CENTRUL DE CALCUL S.A.

Prestator de servicii de încredere calificat – marca comercială CertDigital

Politica și declarația de practici a serviciului calificat de gestionare la distanță a dispozitivelor calificate de creare a semnăturilor și sigiliilor electronice (PDP-rQSCD)

Remote QSCD Management Service Policy and Practice Statement

Identificator (OID): 1.3.6.1.4.1.47898.11.1 (politica și declarația de practici)

Cod document: PDP-rQSCD · Versiunea: 2.3 · Data: 27.10.2026

Stare: Proiect (Draft) – în pregătire pentru evaluarea conformității

EMISĂ DE		
Departament	Rol / Nume	Data
Securitate și administrare IT – Servicii electronice (CertDigital)	Ofițer de Securitate IT	_____

APROBATĂ DE		
Organism	Rol / Nume	Data
Conducerea CENTRUL DE CALCUL S.A.	Director General	_____

ISTORICUL MODIFICĂRILOR			
Versiune	Autor	Detalii modificări	Data
1.0	Ofițer de Securitate IT	Prima versiune a declarației de practici a serviciului rQSCD (DPP-rQSCD)	08.10.2026
2.0	Ofițer de Securitate IT	Document unic PDP-rQSCD: politica (Partea I) și declarația de practici (Partea a II-a) a serviciului calificat de gestionare la distanță a QSCD; Reg. (UE) 2025/1567, ETSI TS 119 431-1 (EUSPv2); înlocuiește DPP-rQSCD v1.0 și proiectele DPP-rQSCD v1.1 / Politica rQSCD v1.0; temeiul publicării tarifelor: art. 11 alin. (1) și, pentru certificatele calificate, alin. (3) lit. b) din Legea nr. 214/2024	22.10.2026
2.1	Ofițer de Securitate IT	Statutul calificat descris exact: pentru serviciu se solicită acordarea statutului calificat și înscrierea în Lista de încredere a României, iar până la înscriere serviciul nu se prestează ca serviciu calificat (art. 21 alin. (3) din Regulamentul eIDAS); legătura ANPC pentru SAL devine https://anpc.ro/sal; trimiterile la documentele asociate, la versiunile în vigoare	27.10.2026
2.2	Ofițer de Securitate IT	Coperta, antetul și tabelul de identificare arată versiunea și data în vigoare (în versiunea 2.1 rămăseseră cele ale versiunii 2.0); trimiterile la documentele asociate, la versiunile în vigoare (PC v2.1, DPC CERTDIGITAL G4 v2.1, DPC CERTDIGITAL G5 v1.1, PDP-QTST v2.1, TC-CERT v2.1, TC-rQSCD v1.2)	27.10.2026
2.3	Ofițer de Securitate IT	Trimiterile la celelalte documente CertDigital nu mai au număr de versiune: se aplică versiunea în vigoare, publicată la adresa fixă din depozit, iar versiunile anterioare sunt în arhivă	27.10.2026

© Centrul de Calcul S.A. Toate drepturile rezervate. CertDigital este marcă înregistrată a Centrul de Calcul S.A. Orice întrebare referitoare la conținutul acestui document se adresează la office@certdigital.ro.

Cuprins

PARTEA I – Politica serviciului 10
1. Introducere 10
1.1. Prezentare generală 10
1.2. Identificarea documentului 11
1.3. Participanții 12
1.3.1. Prestatorul serviciului (SSASP) 12
1.3.2. Abonatul 13
1.3.3. Semnatarul / creatorul sigiliului 13
1.3.4. Părțile utilizatoare 14
1.3.5. Aplicațiile client și integratorii 14
1.3.6. Terții și subcontractanții 14
1.4. Utilizarea serviciului 14
1.4.1. Serviciile acoperite 14
1.4.2. Utilizări permise 15
1.4.3. Utilizări interzise 15
1.4.4. Limitări 16
1.5. Administrarea documentului 16
1.5.1. Organizația care administrează documentul 16
1.5.2. Datele de identificare și de contact 16
1.5.3. Procedura de aprobare și de revizuire 16
2. Referințe normative 17
2.1. Legislația Uniunii Europene 17
2.2. Legislația națională 17
2.3. Standarde și specificații tehnice 17
3. Definiții și acronime 19
3.1. Definiții 19
3.2. Acronime 20
4. Concepte generale 22
4.1. Serviciul și componentele sale 22
4.2. Dispozitivul calificat la distanță 22
4.3. Controlul exclusiv al semnatarului 22
4.4. Modelele de chei de semnare 23
4.5. Relația cu emiterea certificatelor calificate 23
5. Politica serviciului 24
5.1. Identificare și conformitate 24

5.2. Comunitatea utilizatorilor și aplicabilitatea ... 24
5.3. Modificarea politicii ... 24
6. Cerințele privind practicile ... 25
6.1. Publicare și depozit ... 25
6.2. Generarea cheii de semnare ... 25
6.3. Verificarea identității și legarea mijlocului eID ... 25
6.4. Furnizarea mijlocului eID ... 25
6.5. Legarea certificatului ... 26
6.6. Activarea semnăturii ... 26
6.7. Ștergerea cheii de semnare ... 26
6.8. Copiile de rezervă ... 26
6.9. Blocarea activării și revocarea ... 26
6.10. Controale privind facilitățile, managementul și operarea ... 26
6.11. Controale tehnice ... 27
6.12. Evaluarea conformității ... 27
7. Obligații și răspundere ... 28
7.1. Obligațiile CERTDIGITAL ... 28
7.2. Obligațiile abonatului și ale semnatarului ... 28
7.3. Obligațiile părților care se bazează ... 28
7.4. Răspunderea ... 28
7.5. Asigurarea ... 28
8. Alte aspecte comerciale și juridice ... 30
8.1. Tarife ... 30
8.2. Protecția datelor cu caracter personal ... 30
8.3. Modificări ... 30
8.4. Soluționarea litigiilor ... 30
8.5. Legea aplicabilă și cadrul legal ... 30
8.6. Alte prevederi ... 31
9. Corespondența cu cerințele ETSI TS 119 431-1 și ale Regulamentului (UE) 2025/1567 ... 32
9.1. Tabel de corespondență ... 32
PARTEA A II-A – Declarația de practici ... 33
10. Publicarea și responsabilitățile privind depozitul ... 33
10.1. Depozitul (repository) ... 33
10.2. Publicarea informațiilor ... 33
10.3. Frecvența publicării și disponibilitatea ... 34
10.4. Controlul accesului la depozit ... 34
11. Arhitectura serviciului și componentele acestuia ... 35

11.1. Modelul de referință și nivelul de asigurare a controlului exclusiv 35
11.2. Componentele serviciului conform ETSI TS 119 431-1 36
11.3. Dispozitivul calificat de creare a semnăturii la distanță (rQSCD) 36
11.3.1. Dispozitivul calificat și modulul criptografic 36
11.3.2. Modulul de activare a semnăturii (SAM) 37
11.3.3. Izolarea arhitecturală 38
11.4. Protocolul de activare a semnăturii (SAP) și datele de activare (SAD) 38
11.4.1. Conținutul SAD 38
11.4.2. Fluxul protocolului de activare 39
11.4.3. Proprietăți de securitate ale SAP 40
11.5. Modelele de chei de semnare 40
11.6. Interfețele serviciului și protocoalele de integrare 40
11.6.1. Interfața de semnare la distanță 40
11.6.2. Autentificarea aplicațiilor client și a semnatarilor 41
11.6.3. Integrarea cu portofelul european pentru identitate digitală (EUDIW) 41
11.6.4. Legătura cu serviciile CERTDIGITAL conexe 41
12. Identificarea și autentificarea semnatarului 42
12.1. Înrolarea și înregistrarea 42
12.1.1. Cererea de înrolare 42
12.1.2. Verificarea cererii 42
12.2. Verificarea identității (identity proofing) 42
12.2.1. Nivelul de verificare a identității 42
12.2.2. Metode de verificare a identității acceptate 43
12.2.3. Reutilizarea verificării identității 43
12.2.4. Identitatea pentru cheile de unică folosință 43
12.3. Legarea mijlocului de identificare electronică de cheia de semnare 44
12.3.1. Principiu 44
12.3.2. Nivelul de asigurare al mijlocului eID 44
12.3.3. Protecția legăturilor 44
12.4. Furnizarea mijlocului de identificare electronică de către CERTDIGITAL 44
12.4.1. Aplicația CertDigital ID 44
12.4.2. Înrolarea dispozitivului și datele de activare 45
12.4.3. Gestionarea ciclului de viață al mijlocului eID 45
12.5. Autentificarea delegată și utilizarea mijloacelor eID externe 45
12.6. Legarea certificatului de cheia de semnare 45
13. Ciclul de viață al cheilor de semnare 47
13.1. Generarea cheilor de semnare 47

13.1.1. Mediul de generare 47
13.1.2. Algoritmi și parametri 47
13.1.3. Momentul generării și atributele cheii 47
13.1.4. Dovada de posesie și certificarea 48
13.2. Activarea semnăturii 48
13.2.1. Condiții de activare 48
13.2.2. Prezentarea datelor de semnat și consimțământul (WYSIWYS) 48
13.2.3. Sesiunile de semnare 49
13.2.4. Formate de semnătură și servicii conexe 49
13.3. Utilizarea cheii de semnare 49
13.4. Copiile de siguranță și recuperarea cheilor de semnare 50
13.5. Ștergerea cheilor de semnare 50
13.6. Blocarea activării cheii 51
13.7. Reînnoirea cheilor și schimbarea cheilor 51
14. Controale privind facilitățile, managementul și operarea 52
14.1. Cerințe generale 52
14.1.1. Evaluarea riscurilor 52
14.1.2. Politica de securitate a informației 52
14.1.3. Managementul activelor 53
14.2. Controale de securitate fizică 53
14.2.1. Amplasarea și construcția 53
14.2.2. Zonele de securitate și accesul fizic 53
14.2.3. Controale de mediu 53
14.2.4. Dezafectarea echipamentelor criptografice 54
14.3. Controale procedurale 54
14.3.1. Rolurile de încredere 54
14.3.2. Separarea sarcinilor și controlul multiplu 54
14.3.3. Proceduri operaționale documentate 55
14.4. Controale de personal 55
14.5. Procedurile de jurnalizare a evenimentelor (audit logging) 56
14.5.1. Evenimente jurnalizate 56
14.5.2. Protecția jurnalelor 56
14.6. Arhivarea înregistrărilor 57
14.7. Schimbarea cheilor infrastructurii 57
14.8. Compromiterea, incidentele și recuperarea în caz de dezastru 57
14.8.1. Gestionarea incidentelor de securitate 57
14.8.2. Notificarea organismului de supraveghere și a CSIRT 58

14.8.3. Continuitatea activității și recuperarea în caz de dezastru 59
14.8.4. Compromiterea cheilor infrastructurii 59
14.9. Încetarea serviciului 59
14.9.1. Planul de încetare 59
14.9.2. Procedurile de încetare 60
15. Controale tehnice de securitate 61
15.1. Managementul sistemelor și al securității 61
15.2. Sisteme și operațiuni 61
15.3. Controale de securitate ale calculatoarelor 61
15.4. Controale de securitate ale ciclului de viață 62
15.4.1. Dezvoltarea și achiziția sistemelor 62
15.4.2. Gestionarea schimbărilor și a vulnerabilităților 62
15.4.3. Lanțul de aprovizionare 63
15.5. Controale de securitate a rețelei 64
15.6. Controale criptografice 64
15.7. Sincronizarea timpului 65
16. Evaluarea conformității și auditul 66
16.1. Evaluarea conformității de către organismul de evaluare a conformității 66
16.2. Auditul intern 66
16.3. Pre-audituri și teste de pregătire 66
16.4. Supravegherea de către ADR 67
17. Profilurile certificatelor, ale datelor de activare și ale semnăturilor 68
17.1. Profilul certificatelor calificate asociate cheilor rQSCD 68
17.2. Profilul datelor de activare a semnăturii (SAD) 68
17.3. Profilul aserțiunilor de autentificare 68
17.4. Profilurile semnăturilor create 68
17.5. Profilul CRL și OCSP 69
18. Alte aspecte de afaceri și juridice 70
18.1. Tarife 70
18.2. Răspunderea financiară și asigurarea 70
18.3. Confidențialitatea informațiilor de afaceri 70
18.4. Protecția datelor cu caracter personal 71
18.5. Drepturile de proprietate intelectuală 71
18.6. Declarații, garanții și obligații ale participanților 72
18.6.1. Obligațiile CERTDIGITAL 72
18.6.2. Obligațiile abonatului și ale semnatarului 72
18.6.3. Obligațiile integratorilor (aplicații client) 73

18.6.4. Obligațiile părților utilizatoare 73
18.6.5. Obligațiile organizațiilor externe care sprijină serviciul 73
18.7. Exonerări de garanții 73
18.8. Limitarea răspunderii 73
18.9. Despăgubiri 74
18.10. Durata și încetarea 74
18.11. Notificări individuale și comunicarea cu participanții 74
18.12. Modificări 74
18.13. Soluționarea disputelor și reclamațiile 74
18.14. Legea aplicabilă și conformitatea cu legislația 74
18.15. Termenii și condițiile 75
18.16. Accesibilitatea pentru persoanele cu dizabilități 75
19. Administrarea documentului 76
19.1. Procedura de modificare 76
19.2. Mecanismul de publicare și notificare 76
19.3. Procedura de aprobare 76
19.4. Documente asociate 77
Anexa A – Matricea de conformitate cu ETSI TS 119 431-1 V1.3.1 (EUSPv2) și Regulamentul (UE) 2025/1567 78
Anexa B – Corespondența cu Regulamentul (UE) nr. 910/2014 modificat prin Regulamentul (UE) 2024/1183 81
Anexa C – Documentele interne asociate 82

PARTEA I – Politica serviciului

1. Introducere

1.1. Prezentare generală

Prezentul document stabilește cerințele și descrie practicile pe care CENTRUL DE CALCUL S.A. (marca CertDigital, denumită în continuare „CERTDIGITAL”), prestator de servicii de încredere calificat, le aplică la prestarea serviciilor calificate de **gestionare la distanță a dispozitivelor calificate de creare a semnăturilor electronice** și, mutatis mutandis, **a sigiliilor electronice** (serviciul rQSCD), astfel cum sunt definite la art. 3 pct. 23a și 31a, art. 29 alin. (1a), art. 29a și art. 39a din Regulamentul (UE) nr. 910/2014, modificat prin Regulamentul (UE) 2024/1183 (denumit în continuare „Regulamentul eIDAS”).

Serviciul permite semnatarilor să creeze semnături și sigilii electronice calificate cu chei de semnare generate, păstrate și utilizate de CERTDIGITAL într-un dispozitiv calificat de creare a semnăturilor aflat în centrele de date ale CERTDIGITAL (QSCD la distanță), **în numele semnatarului și sub controlul exclusiv al acestuia** (pentru sigilii: sub controlul creatorului sigiliului). În terminologia ETSI, serviciul este un serviciu de aplicație de semnare pe server (**Server Signing Application Service – SSAS**), iar CERTDIGITAL acționează ca prestator al acestuia (**Server Signing Application Service Provider – SSASP**). Serviciul este compus dintr-o aplicație de semnare pe server (Server Signing Application – SSA), un modul de activare a semnăturii (Signature Activation Module – SAM) și un dispozitiv calificat de creare a semnăturii electronice (QSCD) operat la distanță, pe seama semnatarului, într-un mediu protejat împotriva manipulării.

Documentul are două părți. Partea I (capitolele 1–9) cuprinde politica serviciului și stabilește **ce** garantează CERTDIGITAL. Partea a II-a (capitolele 10–19 și anexele A–C) este declarația de practici a serviciului (Trust Service Practice Statement – TSPS, respectiv SSAS Practice Statement în terminologia ETSI TS 119 431-1) și descrie **cum** sunt îndeplinite cerințele: practicile, procedurile și controalele pe care CERTDIGITAL le aplică pentru a îndeplini cerințele politicii **EU SSAS Policy v2 (EUSPv2)** definite în ETSI TS 119 431-1 V1.3.1 (2024-12), anexa A, astfel cum este referită, cu adaptări, în anexa la Regulamentul de punere în aplicare (UE) 2025/1567, precum și cerințele generale aplicabile prestatorilor de servicii de încredere calificate prevăzute de ETSI EN 319 401 V3.1.1 și de Regulamentul de punere în aplicare (UE) 2025/2530. În caz de neconcordanță între cele două părți, prevalează Partea I. Pentru certificatele calificate asociate cheilor se aplică DPC CERTDIGITAL G4 (certificatele emise de CERTDIGITAL QUALIFIED CA G4) sau DPC CERTDIGITAL G5 (certificatele emise de CERTDIGITAL QCA G5); trimiterile din prezentul document la secțiuni ale DPC CERTDIGITAL G4 se aplică certificatelor emise de CERTDIGITAL QCA G5 prin secțiunile corespunzătoare ale DPC CERTDIGITAL G5. Pentru cerințele comune tuturor serviciilor se aplică Politicile generale CertDigital (PG).

Scopul documentului este triplu:

– să constituie **referința operațională** pe baza căreia CERTDIGITAL implementează, menține și îmbunătățește serviciul rQSCD;

– să furnizeze **organismului de evaluare a conformității (CAB)** și **Autorității pentru Digitalizarea României (ADR)**, în calitate de organism de supraveghere, dovezile documentare necesare evaluării conformității serviciului calificat RemoteQSigCDManagement/Q și RemoteQSealCDManagement/Q, înscris în Lista de încredere (Trusted List) a României;

– să informeze **abonații, semnatarii și părțile utilizatoare** cu privire la modul în care sunt generate, protejate, activate și distruse datele de creare a semnăturii electronice gestionate pe seama lor, astfel încât aceștia să poată evalua nivelul de încredere al serviciului.

Notă privind structura: Partea a II-a este structurată în conformitate cu cadrul IETF RFC 3647, astfel cum este instanțiat de ETSI TS 119 431-1 (clauzele 5 și 6 și anexa A), care încorporează prin referință cerințele ETSI EN 319 401 și ale CEN EN 419 241-1. Fiecare secțiune a Părții a II-a indică, între paranteze, identificatorii cerințelor ETSI/CEN pe care le acoperă, pentru a facilita trasabilitatea în cadrul auditului. Matricea completă de conformitate este prezentată în Anexa A, iar corespondența cerințelor cu Partea I, în capitolul 9.

1.2. Identificarea documentului

Element	Valoare
Titlu	Politica și declarația de practici a serviciului calificat de gestionare la distanță a dispozitivelor calificate de creare a semnăturilor și sigiliilor electronice CertDigital (PDP-rQSCD)
Denumirea în limba engleză	CertDigital Remote QSCD Management Service Policy and Practice Statement
Cod	PDP-rQSCD
Versiune / data	2.3 / 27.10.2026
Identificatorul documentului și al politicii (OID)	1.3.6.1.4.1.47898.11.1
OID – chei de semnare de lungă durată	1.3.6.1.4.1.47898.11.1.1; inclus în certificatele cheilor gestionate prin serviciu
OID – chei de semnare de unică folosință	1.3.6.1.4.1.47898.11.1.2 – planificat; modelul nu se oferă la data prezentei versiuni
OID 1.3.6.1.4.1.47898.11.2	nu se mai folosește: declarația de practici este inclusă în prezentul document (Partea a II-a)
Politica ETSI respectată	EUSPv2 – EU SSAS Policy v2, ETSI TS 119 431-1 V1.3.1, anexa A: itu-t(0) identified-organization(4) etsi(0) signature-creation-service-policies(19431) ops(1) policy-identifiers(1) eu-remote-qscd-v2(4), respectiv OID **0.4.0.19431.1.1.4**, inclus și în certificatele cheilor gestionate prin serviciu
Tipuri de servicii (ETSI TS 119 612)	`http://uri.etsi.org/TrstSvc/Svctype/RemoteQSigCDManagement/Q` și `http://uri.etsi.org/TrstSvc/Svctype/RemoteQSealCDManagement/Q`
Identitatea serviciilor în Lista de încredere (după înscriere)	certificatele CERTDIGITAL QUALIFIED CA G4 și CERTDIGITAL QCA G5
Generații	serviciul se prestează în generațiile G4 și G5 ale infrastructurii CERTDIGITAL: certificatele asociate cheilor sunt emise de CERTDIGITAL QUALIFIED CA G4 (DPC CERTDIGITAL G4) și de CERTDIGITAL QCA G5 (DPC CERTDIGITAL G5, secțiunile 1.2 și 7.1.2)

Element	Valoare
Publicat la	https://www.certdigital.ro/repository/politici/certdigital_pdp-rqscd_ro.pdf; versiunile anterioare: https://www.certdigital.ro/repository/arhiva/
Documente înlocuite	Declarația de practici pentru serviciul de gestionare la distanță a rQSCD (DPP-rQSCD) v1.0, cod CD_SI_013_DPP-rQSCD; proiectele neaprobate DPP-rQSCD v1.1 și Politica serviciului de gestionare la distanță a QSCD (Politica rQSCD) v1.0, unite în prezentul document

Arcul OID **1.3.6.1.4.1.47898** este arcul de întreprindere alocat de IANA societății CENTRUL DE CALCUL S.A. Sub-arcul **.11** este alocat serviciului de gestionare la distanță a QSCD (CERTDIGITAL_OID_MAP): .11.1 – prezentul document (politica și declarația de practici a serviciului); .11.1.1 – chei de semnare de lungă durată; .11.1.2 – chei de semnare de unică folosință (planificat); .11.2 – nefolosit (fostul identificator al declarației de practici, inclusă acum în Partea a II-a).

În certificatul de serviciu QEArch G4 (seria hex. 2011042094040107), care se revocă, identificatorul 1.3.6.1.4.1.47898.11.1 are sensul din numerotarea anterioară a arcurilor (politica serviciului de arhivare electronică), conform CERTDIGITAL_OID_MAP, secțiunea 18; el nu se referă la prezentul serviciu.

Certificatele calificate emise de CERTDIGITAL QUALIFIED CA G4 și de CERTDIGITAL QCA G5 pentru cheile gestionate prin serviciu conțin, în extensia certificatePolicies: QCP-n-qscd (0.4.0.194112.1.2) pentru semnătură sau QCP-l-qscd (0.4.0.194112.1.3) pentru sigiliu; identificatorul CERTDIGITAL `1.3.6.1.4.1.47898.4.2.2.{identificare}.{tip subiect}` (G4), respectiv `1.3.6.1.4.1.47898.5.2.2.{identificare}.{tip subiect}` (G5) (dispozitiv 2 = QSCD gestionat de CERTDIGITAL; cheie generată de CERTDIGITAL); identificatorul 1.3.6.1.4.1.47898.11.1.1; și identificatorul politicii EUSPv2 (0.4.0.19431.1.1.4). În extensia qcStatements, certificatele conțin declarația QcSSCD (0.4.0.1862.1.4), conform ETSI EN 319 411-2 și ETSI EN 319 412-5 (secțiunea 17.1).

1.3. Participanții

1.3.1. Prestatorul serviciului (SSASP)

CENTRUL DE CALCUL S.A. (marca CertDigital), persoană juridică română, cu datele de identificare din secțiunea 1.5.2, este prestator de servicii de încredere calificat înscris în Lista de încredere a României și poartă **responsabilitatea integrală** pentru conformitatea serviciului rQSCD cu Regulamentul eIDAS, cu Legea nr. 214/2024 și cu prezentul document, inclusiv atunci când anumite componente sunt furnizate de terți; CERTDIGITAL răspunde în ansamblu de serviciu (ETSI TS 119 431-1: OVR-5.3.1-01).

În cadrul serviciului, CERTDIGITAL îndeplinește următoarele funcții:

– **operator al dispozitivului calificat la distanță** (Ascertia ADSS Server SAM Appliance v7.0.2, cu modulul criptografic Utimaco CryptoServer CP5 Se500, secțiunea 11.3), în centrele de date proprii din Târgu Jiu;

– **serviciul de generare a cheilor de semnare** (Signing Key Generation Service – GEN);

– **serviciul de legare a certificatului și a mijlocului de identificare electronică** (Certificate / eID means Linking Service – LNK);

– **serviciul de activare a semnăturii** (Signature Activation Service – SIG);

– **serviciul de ștergere a cheilor de semnare** (Signing Key Deletion Service – DEL);

– **serviciul de furnizare a mijloacelor de identificare electronică** (eID Means Provision Service – EID), prin aplicația mobilă CertDigital ID;

– **autoritate de certificare** pentru certificatele calificate asociate cheilor gestionate (CERTDIGITAL QUALIFIED CA G4 și CERTDIGITAL QCA G5), conform Declarației practicilor de certificare a CERTDIGITAL ROOT CA G4 și CERTDIGITAL QUALIFIED CA G4 (DPC CERTDIGITAL G4), respectiv DPC CERTDIGITAL G5, și Politicii serviciilor de certificare CertDigital;

– **autoritate de înregistrare**, cu verificarea identității prin prezență fizică sau prin soluția CERTDIGITAL KYC (secțiunea 12.2);

– **autoritate de marcare temporală calificată** (CertDigital TSA) pentru mărcile temporale incluse în semnăturile create.

1.3.2. Abonatul

Abonatul este persoana fizică sau juridică ce încheie cu CERTDIGITAL contractul de furnizare a serviciului (Termeni și condiții) și care răspunde de respectarea obligațiilor contractuale. Abonatul poate fi:

– semnatarul însuși (persoană fizică);

– o persoană juridică (angajator, instituție, organizație) care contractează serviciul pentru semnatarii pe care îi desemnează (angajați, reprezentanți);

– o persoană juridică titulară a unui sigiliu electronic calificat;

– un integrator / parte utilizatoare care oferă semnarea în propriile fluxuri de afaceri (de exemplu, platforme de contractare, bănci, instituții publice), caz în care abonatul rămâne semnatarul, iar integratorul acționează în calitate de **aplicație client autorizată** (Signature Creation Application – SCA) conform secțiunii 11.6.

Relația dintre abonat și semnatar este echivalentă cu relația dintre abonat și subiect descrisă în ETSI EN 319 411-1, clauza 5.4.2 (ETSI TS 119 431-1: clauza 5.3.2).

