

Politica și declarația de practici a serviciului calificat de validare

CertDigital QESVal

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, structurată după anexa A din ETSI TS 119 441) a serviciului calificat de validare; Reg. (UE) 2025/1942 și 2025/1945; serviciu calificat din 10.11.2025 (VA G4), cu versiune G5; temeiul publicării tarifelor: art. 11 alin. (1) din Legea nr. 214/2024	22/10/2026
1.1	Ofițer de Securitate IT	Legătura ANPC pentru SAL devine https://anpc.ro/sal; trimiterile la documentele asociate, la versiunile în vigoare (PG v2.1); tabelul de identificare arată versiunea în vigoare	27/10/2026
1.2	Ofițer de Securitate IT	Trimiterile la celelalte documente CertDigital nu mai au număr de versiune: se aplică versiunea în vigoare, publicată la adresa fixă din depozit, iar versiunile anterioare sunt în arhivă	27/10/2026

Cuprins

PARTEA I – Politica serviciului 7
1. Introducere 7
1.1. Prezentare generală 7
1.2. Identificarea documentului și a politicii 7
1.3. Participanții și furnizorii externi 8
1.4. Utilizarea serviciului 9
1.5. Administrarea documentului 9
2. Referințe normative 10
2.1. Acte normative și standarde 10
3. Definiții și acronime 11
3.1. Definiții 11
3.2. Acronime 11
4. Concepte generale 12
4.1. Serviciul și componentele sale 12
4.2. Platforma serviciului 12
4.3. Profilurile de validare 12
4.4. Identitatea serviciului și sigiliul serviciului 12
5. Politica serviciului 14
5.1. Identificare și conformitate 14
5.2. Comunitatea utilizatorilor și aplicabilitatea 14
5.3. Modificarea politicii 14
6. Cerințele privind practicile 15
6.1. Publicare și depozit 15
6.2. Termeni și condiții 15
6.3. Cererea de validare 15
6.4. Procesul de validare 15
6.5. Raportul de validare 16
6.6. Datele transmise și păstrarea lor 16
6.7. Timpul de încredere și jurnalele 16
6.8. Personalul 17

6.9. Controale privind facilitățile, managementul și operarea 17
6.10. Actualizarea componentelor de validare 17
6.11. Controale criptografice și de rețea 17
6.12. Notificări către ADR și încetarea serviciului 18
6.13. Evaluarea conformității 18
7. Obligații și răspundere 19
7.1. Obligațiile CERTDIGITAL 19
7.2. Obligațiile beneficiarului și ale abonatului 19
7.3. Obligațiile părților care se bazează 19
7.4. Răspunderea 19
7.5. Asigurarea 19
8. Alte aspecte comerciale și juridice 21
8.1. Tarife 21
8.2. Protecția datelor cu caracter personal 21
8.3. Modificări 21
8.4. Soluționarea litigiilor 21
8.5. Legea aplicabilă și cadrul legal 21
8.6. Alte prevederi 22
9. Corespondența cu cerințele art. 32, 32a și 33 și ale regulamentelor de punere în aplicare 23
9.1. Tabel de corespondență 23
PARTEA A II-A – Declarația de practici 24
10. Publicare și depozit 24
11. Accesul la serviciu 25
11.1. Interfața web 25
11.2. Interfața de programare 25
11.3. Limite 25
12. Procesul de validare 26
12.1. Obiectele acceptate 26
12.2. Politica de validare și constrângerile ei 26
12.3. Determinarea calificării 26
12.4. Rezultatul validării 27
12.5. Testarea și controlul calității 27
13. Raportul de validare 28

13.1. Formatul și conținutul 28
13.2. Sigilarea și marca temporală 28
13.3. Verificarea raportului 28
14. Datele transmise, păstrarea și protecția datelor 29
14.1. Ștergerea documentelor 29
14.2. Durata păstrării 29
14.3. Protecția datelor 29
15. Controale de management și operare 30
16. Aspecte juridice și comerciale 32
Anexa A – Corespondența practicilor din Partea a II-a cu cerințele 33

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 **serviciului calificat de validare a semnăturilor electronice calificate și a sigiliilor electronice calificate** (art. 32, 33 și 40 din Regulamentul (UE) nr. 910/2014, astfel cum a fost modificat prin Regulamentul (UE) 2024/1183) și descrie practicile prin care acestea sunt îndeplinite. Serviciul validează, în aceleași condiții, și semnăturile și sigiliile electronice avansate bazate pe certificate calificate (art. 32a și 40a).

Serviciul permite părților care se bazează (beneficiarilor) să primească, în mod automat, fiabil și eficient, rezultatul validării unei semnături sau al unui sigiliu, sub forma unui raport de validare care poartă sigiliul electronic al CERTDIGITAL (art. 33 alin. (1) lit. (b)).

Serviciul este **calificat și înscris în Lista de încredere a României din 10.11.2025** (tipul `QESValidation/Q`, pentru semnături și sigilii), cu identitatea dată de certificatul CERTDIGITAL VALIDATION AUTHORITY G4, și este accesibil la https://ca.certdigital.ro/vs/. Prezentul document se aplică serviciului din generația G4 și versiunii lui din generația G5.

Documentul are două părți. Partea I, politica serviciului, stabilește **ce** garantează CERTDIGITAL. **Cum** sunt îndeplinite cerințele este descris în Partea a II-a, declarația de practici. Pentru mărcile temporale calificate se aplică Politica și declarația de practici a serviciului calificat de marcare temporală (PDP-QTST), iar pentru cerințele comune tuturor serviciilor, Politicile generale CertDigital (PG).

