QSIGN S.R.L.

Prestator de servicii de încredere — Trust Service Provider (TSP)

POLITICA DE CERTIFICARE (CP)

ȘI

CODUL DE PRACTICI ȘI PROCEDURI (CPS)

SERVICII DE ÎNCREDERE CALIFICATE

Aplicabil(e):

• Certificate calificate pentru semnătura electronică (QCP-n, QCP-n-qscd)

• Certificate calificate pentru sigiliul electronic (QCP-l, QCP-l-qscd)

• Marcă temporală electronică calificată (QTSA — Anexa Politica TSA)

INFORMAȚII DOCUMENT

Denumire document	Politica de Certificare și Codul de Practici și Proceduri — Servicii Calificate
Cod intern	QSIGN-CP-CPS-QC-v1.0
Versiune	1.0
Data publicării	06.05.2026
Data intrării în vigoare	06.05.2026

Stare	Aprobat (versiune pentru depunere ADR — Anexa 1 la Ordinul MEDAT nr. 102/2026)
Clasificare	Public
Aprobat de	Policy Management Authority (PMA) — QSIGN S.R.L.
Limba originală	Română (cu termeni tehnici bilingvi RO/EN)
Cadru de structurare	RFC 3647 — Internet X.509 PKI Certificate Policy and Certification Practices Framework
Conformitate principală	Reg. (UE) 910/2014 (eIDAS), modificat prin Reg. (UE) 2024/1183 (eIDAS 2.0); Legea nr. 214/2024; Ordin MEDAT nr. 102/29.01.2026 (Anexa 1); Decizia ADR nr. 162/20.03.2026 (Anexa 2); ETSI EN 319 401 v3.1.1+; ETSI EN 319 411-1 v1.4.1+; ETSI EN 319 411-2 v2.5.1+; ETSI EN 319 412 părțile 1–5; ETSI TS 119 461 v2.1.1+; ETSI EN 319 421/422 (TSA)

CUPRINS

Preambul și domeniu de aplicare

Prezentul document conține, în formă combinată conform RFC 3647 §3.4, Politica de Certificare (Certificate Policy — CP) și Codul de Practici și Proceduri (Certification Practice Statement — CPS) ale QSIGN S.R.L., aplicabile exclusiv serviciilor de încredere CALIFICATE prestate în temeiul Regulamentului (UE) nr. 910/2014, modificat prin Regulamentul (UE) 2024/1183, al Legii nr. 214/2024, al Ordinului ministrului economiei, digitalizării, antreprenoriatului și turismului nr. 102 din 29 ianuarie 2026 (Anexa 1) și al Deciziei Autorității pentru Digitalizarea României nr. 162 din 20 martie 2026 (Anexa 2).

Documentul acoperă următoarele tipuri de servicii de încredere calificate prestate de QSIGN:

- **(i) emiterea și gestionarea certificatelor calificate pentru semnătura electronică** (art. 28 și Anexa I la Reg. (UE) 910/2014), cu și fără QSCD (politici QCP-n, QCP-n-qscd);
- **(ii) emiterea și gestionarea certificatelor calificate pentru sigiliul electronic** (art. 38 și Anexa III la Reg. (UE) 910/2014), cu și fără QSCD (politici QCP-l, QCP-l-qscd);
- **(iii) gestionarea dispozitivelor calificate de creare a semnăturilor și sigiliilor electronice la distanță (remote QSCD)** ca serviciu de încredere calificat distinct, conform art. 29a și 39a introduse prin Reg. (UE) 2024/1183 și Reg. de punere în aplicare (UE) 2025/1567.
- **(iv) emiterea de mărci temporale electronice calificate (QTSA)** în conformitate cu art. 42 din Reg. (UE) 910/2014. Politica TSA detaliată se publică ca document anexă (QSIGN-TSA-Policy), referențiată în prezentul CP/CPS.

Serviciile de încredere necalificate prestate de QSIGN (certificate pentru semnătura electronică avansată — politici NCP, NCP+, LCP) fac obiectul unui document separat (QSIGN-CP-CPS-AC-v1.0).

Identificarea documentului și OID-uri

Acest document este identificat unic prin OID atribuit în arborele OID al QSIGN. Politicile specifice tipurilor de certificate emise sunt aliniate cu identificatorii standardizați ETSI și sunt înregistrate cu OID-uri proprii.

Arborele OID QSIGN

QSIGN va opera sub un Private Enterprise Number (PEN) IANA propriu, înregistrat în arborele 1.3.6.1.4.1. Pentru documentele aflate în curs de înregistrare la momentul depunerii, este utilizat un OID provizoriu în formatul 1.3.6.1.4.1.59019; PEN-ul efectiv va fi înregistrat și actualizat în acest document anterior emiterii primului certificat în producție.

Element	Valoare	Descriere
Arc rădăcină QSIGN	1.3.6.1.4.1.59019	Spațiul OID propriu al QSIGN S.R.L.
Documente politici	1.3.6.1.4.1.59019.1	CP, CPS, Termeni și condiții
Politici certificate (CP)	1.3.6.1.4.1.59019.2	OID-uri politici de certificat
Politici TSA	1.3.6.1.4.1.59019.3	Politici Time-Stamping (QTSA)
Politici validare/conservare	1.3.6.1.4.1.59019.4	Servicii de validare și păstrare LTP

OID-uri politici aplicate (servicii calificate)

Tip certificat / serviciu	OID politică ETSI standard	OID politică QSIGN
Certificat calificat semnătură electronică — persoană fizică (QCP-n)	0.4.0.194112.1.0	1.3.6.1.4.1.59019.2.2.1
Certificat calificat semnătură electronică — persoană fizică, cu QSCD (QCP-n-qscd)	0.4.0.194112.1.2	1.3.6.1.4.1.59019.2.2.2
Certificat calificat sigiliu electronic — persoană juridică (QCP-l)	0.4.0.194112.1.1	1.3.6.1.4.1.59019.2.3.1
Certificat calificat sigiliu electronic — persoană juridică, cu QSCD (QCP-l-qscd)	0.4.0.194112.1.3	1.3.6.1.4.1.59019.2.3.2
Politică QTSA (marcă temporală calificată) — referință în Anexă	0.4.0.2023.1.1 (BTSP) / specifică QSIGN	1.3.6.1.4.1.59019.3.1

Convenții de redactare

Termenii englezi sunt utilizați pentru a păstra conformitatea cu vocabularul tehnic standardizat ETSI/IETF; corespondentul în limba română este indicat la prima utilizare. Verbele "trebuie", "este obligat", "va" exprimă cerințe normative; "poate" exprimă facultăți. Trimiterile la articole din Regulamentul (UE) nr. 910/2014 sunt făcute la versiunea consolidată după Reg. (UE) 2024/1183. Trimiterile la standardele ETSI sunt făcute la versiunile în vigoare la data aprobării prezentului document, urmând regula de versiune mobilă ("sau ulterioare"), cu evaluare a substanței conformității la auditurile periodice.

1. Introducere

1.1 Prezentare generală

QSIGN S.R.L. (denumită în continuare "QSIGN" sau "TSP") este o societate comercială română înregistrată la Oficiul Registrului Comerțului sub nr. J2024010825402, având cod unic de înregistrare fiscală 34633481, cu sediul social în București, str. Drumea Rădulescu, nr. 26, sector 4, care prestează servicii de încredere calificate în sensul Regulamentului (UE) nr. 910/2014, modificat și completat prin Reg. (UE) 2024/1183.

QSIGN operează o infrastructură de chei publice (PKI) proprie, având ca scop emiterea și gestionarea serviciilor de încredere calificate enumerate în Preambul. Toate serviciile sunt proiectate pentru a îndeplini cumulativ cerințele eIDAS, Legii 214/2024, Ordinului MEDAT 102/2026 (Anexa 1), Deciziei ADR 162/2026 (Anexa 2) și standardelor ETSI relevante, în vederea recunoașterii transfrontaliere automate în Spațiul Economic European prin includerea în Lista sigură (Trusted List) națională publicată de ADR.

1.1.1 Scopul Politicii de Certificare (CP)

Politica de Certificare stabilește regulile, principiile și cerințele aplicabile certificatelor calificate emise de QSIGN. CP indică, pentru fiecare tip de certificat: (i) condițiile de eligibilitate ale solicitanților; (ii) cerințele de identificare și verificare a identității; (iii) drepturile, obligațiile și răspunderile părților; (iv) limitele de utilizare; (v) profilul tehnic al certificatului; (vi) modalitățile de revocare, suspendare și reînnoire.

1.1.2 Scopul Codului de Practici și Proceduri (CPS)

Codul de Practici și Proceduri descrie practicile concrete prin care QSIGN implementează politica/politicile de certificare. CPS detaliază procesele operaționale, controalele tehnice și organizatorice, infrastructura fizică, măsurile criptografice, procedurile de înregistrare, emitere, revocare și gestiune a ciclului de viață al certificatelor, în conformitate cu cerințele ETSI EN 319 401 și ETSI EN 319 411-1 (cerințe generale) și ETSI EN 319 411-2 (cerințe specifice certificatelor calificate UE).

1.1.3 Relația cu alte documente

Acest CP/CPS constituie documentul-cadru al QSIGN pentru servicii calificate. Documentele subordonate, care formează corpul documentar complet al TSP-ului, includ: PKI Disclosure Statement (PDS); Politica de Securitate a Informațiilor; Planul de Securitate al Sistemului Informatic; Planul de Continuitate a Activității și Recuperare în Caz de Dezastru (BCP/DRP); Planul de Încetare a Activității (Termination Plan, conform art. 24 alin. (2) lit. (i) eIDAS); Documentația de evaluare a riscurilor (art. 24 eIDAS); Procedura de notificare a incidentelor (art. 19 alin. (2) eIDAS); Subscriber Agreement / Relying Party Agreement / Termeni și condiții; Politica TSA (QTSA Policy); Politica de validare și conservare. Toate aceste documente sunt elaborate consistent cu prezentul CP/CPS și sunt aprobate de Policy Management Authority (PMA).

1.2 Numele și identificarea documentului

Titlu	QSIGN — Politica de Certificare și Codul de Practici și Proceduri — Servicii Calificate
Cod intern	QSIGN-CP-CPS-QC-v1.0

OID document	1.3.6.1.4.1.59019.1.1.1.0
Versiune	1.0
Tip	Document combinat CP + CPS, conform RFC 3647 §3.4
Aplicabilitate	Servicii de încredere CALIFICATE: certificate calificate de semnătură (QCP-n, QCP-n-qscd), certificate calificate de sigiliu (QCP-l, QCP-l-qscd), gestiune QSCD la distanță, mărci temporale calificate (referință la Politica TSA)
Limba	Română
Versiune publică	Disponibilă pe https://www.qsign.ro/repository, în PDF semnat cu sigiliu calificat și marcat temporal calificat

1.3 Participanți la PKI

1.3.1 Autorități de Certificare (Certification Authorities — CAs)

QSIGN operează o ierarhie PKI cu separare strictă între nivelul rădăcină (Root CA) și nivelul emitent (Issuing CAs). Această separare urmărește limitarea expunerii cheii rădăcină, îmbunătățirea rezilienței la compromitere și posibilitatea introducerii de noi CA-uri emitente fără re-emiterea ancorei de încredere.

Nivel	Denumire	Funcție
Root	QSIGN Root CA G1	Ancora de încredere; emite exclusiv certificate pentru CA-uri subordonate; off-line, în airgap
Issuing — Calificat	QSIGN Qualified Signature CA G1	Emite certificate calificate pentru semnătură electronică (QCP-n, QCP-n-qscd)
Issuing — Calificat	QSIGN Qualified Seal CA G1	Emite certificate calificate pentru sigiliu electronic (QCP-l, QCP-l-qscd)
Calificat — TSA	QSIGN Qualified TSA G1	Emite mărci temporale calificate (art. 42 eIDAS); cheie separată
Calificat — OCSP	QSIGN Qualified OCSP Responder G1 (per Issuing CA)	Răspuns OCSP semnat (RFC 6960), cu rotație frecventă a cheii

Caracteristicile Root CA

- Stocată exclusiv în HSM (Hardware Security Module) certificat FIPS 140-3 Nivel 3 sau Common Criteria EAL 4+ AVA_VAN.5 (echivalent EN 419 221-5).
- Operată în airgap fizic; activarea cheii necesită cvorum dual (m-of-n, minimum 3 din 5 deținători de smart card).
- Algoritm și lungime: RSA 4096 biți (recomandat) sau ECDSA P-384 (alternativă).
- Hash: SHA-384 sau SHA-512.
- Validitate: 20 ani.
- CRL: emis o dată la 6 luni sau imediat la revocarea unei sub-CA.

Caracteristicile Issuing CA-urilor calificate

- HSM-uri certificate Common Criteria EAL 4+ AVA_VAN.5 / EN 419 221-5 (compatibile QSCD pentru gestiune QSCD la distanță, conform EN 419 241-2).

- Operate online, în clusters geografic redundante (centrul de date primar și DR).
- Algoritm și lungime: RSA 4096 biți (recomandat) sau ECDSA P-384.
- Validitate certificat: 10 ani; re-key planificat la 7 ani (overlap 3 ani).

1.3.2 Autoritate de Înregistrare (Registration Authority — RA)

RA este componenta funcțională a TSP-ului responsabilă cu primirea cererilor, verificarea identității solicitanților, validarea atributelor incluse în certificat, păstrarea înregistrărilor de identificare și transmiterea cererii aprobate către Issuing CA pentru emitere. QSIGN operează RA atât în mod centralizat cât și descentralizat, prin Local Registration Authorities (LRAs) contractate, supravegheate direct de QSIGN. Toate componentele LRA sunt obligate, prin contract și prin politica de securitate aplicabilă, să respecte cerințele ETSI EN 319 411-1 (clauza 6.2), ETSI EN 319 411-2 și ETSI TS 119 461 pentru identity proofing. Lista LRA-urilor active este publicată în repository-ul QSIGN.

