

Specificația dovezilor și codurile de respingere – QeRDS și QREM

CertDigital

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: evenimentele și dovezile, componentele și interpretarea lor, formatul și sigilarea, codurile de motiv și de respingere, obținerea, verificarea și păstrarea dovezilor	02/11/2026

Cuprins

1. Scop și domeniu 6
1.1. Prezentare generală 6
1.2. Identificarea documentului 6
1.3. Administrarea documentului 7
2. Referințe 8
2.1. Acte normative și standarde 8
2.2. Termeni 8
3. Tipurile de evenimente și dovezile emise 10
3.1. Regulile generale 10
3.2. Depunerea (A) 10
3.3. Transmiterea între prestatori (B) 11
3.4. Acceptarea sau refuzul de către destinatar (C) 11
3.5. Punerea la dispoziție (D) 12
3.6. Predarea (E) 12
3.7. Sistemele necalificate (F) 13
4. Structura și conținutul unei dovezi 14
4.1. Principiul 14
4.2. Componentele și interpretarea lor 14
4.3. Exemplu de citire 15
5. Formatul și sigilarea 16
5.1. Dovezile XML 16
5.2. Dovezile QREM în mesajele de e-mail 16
5.3. Varianta PDF 17
5.4. Dovezile QeRDS la interoperabilitate 17
6. Codurile de motiv, de respingere și de eroare 18
6.1. Regulile 18
6.2. Depunerea (A.1, A.2) 18
6.3. Transmiterea între prestatori (B.1, B.2, B.3) 18
6.4. Acceptarea sau refuzul de către destinatar (C.1–C.5) 19

6.5. Punerea la dispoziție (D.1–D.4) 19
6.6. Predarea (E.1, E.2) 20
6.7. Sistemele necalificate (F.1, F.2, F.3) 20
7. Obținerea și verificarea dovezilor 21
7.1. Obținerea dovezilor 21
7.2. Verificarea dovezilor 21
7.3. Augmentarea și păstrarea pe termen lung 22
8. Păstrarea și limitele de valabilitate 23
8.1. Păstrarea 23
8.2. Limitele de valabilitate a dovezilor 23

1. Scop și domeniu

1.1. Prezentare generală

Prezentul document este specificația publică a dovezilor emise de CENTRUL DE CALCUL S.A. (marca CertDigital, denumită în continuare „CERTDIGITAL”), prestator de servicii de încredere calificat, prin **serviciile calificate de transmitere electronică înregistrată**:

– **QeRDS** — serviciul calificat de transmitere electronică înregistrată prin portal, interfețe de programare și conectori AS4 (tipul `EDS/Q`);

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

Documentul stabilește, pentru fiecare dovadă: evenimentul care o declanșează, momentul emiterii, emitentul și destinatarul dovezii, componentele ei și modul în care se interpretează fiecare componentă, formatul și sigilarea, precum și codurile de motiv, inclusiv codurile de respingere și de eroare. Documentul completează Politica și declarația de practici a serviciilor calificate de transmitere electronică înregistrată (PDP-QERDS), capitolul 13, și Termenii și condițiile serviciilor, secțiunea 2.6, și îndeplinește cerințele privind informațiile despre dovezi (ETSI EN 319 521, cl. 4.1.1-10 și -11; ETSI EN 319 531, REQ-REMS-4.1.1-13 și -14). În caz de neconcordanță, prevalează PDP-QERDS. Documentul se adresează expeditorilor, destinatarilor și abonaților, părților care se bazează pe dovezi și prestatorilor calificați parteneri.

1.2. Identificarea documentului

Element	Valoare
Titlu	Specificația dovezilor și codurile de respingere – serviciile calificate de transmitere electronică înregistrată (QeRDS) și de e-mail înregistrat (QREM) (SPEC-DOVEZI-QERDS)
Versiune	1.0 (02.11.2026)
Documentul de bază	PDP-QERDS, identificatorul politicii (OID) 1.3.6.1.4.1.47898.14.1
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)
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)
Sigiliile serviciilor	CERTDIGITAL QERDS SERVICE G5, pentru dovezile QeRDS, și CERTDIGITAL QREM SERVICE G5, pentru dovezile QREM, emise de CERTDIGITAL QCA G5
Natura documentului	document public; se aplică împreună cu PDP-QERDS și cu Termenii și condițiile serviciilor
Publicat la	https://www.certdigital.ro/repository/politici/certdigital_spec-dovezi-qerds_ro.pdf; versiunile anterioare: https://www.certdigital.ro/repository/arhiva/

1.3. Administrarea documentului

Compartimentul Servicii Electronice răspunde de menținerea documentului și pregătește reviziile; documentul este verificat de ofițerul de securitate IT și aprobat de Directorul General. Documentul se revizuiește odată cu PDP-QERDS și la orice modificare a dovezilor, a formatelor sau a codurilor folosite. Modificările se publică în depozitul de documente cu cel puțin 30 de zile înainte de aplicare, iar versiunile anterioare rămân în arhiva depozitului (PDP-QERDS, secțiunea 8.3). O dovadă se interpretează conform versiunii prezentului document în vigoare la data emiterii ei. Documentul este redactat în limba română; în caz de neconcordanță cu o traducere, prevalează versiunea în limba română.