1.2. Identificarea documentului și a politicii

Element	Valoare
Titlu	Politica și declarația de practici a serviciului calificat de validare a semnăturilor și sigiliilor electronice calificate CertDigital (PDP-QESVal)
Denumirea în limba engleză	CertDigital Qualified Signature and Seal Validation Service Policy and Practice Statement
Versiune	1.2
Identificator (OID)	1.3.6.1.4.1.47898.9.1 (identifică politica serviciului și prezentul document)
Profilul de validare calificată	1.3.6.1.4.1.47898.9.1.1: validarea calificată a semnăturilor și sigiliilor electronice calificate (art. 32, 33 și 40)

Element	Valoare
Profilul de validare AdES bazată pe certificat calificat	1.3.6.1.4.1.47898.9.1.2: validarea semnăturilor și sigiliilor electronice avansate bazate pe certificate calificate (art. 32a și 40a)
Identificatorul alocat inițial declarației de practici (1.3.6.1.4.1.47898.9.2)	nu se mai folosește; declarația de practici este inclusă în prezentul document (Partea a II-a)
Politica ETSI respectată	politica serviciului calificat de validare din ETSI TS 119 441 V1.2.1, OID **0.4.0.19441.1.2**, cu adaptările din Regulamentul de punere în aplicare (UE) 2025/1942
Specificații de referință	RE (UE) 2025/1942 (serviciul calificat de validare: TS 119 441 V1.2.1 și TS 119 172-4 V1.1.1, adaptate) și RE (UE) 2025/1945 (procesul de validare: TS 119 172-4 V1.1.1 adaptat, EN 319 102-1 V1.4.1, TS 119 102-2 V1.4.1)
Tipul de serviciu (ETSI TS 119 612)	`http://uri.etsi.org/TrstSvc/Svctype/QESValidation/Q`, pentru semnături (ForeSignatures) și sigilii (ForeSeals)
Identitatea serviciului în Lista de încredere	G4: CERTDIGITAL VALIDATION AUTHORITY G4 (înscris din 10.11.2025); G5: CERTDIGITAL QESVAL SERVICE G5 (secțiunea 4.4)
Punctul de acces	https://ca.certdigital.ro/vs/ (interfața web) și interfața de programare (secțiunea 11.2)
Publicat la	https://www.certdigital.ro/repository/politici/certdigital_pdp-qesval_ro.pdf; versiunile anterioare: https://www.certdigital.ro/repository/arhiva/

Identificatorii sunt înscriși în CERTDIGITAL_OID_MAP. Rapoartele de validare conțin identificatorul politicii și al profilului aplicat; certificatul de sigiliu QESVal G5 conține identificatorul politicii (1.3.6.1.4.1.47898.9.1). Certificatul G4 (CERTDIGITAL VALIDATION AUTHORITY G4) a fost emis înainte de alocarea acestor identificatori și nu îi conține.

1.3. Participanții și furnizorii externi

– **prestatorul serviciului de validare**: CERTDIGITAL, care răspunde în ansamblu de serviciu, inclusiv atunci când folosește propriul serviciu calificat de marcare temporală;

– **beneficiarul**: persoana fizică sau juridică care transmite o semnătură sau un sigiliu spre validare și primește raportul de validare; poate fi parte care se bazează sau acționează în numele acesteia;

– **abonatul**: persoana care încheie un contract pentru utilizarea serviciului prin interfața de programare;

– **părțile care se bazează** pe raportul de validare;

– **surse externe de date**, folosite numai ca date de intrare: Lista listelor de încredere a Comisiei Europene (LOTL) și listele naționale, serviciile OCSP și CRL ale emitenților de certificate, serviciile de marcare temporală care au emis mărcile temporale din semnături;

– **serviciul calificat de marcare temporală CERTDIGITAL**, pentru marca temporală a rapoartelor.

CERTDIGITAL nu deleagă către terți validarea sau gestionarea cheilor serviciului.

1.4. Utilizarea serviciului

Serviciul se utilizează pentru a stabili dacă o semnătură sau un sigiliu electronic este valid la momentul relevant și dacă este calificat. Raportul de validare nu atestă conținutul documentului și nici capacitatea juridică a semnatarului, ci numai rezultatul procesului de validare, pe baza informațiilor disponibile la momentul validării.

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. 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. 13, 15, 20, 21, 24, 26, 32, 32a, 33, 40 și 40a și anexele I și III;

– Regulamentul de punere în aplicare (UE) 2025/1942 (serviciile calificate de validare a semnăturilor și sigiliilor electronice calificate);

– Regulamentul de punere în aplicare (UE) 2025/1945 (validarea semnăturilor și sigiliilor electronice calificate și a celor avansate bazate pe certificate calificate);

– Regulamentul de punere în aplicare (UE) 2025/2530 (cerințe pentru prestatorii calificați: notificări, gestionarea riscurilor, planul de încetare); Regulamentul de punere în aplicare (UE) 2025/1929 (marcarea temporală calificată); Regulamentul de punere în aplicare (UE) 2025/2162 (acreditarea organismelor de evaluare a conformității);

– ETSI TS 119 441 V1.2.1 (cerințe de politică pentru prestatorii de servicii de validare a semnăturilor), cu adaptările din RE 2025/1942; versiunea V1.3.1 (2025-10) se folosește numai informativ;

– ETSI TS 119 172-4 V1.1.1 (validarea semnăturilor în contextul UE), cu adaptările din RE 2025/1942 și din RE 2025/1945, anexele I și II;

– ETSI EN 319 102-1 V1.4.1 (procedurile de validare a semnăturilor AdES); ETSI TS 119 102-2 V1.4.1 (raportul de validare); ETSI TS 119 101 V1.1.1; ETSI TS 119 612 V2.3.1 și ETSI TS 119 615 (listele de încredere și utilizarea lor);