1.3.3 Subscribers (Titulari de certificate)

Titularul (Subscriber) este persoana fizică sau juridică în numele căreia este emis certificatul calificat:

- Pentru certificate QCP-n / QCP-n-qscd — persoane fizice identificate în câmpul Subject (givenName, surname, serialNumber).
- Pentru certificate QCP-l / QCP-l-qscd — persoane juridice identificate în câmpul Subject (organizationName, organizationIdentifier conform ETSI EN 319 412-1).

1.3.4 Relying Parties (Părți utilizatoare)

Relying Party este orice persoană fizică sau juridică ce, în mod rezonabil, se bazează pe un certificat calificat emis de QSIGN în luarea unei decizii sau efectuarea unei acțiuni. Drepturile și obligațiile părților utilizatoare sunt detaliate în Relying Party Agreement publicat de QSIGN și în Capitolul 9 al prezentului document.

1.3.5 Alte participanți

- **Conformity Assessment Bodies (CAB)** acreditați conform Reg. (CE) 765/2008 și ETSI EN 319 403-1, care efectuează evaluările de conformitate eIDAS la fiecare 24 luni.
- **ADR** — Autoritatea pentru Digitalizarea României, organism național de supraveghere desemnat conform art. 19 din Legea 214/2024.
- **DNSC** — Directoratul Național de Securitate Cibernetică, autoritate națională de securitate cibernetică.
- **ANSPDCP** — Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal.
- Furnizori de servicii de încredere parteneri (cross-certification, agregatori de validare LOTL, prestatori de arhivă electronică calificată conform Legii 135/2007).

1.4 Utilizarea certificatelor

1.4.1 Utilizări permise

1.4.1.1 Certificate calificate pentru semnătura electronică (QCP-n, QCP-n-qscd)

Certificatele calificate pentru semnătura electronică emise de QSIGN respectă cerințele art. 28 și Anexei I la Regulamentul (UE) nr. 910/2014. Atunci când datele de creare a semnăturii sunt deținute într-un

dispozitiv calificat de creare a semnăturii electronice (Qualified Signature Creation Device — QSCD) conform art. 30 și Anexei II — caz aplicabil pentru politica QCP-n-qscd — semnătura produsă este o semnătură electronică calificată (QES) care, potrivit art. 25 alin. (2) eIDAS și art. 4 alin. (1) din Legea nr. 214/2024, are efectul juridic echivalent al semnăturii olografe și este recunoscută în toate statele membre UE.

Aplicații tipice: semnarea actelor juridice care necesită formă scrisă ad validitatem; înscrisuri sub semnătură privată; depunerea declarațiilor fiscale; încheierea contractelor cu autoritățile publice; documente bancare și notariale electronice; registre electronice de stare civilă; dosare de instanță electronice.

1.4.1.2 Certificate calificate pentru sigiliul electronic (QCP-l, QCP-l-qscd)

Certificatele calificate pentru sigiliul electronic emise de QSIGN respectă cerințele art. 38 și Anexei III la Regulamentul (UE) nr. 910/2014, fiind asociate persoanelor juridice. Sigiliul electronic calificat se bucură de prezumția de integritate a datelor și de corectitudine a originii datelor cu care este asociat, conform art. 35 alin. (2) eIDAS.

Aplicații tipice: facturi electronice (e-Factura); sigilarea automată a documentelor emise de organizații (rapoarte, certificate, atestate); API-uri securizate cu autentificare bazată pe sigiliu; sisteme de arhivare electronică (sigilarea pachetelor de arhivare); marcă temporală (TSA-ul însuși operează cu certificat de sigiliu); notificări electronice oficiale.

1.4.2 Utilizări interzise

- Utilizarea certificatelor pentru scopuri ilegale, inclusiv pentru încălcarea drepturilor de proprietate intelectuală sau pentru fraudă.
- Utilizarea certificatelor calificate de semnătură/sigiliu pentru autentificarea unui site web (TLS/SSL) — pentru aceasta este necesar un certificat QWAC distinct, conform art. 45 eIDAS.
- Utilizarea certificatelor de tip QCP-l (sigiliu) pentru semnarea actelor juridice care necesită semnătura unei persoane fizice.
- Utilizarea certificatelor după expirarea termenului de valabilitate sau după revocare/suspendare.
- Utilizarea certificatelor pentru CA-uri subordonate, autorități de timestamping sau alte componente PKI care emit, la rândul lor, certificate (cu excepția cazurilor explicite de cross-certification aprobate de PMA).
- Utilizarea cheilor private în alte dispozitive decât cele autorizate prin politica certificatului (de ex. extragerea cheii dintr-un QSCD în software).

1.5 Administrarea politicii

1.5.1 Organizația care administrează documentul

Denumire	QSIGN S.R.L.
Adresă	Str. Drumea Rădulescu, nr. 26, sector 4, București, România
CUI / J	34633481 / J2024010825402
E-mail (general)	alex@qsign.ro
E-mail (incidente)	incident@qsign.ro

E-mail (revocare)	revoke@qsign.ro
Telefon	+40 724 167 333
Web (repository)	https://www.qsign.ro/repository
Reprezentant legal	Trandafirescu Alexandru Florin — Administrator

1.5.2 Persoana de contact

Punctul unic de contact (Single Point of Contact — SPoC) pentru aspecte legate de prezentul CP/CPS și pentru relația cu ADR este: Administratorul QSIGN, Trandafirescu Alexandru Florin, alex@qsign.ro. Pentru chestiuni operaționale curente (incidente, revocări, asistență tehnică) se utilizează adresele dedicate menționate în secțiunea 1.5.1.

1.5.3 Persoana / organul care determină adecvarea CPS la CP

Determinarea adecvării CPS la CP, precum și aprobarea modificărilor ulterioare ale prezentului document, sunt în competența Policy Management Authority (PMA) a QSIGN — organism intern compus din: (a) Administratorul societății; (b) Responsabilul cu Securitatea Informațiilor (Trust Service Officer / CISO); (c) Responsabilul Tehnic PKI (PKI Manager); (d) Responsabilul Conformitate (Compliance Officer); (e) Responsabilul cu Protecția Datelor (DPO). Deciziile PMA se adoptă cu majoritate, reprezentantul legal având drept de veto motivat. Hotărârile PMA se consemnează în Registrul deciziilor PMA, publicat în extras pe portalul QSIGN.

1.5.4 Procedura de aprobare CPS

1. Propunerea de modificare se inițiază de orice membru PMA, sau ca rezultat al unui audit de conformitate, control ADR, sau incident de securitate.
2. Propunerea este analizată tehnic, juridic și de securitate; analizele se atașează la dosarul deciziei.
3. Pentru modificări substanțiale (de exemplu, schimbări de algoritm criptografic, modificări ale procesului de identificare la distanță, schimbări de QSCD), PMA solicită opinie consultativă de la auditorul de conformitate.
4. Modificările substanțiale sunt notificate ADR cu cel puțin 30 de zile înainte de intrarea în vigoare, conform art. 4 alin. (1)–(2) din Anexa 1 la Decizia 162/2026.
5. Documentul actualizat este publicat în repository, sigilat electronic cu sigiliu calificat al QSIGN și marcat temporal calificat, însoțit de un istoric al modificărilor (changelog) și de OID-ul nou alocat versiunii.
6. Versiunile anterioare rămân disponibile public timp de minimum 10 ani de la data înlocuirii, în vederea valorii probatorii a documentelor semnate sub politicile anterioare.

1.6 Definiții și acronime

1.6.1 Definiții

În prezentul document, termenii definiți la art. 3 din Reg. (UE) nr. 910/2014 și la art. 2 din Legea 214/2024 își păstrează semnificația din actele respective. Suplimentar:

Termen	Definiție
Cheie privată	Cheia matematică din perechea criptografică, păstrată sub controlul exclusiv al titularului, utilizată pentru crearea semnăturii/sigiliului electronic calificat.
Cheie publică	Cheia matematică perechea cu cheia privată, distribuită prin certificat și utilizată pentru verificarea semnăturii/sigiliului.
CRL	Certificate Revocation List — lista certificatelor revocate, semnată de CA-ul emitent (RFC 5280).
OCSP	Online Certificate Status Protocol — protocol de interogare a stării certificatelor în timp real (RFC 6960).
HSM	Hardware Security Module — modul criptografic hardware utilizat pentru generarea și protecția cheilor private.
QSCD	Qualified Signature/Seal Creation Device — dispozitiv calificat de creare a semnăturilor/sigiliilor (Anexa II la eIDAS).
LoIP	Level of Identity Proofing — nivelul de asigurare al verificării identității, conform ETSI TS 119 461.
LoA	Level of Assurance — nivel de asigurare a încrederii (low/substanțial/ridicat), conform Reg. (UE) 2015/1502.
TSA / QTSA	Time-Stamping Authority / Qualified Time-Stamping Authority — autoritate care emite mărci temporale calificate (RFC 3161 / ETSI EN 319 422).
RA / LRA	Registration Authority / Local Registration Authority — entități care primesc și verifică cererile.
PMA	Policy Management Authority — organism care administrează prezentul document.
LTP	Long-Term Preservation — conservare pe termen lung a valabilității și valorii probatorii.
TSP / QTSP	Trust Service Provider / Qualified Trust Service Provider.
CAB	Conformity Assessment Body — organism de evaluare a conformității, acreditat conform Reg. (CE) 765/2008.
TL / LOTL	Trusted List / List of Trusted Lists — lista sigură națională / lista listelor sigure UE.
QES / QESeal	Qualified Electronic Signature / Qualified Electronic Seal.

1.6.2 Acronime

ADR — Autoritatea pentru Digitalizarea României; ANSPDCP — Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal; CA — Certification Authority; CAB — Conformity Assessment Body; CP — Certificate Policy; CPS — Certification Practice Statement; DNSC — Directoratul Național de Securitate Cibernetică; eIDAS — Reg. (UE) nr. 910/2014; ETSI — European Telecommunications Standards Institute; GDPR — Reg. (UE) 2016/679; HSM — Hardware Security Module; ISMS — Information Security Management System; LOTL — List of Trusted Lists; OCSP — Online Certificate Status Protocol; OID — Object Identifier; PEN — Private Enterprise Number (IANA); PKI — Public Key Infrastructure; PMA — Policy Management Authority; QCP — Qualified Certificate Policy; QSCD — Qualified Signature/Seal Creation Device; QTSA — Qualified Time-Stamping Authority; QTSP — Qualified Trust Service Provider; QWAC — Qualified Website Authentication Certificate; RA —

Registration Authority; SLA — Service Level Agreement; SOC — Security Operations Center; TSA — Time-Stamping Authority; TSP — Trust Service Provider.

2. Responsabilități privind publicarea și repository-ul

2.1 Repository

QSIGN operează un repository public, accesibil 24/7 la adresa https://www.qsign.ro/repository, în care publică toate documentele de politici aplicabile, certificatele rădăcină și subordonate, listele de revocare (CRL), informațiile pentru relying parties și istoricul versiunilor documentelor. Repository-ul este conceput cu redundanță geografică, având două instanțe oglindite în centre de date diferite, cu un SLA de disponibilitate ≥ 99,9% pentru repository-ul public și ≥ 99,95% pentru endpoint-urile operaționale (OCSP, CRL distribution points, QTSA).

2.2 Publicarea informațiilor de certificare

QSIGN publică în repository următoarele informații, conform art. 24 alin. (2) lit. (k) eIDAS:

- Politica de Certificare (CP) și Codul de Practici și Proceduri (CPS) — prezentul document, în versiune curentă și în versiunile istorice.
- PKI Disclosure Statement (PDS) — sinteză publică a informațiilor critice pentru utilizatori, conform Anexei A la ETSI EN 319 411-1.
- Termeni și condiții pentru titulari (Subscriber Agreement) și pentru relying parties (Relying Party Agreement).
- Certificatele Root CA, Issuing CAs și QTSA, în formatele cer (binar) și pem (Base64).
- CRL-uri pentru fiecare CA emitentă, actualizate conform secțiunii 4.9 a prezentului document.
- Politica QTSA (Time-Stamping Policy) și Politica de validare/conservare.
- Lista LRA-urilor active și a metodelor de identificare aprobate, cu OID-urile corespunzătoare.
- Schema personalului implicat și certificările deținute (versiune anonimizată conform GDPR).
- Raportul anual de transparență al QSIGN.
- Informațiile privind incidentele de securitate notificate, în formă agregată, păstrând confidențialitatea utilizatorilor afectați.

2.3 Frecvența publicării

Element	Frecvența publicării / actualizării
Certificate CA (Root, Issuing)	La emitere și la fiecare re-key; rămân publicate până la expirare + 35 ani
CRL — Issuing CA Calificat (Signature)	La fiecare 24 ore (nextUpdate la 7 zile)
CRL — Issuing CA Calificat (Seal)	La fiecare 24 ore (nextUpdate la 7 zile)
CRL — Root CA	La 6 luni sau imediat la revocarea unei sub-CA
OCSP	Răspuns dinamic; valabilitate ≤ 7 zile, prospețime info ≤ 1 oră
CP/CPS	La fiecare modificare; revizuire anuală formală obligatorie
PDS	Sincronizat cu CP/CPS
Lista LRA / metode de identificare	În maxim 5 zile lucrătoare de la modificare

Element	Frecvența publicării / actualizării
Raport anual transparență	În primul trimestru al anului următor anului de raportare

2.4 Controale de acces la repository

Informațiile publicate sunt liber accesibile, fără autentificare. QSIGN aplică următoarele controale pentru integritatea și autenticitatea conținutului: (i) toate documentele PDF publicate sunt sigilate electronic cu sigiliul calificat al QSIGN și marca temporală calificată; (ii) repository-ul este servit exclusiv prin HTTPS; (iii) integritatea fișierelor este verificabilă prin hash-uri publicate; (iv) modificările sunt jurnalizate și păstrate timp de minimum 10 ani; (v) accesul administrativ este restricționat la personalul autorizat, cu autentificare puternică (MFA cu certificat hardware).

3. Identificare și autentificare

3.1 Numire (Naming)

3.1.1 Tipuri de nume

Toate certificatele calificate emise de QSIGN utilizează nume distincte X.500 conforme cu RFC 5280 și ETSI EN 319 412 (părțile 1, 2, 3, 5). Câmpurile Subject DN și Issuer DN sunt formate dintr-o secvență de atribute relativ distincte (RDN), codate UTF-8, în ordinea alocată conform standardelor.

