

Politica și declarația de practici a serviciilor calificate de transmitere electronică înregistrată

CertDigital QERDS

EMISĂ DE:			
DEPARTAMENT	**NUME**	**SEMNĂTURA**	**DATA**
MANAGEMENTUL POLITICILOR ȘI PROCEDURILOR	Ofițer de Securitate IT		_____

APROBATĂ DE:			
DEPARTAMENT	**NUME**	**SEMNĂTURA**	**DATA**
MANAGEMENTUL POLITICILOR ȘI PROCEDURILOR	Director General		_____

ISTORICUL MODIFICĂRILOR:			
VERSIUNE	**AUTOR**	**DETALII MODIFICĂRI**	**DATA:**
1.0	Ofițer de Securitate IT	Prima versiune, document unic: politica (Partea I) și declarația de practici (Partea a II-a) comune serviciilor QREM și QeRDS; ETSI EN 319 521 / 531, adaptate prin Reg. (UE) 2025/1944; temeiul publicării tarifelor: art. 11 alin. (1) din Legea nr. 214/2024	22/10/2026
1.1	Ofițer de Securitate IT	Statutul calificat descris exact: pentru serviciile QREM și QeRDS se solicită acordarea statutului calificat și înscrierea în Lista de încredere a României, iar până la înscriere ele nu se prestează ca servicii calificate (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
1.2	Ofițer de Securitate IT	Tabelul de identificare arată versiunea și data în vigoare (în versiunea 1.1 rămăseseră cele ale versiunii 1.0)	27/10/2026
1.3	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
1.4	Ofițer de Securitate IT	Completări pentru evaluarea conformității (ETSI EN 319 521 / 531): prestatorii calificați implicați (1.3), responsabilitățile de revizuire (1.5), comunicarea termenilor și condițiilor pe suport durabil și dovada acceptării (6.2), dovezile de notificare aliniate la ETSI EN 319 522-1 (6.6, 12.3, 13.1), perioadele de păstrare aplicate și exportul în 30 de zile (6.11, 16), operatorul de înregistrare și responsabilul cu verificarea identității (6.13), încetarea (6.16, 18), specificația dovezilor publicată separat (10), disponibilitatea conținutului (12.6), particularitățile QREM	02/11/2026

		(12.9), limitele de valabilitate a dovezilor (13.5), referința de timp (15), organizațiile externe (19), anexa A	
1.5	Ofițer de Securitate IT	Completări pentru evaluarea conformității (ETSI EN 319 521 și ETSI EN 319 401 V3.1.1, cu adaptările din RE (UE) 2025/1944): evenimentele de securitate jurnalizate (6.12); compromiterea cheilor de sigiliu ale serviciilor – oprirea sigilării, revocarea, notificarea părților, valabilitatea dovezilor și tratarea ca dezastru (14.2); certificatele de autentificare a site-ului web pentru TLS (14.3); trimiterile la cerințele de identificare din RE (UE) 2025/1944 (6.4, 11.2); anexa A; subsecțiunile noi 18.1–18.6 (securitatea rețelei, monitorizarea și jurnalizarea, incidentele și vulnerabilitățile, copiile de siguranță și continuitatea, lanțul de aprovizionare, verificarea configurației)	02/11/2026
1.6	Ofițer de Securitate IT	Securitatea fizică (capitolul 18): accesul se descrie ca autentificare în mai mulți factori, fără enumerarea factorilor, care rămân în documentația internă de securitate; conținutul neschimbat în rest	03/11/2026

Cuprins

PARTEA I – Politica serviciului 8
1. Introducere 8
1.1. Prezentare generală 8
1.2. Identificarea documentului și a politicii 9
1.3. Participanții și prestatorii implicați 9
1.4. Utilizarea serviciilor și limitele de utilizare 11
1.5. Administrarea documentului 11
2. Referințe normative 12
2.1. Acte normative și standarde 12
3. Definiții și acronime 13
3.1. Definiții 13
3.2. Acronime 13
4. Concepte generale 15
4.1. Serviciile și componentele lor 15
4.2. Cele două profiluri 15
4.3. Identitatea serviciilor și sigiliile serviciilor 15
5. Politica serviciilor 17
5.1. Identificare și conformitate 17
5.2. Comunitatea utilizatorilor și aplicabilitatea 17
5.3. Modificarea politicii 17
6. Cerințele privind practicile 18
6.1. Publicare și depozit 18
6.2. Termeni și condiții 18
6.3. Identificarea expeditorului 18
6.4. Identificarea destinatarului înainte de livrare 19
6.5. Securizarea trimiterii și primirii 19
6.6. Dovezile 19
6.7. Data și ora trimiterii și primirii 20
6.8. Modificările necesare transmiterii 20
6.9. Protecția datelor transmise 20

6.10. Interoperabilitatea și transmiterea între prestatori 21
6.11. Păstrarea datelor, a dovezilor și a jurnalelor 21
6.12. Timpul de încredere și jurnalele 21
6.13. Personalul 22
6.14. Controale privind facilitățile, managementul și operarea 22
6.15. Controale criptografice și de rețea 22
6.16. Notificări către ADR și încetarea serviciilor 23
6.17. Evaluarea conformității 23
7. Obligații și răspundere 24
7.1. Obligațiile CERTDIGITAL 24
7.2. Obligațiile expeditorului, ale destinatarului și ale abonatului 24
7.3. Obligațiile părților care se bazează 24
7.4. Răspunderea 24
7.5. Asigurarea 25
8. Alte aspecte comerciale și juridice 26
8.1. Tarife 26
8.2. Protecția datelor cu caracter personal 26
8.3. Modificări 26
8.4. Soluționarea litigiilor 26
8.5. Legea aplicabilă și cadrul legal 26
8.6. Alte prevederi 27
9. Corespondența cu cerințele art. 44 și ale Regulamentului (UE) 2025/1944 28
9.1. Tabel de corespondență 28
PARTEA A II-A – Declarația de practici 29
10. Publicare și depozit 29
11. Identificare și autentificare 30
11.1. Înregistrarea utilizatorilor 30
11.2. Autentificarea la fiecare utilizare 30
11.3. Destinatarii fără cont 30
11.4. Păstrarea dovezilor identificării 31
12. Ciclul de viață al trimiterii 32
12.1. Depunerea 32
12.2. Transmiterea 32

12.3. Notificarea destinatarului 32
12.4. Punerea la dispoziție („livrat”) 32
12.5. Predarea și acceptarea 32
12.6. Disponibilitatea conținutului 33
12.7. Sistemele necalificate 33
12.8. Modificările necesare transmiterii 33
12.9. Particularitățile QREM (ETSI EN 319 531) 33
12.10. Particularitățile QeRDS (ETSI EN 319 522) 34
13. Dovezile 35
13.1. Evenimentele și dovezile emise 35
13.2. Conținutul dovezilor 35
13.3. Formatul și sigilarea 36
13.4. Obținerea și verificarea dovezilor 36
13.5. Limitele de valabilitate a dovezilor 36
14. Protecția datelor transmise și controale tehnice 37
14.1. Integritate și confidențialitate 37
14.2. Cheile serviciilor 37
14.3. Rețea și vulnerabilități 37
15. Timpul 39
16. Păstrarea, reversibilitatea și portabilitatea 40
17. Interoperabilitatea 41
18. Controale de management și operare 42
18.1. Securitatea rețelei 42
18.2. Monitorizarea și jurnalizarea 44
18.3. Incidentele și vulnerabilitățile 45
18.4. Copiile de siguranță și continuitatea 47
18.5. Lanțul de aprovizionare 47
18.6. Verificarea configurației 50
19. Obligațiile părților și ale organizațiilor externe 51
20. Aspecte juridice și comerciale 52
Anexa A – Corespondența cu ETSI EN 319 521 (adaptat prin RE 2025/1944) și EN 319 531 53

PARTEA I – Politica serviciului

1. Introducere

1.1. Prezentare generală

Prezentul document stabilește cerințele 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 transmitere electronică înregistrată** (în terminologia Regulamentului eIDAS: servicii de distribuție electronică înregistrată calificate; art. 3 pct. 36 și 37, art. 43 și 44 din Regulamentul (UE) nr. 910/2014, astfel cum a fost modificat prin Regulamentul (UE) 2024/1183) și descrie practicile prin care CERTDIGITAL le îndeplinește. Documentul acoperă două servicii, cu intrări distincte în Lista de încredere:

– **QeRDS** — serviciul calificat de transmitere electronică înregistrată (tipul `EDS/Q`), prin portalul și interfețele de programare ale CERTDIGITAL și prin conectorii de interoperabilitate cu alți prestatori;

– **QREM** — serviciul calificat de transmitere electronică înregistrată prin e-mail (tipul `EDS/REM/Q`), prin mesaje de e-mail securizate S/MIME.

Serviciile permit transmiterea de date între expeditor și destinatar prin mijloace electronice, furnizează dovezi privind manipularea datelor transmise, inclusiv dovezi privind trimiterea și primirea lor, și protejează datele împotriva riscului de pierdere, furt, deteriorare sau orice modificare neautorizată. Datele trimise și primite prin serviciile calificate beneficiază de prezumția integrității datelor, a trimiterii lor de către expeditorul identificat, a primirii lor de către destinatarul identificat și a exactității datei și orei trimiterii și primirii indicate de serviciu (art. 43 alin. (2)).

Partea I (politica serviciilor) stabilește **ce** garantează CERTDIGITAL. **Cum** sunt îndeplinite cerințele este descris în Partea a II-a (declarația de practici), comună celor două servicii, cu o secțiune distinctă pentru QREM (secțiunea 12.9). Pentru verificarea identității se aplică DPC CERTDIGITAL G4, pentru mărcile temporale calificate Politica și declarația de practici a serviciului calificat de marcare temporală (PDP-QTST), iar pentru cerințele comune tuturor serviciilor, Politicile generale CertDigital (PG).

Ambele servicii sunt destinate prestării ca **servicii de încredere calificate** în sensul Regulamentului (UE) nr. 910/2014, de către un prestator calificat, după înscrierea lor în Lista de încredere a României (ETSI EN 319 521, cl. 4.1.2-01); până la înscriere, ele nu se prestează ca servicii de încredere calificate (art. 21 alin. (3) din Regulamentul eIDAS).

1.2. Identificarea documentului și a politicii

Element	Valoare
Titlu	Politica și declarația de practici a serviciilor calificate de transmitere electronică înregistrată CertDigital (PDP-QERDS)
Versiune	1.6 (03.11.2026)
Identificator (OID)	1.3.6.1.4.1.47898.14.1 — prezentul document (politica și declarația de practici), comun celor două servicii
Profilul QREM	1.3.6.1.4.1.47898.14.1.1 — transmitere prin e-mail S/MIME (ETSI EN 319 532)
Profilul QeRDS	1.3.6.1.4.1.47898.14.1.2 — transmitere prin portal, interfețe de programare și conectori AS4 (ETSI EN 319 522)
Declarația de practici	declarația de practici este inclusă în prezentul document (Partea a II-a)
Specificații de referință	Regulamentul de punere în aplicare (UE) 2025/1944: anexa I = ETSI EN 319 521 V1.1.1, cu adaptările din anexă (trimiteri la EN 319 401 V3.1.1, EN 319 411-1 V1.5.1, EN 319 522-1 și -2 V1.2.1); anexa II (interoperabilitate), când CERTDIGITAL convine interoperabilitatea cu alți prestatori. Pentru QREM se aplică, în plus, ETSI EN 319 531 și EN 319 532
Tipurile de servicii (ETSI TS 119 612)	`http://uri.etsi.org/TrstSvc/Svctype/EDS/Q` (QeRDS) și `http://uri.etsi.org/TrstSvc/Svctype/EDS/REM/Q` (QREM)
Identitatea serviciilor în Lista de încredere (după înscriere) și sigiliile serviciilor	câte un certificat calificat de sigiliu pentru fiecare serviciu: CERTDIGITAL QERDS SERVICE G5 și CERTDIGITAL QREM SERVICE G5 (secțiunile 4.3 și 14.2)
Generație	serviciile se prestează în generația G5 a infrastructurii CERTDIGITAL
Publicat la	https://www.certdigital.ro/repository/politici/certdigital_pdp-qerds_ro.pdf; versiunile anterioare: https://www.certdigital.ro/repository/arhiva/

Identificatorii sunt înscriși în CERTDIGITAL_OID_MAP. Certificatele de sigiliu ale celor două servicii conțin identificatorul politicii (1.3.6.1.4.1.47898.14.1); identificatorul profilului se înscrie în dovezi.

1.3. Participanții și prestatorii implicați

– **prestatorul**: CERTDIGITAL, care operează ambele servicii și răspunde în ansamblu de ele, inclusiv atunci când folosește propriile servicii calificate de marcare temporală și de emitere a certificatelor;

– **prestatorii calificați implicați** în prestarea serviciilor (ETSI EN 319 521, cl. 4.1.2-02): cei din tabelul de mai jos;

– **expeditorul**: persoana fizică sau juridică, identificată, care trimite date prin serviciu;

– **destinatarul**: persoana fizică sau juridică, identificată înainte de livrare, căreia îi sunt adresate datele;

– **delegații** expeditorilor și ai destinatarilor: persoanele autorizate să trimită sau să primească în numele unei organizații;

– **abonatul**: persoana care încheie contractul cu CERTDIGITAL; poate fi expeditorul, destinatarul sau organizația căreia aceștia îi aparțin;

– **alți prestatori de servicii calificate de transmitere electronică înregistrată**, cu care CERTDIGITAL schimbă date în cadrul interoperabilității (secțiunea 6.10);

– **părțile care se bazează** pe datele transmise și pe dovezile serviciului.

