PKI DISCLOSURE STATEMENT (PDS)

QSIGN S.R.L. — Servicii de încredere AVANSATE (necalificate)

NCP+ · NCP · LCP — semnătură și sigiliu electronic avansat

Informații document

Denumire document	PKI Disclosure Statement — Servicii de încredere AVANSATE (necalificate)
Cod intern	QSIGN-PDS-AC-v1.0
OID document	1.3.6.1.4.1.59019.1.2.2.0
Versiune	1.0
Data publicării	06.05.2026
Data intrării în vigoare	06.05.2026
Stare	Aprobat (versiune pentru notificare ADR — Anexa 2, Ordin MEDAT 102/2026)
Aprobat de	Policy Management Authority (PMA) — QSIGN S.R.L.
Limba originală	Română (versiunea autentică)
Cadru de referință	ETSI EN 319 411-1 v1.4.1+ — Anexa A (PKI Disclosure Statement) Reg. (UE) nr. 910/2014 (eIDAS), modificat prin Reg. (UE) 2024/1183 — art. 26, 36 Legea nr. 214/2024; Ordin MEDAT nr. 102/29.01.2026 (Anexa 2) Decizia ADR nr. 162/20.03.2026
Document-cadru asociat	QSIGN-CP-CPS-AC-v1.0 (CP/CPS — Servicii Avansate, §2.2)
Servicii acoperite	Certificate avansate de semnătură electronică — persoană fizică (NCP+, NCP, LCP) Certificate avansate de sigiliu electronic — persoană juridică (NCP+, NCP, LCP) Serviciu de remote signing avansat (SCAL2-aligned)

Preambul

Prezentul PKI Disclosure Statement (denumit în continuare „PDS”) este un rezumat public al informațiilor critice pe care orice solicitant, titular (Subscriber) și parte utilizatoare (Relying Party) trebuie să le cunoască înainte de a solicita, a accepta sau de a se baza pe un certificat avansat — necalificat — emis de QSIGN S.R.L. PDS-ul este redactat în conformitate cu cerințele clauzei 6.3.4 și ale Anexei A din ETSI EN 319 411-1 și completează — fără a înlocui

— Politica de Certificare și Codul de Practici și Proceduri pentru servicii avansate (QSIGN-CP-CPS-AC-v1.0), Subscriber Agreement, Relying Party Agreement și Termenii și Condițiile (T&C) publicate de QSIGN.

AVERTISMENT IMPORTANT: certificatele descrise în prezentul PDS sunt certificate AVANSATE (necalificate) în sensul art. 26, respectiv 36 din Reg. (UE) 910/2014. Ele NU beneficiază de prezumția automată de echivalență cu semnătura olografă (art. 25 alin. 2 eIDAS) și nici de prezumția de integritate și de corectitudine a originii datelor specifică sigiliilor calificate (art. 35 alin. 2 eIDAS). Pentru aceste efecte juridice este necesar un certificat calificat — vezi QSIGN-PDS-QC-v1.0.

1. Informațiile de contact ale prestatorului (TSP)

QSIGN S.R.L. este prestator de servicii de încredere necalificate, înscris în Registrul prestatorilor de servicii de încredere necalificate operat de ADR în temeiul art. 5 alin. (1) Anexa 2 la Ordinul MEDAT nr. 102/2026.

Denumire prestator	QSIGN S.R.L.
CUI / ONRC	34633481 / J2024010825402
Sediu social	Str. Drumea Rădulescu nr. 26, sector 4, București, România
Reprezentant legal	Trandafirescu Alexandru-Florin — Administrator
Web (repository)	https://www.qsign.ro/repository
E-mail general / SPoC	alex@qsign.ro
E-mail incidente securitate	incident@qsign.ro
E-mail revocări certificate	revoke@qsign.ro
Telefon (24/7 — incidente, revocări)	+40 724 167 333
Autoritate de supraveghere	ADR — Autoritatea pentru Digitalizarea României Strada Italiană nr. 22, sector 2, București https://www.adr.gov.ro

Cererile de revocare se transmit 24/7 prin telefon la +40 724 167 333, prin e-mail la revoke@qsign.ro sau prin portalul de auto-revocare la https://www.qsign.ro/portal/revocare. Termenul maxim de procesare a unei cereri legitime de revocare este de 24 de ore.