3.1.2 Necesitatea ca numele să fie semnificative

Pentru certificate QCP-n / QCP-n-qscd (persoane fizice), câmpurile commonName (CN), givenName (GN), surname (SN) reflectă numele real al persoanei, așa cum apare în actul de identitate prezentat la identificare. Pentru certificate QCP-l / QCP-l-qscd (persoane juridice), commonName și organizationName reflectă denumirea juridică oficială a entității din registrele publice (ONRC pentru entități române).

3.1.3 Anonimat și pseudonime

QSIGN permite utilizarea pseudonimelor pentru certificate calificate de tip QCP-n / QCP-n-qscd, cu condiția ca: (i) identitatea reală a titularului să fi fost verificată cu LoIP corespunzător tipului de certificat (vezi 3.2.3); (ii) certificatul să indice în mod expres faptul că identitatea utilizată este un pseudonim, prin atributul pseudonym în Subject DN, fără atributele givenName/surname/CN cu numele real, și prin marcarea explicită în extensia QCStatements; (iii) identitatea reală să poată fi divulgată exclusiv în condițiile art. 12 alin. (5) din Legea 214/2024 — la solicitarea autorităților competente sau cu consimțământul titularului. Pentru certificate de sigiliu (QCP-l, QCP-l-qscd), pseudonimele NU sunt permise.

3.1.4 Reguli pentru interpretarea diverselor formate de nume

- Diacriticele românești sunt păstrate (ș, ț, ă, î, â) în UTF-8; nu se aplică transliterare ASCII.
- Numerele de identificare sunt incluse în atributul serialNumber sau organizationIdentifier conform ETSI EN 319 412-1, cu prefix de tip semantic: "PNORO-<CNP>" pentru cetățeni români (natural person), "NTRRO-<număr ONRC>" sau "VATRO-<CIF>" pentru entități juridice românești (legal person).
- Numele complete care depășesc limita de 64 de caractere a CN sunt distribuite în GN/SN; commonName este compus în formatul "GN SN" trunchiat dacă necesar.
- Caracterele speciale (\, /, =, +, virgulă, ghilimele) din numele juridice sunt escape-uite conform RFC 4514.

3.1.5 Unicitatea numelor

Subject DN-ul este unic în cadrul fiecărei Issuing CA, prin combinarea atributelor commonName și serialNumber/organizationIdentifier. În cazul în care două persoane au același nume, dezambiguizarea este asigurată prin serialNumber (cuprinzând CNP-ul sau alt identificator unic stabil).

3.1.6 Recunoașterea, autentificarea și rolul mărcilor de comerț

QSIGN nu efectuează verificări proactive asupra eventualelor încălcări ale drepturilor de marcă în denumirile incluse în certificatele de sigiliu. Solicitantul declară pe propria răspundere, prin acceptarea Subscriber Agreement, că deține drepturile de utilizare a denumirii și că nu încalcă drepturile terților. QSIGN își rezervă dreptul de a refuza emiterea sau de a revoca un certificat în cazul în care are cunoștință rezonabilă despre o încălcare evidentă sau în cazul unei hotărâri judecătorești.

3.2 Validarea inițială a identității

3.2.1 Metoda de demonstrare a posesiei cheii private

Demonstrarea posesiei cheii private (Proof-of-Possession — PoP) se realizează în conformitate cu RFC 4211 (CMP / CRMF) sau prin solicitarea de certificat în format PKCS#10 (CSR) semnat cu cheia privată. Pentru certificate calificate cu QSCD la distanță (QCP-n-qscd, QCP-l-qscd), în care cheia privată este generată direct în QSCD-ul operat de TSP, PoP este garantat prin proces controlat de TSP: (a) generarea cheii are loc exclusiv în HSM sub controlul titularului prin autentificare puternică (SAD — Signature Activation Data, conform EN 419 241-2); (b) procesul este atestat criptografic prin metadate semnate de QSCD; (c) cheia nu părăsește niciodată HSM-ul în formă neprotejată.

3.2.2 Autentificarea identității organizației

Pentru certificate calificate de sigiliu (QCP-l, QCP-l-qscd), identitatea organizației este verificată conform ETSI TS 119 461 (clauza referitoare la verificarea identității persoanei juridice) prin combinația următoarelor metode:

7. Verificarea existenței juridice prin consultarea registrelor publice oficiale (ONRC pentru România, registrele comerțului ale altor state membre UE), cu obținerea unui certificat constatator nu mai vechi de 30 de zile.
8. Verificarea statutului fiscal și a CUI/CIF prin interogarea bazelor publice ale ANAF (PlatitorTvaRest API), pentru titulari români.
9. Verificarea identității reprezentantului legal prin metodele aplicabile persoanelor fizice (vezi 3.2.3).
10. Verificarea împuternicirii (mandatului) reprezentantului legal de a solicita certificat în numele organizației — prin actul constitutiv, hotărârea organului de conducere sau procura specială autentică.

3.2.3 Autentificarea identității persoanei fizice

Identificarea persoanei fizice este pasul critic al întregului proces de emitere și se realizează cu un Level of Identity Proofing (LoIP) corespunzător tipului de certificat solicitat, conform ETSI TS 119 461 v2.1.1 (sau ulterior) și art. 24 alin. (1) lit. (d) eIDAS. Tabelul de mai jos sintetizează cerințele aplicabile certificatelor calificate emise de QSIGN.

Tip certificat calificat	LoIP minim	Metode acceptate
QCP-n — semnătură calificată (cheie utilizator)	Substantial sau High LoIP	Prezență fizică; mijloace eID notificate cu LoA Substanțial sau Ridicat (ROeID, eIDAS nodes); certificat calificat existent valabil; video-identificare cu LoA Substanțial aprobată

Tip certificat calificat	LoIP minim	Metode acceptate
QCP-n-qscd — semnătură calificată cu QSCD	Substantial sau High LoIP	Prezență fizică; mijloace eID notificate cu LoA Substanțial sau Ridicat; certificat calificat existent; video-identificare cu LoA Substanțial/Ridicat aprobată
QCP-l — sigiliu calificat (cheie utilizator)	Substantial LoIP (pers. fiz.) + verificare juridică	Identificare reprezentant legal (ca QCP-n) + validare existență juridică (3.2.2)
QCP-l-qscd — sigiliu calificat cu QSCD	Substantial LoIP (pers. fiz.) + verificare juridică	Idem QCP-l, cu verificare suplimentară a controlului asupra QSCD-ului

3.2.3.1 Identificare prin prezența fizică

Solicitantul se prezintă personal la sediul unei RA sau LRA aprobate. Operatorul RA verifică actul de identitate (carte de identitate, pașaport sau permis de ședere) — în original — , validează autenticitatea acestuia (caracteristici de securitate vizibile, holograme, microprint, MRZ), captează datele biometrice limitate la fotografie facială și semnătură olografă pe formularul de cerere. Operatorul efectuează o verificare "liveness" prin comparare facială cu fotografia de pe actul de identitate. Întreaga sesiune este consemnată în jurnalul de identificare, semnat electronic de operator. Această metodă asigură LoIP High și este metoda preferată pentru QCP-n-qscd cu LoIP High.

3.2.3.2 Identificare la distanță cu agent uman (video-identificare)

Sesiunea video se desfășoară în condițiile ETSI TS 119 461 §6.3 (Substantial LoIP) sau §6.4 (High LoIP), cu cerințe critice:

- Sesiunea este realizată în timp real, în limba română (sau altă limbă agreată), cu un agent uman instruit, certificat și înregistrat în sistemul de management al RA.
- Conexiunea video este criptată end-to-end (TLS 1.3 minimum); platforma este auto-hosted (BigBlueButton configurat conform politicii de securitate), cu jurnalizare integrală a evenimentelor.
- Agentul verifică actul de identitate prin: (i) prezentare frontală și verso; (ii) verificare automată OCR cu validare structurală (MRZ, cifre de control); (iii) detectarea elementelor de securitate dinamice (holograme prin modificare de unghi); (iv) comparare facială cu un model 3D obținut prin solicitarea unor mișcări specifice ale capului (anti-spoofing PAD — Presentation Attack Detection conform ISO/IEC 30107-3).
- Solicitantul rostește o frază secret furnizată live de agent (test de liveness vocal).
- Sesiunea video se înregistrează integral; înregistrarea este sigilată electronic cu marcă temporală calificată și păstrată conform secțiunii 5.5 (minim 7 ani de la încetarea valabilității certificatului — cerință ETSI TS 119 461).
- Pentru High LoIP: dublă autentificare a agentului uman; verificare automată suplimentară prin servicii de fraud detection; verificare incrucișată cu listele de sancțiuni (PEP, sancțiuni internaționale).
- Mecanismul de identificare la distanță este aprobat de ADR conform Anexei 5 la Ordinul MEDAT 102/2026 (Norme de aprobare a mecanismelor de validare).

3.2.3.3 Identificare prin certificat calificat existent

Solicitantul poate fi identificat printr-un certificat calificat valid pentru semnătura electronică, emis de orice prestator calificat din UE listat în LOTL. Solicitantul semnează electronic cererea de emitere cu certificatul

calificat existent; QSIGN verifică criptografic semnătura, validitatea certificatului (CRL/OCSP), și extrage atributele de identitate (commonName, serialNumber). Această metodă asigură LoIP echivalent cu cel al certificatului-sursă; este acceptabilă pentru QCP-n / QCP-n-qscd / QCP-l / QCP-l-qscd dacă certificatul-sursă a fost emis cu LoIP cel puțin egal.

3.2.3.4 Identificare prin mijloace eID notificate (ROeID, eIDAS nodes)

Pentru titulari care dețin un mijloc de identificare electronică notificat conform Reg. (UE) 2015/1502, cu LoA Substanțial sau Ridicat, identificarea se poate realiza prin nodul eIDAS național (Platforma PSCID — ROeID în România) sau prin nodul eIDAS al statului membru emitent. Atributele de identitate (eIDAS Minimum Data Set) sunt extrase direct prin protocolul SAML 2.0 standardizat la nivel UE, fără intervenție umană. Această metodă este recomandată pentru QCP-n / QCP-n-qscd cu LoIP High.

3.2.4 Informații neverificate ale titularului

QSIGN nu include în certificate calificate informații despre titular care nu au fost verificate. Atributele opționale (titlu profesional, calitatea de membru al unei organizații, atestarea unui rol) sunt incluse exclusiv dacă există documente justificative verificabile la sursă, cu valabilitate confirmată de un terț de încredere (de exemplu, ordinul profesional pentru avocat, medic, notar).

3.2.5 Validarea autorității

Pentru certificate de sigiliu, atunci când persoana fizică care solicită certificatul nu este reprezentantul legal al persoanei juridice, autoritatea de a solicita în numele organizației este validată prin: (i) procură autentică notarială; sau (ii) împuternicire sub semnătură electronică calificată a reprezentantului legal cu împuternicire generală sau specială pentru aceste operațiuni; sau (iii) documente interne ale organizației (decizie a consiliului de administrație, regulament intern) care atestă mandatul. Documentele justificative sunt arhivate ca parte a dosarului de înregistrare.

3.2.6 Criterii pentru interoperabilitate

Toate certificatele calificate emise de QSIGN sunt interoperabile cu standardele europene aplicabile, listate în Decizia ADR și recunoscute prin includerea în Trusted List națională. QSIGN urmărește respectarea specificațiilor ETSI EN 319 412 (părțile 1–5) pentru profilul de certificat, ETSI EN 319 411-2 pentru cerințele specifice certificatelor calificate, ETSI EN 319 102-1 pentru semnături AdES (CAdES, XAdES, PAdES, ASiC). Tools de validare publice (DSS-ul Comisiei Europene, demo-uri ETSI) sunt utilizate periodic pentru confirmarea interoperabilității.

3.3 Identificare și autentificare pentru cereri de re-key

3.3.1 Re-key de rutină

La solicitarea unui certificat nou cu chei noi, înainte de expirarea certificatului curent, titularul poate fi re-identificat prin: (i) semnarea electronică a cererii cu certificatul curent valid (metoda preferată); (ii) repetarea unui proces de identificare integral, conform tipului de certificat. Conform ETSI EN 319 411-2, dacă au trecut mai mult de 5 ani de la identificarea inițială, este obligatorie re-identificarea completă pentru certificate calificate.

3.3.2 Re-key după revocare

Dacă certificatul anterior a fost revocat din motive de compromitere a cheii sau erori în datele de identitate, este obligatorie re-identificarea completă, în conformitate cu metodele specifice tipului de certificat. Cererea anterioară este invalidată automat.

3.4 Identificare și autentificare pentru cereri de revocare

QSIGN acceptă cereri de revocare prin următoarele metode autentificate:

11. Cerere semnată electronic cu certificatul ce urmează a fi revocat (auto-revocare).
12. Cerere semnată cu un alt certificat calificat valid al titularului.
13. Cerere transmisă prin portalul autentificat al titularului (cu autentificare MFA: certificat hardware + parolă/PIN).
14. Cerere telefonică sau e-mail urgentă, urmată de un proces secundar de autentificare bazat pe răspunsuri la întrebări secrete stabilite la înrolare; revocarea este efectuată provizoriu (suspendare temporară până la 24 ore) până la confirmarea finală prin metode (1)–(3) — notă: pentru certificate calificate, suspendarea finală nu există (a se vedea 4.9.8); revocare devine definitivă.
15. Cerere venită din partea ADR, instanței judecătorești sau altei autorități competente, în temeiul unei dispoziții legale; QSIGN execută imediat și informează titularul, exceptând cazurile de secret legal.

4. Cerințe operaționale privind ciclul de viață al certificatelor

4.1 Cererea de certificat

4.1.1 Cine poate solicita un certificat calificat

- Pentru certificate QCP-n / QCP-n-qscd: orice persoană fizică majoră, cu capacitate deplină de exercițiu, care prezintă un act de identitate valid și acceptă Subscriber Agreement.
- Pentru certificate QCP-l / QCP-l-qscd: orice persoană juridică legal constituită (societate comercială, asociație, fundație, autoritate sau instituție publică, persoană juridică străină cu reprezentanță în România etc.), reprezentată de o persoană fizică al cărei mandat este valid și verificabil.