1.3.3. Semnatarul / creatorul sigiliului

Semnatarul este persoana fizică ale cărei date de creare a semnăturii electronice (cheia privată de semnare) sunt generate și gestionate de CERTDIGITAL în rQSCD, pe seama sa, și care deține **controlul exclusiv** asupra utilizării acestora, la nivelul de asigurare SCAL2 definit în CEN EN 419 241-1. Semnatarul poate fi:

– o persoană fizică acționând în nume propriu;

– o persoană fizică identificată în asociere cu o persoană juridică (reprezentant, angajat), caz în care certificatul calificat conține atributele organizației conform ETSI EN 319 412-2.

Creatorul sigiliului este persoana juridică pe seama căreia sunt gestionate datele de creare a sigiliului electronic, reprezentată de persoanele desemnate de aceasta; controlul asupra activării este exercitat de persoana (persoanele) fizice autorizate de persoana juridică, înregistrate de CERTDIGITAL la înrolare, conform secțiunii 12.2.2. În cazul sigiliilor, termenul „control exclusiv” se citește „control”, conform CEN EN 419 241-1, clauza 5.3 (ETSI TS 119 431-1: SIG-A.6-07A).

1.3.4. Părțile utilizatoare

Părțile utilizatoare (relying parties; părțile care se bazează) sunt persoanele fizice sau juridice care se bazează pe semnăturile electronice calificate sau pe sigiliile electronice calificate create prin intermediul serviciului rQSCD. Acestea pot valida semnăturile utilizând certificatul calificat al semnatarului, informațiile de stare (CRL/OCSP) publicate de CERTDIGITAL și serviciul de validare CertDigital. Părțile utilizatoare nu intră într-o relație contractuală directă cu serviciul rQSCD; informațiile relevante pentru acestea sunt publicate în depozit (secțiunea 10).

1.3.5. Aplicațiile client și integratorii

Aplicația client (Signature Creation Application – SCA) este componenta software, operată de CERTDIGITAL sau de un integrator autorizat prin contract, care pregătește documentul de semnat, calculează reprezentarea datelor de semnat (DTBS/R) și o transmite serviciului prin interfața de semnare la distanță (secțiunea 11.6). Aplicațiile client ale integratorilor sunt înregistrate, autentificate și autorizate individual și nu au niciodată acces la datele de activare a semnăturii (SAD) sau la cheile de semnare.

1.3.6. Terții și subcontractanții

CERTDIGITAL poate utiliza terți pentru furnizarea unor componente sau servicii-suport (de exemplu, producătorul dispozitivului calificat și al modulului criptografic, furnizorii de conectivitate și de componente software). În toate cazurile, CERTDIGITAL **păstrează responsabilitatea integrală** și se asigură, prin contracte, acorduri de nivel de serviciu și evaluări de furnizori (secțiunea 15.4.3), că terții respectă cerințele aplicabile ale prezentului document (ETSI TS 119 431-1: OVR-5.3.1-01; ETSI EN 319 401: clauza 7.14). Obligațiile organizațiilor externe care sprijină serviciul sunt identificate în secțiunea 18.6 (ETSI EN 319 401: REQ-6.1-04). CERTDIGITAL nu deleagă către terți verificarea identității, autentificarea semnatarilor sau operarea dispozitivului.

1.4. Utilizarea serviciului

1.4.1. Serviciile acoperite

Prezentul document acoperă următoarele servicii de încredere calificate, înscrise sau solicitate a fi înscrise în Lista de încredere:

Nr.	Serviciu	Identificator tip serviciu (ETSI TS 119 612)	Politica aplicabilă
1	Gestionarea calificată la distanță a dispozitivelor calificate de creare a semnăturilor electronice	http://uri.etsi.org/TrstSvc/Svctype/RemoteQSigCDManagement/Q	EUSPv2; prezentul document (1.3.6.1.4.1.47898.11.1)
2	Gestionarea calificată la distanță a dispozitivelor calificate de creare a sigiliilor electronice	http://uri.etsi.org/TrstSvc/Svctype/RemoteQSealCDManagement/Q	EUSPv2 (mutatis mutandis, art. 39a); prezentul document (1.3.6.1.4.1.47898.11.1)

Serviciul oferă **chei de semnare de lungă durată** (long-term signing keys), generate în rQSCD la înrolare, asociate unui certificat calificat cu valabilitate de cel mult 3 ani și utilizate în mai multe sesiuni de semnare, pe baza autentificării semnatarului cu mijlocul de identificare electronică legat de cheie.

Modelul cheilor de semnare de unică folosință (one-time signing keys) nu se oferă la data prezentei versiuni; identificatorul 1.3.6.1.4.1.47898.11.1.2 este planificat, iar practicile aplicabile acestui model (ETSI TS 119 431-1: GEN-6.2.1-09, LNK-6.2.2-00, LNK-6.2.2-03B, SIG-6.3.1-11 ÷ SIG-6.3.1-16, SIG-A.5-09, DEL-6.3.2-05) se vor descrie într-o versiune ulterioară, înainte de oferirea lui.

Generațiile în care se prestează serviciul sunt indicate în secțiunea 1.2, iar statutul calificat, în secțiunea 5.1.

1.4.2. Utilizări permise

Cheile de semnare gestionate prin serviciu pot fi utilizate exclusiv pentru:

– crearea de **semnături electronice calificate** de către persoane fizice, în formatele AdES baseline (PAdES, XAdES, CAdES, JAdES și containere ASiC) conform Regulamentului de punere în aplicare (UE) 2026/248;

– crearea de **sigilii electronice calificate** de către persoane juridice, în aceleași formate;

– semnarea reprezentărilor datelor de semnat (hash) transmise de aplicațiile client autorizate, în cadrul sesiunilor de semnare autorizate explicit de semnatar.

Cheile se utilizează numai pe baza reprezentării datelor de semnat aprobate explicit de semnatar. Orice altă utilizare este interzisă.

1.4.3. Utilizări interzise

– utilizarea cheilor de semnare în alte scopuri decât cele pentru care semnatarul și-a exprimat consimțământul (ETSI TS 119 431-1: SIG-6.3.1-09);

– utilizarea cheilor de semnare pentru autentificare sau criptare (cheile rQSCD au exclusiv utilizarea nonRepudiation / contentCommitment);

– exportul, copierea sau transferul cheilor de semnare în afara rQSCD, cu excepția copiilor de siguranță realizate în condițiile art. 29a alin. (1) lit. (b) din Regulamentul eIDAS (secțiunea 13.4);

– utilizarea serviciului de către persoane neidentificate sau prin mijloace de identificare electronică nelegate de cheia de semnare;

– utilizarea serviciului de către agenți software autonomi, roboți sau sisteme care ar exclude intervenția explicită a semnatarului în autorizarea fiecărei sesiuni de semnare;

– utilizarea în aplicații în care eșecul serviciului ar putea pune în pericol viața, sănătatea sau mediul, fără măsuri suplimentare de siguranță convenite contractual.

1.4.4. Limitări

Serviciul nu include validarea semnăturilor (acoperită de serviciul de validare CertDigital), păstrarea pe termen lung (acoperită de CertDigital QPS) și nici emiterea certificatelor calificate, care este reglementată de Declarația practicilor de certificare a CERTDIGITAL ROOT CA G4 și CERTDIGITAL QUALIFIED CA G4 (DPC CERTDIGITAL G4) și de DPC CERTDIGITAL G5. Interacțiunile dintre aceste servicii sunt descrise în secțiunea 11.

1.5. Administrarea documentului

1.5.1. Organizația care administrează documentul

Prezentul document este administrat de CENTRUL DE CALCUL S.A. Autoritatea finală pentru aprobarea politicii și a declarației de practici a serviciului este **Directorul General**; documentul este elaborat și verificat de Ofițerul de Securitate IT (ETSI EN 319 401: REQ-6.1-06; ETSI TS 119 431-1: OVR-7-04). Prezentul document este redactat în limba română; în caz de neconcordanță cu o traducere, prevalează versiunea în limba română.

1.5.2. Datele de identificare și de contact

Element	Informație
Prestatorul	CENTRUL DE CALCUL S.A. (marca CertDigital), persoană juridică română, Str. Tudor Vladimirescu nr. 17, Târgu Jiu, județul Gorj, cod poștal 210132, România; înregistrată la Registrul Comerțului sub nr. J1991000103187; EUID ROONRC.J1991000103187; CUI RO2163993
Responsabil de document	Ofițer de Securitate IT – [redacted]
E-mail	office@certdigital.ro
Telefon	+40 253 214 767; [redacted]
Site web	https://www.certdigital.ro/
Program	Luni – Vineri, 09:00 – 17:00 (suport tehnic pentru incidente de securitate: 24/7, conform secțiunii 14.8)

1.5.3. Procedura de aprobare și de revizuire

Documentul este elaborat și verificat de Ofițerul de Securitate IT și aprobat de Directorul General. Documentul este revizuit **cel puțin anual** și ori de câte ori intervin modificări legislative, ale standardelor de referință, ale arhitecturii tehnice sau ale rezultatelor evaluării riscurilor. Procedura de modificare, publicare și notificare este descrisă în secțiunea 19 (ETSI EN 319 401: REQ-6.1-08 ÷ REQ-6.1-10).

2. Referințe normative

2.1. Legislația Uniunii Europene

Act normativ	Relevanță pentru serviciu
Regulamentul (UE) nr. 910/2014 (eIDAS), modificat prin Regulamentul (UE) 2024/1183	Art. 3 (definiții), art. 13 (răspundere), art. 19a, 20, 21 (supraveghere, evaluarea conformității, autorizare), art. 24 (cerințe QTSP), art. 29, inclusiv alin. (1a), art. 29a (serviciul calificat de gestionare a rQSCD), art. 30 și 31 (certificarea QSCD și lista dispozitivelor certificate), art. 39, 39a (sigilii), anexa II
Regulamentul de punere în aplicare (UE) 2025/1567	Standardele de referință pentru gestionarea rQSCD: ETSI TS 119 431-1 V1.3.1, EUSPv2 (anexa A), cu adaptări; aplicabil de la 19.08.2027
Regulamentul de punere în aplicare (UE) 2025/2530	Cerințe pentru QTSP (art. 24 alin. (5)): notificări, cadrul de gestionare a riscurilor, planul de încetare, standardele de referință (ETSI EN 319 401)
Regulamentul de punere în aplicare (UE) 2025/1566	Standardele de referință pentru verificarea identității (ETSI TS 119 461) – aplicabil de la 19.08.2027
Regulamentul de punere în aplicare (UE) 2025/1943	Standardele de referință pentru certificatele calificate (ETSI EN 319 411-2, 319 412-x)
Regulamentul de punere în aplicare (UE) 2025/1929	Mărci temporale calificate (ETSI EN 319 421/422)
Regulamentul de punere în aplicare (UE) 2026/248	Formatele semnăturilor și sigiliilor electronice avansate (XAdES, CAdES, PAdES, JAdES, ASiC)
Decizia de punere în aplicare (UE) 2016/650	Standardele pentru evaluarea securității QSCD (ISO/IEC 15408, EN 419 211)
Regulamentul de punere în aplicare (UE) 2025/2162	Acreditarea organismelor de evaluare a conformității (EN ISO/IEC 17065 + ETSI EN 319 403-1)
Directiva (UE) 2022/2555 (NIS2) și Regulamentul de punere în aplicare (UE) 2024/2690	Măsurile de gestionare a riscurilor de securitate cibernetică și raportarea incidentelor, aplicabile QTSP ca entități esențiale
Regulamentul (UE) 2016/679 (GDPR)	Protecția datelor cu caracter personal ale semnatarilor
Regulamentul de punere în aplicare (UE) 2024/482 (EUCC), modificat prin (UE) 2024/3144	Schema europeană de certificare a securității cibernetice bazată pe Common Criteria

2.2. Legislația națională

Act normativ	Relevanță
Legea nr. 214/2024 privind utilizarea semnăturii electronice, a mărcii temporale și prestarea serviciilor de încredere bazate pe acestea	Cadrul intern de aplicare a Regulamentului eIDAS; desemnarea ADR ca organism de supraveghere; obligațiile și sancțiunile aplicabile prestatorilor
Ordinul ministrului economiei, digitalizării, antreprenoriatului și turismului (MEDAT) nr. 102/2026	Procedura de acordare, suspendare și retragere a statutului de prestator de servicii de încredere calificate (anexa nr. 1); documentele dosarului de acreditare (art. 5 alin. (2))
Legea nr. 190/2018	Măsuri de punere în aplicare a GDPR
OUG nr. 155/2024 (transpunerea Directivei NIS2)	Securitatea cibernetică a rețelelor și sistemelor informatice; CENTRUL DE CALCUL S.A. este entitate esențială (Decizia DNSC nr. 50163/14.11.2025, Registrul entităților E-210D02); raportarea incidentelor către DNSC

2.3. Standarde și specificații tehnice

Standard	Versiune	Obiect

Standard	Versiune	Obiect
ETSI TS 119 431-1	V1.3.1 (2024-12)	Cerințe de politică și securitate pentru TSP care operează un QSCD/SCDev la distanță – **standard principal al serviciului**; politica EUSPv2 (anexa A)
ETSI TS 119 431-2	ediția în vigoare	Componente de serviciu TSP care sprijină crearea semnăturilor digitale AdES
ETSI TS 119 432	ediția în vigoare	Protocoale pentru crearea la distanță a semnăturilor digitale
ETSI EN 319 401	V3.1.1 (2024-06)	Cerințe generale de politică pentru TSP (încorporate prin referință)
ETSI EN 319 411-1 / 411-2	V1.5.1 (2025-04) / V2.6.1	Cerințe pentru TSP care emit certificate (generale / calificate)
ETSI EN 319 412-1, -2, -3, -5	curente	Profilurile certificatelor
ETSI TS 119 461	V2.1.1 (2025-02)	Verificarea identității subiecților serviciilor de încredere (LoIP extins)
ETSI EN 319 403-1	V2.3.1	Cerințe pentru CAB care evaluează TSP
ETSI TS 119 612	V2.4.1 (2025-08)	Liste de încredere
CEN EN 419 241-1	2018	Trustworthy Systems Supporting Server Signing – Part 1: General System Security Requirements (SCAL1/SCAL2): sisteme de încredere pentru semnarea pe server
CEN EN 419 241-2	2019	Protection Profile for QSCD for Server Signing (SAM): profilul de protecție pentru QSCD pentru semnarea pe server
CEN EN 419 221-5	2018	Protection Profiles for TSP Cryptographic Modules – Part 5: Cryptographic Module for Trust Services: module criptografice pentru servicii de încredere
ISO/IEC 15408 (părțile 1–5)	2022	Common Criteria
ISO/IEC 27001 / 27002 / 27005	2022	Managementul securității informației și al riscurilor
ENISA – Agreed Cryptographic Mechanisms (ECCG)	ediția curentă	Algoritmi și lungimi de cheie acceptate (OVR-6.8.5-02, Reg. 2025/1567)
Cloud Signature Consortium – CSC API	v2	Specificația API pentru semnarea la distanță (secțiunea 11.6.1)
IETF RFC 3647, RFC 5280, RFC 6960	–	Cadrul declarațiilor de practici; profilul certificatelor și al CRL; protocolul OCSP

Lista completă a actelor normative și a standardelor aplicate este în documentul 00n și în DPC CERTDIGITAL G4, secțiunea 9.15.

Precizare privind aplicabilitatea în timp: Regulamentul de punere în aplicare (UE) 2025/1567 se aplică de la 19 august 2027. CERTDIGITAL adoptă voluntar, de la data intrării în vigoare a prezentului document, standardele și adaptările prevăzute de acesta, astfel încât serviciul să fie evaluat de la început în raport cu cerințele definitive ale cadrului eIDAS 2.0.

3. Definiții și acronime

3.1. Definiții

Termen	Definiție
Abonat	Persoana fizică sau juridică ce a încheiat cu CERTDIGITAL contractul privind furnizarea serviciului rQSCD.
Aplicație client (SCA)	Signature Creation Application: aplicația care pregătește documentul, calculează DTBS/R și apelează serviciul de semnare, operată de CERTDIGITAL sau de un integrator autorizat.
Aplicație de semnare pe server (SSA)	Server Signing Application: componenta serverului care primește cererile de semnare, orchestrează autentificarea, prezentarea datelor de semnat și transmiterea SAD către SAM.
Cheie de semnare	Cheia privată a semnatarului, păstrată și utilizată în QSCD-ul la distanță.
Cheie de semnare de unică folosință	Cheie de semnare generată, certificată, utilizată și distrusă pe baza unei singure autorizări, în cadrul unei singure sesiuni de semnare (model neoferit la data prezentei versiuni).
Componenta de interacțiune cu semnatarul (SIC)	Signer Interaction Component: componenta aflată sub controlul semnatarului (aplicația mobilă CertDigital ID) prin care semnatarul se autentifică, vizualizează datele de semnat și își exprimă consimțământul, generând SAD.
Control exclusiv (sole control)	Capacitatea semnatarului de a utiliza datele de creare a semnăturii electronice cu un nivel ridicat de încredere că acestea sunt utilizate numai sub controlul său, conform CEN EN 419 241-1 (SCAL2): cheia de semnare poate fi activată numai de semnatar (pentru sigilii: sub controlul creatorului sigiliului).
Date de activare a semnăturii (SAD)	Signature Activation Data: setul de date care leagă criptografic autentificarea semnatarului, cheia de semnare și DTBS/R și prin care semnatarul autorizează SAM să activeze cheia de semnare pentru o operațiune de semnare determinată.
Date de creare a semnăturii electronice	Date unice (cheia privată de semnare) utilizate de semnatar pentru crearea semnăturii electronice (art. 3 pct. 13 din Regulamentul eIDAS).
Dispozitiv calificat de creare a semnăturii electronice (QSCD)	Dispozitiv de creare a semnăturii electronice care îndeplinește cerințele din anexa II la Regulamentul eIDAS și este certificat conform art. 30.
Dispozitiv calificat de creare a semnăturii electronice la distanță (rQSCD)	QSCD gestionat de un prestator de servicii de încredere calificat în conformitate cu art. 29a din Regulamentul eIDAS, pe seama semnatarului.
DTBS/R	Data To Be Signed Representation: reprezentarea datelor de semnat (de regulă valoarea hash a documentului sau a structurii de semnătură) transmisă rQSCD pentru calculul valorii semnăturii.
Mijloc de identificare electronică (eID means)	Unitate materială și/sau imaterială care conține date de identificare personală și care este utilizată pentru autentificare în cadrul unui serviciu online (art. 3 pct. 2 din Regulamentul eIDAS). Mijlocul eID al semnatarului este mijlocul cu care acesta se autentifică la activarea semnăturii; pentru serviciul CERTDIGITAL, aplicația mobilă CertDigital ID.

Termen	Definiție
Modul criptografic (HSM)	Hardware Security Module: dispozitivul hardware în care sunt generate, stocate și utilizate cheile de semnare; certificat conform CEN EN 419 221-5.
Modul de activare a semnăturii (SAM)	Signature Activation Module: componenta dispozitivului calificat care, în mediul protejat al acestuia, validează SAD și autorizează utilizarea cheii de semnare exclusiv pentru DTBS/R autorizate (CEN EN 419 241-2).
Nivel de asigurare a controlului exclusiv (SCAL)	Sole Control Assurance Level, definit în CEN EN 419 241-1: SCAL1 (autorizare de către SSA) și SCAL2 (autorizare de către SAM în mediu protejat, pe baza SAD). Serviciul CERTDIGITAL operează exclusiv la SCAL2.
Organism de evaluare a conformității (CAB)	Organism acreditat conform Regulamentului (CE) nr. 765/2008 și Regulamentului de punere în aplicare (UE) 2025/2162 (EN ISO/IEC 17065 + ETSI EN 319 403-1) care evaluează conformitatea prestatorilor de servicii de încredere calificate.
Organism de supraveghere	Autoritatea pentru Digitalizarea României (ADR), conform Legii nr. 214/2024.
Parte utilizatoare (parte care se bazează)	Persoana fizică sau juridică ce se bazează pe o semnătură sau pe un sigiliu electronic creat prin intermediul serviciului.
Protocol de activare a semnăturii (SAP)	Signature Activation Protocol: protocolul prin care SAD sunt colectate de la semnatar, protejate și transmise către SAM.
Referință a mijlocului eID	Datele utilizate de SSAS pentru a face referire la mijlocul de identificare electronică al semnatarului în scopul autentificării (de exemplu, cheia publică a dispozitivului mobil înrolat).
Rol de încredere	Funcție în cadrul CERTDIGITAL care implică acces la sistemele sau informațiile critice ale serviciului și care este supusă cerințelor de verificare, instruire și separare a sarcinilor.
Sesiune de semnare	Intervalul delimitat în care semnatarul autentificat autorizează semnarea unuia sau mai multor documente identificate în SAD.

3.2. Acronime

Acronim	Semnificație
ADR	Autoritatea pentru Digitalizarea României
AdES / PAdES / XAdES / CAdES / JAdES	Advanced Electronic Signature și profilurile baseline pentru PDF, XML, CMS și JSON
API	Application Programming Interface
CA	Certification Authority (autoritate de certificare)
CAB	Conformity Assessment Body (organism de evaluare a conformității)
CC	Common Criteria (ISO/IEC 15408)
CRL	Certificate Revocation List
CSC	Cloud Signature Consortium
CSIRT	Computer Security Incident Response Team (DNSC)
DR	Disaster Recovery
DTBS/R	Data To Be Signed (Representation): reprezentarea datelor de semnat
EAL	Evaluation Assurance Level
EUDIW	European Digital Identity Wallet (portofel european pentru identitate digitală)
EUSPv2	EU Server Signing Application Service Policy v2: politica UE pentru serviciile de semnare pe server, versiunea 2 (ETSI TS 119 431-1, anexa A)

Acronim	Semnificație
GDPR	Regulamentul (UE) 2016/679
HSM	Hardware Security Module
LoA	Level of Assurance (nivel de asigurare – scăzut / substanțial / ridicat)
LoIP	Level of Identity Proofing: nivelul de verificare a identității (ETSI TS 119 461: baseline / extended)
NIS2	Directiva (UE) 2022/2555
OCSP	Online Certificate Status Protocol
OID	Object Identifier
QSCD / rQSCD	(remote) Qualified electronic Signature/Seal Creation Device: dispozitiv calificat de creare a semnăturilor sau sigiliilor electronice (la distanță)
QTSP	Qualified Trust Service Provider
SAD / SAM / SAP	Signature Activation Data / Module / Protocol: date de activare a semnăturii / modul de activare a semnăturii / protocol de activare a semnăturii
SCA	Signature Creation Application
SCAL / SCAL2	Sole Control Assurance Level: nivelul de asigurare a controlului exclusiv; SCAL2 – nivelul 2 de asigurare a controlului exclusiv (EN 419 241-1)
SIC	Signer Interaction Component: componenta de interacțiune cu semnatarul
SSA / SSAS / SSASP	Server Signing Application / Service / Service Provider: aplicație de semnare pe server / serviciu de aplicație de semnare pe server / prestatorul acestuia
TSA	Time-Stamping Authority
TSPS	Trust Service Practice Statement
TW4S	Trustworthy System Supporting Server Signing
WYSIWYS	What You See Is What You Sign

4. Concepte generale

4.1. Serviciul și componentele sale

Conform ETSI TS 119 431-1 (cl. 4.4), serviciul cuprinde:

– **generarea cheii de semnare** în QSCD-ul la distanță;

– **legarea certificatului** emis de CERTDIGITAL QUALIFIED CA G4 sau de CERTDIGITAL QCA G5 de cheia de semnare;

– **legarea mijlocului eID** al semnatarului de cheia de semnare, pentru asigurarea controlului exclusiv;

– **activarea semnăturii**: verificarea SAD și activarea cheii de către SAM;

– **ștergerea cheii de semnare**, astfel încât aceasta să nu mai poată fi utilizată;

– **furnizarea mijlocului eID** către semnatar.

4.2. Dispozitivul calificat la distanță

Cheile de semnare se generează, se păstrează și se utilizează exclusiv în dispozitivul calificat la distanță format din:

Componentă	Produs	Certificare
Modulul de activare a semnăturii (SAM)	Ascertia ADSS Server SAM Appliance v7.0.2	dispozitiv calificat la distanță pentru semnătură (QSigCD) și sigiliu (QSealCD), certificat de OCSI (Italia) conform art. 30 alin. (3) lit. (b) din Regulamentul eIDAS: OCSI/ACC/ASC/01/2022/RA, în vigoare din 23.05.2022; potrivit art. 30 alin. (3a) din Regulamentul eIDAS, certificarea este valabilă cel mult 5 ani, cu evaluarea vulnerabilităților o dată la 2 ani, iar recertificarea SAM se face înainte de 23.05.2027; raport de certificare Common Criteria OCSI/CERT/CCL/11/2021/RC (29.04.2022); înscris pe lista dispozitivelor calificate publicată de Comisia Europeană (art. 31)
Modulul criptografic	Utimaco CryptoServer CP5 Se500	Common Criteria EAL4+ conform EN 419 221-5, NSCIB-CC-2300142-01 (firmware 5.1.0.0), certificare eIDAS eIDAS-2300143-01.1, valabilă până la 05.12.2028

Dispozitivul este operat numai în configurația evaluată, descrisă în documentația de certificare, iar CERTDIGITAL respectă cerințele din rapoartele de certificare (art. 29a alin. (1) lit. (c) din Regulamentul eIDAS; TS 119 431-1, OVR-A.3-02, OVR-A.3-03, GEN-A.4-02).

4.3. Controlul exclusiv al semnatarului

Serviciul funcționează la nivelul de asigurare **SCAL2** din EN 419 241-1: activarea cheii nu este decisă de aplicația de semnare pe server, ci de SAM, care rulează în mediul protejat al dispozitivului și activează cheia numai pe baza unor SAD valide. SAD leagă, într-o structură protejată: autentificarea semnatarului cu mijlocul eID legat de cheie, cheia de semnare și reprezentarea datelor de semnat aprobată de semnatar. Personalul CERTDIGITAL, aplicațiile

client sau un atacator care ar controla aplicația de semnare nu pot activa cheia fără SAD valide, generate sub controlul semnatarului.

