

# PKI DISCLOSURE STATEMENT (PDS)

## QSIGN S.R.L. — Servicii de încredere CALIFICATE

QCP-n / QCP-n-qscd · QCP-I / QCP-I-qscd · QTSA

### Informații document

Denumire document	PKI Disclosure Statement — Servicii de încredere CALIFICATE
Cod intern	QSIGN-PDS-QC-v1.0
OID document	1.3.6.1.4.1.59019.1.1.2.0
Versiune	1.0
Data publicării	06.05.2026
Data intrării în vigoare	06.05.2026
Stare	Aprobat (versiune pentru depunere ADR — Anexa 1, 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) ETSI EN 319 411-2 v2.5.1+ — cerințe certificate calificate UE Reg. (UE) nr. 910/2014 (eIDAS), modificat prin Reg. (UE) 2024/1183 Legea nr. 214/2024; Ordin MEDAT nr. 102/29.01.2026 (Anexa 1) Decizia ADR nr. 162/20.03.2026 (Anexa 2)
Document-cadru asociat	QSIGN-CP-CPS-QC-v1.0 (CP/CPS — Servicii Calificate, §2.2)
Servicii acoperite	Certificate calificate de semnătură electronică — persoană fizică (QCP-n, QCP-n-qscd) Certificate calificate de sigiliu electronic — persoană juridică (QCP-I, QCP-I-qscd) Marcă temporală electronică calificată — QTSA

### 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 calificat ori pe o marcă temporală calificată emisă 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 calificate (QSIGN-CP-CPS-QC-v1.0), Subscriber Agreement, Relying Party Agreement, Termenii și Condițiile (T&C) și Politica de Protecție a Datelor publicate de QSIGN.

În caz de neconcordanță între prezentul PDS și documentele referite, prevalează ordinea: (i) Reg. (UE) 910/2014 și actele de punere în aplicare; (ii) Legea 214/2024 și actele subsecvente; (iii) CP/CPS aplicabil; (iv) Subscriber/Relying Party Agreement; (v) prezentul PDS.

## 1. Informațiile de contact ale prestatorului (TSP)

QSIGN S.R.L. este prestatorul calificat de servicii de încredere (Qualified Trust Service Provider — QTSP) în sensul art. 3 pct. 20 din Reg. (UE) 910/2014. Datele de contact și punctul unic de contact (SPoC) cu autoritatea de supraveghere ADR sunt:

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)	<a href="https://www.qsign.ro/repository">https://www.qsign.ro/repository</a>
E-mail general / SPoC	<a href="mailto:alex@qsign.ro">alex@qsign.ro</a>
E-mail incidente securitate	<a href="mailto:incident@qsign.ro">incident@qsign.ro</a>
E-mail revocări certificate	<a href="mailto:revoke@qsign.ro">revoke@qsign.ro</a>
Telefon (24/7 — incidente, revocări)	+40 724 167 333
Autoritate de supraveghere	ADR — Autoritatea pentru Digitalizarea României Strada Italiană nr. 22, sector 2, București <a href="https://www.adr.gov.ro">https://www.adr.gov.ro</a>

Cererile de revocare se transmit 24/7 prin telefon la +40 724 167 333, prin e-mail la [revoke@qsign.ro](mailto:revoke@qsign.ro) sau prin portalul de auto-revocare disponibil la <https://www.qsign.ro/portal/revocare>. Termenul maxim de procesare a unei cereri legitime de revocare este de 24 de ore (art. 24 alin. (3) eIDAS, art. 26 din Legea 214/2024).

## 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
QCP-n — semnătură calificată,	0.4.0.194112.1.0	1.3.6.1.4.1.59019.2.2.1

Tip certificat / serviciu	OID politică ETSI	OID politică QSIGN
persoană fizică, cheie pe dispozitiv obișnuit		
QCP-n-qscd — semnătură calificată, persoană fizică, cheie în QSCD	0.4.0.194112.1.2	1.3.6.1.4.1.59019.2.2.2
QCP-I — sigiliu calificat, persoană juridică, cheie pe dispozitiv obișnuit	0.4.0.194112.1.1	1.3.6.1.4.1.59019.2.3.1
QCP-I-qscd — sigiliu calificat, persoană juridică, cheie în QSCD	0.4.0.194112.1.3	1.3.6.1.4.1.59019.2.3.2
Marcă temporală calificată — QTSA	0.4.0.2023.1.1 (BTSP)	1.3.6.1.4.1.59019.3.1

