TERMENI ȘI CONDIȚII

pentru prestarea serviciilor de încredere necalificate — semnături electronice avansate cu certificat

comunicați și acceptați în relația dintre QSIGN S.R.L., în calitate de prestator, și utilizatorul final

Document	Termeni și Condiții — TSP QSIGN
Prestator	QSIGN S.R.L., CUI 34633481, J2024010825402
Sediu social	București, str. Drumea Rădulescu nr. 26, sector 4
Contact	alex@qsign.ro | 0724.167.333 | www.qsign.ro
Reprezentant legal	Trandafirescu Alexandru Florin
Cadru legal de referință	Reg. (UE) nr. 910/2014 (eIDAS); Legea nr. 214/2024; Ordinul MEDAT nr. 102/29.01.2026; Decizia ADR nr. 162/20.03.2026
Temei juridic al T&C	art. 5 alin. (2) lit. i) — Anexa nr. 2 la Ordinul MEDAT nr. 102/2026 (servicii de încredere necalificate)
Revizie	01
Limbă	Română (versiunea autentică)

*Prezentul document stabilește **termenii și condițiile aplicabile exclusiv serviciilor de încredere necalificate** prestate de QSIGN S.R.L., constând în emiterea de certificate pentru semnătura electronică avansată în sensul art. 26 din Regulamentul (UE) nr. 910/2014 și art. 12 alin. (2), art. 15 alin. (2), art. 16 din Legea nr. 214/2024, notificate ADR conform Anexei nr. 2 la Ordinul MEDAT nr. 102/2026. Termenii și condițiile pentru serviciile de încredere calificate prestate de QSIGN sunt cuprinse într-un document distinct (08.QSIGN-TC-QC-v1_0).*

PARTEA I — DISPOZIȚII COMUNE

Articolul 1 — Părțile

(1) Prestatorul: **QSIGN S.R.L.**, persoană juridică română, cu sediul în București, str. Drumea Rădulescu nr. 26, sector 4, înmatriculată la Oficiul Registrului Comerțului sub nr. J2024010825402, cod unic de înregistrare 34633481, denumită în continuare „**QSIGN**" sau „**Prestatorul**".

(2) Utilizatorul final: persoana fizică sau juridică, română sau străină, care contractează cu QSIGN un serviciu de încredere reglementat de prezentul document, în nume propriu sau prin reprezentant legal/împuternicit, denumită în continuare „**Utilizatorul**", „**Titularul**" (atunci când deține un certificat) sau „**Beneficiarul**".

(3) Calitatea QSIGN este aceea de **prestator de servicii de încredere** în sensul art. 3 pct. 19 din Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014, denumit în continuare „**Regulamentul eIDAS**", și al Legii nr. 214/2024 privind utilizarea semnăturii electronice, a mărcii temporale și prestarea serviciilor de încredere bazate pe acestea, denumită în continuare „**Legea nr. 214/2024**".

Articolul 2 — Obiect

(1) Prezentul document stabilește termenii și condițiile generale aplicabile relației contractuale dintre QSIGN și Utilizatorul final pentru serviciile de încredere **necalificate** (Partea II), precum și mecanismul detaliat de validare a semnăturii avansate (Partea IV), inclusiv drepturile și obligațiile părților, modalitățile de utilizare a serviciilor, condițiile de emitere/suspendare/revocare a certificatelor, răspunderea, tarifele și soluționarea litigiilor.

(2) Documentele subsecvente care completează prezentul (Politica de certificare — CP, Codul de practici și proceduri — CPS, Politica privind serviciul de marcare temporală — TSP, Termenii specifici ai produsului), publicate la adresa **https://www.qsign.ro/repository**, fac parte integrantă din raportul contractual dintre părți. În caz de neconcordanță, prevalează ordinea: (i) Reg. eIDAS și actele de punere în aplicare; (ii) Legea nr. 214/2024 și actele subsecvente; (iii) prezentul document; (iv) CP/CPS aplicabile; (v) condițiile particulare ale produsului.

