului 37
4.9.1. Circumstanțele de revocare 37
4.9.2. Cine poate cere revocarea 38
4.9.3. Procedura pentru cererea de revocare 38
4.9.4. Perioada de grație a cererii de revocare 39
4.9.5. Timpul în care CA trebuie să proceseze cererea de revocare 39
4.9.6. Cerințele de verificare a revocării pentru părțile implicate 39
4.9.7. Frecvența emiterii CRL 40
4.9.8. Latența maximă pentru CRL-uri 40
4.9.9. Disponibilitatea on-line a revocării / verificării stării 40
4.9.10. Cerințe de verificare on-line de revocare 40
4.9.11. Alte forme de anunțuri de revocare disponibile 40
4.9.12. Cerințe speciale privind compromisul cheie 40
4.9.13. Circumstanțele pentru suspensie 41
4.9.14. Cine poate solicita suspendarea 41
4.9.15. Procedura pentru cererea de suspendare 41
4.9.16. Limitele perioadei de suspendare 41
4.10. Servicii de stare a certificatului 41
4.10.1. Caracteristicile operaționale 41
4.10.2. Disponibilitatea serviciului 41
4.10.3. Caracteristici opționale 42
4.11. Încheierea abonamentului 42

4.12. Key escrow și recuperare cheie....42
5. Facilitatea, managementul și controlul operațional....42
5.1. Controale fizice....43
5.1.1. Localizarea și construcția amplasamentului....43
5.1.2. Accesul fizic....44
5.1.3. Energie și aer condiționat....45
5.1.4. Expunerea la apă....45
5.1.5. Prevenirea și protejarea incendiilor....45
5.1.6. Mediile de stocare....45
5.1.7. Eliminarea deșeurilor....45
5.1.8. Backup de rezervă....46
5.2. Controale procedurale....46
5.2.1. Roluri de încredere....46
5.2.2. Numărul de persoane necesare pentru fiecare sarcină....47
5.2.3. Identificarea și autentificarea pentru fiecare rol....48
5.2.4. Roluri care necesită separarea sarcinilor....48
5.3. Controlul personalului....48
5.3.1. Cerințe de calificare, experiență și cerințe de verificare....49
5.3.2. Proceduri de verificare de fond....49
5.3.3. Cerințe de formare....49
5.3.4. Frecvența și cerințele de recalificare....50
5.3.5. Frecvența și secvența de rotație a lucrării....50
5.3.6. Sancțiuni pentru acțiuni neautorizate....50
5.3.7. Cerințele contractorului independent....50
5.3.8. Documentația furnizată personalului....50
5.4. Procedurile de înregistrare a auditului....51
5.4.1. Tipuri de evenimente înregistrate....51
5.4.2. Frecvența procesării jurnalului....53
5.4.3. Perioada de păstrare pentru jurnalul de audit....53
5.4.4. Protecția jurnalului de audit....54
5.4.5. Proceduri de salvare a jurnalelor de audit....54
5.4.6. Auditul sistemului de colectare (intern/extern)....54
5.4.7. Notificarea subiectului care provoacă evenimente....55
5.4.8. Evaluări de vulnerabilitate....55

5.5. Arhivarea înregistrărilor 55
5.5.1. Tipuri de date arhivate 55
5.5.2. Perioada de păstrare pentru arhivă 56
5.5.3. Protecția arhivei 56
5.5.4. Proceduri de salvare a arhivelor 56
5.5.5. Cerințe pentru marcarea temporală a înregistrărilor 56
5.5.6. Arhiva sistemului de colectare (intern sau extern) 57
5.5.7. Proceduri de obținere și verificare a informațiilor de arhivă 57
5.6. Schimbarea cheii 57
5.7. Recuperarea după compromitere și dezastre 57
5.7.1. Proceduri de tratare a incidentelor și a compromisurilor 57
5.7.2. Resursele de calcul, software-ul și/sau datele sunt corupte 58
5.7.3. Proceduri de compromis ale cheii private a entității 60
5.7.4. Capacitățile de continuitate a activității după un dezastru 60
5.8. Terminarea CA sau RA 61
6. Controalele tehnice de securitate 63
6.1. Generarea și instalarea perechilor de chei 63
6.1.2. Livrarea cheii private către abonat 65
6.1.3. Livrarea cheii publice către emitentul de certificate 66
6.1.4. Furnizarea de chei publice CA către părțile implicate 66
6.1.5. Dimensiunile cheilor 66
6.1.6. Generarea parametrilor cheilor publice și verificarea calității 67
6.1.7. Obiective de utilizare cheie (conform câmpului de utilizare al cheii X.509 v3) 67
6.2. Protecția cheii private și controlul tehnic al modulelor criptografice 68
6.2.1. Standardele și comenzile modulului criptografic 69
6.2.2. Controlul multi-persoană al cheii private 69
6.2.3. Cheie privată escrow 70
6.2.4. Backup-ul cheii private 71
6.2.5. Arhivarea cheii private 71
6.2.6. Transferul cheii private în sau din modulul criptografic 71
6.2.7. Depozitarea cheii private pe modulul criptografic 72
6.2.8. Metoda de activare a cheii private 72
6.2.9. Metoda de dezactivare a cheii private 73
6.2.10. Metoda de distrugere a cheii private 73

6.2.11. Evaluarea modulului criptografic 73
6.3. Alte aspecte ale gestionării perechii de chei 74
6.3.1. Arhivarea cheilor publice 74
6.3.2. Perioadele de funcționare a certificatului și perioadele de utilizare a perechilor de chei 74
6.4. Datele de activare 75
6.4.1. Generarea și instalarea de date de activare 75
6.4.2. Protecția datelor de activare 76
6.4.3. Alte aspecte ale datelor de activare 76
6.5. Controalele de securitate ale computerului 76
6.5.1. Cerințe tehnice specifice privind securitatea calculatoarelor 76
6.5.2. Evaluarea securității calculatorului 78
6.6. Controalele de securitate ale ciclului de viață 78
6.6.1. Controlul dezvoltării sistemului 78
6.6.2. Controalele managementui securității 78
6.6.3. Controalele de securitate ale ciclului de viață 79
6.7. Controalele de securitate a rețelei 79
6.8. Marcare temporară (Time-stamping) 81
7. Certificatul, CRL și profilul OCSP 81
7.1. Profilul certificatului 81
7.1.1. Numărul (numerele) versiunii 83
7.1.2. Extensiile certificatelor 83
7.1.3. Identificatori de obiect al algoritmului 87
7.1.4. Formulare de nume 88
7.1.5. Constrângeri de nume 88
7.1.6. Identificatorul obiectului politicii certificatului 88
7.1.7. Utilizarea politicii de constrângerii a extensiei 89
7.1.8. Sintaxa și semantica calificărilor de politică 89
7.1.9. Semantica de procesare a Politicii extinderii critice a certificatului 89
7.2. Profilul CRL 89
7.2.1. Numărul (numerele) versiunii 90
7.2.2. CRL și extensii de intrare CRL 90
7.3. Profil OCSP 90
7.3.1. Numărul (versiunile) versiunii 91
7.3.2. Extensii OCSP 91

8. Auditul de conformitate și alte evaluări 91
8.1. Frecvența sau circumstanțele de evaluare 92
8.2. Identitatea / calificările evaluatorului 92
8.3. Relația evaluatorului cu entitatea evaluată 92
8.4. Subiectele acoperite de evaluare 92
8.5. Acțiuni întreprinse ca urmare a deficienței 92
8.6. Comunicarea rezultatelor 93
9. Alte probleme de afaceri și juridice 93
9.1. Taxe 93
9.1.1. Taxele de emitere sau reînnoire a certificatului 93
9.1.2. Taxele de acces la certificat 93
9.1.3. Cheltuieli de revocare sau de acces la informații privind statutul 94
9.1.4. Taxe pentru alte servicii 94
9.1.5. Rambursarea taxelor 94
9.2. Responsabilitatea financiară 94
9.2.1. Acoperire de asigurare 94
9.2.2. Alte active 94
9.2.3. Asigurarea sau acoperirea garanției pentru entitățile finale 94
9.3. Confidențialitatea informațiilor despre afaceri 94
9.3.1. Domeniul de aplicare a informațiilor confidențiale 94
9.3.2. Informații care nu intră sub incidența informațiilor confidențiale 96
9.3.3. Responsabilitatea de a proteja informațiile confidențiale 97
9.4. Confidențialitatea informațiilor personale 97
9.5. Drepturi de proprietate intelectuală 97
9.6. Reprezentări și garanții 98
9.6.1. Reprezentări și garanții ale CA 98
9.6.2. Reprezentări și garanții ale RA 98
9.6.3. Reprezentări și garanții ale abonaților 98
9.6.4. Reprezentări și garanții ale părților asociate 98
9.6.5. Reprezentări și garanții ale altor participanți 99
9.7. Renunțarea la garanții 99
9.8. Limitarea răspunderii 99
9.9. Despăgubirile 99
9.10.1. Termen 99

9.10.2. Terminare 100
9.10.3. Efectul terminării și al supraviețuirii 100
9.11. Observații individuale și comunicări cu participanții 100
9.12. Modificări 100
9.12.1. Procedura de modificare 100
9.12.2. Mecanismul de notificare și perioada 101
9.12.3. Circumstanțele în care OID trebuie schimbat 101
9.13. Proceduri de soluționare a litigiilor 101
9.14. Legea aplicabilă 101
9.15. Respectarea legislației în vigoare 101
9.16. Dispoziții diverse 101
9.17. Alte prevederi 101

1. Introducere

Procedura de certificare pentru CertDigital QUALIFIED CA G3 (denumită în continuare CPS Qualified CA sau CPS) detaliază politica de certificare și practicile pe care CertDigital le aplică pentru emiterea de certificate calificate pentru semnătură electronică și certificate calificate pentru sigilii electronice.

Structura și conținutul CPS Qualified CA sunt în conformitate cu 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.Prezentare generală

CertDigital, abonații, subiecții și partenerii depind de **CPS Qualified CA** pentru emiterea de certificate calificate pentru semnături electronice și certificate calificate pentru sigilii electronice. De asemenea, acest document descrie regulile generale pentru furnizarea de livrare de servicii de certificare, cum ar fi înregistrarea subiectului, certificarea cheii publice, recheierea și revocarea certificatelor.

1.2.Numele și identitarea documentului

Titlul acestui document este **Declaratia practicilor de certificare pentru CertDigital QUALIFIED CA G3**, denumit în continuare **CPS Qualified CA** sau **CPS**.

Formularul electronic al acestui document este disponibil în depozit la adresa http://www.certdigital.ro/repository.

1.3.Participanții la PKI

CPS Qualified CA reglementează cele mai importante relații dintre entitățile care aparțin CertDigital, echipele de consultanță (inclusiv auditorii) și clienții (utilizatorii serviciilor oferite) din acest domeniu:

- CertDigital QUALIFIED CA G3
- Autoritatea de Înregistrare,
- Depozitul,
- Protocolul privind starea certificatului online (Autoritatea OCSP),
- Subiecții,

- 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 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 QUALIFIED CA G3 este o Autoritate de Certificare Subordonată pentru domeniul CertDigital. Este subordonată CertDigital ROOT CA G3. CertDigital QUALIFIED CA G3 este identificat de următoarele OID: 1.3.6.1.4.1. 47898.3.1.3

Înainte de începerea activității, CertDigital QUALIFIED CA G3 trimite o cerere către Autoritatea de Certificare Primară, CertDigital ROOT CA G3 pentru emiterea certificatului de înregistrare și a cheii publice.

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 aplicații) atât abonatul/subiectul, cât și datele specificate în cerere. De asemenea, Autoritatea de Înregistrare poate depune cereri către Autoritatea de Certificare corespunzătoare pentru a anula o cerere sau pentru a retrage un certificat.

Autoritatea de Înregistrare este administrată de CertDigital sau de o terță parte delegată, dacă legislația permite acest lucru.

1.3.3. Abonați

Abonat

Abonații sunt persoane juridice sau fizice care solicită CertDigital emiterea unui certificat și cu care semnează contractul de Abonat.

Abonații pot fi:

- Persoane fizice - în acest caz, Abonatul este obiectul certificatului emis de CertDigital,
- Persoane juridice care încheie un contract cu CertDigital pentru emiterea de certificate unor subiecți (de exemplu, lucrători independenți, angajați),
- Persoane juridice care încheie un contract cu CertDigital pentru emiterea de certificate de sigiliu electronic.