2. Referințe

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. 43 și 44;

– Regulamentul de punere în aplicare (UE) 2025/1944: anexa I (ETSI EN 319 521 V1.1.1, cu adaptările din anexă, inclusiv dovezile obligatorii ERDS-5.4.1-06…08) și anexa II (interoperabilitatea);

– ETSI EN 319 521 V1.1.1 (cerințe de politică și securitate pentru prestatorii de servicii de transmitere electronică înregistrată) și ETSI EN 319 531 V1.1.1 (cerințe de politică și securitate pentru prestatorii de servicii de e-mail înregistrat);

– ETSI EN 319 522-1 V1.2.1 (cadrul și arhitectura; clauza 6, evenimentele și setul de dovezi), ETSI EN 319 522-2 V1.2.1 (conținutul semantic; clauza 8, componentele dovezilor și valorile lor) și ETSI EN 319 522-3 V1.2.1 (formatele; clauza 5, formatul XML al dovezilor);

– ETSI EN 319 522-4-1 V1.2.1 (legătura AS4), EN 319 522-4-2 V1.1.1 (dovezi și identificare) și EN 319 522-4-3 V1.1.1 (capabilități și încredere), pentru interoperabilitatea QeRDS;

– ETSI EN 319 532-1 V1.1.1 (cadrul REM; clauza 6, evenimentele și dovezile REM), EN 319 532-2 V1.1.1 (conținutul semantic REM), EN 319 532-3 V1.3.1 (formatele REM: mesajul S/MIME și părțile MIME ale dovezilor) și EN 319 532-4 V1.3.1 (profilurile de interoperabilitate, inclusiv profilul de bază REM și tabelul C.28 al codurilor de motiv);

– ETSI EN 319 132-1 (XAdES), ETSI EN 319 122-1 (CAdES) și ETSI EN 319 142-1 (PAdES), pentru sigiliile dovezilor; ETSI EN 319 102-1, pentru validarea lor;

– documentul „Agreed Cryptographic Mechanisms” al ECCG, publicat de ENISA.

2.2. Termeni

Termen	Semnificație
dovadă	înregistrarea sigilată de CERTDIGITAL și marcată temporal calificat, care atestă producerea unui eveniment din ciclul de viață al trimiterii („ERDS evidence”, ETSI EN 319 522-1)
eveniment	faptul din ciclul de viață al trimiterii care declanșează emiterea unei dovezi; evenimentele au codurile A.1…F.3 din ETSI EN 319 522-1, tabelul 1
cod de motiv	identificatorul standardizat al cauzei evenimentului (componenta G04, ETSI EN 319 522-2, cl. 8.3.3); la evenimentele negative, el este codul de respingere sau de eroare
serviciul expeditorului / serviciul destinatarului	serviciul la care este înregistrat expeditorul, respectiv destinatarul (S-ERDS / R-ERDS); când ambele părți sunt utilizatori CERTDIGITAL, CERTDIGITAL are ambele roluri
prestatorul anterior / următor	la interoperabilitate, prestatorul de la care CERTDIGITAL primește trimiterea, respectiv cel căruia i-o transmite

Termen	**Semnificație**
„livrat”	punerea la dispoziție a conținutului în căsuța sau în contul destinatarului identificat (dovada D.1; PDP-QERDS, secțiunea 12.4)
termen de acceptare	perioada stabilită de expeditor, implicit 15 zile, cel mult 30 de zile, în care destinatarul fără cont se poate înregistra și în care destinatarul poate accepta sau refuza trimiterea, când acceptarea este cerută
perioada de disponibilitate	90 de zile calendaristice de la punerea la dispoziție (D.1), după care conținutul se șterge

3. Tipurile de evenimente și dovezile emise

3.1. Regulile generale

– CERTDIGITAL emite automat o dovadă pentru fiecare eveniment din tabelele de mai jos, pentru fiecare trimitere și, dacă trimiterea are mai mulți destinatari, separat pentru fiecare destinatar (componenta I09); dovezile sunt obligatorii pentru toate evenimentele enumerate (RE 2025/1944, anexa I: ERDS-5.4.1-06…08), inclusiv pentru cele pe care ETSI EN 319 522-1 le lasă facultative;

– emitentul dovezii este CERTDIGITAL, ca serviciu al expeditorului, ca serviciu al destinatarului sau ca prestator care transmite ori primește trimiterea la interoperabilitate; dovezile emise de prestatorii parteneri și primite de CERTDIGITAL se pun, nemodificate, la dispoziția expeditorului;

– fiecare dovadă se sigilează separat și se marchează temporal calificat (capitolul 5); data și ora evenimentului se exprimă în UTC;

– dovezile se pun la dispoziția persoanei indicate în coloana „Cine primește dovada”; toate dovezile unei trimiteri se pot descărca din cont de expeditor și, pentru evenimentele care îl privesc, de destinatar, pe toată durata de păstrare (capitolul 7);

– livrarea se dovedește prin D.1, iar preluarea efectivă a conținutului prin E.1; CERTDIGITAL nu emite dovezile C.6 (NotificationDelivered), D.5 (NotificationAccessTracking) și D.6 (ContentAccessTracking);

– identificatorul evenimentului din dovadă (componenta G03) este URI-ul format din prefixul de la secțiunea 5.1 și denumirea evenimentului din tabelele de mai jos (ETSI EN 319 522-3, tabelul 2).