Articolul 3 — Definiții

În sensul prezentului document, definițiile prevăzute la art. 3 din Regulamentul eIDAS și la art. 2 din Legea nr. 214/2024 se completează cu următoarele:

a) Certificat — atestare electronică care leagă datele de validare a unei semnături sau a unui sigiliu electronic de o persoană fizică sau juridică, confirmând cel puțin numele/denumirea acesteia, în sensul art. 3 pct. 14 și 29 din Reg. eIDAS;

b) CRL — Certificate Revocation List, lista certificatelor revocate, semnată de CA emitentă și publicată periodic;

c) OCSP — Online Certificate Status Protocol, serviciu de verificare în timp real a statusului certificatului (RFC 6960);

d) PKI — Public Key Infrastructure, infrastructura cheii publice a QSIGN (Root CA, Issuing CA, RA, OCSP responder, TSA);

e) QSCD — Qualified Signature/Seal Creation Device, dispozitiv calificat de creare a semnăturii/sigiliului, conform Anexei II la Reg. eIDAS;

f) TSA — Time-Stamping Authority, autoritate de marcare temporală, conform ETSI EN 319 421;

g) LoIP — Level of Identity Proofing, nivel de verificare a identității, conform ETSI TS 119 461;

h) LTP — Long-Term Preservation, conservarea pe termen lung a semnăturilor și a evidențelor, conform ETSI TS 119 511 / EN 319 522.

Articolul 4 — Acceptarea Termenilor și Condițiilor

(1) Prezentul document se comunică Utilizatorului final anterior emiterii certificatului sau prestării serviciului, prin publicare permanentă pe pagina **www.qsign.ro** și prin transmitere/punere la dispoziție în cadrul fluxului de înregistrare. Utilizatorul confirmă în mod expres acceptarea acestora prin bifarea opțiunii corespunzătoare în interfața de înregistrare, prin semnarea unui formular de acceptare sau prin orice altă modalitate echivalentă admisă de lege.

(2) Acceptarea Termenilor și Condițiilor reprezintă o condiție prealabilă obligatorie pentru emiterea oricărui certificat și pentru utilizarea oricărui serviciu de încredere prestat de QSIGN.

(3) Versiunea aplicabilă raportului juridic este cea în vigoare la momentul emiterii certificatului sau al prestării serviciului. Modificările ulterioare se comunică Utilizatorului conform art. 24 din prezentul document și nu afectează valabilitatea certificatelor deja emise, decât cu acordul expres al Titularului sau în condițiile legii.

PARTEA II — TERMENI ȘI CONDIȚII PENTRU SERVICII DE ÎNCREDERE NECALIFICATE

Servicii: emiterea de certificate pentru semnătura electronică avansată și gestionarea semnăturilor electronice la distanță.

Temei: art. 26 din Reg. eIDAS; art. 12 alin. (2), art. 15 alin. (2), art. 16 din Legea nr. 214/2024; art. 5 alin. (2) lit. i) din Anexa nr. 2 la Ordinul MEDAT nr. 102/2026.

Articolul 5 — Domeniul de aplicare

(1) Prezenta Parte se aplică serviciilor de încredere **necalificate** prestate de QSIGN, constând în emiterea, gestionarea, suspendarea, revocarea și înregistrarea certificatelor pentru semnătura electronică avansată în sensul art. 3 pct. 11 și art. 26 din Reg. eIDAS, precum și în servicii adiacente (validare, repository CRL/OCSP, marcare temporală necalificată — atunci când este oferită distinct).

(2) O semnătură electronică avansată îndeplinește, conform art. 26 din Reg. eIDAS, cumulativ următoarele cerințe: este legată în mod unic de semnatar, permite identificarea acestuia, este creată cu date pe care semnatarul le poate utiliza sub controlul său exclusiv cu un grad ridicat de încredere și este legată de datele semnate astfel încât orice modificare ulterioară a datelor poate fi detectată.

(3) Efectele juridice ale semnăturii avansate sunt cele prevăzute la art. 3 alin. (1), art. 4 alin. (3)–(5), (9) și art. 5 din Legea nr. 214/2024. În cazurile expres prevăzute la art. 4 alin. (5) lit. a)–c) din Legea nr. 214/2024, semnătura avansată produce **aceleași efecte juridice ca semnătura olografă**.