Abonații pot solicita emiterea, revocarea sau recheierea certificatelor entității finale pentru subiecții aflați în grija lor. Un abonat este, de asemenea, responsabil pentru notificarea imediată a CertDigital asupra compromisului privind cheia privată (suspiciunea de compromis);

Subiect

Subiectul este entitatea (persoana juridică sau fizică) căreia i se eliberează un certificat și care este identificată într-un certificat ca titular al cheii private asociate cheii publice din certificat.

Subiectul poate fi:

- Abonatul, în cazul în care solicită certificatul pentru el însuși,
- Persoana fizica pentru care Abonatul solicita certificatul, avand un acord obligatoriu din punct de vedere juridic sau acționând ca angajator
- Persoana juridica pentru care Abonatul solicita certificatul de sigiliu electronic.

Un subiect este de asemenea responsabil pentru:

- Notificarea imediată a CertDigital asupra compromiterii cheii private;
- Transmiterea cererilor de reînnoire a cheilor și/sau certificatelor către CertDigital în timp util;
- Asigurarea faptului că, confidențialitatea cheii private este protejată într-o manieră compatibilă cu acest document;
- Asigurarea faptului că accesul la utilizarea cheii private este controlat într-o manieră compatibilă cu acest document.

1.3.4. Partenerii

Partenerul care utilizeaza serviciile CertDigital poate fi orice entitate care ia decizii bazate pe corectitudinea legăturii dintre identitatea unui subiect și cheia publică.

Partenerul este responsabilă pentru modul în care verifică starea actuală a certificatului unui subiect. O astfel de decizie trebuie luată de fiecare dată când partenerul este dispus să utilizeze un certificat pentru a verifica o semnătură electronică, pentru a verifica identitatea sursei sau a autorului unui mesaj sau pentru a crea un canal de comunicare securizat cu subiectul certificatului. Partenerul va utiliza informațiile dintr-un certificat (de exemplu, identificatori și calificări ale politicii de certificare) pentru a decide dacă un certificat a fost utilizat în conformitate cu scopul declarat.

1.3.5. Alți participanți

Furnizori de servicii CertDigital: furnizori externi care susțin activitățile CertDigital în baza unui acord contractual semnat.

Notarii publici: pot efectua identificarea și garantarea identității reale a subiecților.

Furnizori de dispozitive electronice de creare a semnăturilor calificate: furnizorii externi care susțin activitățile CertDigital în baza unui acord contractual semnat asigură furnizarea dispozitivelor fizice criptografice utilizate de către subiecți.

1.4.Utilizarea certificatului

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

- unul care definește aplicabilitatea certificatului (de exemplu, semnătura electronică, confidențialitatea)
- un altul care implică o listă sau o descriere a aplicațiilor permise și interzise.

Partenerul este responsabilă pentru stabilirea nivelului de credibilitate necesar pentru ca un certificat să poată fi utilizat într-un anumit scop. Partenerul va decide, luând în considerare factorii de risc semnificativi, ce tip de certificat emis de CertDigital îndeplinește cererile formulate. Subiecții cunosc solicitările partenerilor (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

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 parteneri pe baza naturii și scopului (inclusiv utilizarea cheii) certificatului, inclusiv orice limitare aplicabilă așa cum este ea înscrisă în certificat.

Este responsabilitatea Subiectului de a utiliza certificatele în conformitate cu acest CPS. Este responsabilitatea Subiectului sau a Abonatului de a utiliza aplicații software care interpretează corect, afișează și utilizează informațiile și restricțiile codificate în certificate, cum ar fi, dar nu se limitează la utilizarea cheii, răspunderea limitată pe tranzacție etc.

Este responsabilitatea abonatului, a subiectului și a partenerului să decidă în ce scop se consideră că certificatele sunt de încredere. Partenerul trebuie să ia întotdeauna în considerare nivelul de asigurare și alte informații din CPS înainte de a decide cu privire la aplicabilitatea certificatului.

1.4.2. Utilizări interzise ale certificatelor

Orice utilizare a unui alt certificat decât utilizarea permisă explicit în CPS este interzisă.

1.5. Administrarea politicilor

1.5.1. Organizația care administrează documentul

Prezentul document este administrat de Compartimenul Managementul Politicilor și Procedurilor CertDigital (CMPP). CMPP include membrii din conducere, precum și personalul responsabil cu gestionarea operațională a mediului CertDigital TSP PKI.

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)-214.767

Fax	(+40253)-213.409
E-mail	office@certdigital.ro
Web	www.certdigital.ro

1.5.2. Persoana de contact

Nume	Compartimentul Managementul Politicilor și Procedurilor (CMPP)
Telefon	(+40253)-214.767
Fax	(+40253)-213.409
E-mail	office@certdigital.ro
Web	www.certdigital.ro

1.5.3. Persoana care determină adecvarea CPS pentru politică

Nume	Organismul de gestionare a politicilor și procedurilor
Telefon	(+40253)-214.767
Fax	(+40253)-213.409
E-mail	office@certdigital.ro
Web	www.certdigital.ro

1.5.4. Procedurile de aprobare a CPS

Compartimentul Managementul 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 modificate ale CPS trebuie să facă o declarație adecvată în termen de 15 zile de la data noii versiuni aprobate a CPS. Aceasta va conduce la rezilierea contractului privind serviciile de certificare furnizate și la revocarea certificatului eliberat.

1.6.Definiții și acronime

Auditor - persoană care evaluează conformitatea cu cerințele specificate în documentele de cerințe date

Autentificare - proces electronic care permite confirmarea electronică a unei persoane fizice sau juridice sau originea și integritatea datelor electronice

Certificat - cheia publică a unui utilizator, împreună cu unele informații suplimentare, redate nereligibile prin criptare cu cheia privată emisă de o autoritate de certificare

Lista de revocare a certificatelor (CRL) - o listă semnată indicând un set de certificate care nu mai sunt considerate valabile de către emitentul certificatului

Autoritatea de certificare - autoritate de încredere de către unul sau mai mulți utilizatori pentru a crea și a atribui certificate

Lista autorităților de certificare revocate - O listă de revocare cu certificate CA emise autorităților de certificare care nu mai sunt considerate valabile de către emitentul certificatului

Procedura de certificare (CPS) - o declarație de practici pe care o autoritate de certificare o folosește în emiterea, gestionarea, revocarea și reînnoirea sau re-introducerea certificatelor

Cross-certification - un certificat care este utilizat pentru a stabili o relație de încredere între două autorități de certificare

Semnătura electronică - date în format electronic care sunt atașate sau asociate în mod logic cu alte date în format electronic și care sunt utilizate de semnatar pentru a semna

Identificator 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 disponibilă 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.

Infrastructură cheie publică (PKI) - arhitectură, tehnici, practici și proceduri care sprijină în mod colectiv implementarea și funcționarea sistemelor de criptografie bazate pe certificat public; PKI constă în hardware, software, baze de date, resurse de rețea, proceduri de securitate și obligații legale care se conectează împreună, care colaborează pentru a furniza și implementa servicii de certificare, precum și alte servicii asociate infrastructurii (de exemplu, ștampila de timp).

Certificat calificat pentru semnătura electronică - un certificat pentru semnături electronice, eliberat de un furnizor de servicii de încredere calificat și care îndeplinește cerințele stabilite în anexa I la Regulamentul (UE) nr. 910/2014;

Certificat calificat pentru sigiliu electronic - certificat pentru sigiliu electronic eliberat de un furnizor de servicii de încredere calificat și care îndeplinește cerințele stabilite în anexa III la Regulamentul (UE) 910/2014;

Dispozitiv de creare a semnăturilor electronice calificate - se referă la un dispozitiv de creare a semnăturii electronice care îndeplinește cerințele stabilite în anexa II la Regulamentul (UE) nr. 910/2014.

Regulamentul (UE) nr. 910/2014 – Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind serviciile de identificare electronică și servicii

de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93 / CE,

Autoritatea de Înregistrare - entitate responsabilă în principal de identificarea și autentificarea subiecților certificatelor

Root CA - autoritatea de certificare care se află la cel mai înalt nivel din domeniul TSP și care este utilizată pentru a semna CA subordonat

Subiect: entitatea identificată într-un certificat ca titular al cheii private asociată cu cheia publică furnizată în certificat

Autoritate de certificare subordonată CA a cărei certificat este semnat de autoritatea de bază a autorității sau de un alt CA subordonat

Abonat - entitate juridică sau fizică obligată prin acordul cu un furnizor de servicii de încredere tuturor obligațiilor abonatului

Furnizor de servicii de încredere - o entitate fizică sau juridică care oferă unul sau mai multe servicii de încredere fie ca un furnizor de servicii de încredere calificat, fie ca un furnizor de servicii de încredere necalificat;

CA Autoritatea de certificare (Certification Authority)
CPS Procedura de certificare (certification Practice Statement)
CRL Lista certificatelor de revocare (certificate Revocation List)
CARL Lista autorităților de certificare revocate (Certification Authority Revocation List)
DN Nume distincte (Distinguished Name)
NIMB Institutul Național de Metrologie București (National Institute of Metrology Bucharest)
OCSP Protocolul de stare certificat on-line (On-line Certificate Status Protocol)
PKI Infrastructura cheii publice (Public Key Infrastructure)
CMPP Compartimentul managementul politicilor și procedurilor (Policies and Procedures Management Body)
QSCD Dispozitiv de creare a semnăturilor electronice calificate (Qualified Electronic Signature Creation Device)
RA Autoritatea de Înregistrare (Registration Authority)
RSA Algoritmul criptografic asimetric Rivest, Shamir, Adleman (Rivest, Shamir, Adleman asymmetric cryptographic algorithm)
TSP Furnizor de servicii de încredere (Trust Services Provider)
UTC Ora universală coordonată (Coordinated Universal Time)

2. Responsabilități de publicare și de depozit

2.1.Depozit

Depozit este disponibil on-line: http://www.certdigital.ro/repository si contine urmatoarele :

- Declaratia privind parcticile de certificare ale CA operat de CertDigital
- Certificatele Root CA și certificatele de subordonare CA
- Certificate ale subiecților

- Liste de revocare a certificatelor
- Termeni și condiții pentru utilizarea certificatelor digitale
- Șabloane pentru contracte cu subiecți și abonați

Depozitul este gestionat și controlat de CertDigital; Prin urmare, CertDigital se angajează:

- Să efectueze toate eforturile necesare pentru a se asigura că toate certificatele publicate în Depozit aparțin 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,
- Să asigure publicărea și arhivărea CPS, a listelor de aplicații și a dispozitivelor recomandate,
- Să ofere acces la informații despre starea certificatului prin publicarea listelor de revocare a certificatului (CRL), prin intermediul serverelor OCSP sau al solicitărilor HTTP,
- Să asigure accesului permanent la informații în Depozit pentru Autoritățile de Certificare, Autoritatea de Înregistrare, Subiecții și Parteneri,
- Să publice CRL sau alte informații în timp util și în conformitate cu termenele limită menționate în CPS,
- Să asigure accesul sigur și controlat la informațiile din Depozit.

2.2.Publicarea informațiilor de certificare

La emiterea unui certificat digital, certificatul complet și precis este comunicat de CertDigital persoanei pentru care se eliberează certificatul.

Certificatele trebuie să fie disponibile pentru recuperare numai în acele cazuri pentru care a fost obținut consimțământul subiectului, așa cum este descris în documentul Termeni și Condiții.

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.

În caz de indisponibilitate datorata unei catastrofe, defecțiuni ale infrastructurii aflate în afara controlului CertDigital sau din orice alta cauză, CertDigital va depune toate eforturile pentru a restabili disponibilitatea serviciului în termen de 5 zile lucrătoare.

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

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;
- Certificatele subiecților - după obținerea consimțământului, după fiecare eliberare a unui nou certificat;
- Lista de revocare a certificatelor - este creată fie la fiecare 24 de ore, fie când un certificat este revocat;
- Rapoartele de audit efectuate de instituțiile autorizate - atunci când CertDigital le primește;
- Informații suplimentare - după fiecare actualizare

2.4.Controalele de acces în depozite

Toate informațiile publicate de CertDigital în depozit la adresa http://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 partenerii 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 Numele Distinctive - DN - (cunoscute și sub numele de director), create după recomandările X.500 și X.520. În DN, este posibil să se definească atributele DNS (Domain Name Service). 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.

Pentru a asigura o comunicare electronică ușoară cu Subiectul, în certificatele CertDigital se utilizează un nume suplimentar pentru Subiect. Acest nume poate conține, de asemenea, adresa de e-mail a subiectului, în conformitate cu recomandările RFC 822.

3.1.2. Nevoia de Nume este semnificativă

Numele inclus în Numele Distinct al Subiectului este semnificativ atât în limba română, cât și în orice altă limbă care folosește alfabetul latin. Structura Numelui Distinct, aprobată și verificată de către o Autoritate de Înregistrare depinde de tipul Subiectului.