3.2. Depunerea (A)

Se aplică ambelor servicii.

Cod și dovadă (EN 319 522-1)	Când se emite	Cine primește dovada
A.1 SubmissionAcceptance – acceptarea depunerii	imediat după ce serviciul a verificat identitatea și drepturile expeditorului, formatul și dimensiunea trimiterii, existența destinatarilor și absența codului malițios, iar trimiterea a primit identificatorul unic și a fost sigilată și marcată temporal; din acest moment, CERTDIGITAL răspunde de transmiterea trimiterii către toți destinatarii	expeditorul
A.2 SubmissionRejection – respingerea depunerii	imediat după ce una dintre verificările de mai sus eșuează; dovada conține obligatoriu codul de respingere (secțiunea 6.2); trimiterea nu se transmite	expeditorul

3.3. Transmiterea între prestatori (B)

Se aplică numai la interoperabilitate: pentru QeRDS, prin conectorul AS4 (ETSI EN 319 522-4-1, -4-2 și -4-3); pentru QREM, între prestatori calificați de REM, conform profilului de bază REM (ETSI EN 319 532-4).

Cod și dovadă (EN 319 522-1)	Când se emite	Cine primește dovada
B.1 RelayAcceptance – acceptarea transmiterii	când prestatorul care primește trimiterea o acceptă; dovada este emisă de acesta (de CERTDIGITAL, când CERTDIGITAL primește trimiterea); de la acest moment, prestatorul care a acceptat trimiterea răspunde de ea	prestatorul anterior; CERTDIGITAL o pune și la dispoziția expeditorului său
B.2 RelayRejection – refuzul transmiterii	când prestatorul care primește trimiterea o refuză din motive de politică, de format sau tehnice; conține obligatoriu codul de motiv (secțiunea 6.3); răspunderea pentru trimitere rămâne la prestatorul care a transmis-o	prestatorul anterior; CERTDIGITAL o pune și la dispoziția expeditorului său
B.3 RelayFailure – eșecul transmiterii	emisă de CERTDIGITAL, ca prestator care transmite, când transmiterea eșuează sau când nu primește dovada B.1 ori B.2 în intervalul stabilit prin acordul de interoperabilitate	expeditorul sau, după caz, prestatorul anterior

3.4. Acceptarea sau refuzul de către destinatar (C)

Se aplică numai trimiterilor cu acceptare: stilul QREM „store and notify” și modul QeRDS cu acceptare. La mesajele QREM primite de la un prestator REM care operează el însuși stilul „store and notify”, CERTDIGITAL emite, ca serviciu al destinatarului, dovezile C.1 și C.2, iar dovezile C.3, C.4 și C.5 le emite prestatorul expeditorului (ETSI EN 319 532-1, cl. 6.2.3).

Cod și dovadă (EN 319 522-1)	Când se emite	Cine primește dovada
C.1 NotificationForAcceptance – notificarea pentru acceptare	când serviciul destinatarului a transmis destinatarului notificarea pentru acceptare, fără conținutul trimiterii, pe canalul indicat	expeditorul sau, după caz, prestatorul anterior
C.2 NotificationForAcceptanceFailure – eșecul notificării pentru acceptare	când notificarea pentru acceptare nu a putut fi transmisă destinatarului după epuizarea încercărilor	expeditorul sau, după caz, prestatorul anterior
C.3 ConsignmentAcceptance – acceptarea de către destinatar	când destinatarul, autentificat, acceptă trimiterea printr-o acțiune expresă; urmează punerea la dispoziție (D.1)	expeditorul și destinatarul
C.4 ConsignmentRejection – refuzul de către destinatar	când destinatarul, autentificat, refuză trimiterea printr-o acțiune expresă; conținutul nu i se predă și se șterge la expirarea termenului de acceptare	expeditorul și destinatarul
C.5 AcceptanceRejectionExpiry – expirarea termenului de acceptare	la expirarea termenului de acceptare, dacă destinatarul nu a acceptat și nici nu a refuzat trimiterea; conținutul nu mai poate fi preluat și se șterge la expirarea termenului	expeditorul

3.5. Punerea la dispoziție (D)

Se aplică ambelor servicii.

Cod și dovadă (EN 319 522-1)	Când se emite	Cine primește dovada
D.1 ContentConsignment – punerea la dispoziție („livrat”)	când conținutul este pus la dispoziție în căsuța sau în contul destinatarului identificat, astfel încât acesta îl poate prelua numai prin autentificare; la destinatarul fără cont, după înregistrarea și verificarea identității lui; la trimiterile cu acceptare, după acceptare (C.3); momentul D.1 este momentul livrării și începutul perioadei de disponibilitate	expeditorul sau, după caz, prestatorul anterior
D.2 ContentConsignmentFailure – eșecul punerii la dispoziție, inclusiv neridicarea	când conținutul nu a putut fi pus la dispoziție: destinatarul fără cont nu s-a înregistrat în termenul de acceptare („dovada de neridicare”), spațiul de stocare al destinatarului este depășit, tipul trimiterii nu este acceptat, a apărut o defecțiune tehnică ori, la transmiterea către alt prestator, acesta nu a confirmat punerea la dispoziție în intervalul stabilit prin acordul de interoperabilitate	expeditorul sau, după caz, prestatorul anterior
D.3 ConsignmentNotification – notificarea destinatarului	când destinatarul a fost notificat că o trimitere îi este pusă la dispoziție sau, la destinatarul fără cont, că o trimitere îl așteaptă și cum se înregistrează; notificarea se face pe canalul ales (e-mail, notificare în aplicație, iar la destinatarul fără cont, e-mail sau SMS) și nu conține conținutul trimiterii	expeditorul
D.4 ConsignmentNotificationFailure – eșecul notificării	când notificarea nu a putut fi transmisă destinatarului după epuizarea încercărilor	expeditorul

3.6. Predarea (E)

Se aplică ambelor servicii.