Articolul 6 — Procedura de creare și verificare a semnăturii

(1) Procedura de înregistrare include: (a) inițierea cererii pe portalul QSIGN sau prin API; (b) identificarea Solicitantului — fizic sau electronic la distanță, conform art. 16 alin. (3) din Legea nr. 214/2024; (c) verificarea de către QSIGN a documentelor și a identității; (d) generarea perechii de chei (de către Titular sau de QSIGN, după caz, conform CP/CPS); (e) emiterea certificatului și transmiterea acestuia prin canale securizate; (f) acceptarea certificatului de către Titular și înscrierea în Registrul electronic prevăzut la art. 14 din Legea nr. 214/2024.

(2) Identificarea Solicitantului se realizează prin oricare dintre modalitățile prevăzute la art. 16 alin. (3) din Legea nr. 214/2024, cu nivel minim Baseline LoIP conform ETSI TS 119 461, inclusiv prin: prezență fizică, certificat calificat valid, mijloace de identificare electronică notificate (eIDAS), proceduri video la distanță aprobate de ADR sau prin terț de verificare.

(3) Crearea semnăturii se realizează cu mijloace tehnice puse la dispoziție de QSIGN (semnare la distanță, prin platformă autentificată multifactor) sau cu mijloace ale Titularului (token/smart-card, semnare locală). În cazul semnării la distanță, controlul exclusiv al Titularului asupra datelor de creare este asigurat prin autentificare puternică (factor cunoscut + factor posedat) și autorizare per-tranzacție (Sole-Control Assurance Level conform CEN EN 419241-1).

(4) Verificarea semnăturii avansate se realizează conform mecanismului de validare descris la art. 30 din prezentul document.

Articolul 7 — Modalități, condiții și limite de utilizare

a) certificatul se utilizează exclusiv în scopul, pentru tipul de tranzacție și în limitele indicate în câmpurile keyUsage, extendedKeyUsage și qcStatements ale acestuia, precum și în limitele declarate în CP/CPS;

b) utilizarea certificatului în afara perioadei de valabilitate, după suspendare sau revocare, este interzisă și produce efectele art. 17 alin. (4) din Legea nr. 214/2024 (opozabilitate de la data înscrierii în Registrul electronic);

c) perioada maximă de valabilitate a certificatului pentru semnătura avansată este de 2 ani, conform art. 3 alin. (4) din Legea nr. 214/2024;

d) certificatul poate conține limitări valorice pentru tranzacții, opozabile terților dacă pot fi cunoscute (art. 15 alin. (5) din Legea nr. 214/2024);

e) certificatul nu se folosește pentru a semna acte juridice care, potrivit legii, impun forma autentică (art. 4 alin. (11) din Legea nr. 214/2024);

f) certificatul este personal și nu poate fi transferat, partajat sau utilizat de terți; cheile private nu se reproduc, nu se exportă, nu se divulgă.

Articolul 8 — Obligațiile QSIGN

QSIGN, ca prestator de servicii de încredere necalificate, asumă obligațiile prevăzute la art. 11 și 12 din Legea nr. 214/2024, inclusiv:

a) punerea la dispoziție a informațiilor necesare utilizării corecte și sigure a serviciilor, prin publicare pe www.qsign.ro;

b) verificarea cu mijloace corespunzătoare a identității și, dacă este cazul, a atributelor specifice ale Titularului;

c) menținerea unui registru electronic public, disponibil 24/7 online, cuprinzând data și ora exactă a eliberării, expirării, suspendării sau revocării certificatelor (art. 14 din Legea nr. 214/2024);

d) menținerea unui serviciu de suspendare și revocare, cu termen de procesare de cel mult 24 de ore;

e) utilizarea de personal cu cunoștințe de specialitate, experiență și calificare;

f) protejarea datelor cu caracter personal conform Regulamentului (UE) 2016/679 (GDPR) și Legii nr. 190/2018;

g) păstrarea informațiilor referitoare la certificate pentru o perioadă de minimum 10 ani de la încetarea valabilității acestora;

h) neconservarea, nereproducerea și nedezvăluirea către terți a datelor de creare a semnăturii, cu excepția cazului în care Titularul solicită aceasta;

