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 NECALIFICATE

(Servicii Avansate)

Aplicabil(e):

- **Certificate pentru semnătura electronică avansată (NCP+, NCP, LCP)**
- **Certificate pentru sigiliul electronic avansat (NCP+, NCP, LCP)**
- **Gestionarea semnăturilor și sigiliilor electronice avansate la distanță**

(server signing — sole control utilizator, SCAL2-aligned)

INFORMAȚII DOCUMENT

Element	Valoare
Denumire document	Politica de Certificare și Codul de Practici și Proceduri — Servicii de Încredere Necalificate (Avansate)
Cod intern	QSIGN-CP-CPS-AC-v1.0
Versiune	1.0

Element	Valoare
Data publicării	06.05.2026
Data intrării în vigoare	06.05.2026
Stare	Aprobat (versiune pentru depunere ADR — Anexa 2 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 — în special art. 26 (semnătura electronică avansată) și art. 36 (sigiliul electronic avansat); Legea nr. 214/2024; Ordin MEDAT nr. 102/29.01.2026 (Anexa 2 — Procedura privind înregistrarea prestatorilor de servicii de încredere necalificate); ETSI EN 319 401 v3.1.1+; ETSI EN 319 411-1 v1.4.1+ (politici NCP, NCP+, LCP); ETSI EN 319 412 părțile 1–5; ETSI TS 119 461 v2.1.1+ (Baseline LoIP minim); ETSI EN 319 403-1 v2.3.1+; ISO/IEC 27001; ISO/IEC 27002

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 NECALIFICATE — denumite în prezentul document servicii avansate — prestate în temeiul Regulamentului (UE) nr. 910/2014, modificat prin Regulamentul (UE) 2024/1183, al Legii nr. 214/2024 privind utilizarea semnăturii electronice, a mărcii temporale și prestarea serviciilor de încredere bazate pe acestea, precum și al Ordinului ministrului economiei, digitalizării, antreprenoriatului și turismului nr. 102 din 29 ianuarie 2026 (Anexa 2 — Procedura de înregistrare și radiere a prestatorilor de servicii de încredere necalificate în Registrul prestatorilor de servicii de încredere necalificate).

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

- **(i) emiterea și gestionarea certificatelor pentru semnătura electronică avansată** emise persoanelor fizice, conform art. 26 din Reg. (UE) 910/2014, sub politicile NCP+, NCP și LCP definite în ETSI EN 319 411-1 v1.4.1+;
- **(ii) emiterea și gestionarea certificatelor pentru sigiliul electronic avansat** emise persoanelor juridice, conform art. 36 din Reg. (UE) 910/2014, sub aceleași politici NCP+, NCP, LCP;
- **(iii) gestionarea semnăturilor și sigiliilor electronice avansate la distanță** (remote AdES signing) — generare, păstrare și operare a cheilor private în HSM-uri ale QSIGN, sub controlul exclusiv al titularului prin Signature Activation Data (SAD), fără ca dispozitivul să dețină certificare QSCD; serviciul respectă principiile EN 419 241-1 (Sole Control Assurance Level 2 — SCAL2) cu adaptările aplicabile contextului necalificat.

Serviciile de încredere CALIFICATE prestate de QSIGN (certificate calificate de semnătură QCP-n / QCP-n-qscd, certificate calificate de sigiliu QCP-l / QCP-l-qscd, marcă temporală calificată QTSA, gestiune QSCD la distanță) fac obiectul unui document distinct (QSIGN-CP-CPS-QC-v1.0), aprobat conform Anexei 1 la Ordinul MEDAT nr. 102/2026.

QSIGN solicită ADR înscrierea în Registrul prestatorilor de servicii de încredere necalificate pentru serviciile descrise mai sus, în temeiul art. 5 alin. (1) din Anexa 2 la Ordinul MEDAT nr. 102/2026. Statutul de prestator necalificat se acordă prin Decizia președintelui ADR conform art. 7 alin. (2) din aceeași Procedură.

Diferența esențială între serviciile calificate și serviciile avansate prestate de QSIGN constă în: (a) absența prezumției automate de echivalență cu semnătura olografă (semnătura avansată cu certificat necalificat are forța probantă lăsată la aprecierea instanței, iar nu prezumția art. 25 alin. (2) eIDAS); (b) lipsa includerii în Lista sigură națională (Trusted List) și în LOTL UE (înscriere doar în Registrul prestatorilor necalificate operat de ADR); (c) regimul de evaluare prin auditori înscriși în Lista auditorilor de securitate cibernetică valabil atestați (LASC) la DNSC, deținători ai atestatului de tip General, în locul evaluării prin Conformity Assessment Body acreditat conform Reg. (CE) 765/2008; (d) cerințe de asigurare reduse (100.000 EUR

per serviciu, conform art. 5 alin. (2) lit. b) din Anexa 2 la Ordinul MEDAT nr. 102/2026); (e) Level of Identity Proofing minim Baseline conform ETSI TS 119 461, în loc de Substantial/High.

Identificarea documentului și OID-uri

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. Arborele OID este partajat cu serviciile calificate, fiecare ramură fiind dedicată unei familii distincte de politici.

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, T&C, PDS
Politici certificate avansate	1.3.6.1.4.1.59019.2.1	OID-uri politici avansate (NCP, NCP+, LCP)
Politici remote signing avansat	1.3.6.1.4.1.59019.2.5	Server signing necalificat (SCAL2-aligned)
Politici servicii calificate	1.3.6.1.4.1.59019.2.2 – .2.4	Document separat (QSIGN-CP-CPS-QC)

OID-uri politici aplicate (servicii avansate)

Politicile de certificat sunt aliniate cu identificatorii standardizați ETSI definiți în ETSI EN 319 411-1 (clauza 5.3) și sunt complementate de OID-uri proprii QSIGN. Tabelul de mai jos sintetizează maparea.

Tip certificat / serviciu	OID politică ETSI	OID politică QSIGN
Certificat avansat semnătură — pers. fizică — NCP+ (cheie pe SSCD/HSM utilizator)	0.4.0.2042.1.2	1.3.6.1.4.1.59019.2.1.1.1
Certificat avansat semnătură — pers. fizică — NCP	0.4.0.2042.1.1	1.3.6.1.4.1.59019.2.1.1.2
Certificat avansat semnătură — pers. fizică — LCP	0.4.0.2042.1.3	1.3.6.1.4.1.59019.2.1.1.3
Certificat avansat sigiliu — pers. juridică — NCP+	0.4.0.2042.1.2	1.3.6.1.4.1.59019.2.1.2.1
Certificat avansat sigiliu — pers. juridică — NCP	0.4.0.2042.1.1	1.3.6.1.4.1.59019.2.1.2.2

Tip certificat / serviciu	OID politică ETSI	OID politică QSIGN
Certificat avansat sigiliu — pers. juridică — LCP	0.4.0.2042.1.3	1.3.6.1.4.1.59019.2.1.2.3
Serviciu remote signing avansat (SCAL2-aligned)	—	1.3.6.1.4.1.59019.2.5.1

Politicile NCP+ (Normalized Certificate Policy with Secure User Device), NCP (Normalized Certificate Policy) și LCP (Lightweight Certificate Policy) sunt definite în ETSI EN 319 411-1 §5.3. Diferențele esențiale privesc: nivelul de identificare a titularului, cerințele asupra dispozitivului care păstrează cheia privată și cerințele documentare. Pentru serviciul de remote signing avansat, QSIGN aplică cerințele SCAL2 din EN 419 241-1 ca model de control exclusiv al utilizatorului asupra cheii, fără a urmări certificarea HSM ca QSCD.

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. Atunci când se face referire la „certificat avansat”, „semnătură avansată” sau „sigiliu avansat”, se înțeleg cele definite la art. 3 pct. 11–12 și art. 26, respectiv art. 36, din Reg. (UE) 910/2014.

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 — atât calificate, cât și necalificate (avansate) — în sensul Regulamentului (UE) nr. 910/2014, modificat și completat prin Reg. (UE) 2024/1183.

QSIGN operează o infrastructură de chei publice (PKI) proprie. Pentru serviciile avansate descrise în prezentul document, QSIGN exploatează o ierarhie de Issuing CA-uri subordonate aceleiași Root CA care deservește și serviciile calificate, asigurându-se separarea logică, prin Issuing CA-uri distincte și OID-uri de politică distincte, între cele două familii de servicii. Toate serviciile avansate sunt proiectate pentru a îndeplini cumulativ cerințele Reg. (UE) 910/2014 (art. 26, art. 36), Legii 214/2024, Anexei 2 la Ordinul MEDAT 102/2026 și standardelor ETSI relevante (în principal ETSI EN 319 401 și ETSI EN 319 411-1).

1.1.1 Scopul Politicii de Certificare (CP)

Politica de Certificare descrie regulile aplicabile emiterii, gestionării și utilizării certificatelor pentru semnătura/sigiliul electronic avansat de către QSIGN. CP definește obligațiile QSIGN, ale titularilor (subscriberilor) și ale părților utilizatoare (relying parties), precum și cerințele tehnice, organizaționale și de conformitate aplicabile fiecărei politici suportate (NCP+, NCP, LCP).

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 avansate. 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 avansate, în conformitate cu cerințele ETSI EN 319 401 (cerințe generale TSP) și ETSI EN 319 411-1 (cerințe pentru emitenți de certificate de încredere).

1.1.3 Relația cu alte documente

Acest CP/CPS constituie documentul-cadru al QSIGN pentru servicii avansate. Documentele subordonate, care formează corpul documentar complet aplicabil acestor servicii, includ: PKI Disclosure Statement (PDS) pentru servicii avansate (QSIGN-PDS-AC); 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); Procedura de notificare a incidentelor (cu ANSPDCP, ADR, DNSC); Subscriber Agreement / Relying Party Agreement / Termeni și condiții pentru servicii avansate; Politica de validare avansată (validare AdES); Politica internă de identity proofing (alineată ETSI TS 119 461 Baseline LoIP). Toate aceste documente sunt elaborate consistent cu prezentul CP/CPS și sunt aprobate de Policy Management Authority (PMA).

1.2 Numele și identificarea documentului

Element	Valoare
Titlu	QSIGN — Politica de Certificare și Codul de Practici și Proceduri — Servicii Avansate (Necalificate)
Cod intern	QSIGN-CP-CPS-AC-v1.0
OID document	1.3.6.1.4.1.59019.1.2.1.0
Versiune	1.0
Tip	Document combinat CP + CPS, conform RFC 3647 §3.4
Aplicabilitate	Servicii de încredere NECALIFICATE: certificate avansate de semnătură (NCP+, NCP, LCP), certificate avansate de sigiliu (NCP+, NCP, LCP), gestiune semnături avansate la distanță (server signing, sole control utilizator)
Limba	Română
Versiune publică	Disponibilă pe https://www.qsign.ro/repository, în PDF semnat cu sigiliu calificat al QSIGN (din serviciul 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), partajat cu serviciile calificate, și nivelul emitent (Issuing CAs) dedicat serviciilor avansate. Această separare urmărește limitarea expunerii cheii rădăcină, izolarea responsabilităților operaționale între familii de servicii 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 (comună cu serviciile calificate); emite exclusiv certificate pentru CA-uri subordonate; off-line, în airgap
Issuing — Avansat	QSIGN Advanced Signature CA G1	Emite certificate avansate de semnătură electronică pentru persoane fizice (NCP+, NCP, LCP)
Issuing — Avansat	QSIGN Advanced Seal CA G1	Emite certificate avansate de sigiliu electronic pentru persoane juridice (NCP+, NCP, LCP)
Issuing — Avansat	QSIGN Advanced 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 avansate

- HSM-uri certificate FIPS 140-3 Nivel 3 sau Common Criteria EAL 4+ AVA_VAN.5; pentru serviciile avansate, certificarea EN 419 221-5 nu este obligatorie, însă echipamentele utilizate sunt eligibile pentru aceasta (sunt aceleași HSM-uri care deservesc Issuing CA-urile calificate, prin partajare logică în partiții independente).
- 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) și ETSI TS 119 461 pentru identity proofing la nivel minim Baseline LoIP. 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 avansat:

- Pentru certificate avansate de semnătură (politici NCP+, NCP, LCP) — persoane fizice identificate în câmpul Subject (commonName, givenName, surname, serialNumber).
- Pentru certificate avansate de sigiliu (politici NCP+, NCP, LCP) — persoane juridice identificate în câmpul Subject (commonName, organizationName, organizationIdentifier conform ETSI EN 319 412-1).

Pentru ambele categorii, certificatul nu se bucură de prezumția automată de echivalență cu semnătura olografă; însă semnătura/sigiliul produs cu acest certificat constituie semnătură avansată în sensul art. 26, respectiv sigiliu avansat în sensul art. 36 din Reg. (UE) 910/2014, cu efecte juridice corespunzătoare.