Cod și dovadă (EN 319 522-1)	Când se emite	Cine primește dovada
E.1 ContentHandover – predarea	când destinatarul sau delegatul lui, autentificat, preia efectiv conținutul: descărcare din interfața web sau prin interfața de programare; la QREM, numai prin interfața web	expeditorul și destinatarul
E.2 ContentHandoverFailure – eșecul predării	la ștergerea conținutului la sfârșitul perioadei de disponibilitate, dacă destinatarul nu l-a preluat, sau când predarea nu se poate face, de exemplu pentru că tipul trimiterii nu este acceptat de destinatar	expeditorul

3.7. Sistemele necalificate (F)

Se aplică ambelor servicii. Partea necalificată a transmiterii nu beneficiază de prezumțiile de la art. 43 alin. (2) din Regulamentul eIDAS.

Cod și dovadă (EN 319 522-1)	**Când se emite**	**Cine primește dovada**
F.1 RelayToNonERDS – transmiterea către un sistem necalificat	când serviciul a transmis trimiterea, la cererea expeditorului, către un sistem care nu este serviciu de transmitere electronică înregistrată, de exemplu o adresă de e-mail obișnuită	expeditorul
F.2 RelayToNonERDSFailure – eșecul transmiterii către un sistem necalificat	când sistemul extern nu este accesibil sau refuză mesajul	expeditorul
F.3 ReceivedFromNonERDS – primirea de la un sistem necalificat	când serviciul primește un mesaj de la un sistem necalificat, de exemplu un e-mail obișnuit trimis la adresa QREM a unui utilizator; mesajul se marchează ca necalificat	destinatarul

4. Structura și conținutul unei dovezi

4.1. Principiul

Fiecare dovadă cuprinde componentele semantice din ETSI EN 319 522-2, cl. 8.2 (pentru QREM, aplicate prin ETSI EN 319 532-2), codificate în elementele XML din ETSI EN 319 522-3, cl. 5.2.2. Componentele G01, G03, G05, R01, R02, R03, I02, I06, M01 și M02 sunt prezente în toate dovezile; celelalte apar atunci când evenimentul le cere. Textele libere din dovezi se scriu în limba engleză, conform ETSI EN 319 522-2, cl. 8.3.1, iar CERTDIGITAL adaugă traducerea lor în limba română. Dovezile CERTDIGITAL nu conțin extensii proprietare (componenta E01 nu se folosește).

4.2. Componentele și interpretarea lor

Tabelul de mai jos definește modul în care se interpretează fiecare componentă (ETSI EN 319 531, REQ-REMS-4.1.1-13).

Componenta (EN 319 522-2) și elementul XML (EN 319 522-3)	Ce conține în dovezile CERTDIGITAL	Cum se interpretează
G01 – identificatorul dovezii (EvidenceIdentifier)	un identificator unic, atribuit de serviciu fiecărei dovezi	identifică dovada în cererile de descărcare, de verificare sau în reclamații; două dovezi diferite nu au același identificator
G02 – versiunea dovezii (atributul version al elementului Evidence)	valoarea cerută de ETSI EN 319 522-3, cl. 5.2.2.3	arată după ce versiune a formatului se citește dovada
G03 – evenimentul (ERDSEventId)	URI-ul evenimentului (secțiunea 3.1)	arată ce eveniment atestă dovada; semnificația evenimentului este cea din capitolul 3
G04 – motivul (EventReasons)	codul de motiv, ca URI, cu detaliile textuale (capitolul 6)	la evenimentele negative (respingere, refuz, eșec, expirare) arată cauza; la evenimentele pozitive confirmă rezultatul
G05 – data și ora evenimentului (EventTime)	data și ora evenimentului, în UTC	momentul la care s-a produs evenimentul, înregistrat de serviciu cu o sursă de timp sincronizată cu UTC; marca temporală calificată a sigiliului atestă, în plus, că dovada exista la momentul indicat de ea
G06 – jurnalul tranzacției (TransactionLogInformation)	extrasul din jurnalul protocolului de transport (de exemplu tranzacția SMTP la QREM sau mesajul AS4 la QeRDS), atunci când există	detaliu tehnic de susținere; nu modifică semnificația dovezii
R01 – politica emitentului (EvidenceIssuerPolicyID)	identificatorul politicii PDP-QERDS și identificatorul profilului QREM sau QeRDS, sub formă de URN (RFC 3061; valorile de la secțiunea 1.2)	arată politica și profilul după care a fost emisă dovada
R02 – emitentul (EvidenceIssuerDetails)	denumirea CENTRUL DE CALCUL S.A., identificatorul acestuia și certificatul de sigiliu al serviciului	identifică prestatorul care răspunde de dovadă