2. Tipuri de certificate, proceduri de validare și utilizare

2.1 Tipuri de certificate emise sub prezentul PDS

Tip certificat / serviciu	OID politică ETSI	OID politică QSIGN
Semnătură avansată — persoană fizică — NCP+ (cheie pe SSCD/HSM utilizator)	0.4.0.2042.1.2	1.3.6.1.4.1.59019.2.1.1.1
Semnătură avansată — persoană fizică — NCP	0.4.0.2042.1.1	1.3.6.1.4.1.59019.2.1.1.2
Semnătură avansată — persoană fizică — LCP	0.4.0.2042.1.3	1.3.6.1.4.1.59019.2.1.1.3
Sigiliu avansat — persoană juridică — NCP+	0.4.0.2042.1.2	1.3.6.1.4.1.59019.2.1.2.1
Sigiliu avansat — persoană juridică — NCP	0.4.0.2042.1.1	1.3.6.1.4.1.59019.2.1.2.2
Sigiliu avansat — persoană juridică — LCP	0.4.0.2042.1.3	1.3.6.1.4.1.59019.2.1.2.3
Remote AdES signing avansat (SCAL2-aligned, EN 419 241-1)	—	1.3.6.1.4.1.59019.2.5.1

2.2 Proceduri de validare a identității

Identificarea solicitanților se realizează la nivelul minim Baseline LoIP conform ETSI TS 119 461. Politicile NCP+ și NCP impun verificări mai riguroase decât LCP, după cum urmează:

- LCP — Lightweight Certificate Policy: identificare prin probe documentare la distanță (copie act identitate + verificare e-mail/telefon), suficientă pentru scenarii cu risc scăzut.
- NCP — Normalized Certificate Policy: identificare prin video-identificare asistată sau prezență fizică; verificare ONRC pentru persoane juridice.
- NCP+ — Normalized Certificate Policy with Secure User Device: identitate validată ca la NCP, plus generarea/protecția cheii pe un dispozitiv securizat al utilizatorului (SSCD/HSM utilizator), cu PoP demonstrat.

Detaliile complete ale procedurilor sunt în CP/CPS-AC §3.2 și în Politica internă de identity proofing aliniată ETSI TS 119 461 Baseline.

2.3 Utilizări permise

- Semnătură avansată (NCP+/NCP/LCP): contracte între profesioniști care nu impun formă autentică sau scrisă ad validitatem; corespondență comercială formală; aprobări

interne de organizație (workflow electronic); declarații care nu se depun la autorități publice; circuite de aprobare în industrii reglementate, atunci când reglementările proprii nu impun semnătură calificată.

- Sigiliu avansat (NCP+/NCP/LCP): sigilarea documentelor emise de organizații (rapoarte, certificate emise de companii, atestate); securizarea API-urilor; sigilarea pachetelor de date EDI/B2B; sigilarea automată din sisteme ERP.
- Remote AdES signing avansat (SCAL2): semnarea la distanță, cu cheia păstrată în HSM-ul QSIGN și activată exclusiv pe baza Signature Activation Data (SAD) a titularului. Sistemul NU este certificat ca QSCD, deci semnătura produsă este avansată, nu calificată.

2.4 Utilizări interzise

- Utilizarea în scopuri ilegale, frauduloase sau care încalcă drepturile terților.
- Utilizarea ca probă de echivalență cu semnătura olografă în cazurile în care legea sau părțile interesate impun semnătură calificată sau formă autentică.
- Utilizarea pentru autentificarea site-urilor web (TLS/SSL).
- Utilizarea unui certificat de sigiliu pentru semnarea actelor juridice care impun semnătura unei persoane fizice.
- Utilizarea după expirare, suspendare sau revocare.
- Utilizarea ca CA subordonată sau ca TSA fără cross-certification expres aprobată de PMA.
- Extragerea cheii private dintr-un dispozitiv securizat (cazul NCP+) în software.