4.1.2 Procesul de înregistrare și responsabilități

Procesul de înregistrare se desfășoară în următorii pași standardizați, cu jurnalizare exhaustivă a fiecărui eveniment, în conformitate cu ETSI EN 319 411-2 §6.2.2:

16. Solicitantul accesează portalul QSIGN sau LRA și inițiază cererea, completând datele preliminare și selectând tipul de certificat calificat dorit.
17. Solicitantul citește și acceptă electronic Subscriber Agreement, T&C, precum și consimțământul GDPR pentru prelucrarea datelor cu caracter personal.
18. Solicitantul achită tariful aplicabil tipului de certificat (sau prezintă dovada plății, în cazul plății în avans pentru organizații).
19. Solicitantul efectuează identificarea conform metodei aplicabile tipului de certificat (vezi secțiunea 3.2.3).
20. Sistemul colectează informațiile necesare emiterii (Subject DN, atribute extra, KeyUsage solicitat, durată).
21. Pentru certificate cu chei generate de utilizator (QCP-n, QCP-l fără QSCD): solicitantul transmite CSR (PKCS#10) semnat cu cheia privată, demonstrând PoP.
22. Pentru certificate cu chei generate în QSCD la distanță operat de QSIGN (QCP-n-qscd, QCP-l-qscd): cheia este generată în HSM al QSIGN, sub controlul exclusiv al titularului prin SAD; metadatele de generare sunt sigilate.
23. Operatorul RA validează manual sau semi-automat dosarul, marchează aprobat/respins și transmite spre emitere.
24. Issuing CA emite certificatul, îl publică în repository (dacă titularul a consimțit) și îl livrează titularului prin canal securizat.
25. Titularul confirmă recepția și acceptă certificatul (acceptarea poate fi expresă sau prin utilizarea efectivă, conform secțiunii 4.4).

4.2 Procesarea cererilor de certificat

4.2.1 Realizarea funcțiilor de identificare și autentificare

Funcțiile de identificare și autentificare sunt detaliate în secțiunea 3.2 a prezentului document. Operatorii RA sunt instruiți și certificați; orice abatere de la procesul standard impune escaladare către CISO și consemnare formală.

4.2.2 Aprobarea sau respingerea cererii

Decizia de aprobare se ia în temeiul evaluării integrale a dosarului. Motive de respingere includ:

- Documente de identitate falsificate sau alterate.
- Imposibilitatea de a confirma identitatea cu LoIP-ul cerut.
- Solicitant inclus pe liste de sancțiuni (UE, ONU, OFAC) sau cu rol de PEP în condiții care impun due diligence sporit ce nu poate fi parcurs.
- Existența unui certificat valid identic, deja emis (prevenirea duplicatelor).
- Obiect de activitate sau atribute solicitate care nu corespund titularului.
- Plata neefectuată sau respinsă.
- Neacceptarea Subscriber Agreement.

În caz de respingere, solicitantul este informat în scris cu motivarea (cu respectarea reglementărilor antifraudă) și i se restituie eventuala plată anticipată, mai puțin tariful de procesare administrativă, dacă acesta a fost agreat anterior.

4.2.3 Termen de procesare

Tip certificat calificat	Termen standard	Termen maxim
QCP-n / QCP-n-qscd — semnătură	1 zi lucrătoare	5 zile lucrătoare
QCP-l / QCP-l-qscd — sigiliu	2 zile lucrătoare	10 zile lucrătoare

4.3 Emiterea certificatelor

4.3.1 Acțiunile CA în timpul emiterii

26. Issuing CA primește o cerere de emitere semnată digital de RA (event-driven, prin API intern protejat cu mTLS și jurnalizat).
27. CA verifică integritatea cererii și autorizarea operatorului RA.
28. CA verifică unicitatea Subject DN-ului în baza sa de date.
29. CA generează numărul serial al certificatului — număr aleator de 64 de biți minimum (entropie criptografică), conform CAB Forum Baseline Requirements și RFC 5280.
30. CA construiește profilul certificatului conform secțiunii 7 a prezentului document și ETSI EN 319 412-2 (semnătură) sau 412-3 (sigiliu).
31. CA semnează certificatul cu cheia privată, în interiorul HSM-ului.
32. Certificatul este înregistrat în baza de date de certificate active, în jurnalul de emitere și (dacă aplicabil) în log-uri de Certificate Transparency.
33. Certificatul este transmis înapoi către RA pentru livrare.

4.3.2 Notificare către titular

Titularul este notificat prin e-mail (la adresa indicată și verificată) și prin portalul autentificat. Pentru certificatele cu cheie generată în QSCD la distanță (QCP-n-qscd, QCP-l-qscd), certificatul este disponibil în containerul utilizator al titularului în interfața QSIGN; cheia privată rămâne în HSM. Pentru certificatele pe smart card / token / smartphone, certificatul este livrat fizic (smart card) sau instalat de la distanță (mobile). Marca temporală a livrării este sigilată cu mărci temporale calificate ale QSIGN QTSA.

4.4 Acceptarea certificatului

4.4.1 Acțiuni constituind acceptarea

Titularul este considerat să fi acceptat certificatul prin oricare dintre următoarele acțiuni:

- Confirmarea explicită a recepției prin click pe link-ul "Accept" în portalul QSIGN, semnat cu certificatul însuși sau cu metode de autentificare puternică.
- Utilizarea certificatului pentru a semna primul document (utilizare efectivă).
- Trecerea unui termen de 30 de zile de la livrare fără ca titularul să formuleze obiecțiune și fără solicitare de revocare.

4.4.2 Publicarea certificatului

Certificatele de sigiliu calificat (QCP-l, QCP-l-qscd) și certificatele CA sunt publicate în repository-ul QSIGN în mod implicit. Certificatele asociate persoanelor fizice (QCP-n, QCP-n-qscd) NU sunt publicate fără consimțământul expres al titularului, în concordanță cu principiul minimizării datelor cu caracter personal (GDPR). Pentru relying parties, validarea statusului unui certificat se realizează prin OCSP/CRL — care nu necesită publicarea certificatului în sine.

4.4.3 Notificarea altor entități

Atunci când relevant (de exemplu, integrare cu sisteme închise, integrare cu Platforma de interoperabilitate ROeID), QSIGN notifică automat sistemele integrate cu privire la emiterea certificatului, conform scopului consimțit de titular. Notificările respectă principiile GDPR (legitimitate, minimizare, limitarea scopului).

4.5 Utilizarea perechii de chei și a certificatului

4.5.1 Utilizarea de către titular

Titularul are obligația, conform Subscriber Agreement și art. 26 din Legea 214/2024, de a:

- Păstra cheia privată sub control exclusiv: pentru chei pe QSCD — necunoaștere a PIN/SAD de către alte persoane; pentru QSCD la distanță — păstrarea credențialelor de activare în siguranță, cu autentificare MFA configurată.
- Utiliza certificatul exclusiv pentru scopurile permise prin KeyUsage, ExtendedKeyUsage și politica de certificat (OID inclus în Certificate Policies).
- Solicita revocarea în maximum 24 ore de la momentul aflării unui motiv de revocare (compromitere, pierdere, modificarea informațiilor esențiale, suspiciune de utilizare frauduloasă) — conform art. 26 alin. (2) din Legea 214/2024.
- Nu utiliza certificatul după expirare sau revocare.
- Notifica QSIGN în 24 ore în cazul oricărui incident de securitate care afectează certificatul.

4.5.2 Utilizarea de către relying party

Relying party are obligația, conform Relying Party Agreement, de a:

- Verifica criptografic integritatea semnăturii / sigiliului.

- Verifica statutul certificatului utilizând OCSP sau CRL la momentul procesului de validare; pentru valoare probatorie pe termen lung, verificarea se face contra surselor LTV (DSS — Document Time-Stamp și/sau servicii de păstrare calificată conform art. 34 / 40 eIDAS).
- Construi și valida lanțul de încredere până la o ancoră de încredere oficială (Lista sigură națională / LOTL UE).
- Verifica că OID-ul politicii incluse în certificat corespunde cerințelor cazului de utilizare (QCP-n, QCP-n-qscd, QCP-l, QCP-l-qscd).
- Verifica QCStatements (id-etsi-qcs-QcCompliance, id-etsi-qcs-QcType, id-etsi-qcs-QcSSCD) pentru a confirma natura calificată a certificatului și prezența QSCD.
- Lua în considerare orice limitări sau restricții indicate în certificat (qcStatement-uri, valoare maximă a tranzacțiilor unde aplicabil).

4.6 Reînnoirea certificatului (renewal)

Reînnoirea (renewal) — emiterea unui nou certificat cu aceeași cheie publică — NU este permisă pentru certificatele calificate, conform recomandărilor ETSI EN 319 411-2. Pentru continuitatea serviciilor, se utilizează re-key (secțiunea 4.7).

4.7 Re-key (generare cheie nouă)

4.7.1 Circumstanțe pentru re-key

- Apropierea expirării certificatului curent (cu cel mult 60 de zile înainte de expirare).
- Schimbarea algoritmului criptografic recomandat (de exemplu, migrare de la RSA-2048 la RSA-3072+ sau la algoritmi post-cuantici).
- Compromiterea cheii curente sau suspiciune rezonabilă de compromitere.
- Modificări de legislație, standarde sau politici care impun reemiterea.

4.7.2 Cine poate solicita re-key

Re-key poate fi solicitat doar de titularul certificatului curent (sau, în cazul certificatelor de sigiliu, de reprezentantul legal autorizat). Re-key impus de TSP (de exemplu, ca urmare a migrării algoritmice) este notificat titularilor cu cel puțin 90 de zile în avans.

4.7.3 Procesul de re-key

Re-key urmează același proces ca emiterea inițială, cu excepția identificării: dacă certificatul curent este valabil și nu compromis, identificarea se poate face prin semnarea cererii cu certificatul curent (secțiunea 3.3.1). Conform ETSI EN 319 411-2, dacă au trecut peste 5 ani de la identificarea inițială, este obligatorie re-identificarea completă.

4.8 Modificarea certificatului

Modificarea unui certificat existent (de exemplu, modificarea atributelor) NU este permisă: orice modificare necesită revocarea certificatului curent și emiterea unui nou certificat.

4.9 Revocarea și suspendarea certificatului

4.9.1 Circumstanțe pentru revocare

Conform art. 17 alin. (2) din Legea 214/2024 și ETSI EN 319 411-2 §6.3.9, QSIGN are obligația de a revoca certificatul în maxim 24 ore din momentul în care a luat cunoștință despre apariția uneia dintre următoarele situații:

- La cererea titularului, după verificarea identității acestuia.
- Decesul titularului persoană fizică (cunoscut la TSP prin notificare oficială sau prin verificări periodice cu Registrul național al persoanelor).
- Hotărâre judecătorească definitivă care dispune revocarea.
- Dacă se dovedește că certificatul a fost emis în baza unor informații eronate sau false.
- Dacă informațiile esențiale conținute în certificat nu mai corespund realității.
- Atunci când a fost încălcată confidențialitatea datelor de creare a semnăturii.
- În cazul în care certificatul a fost utilizat în mod fraudulos.
- Dacă este semnalat un incident de securitate care ar putea duce la compromiterea certificatului.
- La solicitarea ADR sau a altei autorități competente, în temeiul legii.
- La încetarea activității QSIGN, dacă activitatea nu este preluată de un alt prestator (art. 13 din Legea 214/2024).
- La nerespectarea de către titular a obligațiilor contractuale (Subscriber Agreement), constatată în mod clar.

4.9.2 Cine poate solicita revocarea

- Titularul certificatului (auto-revocare).
- Reprezentantul legal al titularului persoană juridică (pentru sigilii).
- Moștenitorii sau persoana împuternicită la decesul titularului.
- ADR, instanța judecătorească, autoritățile competente.
- QSIGN, din proprie inițiativă, în condițiile menționate la 4.9.1.
- Orice persoană care semnalează în mod credibil un incident de securitate; QSIGN investighează rapid și revocă dacă semnalarea este confirmată.

4.9.3 Procedura cererii de revocare

Cererea de revocare se transmite prin oricare dintre canalele:

- Portalul autentificat al titularului (recomandat) — disponibil 24/7.
- E-mail la revoke@qsign.ro — semnat electronic de titular cu certificat valid sau confirmat ulterior prin proces secundar.
- Telefon la +40 724 167 333 (orele de program 08:00–20:00) sau linia de urgență 24/7 (publicată în repository) — cu autentificare prin întrebări secrete.
- Personal, la sediul QSIGN sau LRA.

4.9.4 Termenul de execuție a cererii de revocare

Conform art. 17 alin. (2) din Legea 214/2024, QSIGN execută revocarea în maxim 24 ore de la primirea cererii valid autentificate. Pentru cereri urgente cu evidență prima facie de compromitere (de exemplu,

cerere semnată electronic cu certificatul însuși conținând declarația de compromitere), execuția este imediată — în maxim 1 oră — și informarea în CRL/OCSP urmează imediat (vezi 4.9.5).

4.9.5 Frecvența emiterii CRL

CRL	Frecvența emiterii	Perioada de valabilitate (nextUpdate)
Issuing CA — Calificat (Signature)	La fiecare 24 ore (sau imediat la revocare)	7 zile
Issuing CA — Calificat (Seal)	La fiecare 24 ore (sau imediat la revocare)	7 zile
Root CA	La 6 luni sau imediat la revocarea sub-CA	12 luni

4.9.6 Latență maximă a CRL

Latența maximă între momentul revocării unui certificat și momentul în care revocarea apare în CRL publicat este de maximum 60 de minute (recomandat: emitere imediată după fiecare revocare, fără batch). OCSP-ul reflectă revocarea în maxim 5 minute, conform ETSI EN 319 411-2 §6.3.9 și art. 6 alin. (2) din Anexa 2 la Decizia 162/2026.