– ETSI TS 119 442 V1.1.1 (profilurile protocolului serviciului de validare), recomandat de TS 119 441 (SVP-8.2-01);

– ETSI EN 319 401 V3.1.1; ETSI EN 319 411-1 (politica NCP+) și ETSI EN 319 411-2 (politica QCP-l-qscd), pentru certificatul de sigilare a rapoartelor; documentul „Agreed Cryptographic Mechanisms” al ECCG, publicat de ENISA; schema EUCC (RE 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

– **validare** — procesul de verificare și confirmare a validității unei semnături sau a unui sigiliu electronic (art. 3 pct. 41 din Regulamentul eIDAS);

– **date de validare** — datele utilizate pentru validarea unei semnături sau a unui sigiliu electronic (art. 3 pct. 40);

– **politica de validare** — setul de reguli și constrângeri aplicate la validare, identificat în raport;

– **raport de validare** — documentul structurat, conform ETSI TS 119 102-2, care cuprinde rezultatul validării, motivele și datele folosite;

– **indicația principală** — rezultatul global al validării: TOTAL-PASSED (valid), TOTAL-FAILED (nevalid) sau INDETERMINATE (nedeterminat), conform ETSI EN 319 102-1;

– **calificarea** — încadrarea semnăturii sau a sigiliului: semnătură / sigiliu electronic calificat, avansat bazat pe certificat calificat, avansat sau neîncadrat, conform ETSI TS 119 172-4 și TS 119 615.

3.2. Acronime

Acronim	Semnificație
AdES	semnătură sau sigiliu electronic avansat (CAdES, XAdES, PAdES, JAdES, ASiC)
ADR	Autoritatea pentru Digitalizarea României, organismul de supraveghere
CAB	organism de evaluare a conformității (conformity assessment body)
CRL	lista certificatelor revocate (certificate revocation list)
DSS	biblioteca europeană de referință pentru semnăturile electronice (Digital Signature Service)
ECCG ACM	documentul „Agreed Cryptographic Mechanisms” al Grupului european de certificare a securității cibernetice (ECCG), publicat de ENISA
GDPR	Regulamentul (UE) 2016/679 (Regulamentul general privind protecția datelor)
HSM	modul criptografic hardware (hardware security module)
LOTL	lista listelor de încredere a Comisiei Europene
OCSP	protocolul de verificare online a stării certificatelor (Online Certificate Status Protocol)
PoE	dovadă de existență (proof of existence)
QESVal	serviciul calificat de validare a semnăturilor și sigiliilor electronice calificate
QSCD	dispozitiv calificat de creare a semnăturilor sau a sigiliilor electronice
QTST	marcă temporală electronică calificată
SVSP	prestator de servicii de validare a semnăturilor (ETSI TS 119 441)

4. Concepte generale

4.1. Serviciul și componentele sale

– **primirea cererii**: beneficiarul transmite semnătura sau sigiliul (documentul semnat, eventual cu documentul detașat și datele de validare suplimentare) prin interfața web sau prin interfața de programare (ETSI TS 119 442);

– **validarea**: aplicarea procesului din ETSI EN 319 102-1, cu politica de validare corespunzătoare profilului (secțiunea 6.4);

– **determinarea calificării**: pe baza listelor de încredere ale UE (ETSI TS 119 615) și a regulilor din ETSI TS 119 172-4;

– **raportul**: emiterea raportului de validare conform ETSI TS 119 102-2, sigilat de CERTDIGITAL și marcat temporal calificat (secțiunea 6.5);

– **ștergerea**: documentele transmise se șterg după emiterea raportului (secțiunea 6.6).

4.2. Platforma serviciului

Serviciul este prestat prin aplicația de validare a CERTDIGITAL, accesibilă la https://ca.certdigital.ro/vs/, construită pe biblioteca europeană de referință pentru semnăturile electronice (DSS, versiunea 6.2, conform rapoartelor din 24.06.2025), cu politica de validare „QES AdESQC TL based”, și prin interfața de programare pentru abonați (secțiunea 11.2). Actualizările bibliotecii DSS se testează și se aprobă înainte de producție (secțiunea 15). Adresa serviciului rămâne aceeași și după trecerea sigilării pe CERTDIGITAL QESVAL SERVICE G5 (secțiunea 4.4).

4.3. Profilurile de validare

Profil	Ce validează	Rezultatul
Validare calificată (47898.9.1.1)	semnături și sigilii electronice calificate, conform art. 32 alin. (1) și art. 40	indicația principală și calificarea (inclusiv dacă semnătura este calificată), cu motivele
Validare AdES bazată pe certificat calificat (47898.9.1.2)	semnături și sigilii electronice avansate bazate pe certificate calificate, conform art. 32a și 40a	indicația principală și calificarea

Profilul aplicat și politica de validare folosită se înscriu în raport.

4.4. Identitatea serviciului și sigiliul serviciului

Rapoartele de validare poartă **sigiliul electronic al CERTDIGITAL**, creat cu certificatul calificat de sigiliu dedicat serviciului, cu cheia păstrată într-un modul criptografic certificat (secțiunea 6.11): în generația G4, CERTDIGITAL VALIDATION AUTHORITY G4, care identifică serviciul în Lista de încredere din 10.11.2025; în generația G5, CERTDIGITAL QESVAL SERVICE G5.

Certificatul CERTDIGITAL QESVAL SERVICE G5 a fost emis de CERTDIGITAL QCA G5 în ceremonia cheilor G5 din 23.10.2026 (RSA 4096, valabil 5 ani) și se publică la http://certs.certdigital.ro/certdigital_qesval_g5.crt. Până la înscrierea lui în Lista de încredere ca identitate a serviciului, rapoartele se sigilează cu certificatul CERTDIGITAL VALIDATION AUTHORITY G4; după înscriere, sigilarea trece pe CERTDIGITAL QESVAL SERVICE G5.