4.4. Modelele de chei de semnare

Model	Situația
Chei de lungă durată	se generează după verificarea identității, se leagă de mijlocul eID al semnatarului, au certificat calificat cu valabilitate de cel mult 3 ani și pot fi utilizate în mai multe sesiuni de semnare, fiecare cu autentificare și SAD noi
Chei de unică folosință	nu se oferă la data prezentei versiuni; identificatorul 1.3.6.1.4.1.47898.11.1.2 este planificat

4.5. Relația cu emiterea certificatelor calificate

Certificatele asociate cheilor sunt emise de CERTDIGITAL QUALIFIED CA G4, conform DPC CERTDIGITAL G4, și de CERTDIGITAL QCA G5, conform DPC CERTDIGITAL G5. Serviciul furnizează autorității de înregistrare dovada deținerii cheii și dovada autentificării semnatarului legate de cheie (ETSI EN 319 411-1, REG-6.3.1-01). Serviciul de gestionare la distanță este un serviciu de încredere distinct de emiterea certificatelor.

5. Politica serviciului

5.1. Identificare și conformitate

CERTDIGITAL declară conformitatea serviciului cu politica **EUSPv2** (OID 0.4.0.19431.1.1.4) din ETSI TS 119 431-1 V1.3.1, cu adaptările din Regulamentul de punere în aplicare (UE) 2025/1567. Regulamentul se aplică de la 19.08.2027; până la această dată, CERTDIGITAL aplică voluntar aceleași cerințe. Conformitatea este evaluată de un organism de evaluare a conformității acreditat (secțiunea 6.12). Pentru serviciu se solicită acordarea statutului calificat și înscrierea în Lista de încredere a României (art. 21 din Regulamentul eIDAS); până la înscriere, serviciul nu se prestează ca serviciu de încredere calificat (art. 21 alin. (3)).

5.2. Comunitatea utilizatorilor și aplicabilitatea

Serviciul se adresează abonaților, semnatarilor și părților care se bazează pe semnăturile și sigiliile create prin serviciu, susținute de certificate calificate emise de CERTDIGITAL QUALIFIED CA G4 sau de CERTDIGITAL QCA G5 conform politicilor QCP-n-qscd și QCP-l-qscd.

5.3. Modificarea politicii

Dacă o modificare a politicii (Partea I) afectează aplicabilitatea acesteia, identificatorul politicii, care identifică și prezentul document, se schimbă (TS 119 431-1, OVR-5.2-01).

6. Cerințele privind practicile

6.1. Publicare și depozit

Prezentul document, termenii și condițiile serviciului și certificatele autorităților sunt publicate la https://www.certdigital.ro/repository/, 24/7, public și fără restricții de acces (TS 119 431-1, OVR-5.1-03, OVR-6.1-04; secțiunea 10). Partea a II-a indică algoritmii de semnare și de generare a cheilor și ceilalți parametri critici pentru securitatea serviciului (OVR-5.1-02; secțiunile 13.1.2, 15.6 și 17).

6.2. Generarea cheii de semnare

– cheia se generează în QSCD-ul la distanță (secțiunea 4.2), după verificarea identității semnatarului și numai la cererea acestuia (art. 29a alin. (1) lit. (a));

– algoritmii și lungimile cheilor respectă documentul „Agreed Cryptographic Mechanisms" al ECCG: RSA de cel puțin 3072 de biți sau ECDSA pe curbele NIST P-256 / P-384, incluse în configurația certificată a QSCD (secțiunea 13.1.2);

– dovada deținerii cheii se transmite autorității de înregistrare odată cu cererea de certificat.

6.3. Verificarea identității și legarea mijlocului eID

– verificarea identității semnatarului respectă **nivelul extins (LoIP extended) din ETSI TS 119 461** (TS 119 431-1, LNK-A.7-01), cu metodele din DPC CERTDIGITAL G4, secțiunea 3.2.3: prezență fizică, CERTDIGITAL KYC sau, la reînnoire, certificat calificat CERTDIGITAL valabil;

– pentru sigilii se verifică, în plus, existența persoanei juridice și calitatea reprezentantului (DPC, secțiunea 3.2.2);

– cheia de semnare se leagă de referința mijlocului eID al semnatarului; datele de identificare legate de mijlocul eID sunt aceleași cu cele ale subiectului certificatului; integritatea legăturilor este protejată (LNK-6.2.2-10A);

– mijlocul eID asigură o autentificare de nivel cel puțin substanțial, cu doi factori (posesie și cunoaștere sau biometrie), conform EN 419 241-1, anexa A.

6.4. Furnizarea mijlocului eID

Mijlocul eID al semnatarului este aplicația mobilă **CertDigital ID**, care îndeplinește și rolul de componentă de interacțiune cu semnatarul (SIC): prin ea, semnatarul se autentifică, vizualizează sau identifică datele de semnat și autorizează activarea cheii. Aplicația se distribuie numai prin magazinele oficiale de aplicații și se leagă de dispozitivul semnatarului la înrolare, după verificarea identității; codul de înrolare și datele de activare inițiale se transmit separat, pe un canal independent (TS 119 431-1, EID-6.2.4-01, EID-6.2.4-02).

6.5. Legarea certificatului

Certificatul calificat emis pentru cheie se leagă de cheia de semnare, iar integritatea legăturii este protejată în sistemul de încredere (EN 419 241-1, SRC_SKS.1.2, 1.4 și 1.5).

6.6. Activarea semnăturii

– cheia de semnare se activează numai prin SAM, pe baza unor SAD valide, la nivelul SCAL2 (secțiunea 4.3);

– semnatarul vizualizează sau identifică datele de semnat și își exprimă explicit acordul pentru fiecare activare;

– SAD sunt protejate în integritate și confidențialitate la colectare, transmitere și utilizare și nu pot fi reutilizate;

– înainte de utilizarea cheii se verifică faptul că certificatul asociat este valabil (nu a expirat și nu a fost revocat);

– toate activările, reușite sau eșuate, se jurnalizează.

6.7. Ștergerea cheii de semnare

Cheia de semnare și copiile ei de rezervă se distrug astfel încât să nu mai poată fi utilizate: la revocarea sau expirarea certificatului asociat, la cererea semnatarului (pentru sigilii, a reprezentantului creatorului sigiliului) și la încetarea serviciului. Distrugerea se jurnalizează.

6.8. Copiile de rezervă

Datele de creare a semnăturii se duplică **numai pentru copii de rezervă**, în numele și la cererea semnatarului (exprimată prin contract), cu respectarea condițiilor din art. 29a alin. (1) lit. (b) din Regulamentul eIDAS:

– copiile au același nivel de securitate ca originalul: se realizează numai prin mecanismele interne ale dispozitivului certificat, criptat, și se restaurează numai într-un dispozitiv certificat de același tip, sub control dual;

– numărul copiilor nu depășește minimul necesar continuității serviciului.

6.9. Blocarea activării și revocarea

CERTDIGITAL nu oferă suspendarea certificatelor. Activarea unei chei se poate bloca imediat, 24/7, la cererea semnatarului (de exemplu la pierderea mijlocului eID), la indicii de compromitere sau de fraudă ori în gestionarea unui incident; deblocarea se face numai după reautentificarea sau reverificarea identității semnatarului. Revocarea certificatului se face conform DPC CERTDIGITAL G4, secțiunea 4.9 (în cel mult 24 de ore), și este urmată de ștergerea cheii (secțiunea 6.7).

6.10. Controale privind facilitățile, managementul și operarea

Se aplică Politicile generale CertDigital și cerințele din EN 419 241-1 (SRG), cu următoarele precizări:

– personalul cu roluri de încredere este angajat al CENTRUL DE CALCUL S.A., calificat, și primește cel puțin o dată la 12 luni instruire privind amenințările și practicile de securitate actuale (Reg. (UE) 2025/1567, OVR-6.4.4-02/03);

– operațiile administrative asupra dispozitivului se fac sub control dual (M din N);

– se jurnalizează evenimentele de securitate, tranzacțiile SAP, activările și evenimentele din ciclul de viață al cheilor; jurnalele se păstrează cel puțin 10 ani;

– incidentele se notifică conform Procedurii de notificare a incidentelor (00q): ADR în cel mult 24 de ore de la luarea la cunoștință, DNSC, ANSPDCP și persoanele afectate;

– continuitatea serviciului este asigurată conform Procedurii de continuitate operațională (PO/SI/63), cu dispozitive în ambele centre de date; durata maximă de restabilire a serviciului rQSCD este de 8 ore (PO/SI/63);

– încetarea serviciului se face conform Planului de încetare a serviciilor (00r), elaborat potrivit Regulamentului de punere în aplicare (UE) 2025/2530 (OVR-6.4.9-02): cheile de semnare și copiile lor se distrug, iar certificatele asociate se revocă.

6.11. Controale tehnice

– scanarea de vulnerabilități se efectuează cel puțin o dată pe trimestru (OVR-6.5.5-02);

– firewall-urile blochează toate protocoalele și accesele care nu sunt necesare funcționării serviciului (OVR-6.5.5-03);

– tehnicile criptografice sunt gestionate pe tot ciclul de viață și sunt conforme cu documentul „Agreed Cryptographic Mechanisms” al ECCG (OVR-6.8.5-01/02);

– comunicațiile dintre componentele de interacțiune cu semnatarul și SAM sunt protejate criptografic.

6.12. Evaluarea conformității

Serviciul este evaluat de un organism de evaluare a conformității acreditat conform Regulamentului de punere în aplicare (UE) 2025/2162, cel puțin o dată la 24 de luni (art. 20 din Regulamentul eIDAS); ADR este informată cu cel puțin o lună înainte, iar raportul se transmite ADR în cel mult 3 zile lucrătoare. CERTDIGITAL efectuează anual un audit intern.

7. Obligații și răspundere

7.1. Obligațiile CERTDIGITAL

– generează și gestionează datele de creare a semnăturii numai în numele și la cererea semnatarului (art. 29a alin. (1) lit. (a));

– duplică datele numai pentru copii de rezervă, în condițiile secțiunii 6.8;

– utilizează exclusiv un QSCD certificat, în configurația evaluată, și respectă cerințele din raportul de certificare (art. 29a alin. (1) lit. (c));

– asigură controlul exclusiv al semnatarului prin SAM și SAP certificate;

– publică documentația serviciului 24/7.

7.2. Obligațiile abonatului și ale semnatarului

– păstrează mijlocul eID și factorii de autentificare sub control exclusiv și nu le divulgă;

– solicită imediat blocarea cheii și revocarea certificatului la suspiciunea de compromitere sau la pierderea controlului asupra mijlocului eID (art. 26 din Legea nr. 214/2024);

– verifică datele de semnat înainte de a-și exprima acordul;

– utilizează serviciul numai în scopuri legale, conform termenilor și condițiilor.

7.3. Obligațiile părților care se bazează

Verifică semnătura sau sigiliul, starea certificatului (OCSP sau CRL) și statutul calificat al serviciilor în Lista de încredere a României.

7.4. Răspunderea

CERTDIGITAL răspunde, conform art. 13 din Regulamentul eIDAS, pentru prejudiciile cauzate cu intenție sau din neglijență oricărei persoane fizice sau juridice, inclusiv titularilor și părților care se bazează, prin nerespectarea obligațiilor care îi revin. Intenția sau neglijența CERTDIGITAL se prezumă, cu excepția cazului în care CERTDIGITAL dovedește că prejudiciul s-a produs fără intenția sau neglijența sa.

CERTDIGITAL nu răspunde pentru prejudiciile rezultate din: utilizarea serviciului peste limitările notificate în prealabil și recognoscibile de terți; nerespectarea de către semnatar a obligațiilor de la secțiunea 7.2; neverificarea de către partea care se bazează a stării certificatului și a statutului din Lista de încredere; forța majoră. Nicio prevedere nu exclude și nu limitează răspunderea pentru intenție sau culpă gravă (art. 1355 Cod civil); în raporturile cu consumatorii se aplică Legea nr. 193/2000.

7.5. Asigurarea

CENTRUL DE CALCUL S.A. deține, pentru fiecare dintre cele două servicii, câte o poliță distinctă de asigurare de răspundere civilă profesională, cu limita răspunderii de 500.000 EUR pe perioada asigurată, în condițiile art. 24 alin. (2) lit. c) din Regulamentul eIDAS și ale art. 5

alin. (2) lit. b) din procedura aprobată prin Ordinul MEDAT nr. 102/2026; în fiecare poliță, ADR, în calitate de organism de supraveghere, are calitatea de asigurat adițional. Polițele se reînnoiesc înainte de expirare; datele lor de identificare (asigurătorul, seria și numărul, perioada de valabilitate) sunt comunicate ADR și se pun la dispoziție la cerere.

8. Alte aspecte comerciale și juridice

8.1. Tarife

Tarifele serviciilor sunt cele din lista de tarife publicată pe site-ul https://www.certdigital.ro/ sau cele din oferta transmisă la cerere (art. 11 alin. (1) și, pentru certificatele calificate, alin. (3) lit. b) din Legea nr. 214/2024). Informațiile privind starea certificatelor sunt gratuite.

8.2. Protecția datelor cu caracter personal

CERTDIGITAL prelucrează datele de identificare și de autentificare ale semnatarilor în calitate de operator, conform Regulamentului (UE) 2016/679, Legii nr. 190/2018 și Politicii de protecție a datelor (00d). Serviciul primește numai reprezentarea datelor de semnat; atunci când abonatul utilizează aplicațiile CERTDIGITAL pentru încărcarea documentelor, CERTDIGITAL acționează pentru acestea ca persoană împuternicită (art. 28 GDPR). Responsabilul cu protecția datelor: dpo@centruldecalcul.ro.

8.3. Modificări

Orice modificare a prezentului document primește o versiune nouă, aprobată de Directorul General și publicată în depozitul de documente; versiunile anterioare rămân disponibile. Modificările care afectează prestarea serviciilor calificate se comunică ADR cu cel puțin o lună înainte de aplicare (cu cel puțin trei luni în cazul încetării unui serviciu). Abonații și părțile care se bazează sunt informați prin publicare pe site cu cel puțin 30 de zile înainte de intrarea în vigoare. Corecturile de redactare care nu modifică drepturile sau obligațiile părților se publică cu versiune nouă, fără termen de preaviz.

8.4. Soluționarea litigiilor

Litigiile se soluționează pe cale amiabilă, pe baza unei reclamații transmise la office@certdigital.ro, la care CERTDIGITAL răspunde în cel mult 30 de zile. În lipsa unei soluții amiabile, litigiile cu profesioniștii sunt de competența instanțelor de la sediul CENTRUL DE CALCUL S.A. (Târgu Jiu). Consumatorii se pot adresa instanțelor competente potrivit legii, inclusiv celor de la domiciliul lor, și pot apela la procedurile de soluționare alternativă a litigiilor (SAL) prevăzute de OG nr. 38/2015 (ANPC – https://anpc.ro/sal).

8.5. Legea aplicabilă și cadrul legal

Prezentul document și raporturile juridice decurgând din furnizarea serviciului sunt guvernate de dreptul român, sub rezerva dispozițiilor direct aplicabile ale dreptului Uniunii Europene. Serviciul este furnizat în conformitate cu actele normative de la capitolul 2. Organismul de supraveghere este Autoritatea pentru Digitalizarea României.

8.6. Alte prevederi

CERTDIGITAL urmărește accesibilitatea serviciilor pentru persoanele cu dizabilități (art. 15 din Regulamentul eIDAS); persoanele cu dizabilități pot solicita asistență prin telefon, e-mail sau la sediu.

9. Corespondența cu cerințele ETSI TS 119 431-1 și ale Regulamentului (UE) 2025/1567

9.1. Tabel de corespondență

Cerință	Conținut	Secțiune
TS 119 431-1, cl. 5.1 / OVR-5.1-02, 5.1-03	declarația de practici; algoritmi; publicare 24/7	1.1, 6.1
TS 119 431-1, cl. 5.2 / A.2	identificarea politicii (EUSPv2)	1.2, 5.1
TS 119 431-1, cl. 5.3	participanți	1.3
TS 119 431-1, cl. 6.2.1 / A.4	generarea cheii în QSCD	4.2, 6.2
TS 119 431-1, cl. 6.2.2 / A.7 (LNK-A.7-01)	verificarea identității (LoIP extins), legarea mijlocului eID	6.3
TS 119 431-1, cl. 6.2.3	legarea certificatului	6.5
TS 119 431-1, cl. 6.2.4	furnizarea mijlocului eID	6.4
TS 119 431-1, cl. 6.3.1 / A.5, A.6	activarea semnăturii (SAM, SAP, SAD, SCAL2)	4.3, 6.6
TS 119 431-1, cl. 6.3.2	ștergerea cheii	6.7
TS 119 431-1, cl. 6.3.3	copii de rezervă	6.8
TS 119 431-1, cl. 6.4–6.5	controale de facilitate, management, operare și tehnice	6.10, 6.11
TS 119 431-1, cl. 6.6	evaluarea conformității	6.12
TS 119 431-1, cl. 6.7–6.8	aspecte comerciale și juridice; termeni și condiții	7, 8
TS 119 431-1, A.3 (OVR-A.3-02, A.3-03)	certificarea QSCD și cerințele din raportul de certificare	4.2
Reg. (UE) 2025/1567, OVR-6.1-04	disponibilitate publică și internațională	1.5, 6.1
Reg. (UE) 2025/1567, OVR-6.4.4-02/03	personal calificat, instruire la 12 luni	6.10
Reg. (UE) 2025/1567, OVR-6.4.9-02	plan de încetare conform 2025/2530	6.10
Reg. (UE) 2025/1567, OVR-6.5.5-02/03	scanare trimestrială; firewall	6.11
Reg. (UE) 2025/1567, OVR-6.8.5-01/02	criptografie conform ECCG ACM	6.2, 6.11
Regulamentul eIDAS, art. 29a alin. (1)	gestionare în numele semnatarului; copii de rezervă; QSCD certificat	6.2, 6.8, 7.1

Practicile detaliate pentru fiecare cerință sunt descrise în Partea a II-a; corespondența completă a cerințelor cu secțiunile acesteia este prezentată în anexa A.

PARTEA A II-A – Declarația de practici

10. Publicarea și responsabilitățile privind depozitul

Partea a II-a descrie practicile, procedurile și controalele prin care CERTDIGITAL îndeplinește cerințele politicii din Partea I. Identificarea documentului, participanții, utilizarea serviciului, administrarea documentului, cadrul normativ, definițiile și acronimele sunt cele din Partea I (capitolele 1–3).

10.1. Depozitul (repository)

CERTDIGITAL menține un depozit public, disponibil online la adresa **https://www.certdigital.ro/repository**, în care publică (ETSI TS 119 431-1: OVR-6.1-01, OVR-5.1-03; ETSI EN 319 401: REQ-6.1-05X):

– prezentul document (politica și declarația de practici a serviciului), în versiunea curentă și în versiunile anterioare (arhivă);

– Politica serviciilor de certificare CertDigital, Declarația practicilor de certificare a CERTDIGITAL ROOT CA G4 și CERTDIGITAL QUALIFIED CA G4 (DPC CERTDIGITAL G4) și DPC CERTDIGITAL G5;

– Termenii și condițiile serviciului rQSCD (document distinct, conform secțiunii 18.15) și modelul de contract de abonat;

– certificatele autorităților de certificare CERTDIGITAL (ROOT CA G4, QUALIFIED CA G4, ROOT CA G5, QCA G5) și amprentele acestora;

– listele de certificate revocate (CRL) și adresa serviciului OCSP;

– informații privind certificarea dispozitivului rQSCD și a modulului SAM (referința certificatului Common Criteria, versiunea evaluată), conform secțiunii 11.3;

– documentația interfeței de semnare la distanță pentru integratori și ghidul de utilizare a aplicației CertDigital ID;

– rapoartele de evaluare a conformității (sumarul public) și referința înscrierii în Lista de încredere;

– politica de divulgare coordonată a vulnerabilităților (CVD) și canalele de contact pentru incidente de securitate;

– informații privind protecția datelor cu caracter personal (nota de informare GDPR);

– notificări privind modificări ale documentelor, întreruperi planificate și incidente cu impact asupra abonaților.

10.2. Publicarea informațiilor

Informațiile din depozit sunt publicate prin HTTPS. Documentele sunt publicate în format PDF, semnate electronic cu sigiliul electronic calificat al CENTRUL DE CALCUL S.A. și marcate temporal, pentru a garanta integritatea și autenticitatea lor. Fiecare document indică

versiunea, data intrării în vigoare și OID-ul aplicabil, astfel încât termenii și condițiile aplicabile unei anumite chei de semnare sau unui anumit certificat să fie ușor identificabile (ETSI TS 119 431-1: OVR-6.1-02).

Depozitul este disponibil public și internațional, fără restricții de acces; documentele sunt publicate în limba română (Reg. 2025/1567, adaptarea OVR-6.1-04; ETSI EN 319 401: REQ-6.2-05).

10.3. Frecvența publicării și disponibilitatea

– Prezentul document și Termenii și condițiile sunt publicate la fiecare versiune nouă, după aprobarea de către Directorul General, cu cel puțin **30 de zile** înainte de intrarea în vigoare a modificărilor care pot afecta acceptarea serviciului de către abonați sau părțile utilizatoare, conform secțiunii 19 (ETSI EN 319 401: REQ-6.1-09X, REQ-6.1-10).

– CRL-urile sunt publicate la intervalele definite în DPPC-CA_G4 (cel mult 24 de ore) și imediat după fiecare revocare; OCSP răspunde în timp real.

– Depozitul este proiectat pentru o disponibilitate de **minimum 99,5 %** pe an, măsurată 24 de ore din 24, 7 zile din 7, cu excepția întreținerilor planificate anunțate cu cel puțin 48 de ore înainte. În caz de indisponibilitate cauzată de factori care nu sunt sub controlul CERTDIGITAL, perioada maximă de indisponibilitate a informațiilor este de **24 de ore** (ETSI TS 119 431-1: OVR-6.1-03). Depozitul este găzduit redundant în centrul de date principal și în centrul de date secundar.

10.4. Controlul accesului la depozit

Informațiile publicate în depozit sunt accesibile public, în mod gratuit, numai pentru citire. Publicarea, modificarea și retragerea documentelor din depozit sunt operațiuni rezervate rolurilor de încredere autorizate (Ofițerul de Securitate IT și Administratorul de sistem desemnat), sunt efectuate prin canale autentificate și sunt înregistrate în jurnalele de audit. Integritatea depozitului este monitorizată prin verificarea periodică a amprentelor documentelor publicate față de registrul intern al documentelor aprobate.

11. Arhitectura serviciului și componentele acestuia

11.1. Modelul de referință și nivelul de asigurare a controlului exclusiv

Serviciul CertDigital rQSCD este construit pe modelul de referință definit în CEN EN 419 241-1 (Trustworthy Systems Supporting Server Signing – TW4S) și operează exclusiv la **nivelul de asigurare a controlului exclusiv SCAL2** (ETSI TS 119 431-1: OVR-A.3-01 – toate cerințele [NSP] se aplică; GEN-6.2.1-02, SIG-6.3.1-05 ÷ SIG-6.3.1-07). Aceasta înseamnă că:

– cheia de semnare a semnatarului este generată, stocată și utilizată exclusiv în modulul criptografic al dispozitivului calificat la distanță, certificat conform CEN EN 419 221-5 (secțiunea 11.3) (GEN-6.2.1-02A, GEN-A.4-01, SIG-A.5-01);

– autorizarea utilizării cheii de semnare nu este decisă de aplicația de semnare pe server (SSA), ci de **modulul de activare a semnăturii (SAM)**, care rulează în mediul protejat al dispozitivului calificat (aparatul ADSS Server SAM Appliance), evaluat împreună cu modulul criptografic;

– SAM activează cheia de semnare numai după validarea **datelor de activare a semnăturii (SAD)**, care leagă criptografic, într-o singură structură autentificată: (i) identitatea semnatarului autentificat, (ii) cheia de semnare selectată și (iii) reprezentarea datelor de semnat (DTBS/R) aprobată explicit de semnatar;

– niciun administrator CERTDIGITAL, niciun operator, nicio aplicație client și niciun atacator care ar compromite rețeaua sau SSA nu poate determina rQSCD să creeze o semnătură în absența unor SAD valide, generate sub controlul semnatarului.

Figura de mai jos (descriere textuală) prezintă componentele și fluxurile principale:

Componentă	Rol	Localizare / control
Componenta de interacțiune cu semnatarul (SIC)	Autentifică semnatarul, afișează datele de semnat (WYSIWYS), colectează consimțământul și generează SAD	Dispozitivul personal al semnatarului (aplicația mobilă CertDigital ID); sub controlul semnatarului
Aplicația client (SCA)	Pregătește documentul, calculează DTBS/R, apelează API-ul de semnare, asamblează semnătura AdES	Portalul CertDigital sau aplicația integratorului autorizat
Aplicația de semnare pe server (SSA)	Primește cererile de semnare, gestionează sesiunile și autorizarea aplicațiilor client, transmite SAD către SAM, returnează valoarea semnăturii	Centrul de date CERTDIGITAL, zonă de rețea dedicată
Modulul de activare a semnăturii (SAM)	Validează SAD, verifică legătura semnatar–cheie–DTBS/R, autorizează modulul criptografic să utilizeze cheia	Aparatul ADSS Server SAM Appliance v7.0.2 (dispozitiv calificat, secțiunea 11.3)
Modulul criptografic (HSM / rQSCD)	Generează, stochează, protejează și utilizează cheile de semnare; realizează copii de siguranță criptate	Utimaco CryptoServer CP5 Se500 al dispozitivului calificat, în zona criptografică a centrului de date (CEN EN 419 221-5)
Serviciul de înregistrare și identificare (RA)	Verifică identitatea semnatarului la înrolare (ETSI TS 119 461), înregistrează legătura identitate–eID–cheie	CertDigital RA (prezență fizică la sediu și la punctele de lucru; CERTDIGITAL KYC)
Autoritatea de certificare (CA)	Emite certificatul calificat pentru cheia publică generată în rQSCD, pe baza dovezii de posesie	CERTDIGITAL QUALIFIED CA G4; CERTDIGITAL QCA G5

Componentă	Rol	Localizare / control
Serviciile de stare și validare	CRL, OCSP, serviciul de validare	CERTDIGITAL OCSP G4; serviciul de validare CertDigital
Autoritatea de marcare temporală	Emite mărci temporale calificate pentru semnăturile B-T/B-LT/B-LTA	CERTDIGITAL TSA G4

11.2. Componentele serviciului conform ETSI TS 119 431-1

În scopul clasificării cerințelor, serviciul este descompus în componentele definite în ETSI TS 119 431-1, clauza 4.4:

Componentă	Cod	Descriere	Secțiunea din prezentul document
Serviciul de generare a cheilor de semnare	GEN	Generează perechea de chei a semnatarului în rQSCD și transmite dovada de posesie serviciului de înregistrare al CA	13.1
Serviciul de legare a certificatului	LNK	Leagă certificatul calificat emis de CA de cheia de semnare corespunzătoare din rQSCD	12.6
Serviciul de legare a mijlocului eID	LNK	Leagă referința mijlocului de identificare electronică al semnatarului de cheia de semnare, pentru a asigura controlul exclusiv	12.3 ÷ 12.5
Serviciul de activare a semnăturii	SIG	Verifică SAD și activează cheia de semnare pentru crearea semnăturii	13.2
Serviciul de ștergere a cheilor de semnare	DEL	Distruge cheile de semnare astfel încât acestea să nu mai poată fi utilizate	13.5
Serviciul de furnizare a mijloacelor eID (opțional)	EID	Pregătește și furnizează semnatarului mijlocul de identificare electronică (aplicația CertDigital ID și datele de activare)	12.4

Această subdiviziune are rol de clarificare a cerințelor și nu impune constrângeri asupra implementării tehnice.