Componenta (EN 319 522-2) și elementul XML (EN 319 522-3)	Ce conține în dovezile CERTDIGITAL	Cum se interpretează
R03 – sigiliul emitentului (ds:Signature)	sigiliul electronic calificat XAdES, încorporat în dovadă, cu marcă temporală calificată (capitolul 5)	garantează integritatea și originea dovezii; o dovadă al cărei sigiliu nu se validează nu poate fi invocată ca dovadă a serviciului
I01, I02 – expeditorul (SenderDetails)	atributele de identitate verificate (numele și prenumele sau denumirea, identificatorul persoanei) și identificatorul expeditorului în serviciu (contul sau adresa QREM)	persoana identificată care a trimis datele
I03, I04 – delegatul expeditorului (SenderDelegateDetails)	aceleași date pentru persoana care a trimis în numele expeditorului, atunci când este cazul	persoana care a acționat efectiv în numele expeditorului
I05, I06 – destinatarul (RecipientDetails)	identificatorul destinatarului indicat de expeditor și, după verificarea identității, atributele de identitate ale destinatarului	persoana căreia i se adresează datele; atributele de identitate apar în dovezile emise după identificarea destinatarului (D.1, E.1)
I07, I08 – delegatul destinatarului (RecipientsDelegateDetails)	aceleași date pentru delegatul care a primit în numele destinatarului	persoana care a preluat efectiv datele în numele destinatarului
I09 – destinatarul la care se referă dovada (EvidenceRefersToRecipient)	identificatorul unuia dintre destinatari, la trimiterile cu mai mulți destinatari	dovada privește numai acel destinatar
I10–I13 – nivelurile de asigurare a identității (în elementele de mai sus)	pentru fiecare persoană: nivelul verificării identității și nivelul autentificării, ca URI, identificatorul politicii de identificare (PDP-QERDS), metoda folosită și momentul autentificării	arată cât de sigur a fost identificată și autentificată persoana: expeditorul cu un nivel de încredere ridicat, destinatarul cu un nivel de încredere foarte ridicat (PDP-QERDS, secțiunile 6.3 și 6.4)
M01 – identificatorul trimiterii (MessageIdentifier)	identificatorul unic atribuit trimiterii la depunere	leagă între ele toate dovezile aceleiași trimiteri
M02 – informațiile despre conținut (UserContentInfo)	structura conținutului: numărul de părți, denumirea și tipul fiecărei părți și amprenta SHA-256 a fiecărei părți	permite verificarea faptului că un document prezentat ulterior este identic cu cel transmis (secțiunea 7.2, lit. e)
M03 – data și ora depunerii (SubmissionTime)	momentul, în UTC, în care expeditorul a inițiat depunerea	poate preceda momentul acceptării depunerii (A.1)
M04 – sistemul extern (ForwardedToExternalSystem)	descrierea sistemului necalificat implicat, de exemplu domeniul de e-mail	prezent numai la F.1–F.3, C.1 și C.2; arată partea necalificată a transmiterii
M05 – prestatorul partener (ExternalERDSDetails)	datele prestatorului calificat cu care s-a schimbat trimiterea	prezent numai la evenimentele care implică un alt prestator

4.3. Exemplu de citire

O dovadă cu evenimentul ContentConsignment (D.1), cu motivul MessageConsignedToRecipient (RD01) și cu data și ora 2026-12-01T09:15:00Z atestă că, la acea oră UTC, conținutul trimiterii identificate în M01, cu amprentele din M02, a fost pus la dispoziția destinatarului indicat în I09, identificat la nivelul arătat în I12. Trimiterea este „livrată” de la acel moment, iar perioada de disponibilitate de 90 de zile începe atunci. Dacă ulterior se emite dovada E.1, ea arată momentul la care destinatarul a preluat efectiv conținutul.

5. Formatul și sigilarea

5.1. Dovezile XML

– dovezile se emit în formatul XML din ETSI EN 319 522-3, cl. 5.2.2, cu elementul rădăcină `Evidence`, codificate UTF-8;

– fiecare dovadă se sigilează separat cu un sigiliu XAdES încorporat (elementul `ds:Signature`, ETSI EN 319 522-3, cl. 5.2.2.28), creat la nivelul XAdES-B-B și augmentat imediat la nivelul XAdES-B-T prin marca temporală calificată a sigiliului (proprietatea SignatureTimeStamp), emisă de serviciul calificat de marcare temporală CertDigital TSA (ETSI EN 319 132-1);

– dovezile QeRDS se sigilează cu certificatul calificat de sigiliu CERTDIGITAL QERDS SERVICE G5, iar dovezile QREM cu certificatul calificat de sigiliu CERTDIGITAL QREM SERVICE G5, ambele emise de CERTDIGITAL QCA G5, cu chei păstrate în module criptografice certificate (PDP-QERDS, secțiunea 14.2); algoritmii respectă documentul „Agreed Cryptographic Mechanisms” al ECCG.