1.3.4 Relying Parties (Părți utilizatoare)

Relying Party este orice persoană fizică sau juridică ce, în mod rezonabil, se bazează pe un certificat avansat 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. Relying party trebuie să fie informată că certificatul utilizat NU este calificat și că, pe cale de consecință, semnătura/sigiliul produs cu acesta nu beneficiază de prezumția art. 25 alin. (2), respectiv art. 35 alin. (2) din Reg. (UE) 910/2014.

1.3.5 Alte participanți

- Auditori înscriși în Lista auditorilor de securitate cibernetică valabil atestați (LASC) la DNSC, deținători ai atestatului de tip General, care efectuează auditurile periodice prevăzute la art. 5 alin. (2) lit. a) din Anexa 2 la Ordinul MEDAT 102/2026, cu respectarea cerințelor ETSI EN 319 403-1.
- ADR — Autoritatea pentru Digitalizarea României, organism național competent pentru ținerea Registrului prestatorilor de servicii de încredere necalificate și pentru supravegherea acestora.
- DNSC — Directoratul Național de Securitate Cibernetică, autoritate națională de securitate cibernetică, care administrează LASC.
- ANSPDCP — Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal.
- Furnizori de servicii de încredere parteneri (administratori de arhivă electronică acreditați conform Legii 135/2007, prestatori de marcă temporală calificată — uzual chiar QTSA-ul propriu QSIGN, prestatori calificați de validare/preservation pentru cazurile în care titularul dorește valoare LTV pe documentele semnate cu certificat avansat).

1.4 Utilizarea certificatelor

1.4.1 Utilizări permise

1.4.1.1 Certificate avansate pentru semnătura electronică (NCP+, NCP, LCP)

Certificatele avansate pentru semnătura electronică emise de QSIGN respectă cerințele art. 26 din Reg. (UE) 910/2014 și produc semnături electronice avansate. Spre deosebire de certificatele calificate (QCP-n, QCP-n-qscd), aceste certificate NU declanșează prezumția echivalenței juridice cu semnătura olografă din art. 25 alin. (2) eIDAS și art. 4 alin. (1) din Legea 214/2024; valoarea probatorie a semnăturilor produse este apreciată concret de instanță, ținând cont de îndeplinirea cumulativă a celor patru cerințe ale art. 26 (legare unică de semnatar; identificare semnatar; control exclusiv asupra datelor de creare; capabilitate de detectare a oricărei modificări ulterioare).

Aplicații tipice ale semnăturii avansate: contracte între profesioniști care nu impun forma autentică sau formă scrisă ad validitatem; corespondență comercială formală; aprobări interne de organizație (workflow electronic); declarații care nu se depun la autorități publice; contracte de adeziune și de prestări servicii; raportări interne semnate; circuite de aprobare în industrii

reglementate (sănătate, financiar) atunci când reglementările proprii nu impun semnătură calificată.

1.4.1.2 Certificate avansate pentru sigiliul electronic (NCP+, NCP, LCP)

Certificatele avansate pentru sigiliul electronic emise de QSIGN respectă cerințele art. 36 din Reg. (UE) 910/2014, fiind asociate persoanelor juridice. Sigiliul electronic avansat NU se bucură de prezumția de integritate și de corectitudine a originii din art. 35 alin. (2) eIDAS; cu toate acestea, atunci când îndeplinește cele patru cerințe ale art. 36, asigură nivel ridicat de încredere asupra integrității documentului și a originii sale, suficient pentru numeroase aplicații enterprise.

Aplicații tipice: sigilarea documentelor emise de organizații (rapoarte interne, certificate emise de companii, atestate eliberate de organizații private); securizarea API-urilor cu autentificare bazată pe sigiliu; sigilarea pachetelor de date în lanțuri de aprovizionare; integrarea în soluții EDI și B2B; sigilarea automată a documentelor generate de sisteme ERP.

1.4.1.3 Gestionarea semnăturilor avansate la distanță (remote AdES signing)

Pentru titularii care optează pentru serviciul de remote signing avansat, QSIGN păstrează cheia privată într-un HSM situat la sediul TSP-ului și operează cheia exclusiv la solicitarea titularului, după autentificare puternică (MFA) și transmiterea Signature Activation Data (SAD). Cheia nu este accesibilă nimănui în afara titularului prin SAD și nu părăsește HSM-ul în formă neprotejată. Modelul respectă principiile SCAL2 din EN 419 241-1 (Sole Control Assurance Level 2): chiar și administratorii TSP nu pot, prin design, semna în numele titularului în lipsa SAD-ului. Sistemul nu este însă certificat ca QSCD — ceea ce ar fi premisa pentru serviciul calificat — și, ca urmare, semnăturile produse rămân semnături avansate, NU calificate.

1.4.2 Utilizări interzise

- Utilizarea certificatelor pentru scopuri ilegale, inclusiv pentru încălcarea drepturilor de proprietate intelectuală sau pentru fraudă.
- Utilizarea certificatelor avansate emise de QSIGN ca dovadă de echivalență cu semnătura olografă, atunci când legea sau părțile interesate impun semnătură calificată sau formă autentică (de exemplu, înscrisuri pentru care legea cere ad validitatem semnătură calificată).
- Utilizarea certificatelor avansate pentru autentificarea unui site web (TLS/SSL) — pentru aceasta este necesar un certificat de autentificare a site-urilor (QWAC pentru servicii calificate, sau certificat web TLS distinct), conform art. 45 eIDAS.
- Utilizarea certificatelor avansate de tip „sigiliu” (persoană juridică) 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 HSM utilizator în software, în cazul NCP+).

1.5 Administrarea politicii

1.5.1 Organizația care administrează documentul

Element	Valoare
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 — același organism intern care administrează și politica calificată, cu următoarea componență: (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

- Propunerea de modificare se inițiază de orice membru PMA, sau ca rezultat al unui audit de conformitate, control ADR, ori incident de securitate.

- Propunerea este analizată tehnic, juridic și de securitate; analizele se atașează la dosarul deciziei.
- Pentru modificări substanțiale (de exemplu, schimbări de algoritm criptografic, modificări ale procesului de identificare la distanță, schimbări ale modalităților de protecție a cheii utilizator), PMA solicită opinie consultativă de la auditorul DNSC LASC.
- Modificările substanțiale sunt notificate ADR cu cel puțin 30 de zile înainte de intrarea în vigoare, conform regulilor de modificare aplicabile prestatorilor înscriși în Registrul prestatorilor necalificate (Anexa 2 la Ordinul MEDAT 102/2026, art. 9).
- 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.
- 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 avansat.
Cheie publică	Cheia matematică pereche 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.
SSCD	Secure Signature Creation Device — dispozitiv securizat de creare a semnăturii (smart card, token criptografic) utilizat de titular în politica NCP+; nu se confundă cu QSCD (cerințe sporite și certificare specifică pentru servicii calificate).
LoIP	Level of Identity Proofing — nivelul de asigurare al verificării identității, conform ETSI TS 119 461; pentru servicii avansate, nivelul minim aplicat de QSIGN este Baseline.
NCP / NCP+ / LCP	Politici de certificat conform ETSI EN 319 411-1; NCP+ presupune

Termen	Definiție
	utilizarea unui dispozitiv securizat (SSCD/HSM) pentru cheia privată, NCP permite stocare în software cu cerințe stricte, LCP este policy-ul lightweight cu cerințe documentare reduse.
AdES	Advanced Electronic Signature — semnătură electronică avansată; formate AdES standardizate: CAdES (RFC 5126/ETSI EN 319 122), XAdES (ETSI EN 319 132), PAdES (ETSI EN 319 142), ASiC (ETSI EN 319 162).
SCAL2	Sole Control Assurance Level 2 conform EN 419 241-1 — model de control exclusiv al utilizatorului asupra cheii server-side, prin SAD; aplicabil serviciului de remote signing avansat al QSIGN.
SAD	Signature Activation Data — datele autentificate transmise de utilizator către HSM-ul TSP pentru autorizarea unei operații de semnare la distanță.
RA / LRA	Registration Authority / Local Registration Authority — entități care primesc și verifică cererile.
PMA	Policy Management Authority — organism care administrează prezentul document.
TSP	Trust Service Provider.
LASC	Lista auditorilor de securitate cibernetică valabil atestați la DNSC.

1.6.2 Acronime

ADR — Autoritatea pentru Digitalizarea României; ADReS — semnătură electronică avansată ADR (notă: termen folosit informal); AdES — Advanced Electronic Signature; ANSPDCP — Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal; CA — Certification Authority; 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; LASC — Lista auditorilor de securitate cibernetică; LCP — Lightweight Certificate Policy; LoIP — Level of Identity Proofing; NCP — Normalized Certificate Policy; NCP+ — Normalized Certificate Policy with Secure User Device; OCSP — Online Certificate Status Protocol; OID — Object Identifier; PEN — Private Enterprise Number (IANA); PKI — Public Key Infrastructure; PMA — Policy Management Authority; RA — Registration Authority; SAD — Signature Activation Data; SCAL — Sole Control Assurance Level; SLA — Service Level Agreement; SOC — Security Operations Center; SSCD — Secure Signature Creation Device; 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 (atât pentru servicii calificate cât și avansate), 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 ≥ 99,5% pentru repository-ul public și ≥ 99,9% pentru endpoint-urile operaționale (OCSP, CRL distribution points).

2.2 Publicarea informațiilor de certificare

QSIGN publică în repository următoarele informații aplicabile serviciilor avansate, conform art. 24 alin. (2) lit. (k) eIDAS (aplicat prin analogie pentru servicii necalificate, în spiritul transparenței reglementate de Anexa 2 la Ordinul MEDAT 102/2026):

- 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) aplicabile serviciilor avansate.
- Certificatele Root CA și Issuing CA-urilor avansate (QSIGN Advanced Signature CA G1, QSIGN Advanced Seal CA G1), în formatele cer (binar) și pem (Base64).
- CRL-uri pentru fiecare CA emitentă avansată, actualizate conform secțiunii 4.9 a prezentului document.
- 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 (combinat pentru ambele linii — calificat și avansat — cu secțiuni distincte).
- Informațiile privind incidentele de securitate notificate, în formă agregată, păstrând confidențialitatea utilizatorilor afectați.
- Decizia ADR privind înscrierea QSIGN în Registrul prestatorilor de servicii de încredere necalificate, însoțită de extrasul aplicabil din Registrul ADR.

2.3 Frecvența publicării

Element	Frecvența publicării / actualizării
Certificate CA (Root, Issuing avansate)	La emitere și la fiecare re-key; rămân publicate până la expirare + 35 ani

Element	Frecvența publicării / actualizării
CRL — Issuing CA Avansat (Signature)	Săptămânal sau imediat la revocare (nextUpdate la 7 zile, conform ETSI EN 319 411-1 §6.2.4 NCP+/LCP); ținta operațională internă QSIGN: 24 ore
CRL — Issuing CA Avansat (Seal)	Săptămânal sau imediat la revocare (nextUpdate la 7 zile, conform ETSI EN 319 411-1 §6.2.4 NCP+/LCP); ținta operațională internă QSIGN: 24 ore
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
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 (emis sub serviciul calificat) 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 avansate emise de QSIGN utilizează nume distincte X.500 conforme cu RFC 5280 și ETSI EN 319 412 (părțile 1, 2, 3). 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 avansate de semnătură (NCP+, NCP, LCP — 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 avansate de sigiliu (NCP+, NCP, LCP — 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 avansate de semnătură (politici NCP+, NCP, LCP), 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; (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 (persoane juridice), pseudonimele NU sunt permise — denumirea juridică oficială este obligatorie.

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 avansate. 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 avansate emise în cadrul serviciului de remote signing al QSIGN — în care cheia privată este generată direct în HSM-ul QSIGN sub controlul exclusiv al titularului prin SAD —, PoP este garantat prin proces controlat de TSP: (a) generarea cheii are loc exclusiv în HSM sub controlul titularului prin autentificare puternică (SAD), conform principiilor SCAL2 din EN 419 241-1; (b) procesul este atestat criptografic prin metadate semnate de HSM; (c) cheia nu părăsește niciodată HSM-ul în formă neprotejată.

3.2.2 Autentificarea identității organizației

Pentru certificate avansate de sigiliu (NCP+, NCP, LCP — persoane juridice), identitatea organizației este verificată conform ETSI TS 119 461 (clauza referitoare la verificarea identității persoanei juridice) prin combinația următoarelor metode:

- 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.
- Verificarea statutului fiscal și a CUI/CIF prin interogarea bazelor publice ale ANAF (PlatitorTvaRest API), pentru titulari români.
- Verificarea identității reprezentantului legal prin metodele aplicabile persoanelor fizice (vezi 3.2.3).
- 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). Spre deosebire de certificatele calificate, pentru certificatele avansate emise de QSIGN nivelul minim aplicat este Baseline LoIP (conform cerinței art. 5

alin. (2) lit. a) din Anexa 2 la Ordinul MEDAT 102/2026 — formularea „nivel minim Baseline LoIP"). Tabelul de mai jos sintetizează cerințele aplicabile.