i) menținerea unui plan actualizat de încetare a serviciului, comunicat ADR;

j) menținerea unui plan de acțiune actualizat pentru cazul producerii unui incident de securitate cibernetică;

k) utilizarea unei surse de timp precise, legate de UTC (a se vedea art. 11 alin. (3) lit. e) din prezentul document și descrierea soluției tehnice notificate ADR);

l) încheierea unei polițe de asigurare de răspundere civilă în valoare de minimum 100.000 EUR, conform art. 5 alin. (2) lit. b) din Anexa nr. 2 la Ordinul MEDAT nr. 102/2026.

Articolul 9 — Obligațiile Titularului

a) să furnizeze date complete, exacte și actuale în procesul de înregistrare;

b) să păstreze datele de creare a semnăturii și factorii de autentificare în mod securizat și să nu le divulge altor persoane (art. 26 alin. (1) din Legea nr. 214/2024);

c) să utilizeze certificatul exclusiv conform limitelor și scopului declarat;

d) să solicite revocarea certificatului în termen de cel mult 24 de ore (art. 26 alin. (2) din Legea nr. 214/2024) în oricare dintre cazurile: pierdere a datelor de creare a semnăturii, suspiciune de divulgare către un terț, schimbare a informațiilor esențiale cuprinse în certificat;

e) să verifice corectitudinea informațiilor cuprinse în certificat la momentul acceptării și să sesizeze QSIGN cu privire la orice neconcordanță;

f) să respecte termenii prezentului document, CP/CPS aplicabile și legislația în vigoare.

Articolul 10 — Conținutul certificatului

(1) Certificatul pentru semnătura electronică avansată cuprinde elementele prevăzute la art. 15 alin. (2) lit. a)–j) din Legea nr. 214/2024 și se conformează profilului ETSI EN 319 412-1/-2/-5: indicarea calității de certificat pentru semnătura avansată, datele de identificare a QSIGN și statul membru, numele/pseudonimul Titularului, datele de verificare a semnăturii, perioada de valabilitate, codul de identificare, limitele de utilizare (după caz) și semnătura/sigiliul electronic al CA emitente.

(2) La solicitarea Titularului, QSIGN poate înscrie informații suplimentare, după verificarea exactității acestora.

(3) Atunci când Titularul utilizează un pseudonim, certificatul indică expres acest fapt; identitatea reală nu se divulgă decât cu consimțământul Titularului sau la cererea autorităților competente.

Articolul 11 — Suspendarea și revocarea certificatului

(1) Suspendarea — QSIGN suspendă certificatul în termen de cel mult 24 de ore, conform art. 17 alin. (1) din Legea nr. 214/2024, în următoarele situații: la cererea Titularului (după verificarea identității); prin hotărâre judecătorească; când informațiile din certificat nu mai corespund realității, dacă nu se impune revocarea; la solicitarea justificată a ADR; în orice alte cazuri prevăzute de CP/CPS.

(2) Revocarea — QSIGN revocă certificatul în termen de cel mult 24 de ore, conform art. 17 alin. (2) din Legea nr. 214/2024, în următoarele situații: cererea Titularului; decesul Titularului; hotărâre judecătorească definitivă; certificat emis pe baza de informații eronate sau false; informații esențiale care nu mai corespund realității; compromiterea confidențialității datelor de creare; utilizare frauduloasă; incident de securitate care ar putea compromite certificatul; alte situații prevăzute de CP/CPS sau de Regulamentul eIDAS.

(3) Cererile de suspendare/revocare se transmit la **revocare@qsign.ro**, telefonic la **0724.167.333** (24/7) sau prin portalul de management al certificatului. Suspendarea/revocarea devin opozabile terților de la data înscrierii în Registrul electronic și a publicării în CRL/OCSP, în termen de cel mult 24 de ore de la decizie.

(4) QSIGN informează prompt Titularul cu privire la suspendare/revocare, motivele acesteia, și acordă dreptul de a solicita verificarea deciziei.