Valorile fixe folosite în dovezi și adresele certificatelor de sigiliu sunt:

Element	Valoare
Spațiul de nume al dovezilor XML	http://uri.etsi.org/19522/v1#
Prefixul identificatorilor de eveniment (G03)	http://uri.etsi.org/19522/Event/
Prefixul identificatorilor de motiv (G04)	http://uri.etsi.org/19522/EventReason/
Algoritmul amprentei conținutului (M02)	SHA-256
Certificatul de sigiliu QeRDS	http://certs.certdigital.ro/certdigital_qerds_g5.crt
Certificatul de sigiliu QREM	http://certs.certdigital.ro/certdigital_qrem_g5.crt

5.2. Dovezile QREM în mesajele de e-mail

– mesajele REM emise de QREM respectă ETSI EN 319 532-3: fiecare mesaj este un mesaj S/MIME `multipart/signed`, sigilat de serviciu cu certificatul CERTDIGITAL QREM SERVICE G5, care conține adresa serviciului, office@rem.certdigital.ro;

– dovezile se atașează mesajului ca părți MIME separate: `application/xml`, pentru dovada XML sigilată conform secțiunii 5.1, și, la cerere, `application/pdf`, pentru varianta PDF de la secțiunea 5.3, cu antetele din ETSI EN 319 532-3, cl. 6.2.6;

– mesajul original al expeditorului se păstrează nemodificat, într-o parte MIME separată; modificările necesare transmiterii se indică în mesaj și în dovezi (PDP-QERDS, secțiunea 12.8);

– la interoperabilitatea cu alți prestatori REM se aplică profilul de bază REM din ETSI EN 319 532-4.

5.3. Varianta PDF

Pentru citirea de către persoane, fiecare dovadă se poate obține și ca fișier PDF, în limba română, care reproduce toate componentele dovezii XML și este sigilat PAdES-B-T cu același certificat de sigiliu și cu marcă temporală calificată (ETSI EN 319 142-1). Varianta PDF este destinată utilizării umane; pentru prelucrarea automată și pentru interoperabilitate se folosește dovada XML (ETSI EN 319 522-3, cl. 5.1). În caz de neconcordanță între cele două variante, prevalează dovada XML.

5.4. Dovezile QeRDS la interoperabilitate

Dovezile schimbate cu prestatorii calificați parteneri se transmit în format XML, prin legătura AS4, conform ETSI EN 319 522-4-1 și EN 319 522-4-2, iar încrederea în sigiliile prestatorilor parteneri se stabilește prin listele de încredere ale statelor membre (ETSI EN 319 522-4-3).

6. Codurile de motiv, de respingere și de eroare

6.1. Regulile

– codul de motiv se înscrie în componenta G04 ca URI, format din prefixul de la secțiunea 5.1 și denumirea din coloana întâi a tabelelor de mai jos; codul scurt (de exemplu RA05) servește numai ca referință;

– CERTDIGITAL înscrie codul de motiv în toate dovezile; la evenimentele negative (A.2, B.2, B.3, C.2, C.4, C.5, D.2, D.4, E.2 și F.2), codul este obligatoriu și reprezintă codul de respingere sau de eroare;

– detaliile textuale ale motivului se scriu în limba engleză, însoțite de traducerea în limba română, și indică, după caz, regula încălcată sau cauza tehnică;

– codurile „Other” (RAXX, RBXX, RCXX, RDXX, REXX) se folosesc numai împreună cu o descriere textuală a motivului, atunci când niciun alt cod nu corespunde; pentru evenimentele D.3 și D.4, pentru care ETSI EN 319 522-2 nu definește coduri specifice, se folosește RDXX, cu descrierea canalului de notificare și a rezultatului;

– codurile sunt cele din ETSI EN 319 522-2, cl. 8.3.3 (tabelele 7–12); numerotarea codurilor B urmează ETSI EN 319 532-4, tabelul C.28.

6.2. Depunerea (A.1, A.2)

Cod și denumire	Explicația
RA01 MessageAccepted	trimiterea a fost acceptată (A.1)
RA02 InvalidMessageFormat	trimiterea nu respectă formatul cerut, de exemplu structura MIME sau metadatele sunt invalide (A.2)
RA03 MalwareFound	în trimitere s-a găsit cod malițios (A.2)
RA04 S_ERDS_ExpiredSenderCertificate	certificatul cu care expeditorul a semnat trimiterea este expirat sau revocat (A.2)
RA05 S_ERDS_PolicyViolation	trimiterea încalcă politica serviciului: depășește dimensiunea maximă (30 MB la QREM, 100 MB la QeRDS), conține formate neacceptate, are un destinatar inexistent sau neacceptat ori expeditorul nu are dreptul să trimită; detaliul textual indică regula încălcată (A.2)
RA06 S_ERDS_Malfunction	trimiterea nu a putut fi acceptată din cauza unei defecțiuni a serviciului; expeditorul poate depune din nou trimiterea (A.2)

6.3. Transmiterea între prestatori (B.1, B.2, B.3)

Cod și denumire	Explicația
RB01 S_ERDS_MessageSuccessfullyRelayed	trimiterea a fost transmisă cu succes prestatorului destinatarului (B.1)
RB02 R_ERDS_MessageRejected	trimiterea a fost transmisă, dar prestatorul destinatarului a refuzat-o pentru format invalid (B.2)
RB03 R_ERDS_MessageRejectedForMalware	trimiterea a fost refuzată de prestatorul destinatarului pentru cod malițios (B.2)