Tip certificat avansat	LoIP minim	Metode acceptate
LCP — Lightweight (cheie utilizator în orice mediu sigur)	Baseline LoIP	Verificare a unei adrese e-mail funcționale; verificare a unui număr de telefon prin OTP; verificare a unui document de identitate prin OCR + comparare facială automatizată; verificare prin nodul eIDAS / ROeID cu LoA Low+
NCP — Normalized (cheie utilizator în orice mediu sigur)	Baseline sau Substantial LoIP	Identical cu LCP (Baseline) sau, pentru Substantial: video-identificare cu agent uman (3.2.3.2), prezență fizică (3.2.3.1), eID notificat cu LoA Substantial (3.2.3.4), certificat existent (3.2.3.3)
NCP+ — Normalized cu SSCD (cheie pe smart card / token / HSM utilizator)	Substantial LoIP recomandat (Baseline acceptat)	Prezență fizică, video-identificare cu agent, eID notificat (Substantial), certificat existent. NCP+ NU înseamnă identificare la nivel calificat — diferența față de QCP-* rămâne în certificare dispozitiv (lipsa QSCD) și în nivelul de detalii contractuale, nu doar în LoIP
Remote signing avansat (chei în HSM al QSIGN, SCAL2-aligned)	Substantial LoIP minim	Identificare echivalentă NCP+; suplimentar, înrolare credențiale puternice (MFA: certificat hardware sau dispozitiv mobil cu cheie hardware-backed + biometrie + parolă) pentru SAD

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 echivalent High, dar este disponibilă și pentru toate politicile avansate.

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

Sesiunea video se desfășoară în condițiile ETSI TS 119 461, cu cerințe minime corespunzătoare nivelului LoIP urmărit:

- Pentru Baseline LoIP (suficient pentru LCP / NCP minim): sesiune video în timp real, agent uman instruit, verificare automată OCR a actului de identitate cu comparare facială automată; conexiune criptată end-to-end (TLS 1.3).

- Pentru Substantial LoIP (recomandat NCP+, obligatoriu remote signing): suplimentar, detectarea elementelor de securitate dinamice (holograme prin modificare de unghi); 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); test de liveness vocal prin frază secret furnizată live; verificare incrucișată cu listele de sancțiuni.
- 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.
- Sesiunea video se înregistrează integral; înregistrarea este sigilată electronic cu marcă temporală calificată (utilizând QTSA-ul propriu QSIGN din serviciul calificat) și păstrată conform secțiunii 5.5 (minim 7 ani de la încetarea valabilității certificatului — cerință ETSI TS 119 461).
- Mecanismul de identificare la distanță este detaliat în Politica internă de identity proofing a QSIGN, publicată în repository și revizuită anual.

3.2.3.3 Identificare prin certificat existent

Solicitantul poate fi identificat printr-un certificat valid pentru semnătura electronică, fie calificat (emis de orice prestator calificat din UE listat în LOTL), fie avansat emis de QSIGN sau de un alt prestator necalificat înscris în registrele naționale. Solicitantul semnează electronic cererea de emitere cu certificatul existent; QSIGN verifică criptografic semnătura, validitatea certificatului (CRL/OCSP) și extrage atributele de identitate. Această metodă asigură LoIP echivalent cu cel al certificatului-sursă; pentru certificate-sursă emise cu LoIP Baseline, metoda este utilizabilă pentru emiterea de noi certificate avansate cu LoIP Baseline. Pentru certificate-sursă calificate, este utilizabilă oriunde.

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, 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. Mapping LoA → LoIP: LoA Low ⇒ LoIP Baseline; LoA Substantial ⇒ LoIP Substantial; LoA High ⇒ LoIP High. Toate aceste niveluri sunt acceptate pentru certificatele avansate emise de QSIGN.

3.2.4 Informații neverificate ale titularului

QSIGN nu include în certificate avansate 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). Pentru atributele afiliate organizațional, se aplică cerințele relevante din ETSI EN 319 412-2 și ETSI TS 119 612.

3.2.5 Validarea autorității

Pentru certificate avansate de sigiliu (persoane juridice), 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 sau avansată 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 avansate emise de QSIGN sunt interoperabile cu standardele europene aplicabile. QSIGN urmărește respectarea specificațiilor ETSI EN 319 412 (părțile 1–4) pentru profilul de certificat, ETSI EN 319 411-1 pentru cerințele aplicabile politicilor non-calificate (NCP, NCP+, LCP), 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, deși semnăturile produse cu certificate avansate nu sunt așteptate să apară ca „qualified” în output-urile DSS.

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. Pentru certificate avansate, dacă au trecut peste 5 ani de la identificarea inițială completă, este recomandată re-identificarea integrală prin una dintre metodele Baseline/Substantial.

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:

- Cerere semnată electronic cu certificatul ce urmează a fi revocat (auto-revocare).
- Cerere semnată cu un alt certificat avansat sau calificat valid al titularului.
- Cerere transmisă prin portalul autentificat al titularului (cu autentificare MFA: certificat hardware sau OTP + parolă/PIN).
- 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 — pentru certificate avansate suspendarea este permisă, vezi 4.9.8) până la confirmarea finală.

- 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 avansat

- Pentru certificate avansate de semnătură (NCP+, NCP, LCP): orice persoană fizică majoră, cu capacitate deplină de exercițiu, care prezintă un act de identitate valid și acceptă Subscriber Agreement. Pentru minori cu capacitate limitată, cererea se face prin reprezentantul legal.
- Pentru certificate avansate de sigiliu (NCP+, NCP, LCP): 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 319 411-1 §6.2:

- Solicitantul accesează portalul QSIGN sau LRA și inițiază cererea, completând datele preliminare și selectând tipul de certificat avansat dorit (NCP+, NCP sau LCP) și — opțional — serviciul de remote signing.
- Solicitantul citește și acceptă electronic Subscriber Agreement, T&C, precum și consimțământul GDPR pentru prelucrarea datelor cu caracter personal. Pentru certificatele avansate, Subscriber Agreement evidențiază expres că certificatul este NECALIFICAT și că semnătura/sigiliul produs nu beneficiază de prezumția echivalenței cu semnătura olografă.
- Solicitantul achită tariful aplicabil tipului de certificat (sau prezintă dovada plății, în cazul plății în avans pentru organizații).
- Solicitantul efectuează identificarea conform metodei aplicabile tipului de certificat (vezi secțiunea 3.2.3).
- Sistemul colectează informațiile necesare emiterii (Subject DN, atribute extra, KeyUsage solicitat, durată).
- Pentru certificate cu chei generate de utilizator (NCP+ pe SSCD/HSM utilizator, NCP în software, LCP în software): solicitantul transmite CSR (PKCS#10) semnat cu cheia privată, demonstrând PoP.
- Pentru certificate cu chei generate în HSM-ul QSIGN (remote signing): cheia este generată în HSM al QSIGN, sub controlul exclusiv al titularului prin SAD; metadatele de generare sunt sigilate.
- Operatorul RA validează manual sau semi-automat dosarul, marchează aprobat/respins și transmite spre emitere.
- Issuing CA emite certificatul, îl publică în repository (dacă titularul a consimțit) și îl livrează titularului prin canal securizat.

- 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 avansat	Termen standard	Termen maxim
LCP (Lightweight) — pers. fizice	1 zi lucrătoare	3 zile lucrătoare
NCP — pers. fizice	1 zi lucrătoare	5 zile lucrătoare
NCP+ — pers. fizice (cu SSCD/HSM utilizator)	2 zile lucrătoare	7 zile lucrătoare
NCP+ / NCP / LCP — pers. juridice (sigiliu)	2 zile lucrătoare	10 zile lucrătoare
Remote signing — emitere certificat + provisioning HSM	3 zile lucrătoare	10 zile lucrătoare

4.3 Emiterea certificatelor

4.3.1 Acțiunile CA în timpul emiterii

- Issuing CA primește o cerere de emitere semnată digital de RA (event-driven, prin API intern protejat cu mTLS și jurnalizat).
- CA verifică integritatea cererii și autorizarea operatorului RA.
- CA verifică unicitatea Subject DN-ului în baza sa de date.
- CA generează numărul serial al certificatului — număr aleator de 64 de biți minimum (entropie criptografică), conform CAB Forum Baseline Requirements și RFC 5280.

- CA construiește profilul certificatului conform secțiunii 7 a prezentului document și ETSI EN 319 412-2 (semnătură) sau 412-3 (sigiliu).
- CA semnează certificatul cu cheia privată, în interiorul HSM-ului.
- Certificatul este înregistrat în baza de date de certificate active și în jurnalul de emitere.
- 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 HSM-ul QSIGN (remote signing), certificatul este disponibil în containerul utilizator al titularului în interfața QSIGN; cheia privată rămâne în HSM și nu poate fi extrasă în afara HSM-ului. Pentru certificatele pe SSCD fizic (smart card / token / smartphone cu element securizat), certificatul este livrat fizic (smart card) sau instalat de la distanță (mobile). Pentru certificatele cu cheie generată de utilizator în software, titularul descarcă fișierul certificat în formatele suportate (cer, pem) prin portal.

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 avansat și certificatele CA sunt publicate în repository-ul QSIGN în mod implicit. Certificatele asociate persoanelor fizice (NCP+, NCP, LCP de semnătură) 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 ale unei organizații), 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 (aplicabil prin analogie, deși articolul vizează în principal certificatele calificate), de a:

- Păstra cheia privată sub control exclusiv: pentru NCP+ — necunoaștere a PIN-ului SSCD/HSM utilizator de către alte persoane; pentru NCP/LCP cu cheie în software — protejarea fișierului PKCS#12 cu parolă puternică și păstrarea acestuia în mediu de stocare securizat (computer cu cont protejat, dispozitiv mobil cu cifrare); pentru remote signing — păstrarea credențialelor MFA și a SAD în siguranță.
- 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).
- Nu utiliza certificatul după expirare sau revocare.
- Notifica QSIGN în 24 ore în cazul oricărui incident de securitate care afectează certificatul.
- Conștientiza că certificatul este AVANSAT, NU calificat — semnăturile produse nu beneficiază de prezumția automată de echivalență cu semnătura olografă; titularul este sfătuit să utilizeze certificatul calificat al QSIGN (sau al altui prestator) atunci când reglementarea aplicabilă, contractul cu cealaltă parte sau alte considerente impun semnătură calificată.

4.5.2 Utilizarea de către relying party

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

- Verifica criptografic integritatea semnăturii / sigiliului avansat.
- 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).
- Construi și valida lanțul de încredere până la o ancoră de încredere — Root CA-ul QSIGN, distribuit prin repository și prin lanțuri de încredere proprii ale relying party (NU prin LOTL UE, întrucât certificatele avansate nu sunt incluse acolo).
- Verifica că OID-ul politicii incluse în certificat corespunde cerințelor cazului de utilizare (NCP+, NCP, LCP).
- Conștientiza că certificatul este AVANSAT, NU calificat. Pentru cazuri de utilizare unde reglementarea sau contractul impun semnătură calificată, certificatul avansat NU este suficient — chiar dacă semnătura este criptografic validă.
- Lua în considerare orice limitări sau restricții indicate în certificat (extensia QCStatement-uri pentru limitări specifice servicii non-calificate, atunci când există).

4.6 Reînnoirea certificatului (renewal)

Reînnoirea (renewal) — emiterea unui nou certificat cu aceeași cheie publică — este permisă pentru certificatele avansate sub condiții stricte: (i) cheia privată curentă să nu fi fost compromisă; (ii) algoritmul și lungimea cheii să fie încă conforme recomandărilor ETSI TS 119 312 / ENISA; (iii) titularul să fie identificat conform secțiunii 3.3 (Re-key — re-identificare prin semnătură cu certificat curent acceptabilă, dacă < 5 ani de la identificarea inițială). Spre deosebire de certificatele calificate (unde renewal este interzis), pentru NCP/LCP renewal

este admis în mod controlat. Pentru NCP+ cu SSCD, renewal este admis doar dacă SSCD-ul este același și nu a fost suspect de compromitere; altminteri se aplică re-key.

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.
- Pierdere a accesului la cheia privată (utilizator a uitat parola PKCS#12, a defectat SSCD-ul) — în această situație se aplică revocarea certificatului curent urmată de emitere nouă cu chei noi.

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). Dacă au trecut peste 5 ani de la identificarea inițială, este recomandată 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 principiilor art. 17 alin. (2) din Legea 214/2024 (aplicabil prin analogie certificatelor avansate) și ETSI EN 319 411-1 §6.2.4, QSIGN are obligația de a revoca certificatul avansat 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 ca prestator necalificat, dacă activitatea nu este preluată de un alt prestator.
- 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

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 Avansat (Signature)	Săptămânal sau imediat la revocare (conform ETSI EN 319 411-1 §6.2.4 NCP+/LCP); țința operațională	7 zile

CRL	Frecvența emiterii	Perioada de valabilitate (nextUpdate)
	internă QSIGN: 24 ore	
Issuing CA Avansat (Seal)	Săptămânal sau imediat la revocare (conform ETSI EN 319 411-1 §6.2.4 NCP+/LCP); ținta operațională internă QSIGN: 24 ore	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 319 411-1 §6.2.4.