4.9.7 Verificarea revocării (OCSP)

QSIGN operează un Responder OCSP per Issuing CA, conform RFC 6960, cu următoarele caracteristici: (i) răspunsuri semnate cu certificat OCSP delegat dedicat (extensia id-pkix-ocsp-nocheck); (ii) statusurile suportate: good, revoked, unknown; (iii) răspunsuri valide timp de 7 zile maximum, cu ThisUpdate ≤ 1 oră de la cererea curentă; (iv) suport HTTP GET și POST; (v) endpoint indicat în extensia AIA (Authority Information Access) a certificatelor emise; (vi) disponibilitate ≥ 99,95% — conform cerinței art. 6 alin. (1) din Anexa 2 la Decizia 162/2026 (24/7 disponibilitate continuă).

4.9.8 Suspendarea (hold)

Conform recomandărilor ETSI EN 319 411-2, suspendarea (certificateHold) NU este permisă pentru certificatele calificate emise de QSIGN — pentru a evita ambiguitățile privind valabilitatea în timp ale semnăturilor calificate. Cererile care ar putea conduce la suspendare (de exemplu, suspiciune de compromitere care necesită investigare) sunt tratate fie ca revocare definitivă (din motive de precauție), fie ca revocare provizorie cu termen scurt de investigare maxim 24 ore, după care se decide definitivarea revocării.

4.10 Servicii pentru starea certificatului

QSIGN furnizează două servicii independente pentru determinarea stării certificatelor: (i) CRL — descărcabil HTTP de la URL-ul indicat în extensia CRL Distribution Points a fiecărui certificat emis; (ii) OCSP — interogare în timp real, endpoint indicat în extensia AIA. Ambele servicii au disponibilitate ≥ 99,95% (SLA contractual cu utilizatorii enterprise) și sunt monitorizate continuu.

4.11 Încetarea utilizării (end of subscription)

Titularul poate înceta utilizarea certificatului prin solicitarea revocării. Încetarea normală prin expirare nu necesită acțiuni din partea titularului, însă acesta este informat în avans (cu 60, 30, 15 și 7 zile înainte de expirare) prin e-mail.

4.12 Escrow și recuperarea cheii

Cheile private utilizate pentru semnătura/sigiliul electronic calificat NU fac obiectul niciunei forme de escrow sau recuperare la QSIGN — această practică ar contraveni cerinței de control exclusiv al semnatarului asupra cheii (art. 24 alin. (2) lit. (j) eIDAS și Anexa II punctul 1 (a) eIDAS pentru QSCD). Pentru cazurile în care titularul pierde accesul la cheia privată, singura soluție este revocarea certificatului și emiterea unuia nou.

5. Controale de facilitate, management și operaționale

5.1 Controale de securitate fizică

5.1.1 Locația și construcția centrului de date

Componentele critice ale infrastructurii QSIGN (Root CA, Issuing CAs, HSM-uri, sistemele de jurnalizare centrale) sunt găzduite în centre de date Tier III/IV certificate, cu amplasare geografică redundantă (centru primar + DR în zone seismice diferite, distanță minimă 100 km). Cerințele structurale includ: compartimentare anti-incendiu (REI 120), protecție anti-inundație, sisteme HVAC redundante, alimentare redundantă cu UPS și generatoare diesel autonome, conexiuni de rețea redundante prin furnizori diferiți.

5.1.2 Acces fizic

- Perimetru fizic cu badge access, urmărit prin sistem de monitorizare video 24/7.
- Zone de securitate cascade: zonă publică → zonă controlată (badge) → zonă securizată (badge + biometrie) → cameră HSM/CA (cvorum dual + biometrie).
- Toate accesările sunt jurnalizate; jurnalele sunt corelate cu activitățile sistemului.
- Vizitatorii sunt obligatoriu însoțiți, semnează NDA și sunt înregistrați video.
- Camerele cu HSM-uri sunt protejate cu sigilii anti-tamper și senzori de mișcare.

5.1.3 Energie și aer condiționat

Centrele de date dispun de UPS-uri cu autonomie minim 30 minute și generatoare diesel cu autonomie minim 72 ore (cu contracte de combustibil de urgență). HVAC redundant cu setpoint controlat (20–24 °C, umiditate 40–60%); monitorizare cu alarme la depășirea pragurilor.

5.1.4 Expunere la apă

Sistemele critice sunt amplasate la minim 30 cm peste pardoseală, cu detecție de scurgeri și sisteme automate de oprire alimentare apă.

5.1.5 Prevenirea și protecția împotriva incendiilor

Detecție foarte timpurie cu aspirație (VESDA), supresie cu gaz inert (Inergen sau echivalent), compartimentare REI 120, evacuare automatizată conform normativelor.

5.1.6 Stocarea mediilor

Mediile cu copii de siguranță offline (key shares, log-uri, snapshot-uri) sunt păstrate în seifuri certificate UL Class 350-2 (rezistență 2 ore la incendiu, 350 °F intern), în două locații geografic separate.

5.1.7 Eliminarea deșeurilor

Mediile care au conținut date sensibile sunt distruse fizic (shredding la nivel DIN 66399 P-7 pentru media optice/HDD, distrugere cu muta-cifrare pentru SSD-uri). Documentele tipărite sunt distruse cu shredder DIN 66399 P-5 minim. Procesul este urmărit prin certificat de distrugere și înregistrare video.

5.1.8 Backup off-site

Copiile de siguranță ale datelor critice (înregistrări de identificare, baza de date a certificatelor emise/revocate, jurnale de audit) sunt replicate online către locația DR și exportate offline pe medii criptate (LTO-9 cu AES-256-GCM) cu păstrare la o locație terță, contractuală.

5.2 Controale de procedură

5.2.1 Roluri de încredere (Trusted Roles)

QSIGN definește următoarele roluri de încredere, separate prin principiul Separation of Duties (SoD), conform ETSI EN 319 401 §7.4 și ETSI EN 319 411-2:

Rol	Responsabilități principale
Trust Service Officer (CISO)	Răspunde global de securitatea TSP-ului; aprobă politicile; relația cu ADR/auditori.
PKI Manager	Operarea zilnică a CA-urilor; gestiunea HSM-urilor; ceremonialele de cheie.
RA Officer	Aprobarea cererilor de certificat; supravegherea LRA-urilor.
RA Operator	Execuția identificării solicitanților; înregistrarea în sistem.
System Administrator	Administrare OS, baze de date, aplicații, infrastructură.
Network/Security Engineer	Firewall, IDS/IPS (Suricata), SIEM (Wazuh), monitorizare.
Auditor intern	Verificare independentă, conform programului anual; raport către CISO.
DPO	Conformitate GDPR; gestiunea drepturilor persoanelor vizate.
Compliance Officer	Conformitate eIDAS; raportarea către ADR; gestiunea Trust List.
Custodian de cheie (Key Custodian)	Membru al cvorumului pentru activarea cheilor Root CA și Issuing CA.

5.2.2 Numărul de persoane necesare per sarcină

- Activarea cheii Root CA: cvorum 3-din-5 custodieni de cheie cu smart card-uri personale, în prezența CISO și PKI Manager.
- Activarea cheilor Issuing CA Calificat: cvorum 2-din-3 plus PKI Manager.
- Emiterea certificatului Root CA / sub-CA: ceremonie filmată, cu witness independent (auditor).
- Modificarea politicilor de securitate: aprobare PMA + revizuire CISO + DPO.
- Acces la jurnalele de identificare nominalizate: permisiune RA Officer + DPO + jurnalizare integrală.

5.2.3 Identificare și autentificare pentru fiecare rol

Toți membrii personalului în roluri de încredere se autentifică în sisteme cu MFA: certificat hardware calificat (token QSCD personal) + parolă/PIN + (pentru roluri critice) biometrie. Sesiunile expiră după 15 minute de inactivitate; re-autentificare obligatorie pentru operațiuni privilegiate.

5.2.4 Roluri ce necesită separare

Conform principiului SoD, următoarele perechi de roluri NU pot fi îndeplinite de aceeași persoană: (i) PKI Manager și Auditor; (ii) RA Operator și RA Officer (aprobator); (iii) Custodian de cheie cu rol care emite certificate; (iv) DPO și CISO (deși ambele răspund de securitate, DPO trebuie să păstreze independența funcțională).

5.3 Controale de personal

5.3.1 Calificări, experiență, verificare

- Personalul în roluri de încredere are pregătire universitară în domenii relevante (IT, juridic, securitate informațională) sau certificări profesionale relevante.
- Pentru roluri tehnice: certificări recunoscute internațional (ex. CISSP, CISM, GICSP, OSCP, certificări de furnizor HSM).
- Pentru auditori: certificări lead auditor ISO 27001 sau ETSI EN 319 403.
- Verificare antecedente penale (cazier judiciar) la angajare și la fiecare 3 ani.
- Verificare credit bureau (pentru roluri cu acces la cheile criptografice critice).

5.3.2 Procedura de verificare la angajare

Cuprinde: verificare CV/referințe; verificare diplome; verificare antecedente penale; cazier fiscal; verificare cu listele PEP/sancțiuni; interviuri specializate; perioadă de probă cu instruire.

5.3.3 Cerințe de instruire

Toți angajații în roluri de încredere parcurg, la angajare și anual, programe de instruire pe:

- Reglementarea eIDAS și legislația națională aplicabilă (Legea 214/2024, GDPR, NIS2/OUG 155/2024).
- Politicile interne ale QSIGN (acest CP/CPS, Information Security Policy, Acceptable Use Policy).
- Standarde tehnice: ETSI EN 319 401, 319 411-1, 319 411-2, 319 412 (1–5), 319 421/422, RFC 5280, RFC 6960, RFC 3161.
- Securitate informatică, securitate cibernetică, social engineering, phishing.
- Operațiuni specifice rolului (RA, ceremonialele de cheie, OCSP, QTSA).
- Etică profesională și gestionarea conflictelor de interese.

Instruirile sunt evaluate prin teste; rezultatele și certificatele sunt arhivate.

5.3.4 Frecvența re-instruirii

Anual (minim), cu instruiri suplimentare la modificări semnificative ale politicilor, standardelor sau infrastructurii. Re-instruire obligatorie după orice incident de securitate.

5.3.5 Frecvența rotației rolurilor

Pentru rolurile critice, rotația este recomandată o dată la 3 ani (fără a afecta operativitatea), pentru a evita acumularea de cunoștințe punctuale și a permite verificări încrucișate.

5.3.6 Sancțiuni pentru abateri

Abaterile de la procedurile interne sunt analizate de Comitetul de Disciplină. Sancțiunile pot include: avertisment scris, suspendarea temporară a accesului, retragerea rolului de încredere, terminarea contractului. Faptele penale sunt sesizate organelor de urmărire penală.

5.3.7 Cerințe pentru contractori

Personalul terților părți (LRA-uri, furnizori de mentenanță, auditori) este obligat contractual să respecte aceleași cerințe ca personalul propriu și să semneze NDA-uri. Verificările la angajare se aplică egal, prin obligația contractuală a furnizorului.

5.3.8 Documentație furnizată personalului

Acest CP/CPS, politicile derivate, manualele de operare, manualele HSM, ghiduri specifice rolului, formularele standard, contactele de urgență.

5.4 Procedurile de jurnalizare a auditurilor

5.4.1 Tipuri de evenimente jurnalizate

- Toate operațiunile asupra cheilor (generare, activare, dezactivare, exportare backup, distrugere).
- Toate emiterele și revocările de certificate, cu detalii complete (timestamp, operator, identificator certificat).
- Toate cererile primite și deciziile RA, cu motivare în caz de respingere.
- Toate accesările sistemelor critice (autentificări reușite și nereușite).
- Modificările configurației sistemelor (managementul schimbărilor).
- Activarea/dezactivarea componentelor critice (Issuing CA, OCSP, QTSA, repository).
- Toate evenimentele de securitate detectate (IDS/IPS, SIEM, Suricata, Wazuh).
- Toate accesele fizice la zonele securizate.
- Sesiunile video de identificare la distanță (cu păstrarea integrală a înregistrării).
- Migrațiile sau modificările arhitecturii.

5.4.2 Frecvența procesării jurnalelor

Jurnalele sunt agregate în timp real de SIEM-ul QSIGN (Wazuh + custom analytics). Reviziile umane se realizează: (i) zilnic — review automat cu alerting; (ii) săptămânal — review manual de către CISO/Security Engineer pentru tendințe; (iii) lunar — analiză statistică agregată; (iv) anual — review formal pentru raportul anual de transparență.

5.4.3 Perioada de păstrare a jurnalelor de audit

Jurnalele sunt păstrate, cu integritate criptografică, conform următoarelor termene minime: (i) jurnalele privind certificatele (emitere, revocare, statusuri) — minim 10 ani de la încetarea valabilității certificatului (art. 12 alin. (2) lit. i) și art. 16 alin. (2) din Legea 214/2024); (ii) jurnalele de identificare (inclusiv sesiuni video) — minim 7 ani de la încetarea valabilității certificatului (ETSI TS 119 461 / Ordin MEDAT 102/2026); (iii) jurnalele operaționale și de securitate — minim 10 ani; (iv) jurnale QTSA — minim 10 ani; (v) sigilarea criptografică zilnică, cu re-marcare temporală calificată la fiecare 3 ani.

5.4.4 Protecția jurnalului de audit

Jurnalele sunt protejate prin: (i) integritate criptografică — fiecare înregistrare este sigilată în lanț (chaining cu hash-uri SHA-384) și mărci temporale calificate; (ii) replicare în timp real către locația DR; (iii) acces strict limitat (read-only pentru analiști, modificare imposibilă fără cvorum CISO+DPO+Auditor); (iv) imutabilitate — sistemele de stocare suportă WORM (Write Once Read Many) sau replication append-only; (v) backup offline pe LTO-9 criptat.

5.4.5 Procedura de backup a jurnalului

Backup zilnic (incremental) + săptămânal (full) către sistemul DR; export săptămânal pe medii LTO-9 către locație terță (off-site); test de restaurare trimestrial.