11.3. Dispozitivul calificat de creare a semnăturii la distanță (rQSCD)

11.3.1. Dispozitivul calificat și modulul criptografic

Cheile de semnare ale semnatarilor sunt generate, stocate și utilizate exclusiv în dispozitivul calificat la distanță format din aparatul **Ascertia ADSS Server SAM Appliance v7.0.2** și modulul criptografic **Utimaco CryptoServer CP5 Se500** (ETSI TS 119 431-1: GEN-6.2.1-02A, GEN-A.4-01, SIG-A.5-01; checklist 2.1). CERTDIGITAL deține două astfel de aparate, unul în centrul de date principal și unul în cel secundar.

Element	Valoare
Dispozitiv	Ascertia Ltd. – ADSS Server SAM Appliance v7.0.2: dispozitiv calificat la distanță pentru crearea semnăturilor (QSigCD) și a sigiliilor (QSealCD) electronice
Certificarea conform art. 30 din Regulamentul eIDAS	OCSI (Italia), OCSI/ACC/ASC/01/2022/RA, în vigoare din 23.05.2022 (procesul de la art. 30 alin. (3) lit. (b)); lista Comisiei indică „valabil până la revocare”; potrivit art. 30 alin. (3a) din Regulamentul eIDAS, certificarea este valabilă cel mult 5 ani, cu evaluarea vulnerabilităților o dată la 2 ani; recertificarea SAM se face înainte de 23.05.2027
Raportul de certificare Common Criteria	OCSI/CERT/CCL/11/2021/RC (29.04.2022)

Element	Valoare
Lista Comisiei Europene (art. 31)	dispozitivul figurează pe listă, în combinație cu modulul criptografic de mai jos (verificat la 20.10.2026)
Modul criptografic	Utimaco CryptoServer CP5 Se500 – Common Criteria EAL4+ conform CEN EN 419 221-5, NSCIB-CC-2300142-01 (firmware 5.1.0.0); certificare eIDAS eIDAS-2300143-01.1, valabilă până la 05.12.2028
Versiunea de firmware CP5 în producție	5.1.0.0, versiunea din combinația listată; firmware-ul se actualizează numai după confirmarea scrisă Ascertia/OCSI că noua versiune face parte din combinația certificată

Dispozitivul și modulul criptografic sunt operate **strict în configurația evaluată** descrisă în documentația de certificare (Security Target, ghidul de operare securizată / „Guidance Documentation") sau într-o configurație echivalentă care atinge aceleași obiective de securitate (GEN-A.4-02, SIG-A.5-02). CERTDIGITAL respectă toate cerințele identificate în raportul de certificare al dispozitivului (OVR-A.3-03; art. 29a alin. (1) lit. (c) din Regulamentul eIDAS), inclusiv:

– activarea modului de operare conform EN 419 221-5 (restricții privind exportul cheilor, autentificarea utilizatorilor, politici de utilizare a cheilor);

– autentificarea bazată pe smartcard-uri și controlul dual (M din N) pentru operațiunile administrative;

– verificarea, la fiecare instalare, actualizare sau audit, a corespondenței exacte dintre versiunea de firmware instalată și versiunea din combinația certificată (pentru modulele CP5 ale aparatelor SAM: 5.1.0.0); o neconcordanță determină scoaterea imediată din producție a dispozitivului până la restabilirea conformității (checklist 2.1);

– aplicarea politicilor de utilizare a cheilor de semnare conform cărora cheia poate fi utilizată numai pentru operațiunea de semnare și numai după autorizarea de către SAM.

Declarația de practici (Partea a II-a a prezentului document) include, conform cerinței **OVR-A.3-02 [EUSPv2]**, referința la certificarea QSCD în raport cu anexa II la Regulamentul eIDAS; copia certificării și a raportului de certificare este păstrată în dosarul de acreditare (CD_SI_017) și este pusă la dispoziția CAB și ADR.

11.3.2. Modulul de activare a semnăturii (SAM)

Modulul de activare a semnăturii este componenta aparatului ADSS Server SAM Appliance care, în mediul protejat al dispozitivului calificat, verifică datele de activare a semnăturii și autorizează utilizarea cheii de semnare exclusiv pentru DTBS/R autorizate.

Element	Valoare
Produs	Ascertia ADSS Server SAM Appliance v7.0.2 (componenta SAM)
Evaluarea de securitate	Common Criteria 3.1 rev. 5, raportul de certificare OCSI/CERT/CCL/11/2021/RC (29.04.2022): conformitate strictă cu profilul de protecție CEN EN 419 241-2:2019, nivelul EAL4 augmentat cu AVA_VAN.5; controlul exclusiv la nivelul SCAL2 (CEN EN 419 241-1); Security Target v8 (19.04.2022)
Combinația QSCD evaluată	SAM + modulul criptografic Utimaco CP5 (NSCIB-CC-2300142-01), conform intrării de pe lista Comisiei

SAM-ul garantează, prin construcție, că (ETSI TS 119 431-1: SIG-A.5-03 ÷ SIG-A.5-08; CEN EN 419 241-1: SRA_SAP.1.3 ÷ SRA_SAP.1.7):

– semnatarul a fost autentificat la un nivel de asigurare cel puțin substanțial, prin mijlocul eID legat de cheia de semnare (secțiunea 12.3);

– semnatarul a aprobat explicit semnarea DTBS/R identificate în SAD;

– cheia de semnare activată este exact cheia asociată semnatarului autentificat și sesiunii de semnare;

– SAD nu pot fi falsificate, reutilizate (replay) sau modificate în tranzit: ele sunt legate de sesiunea de semnare, conțin o valoare unică și un interval de valabilitate și sunt autentificate cu mijlocul eID al semnatarului;

– legătura dintre SIC și SAM este protejată criptografic (de la un capăt la altul, independent de securitatea TLS a SSA), astfel încât SSA și operatorii CERTDIGITAL nu pot genera, modifica sau reutiliza SAD;

– toate tentativele de activare, reușite sau eșuate, sunt jurnalizate în mod securizat (secțiunea 14.5).

Recomandarea **SIG-A.5-08 [EUSPv2]** (certificarea SAM conform EN 419 241-2) este îndeplinită prin utilizarea dispozitivului certificat de la secțiunea 11.3.1.

11.3.3. Izolarea arhitecturală

Modulele criptografice și SAM sunt amplasate într-un **segment de rețea dedicat (zona criptografică)**, separat prin firewall-uri de restul infrastructurii, cu reguli explicite de tip „deny-all" și cu permiterea exclusivă a fluxurilor (Reg. 2025/1567, adaptarea OVR-6.5.5-03):

– SSA → SAM: transmiterea cererilor de activare (SAD + DTBS/R + referința cheii) și primirea valorii semnăturii;

– stația de administrare HSM (în zona securizată, acces fizic dual) → HSM: operațiuni administrative autorizate M din N;

– HSM → serverul de jurnalizare: exportul jurnalelor de audit semnate.

Orice alt flux este blocat. Dovada izolării (configurațiile firewall, diagramele de rețea, rezultatele testelor de penetrare) este păstrată în documentația de arhitectură CD_SI_014 și este pusă la dispoziția CAB (checklist 3.1).

11.4. Protocolul de activare a semnăturii (SAP) și datele de activare (SAD)

11.4.1. Conținutul SAD

Datele de activare a semnăturii leagă, într-o structură protejată în integritate și autentificată cu mijlocul eID al semnatarului, următoarele elemente (CEN EN 419 241-1: SRA_SAP.2.1 ÷ SRA_SAP.2.3; ETSI TS 119 431-1: SIG-A.6-01 ÷ SIG-A.6-03):

Element SAD	Scop
Identificarea semnatarului autentificat (referința mijlocului eID)	Legarea de semnatar
Destinatarul: SAM-ul CERTDIGITAL	Destinația unică a SAD (SRA_SAP.2.5)

Element SAD	Scop
O valoare unică, emisă la inițierea sesiunii, și identificatorul sesiunii de semnare	Protecția împotriva reutilizării (replay)
Intervalul de valabilitate (cel mult **5 minute**)	Limitarea temporală a autorizării (checklist 3.2)
Referința cheii de semnare	Legarea de cheia corectă
DTBS/R aprobate (valorile hash și algoritmul)	Legarea indisolubilă de documentele aprobate (WYSIWYS)
Autentificarea cu cheia mijlocului eID, păstrată în zona securizată a dispozitivului mobil	Autentificarea SAD și dovada controlului exclusiv

Formatul SAD, algoritmii și mesajele protocolului sunt cele ale protocolului de activare a semnăturii al dispozitivului ADSS Server SAM Appliance v7.0.2, în configurația evaluată, integrat cu aplicația CertDigital ID; specificația detaliată este documentată în CD_SI_014 și este pusă la dispoziția CAB.

11.4.2. Fluxul protocolului de activare

– **Inițierea**: aplicația client (SCA) transmite SSA cererea de semnare, conținând DTBS/R (una sau mai multe valori hash), identificatorul certificatului/cheii și metadatele documentelor. SSA creează o sesiune de semnare și obține de la SAM valoarea unică a sesiunii.

– **Notificarea semnatarului**: SSA transmite aplicației CertDigital ID a semnatarului, printr-un canal autentificat, cererea de autorizare, conținând DTBS/R, metadatele documentelor și valoarea unică a sesiunii. Pentru fluxurile inițiate chiar din aplicația mobilă sau din portalul web, cererea este afișată direct.

– **Prezentarea datelor de semnat (WYSIWYS)**: aplicația descarcă documentul (sau reprezentarea sa vizuală) prin canal securizat, îl afișează integral semnatarului, calculează local valoarea hash a conținutului afișat și o compară cu DTBS/R primite; în caz de neconcordanță, semnarea este refuzată. Semnatarul trebuie să parcurgă documentul (derulare până la final sau confirmare explicită a vizualizării) înainte ca butonul de autorizare să devină activ (checklist 3.3).

– **Autentificarea și consimțământul**: semnatarul se autentifică prin doi factori (posesia dispozitivului înrolat, demonstrată prin cheia din zona securizată, și cunoașterea codului PIN sau verificarea biometrică locală) și confirmă explicit intenția de a semna documentele afișate.

– **Generarea SAD**: aplicația construiește SAD conform secțiunii 11.4.1 și le autentifică cu cheia mijlocului eID, generată și păstrată, neexportabilă, în zona securizată a dispozitivului.

– **Transmiterea**: SAD sunt protejate criptografic de la aplicație până la SAM și sunt transmise prin SSA; SSA nu poate citi sau modifica SAD (SRA_SAP.2.6, SIG-A.6-06A).

– **Validarea și activarea**: SAM verifică autenticitatea SAD față de referința mijlocului eID legată de cheia de semnare, valoarea unică, valabilitatea, identificatorul sesiunii și corespondența cu cheia solicitată și cu DTBS/R transmise de SSA. Numai dacă toate

verificările reușesc, SAM autorizează modulul criptografic să calculeze semnătura pentru DTBS/R autorizate, și numai pentru acestea (SRA_SAP.2.4, SRA_SKM.2.1, SRA_SKM.2.5).

– **Returnarea semnăturii**: valoarea semnăturii este returnată SSA și apoi SCA, care asamblează semnătura în formatul AdES solicitat, adaugă marca temporală calificată și, după caz, informațiile de validare (B-LT/B-LTA).

– **Închiderea**: SAD sunt invalidate imediat după utilizare; sesiunea de semnare este închisă; evenimentul este jurnalizat (secțiunea 14.5) (SRA_SAP.2.8, SIG-A.6-08).

11.4.3. Proprietăți de securitate ale SAP

– **Unicitatea autorizării**: un SAD autorizează exact DTBS/R enumerate; orice altă cerere de semnare necesită SAD noi.

– **Semnarea în lot (batch)**: autorizarea mai multor documente printr-un singur SAD este permisă numai dacă toate documentele au fost prezentate semnatarului și identificate individual în SAD; aplicația afișează lista completă și permite vizualizarea fiecărui document.

– **Rezistența la atacuri**: protocolul este protejat împotriva ascultării, modificării, reluării și a atacurilor de tip „man-in-the-middle” prin protecția criptografică a SAD de la un capăt la altul, prin fixarea certificatelor (certificate pinning) în aplicația mobilă și prin verificarea integrității aplicației (atestarea dispozitivului, detecția root/jailbreak) (SRA_SAP.1.4, SRA_SAP.1.6, SRA_SAP.1.7).

– **Protecția mediului SIC**: cheia mijlocului eID este generată în zona securizată a dispozitivului și nu poate fi extrasă nici de utilizator, nici de aplicații malițioase; utilizarea ei necesită PIN sau biometrie locală; aplicația este supusă testelor de penetrare anuale (checklist 3.2).

11.5. Modelele de chei de semnare

Caracteristică	Chei de lungă durată
Generare	În rQSCD, la înrolare, după verificarea identității
Legarea controlului	De referința mijlocului eID al semnatarului (aplicația CertDigital ID)
Certificat calificat	Valabilitate de cel mult 3 ani; QCP-n-qscd / QCP-l-qscd
Sesiunea de semnare	Nelimitată ca număr, fiecare necesitând autentificare și SAD noi
Cazuri de utilizare	Semnatari recurenți, angajați, profesioniști, reprezentanți ai persoanelor juridice

Cheile de semnare de unică folosință nu se oferă la data prezentei versiuni (secțiunea 1.4.1).

11.6. Interfețele serviciului și protocoalele de integrare

11.6.1. Interfața de semnare la distanță

Serviciul expune aplicațiilor client o interfață de semnare la distanță, prin care acestea transmit DTBS/R, inițiază sesiunile de semnare (cu notificarea semnatarului în aplicația CertDigital ID) și primesc valoarea semnăturii; aplicațiile client nu au acces la SAD sau la

cheile de semnare. Documentația interfeței (operații, formate, coduri de eroare, metode de autentificare a aplicațiilor client) este publicată în depozit și pusă la dispoziția integratorilor (checklist 5.1).

11.6.2. Autentificarea aplicațiilor client și a semnatarilor

– aplicațiile client sunt înregistrate individual, cu drepturi limitate la operațiunile strict necesare (principiul privilegiului minim) (checklist 5.2);

– autentificarea semnatarului pentru autorizarea accesului și pentru activarea semnăturii se realizează exclusiv prin aplicația CertDigital ID (secțiunea 12.4), niciodată prin parolă statică;

– canalul de comunicare utilizează TLS 1.3 sau TLS 1.2, numai cu suite de cifrare cu Perfect Forward Secrecy; configurația este evaluată periodic;

– interfața aplică limitarea ratei cererilor (rate limiting) și filtrarea traficului anormal.

11.6.3. Integrarea cu portofelul european pentru identitate digitală (EUDIW)

Nu se aplică: la data prezentei versiuni, serviciul nu utilizează portofelul european pentru identitate digitală. Integrarea se va descrie într-o versiune nouă a prezentului document, notificată ADR (secțiunea 16.4), înainte de punerea ei în funcțiune.

11.6.4. Legătura cu serviciile CERTDIGITAL conexe

Serviciu	Interacțiune
CERTDIGITAL QUALIFIED CA G4 / CERTDIGITAL QCA G5	Primește cererea de certificare (PKCS#10) semnată cu cheia generată în rQSCD și însoțită de aserțiunea de autentificare a semnatarului emisă de SSAS (dovada legăturii cheie–identitate, conform ETSI EN 319 411-1 REG-6.3.1-01); emite certificatul calificat; notifică SSAS la revocare pentru declanșarea ștergerii cheii (GEN-6.2.1-08, DEL-6.3.2-01)
CertDigital RA	Furnizează rezultatul verificării identității și identificatorul procesului de verificare; menține evidența identitate–eID–cheie–certificat
CertDigital TSA	Emite mărci temporale calificate incluse în semnăturile B-T și superioare
CERTDIGITAL OCSP G4; serviciul de validare CertDigital	Furnizează CRL/OCSP și validarea semnăturilor pentru părțile utilizatoare
CERTDIGITAL QPS (serviciul calificat de păstrare)	Păstrarea pe termen lung a semnăturilor create, la cererea abonatului

12. Identificarea și autentificarea semnatarului

12.1. Înrolarea și înregistrarea

12.1.1. Cererea de înrolare

Înrolarea în serviciul rQSCD se realizează prin portalul CertDigital, prin aplicația mobilă CertDigital ID, la ghișeele autorităților de înregistrare CERTDIGITAL sau prin intermediul aplicațiilor integratorilor autorizați. Cererea de înrolare conține (CEN EN 419 241-1: A.1.1; ETSI TS 119 431-1: LNK-6.2.2-02C):

– datele de identificare ale semnatarului (nume, prenume, data nașterii, cetățenia, codul numeric personal sau echivalentul pentru cetățenii străini, documentul de identitate);

– pentru persoanele juridice: denumirea, numărul de înregistrare, reprezentantul legal și persoanele fizice autorizate să activeze sigiliul;

– adresa de e-mail și numărul de telefon mobil, verificate prin coduri de confirmare;

– tipul de serviciu solicitat (semnătură / sigiliu) și politica de certificat aplicabilă;

– acceptarea Termenilor și condițiilor, a Politicii de protecție a datelor și consimțământul explicit pentru generarea și gestionarea cheilor de semnare pe seama semnatarului, conform art. 29 alin. (1a) din Regulamentul eIDAS.

Cererea, documentele și dovezile asociate sunt înregistrate în sistemul RA, cu marcarea temporală a fiecărui pas, și sunt păstrate conform secțiunii 14.6.

12.1.2. Verificarea cererii

Operatorul RA (sau, pentru fluxurile automatizate, sistemul de verificare cu supervizare umană) verifică completitudinea și coerența datelor, verifică documentele de identitate (elemente de securitate, valabilitate, consultarea surselor autoritative atunci când sunt disponibile), verifică autoritatea de reprezentare pentru persoanele juridice (extras ONRC, acte constitutive, împuterniciri) și aprobă sau respinge cererea, cu înregistrarea motivului. Regulile detaliate sunt stabilite în „Regulamentul de identificare și solicitare cerere semnătură" și în „Regulamentul de validare și aprobare cerere semnătură", aplicabile și serviciului rQSCD.

12.2. Verificarea identității (identity proofing)

12.2.1. Nivelul de verificare a identității

Pentru toate cheile de semnare gestionate în rQSCD, verificarea identității semnatarului se efectuează la **nivelul extins (extended LoIP)** definit în **ETSI TS 119 461 V2.1.1**, în conformitate cu art. 24 alin. (1) și (1a) din Regulamentul eIDAS și cu Regulamentul de punere în aplicare (UE) 2025/1566 (ETSI TS 119 431-1: LNK-A.7-01 [EUSPv2]; LNK-6.2.2-02A, LNK-6.2.2-02B). Nivelul extins asigură o încredere ridicată că identitatea declarată este reală, că dovezile de identitate sunt autentice și valide și că persoana care se înrolează este titularul identității (legarea persoanei de dovezi), cu rezistență la atacurile de prezentare (deepfake, măști, înregistrări).

12.2.2. Metode de verificare a identității acceptate

Se aplică metodele din DPC CERTDIGITAL G4, secțiunea 3.2.3:

Metodă	Descriere	Referință
Prezența fizică	Semnatarul (sau reprezentantul legal al persoanei juridice) se prezintă în fața unui operator de înregistrare CERTDIGITAL (angajat al CENTRUL DE CALCUL S.A., desemnat și instruit), la sediul sau la punctele de lucru ale CERTDIGITAL, cu actul de identitate, pașaportul sau permisul de ședere, în original	Art. 24 alin. (1a) lit. (d) din Regulamentul eIDAS; art. 16 alin. (3) lit. a) din Legea nr. 214/2024
CERTDIGITAL KYC	Înregistrare video realizată de semnatar, fără operator, cu verificarea automatizată a documentului de identitate și a persoanei, urmată de verificarea înregistrării de către un operator CERTDIGITAL în cel mult 24 de ore; compararea biometrică a imaginii faciale se face numai cu consimțământul explicit al semnatarului, care poate opta pentru prezența fizică	Art. 24 alin. (1a) lit. (c) din Regulamentul eIDAS; art. 16 alin. (3) lit. d) și e) din Legea nr. 214/2024
Certificat calificat CERTDIGITAL valabil	Numai pentru reînnoire, o singură dată consecutiv, pe baza unui certificat calificat emis după verificarea identității prin prezență fizică sau prin CERTDIGITAL KYC (secțiunea 12.2.3)	Art. 24 alin. (1a) lit. (b) din Regulamentul eIDAS; art. 16 alin. (3) lit. b) din Legea nr. 214/2024

Pentru cetățenii români, valabilitatea actului de identitate se verifică prin Platforma națională de interoperabilitate (art. 12 alin. (8) din Legea nr. 214/2024). Metoda utilizată este indicată în certificat prin identificatorul de politică 1.3.6.1.4.1.47898.4.2.2.{identificare}.{tip subiect} (G4), respectiv 1.3.6.1.4.1.47898.5.2.2.{identificare}.{tip subiect} (G5) (1 = prezență fizică; 4 = CERTDIGITAL KYC; 6 = certificat calificat).

Pentru **persoanele juridice**, verificarea include identitatea persoanei juridice (registrul comerțului sau registrul echivalent), identitatea persoanei fizice reprezentante (la nivel extins) și dovada autorității de reprezentare (CEN EN 419 241-1: A.1.3; LNK-6.2.2-02B).

12.2.3. Reutilizarea verificării identității

Reînnoirea pe baza unui certificat calificat CERTDIGITAL valabil, emis după verificarea identității prin prezență fizică sau prin CERTDIGITAL KYC, este permisă o singură dată consecutiv; semnatarul se autentifică cu mijlocul eID legat de cheia existentă, iar datele de identificare se verifică din nou dacă s-au modificat. La reînnoirea următoare, identitatea se verifică din nou prin prezență fizică sau prin CERTDIGITAL KYC (DPC CERTDIGITAL G4, secțiunea 3.3.1). Reînnoirea se face numai cu o pereche nouă de chei (secțiunea 13.7).

12.2.4. Identitatea pentru cheile de unică folosință

Nu se aplică: cheile de semnare de unică folosință nu se oferă la data prezentei versiuni (secțiunea 1.4.1).

12.3. Legarea mijlocului de identificare electronică de cheia de semnare

12.3.1. Principiu

Pentru cheile de lungă durată, controlul exclusiv este asigurat prin legarea criptografică a cheii de semnare de **referința mijlocului de identificare electronică** al semnatarului, înregistrată în SAM/rQSCD la înrolare (LNK-6.2.2-03A, LNK-6.2.2-10A). Referința este:

– pentru aplicația **CertDigital ID**: cheia publică de autentificare generată în elementul securizat al dispozitivului mobil înrolat, împreună cu identificatorul dispozitivului și atestarea hardware;

CERTDIGITAL se asigură că datele de identificare personală legate de referința mijlocului eID sunt identice cu cele ale subiectului certificatului calificat asociat (LNK-6.2.2-05); întrucât referința este stabilită de serviciul de înregistrare CERTDIGITAL în același proces cu emiterea certificatului, corespondența este garantată prin construcție.

12.3.2. Nivelul de asigurare al mijlocului eID

Mijloacele de identificare electronică utilizate pentru activare îndeplinesc cerințele de nivel **substanțial sau ridicat** privind caracteristicile și proiectarea (CEN EN 419 241-1, A.2.1) și mecanismul de autentificare (A.2.2) (LNK-6.2.2-02D, LNK-6.2.2-02E). Aplicația CertDigital ID implementează autentificare multifactor: factor de posesie (cheia dispozitiv-bound, neexportabilă, cu atestare hardware) și factor de cunoaștere sau inerență (PIN de minimum 6 cifre cu limitarea încercărilor, sau biometrie locală cu fallback la PIN), cu protecție dinamică împotriva atacurilor (detecția dispozitivelor compromise, protecția împotriva clonării, invalidarea la schimbarea dispozitivului).

12.3.3. Protecția legăturilor

Legăturile semnatar–referință eID–cheie de semnare–certificat sunt stocate în baza de date a SSAS și, pentru elementele critice controlului exclusiv, în interiorul SAM/HSM, protejate prin integritate criptografică (semnături/MAC cu chei interne HSM) astfel încât o modificare neautorizată (de exemplu, substituirea cheii publice de autentificare) să fie detectată și respinsă (LNK-6.2.2-10A; CEN EN 419 241-1: SRC_SKS.1.5). Modificarea legăturilor (de exemplu, înrolarea unui nou dispozitiv) necesită o nouă autentificare puternică a semnatarului sau o nouă verificare a identității, conform secțiunii 12.4.3, și este jurnalizată.