Cod și denumire	Explicația
RB04 R_ERDS_MessageRejectedForInvalidSignature	trimiterea a fost refuzată pentru sigiliu invalid sau pentru încălcarea politicii de semnătură (B.2)
RB05 R_ERDS_MessageRejectedForInvalidCertificate	trimiterea a fost refuzată pentru că certificatul de sigiliu al serviciului, de pe trimitere sau de pe o dovadă, este expirat sau revocat (B.2)
RB06 R_ERDS_PolicyViolation	trimiterea a fost refuzată pentru încălcarea politicii prestatorului destinatarului, de exemplu dimensiunea, formatele sau prestatorul care transmite nu este acceptat (B.2)
RB07 R_ERDS_Malfunction	trimiterea nu a fost transmisă din cauza unei defecțiuni a prestatorului destinatarului (B.3)
RB08 R_ERDS_NotIdentified	trimiterea nu a fost transmisă: prestatorul destinatarului nu a putut fi identificat (B.3)
RB09 R_ERDS_Unreachable	trimiterea nu a fost transmisă: prestatorul destinatarului nu este accesibil (B.3)
RB10 UnknownRecipient	trimiterea nu a fost transmisă: destinatarul este necunoscut (B.3)
RB21 MessageNotAcceptedForUnregisteredRecipient	trimiterea a fost refuzată de prestatorul destinatarului: destinatarul nu este înregistrat la acesta (B.2)
RB22 S_ERDSP_ReceivedNoRelayAcceptanceInfoFromR_ERDSP	CERTDIGITAL nu a primit de la prestatorul destinatarului, în intervalul stabilit, informația de acceptare a transmiterii (B.3)

6.4. Acceptarea sau refuzul de către destinatar (C.1–C.5)

Cod și denumire	Explicația
RC01 R_ERDS_NotificationForAcceptanceSent	notificarea pentru acceptare a fost transmisă destinatarului (C.1)
RC02 R_ERDS_SubsequentNotificationForAcceptanceSent	a fost transmisă o notificare ulterioară, după ce destinatarul nu a răspuns la notificările anterioare (C.1)
RC03 R_ERDS_NotificationForAcceptanceError	eroare la transmiterea notificării pentru acceptare (C.2)
RC04 R_ERDS_SubsequentNotificationForAcceptanceError	eroare la transmiterea notificării ulterioare (C.2)
RC05 R_ERDS_NotificationForAcceptanceMultipleError	notificarea pentru acceptare nu a putut fi transmisă după mai multe încercări (C.2)
RC06 R_ERDS_SubsequentNotificationForAcceptanceMultipleError	notificarea ulterioară nu a putut fi transmisă după mai multe încercări (C.2)
RC07 R_ERDS_MessageAcceptedByRecipient	destinatarul a acceptat trimiterea (C.3)
RC08 R_ERDS_MessageRejectedByRecipient	destinatarul a refuzat explicit trimiterea (C.4)
RC09 R_ERDS_MessageNotAcceptedByRecipient	destinatarul nu a acceptat trimiterea în termenul de acceptare (C.5)

6.5. Punerea la dispoziție (D.1–D.4)

Cod și denumire	Explicația
RD01 MessageConsignedToRecipient	conținutul a fost pus la dispoziția destinatarului (D.1)
RD02 R_ERDS_MessageConsignedToDelegate	conținutul a fost pus la dispoziția unui delegat al destinatarului (D.1)

Cod și denumire	Explicația
RD03 S_ERDSP_ReceivedNoDeliveryInfoFromR_ERDSP	prestatorul destinatarului nu a confirmat, în intervalul stabilit, punerea la dispoziție (D.2)
RD04 MessageNotConsignedForQuota	conținutul nu a fost pus la dispoziție: spațiul de stocare al destinatarului este depășit (D.2)
RD05 MessageNotConsignedForMalfunction	conținutul nu a fost pus la dispoziție din cauza unei defecțiuni tehnice (D.2)
RD06 MessageNotConsignedForUnallowedType	conținutul nu a fost pus la dispoziție: tipul trimiterii nu este acceptat de destinatar (D.2)
RD21 MessageNotConsignedForUnregisteredRecipient	destinatarul fără cont nu s-a înregistrat în termenul de acceptare; este „dovada de neridicare” (D.2)
RDXX Other	folosit numai pentru D.3 și D.4, cu descrierea canalului de notificare și a rezultatului

Codurile RD31–RD34, care privesc dovezile D.5 și D.6, nu se folosesc.

6.6. Predarea (E.1, E.2)

Cod și denumire	Explicația
RE01 R_ERDS_MessageHandoverToRecipient	conținutul a fost preluat de destinatar (E.1)
RE02 R_ERDS_MessageHandoverToDelegate	conținutul a fost preluat de un delegat al destinatarului (E.1)
RE03 R_ERDS_MessageTypeNotAcceptedByRecipient	predarea nu s-a făcut: tipul trimiterii nu este acceptat de destinatar (E.2)
RE04 R_ERDS_MessageHandoverFailure	conținutul nu a fost preluat până la sfârșitul perioadei de disponibilitate de 90 de zile și a fost șters (E.2)

6.7. Sistemele necalificate (F.1, F.2, F.3)

Cod și denumire	Explicația
RF01 RelayToNonERDS	trimiterea a fost transmisă cu succes către sistemul necalificat (F.1)
RF02 ExternalSystemUnreacheanble	sistemul extern nu este accesibil (F.2); denumirea reproduce exact grafia din standard
RF03 RejectedRelayToNonERDS	sistemul extern a refuzat mesajul (F.2)
RF04 ReceivedFromNonERDS	mesajul a fost primit de la un sistem necalificat (F.3)

ETSI EN 319 522-2, tabelul 12, denumește evenimentele F.1 și F.2 „ContentConsignment” și „ContentConsignmentFailure”; CERTDIGITAL folosește denumirile din ETSI EN 319 522-1, tabelul 1 (RelayToNonERDS și RelayToNonERDSFailure).