3. Limite de utilizare (reliance limits)

Pentru certificatele avansate emise de QSIGN, nu se aplică o limită monetară per tranzacție inclusă în câmpul QCStatement, însă răspunderea agregată a QSIGN față de orice titular sau parte utilizatoare este limitată la valoarea asigurării de răspundere civilă profesională (minim 100.000 EUR pe eveniment, conform art. 5 alin. (2) lit. b) Anexa 2 la Ordinul MEDAT 102/2026). Pentru daune cumulative anuale, plafonul este suma asigurată anuală.

Validitate uzuală a certificatelor avansate emise de QSIGN: până la 36 de luni pentru certificate NCP+/NCP de persoană fizică/juridică; până la 24 de luni pentru certificate LCP; durata maximă este aleasă astfel încât să permită rotația cheilor înainte de epuizarea robusteții criptografice.

4. Obligațiile titularilor (Subscribers)

Prin acceptarea Subscriber Agreement și a prezentului PDS, titularul se obligă:

- Să furnizeze QSIGN/RA/LRA informații corecte, complete și actuale la cerere și la fiecare reînnoire/re-key.
- Să accepte certificatul după verificarea conținutului, în maxim 30 de zile de la emitere; lipsa contestării echivalează cu acceptarea.

- Să păstreze cheia privată sub control exclusiv (dispozitivul deținut sau credențialele SAD pentru remote signing) și să protejeze PIN-ul/parola de protecție.
- Să utilizeze certificatul exclusiv pentru scopurile permise (§2.3), în limitele keyUsage/extendedKeyUsage și ale OID-ului politicii.
- Să recunoască expres că certificatul este AVANSAT (necalificat) și că nu produce efectele juridice rezervate certificatelor calificate.
- Să solicite imediat — și în orice caz în maxim 24 de ore de la luarea la cunoștință — revocarea în caz de pierdere a controlului asupra cheii private, suspiciune de compromitere, schimbare a datelor incluse în certificat sau încetare a calității juridice.
- Să înceteze utilizarea certificatului la data expirării sau revocării.
- Să notifice QSIGN orice incident de securitate prin e-mail la incident@qsign.ro sau telefonic la +40 724 167 333.
- Să achite tarifele în condițiile Subscriber Agreement.

5. Obligațiile de verificare ale părților utilizatoare (Relying Parties)

Înainte de a se baza pe un certificat avansat sau pe o semnătură/sigiliu produs cu acesta, partea utilizatoare (Relying Party) trebuie să întreprindă toate verificările rezonabile, după cum urmează:

- Verificarea valabilității certificatului prin OCSP sau CRL la momentul utilizării — endpoint-uri publicate în certificate (extensiile AIA și CDP) și în repository.
- Construirea și validarea lanțului de încredere până la ancora de încredere publicată de QSIGN; certificatele avansate NU sunt incluse în Trusted List națională și nici în LOTL UE — partea utilizatoare TREBUIE să fie informată asupra acestui fapt.
- Verificarea adecvării politicii certificatului (OID-ul din extensia certificatePolicies) la cazul de utilizare; în special, verificarea că politica este NCP+, NCP sau LCP, NU QCP-* (calificat).
- Verificarea utilizării permise prin keyUsage / extendedKeyUsage și a oricăror QCStatement-uri care indică limitări specifice non-calificate.
- Înțelegerea diferenței dintre certificatele avansate și calificate; valoarea probatorie a semnăturilor avansate este apreciată concret de instanță (art. 26 eIDAS) — nu beneficiază de prezumția echivalenței cu semnătura olografă.
- Acceptarea Relying Party Agreement publicat de QSIGN — utilizarea fără respingere echivalează cu acceptarea.