5.4.6 Sistemul de colectare a evenimentelor de audit

SIEM bazat pe Wazuh, integrat cu rsyslog și fluentd; agenți pe fiecare componentă; eventual corelații cu Suricata IDS. Întregul sistem este sigilat criptografic și jurnalizat cu marcă temporală internă (rolling timestamp).

5.4.7 Notificarea entității ce a generat evenimentul

Evenimentele de securitate sunt notificate prin alertare automată către SOC; gravitatea "critică" generează apel telefonic + SMS + e-mail către responsabilii desemnați (CISO, PKI Manager, DPO).

5.4.8 Evaluarea vulnerabilității

Vulnerability scanning automatizat (zilnic, săptămânal); penetration testing extern (anual minim, plus la modificări majore); reviziile aplicate și retestate.

5.5 Arhivarea înregistrărilor

Toate înregistrările care au valoare probatorie pentru certificatele emise (dosare de cerere, semnături ale solicitanților, sesiuni video, decizii de aprobare/respingere, jurnale de emitere, CRL-uri, OCSP-stat istoric, mărci temporale ale evenimentelor) sunt arhivate într-un sistem electronic de arhivare calificat (cu suport LTP — Long-Term Preservation), fie sistemul propriu al QSIGN avizat ADR conform Anexei 5 la Decizia 162/2026, fie prin contractare cu un administrator de arhivă electronică acreditat conform Legii 135/2007. Arhivarea respectă cerințele LTP — re-marcare temporală calificată periodică, migrări controlate de format, raport de integritate la fiecare extragere.

5.6 Schimbarea cheii (key changeover)

Pentru toate CA-urile, schimbarea cheii (key rollover) se planifică cu cel puțin 12 luni înainte de expirare. Procedură: (i) generare cheie nouă în HSM, în ceremonie filmată, cu cvorum custodieni; (ii) auto-semnare certificat nou (pentru Root CA) sau semnare de către Root cu cheia precedentă (pentru sub-CA); (iii) publicare cheie publică nouă în repository și notificare ADR pentru actualizare TL; (iv) cross-sign între cheia veche și cheia nouă pentru tranziție graduală; (v) emiterea de certificate noi continuă cu cheia nouă; (vi) cheia veche rămâne activă doar pentru semnarea CRL-urilor existente, până la expirarea ultimului certificat emis cu ea.

5.7 Compromitere și recuperare în caz de dezastru

5.7.1 Procedurile de gestiune a incidentelor

QSIGN dispune de un Plan de Răspuns la Incidente de Securitate (Incident Response Plan — IRP), aprobat de CISO. Etapele de gestiune: detectare → triere/clasificare → izolare → eradicare → recuperare → lecții învățate. Notificările legale obligatorii: ADR (în maxim 24 ore — art. 19 alin. (2) eIDAS, art. 12 alin. (1) lit. (b) din Anexa 4 la Decizia 162/2026), ANSPDCP (în maxim 72 ore dacă există afectare a datelor cu caracter personal — art. 33 GDPR), DNSC (conform NIS2/OUG 155/2024, dacă incidentul se încadrează).

5.7.2 Resurse computaționale, software și/sau date corupte

Detecția de corupere prin: (i) verificarea integrității criptografice a jurnalelor; (ii) checksum-uri pe fișierele de configurare critice; (iii) IDS/IPS Suricata; (iv) Wazuh File Integrity Monitoring (FIM); (v) verificări automate de conformitate ale CA și OCSP. La detecție: izolarea componentei, evaluare impact, restaurare din backup, RCA (Root Cause Analysis), implementare contramăsuri.

5.7.3 Compromiterea cheii private a CA

Compromiterea unei chei CA este situația de cea mai mare gravitate. Procedură:

34. Suspendarea imediată a tuturor operațiunilor de emitere și a OCSP-ului afectat.
35. Notificarea ADR în maxim 24 ore, telefonic și în scris.
36. Notificarea publică prin repository și e-mail către titularii afectați.
37. Revocarea cheii compromise prin includerea sa în CRL-ul Root (sau, în cazul Root, prin protocoale de excludere din Trust List).
38. Activarea procedurii de cheie nouă, cu generarea într-o ceremonie de cheie de urgență.
39. Re-emiterea certificatelor afectate sub noul lanț, după validarea controlată a fiecărui titular.
40. Investigație criminalistică completă (forensics).
41. Raport final și remediation plan, transmise ADR și auditorului.

5.7.4 Continuitatea afacerii după dezastru

BCP/DRP-ul QSIGN definește RTO (Recovery Time Objective) ≤ 4 ore pentru servicii critice (OCSP, CRL, QTSA) și ≤ 24 ore pentru funcțiile RA. RPO (Recovery Point Objective) ≤ 5 minute pentru bazele de date ale certificatelor. Centrul DR este operațional în mod hot-standby, cu replicare sincronă (DRBD) pentru date critice și replicare async pentru log-uri masive. Testele DR se efectuează semestrial; rapoartele sunt arhivate.

5.8 Încetarea CA sau RA

Planul de încetare (Termination Plan, conform art. 24 alin. (2) lit. (i) eIDAS) prevede:

42. Notificarea ADR cu minim 30 de zile înainte (art. 13 alin. (1) din Legea 214/2024).
43. Notificarea tuturor titularilor activi cu cel puțin 30 de zile înainte, cu opțiunea de transfer la alt prestator (art. 13 alin. (3) din Legea 214/2024).
44. Identificarea unui prestator succesor calificat pentru preluarea bazei de date a certificatelor și a OCSP/CRL pe perioada reziduală a valabilității certificatelor.

45. Dacă nu există succesor: revocarea tuturor certificatelor înaintea încetării (art. 22 alin. (3) din Legea 214/2024); preluarea evidenței de către ADR.
46. Predarea către arhiva electronică acreditată/calificată a tuturor înregistrărilor cu valoare probatorie, cu menținerea LTP timp de minim 10 ani.
47. Distrugerea controlată a cheilor private (în ceremonie filmată).
48. Publicarea raportului final de încetare.

6. Controale de securitate tehnică

6.1 Generarea perechii de chei și instalarea

6.1.1 Generarea perechii de chei

Tip cheie	Locul generării	Algoritm și lungime	Cerință tehnică
Root CA	HSM offline (FIPS 140-3 L3 / EAL 4+ AVA_VAN.5)	RSA 4096 sau ECDSA P-384	Ceremonie cu cvorum 3-din-5; filmare; auditor martor
Issuing CA — Calificat	HSM online (FIPS 140-3 L3 / EAL 4+ / EN 419 221-5)	RSA 4096 sau ECDSA P-384	Ceremonie 2-din-3 + PKI Manager
QTSA	HSM dedicat (EN 419 221-5)	RSA 3072+ sau ECDSA P-256+	Generare cu cvorum și witness
OCSP Responder	HSM dedicat	RSA 2048+ sau ECDSA P-256	Cheie cu validitate ≤ 1 an, rotație frecventă
Subscriber — QCP-n-qscd, QCP-l-qscd	QSCD certificat (token sau remote QSCD în HSM TSP, EN 419 241-2)	RSA 2048+ sau ECDSA P-256+	Sub controlul exclusiv al titularului prin SAD
Subscriber — QCP-n, QCP-l (fără QSCD)	Mediu securizat al titularului sau HSM TSP	RSA 2048+ sau ECDSA P-256+	Conform politicii de securitate

6.1.2 Livrarea cheii private către titular

Pentru certificate emise pe token fizic (smart card, USB token), tokenul este livrat fizic, sigilat, iar PIN-ul inițial este transmis pe canal separat (e-mail criptat sau SMS). Pentru certificate cu QSCD la distanță (remote QSCD — QCP-n-qscd, QCP-l-qscd), cheia privată nu părăsește niciodată HSM-ul TSP-ului — este controlată exclusiv prin Signature Activation Data (SAD) al titularului, conform EN 419 241-2. Pentru certificate fără QSCD (QCP-n, QCP-l) cu cheie generată în mediul titularului, cheia rămâne în acel mediu și nu este transmisă.

6.1.3 Livrarea cheii publice către emitent

Cheia publică este livrată sub forma unui CSR PKCS#10 semnat cu cheia privată corespunzătoare (PoP). Pentru cheile generate în QSCD remote operat de QSIGN, livrarea internă este efectuată prin canalul HSM-to-CA în interiorul perimetrului de încredere.

6.1.4 Livrarea cheii publice CA către relying parties

Prin includerea în Lista sigură națională (Trusted List) operată de ADR, prin publicare în repository-ul QSIGN, prin LOTL european.

6.1.5 Lungimi și algoritmi de cheie

Algoritmii și lungimile de cheie utilizate respectă recomandările ENISA și ETSI TS 119 312. Algoritmi actuali: RSA 2048+ biți (preferat 3072+ pentru chei cu durată > 5 ani; 4096 pentru CA); ECDSA curbă P-256, P-384 (curbe NIST aprobate FIPS 186-5); EdDSA Ed25519 / Ed448 (recomandare emergentă, în implementare pilot). Pentru hashing: SHA-256 minim, recomandat SHA-384 pentru CA-uri și marcă

temporală. Migrarea la algoritmi post-cuantici (ML-DSA / FN-DSA, conform NIST FIPS 204/205) este urmărită activ; QSIGN va implementa hibrizi PQC odată ce ETSI publică specificațiile aplicabile certificatelor calificate.

6.1.6 Generarea parametrilor cheii publice și verificarea calității

Toate cheile sunt generate în HSM-uri certificate, cu generatoare de numere aleatorii hardware (TRNG) validate. Pentru RSA: verificarea primalității Miller-Rabin cu nivel ridicat de încredere; pentru ECDSA: verificarea că punctul generat este pe curbă; verificarea ordinului. Sunt rejectate chei cu pattern-uri slabe (verificate față de baza de date NIST de chei vulnerabile cunoscute — ROCA etc.).

6.1.7 Scopurile de utilizare a cheii

Definite prin extensia KeyUsage (RFC 5280) și ExtendedKeyUsage. Detalii în secțiunea 7.1.2.

6.2 Protecția cheii private și controale tehnice ale modulului criptografic

6.2.1 Standardele și controalele HSM

- Toate HSM-urile QSIGN sunt certificate FIPS 140-3 Nivel 3 minimum sau Common Criteria EAL 4+ AVA_VAN.5 (compatibil EN 419 221-5).
- Pentru gestiune QSCD la distanță (remote QSCD): conformitate cu EN 419 241-2 (Trustworthy Systems Supporting Server Signing) și EN 419 221-5; certificare ca QSCD conform Reg. de punere în aplicare (UE) 2025/1567.
- Inventarul HSM cu serial number, atestare la nivel de firmware, status de tamper-evident, urmărit prin sistem dedicat.

6.2.2 Controlul cheii private (m-of-n)

Activarea cheii Root CA: cvorum 3-din-5 custodieni de cheie cu smart card-uri personale. Activarea cheii Issuing CA Calificat: cvorum 2-din-3 plus PKI Manager. Toate ceremonialele sunt jurnalizate, filmate și asistate de auditor independent.

6.2.3 Escrow al cheii private

Cheile CA NU sunt escrow-ate la terți. Backup-urile de chei CA sunt criptate cu AES-256-GCM cu chei master derivate prin Shamir Secret Sharing 3-din-5 (custodieni distincți, păstrați în seifuri diferite). Cheile titularilor calificate (semnătură/sigiliu) NU fac obiectul niciunei forme de escrow — cerință strictă a art. 24 alin. (2) lit. (j) eIDAS.

6.2.4 Backup al cheii private

Backup periodic al cheilor CA (lunar pentru active, anual pentru offline) în HSM-uri secundare; transferurile între HSM-uri se fac prin protocol HSM-to-HSM (M-of-N wrapping). Restaurarea necesită cvorum identic. Cheile titularilor calificate NU sunt back-up-ate de TSP.

6.2.5 Arhivarea cheii private

La expirarea cheii CA, aceasta este arhivată în HSM offline (off-line vault) timp de minim 10 ani după expirare, pentru a permite verificarea istorică a semnăturilor (CRL-uri vechi). Cheia nu mai este utilizată pentru emitere.

6.2.6 Transferul cheii private

Transferul între HSM-uri active se face prin canal HSM-to-HSM cu wrap key derivat criptografic. Transferul către locația DR este efectuat în condiții similare. Transferul în afara mediilor controlate este interzis.

6.2.7 Stocarea cheii private în modulul criptografic

Toate cheile private sunt stocate exclusiv în HSM-uri, niciodată în memoria sistemelor sau pe disk în clar. Accesul la chei se face exclusiv prin operațiuni HSM autorizate.

6.2.8 Activarea cheii private

Cheile CA sunt activate prin cvorum, conform 6.2.2. Cheile titularilor se activează prin autentificarea titularului: PIN local (pentru smart card / token), SAD (pentru remote QSCD), MFA puternic (pentru operațiuni administrative).

6.2.9 Dezactivarea cheii private

Sesiunile HSM expiră după inactivitate; cheile titularilor se dezactivează după fiecare operațiune sau după timeout configurat. Sesiunile critice se închid manual de către operator.

6.2.10 Distrugerea cheii private

La sfârșitul ciclului de viață, cheia este distrusă criptografic prin operațiunea HSM "zeroize" (suprascriere multipasă). Distrugerea fizică a HSM-ului (la decommissioning) urmează specificațiile producătorului — degaussing + shredding fizic.

6.2.11 Evaluarea modulului criptografic

HSM-urile sunt evaluate conform certificărilor menționate (FIPS 140-3, CC EAL 4+ AVA_VAN.5). Re-evaluarea este urmărită prin programul de update firmware al furnizorului.

6.3 Alte aspecte ale gestionării cheii

6.3.1 Arhivarea cheii publice

Toate cheile publice ale CA-urilor și ale titularilor (prin certificate) sunt arhivate ca parte a sistemului electronic de arhivare timp de minim 35 ani.