Articolul 12 — Răspunderea și limitări

(1) QSIGN răspunde, conform art. 13 din Reg. eIDAS și art. 30 din Legea nr. 214/2024, pentru prejudiciile cauzate prin încălcarea obligațiilor sale, inclusiv pentru: exactitatea informațiilor din certificat la momentul emiterii; corespondența dintre datele de creare și datele de verificare a semnăturii (când le generează pe ambele); suspendarea/revocarea în condițiile legii; îndeplinirea obligațiilor prevăzute la art. 11–12 din Legea nr. 214/2024.

(2) QSIGN nu răspunde pentru: utilizarea certificatului cu nerespectarea limitelor înscrise în acesta și opozabile terților; prejudicii rezultând din nedivulgarea unei revocări care nu fusese încă cerută de Titular; folosirea frauduloasă a datelor de creare aflate în controlul exclusiv al Titularului; cazuri de forță majoră sau caz fortuit.

(3) Răspunderea contractuală a QSIGN față de Utilizator pentru orice cerere derivată din prezentul document, în lipsa unei culpe grave sau a faptei intenționate, este limitată la valoarea tarifelor încasate pentru serviciul în cauză în ultimele 12 luni anterior evenimentului care a generat răspunderea, fără a aduce atingere răspunderii legale față de terți, garantată prin polița de asigurare prevăzută la art. 8 lit. l).

Articolul 13 — Tarife

(1) Tarifele aplicabile se publică pe **www.qsign.ro/preturi** și fac parte integrantă din raportul contractual la momentul contractării. Modificările tarifare nu se aplică retroactiv certificatelor deja emise.

(2) Plata se efectuează anticipat, prin mijloacele indicate în interfața QSIGN sau în factura aferentă, în RON, cu TVA conform legii. Neefectuarea plății în termenul stabilit poate atrage suspendarea sau, după caz, neemiterea certificatului.

Articolul 14 — Confidențialitate și prelucrarea datelor cu caracter personal

(1) QSIGN colectează și prelucrează datele cu caracter personal ale Solicitanților/Titularilor în condițiile Regulamentului (UE) 2016/679 (GDPR), Legii nr. 190/2018 și ale Legii nr. 506/2004, conform **Politicii de confidențialitate** publicate pe **www.qsign.ro/gdpr**. Temeiurile prelucrării sunt: executarea contractului, obligația legală (art. 11 alin. (6) și art. 12 din Legea nr. 214/2024) și interesul legitim al QSIGN privind securitatea serviciului.

(2) Datele de identificare, sesiunile video, jurnalele și evidențele aferente certificării sunt păstrate timp de minimum 10 ani de la încetarea valabilității certificatului (art. 12 alin. (2) lit. i) din Legea nr. 214/2024).

(3) Drepturile persoanei vizate (acces, rectificare, ștergere — în limita obligațiilor legale de păstrare, restricționare, opoziție, portabilitate, plângere la ANSPDCP) se exercită la **dpo@qsign.ro**.

(4) Personalul QSIGN păstrează secretul profesional asupra informațiilor încredințate, cu excepția celor publice, a celor pentru care Titularul a consimțit divulgarea, sau a celor solicitate de autoritățile competente potrivit legii.

PARTEA IV — DESCRIEREA DETALIATĂ A MECANISMULUI DE VALIDARE A SEMNĂTURII AVANSATE

Temei: art. 5 alin. (2) lit. i) teza finală din Anexa nr. 2 la Ordinul MEDAT nr. 102/2026 — descrierea detaliată a mecanismului de validare a semnăturii avansate, în cazul în care nu a fost solicitată aprobarea acestuia de către ADR conform Anexei nr. 5 la Ordin.