Prestatorii calificați implicați în prestarea serviciilor și serviciile lor sunt următorii (ETSI EN 319 521, cl. 4.1.2-02):

Prestatorul și serviciul	**Rolul în serviciile QeRDS și QREM**
CENTRUL DE CALCUL S.A. (CERTDIGITAL), serviciul calificat de marcare temporală CertDigital TSA (tipul TSA/QTST): CERTDIGITAL TSA G4, înscris în Lista de încredere a României, și CERTDIGITAL TSA G5, de la înscrierea ei în Lista de încredere	emite mărcile temporale calificate aplicate datelor transmise și dovezilor (capitolul 15)
CENTRUL DE CALCUL S.A. (CERTDIGITAL), autoritatea de certificare CERTDIGITAL QCA G5 (tipul CA/QC)	emite certificatele calificate de sigiliu CERTDIGITAL QERDS SERVICE G5 și CERTDIGITAL QREM SERVICE G5 (secțiunea 14.2)
CENTRUL DE CALCUL S.A. (CERTDIGITAL), serviciul calificat de validare a semnăturilor și sigiliilor electronice calificate (QESVal), înscris în Lista de încredere ca CERTDIGITAL VALIDATION AUTHORITY G4	validează semnăturile și sigiliile prin care se identifică destinatarul înainte de predare (QERDS-5.2.1.2-02)
CENTRUL DE CALCUL S.A. (CERTDIGITAL), serviciul calificat de păstrare (PSPPS), la cererea abonatului	păstrează pe termen lung dovezile încredințate de abonat și le menține verificabile prin augmentare (secțiunea 13.5)
alți prestatori calificați de transmitere electronică înregistrată, numai în cadrul interoperabilității convenite (capitolul 17)	transmit sau primesc trimiteri și emit dovezile care le revin; la data prezentei versiuni nu este convenită interoperabilitatea cu niciun prestator, iar lista prestatorilor parteneri se publică în depozitul de documente și se actualizează la fiecare acord nou

Pentru serviciile calificate QeRDS și QREM, CERTDIGITAL folosește numai servicii de încredere înscrise ca servicii calificate în Lista de încredere a României și nu folosește mărci temporale sau certificate de sigiliu emise de alți prestatori. Prestatorii calificați care au emis certificatele calificate sau mijloacele de identificare electronică folosite de expeditori și de destinatari la identificare nu participă la prestarea serviciilor; încrederea în acestea se stabilește prin listele de încredere ale statelor membre. Statutul calificat al serviciilor de mai sus se verifică în Lista de încredere a României, la https://trustedlist.adr.gov.ro/.

CERTDIGITAL nu deleagă către terți operarea serviciilor, verificarea identității sau gestionarea cheilor serviciilor. Furnizorii de componente și de servicii-suport și obligațiile lor sunt cei din capitolul 19.

1.4. Utilizarea serviciilor și limitele de utilizare

Serviciile se utilizează pentru transmiterea de date și documente electronice cu efect juridic de dovadă a trimiterii și a primirii (de exemplu notificări, somații, comunicări contractuale sau administrative, documente semnate). Serviciile nu verifică și nu garantează conținutul datelor transmise, ci identitatea părților, integritatea datelor și momentul trimiterii și al primirii.

Limitele de utilizare ale celor două servicii sunt următoarele:

Element	QREM	QeRDS
Canal	e-mail S/MIME, clienți de e-mail standard (SMTP, pentru trimitere și pentru notificări) și interfața web, prin care se preia conținutul	portal web, interfață de programare (API) și conector AS4
Dimensiunea maximă a unei trimiteri	30 MB	100 MB
Destinatari	utilizatori QREM CERTDIGITAL sau ai altor prestatori calificați de REM; adrese externe numai cu dovezile F.1–F.3	utilizatori QeRDS CERTDIGITAL sau ai altor prestatori calificați, prin interoperabilitate
Conținut interzis	cod malițios, conținut ilegal; conținutul criptat de expeditor e acceptat, dar nu se poate scana	idem

Limitele sunt cuprinse și în termenii și condițiile serviciilor (EN 319 521, cl. 4.1.2-03).

1.5. Administrarea documentului

CENTRUL DE CALCUL S.A. (marca CertDigital), Str. Tudor Vladimirescu nr. 17, Târgu Jiu, județul Gorj, cod poștal 210132, România; J1991000103187; EUID ROONRC.J1991000103187; CUI RO2163993; tel. +40 253 214 767; office@certdigital.ro; https://www.certdigital.ro/. Documentul este verificat de ofițerul de securitate IT și aprobat de Directorul General; Compartimentul Servicii Electronice răspunde de menținerea documentului și pregătește reviziile, Directorul Tehnic evaluează dacă o modificare trebuie notificată ADR (Procedura de notificare, 00q, cap. 12), iar reviziile se consemnează în istoricul documentului. Documentul se revizuiește cel puțin anual și la orice schimbare a serviciilor. Modificările se notifică ADR cu cel puțin o lună înainte, iar utilizatorii sunt informați prin publicare cu cel puțin 30 de zile înainte (secțiunea 8.3; EN 319 521, cl. 4.1.1-04). Prezentul document este redactat în limba română; în caz de neconcordanță cu o traducere, prevalează versiunea în limba română.

2. Referințe normative

2.1. Acte normative și standarde

– Regulamentul (UE) nr. 910/2014, astfel cum a fost modificat prin Regulamentul (UE) 2024/1183, art. 3 pct. 36 și 37, art. 13, 20, 21, 24, 43 și 44;

– Regulamentul de punere în aplicare (UE) 2025/1944 (standardele de referință pentru procesele de trimitere și primire a datelor și pentru interoperabilitatea serviciilor calificate de distribuție electronică înregistrată);

– Regulamentul de punere în aplicare (UE) 2025/2530 (cerințe pentru prestatorii calificați: notificări, gestionarea riscurilor, planul de încetare); Regulamentul de punere în aplicare (UE) 2025/1566 (verificarea identității);

– Regulamentul de punere în aplicare (UE) 2025/1929 (marcarea temporală calificată); Regulamentul de punere în aplicare (UE) 2025/1945 (validarea semnăturilor și sigiliilor electronice); Regulamentul de punere în aplicare (UE) 2025/2162 (acreditarea organismelor de evaluare a conformității);

– ETSI EN 319 521 V1.1.1 (cerințe de politică și securitate pentru prestatorii de servicii de transmitere electronică înregistrată), cu adaptările din anexa I la RE 2025/1944;

– ETSI EN 319 401 V3.1.1; ETSI EN 319 411-1 V1.5.1 (cerințele preluate pentru verificarea identității);

– ETSI EN 319 522-1, -2 și -3 V1.2.1 (cadrul și arhitectura, conținutul semantic, formatele); ETSI EN 319 522-4-1 V1.2.1 (AS4), EN 319 522-4-2 V1.1.1 (dovezi și identificare) și EN 319 522-4-3 V1.1.1 (capabilități și încredere);

– ETSI EN 319 531 V1.1.1 (cerințe de politică și securitate pentru prestatorii de servicii de e-mail înregistrat); ETSI EN 319 532-1…-4 (REM: cadrul, conținutul semantic, formatele și profilurile de interoperabilitate, inclusiv profilul de bază REM din EN 319 532-4 V1.3.1);

– RFC 2045 (MIME) și RFC 5322 (formatul mesajelor de e-mail), pentru QREM;

– documentul „Agreed Cryptographic Mechanisms” al ECCG, publicat de ENISA; schema EUCC (Regulamentele de punere în aplicare (UE) 2024/482 și 2024/3144);

– Legea nr. 214/2024; Ordinul MEDAT nr. 102/2026; Regulamentul (UE) 2016/679 și Legea nr. 190/2018.

Lista completă a actelor normative și a standardelor aplicate este în documentul 00n.

3. Definiții și acronime

3.1. Definiții

– **serviciu de transmitere (distribuție) electronică înregistrată** — un serviciu care permite transmiterea de date între părți terțe prin mijloace electronice și furnizează dovezi referitoare la manipularea datelor transmise, inclusiv dovezi privind trimiterea și primirea datelor, și care protejează datele transmise împotriva riscului de pierdere, furt, deteriorare sau orice modificare neautorizată (art. 3 pct. 36 din Regulamentul eIDAS);

– **serviciu calificat de transmitere (distribuție) electronică înregistrată** — serviciul care îndeplinește cerințele art. 44 (art. 3 pct. 37);

– **e-mail înregistrat (REM)** — serviciul de transmitere electronică înregistrată realizat prin mesaje de e-mail, conform ETSI EN 319 532;

– **trimitere** — ansamblul datelor transmise de expeditor către unul sau mai mulți destinatari printr-o singură operație, împreună cu metadatele lor;

– **dovadă** — înregistrarea sigilată de prestator și marcată temporal calificat, care atestă producerea unui eveniment din ciclul de viață al trimiterii (depunere, transmitere, punere la dispoziție, predare, refuz, eșec);

– **punere la dispoziție (consignare)** — momentul în care trimiterea devine accesibilă destinatarului în căsuța sau în contul acestuia;

– **predare** — momentul în care destinatarul, după identificare, preia efectiv datele;

– **delegat** — persoana autorizată să trimită sau să primească trimiteri în numele unei organizații;

– **„store and forward”** — stilul QREM în care conținutul se transmite destinatarului fără acceptarea lui prealabilă (secțiunea 12.5);

– **„store and notify”** — stilul QREM, opțional, în care conținutul se predă numai după acceptarea explicită a destinatarului, în termenul de acceptare (secțiunea 12.5).

3.2. Acronime

Acronim	Semnificație
ADR	Autoritatea pentru Digitalizarea României, organismul de supraveghere
API	interfață de programare a aplicațiilor
AS4	profilul de mesagerie OASIS ebMS 3.0 folosit pentru interoperabilitate (ETSI EN 319 522-4-1)
CAB	organism de evaluare a conformității
eID	identificare electronică; mijloc de identificare electronică
ERDS / QeRDS	serviciu de transmitere electronică înregistrată / varianta calificată
IMAP / POP / SMTP	protocoalele de preluare (IMAP, POP) și de trimitere (SMTP) a mesajelor de e-mail
KYC	verificarea identității clientului; CERTDIGITAL KYC este soluția de identificare video la distanță a CERTDIGITAL
MIME	formatul standard al mesajelor de e-mail cu mai multe părți (RFC 2045)

Acronim	Semnificație
NCP	politica de certificare normalizată din ETSI EN 319 411-1
QTST	marcă temporală electronică calificată
REM / QREM	serviciu de e-mail înregistrat / varianta calificată
S/MIME	standardul de securizare a mesajelor de e-mail prin semnături și criptare
SPF / DKIM / DMARC	mecanismele de autentificare a domeniului de e-mail al expeditorului
TLS	protocolul de securizare a comunicațiilor în rețea
UTC	timpul universal coordonat
XAdES / CAdES / PAdES	formatele ETSI de semnătură și sigiliu electronic avansat pentru documente XML, structuri CMS și documente PDF

4. Concepte generale

4.1. Serviciile și componentele lor

Conform ETSI EN 319 522-1 și EN 319 532-1, fiecare serviciu cuprinde:

– **depunerea**: primirea trimiterii de la expeditorul identificat și autentificat, verificarea și sigilarea ei (secțiunile 6.3 și 6.5);

– **transmiterea**: transferul către căsuța destinatarului sau către prestatorul calificat al destinatarului (secțiunea 6.10);

– **punerea la dispoziție și predarea**: notificarea destinatarului și predarea datelor după identificarea lui (secțiunea 6.4);

– **dovezile**: emiterea dovezilor pentru fiecare eveniment și transmiterea lor către expeditor și, după caz, către destinatar (secțiunea 6.6);

– **păstrarea** datelor, a dovezilor și a jurnalelor (secțiunea 6.11).

4.2. Cele două profiluri

Profil	Canal	Formatul dovezilor	Interoperabilitate
QREM (47898.1 4.1.1)	e-mail: mesaje S/MIME semnate și sigilate de prestator; adresele de e-mail ale utilizatorilor sunt legate de identitatea verificată; stilul „store and forward” (obligatoriu), iar stilul „store and notify”, cu acceptarea de către destinatar, opțional (ETSI EN 319 531, cl. 4.5)	dovezi REM conform ETSI EN 319 532-2 / -3, ca părți MIME XML sau PDF, sigilate XAdES-B-T (profilul de bază REM, EN 319 532-4)	numai cu alți prestatori calificați de REM, conform EN 319 532-4
QeRDS (47898.1 4.1.2)	portal web și interfețe de programare ale CERTDIGITAL; conectori AS4	dovezi ERDS conform ETSI EN 319 522-2 / -3	cu alți prestatori calificați, prin AS4, conform EN 319 522-4-1, -4-2, -4-3 și anexei II la RE 2025/1944

Domeniile serviciilor sunt erds.certdigital.ro (QeRDS) și rem.certdigital.ro (QREM).

4.3. Identitatea serviciilor și sigiliile serviciilor

Fiecare serviciu are un **certificat calificat de sigiliu** propriu, emis pentru CENTRUL DE CALCUL S.A., care va identifica serviciul în Lista de încredere a României, după înscriere, și cu care se sigilează datele transmise și dovezile: CERTDIGITAL QREM SERVICE G5 (cu adresa de e-mail a serviciului, pentru semnarea S/MIME) și CERTDIGITAL QERDS SERVICE G5. Cheile se păstrează în module criptografice certificate (secțiunea 6.15).