12.4. Furnizarea mijlocului de identificare electronică de către CERTDIGITAL

12.4.1. Aplicația CertDigital ID

CERTDIGITAL furnizează semnatarilor, ca mijloc de identificare electronică pentru activarea semnăturii, aplicația mobilă **CertDigital ID** (iOS/Android), distribuită exclusiv prin magazinele oficiale de aplicații, semnată de CERTDIGITAL și verificată la instalare (ETSI TS 119 431-1: EID-6.2.4-01, LNK-6.2.2-04).

12.4.2. Înrolarea dispozitivului și datele de activare

Înrolarea aplicației pe dispozitivul semnatarului se realizează numai după verificarea identității, printr-un proces care leagă dispozitivul de identitatea verificată: semnatarul scanează un cod de înrolare afișat în sesiunea autentificată (sau îl primește pe un canal distinct), aplicația generează perechea de chei de autentificare în elementul securizat, iar cheia publică și atestarea hardware sunt transmise SSAS și înregistrate ca referință a mijlocului eID. Codul PIN este ales de semnatar în aplicație și nu este niciodată transmis sau stocat de CERTDIGITAL; codurile de înrolare sunt de unică folosință, cu valabilitate de cel mult 15 minute, și sunt transmise pe un canal distinct de cel al aplicației (e-mail/SMS/afișare la ghișeu) (EID-6.2.4-02).

12.4.3. Gestionarea ciclului de viață al mijlocului eID

– **Înrolarea unui dispozitiv suplimentar / înlocuirea dispozitivului**: necesită autentificarea cu dispozitivul existent sau o nouă verificare a identității la nivel extins;

– **Blocarea**: după 5 încercări eșuate consecutive de PIN, aplicația se blochează; deblocarea necesită reverificarea identității; semnatarul poate solicita blocarea imediată prin portal, telefonic (cu verificarea identității) sau prin e-mail;

– **Revocarea mijlocului eID**: la pierderea sau compromiterea dispozitivului, la cererea semnatarului sau a abonatului, ori la detectarea unui comportament anormal; revocarea invalidează imediat referința eID în SAM, făcând imposibilă activarea cheii de semnare până la înrolarea unui nou dispozitiv;

– **Actualizarea aplicației**: versiunile cu vulnerabilități cunoscute sunt blocate la server; actualizarea este obligatorie.

12.5. Autentificarea delegată și utilizarea mijloacelor eID externe

Nu se aplică. Semnatarii se autentifică exclusiv cu aplicația CertDigital ID, furnizată de CERTDIGITAL (secțiunea 12.4); serviciul nu deleagă autentificarea către furnizori de identitate externi și nu utilizează, la data prezentei versiuni, mijloace eID notificate sau portofelul european pentru identitate digitală (ETSI TS 119 431-1: LNK-6.2.2-06 ÷ LNK-6.2.2-09). Orice extindere se descrie într-o versiune nouă a prezentului document, notificată ADR (secțiunea 16.4).

12.6. Legarea certificatului de cheia de semnare

După generarea perechii de chei în rQSCD (secțiunea 13.1), SSAS construiește cererea de certificare (PKCS#10) semnată cu cheia privată din rQSCD (dovada de posesie) și o transmite autorității de certificare (CERTDIGITAL QUALIFIED CA G4 sau CERTDIGITAL QCA G5) împreună cu aserțiunea de autentificare a semnatarului și cu referința procesului de verificare a identității (GEN-6.2.1-08; ETSI EN 319 411-1: REG-6.3.1-01). După emitere, certificatul este importat în SSAS și legat de cheia de semnare și de referința eID, cu verificarea corespondenței dintre cheia publică certificată și cheia din rQSCD (LNK-6.2.3-01 ÷ LNK-6.2.3-03; CEN EN 419 241-1: SRC_SKS.1.2, SRC_SKS.1.4, SRC_SKS.1.5).

Evidența SSAS menține, pentru fiecare cheie, legătura **unu-la-unu** între: identificatorul semnatarului (Subject ID), identificatorul cheii în rQSCD (Key ID), referința mijlocului eID și numărul de serie al certificatului calificat (Certificate ID), împreună cu jurnalul complet al etapelor: verificarea identității → generarea cheii → cererea de certificare → emiterea certificatului → legarea → acceptarea de către semnatar (checklist 4.2). Certificatul este pus la dispoziția semnatarului pentru acceptare; semnatarul este informat că poate solicita oricând revocarea certificatului și ștergerea cheii.

13. Ciclul de viață al cheilor de semnare

13.1. Generarea cheilor de semnare

13.1.1. Mediul de generare

Perechile de chei ale semnatarilor sunt generate **exclusiv în interiorul modulului criptografic certificat CEN EN 419 221-5** (rQSCD), utilizând generatorul de numere aleatoare al acestuia, evaluat în cadrul certificării, sub controlul SAM, fără ca vreo componentă a cheii private să părăsească vreodată mediul protejat în clar (CEN EN 419 241-1: SRA_SKM.1.1, SRG_KM.1.3, SRG_KM.1.4; ETSI TS 119 431-1: GEN-6.2.1-02, GEN-6.2.1-02A, GEN-6.2.1-04, GEN-6.2.1-05; GEN-A.4-01, GEN-A.4-02). Generarea are loc numai la cererea semnatarului (sau a abonatului pe seama semnatarului), după verificarea identității și acordarea consimțământului, conform art. 29 alin. (1a) din Regulamentul eIDAS.

13.1.2. Algoritmi și parametri

Algoritmii și lungimile de cheie utilizate sunt conforme cu documentul ENISA „Agreed Cryptographic Mechanisms" (ECCG) și cu ETSI TS 119 312 (GEN-6.2.1-03, GEN-6.2.1-06; CEN EN 419 241-1: SRG_KM.1.2, SRC_SKS.1.1; Reg. 2025/1567: OVR-6.8.5-02):

Tip cheie	Algoritm	Parametri acceptați	Valoare implicită
Chei de semnare (semnătură / sigiliu)	RSA	3072 sau 4096 biți, exponent public 65537	RSA 3072
Chei de semnare (semnătură / sigiliu)	ECDSA	curbele NIST P-256, P-384	–
Algoritm de semnătură	RSASSA-PKCS1-v1_5 sau RSA-PSS cu SHA-256, SHA-384, SHA-512; ECDSA cu SHA-256/384	conform ETSI TS 119 312	–
Funcții hash pentru DTBS/R	SHA-256, SHA-384, SHA-512	SHA-1 și MD5 sunt respinse	SHA-256

Parametrii sunt revizuiți cel puțin anual și ori de câte ori ENISA/ECCG sau ETSI publică actualizări; mecanismele devenite inadecvate sunt dezactivate pentru chei noi, iar cheile existente sunt migrate în perioada stabilită (secțiunea 15.6).

Parametrii de mai sus se încadrează în configurația certificată a QSCD: ADSS SAM v7.0.2 (Security Target v8, tabelul 6-4: RSASSA-PKCS1-v1_5 și RSASSA-PSS cu chei RSA de 2048–8192 de biți; ECDSA pe curbele NIST P-256, P-384, P-521 și Brainpool; SHA-2 și SHA-3) și Utimaco CryptoServer CP5, firmware 5.1.0.0 (Security Target Lite v2.1.2: RSA de 2048–8192 de biți; ECDSA de cel puțin 224 de biți pe curbele NIST și Brainpool).

13.1.3. Momentul generării și atributele cheii

Cheile de semnare sunt generate în procesul de înrolare, imediat înainte de cererea de certificare (GEN-6.2.1-07; SRC_SKS.1.3). Fiecare cheie este creată cu atribute impuse de modulul criptografic: neexportabilă, utilizabilă exclusiv pentru semnare, utilizabilă numai cu autorizarea SAM, asociată identificatorului semnatarului; momentul generării, identificatorul

cheii, algoritmul și identitatea operatorului/sistemului care a declanșat operațiunea sunt jurnalizate.

13.1.4. Dovada de posesie și certificarea

Cheia publică este transmisă serviciului de înregistrare al CA în cererea PKCS#10 semnată cu cheia privată corespunzătoare, împreună cu aserțiunea de autentificare a semnatarului (secțiunea 12.6). CA emite certificatul calificat numai pentru chei generate în rQSCD, incluzând declarația QcSSCD, politica QCP-n-qscd / QCP-l-qscd și identificatorii CERTDIGITAL 1.3.6.1.4.1.47898.4.2.2.{identificare}.{tip subiect} (G4) sau 1.3.6.1.4.1.47898.5.2.2.{identificare}.{tip subiect} (G5) și 1.3.6.1.4.1.47898.11.1.1, precum și identificatorul politicii EUSPv2 (0.4.0.19431.1.1.4) (secțiunea 17.1).

13.2. Activarea semnăturii

13.2.1. Condiții de activare

Cheia de semnare este activată de SAM pentru o operațiune de semnare **numai dacă sunt îndeplinite cumulativ** următoarele condiții (CEN EN 419 241-1: SRC_SA.1.2 ÷ SRC_SA.1.5, SRA_SKM.2.1, SRA_SAP.1.2, SRA_SKM.2.5; ETSI TS 119 431-1: SIG-6.3.1-01 ÷ SIG-6.3.1-07, SIG-6.3.1-09):

– SAD valide au fost primite, autentificate cu cheia corespunzătoare referinței eID legate de cheia de semnare;

– semnatarul a fost autentificat cu cel puțin doi factori, la nivel substanțial sau ridicat, în cadrul aceleiași sesiuni;

– SAD identifică explicit cheia de semnare și DTBS/R autorizate, iar acestea corespund cererii transmise de SSA;

– SAD nu sunt expirate, nu au fost utilizate anterior (valoare unică) și sunt destinate SAM-ului CERTDIGITAL;

– certificatul asociat cheii este valabil – nu este expirat sau revocat –, verificarea fiind efectuată de SSA față de baza de date a CA și de OCSP înainte de transmiterea cererii către SAM (SIG-6.3.1-08);

– cheia nu este blocată administrativ (secțiunea 13.6);

Activarea este valabilă exclusiv pentru DTBS/R enumerate în SAD; orice altă cerere de semnare, chiar în aceeași sesiune, necesită SAD noi. Semnătura este calculată de modulul criptografic cu algoritmul și parametrii indicați în cerere, verificați față de lista de algoritmi aprobați (SIG-6.3.1-10; SRC_DSC.1.1).

13.2.2. Prezentarea datelor de semnat și consimțământul (WYSIWYS)

CERTDIGITAL garantează principiul „ceea ce vezi este ceea ce semnezi" (anexa II pct. 2 din Regulamentul eIDAS; checklist 3.3):

– SIC afișează semnatarului documentul integral (sau conținutul critic, pentru documentele structurate, cu posibilitatea vizualizării complete), în format nealterat, înainte de solicitarea factorului de autentificare;

– hash-ul inclus în SAD este calculat de SIC asupra conținutului afișat și este comparat cu DTBS/R transmise de SCA; neconcordanța blochează semnarea;

– aplicația client nu poate modifica DTBS/R după prezentare; SAM semnează exact hash-urile din SAD;

– consimțământul este exprimat printr-o acțiune explicită (derularea documentului până la final și apăsarea butonului „Semnează", urmată de PIN/biometrie), nu prin simpla bifare a unei casete;

– pentru sigilii, acțiunea explicită este efectuată de persoana fizică autorizată de persoana juridică, identificată la înrolare;

– mecanismul WYSIWYS este supus revizuirii de cod și testării independente, iar raportul este pus la dispoziția CAB.

13.2.3. Sesiunile de semnare

Sesiunea de semnare este creată de SSA la primirea cererii, este identificată unic și este legată de semnatar, de aplicația client și de cheia de semnare. Durata maximă a unei sesiuni este de 10 minute între inițiere și primirea SAD (reînnoibilă numai prin nouă autorizare a semnatarului). La expirare, sesiunea și SAD aferente sunt invalidate.

13.2.4. Formate de semnătură și servicii conexe

Valoarea semnăturii returnată de rQSCD este asamblată de aplicația client în formatele baseline PAdES (ETSI EN 319 142-1), XAdES (ETSI EN 319 132-1), CAdES (ETSI EN 319 122-1), JAdES (ETSI TS 119 182-1) sau în containere ASiC (ETSI EN 319 162-1/-2), la nivelurile B-B, B-T, B-LT și B-LTA. Nivelul implicit este **B-T** (cu marcă temporală calificată CERTDIGITAL TSA G4); nivelul **B-LT/B-LTA** este aplicat la cererea abonatului, cu includerea răspunsurilor OCSP și a lanțului de certificate. Semnăturile produse sunt verificate periodic cu aplicația DSS a Comisiei Europene și cu serviciul de validare CertDigital (checklist 5.3).

13.3. Utilizarea cheii de semnare

– Cheia de semnare este utilizată numai pentru crearea semnăturilor electronice calificate sau a sigiliilor electronice calificate, în cazurile pentru care semnatarul și-a dat consimțământul (SIG-6.3.1-09).

– Fiecare utilizare este jurnalizată de SAM/HSM (identificatorul cheii, identificatorul sesiunii, hash-urile semnate, momentul, rezultatul) și corelată cu jurnalul SSA.

– Semnatarul are acces, prin portal și aplicație, la istoricul propriilor operațiuni de semnare (data, aplicația client, denumirea documentului) și primește notificări la fiecare semnare.

– Frecvența anormală a operațiunilor, tentativele eșuate de activare și utilizarea din locații/dispozitive necunoscute declanșează alerte și, după caz, blocarea preventivă a cheii.

13.4. Copiile de siguranță și recuperarea cheilor de semnare

În conformitate cu art. 29a alin. (1) lit. (b) din Regulamentul eIDAS, CERTDIGITAL duplică datele de creare a semnăturii electronice **exclusiv în scopul asigurării continuității serviciului**, cu respectarea următoarelor condiții (CEN EN 419 241-1: SRG_KM.2.1 ÷ SRG_KM.2.3; ETSI TS 119 431-1: GEN-6.3.3-01 ÷ GEN-6.3.3-04):

– copiile de siguranță sunt realizate exclusiv prin mecanismele interne ale modulului criptografic certificat (export criptat cu chei de backup gestionate de HSM, sub control dual M din N), astfel încât cheile nu sunt niciodată disponibile în clar în afara unui HSM certificat CEN EN 419 221-5; nivelul de securitate al copiilor este identic cu cel al originalului;

– copiile pot fi restaurate numai într-un modul criptografic de același tip, certificat și configurat identic, aparținând CERTDIGITAL, prin procedură cu control dual și martori, jurnalizată;

– numărul copiilor este limitat la **minimul necesar continuității**: cheile se află în dispozitivul de producție și, pentru continuitatea serviciului, în dispozitivul de rezervă, iar copiile de rezervă criptate se păstrează în spații securizate, cu control dual;

– copiile de siguranță sunt distruse odată cu ștergerea cheii (secțiunea 13.5), prin ștergerea criptografică a materialului de backup și reînnoirea periodică a cheilor de backup (SRG_KM.7.3, DEL-6.3.2-04);

– legătura cheie–referință eID–certificat este inclusă în backup, astfel încât restaurarea să nu afecteze controlul exclusiv.

Procedura de backup și restaurare este descrisă în „Procedura de salvare și restaurare a datelor" (P.SMSI-0.14) și în procedura specifică HSM; testarea restaurării este efectuată cel puțin anual, în cadrul testelor de continuitate (secțiunea 14.8).

13.5. Ștergerea cheilor de semnare

Cheia de semnare este distrusă ireversibil în modulul criptografic (ștergere criptografică a obiectului de cheie și a eventualelor copii) în următoarele situații (CEN EN 419 241-1: SRG_KM.7.1 ÷ SRG_KM.7.3; ETSI TS 119 431-1: DEL-6.3.2-01 ÷ DEL-6.3.2-05):

Situație	Acțiune	Termen
Revocarea certificatului calificat asociat (din orice motiv)	CA notifică SSAS; SSAS blochează imediat cheia și declanșează ștergerea	Blocare imediată; ștergere în cel mult 24 de ore de la revocare
Cererea semnatarului sau a abonatului	După autentificarea solicitantului și verificarea dreptului acestuia; certificatul este revocat simultan	Imediat după validarea cererii
Expirarea certificatului	Cheia este ștearsă, nemaiavând utilizare legitimă	În cel mult 24 de ore de la expirare

Situație	Acțiune	Termen
Decesul semnatarului, încetarea persoanei juridice, încetarea raportului cu abonatul (pentru chei de angajat)	La cererea documentată a persoanelor îndreptățite	Imediat după validare
Încetarea serviciului	Conform planului de încetare (secțiunea 14.9)	Conform planului

Ștergerea include materialul de backup asociat și este jurnalizată (identificatorul cheii, motivul, momentul, operatorul/sistemul). Datele de sesiune și SAD sunt distruse la închiderea sesiunii (SRG_KM.7.2, DEL-6.3.2-03). Semnatarul este informat prin notificare despre ștergerea cheii sale.

13.6. Blocarea activării cheii

CERTDIGITAL nu oferă suspendarea certificatelor (DPC CERTDIGITAL G4, secțiunea 4.9). Independent de revocarea certificatului, activarea unei chei de semnare poate fi blocată imediat, 24/7: la cererea semnatarului (de exemplu, la pierderea telefonului), la detectarea unor indicatori de compromitere a mijlocului eID sau de fraudă ori la decizia Ofițerului de Securitate IT în cadrul gestionării unui incident. Blocarea este aplicată în SAM (marcarea cheii ca inactivă) și poate fi ridicată numai după reautentificarea puternică a semnatarului sau reverificarea identității, cu înregistrarea motivului. Blocarea nu afectează valabilitatea semnăturilor create anterior și nu modifică starea certificatului; dacă motivul blocării persistă, certificatul se revocă (DPC CERTDIGITAL G4, secțiunea 4.9), iar cheia se distruge (secțiunea 13.5).

13.7. Reînnoirea cheilor și schimbarea cheilor

Reînnoirea certificatului calificat se face numai cu generarea unei perechi noi de chei (re-key), conform secțiunii 13.1 (DPC CERTDIGITAL G4, secțiunea 3.3.1); nu se emit certificate noi pentru o cheie existentă. Vechea cheie este distrusă la expirarea sau revocarea vechiului certificat (secțiunea 13.5).

Cheile infrastructurii (cheile interne ale dispozitivului, cheile de backup, cheile TLS, cheile de sigilare a jurnalelor) sunt supuse propriului ciclu de viață, descris în secțiunea 15.6.

14. Controale privind facilitățile, managementul și operarea

14.1. Cerințe generale

14.1.1. Evaluarea riscurilor

CERTDIGITAL efectuează și menține o **evaluare a riscurilor** specifică serviciului rQSCD, integrată în sistemul de management al securității informației al CENTRUL DE CALCUL S.A. și în cadrul de gestionare a riscurilor de securitate cibernetică impus de art. 21 din Directiva NIS2, de Regulamentul de punere în aplicare (UE) 2024/2690, de art. 24 alin. (2) lit. (fa) din Regulamentul eIDAS și de Regulamentul de punere în aplicare (UE) 2025/2530 (ETSI EN 319 401: REQ-5-01 ÷ REQ-5-05; ETSI TS 119 431-1: OVR-6.4.1-01; checklist 1.2). Evaluarea:

– identifică, analizează și evaluează riscurile de afaceri și tehnice ale serviciului, inclusiv amenințările specifice semnării la distanță: compromiterea dispozitivului calificat, falsificarea sau reutilizarea SAD, compromiterea aplicației CertDigital ID (malware pe dispozitivul mobil), substituirea documentelor, atacuri asupra procesului de identificare (deepfake), atacuri asupra lanțului de aprovizionare (firmware, biblioteci software), indisponibilitatea serviciului, erori ale personalului în roluri de încredere;

– utilizează metodologia ISO/IEC 27005 (probabilitate × impact, scale definite), documentată în „Procedura de evaluare și tratare a riscurilor IT" (CD_SI_020) și în „Identificarea și evaluarea riscurilor" (P.SMSI-0.17);

– selectează măsurile de tratare proporționale cu riscul și le documentează în Planul de tratare a riscurilor IT (CD_SI_019), din care decurg controalele descrise în prezentul document și în politica de securitate;

– include evaluarea riscurilor induse de furnizorii critici (producătorul dispozitivului și al modulului criptografic, furnizorii de software și de conectivitate), conform secțiunii 15.4.3;

– este revizuită **cel puțin anual** și la fiecare modificare semnificativă (arhitectură, standarde, incidente majore, rezultate ale testelor de penetrare);

– este aprobată de management, care acceptă formal riscurile reziduale prin semnătura Directorului General și a Ofițerului de Securitate IT; registrul riscurilor este actualizat cel puțin semestrial.

14.1.2. Politica de securitate a informației

CERTDIGITAL menține „Politica de securitate a informațiilor" (P.SMSI-0.10) și „Politica Sistemului de Management al Securității Informației" (P.SMSI-0.16), aprobate de management, care stabilesc abordarea organizației privind securitatea, controalele și procedurile operaționale aplicabile facilităților, sistemelor și activelor informaționale ale serviciului rQSCD (ETSI EN 319 401: clauza 6.3). Politica este comunicată personalului și, în măsura în care este relevant, terților; modificările sunt comunicate părților interesate (abonați, CAB, ADR) atunci când le afectează. Politica este completată de setul de proceduri SMSI enumerat în Anexa C.

14.1.3. Managementul activelor

Toate activele serviciului rQSCD (module criptografice, smartcard-uri de administrare, servere SSA, baze de date, aplicații, chei criptografice, documentație, medii de stocare, dispozitive de backup) sunt inventariate, clasificate în funcție de criticitate și de nivelul de confidențialitate (public / intern / restricționat / strict secret – material criptografic) și au un proprietar desemnat (ETSI EN 319 401: clauza 7.3). Mediile de stocare care conțin material criptografic sau date de identificare sunt manipulate conform clasificării: transport în containere sigilate cu evidență de custodie, stocare în seifuri, distrugere securizată conform DIN 66399 (nivel H-5/P-5 sau superior) cu certificat de distrugere; echipamentele retrase sunt zeroizate conform procedurii de dezafectare (secțiunea 14.2.4).

14.2. Controale de securitate fizică

14.2.1. Amplasarea și construcția

Componentele critice ale serviciului (aparatele SAM, servere SSA, servere RA/CA, echipamente de rețea) sunt găzduite în două centre de date proprii din Târgu Jiu, separate geografic: un centru principal și un centru secundar de rezervă, pregătit să preia serviciile (activ-pasiv). Centrul principal este proiectat după recomandările TIA-942 pentru nivelul Tier 3. Accesul fizic este controlat pe zone de securitate (ETSI EN 319 401: clauza 7.6; ETSI TS 119 431-1: OVR-6.4.2-01, OVR-6.4.2-02; ETSI EN 319 411-1: OVR-6.4.2-02 ÷ OVR-6.4.2-10; checklist 2.2).

14.2.2. Zonele de securitate și accesul fizic

Zonă	Conținut	Control de acces
Zona 1 – perimetru	Clădirea	Control la intrare, supraveghere video
Zona 2 – zona operatorilor	Stațiile operatorilor de înregistrare, birourile personalului cu roluri de încredere	Cartelă de acces individuală, jurnalizare; vizitatorii au acces numai însoțiți
Zona 3 – sala serverelor	Servere SSA, RA, CA, rețea, stocare	Autentificare în patru factori (cheie, cartelă, cod și amprentă), jurnalizare electronică, supraveghere video
Zona 4 – zona criptografică	Aparatele SAM și modulele criptografice, suporturile cu copii de rezervă, cardurile de administrare	Acces numai pentru persoanele cu roluri de încredere autorizate, autentificare în patru factori (cheie, cartelă, cod și amprentă), control dual pentru operațiunile asupra dispozitivelor, supraveghere video

Toate intrările și ieșirile sunt înregistrate electronic. Accesul persoanelor externe (întreținere, auditori) este permis numai însoțit, pe baza aprobării prealabile a Ofițerului de Securitate IT, cu consemnare în registrul de acces. Măsurile detaliate de protecție sunt descrise în documentația internă de securitate și sunt puse la dispoziția CAB și ADR (checklist 2.2).

14.2.3. Controale de mediu

Centrele de date au alimentare electrică redundantă, surse neîntreruptibile (UPS) și generator, climatizare redundantă, sisteme de detecție și alarmare la incendiu cu mijloace de

stingere adecvate echipamentelor electronice și protecție împotriva inundațiilor, dimensionate pentru funcționarea continuă a serviciilor.

14.2.4. Dezafectarea echipamentelor criptografice

Scoaterea din uz a unui modul criptografic (defectare, înlocuire, sfârșitul ciclului de viață) se efectuează conform procedurii standard de operare „HSM Zeroization": verificarea migrării/ștergerii cheilor, zeroizarea memoriei nevolatile prin comanda certificată a producătorului, executată cu control dual și martor, verificarea stării zeroizate, consemnarea în registrul de distrugere; în cazul în care zeroizarea nu este posibilă, echipamentul este distrus fizic printr-un furnizor specializat, cu certificat de distrugere (checklist 2.3). Smartcard-urile de administrare retrase sunt distruse fizic.

