

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

Cuprins

PARTEA I – Politica serviciului 7
1. Introducere 7
1.1. Prezentare generală 7
1.2. Identificarea documentului și a politicii 8
1.3. Participanții și prestatorii implicați 8
1.4. Utilizarea serviciilor și limitele de utilizare 9
1.5. Administrarea documentului 9
2. Referințe normative 11
2.1. Acte normative și standarde 11
3. Definiții și acronime 12
3.1. Definiții 12
3.2. Acronime 12
4. Concepte generale 14
4.1. Serviciile și componentele lor 14
4.2. Cele două profiluri 14
4.3. Identitatea serviciilor și sigiliile serviciilor 14
5. Politica serviciilor 16
5.1. Identificare și conformitate 16
5.2. Comunitatea utilizatorilor și aplicabilitatea 16
5.3. Modificarea politicii 16
6. Cerințele privind practicile 17
6.1. Publicare și depozit 17
6.2. Termeni și condiții 17
6.3. Identificarea expeditorului 17
6.4. Identificarea destinatarului înainte de livrare 17
6.5. Securizarea trimiterii și primirii 18
6.6. Dovezile 18
6.7. Data și ora trimiterii și primirii 19
6.8. Modificările necesare transmiterii 19
6.9. Protecția datelor transmise 19

6.10. Interoperabilitatea și transmiterea între prestatori 19
6.11. Păstrarea datelor, a dovezilor și a jurnalelor 20
6.12. Timpul de încredere și jurnalele 20
6.13. Personalul 20
6.14. Controale privind facilitățile, managementul și operarea 20
6.15. Controale criptografice și de rețea 20
6.16. Notificări către ADR și încetarea serviciilor 21
6.17. Evaluarea conformității 21
7. Obligații și răspundere 22
7.1. Obligațiile CERTDIGITAL 22
7.2. Obligațiile expeditorului, ale destinatarului și ale abonatului 22
7.3. Obligațiile părților care se bazează 22
7.4. Răspunderea 22
7.5. Asigurarea 23
8. Alte aspecte comerciale și juridice 24
8.1. Tarife 24
8.2. Protecția datelor cu caracter personal 24
8.3. Modificări 24
8.4. Soluționarea litigiilor 24
8.5. Legea aplicabilă și cadrul legal 24
8.6. Alte prevederi 25
9. Corespondența cu cerințele art. 44 și ale Regulamentului (UE) 2025/1944 26
9.1. Tabel de corespondență 26
PARTEA A II-A – Declarația de practici 27
10. Publicare și depozit 27
11. Identificare și autentificare 28
11.1. Înregistrarea utilizatorilor 28
11.2. Autentificarea la fiecare utilizare 28
11.3. Destinatarii fără cont 28
11.4. Păstrarea dovezilor identificării 29
12. Ciclul de viață al trimiterii 30
12.1. Depunerea 30
12.2. Transmiterea 30

12.3. Notificarea destinatarului 30
12.4. Punerea la dispoziție („livrat”) 30
12.5. Predarea și acceptarea 30
12.6. Disponibilitatea conținutului 31
12.7. Sistemele necalificate 31
12.8. Modificările necesare transmiterii 31
12.9. Particularitățile QREM (ETSI EN 319 531) 31
12.10. Particularitățile QeRDS (ETSI EN 319 522) 31
13. Dovezile 33
13.1. Evenimentele și dovezile emise 33
13.2. Conținutul dovezilor 33
13.3. Formatul și sigilarea 33
13.4. Obținerea și verificarea dovezilor 33
13.5. Limitele de valabilitate a dovezilor 33
14. Protecția datelor transmise și controale tehnice 34
14.1. Integritate și confidențialitate 34
14.2. Cheile serviciilor 34
14.3. Rețea și vulnerabilități 34
15. Timpul 35
16. Păstrarea, reversibilitatea și portabilitatea 36
17. Interoperabilitatea 37
18. Controale de management și operare 38
19. Obligațiile părților și ale organizațiilor externe 39
20. Aspecte juridice și comerciale 40
Anexa A – Corespondența cu ETSI EN 319 521 (adaptat prin RE 2025/1944) și EN 319 531 41

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, v2.0).

Ambele servicii sunt **servicii de încredere calificate** în sensul Regulamentului (UE) nr. 910/2014, prestate de un prestator calificat și înscrise în Lista de încredere a României (ETSI EN 319 521, cl. 4.1.2-01).

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	1.0 (22.10.2026)
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 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** (EN 319 521, cl. 4.1.2-02): CERTDIGITAL, pentru mărcile temporale calificate (CERTDIGITAL TSA) și pentru certificatele calificate de sigiliu ale serviciilor (CERTDIGITAL QCA G5); alți prestatori calificați numai în cadrul interoperabilității (secțiunea 17);

– **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.

CERTDIGITAL nu deleagă către terți operarea serviciilor, verificarea identității sau gestionarea cheilor serviciilor.

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; 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 identifică serviciul în Lista de încredere a României 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). Serviciile sunt prestate ca servicii calificate, înscrise în Lista de încredere a României (art. 21 din Regulamentul eIDAS).

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 certificatele de sigiliu ale serviciilor sunt publicate la https://www.certdigital.ro/repository/, 24/7, public și fără restricții de acces.

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.

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 / -04); 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); predarea conținutului sau eșecul ei (E.1 / E.2); pentru QREM, și notificarea destinatarului (C.1 / C.2), iar la stilul „store and notify”, acceptarea, refuzul sau expirarea termenului de acceptare; 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).