4.9.7 Verificarea revocării (OCSP)

QSIGN operează un Responder OCSP per Issuing CA Avansat, 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 ≥ 99,9%.

4.9.8 Suspendarea (hold)

Spre deosebire de certificatele calificate (unde suspendarea este interzisă pentru a evita ambiguitățile probatorii), pentru certificatele avansate emise de QSIGN suspendarea (certificateHold) este permisă în condiții controlate, ca instrument operațional de gestiune a riscului în cazurile în care: (i) titularul semnalează o suspiciune de compromitere care necesită investigare suplimentară; (ii) există o procedură juridică în curs care ar putea conduce la revocare; (iii) titularul solicită expres suspendarea pentru o perioadă determinată (de exemplu, concediu medical prelungit, plecare temporară). Suspendarea are durată maximă de 30 de zile, după care, în lipsa unei decizii de re-activare sau de revocare definitivă, certificatul este revocat automat. Reactivarea suspendării necesită aceeași identificare ca o cerere de revocare. Toate evenimentele de suspendare/reactivare sunt jurnalizate și reflectate în CRL prin reasonCode = certificateHold (RFC 5280) și prin OCSP cu status revoked + reasonCode = certificateHold.

4.10 Servicii pentru starea certificatului

QSIGN furnizează două servicii independente pentru determinarea stării certificatelor avansate: (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 ≥ 99,9% (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 avansat NU fac obiectul niciunei forme de escrow sau recuperare la QSIGN — acest principiu se aplică pentru a păstra controlul exclusiv al semnatarului asupra cheii (cerință a definiției art. 26 lit. c) eIDAS pentru semnătura avansată). Pentru cazurile în care titularul pierde accesul la cheia privată, singura soluție este revocarea certificatului și emiterea unuia nou. Pentru serviciul de remote signing avansat, deși cheia este păstrată în HSM-ul QSIGN, controlul rămâne exclusiv al titularului prin SAD; pierderea credențialelor SAD impune revocarea certificatului și re-provisioning.

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 aplicabile serviciilor avansate (Issuing CA-uri avansate, partiții HSM dedicate, sistemele de jurnalizare centrale) sunt găzduite în aceleași centre de date Tier III/IV certificate utilizate pentru serviciile calificate, 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. Detaliile sunt în Planul de Securitate al Sistemului Informatic (QSIGN-ISP-v1.0).

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 319 411-1 — aceleași roluri sunt aplicate atât serviciilor calificate, cât și avansate, pentru consistență organizațională:

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/Legea 214; raportarea către ADR; gestiunea Registrului prestatorilor necalificate / 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 Avansate: cvorum 2-din-3 plus PKI Manager.
- Emiterea certificatului Root CA / sub-CA: ceremonie filmată, cu witness independent (auditor LASC).
- 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 — emis sub serviciul calificat al QSIGN) + 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, inclusiv atestat DNSC LASC de tip General pentru auditorii externi.
- 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), cu accent pe diferențele dintre serviciile calificate și avansate.
- Politicile interne ale QSIGN (acest CP/CPS, CP/CPS calificat, Information Security Policy, Acceptable Use Policy).
- Standarde tehnice: ETSI EN 319 401, 319 411-1 (cu accent pe NCP, NCP+, LCP), 319 412 (1–4), RFC 5280, RFC 6960.

- Securitate informatică, securitate cibernetică, social engineering, phishing.
- Operațiuni specifice rolului (RA, ceremonialele de cheie, OCSP, gestiune SSCD, gestiune HSM remote signing).
- Etică profesională și gestionarea conflictelor de interese.

Instruirile sunt evaluate prin teste; rezultatele și certificatele sunt arhivate. Planul de instruire este descris în detaliu în documentul anexă „Plan de instruire personal — QSIGN-PI-v1.0”, conform art. 5 alin. (2) lit. h) și u) din Anexa 2 la Ordinul MEDAT 102/2026.

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, 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).
- Pentru remote signing avansat: fiecare operație de semnare, cu metadate (titular, timestamp, hash document, OID politică, success/failure).
- 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. 16 alin. (2) din Legea 214/2024 aplicabil prin analogie); (ii) jurnalele de identificare (inclusiv sesiuni video) — minim 7 ani de la încetarea valabilității certificatului (ETSI TS 119 461); (iii) jurnalele operaționale și de securitate — minim 10 ani; (iv) 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; 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. Rapoartele sunt incluse în raportul anual de transparență (formă agregată) și în raportul de audit DNSC LASC bienal.

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 cu suport LTP — Long-Term Preservation, prin contractare cu un administrator de arhivă electronică acreditat conform Legii 135/2007 (cerință a art. 5 alin. (2) lit. t) din Anexa 2 la Ordinul MEDAT 102/2026). 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 în Registrul prestatorilor necalificate; (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 — pentru orice incident semnificativ care afectează serviciile avansate prestate, conform principiilor art. 19 alin. (2) eIDAS aplicate prin analogie; obligație concretă în temeiul art. 13 din Anexa 2 la Ordinul MEDAT 102/2026), 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 — QSIGN este entitate esențială în sensul OUG 155/2024 prin natura activității de prestator de servicii de încredere).

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 Avansate este situația de cea mai mare gravitate pentru această linie de servicii. Procedură:

- Suspendarea imediată a tuturor operațiunilor de emitere și a OCSP-ului afectat.
- Notificarea ADR în maxim 24 ore, telefonic și în scris.
- Notificarea publică prin repository și e-mail către titularii afectați.
- Revocarea cheii compromise prin includerea sa în CRL-ul Root (sau, în cazul Root, prin anunț public și retragere din Registrul prestatorilor necalificate).
- Activarea procedurii de cheie nouă, cu generarea într-o ceremonie de cheie de urgență.
- Re-emiterea certificatelor afectate sub noul lanț, după validarea controlată a fiecărui titular.
- Investigație criminalistică completă (forensics).
- Raport final și remediation plan, transmise ADR și auditorului DNSC LASC.

5.7.4 Continuitatea afacerii după dezastru

BCP/DRP-ul QSIGN definește RTO (Recovery Time Objective) ≤ 8 ore pentru servicii critice ale liniei avansate (OCSP, CRL, repository) și ≤ 24 ore pentru funcțiile RA (RTO mai relaxat decât pentru servicii calificate, unde este de 4 ore). 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. 5 alin. (2) lit. r) din Anexa 2 la Ordinul MEDAT 102/2026 — denumit Plan de încetare a activității) prevede:

- Notificarea ADR cu minim 30 de zile înainte (art. 11 din Anexa 2 la Ordinul MEDAT 102/2026).
- Notificarea tuturor titularilor activi cu cel puțin 30 de zile înainte, cu opțiunea de transfer la alt prestator sau de revocare.
- Identificarea unui prestator succesor pentru preluarea bazei de date a certificatelor și a OCSP/CRL pe perioada reziduală a valabilității certificatelor.
- Dacă nu există succesor: revocarea tuturor certificatelor înaintea încetării; preluarea evidenței de către ADR.
- Predarea către arhiva electronică acreditată/calificată a tuturor înregistrărilor cu valoare probatorie, cu menținerea LTP timp de minim 10 ani.
- Distrugerea controlată a cheilor private (în ceremonie filmată).

- Publicarea raportului final de încetare și radierea din Registrul prestatorilor de servicii de încredere necalificate prin solicitarea ADR conform art. 11–12 din Anexa 2 la Ordinul MEDAT 102/2026.

6. Controale de securitate tehnică

6.1 Generarea și instalarea perechii de chei

6.1.1 Generarea perechii de chei

Generarea cheilor pentru toate CA-urile QSIGN (Root CA, Issuing CA Avansate Persoane Fizice, Issuing CA Avansate Persoane Juridice, OCSP Responder pentru linia avansată) se efectuează în module hardware dedicate (HSM-uri), în cadrul unor ceremoniale formalizate (Key Generation Ceremony), filmate, jurnalizate și verificate de un auditor independent. Modulele HSM utilizate pentru CA-uri sunt certificate FIPS 140-3 nivel 3 (sau FIPS 140-2 nivel 3 cu plan de migrare către FIPS 140-3) și/sau Common Criteria EAL4+. Pentru cheile CA dedicate liniei avansate, certificarea EN 419 221-5 NU este obligatorie, însă QSIGN reutilizează HSM-uri certificate EN 419 221-5 (cele utilizate și pentru linia calificată) pentru a maximiza nivelul de protecție; segregarea logică între liniile de servicii este asigurată prin partiții HSM separate, slot-uri PKCS#11 distincte și politici de acces diferențiate.

Pentru certificate avansate de utilizator (subscriber), generarea cheilor are loc în următoarele moduri, în funcție de modul de livrare a serviciului:

- Generare locală pe dispozitivul titularului (smart card, token USB, soft-token, browser) — cheia privată este creată și păstrată exclusiv sub controlul titularului; QSIGN primește doar CSR-ul (PKCS#10) cu cheia publică. Acesta este modul implicit pentru certificate avansate „desktop”, conform descrierii din cerere („Cheile criptografice utilizate pentru semnătură vor fi generate și protejate de către utilizator”).
- Generare în HSM-ul QSIGN sub control exclusiv al titularului — pentru serviciul de remote signing avansat. Cheia este creată într-o partiție logică alocată titularului (one key per subscriber), activarea cheii se face exclusiv prin SAD (Signature Activation Data) sub controlul exclusiv al titularului, conform principiilor SCAL2 din EN 419 241-1 (deși certificarea formală EN 419 241-2 nu este obligatorie pentru servicii avansate). Cheia nu părăsește niciodată HSM-ul în formă neprotejată.
- Generare pe SSCD (Secure Signature Creation Device) opțional — în cazurile în care titularul preferă un nivel mai ridicat de protecție, QSIGN poate emite certificate avansate pe smart card SSCD, dar această configurație nu este obligatorie pentru calificarea „avansată” și este oferită ca opțiune comercială.

Tabelul de mai jos sintetizează modul de generare a cheilor pentru fiecare tip de CA și certificat de utilizator emis sub acest CP/CPS.

Componentă / Tip certificat	Locație generare cheie	Standard HSM/SCD	Cerință obligatorie
Root CA Avansate	HSM dedicat, ceremonie offline	FIPS 140-3 L3 + CC EAL4+	Da — HSM
Issuing CA NCP+ / NCP / LCP (PF)	HSM dedicat, ceremonie online	FIPS 140-3 L3 + CC EAL4+	Da — HSM
Issuing CA NCP+ / NCP / LCP	HSM dedicat, ceremonie	FIPS 140-3 L3 +	Da — HSM

Componentă / Tip certificat	Locație generare cheie	Standard HSM/SCD	Cerință obligatorie
(PJ)	online	CC EAL4+	
OCSP Responder (linie avansată)	HSM partajat sau dedicat	FIPS 140-2/3 L2+	Recomandat — HSM
Certificat utilizator (NCP+ — PF)	Token / smart card titular sau HSM remote QSIGN	Soft-store sau HSM SCAL2-eq.	Cheia să fie sub controlul titularului
Certificat utilizator (NCP — PF)	Token / soft-token titular sau HSM remote QSIGN	Soft-store sau HSM SCAL2-eq.	Cheia să fie sub controlul titularului
Certificat utilizator (LCP — PF)	Soft-token / browser / mobil titular	Soft-store	Cheia să fie sub controlul titularului
Certificat utilizator (NCP+ / NCP — PJ)	HSM organizație sau HSM remote QSIGN	FIPS 140-2 L2+ recomandat	Cheia să fie sub controlul titularului

6.1.2 Livrarea cheii private către titular

Pentru cheile generate local de titular, întrebarea este irelevantă — cheia nu părăsește mediul titularului. Pentru cheile generate în HSM-ul QSIGN (remote signing avansat), cheia privată nu este livrată titularului în niciun moment; titularul are control exclusiv asupra cheii prin SAD (autentificare puternică multi-factor: parolă + OTP + biometrie sau certificat de autentificare). Pentru cazurile excepționale în care QSIGN livrează un dispozitiv pre-personalizat (smart card cu cheie pre-generată), livrarea se face în plic securizat sigilat, separat de PIN-ul de activare (livrat pe canal distinct), iar titularul este obligat să schimbe PIN-ul la prima utilizare.

6.1.3 Livrarea cheii publice CA-ului emitent

Pentru certificatele cu cheie generată local, cheia publică este transmisă către QSIGN într-o cerere PKCS#10 (CSR) semnată cu cheia privată corespunzătoare, prin canal autentificat (portal QSIGN cu autentificare puternică sau API mTLS). Pentru cheile generate în HSM-ul QSIGN, cheia publică este disponibilă imediat după generare în sistemul intern de certificare.