Frecvența de actualizare a informațiilor de revocare: CRL emis cel puțin la fiecare 24 ore pentru NCP+/NCP și la fiecare 7 zile pentru LCP; OCSP răspuns dinamic. Suspendarea (certificateHold) este permisă pentru certificate avansate.

6. Garanție limitată, exonerări și limitarea răspunderii

6.1 Garanțiile QSIGN

- Conformitatea serviciilor cu Reg. (UE) 910/2014 (art. 26, 36), Legea 214/2024, Anexa 2 la Ordinul MEDAT 102/2026 și ETSI EN 319 401 / 411-1.
- Aplicarea Baseline LoIP (sau superior, în funcție de politica selectată) la identificarea persoanelor.
- Disponibilitatea repository-ului public ≥ 99,9%; respectarea termenelor de revocare/suspendare prevăzute la §4.9 din CP/CPS-AC.
- Menținerea unei asigurări de răspundere civilă profesională de minim 100.000 EUR pe eveniment.

6.2 Exonerări de garanție

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

6.3 Limitarea răspunderii

Răspunderea QSIGN pentru servicii avansate este reglementată în principal de art. 13 alin. (2) Reg. (UE) 910/2014, cu următoarele particularități față de regimul calificat:

- Pentru daune directe imputabile QSIGN, plafonul global de despăgubire pe eveniment este suma asigurată prin polița de răspundere civilă (minim 100.000 EUR).
- QSIGN nu răspunde pentru daune indirecte, pierderi de profit, pierderi de oportunitate, întreruperi de afaceri sau pierderi de date neaferente serviciului propriu.
- QSIGN nu răspunde pentru utilizarea unui certificat în condiții ce încalcă acest PDS ori CP/CPS sau Subscriber/Relying Party Agreement.
- 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 la nivelul Baseline.
- Pentru servicii avansate, NU se aplică prezumția de eroare imputabilă TSP din art. 13 alin. (1) eIDAS în aceeași formă ca pentru serviciile calificate; sarcina probei daunei și a culpabilității revine părții reclamante, conform regulilor generale ale dreptului civil român.
- Aceste limitări nu se aplică în cazul faptelor comise cu intenție sau culpă gravă.

7. Acorduri aplicabile, CPS și politica de certificare

Cadrul contractual și politic complet aplicabil serviciilor avansate ale QSIGN cuprinde documentele enumerate mai jos, toate disponibile în repository-ul public:

Document	Cod intern	Adresă publicare
Politica de Certificare și Codul de Practici și Proceduri — Servicii Avansate	QSIGN-CP-CPS-AC-v1.0	https://www.qsign.ro/repository/cpcps-advanced
Subscriber Agreement (servicii avansate)	QSIGN-SA-AC-v1.0	https://www.qsign.ro/repository/subscriber-agreement-ac
Relying Party Agreement (servicii avansate)	QSIGN-RPA-AC-v1.0	https://www.qsign.ro/repository/relying-party-ac
Termeni și Condiții	QSIGN-TC-AC-v1.0	https://www.qsign.ro/repository/terms-ac
Politica de Protecție a Datelor	QSIGN-PP-AC-v1.0	https://www.qsign.ro/repository/privacy

8. Politica de protecție a datelor

Prelucrarea datelor cu caracter personal se efectuează în conformitate cu Reg. (UE) 2016/679 (GDPR), Legea 190/2018 și Politica de Protecție a Datelor a QSIGN. QSIGN este Operator de date pentru toate prelucrările legate de emiterea, gestionarea și revocarea certificatelor avansate.

- Temeiuri juridice: executarea contractului; obligația legală de păstrare a evidențelor probatorii; interesul legitim al QSIGN și al utilizatorilor (securitate, prevenirea fraudei).
- Categorii de date: nume complet, CNP/identificator național, seria/nr. act identitate, e-mail, telefon, adresă, fotografia/scanarea actului de identitate, înregistrarea video a sesiunii de identificare, date biometrice (temporar).
- Perioada de păstrare: cf. CP/CPS-AC §5.5 și obligațiilor legale; ulterior, ștergere sau anonimizare controlată.
- Drepturile persoanelor vizate (acces, rectificare, ștergere, restricție, opoziție, portabilitate, plângere ANSPDCP) se exercită prin e-mail la dpo@qsign.ro.
- Transferuri internaționale: nu se efectuează în afara SEE; eventualele transferuri se realizează numai pe baza unui mecanism adecvat (decizie de adecvare, SCC).