14.3. Controale procedurale

14.3.1. Rolurile de încredere

CERTDIGITAL definește următoarele roluri de încredere pentru serviciul rQSCD, descrise în fișele de post (CD_SI_000) și în „Procedura de administrare a utilizatorilor cu drepturi privilegiate" (P.SMSI-0.9) (ETSI EN 319 401: REQ-7.4-03X, REQ-7.4-04X, REQ-7.4-07X ÷ REQ-7.4-12X; ETSI TS 119 431-1: OVR-6.4.3-01A, OVR-6.8.1-01; checklist 6.3):

Rol	Responsabilități principale
Ofițer de Securitate IT (Security Officer)	Responsabilitatea generală pentru implementarea politicilor și practicilor de securitate; aprobarea accesului; coordonarea răspunsului la incidente; relația cu ADR/CSIRT; custode al unei părți din secretele HSM
Administrator HSM / Custode de chei (Key Custodian)	Administrarea modulelor criptografice și a SAM în regim M din N; participarea la ceremoniile de chei; gestionarea backup-urilor criptografice; nu are acces la aplicațiile de operare
Administrator de sistem	Instalarea, configurarea și întreținerea serverelor, rețelei și aplicațiilor SSA/RA; nu deține smartcard-uri HSM și nu poate modifica configurația SAM
Operator de sistem	Operarea zilnică, monitorizarea, backup-ul și restaurarea sistemelor; fără drepturi administrative asupra HSM
Operator RA / Agent de înregistrare	Verificarea identității, validarea cererilor de înrolare, aprobarea generării cheilor și a cererilor de certificare; verificarea înregistrărilor CERTDIGITAL KYC
Auditor de sistem	Accesul în citire la jurnalele de audit și la configurații, pentru revizuire; independent de administrare și operare
Responsabil cu protecția datelor (DPO)	Supravegherea conformității cu GDPR
Manager Servicii Electronice Calificate	Responsabilitatea operațională a serviciului; aprobarea procedurilor operaționale

14.3.2. Separarea sarcinilor și controlul multiplu

– Nicio persoană nu poate cumula rolurile de Administrator HSM, Administrator de sistem și Auditor de sistem; rolul de Operator RA este incompatibil cu rolul de Administrator de sistem; Ofițerul de Securitate IT nu administrează singur sistemele de producție.

– Operațiunile critice asupra dispozitivului calificat (inițializare, modificarea politicilor, restaurarea copiilor de rezervă, activarea modului administrativ, actualizarea firmware-

ului) necesită prezența simultană a unui număr minim de custozi de chei (M din N), autentificați cu smartcard-uri distincte, în prezența Ofițerului de Securitate IT sau a unui martor independent, cu proces-verbal semnat și, pentru ceremoniile de chei ale infrastructurii, înregistrare video (checklist 6.3).

– Platforma respinge și alertează automat orice tentativă individuală de a modifica profilurile de autorizare către nucleul criptografic; tentativele sunt analizate ca incidente de securitate.

– Accesul privilegiat la sistemele de producție se realizează prin stații de administrare dedicate (jump hosts), cu autentificare multifactor, sesiuni înregistrate și revizuite de Auditorul de sistem.

14.3.3. Proceduri operaționale documentate

Toate activitățile operaționale ale serviciului sunt executate conform procedurilor documentate și aprobate (Anexa C), inclusiv: ceremonia de inițializare a HSM/SAM, înrolarea și revocarea mijloacelor eID, generarea și ștergerea cheilor, gestionarea sesiunilor blocate, backup și restaurare, gestionarea schimbărilor, gestionarea incidentelor, dezafectarea. Procedurile sunt revizuite anual.

14.4. Controale de personal

CERTDIGITAL aplică cerințele ETSI EN 319 401, clauza 7.2, și adaptările din Regulamentul de punere în aplicare (UE) 2025/1567 (ETSI TS 119 431-1: OVR-6.4.4-01 ÷ OVR-6.4.4-03):

– **Angajarea**: personalul în roluri de încredere este angajat al CENTRUL DE CALCUL S.A., pe baza unui contract individual de muncă care include obligații de confidențialitate și de respectare a politicilor de securitate; verificarea antecedentelor (cazier judiciar, verificarea identității, a studiilor și a experienței, referințe) este efectuată înainte de acordarea accesului și reînnoită la cel mult 3 ani; persoanele condamnate pentru infracțiuni incompatibile cu rolul nu pot ocupa roluri de încredere.

– **Competența**: personalul în roluri de încredere, inclusiv eventualii subcontractanți, deține cunoștințele de specialitate, experiența și calificările necesare, dobândite prin instruire formală, certificări (de exemplu, certificări de securitate a informației, certificări ale producătorului HSM) sau experiență, documentate în dosarul de personal (OVR-6.4.4-02).

– **Instruirea**: instruire inițială înainte de acordarea accesului (politici, proceduri, utilizarea dispozitivului calificat, protecția datelor, recunoașterea atacurilor de inginerie socială) și instruire de actualizare **cel puțin o dată la 12 luni** privind noile amenințări și practicile curente de securitate, cu evidența participării și evaluarea cunoștințelor (OVR-6.4.4-03); operatorii RA care verifică înregistrările CERTDIGITAL KYC sunt instruiți suplimentar în detectarea fraudelor documentare și a atacurilor de prezentare.

– **Sancțiuni**: încălcarea politicilor atrage măsuri disciplinare conform Regulamentului intern, până la încetarea contractului și sesizarea organelor competente; accesul este revocat imediat la încetarea raporturilor de muncă sau la schimbarea rolului.

– **Conflicte de interese**: personalul în roluri de încredere nu poate desfășura activități care ar putea afecta imparțialitatea (de exemplu, operatorul RA nu poate valida propria cerere sau cererile rudelor).

– **Lista personalului**: lista actualizată a personalului cu roluri de încredere (CD_SI_000) este transmisă ADR conform procedurii de acreditare.

14.5. Procedurile de jurnalizare a evenimentelor (audit logging)

14.5.1. Evenimente jurnalizate

CERTDIGITAL înregistrează toate evenimentele relevante pentru securitatea și operarea serviciului (ETSI EN 319 401: clauza 7.10; ETSI TS 119 431-1: OVR-6.4.5-01 ÷ OVR-6.4.5-07; CEN EN 419 241-1: SRG_AA.1 ÷ SRG_AA.3, SRG_AA.7, SRG_AA.8; checklist 6.1):

Categorie	Evenimente
Ciclul de viață al cheilor	Generarea, legarea certificatului, legarea referinței eID, blocarea/deblocarea, ștergerea, backup-ul și restaurarea cheilor de semnare
Activarea semnăturii	Inițierea sesiunii, emiterea valorii unice a sesiunii, primirea SAD, rezultatul validării SAD (inclusiv motivul respingerii: semnătură invalidă, expirare, replay, neconcordanță hash), activarea cheii, calculul semnăturii, închiderea sesiunii
Înregistrare și identificare	Cererile de înrolare, rezultatele verificării identității (metodă, operator, decizie, identificatorul procesului), înrolarea și revocarea mijloacelor eID
HSM / SAM	Autentificările administrative, operațiunile M din N, modificările de politică, actualizările de firmware, alarmele de tamper, pornirea/oprirea, erorile hardware, auto-testele
Sisteme și rețea	Pornirea/oprirea sistemelor, căderile și defecțiunile hardware, activitatea firewall-urilor și routerelor (conexiuni respinse, modificări de reguli), tentativele de acces la sistemele SSAS, modificările de configurație, activitatea conturilor privilegiate
Securitate	Modificările politicii de securitate, alertele IDS/IPS, rezultatele scanărilor de vulnerabilități, evenimentele antivirus/EDR, accesul fizic
Aplicații client	Înregistrarea, autentificarea și autorizarea aplicațiilor client; cererile API (fără conținutul documentelor)

Fiecare înregistrare conține: tipul evenimentului, data și ora (UTC, cu precizie de milisecundă), identitatea entității care a declanșat evenimentul (utilizator, rol, sistem, aplicație client), identificatorii obiectelor afectate (cheie, sesiune, certificat), rezultatul și, după caz, adresa sursă. Conținutul documentelor semnate **nu este jurnalizat și nu este stocat** de serviciu, cu excepția hash-urilor și a metadatelor.

14.5.2. Protecția jurnalelor

– Jurnalele sunt generate la sursă și transmise către sistemul centralizat de jurnalizare (intern), cu acces limitat la Ofițerul de Securitate IT, la auditorii de sistem și la evaluatori, și sunt protejate împotriva modificării și ștergerii neautorizate, cu verificarea integrității.

– Jurnalele aparatelor SAM sunt protejate în integritate de dispozitiv, conform configurației evaluate.

– Toate sistemele sunt sincronizate cu o sursă de timp de referință trasabilă la UTC (secțiunea 15.7), cu monitorizarea deviațiilor mai mari de 1 secundă (SRG_AA.8).

– Jurnalele sunt analizate zilnic, automat, cu alertare la evenimente anormale; analiza manuală se face cel puțin lunar, cu consemnarea concluziilor.

– Capacitatea de stocare este monitorizată; jurnalele sunt incluse în copiile de siguranță conform secțiunii 14.8.

14.6. Arhivarea înregistrărilor

CERTDIGITAL arhivează și păstrează (ETSI TS 119 431-1: OVR-6.4.6-01; Legea nr. 214/2024; DPPC-CA_G4):

Înregistrări	Perioada minimă de păstrare
Jurnalele de audit ale serviciului (inclusiv activările semnăturii, ciclul de viață al cheilor, identificarea)	**10 ani** de la momentul în care orice certificat bazat pe aceste înregistrări încetează să mai fie valabil (cerința minimă ETSI fiind de 7 ani)
Dovezile verificării identității (copii ale documentelor, înregistrări video, rezultate biometrice, rapoarte ale proceselor automate)	10 ani de la încetarea valabilității certificatului, cu respectarea principiului minimizării (înregistrările video și datele biometrice sunt păstrate criptat, cu acces restricționat, și sunt șterse la expirarea termenului)
Contractele, acceptările termenilor și condițiilor, consimțămintele	10 ani de la încetarea relației contractuale
Procesele-verbale ale ceremoniilor de chei, registrele de acces fizic, rapoartele de audit intern/extern, rapoartele de incident	10 ani
Documentele de politică și practici, în toate versiunile	Permanent (pe durata existenței organizației și conform planului de încetare)

Arhiva este stocată în două locații (centrul principal și DR), în formă criptată și cu integritate verificabilă (sigiliu electronic + marcă temporală), cu acces controlat și jurnalizat, și este disponibilă pentru CAB, ADR și, în condițiile legii, pentru instanțe. Prelucrarea datelor cu caracter personal din arhivă respectă secțiunea 18.4.

14.7. Schimbarea cheilor infrastructurii

Nu există cerințe de politică specifice pentru cheile semnatarilor (ETSI TS 119 431-1: clauza 6.4.7); schimbarea cheilor infrastructurii (CA, TSA, SAM, backup HSM, TLS) este descrisă în secțiunea 15.6 și în declarațiile de practici ale serviciilor respective.

14.8. Compromiterea, incidentele și recuperarea în caz de dezastru

14.8.1. Gestionarea incidentelor de securitate

CERTDIGITAL aplică „Procedura de management al incidentelor de securitate a informației” (P.SMSI-0.11), Planul de răspuns la incidente de securitate și Procedura de notificare a incidentelor (00q), aliniate la ETSI EN 319 401, clauza 7.9, la art. 23 din Directiva NIS2 și la Regulamentul de punere în aplicare (UE) 2024/2690 (ETSI TS 119 431-1: OVR-6.4.8-01; checklist 1.5):

– **Detecția**: monitorizare 24/7 a evenimentelor de securitate (sistemul centralizat de jurnalizare, IDS/IPS, protecția stațiilor), alertele dispozitivului calificat (tamper, auto-teste eșuate, rate anormale de SAD respinse), monitorizarea disponibilității; canalul public de raportare publicat în depozit (politica CVD).

– **Clasificarea**: incidentele sunt clasificate în funcție de impactul asupra confidențialității, integrității și disponibilității serviciului și asupra persoanelor (nivelurile: minor / major / critic), conform matricei din procedură; evaluarea inițială se face în cel mult 4 ore de la detecție.

– **Răspunsul**: echipa de răspuns (Ofițerul de Securitate IT – coordonator, Administratorul HSM, Administratorul de sistem, Managerul Servicii Electronice Calificate, DPO, reprezentant juridic) acționează conform scenariilor predefinite: compromiterea SIC (revocarea mijlocului eID, blocarea cheilor), compromiterea SSA (izolarea, blocarea activărilor – SAM continuă să refuze SAD invalide), suspiciunea de compromitere a HSM/SAM (oprirea serviciului, blocarea cheilor, revocarea certificatelor afectate, notificare), compromiterea cheilor infrastructurii, atac DDoS, ransomware, breșă de date personale.

– **Comunicarea**: în cazul unei compromiteri care afectează cheile de semnare, semnatarii afectați sunt informați fără întârziere, certificatele sunt revocate, iar părțile utilizatoare sunt informate prin depozit.

– **Învățarea**: fiecare incident major sau critic este urmat de o analiză post-incident, cu cauze, măsuri corective și actualizarea evaluării riscurilor.

– **Testarea**: planul este testat cel puțin anual prin exerciții de tip tabletop (scenarii: ransomware, compromiterea SAM, deepfake în identificare), consemnate în procese-verbale.

14.8.2. Notificarea organismului de supraveghere și a CSIRT

Orice încălcare a securității sau perturbare cu impact semnificativ asupra serviciului sau asupra datelor cu caracter personal este notificată conform art. 24 alin. (2) lit. (fb) din Regulamentul eIDAS, art. 23 din Directiva (UE) 2022/2555, OUG nr. 155/2024, Legii nr. 214/2024 și Procedurii de notificare a incidentelor (00q):

Termen	Destinatar	Conținut
Fără întârziere, dar nu mai târziu de **24 de ore** de la luarea la cunoștință	ADR (organism de supraveghere) și DNSC (CSIRT național)	Avertizare timpurie: natura incidentului, suspiciunea de acțiune ilegală/rău-intenționată, impactul transfrontalier
În cel mult **72 de ore**	ADR, DNSC	Notificarea incidentului: evaluarea inițială a gravității și impactului, indicatorii de compromitere
În cel mult **o lună**	ADR, DNSC	Raport final: descriere detaliată, tipul amenințării, cauza, măsurile aplicate, impactul transfrontalier
Fără întârziere	Persoanele fizice/juridice afectate, publicul (dacă este în interesul public)	Informare privind breșa și măsurile recomandate
În cel mult 72 de ore	ANSPDCP	Breșele de date cu caracter personal (art. 33 GDPR)

Datele de contact oficiale ale ADR, DNSC și ANSPDCP sunt configurate în sistemul de gestionare a incidentelor; persoana de contact desemnată în relația cu ADR este Ofițerul de Securitate IT.

14.8.3. Continuitatea activității și recuperarea în caz de dezastru

CERTDIGITAL aplică Planul de continuitate a afacerii (PO/C/SI/S/63) și Procedura de recuperare în caz de dezastru (PO/SI/63), aplicabile serviciului rQSCD (ETSI EN 319 401: clauza 7.11; checklist 1.3):

– **Arhitectură redundantă**: două centre de date proprii (principal și secundar, activ-pasiv), câte un aparat SAM în fiecare, servere în configurație redundantă, baze de date replicate asincron către centrul secundar, conectivitate dublă.

– **Obiective**: durata maximă de restabilire a serviciului rQSCD de 8 ore (PO/SI/63, cap. 3.3); pierderea maximă de date (RPO) de cel mult 5 minute pentru bazele de date ale serviciului, conform programului de replicare din PO/SI/63; serviciile de revocare și de stare a certificatelor au obiectivele stabilite în PO/SI/63.

– **Backup**: copii de siguranță ale bazelor de date și ale configurațiilor, păstrate criptat în ambele centre; copiile cheilor conform secțiunii 13.4.

– **Testare**: test anual de comutare către centrul secundar și test anual de restaurare a copiilor de rezervă ale cheilor într-un dispozitiv de rezervă, cu procese-verbale care demonstrează atingerea obiectivelor.

– **Gestionarea crizei**: echipa de criză, lanțul de comandă, comunicarea cu abonații, ADR și furnizorii, conform planului.

14.8.4. Compromiterea cheilor infrastructurii

În cazul compromiterii (sau al suspiciunii de compromitere) a cheilor SAM, ale CA sau ale altor componente ale infrastructurii, CERTDIGITAL aplică procedura de compromitere: oprirea imediată a utilizării cheii, revocarea certificatelor corespunzătoare, informarea ADR, a semnatarilor și a părților utilizatoare, generarea de noi chei printr-o ceremonie documentată, reemiterea certificatelor afectate și analiza cauzelor. Evaluarea impactului asupra semnăturilor create anterior este comunicată public în depozit.

14.9. Încetarea serviciului

14.9.1. Planul de încetare

CERTDIGITAL menține un **Plan de încetare a serviciilor** (00r; CD_SI_023), actualizat pentru serviciul rQSCD, conform ETSI EN 319 401, clauza 7.12, art. 24 alin. (2) lit. (i) din Regulamentul eIDAS și Regulamentului de punere în aplicare (UE) 2025/2530 (ETSI TS 119 431-1: OVR-6.4.9-01, OVR-6.4.9-02; ETSI EN 319 401: REQ-6.1-11; checklist 2.3). Planul este revizuit cel puțin o dată la 2 ani și la fiecare modificare relevantă, riscurile asociate încetării sunt gestionate în cadrul de gestionare a riscurilor, iar CERTDIGITAL deține resursele financiare și asigurarea necesare executării planului.

14.9.2. Procedurile de încetare

În cazul încetării serviciului (decizie voluntară, retragerea statutului calificat, insolvență), CERTDIGITAL:

– notifică ADR și abonații cu cel puțin **3 luni** înainte de data încetării (sau imediat, în cazurile neanticipate), indicând consecințele și opțiunile;

– încetează generarea de noi chei și înrolarea de noi semnatari de la data notificării;

– transferă, cu acordul semnatarilor și al ADR, obligațiile privind cheile și certificatele active către un alt prestator calificat de servicii de gestionare a rQSCD, dacă acest lucru este posibil tehnic (migrarea cheilor exclusiv între module criptografice certificate, prin mecanisme de backup/restore sub control dual) și convenit contractual; în caz contrar, revocă toate certificatele calificate încă valabile și **distruge ireversibil toate cheile de semnare și copiile acestora** în rQSCD, cu procese-verbale;

– revocă certificatele și distruge cheile SAM și cheile infrastructurii care nu sunt transferate;

– transferă arhivele (jurnale, dovezi de identificare, înregistrări) către ADR sau către prestatorul succesor, astfel încât acestea să rămână accesibile pe durata perioadelor de păstrare, inclusiv pentru verificarea ulterioară a semnăturilor create;

– solicită actualizarea Listei de încredere în timp util, inclusiv marcarea stării serviciului;

– menține disponibile informațiile de stare (CRL/OCSP) și depozitul pe perioada necesară validării semnăturilor create;

– notifică părțile afectate (abonați, integratori, furnizori) și publică informațiile relevante în depozit;

– păstrează înregistrările care demonstrează executarea planului.

Planul acoperă scenariile anticipate (decizie comercială, fuziune) și neanticipate (insolvență, retragerea statutului, dezastru nerecuperabil) și identifică persoanele responsabile și succesiunea în cazul indisponibilității managementului.

15. Controale tehnice de securitate

15.1. Managementul sistemelor și al securității

Sistemele serviciului rQSCD sunt administrate în conformitate cu cerințele CEN EN 419 241-1, clauza SRG_M.1 (managementul securității TW4S) (ETSI TS 119 431-1: OVR-6.5.1-01):

– rolurile administrative ale TW4S (administrator de securitate, administrator de sistem, operator, auditor) sunt distincte și corespund rolurilor de încredere din secțiunea 14.3;

– funcțiile de administrare a securității (gestionarea politicilor SAM, a utilizatorilor privilegiați, a configurațiilor firewall) sunt separate de funcțiile de operare;

– orice modificare a parametrilor de securitate ai SAM/HSM (fereastra de valabilitate SAD, algoritmi, politici de chei) este efectuată numai prin procedura de gestionare a schimbărilor, cu control dual și jurnalizare;

– configurațiile de securitate sunt documentate (baseline) și verificate periodic față de configurația de referință, abaterile fiind tratate ca incidente.

15.2. Sisteme și operațiuni

În conformitate cu CEN EN 419 241-1, clauzele SRG_SO.1 și SRG_SO.2 (ETSI TS 119 431-1: OVR-6.5.2-01, OVR-6.5.2-02):

– sistemele sunt operate conform procedurilor documentate, de personal instruit, cu monitorizarea capacității și a performanței;

– mediile de dezvoltare, testare și producție sunt separate fizic sau logic; datele de producție (în special datele de identificare și cheile) nu sunt utilizate în medii de test;

– procedurile de pornire, oprire, repornire și recuperare a componentelor SSAS sunt documentate; repornirea HSM/SAM necesită reautentificarea custozilor conform politicii M din N;

– integritatea software-ului SSA/SAM este verificată la pornire și periodic (semnături de cod, verificarea hash-urilor, Secure Boot pe servere);

– programele utilitare care pot ocoli controalele sistemului sunt restricționate și controlate.

15.3. Controale de securitate ale calculatoarelor

CERTDIGITAL aplică cerințele ETSI EN 319 401 REQ-7.4-01, REQ-7.4-02X, REQ-7.4-05X, REQ-7.4-06X și REQ-7.4-13X și monitorizarea sistemului conform CEN EN 419 241-1, SRG_AA.6.1 (ETSI TS 119 431-1: OVR-6.5.3-01A, OVR-6.5.3-02):

– **Sisteme de încredere**: componentele TW4S (SSA, SAM, HSM) sunt produse și configurate conform CEN EN 419 241-1 și profilurilor de protecție aplicabile; serverele SSA rulează sisteme de operare consolidate (hardening conform ghidurilor CIS), cu servicii minime, fără acces direct la Internet, actualizate conform secțiunii 15.4;

– **Controlul accesului**: accesul la sistemele SSAS este acordat pe baza principiului „need-to-know" și al privilegiului minim, prin conturi nominale, cu autentificare multifactor pentru toate accesele administrative, revizuire trimestrială a drepturilor, dezactivare imediată la încetarea rolului; conturile generice și parolele partajate sunt interzise („Procedura de control al accesului" – P.SMSI-0.15, „Procedura de administrare a utilizatorilor" – P.SMSI-0.1, „Procedura de administrare a parolelor" – P.SMSI-0.2);

– **Protecția împotriva codului malițios**: soluții EDR/antimalware pe toate sistemele, actualizate automat, cu alertare în sistemul centralizat de jurnalizare; stațiile de administrare sunt dedicate și nu au acces la e-mail sau Internet;

– **Monitorizarea**: toate sistemele sunt monitorizate continuu (disponibilitate, integritate, evenimente de securitate), cu alerte în timp real către echipa de operare și, pentru evenimentele critice, către Ofițerul de Securitate IT;

– **Sesiuni**: sesiunile administrative expiră după inactivitate; sesiunile privilegiate sunt înregistrate.

15.4. Controale de securitate ale ciclului de viață

CERTDIGITAL aplică cerințele ETSI EN 319 401, clauzele 7.7 (securitatea operațiunilor) și 7.14 (lanțul de aprovizionare) (ETSI TS 119 431-1: OVR-6.5.4-01).

15.4.1. Dezvoltarea și achiziția sistemelor

– Componentele software dezvoltate de CERTDIGITAL (aplicația CertDigital ID, portalul, aplicațiile client CERTDIGITAL, integrările RA) sunt dezvoltate conform unui ciclu de viață securizat (Secure SDLC): cerințe de securitate, modelarea amenințărilor, standarde de codare securizată (OWASP ASVS/MASVS), revizuirea codului de către o a doua persoană, analiză statică și dinamică (SAST/DAST), analiza dependențelor vulnerabile, testare de securitate înainte de lansare, semnarea codului;

– Componentele achiziționate (dispozitivul ADSS SAM și modulul criptografic, aplicația de semnare pe server, biblioteci criptografice) sunt selectate pe baza certificărilor (CC, FIPS 140-3) și a evaluărilor de furnizor; versiunile sunt urmărite, iar actualizările sunt validate în mediul de test înainte de producție;

– Mediile de dezvoltare și testare sunt separate de producție; accesul dezvoltatorilor la producție este interzis.

15.4.2. Gestionarea schimbărilor și a vulnerabilităților

– Toate modificările sistemelor de producție sunt gestionate conform „Procedurii de administrare a modificărilor în sistemele IT" (P.SMSI-0.13) și „Procedurii de administrare a configurărilor" (P.SMSI-0.12): cerere, evaluarea impactului asupra securității și conformității, testare, aprobare (modificările componentelor critice necesită aprobarea Ofițerului de Securitate IT și a Managerului Servicii Electronice Calificate), implementare cu plan de revenire, verificare post-implementare, documentare;

– Modificările care afectează configurația evaluată a dispozitivului calificat sunt permise numai dacă mențin conformitatea cu certificarea; actualizările de firmware sunt aplicate numai la versiuni acoperite de certificare (pentru modulele CP5 ale aparatelor SAM: 5.1.0.0, secțiunea 11.3.1), cu control dual (M din N);

– **Gestionarea patch-urilor**: patch-urile de securitate critice sunt evaluate în cel mult 48 de ore și aplicate în cel mult 7 zile (sau mai rapid în caz de exploatare activă), celelalte în cadrul ciclului lunar; registrul de patch management este păstrat (checklist 6.2);

– **Scanarea vulnerabilităților**: scanări automate ale tuturor componentelor expuse și interne **cel puțin trimestrial** și după fiecare modificare semnificativă (Reg. 2025/1567: OVR-6.5.5-02; ETSI EN 319 401: REQ-7.8-13); vulnerabilitățile critice/ridicate sunt remediate sau atenuate în cel mult 7, respectiv 30 de zile;

– **Testarea de penetrare**: anual și după modificări majore, efectuată de un terț independent calificat, acoperind infrastructura de rețea, interfața de semnare la distanță, portalul, aplicația mobilă CertDigital ID (inclusiv rezistența la extragerea cheii de autentificare și la manipularea afișării WYSIWYS) și fluxurile de identificare la distanță; raportul și dovada remedierii sunt puse la dispoziția CAB (checklist 3.2, 6.2);

– **Divulgarea coordonată a vulnerabilităților**: politica CVD este publicată în depozit, cu un canal securizat de raportare și angajamentul de răspuns în 5 zile lucrătoare.