6.1.4 Livrarea cheii publice CA către părțile încrezătoare

Cheile publice ale Root CA și Issuing CA-urilor pentru linia avansată sunt publicate în repository-ul QSIGN (https://www.qsign.ro/repository). Întrucât serviciile avansate NU sunt incluse în Romanian Trusted List (TL), validarea de încredere se realizează: (i) prin instalarea voluntară a Root CA QSIGN Avansate în trust store-ul aplicației; (ii) prin lanțul de certificate distribuit cu certificatul utilizatorului (AIA — Authority Information Access). QSIGN publică certificatele CA atât în format DER, cât și PEM, alături de hash-urile SHA-256 și SHA-384 ale acestora.

6.1.5 Lungimile cheilor

Pentru certificate emise sub acest CP/CPS:

- Root CA Avansate: RSA 4096 biți sau ECDSA P-384 (curbă brainpoolP384r1 sau secp384r1).
- Issuing CA-uri: RSA 4096 biți sau ECDSA P-384.
- Certificate utilizator (subscriber): minim RSA 2048 biți (recomandat 3072) sau ECDSA P-256/P-384. Cheile cu lungime sub minim sunt respinse de RA.
- Algoritm hash: SHA-256, SHA-384 sau SHA-512. SHA-1 este interzis pentru semnături. MD5 este interzis.
- Aceste lungimi respectă cerințele ETSI TS 119 312 și recomandările NIST SP 800-57.

6.1.6 Generarea parametrilor cheilor publice și verificarea calității

Toate cheile generate sunt verificate prin: (i) testele FIPS 140-3 ale HSM-ului (continuous random number test, pair-wise consistency test); (ii) la nivel software, QSIGN aplică verificări post-generare: dimensiunea modulului RSA, pătratul perfect (test simplu de calitate), absența factorilor mici. Pentru cheile primite în CSR, QSIGN verifică conformitatea cu lungimile minime și absența cheilor compromise (verificare împotriva listei publice de chei compromise — debian weak keys, ROCA Infineon TPM).

6.1.7 Scopurile de utilizare a cheii (Key Usage)

Conform ETSI EN 319 412-2, valorile permise pentru extensia keyUsage a certificatelor avansate emise sub acest CP/CPS sunt:

Tip certificat	keyUsage permis	extKeyUsage tipic
Avansat semnătură (PF) — NCP+/NCP/LCP	digitalSignature, nonRepudiation	emailProtection (opțional)
Avansat sigiliu (PJ) — NCP+/NCP	digitalSignature, nonRepudiation	emailProtection (opțional)
Issuing CA Avansate	keyCertSign, cRLSign	—
Root CA Avansate	keyCertSign, cRLSign	—
OCSP Responder	digitalSignature	id-kp-OCSPSigning

6.2 Protecția cheii private și controale tehnice asupra modulelor criptografice

6.2.1 Standarde și controale ale modulelor criptografice

HSM-urile utilizate de QSIGN pentru CA-urile liniei avansate respectă FIPS 140-3 nivel 3 sau, în perioada de migrare, FIPS 140-2 nivel 3 cu plan de tranziție. Common Criteria EAL4+ este obținut adițional. Pentru remote signing avansat, configurația tehnică respectă principiile SCAL2 din EN 419 241-1 (Sole control by the signer assured through Signature Activation Module — SAM). Configurațiile HSM sunt jurnalizate și verificate semestrial.

6.2.2 Controlul cheii private prin mai multe persoane (m-of-n)

Toate operațiunile critice asupra cheilor CA Avansate (generare, activare după re-pornire, backup, restaurare, distrugere) necesită cvorum „m-of-n”: 3 din 5 custodieni autorizați, fiecare deținând un smart card de activare cu PIN propriu. Pentru funcționarea operațională a CA-ului (semnare certificate, semnare CRL), modul „auto-activate” cu „auto-resume” este permis, dar cu jurnalizare strictă; activarea inițială rămâne sub control m-of-n.

6.2.3 Custodia cheii private

QSIGN nu plasează niciodată cheile private CA în custodia unei terțe părți (no key escrow). Pentru remote signing avansat, cheile titularilor sunt sub control exclusiv al titularului (prin SAD); QSIGN este custode tehnic al containerului HSM, dar nu are capacitatea operațională de a utiliza cheia titularului. Pentru cheile generate de utilizator pe propriul dispozitiv, QSIGN nu are acces sub nicio formă.

6.2.4 Backup-ul cheii private

Cheile private CA sunt backup-uite în formă criptată („wrapped key” sau „encrypted backup”) către un al doilea HSM (DR site) și către medii offline criptate (HSM smart cards de backup), păstrate în safe-uri certificate, în două locații geografice distincte. Restaurarea necesită cvorum m-of-n. Pentru cheile titularilor în remote signing, backup-ul este parte integrantă a containerului HSM, supus aceleași politici de păstrare și control de acces.

6.2.5 Arhivarea cheii private

Cheile private CA Avansate ieșite din uz (după key changeover) sunt păstrate în formă criptată într-un seif HSM offline, exclusiv pentru a permite generarea de CRL-uri sau pentru investigații forensic ulterioare, până la expirarea ultimului certificat emis cu acea cheie. După această perioadă, cheile sunt distruse (vezi 6.2.10). Cheile titularilor (remote signing) NU sunt arhivate după revocare — sunt distruse.

6.2.6 Transferul cheii private în/din modulul criptografic

Cheile private CA nu sunt exportate în formă neprotejată. Transferul (între HSM principal și HSM DR/backup) se face exclusiv în formă wrapped, criptată cu cheie de transport HSM-internă (Key Transport Key — KTK). Procedura este executată sub cvorum și jurnalizată. Pentru cheile titularilor (remote signing), nu există mecanism de export.

6.2.7 Stocarea cheii private în modulul criptografic

În interiorul HSM-ului, cheile private sunt stocate criptat cu master key-ul HSM-ului și protejate de mecanismele hardware împotriva extracției (tamper-evident și tamper-responsive).

6.2.8 Metoda de activare a cheii private

Activarea cheii CA: cvorum m-of-n de custodieni cu smart card-uri de activare și PIN-uri, în prezența unui supervizor; sesiune de activare jurnalizată. Activarea cheii titularului (remote signing): SAD cu autentificare puternică multi-factor (parolă + OTP + biometrie sau autentificare cu certificat de autentificare avansat).

6.2.9 Metoda de dezactivare a cheii private

Cheile CA pot fi dezactivate manual de către PKI Manager în caz de incident; dezactivarea automată se aplică la repornirea HSM-ului (cheia rămâne necesară pentru re-activare, m-of-n). Pentru cheile titularilor, sesiunea SAD expiră automat după interval de inactivitate configurabil (implicit 5 minute).

6.2.10 Metoda de distrugere a cheii private

Cheile CA ieșite definitiv din uz (după expirarea ultimului certificat emis cu ele) sunt distruse într-o ceremonie de distrugere (Key Destruction Ceremony), filmată, cu m-of-n custodieni; HSM-ul execută operațiunea „zeroize” și raportul HSM atestă distrugerea. Smart card-urile de backup sunt distruse fizic. Cheile titularilor (remote signing) sunt zeroizate la revocare, iar partiția HSM este eliberată.

6.2.11 Aprecierea modulului criptografic

HSM-urile utilizate sunt evaluate de producător și certificate. QSIGN verifică valabilitatea certificărilor anual și aplică patch-urile de firmware după evaluare de impact. Migrarea către niveluri superioare (FIPS 140-3) este planificată în roadmap-ul tehnic 2026–2027.

6.3 Alte aspecte ale managementului perechii de chei

6.3.1 Arhivarea cheii publice

Toate cheile publice ale CA-urilor și ale certificatelor emise sunt arhivate în baza de date a certificatelor (CertDB) și în arhiva electronică acreditată/calificată, cu păstrare minim 10 ani după încetarea valabilității. Arhivarea este integrată cu jurnalele de audit (vezi 5.5).

6.3.2 Perioadele operaționale ale certificatelor și perechilor de chei

Tabelul de mai jos sintetizează perioadele de valabilitate (validity period) aplicabile certificatelor emise sub acest CP/CPS. Aceste valori sunt orientative; perioada exactă este selectată de titular în limita maxim admisă, cu ținta de a permite înlocuirea cheilor înainte ca algoritmii sau lungimile să devină depreciate.

Componentă / certificat	Validitate maximă cheie	Validitate maximă certificat
Root CA Avansate	25 ani	25 ani (auto-semnat)
Issuing CA Avansate	12 ani	12 ani
OCSP Responder Avansate	1 an (rotație frecventă recomandată)	1 an
Certificat avansat (NCP+) — PF/PJ	3 ani	3 ani (recomandat); maxim 5 ani
Certificat avansat (NCP) — PF/PJ	3 ani	3 ani (recomandat); maxim 5 ani

Componentă / certificat	Validitate maximă cheie	Validitate maximă certificat
Certificat avansat (LCP) — PF	1 an	1 an (recomandat); maxim 2 ani

Notă: pentru certificatele avansate, durata maximă acceptată reflectă echilibrul dintre ușurință de utilizare și risc criptografic — limita de 5 ani pentru NCP+/NCP este conservatoare și aliniată recomandărilor ETSI EN 319 411-1; LCP, cu un nivel de încredere mai redus, este limitat la maxim 2 ani.

6.4 Datele de activare

6.4.1 Generarea și instalarea datelor de activare

Datele de activare (PIN-uri, parole, SAD pentru remote signing) sunt generate cu entropie criptografică suficientă (minim 12 caractere, mix de litere mari, mici, cifre și simboluri pentru parole; PIN minim 6 cifre cu blocare după 3 încercări greșite pentru smart card-uri custodieni). Pentru SAD-ul de remote signing, sunt aplicabile politici NIST SP 800-63B nivel AAL2 sau echivalent.

6.4.2 Protecția datelor de activare

PIN-urile și parolele nu sunt niciodată jurnalizate în clar; QSIGN păstrează doar valori hash-uite (cu salt și algoritm rezistent la atacuri brute-force, e.g. Argon2id). Smart card-urile custodieni sunt păstrate în safe-uri individuale, separate de HSM-uri. Pentru remote signing, SAD-ul nu este niciodată stocat persistent; sesiunile sunt cu durată limitată și legate la dispozitivul autentificat.

6.4.3 Alte aspecte ale datelor de activare

Politica de schimbare obligatorie: PIN-urile custodieni — la rotația anuală sau la schimbarea unui custode; parolele de administrare a sistemelor — la 90 zile; SAD-ul de remote signing — schimbarea credențialelor de bază (parolă, factor secundar) la solicitarea titularului sau forțat la suspiciune de compromitere.

6.5 Controale de securitate ale calculatoarelor

6.5.1 Cerințe tehnice specifice de securitate ale calculatoarelor

Sistemele care găzduiesc CA-urile, RA-urile, OCSP-urile și SIEM-ul respectă cerințele ETSI EN 319 401 (clauza referitoare la controale tehnice) și CIS Benchmarks aplicabile. Cerințe esențiale: (i) hardening conform CIS Benchmark Linux (Ubuntu/Debian); (ii) actualizări de securitate aplicate în maxim 7 zile de la publicare (sau 24 ore pentru critical CVE); (iii) auditarea sistemică prin auditd; (iv) integrity monitoring (Wazuh FIM); (v) rețea segregată în VLAN-uri dedicate, cu firewall de tip stateful (nftables); (vi) accesul administrativ prin bastion-host cu MFA; (vii) anti-malware actualizat în mod automat; (viii) verificare integritate la boot (Secure Boot, dm-verity unde aplicabil); (ix) absolutele „no shell on production” pentru aplicațiile CA — toate operațiunile prin API jurnalizat.

6.5.2 Aprecierea calității controalelor de securitate ale calculatoarelor

Auditul intern semestrial verifică implementarea fiecărui control. Pen-testing extern anual evaluează rezistența la atacuri reale. Vulnerability scanning automat săptămânal.

6.6 Controale tehnice ale ciclului de viață

6.6.1 Controale de dezvoltare a sistemelor

Întreaga dezvoltare software (componente proprii ale platformei QSIGN) urmează un Secure Development Lifecycle (SDLC): cerințe de securitate documentate; threat modeling; review de cod (peer review obligatoriu); testare automată (unit, integration, security tests); SAST și DAST; gestiunea dependențelor (SBOM, vulnerability scanning); revizia înainte de release.

6.6.2 Controale ale managementului securității

Sistemul de management al securității informației (ISMS) este aliniat cu ISO/IEC 27001 (certificare planificată în 2027) și cu ETSI EN 319 401. Politici scrise pentru fiecare arie de control, revizuite anual de Comitetul de Management al Securității.