5. Politica serviciului

5.1. Identificare și conformitate

CERTDIGITAL declară conformitatea serviciului cu standardele și specificațiile din Regulamentul de punere în aplicare (UE) 2025/1942, ceea ce atrage prezumția de conformitate cu cerințele art. 33 alin. (1) (art. 33 alin. (2)), și a procesului de validare cu Regulamentul de punere în aplicare (UE) 2025/1945, ceea ce atrage prezumția de conformitate cu art. 32 alin. (1) și art. 32a. Serviciul are statut calificat din 10.11.2025; conformitatea este reevaluată de un organism de evaluare a conformității acreditat cel puțin o dată la 24 de luni (secțiunea 6.13).

5.2. Comunitatea utilizatorilor și aplicabilitatea

Serviciul se adresează oricărei persoane care trebuie să verifice o semnătură sau un sigiliu electronic: părți care se bazează, autorități și instituții publice, instanțe, profesioniști și persoane fizice.

5.3. Modificarea politicii

Dacă o modificare a prezentului document sau a unui profil afectează garanțiile oferite, identificatorul politicii sau al profilului se schimbă. Rapoartele 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 serviciului, politicile de validare folosite, specificația raportului și certificatele de sigiliu ale serviciului sunt publicate la https://www.certdigital.ro/repository/, 24/7, public și fără restricții de acces.

6.2. Termeni și condiții

Înainte de utilizarea serviciului, beneficiarii și abonații sunt informați, clar, complet și ușor accesibil, atât public, cât și individual, despre termenii și condițiile serviciului: profilurile și politicile de validare, formatele acceptate, limitele de dimensiune, durata păstrării datelor, tarifele, răspunderea și limitările ei.

6.3. Cererea de validare

– serviciul acceptă semnături și sigilii în formatele CAdES, XAdES, PAdES, JAdES și containere ASiC, atașate sau detașate de document, împreună cu datele de validare suplimentare furnizate de beneficiar;

– pentru semnăturile detașate, beneficiarul transmite și documentul semnat; amprenta documentului se calculează numai de serviciu, iar cererile care conțin doar amprenta nu se acceptă (RE 2025/1942, VPR-B-11);

– abonații care folosesc interfața de programare se autentifică prin TLS cu autentificare reciprocă sau prin mijloace echivalente; interfața web publică nu cere autentificare;

– dimensiunea maximă a unei cereri este stabilită în termenii și condițiile serviciului.

6.4. Procesul de validare

– validarea respectă ETSI EN 319 102-1, cu politica de validare a profilului ales, și confirmă, pentru validarea calificată, condițiile de la art. 32 alin. (1) lit. (a)–(h): certificatul era calificat la momentul semnării și emis de un prestator calificat; era valabil la momentul semnării; datele de validare corespund datelor furnizate de beneficiar; datele care reprezintă semnatarul sunt furnizate corect; pseudonimul, dacă există, este indicat clar; semnătura a fost creată cu un dispozitiv calificat; integritatea datelor semnate nu a fost compromisă; cerințele art. 26 erau îndeplinite la momentul semnării;

– statutul calificat al certificatelor și al dispozitivelor se stabilește din listele de încredere ale statelor membre, obținute prin LOTL și verificate criptografic (ETSI TS 119 615), cu istoricul lor la momentul semnării;

– starea certificatelor se stabilește din informațiile de revocare (OCSP sau CRL) încorporate în semnătură sau obținute la validare; pentru certificatul semnatarului, informațiile de revocare

nu pot fi mai vechi de 24 de ore față de momentul relevant (TS 119 172-4, REQ-4.2-03, adaptat); momentul semnării se stabilește din mărcile temporale existente;

– dacă verificarea calificării eșuează, procesul se încheie cu rezultatul INDETERMINATE, consemnat în raport (REQ-4.4.2-03); același obiect, validat în aceleași condiții, produce același rezultat;

– algoritmii și parametrii criptografici se evaluează conform documentului „Agreed Cryptographic Mechanisms" al ECCG, la momentul relevant;

– sistemul furnizează beneficiarului rezultatul corect al validării și îi permite să detecteze orice aspect relevant pentru securitate (art. 32 alin. (2)).

6.5. Raportul de validare

– serviciul furnizează rezultatul **în mod automat, fiabil și eficient**, sub forma unui raport de validare care poartă întotdeauna **sigiliul electronic calificat al CERTDIGITAL**, bazat pe certificatul calificat de sigiliu al serviciului (cu declarația QcSSCD), emis pe numele CENTRUL DE CALCUL S.A. conform politicii QCP-l-qscd (minimul cerut de OVR-7.5-02 este NCP+), cu marcă temporală calificată (art. 33 alin. (1) lit. (b); SVR-8.4-16; OVR-7.5-02);

– răspunsul și raportul conțin OID-ul politicii serviciului (SVP-8.2-03), constrângerile ignorate (SVR-8.4-07) și originea dovezilor de existență folosite (SVR-8.4-15);

– raportul respectă ETSI TS 119 102-2 (format XML) și este însoțit de o variantă lizibilă (PDF); cuprinde: identificarea obiectului validat și amprenta lui, indicația principală și subindicațiile, calificarea, politica de validare și profilul aplicate, datele folosite (certificate, informații de revocare, mărci temporale, liste de încredere), momentul validării și motivele rezultatului;

– raportul se poate verifica independent de serviciu, prin validarea sigiliului și a mărcii temporale.