15.4.3. Lanțul de aprovizionare

În conformitate cu ETSI EN 319 401, clauza 7.14, și cu art. 21 alin. (2) lit. (d) din Directiva NIS2:

– **Politica**: CERTDIGITAL menține o politică privind securitatea lanțului de aprovizionare, care identifică furnizorii critici ai serviciului rQSCD (producătorul dispozitivului calificat și al modulului criptografic, furnizorii de conectivitate și de componente software terțe), riscurile asociate și cerințele de securitate contractuale;

– **Evaluarea furnizorilor**: fiecare furnizor critic este evaluat înainte de contractare și cel puțin anual (certificări, rapoarte de audit, practici de dezvoltare securizată, gestionarea vulnerabilităților, continuitate, localizarea datelor, conformitatea cu GDPR), cu înregistrarea rezultatului în registrul riscurilor (checklist 1.2);

– **Contracte și SLA**: contractele includ cerințe de securitate, de notificare a incidentelor și vulnerabilităților (în cel mult 24 de ore), de audit, de confidențialitate, de returnare/distrugere a datelor și de continuitate; CERTDIGITAL rămâne responsabil față de abonați și ADR (REQ-7.14.3-01X, REQ-7.14.3-02X);

– **Integritatea componentelor**: echipamentele criptografice sunt achiziționate direct de la producător sau de la distribuitori autorizați, livrate în ambalaje sigilate, cu verificarea sigiliilor, a numerelor de serie și a autenticității firmware-ului la recepție (lanț de custodie documentat); bibliotecile software sunt obținute din surse verificate, cu verificarea semnăturilor, iar lista componentelor (SBOM) este menținută.

15.5. Controale de securitate a rețelei

CERTDIGITAL aplică cerințele ETSI EN 319 401, clauza 7.8, și adaptările din Regulamentul de punere în aplicare (UE) 2025/1567 (ETSI TS 119 431-1: OVR-6.5.5-01 ÷ OVR-6.5.5-03):

– **Segmentarea**: rețeaua este împărțită în zone de securitate (DMZ publică – API Gateway/portal; zona aplicațiilor – SSA, RA; zona bazelor de date; zona criptografică – HSM/SAM; zona de administrare; zona de jurnalizare), separate prin firewall-uri redundante cu inspecție la nivel de aplicație; comunicarea între zone este permisă numai pentru fluxurile documentate explicit, toate celelalte protocoale și accese fiind **blocate implicit** (OVR-6.5.5-03);

– **Zona criptografică**: HSM/SAM sunt accesibile exclusiv din zona aplicațiilor (SSA) și din stația de administrare, pe porturile strict necesare, prin canale autentificate reciproc (TLS cu certificate client); nicio rută nu permite accesul direct din DMZ sau Internet;

– **Protecția perimetrului**: firewall-uri de nouă generație, IDS/IPS, protecție anti-DDoS și filtrare la nivelul API Gateway (rate limiting, validarea schemelor JSON, blocarea tiparelor de atac), WAF pentru portal;

– **Administrarea la distanță**: permisă numai prin VPN cu autentificare multifactor, de pe dispozitive gestionate, către stațiile de administrare (jump hosts), cu sesiuni înregistrate; „Procedura privind accesul de la distanță" (P.SMSI-0.7);

– **Protecția comunicațiilor**: TLS 1.3 / 1.2 cu Perfect Forward Secrecy pe toate interfețele; SAD protejate criptografic de la un capăt la altul, suplimentar față de TLS;

– **Monitorizarea rețelei**: fluxurile sunt monitorizate (NetFlow, IDS) și corelate în sistemul centralizat de jurnalizare; modificările regulilor firewall sunt supuse gestionării schimbărilor și revizuite trimestrial;

– **Scanarea vulnerabilităților** cel puțin trimestrial, conform secțiunii 15.4.2.

15.6. Controale criptografice

CERTDIGITAL aplică controale de securitate adecvate pe întregul ciclu de viață al tehnicilor criptografice utilizate, în conformitate cu ETSI EN 319 401, clauza 7.5, și cu adaptările din Regulamentul de punere în aplicare (UE) 2025/1567 (OVR-6.8.5-01, OVR-6.8.5-02):

Cheie / mecanism	Scop	Mediu de protecție	Ciclu de viață
Cheile de semnare ale semnatarilor	Semnătură / sigiliu calificat	rQSCD (CEN EN 419 221-5), sub controlul SAM	Secțiunea 13
Cheile interne ale dispozitivului (SAM)	Protecția protocolului de activare și a jurnalelor	Generate și păstrate în dispozitivul calificat, conform configurației evaluate	Conform ghidurilor producătorului; operații cu control dual, cu proces-verbal
Cheile de backup ale modulului criptografic (Key Encryption Keys)	Protecția copiilor de siguranță ale cheilor	Modulul criptografic, cu partajarea secretului între custozi (smartcard-uri), păstrate în spații securizate, cu control dual	Conform ghidurilor producătorului; distrugere la dezafectare

Cheie / mecanism	Scop	Mediu de protecție	Ciclu de viață
Cheile de autentificare ale semnatarilor (SIC)	Autentificarea SAD	Zona securizată a dispozitivului mobil (aplicația CertDigital ID)	Secțiunea 12.4
Cheile de autentificare ale aplicațiilor client	Autentificarea aplicațiilor client	Gestionate de integratori, conform documentației de integrare (secțiunea 11.6)	Conform contractului
Cheile TLS ale serviciului	Protecția canalelor	Serverele serviciului, cu certificate TLS	Conform politicii emitentului
Cheile CA / TSA	Emiterea certificatelor și a mărcilor temporale	HSM-urile CA/TSA	Conform DPPC-CA_G4 și PDP-QTST
Cheile de sigilare a jurnalelor și arhivelor	Integritatea dovezilor	Sigiliul electronic calificat al CENTRUL DE CALCUL S.A.	Conform DPPC-CA_G4

Algoritmii și parametrii utilizați pentru toate aceste mecanisme sunt conformi cu documentul ENISA/ECCG „Agreed Cryptographic Mechanisms” și sunt revizuiți anual. CERTDIGITAL monitorizează evoluțiile privind criptografia post-cuantică și va adopta mecanismele hibride sau post-cuantice recomandate de ENISA/ETSI atunci când acestea vor fi incluse în mecanismele agreate și suportate de dispozitivele certificate.

15.7. Sincronizarea timpului

Toate componentele serviciului (aparatele SAM, SSA, RA, sistemul de jurnalizare, TSA) sunt sincronizate cu o sursă de timp trasabilă la UTC, prin serverele de timp GNSS din cele două centre de date și surse externe redundante, conform documentului 00u; deviația este monitorizată, iar o abatere mai mare de 1 secundă declanșează alertă și, pentru TSA, oprirea emiterii mărcilor temporale. Ora este utilizată în SAD, în jurnale și în mărcile temporale (CEN EN 419 241-1: SRG_AA.8; checklist 6.1).

16. Evaluarea conformității și auditul

16.1. Evaluarea conformității de către organismul de evaluare a conformității

În conformitate cu art. 20 alin. (1) din Regulamentul eIDAS, cu Legea nr. 214/2024 și cu procedura aprobată prin Ordinul nr. 102/2026, CERTDIGITAL este auditat, pe propria cheltuială, **cel puțin o dată la 24 de luni**, de un organism de evaluare a conformității acreditat conform Regulamentului de punere în aplicare (UE) 2025/2162 (EN ISO/IEC 17065 completat de ETSI EN 319 403-1), pentru a confirma că serviciul rQSCD îndeplinește cerințele Regulamentului eIDAS, ale actelor de punere în aplicare și ale standardelor enumerate în secțiunea 2 (ETSI TS 119 431-1: clauza 6.6; Lista standardelor aplicabile, 00n). CERTDIGITAL informează ADR cu cel puțin o lună înainte de auditul planificat și îi permite, la cerere, să participe ca observator (art. 20 alin. (1a) din Regulamentul eIDAS). Raportul de evaluare a conformității (CAR) este transmis ADR în cel mult 3 zile lucrătoare de la primire, iar sumarul public al acestuia este publicat în depozit. Între evaluări, CERTDIGITAL efectuează anual un audit intern (secțiunea 16.2) și se supune controalelor ADR.

Evaluarea acoperă cel puțin: prezentul document și politicile asociate; conformitatea cu ETSI TS 119 431-1 (EUSPv2, inclusiv anexa A) și adaptările din Regulamentul (UE) 2025/1567; conformitatea cu ETSI EN 319 401 și cu Regulamentul (UE) 2025/2530; certificarea și configurația rQSCD/SAM; procesele de identificare (ETSI TS 119 461); controalele fizice, de personal, operaționale și tehnice; gestionarea incidentelor și continuitatea; planul de încetare; măsurile NIS2.

16.2. Auditul intern

CERTDIGITAL efectuează audituri interne ale serviciului **cel puțin anual**, conform „Procedurii de audit intern" (P.SMSI-0.19), prin auditori independenți de activitățile auditate, cu verificarea prin eșantionare a jurnalelor de activare a semnăturii, a dosarelor de înrolare, a proceselor-verbale ale ceremoniilor, a registrelor de acces fizic, a configurațiilor HSM/SAM și a conformității cu prezentul document. Neconformitățile sunt tratate prin „Procedura de acțiuni corective și preventive" (P.SMSI-0.22); rezultatele sunt analizate de management (P.SMSI-0.21) și raportate Directorului General.

16.3. Pre-audituri și teste de pregătire

Înainte de evaluarea inițială și de fiecare reevaluare, CERTDIGITAL efectuează un pre-audit intern („dry-run") pe baza listei de verificare pentru acreditarea serviciului rQSCD, documentând dovezile pentru fiecare poziție, astfel încât toate cerințele să fie îndeplinite integral la data evaluării, având în vedere că ETSI EN 319 403-1 nu mai permite rapoarte favorabile cu neconformități majore nesoluționate.

16.4. Supravegherea de către ADR

CERTDIGITAL cooperează cu ADR, furnizând, la cerere, toate informațiile necesare supravegherii, permițând controalele la fața locului și notificând, conform art. 24 alin. (2) lit. (a) din Regulamentul eIDAS și Regulamentului de punere în aplicare (UE) 2025/2530, orice modificare în prestarea serviciului cu cel puțin o lună înainte de punerea ei în aplicare (cu cel puțin trei luni înainte, în cazul încetării), inclusiv: modificări ale prezentului document, ale Termenilor și condițiilor, ale arhitecturii tehnice (schimbarea dispozitivului calificat, a SIC), ale mecanismelor criptografice, ale procedurilor de înregistrare, ale guvernanței, ale planului de încetare, ale resurselor financiare și asigurării, ale terților implicați și ale datelor din Lista de încredere. Notificarea descrie modificarea, data planificată, motivele și documentele actualizate.

17. Profilurile certificatelor, ale datelor de activare și ale semnăturilor

17.1. Profilul certificatelor calificate asociate cheilor rQSCD

Certificatele calificate emise pentru cheile gestionate în rQSCD respectă ETSI EN 319 412-1, -2 (persoane fizice), -3 (persoane juridice) și -5 (QCStatements) și profilul din DPC CERTDIGITAL G4, secțiunea 7.1.2 (certificatele G4), respectiv din DPC CERTDIGITAL G5, secțiunea 7.1.2 (certificatele G5):

Câmp / extensie	Valoare
issuer	CERTDIGITAL QUALIFIED CA G4 sau CERTDIGITAL QCA G5
validity	cel mult 3 ani
subjectPublicKeyInfo	RSA ≥ 3072 sau ECDSA pe curbele NIST P-256 / P-384 (secțiunea 13.1.2)
keyUsage	nonRepudiation (contentCommitment) – critic
extKeyUsage	nu se include
certificatePolicies	QCP-n-qscd (0.4.0.194112.1.2) pentru semnătură / QCP-l-qscd (0.4.0.194112.1.3) pentru sigiliu; 1.3.6.1.4.1.47898.4.2.2.{identificare}.{tip subiect} (G4) sau 1.3.6.1.4.1.47898.5.2.2.{identificare}.{tip subiect} (G5) (dispozitiv 2 = QSCD gestionat de CERTDIGITAL; cheie generată de CERTDIGITAL; identificare 1 / 4 / 6; tip subiect 1 / 2); 1.3.6.1.4.1.47898.11.1.1 (chei de lungă durată); 0.4.0.19431.1.1.4 (EUSPv2)
qcStatements	QcCompliance; QcSSCD (0.4.0.1862.1.4); QcType eSign / eSeal; QcPDS
subject	conform DPC CERTDIGITAL G4, secțiunea 3.1.1
Extensia 1.3.6.1.4.1.47898.30.1	numai pentru persoane fizice, conform DPC CERTDIGITAL G4, secțiunea 7.1.2 (SHA-256 până la 28.02.2027; HMAC-SHA-256 de la 01.03.2027)
cRLDistributionPoints / authorityInfoAccess	conform DPC CERTDIGITAL G4, secțiunea 7.1.2

17.2. Profilul datelor de activare a semnăturii (SAD)

Conținutul SAD este descris în secțiunea 11.4.1. Formatul SAD, algoritmii și mesajele protocolului de activare sunt cele ale dispozitivului ADSS Server SAM Appliance v7.0.2, în configurația evaluată, integrat cu aplicația CertDigital ID; structura este documentată în specificația internă a protocolului SAP (CD_SI_014) și este disponibilă CAB.

17.3. Profilul aserțiunilor de autentificare

Nu se aplică: serviciul nu utilizează furnizori de identitate externi (secțiunea 12.5).

17.4. Profilurile semnăturilor create

Semnăturile sunt create în formatele baseline conform Regulamentului de punere în aplicare (UE) 2026/248 (secțiunea 13.2.4), cu următorii parametri impliciți: algoritm de rezumat SHA-256; semnătură RSA sau ECDSA; nivel B-T cu marcă temporală calificată CERTDIGITAL TSA G4 (ETSI EN 319 422); includerea atributelor signing-certificate-v2, signing-time și, la cerere, commitment-type-indication. Pentru PAdES, câmpul de semnătură vizibil include, la

cerere, numele semnatarului, data și mențiunea „Semnat electronic cu certificat calificat – CertDigital rQSCD”.

17.5. Profilul CRL și OCSP

Conform DPC CERTDIGITAL G4, secțiunile 4.9 și 7.2–7.3: CRL v2, emise cel puțin la 24 de ore și la fiecare revocare; răspunsuri OCSP conform RFC 6960, semnate cu certificatul CERTDIGITAL OCSP G4 (certificatele G4), respectiv CERTDIGITAL OCSP G5 (certificatele G5).

18. Alte aspecte de afaceri și juridice

18.1. Tarife

Tarifele pentru înrolare, generarea și gestionarea cheilor de semnare, emiterea certificatelor calificate, operațiunile de semnare și serviciile conexe sunt cele din lista de tarife publicată pe site-ul https://www.certdigital.ro/ sau cele din oferta transmisă la cerere (art. 11 alin. (1) și, pentru certificatele calificate, alin. (3) lit. b) din Legea nr. 214/2024). Accesul la depozit, la informațiile de stare a certificatelor (CRL/OCSP) și la prezentul document este gratuit. Revocarea certificatului și ștergerea cheii la cererea semnatarului sunt gratuite (ETSI TS 119 431-1: clauza 6.7.1).

18.2. Răspunderea financiară și asigurarea

CENTRUL DE CALCUL S.A. răspunde, conform art. 13 din Regulamentul eIDAS, pentru prejudiciile cauzate cu intenție sau din neglijență oricărei persoane fizice sau juridice prin nerespectarea obligațiilor care îi revin; intenția sau neglijența se prezumă, cu excepția cazului în care CERTDIGITAL dovedește că prejudiciul s-a produs fără intenția sau neglijența sa. În acest scop, CERTDIGITAL (ETSI EN 319 401: clauza 7.1 – REQ-7.1.1-02; ETSI TS 119 431-1: OVR-6.8.1-01; checklist 1.4):

– deține, pentru fiecare dintre cele două servicii calificate (semnătură și sigiliu), câte o **poliță distinctă de asigurare de răspundere civilă profesională**, cu limita răspunderii de 500.000 EUR pe perioada asigurată, în condițiile art. 24 alin. (2) lit. c) din Regulamentul eIDAS și ale art. 5 alin. (2) lit. b) din procedura aprobată prin Ordinul MEDAT nr. 102/2026 (CD_SI_003), în care ADR are calitatea de asigurat adițional; datele polițelor sunt comunicate ADR;

– dispune de resurse financiare adecvate, demonstrate prin situațiile financiare anuale (CD_SI_002), pentru operarea serviciului și pentru executarea planului de încetare.

Limitările răspunderii sunt stabilite în secțiunea 18.8 și în Termenii și condițiile serviciului.

18.3. Confidențialitatea informațiilor de afaceri

Informațiile referitoare la abonați și semnatari (altele decât cele publicate în certificate), configurațiile de securitate, rezultatele evaluărilor de risc și ale testelor de penetrare, procedurile interne detaliate, jurnalele și materialul criptografic sunt clasificate ca informații confidențiale conform „Procedurii de securitate a informațiilor" (clasele: publică / internă / restricționată) și nu sunt divulgate decât persoanelor autorizate, CAB și ADR în cadrul supravegherii, sau autorităților competente în condițiile legii. Prezentul document, Termenii și condițiile, certificatele CA, CRL/OCSP și documentația API sunt informații publice. Personalul și terții sunt obligați contractual la confidențialitate, inclusiv după încetarea raporturilor.

18.4. Protecția datelor cu caracter personal

CERTDIGITAL prelucrează datele cu caracter personal ale semnatarilor în conformitate cu Regulamentul (UE) 2016/679 (GDPR), cu Legea nr. 190/2018 și cu Politica privind protecția datelor cu caracter personal (00d; CD_SI_022), în calitate de **operator** (ETSI EN 319 401: REQ-7.13-05; ETSI TS 119 431-1: OVR-6.7.4-01):

- **Scopurile și temeiul**: verificarea identității, emiterea certificatelor, generarea și gestionarea cheilor, crearea semnăturilor, prevenirea fraudei, îndeplinirea obligațiilor legale (Regulamentul eIDAS, Legea nr. 214/2024) și executarea contractului; datele biometrice din CERTDIGITAL KYC se prelucrează numai pe baza consimțământului explicit al persoanei (art. 9 alin. (2) lit. (a) GDPR), persoana care nu își dă consimțământul putând opta pentru prezența fizică;
- **Minimizarea**: serviciul primește numai reprezentarea datelor de semnat și nu stochează documentele semnate; documentele încărcate pentru afișare în aplicațiile CertDigital se șterg imediat după returnarea documentului semnat, iar cele ale unei sesiuni nefinalizate, în cel mult 24 de ore de la încărcare; SAD și datele de sesiune sunt șterse la închiderea sesiunii; datele biometrice sunt utilizate exclusiv pentru compararea din procesul de identificare și sunt păstrate criptat numai ca dovadă, conform secțiunii 14.6;
- **Persoana împuternicită**: atunci când abonatul utilizează aplicațiile CERTDIGITAL pentru încărcarea documentelor, CERTDIGITAL acționează pentru acestea ca persoană împuternicită (art. 28 GDPR);
- **Securitatea**: criptarea datelor în repaus și în tranzit, pseudonimizarea în jurnale acolo unde este posibil, controlul accesului, jurnalizarea accesului la date;
- **Drepturile persoanelor**: acces, rectificare, ștergere (în limitele obligațiilor legale de păstrare), restricționare, portabilitate, opoziție; cererile se adresează responsabilului cu protecția datelor la dpo@centruldecalcul.ro; răspuns în cel mult o lună;
- **Transferuri**: datele sunt stocate și prelucrate în centrele de date proprii din România și nu se transferă în afara Spațiului Economic European; CERTDIGITAL nu utilizează persoane împuternicite pentru operarea serviciului (Politica privind protecția datelor, 00d, cap. 8);
- **Breșele**: notificarea ANSPDCP în 72 de ore și informarea persoanelor afectate conform secțiunii 14.8.2;
- **Evaluarea impactului**: CERTDIGITAL efectuează, înaintea lansării serviciului, o evaluare a impactului asupra protecției datelor (DPIA) pentru serviciul rQSCD, actualizată ori de câte ori se modifică prelucrările.

18.5. Drepturile de proprietate intelectuală

Prezentul document, politicile, aplicația CertDigital ID, portalul și aplicațiile client CERTDIGITAL, documentația de integrare, marca CertDigital și OID-urile din arcul 1.3.6.1.4.1.47898 sunt proprietatea CENTRUL DE CALCUL S.A. Abonații pot reproduce și distribui prezentul document integral și nemodificat. Cheile de semnare sunt generate în numele

semnatarului și sunt utilizate exclusiv sub controlul acestuia; certificatele calificate rămân proprietatea CERTDIGITAL, semnatarul având dreptul de utilizare conform Termenilor și condițiilor.

18.6. Declarații, garanții și obligații ale participanților

18.6.1. Obligațiile CERTDIGITAL

CERTDIGITAL se obligă (ETSI TS 119 431-1: clauza 6.7.6; ETSI EN 319 401: REQ-6.1-04):

– să opereze serviciul în conformitate cu prezentul document, cu Regulamentul eIDAS, cu Legea nr. 214/2024 și cu standardele aplicabile, inclusiv atunci când utilizează terți;

– să genereze, să stocheze și să utilizeze cheile de semnare exclusiv în rQSCD certificat, sub controlul exclusiv al semnatarului (SCAL2), și să nu creeze semnături fără SAD valide ale semnatarului;

– să nu duplice cheile decât pentru copii de siguranță, în condițiile secțiunii 13.4;

– să verifice identitatea semnatarilor la nivelul extins ETSI TS 119 461 înainte de legarea cheilor;

– să șteargă cheile la revocarea certificatului, la cerere sau la expirare;

– să informeze semnatarii despre fiecare operațiune de semnare și să le pună la dispoziție istoricul;

– să mențină disponibilitatea serviciului conform angajamentelor din Termeni și condiții și SLA;

– să notifice incidentele conform secțiunii 14.8.2 și să informeze abonații cu privire la modificările relevante;

– să respecte obligațiile privind protecția datelor;

– să mențină asigurarea și resursele financiare prevăzute în secțiunea 18.2.

18.6.2. Obligațiile abonatului și ale semnatarului

– să furnizeze informații exacte, complete și actualizate la înrolare și să notifice imediat orice modificare;

– să păstreze sub control exclusiv dispozitivul pe care este instalată aplicația CertDigital ID, să nu divulge codul PIN, să nu permită utilizarea de către alte persoane, să mențină dispozitivul actualizat și protejat;

– să verifice conținutul documentelor afișate înainte de a autoriza semnarea;

– să solicite imediat blocarea cheii și revocarea certificatului în caz de pierdere, furt sau suspiciune de compromitere a dispozitivului sau a PIN-ului, ori la modificarea datelor din certificat;

– să utilizeze cheia de semnare numai în scopurile permise (secțiunea 1.4);

– să respecte Termenii și condițiile și să achite tarifele;

– pentru persoanele juridice: să notifice încetarea autorizării persoanelor fizice care activează sigiliul și să răspundă pentru utilizarea sigiliului de către acestea.

18.6.3. Obligațiile integratorilor (aplicații client)

– să protejeze credențialele de aplicație client și să le utilizeze numai pentru scopurile autorizate;

– să transmită spre semnare exact documentele prezentate semnatarului și să nu altereze DTBS/R;

– să implementeze corect interfața și fluxurile de autorizare definite în documentația de integrare (secțiunea 11.6);

– să notifice CERTDIGITAL incidentele de securitate care pot afecta serviciul în cel mult 24 de ore;

– să respecte GDPR în calitate de operator pentru datele proprii.

18.6.4. Obligațiile părților utilizatoare

– să valideze semnăturile/sigiliile conform ETSI EN 319 102-1 (de exemplu, prin serviciul de validare CertDigital), verificând lanțul de certificare, starea certificatului la momentul semnării, statutul calificat al serviciilor în Lista de încredere a României și respectarea politicii;

– să țină seama de limitările de utilizare indicate în certificat și în Termeni și condiții.

18.6.5. Obligațiile organizațiilor externe care sprijină serviciul

Furnizorii identificați în secțiunea 15.4.3 sunt obligați contractual să respecte cerințele de securitate, confidențialitate, notificare, audit și continuitate stabilite de CERTDIGITAL, politicile și practicile aplicabile părții de serviciu pe care o susțin, și să permită verificarea conformității de către CERTDIGITAL, CAB și ADR.

18.7. Exonerări de garanții

CERTDIGITAL nu garantează adecvarea serviciului pentru scopuri care nu au fost convenite contractual și nu răspunde pentru consecințele utilizării serviciului cu încălcarea prezentului document sau a Termenilor și condițiilor, nici pentru conținutul documentelor semnate.

18.8. Limitarea răspunderii

CERTDIGITAL nu răspunde pentru prejudiciile rezultate din: utilizarea serviciului peste limitările notificate în prealabil și recognoscibile de terți (art. 13 alin. (2) din Regulamentul eIDAS); nerespectarea de către semnatar a obligațiilor de la secțiunea 18.6.2, inclusiv a celor de protecție a dispozitivului și a PIN-ului; furnizarea de informații false la înrolare; neverificarea de către partea care se bazează a stării certificatului și a statutului din Lista de încredere; forța majoră. Nicio prevedere nu exclude și nu limitează răspunderea pentru intenție sau culpă gravă (art. 1355 din Codul civil); în raporturile cu consumatorii se aplică Legea nr. 193/2000.

18.9. Despăgubiri

Abonatul despăgubește CERTDIGITAL pentru prejudiciile cauzate de încălcarea obligațiilor sale, de furnizarea de informații false sau de utilizarea neautorizată a serviciului imputabilă abonatului/semnatarului.

18.10. Durata și încetarea

Prezentul document intră în vigoare la data aprobării de către Directorul General și a publicării în depozit și rămâne în vigoare până la înlocuirea cu o versiune nouă sau până la încetarea serviciului. Contractul cu abonatul încetează la expirare, prin reziliere conform Termenilor și condițiilor, la cererea abonatului sau la încetarea serviciului (secțiunea 14.9); la încetare, cheile de semnare sunt șterse, iar certificatele sunt revocate, fără a afecta valabilitatea semnăturilor create anterior.

18.11. Notificări individuale și comunicarea cu participanții

Comunicările CERTDIGITAL către abonați și semnatari se efectuează prin e-mail la adresa înregistrată, prin notificări în aplicația CertDigital ID, prin portal sau, atunci când legea o impune, în scris. Comunicările către CERTDIGITAL se transmit la adresele din secțiunea 1.5.2; cererile de blocare, revocare și ștergere sunt disponibile 24/7 prin portal și aplicație.