DN constă din câmpuri obligatorii și opționale care respectă recomandările RFC 5280 și X.520.

Câmpurile obligatorii ale DN pentru persoanele fizice sunt următoarele:

- **C** - abreviere internațională pentru numele țării (de ex. RO pentru România) -

international abbreviation for country name (e.g. RO for Romania)
- **SN** - Numele de familie al Subiectului - (Subject's surname)
- **G** - Prenumele Subiectului - (Subject's first name)
- **CN** - Numele subiectului - (Subject's name)
- **SerialNumber** - CA generează un cod personal unic de identificare a subiectului - CA generated unique personal identification code of the Subject

Câmpurile opționale ale DN pentru persoanele fizice sunt următoarele:

- **S** - Județul unde rezidentul are domiciliul, - county / district where the Subject has his/her residence
- **L** - Localitate unde Subiectul are reședința, - Locality where the Subject has his/her residence ct
- **Street** - Adresa domiciliului Subiectului, - Subject residence address,
- **Phone** - Numărul de telefon al subiectului. - Subject's phone number

Câmpuri obligatorii ale DN pentru persoanele fizice asociate unei organizații sunt următoarele:

- **C** – abreviere internațională pentru numele țării (de ex. RO pentru România), - international abbreviation for country name (e.g. RO for Romania),
- **Organization name**, atunci când Abonatul este angajatorul Subiectului sau există un acord legal între aceștia, -
organization name of the Subscriber, when the Subscriber is the employer of the Subject or there is a legally binding agreement between them
- **OrganizationIdentifier** – Un identificator oficial unic al Abonatului ca persoană juridică, - An official unique identifier of the Subscriber as legal entity
- **SN** – Numele de familie al Subiectului - Subject's surname
- **G** – Prenumele Subiectului, - Subject's first name
- **CN** – Numele subiectului, - Subject's name (first name surname)
- **SerialNumber** - CA generează un cod personal unic de identificare a subiectului. - CA generated unique personal identification code of the Subject.

Câmpurile opționale ale DN pentru persoana fizică asociată unei organizații sunt următoarele:

- **S** – Județul în care este înregistrat Abonatul, - county / district where the Subscriber is registered
- **L** – localitatea în care abonatul este înregistrat, - locality where the Subscriber si registered
- **Street** – adresa abonatului, - Subscriber's address
- **T** – titlu, - Title
- **Field Phone**– număr de telefon, - phone number,

Câmpurile obligatorii ale DN pentru persoanele juridice sunt următoarele:

- **C** – abreviere internațională pentru numele țării (de ex. RO pentru România), - international abbreviation for country name (e.g. RO for Romania)
- **name of the organization** - numele organizației,

- **OrganizationIdentifier** – Un identificator oficial unic al Abonatului ca persoană juridică, - An official unique identifier of the Subscriber as legal entity
- **CN** - numele organizației - name of the organisation

Câmpurile opționale ale DN pentru persoanele juridice sunt următoarele:

- **OU** – numele departamentului organizației, - name of the organization's department
- **S** – județul în care este înregistrată organizația, - county/district where the organization is registered
- **L** – localitatea în care este înregistrată organizația, - locality where the organization is registered
- **Phone** - număr de telefon. - phone number

Numele Subiectului este confirmat de un operator al Autorității de Înregistrare și aprobat de o Autoritate de Certificare. CertDigital asigură (în domeniul său) unicitatea DN-urilor.

3.1.3. Anonimitatea sau pseudonimitatea abonaților

Nu se aplică.

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 Profilurile Certificatelor și CRL-urilor (Capitolul 7). Crearea și interpretarea DN se efectuează în conformitate cu recomandările din Capitolul 3.1.2.

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 este necesară generarea certificatului solicitat, 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.

Cererea de prezentare a dovezii privind posesia cheii private nu se aplică dacă, la solicitarea Abonatului sau a Subiectului, perechea de chei este generată de Autoritatea de Certificare sau de

Autoritatea de Înregistrare.

Cheile Private vor fi generate folosind un QSCD. O entitate poate avea un QSCD atunci când generează cheia sau QSCD poate fi furnizată entității de către CertDigital după procesul de generare a cheilor. În cazul din urmă, CertDigital garantează că QSCD și cheia vor merge în siguranță către entitatea respectivă (vezi Capitolul 6.1.2).

3.2.2. Autentificarea identității organizației

Autentificarea identității organizației este realizată pentru a dovedi că persoana juridică există într-adevăr. Atunci când persoana juridică încheie un contract cu CertDigital pentru emiterea de certificate pentru Subiecți (de exemplu, lucrător care desfășoară o activitate independentă, angajat), sunt necesare următoarele documente pentru identificarea Abonatului (persoană juridică) și pentru validarea relației dintre o persoană fizică și o persoană juridică:

- Documente oficiale care demonstrează că persoana juridică acționează ca angajator al persoanei fizice sau că există un acord obligatoriu din punct de vedere juridic între ele.

Atunci când persoanele juridice încheie un contract cu CertDigital pentru emiterea certificatelor pentru sigiliul electronic, sunt necesare următoarele documente pentru identificarea Abonatului (persoană juridică:

- Extras valid din registrul comerțului (sau echivalentul străin pentru societățile străine înregistrate conform legislației străine);
- Mandatul oficial, atunci când persoana fizică care reprezintă persoana juridică nu este administratorul legal al entității.

Toate documentele sunt documente originale sau sunt certificate de notari publici.

Autoritatea de Certificare Emitentă	**Cerinţe** **Operatorii Autorității de Înregistrare compară datele primite ale subiectului / abonatului utilizând una dintre posibilitățile:**
CertDigital QUALIFIED CA G3	Prin participarea personală la Autoritatea de Înregistrare (opțiunea recomandată)
	Printr-o scrisoare care conține copii ale tuturor documentelor originale confirmate de un notar public (opțional)

	Formatul electronic care va conține copii ale tuturor documentelor originale autentificate de un notar public în conformitate cu prevederile Legii electronice notariale nr. 589 / 15.12.2004 (opțional)

Tabelul 1 Cerințe pentru verificarea identității organizației

Procedura descrisă în acest capitol se aplică la fiecare 3 ani pentru a autentifica identitatea organizației.

3.2.3. Autentificarea identității individuale

Documentele de identitate (carte de identitate sau pașaport pentru cetățenii români și pașaport pentru cetățenii străini) sunt necesare pentru identificarea unei persoane fizice:

- Când persoana fizică este Subiectul unui certificat digital emis de CertDigital.
- Atunci când persoana fizică reprezintă o entitate juridică care încheie un acord contractual cu CertDigital.

Toate documentele sunt documente originale sau sunt certificate de notari publici.

Politica de certificare	**Cerințe** **Operatorii autorității de înregistrare compară datele primite ale subiectului / abonatului utilizând una dintre posibilitățile:**
CertDigital QUALIFIED CA G3	Prin participarea personală la Autoritatea de Înregistrare (opțiunea recomandată)
	Printr-o scrisoare care să conțină toate documentele originale confirmate de un notar public (opțional)
	Formatul electronic care va conține copii ale tuturor documentelor originale autentificate de notarul public conform prevederilor legii electronice notariale nr. 589 / 15.12.2004 (opțional)

Tabelul 2 Cerințe pentru verificarea identității individuale

Procedura descrisă în acest capitol se aplică la fiecare 3 ani pentru autentificarea identității individuale.

3.2.4. Informațiile neverificate ale abonaților

Adresa de e-mail a subiectului nu este verificată. Subiectul sau abonatul, după caz, este în întregime responsabil pentru furnizarea de informații actualizate, corecte și corecte în timpul procesului de

înregistrare.

3.2.5. Validarea autorității

CertDigital verifică dacă o persoană fizică are drepturi sau permisiuni specifice, inclusiv permisiunea de a acționa în numele unei persoane juridice pentru a obține un certificat.

3.2.6. Criterii de interoperare

Nu se aplică.

3.3.Identificarea și autentificarea pentru solicitările de re-key

3.3.1. Identificarea și autentificarea pentru re-cheia de rutină

Capitolele 4.7 și 4.8 din prezentul document descriu 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

Următoarele entități pot trimite cereri de revocare a certificatelor:

- Subiectul care deține certificatul privat asociat cheii publice trebuie să trimită cererea de revocare utilizând oricare dintre următoarele metode:
  a) în format electronic, prin trimiterea unei cereri autentificate utilizând codul de revocare primit de la CertDigital. În această situație, certificatul este revocat după ce CertDigital primește solicitarea.
  b) în format electronic, prin trimiterea unei cereri autentificate semnat cu o semnătură electronică calificată creată folosind un certificat digital calificat emis Subiectului (adică cu același nume comun). În această situație, certificatul este revocat după ce CertDigital verifică și validează solicitarea.
  c) într-un format diferit de cel electronic, prin trimiterea unei cereri autentificate. În această situație, certificatul este revocat după ce CertDigital verifică și validează solicitarea.
- Abonatul care încheie un acord contractual cu CertDigital pentru emiterea de certificate

pentru subiecți va trimite cererea de revocare utilizând oricare dintre următoarele metode:

a) În format electronic, prin trimiterea unei cereri autentificate utilizând codul de revocare primit de la CertDigital. În această situație, certificatul este revocat după ce CertDigital primește solicitarea.
b) În format electronic, prin trimiterea unei cereri autentificate semnat cu o semnătură electronică calificată sau un sigiliu electronic calificat. În această situație, certificatul este revocat după ce CertDigital verifică și validează solicitarea.
c) Într-un format diferit de cel electronic, prin trimiterea unei cereri autentificate. În această situație, certificatul este revocat după ce CertDigital verifică și validează solicitarea.

- Autoritatea de înregistrare care poate solicita revocarea fie în numele unui subiect, fie în cazul în care dispune de informații care justifică revocarea certificatului, prin crearea unei cereri autentificate utilizând mecanismele de securitate ale software-ului autorității de înregistrare
- Roluri de încredere asociate CertDigital CA, sub supravegherea Compartimentului de Management al Politicii și Procedurilor (CMPP), prin crearea unei cereri autentificate utilizând mecanismele de securitate ale software-ului Autorității de Certificare.

4. Cerințe operaționale ale ciclului de viață al certificatului

Acest capitol descrie procedurile de bază care se aplică tuturor tipurilor de certificate emise de CertDigital QUALIFIED CA G3.

Procedurile detaliate referitoare la serviciile componente ale PKI (CA, RA, semnatarii CRL, responsabili ai OCSP etc.) și persoanele / rolurile implicate în procesul operațional al acestor componente sunt descrise în documentația internă confidențială.

CertDigital oferă acces la următoarele servicii:

a) înregistrare, certificare, rekey;

b) revocarea certificatului;

c) verificarea valabilității certificatului.

4.1.Cererea de certificat

4.1.1. Cine poate depune o cerere de certificat

Cererea de certificate de către persoanele fizice

CertDigital emite certificate:

- persoanelor fizice, în cazul în care solicită certificatul pentru el însuși
- persoanei (persoanelor) fizice (subiecți) pentru care solicitantul a solicitat certificatul, având un acord obligatoriu din punct de vedere juridic sau care acționează ca angajator.

Abonatul și Subiectul vor respecta prevederile și obligațiile stabilite în formularul de înregistrare, în Contractul de abonat aplicabil și în Termenii și condițiile serviciilor de certificare care încorporează acest CPS și Declarațiile de dezvăluire a PKI.

Autoritatea de Certificare eliberează certificate numai ca răspuns la o solicitare autentificată din partea Autorității de Înregistrare, administrată de CertDigital sau de o terță parte delegată, în cazul în care legislația permite acest lucru.

CertDigital arhivează informațiile referitoare la înscriere. Arhiva este menținută în conformitate cu cerințele definite în CPS și în legislația aplicabilă.

Cererea de certificate de către entitățile juridice (organizații)

CertDigital emite certificate pentru sigiliile electronice persoanelor juridice.

Subiectul respectă prevederile și obligațiile stabilite în formularul de înregistrare, în Contractul de abonați aplicabil și în Termenii și condițiile serviciilor de certificare care încorporează acest CPS și Declarațiile de Informare PKI.

Autoritatea de Certificare eliberează certificate numai ca răspuns la o solicitare autentificată din partea Autorității de Înregistrare, operată de CertDigital.

CertDigital arhivează informațiile referitoare la înscriere. Arhiva este menținută în conformitate cu cerințele definite în CPS și în legislația aplicabilă.