Certificatele CERTDIGITAL QERDS SERVICE G5 și CERTDIGITAL QREM SERVICE G5 sunt emise de CERTDIGITAL QCA G5, sunt valabile 5 ani și au chei RSA 4096 generate în ceremonia cheilor G5 din 23.10.2026, în modulul Thales Luna PCIe HSM 7 A790 (secțiunea 14.2);

certificatul QREM conține adresa serviciului, office@rem.certdigital.ro. Profilurile sunt descrise în DPC CERTDIGITAL G5, secțiunea 7.1.2, iar certificatele se publică la http://certs.certdigital.ro/certdigital_qerds_g5.crt și http://certs.certdigital.ro/certdigital_qrem_g5.crt.

5. Politica serviciilor

5.1. Identificare și conformitate

CERTDIGITAL declară conformitatea procesului de trimitere și primire a datelor cu ETSI EN 319 521 V1.1.1, cu adaptările din anexa I la Regulamentul de punere în aplicare (UE) 2025/1944, ceea ce atrage prezumția de conformitate cu cerințele art. 44 alin. (1) din Regulamentul eIDAS (art. 44 alin. (1a)). Atunci când convine interoperabilitatea cu alți prestatori, CERTDIGITAL aplică și anexa II. Pentru QREM se aplică, în plus, ETSI EN 319 531 și EN 319 532, care nu sunt citate în regulament, dar preiau cerințele EN 319 521. Conformitatea este evaluată de un organism de evaluare a conformității acreditat, al cărui domeniu acoperă ambele tipuri de servicii (secțiunea 6.17). Pentru ambele servicii se solicită acordarea statutului calificat și înscrierea în Lista de încredere a României (art. 21 din Regulamentul eIDAS); până la înscriere, ele nu se prestează ca servicii de încredere calificate (art. 21 alin. (3)).

5.2. Comunitatea utilizatorilor și aplicabilitatea

Serviciile se adresează persoanelor fizice și juridice, autorităților și instituțiilor publice care trimit sau primesc comunicări cu valoare de dovadă, precum și părților care se bazează pe acestea.

5.3. Modificarea politicii

Dacă o modificare a prezentului document sau a unui profil afectează garanțiile oferite, identificatorul politicii sau al profilului se schimbă. Modificările practicilor care nu afectează garanțiile oferite se fac printr-o versiune nouă a documentului, cu același identificator. Dovezile emise anterior rămân verificabile conform regulilor în vigoare la data emiterii lor.

6. Cerințele privind practicile

6.1. Publicare și depozit

Prezentul document, termenii și condițiile serviciilor, specificația dovezilor și codurile de respingere (SPEC-DOVEZI-QERDS) și certificatele de sigiliu ale serviciilor sunt publicate la https://www.certdigital.ro/repository/, 24/7, public și fără restricții de acces (secțiunea 10).

6.2. Termeni și condiții

Înainte de încheierea contractului, abonații, expeditorii, destinatarii și părțile care se bazează sunt informați, clar, complet și ușor accesibil, atât public, cât și individual, despre termenii și condițiile serviciilor (TC-QERDS): modul de identificare, dovezile emise, termenele de punere la dispoziție și de păstrare, limitele de dimensiune, interoperabilitatea, tarifele, răspunderea și limitările ei.

Termenii și condițiile se comunică înainte de încheierea contractului și înainte de prima utilizare a serviciilor, pe un suport durabil și în formă lizibilă: (a) sunt publicați, ca fișier PDF/A sigilat electronic de CERTDIGITAL, la adresa fixă din depozitul de documente indicată în Termenii și condițiile, secțiunea 1.2, iar versiunile anterioare rămân în arhiva depozitului; (b) se transmit solicitantului, ca fișier PDF, împreună cu oferta sau cu contractul; (c) la crearea contului, inclusiv pentru utilizatorii desemnați de abonat și pentru destinatarii care se înregistrează prin legătura primită, documentul este afișat integral, se poate descărca, iar utilizatorul îl acceptă printr-o acțiune expresă înainte de prima utilizare. CERTDIGITAL păstrează dovada acceptării (identitatea utilizatorului, versiunea și amprenta documentului acceptat, data și ora) pe durata de păstrare a datelor de identificare (capitolul 16); pentru abonat, dovadă este și contractul semnat, în care acesta declară versiunea primită (ETSI EN 319 521, cl. 4.2-04, 4.2-05 și 4.2-07; ETSI EN 319 401, REQ-6.2-03 și 6.2-04).

6.3. Identificarea expeditorului

– identitatea expeditorului se verifică inițial, la înregistrarea contului, cu un nivel de încredere ridicat (art. 44 alin. (1) lit. (b)), prin una dintre metodele din RE 2025/1944, anexa I (QERDS-5.2.1.1-01A): prezență fizică; portofelul european pentru identitatea digitală sau un mijloc de identificare electronică notificat de nivel cel puțin substanțial, emis după verificarea prin prezență fizică; certificat pentru semnătură sau sigiliu avansat emis conform politicii NCP (inclusiv certificatele calificate CERTDIGITAL); altă metodă confirmată de organismul de evaluare a conformității. Se aplică cerințele preluate din ETSI EN 319 411-1 și metodele din DPC CERTDIGITAL G4, secțiunea 3.2;

– la fiecare utilizare, expeditorul se autentifică prin: autentificare cu doi factori, portofelul european sau un mijloc eID, conexiune TLS cu autentificare reciprocă sau semnătură bazată

pe un certificat NCP (QERDS-5.2.2-03); pentru transmiterile automate între sisteme, prin TLS cu autentificare reciprocă și cel puțin un factor suplimentar;

– pentru persoanele juridice se verifică, în plus, existența persoanei juridice și împuternicirea persoanei care acționează în numele ei;

– dovezile identificării se păstrează (secțiunea 6.11).

6.4. Identificarea destinatarului înainte de livrare

– destinatarul este identificat înainte de predarea datelor (art. 44 alin. (1) lit. (c); EN 319 521, QERDS-5.2.1.2-01), iar identificarea se face într-un mediu controlat (QERDS-5.2.1.2-03);

– identitatea destinatarului se verifică inițial cu un **nivel de încredere foarte ridicat**, prin una dintre metodele din RE 2025/1944, anexa I (QERDS-5.2.1.1-01): prezență fizică; mijloc de identificare electronică de nivel ridicat sau portofelul european pentru identitatea digitală; certificat calificat pentru semnătură sau sigiliu electronic; altă metodă confirmată de organismul de evaluare a conformității. Un mijloc eID de nivel substanțial nu este suficient singur;

– la preluare, destinatarul se autentifică prin autentificare cu mai mulți factori, portofelul european sau un mijloc eID, ori semnătură sau sigiliu calificat (QERDS-5.2.2-03A); dacă identificarea se bazează pe o semnătură, aceasta se validează înainte de predare (QERDS-5.2.1.2-02);

– dacă destinatarul nu are cont, el este notificat pe canalul indicat de expeditor și poate prelua datele numai după verificarea identității; identificarea se repetă dacă destinatarul nu are un mijloc de autentificare legat de identitatea verificată (5.2.1.1-02);

– dovezile identificării destinatarului se păstrează (QERDS-5.2.1.2-04).

6.5. Securizarea trimiterii și primirii

Datele trimise și primite sunt securizate cu **sigiliul electronic calificat al serviciului** (sigiliu avansat bazat pe certificat calificat și creat cu un dispozitiv calificat, secțiunea 14.2), astfel încât orice modificare a datelor să fie detectată (art. 44 alin. (1) lit. (d)). Dacă serviciul detectează o modificare a datelor, trimiterea se oprește, iar expeditorul și destinatarul sunt notificați automat.

6.6. Dovezile

– serviciul emite automat dovezi pentru evenimentele din ETSI EN 319 522-1, cl. 6, cu semantica din EN 319 522-2, cl. 8 (RE 2025/1944, anexa I: ERDS-5.4.1-06…08); pentru QREM, conform EN 319 532-2 și profilului de bază REM;

– dovezile obligatorii acoperă cel puțin: acceptarea sau respingerea depunerii (A.1 / A.2); acceptarea, refuzul sau eșecul transmiterii către alt prestator (B.1 / B.2 / B.3); punerea la dispoziție a conținutului sau eșecul ei (D.1 / D.2); notificarea destinatarului despre punerea

la dispoziție sau eșecul ei (D.3 / D.4); predarea conținutului sau eșecul ei (E.1 / E.2); la stilul QREM „store and notify” și la modul QeRDS cu acceptare, notificarea pentru acceptare sau eșecul ei (C.1 / C.2) și acceptarea, refuzul sau expirarea termenului de acceptare (C.3 / C.4 / C.5); transmiterile către sau de la sisteme necalificate (F.1–F.3);

– **„livrat”** înseamnă, pentru ambele servicii, punerea la dispoziție a conținutului în căsuța sau contul destinatarului identificat (dovada D.1); preluarea efectivă se dovedește separat (E.1);

– fiecare dovadă conține identificatorul ei, evenimentul și motivul, data și ora (UTC), identitatea expeditorului și a destinatarului cu nivelurile de asigurare a identificării, amprenta datelor transmise și politica emitentului; fiecare dovadă se sigilează separat cu sigiliul calificat al serviciului, la nivelul B-T (XAdES, CAdES sau PAdES), cu marcă temporală calificată;

– dovezile se transmit expeditorului și, după caz, destinatarului, în format XML (EN 319 522-3) și, la cerere, în format PDF lizibil, iar oricare dintre ei le poate obține din nou pe toată durata de păstrare (secțiunea 6.11);

– structura dovezilor, semnificația fiecărei componente, momentul emiterii și destinatarul fiecărei dovezi, precum și codurile de motiv, inclusiv cele de respingere, sunt descrise în documentul public „Specificația dovezilor și codurile de respingere” (SPEC-DOVEZI-QERDS, secțiunea 10).

6.7. Data și ora trimiterii și primirii

Data și ora trimiterii, primirii și ale oricărei modificări a datelor sunt indicate prin **mărci temporale calificate**, emise de serviciul calificat de marcare temporală CERTDIGITAL (art. 44 alin. (1) lit. (f)).

6.8. Modificările necesare transmiterii

Orice modificare a datelor necesară pentru trimiterea sau primirea lor (de exemplu adăugarea dovezilor la mesaj, schimbarea formatului de transport sau conversia cerută de prestatorul destinatarului) este indicată clar expeditorului și destinatarului, prin dovezi și prin metadatele trimiterii (art. 44 alin. (1) lit. (e)). Conținutul transmis de expeditor nu se modifică.

6.9. Protecția datelor transmise

– datele transmise sunt protejate împotriva pierderii, furtului, deteriorării sau modificării neautorizate (art. 3 pct. 36): comunicații criptate (TLS 1.2 sau superior), criptarea datelor la stocare, control strict al accesului și jurnalizarea accesărilor;

– conținutul trimiterilor este accesibil numai expeditorului, destinatarului și persoanelor autorizate de aceștia;

– pentru QREM, domeniile de e-mail ale serviciului folosesc SPF, DKIM și DMARC, iar transportul între servere este criptat.

6.10. Interoperabilitatea și transmiterea între prestatori

– atunci când convine interoperabilitatea cu alți prestatori de servicii calificate de transmitere electronică înregistrată (art. 44 alin. (2a)), CERTDIGITAL folosește conectori conformi anexei II la Regulamentul de punere în aplicare (UE) 2025/1944 (ETSI EN 319 522-4-1, -4-2 și -4-3: AS4, dovezi și identificare, capabilități și încredere prin listele de încredere), iar pentru e-mail, profilul ETSI EN 319 532-4; partenerul este cel puțin un serviciu de transmitere electronică înregistrată, autentificat, iar comunicațiile sunt protejate (EN 319 521, cl. 5.5);

– atunci când datele sunt transferate între doi sau mai mulți prestatori, cerințele art. 44 alin. (1) lit. (a)–(f) se aplică tuturor prestatorilor calificați implicați; CERTDIGITAL transmite trimiteri calificate numai către prestatori calificați înscriși în listele de încredere ale statelor membre;

– trimiterile către sau de la sisteme necalificate (de exemplu e-mail obișnuit) se marchează ca atare în dovezi și nu beneficiază de prezumțiile de la art. 43 alin. (2) pentru partea necalificată.

6.11. Păstrarea datelor, a dovezilor și a jurnalelor

– conținutul trimiterilor rămâne la dispoziția destinatarului 90 de zile calendaristice de la punerea la dispoziție (dovada D.1), după care se șterge, cu jurnalizarea ștergerii; conținutul trimiterilor neacceptate sau neridicate în termenul de acceptare se șterge la expirarea acestui termen (secțiunea 12.6);

– arhiva serviciului cuprinde datele de identificare și de autentificare ale părților, dovezile, amprentele conținutului transmis, mărcile temporale și jurnalele (EN 319 521, cl. 5.4.1-03);

– perioadele de păstrare aplicate efectiv sunt: dovezile și amprentele conținutului – 10 ani de la emiterea dovezii; datele de identificare și de autentificare ale părților – 10 ani de la închiderea contului; jurnalele serviciilor – 10 ani de la înregistrare, peste minimul de 2 ani din EN 319 521, cl. 7.10-04 (EN 319 521, cl. 4.1.2-04 și 5.4.1); acestea se protejează împotriva modificării, iar dovezile se pot obține de expeditor și de destinatar pe toată această perioadă;

– reversibilitatea și portabilitatea: abonatul și, pentru dovezile care îi privesc, expeditorul și destinatarul descarcă oricând, gratuit, din cont, dovezile și trimiterile încă disponibile, în formate standardizate; la cerere sau la încetarea contractului, CERTDIGITAL furnizează exportul complet în cel mult 30 de zile (capitolul 16).