6.6. Datele transmise și păstrarea lor

– documentele și semnăturile transmise spre validare se folosesc numai pentru validare și **se șterg după emiterea raportului**; se păstrează raportul de validare, amprenta obiectului validat și jurnalele (angajamentul din Politica de protecție a datelor, 00d);

– rapoartele de validare și jurnalele se păstrează cel puțin 10 ani și se pot obține din nou de beneficiar pe baza identificatorului raportului.

6.7. Timpul de încredere și jurnalele

– serverele serviciului sunt sincronizate cu o sursă de timp legată de UTC; momentul emiterii raportului se atestă printr-o marcă temporală calificată emisă de serviciul calificat de marcare temporală CERTDIGITAL;

– se jurnalizează cererile de validare (fără conținutul documentelor), rezultatele, emiterea rapoartelor, actualizările listelor de încredere și ale politicilor de validare, operațiile administrative și evenimentele de securitate, conform ETSI EN 319 401, cl. 7.10.

6.8. 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.

6.9. Controale privind facilitățile, managementul și operarea

Se aplică Politicile generale CertDigital, cu următoarele precizări:

– serviciul este operat 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 cu pierderea maximă de date de cel mult 5 minute pentru rapoartele de validare;

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

6.10. Actualizarea componentelor de validare

Listele de încredere se reîncarcă automat, cel puțin zilnic și la fiecare actualizare publicată, cu verificarea semnăturii LOTL. Politicile de validare și biblioteca de validare se actualizează controlat: orice schimbare se testează înainte de punerea în producție, se documentează și, dacă afectează rezultatele, se anunță prin publicarea unei versiuni noi a politicii de validare.

6.11. Controale criptografice și de rețea

– cheia privată a sigiliului serviciului se generează, se păstrează și se utilizează numai într-un dispozitiv criptografic certificat Common Criteria EAL4 sau superior, ori EUCC EAL4 sau superior, ori, până la 31.12.2030, FIPS 140-3 nivel 3, configurat 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 serviciului.

6.12. Notificări către ADR și încetarea serviciului

– CERTDIGITAL notifică ADR orice modificare a prestării serviciului 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: rapoartele de validare și jurnalele se păstrează în continuare sau se transferă unui prestator calificat acceptat de ADR, iar certificatul de sigiliu al serviciului se revocă după încetare.

6.13. Evaluarea conformității

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

7. Obligații și răspundere

7.1. Obligațiile CERTDIGITAL

– validează semnăturile și sigiliile conform art. 32 alin. (1), art. 32a și art. 40;

– furnizează rezultatul în mod automat, fiabil și eficient, într-un raport sigilat și marcat temporal calificat;

– menține la zi listele de încredere, politicile de validare și componentele de validare;

– șterge documentele transmise după emiterea raportului și păstrează rapoartele și jurnalele;

– publică documentația serviciului 24/7.

7.2. Obligațiile beneficiarului și ale abonatului

– transmite obiectul complet al validării (semnătura, documentul semnat, datele de validare disponibile);

– citește raportul în întregime, inclusiv subindicațiile și avertismentele, și ia în considerare momentul validării;

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

7.3. Obligațiile părților care se bazează

Verifică sigiliul și marca temporală calificată de pe raportul de validare 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 documentelor validate; informațiile incomplete transmise de beneficiar; informațiile eronate publicate de alți prestatori sau în listele de încredere, pe care CERTDIGITAL nu le putea detecta; utilizarea raportului în afara momentului și a contextului validării; utilizarea serviciului peste limitările notificate în prealabil și recognoscibile de terți; 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 de validare (a semnăturilor și a sigiliilor), 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

Validarea prin interfața web publică este gratuită. Utilizarea prin interfața de programare se face pe bază de contract, la tarifele din lista publicată pe site-ul https://www.certdigital.ro/ sau din oferta transmisă la cerere (art. 11 alin. (1) din Legea nr. 214/2024).

8.2. Protecția datelor cu caracter personal

Pentru documentele transmise spre validare, CERTDIGITAL acționează în calitate de **persoană împuternicită** (art. 28 din Regulamentul (UE) 2016/679) și le șterge după emiterea raportului; pentru rapoartele de validare, datele de cont și jurnalele serviciului, CERTDIGITAL este **operator**, conform Politicii de protecție a datelor (00d). CERTDIGITAL nu folosește persoane împuternicite pentru operarea serviciului. 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 serviciului se comunică ADR cu cel puțin o lună înainte de aplicare (cu cel puțin trei luni în cazul încetării serviciului). Beneficiarii și abonații sunt informați prin publicare pe site cu cel puțin 30 de zile înainte de intrarea în vigoare. Corecturile de redactare care nu modifică drepturile sau obligațiile părților se publică cu versiune nouă, fără termen de preaviz.

8.4. Soluționarea litigiilor

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

8.5. Legea aplicabilă și cadrul legal

Prezentul document și raporturile juridice decurgând din furnizarea serviciului sunt guvernate de dreptul român, sub rezerva dispozițiilor direct aplicabile ale dreptului Uniunii Europene. Serviciul este furnizat în conformitate cu actele normative de la secțiunea 2.1. Organismul de supraveghere este Autoritatea pentru Digitalizarea României.