4.1.2. Procesul de înscriere și responsabilitățile

Procesul de înscriere este gestionat de o entitate specifică numită Autoritatea de Înregistrare sau RA care este operată direct de către CertDigital sau bazându-se pe o terță parte în conformitate cu legislația națională.

RA este responsabilă pentru verificarea următoarelor elemente:

- identitatea solicitată a subiectului/abonatului,
- atributele revendicate ale subiectului/abonatului,
- dreptul titularului/abonatului la certificatul solicitat

Procesul de înscriere se efectuează în conformitate cu regulile și metodele descrise aici în CPS și în instrucțiunile și procedurile interne ale RA și legea aplicabilă.

Subiectul este furnizat cu următoarele informații care fac parte din Acordul abonaților:

- formularul de înregistrare
- adresa online pentru Termenii și condițiile certificatului
- adresa online pentru CPS
- regulamentele, avizele sau alte documente furnizate de Subiect (care vor fi definite în Contractul de abonat)

Formularul de înregistrare semnat este considerat acceptat oficial de către Subiectul Contractului de Abonat prin care Subiectul acceptă următoarele:

- responsabilitatea sa ca informațiile furnizate de către Subiect să fie corecte, complete, valabile și actualizate,
- că CertDigital menține o perioadă de păstrare de minimum 10 ani de la data emiterii certificatului pentru toate informațiile referitoare la înregistrare și înscriere, la cererea de certificat și la revocarea certificatului
- că, în cazul în care CertDigital (CA și RA) își încetează activitatea, aceste date pot fi transferate către o terță parte, în conformitate cu aceleași termeni și condiții definite în contractul de abonați,

- recunoaște drepturile, obligațiile și responsabilitățile CertDigital și ale altor participanți la PKI, astfel cum sunt definite în acordul abonatului și în legislațiile naționale,
- că Subiectul are obligația de a informa CertDigital cu privire la orice schimbare sau eveniment care poate afecta valabilitatea sau conținutul certificatului.

Procesul de înscriere

Procesul de înscriere începe la RA.

Responsabilitatea entității RA este de a colecta documentele și atestatele necesare pentru validarea ulterioară a identității și atributelor subiectului/abonatului.

Operatorul RA efectuează o primă verificare a documentelor și atestărilor și verifică dacă informațiile colectate sunt complete și corecte.

După verificarea completă a formularelor Subiectului / Abonatului, RA informează de asemenea Subiectul / Abonatul cu privire la drepturile și obligațiile sale.

RA este responsabilă pentru furnizarea și / sau verificarea informațiilor privind atributele abonatului / subiectului (atribute profesionale, atribute organizaționale etc.). RA verifică și completează datele de înscriere. RA este responsabilă de corectitudinea datelor care vor fi incluse în cererea de certificat trimisă la CA. RA este responsabil pentru înregistrarea corectă / înscriere a subiecților și pentru furnizarea CA cu conținutul corect pentru câmpurile variabile din certificat.

4.2.Prelucrarea cererilor de certificate

CertDigital acceptă cererile depuse individual sau colectiv. Cererile pot fi trimise on-line și off-line.

Cererea de certificat este completată în format electronic:

- Cererea de certificat se completează prin paginile WWW de pe site-ul web al CertDigital folosind următoarea adresă: https://ca.certdigital.ro/client/ sau pe www.certdigital.ro . O persoana care vizitează site-ul respectiv completează (în conformitate cu instrucțiunile de pe site-ul web) un formular de cerere și :
  - ❑ fie în mod personal, să o transmită unei RA sau direct Autorității de Certificare
    - ➢ Site-ul generează o parolă care îi ajută să administreze certificatul sau să genereze date de activare secretă (adică cod PIN) pentru acces securizat la QSCD care conține cheile și certificatele,
    - ➢ sau persoana primește QSCD și datele de activare secretă (adică cod PIN) fie la

fața locului, fie trimise într-o manieră sigură la solicitarea acesteia,

- ❑ sau îl depune la CA prin intermediul serviciilor de curierat / poștă, împreună cu o scrisoare care conține copii ale tuturor documentelor originale, confirmate de un notar public. (QSCD și datele de activare secretă (adică codul PIN) sunt trimise într-o manieră sigură, la solicitarea persoanei).

- Formularul de înregistrare (primit prin e-mail sau de pe site-ul www.certdigital.ro) este semnat electronic cu un certificat digital valid (nu revocat sau expirat) eliberat de CertDigital și transmis Autorității de Certificare prin e-mail sau www.certdigital.ro . QSCD și datele de activare secretă (adică codul PIN) sunt trimise într-o manieră sigură, la solicitarea persoanei.

Solicitarea certificatului este completă off-line:

- Participarea personală a Subiectului la Autoritatea de Înregistrare sau la Autoritatea de Certificare, caz în care cererea este completat și semnat cu semnătură manuală. Subiectul semnează acordul privind serviciile de certificare furnizate și este generată o parolă pentru a ajuta Subiectul să gestioneze certificatul sau să genereze date de activare secretă (adică cod PIN) pentru acces securizat la QSCD care conține cheile și certificatele sau
- Participarea personală a Subiectului la Autoritatea de Înregistrare sau la Autoritatea de Certificare, caz în care cererea este completată și semnată manual. Subiectul semnează acordul privind serviciile de certificare și primește QSCD și datele de activare secretă (adică codul PIN) fie la fața locului, fie trimise în mod sigur după solicitarea Subiectului, sau
- Subiectul transmite CA, împreună cu o scrisoare care conține copii ale tuturor documentelor originale, confirmată de un notar public, semnată manual, prin intermediul serviciilor poștale / poștale. QSCD și datele de activare secretă (adică codul PIN) sunt trimise într-o manieră sigură, la solicitarea Subiectului.

4.2.1. Efectuarea funcțiilor de identificare și autentificare

RA efectuează identificarea și autentificarea conform procedurii definite în capitolul 3.2. și în documentația internă confidențială.

RA colectează și validează informațiile despre identitate ale subiectului și ale abonatului și atributii.

4.2.2. Aprobarea sau respingerea cererilor de certificate

Aprobarea sau respingerea cererilor de certificate este efectuată de RA. RA validează fiecare solicitare și poate respinge o solicitare de certificat în cazul în care cererea nu poate fi autentificată sau dacă cererea nu respectă regulile și standardele care guvernează CertDigital QUALIFIED CA G3 sau din alte motive, la discreția și sub responsabilitatea RA.

Solicitările de certificate sunt procesate în cele din urmă de sistemul CertDigital CA care validează fiecare solicitare și poate respinge o cerere de certificat în cazul în care cererea nu poate fi autentificată sau dacă solicitarea nu respectă regulile și standardele definite pentru tipul de certificat, sub responsabilitatea CertDigital.

4.2.3. Timpul de procesare a cererilor de certificate

CertDigital nu emite un certificat imediat după înregistrare. Certificatele trebuie să fie eliberate de autoritatea de certificare prin aprobarea cererii de certificat după ce a fost validată de RA.

Certificatele sunt stocate pe un QSCD. QSCD poate fi furnizată entității de către CertDigital după procesul generării de chei sau entitatea poate avea un QSCD la generarea cheilor. Procesul de livrare a certificatelor poate dura câteva ore sau mai multe zile și depinde de disponibilitatea persoanei de a primi sau colecta QSCD-ul care stochează certificatul digital sau de a stoca certificatul pe QSCD-ul pe care îl are deja.

4.3.Eliberarea certificatului

4.3.1. Acțiunile CA în cursul emiterii certificatului

Certificatul este emis de CA numai după ce a primit o solicitare de certificat de la RA. CA și RA sunt sisteme integrate și comunică prin conexiuni de rețea închise. CA tratează numai cererile care provin de la certificatul de securitate CertDigital de încredere.
CA asigură unicitatea fiecărui certificat pe care îl emite utilizând câmpul ***certificateSerialNumber*** din fiecare certificat.

4.3.2. Notificarea către abonat de către CA a eliberării certificatului

CA utilizează următoarele metode pentru a informa un subiect despre emiterea certificatului:

- Când cheile sunt generate pe QSCD de către Subiect, CA trimite un e-mail Subiectului utilizând adresa de e-mail furnizată în timpul aplicației. E-mail-ul informează Subiectul despre eliberarea certificatului și oferă informații care permit Subiectului să obțină certificatul și să-l încarce pe QSCD.
- Când cheile sunt generate pe QSCD de către CertDigital, QSCD unde este stocat certificatul digital este fie livrat personal Subiectului, fie trimis prin intermediul serviciilor poștale sau de curierat către Subiect. Datele de activare secretă (adică codul PIN) necesare pentru a accesa QSCD sunt trimise utilizând un plic special securizat.

Fiecare certificat emis este publicat în depozitul de certificate al CertDigital. Publicarea certificatului este echivalentă cu notificarea de către alte părți invocate a faptului că a fost emis un certificat pentru un subiect.

4.4.Acceptarea certificatelor

4.4.1. Desfășurarea acceptării certificatului

Certificatul va fi considerat acceptat de către Subiect după prima utilizare sau după perioada definită în Termeni și condiții, indiferent de evenimentul care survine primul.

RA și Subiectul are dreptul să respingă certificatul sau QSCD și să returneze QSCD, cu condiția să se aplice cel puțin una dintre următoarele obiecții:

- informațiile din certificat sunt incorecte,
- informațiile din certificat au devenit nevalide de la data înregistrării,
- QSCD prezintă semne de deteriorare sau de manipulare,
- QSCD funcționează defectuos sau nu poate fi activat,
- plicul care conține datele de activare secretă (adică codul PIN) necesar pentru a accesa QSCD prezintă semne de manipulare frauduloasă,
- nu a fost respectată procedura de livrare pentru QSCD și plicul care conține datele de activare secretă (adică codul PIN) necesare pentru a accesa QSCD.

Respingerea QSCD implică respingerea tuturor certificatelor Subiectului care sunt stocate pe dispozitiv.

Respingerea unuia dintre certificatele Subiectului care sunt stocate pe QSCD implică implicit respingerea dispozitivului.

Obligațiile subiectului și ale RA în caz de respingere:

- QSCD este returnat la CA
- RA solicită revocarea certificatelor
- RA execută revocarea certificatului

Datele de activare secretă (adică codul PIN) sunt necesare pentru a utiliza cheile private stocate pe QSCD. Atunci când CertDigital furnizează QSCD, datele de activare secretă (adică codul PIN) sunt generate și livrate de un sistem care permite păstrarea confidențialității necesare.

4.4.2. Publicarea certificatului de către CA

Vezi capitolul 2.

4.4.3. Notificarea eliberării certificatului de către CA altor entități

Eliberarea certificatului este notificată de CertDigital altor entități prin publicarea certificatului în depozit, așa cum este descris în capitolul 2.

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 standardele specificate în extensia de utilizare a cheilor.

Vezi secțiunile 1.4.1, 6.1.7 și 7.1.

CertDigital emite certificate pentru cheile stocate pe QSCD:

- cheia privată nu poate fi extrasă din QSCD
- cheia privată se află sub controlul (exclusiv) al subiectului prin intermediul datelor de activare secretă (adică codul PIN)

Aceste date de activare secretă (adică cod PIN) pot fi:

- Definit de Subiect, atunci când cheile sunt generate pe QSCD de către el
- Setarea automată de către CertDigital și modificarea de către Subiect

Când se furnizează QSCD, CertDigital este responsabil pentru:

- inițializarea QSCD și a datelor sale de activare secretă asociate inițial (adică cod PIN)

- distribuirea sigură a QSCD către subiect
- distribuirea sigură a datelor asociate inițial asociate activării (adică codul PIN) către subiect

Subiectul este legat de condițiile și obligațiile menționate în Contractul de abonați, care include acest CPS. Subiectul va proteja QSCD și orice date de activare secretă asociate (adică cod PIN) sau alte informații împotriva pierderii, furtului, dezvăluirii, compromisului sau modificării.

Odată ce QSCD sau datele de activare secretă asociate (adică codul PIN) sunt transmise subiectului, subiectul este responsabil personal pentru:

- utilizarea cheilor numai pentru utilizarea prevăzută, așa cum este definită în CPS și codificată în certificate
- utilizarea unor instrumente care pot interpreta corect utilizarea cheie ca fiind codificată în certificat și care respectă condițiile cheie de utilizare
- utilizarea corectă a QSCD
- nu împărțiți QSCD cu o altă persoană
- setarea datelor de activare secretă (adică cod PIN) care sunt unice și respectă instrucțiunile date în CPS
- păstrarea confidentialității acestor informații secrete
- stocarea în siguranță a oricărui document sau a unui mediu care conține transcrierile unei părți sau a tuturor datelor de activare secretă asociate (adică cod PIN)
- separarea spațiului de stocare pentru QSCD și datele de activare secretă asociate (adică cod PIN)
- nu dezvăluie datele de activare secretă (adică codul PIN) altei persoane

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, 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 care se bazează pe un certificat verifică în orice moment o semnătură digitală prin verificarea valabilității unui certificat digital împotriva serviciului OCSP la adresa

http://ocsp.certdigital.ro sau a CRL - ului publicat de CertDigital pe http://crl.certdigital.ro .