6.12. Timpul de încredere și jurnalele

– evenimentele serviciilor sunt datate cu o sursă de timp sincronizată cu UTC, iar momentele de la secțiunea 6.7 cu mărci temporale calificate;

– se jurnalizează evenimentele critice și necritice: depuneri, transmiteri, puneri la dispoziție, predări, refuzuri și eșecuri, autentificări reușite și eșuate, accesări, ștergeri, detectarea

modificărilor, operații administrative și evenimente de securitate, conform ETSI EN 319 401, cl. 7.10; evenimentele de securitate jurnalizate cuprind cel puțin modificările politicii de securitate și ale configurațiilor, pornirea și oprirea sistemelor, căderile sistemelor și defecțiunile echipamentelor, activitatea firewall-urilor și a routerelor și încercările de acces la sistemele PKI și la modulele criptografice (ETSI EN 319 521, REQ-ERDSP-7.10-03).

6.13. Personalul

Personalul cu roluri de încredere este angajat al CENTRUL DE CALCUL S.A. și are cunoștințele, experiența și calificările necesare, dovedite prin instruire formală, atestări sau experiență practică, și primește cel puțin o dată la 12 luni instruire privind amenințările noi și practicile de securitate actuale.

Identitatea expeditorilor și a destinatarilor se verifică de operatorul de înregistrare al serviciului, din Compartimentul Servicii Electronice, numit prin decizie a Directorului General, sub supravegherea responsabilului cu verificarea identității pentru transmiterea electronică înregistrată calificată, numit de asemenea prin decizie a Directorului General; responsabilul cu verificarea identității asigură că verificările efectuate în fapt sunt conforme procesului de verificare inițială a identității descris în secțiunile 6.3, 6.4 și 11.1 (ETSI EN 319 521, REQ-QERDSP-7.2.2-01 și 7.2.2-02). Funcțiile, subordonarea și separarea rolurilor sunt stabilite în documentul intern „Structura organizatorică a serviciilor de încredere și asigurarea imparțialității” (SOI).

6.14. Controale privind facilitățile, managementul și operarea

Se aplică Politicile generale CertDigital, cu următoarele precizări:

– serviciile sunt operate în centrul de date principal și în centrul de date secundar, conform Procedurii DRP (PO_SI_63), cu durata maximă de restabilire de 8 ore și pierderea maximă de date de cel mult 5 minute;

– 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;

– disponibilitatea fiecărui serviciu este de cel puțin 99,5%, cu excepția intervențiilor planificate anunțate în prealabil.

6.15. Controale criptografice și de rețea

– cheile private ale sigiliilor serviciilor se generează, se păstrează și se utilizează numai în dispozitive criptografice certificate Common Criteria EAL4 sau superior, ori EUCC EAL4 sau superior, ori, până la 31.12.2030, FIPS 140-3 nivel 3, configurate conform certificării;

– tehnicile criptografice respectă documentul „Agreed Cryptographic Mechanisms” al ECCG și se gestionează pe tot ciclul de viață;

– scanarea de vulnerabilități se efectuează cel puțin o dată pe trimestru, testul de penetrare cel puțin o dată pe an, iar firewall-urile blochează toate protocoalele și accesele care nu sunt necesare funcționării serviciilor (Regulamentul de punere în aplicare (UE) 2025/1944, anexa I).

6.16. Notificări către ADR și încetarea serviciilor

– CERTDIGITAL notifică ADR orice modificare a prestării serviciilor cu cel puțin **o lună** înainte de aplicare și intenția de încetare cu cel puțin **trei luni** înainte;

– încetarea se face conform Planului de încetare a serviciilor (00r), elaborat potrivit Regulamentului de punere în aplicare (UE) 2025/2530: trimiterile în curs se finalizează sau se returnează expeditorilor cu dovezile aferente; dovezile, datele de identificare și jurnalele se predau succesorului, dacă există, sau custodelui înregistrărilor desemnat conform Planului de încetare și se păstrează pe perioadele din capitolul 16, iar dovezile rămân accesibile părților 10 ani de la emitere; înainte de data încetării, abonații primesc exportul dovezilor lor (capitolul 16; EN 319 521, cl. 4.1.2-05).

6.17. Evaluarea conformității

Serviciile sunt evaluate 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), cu un domeniu care acoperă explicit ambele tipuri (EDS/Q și EDS/REM/Q) și cadrul de interoperabilitate (art. 44 alin. (2a)); 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

– identifică expeditorul cu un nivel de încredere ridicat și destinatarul înainte de livrare;

– securizează trimiterea și primirea cu sigiliul calificat al serviciului și indică data și ora prin mărci temporale calificate;

– emite și păstrează dovezile și le pune la dispoziția expeditorului și a destinatarului;

– indică expeditorului și destinatarului orice modificare necesară transmiterii;

– transmite trimiteri calificate numai către prestatori calificați;

– publică documentația serviciilor 24/7.

7.2. Obligațiile expeditorului, ale destinatarului și ale abonatului

– furnizează date de identificare corecte și actualizate și păstrează sub control exclusiv mijloacele de autentificare;

– expeditorul răspunde pentru conținutul datelor transmise și pentru corectitudinea datelor destinatarului;

– destinatarul își verifică periodic căsuța sau contul în care primește trimiterile, conform termenilor și condițiilor;

– notifică imediat CERTDIGITAL la suspiciunea de compromitere a mijloacelor de autentificare;

– utilizează serviciile numai în scopuri legale.

7.3. Obligațiile părților care se bazează

Verifică sigiliul calificat și marca temporală calificată de pe dovezi și statutul calificat al serviciului 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 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: conținutul datelor transmise; datele de contact greșite furnizate de expeditor; neverificarea căsuței de către destinatar; faptele prestatorilor necalificați sau ale sistemelor de e-mail obișnuite, pentru partea necalificată a transmiterii; utilizarea serviciilor peste limitările notificate în prealabil și recognoscibile de terți; nerespectarea obligațiilor de la secțiunea 7.2; neverificarea dovezilor și a statutului din Lista de

încredere de către partea care se bazează; 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 (QREM și QeRDS), 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) din Legea nr. 214/2024). Verificarea dovezilor de către părțile care se bazează este gratuită.

8.2. Protecția datelor cu caracter personal

Pentru conținutul trimiterilor, CERTDIGITAL acționează în calitate de **persoană împuternicită** a abonatului (art. 28 din Regulamentul (UE) 2016/679), pe baza clauzelor din contract; pentru datele de identificare și de cont ale expeditorilor și destinatarilor, pentru dovezi și pentru jurnalele serviciilor, CERTDIGITAL este **operator**, conform Politicii de protecție a datelor (00d). Pentru conținutul trimiterilor, CERTDIGITAL nu folosește alte persoane împuternicite. Notificările prin SMS către destinatarii fără cont se transmit prin furnizorul de SMS (capitolul 19), care prelucrează, în calitate de persoană împuternicită a CERTDIGITAL, numai numărul de telefon al destinatarului și textul notificării, pe baza unui contract încheiat conform art. 28 din Regulamentul (UE) 2016/679. 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 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 serviciilor sunt guvernate de dreptul român, sub rezerva dispozițiilor direct aplicabile ale dreptului Uniunii Europene.

Serviciile sunt furnizate în conformitate cu actele normative de la secțiunea 2.1. Organismul de supraveghere este Autoritatea pentru Digitalizarea României.

8.6. Alte prevederi

Expeditorul păstrează toate drepturile asupra datelor transmise; CERTDIGITAL dobândește numai dreptul de a le prelucra în măsura necesară prestării serviciilor. 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 art. 44 și ale Regulamentului (UE) 2025/1944

9.1. Tabel de corespondență

Cerință	Conținut	Secțiune
Regulamentul eIDAS, art. 43 alin. (2)	prezumțiile: integritate, trimitere de expeditorul identificat, primire de destinatarul identificat, exactitatea datei și orei	1.1
art. 44 alin. (1) lit. (a)	prestat de unul sau mai mulți prestatori calificați	1.3, 5.1, 6.10
art. 44 alin. (1) lit. (b)	identificarea expeditorului cu nivel de încredere ridicat	6.3
art. 44 alin. (1) lit. (c)	identificarea destinatarului înainte de livrare	6.4
art. 44 alin. (1) lit. (d)	securizare prin sigiliul avansat al prestatorului; detectarea modificărilor	6.5
art. 44 alin. (1) lit. (e)	indicarea modificărilor necesare transmiterii	6.8
art. 44 alin. (1) lit. (f)	mărci temporale calificate pentru trimitere, primire și modificări	6.7
art. 44 alin. (1), ultimul paragraf	cerințele se aplică tuturor prestatorilor implicați	6.10
art. 44 alin. (1a) / RE 2025/1944, anexa I	prezumția de conformitate: ETSI EN 319 521 V1.1.1 cu adaptări (EN 319 401, EN 319 411-1, EN 319 522-1/-2)	5.1, 6.3–6.15
RE 2025/1944, anexa I: QERDS-5.2.1.1-01A, 5.2.2-03	verificarea și autentificarea expeditorului	6.3
RE 2025/1944, anexa I: QERDS-5.2.1.1-01, 5.2.1.2-01…04, 5.2.2-03A/-04	verificarea „foarte ridicată” și autentificarea destinatarului; predare după identificare	6.4
RE 2025/1944, anexa I: ERDS-5.4.1-06…08	dovezi obligatorii pentru evenimentele din EN 319 522-1, cu semantica din EN 319 522-2	6.6
EN 319 521, cl. 4.1.1, 4.1.2, 4.2	conținutul declarației de practici și al termenilor și condițiilor (inclusiv definiția „livrat”)	6.1, 6.2, 6.6; Partea a II-a
EN 319 521, cl. 5.4.1-03, 7.10-04	arhiva serviciului; jurnale (minimum 2 ani)	6.11
art. 44 alin. (2a) / RE 2025/1944, anexa II	interoperabilitate (EN 319 522-1…-4, AS4)	4.2, 6.10
RE 2025/1944, anexa I	chei în dispozitive certificate; ECCG ACM; scanare trimestrială; test de penetrare anual	6.15
RE 2025/2530	notificări ADR; plan de încetare	6.16
ETSI EN 319 522-2 / EN 319 532-2	dovezile și conținutul lor	6.6
ETSI EN 319 531 / EN 319 532	cerințe specifice QREM (e-mail S/MIME)	4.2, 6.9, 6.10

Practicile detaliate pentru fiecare cerință sunt descrise în Partea a II-a.

PARTEA A II-A – Declarația de practici

10. Publicare și depozit

Partea a II-a descrie modul în care CERTDIGITAL prestează serviciile QeRDS (tipul `EDS/Q`) și QREM, prin e-mail (tipul `EDS/REM/Q`), și îndeplinește cerințele din Partea I. Prezentarea serviciilor, identificarea documentului, participanții și prestatorii implicați, limitele de utilizare și administrarea documentului sunt cele din capitolul 1, referințele normative sunt cele din capitolul 2, iar definițiile și acronimele, cele din capitolul 3. Partea a II-a păstrează structura declarației de practici a serviciilor, întocmită conform ETSI EN 319 521 (cl. 4.1.1 și 4.1.2), cu adaptările din anexa I la Regulamentul de punere în aplicare (UE) 2025/1944, și, pentru QREM, conform ETSI EN 319 531; corespondența cu aceste cerințe este în anexa A.

Prezentul document, termenii și condițiile și certificatele de sigiliu ale serviciilor sunt publicate la https://www.certdigital.ro/repository/, 24/7, fără restricții (EN 319 521, cl. 4.1.1-02 și -03). Versiunile anterioare rămân disponibile în secțiunea „Arhivă”.

Specificația dovezilor și lista codurilor de respingere sunt publicate în același depozit, ca document public separat: „Specificația dovezilor și codurile de respingere – serviciile calificate de transmitere electronică înregistrată (QeRDS) și de e-mail înregistrat (QREM)” (SPEC-DOVEZI-QERDS). Documentul descrie, pentru fiecare dovadă, evenimentul, momentul emiterii și destinatarul, componentele dovezii și modul de interpretare a fiecăreia, formatul și sigilarea, codurile de motiv folosite, inclusiv cele de respingere, precum și modul de obținere și de verificare a dovezilor (EN 319 521, cl. 4.1.1-10 și -11; EN 319 531, REQ-REMS-4.1.1-13 și -14). Adresa lui fixă este:

Document	Adresa fixă
SPEC-DOVEZI-QERDS	https://www.certdigital.ro/repository/politici/certdigital_spec-dovezi-qerds_ro.pdf

11. Identificare și autentificare

11.1. Înregistrarea utilizatorilor

Fiecare expeditor și destinatar își creează un cont, legat de identitatea verificată și de mijloacele de autentificare (EN 319 521, cl. 4.1.1-07). Identitatea se verifică astfel:

Metoda	Expeditor (QERDS-5.2.1.1-01A)	Destinatar (QERDS-5.2.1.1-01, „foarte ridicat”)
Prezență fizică, la punctele de înregistrare CERTDIGITAL, cu actul de identitate în original	da	da
Certificat calificat valabil pentru semnătură sau sigiliu (al CERTDIGITAL sau al altui prestator din listele de încredere)	da	da
Certificat pentru semnătură sau sigiliu avansat emis conform NCP	da	nu
Portofelul european pentru identitatea digitală	da	da
Mijloc eID notificat de nivel ridicat	da	da
Mijloc eID notificat de nivel substanțial, emis după prezență fizică	da	nu, singur
CERTDIGITAL KYC (identificare video la distanță)	numai după confirmarea CAB	numai după confirmarea CAB

Pentru persoanele juridice se verifică existența persoanei juridice (registrul comerțului sau registrul echivalent) și împuternicirea persoanei care o reprezintă sau a delegaților. Datele de identificare se verifică și prin Platforma națională de interoperabilitate, unde este posibil.