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 timp de 90 de zile de la punerea la dispoziție, după care se șterge;

– 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);

– dovezile și arhiva se păstrează cel puțin 10 ani de la emitere, iar jurnalele cel puțin 10 ani (peste minimul de 2 ani din EN 319 521, cl. 7.10-04); acestea se protejează împotriva modificării și se pot obține de expeditor și de destinatar pe toată această perioadă.

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.

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.

6.14. Controale privind facilitățile, managementul și operarea

Se aplică Politicile generale CertDigital (v2.0), 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 și jurnalele se transferă unui alt prestator calificat acceptat de ADR, iar abonații primesc exportul dovezilor lor.

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). CERTDIGITAL nu folosește persoane împuternicite pentru operarea serviciilor. 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/ce-este-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, specificația dovezilor, lista codurilor de respingere 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”.

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, plus un factor suplimentar (cheie de acces)
Destinatar	autentificare cu mai mulți factori, portofelul european sau mijloc eID, semnătură sau sigiliu calificat (QERDS-5.2.2-03A / -04)
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, se emite dovada de neridicare.

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: cod malițios (RA03), încălcarea politicii, de exemplu dimensiunea (RA05), destinatar inexistent, expeditor neautorizat.

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); pentru QREM se emit dovezile de notificare sau de eșec al notificării (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, iar acceptarea, refuzul sau expirarea termenului se consemnează prin dovezile corespunzătoare;

– 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 cel puțin 90 de zile de la punerea la dispoziție, după care se șterge; dovezile și amprentele conținutului se păstrează conform secțiunii 16. Termenul este cuprins în termenii și condițiile serviciului (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.

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	da	da
B.1 / B.2 / B.3	acceptarea / refuzul / eșecul transmiterii către alt prestator	da, la interoperabilitate	da, la transmiterea între prestatori REM
C.1 / C.2	notificarea destinatarului / eșecul notificării	opțional	da
C.3 / C.4 / C.5	acceptarea / refuzul / expirarea termenului de acceptare	la modul cu acceptare	la stilul „store and notify”
D.1 / D.2	punerea la dispoziție / eșecul ei	da	da
E.1 / E.2	predarea / eșecul predării	da	da
F.1 / F.2 / F.3	transmiterea către un sistem necalificat / eșecul ei / primirea de la un sistem necalificat	da	da

Dovezile sunt obligatorii pentru evenimentele de mai sus (RE 2025/1944, anexa I: ERDS-5.4.1-06…08). E.1 și D.6 (urmărirea accesului la conținut) nu se folosesc împreună.

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.

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, folosind Lista de încredere a României (EN 319 521, cl. 4.1.1-10 și -11).

13.5. Limitele de valabilitate a dovezilor

Dovezile rămân verificabile după expirarea certificatului de sigiliu datorită mărcii temporale calificate. Pentru păstrarea pe termen lung, la cerere sau după perioada standard, dovezile se pot încredința serviciului calificat de păstrare CERTDIGITAL (PSPPS), care le menține verificabile prin augmentare (EN 319 521, cl. 4.1.1-12).

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.

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.

15. Timpul

Data și ora trimiterii, primirii și ale oricărei modificări se indică prin mărci temporale calificate emise de CERTDIGITAL TSA, legate de conținutul sau de dovada respectivă (art. 44 alin. (1) lit. (f); EN 319 521, cl. 5.3.2). Serverele serviciilor sunt sincronizate cu sursa de timp a CERTDIGITAL (00u), legată de UTC.

16. Păstrarea, reversibilitatea și portabilitatea

Ce se păstrează	Cât	Observații
Conținutul trimiterilor	până la expirarea disponibilității (secțiunea 12.6)	apoi se șterge, cu jurnalizarea ștergerii
Dovezile și amprentele conținutului	cel puțin 10 ani	protejate împotriva modificării; obtenabile de părți
Datele de identificare și de autentificare	cel puțin 10 ani de la închiderea contului	EN 319 521, cl. 5.4.1-03, 5.4.2
Jurnalele serviciilor	cel puțin 10 ani	peste minimul de 2 ani din EN 319 521, cl. 7.10-04

Abonatul poate obține oricând exportul dovezilor și al trimiterilor încă disponibile, în format XML și PDF; la încheierea contractului, exportul se furnizează înainte de închiderea contului (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 (v2.0) 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 în patru factori (cheie, cartelă, cod și amprentă) 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 și supuși unor obligații contractuale de securitate;

– **încetarea**: conform planului 00r (RE 2025/2530): trimiterile în curs se finalizează sau se returnează cu dovezi, dovezile și jurnalele se transferă unui prestator calificat acceptat de ADR, iar abonații primesc exportul (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.

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** (furnizori, prestatori parteneri): respectă obligațiile de securitate și confidențialitate din contracte (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).

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	10
EN 319 521, cl. 4.1.1-04	revizuire; notificarea modificărilor	1.5
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	13
EN 319 521, cl. 4.1.2-01…05	serviciu calificat; prestatorii implicați; limitele; păstrarea, reversibilitatea; încetarea	1.1, 1.3, 1.4, 16, 18
EN 319 521, cl. 4.2-02, -03	definiția „livrat”; disponibilitatea datelor	12.4, 12.6
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. 5.3.2	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
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
RE 2025/1944, anexa II	AS4; dovezi și identificare; capabilități și încredere	17
EN 319 531, cl. 4.1.1, 4.4, 4.5, 5.5	particularitățile QREM: canale, MIME, „store and forward” / „store and notify”, transmitere numai între prestatori calificați	12.5, 12.9