> *QSIGN nu a solicitat aprobarea ADR pentru un mecanism de validare distinct conform Anexei nr. 5 la Ordinul MEDAT nr. 102/2026. Mecanismul de validare descris în prezenta Parte se bazează exclusiv pe standardele europene de referință și pe metodele de validare publicate de ADR, conform art. 5 alin. (2) lit. a) din Legea nr. 214/2024.*

Articolul 29 — Cadrul standardizat de validare

Mecanismul de validare a semnăturii electronice avansate cu certificat, prestat și recomandat de QSIGN, este conform integral cu următoarele standarde și specificații europene de referință:

a) ETSI EN 319 102-1 — „Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation" — definește procesul standardizat de validare în 4 etape: **Format Checking** → **Identification** → **Validation Process for Basic Signatures** → **Validation Process for Signatures with Time and Signatures with Long-Term Validation Material**;

b) ETSI TS 119 102-2 — „Validation Report for Signature Validation"; structura raportului de validare;

c) ETSI TS 119 101 — „Policy and security requirements for applications for signature creation and signature validation";

d) ETSI EN 319 122 (CAdES), 132 (XAdES), 142 (PAdES), 162 (ASiC) — formatele de semnătură avansată susținute (CMS Advanced Electronic Signatures, XML Advanced Electronic Signatures, PDF Advanced Electronic Signatures, Associated Signature Containers);

e) RFC 5280 — „Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" — algoritmul de validare a lanțului de certificare (path discovery and validation);

f) RFC 6960 — „Online Certificate Status Protocol (OCSP)";

g) Reg. de punere în aplicare (UE) 2025/1.945 — privind validarea semnăturilor electronice calificate și a sigiliilor electronice calificate și validarea semnăturilor electronice avansate bazate pe certificate calificate;

h) Reg. de punere în aplicare (UE) 2026/248 — privind formatele semnăturilor electronice avansate care trebuie recunoscute de organismele din sectorul public.

Articolul 30 — Procesul de validare în 4 etape

30.1 Etapa 1 — Verificarea formatului

Sistemul de validare verifică sintactic semnătura primită, identifică formatul (CAdES, XAdES, PAdES, ASiC), nivelul (B-B, B-T, B-LT, B-LTA) conform **ETSI EN 319 122/132/142** și extrage componentele structurale: **SignedData**, certificate atașate, atribute semnate (signed attributes), atribute nesemnate (unsigned attributes), token-uri de timp (signature-time-stamp), informații de revocare (revocation values), referințe complete (complete-certificate-references, complete-revocation-references). Erorile de format produc un rezultat **INDETERMINATE** cu cod **FORMAT_FAILURE**.

30.2 Etapa 2 — Identificarea semnatarului

Sistemul identifică certificatul semnatarului din câmpul **SignerInfo.sid** (issuer/serial sau SubjectKeyIdentifier) și extrage: numele/pseudonimul, datele de verificare a semnăturii (cheia publică), perioada de valabilitate, OID-ul politicii, qcStatements (esi4-qcStatement-1, qcCompliance), keyUsage și extendedKeyUsage. Certificatul se verifică sintactic conform **RFC 5280** și a profilului ETSI EN 319 412.

30.3 Etapa 3 — Validarea semnăturii de bază (Basic Signature Validation)

Această etapă, principală în validare, cuprinde sub-procese detaliate, executate în ordinea logică:

a) X.509 Certificate Path Validation — construirea și validarea lanțului de certificate de la certificatul semnatarului până la o ancoră de încredere (Trust Anchor), conform **RFC 5280 §6.1**. Trust Anchor-urile sunt: (i) certificatele Root CA ale QSIGN; (ii) certificatele prestatorilor calificați europeni publicate în Listele Sigure (Trusted Lists) ale statelor membre UE și agregate în **LOTL** (List of Trusted Lists) publicate de Comisia Europeană conform Deciziei (UE) 2015/1.505, cu modificările aduse prin Decizia (UE) 2025/2.164. Verificările includ: nume distinctiv (DN) chain matching, perioada de valabilitate la momentul semnării, semnătura emitentului, conformitatea Basic Constraints (cA=true pentru CA), Key Usage (digitalSignature/nonRepudiation pentru EE) și politicile de certificate.