11.2. Autentificarea la fiecare utilizare

Situația	Mijloace acceptate
Expeditor, persoană	autentificare cu doi factori (parolă + cod unic din aplicația mobilă CertDigital sau echivalent), portofelul european, mijloc eID, semnătură cu certificat NCP sau calificat (QERDS-5.2.2-03)
Expeditor, sistem informatic (API, AS4)	TLS cu autentificare reciprocă, cu certificat emis pentru organizație conform politicii NCP din ETSI EN 319 411-1, plus un factor suplimentar (cheie de acces) (QERDS-5.2.2-04)
Destinatar	autentificare cu mai mulți factori, portofelul european sau mijloc eID, semnătură sau sigiliu calificat (QERDS-5.2.2-03A)
QREM, client de e-mail	numai trimiterea mesajelor și primirea notificărilor, prin conexiune TLS și parolă de aplicație generată după autentificarea cu doi factori în interfața web; preluarea conținutului se face numai prin interfața web

Încercările de autentificare eșuate se jurnalizează, iar contul se blochează temporar după depășirea unui prag.

11.3. Destinatarii fără cont

Dacă destinatarul nu are cont, CERTDIGITAL îl notifică pe canalul indicat de expeditor (e-mail sau SMS), cu o legătură de înregistrare. Datele se predau numai după verificarea identității conform

secțiunii 11.1 (QERDS-5.2.1.2-01). Dacă destinatarul nu se înregistrează în termenul de acceptare, nu mai poate prelua conținutul: se emite dovada de neridicare, adică dovada de eșec al punerii la dispoziție (D.2), iar conținutul se șterge la expirarea termenului de acceptare (secțiunea 12.6).

11.4. Păstrarea dovezilor identificării

Dovezile verificării identității (metoda, documentele verificate, nivelul de asigurare, data) și ale fiecărei autentificări se păstrează conform secțiunii 16 (QERDS-5.2.1.2-04; EN 319 521, cl. 5.4.2).

12. Ciclul de viață al trimiterii

12.1. Depunerea

– expeditorul autentificat depune trimiterea (conținut, metadate, destinatari, opțiuni);

– serviciul verifică: identitatea și drepturile expeditorului, formatul și dimensiunea, existența destinatarilor, absența codului malițios;

– trimiterea acceptată primește un identificator unic, este sigilată cu sigiliul calificat al serviciului și marcată temporal calificat, iar expeditorul primește dovada de acceptare a depunerii (A.1);

– trimiterea respinsă generează dovada de respingere (A.2), cu motivul codificat conform SPEC-DOVEZI-QERDS: format invalid (RA02), cod malițios (RA03), certificatul de semnătură al expeditorului expirat sau revocat (RA04), încălcarea politicii serviciului – de exemplu depășirea dimensiunii maxime, destinatar inexistent sau expeditor neautorizat (RA05), funcționarea defectuoasă a serviciului (RA06).

12.2. Transmiterea

În cadrul CERTDIGITAL, trimiterea ajunge direct în căsuța destinatarului. Către alt prestator calificat, trimiterea se transmite prin conectorul de interoperabilitate (secțiunea 17), cu dovezile de acceptare, refuz sau eșec al transmiterii (B.1 / B.2 / B.3).

12.3. Notificarea destinatarului

Destinatarul este notificat despre trimitere pe canalul ales (e-mail, notificare în aplicație); se emit dovezile de notificare sau de eșec al notificării (D.3 / D.4), iar la trimiterile cu acceptare, notificarea pentru acceptare se dovedește prin dovezile C.1 / C.2. Notificarea nu conține conținutul trimiterii.

12.4. Punerea la dispoziție („livrat”)

Trimiterea se consideră **livrată** în momentul punerii la dispoziție a conținutului în căsuța sau contul destinatarului identificat; se emite dovada de punere la dispoziție (D.1) sau, în caz de eșec, dovada D.2.

12.5. Predarea și acceptarea

– predarea înseamnă preluarea efectivă a conținutului de către destinatarul autentificat (descărcare prin interfața web sau prin API; pentru QREM, numai prin interfața web); se emite dovada de predare (E.1) sau de eșec al predării (E.2);

– pentru QREM, stilul „store and forward” (obligatoriu de oferit și implicit) transmite conținutul fără acceptare prealabilă; stilul „store and notify” (opțional) cere acceptarea explicită a destinatarului: după autentificarea în interfața web, destinatarul acceptă sau refuză trimiterea

printr-o acțiune expresă, înainte ca aceasta să-i fie predată; acceptarea, refuzul sau expirarea termenului se consemnează prin dovezile C.3, C.4 sau C.5 (EN 319 531, REQ-REMS-4.1.1-07);

– termenul de acceptare este stabilit de expeditor, în limitele din termenii și condițiile serviciului: implicit 15 zile, cel mult 30 de zile.

12.6. Disponibilitatea conținutului

Conținutul rămâne disponibil destinatarului 90 de zile calendaristice de la punerea la dispoziție (dovada D.1), după care se șterge definitiv, cu jurnalizarea ștergerii, și nu mai poate fi recuperat de CERTDIGITAL; rămân dovezile și amprenta conținutului (capitolul 16). Dacă destinatarul nu a preluat conținutul până la ștergere, se emite dovada de eșec al predării (E.2).

Dacă trimiterea cere acceptarea destinatarului și acesta nu o acceptă în termenul de acceptare, se emite dovada de expirare a termenului (C.5), iar conținutul nu mai poate fi preluat și se șterge la expirarea termenului de acceptare. Destinatarul fără cont care nu se înregistrează în termenul de acceptare nu mai poate prelua conținutul; se emite dovada de neridicare (D.2), iar conținutul se șterge la expirarea termenului de acceptare. Expeditorul este informat prin dovezi despre fiecare dintre aceste situații. Termenele sunt cuprinse în termenii și condițiile serviciilor (EN 319 521, cl. 4.2-03).

12.7. Sistemele necalificate

Trimiterile către o adresă de e-mail obișnuită sau primite de la un sistem necalificat se marchează clar ca atare, iar dovezile corespunzătoare (F.1–F.3) arată că prezumțiile de la art. 43 alin. (2) nu se aplică pentru partea necalificată a transmiterii.

12.8. Modificările necesare transmiterii

Serviciul nu modifică conținutul transmis de expeditor. Modificările necesare transmiterii (adăugarea dovezilor ca părți MIME, schimbarea plicului de transport, conversia formatului cerută de prestatorul destinatarului) se indică în dovezi și în metadatele trimiterii, astfel încât expeditorul și destinatarul să le cunoască (art. 44 alin. (1) lit. (e); EN 319 521, cl. 4.1.1-06 și 5.1.1-04).

12.9. Particularitățile QREM (ETSI EN 319 531)

– mesajele respectă MIME (RFC 2045, RFC 5322); serviciul folosește SMTP pentru trimitere și pentru notificări, iar preluarea conținutului se face prin interfața web;

– clienții de e-mail suportați sunt cei standard, cu suport S/MIME, iar lista clienților de e-mail testați de CERTDIGITAL se publică împreună cu instrucțiunile de utilizare ale serviciului;

– dovezile se atașează mesajelor ca părți MIME `application/xml` și, la cerere, `application/pdf`, conform EN 319 532-3;

– transmiterea către alți prestatori REM se face numai către prestatori calificați, conform profilului de bază REM din EN 319 532-4;
– domeniile de e-mail ale serviciului folosesc SPF, DKIM și DMARC; QREM folosește subdomeniul rem.certdigital.ro, cu server de e-mail propriu (varianta A2), iar adresa serviciului este office@rem.certdigital.ro;
– stilul „store and notify” se oferă pentru mesajele depuse în QREM (EN 319 531, REQ-REMS-4.1.1-05); pentru mesajele primite prin transmitere de la alt prestator REM, QREM nu aplică propriul stil „store and notify”, ci pune conținutul la dispoziția destinatarului în stilul „store and forward”; dacă prestatorul expeditorului operează el însuși stilul „store and notify”, QREM transmite destinatarului notificarea pentru acceptare primită de la acesta și emite dovezile C.1 / C.2, iar destinatarul acceptă sau refuză prin legătura din notificare, la prestatorul expeditorului, care emite dovezile C.3 / C.4 / C.5 (REQ-REMS-4.1.1-06; EN 319 532-1, cl. 6.2.3);
– QREM transmite mesaje către alți prestatori REM numai dacă aceștia sunt prestatori calificați de REM înscriși în listele de încredere ale statelor membre, cu care CERTDIGITAL a convenit interoperabilitatea conform profilului de bază REM (EN 319 532-4), cu autentificare reciprocă și cu verificarea sigiliului mesajelor; în aceleași condiții, QREM acceptă mesajele transmise de acești prestatori, dacă respectă limitele de la secțiunea 1.4 și politica serviciului, iar în caz contrar le refuză, cu dovada B.2 și cu motivul codificat (REQ-REMS-4.1.1-09 și -10);
– QREM nu transmite mesaje către servicii de transmitere electronică înregistrată care nu sunt servicii REM (de exemplu servicii bazate pe AS4, inclusiv serviciul QeRDS al CERTDIGITAL) și nu acceptă mesaje transmise de acestea; pentru comunicarea cu utilizatorii acestor servicii se folosește serviciul QeRDS (REQ-REMS-4.1.1-11 și -12);
– componentele dovezilor și modul în care se interpretează fiecare dintre ele sunt definite în SPEC-DOVEZI-QERDS, capitolul 4 (REQ-REMS-4.1.1-13); dovezile se atașează mesajelor REM și se pot descărca din interfața web pe toată durata de păstrare (secțiunea 13.4; REQ-REMS-4.1.1-14).

12.10. Particularitățile QeRDS (ETSI EN 319 522)

– utilizatorii folosesc portalul web sau interfața de programare documentată în specificația publicată;
– dovezile se furnizează în format XML (spațiul de nume `http://uri.etsi.org/19522/v1#`) și, la cerere, în format PDF lizibil;
– transmiterea către alți prestatori se face prin conectorul AS4 (secțiunea 17).

13. Dovezile

13.1. Evenimentele și dovezile emise

Cod	Eveniment (ETSI EN 319 522-1)	QeRDS	QREM
A.1 / A.2	acceptarea / respingerea depunerii (SubmissionAcceptance / SubmissionRejection)	da	da
B.1 / B.2 / B.3	acceptarea / refuzul / eșecul transmiterii către alt prestator (RelayAcceptance / RelayRejection / RelayFailure)	da, la interoperabilitate	da, la transmiterea între prestatori REM
C.1 / C.2	notificarea destinatarului pentru acceptare / eșecul ei (NotificationForAcceptance / NotificationForAcceptanceFailure)	la modul cu acceptare	la stilul „store and notify” și la mesajele primite de la un prestator REM care operează acest stil
C.3 / C.4 / C.5	acceptarea / refuzul / expirarea termenului de acceptare (ConsignmentAcceptance / ConsignmentRejection / AcceptanceRejectionExpiry)	la modul cu acceptare	la stilul „store and notify”
D.1 / D.2	punerea la dispoziție / eșecul ei, inclusiv neridicarea (ContentConsignment / ContentConsignmentFailure)	da	da
D.3 / D.4	notificarea destinatarului despre punerea la dispoziție / eșecul ei (ConsignmentNotification / ConsignmentNotificationFailure)	da	da
E.1 / E.2	predarea / eșecul predării (ContentHandover / ContentHandoverFailure)	da	da
F.1 / F.2 / F.3	transmiterea către un sistem necalificat / eșecul ei / primirea de la un sistem necalificat (RelayToNonERDS / RelayToNonERDSFailure / ReceivedFromNonERDS)	da	da

Dovezile sunt obligatorii pentru evenimentele de mai sus (RE 2025/1944, anexa I: ERDS-5.4.1-06…08). CERTDIGITAL nu emite dovezile C.6, D.5 și D.6; livrarea se dovedește prin D.1, iar preluarea efectivă prin E.1. Momentul emiterii, emitentul și destinatarul fiecărei dovezi și codurile de motiv sunt descrise în SPEC-DOVEZI-QERDS, capitolele 3 și 6.

13.2. Conținutul dovezilor

Fiecare dovadă cuprinde, conform ETSI EN 319 522-2, cl. 8: identificatorul dovezii, evenimentul și, după caz, motivul; data și ora (UTC); politica emitentului (OID 1.3.6.1.4.1.47898.14.1), emitentul și sigiliul; identitatea expeditorului și a destinatarului, cu nivelurile de asigurare a identificării, exprimate ca URI; identificatorul trimiterii, amprenta conținutului și ora trimiterii. Modul de interpretare a fiecărei componente este descris în SPEC-DOVEZI-QERDS, capitolul 4 (EN 319 531, REQ-REMS-4.1.1-13).

13.3. Formatul și sigilarea

Fiecare dovadă se sigilează separat cu sigiliul calificat al serviciului, la nivelul B-T, cu marcă temporală calificată: XAdES pentru dovezile XML (obligatoriu în profilul de bază REM) și PAdES pentru varianta PDF lizibilă.

13.4. Obținerea și verificarea dovezilor

Dovezile se transmit automat expeditorului (și, pentru evenimentele care îl privesc, destinatarului) și pot fi descărcate din cont pe toată durata de păstrare. Oricine le poate verifica gratuit cu orice validator de semnături sau sigilii calificate, inclusiv cu serviciul calificat de validare CERTDIGITAL (QESVal), folosind Lista de încredere a României; pașii verificării sunt descriși în SPEC-DOVEZI-QERDS, capitolul 7 (EN 319 521, cl. 4.1.1-10 și -11).