8.6. Alte prevederi

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

9. Corespondența cu cerințele art. 32, 32a și 33 și ale regulamentelor de punere în aplicare

9.1. Tabel de corespondență

Cerință	Conținut	Secțiune
Regulamentul eIDAS, art. 32 alin. (1) lit. (a)–(h)	condițiile validării semnăturii calificate	6.4
art. 32 alin. (1), al doilea paragraf / RE 2025/1945	prezumția de conformitate a procesului de validare	5.1, 6.4
art. 32 alin. (2)	rezultatul corect; detectarea aspectelor relevante pentru securitate	6.4, 6.5
art. 32a / art. 40a	validarea semnăturilor și sigiliilor avansate bazate pe certificate calificate	4.3, 6.4
art. 33 alin. (1) lit. (a)	prestator calificat care validează conform art. 32 alin. (1)	1.1, 5.1
art. 33 alin. (1) lit. (b)	rezultat automat, fiabil, eficient, cu sigiliul avansat al prestatorului	6.5
art. 33 alin. (2) / RE 2025/1942	prezumția de conformitate a serviciului	5.1
art. 40	aplicarea mutatis mutandis pentru sigiliile calificate	1.1, 4.3
ETSI EN 319 102-1	procesul de validare	6.4
ETSI TS 119 102-2	raportul de validare	6.5
ETSI TS 119 172-4, TS 119 615	calificarea; utilizarea listelor de încredere	4.1, 6.4, 6.10
ETSI TS 119 441 V1.2.1 (politica 0.4.0.19441.1.2), adaptat prin RE 2025/1942	cerințe de politică pentru prestatorul serviciului de validare	1.2, 6.1–6.13
RE 2025/1942: OVR-6.1-02, -03	declarația de practici după anexa A; politici cu OID	1.2, 6.1, Partea a II-a
RE 2025/1942: OVR-7.5-02, -03	certificatul de sigilare NCP+; cheia în HSM certificat	4.4, 6.11
RE 2025/1942: SVP-8.2-03; SVR-8.4-07, -15, -16	OID-ul politicii în răspuns; constrângerile ignorate; originea dovezilor de existență; raport sigilat obligatoriu	6.5
RE 2025/1942: VPR-B-11	amprenta calculată de serviciu	6.3
TS 119 172-4, REQ-4.2-03, REQ-4.4.2-03 (adaptate)	revocare ≤ 24 h pentru certificatul semnatarului; INDETERMINATE la eșecul verificării calificării	6.4
ETSI TS 119 442 V1.1.1	protocolul serviciului (recomandat, SVP-8.2-01)	4.1, 6.3
RE 2025/2530	notificări ADR; plan de încetare	6.12

Practicile detaliate pentru fiecare cerință sunt descrise în Partea a II-a, iar corespondența lor cu cerințele, în anexa A.

PARTEA A II-A – Declarația de practici

10. Publicare și depozit

Partea a II-a păstrează structura declarației de practici din anexa A la ETSI TS 119 441, impusă de Regulamentul de punere în aplicare (UE) 2025/1942 (OVR-6.1-02). Ea pune în aplicare politica serviciului din Partea I (OID 1.3.6.1.4.1.47898.9.1) și descrie modul în care CERTDIGITAL prestează serviciul; identificarea documentului, participanții și furnizorii externi, referințele normative și definițiile sunt cele din Partea I, capitolele 1–3.

La https://www.certdigital.ro/repository/ se publică, 24/7: prezentul document, termenii și condițiile, politicile de validare (cu tabelul constrângerilor de la secțiunea 12.2), specificația raportului de validare, lista formatelor acceptate și certificatele de sigiliu ale serviciului. Versiunile anterioare rămân disponibile în secțiunea „Arhivă”.

11. Accesul la serviciu

11.1. Interfața web

Interfața web https://ca.certdigital.ro/vs/ este publică și gratuită. Beneficiarul încarcă documentul semnat (și, pentru semnăturile detașate, documentul original) și primește raportul de validare în format PDF și XML.

11.2. Interfața de programare

Abonații folosesc interfața de programare conform ETSI TS 119 442 V1.1.1 (recomandat de TS 119 441, SVP-8.2-01), în mod sincron (răspuns imediat) sau asincron (cerere înregistrată, răspuns ulterior pe baza identificatorului), prin HTTPS cu autentificare reciprocă TLS sau cu o cheie de acces emisă pentru abonat. Serviciul expune, pe lângă interfața web, o interfață B2B pentru integrare programatică și protocolul SCVP (IETF RFC 5055). Specificația interfeței se pune la dispoziția abonaților.

11.3. Limite

Dimensiunea maximă a unei cereri este de 50 MB, numărul maxim de cereri pe unitatea de timp se stabilește prin contract, iar disponibilitatea este publicată în termenii și condițiile serviciului.

12. Procesul de validare

12.1. Obiectele acceptate

Element	Valori
Formate	CAdES, XAdES, PAdES, JAdES, containere ASiC-S și ASiC-E
Forme	semnătură înglobată (enveloped, enveloping) și detașată
Niveluri	B, T, LT și LTA
Date suplimentare	certificate, informații de revocare și mărci temporale furnizate de beneficiar, folosite numai dacă sunt valide
Documentul semnat	pentru semnăturile detașate, beneficiarul transmite și documentul; amprenta se calculează numai de serviciu, iar cererile care conțin doar amprenta nu se acceptă (RE 2025/1942, VPR-B-11)

Toate formatele, formele și nivelurile din tabel se validează conform ETSI EN 319 102-1, iar raportul respectă ETSI TS 119 102-2.