b) Verificarea statusului de revocare — pentru fiecare certificat din lanț (cu excepția Trust Anchor-ului), se verifică statusul revocării prin: (i) interogare **OCSP** (RFC 6960) la URL-ul indicat în extensia **AuthorityInformationAccess.id-ad-ocsp**; (ii) descărcarea și verificarea **CRL** indicate în extensia **CRLDistributionPoints**. Răspunsurile OCSP/CRL trebuie să fie semnate, valide și actuale la momentul validării. Pentru semnături B-LT/B-LTA, se utilizează informațiile de revocare incorporate (revocation values) — **grace period** aplicat conform politicilor pentru a permite includerea ulterioară a informațiilor de revocare;

c) Verificarea integrității criptografice — verificarea semnăturii efective asupra **SignedAttributes** (CAdES) sau **SignedInfo** (XAdES) ori a digestului obiectelor semnate (PAdES) folosind cheia publică din certificat, cu algoritmii recomandați **ENISA** și conformi cu **ETSI TS 119 312** (RSA ≥ 3072 sau ECDSA cu curbe NIST P-256/-384/-521 sau Brainpool, hash SHA-256 / SHA-384 / SHA-512). Algoritmii deprecați (MD5, SHA-1, RSA-1024) determină respingerea semnăturii cu rezultat **INVALID/CRYPTO_CONSTRAINTS_FAILURE**.

d) Verificarea atributelor semnate — **contentType**, **messageDigest** (consistent cu obiectele semnate), **signing-time** (atribut), **signing-certificate-v2** (referința la certificat conform RFC 5035 / ETSI), **signature-policy-identifier** (când este aplicabilă o politică de semnare).

30.4 Etapa 4 — Validarea cu element temporal (Time / Long-Term)

Pentru semnături cu nivel B-T, B-LT sau B-LTA, se efectuează verificări suplimentare pentru a stabili momentul aplicării semnăturii și pentru a permite validarea după expirarea sau revocarea certificatului:

a) Validarea token-urilor de timp — fiecare **signature-time-stamp** (CAdES) / XML time-stamp (XAdES) / DSS-DOC-TIMESTAMP (PAdES) este validat ca semnătură independentă conform **ETSI EN 319 422**, cu lanț de încredere până la TSA Trust Anchor (calificat sau necalificat conform politicii). Token-ul stabilește limita superioară (POE — Proof of Existence) a momentului semnării.

b) Past Signature Validation — algoritmul prevăzut la **ETSI EN 319 102-1 §5.6** care permite validarea unei semnături după expirarea/revocarea certificatului, prin reconstrucția stării certificatelor și a algoritmilor la momentul semnării (atestat de POE), folosind: (i) informațiile de revocare incorporate în signature; (ii) marca temporală a semnăturii; (iii) marcaje temporale de arhivare ulterioare (archive-time-stamp pentru B-LTA).

c) Long-Term Availability and Integrity (LTV) — pentru documente cu nivel **B-LTA**, fiecare archive-time-stamp re-protejează criptografic întregul ansamblu (semnătură + atribute + chain + revocation data + token-uri anterioare). Verificarea unei semnături LTA validează lanțul recursiv de archive-time-stamps și permite admisibilitatea probatorie chiar și după depășirea termenului de valabilitate al algoritmilor inițiali.

Articolul 31 — Surse de informații de încredere și surse de timp

Mecanismul de validare se bazează pe următoarele surse de încredere și de timp:

a) Trusted List României — Lista Sigură publicată de ADR conform art. 22 din Reg. eIDAS și Deciziei (UE) 2015/1.505;

b) **LOTL — List of Trusted Lists** — agregator european publicat de Comisia Europeană la **https://ec.europa.eu/tools/lotl/eu-lotl.xml**, semnat și actualizat periodic;

c) **Surse de timp** — minimum 3 surse stratum-1 NTP cu trasabilitate la UTC(k), gestionate de NMI europene/internaționale: **PTB (Germania)** — **ptbtime1-4.ptb.de** (NTP/NTS, RFC 8915), trasabilitate UTC(PTB); **NIST (SUA)** — **time.nist.gov** și time-a-g/time-b-g, trasabilitate UTC(NIST); **INRIM (Italia)** — **ntp1.inrim.it**, **ntp2.inrim.it**, trasabilitate UTC(IT). Configurația respectă RFC 5905 (NTPv4) și — unde este suportat — RFC 8915 (Network Time Security). Offset-ul față de UTC este monitorizat continuu.