## 2.2 Proceduri de validare a identității

Identificarea solicitanților se realizează la nivelul Substantial sau High al asigurării identității (LoIP) conform ETSI TS 119 461 și art. 24 alin. (1) lit. (d) din Reg. (UE) 910/2014. Metodele permise pentru emiterea certificatelor calificate sunt:

- Prezență fizică la sediu QSIGN, la un LRA contractat sau la notar (LoIP High).
- Identificare la distanță prin video-identificare automată sau asistată de operator, conformă ETSI TS 119 461 și Reg. UE 2025/1567.
- Identificare prin mijloace electronice notificate eIDAS de nivel Substantial/High (eID național, EUDI Wallet conform eIDAS 2.0).
- Identificare prin certificat calificat anterior valid al aceleiași persoane (re-utilizarea probelor de identitate, în condițiile §3.2 CP/CPS).

Pentru persoane juridice (QCP-I/QCP-I-qscd), se verifică, în plus, existența juridică prin extras ONRC actualizat la maxim 30 de zile, statutul fiscal, calitatea reprezentantului legal și mandatul expres pentru solicitarea certificatului de sigiliu.

## 2.3 Utilizări permise

- QCP-n / QCP-n-qscd: crearea de semnături electronice calificate (QES) cu efectul juridic echivalent al semnăturii olografe, conform art. 25 alin. (2) eIDAS și art. 4 alin. (1) Legea 214/2024 — semnarea actelor juridice care necesită formă scrisă, declarații fiscale, contracte cu autoritățile, documente bancare și notariale electronice, dosare instanță electronice.
- QCP-I / QCP-I-qscd: aplicarea de sigilii electronice calificate cu prezumția de integritate și corectitudine a originii datelor (art. 35 alin. (2) eIDAS) — facturi electronice

(e-Factura), rapoarte și certificate emise automat de organizație, securizarea API-urilor, sigilarea pachetelor de arhivare.

- QTSA: marcarea temporală a documentelor și semnăturilor cu probarea existenței datelor la un moment determinat (art. 41–42 eIDAS).

## 2.4 Utilizări interzise

- Utilizarea în scopuri ilegale, frauduloase sau care încalcă drepturile terților.
- Utilizarea pentru autentificarea site-urilor web (TLS/SSL) — necesită un certificat QWAC distinct (art. 45 eIDAS).
- Utilizarea unui certificat de sigiliu (QCP-I/QCP-I-qscd) 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 QSCD în software sau utilizarea cheii în alt dispozitiv decât cel autorizat prin politica certificatului.

## 3. Limite de utilizare (reliance limits)

Pentru certificatele calificate emise de QSIGN, nu se aplică o limită monetară per tranzacție inclusă în câmpul QCStatement; certificatele pot fi utilizate pentru orice valoare tranzacțională permisă de lege și de natura aplicației, cu respectarea utilizărilor interzise enumerate la §2.4. Cu toate acestea, răspunderea agregată a QSIGN față de orice titular sau parte utilizatoare este limitată conform §6 din prezentul PDS și art. 13 alin. (2) eIDAS — la valoarea asigurării de răspundere civilă profesională (500.000 EUR pe eveniment per serviciu calificat, conform art. 5 alin. (2) lit. b) Anexa 1 la Ordinul MEDAT 102/2026).

Validitate uzuală a certificatelor calificate emise de QSIGN: până la 36 de luni pentru QCP-n/QCP-n-qscd și până la 60 de luni pentru QCP-I/QCP-I-qscd, fără a depăși orizontul de valabilitate criptografică a algoritmilor folosiți. Mărcile temporale calificate sunt valabile pentru verificare pe întreaga durată a documentului probator, în condițiile validării/preservation calificate.

## 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 (QSCD-ul, dispozitivul deținut sau credențialele SAD pentru remote signing) și să protejeze PIN-ul/parola conform instrucțiunilor primite.