6.6.3 Controale ale ciclului de viață a securității

Schimbările sunt gestionate prin Change Management Process (CMP) cu aprobare CISO + PKI Manager pentru schimbări critice. Mediul de testare (staging) este izolat de producție, cu date sintetice; nicio dată reală de producție nu este utilizată în staging.

6.7 Controale de securitate a rețelei

Toate sistemele critice ale liniei avansate sunt amplasate într-o zonă de rețea dedicată (VLAN PKI), separată prin firewall-uri stateful (BPI-R4 cu nftables) atât de Internet, cât și de rețeaua corporativă QSIGN. Fluxurile permise sunt minimaliste: (i) ieșire pentru OCSP/CRL/repository (HTTPS publice); (ii) replicare DR (canal IPsec); (iii) accesare administrativă prin bastion (SSH cu certificat, MFA). IDS/IPS Suricata monitorizează tot traficul. Conform memoriilor anterioare, infrastructura include: BPI-R4 ca gateway/edge security, nftables ca firewall principal, Suricata ca IDS/IPS în mod NFQueue, Wazuh ca SIEM, knockd pentru port knocking pe interfețele de management. Toate canalele de management sunt criptate (TLS 1.3 minim, mTLS unde este posibil).

6.8 Marca temporală

Operațiunile interne ale CA-urilor (semnare certificate, semnare CRL, emitere OCSP) sunt sincronizate la o sursă de timp UTC trasabilă (servere NTP stratum 1 cu referință GPS sau prin radio); abaterea maximă admisă este de ±100 ms. Pentru sigilarea jurnalelor și a evidențelor de audit, QSIGN aplică marca temporală calificată (QTSA) emisă de propriul serviciu calificat (descris în CP/CPS Calificat — QSIGN-CP-CPS-QC-v1.0). Notă: serviciul de marcare temporală este oferit exclusiv ca serviciu calificat de QSIGN; nu există un serviciu separat de marcare temporală necalificată sub acest CP/CPS.

7. Profilele certificatelor, CRL-urilor și OCSP

7.1 Profilul certificatului

Toate certificatele avansate emise sub acest CP/CPS respectă RFC 5280 și ETSI EN 319 412 (părțile 1, 2 și 3). Spre deosebire de certificatele calificate, certificatele avansate emise de QSIGN NU includ extensia QCStatements cu valorile id-etsi-qcs-QcCompliance, id-etsi-qcs-QcSSCD sau id-etsi-qcs-QcType pentru certificate calificate; identificarea politicii se face exclusiv prin extensia certificatePolicies cu OID-urile ETSI corespunzătoare.

7.1.1 Numărul versiunii

Toate certificatele sunt emise în versiunea 3 (v3) conform RFC 5280, codate DER.

7.1.2 Extensiile certificatului

7.1.2.1 Extensii comune tuturor certificatelor de utilizator avansate

Extensie	Critică?	Conținut tipic
Authority Key Identifier	Nu	SHA-1 hash al cheii publice CA emitente
Subject Key Identifier	Nu	SHA-1 hash al cheii publice a subiectului
Key Usage	Da	digitalSignature, nonRepudiation
Extended Key Usage	Nu	Opțional: emailProtection (id-kp-emailProtection)
Certificate Policies	Nu	OID politică ETSI (vezi 7.1.6) + CPS URI + UserNotice
CRL Distribution Points	Nu	URL CRL public QSIGN
Authority Information Access	Nu	URL OCSP + URL caIssuers (CA chain)
Subject Alternative Name	Nu (Da pt. SAN unic)	rfc822Name (e-mail) opțional; alte forme conform ETSI EN 319 412
Basic Constraints	Da	cA = FALSE pentru certificate end-entity

7.1.2.2 Extensii specifice persoanelor fizice (NCP+, NCP, LCP)

Subject DN include atributele: CN (commonName) — numele complet sau pseudonimul; givenName, surname (în cazul utilizării numelui real); serialNumber — cu prefix semantic „PNORO-” urmat de CNP pentru cetățeni români, sau „PI-” cu identificator pașaport pentru alți titulari, conform ETSI EN 319 412-1; pseudonym — atunci când este utilizat pseudonimul (vezi 3.1.3); countryName — codul ISO al țării de identificare. SubjectAltName (SAN) poate include rfc822Name (e-mail confirmat).

7.1.2.3 Extensii specifice persoanelor juridice (NCP+, NCP)

Subject DN include: CN — denumirea juridică oficială; organizationName (O) — aceeași denumire; organizationIdentifier — cu prefix semantic „NTRRO-" urmat de numărul de înregistrare la ONRC, sau „VATRO-" urmat de codul de TVA, sau alte prefixe ETSI EN 319 412-1 conform țării/identificatorului; countryName. Opțional, SAN poate include URI și/sau rfc822Name.

7.1.2.4 Extensii specifice CA-urilor

Pentru Issuing CA Avansate: Basic Constraints cu cA=TRUE și pathLenConstraint=0; Key Usage = keyCertSign, cRLSign; Certificate Policies = OID-uri politici emise de această CA; AIA pentru OCSP (al CA-ului superior) și caIssuers; CRL Distribution Points — URL CRL al CA-ului superior. Pentru Root CA Avansate: Basic Constraints cu cA=TRUE; Key Usage = keyCertSign, cRLSign; Subject DN = Issuer DN (auto-semnat); fără AIA (este rădăcină de încredere).

7.1.3 Identificatorii algoritmilor

Algoritmi de semnare suportați: ecdsa-with-SHA256 (1.2.840.10045.4.3.2), ecdsa-with-SHA384 (1.2.840.10045.4.3.3), sha256WithRSAEncryption (1.2.840.113549.1.1.11), sha384WithRSAEncryption (1.2.840.113549.1.1.12). Algoritmul de hash al amprentei certificatului (la sigilare repository) este SHA-256 minim.

7.1.4 Formele numelor

Atributele Subject DN sunt codate UTF-8 (UTF8String); excepție notabilă: countryName este codat PrintableString conform RFC 5280. Caracterele speciale RFC 4514 sunt escape-uite. Diacriticele românești sunt păstrate.

7.1.5 Constrângerile asupra numelor

QSIGN nu emite, sub acest CP/CPS, certificate de tip „Name Constraints CA".

7.1.6 Identificatorul OID al politicii certificatului

Extensia certificatePolicies include OID-urile ETSI ale politicilor implementate, plus OID-urile interne QSIGN pentru identificarea acestui CP/CPS și a profilului specific. Tabelul de mai jos sintetizează maparea politicilor.

Politică ETSI	OID ETSI	OID intern QSIGN	Aplicare
NCP+ (Normalized Certificate Policy +)	0.4.0.2042.1.2	1.3.6.1.4.1.59019.2.1.1	Avansat PF/PJ; SSCD recomandat sau remote signing SCAL2
NCP (Normalized Certificate Policy)	0.4.0.2042.1.1	1.3.6.1.4.1.59019.2.2.1	Avansat PF/PJ; soft-token sau remote signing

Politică ETSI	OID ETSI	OID intern QSIGN	Aplicare
LCP (Lightweight Certificate Policy)	0.4.0.2042.1.3	1.3.6.1.4.1.59019.2.3.1	Avansat PF — uz redus / e-mail signing

Notă: OID-ul intern QSIGN (1.3.6.1.4.1.59019) reprezintă rădăcina IANA Private Enterprise Number alocată QSIGN; valoarea concretă este publicată în repository și menționată în versiunea publicată a CP/CPS-ului.

7.1.7 Utilizarea extensiei „Policy Constraints”

QSIGN nu utilizează extensia policyConstraints în certificatele de utilizator. Extensia poate fi utilizată în certificatele Issuing CA pentru a impune cerințe de policy mapping; valoarea implicită este absentă.

7.1.8 Sintaxa și semantica calificatorilor de politică

Calificatorii utilizați: id-qt-cps (1.3.6.1.5.5.7.2.1) cu URI către documentul CP/CPS publicat (https://www.qsign.ro/repository/cpcps-advanced); id-qt-unotice (1.3.6.1.5.5.7.2.2) cu textul „Acest certificat este un certificat de încredere AVANSAT (NECALIFICAT) emis de QSIGN S.R.L. în conformitate cu CP/CPS-ul publicat la URL-ul indicat. Certificatul nu este calificat în sensul art. 3 pct. 14 din Regulamentul (UE) nr. 910/2014.”.

7.1.9 Prelucrarea semantică a extensiei „Critical Certificate Policies”

Extensia certificatePolicies este marcată ne-critică, conform practicilor uzuale; aplicațiile încrezătoare sunt totuși așteptate să verifice OID-ul politicii pentru a determina nivelul de încredere.

7.2 Profilul listei de revocare (CRL)

7.2.1 Numărul versiunii

Toate CRL-urile sunt emise în versiunea 2 (v2) conform RFC 5280.

7.2.2 Extensiile CRL și extensiile intrărilor CRL

CRL-ul include următoarele extensii: Authority Key Identifier; CRL Number (incremental); Issuing Distribution Point (URL CRL); next publish (thisUpdate, nextUpdate). Pentru intrări individuale: revocation date; reason code (cu valori uzuale: keyCompromise, cACompromise, affiliationChanged, superseded, cessationOfOperation, certificateHold) — notabil, certificateHold (suspendarea) ESTE permis pentru certificate avansate (vezi 4.9.13).

7.3 Profilul OCSP

7.3.1 Numărul versiunii

Răspunsurile OCSP sunt emise conform RFC 6960 (versiunea 1).

7.3.2 Extensiile OCSP

Extensii suportate: nonce (id-pkix-ocsp-nonce, 1.3.6.1.5.5.7.48.1.2) — opțional, recunoscut de responder; preferred response signature algorithm — recunoscut. Răspunsurile sunt semnate cu cheia OCSP Responder, care este la rândul său un certificat dedicat emis de Issuing CA-ul corespunzător, cu extensia id-kp-OCSPSigning în EKU; certificatul OCSP Responder include extensia id-pkix-ocsp-nocheck pentru a evita bucla de verificare. Notă: pentru certificate avansate, statusul „suspendat” este reflectat OCSP cu reason code certificateHold; ridicarea suspendării este reflectată în CRL-ul următor și OCSP corespunzător.

8. Auditul conformității

Auditul conformității reprezintă mecanismul prin care se demonstrează către ADR și către părțile interesate că serviciile avansate prestate de QSIGN respectă cerințele eIDAS, ale Anexei 2 la Ordinul MEDAT 102/2026 și ale standardelor tehnice aplicabile. Spre deosebire de auditul serviciilor calificate (care se efectuează de către un Conformity Assessment Body — CAB acreditat conform ISO/IEC 17065 pentru ETSI EN 319 403-1), pentru serviciile avansate se aplică modelul prevăzut de Decizia ADR pentru auditori autorizați conform Listei Auditorilor pentru Servicii de Comunicații Electronice (LASC), tip auditor „General” (sau echivalentul stabilit de DNSC pentru servicii necalificate).

8.1 Frecvența evaluării

Auditul conformității se efectuează la momente cheie:

- Audit inițial — anterior depunerii cererii de înregistrare la ADR în Registrul prestatorilor de servicii de încredere necalificate, conform documentației solicitate la art. 5 din Anexa 2 la Ordinul MEDAT 102/2026.
- Auditul de re-evaluare — minim o dată la 24 de luni (regula generală pentru servicii avansate, aliniată cu cea pentru serviciile calificate prevăzută la art. 20 alin. (1) eIDAS, aplicată prin analogie). Frecvența mai des poate fi solicitată de ADR în cazuri specifice.
- Audit ad-hoc — la solicitarea ADR, în cazul unui incident semnificativ, al unei plângeri întemeiate sau al modificării substanțiale a serviciului.
- Audit intern — anual, cu raport către management; nu substituie auditul extern.

8.2 Identitatea/calificările auditorului

Auditorul extern este selectat din Lista Auditorilor pentru Servicii de Comunicații Electronice (LASC) publicată de DNSC, având tipul de calificare aplicabil pentru servicii necalificate (tip „General” sau echivalentul actual stabilit prin reglementare). Auditorul trebuie să dispună de personal cu competențe în: (i) PKI, criptografie, OCSP/CRL, eIDAS; (ii) ETSI EN 319 401, 319 411-1; (iii) ISO/IEC 27001 (cunoștințe generale); (iv) legislația română aplicabilă (Legea 214/2024, Ordinul MEDAT 102/2026, GDPR, NIS2/OUG 155/2024). QSIGN solicită CV-urile auditorilor și verifică absența conflictelor de interese (independența auditorului).

8.3 Relația auditorului cu entitatea auditată

Auditorul este independent de QSIGN; nu este angajat, partener comercial sau consultant al QSIGN și nu prestează alte servicii care ar putea afecta independența. Contractul de audit prevede obligații de confidențialitate și clauze anti-conflict de interese. Rotația auditorului (sau a echipei auditoare) este recomandată o dată la maxim 6 ani.