12.2. Politica de validare și constrângerile ei

Serviciul aplică procesul de validare din ETSI EN 319 102-1 (validare de bază, validare cu informații de validare pe termen lung și validare pe termen lung cu dovezi de existență), cu următoarele constrângeri, publicate în politicile de validare:

Constrângere	Valoare în profilul de validare calificată
Ancore de încredere	**numai** listele de încredere ale statelor membre, obținute prin LOTL; alte ancore de încredere nu se folosesc
Statutul calificat al certificatului	obligatoriu certificat calificat UE pentru semnătură, respectiv pentru sigiliu, la momentul semnării
Dispozitivul de creare	QSCD, conform certificatului și listelor de încredere
Starea certificatului	verificată prin OCSP sau CRL („eitherCheck”); pentru certificatul semnatarului, informațiile de revocare nu pot fi mai vechi de 24 de ore față de momentul relevant; pentru celelalte certificate nu se impune o limită (TS 119 172-4, REQ-4.2-03, adaptat prin RE 2025/1942 și 2025/1945)
Algoritmi și lungimi de cheie	evaluați conform documentului „Agreed Cryptographic Mechanisms” al ECCG, la data relevantă
Momentul semnării	stabilit din mărcile temporale existente; în lipsa lor, se raportează ca atare
Formatul	conform standardelor de format (CAdES, XAdES, PAdES, JAdES, ASiC)

Profilul de validare AdES bazată pe certificat calificat aplică aceleași constrângeri, fără cerința dispozitivului calificat. Politica aplicată și profilul se înscriu în raport.

12.3. Determinarea calificării

Calificarea semnăturii sau a sigiliului (calificat, avansat bazat pe certificat calificat, avansat, neîncadrat) se stabilește conform ETSI TS 119 172-4 V1.1.1, adaptat, din certificat (declarațiile QcStatements) și din listele de încredere (ETSI TS 119 615), la momentul semnării. Dacă verificarea calificării eșuează, procesul se încheie cu rezultatul INDETERMINATE, consemnat în raport (REQ-4.4.2-03). Dacă obiectul nu poate fi legat de listele de încredere ale UE, raportul nu atribuie

calificarea „calificat”. În profilul AdES bazat pe certificat calificat, un certificat calificat și rezultatul TOTAL-PASSED înseamnă „semnătură (sigiliu) avansată bazată pe certificat calificat UE” (RE 2025/1945, anexa II, REQ-4.4.2-06).

12.4. Rezultatul validării

Rezultatul cuprinde indicația principală (TOTAL-PASSED, TOTAL-FAILED, INDETERMINATE), subindicațiile din ETSI EN 319 102-1 și motivele, pentru fiecare semnătură sau sigiliu din obiect.

12.5. Testarea și controlul calității

CERTDIGITAL menține un set de teste pozitive și negative (semnături valide, nevalide, expirate, revocate, necalificate, cu format greșit), rulat la fiecare actualizare a bibliotecii de validare, a politicilor sau a configurației, înainte de punerea în producție. Rezultatele testelor se păstrează. Aceleași date de intrare, validate în aceleași condiții, produc același rezultat.

13. Raportul de validare

13.1. Formatul și conținutul

Raportul respectă ETSI TS 119 102-2 (XML), cu o variantă lizibilă în PDF, și cuprinde:

– identificatorul unic al raportului și momentul validării;

– identificarea obiectului validat (nume, amprentă calculată de serviciu);

– pentru fiecare semnătură sau sigiliu: indicația, subindicația și motivele; calificarea; formatul și nivelul; semnatarul sau creatorul sigiliului, cu mențiunea pseudonimului, dacă este cazul; momentul semnării și dovezile de existență folosite; atributele semnate relevante;

– certificatele, informațiile de revocare și mărcile temporale folosite, cu sursa lor;

– OID-ul politicii serviciului (0.4.0.19441.1.2 și 1.3.6.1.4.1.47898.9.1), politica de validare și profilul aplicate (SVP-8.2-03), constrângerile ignorate, dacă este cazul (SVR-8.4-07), și originea dovezilor de existență folosite (SVR-8.4-15);

– avertismentele relevante pentru securitate (art. 32 alin. (2)).

13.2. Sigilarea și marca temporală

Fiecare raport, XML și PDF, poartă obligatoriu **sigiliul electronic calificat al serviciului** (XAdES, respectiv PAdES, nivel B-T), creat cu certificatul calificat de sigiliu al serviciului, emis pe numele CENTRUL DE CALCUL S.A. conform politicii QCP-l-qscd (minimul cerut de OVR-7.5-02 este NCP+), și o **marcă temporală calificată** CERTDIGITAL (art. 33 alin. (1) lit. (b); SVR-8.4-16, -17; OVR-7.5-02). Raportul constituie astfel și o dovadă de existență a obiectului validat la momentul validării.

13.3. Verificarea raportului

Raportul se poate verifica independent de serviciu, cu orice validator de sigilii calificate și cu Lista de încredere a României.

14. Datele transmise, păstrarea și protecția datelor

14.1. Ștergerea documentelor

Documentele și semnăturile transmise se prelucrează numai în memoria și spațiul temporar al serviciului și **se șterg imediat după emiterea raportului**; nu se păstrează copii. Se păstrează numai raportul de validare, amprenta obiectului validat, metadatele cererii și jurnalele.

14.2. Durata păstrării

Ce se păstrează	Cât
Rapoartele de validare (pentru reemitere pe baza identificatorului)	cel puțin 10 ani
Metadatele cererilor și jurnalele	cel puțin 10 ani
Listele de încredere și politicile de validare folosite (versiuni istorice)	cel puțin 10 ani, pentru reproducerea validărilor

14.3. Protecția datelor

Comunicațiile folosesc TLS conform ECCG ACM. CERTDIGITAL este persoană împuternicită pentru documentele transmise și operator pentru rapoarte, datele de cont și jurnale (Politica de protecție a datelor, 00d); temeiul prelucrării este executarea serviciului solicitat (art. 6 alin. (1) lit. (b) GDPR).