- Să utilizeze certificatul exclusiv pentru scopurile permise (§2.3), în limitele keyUsage/extendedKeyUsage și ale OID-ului politicii.
- 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, încetare a calității juridice (art. 26 alin. (2) Legea 214/2024).
- Să înceteze utilizarea certificatului la data expirării sau revocării.
- Să notifice QSIGN orice incident de securitate care afectează cheia privată sau datele de activare, 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 sau pe o marcă temporală emisă de QSIGN, partea utilizatoare (Relying Party) trebuie să întreprindă toate verificările rezonabile, după cum urmează:

- Verificarea valabilității certificatului prin OCSP (recomandat) sau CRL la momentul utilizării — endpoint-uri publicate în certificate (extensiile AIA și CDP) și în repository-ul <https://www.qsign.ro/repository>.
- Construirea și validarea lanțului de încredere până la o ancoră oficială: Lista sigură națională a ADR (EU Trusted List) sau LOTL UE.
- Verificarea adecvării politicii certificatului (OID-ul din extensia certificatePolicies) la cazul de utilizare — în special, verificarea că certificatul este de tip QCP-n/QCP-n-qscd atunci când se așteaptă o semnătură electronică calificată.
- Verificarea utilizării permise prin keyUsage / extendedKeyUsage și a oricăror QCStatement-uri care indică limitări (de ex. limita financiară per tranzacție, dacă există).
- Verificarea integrității și autenticității documentului semnat: hash, semnătura, marca temporală asociată; pentru valoare probatorie pe termen lung — utilizarea unui serviciu calificat de validare/preservation (ETSI EN 319 102, ETSI TS 119 511).
- Acceptarea Relying Party Agreement publicat de QSIGN în repository — utilizarea certificatului fără respingere echivalează cu acceptare.

Frecvența de actualizare a informațiilor de revocare: CRL emis la fiecare 24 ore (nextUpdate la 7 zile), OCSP răspuns dinamic cu prosepțime ≤ 1 oră.

## 6. Garanție limitată, exonerări și limitarea răspunderii

### 6.1 Garanțiile QSIGN

- Conformitatea serviciilor cu Reg. (UE) 910/2014 (modificat prin Reg. UE 2024/1183), Legea 214/2024, Ordinul MEDAT 102/2026 și ETSI EN 319 401 / 411-1 / 411-2 / 412 / 421 / 422 / TS 119 461.

- Acuratețea informațiilor incluse în certificatele calificate la momentul emiterii, verificate conform §3.2 din CP/CPS-QC.
- Disponibilitatea infrastructurii la nivelul SLA declarat:  $\geq 99,9\%$  pentru repository-ul public;  $\geq 99,95\%$  pentru OCSP, CRL distribution points, QTSA.
- Procesarea cererilor legitime de revocare în maxim 24 ore.
- Notificarea ADR și a titularilor cu privire la incidentele de securitate semnificative, în termenele art. 19 alin. (2) eIDAS și art. 14 Legea 214/2024 (24 ore).

## 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 / 122).

## 6.3 Limitarea răspunderii

Răspunderea QSIGN este reglementată de art. 13 din Reg. (UE) 910/2014 și de art. 30 din Legea 214/2024. QSIGN răspunde pentru prejudiciul cauzat ca urmare a nerespectării cerințelor regulamentare, în limitele asigurării de răspundere profesională (500.000 EUR pe eveniment per serviciu calificat, cesionată în favoarea ADR conform art. 5 alin. (2) lit. b) Anexa 1 la Ordinul MEDAT 102/2026 și art. 3 alin. (2) lit. b) Anexa 1 la Decizia ADR 162/2026).

- QSIGN nu răspunde pentru daune indirecte, pierderi de profit, pierderi de oportunitate sau întreruperi de afaceri, în măsura permisă de lege.
- QSIGN nu răspunde pentru utilizarea unui certificat în condiții ce încalcă acest PDS ori CP/CPS sau Subscriber/Relying Party Agreement (utilizare în afara keyUsage, ignorarea statusului 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 diligența rezonabilă aplicabilă verificării identității.
- 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 calificate 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 Calificate	QSIGN-CP-CPS-QC-v1.0	<a href="https://www.qsign.ro/repository/cpcps-qualified">https://www.qsign.ro/repository/cpcps-qualified</a>
Politica QTSA (Time-Stamping Policy)	QSIGN-TSA-Policy-v1.0	<a href="https://www.qsign.ro/repository/tsa-policy">https://www.qsign.ro/repository/tsa-policy</a>
Politica de validare calificată	QSIGN-VAL-Policy-v1.0	<a href="https://www.qsign.ro/">https://www.qsign.ro/</a>