Părțile implicate sunt avertizate că o semnătură digitală neconfirmată nu poate fi atribuită ca semnătură valabilă a Abonatului.

Decizia finală privind posibilitatea de a se baza sau nu pe o semnătură digitală verificată este exclusiv cea a părții care se bazează. Partea care se bazeaza pe o semnătură digitală ar trebui să aibă loc numai dacă:

- Semnătura digitală a fost creată în perioada de funcționare a unui certificat valid și poate fi verificată prin trimiterea la un certificat validat.
- Partea de bază a verificat starea de revocare a certificatului prin trimiterea la CRL, iar certificatul nu a fost revocat.
- Partea de bază înțelege că un abonat a emis un certificat digital pentru un anumit scop și că cheia privată asociată cu certificatul digital poate fi utilizată numai în conformitate cu uzanțele specificate în acest CPS și conținute în certificat.

Încrederea este acceptată ca fiind rezonabilă în conformitate cu prevederile făcute pentru partea care stă la baza acestui CPS și în cadrul Acordului privind Partea invocată. În cazul în care circumstanțele de încredere depășesc garanțiile emise de CertDigital în conformitate cu prevederile prezentului CPS, partea care stăpânește trebuie să obțină asigurări suplimentare.

Garanțiile sunt valabile numai dacă s-au efectuat pașii detaliați mai sus.

Bazându-se pe o semnătură digitală care nu poate fi verificată, poate să ducă la riscuri pe care partea de bază își asumă în întregime și pe care CertDigital nu o asumă în nici un fel.

4.6.Reînnoirea certificatului

Nu se aplică.

4.7.Certificate Re - key

4.7.1. Circumstanța pentru Re-key certificat

CertDigital efectuează recuperarea certificatelor pentru certificatele digitale valide (neexpirate și nu revocate) CertDigital emise, care nu necesită modificări ale datelor de certificat sau ale

extensiilor. Procesul de re-key constă în re-emiterea unui certificat cu o pereche nouă de chei pentru a extinde data de expirare fără a schimba identitatea sau alte extensii de certificate.

4.7.2. Cine poate solicita certificarea unei noi chei publice

CertDigital informează permanent Subiecții (cu cel puțin 30 de zile înainte) despre apropierea perioadei de expirare.

Recodificarea se efectuează atunci când un subiect care deține un certificat digital valabil (nu este revocat și nu expirat) generează o nouă pereche de chei (sau solicită CertDigital să genereze o astfel de pereche cheie) și solicită emiterea unui nou certificat pentru a confirma deținerea unei noi chei publice.

Revocarea certificatului se face numai la solicitarea Subiectului și va fi precedată de depunerea unei cereri sau un formular corespunzător, completat de Abonat/Subiect.

4.7.3. Prelucrarea cererilor de re-cheiere a certificatului

Procesul solicitării inițiale a certificatului va fi modificat după cum urmează:

- Identificarea solicitantului este înlocuită cu verificarea semnăturii digitale pe formularul de cerere.
- Rezultatele validării din cererile anterioare sunt considerate valide în timp ce informațiile validate nu s-au modificat.
- Orice date care s-au schimbat vor fi validate ca și când ar fi o nouă cerere.

4.7.4. Notificarea emiterii noului certificat către abonat

RA utilizează aceleași procese de notificare ca și pentru un certificat nou solicitat.

4.7.5. Desfășurarea acceptării unui certificat reîncadrat

RA utilizează aceleași procese ca și pentru un certificat nou solicitat.

4.7.6. Publicarea certificatului reîncadrat de către CA

RA utilizează aceleași procese ca și pentru un certificat nou solicitat.

4.7.7. Notificarea eliberării certificatului de către CA altor entități

RA utilizează aceleași procese ca și pentru un certificat nou solicitat.

4.8.Modificarea certificatului

CertDigital nu modifică certificatele emise.

Subiectul sau abonatul, după caz, solicită CertDigital să revocă certificatul imediat ce informațiile incluse în certificat nu mai corespund realității.

4.9.Revocarea și suspendarea certificatului

Certificatele emise de CertDigital QUALIFIED CA G3 pot fi revocate, dar nu sunt suspendate. Revocarea certificatului este ireversibilă.

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

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

Dacă o cheie privată care corespunde unei chei publice conținute într-un certificat revocat rămâne sub controlul Subiectului, după revocare ar trebui să fie stocată în siguranță până când va fi distrusă.

4.9.1. Circumstanțele de revocare

Certificatul este revocat când:

- Informațiile din certificat s-au modificat,
- O cheie privată asociată unei chei publice din certificat a fost compromisă sau există motive serioase pentru a suspecta că a fost compromisă,
- Se încheie raportul de muncă sau acordurile legale obligatorii între Abonat și Subiect,
- Subiectul, deținătorul cheii private asociate cheii publice din certificat, solicită revocarea,
- Abonatul solicită revocarea certificatelor entității finale pentru subiecți aflați în grija sa,
- Subiecții / abonații nu acceptă termenii și regulamentele noi modificate ale CPS

- 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,
- Întârzierile la subiect sau nu plătesc valoarea serviciilor furnizate de CertDigital QUALIFIED CA G3,
- Cheia privată sau securitatea certificatului certificat CertDigital au fost compromise într-o manieră care amenință credibilitatea certificatelor,
- În alte cazuri în care Subiectul nu respectă regulile prezentului CPS, Acordul abonatului, Termenii și condițiile sau alte acorduri încheiate între părți în legătură cu serviciile furnizate de CertDigital QUALIFIED CA G3.

Cheia privată compromisă înseamnă: (a) accesul neautorizat la cheia privată sau un motiv serios de a suspecta un astfel de lucru; (b) pierderea cheii private sau apariția unui motiv pentru a suspecta o astfel de pierdere; (c) cheia privată furată sau apariția A unui motiv de a suspecta un astfel de jaf, (d) ștergerea accidentală a cheii private.

4.9.2. Cine poate cere revocarea

Următoarele entități pot trimite cereri de revocare a certificatelor:

- Subiectul care deține cheia privata asociata cu cheia publica a certificatului
- Abonatul care încheie un contract cu CertDigital pentru emiterea de certificate pentru Subiecți
- Autoritatea de înregistrare care poate cere revocarea fie în numele unui subiect, fie în cazul în care dispune de informații care justifică revocarea certificatului
- Roluri de încredere asociate CertDigital QUALIFIED CA G3, sub supravegherea Compartimentului de Management al Politicii și Procedurilor (CMPP)

Cererea de revocare poate viza mai multe certificate.

4.9.3. Procedura pentru cererea de revocare

Prezentarea cererii de revocare este descrisă în capitolul 3.4.

Cererea de revocare a certificatului trebuie să identifice cu exactitate fiecare certificat, să conțină motivul (motivele) pentru care se solicită revocarea și să fie autentificat.

Informațiile despre certificatele revocate sunt plasate pe Lista de revocare a certificatelor eliberată

de CertDigital QUALIFIED CA G3.

Cererea de revocare a certificatului are loc după cum urmează:

- CertDigital verifică cererea de revocare, inclusiv că este trimisă de o entitate legitimă. Dacă cererea este verificată cu succes, CertDigital QUALIFIED CA G3 plasează informațiile privind revocarea certificatului în Lista de Revocare a Certificatelor (CRL);
- CertDigital notifică Subiectul despre revocare sau despre decizia de anulare a cererii, împreună cu motivele acestei anulări.

Ori de câte ori un certificat sau o cheie privată care corespunde unui certificat care urmează să fie revocat sunt stocate pe un QSCD, în urma revocării certificatului, QSCD este șters în condiții de siguranță. Această acțiune este efectuată de proprietarul QSCD - o persoană fizică sau juridică (un reprezentant al unei astfel de entități). Proprietarul QSCD trebuie să îl păstreze în siguranță, pentru a preveni furtul sau utilizarea neautorizată până la ștergerea cheii private.

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 posibil.

4.9.5. Timpul în care CA trebuie să proceseze cererea de revocare

CertDigital garantează o perioadă maximă de 24 de ore pentru procesarea unei cereri de revocare a certificatului. Prin trimiterea unei cereri autentificate utilizând codul de revocare primit de la CertDigital. În această situație, certificatul este revocat după ce CertDigital primește solicitarea. Prin trimiterea unei cereri autentificate utilizând codul de revocare primit de la CertDigital. În această situație, certificatul este revocat după ce CertDigital primește solicitarea. Atunci când se trimite o cerere autentificată utilizând codul de revocare primit de la CertDigital, certificatul este revocat automat.

Informațiile privind revocarea certificatului sunt stocate în baza de date a CertDigital. Certificatele revocate sunt plasate pe Lista de Revocare a Certificatului (CRL), în conformitate cu frecvența de emisie a CRL.

4.9.6. Cerințele de verificare a revocării pentru părțile implicate

Părțile implicate utilizează toate resursele furnizate de CertDigital (CRL, OCSP) pentru a verifica

starea unui certificat înainte de a se baza pe acesta.

4.9.7. Frecvența emiterii CRL

Fiecare parte a autorității de certificare a CertDigital emite diferite liste de revocare a certificatelor. Un nou CRL este publicat în depozit imediat după fiecare revocare a certificatului sau în maxim o zi. Perioada de disponibilitate a CRL este de 48 de ore și se actualizează zilnic.

Lista de revocare a certificatelor (CRL) pentru autoritatea CertDigital ROOT CA G3 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-uri

CRL-ul din prezentul CA și al tuturor CA-urilor sale emitente subordonate se eliberează în conformitate cu capitolul 4.9.7 și se publică fără întârziere.

4.9.9. Disponibilitatea on-line a revocării / verificării stării

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 RFC6 960.

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

Dacă un subiect cunoaște sau suspectează că integritatea cheii private a certificatului său a fost compromisă, Subiectul trebuie:

- să înceteze imediat utilizarea certificatului,
- să inițieze imediat revocarea certificatului;
- să ștergeți certificatul de pe toate dispozitivele și sistemele,
- să informeze toate părțile invocate care pot depinde de acest certificat.

Compromisul cheii private poate avea implicații asupra informațiilor protejate cu această cheie. Subiectul decide cum să se ocupe de informațiile afectate înainte de a șterge cheia compromisă.

4.9.13. Circumstanțele pentru suspensie

Nu se aplică.

4.9.14. Cine poate solicita suspendarea

Nu se aplică.

4.9.15. Procedura pentru cererea de suspendare

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 , 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

Sfârșitul abonamentului are loc după:

- Revocarea cu succes a ultimului certificat al unui abonat / subiect,
- Expirarea ultimului certificat al unui abonat / subiect.

Din motive de respectare a legii, CertDigital și toate autoritățile de înregistrare păstrează toate datele și documentele pentru o perioadă de minimum 10 ani de la terminarea abonamentului.

4.12. Key escrow și recuperare cheie

CertDigital nu permite key escrow pentru certificate calificate.

5. Facilitatea, managementul și controlul operațional

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 standard 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 și 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

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 astfel încât să permită accesul numai la persoanele care au fost eliminate în mod corespunzător și autorizate în mod specific să intre în zonă;
- monitorizarea cu control personal și electronic a intruziunilor neautorizate în orice moment;
- personalul care nu se află pe lista de acces este escortat și supravegheat în mod corespunzător;
- un jurnal de acces la site este menținut și inspectat periodic;
- fiecare echipament este bine întreținut pentru a asigura disponibilitatea și integritatea acestuia.

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 de persoanele autorizate, acesta din urmă fiind acordat acces doar 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. Energie 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, echipament 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 de senzori de umiditate si de inundatie.

5.1.5. Prevenirea și protejarea 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. Mediile de stocare

În conformitate cu cerințele politicii de clasificare a informației, mediile 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 a mediilor, cu aceeași securitate ca și locația primară. Mediile care conține date sensibile sunt dezafectate în siguranță 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 cu roluri de încredere vor fi distruse. Ștergerea securizată se face în conformitate cu Politica de Securitate a Informațiilor CertDigital.

5.1.8. Backup de rezervă

Copiile cardurilor criptografice sunt stocate în depozit în afara locației primare CertDigital.