13.5. Limitele de valabilitate a dovezilor

Dovezile se sigilează la nivelul B-T, cu marcă temporală calificată. Limitele de valabilitate a dovezilor sunt următoarele (EN 319 521, cl. 4.1.1-12):

– verificarea unei dovezi după expirarea sau revocarea certificatului de sigiliu cere informațiile de revocare ale acestuia; CERTDIGITAL publică aceste informații (CRL și OCSP pentru CERTDIGITAL QCA G5) și le păstrează disponibile cel puțin pe durata de păstrare a dovezilor (capitolul 16);

– CERTDIGITAL pune dovezile la dispoziția părților 10 ani de la emitere; după acest termen, dovezile păstrate de părți rămân verificabile pe termen lung numai dacă au fost augmentate (de exemplu la nivelul LTA) sau încredințate unui serviciu calificat de păstrare, cum este serviciul calificat de păstrare CERTDIGITAL (PSPPS);

– valoarea probatorie a unei dovezi poate scădea dacă algoritmii sau lungimile de cheie folosite la sigiliu sau la marca temporală nu mai sunt considerate sigure (documentul „Agreed Cryptographic Mechanisms” al ECCG); în acest caz, CERTDIGITAL anunță părțile în depozitul de documente și augmentează dovezile pe care le păstrează încă;

– dovezile privind partea necalificată a unei transmiteri (F.1–F.3) nu beneficiază de prezumțiile de la art. 43 alin. (2) din Regulamentul eIDAS.

14. Protecția datelor transmise și controale tehnice

14.1. Integritate și confidențialitate

– conținutul se sigilează la depunere cu sigiliul calificat al serviciului (certificat calificat, emis conform politicilor QCP-l-qscd/NCP+; EN 319 521, cl. 5.1.2-01); orice modificare se detectează la verificare, iar trimiterea afectată se oprește, cu notificarea expeditorului și a destinatarului;

– comunicațiile folosesc TLS conform ECCG ACM; conținutul și identitățile părților se criptează la stocare și sunt accesibile numai expeditorului, destinatarului și delegaților autorizați (EN 319 521, cl. 5.1.1);

– se aplică scanarea antimalware la depunere și jurnalizarea tuturor accesărilor (EN 319 521, cl. 4.1.1-08).

14.2. Cheile serviciilor

Cheile private ale sigiliilor CERTDIGITAL QERDS SERVICE G5 și CERTDIGITAL QREM SERVICE G5 se generează în ceremonie, sub control dual, și se păstrează în modulele criptografice Thales Luna PCIe HSM 7 A790 (FIPS 140-3 nivel 3; Common Criteria; înscrise pe lista QSCD), configurate conform certificării (RE 2025/1944, anexa I: 7.5-03). Certificatul QREM include adresa de e-mail a serviciului, pentru semnătura S/MIME.

La compromiterea sau la suspiciunea de compromitere a serviciilor ori a cheii private CERTDIGITAL QERDS SERVICE G5 sau CERTDIGITAL QREM SERVICE G5, CERTDIGITAL oprește sigilarea cu cheia afectată, solicită revocarea certificatului de sigiliu de către CERTDIGITAL QCA G5 și notifică, conform Procedurii de notificare a incidentelor (00q), ADR, în cel mult 24 de ore de la luarea la cunoștință, DNSC și, după caz, ANSPDCP, precum și toți abonații, expeditorii și destinatarii, direct, prin e-mail, părțile care se bazează, prin publicare în depozitul de documente, și prestatorii calificați cu care a convenit interoperabilitatea. Informarea precizează că dovezile și datele sigilate cu cheia compromisă pot să nu mai fie valabile de la momentul cunoscut al compromiterii, iar dovezile a căror marcă temporală calificată este anterioară acestui moment rămân verificabile, deoarece mărcile temporale sunt emise cu cheia distinctă a serviciului calificat de marcare temporală. Cheia nouă se generează în ceremonie, conform Procedurii privind generarea cheilor, iar evenimentul se tratează ca dezastru, conform Planului de continuitate a afacerii, Anexa 6, secțiunea 3.8 (ETSI EN 319 521, REQ-ERDSP-7.11-07 și 7.11-09).

14.3. Rețea și vulnerabilități

Se aplică ETSI EN 319 401, cl. 7.8, cu adaptările din RE 2025/1944: TLS conform ECCG ACM, scanare de vulnerabilități cel puțin trimestrială, test de penetrare cel puțin anual, firewall-uri care blochează tot ce nu e necesar serviciilor; componentele se autentifică reciproc.

Punctele de acces publice ale serviciilor – portalul și interfața de programare QeRDS (erds.certdigital.ro), interfața web și serverul de e-mail QREM (rem.certdigital.ro) și conectorul AS4 – folosesc TLS cu certificate de autentificare a site-ului web emise pentru numele de domeniu ale serviciilor; datele care ies din rețelele interne ale CERTDIGITAL se transmit numai prin astfel de conexiuni (ETSI EN 319 521, REQ-ERDSP-7.8-05).

15. Timpul

Data și ora trimiterii, primirii și ale oricărei modificări se indică prin mărci temporale calificate emise de serviciul calificat de marcare temporală CertDigital TSA (CERTDIGITAL TSA G4; CERTDIGITAL TSA G5, de la înscrierea ei în Lista de încredere), legate de conținutul sau de dovada respectivă, cu exactitatea față de UTC declarată în PDP-QTST (art. 44 alin. (1) lit. (f); EN 319 521, cl. 5.3.2).

Referința de timp a serviciilor este timpul universal coordonat (UTC). Serverele serviciilor se sincronizează cu sursa de timp a CERTDIGITAL (servere de timp cu receptor GNSS în ambele centre de date; documentul „Sursa de timp”, 00u). Data și ora din dovezi și din jurnale se exprimă în UTC; interfața web le poate afișa și în ora României (EET/EEST), cu indicarea fusului orar (EN 319 521, cl. 5.3.1-01).

16. Păstrarea, reversibilitatea și portabilitatea

Ce se păstrează	Cât	Observații
Conținutul trimiterilor	90 de zile calendaristice de la punerea la dispoziție (dovada D.1); conținutul neacceptat sau neridicat în termenul de acceptare, până la expirarea acestui termen (secțiunea 12.6)	apoi se șterge, cu jurnalizarea ștergerii
Dovezile și amprentele conținutului	10 ani de la emiterea dovezii	protejate împotriva modificării; obtenabile de părți
Datele de identificare și de autentificare ale părților, inclusiv dovada acceptării termenilor și condițiilor	10 ani de la închiderea contului	EN 319 521, cl. 5.4.1-03, 5.4.2
Jurnalele serviciilor	10 ani de la înregistrare	peste minimul de 2 ani din EN 319 521, cl. 7.10-04

Perioadele de mai sus sunt cele aplicate efectiv (EN 319 521, cl. 4.1.2-04 și 5.4.1).

Reversibilitate și portabilitate: abonatul și, pentru dovezile care îi privesc, expeditorul și destinatarul pot descărca oricând, gratuit, din cont, dovezile în format XML (ETSI EN 319 522-3, sigilate XAdES) și PDF (sigilate PAdES), precum și trimiterile încă disponibile. La cerere sau la încetarea contractului, CERTDIGITAL furnizează exportul complet, ca arhivă cu index, în cel mult 30 de zile, pe un canal securizat; la încetarea contractului, conturile se închid numai după furnizarea exportului. Formatele sunt standardizate și pot fi preluate de un alt prestator de servicii de transmitere electronică înregistrată sau de un serviciu calificat de păstrare (EN 319 521, cl. 4.1.2-04).

17. Interoperabilitatea

– CERTDIGITAL poate conveni interoperabilitatea cu alți prestatori calificați (art. 44 alin. (2a)); în acest caz folosește conectorul AS4 conform ETSI EN 319 522-4-1, dovezile și identificarea conform EN 319 522-4-2 și descoperirea capabilităților și încrederea prin listele de încredere conform EN 319 522-4-3 (RE 2025/1944, anexa II);

– partenerii sunt prestatori calificați înscriși în listele de încredere, autentificați reciproc; comunicațiile sunt protejate (EN 319 521, cl. 5.5);

– cerințele art. 44 alin. (1) lit. (a)–(f) se aplică tuturor prestatorilor implicați în transmitere.

18. Controale de management și operare

Se aplică Politicile generale CertDigital și ETSI EN 319 401, cl. 5–7, cu adaptările din RE 2025/1944:

– **evaluarea riscurilor**: anuală și la orice schimbare semnificativă; rezultatele stau la baza măsurilor de securitate;

– **personalul**: roluri de încredere separate (administrator, operator, auditor), instruire cel puțin o dată la 12 luni privind amenințările și practicile de securitate actuale;

– **controlul accesului**: acces cu privilegii minime, autentificare cu doi factori pentru administratori, revizuirea periodică a drepturilor;

– **securitatea fizică**: centrul de date principal și centrul de date secundar ale CERTDIGITAL, cu acces controlat prin autentificare în mai mulți factori și supraveghere;

– **operarea**: gestionarea schimbărilor, copii de rezervă criptate în celălalt centru de date, monitorizare continuă;

– **incidentele**: notificate conform 00q (ADR în cel mult 24 de ore, DNSC, ANSPDCP, persoanele afectate);

– **jurnalizarea**: evenimentele de la secțiunea 13.1, autentificările, accesările, operațiile administrative și evenimentele de securitate, cu timp sincronizat;

– **continuitatea**: conform PO_SI_63, disponibilitate de cel puțin 99,5%, RTO de 8 ore și RPO de cel mult 5 minute;

– **lanțul de aprovizionare**: furnizorii platformei și ai componentelor critice sunt evaluați cel puțin anual și supuși unor obligații contractuale de securitate (capitolul 19);

– **încetarea**: conform planului 00r (RE 2025/2530): trimiterile în curs se finalizează sau se returnează cu dovezi; dovezile, datele de identificare și jurnalele se predau succesorului, dacă există, sau custodelui înregistrărilor desemnat conform Planului de încetare și se păstrează pe perioadele din capitolul 16, iar dovezile rămân accesibile părților 10 ani de la emitere; înainte de data încetării, abonații primesc exportul dovezilor lor (EN 319 521, cl. 4.1.2-05);

– **conformitatea**: evaluare de către un CAB acreditat cel puțin o dată la 24 de luni, cu un domeniu care acoperă ambele tipuri de servicii, și audit intern anual.

18.1. Securitatea rețelei

Pe lângă măsurile din Politicile generale (cap. 9), din planul de securitate al sistemului informatic și din secțiunea 14.3, pentru servicii se aplică următoarele (ETSI EN 319 401, cl. 7.8, cu adaptările din RE 2025/1944):

– Toate sistemele dintr-o zonă de securitate au aceleași controale de securitate: configurația întărită, protecția anti-malware, jurnalizarea centralizată și regulile de filtrare ale zonei; un

sistem care cere alte controale se mută într-o zonă proprie. Accesul la o rețea sau la o zonă se acordă pe baza evaluării cerințelor ei de securitate (GR-TSP), cu aprobarea ofițerului de securitate IT (REQ-7.8-03).

– Comunicațiile dintre zone și, în interiorul fiecărei zone, dintre sisteme se limitează la cele necesare funcționării serviciilor, prin firewall-uri cu filtrare și monitorizare și prin reguli de filtrare la nivelul platformei de virtualizare și al containerelor; restul traficului este blocat (REQ-7.8-04).

– Conexiunile și serviciile care nu sunt necesare se interzic sau se dezactivează pe toate sistemele (porturi, protocoale, servicii și conturi implicite); la rețeaua CERTDIGITAL și la sistemele serviciilor se conectează numai echipamente autorizate și înscrise în inventar (REQ-7.8-05).

– Regulile firewall, segmentarea rețelei și măsurile de protecție se revizuiesc cel puțin anual, după incidente semnificative și după modificări semnificative ale operațiunilor sau ale riscurilor; revizuirea se consemnează în proces-verbal (REQ-7.8-06).

– Rețeaua de administrare este separată de rețeaua operațională, iar canalele de administrare sunt separate de restul traficului. Stațiile de administrare sunt dedicate: se folosesc numai pentru administrarea sistemelor și a măsurilor de securitate, nu pentru e-mail, navigare pe internet sau alte activități (REQ-7.8-08, REQ-7.8-09X).

– Comunicațiile dintre sisteme de încredere distincte (aplicațiile și modulele criptografice, aplicațiile și bazele de date, cele două centre de date) se fac numai prin canale separate logic de celelalte comunicații, criptate și cu autentificarea reciprocă a capetelor, prin TLS sau VPN cu certificate (REQ-7.8-11X).

– Mediile de dezvoltare, de test și de producție sunt separate, inclusiv copiile lor de siguranță: copiile mediilor de dezvoltare și de test se păstrează separat de copiile sistemelor de producție, în depozite la care sistemele de producție nu au acces (REQ-7.8-10).

– Protecția împotriva programelor malițioase este activă pe toate stațiile și serverele; semnăturile și motorul de detecție se actualizează automat, cel puțin o dată pe zi, iar consola centrală semnalează sistemele neactualizate în ultimele 24 de ore (REQ-7.8-15X, REQ-7.8-16X).

– Scanările de vulnerabilitate acoperă adresele IP publice și private ale sistemelor serviciilor, din lista ținută de ofițerul de securitate IT și actualizată la fiecare modificare a infrastructurii. Pentru fiecare scanare de vulnerabilități și pentru fiecare test de penetrare se păstrează, împreună cu raportul, dovezile că a fost efectuat de o persoană sau entitate cu competențele, instrumentele, experiența, angajamentul deontologic și independența necesare unui raport credibil: calificările și certificările profesionale ale echipei, instrumentele folosite și declarația de independență față de activitatea testată (REQ-7.8-13, REQ-7.8-19X).