18.12. Modificări

Modificările prezentului document se efectuează conform secțiunii 19. Modificările Termenilor și condițiilor sunt notificate abonaților cu cel puțin 30 de zile înainte de intrarea în vigoare; continuarea utilizării serviciului după această dată constituie acceptare, abonatul având dreptul de a rezilia contractul fără penalități.

18.13. Soluționarea disputelor și reclamațiile

Litigiile se soluționează pe cale amiabilă, pe baza unei reclamații transmise la office@certdigital.ro sau în scris la sediu, la care CERTDIGITAL răspunde în cel mult 30 de zile, conform „Procedurii operaționale privind soluționarea sesizărilor și reclamațiilor” (P.SMSI-0.23). În lipsa unei soluții amiabile, litigiile cu profesioniștii sunt de competența instanțelor de la sediul CENTRUL DE CALCUL S.A. (Târgu Jiu). Consumatorii se pot adresa instanțelor competente potrivit legii, inclusiv celor de la domiciliul lor, și pot apela la procedurile de soluționare alternativă a litigiilor (SAL) prevăzute de OG nr. 38/2015 (ANPC – https://anpc.ro/sal). Abonații pot sesiza și ADR, în calitate de organism de supraveghere (ETSI EN 319 401: REQ-6.2-02 lit. h).

18.14. Legea aplicabilă și conformitatea cu legislația

Prezentul document și relațiile contractuale aferente serviciului sunt guvernate de legea română și de dreptul Uniunii Europene (Regulamentul eIDAS și actele de punere în aplicare). CERTDIGITAL respectă legislația aplicabilă, inclusiv Legea nr. 214/2024, Ordinul nr.

102/2026, GDPR, OUG nr. 155/2024 (NIS2) și reglementările privind accesibilitatea (ETSI TS 119 431-1: OVR-6.7.15-01; ETSI EN 319 401: REQ-7.13-01, REQ-7.13-02).

18.15. Termenii și condițiile

CERTDIGITAL publică în depozit **Termenii și condițiile serviciului de gestionare la distanță a rQSCD** (document distinct, TC-rQSCD, cod CD_SI_018-rQSCD), puse la dispoziția abonaților și părților utilizatoare înainte de încheierea contractului, printr-un mijloc durabil de comunicare, într-un limbaj ușor de înțeles, în limba română (ETSI TS 119 431-1: OVR-6.8.4-01; ETSI EN 319 401: clauza 6.2). Termenii și condițiile specifică cel puțin:

– politica de serviciu aplicată (EUSPv2; prezentul document, OID 1.3.6.1.4.1.47898.11.1) și politicile de certificat asociate;

– limitările de utilizare a serviciului (secțiunea 1.4) și limitarea răspunderii pentru utilizările care depășesc aceste limite;

– obligațiile abonatului și ale semnatarului (secțiunea 18.6.2), inclusiv protecția mijlocului eID și a PIN-ului;

– informații pentru părțile utilizatoare: modul de validare a semnăturilor, verificarea stării certificatului, limitările;

– perioada de păstrare a jurnalelor de evenimente (10 ani);

– limitările răspunderii și limitele valorice;

– legea aplicabilă și instanțele competente;

– procedurile de reclamații și de soluționare a disputelor;

– confirmarea că serviciul a fost evaluat conform ETSI EN 319 403-1 de un CAB acreditat și statutul calificat al serviciului;

– datele de contact ale CERTDIGITAL;

– angajamentele privind disponibilitatea serviciului (SLA) și condițiile de suport;

– informațiile privind protecția datelor cu caracter personal;

– consimțământul explicit al semnatarului pentru generarea și gestionarea cheilor de semnare de către CERTDIGITAL pe seama sa (art. 29 alin. (1a) din Regulamentul eIDAS) și informarea privind realizarea copiilor de siguranță.

18.16. Accesibilitatea pentru persoanele cu dizabilități

CERTDIGITAL urmărește accesibilitatea serviciilor și a informațiilor destinate publicului (portalul, aplicația CertDigital ID, depozitul, Termenii și condițiile) pentru persoanele cu dizabilități, conform art. 15 din Regulamentul eIDAS și Directivei (UE) 2019/882, cu referință la standardul EN 301 549. Persoanele cu dizabilități pot solicita asistență prin telefon, e-mail sau la sediu, iar verificarea identității prin prezență fizică, cu asistență, este disponibilă ca alternativă la verificarea la distanță (ETSI TS 119 431-1: OVR-6.8.3-01; ETSI EN 319 401: REQ-7.13-03, REQ-7.13-04).

19. Administrarea documentului

19.1. Procedura de modificare

Propunerile de modificare pot fi inițiate de orice membru al personalului în roluri de încredere, ca urmare a: modificărilor legislative sau ale standardelor; rezultatelor evaluării riscurilor, auditurilor interne sau externe, incidentelor; modificărilor arhitecturii tehnice sau ale furnizorilor; solicitărilor ADR sau CAB. Ofițerul de Securitate IT analizează propunerea, elaborează și verifică versiunea revizuită, cu evidențierea modificărilor, și o supune aprobării Directorului General. Documentul este revizuit integral cel puțin **anual**, cu consemnarea revizuirii chiar și atunci când nu sunt necesare modificări (ETSI EN 319 401: REQ-6.1-08; ETSI TS 119 431-1: OVR-7-06, OVR-7-07).

Modificările sunt clasificate astfel:

Tip	Exemple	Efect
Editoriale	Corecturi, clarificări, actualizarea datelor de contact	Nu modifică numărul versiunii majore; publicare fără notificare prealabilă
Minore	Detalieri procedurale fără impact asupra abonaților sau părților utilizatoare	Incrementarea versiunii minore (x.y); notificare prin depozit
Majore	Modificări care pot afecta acceptarea serviciului (schimbarea nivelului de verificare a identității, a mijloacelor eID, a algoritmilor, a limitărilor, a răspunderii, a modelului de chei)	Incrementarea versiunii majore; notificare prealabilă cu cel puțin 30 de zile către abonați (e-mail/portal) și cu cel puțin o lună către ADR; după caz, modificarea OID-ului politicii (OVR-5.2-01, REQ-6.1-09X)

19.2. Mecanismul de publicare și notificare

Versiunea aprobată este publicată în depozit (https://www.certdigital.ro/repository) imediat după aprobare, semnată cu sigiliul electronic calificat al CENTRUL DE CALCUL S.A. și marcată temporal, împreună cu un sumar al modificărilor; versiunile anterioare rămân disponibile în arhiva depozitului. Modificările majore sunt notificate ADR conform secțiunii 16.4 și abonaților conform secțiunii 18.12. Documentul este comunicat personalului CERTDIGITAL și terților relevanți, cu confirmarea luării la cunoștință (ETSI EN 319 401: REQ-6.1-02, REQ-6.1-10).

19.3. Procedura de aprobare

Documentul și fiecare versiune nouă sunt verificate de Ofițerul de Securitate IT și aprobate de **Directorul General** al CENTRUL DE CALCUL S.A., care are autoritatea finală pentru aprobarea politicii și a declarației de practici a serviciului; aprobarea se consemnează în tabelul de control al documentului. Înainte de aprobare se verifică faptul că practicile descrise sunt implementate efectiv și sunt susținute de procedurile operaționale și de dovezile de conformitate; conducerea CENTRUL DE CALCUL S.A. răspunde de implementarea practicilor (ETSI EN 319 401: REQ-6.1-06, REQ-6.1-07; ETSI TS 119 431-1: OVR-7-04).

19.4. Documente asociate

Prezentul document se citește împreună cu: Politica serviciilor de certificare CertDigital (POL); Politicile generale CertDigital (PG); DPC CERTDIGITAL G4 (DPPC-CA_G4); DPC CERTDIGITAL G5; Termenii și condițiile serviciului rQSCD (TC-rQSCD) și contractul de furnizare a serviciului (CTR-rQSCD); Termenii și condițiile și PDS pentru certificatele calificate (TC-CERT); Politica și declarația de practici a serviciului calificat de marcare temporală (PDP-QTST); Politica de securitate a informațiilor; Planul de continuitate a afacerii și Procedura de recuperare în caz de dezastru; Planul de încetare a serviciilor; Politica privind protecția datelor cu caracter personal; Lista standardelor aplicabile; Descrierea TSP și arhitectura detaliată (CD_SI_014). Lista completă este prezentată în Anexa C.

Anexa A – Matricea de conformitate cu ETSI TS 119 431-1 V1.3.1 (EUSPv2) și Regulamentul (UE) 2025/1567

Tabelul de mai jos indică, pentru fiecare cerință aplicabilă politicii EUSPv2 (inclusiv cerințele [NSP] aplicabile prin OVR-A.3-01 și adaptările din anexa la Regulamentul de punere în aplicare (UE) 2025/1567), secțiunea prezentului document în care este tratată și tipul de dovadă pusă la dispoziția CAB.

Cerință	Obiect	Secțiune	Dovezi principale
OVR-5.1-01	Aplicarea ETSI EN 319 401 clauza 6.1 (declarația de practici)	1, 19	Prezentul document, aprobarea Directorului General
OVR-5.1-02	Algoritmi, parametri și mecanisme critice incluse în declarația de practici	13.1.2, 15.6, 17	Secțiunile indicate
OVR-5.1-03	Publicarea online 24×7 a declarației de practici	10	Depozit, rapoarte de disponibilitate
OVR-5.2-01	Schimbarea OID la modificarea politicii	1.2, 19.1	CERTDIGITAL_OID_MAP
OVR-5.3.1-01	Responsabilitatea SSASP pentru terți	1.3.1, 1.3.6, 15.4.3	Contracte, evaluări furnizori
OVR-6.1-01 ÷ OVR-6.1-04	Publicare, identificarea T&C, disponibilitate 24/7, disponibilitate internațională (adaptare Reg. 2025/1567)	10.1 ÷ 10.3	Depozit
GEN-6.2.1-02, -02A	Mediul cheilor (SRA_SKM.1.1); SCDev certificat EN 419 221-5	11.3.1, 13.1.1	Certificările OCSI și NSCIB, Security Target
GEN-6.2.1-03 ÷ -07	Algoritmi și lungimi (SRG_KM.1.2), protecția cheilor (SRG_KM.1.3), inițializarea dispozitivului (SRG_KM.1.4), parametrii (SRC_SKS.1.1), momentul generării (SRC_SKS.1.3)	13.1	Configurații HSM, proceduri, jurnale
GEN-6.2.1-08	Suport pentru REG-6.3.1-01 din EN 319 411-1 (asertiune de autentificare)	11.6.4, 12.6	Specificația interfeței SSAS–CA
GEN-6.2.1-09	Chei de unică folosință legate de o singură sesiune (model neoferit)	1.4.1, 11.5	–
LNK-6.2.2-00, -03B, SIG-6.3.1-11 ÷ -16	Legarea directă de identitate pentru chei de unică folosință (model neoferit)	1.4.1, 12.2.4	–
LNK-6.2.2-02A ÷ -02E	Verificarea identității persoane fizice/juridice (A.1.2/A.1.3), înrolarea (A.1.1), caracteristicile și mecanismul eID (A.2.1/A.2.2) la nivel substanțial+	12.1 ÷ 12.3	Proceduri RA, evaluarea aplicației CertDigital ID
LNK-6.2.2-03A, -04, -05	Legarea cheii de referința eID; furnizarea eID; coerența datelor cu certificatul	12.3, 12.4	Evidența SSAS, jurnale
LNK-6.2.2-06, -08, -08A, -09	Autentificare delegată, referință furnizată de terț (nu se utilizează)	12.5	–
LNK-6.2.2-10A	Integritatea legăturilor	12.3.3	Mecanisme HSM, teste
LNK-6.2.3-01 ÷ -03	Legarea certificatului (SRC_SKS.1.2, .1.4, .1.5)	12.6	Evidența SSAS, jurnale de înrolare
EID-6.2.4-01, -02	Furnizarea securizată a eID și a datelor de activare pe canale separate	12.4.2	Procedura de înrolare dispozitiv
SIG-6.3.1-01 ÷ -07	Autentificare (SRC_SA.1.2), securitatea protocolului (SRC_SA.1.3, SRA_SAP.1.2), control acces (SRC_SA.1.4), controlul cheii (SRC_SA.1.5, SRA_SKM.2.5), activarea cheii (SRA_SKM.2.1)	11.4, 13.2.1	Security Target SAM, specificația SAP, teste de penetrare

Cerință	Obiect	Secțiune	Dovezi principale
SIG-6.3.1-08, -09, -10	Verificarea valabilității certificatului; consimțământul; parametrii semnăturii (SRC_DSC.1.1)	13.2, 13.3	Configurație SSA, jurnale
DEL-6.3.2-01 ÷ -05	Ștergerea la revocare, la cerere, gestionarea sesiunii, ștergerea backup-ului (DEL-6.3.2-05, chei de unică folosință: model neoferit)	13.5	Proceduri, jurnale HSM
GEN-6.3.3-01 ÷ -04	Backup (SRG_KM.2.1 ÷ .2.3), numărul minim de seturi	13.4	Procedura backup HSM, registre
OVR-6.4.1-01	EN 319 401 clauzele 5, 6.3, 7.3 (risc, politică de securitate, active)	14.1	Evaluarea riscurilor, SMSI
OVR-6.4.2-01, -02	Securitate fizică (EN 319 401 7.6; EN 319 411-1 OVR-6.4.2-02 ÷ -10)	14.2	Registre acces, CCTV, sigilii
OVR-6.4.3-01A	Controale procedurale (REQ-7.4-03X, -04X, -07X ÷ -12X)	14.3	Fișe de post, matrice roluri, procese-verbale
OVR-6.4.4-01 ÷ -03	Personal (EN 319 401 7.2); competență; actualizare la 12 luni (adaptare Reg. 2025/1567)	14.4	Dosare de personal, evidența instruirii
OVR-6.4.5-01 ÷ -07	Jurnalizare (EN 319 401 7.10; SRG_AA.1 ÷ .3, .7, .8); toate evenimentele de securitate	14.5	Sistemul centralizat de jurnalizare, sincronizarea timpului
OVR-6.4.6-01	Păstrarea jurnalelor minimum 7 ani după expirarea certificatelor	14.6	Politica de retenție (10 ani)
OVR-6.4.8-01	Incidente și continuitate (EN 319 401 7.9, 7.11)	14.8	Plan de răspuns, BCP/DRP, rapoarte de test
OVR-6.4.9-01, -02	Încetare (EN 319 401 7.12); conformitatea cu actele art. 24(5) (adaptare Reg. 2025/1567)	14.9	Planul de încetare
OVR-6.5.1-01, OVR-6.5.2-01, -02	SRG_M.1, SRG_SO.1, SRG_SO.2	15.1, 15.2	Proceduri operaționale
OVR-6.5.3-01A, -02	REQ-7.4-01, -02X, -05X, -06X, -13X; SRG_AA.6.1	15.3	Configurații, monitorizare
OVR-6.5.4-01	EN 319 401 7.7 și 7.14	15.4	SDLC, patch management, evaluări furnizori
OVR-6.5.5-01 ÷ -03	EN 319 401 7.8; scanare trimestrială; deny-all (adaptări Reg. 2025/1567)	15.5	Rapoarte de scanare, reguli firewall
OVR-6.7.4-01	REQ-7.13-05 (protecția datelor)	18.4	Politica GDPR, DPIA
OVR-6.7.15-01	REQ-7.13-01, -02 (conformitatea cu legislația)	18.14	–
OVR-6.8.1-01	EN 319 401 7.1 (organizare, răspundere financiară)	14.3, 18.2	Poliță de asigurare, situații financiare
OVR-6.8.3-01	REQ-7.13-03, -04 (accesibilitate)	18.16	Declarația de accesibilitate
OVR-6.8.4-01	EN 319 401 6.2 (termeni și condiții)	18.15	Termeni și condiții rQSCD (TC-rQSCD)
OVR-6.8.5-01, -02	Controale criptografice pe ciclul de viață; ENISA Agreed Cryptographic Mechanisms (adaptare Reg. 2025/1567)	13.1.2, 15.6	Inventar de chei, revizuire anuală
OVR-A.3-01	Toate cerințele [NSP] se aplică	întregul document	–
OVR-A.3-02	Referința la certificarea QSCD (anexa II eIDAS) în declarația de practici	11.3.1	Certificat CC, lista CE
OVR-A.3-03	Respectarea cerințelor din raportul de certificare	11.3.1, 15.4.2	Ghidul de operare securizată, verificări
GEN-A.4-01, -02	Generare în QSCD, în configurația certificată	11.3.1, 13.1.1	Configurație HSM

Cerință	Obiect	Secțiune	Dovezi principale
SIG-A.5-01 ÷ -08	Utilizare în QSCD; configurație; SRA_SAP.1.3 ÷ 1.7 (forță criptografică, atenuarea amenințărilor, protecția mediului, tamper, atacator); SAM certificat EN 419 241-2	11.3, 11.4	Certificarea OCSI a ADSS SAM, Security Target, teste
SIG-A.5-09	Sesiune ≤ 30 min după verificarea identității (chei de unică folosință; model neoferit)	1.4.1, 12.2.4	–
SIG-A.6-01 ÷ -08	SRA_SAP.2.1 ÷ 2.8: format SAD, colectare/generare, parametri, utilizare, destinație, colectare și protecție, transmitere sub control exclusiv (pers. fizice / „control" pentru pers. juridice), protecție după activare	11.4, 17.2	Specificația SAP, Security Target SAM
LNK-A.7-01	Verificarea identității la nivel extins ETSI TS 119 461	12.2	Proceduri RA, rapoarte de evaluare a identificării
Reg. 2025/1567 – 2.1	Referințe normative suplimentare: EN 319 401 V3.1.1, ENISA ACM	2	–

Anexa B – Corespondența cu Regulamentul (UE) nr. 910/2014 modificat prin Regulamentul (UE) 2024/1183

Prevedere	Conținut	Secțiune
Art. 24 alin. (1) și (1a)	Verificarea identității înainte de emiterea certificatului calificat: prezență fizică (lit. (d)), metode confirmate de CAB – CERTDIGITAL KYC (lit. (c)), certificat calificat (lit. (b))	12.2
Art. 24 alin. (2) lit. (a)	Informarea organismului de supraveghere cu cel puțin o lună înainte de modificări și cu cel puțin trei luni înainte de încetare	16.4, 14.9
Art. 24 alin. (2) lit. (b)	Personal și subcontractanți cu expertiză, fiabilitate, experiență, calificări; instruire	14.4
Art. 24 alin. (2) lit. (c)	Resurse financiare și asigurare de răspundere	18.2
Art. 24 alin. (2) lit. (d)	Informarea prealabilă privind termenii și condițiile	18.15
Art. 24 alin. (2) lit. (e)	Sisteme și produse de încredere, protejate împotriva modificării; securitatea și fiabilitatea proceselor	11, 15
Art. 24 alin. (2) lit. (f)	Sisteme de încredere pentru stocarea datelor, verificabile, accesibile numai persoanelor autorizate	14.5, 14.6, 15.3
Art. 24 alin. (2) lit. (fa)	Gestionarea riscurilor de securitate cibernetică (art. 21 NIS2)	14.1.1
Art. 24 alin. (2) lit. (fb)	Notificarea încălcărilor securității și a perturbărilor, în cel mult 24 de ore	14.8.2
Art. 24 alin. (2) lit. (g)	Măsuri împotriva falsificării și furtului de date	11.4, 12, 15
Art. 24 alin. (2) lit. (h)	Înregistrarea și păstrarea informațiilor relevante, inclusiv după încetare	14.6, 14.9
Art. 24 alin. (2) lit. (i)	Plan de încetare actualizat	14.9
Regulamentul (UE) 2016/679	Prelucrarea legală a datelor cu caracter personal	18.4
Art. 24 alin. (2) lit. (k)	Baza de date a certificatelor (pentru QTSP care emit certificate)	17.5, DPPC-CA_G4
Art. 29 alin. (1a)	Generarea/gestionarea/duplicarea datelor de creare a semnăturii numai pe seama semnatarului, la cererea sa, de un QTSP calificat pentru rQSCD	12.1.1, 13.1, 13.4
Art. 29a alin. (1) lit. (a)	QTSP generează sau gestionează datele de creare a semnăturii pe seama semnatarului	13.1, 13.2, 13.3
Art. 29a alin. (1) lit. (b)	Duplicarea numai pentru backup, la același nivel de securitate, în numărul minim necesar	13.4
Art. 29a alin. (1) lit. (c)	Respectarea cerințelor din raportul de certificare al rQSCD (art. 30)	11.3.1
Art. 29a alin. (2)	Standardele de referință (Reg. 2025/1567)	2
Art. 30 / 31	Certificarea QSCD și lista Comisiei	11.3.1
Art. 39, 39a	Aplicarea mutatis mutandis pentru sigilii	1.3.3, 1.4.1
Anexa II pct. 1 lit. (a) ÷ (d)	Confidențialitatea, unicitatea, nederivabilitatea și protecția datelor de creare a semnăturii împotriva utilizării de către alții	11.1, 11.3, 13.1, 13.2
Anexa II pct. 2	Nealterarea datelor de semnat și prezentarea lor semnatarului înainte de semnare (WYSIWYS)	11.4.2, 13.2.2
Anexa II pct. 3	Generarea sau gestionarea datelor de creare a semnăturii pe seama semnatarului numai de un QTSP	1.3.1, 13
Art. 13	Răspunderea prestatorului	18.2, 18.8
Art. 15	Accesibilitatea pentru persoanele cu dizabilități	18.16
Art. 20 / 21	Evaluarea conformității cel puțin la 24 de luni și informarea ADR înaintea auditului; inițierea serviciului calificat	16
Art. 24a	Recunoașterea serviciilor de încredere calificate	1.2

Anexa C – Documentele interne asociate

Nr.	Document	Cod / referință
1	Politica serviciilor de certificare CertDigital (POL); Politicile generale CertDigital (PG)	CD_SI_012
2	Declarația practicilor de certificare a CERTDIGITAL ROOT CA G4 și CERTDIGITAL QUALIFIED CA G4 (DPC CERTDIGITAL G4)	CD_SI_014 / 10.10
3	Termenii și condițiile serviciului rQSCD (TC-rQSCD); contractul de furnizare a serviciului rQSCD (CTR-rQSCD)	CD_SI_018-rQSCD / CTR-rQSCD
4	Termenii și condițiile și PDS pentru certificatele calificate (TC-CERT)	TC-CERT
5	Politica și declarația de practici a serviciului calificat de marcare temporală (PDP-QTST)	PDP-QTST
6	Regulamentul de identificare și solicitare cerere semnătură; Regulamentul de validare și aprobare cerere semnătură	CD_SI_013
7	Descrierea TSP și arhitectura detaliată a serviciului (inclusiv specificația SAP și diagramele rQSCD)	CD_SI_014
8	Planul de continuitate a afacerii (PO/C/SI/S/63); Procedura de recuperare în caz de dezastru (PO/SI/63); rapoartele de testare	CD_SI_015 (00m)
9	Lista standardelor aplicabile	CD_SI_016 (00n)
10	Certificarea dispozitivului ADSS Server SAM Appliance v7.0.2 (OCSI) și a modulului Utimaco CP5 (NSCIB); extrasul din lista Comisiei	CD_SI_017 / CD_SI_025
11	Planul de tratare a riscurilor IT; Procedura de evaluare și tratare a riscului IT; Identificarea și evaluarea riscurilor	CD_SI_019 / CD_SI_020 / P.SMSI-0.17
12	Modelul notificării organismului de supraveghere; Procedura de notificare a incidentelor (00q)	CD_SI_021 / P.SMSI-0.28
13	Politica privind protecția datelor cu caracter personal (00d); DPIA rQSCD	CD_SI_022 / P.SMSI-0.27
14	Planul de încetare a serviciilor (00r)	CD_SI_023 / P.SMSI-0.26
15	Politica de securitate a informațiilor; Politica SMSI; Declarația de aplicabilitate	P.SMSI-0.10 / 0.16 / 0.18
16	Procedura de administrare a utilizatorilor; a parolelor; a utilizatorilor cu drepturi privilegiate; de control al accesului; privind accesul de la distanță; de reglementare a accesului terților	P.SMSI-0.1 / 0.2 / 0.9 / 0.15 / 0.7 / 0.8
17	Procedura de administrare a incidentelor și problemelor IT; Procedura de management al incidentelor de securitate a informației; Planul de răspuns la incidente	P.SMSI-0.3 / 0.11
18	Procedura de administrare a configurărilor; a modificărilor în sistemele IT; de mentenanță a echipamentelor	P.SMSI-0.12 / 0.13 / 0.24
19	Procedura de salvare și restaurare a datelor; Procedura de backup/restore HSM	P.SMSI-0.14
20	Procedura privind generarea cheii; Raport de generare a cheii; procedurile ceremoniilor de chei HSM/SAM	CD_SI_010 / CD_SI_011 / P.SMSI-0.30
21	Procedura de audit intern; Analiza efectuată de management; Procedura de acțiuni corective și preventive	P.SMSI-0.19 / 0.21 / 0.22
22	Procedura operațională privind soluționarea sesizărilor și reclamațiilor	P.SMSI-0.23
23	Fișele de post; lista personalului cu roluri de încredere; organigrama	CD_SI_000
24	Polițele de asigurare; situațiile financiare	CD_SI_003 / CD_SI_002
25	Datele de contact ale prestatorului	CD_SI_026
26	Procedura standard de operare „HSM Zeroization" și registrul de distrugere	de elaborat / actualizat pentru rQSCD
27	Politica privind securitatea lanțului de aprovizionare și registrul furnizorilor critici	de elaborat / actualizat pentru rQSCD

Nr.	Document	Cod / referință
28	Politica de divulgare coordonată a vulnerabilităților (CVD)	de publicat în depozit
29	Documentația interfeței de semnare la distanță; ghidul de integrare	CD_SI_014 / depozit

Documente citate în versiunile anterioare ale declarației de practici, care nu se mai aplică: Declarația politicilor și practicilor de certificare (document general, DPPC v1.6) și Declarația de informare a PKI (PDS v1.6) sunt înlocuite sau retrase; pentru certificatele calificate asociate cheilor se aplică DPC CERTDIGITAL G4 sau DPC CERTDIGITAL G5 și TC-CERT. Declarația de practici pentru marcarea temporală (DPP-TSA) este retrasă și înlocuită de PDP-QTST.