8.4 Domeniile evaluate prin audit

Auditul evaluează:

- Conformitatea cu acest CP/CPS (toate capitolele 1–9).

- Conformitatea cu cerințele Anexei 2 la Ordinul MEDAT 102/2026 (toate articolele aplicabile).
- Conformitatea cu ETSI EN 319 401 și ETSI EN 319 411-1 (NCP, NCP+, LCP).
- Conformitatea cu ETSI TS 119 461 (Identity Proofing — minim Baseline LoIP).
- Conformitatea cu cerințele specifice eIDAS aplicabile serviciilor avansate (art. 26 — semnătură; art. 36 — sigiliu).
- Conformitatea cu GDPR și legislația de protecție a datelor.
- Conformitatea cu cerințele de securitate cibernetică NIS2/OUG 155/2024.
- Securitatea fizică, securitatea personalului, controale tehnice.
- Procesul de identificare la distanță (sesiunile video, înregistrările, deciziile).
- Sistemele de jurnalizare, arhivare, BCP/DRP.
- Procesul de revocare/suspendare/reactivare.

8.5 Acțiunile întreprinse ca rezultat al deficiențelor

Neconformitățile (NC) identificate sunt clasificate:

- NC majoră — afectează capacitatea TSP-ului de a furniza serviciul în conformitate cu cerințele; necesită remediere imediată (în max. 30 zile) și raportare către ADR.
- NC minoră — abatere localizată sau procedurală, fără impact asupra serviciilor curente; remediere în max. 90 zile.
- Observație — recomandare de îmbunătățire, fără caracter obligatoriu.

QSIGN elaborează un Plan de Acțiuni Corective (PAC) cu termene și responsabili pentru fiecare NC; auditorul verifică implementarea la următorul audit (sau în audit follow-up). Neconformitățile majore nesoluționate pot atrage radierea din Registrul prestatorilor necalificate, conform art. 11–12 din Anexa 2 la Ordinul MEDAT 102/2026.

8.6 Comunicarea rezultatelor

Raportul de audit este transmis: (i) ADR — în maxim 30 de zile de la finalizare, în format electronic semnat de auditor; (ii) Conducerii QSIGN — pentru informare și decizii de remediere; (iii) DNSC — la solicitare. O sinteză anonimizată poate fi inclusă în Raportul Anual de Transparență publicat în repository.

9. Alte aspecte comerciale și juridice

9.1 Tarifele

QSIGN aplică tarife transparente, publicate în repository și în Anexa Comercială la Subscriber Agreement. Structura tarifelor pentru serviciile avansate este distinctă de cea pentru serviciile calificate.

9.1.1 Tarife pentru emiterea sau reînnoirea certificatelor

Tarifele de emitere variază în funcție de tipul de certificat (NCP+/NCP/LCP), titular (PF/PJ) și durata aleasă. Reînnoirile (renewal) cu re-validare a identității la LoIP minim Baseline sunt tarifate la prețul standard de emitere. Re-key (cu identitate validată în maxim 12 luni) beneficiază de tarif redus.

9.1.2 Tarife pentru accesul la certificate

Accesul la certificate publicate în repository este gratuit.

9.1.3 Tarife pentru accesul la informațiile de revocare/status

Accesul la CRL și OCSP este gratuit pentru toți utilizatorii și părțile încrezătoare.

9.1.4 Tarife pentru alte servicii

Servicii adiționale (consultanță, integrare API, on-boarding entități cu volum mare) sunt tarifate conform contractelor individuale. Re-emiterea unui certificat ca urmare a unei erori imputabile QSIGN este gratuită.

9.1.5 Politica de rambursare

În cazul unei erori imputabile QSIGN (date incorecte din procesul intern al QSIGN, neîndeplinirea SLA-ului, certificat respins de aplicații încrezătoare din motive tehnice de emitere), tariful aferent este rambursat integral. Pentru certificatele revocate la solicitarea titularului, nu există rambursare a tarifului, sub rezerva dreptului imperativ de retragere de 14 zile pentru consumatori conform OUG nr. 34/2014 (transpunere Directiva 2011/83/UE), aplicabil contractelor încheiate la distanță sau în afara spațiilor comerciale. Acest drept poate fi exclus, conform art. 16 lit. a) din OUG nr. 34/2014, dacă consumatorul a solicitat expres prestarea serviciului în interiorul perioadei de 14 zile și a confirmat în prealabil că își pierde dreptul de retragere odată cu executarea integrală a serviciului (emiterea efectivă a certificatului). În cazul în care emiterea nu a fost executată integral cu acordul prealabil al consumatorului, acesta beneficiază de rambursare integrală a tarifului în termen de 14 zile de la solicitarea de retragere.

9.2 Răspunderea financiară

9.2.1 Acoperirea asigurărilor

QSIGN menține o asigurare de răspundere civilă profesională cu o sumă asigurată de minim 100.000 EUR pe eveniment, conform cerinței art. 5 alin. (2) lit. n) din Anexa 2 la Ordinul

MEDAT 102/2026 (formulare „acoperă serviciile avansate cu sumă minimă 100.000 EUR”). Polița este reînnoită anual și o copie este transmisă ADR la fiecare reînnoire.

9.2.2 Alte active

Activele lichide ale QSIGN și capitalul social sunt menținute la nivel suficient pentru asigurarea continuității operaționale a serviciilor avansate prestate; situațiile financiare sunt depuse la ONRC conform legii.

9.2.3 Acoperirea asigurării sau garanție pentru entitățile finale

Asigurarea acoperă atât răspunderea față de titulari (subscriber), cât și față de părțile încrezătoare (relying party), în limita sumei asigurate și conform clauzelor contractului de asigurare.

9.3 Confidențialitatea informațiilor de afaceri

9.3.1 Domeniul de aplicare al informațiilor confidențiale

Sunt confidențiale: cheile private, datele de activare, parolele, jurnalele detaliate de audit (cu excepția extraselor publicate în Raportul Anual de Transparență), procedurile interne nu publicate, datele cu caracter personal ale titularilor (nume complet, CNP, adrese, copii ale actelor de identitate, înregistrări video de identificare), informațiile comerciale ale QSIGN (contracte, prețuri individualizate, structura furnizorilor).

9.3.2 Informații care nu sunt considerate confidențiale

Sunt publice: certificatele emise (cu excepția cazurilor în care titularul a solicitat retragerea — pentru certificatele care nu sunt publicate proactiv), CRL-urile, statusurile OCSP, certificatele CA-urilor, acest CP/CPS și toate documentele publicate în repository, informațiile generale despre QSIGN (datele de identificare, structura organizatorică).

9.3.3 Responsabilitatea de protejare a informațiilor confidențiale

QSIGN protejează informațiile confidențiale prin politici de securitate documentate, controale tehnice și organizatorice, contracte de confidențialitate cu personalul și contractorii, sancțiuni în caz de încălcare. Divulgarea către terți este permisă exclusiv în temeiul legii (cerere a autorităților competente, cerință de probatoriu judiciar) sau cu consimțământul expres al persoanei vizate.

9.4 Confidențialitatea informațiilor personale (politica de confidențialitate)

9.4.1 Politica de confidențialitate

QSIGN menține o Politică de Confidențialitate și prelucrare a datelor cu caracter personal (Privacy Policy — QSIGN-PP-AC-v1.0) publicată în repository, conformă cu GDPR (Regulamentul (UE) 2016/679) și cu Legea 190/2018. Politica detaliază: temeiurile prelucrării (executarea contractului, obligația legală pentru păstrarea evidențelor probatorii, consimțământul pentru prelucrări secundare); categoriile de date prelucrate; destinatari;

perioada de păstrare; drepturile persoanelor vizate; modalitățile de exercitare; transferurile internaționale (în principiu, nu există).

9.4.2 Informații tratate ca private

Sunt tratate ca date cu caracter personal (private): nume complet, CNP, seria și numărul actului de identitate, adresa de domiciliu/reședință, adresa de e-mail, numărul de telefon, fotografia/scanarea actului de identitate, înregistrarea video a sesiunii de identificare, datele biometrice extrase pentru verificare (în formă temporară, în timpul procesului).

9.4.3 Informații care nu sunt considerate private

Conform GDPR și practicii eIDAS, datele incluse în certificatul însuși (nume, organizație, identificator semantic) — odată ce certificatul este emis și acceptat de titular — sunt considerate publice prin natura instrumentului; titularul își dă consimțământul la publicare prin acceptarea Subscriber Agreement.

9.4.4 Responsabilitatea de protejare a informațiilor private

QSIGN este Operator de date cu caracter personal pentru prelucrările aferente serviciilor avansate. Datele sunt protejate prin: criptare la nivel de stocare (LUKS/dm-crypt pentru baze de date, ZFS native encryption pentru depozite); criptare în tranzit (TLS 1.3 minim); minimizare; pseudonimizare unde este aplicabil; controale de acces (rol-base, principiul minimului privilegiu); jurnalizare audit; ștergere automată la expirarea termenelor de păstrare.

9.4.5 Notificarea și consimțământul de folosire a informațiilor private

Consimțământul informat este obținut de la solicitant la depunerea cererii de certificare, prin acceptarea Subscriber Agreement și a Politicii de Confidențialitate. Pentru prelucrări care nu sunt strict necesare contractului (e.g. comunicări comerciale ulterioare), consimțământul este opțional și separat (granular).

9.4.6 Divulgarea conform unei proceduri judiciare sau administrative

QSIGN divulgă date cu caracter personal exclusiv în temeiul unei cereri scrise legitime — hotărâre judecătorească, ordin al procurorului, cerere a autorităților de control conform legilor în vigoare; cererea este verificată din punct de vedere al competenței și al cadrului legal. Persoana vizată este informată despre divulgare ulterior, dacă legea permite acest lucru.

9.4.7 Alte circumstanțe de divulgare

Divulgarea către terți este interzisă în absența unui temei legal sau a consimțământului expres.

9.5 Drepturi de proprietate intelectuală

Dreptul de autor asupra acestui CP/CPS, asupra procedurilor interne și asupra software-ului dezvoltat intern de QSIGN aparține QSIGN S.R.L. Permisiunea de a reproduce și redistribui acest CP/CPS în formă neschimbată este acordată gratuit, cu condiția păstrării atribuirii. Mărcile, logo-urile și siglele QSIGN sunt protejate; utilizarea lor de către terți necesită

consimțământ scris. Certificatele emise sunt deținute de titulari, dar utilizarea lor este reglementată de Subscriber Agreement și de regulile aplicabile certificatelor avansate.

9.6 Reprezentări și garanții

9.6.1 Reprezentările și garanțiile CA

QSIGN garantează că:

- Va emite certificate avansate în conformitate cu acest CP/CPS, cu Anexa 2 la Ordinul MEDAT 102/2026 și cu standardele ETSI aplicabile.
- Va menține un repository public funcțional, cu informații de revocare actualizate.
- Va aplica Baseline LoIP (sau superior, în funcție de politica selectată) pentru identificarea persoanelor.
- Va respecta termenele de revocare/suspendare prevăzute la 4.9.5.
- Va păstra confidențialitatea informațiilor sub controlul său.
- Va comunica titularilor și ADR orice modificare semnificativă a serviciului.
- Va menține o asigurare de răspundere civilă conform 9.2.1.

9.6.2 Reprezentările și garanțiile RA

RA-ul (operat intern de QSIGN sau prin LRA-uri contractate) garantează că: va aplica procedurile de identificare conform 3.2 și 4.2; va păstra evidențele aferente; va respecta cerințele de confidențialitate.

9.6.3 Reprezentările și garanțiile titularului

Titularul (subscriber) garantează că:

- Informațiile furnizate la cerere sunt corecte, complete și actuale.
- Va proteja cheia privată conform Subscriber Agreement (în special — pentru cheile generate local — că nu va divulga PIN-ul/parola de protecție).
- Va utiliza certificatul exclusiv în scopuri legale și în limitele indicate în CP/CPS și certificat (keyUsage, OID politică).
- Va notifica imediat QSIGN în caz de pierdere a controlului asupra cheii private (compromitere, pierdere dispozitiv, suspiciune de utilizare neautorizată).
- Va înceta utilizarea certificatului în momentul expirării sau revocării acestuia.
- Înțelege că certificatul este AVANSAT (necalificat) și că nu beneficiază de prezumția legală a echivalenței cu semnătura olografă, conform art. 25 alin. (2) Reg. (UE) 910/2014 (acest beneficiu se aplică doar semnăturilor calificate).

9.6.4 Reprezentările și garanțiile părții încrezătoare

Partea încrezătoare (relying party) garantează că:

- Va valida certificatul (lanț, statusul revocării, expirare) la fiecare utilizare.
- Va respecta limitele de utilizare indicate în certificat și în acest CP/CPS.
- Înțelege diferența dintre certificate avansate și calificate și ia decizii informate.
- Va respecta termenii Relying Party Agreement publicat în repository.