– CERTDIGITAL aplică un plan de implementare, aprobat de Directorul General, pentru: a) trecerea treptată și sigură la protocoalele de rețea de ultimă generație (IPv6, în regim dual-stack, pentru punctele de acces publice), cu măsuri de accelerare a trecerii; b) standardele moderne de securitate a e-mailului pentru toate domeniile de e-mail ale CERTDIGITAL (SPF, DKIM și DMARC cu politică de respingere, MTA-STS și TLS-RPT; DANE, unde infrastructura permite); c) bunele practici de securitate DNS (DNSSEC pentru zonele certdigital.ro), de securitate a rutării (RPKI, cu înregistrări ROA pentru prefixele folosite, prin furnizorii de internet) și de igienă a rutării, prin filtrarea adreselor sursă false conform BCP 38.

18.2. Monitorizarea și jurnalizarea

Monitorizarea și jurnalizarea se fac conform Politicilor generale (secțiunea 9.4), planului de securitate al sistemului informatic și secțiunii 6.12, cu următoarele precizări (ETSI EN 319 401, cl. 7.9.1):

– Jurnalele cuprind cel puțin: a) traficul de rețea de intrare și de ieșire (jurnalele firewall-urilor și ale sistemelor de detecție și prevenire a intruziunilor); b) crearea, modificarea și ștergerea conturilor și extinderea drepturilor; c) accesul la sisteme și aplicații; d) evenimentele de autentificare, reușite și eșuate; e) pornirea, oprirea și suspendarea jurnalizării; f) administrarea utilizatorilor și a drepturilor, inclusiv accesul privilegiat; g) activitățile efectuate cu conturile de administrator; h) accesul la fișierele de configurație critice și la copiile de siguranță și modificarea lor; i) jurnalele instrumentelor de securitate (anti-malware, detecția și prevenirea intruziunilor, firewall-uri); j) utilizarea și performanța resurselor sistemelor; k) accesul fizic în zonele de securitate; l) accesul la echipamentele de rețea și utilizarea lor; m) evenimentele de mediu: alarmele de incendiu, inundație, temperatură, umiditate, alimentare și climatizare (REQ-7.9.1-04X).

– Regulile de corelare și pragurile de alertare se ajustează la revizuirea lunară a jurnalelor și după fiecare incident sau alertă falsă, pentru a reduce alertele fals pozitive și evenimentele nedetectate; ajustările se consemnează.

– Lista activelor jurnalizate (sistemele, aplicațiile, echipamentele de rețea și de securitate și categoriile de evenimente colectate de la fiecare) se stabilește pe baza evaluării riscurilor (GR-TSP), face parte din inventarul activelor și se revizuiește, împreună cu procedurile de jurnalizare și monitorizare, cel puțin anual și după incidente semnificative.

– Pragurile de alarmă se stabilesc pentru fiecare categorie monitorizată (disponibilitatea serviciilor și a punctelor de acces, utilizarea resurselor, autentificările eșuate repetate, modificările de configurație și de drepturi, evenimentele de securitate, sincronizarea timpului, parametrii de mediu) și se documentează în configurația sistemului de monitorizare; depășirea unui prag declanșează automat alarma către personalul de serviciu și ofițerul de

securitate IT, care inițiază fără întârziere răspunsul, conform Procedurii de notificare a incidentelor.

– Sistemele de jurnalizare și de monitorizare sunt redundante: rulează pe platforma de virtualizare din ambele centre de date, iar jurnalele se replică în DC2 și se includ în copiile de siguranță. Funcționarea lor este supravegheată de un sistem independent de ele, care alertează personalul de serviciu la oprirea colectării jurnalelor sau a monitorizării.

18.3. Incidentele și vulnerabilitățile

Incidentele se gestionează și se notifică conform Politicilor generale (cap. 10), Procedurii de notificare a incidentelor (00q) și secțiunii 6.14, cu următoarele precizări (ETSI EN 319 401, cl. 7.9.2–7.9.5 și 7.11.3):

– Un incident este semnificativ dacă este îndeplinit cel puțin unul dintre criteriile de mai jos (Regulamentul de punere în aplicare (UE) 2024/2690, art. 3 și 14): a) a cauzat sau poate cauza CERTDIGITAL o pierdere financiară directă mai mare de 500.000 EUR sau de 5 % din cifra de afaceri anuală totală din exercițiul financiar anterior, oricare dintre acestea este mai mică; b) a cauzat sau poate cauza exfiltrarea secretelor comerciale ale CERTDIGITAL; c) a cauzat sau poate cauza decesul unei persoane fizice; d) a cauzat sau poate cauza prejudicii considerabile sănătății unei persoane fizice; e) s-a produs un acces reușit, suspectat a fi rău intenționat și neautorizat, la rețelele și sistemele informatice, care poate cauza perturbări operaționale grave; f) îndeplinește criteriile incidentelor recurente de mai jos; g) un serviciu de încredere este complet indisponibil mai mult de 20 de minute; h) un serviciu de încredere este indisponibil pentru utilizatori sau pentru părțile care se bazează mai mult de o oră, calculat pe o săptămână calendaristică; i) mai mult de 1 % dintre utilizatorii sau părțile care se bazează din Uniune, ori mai mult de 200.000 dintre aceștia, oricare dintre numere este mai mic, sunt afectați de disponibilitatea limitată a unui serviciu de încredere; j) este compromis accesul fizic într-o zonă în care se află rețelele și sistemele informatice și la care accesul este restricționat personalului de încredere, ori protecția acestui acces; k) este compromisă integritatea, confidențialitatea sau autenticitatea datelor stocate, transmise sau prelucrate în legătură cu prestarea unui serviciu de încredere, cu impact asupra a mai mult de 0,1 % dintre utilizatorii sau părțile care se bazează din Uniune ori a mai mult de 100 dintre aceștia, oricare dintre numere este mai mic. Întreruperile programate și consecințele planificate ale lucrărilor de mentenanță programate, efectuate de CERTDIGITAL sau în numele său, nu se consideră incidente semnificative. La calculul numărului de utilizatori afectați se iau în considerare clienții care au un contract cu CERTDIGITAL prin care au acces la rețelele și sistemele informatice sau la serviciile oferite prin acestea, precum și persoanele fizice și juridice asociate clienților persoane juridice care folosesc aceste rețele, sisteme sau servicii. Incidentele care, separat, nu sunt semnificative se consideră împreună un incident

semnificativ dacă s-au produs de cel puțin două ori în 6 luni, au aceeași cauză aparentă și, împreună, depășesc pragul pierderii financiare directe de mai sus.

– Evaluarea și clasificarea evenimentelor se fac după criteriile de mai sus, stabilite în prealabil, și printr-o triere care stabilește prioritatea izolării incidentului și a eliminării cauzei; pentru evaluare se analizează jurnalele relevante, corelate în sistemul centralizat de jurnale. Clasificarea se reevaluează ori de câte ori apar informații noi sau după analiza informațiilor existente; modificarea se consemnează în registrul incidentelor și, dacă este cazul, se comunică destinatarilor notificării. Ofițerul de securitate IT analizează trimestrial registrul incidentelor pentru a identifica incidentele recurente (REQ-7.9.4-02X).

– Răspunsul la incident cuprinde izolarea, pentru a împiedica extinderea efectelor, eliminarea cauzei (eradicarea), astfel încât incidentul să nu continue și să nu se repete, și recuperarea, inclusiv prin planul de continuitate; după închidere, analiza post-incident consemnează în registrul incidentelor cauza, lecțiile învățate și măsurile (REQ-7.9.2-01X).

– Angajații raportează imediat ofițerului de securitate IT orice eveniment suspect. Clienții, titularii, părțile care se bazează și furnizorii raportează orice eveniment suspect sau posibil incident de securitate la office@certdigital.ro sau la +40 253 214 767, iar suspiciunea de compromitere a mijloacelor de autentificare, a cheilor sau a portofelului se poate transmite oricând și prin canalele de revocare ale serviciilor. Canalul se comunică clienților prin prezentul document, prin termenii și condițiile serviciilor și prin Politica privind relațiile cu clienții, iar furnizorilor, prin contract; raportările se înregistrează și se transmit imediat ofițerului de securitate IT, iar personalul este instruit, la angajare și cel puțin anual, să folosească procedura și să se adreseze punctului de contact (REQ-7.9.3-03X, REQ-7.9.3-04X).

– Ofițerul de securitate IT verifică trimestrial, pe baza registrului incidentelor, că fiecare incident închis are analiza post-incident documentată (cauza, lecțiile învățate, măsurile) și raportează rezultatul Directorului General; verificarea se reia la auditul intern anual. Procedura de gestionare a incidentelor se testează și se revizuiește cel puțin anual, după incidente semnificative și la modificări semnificative ale operațiunilor sau ale riscurilor (REQ-7.9.2-08X).

– Avertizările și informările primite de la DNSC, în calitate de CSIRT național, și de la ADR privind incidente, vulnerabilități, amenințări sau măsuri de atenuare se primesc de ofițerul de securitate IT, se înregistrează, se evaluează fără întârziere în raport cu sistemele serviciilor și, după caz, se transformă în măsuri, cu actualizarea GR-TSP; cele care privesc o criză în desfășurare se transmit echipei de management și acțiune în caz de urgență (REQ-7.11.3-02X).

18.4. Copiile de siguranță și continuitatea

Copiile de siguranță și continuitatea respectă Politicile generale (cap. 12), Procedura DRP (PO_SI_63), Planul de continuitate a afacerii (PO_C_SI_S_63, cu Anexa 6) și secțiunea 6.14, cu următoarele precizări (ETSI EN 319 401, cl. 7.11):

– Planul de copii de siguranță stabilește, pentru fiecare sistem al serviciilor: datele copiate, inclusiv datele de configurație ale sistemelor, ale echipamentelor de rețea și ale platformei de virtualizare; frecvența; legătura cu duratele de recuperare (RTO/RPO); locațiile (DC2, în afara rețelei sistemului copiat, și copia offline, păstrată separat de ambele centre de date); controalele fizice și logice, după clasa informațiilor (criptare pentru datele restricționate, acces numai pentru administratorii desemnați, jurnalizarea accesului); restaurarea (cererea, aprobarea Directorului Tehnic, verificarea după restaurare); duratele de păstrare ale copiilor, stabilite după cerințele de afaceri și cele legale. Datele serviciilor și copiile lor se păstrează numai în centrele de date proprii și pe copia offline, fără servicii cloud ale terților. Planul se actualizează la fiecare modificare a sistemelor și cel puțin anual (REQ-7.11.2-02X).

– Integritatea și completitudinea copiilor se verifică automat la fiecare copiere (sume de control, rapoartele de execuție) și la fiecare restaurare de probă; erorile generează alertă și se tratează ca incidente (REQ-7.11.2-03X).

– Planul de continuitate al serviciilor (Anexa 6 la PCA) se revizuiește cel puțin anual, după fiecare test sau activare a centrului de date secundar, după incidentele semnificative și la modificările semnificative ale serviciilor, ale operațiunilor sau ale riscurilor (REQ-7.11.3-03X).

18.5. Lanțul de aprovizionare

Politica de securitate a lanțului de aprovizionare, comună serviciilor de încredere CERTDIGITAL și aplicată serviciilor, este următoarea (ETSI EN 319 401, cl. 7.14, aplicabilă prin anexa I la RE 2025/1944); organizațiile externe care susțin serviciile și obligațiile lor sunt cele din capitolul 19:

– **Domeniul și rolul**: politica guvernează relațiile cu furnizorii direcți și cu prestatorii de servicii care livrează produse, servicii sau procese TIC pentru servicii (producătorii și distribuitorii modulelor criptografice, furnizorii platformei și ai componentelor software, furnizorii de conectivitate, de e-mail și de SMS, mentenanța echipamentelor și a clădirilor, colaboratorii externi), pentru a reduce riscurile identificate în GR-TSP (art. 21 alin. (2) lit. (d) din Directiva (UE) 2022/2555). Rolul CERTDIGITAL în lanțul de aprovizionare este cel de client și integrator al produselor și serviciilor TIC, care prestează serviciile în propriile centre de date și răspunde, în ansamblu, de conformitatea lor; CERTDIGITAL nu deleagă terților operarea serviciilor, verificarea identității sau a atributelor ori gestionarea cheilor. Rolul se comunică fiecărui furnizor direct prin contract (REQ-7.14.1-01X, REQ-7.14-03X).