Depozitul din 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:

- **Ofițer 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 Persoane / 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 funcție de funcție (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 trasabile 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. Segregarea sarcinilor și principiile celor mai puțin privilegiate sunt în vigoare. Sensibilitatea poziției bazată pe taxe 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 de calificare, experiență și cerințe 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 clearance-ul necesar și că sunt adecvate să li se încredințeze roluri de încredere și să îndeplinească funcția specifică a postului respectiv. 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 controalelor relevante personalului potențial prin intermediul rapoartelor de stare emise de o autoritate competentă, al declarațiilor de la terțe părți sau al declarațiilor autodepresive semnate.

5.3.3. Cerințe de formare

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 jucat 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 implicate, 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 stației 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 rechetare, 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-cheie de certificate, sunt înregistrate.

Sunt înregistrate toate informațiile de înregistrare, inclusiv următoarele:

- 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;
- locul de depozitare a copiilor aplicațiilor și 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 jurnalele de sistem este permis exclusiv pentru ofițerul de securitate, personalul special desemnat și auditorii.

Se păstrează confidențialitatea informațiilor despre subiect.

5.4.2. Frecvența procesării jurnalului

Jurnalele de sistem 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 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, controalele de protecție a jurnalului sunt implementate în așa fel încât, chiar și după arhivarea jurnalului, este imposibil să se șteargă înregistrările sau jurnalul întreg, înainte de expirarea timpului de retenție globală a jurnalului.

5.4.5. Proceduri de salvare a jurnalelor 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 rapoartele de audit sunt ținute în conformitate cu procedurile interne.

5.4.6. Auditul sistemului de colectare (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
- Depozit
- Analiza
- Corelate
- Arhiva
- Back-up pe termen lung.

5.4.7. Notificarea subiectului care provoacă 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 27001:2013. 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.

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, chei utilizate de Autoritățile de Certificare și Înregistrare, întreaga corespondență între CertDigital și subiecți/Abonați ar trebui supuse arhivării.

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. Arhiva certificatului revocat conține informațiile despre 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 date 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 logo-urilor este păstrat cel puțin 10 ani.
- Jurnalele 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:
  - ❑ înregistrarea tuturor evenimentelor legate de ciclul de viață al cheilor gestionate de CA, inclusiv orice perechi de chei de subiecte generate de CA
  - ❑ 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 și integrității datelor 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. Arhiva sistemului de colectare (intern sau extern)

Arhivele sistemelor de colectare a 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 cheii

Procedurile de schimbare prin cheie permit 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 CA de semnare a perechii de chei este comandată și toate certificatele emise ulterior, iar CRL-urile sunt semnate cu noua cheie privată de semnare. Atât vechile, cât și cele noi perechi de chei pot fi active simultan. Acest proces de schimbare cheie ajută la minimizarea oricăror efecte negative ale expirării certificatului CA. Certificatul corespunzător certificatului public CA nou este furnizat abonaților și partenerilor aflați în întreținere prin metodele de difuzare detaliate în capitolul 6.1.4.

5.7.Recuperarea după compromitere 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. Proceduri de tratare a incidentelor și a 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 identificarea incidentului de securitate.

În cazul unui incident de securitate, se utilizează proceduri interne. Procedurile includ notificarea Ofițerului de securitate (Supervisory body).

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 posibilele evenimente critice de securitate.

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:

- coruperea fizică a sistemului informatic al CertDigital, incluzând corupția resurselor de rețea - această amenințare abordează corupțiile generate de situații de urgență,
- funcționarea necorespunzătoare a software-ului și a aplicațiilor, astfel încât aceste date să fie inaccesibile - astfel de corupții se adresează sistemului de operare, aplicațiilor utilizatorilor și execuției de software rău intenționat, de exemplu viruși, troieni,
- pierderea serviciilor de rețea, importantă pentru activitatea CertDigital. Eroarea sa principală de alimentare a site-ului și deteriorarea conexiunilor de rețea,
- coruperea unei părți din infrastructura internă a rețelei, utilizată de CertDigital pentru a furniza servicii - corupția poate implica obstrucționarea clienților și negarea (neintenționată) a serviciilor.

Pentru a preveni sau a limita rezultatele unor amenințări 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 importante ale unei autorități de certificare până la restaurarea serviciilor din instalația primară. 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 timestamp 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.
- De asemenea, sunt monitorizate 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 acesteia. 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. Proceduri de compromis ale cheii private a entității

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

În cazul în care Autoritățile de Certificare (afiliate cu CertDigital) au compromis sau suspiciune cu privire la cheia privată, 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 intermediul mijloacelor de informare în masă și prin poșta electronică
- Notificarea publicului larg prin intermediul mai multor canale, inclusiv un mesaj pe depozit și site-ul CA al CertDigital, 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 corupte sunt revocate și motivul pentru care revocare este efectuata.
- 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.

Atunci când o cheie privată asociată unei chei publice din certificat a fost compromisă sau există motive serioase pentru a suspecta că aceasta a fost compromisă, Subiectul sau Abonatul, după caz, va solicita CertDigital să revocare a certificatului.

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. Se oferă facilități adecvate de back-up 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 compromisul, pierderea sau presupusul compromis al cheii private a CA ca 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 procedura terminare actualizată pentru a reduce la minimum întreruperile pentru subiecți/abonați și Părți implicate 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 supusă anulării (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 stabilite, printre care părțile implicate, 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 informațiile de înregistrare, statutul de revocare a certificatelor neexpirtate 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;
- Dacă este posibil, să ia măsuri pentru a transfera furnizarea de servicii de certificare pentru clienții existenți unui alt furnizor de servicii de certificare.

CertDigital va menține sau va transfera către o parte sigură 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 angajament 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 G3 în cazul încetării serviciilor CertDigital QUALIFIED CA G3.

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 subiecților CA și a altor participanți la PKI și alți parametri critici de securitate.

Procedurile pentru gestionarea cheie 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.

CertDigital QUALIFIED CA G3 deține cel puțin un certificat semnat de CertDigital ROOT CA G3. Cheia privată corespunzătoare cheii publice conținute în certificat este utilizată exclusiv pentru a semna cheile publice ale subiecților și lista de revocare a certificatelor necesare pentru funcționarea CA.

O semnătură electronică este creată prin intermediul algoritmului RSA în combinație cu criptarea SHA-2.

Cheile private ale unui Subiect vor fi generate folosind un QSCD. O entitate poate avea un QSCD atunci când generează cheia sau QSCD poate fi furnizată entității de către CertDigital după procesul de generare a cheilor.

6.1.1. Generarea perechii de chei

CertDigital are o procedură documentată pentru efectuarea generării de perechi de chei CA pentru CertDigital QUALIFIED CA G3. 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;
- Cerințele dovezilor care trebuie colectate în timpul generării.

După generarea cheii, CertDigital va prezenta un raport de generare a cheii 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 va fi semnat de către rolul de încredere responsabil pentru securitatea ceremoniei de gestionare a cheilor CertDigital (de exemplu, ofițer de securitate) ca martor că raportul înregistrează corect generarea cheilor în timp ce este efectuată.

În toate cazurile, CertDigital:

- 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 G3**, precum și cheile altor autorități subordonate și certificarea ulterioară a cheilor publice sunt efectuate într-un mediu fizic securizat de către personal cu roluri de încredere sub cel puțin control dual:

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

Perechile cheii ale **CertDigital QUALIFIED CA G3** sunt generate pe stații de lucru desemnate și autentificate și conectate la modulele 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 perechii de chei **CertDigital QUALIFIED CA G3** este similar cu procesul acceptat 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 se realizează 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, părți dependente, CA mai mari în ierarhia CA etc.) să confirme acest lucru schimbarea cheii și punerea în aplicare a operațiunilor necesare pentru a evita orice inconvenient și funcționare defectuoasă. Acest lucru nu se aplică cazului în care ne-ar înceta operațiunile înainte de data de expirare a certificatului de semnătură sau a certificatului.

Cheile subiecților sunt generate:

- De către subiect, prin intermediul aplicațiilor software și dispozitivelor criptografice certificate ca QCSD în conformitate cu Regulamentul UE 910/2014. Subiectul este responsabil pentru verificarea faptului că dispozitivul este un QSCD definit de Regulamentul UE 910/2014.
- Prin CertDigital, în numele subiectului, prin aplicații software și dispozitive criptografice certificate ca QCSD în conformitate cu Regulamentul UE 910/2014. În timp ce sunt deținute de CertDigital, cheile de subiect generate de CA sunt stocate în siguranță.

Cheile generate de CA sunt generate folosind un algoritm recunoscut ca fiind potrivit pentru utilizări, pe durata valabilității certificatului.

6.1.2. Livrarea cheii private către abonat

Atunci când cheile sunt generate pe QSCD de către CertDigital, QSCD unde se stochează cheia privată și certificatul digital este fie livrat personal către subiect, fie trimis prin intermediul serviciilor poștale sau de curierat către subiect. Datele de activare secretă (adică codul PIN) necesare pentru a accesa QSCD sunt trimise utilizând un plic obisnuit.

6.1.3. Livrarea cheii publice către emitentul de certificate

Subiecții prezintă cheile publice generate ca o solicitare electronică a cărei formă trebuie să respecte protocoalele din PKCS # 10 (CSR).

Prezentarea unei chei publice nu se aplică în cazul în care o pereche de chei este generată la cererea subiectului/abonatului de către CertDigital, care emite un certificat pentru perechea de chei generate.

6.1.4. Furnizarea de chei publice CA către părțile implicate

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

Cheile publice ale unei autorități 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 CA calificată CertDigital, certificatele sunt semnate.

Autoritățile de certificare CertDigital își publică certificatele prin plasarea lor în sectiunea publica a CertDigital: http://www.certdigital.ro .

Certificatele autorităților de certificare CertDigital pot fi transmise părților invocate împreună cu software-ul (sisteme de operare, browsere web, clienți de e-mail etc.), care permit utilizarea serviciilor oferite de CertDigital.

Certificatul de depozitare impune controlul accesării după adăugarea, ștergerea certificatelor sau modificarea informațiilor aferente.

6.1.5. Dimensiunile cheilor

CertDigital QUALIFIED CA G3 utilizează o cheie de 4096 biți pentru semnarea certificatului și CRL.

Certificatele digitale emise de CertDigital QUALIFIED CA G3 utilizează chei RSA de 2048 biți.

Certificatele digitale sunt semnate folosind algoritmul RSA în combinație cu criptarea SHA-2.

CertDigital își rezervă dreptul de a introduce în viitor alți algoritmi și protocoale decât RSA cu SHA-2 sau lungimi de chei mai lungi. Aceasta poate include algoritmi de curbă eliptică în loc de RSA și alți algoritmi de hash.

6.1.6. Generarea parametrilor cheilor publice și verificarea calității

CertDigital are o procedură documentată pentru efectuarea generării de perechi de chei CA pentru toate CA-urile, inclusiv CertDigital QUALIFIED CA G3.

Perechea cheie a unui subiect este generată utilizând un QSCD care îndeplinește cerințele stabilite în Anexa II la Regulamentul (UE) 910/2014, cu specificații tehnice care le permit să proceseze algoritmi și lungimi de chei, așa cum este descris în capitolul 7.

Cheile Subiectului sunt generate fie de CertDigital, fie de Subiect. Înainte de a genera cheile, Subiectul are întreaga responsabilitate pentru a verifica dacă dispozitivul hardware utilizat pentru generarea cheilor îndeplinește cerințele QSCD.

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

Scopurile de utilizare a tastelor permise sunt descrise în câmpul KeyUsage (vezi Capitolul 7.1.2) 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 cripării datelor Subiectului, altele decât cele descrise în c) și e),
e) **keyAgreement**: destinat pentru protocoale de schimb de cheie,
f) **keyCertSign**: 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 cheii private și controlul tehnic al modulelor criptografice

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 alterate 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 control 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

CertDigital QUALIFIED CA G3 folosește protecție hardware pentru 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.

Subiectul utilizează dispozitive de protecție hardware cheie care sunt dispozitive de creare a semnăturilor electronice calificate (QSCD).

Generarea perechii de chei poate fi efectuată de către Subiectul din QSCD, care este un sistem de încredere.

Când CertDigital generează cheile în numele subiectului, utilizează întotdeauna QSCD.

6.2.2. Controlul multi-persoană al cheii private

Controlul multi-persoană al unei chei private se aplică cheilor private ale certificatului CertDigital QUALIFIED CA G3 folosit pentru semnarea certificatului și 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 proprietarului lor.

Procedura comună de transfer secret trebuie să includă: generarea și procesul de distribuire a cheilor, acceptarea secretului și a responsabilităților rezultate pentru păstrarea sa.