6.3.2 Perioada operațională a certificatelor și a perechilor de chei

Element	Validitate certificat	Validitate cheie privată
Root CA	20 ani	20 ani (utilizare exclusivă pentru sub-CA)
Issuing CA — Calificat (Signature)	10 ani	7 ani (ulterior doar pentru semnare CRL)
Issuing CA — Calificat (Seal)	10 ani	7 ani
QTSA — calificată	5 ani (cu re-key periodic)	3 ani efectiv
OCSP Responder	1 an (auto-rotație)	1 an

Element	Validitate certificat	Validitate cheie privată
Subscriber — QCP-n / QCP-n-qscd	Maxim 3 ani (recomandat 1 an)	Egală cu valabilitatea certificatului
Subscriber — QCP-l / QCP-l-qscd	Maxim 3 ani	Egală cu valabilitatea certificatului

6.4 Date de activare

PIN-uri, parole și alte date de activare (inclusiv SAD pentru remote QSCD) sunt: generate aleator de către sistem; transmise pe canale separate; obligatorie schimbarea la prima utilizare; complexitate minimă (8 caractere, alfanumerice + simboluri, sau echivalent în entropie); încercări limitate (5 încercări nereușite → blocare).

6.5 Controale de securitate ale calculatoarelor

- Hardening OS conform CIS Benchmarks; utilizare distribuții Linux minimaliste (Debian / Ubuntu LTS / sisteme custom Buildroot pentru appliances).
- Sisteme dedicate funcției: nu se permite utilizare multifuncțională a serverelor critice.
- Patching planificat (lunar pentru update-uri uzuale, urgent pentru CVE critice).
- Antivirus / EDR pe stațiile de lucru și serverele de aplicații; nu pe sistemele HSM-only.
- Toate sistemele rulează cu privilegii minime (least privilege).
- Sisteme critice operează în mod airgap (Root CA) sau în VLAN-uri izolate cu firewall stateful (Issuing CA, HSM-uri online).

6.6 Controale tehnice ale ciclului de viață

- Dezvoltare software conform Secure SDLC (SAST, DAST, dependency scanning).
- Code review obligatoriu pentru orice modificare a componentelor critice; minim 2 revizori.
- Mediu de testare separat de producție; date sintetice utilizate; date de producție anonimizate când e necesar.
- Change management formal: RFC → analiză impact → aprobare CISO → implementare → test → rollback plan.
- Versionare cu Git; pipeline CI/CD cu semnături obligatorii pe tag-uri; deploy-uri imutabile (containere semnate).

6.7 Controale de securitate a rețelei

- Arhitectură "defense in depth" cu multiple straturi (perimetru → DMZ → zone aplicații → zone de date → zona criptografică).
- Firewall principal cu nftables (BPI-R4 sau echivalent enterprise) cu politică default-deny; reguli minime explicite.
- IDS/IPS Suricata pe traficul perimetral și inter-zone; semnături Emerging Threats actualizate; alertare în Wazuh.
- Monitorizare DDoS și capacități anti-DDoS; integrare cu DNSC pentru notificare incidentelor și mitigation coordonat.

- Conexiuni externe critice (mTLS pentru auth.qsign.ro, OCSP, QTSA) cu certificate dedicate; logging XFF pentru identificarea atacatorilor reali.
- Knockd / port knocking pentru endpoint-urile administrative (pre-condiție pentru SSH).
- Segmentare strictă: zonele Root CA și HSM critice nu au conectivitate la internet.
- VPN pentru personal remote: WireGuard sau OpenVPN cu certificate hardware obligatorii.
- Wazuh SIEM pentru corelație centralizată a evenimentelor.

6.8 Marcarea temporală (time-stamping)

QSIGN operează un serviciu Qualified Time-Stamping Authority (QTSA), în conformitate cu art. 42 eIDAS, ETSI EN 319 421 (politica TSA) și ETSI EN 319 422 (protocoale RFC 3161 / RFC 5816). Politica detaliată QTSA este publicată ca document anexă (QSIGN-TSA-Policy). Caracteristici sumare:

- Cerere/răspuns conform RFC 3161 (TimeStampReq / TimeStampResp).
- Precizia mărcii temporale: ≤ ±1 secundă față de UTC; pentru aplicații care necesită precizie mai mare, ≤ ±1 ms (art. 7 alin. (1) Anexa 2 la Decizia 162/2026).
- Surse de timp: 3 surse stratum-1 NTP independente: PTB Germania (ptbtime1–4.ptb.de) ca primar, NIST SUA (time.nist.gov) ca secundar, INRIM Italia (ntp1.inrim.it) ca terțiar; suport NTS (RFC 8915) acolo unde este disponibil.
- Două surse independente cu verificare de consistență (art. 7 alin. (2) Anexa 2 Decizie 162/2026).
- Sigilarea criptografică zilnică a jurnalelor TSA, cu re-marcare la fiecare 3 ani (art. 7 alin. (3) Anexa 2 Decizie 162/2026).
- Cheia QTSA este în HSM dedicat, separat de cheile CA.
- Disponibilitate ≥ 99,95%.
- Audit logs păstrate minim 10 ani.

7. Profilurile certificatelor, CRL și OCSP

7.1 Profilul certificatelor

7.1.1 Câmpuri de bază (Base Certificate Fields)

Toate certificatele calificate emise de QSIGN sunt X.509 v3, conforme cu RFC 5280 și ETSI EN 319 412 (părțile 1, 2, 3, 5). Câmpurile de bază sunt:

Câmp	Valoare / Format
Version	v3 (valoare 2)
Serial Number	Aleator, minim 64 biți entropie, unicitate per Issuing CA
Signature Algorithm	sha384WithRSAEncryption (preferat) sau ecdsa-with-SHA384 / ecdsa-with-SHA256
Issuer DN	DN-ul Issuing CA, conform structurii prezentate în Capitolul 1.3
Validity (notBefore, notAfter)	Conform tipului de certificat (vezi tabelul de la 6.3.2)
Subject DN	Conform politicii și ETSI EN 319 412 (vezi 7.1.4)
Subject Public Key Info	RSA 2048+ sau ECDSA P-256/P-384
Signature	Semnătura Issuing CA aplicată asupra TBSCertificate

7.1.2 Extensii (Extensions)

7.1.2.1 KeyUsage (RFC 5280 §4.2.1.3)

Tip certificat calificat	KeyUsage (critică)
Root CA	keyCertSign, cRLSign
Issuing CA	keyCertSign, cRLSign
QTSA	digitalSignature, nonRepudiation
OCSP Responder	digitalSignature
Subscriber — QCP-n / QCP-n-qscd	nonRepudiation (cu/fără digitalSignature, conform politicii titularului)
Subscriber — QCP-l / QCP-l-qscd	nonRepudiation

7.1.2.2 ExtendedKeyUsage (EKU)

Pentru certificate de signatari/sigilii calificate, EKU este de regulă absent. Pentru QTSA: id-kp-timeStamping (1.3.6.1.5.5.7.3.8) marcată drept critical. Pentru OCSP: id-kp-OCSPSigning (1.3.6.1.5.5.7.3.9).

7.1.2.3 BasicConstraints

CA=TRUE pentru Root CA (cu pathLenConstraint=1) și pentru Issuing CA (pathLenConstraint=0). CA=FALSE pentru toate celelalte.

7.1.2.4 SubjectKeyIdentifier și AuthorityKeyIdentifier

Ambele extensii sunt obligatorii pe toate certificatele, conform RFC 5280. SKI calculat ca SHA-1 al cheii publice (metoda 1 din RFC 5280).

7.1.2.5 CertificatePolicies

Conține OID-ul politicii de certificat aplicabile (vezi Capitolul 1.2). Pentru certificate calificate, include și PolicyQualifierInfo cu id-qt-cps (URI către CPS) și id-qt-unotice (text scurt cu mențiunea "This is a qualified certificate issued in accordance with Regulation (EU) 910/2014 ...").

7.1.2.6 CRLDistributionPoints

URI HTTP(S) către CRL-ul Issuing CA. Exemple: http://crl.qsign.ro/qualified-sign-ca-g1.crl, http://crl.qsign.ro/qualified-seal-ca-g1.crl

7.1.2.7 AuthorityInformationAccess (AIA)

- ocsp = http://ocsp.qsign.ro/qualified-sign-ca-g1 (URL OCSP responder)
- caIssuers = http://crt.qsign.ro/qualified-sign-ca-g1.cer (URL pentru certificatul Issuing CA)

7.1.2.8 SubjectAlternativeName (SAN)

Pentru certificate de semnătură electronică calificată: opțional rfc822Name (e-mail-ul titularului). Pentru sigilii calificate: opțional URI sau dNSName asociate organizației.

7.1.2.9 QCStatements (ETSI EN 319 412-5) — OBLIGATORIU pentru certificate calificate

Pentru certificatele calificate, extensia QCStatements (OID 1.3.6.1.5.5.7.1.3) este obligatorie și conține:

- **id-etsi-qcs-QcCompliance** (0.4.0.1862.1.1) — declarație de conformitate cu eIDAS (cerință obligatorie pentru toate certificatele calificate).
- **id-etsi-qcs-QcType** — tipul certificatului: id-etsi-qct-esign (0.4.0.1862.1.6.1) pentru semnătură (QCP-n, QCP-n-qscd); id-etsi-qct-eseal (0.4.0.1862.1.6.2) pentru sigiliu (QCP-l, QCP-l-qscd).
- **id-etsi-qcs-QcSSCD** (0.4.0.1862.1.4) — prezent dacă cheia este în QSCD (variantele -qscd: QCP-n-qscd, QCP-l-qscd).
- **id-etsi-qcs-QcPDS** (0.4.0.1862.1.5) — URI și limbă pentru PKI Disclosure Statement.
- **id-etsi-qcs-QcLimitValue** (0.4.0.1862.1.2) — opțional, valoare maximă a tranzacțiilor.
- **id-etsi-qcs-QcRetentionPeriod** (0.4.0.1862.1.3) — perioada de păstrare a informațiilor de identificare (10 ani, conform Legii 214/2024).

7.1.3 OID algoritmi

Conform recomandărilor ETSI TS 119 312 și NIST FIPS:

Algoritm	OID	Utilizare
sha256WithRSAEncryption	1.2.840.113549.1.1.11	Semnătura certificatelor (suport general)
sha384WithRSAEncryption	1.2.840.113549.1.1.12	Semnătura certificatelor (preferat pentru CA)
sha512WithRSAEncryption	1.2.840.113549.1.1.13	Pentru chei RSA 4096+
ecdsa-with-SHA256	1.2.840.10045.4.3.2	Cheie ECDSA P-256

Algoritm	OID	Utilizare
ecdsa-with-SHA384	1.2.840.10045.4.3.3	Cheie ECDSA P-384
rsaEncryption	1.2.840.113549.1.1.1	Cheie publică RSA
id-ecPublicKey	1.2.840.10045.2.1	Cheie publică ECDSA

7.1.4 Forme de nume

Pentru certificate QCP-n / QCP-n-qscd (persoane fizice):

- CN = numele complet al persoanei (Prenume Nume)
- GN = prenumele
- SN = numele de familie
- serialNumber = identificator unic stabil; format ETSI EN 319 412-1: "PNORO-<CNP>" pentru cetățeni români (natural person semantic identifier); "PI:<eIDAS_PID>" pentru identificatori eIDAS
- C = RO (sau codul de țară al titularului)
- title (opțional) = funcție/titlu profesional (cu verificare la sursă)
- organizationName + organizationIdentifier (opțional) = afilierea profesională (cu verificare specifică)

Pentru certificate QCP-l / QCP-l-qscd (persoane juridice):

- CN = denumirea juridică sau denumirea comercială (max 64 caractere)
- organizationName = denumirea juridică oficială
- organizationIdentifier = format ETSI EN 319 412-1: "NTRRO-<numărul ONRC>" sau "VATRO-<CIF>"
- C = RO
- L (locality), ST (state) — opțional

7.1.5 Constrângeri ale numelor

La nivelul Issuing CA, NameConstraints sunt aplicate dacă politica specifică prevede limitări (de exemplu, restricționarea la titulari români). Aceste constrângeri sunt declarate explicit în certificatul Issuing CA.

7.1.6 OID politică de certificat

Vezi tabelul din Capitolul 1.2.

7.1.7 Utilizarea extensiei PolicyConstraints

Nu este utilizată în mod implicit; potențial inclusă în certificate Issuing CA pentru forțarea evaluării politicii.

7.1.8 Sintaxa și semantica calificatorilor de politică

Calificatorii includ id-qt-cps (URI CPS) și id-qt-unotice (text concis) conform RFC 5280.

7.2 Profilul CRL

CRL-uri X.509 v2, conform RFC 5280, semnate cu cheia Issuing CA emitente. Conțin:

- Version = v2

- Signature algorithm — algoritmul corespunzător cheii Issuing CA
- Issuer DN
- ThisUpdate / NextUpdate
- Lista certificatelor revocate (Revoked Certificates) cu serial number, revocationDate, opțional reason code (CRLReason)
- Extensii: AuthorityKeyIdentifier, CRLNumber (monoton crescător), opțional IssuingDistributionPoint

7.3 Profilul OCSP

Răspunsuri OCSP conform RFC 6960:

- Profil basic OCSP response, semnat cu certificat OCSP delegat (id-pkix-ocsp-nocheck — extensia care indică validatorului să nu interogheze status-ul OCSP-ului însuși)
- Status returnat: good, revoked, unknown
- ThisUpdate ≤ 1 oră de la cererea curentă
- NextUpdate ≤ 7 zile
- Suport HTTP GET (cu cache pe path-uri Base64-encodate, conform RFC 5019) și POST
- Disponibilitate continuă (24/7), conform art. 6 alin. (1) din Anexa 2 la Decizia 162/2026

8. Audituri de conformitate și alte evaluări

8.1 Frecvența și circumstanțele evaluărilor

Conform art. 20 alin. (1) din Reg. (UE) nr. 910/2014, conform Anexei 4 la Decizia ADR 162/2026 (art. 2) și conform art. 7 alin. (1) din Anexa 1 la Ordinul MEDAT 102/2026, prestatorii de servicii de încredere calificate sunt evaluați, pe propria cheltuială, la cel puțin fiecare 24 de luni, de un organism de evaluare a conformității acreditat.