– **Selecția și contractarea**: înainte de contractare, furnizorii se evaluează conform procedurii interne PO_C_SI_S_24, după criteriile: a) practicile de securitate cibernetică ale furnizorului, inclusiv procedurile de dezvoltare securizată; b) capacitatea de a respecta specificațiile de securitate cibernetică, riscurile și nivelurile de clasificare ale serviciilor, sistemelor sau produselor livrate; c) calitatea și reziliența produselor și serviciilor TIC și măsurile de gestionare a riscurilor de securitate cibernetică încorporate în ele, inclusiv certificările (pentru modulele criptografice: Common Criteria EAL4+ sau EUCC și calificarea ca dispozitiv calificat); d) posibilitatea de a diversifica sursele de aprovizionare și de a limita dependența de un singur furnizor; e) rezultatele evaluărilor coordonate la nivelul Uniunii ale riscurilor de securitate ale lanțurilor de aprovizionare critice, unde există. Respectarea politicilor și a cerințelor de securitate ale CERTDIGITAL face parte din criteriile de selecție. Cerințele de securitate pentru achiziția produselor și serviciilor TIC se stabilesc înaintea achiziției, pe baza evaluării riscurilor (REQ-7.14.1-02X, REQ-7.14-04X, REQ-7.14.2-02X, REQ-7.14.3-08X).
– **Cerințele contractuale**: contractele și, unde este cazul, acordurile de nivel de serviciu cu furnizorii direcți cuprind, după caz: a) cerințele de securitate cibernetică, inclusiv pentru achiziția serviciilor și produselor TIC; b) cerințele privind instruirea, competențele și, unde este cazul, certificările personalului furnizorului; c) verificarea antecedentelor personalului furnizorului care are acces la sisteme sau la informații; d) obligația de a notifica CERTDIGITAL fără întârziere, în cel mult 24 de ore, incidentele care prezintă un risc pentru securitatea rețelelor și a sistemelor CERTDIGITAL, precum și canalul de raportare al CERTDIGITAL; e) dreptul de audit sau dreptul de a primi rapoartele de audit; f) obligația de a trata vulnerabilitățile care prezintă un risc pentru securitatea CERTDIGITAL; g) subcontractarea numai cu acordul CERTDIGITAL, cu transmiterea acelorași cerințe de securitate subcontractanților; h) obligațiile la încetarea contractului, inclusiv returnarea sau distrugerea informațiilor obținute, cu proces-verbal; i) răspunderea furnizorului și obligația lui de a aplica controalele cerute de CERTDIGITAL; j) pentru produse: informațiile despre componentele software folosite, despre funcțiile de securitate implementate și despre configurația necesară funcționării în siguranță, precum și obligația furnizorului de a aplica practici de securitate adecvate față de propriii furnizori. Furnizorii care au acces la sisteme respectă planul de securitate și procedura de acces al terților (PO_SI_50); accesul în zonele de securitate se face numai însoțit, conform secțiunii 2.3 din Politica de securitate fizică și de mediu (REQ-7.14.2-03X – REQ-7.14.2-06X, REQ-7.14.3-02X, REQ-7.14.3-04X, REQ-7.14.3-07X, REQ-7.14.3-09X).
– **Recepția, validarea și ciclul de viață**: componentele critice pentru funcționarea serviciilor (modulele criptografice, serverele platformei, echipamentele de rețea și de securitate, aplicațiile serviciilor) se identifică în inventarul activelor și în fișa serviciilor din Anexa 6 la PCA. Echipamentele critice se achiziționează direct de la producător sau de la distribuitori autorizați; la recepție se verifică ambalajul și sigiliile, numerele de serie și versiunea de

firmware sau suma de control a software-ului, cu proces-verbal, iar pentru modulele criptografice seria, firmware-ul și modul de operare se consemnează și la fiecare ceremonie (Procedura privind generarea cheilor, cap. 4 și anexa B). Programele și bibliotecile se obțin din surse verificate, cu verificarea semnăturii sau a sumei de control, iar lista componentelor software se ține pentru fiecare aplicație. Înainte de punerea în producție, produsele se testează în mediul de test pentru funcționarea conform specificației și pentru absența funcțiilor neașteptate sau nedorite; conformitatea cu cerințele de securitate se validează prin verificarea certificărilor, prin scanări de vulnerabilități și prin teste de penetrare. Pentru fiecare componentă se urmăresc versiunea, suportul producătorului și data sfârșitului suportului; înlocuirea se planifică înaintea sfârșitului suportului, iar riscurile componentelor învechite se tratează în GR-TSP (REQ-7.14.2-07X – REQ-7.14.2-11X, REQ-7.14.2-13X).

– **Monitorizarea și revizuirea**: furnizorii critici se evaluează cel puțin anual și după orice incident legat de produsele sau serviciile lor: rapoartele privind nivelul de serviciu, incidentele și vulnerabilitățile raportate, modificările practicilor lor de securitate cibernetică și ale produselor sau serviciilor livrate. Ofițerul de securitate IT stabilește nevoia unei evaluări neprogramate, iar constatările se consemnează. Riscurile rezultate din modificări se analizează și, unde este cazul, se iau fără întârziere măsuri de atenuare. Politica se revizuiește cel puțin anual, după incidente semnificative legate de furnizori și la modificări semnificative ale operațiunilor sau ale riscurilor (REQ-7.14.2-14X, REQ-7.14.3-10X).
– **Registrul furnizorilor**: ofițerul de securitate IT ține registrul furnizorilor direcți și al contractelor lor, cu: datele de contact ale fiecărui furnizor; produsele, serviciile și procesele TIC furnizate; contractul și clauzele de securitate; locul în care furnizorul prelucrează, gestionează sau arhivează informații ale CERTDIGITAL; încadrarea ca furnizor critic. Registrul se revizuiește și se validează cel puțin anual, pentru a verifica valabilitatea și adecvarea contractelor și existența clauzelor de securitate (REQ-7.14.3-11X, REQ-7.14.3-12X).
– **Schimbul de informații**: informațiile despre problemele, vulnerabilitățile și compromiterile din lanțul de aprovizionare se schimbă cu furnizorii numai pe canalele stabilite prin contract, cu respectarea clasificării informațiilor (Politicile generale, secțiunea 4.2); ofițerul de securitate IT este punctul de contact al CERTDIGITAL (REQ-7.14.2-12X).
– **Serviciile cloud**: componentele serviciilor, datele lor și copiile de siguranță se găzduiesc numai în centrele de date proprii ale CERTDIGITAL. Serviciile cloud ale terților se folosesc numai pentru activități-suport (de exemplu, e-mailul domeniului principal), după evaluarea riscurilor și cu aprobarea ofițerului de securitate IT, cu împărțirea responsabilităților de securitate stabilită prin contract și fără date restricționate ale serviciilor de încredere. Regula este publică prin prezentul document (REQ-7.14.2-15X).

– **Componentele furnizate de alte părți și responsabilitatea**: când serviciile folosesc o componentă de serviciu de încredere furnizată de o altă parte, CERTDIGITAL folosește interfața componentei conform cerințelor furnizorului ei și verifică faptul că securitatea și funcționalitatea componentei corespund politicii și practicilor serviciilor. CERTDIGITAL rămâne responsabil, în ansamblu, de conformitatea cu prezenta politică, cu politica de securitate a informației și cu politica serviciilor (REQ-7.14.3-01X, REQ-7.14.3-05X, REQ-7.14.3-06X).

– **Începerea și încetarea utilizării**: la începerea utilizării unui produs sau serviciu al unui furnizor se fac evaluarea, contractul, recepția și testarea, înscrierea în registru și acordarea accesului (PO_SI_50); la încetare se revocă accesul furnizorului, furnizorul returnează sau distruge informațiile CERTDIGITAL, cu proces-verbal, suporturile scoase din uz se șterg securizat, iar registrul se actualizează (REQ-7.14.3-03X).

18.6. Verificarea configurației

Configurația sistemelor serviciilor se verifică față de configurația de referință aprobată, automat, cel puțin o dată la 24 de ore, și manual, cel puțin o dată pe lună; intervalul maxim între două verificări este de 24 de ore, respectiv de o lună. Verificarea manuală cuprinde și setările de securitate, robustețea parolelor și activitățile efectuate cu conturile privilegiate, iar abaterile se tratează ca incidente de securitate (ETSI EN 319 401, REQ-6.3-08X, REQ-6.3-09X, REQ-7.7-10X).

19. Obligațiile părților și ale organizațiilor externe

– **expeditorul**: furnizează date corecte despre sine și despre destinatari, păstrează mijloacele de autentificare sub control exclusiv și răspunde pentru conținutul trimis;

– **destinatarul**: își menține datele de contact actuale și își verifică periodic căsuța sau contul;

– **delegații**: acționează numai în limitele împuternicirii;

– **organizațiile externe** care susțin prestarea serviciilor: au obligațiile din tabelul de mai jos (EN 319 521, cl. 4.1.1-05);

– **părțile care se bazează**: verifică sigiliul și marca temporală ale dovezilor și statutul calificat din Lista de încredere (EN 319 521, cl. 4.1.1-09).

Organizația externă	Obligațiile
Furnizorul platformei QREM/QeRDS și al conectorului AS4, înscris în registrul furnizorilor critici	livrează actualizările de securitate și suportul în termenele din contract; accesează sistemul numai conform procedurii de acces al terților; nu are acces la conținutul trimiterilor
Furnizorul de SMS, înscris în registrul furnizorilor critici	transmite notificările către destinatarii fără cont; mesajul conține numai notificarea și legătura de înregistrare, fără conținutul trimiterii; prelucrează datele numai în Spațiul Economic European, ca persoană împuternicită a CERTDIGITAL, cu obligații de confidențialitate
Furnizorii de internet (RCS & RDS și Orange Romania Communications)	asigură conectivitatea redundantă a centrelor de date, conform contractelor de nivel de serviciu
Producătorul modulelor criptografice (Thales)	furnizează firmware-ul, suportul și menținerea certificărilor modulelor
Platforma națională de interoperabilitate, Oficiul Național al Registrului Comerțului, schemele eID notificate și furnizorii portofelelor europene pentru identitatea digitală	sunt surse folosite la verificarea identității, în condițiile proprii
Prestatorii calificați parteneri, la interoperabilitate	aplică propriile politici și declarații de practici, conforme art. 44 din Regulamentul eIDAS și anexei I la RE 2025/1944, și acordul de interoperabilitate

Obligațiile de securitate și confidențialitate se înscriu în contracte; furnizorii critici se evaluează cel puțin anual. CERTDIGITAL rămâne responsabil, în ansamblu, de prestarea serviciilor.

20. Aspecte juridice și comerciale

Tarifele, răspunderea, asigurarea, protecția datelor cu caracter personal, modificările, soluționarea litigiilor și legea aplicabilă sunt cele din capitolele 7 și 8 și din termenii și condițiile serviciilor (TC-QERDS). Pe scurt: CERTDIGITAL răspunde conform art. 13 din Regulamentul eIDAS; are câte o poliță distinctă pentru fiecare serviciu, cu limita răspunderii de 500.000 EUR pe perioada asigurată și cu ADR ca asigurat adițional; este persoană împuternicită pentru conținutul trimiterilor și operator pentru datele de identificare, dovezi și jurnale.

Anexa A – Corespondența cu ETSI EN 319 521 (adaptat prin RE 2025/1944) și EN 319 531

Cerință	Conținut	Secțiune
EN 319 521, cl. 4.1.1-02, -03	publicarea declarației și a specificației dovezilor	6.1, 10
EN 319 521, cl. 4.1.1-04	revizuire; responsabilitățile; notificarea modificărilor	1.5, 8.3
EN 319 521, cl. 4.1.1-05, -09	obligațiile organizațiilor externe și ale părților	19
EN 319 521, cl. 4.1.1-06	semnalarea modificărilor conținutului	12.8
EN 319 521, cl. 4.1.1-07	identificarea și autentificarea	11
EN 319 521, cl. 4.1.1-08	protecția împotriva pierderii, furtului, deteriorării, modificării	14.1
EN 319 521, cl. 4.1.1-10, -11, -12	evenimentele cu dovadă; obținerea dovezilor; limitele de valabilitate	10, 13; SPEC-DOVEZI-QERDS
EN 319 521, cl. 4.1.2-01…05	serviciu calificat; prestatorii implicați; limitele; păstrarea, reversibilitatea; încetarea	1.1, 1.3, 1.4, 6.11, 6.16, 16, 18
EN 319 521, cl. 4.2-02, -03	definiția „livrat”; disponibilitatea datelor	12.4, 12.6
EN 319 521, cl. 4.2-04, -05, -07	comunicarea termenilor și condițiilor înainte de contract, pe suport durabil; dovada acceptării	6.2, 16
EN 319 521, cl. 5.1	integritate, confidențialitate; sigiliu pe certificat NCP/calificat	14.1
QERDS-5.2.1.1-01 / -01A	verificarea identității destinatarului („foarte ridicat”) și a expeditorului	11.1
QERDS-5.2.1.2-01…04	predarea după identificare; validarea; mediu controlat; dovezile identificării	11.3, 11.4, 12.5
QERDS-5.2.2-03 / -03A / -04	autentificarea expeditorului și a destinatarului	11.2
EN 319 521, cl. 5.3.1, 5.3.2	referința de timp (UTC); mărci temporale calificate	15
ERDS-5.4.1-01…08	dovezi obligatorii; arhivă; semantica EN 319 522-2	13, 16
EN 319 521, cl. 5.5	interoperabilitate	17
EN 319 521, REQ-QERDSP-7.2.2-01, -02	operatorul de înregistrare și responsabilul cu verificarea identității, numiți prin decizie a Directorului General	6.13
RE 2025/1944, anexa I: 7.2.1, 7.5, 7.8, 7.12, 7.14	instruire la 12 luni; chei în dispozitive certificate; TLS, scanări, pentest, firewall; încetare; lanțul de aprovizionare	14.2, 14.3, 18
EN 319 521, REQ-ERDSP-7.8-05, 7.10-03, 7.11-07, 7.11-09	certificatele de autentificare a site-ului web pentru TLS; evenimentele de securitate jurnalizate; compromiterea cheilor de sigiliu ale serviciilor: tratarea ca dezastru, notificarea părților, valabilitatea dovezilor	14.3, 6.12, 14.2
RE 2025/1944, anexa II	AS4; dovezi și identificare; capabilități și încredere	17
EN 319 531, REQ-REMS-4.1.1-02…14, cl. 4.4, 4.5, 5.5	particularitățile QREM: identificare, canale și clienți de e-mail, MIME, „store and forward” / „store and notify” (inclusiv pentru mesajele primite de la alt prestator), transmiterea către și de la alți prestatori REM și ERDS, interpretarea și accesul la dovezi	11, 12.5, 12.9, 13; SPEC-DOVEZI-QERDS