15. Controale de management și operare

Se aplică Politicile generale CertDigital și ETSI EN 319 401, cu adaptările din Regulamentul de punere în aplicare (UE) 2025/1942:

– **cheia sigiliului**: certificat dedicat serviciului (G4: CERTDIGITAL VALIDATION AUTHORITY G4; G5: CERTDIGITAL QESVAL SERVICE G5), cheie generată în ceremonie, sub control dual, într-un modul criptografic certificat (Common Criteria / EUCC EAL4+ sau FIPS 140-3 nivel 3), fără reutilizare pentru alte servicii; certificatul CERTDIGITAL QESVAL SERVICE G5 este emis de CERTDIGITAL QCA G5, iar cheia lui (RSA 4096) se generează în ceremonia G5 direct în modulul Thales Luna PCIe HSM 7 A790 (dispozitiv calificat eIDAS-2400055-01), în partiția SVG5; cheia certificatului CERTDIGITAL VALIDATION AUTHORITY G4 se află în modulul Utimaco CryptoServer Se-Series Gen2 (hardware 5.01.4.0), cu firmware-ul CryptoServer CP5 5.1.2.0, în configurația certificată Common Criteria EAL4+ conform EN 419 221-5 (NSCIB-CC-2300142-02) și ca dispozitiv calificat eIDAS (eIDAS-2300143-02, valabil până la 26.05.2030);

– **actualizarea listelor de încredere**: automată, cel puțin zilnic, cu verificarea semnăturii LOTL și a listelor naționale; eșecul actualizării declanșează alertă;

– **gestionarea schimbărilor**: actualizările bibliotecii DSS și ale politicilor de validare se testează (secțiunea 12.5) și se aprobă înainte de producție; vulnerabilitățile componentelor se remediază prompt;

– **personalul**: roluri de încredere separate; instruire cel puțin o dată la 12 luni privind amenințările și practicile actuale;

– **rețeaua**: scanare de vulnerabilități cel puțin trimestrială, test de penetrare cel puțin anual, firewall-uri restrictive, acces la distanță numai prin canale securizate cu autentificare cu doi factori;

– **jurnalizarea**: cererile (fără conținut), rezultatele, emiterea rapoartelor, actualizările listelor de încredere și ale politicilor, operațiile administrative și evenimentele de securitate;

– **continuitatea**: centrul de date principal și centrul de date secundar, conform PO_SI_63; disponibilitate de cel puțin 99,5%; durata maximă de restabilire de 8 ore și pierderea maximă de date de cel mult 5 minute;

– **lanțul de aprovizionare**: furnizorii de componente sunt evaluați; biblioteca DSS se obține numai din sursa oficială a Comisiei Europene;

– **incidentele**: notificate conform 00q;

– **încetarea**: conform planului 00r (RE 2025/2530); rapoartele și jurnalele se păstrează sau se transferă unui prestator calificat acceptat de ADR;

– **conformitatea**: evaluare de către un CAB acreditat cel puțin o dată la 24 de luni și audit intern anual.

16. Aspecte juridice și comerciale

Tarifele (secțiunea 8.1), răspunderea (art. 13 din Regulamentul eIDAS; secțiunea 7.4), asigurarea (secțiunea 7.5), modificările (secțiunea 8.3), soluționarea litigiilor (secțiunea 8.4) și legea aplicabilă (secțiunea 8.5) sunt cele din capitolele 7 și 8 și din termenii și condițiile serviciului. Validarea prin interfața web este gratuită.

Anexa A – Corespondența practicilor din Partea a II-a cu cerințele

Cerință	Conținut	Secțiune
Regulamentul eIDAS, art. 32 alin. (1) lit. (a)–(h)	condițiile validării calificate	12.2, 12.3
art. 32 alin. (2)	rezultat corect; aspecte de securitate	12.4, 13.1
art. 32a / art. 40a	validarea AdES bazată pe certificat calificat	12.2
art. 33 alin. (1) lit. (b)	rezultat automat, sigilat de prestator	11, 13.2
ETSI TS 119 441, anexa A	structura declarației de practici	1–3, 10–16
ETSI TS 119 442	protocolul serviciului	11.2
ETSI EN 319 102-1	procesul de validare; indicații și subindicații	12.2, 12.4
ETSI TS 119 102-2	raportul de validare	13.1
ETSI TS 119 172-4, TS 119 615	calificarea; listele de încredere	12.2, 12.3, 15
RE 2025/1942: OVR-6.1-02, -03	declarația după anexa A; politici cu OID	1.2, 10
RE 2025/1942: OVR-7.2-02, -03; OVR-7.5-02, -03, -06; OVR-7.7-02, -03; OVR-7.8-02…06; OVR-7.12-02; OVR-7.14-01	instruire la 12 luni; certificat NCP+ și cheie în HSM certificat; patch-uri; acces la distanță, scanare trimestrială, pentest anual, firewall; încetare; lanț de aprovizionare	13.2, 15
RE 2025/1942: VPR-8.1-11; SVP-8.2-03; SVR-8.4-02, -07, -15, -16, -17	TS 119 172-4; OID-ul politicii în răspuns; raport TS 119 102-2; constrângeri ignorate; originea PoE; sigilare obligatorie; formatul semnăturii	12.3, 13
RE 2025/1942, anexa B: VPR-B-02, -11, -15, -16; OVR-B-04	TS 119 172-4; amprenta calculată de serviciu; raport TS 119 102-2; ECCG ACM; teste pozitive și negative	12.1, 12.2, 12.5, 13.1
TS 119 441: OVR-7.13-03	documentele transmise nu se păstrează	14.1
RE 2025/1945, anexele I și II (TS 119 172-4 adaptat: REQ-4.2-03, 4.4.2-03, 4.4.2-06)	constrângeri de revocare; INDETERMINATE; AdES pe certificat calificat UE	12.2, 12.3