9.6.5 Reprezentările și garanțiile altor participanți

LRA-uri, distribuitori autorizați, integratori — sunt obligați contractual la conformitate cu acest CP/CPS și cu cerințele aplicabile.

9.7 Renunțarea la garanții

În măsura permisă de lege, QSIGN nu acordă garanții implicite, altele decât cele expres formulate în acest CP/CPS și în Subscriber Agreement / Relying Party Agreement. În particular, QSIGN nu garantează interoperabilitatea cu orice aplicație terță care utilizează certificatele, deși asigură conformitatea cu standardele uzuale (RFC 5280, RFC 6960, ETSI EN 319 412).

9.8 Limitarea răspunderii

Răspunderea QSIGN pentru servicii avansate este limitată conform următoarelor principii:

- Pentru daune directe imputabile QSIGN, plafonul global de despăgubire pe eveniment este suma asigurată prin polița de răspundere civilă (minim 100.000 EUR); pentru daune cumulative anuale, plafonul este suma asigurată anuală.
- QSIGN nu răspunde pentru daune indirecte, pierderi de profit, pierderi de oportunitate, întreruperi de afaceri, pierderea de date neaferentă serviciului propriu, în măsura permisă de lege.
- QSIGN nu răspunde pentru utilizarea unui certificat în condiții ce încalcă acest CP/CPS sau Subscriber/Relying Party Agreement (utilizare în afara keyUsage, ignorarea status-ului de revocare, depășirea limitelor de utilizare).
- QSIGN nu răspunde pentru consecințele unor erori în datele furnizate de titular dacă acestea nu puteau fi detectate cu mijloacele rezonabile aplicabile la verificarea identității.
- Pentru servicii avansate, NU se aplică prezumția de eroare imputabilă TSP din art. 13 alin. (1) eIDAS în aceeași formă ca pentru servicii calificate; sarcina probei daunei și a culpabilității revine părții reclamante, conform regulilor generale de drept civil român.

Aceste limitări nu se aplică în cazul faptelor comise cu intenție sau culpă gravă, conform legii.

9.9 Indemnizația

Subscriber și Relying Party se obligă să indemnizeze QSIGN pentru prejudiciul direct, cert și demonstrabil cauzat prin nerespectarea propriilor obligații săvârșită cu intenție sau culpă gravă (utilizare neautorizată a certificatului, declarații false la cerere săvârșite cu vinovăție, ignorarea cu rea-credință a statusului de revocare etc.). Indemnizarea nu acoperă prejudiciile indirecte, pierderea de profit sau de oportunitate, întreruperile de afaceri ori prejudiciile care nu pot fi probate cu mijloace obiective. Pentru Abonații 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; orice clauză contrară este considerată nescrisă conform art. 4 alin. (3) din Legea nr. 193/2000. Clauzele detaliate sunt în Subscriber Agreement și Relying Party Agreement.

9.10 Termenul și rezilierea

9.10.1 Termenul

Acest CP/CPS este în vigoare de la data publicării sale (anunțată ca data primei publicări în repository) și până la momentul în care este înlocuit de o versiune ulterioară sau retras explicit.

9.10.2 Rezilierea

CP/CPS-ul poate fi retras: (i) la încetarea activității de prestator de servicii de încredere avansate a QSIGN (vezi 5.8); (ii) la înlocuirea cu o versiune ulterioară (versionare semantică, e.g. v1.0 → v1.1).

9.10.3 Efectul rezilierii și supraviețuirea

Drepturile și obligațiile din clauzele de confidențialitate, de răspundere, de jurisdicție supraviețuiesc rezilierii. Certificatele emise în baza unei versiuni anterioare a CP/CPS-ului rămân valabile conform versiunii sub care au fost emise, până la expirarea sau revocarea acestora; aplicarea unei versiuni ulterioare (revocare conform regulilor mai noi) este permisă numai în condiții explicit declarate.

9.11 Comunicările individuale și notificările

Notificările formale către QSIGN se transmit la sediul social: Str. Drumea Rădulescu, nr. 26, sector 4, București, sau electronic la adresa info@qsign.ro (semnată electronic avansat sau calificat). Notificările către titulari se transmit la adresa de e-mail și/sau adresa fizică declarate la cerere; titularul are obligația să mențină datele de contact actualizate. Notificările către ADR și către alte autorități urmează căile prevăzute de lege și de reglementări.

9.12 Modificările

9.12.1 Procedura de modificare

Modificările acestui CP/CPS se inițiază de Comitetul de Politică (Policy Authority — PA) al QSIGN, format din: Administrator (Trandafirescu Alexandru Florin), CISO, PKI Manager, DPO. PA aprobă modificările. Modificările minore (corectări de erori, clarificări) sunt aprobate prin decizie a PA și sunt publicate cu un nou număr de versiune minor. Modificările majore (schimbări de fond ale serviciilor, ale procedurilor de identificare, ale politicilor de revocare) necesită analiză de impact, eventual consultare publică (30 zile minim) și notificare ADR cu 30 zile înainte de aplicare.

9.12.2 Mecanismul și perioada de notificare

Versiunile noi ale CP/CPS-ului sunt publicate în repository și anunțate prin: (i) buletin pe pagina principală qsign.ro; (ii) notificare e-mail către titularii activi; (iii) notificare ADR. Modificările intră în vigoare la 30 de zile de la publicare (pentru modificări majore), respectiv imediat (pentru modificări minore explicite ca atare).

9.12.3 Circumstanțele în care OID-ul trebuie schimbat

OID-ul intern QSIGN al politicii este schimbat dacă modificarea afectează semnificativ semantica certificatelor emise (e.g. modificarea LoIP-ului impus, modificarea KeyUsage). Modificările care nu afectează semantica păstrează OID-ul, dar incrementează numărul de versiune.

9.13 Procedurile de soluționare a disputelor

Disputele dintre QSIGN și titulari/părți încrezătoare se rezolvă prin:

- Negociere amiabilă — cu durată minimă de 30 zile de la notificarea formală a disputei.
- Mediere voluntară — la solicitarea părților, conform Legii 192/2006.
- Soluționare administrativă — pentru aspecte de conformitate cu reglementările eIDAS și naționale, prin sesizarea ADR.
- Soluționare în instanță — în cazul eșecului celorlalte mecanisme; instanțele competente sunt cele de la sediul QSIGN (București), conform regulilor procedurale.

9.14 Legea aplicabilă

Acest CP/CPS și serviciile avansate prestate sub el sunt guvernate de:

- Regulamentul (UE) nr. 910/2014 (eIDAS), în special art. 26, art. 36 (semnătură/sigiliu avansat) — fără a aplica regimul calificat al art. 28, 38, 42.
- Legea nr. 214/2024 privind utilizarea semnăturii electronice, a sigiliului electronic și a serviciilor de încredere — dispozițiile aplicabile prestatorilor de servicii necalificate.
- Ordinul MEDAT nr. 102/29.01.2026, cu Anexa 2 — Cerințele tehnice și organizaționale pentru prestatorii de servicii de încredere necalificate.
- OUG 155/2024 (transpunere NIS2) — cu privire la securitatea cibernetică.
- Regulamentul (UE) 2016/679 (GDPR) și Legea 190/2018 — cu privire la datele personale.
- Codul Civil al României, Codul Procesuală Civilă, alte acte normative aplicabile.

9.15 Conformitatea cu legea aplicabilă

QSIGN se angajează să respecte continuu legislația aplicabilă, inclusiv evoluțiile acesteia (transpunerea eIDAS 2.0 / Reg. (UE) 2024/1183, modificări ale standardelor ETSI). Modificările legale sunt monitorizate de echipa juridică internă; ajustările CP/CPS-ului se efectuează conform 9.12.

9.16 Diverse

9.16.1 Acordul integral

Acest CP/CPS, împreună cu Subscriber Agreement, Relying Party Agreement, Politica de Confidențialitate, PDS-ul și anexele tehnice, formează acordul integral între QSIGN și titulari/părți încrezătoare cu privire la serviciile avansate prestate. Orice conflict între documente este rezolvat în favoarea acestui CP/CPS.

9.16.2 Cesiunea drepturilor

Drepturile și obligațiile QSIGN nu pot fi cesionate fără notificarea ADR și a titularilor activi, în condițiile prevăzute la 5.8 (încetare/transfer). Drepturile titularilor (certificatul) sunt strict personale și nu pot fi cesionate; o nouă cerere este necesară pentru fiecare entitate.

9.16.3 Divizibilitatea

Dacă o clauză a acestui CP/CPS este declarată nulă sau inaplicabilă, celelalte clauze rămân în vigoare în măsura în care economia documentului permite acest lucru.

9.16.4 Renunțarea

Neexercitarea de către QSIGN a unui drept la un anumit moment nu constituie renunțare la acel drept pentru alte momente.

9.16.5 Forța majoră

Niciuna dintre părți nu este răspunzătoare pentru neexecutarea obligațiilor din cauze de forță majoră (calamități naturale, război, pandemii cu restricții oficiale, atacuri cibernetice masive de natură statală). Partea afectată notifică imediat cealaltă parte și depune eforturile rezonabile de a relua executarea cât mai curând posibil.

9.17 Alte prevederi

Versiunea în limba română este versiunea autoritate a acestui CP/CPS. O traducere în limba engleză poate fi pusă la dispoziție pentru convenabilitatea cititorilor; în caz de discrepanță, versiunea română prevalează.

Anexe

Anexa A — Documente conexe

Următoarele documente, parte integrantă a sistemului documentar QSIGN pentru serviciile avansate, sunt referite în acest CP/CPS și sunt publicate în repository sau pun la dispoziție prin canale de încredere conform clasificării lor:

- PDS-AC — PKI Disclosure Statement pentru servicii avansate (QSIGN-PDS-AC-v1.0) — public, în repository.
- Subscriber Agreement — Avansat (QSIGN-SA-AC-v1.0) — public.
- Relying Party Agreement — Avansat (QSIGN-RPA-AC-v1.0) — public.
- Privacy Policy (QSIGN-PP-AC-v1.0) — public.
- Termination Plan / Plan de încetare a activității (QSIGN-TP-AC-v1.0) — pus la dispoziție ADR; sinteză publică.
- Information Security Policy (QSIGN-ISP-v1.0) — internă.
- Plan de continuitate a afacerii (BCP) și Plan de Recuperare în caz de Dezastru (DRP) (QSIGN-BCPDRP-v1.0) — internă; sinteză publică.
- Plan de instruire personal (QSIGN-PI-v1.0) — internă.
- Plan de întreținere și actualizare a sistemului informatic (QSIGN-PISIT-v1.0) — internă.
- Politica de Identificare la Distanță (QSIGN-IDR-v1.0) — internă; sinteză publică.

Anexa B — Acronime cheie

Acronim	Semnificație
AC / TSP	Autoritate de Certificare / Trust Service Provider
ADR	Autoritatea pentru Digitalizarea României
BCP / DRP	Business Continuity Plan / Disaster Recovery Plan
CA	Certification Authority
CP / CPS	Certificate Policy / Certification Practice Statement
CRL	Certificate Revocation List
DNSC	Directoratul Național de Securitate Cibernetică
eIDAS	Regulamentul (UE) 910/2014 privind identificarea electronică
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module
LCP	Lightweight Certificate Policy (ETSI EN 319 411-1)

Acronim	Semnificație
LoIP	Level of Identity Proofing (ETSI TS 119 461)
NCP / NCP+	Normalized Certificate Policy / NCP Plus
OCSP	Online Certificate Status Protocol (RFC 6960)
OID	Object Identifier
PA	Policy Authority
PKI	Public Key Infrastructure
RA	Registration Authority
RFC	Request for Comments (IETF)
SAD	Signature Activation Data
SAM	Signature Activation Module
SCAL2	Sole Control Assurance Level 2 (EN 419 241-1)
SSCD	Secure Signature Creation Device
TSA / QTSA	Time Stamping Authority / Qualified TSA

Aprobare și semnătură

Prezentul document „QSIGN-CP-CPS-AC-v1.0 — Certificate Policy / Certification Practice Statement pentru serviciile avansate (necalificate) emise de QSIGN S.R.L.” este aprobat și asumat de Comitetul de Politică (Policy Authority) al QSIGN S.R.L. în calitate de prestator de servicii de încredere necalificate.

Documentul intră în vigoare la data publicării în repository-ul oficial https://www.qsign.ro/repository și produce efecte de la momentul înregistrării QSIGN în Registrul prestatorilor de servicii de încredere necalificate ținut de Autoritatea pentru Digitalizarea României, conform art. 5–10 din Anexa 2 la Ordinul MEDAT nr. 102/29.01.2026.

QSIGN S.R.L.

CIF: 34633481 / J2024010825402

Sediu: Str. Drumea Rădulescu, nr. 26, sector 4, București

Trandafirescu Alexandru Florin

Administrator

_____

(semnătură electronică avansată sau calificată)

Data: 06.05.2026