Audituri suplimentare se efectuează în următoarele circumstanțe:

- La inițierea unui nou serviciu de încredere calificat.
- La schimbări semnificative ale arhitecturii tehnice, organizatorice sau procedurale.
- La cererea ADR sau ca urmare a unui control al organismului de supraveghere.
- După un incident de securitate sau o compromitere de cheie.

8.2 Identitatea și calificările auditorului

Organism de evaluare a conformității (CAB), acreditat (în România) sau de alt organism național de acreditare din UE recunoscut, conform Reg. (CE) 765/2008, pe baza schemelor ETSI EN 319 403-1. Auditorul principal (lead auditor) trebuie să îndeplinească cerințele ETSI EN 319 403-1 pentru auditori eIDAS și să dețină experiența necesară pentru evaluarea conformității cu ETSI EN 319 411-2.

8.3 Relația auditorului cu entitatea evaluată

Auditorul trebuie să fie independent de QSIGN, fără conflict de interese. Declarația conflictului de interese a auditorului face parte din raportul de evaluare a conformității, conform Anexei 2 punct 10 la Ordinul MEDAT 102/2026.

8.4 Domeniul de aplicare al evaluării

Auditul cuprinde:

- Auditul arhitecturii — verificarea măsurilor de securitate la nivelul rețelelor și sistemelor.
- Auditul de configurare — verificarea implementării măsurilor în configurația concretă.
- Auditul de penetrare (penetration testing) — extern și intern.
- Auditul securității organizaționale — politici, proceduri, instruire.
- Verificarea respectării politicilor declarate (acest CP/CPS, Politica QTSA, Politica de validare/preservation).
- Conformitatea cu standardele aplicabile: ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2, ETSI EN 319 412 (1–5), ETSI EN 319 421/422, ETSI TS 119 461.
- Conformitatea cu Reg. (UE) 910/2014 (modificat prin Reg. UE 2024/1183) și Legea 214/2024.
- Verificarea conformității QSCD-urilor (EN 419 221-5 / EN 419 241-2 pentru remote QSCD).

8.5 Acțiuni întreprinse ca rezultat al deficiențelor

Neconformitățile sunt clasificate în 4 niveluri (conform art. 24 din Anexa 4 la Decizia 162/2026): minoră, medie, majoră, critică. QSIGN elaborează un Plan de Conformare cu termene precise:

- 60 zile pentru neconformități minore.
- 30 zile pentru neconformități medii.
- 15 zile pentru neconformități majore.
- Imediat (suspendarea serviciului) pentru neconformități critice.

Raportul de implementare a măsurilor este transmis ADR și auditorului, urmat de re-verificare.

8.6 Comunicarea rezultatelor

Raportul de evaluare a conformității este transmis ADR în termen de cinci zile lucrătoare de la primire (art. 2 din Anexa 4 la Decizia 162/2026, art. 7 alin. (2) din Anexa 1 la Ordinul MEDAT 102/2026). Sumar al rezultatelor (fără detalii de securitate confidențiale) este publicat în repository și în raportul anual de transparență.

9. Alte aspecte de afaceri și juridice

9.1 Tarife

Tarifele aplicabile serviciilor sunt publicate pe www.qsign.ro și sunt parte integrantă a Subscriber Agreement. Tarifele actuale acoperă: emiterea inițială, re-key, revocarea (gratuită), marcarea temporală, validarea, conservarea pe termen lung. Tarifele percepute de ADR (2.500 lei cu TVA inclus per serviciu de încredere pentru care se solicită acordarea statutului sau notificarea, conform art. 1 din Decizia 162/2026) sunt achitate de QSIGN și nu sunt re-facturate individual către titulari.

9.2 Răspunderea financiară și asigurarea

QSIGN deține o asigurare de răspundere civilă profesională sau scrisoare de garanție bancară pentru riscurile legate de prestarea serviciilor de încredere calificate, în valoare de 500.000 EUR pentru fiecare serviciu calificat (art. 5 alin. (2) lit. b) din Anexa 1 la Ordinul MEDAT 102/2026 și art. 3 alin. (2) lit. b) din Anexa 1 la Decizia 162/2026), cesionată în favoarea ADR. Asigurarea acoperă inclusiv pretențiile terților rezultate din încălcări ale Reg. (UE) 910/2014 și Legii 214/2024 (art. 13 eIDAS — răspunderea TSP).

9.3 Confidențialitatea informațiilor de afaceri

Toate informațiile primite de la titulari, relying parties și parteneri sunt tratate cu strictă confidențialitate, conform secretului profesional impus prin art. 11 alin. (5) din Legea 214/2024. Excepții: informațiile pe care titularul a consimțit să le facă publice (de exemplu, certificatul în sine, în cazul publicării opționale), și informațiile solicitate prin lege de autoritățile competente.

9.4 Confidențialitatea informațiilor cu caracter personal

Prelucrarea datelor cu caracter personal se efectuează în conformitate cu Reg. (UE) 2016/679 (GDPR), Legea 190/2018 și Politica de protecție a datelor a QSIGN, publicată în repository. Bazele juridice ale prelucrării: (i) executarea contractului de prestare a serviciilor; (ii) obligațiile legale (eIDAS, Legea 214/2024 — păstrare 10 ani); (iii) interesul legitim al QSIGN și al utilizatorilor (securitate, prevenirea fraudei). Datele sunt păstrate pe durata stabilită de lege; după expirarea termenului, se realizează ștergerea sau anonimizarea controlată. DPO este disponibil ca punct de contact dedicat pentru cereri ale persoanelor vizate.

9.5 Drepturi de proprietate intelectuală

Acest CP/CPS este proprietatea QSIGN. Distribuția neautorizată este interzisă; utilizarea în scopuri informaționale sau de validare este permisă cu citarea sursei. Software-ul, marca "QSIGN" și designurile sunt protejate prin drepturi de autor și marcă de comerț, în condițiile legii române.

9.6 Reprezentări și garanții

9.6.1 Reprezentările QSIGN

- Conformitatea cu cerințele Reg. (UE) 910/2014 (modificat prin Reg. UE 2024/1183) și legislației naționale aplicabile.

- Acuratețea informațiilor incluse în certificatele calificate la momentul emiterii.
- Funcționalitatea și disponibilitatea infrastructurii (CRL, OCSP, QTSA, repository) la nivelul SLA declarat.
- Tratarea cu diligență a cererilor de revocare în termenele legale (24 ore).
- Respectarea confidențialității și a obligațiilor de protecție a datelor.
- Notificarea ADR și a titularilor cu privire la incidentele de securitate, în termenele legale.

9.6.2 Reprezentările titularilor

- Acuratețea și integritatea informațiilor furnizate la cerere.
- Păstrarea cheii private sub control exclusiv.
- Utilizarea certificatului exclusiv în scopurile permise.
- Solicitarea revocării în termenele și condițiile prevăzute (art. 26 alin. (2) Legea 214/2024).
- Acceptarea termenilor și condițiilor.

9.6.3 Reprezentările relying parties

- Verificarea valabilității certificatului înainte de a se baza pe acesta (CRL/OCSP la momentul utilizării).
- Verificarea adecvării politicii certificatului la cazul de utilizare.
- Acceptarea termenilor Relying Party Agreement.
- Construirea și validarea lanțului de încredere până la o ancoră oficială (Trusted List națională / LOTL UE).

9.7 Limitarea răspunderii

Răspunderea QSIGN este reglementată de art. 13 din Reg. (UE) 910/2014 și art. 30 din Legea 214/2024. QSIGN răspunde pentru prejudiciul cauzat ca urmare a nerespectării cerințelor regulamentare, în limitele asigurării de răspundere profesională (500.000 EUR per serviciu). Nu se exclude răspunderea pentru dolus sau culpă gravă. Limitările specifice sunt detaliate în Subscriber Agreement și Relying Party Agreement.

9.8 Despăgubiri

Titularul și relying party sunt obligați la despăgubirea QSIGN pentru prejudiciul direct, cert și demonstrabil cauzat prin pretenții ale terților rezultate din încălcarea de către aceștia, cu intenție sau culpă gravă, a obligațiilor contractuale sau a legii. Despăgubirea nu acoperă prejudiciile indirecte, pierderea de profit sau de oportunitate ori prejudiciile care nu pot fi probate cu mijloace obiective. Pentru titularii persoane fizice care au calitatea de consumator în sensul Legii nr. 193/2000, răspunderea nu poate depăși limitele răspunderii pentru fapta proprie recunoscute de Codul civil, iar orice clauză contrară este considerată nescrisă conform art. 4 alin. (3) din Legea nr. 193/2000.

9.9 Termen și încetare

Prezentul CP/CPS este în vigoare de la data publicării și rămâne aplicabil până la înlocuirea cu o versiune nouă. Versiunile anterioare rămân disponibile public timp de minim 10 ani de la data înlocuirii, în

vederea valorii probatorii a documentelor semnate sub politicile anterioare. Încetarea activității QSIGN este reglementată de secțiunea 5.8 a prezentului document și de art. 13 din Legea 214/2024.

9.10 Comunicări individuale și avize

Comunicările între QSIGN și titulari/relying parties se realizează prin: (i) e-mail (la adresa validată); (ii) portal autentificat; (iii) anunțuri publicate în repository. Pentru comunicările oficiale către ADR, se utilizează e-mail semnat electronic, telefon de urgență, fax (acolo unde aplicabil) sau corespondență fizică.

9.11 Modificări

Modificările prezentului document sunt aprobate conform procedurii descrise la secțiunea 1.5.4. Modificările minore (corecturi de redactare, clarificări, actualizări de adrese) nu necesită notificare ADR. Modificările substanțiale sunt notificate ADR cu cel puțin 30 de zile înainte de intrarea în vigoare (art. 4 alin. (2) din Anexa 1 la Decizia 162/2026); modificările urgente necesare în cazuri excepționale (compromiteri de securitate) sunt notificate în 24 ore de la implementare (art. 4 alin. (3) Anexa 1 Decizie 162/2026).

9.12 Soluționarea disputelor

Disputele dintre QSIGN și titulari/relying parties sunt soluționate amiabil; în caz de eșec, sunt supuse instanțelor competente din România. Litigiile cu autoritățile (ADR, ANSPDCP, DNSC) sunt soluționate conform procedurilor administrative aplicabile, cu posibilitatea contestării în contencios administrativ.

9.13 Legea aplicabilă

Prezentul document este guvernat de legea română și de dreptul Uniunii Europene direct aplicabil (Regulamentele eIDAS, GDPR). Pentru titulari nerezidenți care optează în Subscriber Agreement, se aplică legea română cu respectarea normelor de drept internațional privat și a conflictelor de legi.

9.14 Conformitatea cu legea aplicabilă

QSIGN se obligă să respecte continuu legislația națională și a UE aplicabilă serviciilor de încredere calificate, inclusiv: Reg. (UE) 910/2014 (modificat prin Reg. UE 2024/1183), Reg. de punere în aplicare (UE) 2025/1567 (gestiune QSCD la distanță), Reg. de punere în aplicare (UE) 2025/1942–1946 (validare, preservation, certificate calificate), Reg. de punere în aplicare (UE) 2025/2530 (cerințe pentru QTSP), Legea 214/2024, GDPR, Legea 190/2018, Ordin MEDAT 102/2026 (Anexa 1), Decizia ADR 162/2026, OUG 155/2024 (NIS2), Legea 135/2007 privind arhivarea documentelor electronice, Legea 182/2002 privind protecția informațiilor clasificate, alte acte normative aplicabile.

9.15 Diverse

9.15.1 Acordul integral

Subscriber Agreement, Relying Party Agreement, Termenii și condițiile, prezentul CP/CPS, PDS-ul și politicile subordonate (QTSA, validare, preservation) constituie acordul integral dintre QSIGN și utilizatorii serviciilor calificate.

9.15.2 Cesiune

QSIGN poate cesiona drepturile și obligațiile contractuale către un alt prestator de servicii de încredere calificat, exclusiv în condițiile art. 13 alin. (3) din Legea 214/2024 — cu notificarea ADR și a titularilor cu cel puțin 30 de zile înainte și cu acordarea posibilității de refuz.

9.15.3 Divizibilitate

Dacă o clauză a prezentului document este declarată nulă sau inaplicabilă, restul clauzelor rămân în vigoare și se interpretează cu efectul cel mai apropiat de intenția originară.

9.15.4 Forța majoră

QSIGN nu răspunde pentru neîndeplinirea obligațiilor cauzate de forță majoră, în condițiile dreptului comun (art. 1351 Cod civil), cu obligația de a notifica titularii și ADR în 24 ore și de a depune diligența necesară pentru continuitatea serviciului prin BCP/DRP.

9.16 Anexe la prezentul document

Documentele subordonate, parte integrantă a corpului documentar al QSIGN ca QTSP:

- PKI Disclosure Statement (PDS) — QSIGN-PDS-QC-v1.0
- Politica QTSA (Time-Stamping Policy) — QSIGN-TSA-Policy-v1.0
- Politica de validare calificată — QSIGN-VAL-Policy-v1.0
- Politica de preservation calificată (LTP) — QSIGN-PRES-Policy-v1.0
- Subscriber Agreement — QSIGN-SA-QC-v1.0
- Relying Party Agreement — QSIGN-RPA-QC-v1.0
- Termeni și condiții (T&C) — QSIGN-TC-QC-v1.0
- Politica de protecție a datelor (Privacy Policy) — QSIGN-PP-QC-v1.0
- Plan de încetare a activității (Termination Plan) — QSIGN-TP-v1.0
- Plan de continuitate și recuperare (BCP/DRP) — QSIGN-BCP-v1.0
- Plan de securitate al sistemului informatic — QSIGN-ISP-v1.0

Semnătură și aprobare

Prezentul document a fost adoptat de Policy Management Authority (PMA) a QSIGN S.R.L. și aprobat de reprezentantul legal al societății.

Versiune: 1.0

Data aprobării: 06.05.2026

Data intrării în vigoare: 06.05.2026

Data publicării în repository: 06.05.2026

Pentru QSIGN S.R.L.:

Trandafirescu Alexandru Florin — Administrator

Semnătura electronică calificată: _____