7. Obținerea și verificarea dovezilor

7.1. Obținerea dovezilor

– expeditorul primește automat dovezile în cont; la QREM le primește și ca mesaje REM sau ca părți MIME ale mesajelor (secțiunea 5.2);

– destinatarul primește în cont dovezile care îl privesc (C.3, C.4, E.1 și F.3), iar la QREM și în mesajele REM;

– expeditorul și destinatarul pot descărca oricând, gratuit, din cont, dovezile care îi privesc, în format XML și PDF, pe toată durata de păstrare de 10 ani (capitolul 8); utilizatorii QeRDS le pot obține și prin interfața de programare;

– după închiderea contului, dovezile se obțin pe baza unei cereri scrise transmise la office@certdigital.ro, după verificarea identității solicitantului;

– la cerere sau la încetarea contractului, abonatul primește exportul complet, ca arhivă cu index, în cel mult 30 de zile, pe un canal securizat (PDP-QERDS, capitolul 16);

– părțile care se bazează primesc dovezile de la expeditor sau de la destinatar; CERTDIGITAL nu comunică dovezile terților fără acordul părții la care se referă sau fără temei legal.

7.2. Verificarea dovezilor

Oricine poate verifica gratuit o dovadă, astfel:

a) se validează sigiliul dovezii (XAdES pentru dovada XML, PAdES pentru varianta PDF, semnătura S/MIME pentru mesajele REM) cu un validator de semnături și sigilii electronice calificate, de exemplu serviciul calificat de validare CERTDIGITAL (QESVal, descris în PDP-QESVal); rezultatul trebuie să fie „TOTAL-PASSED” pentru un sigiliu electronic calificat (ETSI EN 319 102-1);

b) se verifică faptul că certificatul de sigiliu este CERTDIGITAL QERDS SERVICE G5 sau CERTDIGITAL QREM SERVICE G5, emis de CERTDIGITAL QCA G5, și că serviciul corespunzător (`EDS/Q` sau `EDS/REM/Q`) avea statut calificat în Lista de încredere a României la momentul indicat de marca temporală;

c) se verifică marca temporală calificată a sigiliului, emisă de CertDigital TSA, care atestă momentul la care dovada exista;

d) se citesc evenimentul (G03), motivul (G04) și data și ora evenimentului (G05), conform capitolelor 3, 4 și 6;

e) pentru a stabili că un document este cel transmis, se calculează amprenta SHA-256 a documentului și se compară cu amprenta din componenta M02; amprentele identice arată că documentul nu a fost modificat;

f) se verifică, după caz, că identificatorul trimiterii (M01) este același în toate dovezile invocate pentru aceeași trimitere.

Statutul calificat al serviciilor se verifică la https://trustedlist.adr.gov.ro/.

7.3. Augmentarea și păstrarea pe termen lung

Dovezile se emit la nivelul B-T. Partea care păstrează o dovadă dincolo de termenul de 10 ani sau dincolo de valabilitatea certificatului de sigiliu o poate augmenta, de exemplu la nivelul LTA, ori o poate încredința unui serviciu calificat de păstrare, cum este serviciul calificat de păstrare CERTDIGITAL (PSPPS), care o menține verificabilă prin augmentare, la cererea abonatului și în condițiile PSPPS. CERTDIGITAL augmentează dovezile pe care le păstrează încă, atunci când algoritmii sau lungimile de cheie folosite nu mai sunt considerate sigure (secțiunea 8.2).

8. Păstrarea și limitele de valabilitate

8.1. Păstrarea

– dovezile și amprentele conținutului se păstrează 10 ani de la emiterea dovezii, protejate împotriva modificării, și pot fi obținute de expeditor și de destinatar pe toată această perioadă;

– conținutul trimiterii nu face parte din dovadă: el rămâne disponibil 90 de zile calendaristice de la punerea la dispoziție (D.1) sau, pentru trimiterile neacceptate ori neridicate în termenul de acceptare, până la expirarea acestui termen, apoi se șterge, cu jurnalizarea ștergerii; amprenta lui rămâne în dovezi;

– jurnalele serviciilor, inclusiv jurnalul emiterii dovezilor, se păstrează 10 ani de la înregistrare;

– la încetarea serviciilor, dovezile se predau succesorului, dacă există, sau custodelui înregistrărilor desemnat conform Planului de încetare și rămân accesibile părților 10 ani de la emitere; înainte de data încetării, abonații primesc exportul dovezilor lor (PDP-QERDS, secțiunea 6.16).

8.2. Limitele de valabilitate a dovezilor

Limitele de valabilitate a dovezilor sunt cele din PDP-QERDS, secțiunea 13.5 (ETSI 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;

– 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 sau încredințate unui serviciu calificat de păstrare (secțiunea 7.3);

– 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;

– o dovadă atestă numai evenimentul indicat în ea; dovezile nu atestă conținutul juridic al datelor transmise, pe care serviciile nu îl verifică (PDP-QERDS, secțiunea 1.4).