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 cod 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 secretul pentru a nu fi divulgat. 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 deținător pe site-ul de recuperare de urgență de către deținător într-o manieră care să permită 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 Proceduri de certificare și într-un mod deliberat și responsabil în orice situație posibilă. Un deținător de 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.

Controlul cu mai multe persoane nu se aplică cheii private a Subiectului.

6.2.3. Cheie privată escrow

Cheile private ale Autorităților de Certificare nu sunt supuse custodiei.

Cheile private ale subiectului 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). In 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 Autorității de Certificare.

Cheia privată de semnare CA este supusă copierii de rezervă, este 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.

Copierea de rezervă a cheii private nu se aplică cheii private a Subiectului.

6.2.5. Arhivarea cheii private

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

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 corupție sau defecțiune a modulului) să introduceți 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 QUALIFIED CA G3 necesită restaurarea cheii de pe HSM în prezența unui număr corespunzător de proprietari secreți partajați 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.

Cheia privată a subiectului nu este transferată în sau din modulul criptografic.

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 alterate 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 sediului CA securizat.

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

Cheile private CA rămân sub un control multi-personal. 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 semnăturii electronice calificate (dispozitive/carduri). Cheile sunt întotdeauna generate pe dispozitive și nu se descarcă niciodată. Dispozitivele securizate sunt protejate, de producători pentru CertDigital, în timpul depozitării la CertDigital și în timp ce sunt distribuite.

Cheile private ale subiecților sunt stocate în memoria securizată a QSCD. Microcipul încorporat protejează cheile private și alte informații legate de securitate împotriva atacurilor.

6.2.8. Metoda de activare a cheii private

Toate cheile private ale CertDigital QUALIFIED CA G3 sunt introduse în modul după generarea lor, importate într-o formă criptată dintr-un alt modul sau după restaurarea din secrete partajate. Activarea cheilor private este întotdeauna precedată de autentificarea operatorului. Autentificarea

se efectuează pe baza unui card criptografic deținut de operator.

Cheia privată este stocată pe QSCD, sub controlul subiectului. Cheia poate fi accesată numai prin utilizarea unor date de activare secrete (adică cod PIN).

6.2.9. Metoda de dezactivare a cheii private

Metoda de dezactivare a cheii private CertDigital QUALIFIED CA G3 se aplică dezactivării cheii după utilizarea acesteia sau la încheierea fiecărei sesiuni în timpul căreia a fost utilizată cheia (de exemplu, dezactivarea aplicației).

Cheia privată a subiectului este dezactivată prin deconectarea QSCD de la computer sau de la orice alt dispozitiv.

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 Compartimentului Managementul Politicilor 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, dispozitivele HSM permit zeroirea prin acces fizic la setările pe dispozitiv. Acest proces reinițializează dispozitivul și suprascrie toate datele din acesta cu zerouri binare. În cazurile în care această procedură de zeroizare sau reinițializare 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 cheii. Dosarele asociate sunt arhivate în siguranță. Compartimentul Managementul Politicilor si Procedurilor (CMPP) autorizează distrugerea cheii private a CA și atribuie personalului sarcina.

Fiecare distrugere a cheii private este înregistrată în jurnalul evenimentului.

Subiectul este responsabil pentru distrugerea cheii private. Acest lucru se poate realiza fie cu ajutorul funcțiilor de inițializare middleware ale dispozitivului, fie prin distrugerea fizică a dispozitivului.

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 cheii selectate 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 QUALIFIED CA G3 trebuie să fie compatibile cu utilizarea cheie definită așa cum se prevede în recomandarea ITU-T X.

6.3.1. Arhivarea cheilor publice

CertDigital își arhivează propriile chei publice CA și toate cheile publice certificate de CertDigital QUALIFIED CA G3 sub forma certificatului X509 care conține cheia.

Vezi capitolul 5.5 pentru condițiile de arhivare.

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 domeniului valabilității fiecărui certificat de cheie publică. Perioada de valabilitate se aplica si pentru cheia privata.

Perioada maximă de utilizare a cheilor de la Subiect nu poate depăși perioada de valabilitate a unui certificat.

Perioada de valabilitate a certificatului CertDigital QUALIFIED CA G3 este de 10 ani.

Perioada de valabilitate a unui certificat al Subiectului este de până la 3 ani.

Perioadele de utilizare a certificatelor și cheilor private aferente pot fi reduse în cazul revocării unui certificat.

În general, data de începere a valabilității unui certificat corespunde datei emiterii acestuia.

Nu este permisă setarea acestei date în viitor sau în trecut.

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 unul sau mai multi factori (așa-numita expresie de autentificare, de exemplu, parolă, număr PIN etc.)
- Ca parte a secretului comun.

Operatorii 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 ale 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 cardurilor 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 se asigură că datele de activare asociate cheilor și operațiunilor private ale CA sunt generate, gestionate, stocate și arhivate în siguranță, așa cum este descris în subsecțiunea relevantă din secțiunile 6.1 și 6.2.

Instalarea și recuperarea perechilor de chei ale CA într-un dispozitiv criptografic securizat necesită un control simultan al cel puțin doi angajați în roluri de încredere.

Atunci când subiecții generează chei private utilizând QSCD, este responsabilitatea lor să genereze și datele de activare (adică codul PIN).

Atunci când cheile sunt generate pe QSCD de către CertDigital, QSCD unde se stochează cheia privată și certificatul digital este fie livrat personal Subiectului, fie trimis prin intermediul

serviciilor poștale sau de curierat către subiect. Datele de activare secretă (adică codul PIN) necesare pentru a accesa QSCD sunt trimise utilizând un plic special securizat.

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) de entitatea care este autentificată. Dacă datele de activare sunt scrise, nivelul protecției lor ar trebui să fie același cu datele protejate prin utilizarea cardurilor criptografice. Mai multe încercări nereușite de a accesa modulul criptografic ar trebui să ducă la blocarea acestuia. Datele de activare stocate nu vor fi ținute niciodată împreună cu cardul criptografic.

Subiecții sunt responsabili pentru gestionarea și protejarea sigură a datelor de activare (adică cod PIN).

Datele de activare secretă (adică codul PIN) primite de la CertDigital vor fi imediat modificate de Subiect după primirea acesteia.

6.4.3. Alte aspecte ale datelor de activare

Nu se aplică.

6.5.Controalele de securitate ale computerului

Acest capitol descrie comenzile de securitate ale calculatorului din cadrul domeniului CertDigital.

Subiectul este responsabil pentru propriile controale de securitate ale calculatorului. Aceste aspecte nu sunt acoperite în subcapitolele de mai jos.

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 decurg 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,
- O 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.

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

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

Datele sensibile trebuie să fie 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 siguri pentru mediile de stocare, HSM-urile sunt zeroizate, dispozitivele criptografice securizate (dispozitive/cartele) 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) si CEN CWA 14167 (Cerințe de securitate pentru sisteme de încredere care gestionează certificate pentru semnături electronice).

6.6.Controalele de securitate ale ciclului 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 a cerințelor 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 managementui 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 ale 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 asigură monitorizarea capacității infrastructurii ICT pentru serviciile de certificare și realizarea estimărilor privind cerințele de capacitate pentru a se asigura că există o putere și o capacitate de stocare adecvată.

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, sistemele 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) in 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) se efectuează scanarea periodică 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 entitate cu abilitățile, instrumentele, competența, codul de etică și independența necesară pentru a oferi un raport de evaluare fiabilă.

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 routerele 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 exemplu, routerele) 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 CertDigital QUALIFIED CA G3 se află într-o zonă de securitate ridicată.

6.8.Marcare temporară (Time-stamping)

Timpul de acuratețe al jurnalelor este asigurat de un server de timp care este sincronizat cu cel puțin două surse de timp care pot fi sateliți GPS sau UTC (NIMB).

7. Certificatul, CRL și profilul 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 câmpurilor respective de certificate, CRL și OCSP, standarde și extensii private aplicate de CertDigital.

7.1.Profilul certificatului

Profilul câmpurilor de bază pentru certificatul CertDigital QUALIFIED CA G3 descris în Tabelul 7.1.

Field name	Value or value's constraint	
Version	3	
Serial Number	20 11 04 20 93 03 01	
Signature Algorithm	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)	
Issuer (Distinguished Name)	Department (OU)=	CertDigital ROOT CA G3
	Organization (O) =	Centrul de Calcul S.A.
	Country (C) =	RO
Not before (validity period beginning date)	May 03 00:00:00 2017 GMT	

Not after (validity period end date)	May 03 00:00:00 2027 GMT	
Subject (Distinguished Name)	OrganizationIdentifier (OID: 2.5.4.97) =	VATRO-2163993
	Department (OU)=	CertDigital QUALIFIED CA G3
	Organization (O) =	Centrul de Calcul S.A.
	Country (C) =	RO
Subject Public Key Info	4096 bits RSA key	
Signature	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)	

Tabelul 7.1. Profilul câmpurilor de bază pentru CertDigital QUALIFIED CA G3

Profilul câmpurilor de bază pentru certificatele emise de CertDigital QUALIFIED CA G3 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	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)	
Issuer (Distinguished Name)	OrganizationIdentifier (OID: 2.5.4.97) =	VATRO-2163993
	Department (OU)=	CertDigital QUALIFIED CA G3
	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)	Encoded in accordance with RFC 5280, may contain fields presented in Chapter 3.1.2.	
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 7.2. Profilul câmpurilor de bază ale certificatelor emise de CertDigital QUALIFIED CA G3

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 certificatul CertDigital QUALIFIED CA G3 sunt descrise în Tabelul 7.3.

Extension	Value or value's constraint	Extension status
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.certdigital.ro [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://certs.certdigital.ro/certdigital-rootg3.crt	Non-critical
Basic Constraints	Subject type=CA, Path length constraint=0	Critical
Key Usage	keyCertSign (bit 5), cRLSign (bit 6)	Critical
Authority Key Identifier	KeyID=0f bc 78 c8 03 b5 e5 fb 35 fa 51 d2 a6 2f 85 66 67 2d 32 fb d1 d0 b5 f1 2c 92 d8 87 4f fa 34 e6 Certificate Issuer: Directory Address: OU=CertDigital ROOT CA G3 O=Centrul de Calcul S.A. C=RO Certificate SerialNumber=20 11 04 20 93 02	Non-critical
Subject Key Identifier	18 42 b9 b2 98 54 bd b1 1d 9b a1 68 d3 a4 81 76 2e bb ac b2 0e f5 3f 10 48 fb 87 e9 00 3b 59 24	Non-critical
Certificate Policies	[1]Certificate Policy: Policy Identifier=All issuance policies [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certdigital.ro/repository	Non-critical
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.certdigital.ro/certdigital-rootg3.crl	Non-critical

Tabelul 7.3. Extensiile certificatului CertDigital QUALIFIED CA G3

Certificatul calificat pentru semnătura electronică cu QSCD eliberat persoanelor fizice conține extensii descrise în tabelul 7.4.

Extension	Value or value's constraint	Extension status
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.certdigital.ro [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://certs.certdigital.ro/certdigital-qualifiedg3.crt	Non-critical
Key Usage	digitalSignature (bit 0),nonRepudiation (bit 1)	Critical
Authority Key Identifier	KeyID=18 42 b9 b2 98 54 bd b1 1d 9b a1 68 d3 a4 81 76 2e bb ac b2 0e f5 3f 10 48 fb 87 e9 00 3b 59 24 Certificate Issuer: Directory Address: OU=CertDigital ROOT CA G3 O=Centrul de Calcul S.A. C=RO Certificate SerialNumber=20 11 04 20 93 03 01	Non-critical
Subject Key Identifier	The keyIdentifier is composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).	Non-critical
Certificate Policies	[1]Certificate Policy: Policy Identifier=0.4.0.194112.1.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certdigital.ro/repository [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.47898.3.1.3.1.1.1 or 1.3.6.1.4.1. 47898.3.1.3.1.2.1 (see details in chapter 7.1.6) [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certdigital.ro/repository	Non-critical
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.certdigital.ro/certdigital-qualifiedg3.crl	Non-critical
Subject Alternative Name	Other Name: RFC822 Name and Principal Name (UPN)	Non-critical
Qualified Certificate Statements	esi4-qcStatement-1: 0.4.0.1862.1.1 esi4-qcStatement-4: 0.4.0.1862.1.4 esi4-qcStatement-6: 0.4.0.1862.1.6 id-etsi-qcs-QcType 1: 0.4.0.1862.1.6.1 esi4-qcStatement-5: 0.4.0.1862.1.5 URL=http://www.certdigital.ro/repository Language=EN	Non-critical

Tabelul 7.4. Certificat calificat pentru semnătura electronică cu QSCD eliberat persoanelor fizice

Certificatul calificat pentru sigiliul electronic cu QSCD eliberat persoanei juridice conține extensii descrise în tabelul 7.5.