9. Politica de rambursare

Tarifele aferente serviciilor avansate sunt publicate pe www.qsign.ro și fac parte integrantă din Subscriber Agreement. Politica de rambursare aplicabilă este următoarea:

- În cazul unei erori imputabile QSIGN (date incorecte introduse din procesul intern al QSIGN, neîndeplinirea SLA-ului, certificat respins din motive tehnice de emitere), tariful este rambursat integral.
- Re-emiterea unui certificat ca urmare a unei erori imputabile QSIGN este gratuită.

- Pentru certificatele revocate la solicitarea titularului din motive imputabile acestuia nu există rambursare a tarifului; revocarea propriu-zisă este gratuită pentru titular.
- Accesul la certificate publicate în repository, la CRL și la OCSP este gratuit pentru toți utilizatorii și părțile încrezătoare.
- Servicii adiționale (consultanță, integrare API, on-boarding entități cu volum mare) sunt rambursate conform clauzelor contractelor individuale.

10. Legea aplicabilă, plângeri și soluționarea disputelor

10.1 Legea aplicabilă

Prezentul PDS și serviciile descrise sunt guvernate de legea română și de dreptul Uniunii Europene direct aplicabil — în special Reg. (UE) 910/2014, Reg. (UE) 2016/679 (GDPR), Legea 214/2024, Legea 190/2018, Ordinul MEDAT 102/2026 (Anexa 2), Decizia ADR 162/2026.

10.2 Plângeri

Plângerile titularilor și ale părților utilizatoare se adresează în primă instanță QSIGN, prin oricare dintre canalele de la §1, urmând a fi soluționate în maxim 30 de zile calendaristice. Plângerile referitoare la prelucrarea datelor cu caracter personal se pot adresa direct ANSPDCP. Plângerile privind respectarea obligațiilor de prestator necalificat se pot adresa ADR.

10.3 Soluționarea disputelor

Disputele se soluționează amiabil; în caz de eșec, sunt supuse instanțelor competente din România, cu excepția cazurilor în care părțile convin asupra mediere/arbitraj. Litigiile cu autoritățile (ADR, ANSPDCP, DNSC) se soluționează conform procedurilor administrative aplicabile, cu posibilitatea contestării în contencios administrativ.

11. Statut, audit și mărci

- QSIGN va fi înscris în Registrul prestatorilor de servicii de încredere necalificate operat de ADR, prin Decizia Președintelui ADR conform art. 7 alin. (2) Anexa 2 la Ordinul MEDAT 102/2026; certificatele avansate NU sunt incluse în Trusted List națională și nici în LOTL UE.
- Mărcile, logo-urile și siglele QSIGN sunt protejate; utilizarea Marcii de încredere UE (UE Trust Mark) este REZERVATĂ exclusiv serviciilor calificate și NU se aplică serviciilor descrise în prezentul PDS.
- Auditul periodic al QSIGN pentru servicii avansate este efectuat de un auditor înscris în Lista auditorilor de securitate cibernetică (LASC) — DNSC, deținător al atestatului de tip General, cu respectarea cerințelor ETSI EN 319 403-1 (art. 5 alin. (2) lit. a) Anexa 2 la Ordinul MEDAT 102/2026). Sumar al rezultatelor este publicat în repository și în raportul anual de transparență.

Aprobare

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

Versiune	1.0
Data aprobării	06.05.2026
Data intrării în vigoare	06.05.2026
Data publicării în repository	06.05.2026
Aprobat de	Trandafirescu Alexandru-Florin — Administrator QSIGN S.R.L.
Semnătură electronică calificată	_____