Articolul 32 — Rezultate posibile ale validării

Conform **ETSI EN 319 102-1** și **ETSI TS 119 102-2**, rezultatul validării este unul dintre cele trei statusuri principale, însoțit de sub-coduri de indicație și de sub-indicație:

Status principal	Semnificație	Sub-coduri (Sub-Indication) frecvente
TOTAL_PASSED	Semnătură valabilă, integritate confirmată, certificat valid la momentul semnării.	—
TOTAL_FAILED	Semnătură invalidă: integritate compromisă, certificat revocat la semnare, algoritm respins.	HASH_FAILURE; SIG_CRYPTO_FAILURE; REVOKED; REVOKED_NO_POE
INDETERMINATE	Validitatea nu poate fi stabilită cu informațiile disponibile; nu este invalidă, dar nu poate fi confirmată.	TRY_LATER; OUT_OF_BOUNDS_NO_POE; CRYPTO_CONSTRAINTS_FAILURE_NO_POE; NO_CERTIFICATE_CHAIN_FOUND; CHAIN_CONSTRAINTS_FAILURE; CERTIFICATE_CHAIN_GENERAL_FAILURE; SIGNED_DATA_NOT_FOUND; FORMAT_FAILURE

Articolul 33 — Raportul de validare

Pentru fiecare validare, sistemul QSIGN generează un raport conform ETSI TS 119 102-2, care cuprinde minimum:

a) identificatorul tranzacției de validare și momentul UTC al efectuării;

b) rezultatul (TOTAL_PASSED / TOTAL_FAILED / INDETERMINATE) și sub-codul detaliat;

c) identificarea semnatarului (DN, serial, issuer);

d) datele certificatului (perioada de valabilitate, qcStatements, keyUsage);

e) lanțul de certificare reconstituit, până la Trust Anchor;

f) sursa și momentul probelor de revocare (OCSP/CRL) utilizate;

g) token-urile de timp utilizate și TSA emitentă;

h) algoritmii și parametrii criptografici evaluați și concluzia privind robustețea acestora;

i) identificarea politicii/standardelor aplicate pentru validare;

j) semnătura calificată sau sigiliul calificat al QSIGN aplicat raportului, asigurând autenticitatea și integritatea acestuia.

Articolul 34 — Disponibilitatea informațiilor de stare a certificatelor

(1) Informațiile despre starea certificatelor emise de QSIGN sunt disponibile 24/7 prin: OCSP responder la http://ocsp.qsign.ro (acces public, fără autentificare); CRL repository la http://crl.qsign.ro.

(2) SLA-ul țintit pentru serviciul de verificare a stării certificatelor este: disponibilitate ≥ 99,5% pentru servicii necalificate (≥ 99,95% pentru servicii calificate, după acordarea statutului calificat); timp de răspuns OCSP < 1 secundă (P95); CRL refresh la cel mult 24 ore.

Articolul 35 — Auditul, conformitatea și actualizarea mecanismului

(1) Mecanismul de validare descris este supus auditului efectuat de un auditor înscris în **Lista auditorilor de securitate cibernetică valabil atestați (LASC)** din cadrul DNSC, conform **ETSI EN 319 403-1 V2.3.1** și a cerințelor din Anexa nr. 2 la Ordinul MEDAT nr. 102/2026.

(2) Mecanismul se actualizează ori de câte ori intervin modificări semnificative ale arhitecturii tehnice (motoare de semnătură, module criptografice, mecanisme de autentificare, fluxuri de procesare sau interfețe critice), cu notificarea ADR cu cel puțin 10 zile calendaristice anterior implementării și efectuarea unui nou audit anterior reluării serviciului, conform art. 8 alin. (3) din Anexa nr. 2 la Ordinul MEDAT nr. 102/2026.

(3) QSIGN își rezervă dreptul de a solicita ulterior aprobarea ADR pentru mecanismul de validare conform Normelor de aprobare a mecanismelor de validare aprobate prin Anexa nr. 5 la Ordinul MEDAT nr. 102/2026; în acest caz, prezenta descriere se va completa și/sau înlocui cu mecanismul aprobat.

Întocmit și certificat,

QSIGN S.R.L.
prin Administrator **Trandafirescu Alexandru Florin**

Data: 06.05.2026

Semnătura electronică calificată:

_____