Extension	Value or value's constraint	Extension status
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.certdigital.ro [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://certs.certdigital.ro/certdigital-qualifiedg3.crt	Non-critical
Key Usage	digitalSignature (bit 0),nonRepudiation (bit 1)	Critical
Authority Key Identifier	KeyID=18 42 b9 b2 98 54 bd b1 1d 9b a1 68 d3 a4 81 76 2e bb ac b2 0e f5 3f 10 48 fb 87 e9 00 3b 59 24 Certificate Issuer: Directory Address: OU=CertDigital ROOT CA G3 O=Centrul de Calcul S.A. C=RO Certificate SerialNumber=20 11 04 20 93 03 01	Non-critical
Subject Key Identifier	The keyIdentifier is composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).	Non-critical
Certificate Policies	[1]Certificate Policy: Policy Identifier=0.4.0.194112.1.3 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certdigital.ro/repository [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.47898.3.1.3.1.1.2 or 1.3.6.1.4.1.47898.3.1.3.1.2.2 (see details in chapter 7.1.6) [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certdigital.ro/repository	Non-critical
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.certdigital.ro/certdigital-qualifiedg3.crl	Non-critical
Subject Alternative Name	Other Name: RFC822 Name and Principal Name (UPN)	Non-critical
Qualified Certificate Statements	esi4-qcStatement-1: 0.4.0.1862.1.1 esi4-qcStatement-4: 0.4.0.1862.1.4 esi4-qcStatement-6: 0.4.0.1862.1.6 id-etsi-qcs-QcType 1: 0.4.0.1862.1.6.2 esi4-qcStatement-5: 0.4.0.1862.1.5 URL=http://www.certdigital.ro/repository Language=EN	Non-critical

Tabelul 7.5. Certificat calificat pentru sigiliu electronic cu QSCD eliberat persoanelor juridice

Certificatele calificate pentru CertDigital Time Stamping Authority conțin extensii descrise în tabelul 7.6.

Extension	Value or value's constraint	Extension status
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.certdigital.ro [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://certs.certdigital.ro/certdigital-qualifiedg3.crt	Non-critical
Key Usage	digitalSignature (bit 0),nonRepudiation (bit 1)	Critical
Authority Key Identifier	KeyID=18 42 b9 b2 98 54 bd b1 1d 9b a1 68 d3 a4 81 76 2e bb ac b2 0e f5 3f 10 48 fb 87 e9 00 3b 59 24 Certificate Issuer: Directory Address: OU=CertDigital ROOT CA G3 O=Centrul de Calcul S.A. C=RO Certificate SerialNumber=20 11 04 20 93 03 01	Non-critical
Subject Key Identifier	The keyIdentifier is composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).	Non-critical
Certificate Policies	[1]Certificate Policy: Policy Identifier=0.4.0.194112.1.3 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http:/www.certdigital.ro/repository [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.47898.3.1.3.1.2.3.2 [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certdigital.ro/repository	Non-critical
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.certdigital.ro/certdigital-qualifiedg3.crl	Non-critical
Subject Alternative Name	Other Name: RFC822 Name and Principal Name (UPN)	Non-critical
Enhanced Key Usage	Time Stamping (1.3.6.1.5.5.7.3.8)	Non-critical
Qualified Certificate Statements	esi4-qcStatement-1: 0.4.0.1862.1.1 esi4-qcStatement-4: 0.4.0.1862.1.4 esi4-qcStatement-6: 0.4.0.1862.1.6 id-etsi-qcs-QcType 1: 0.4.0.1862.1.6.2 esi4-qcStatement-5: 0.4.0.1862.1.5 URL=http://www.certdigital.ro/repository Language=EN	Non-critical

Tabelul 7.6. Certificat calificat pentru CertDigital Time Stamping Authority

Certificatul OCSP conține extensii descrise în Tabelul 7.7.

Extension	Value or value's constraint	Extension status
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.certdigital.ro [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://certs.certdigital.ro/certdigital-qualifiedg3.crt	Non-critical
Key Usage	digitalSignature (bit 0),nonRepudiation (bit 1)	Critical
Authority Key Identifier	KeyID=18 42 b9 b2 98 54 bd b1 1d 9b a1 68 d3 a4 81 76 2e bb ac b2 0e f5 3f 10 48 fb 87 e9 00 3b 59 24 Certificate Issuer: Directory Address: OU=CertDigital ROOT CA G3 O=Centrul de Calcul S.A. C=RO Certificate SerialNumber=20 11 04 20 93 03 01	Non-critical
Subject Key Identifier	27 42 ae 4d 98 21 00 ae 01 9f 0a 5a ea 52 35 cf 58 93 1b ae fe 4c 9f 68 87 4b a1 9f 9f 53 19 04	Non-critical
Certificate Policies	[1]Certificate Policy: Policy Identifier=0.4.0.194112.1.3 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.certdigital.ro/repository [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.47898.3.1.3.1.2.4.2 [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.certdigital.ro/repository	Non-critical
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.certdigital.ro/certdigital-qualifiedg3.crl	Non-critical
Subject Alternative Name	Other Name: Principal Name=office@certdigital.ro RFC822 Name=office@certdigital.ro	Non-critical
Enhanced Key Usage	OCSP Signing (1.3.6.1.5.5.7.3.9)	Non-critical
OCSPNoCheck	-	Non-critical

Tabelul 7.7. Extensiile certificatelor pentru certificatele OCSP

7.1.3. Identificatori de obiect al algoritmului

Câmpul signatureAlgorithm conține un identificator criptografic algoritmic utilizat pentru semnătură electronică, creat de o Autoritate de Certificare pe certificat. În cazul CertDigital,

algoritmul utilizat este sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11).

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

Identificatorul obiectului politicii certificatului utilizat la nivelul CertDigital QUALIFIED CA G3 sunt descrise în Tabelul 7.8 și Tabelul 7.9.

Certification Policy Name	Policy identifier
CertDigital QUALIFIED CA G3	{CertDigital}.{id-policy}(3).{id-cp}(1).{id-class}(3).***{id-qscdpresense}.{id-keygenerator}.{id-usage}.****{id-persontype}* ID=1.3.6.1.4.1.47898.3.1.3 ***subpolicy ID*** *See below subpolicyID values.*

Tabelul 7.8. Identificatori de politică și numele acestora

CA Level	Tip	OID
CertDigital Qualified CA G3 1.3.6.1.4.1.47898.3.1.3	**Certificat calificat**	***Certificat calificat pentru semnătura electronică*** with QSCD and key generated by the Subject - ▪ 1.3.6.1.4.1.47898.3.1.3.**1.1.1.***{id-persontype}* with QSCD and key generated by the CertDigital – ▪ 1.3.6.1.4.1.47898.3.1.3.**1.2.1.** *{id-persontype}*
		Certificat calificat pentru sigiliu electronic with QSCD and key generated by the Subject – ▪ 1.3.6.1.4.1.47898.3.1.3.**1.1.2.** *{id-persontype}* with QSCD and key generated by the CertDigital – ▪ 1.3.6.1.4.1.47898.3.1.3.**1.2.2.** *{id-persontype}*
		Timestamp server certificate with QSCD and key generated by the CertDigital – ▪ 1.3.6.1.4.1.47898.3.1.3.**1.2.3.***{id-persontype}*

		OCSP certificate with QSCD and key generated by the CertDigital – ▪ 1.3.6.1.4.1.47898.3.1.3.**1.2.4.***{id-persontype}*
{id-persontype} : *1 – Natural person ; 2 – Legal person*		

Tabelul 7.9 Identificatori de obiect pentru politica de certificare

7.1.7. Utilizarea politicii de constrângerii a extensiei

Nu se aplică.

7.1.8. Sintaxa și semantica calificărilor de politică

Certificatele emise de CertDigital conțin un calificativ de politică în cadrul Politicii extensiei certificatului. Această extensie conține un calificativ CPS pointer care indică CPS.

7.1.9. Semantica de procesare a Politicii extinderii critice a certificatului

Nu se aplică.

7.2.Profilul CRL

Profilul CRL este descris în Tabelul 7.10.

Field name	Value or value's constraint	
Version	V2	
Signature Algorithm	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)	
Issuer	OrganizationIdentifier (OID: 2.5.4.97) =	VATRO-2163993
	Common Name (CN) =	CertDigital QUALIFIED CA G3
	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	

Tabelul 7.10 Profil CRL pentru CertDigital QUALIFIED CA G3

7.2.1. Numărul (numerele) versiunii

Toate CRL-urile emise de CertDigital sunt X.509 versiunea 2.

7.2.2. CRL și extensii de intrare CRL

Extensiile CRL pentru CertDigital QUALIFIED CA G3 sunt descrise în Tabelul 7.11.

Extension	Value or Value constraint	Extension status
Authority Key Identifier	KeyID=18 42 b9 b2 98 54 bd b1 1d 9b a1 68 d3 a4 81 76 2e bb ac b2 0e f5 3f 10 48 fb 87 e9 00 3b 59 24 Certificate Issuer: Directory Address: OU=CertDigital ROOT CA G3 O=Centrul de Calcul S.A. C=RO Certificate SerialNumber=20 11 04 20 93 03 01	Non-critic
CRL Number	monotonically increasing sequence number	Non-critic

Tabelul 7.11. Extensii CRL pentru CertDigital QUALIFIED CA G3

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 primește un răspuns semnat cu cheia privată asociată acestui certificat poate avea încredere în starea certificatului 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**.

Informațiile despre starea certificatului sunt incluse în câmpul **certStatus** din structura **SingleResponse**.

Aceasta poate avea una din următoarele trei valori principale:

- GOOD - indică starea valabilă a certificatului
- REVOKED - indică faptul că certificatul a fost emis și revocat sau 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) versiunii

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 :

Nonce – binding a request and a response to prevent reply attacks. **Nonce** is included in **requestExtension** of the **OCSPRequest** and repeated in the field **responseExtension** of the **OCSPResponse)**.

8. Auditul 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 CertDigital QUALIFIED CA G3 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, așa 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 specificate în CPS CertDigital QUALIFIED CA G3.

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 http://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 emis 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 sau reînnoire a certificatului

Prețurile se formează în conformitate cu 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. Rambursarea taxelor

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

9.2.Responsabilitatea financiară

9.2.1. Acoperire de asigurare

CertDigital va acoperi daunele pe care le-ar putea provoca din cauza serviciilor de certificare pentru persoanele care își construiesc moralul asupra efectelor juridice ale certificatelor calificate emise de CertDigital QUALIFIED CA G3 până la echivalentul în lei a sumei de 50.000 euro pentru fiecare risc asigurat. Riscul asigurat reprezintă fiecare prejudiciu cauzat, chiar dacă există mai multe astfel de daune ca urmare a neîndeplinirii de către prestator a obligațiilor prevăzute de lege.

9.2.2. Alte active

Nu se aplică

9.2.3. Asigurarea sau acoperirea garanției pentru entitățile finale

CertDigital beneficiază de asigurare care acoperă datorii profesionale.

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 asociată 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 protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie 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 primirea acesteia de către cealaltă parte contractantă; sau

b) informațiile au fost dezvăluite după obținerea acordului scris al celeilalte părți; sau

c) partea a fost obligata 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),

- Inregistrări ale tranzacțiilor de sistem (toate tipurile de tranzacții, precum și date pentru controlul tranzacțiilor, așa-numitele jurnale de tranzacții de sistem)
- Inregistrarea 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 informațiilor 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 inregistrare ***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 certificatele emise cu un identificator de obiect (OID) au fost emise în conformitate cu procedurile relevante și CPS după cum se aplică la data 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 asociate 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, atunci când este necesar.

9.6.4. Reprezentări și garanții ale părților asociate

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 încrederii față de un certificat CertDigital dacă a fost revocat sau expirat.

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, CRL-urile utilizate în mod necorespunzător.

9.10. Termen și reziliere

9.10.1. Termen

Prezentul 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 perpetua până la terminarea lor în conformitate cu prezenta secțiune 9.10.

9.10.2. Terminare

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 CPS și vor rămâne în vigoare. Responsabilitățile de protejare a informațiilor confidențiale și a informațiilor personale personale trebuie să supraviețuiască 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 a) scrisoare recomandată, b) livrare manuală, c) transmisie facsimilă, considerată primită la livrarea reală sau facsimilă completă sau d) în format electronic, semnată cu o semnătură electronică calificată si să fie adresate 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 Compartimentul Managementul Politicilor și Procedurilor (CMPP) 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. Proceduri de soluționare a 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.

9.17. Alte prevederi

Nu se aplică.