Document	Cod intern	Adresă publicare
		repository/validation-policy
Politica de preservation calificată (LTP)	QSIGN-PRES-Policy-v1.0	<a href="https://www.qsign.ro/repository/preservation-policy">https://www.qsign.ro/repository/preservation-policy</a>
Subscriber Agreement	QSIGN-SA-QC-v1.0	<a href="https://www.qsign.ro/repository/subscriber-agreement-qc">https://www.qsign.ro/repository/subscriber-agreement-qc</a>
Relying Party Agreement	QSIGN-RPA-QC-v1.0	<a href="https://www.qsign.ro/repository/relying-party-qc">https://www.qsign.ro/repository/relying-party-qc</a>
Termeni și Condiții	QSIGN-TC-QC-v1.0	<a href="https://www.qsign.ro/repository/terms-qc">https://www.qsign.ro/repository/terms-qc</a>
Politica de Protecție a Datelor	QSIGN-PP-QC-v1.0	<a href="https://www.qsign.ro/repository/privacy">https://www.qsign.ro/repository/privacy</a>

Toate documentele sunt sigilate electronic cu sigiliul calificat al QSIGN și marcate temporal calificat; integritatea lor este verificabilă prin hash-urile publicate în repository. Versiunile anterioare rămân disponibile public timp de minimum 10 ani de la data înlocuirii, în vederea valorii probatorii a documentelor semnate sub politicile anterioare (art. 24 alin. (2) lit. (h) eIDAS).

## 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 publicată de QSIGN. QSIGN este Operator de date pentru toate prelucrările legate de emiterea, gestionarea și revocarea certificatelor calificate.

- Temeiuri juridice: executarea contractului (art. 6 alin. 1 lit. b GDPR); obligații legale (art. 6 alin. 1 lit. c — eIDAS, Legea 214/2024, păstrare 10 ani); interes legitim (art. 6 alin. 1 lit. f — securitate și prevenirea fraudei).
- Categoriile de date prelucrate: nume complet, CNP/identificator național, seria și numărul actului de identitate, adresa de e-mail, telefon, adresa de domiciliu, fotografia/scanarea actului de identitate, înregistrarea sesiunii de video-identificare, datele biometrice extrase temporar pentru verificare.
- Perioada de păstrare: 10 ani după expirarea/revocarea ultimului certificat al titularului (art. 24 alin. (2) lit. (h) eIDAS, art. 25 Legea 214/2024); ulterior, ștergere sau anonimizare controlată.
- Drepturile persoanelor vizate (acces, rectificare, ștergere — în limitele obligațiilor legale de păstrare —, restricție, opoziție, portabilitate, plângere ANSPDCP) se exercită prin e-mail la [dpo@qsign.ro](mailto: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).

Detalii complete: <https://www.qsign.ro/repository/privacy>. Punct de contact dedicat: Responsabilul cu Protecția Datelor (DPO) — [dpo@qsign.ro](mailto:dpo@qsign.ro).

## 9. Politica de rambursare

Tarifele aferente serviciilor calificate sunt publicate pe [www.qsign.ro](http://www.qsign.ro) și fac parte integrantă din Subscriber Agreement. Politica de rambursare aplicabilă serviciilor calificate este următoarea:

- În cazul unei erori imputabile QSIGN (date incorecte introduse din procesul intern, neîndeplinirea SLA-ului, certificat respins de aplicații încrezătoare din motive tehnice de emiterie atribuibile QSIGN), tariful aferent 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 (de ex. pierderea cheii private, schimbarea datelor) nu există rambursare a tarifului; revocarea propriu-zisă este gratuită pentru titular.
- Validarea, marca temporală și consultările OCSP/CRL sunt gratuite pentru toți utilizatorii și părțile încrezătoare.
- Tarifele pentru 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 (modificat prin Reg. UE 2024/1183), Reg. de punere în aplicare aplicabile, Reg. (UE) 2016/679 (GDPR), Legea 214/2024, Legea 190/2018, Ordinul MEDAT 102/2026 (Anexa 1), 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 de la înregistrare. Plângerile referitoare la prelucrarea datelor cu caracter personal se pot adresa direct ANSPDCP (<https://www.dataprotection.ro>). Plângerile privind nerespectarea statutului de QTSP sau a obligațiilor eIDAS se pot adresa ADR (<https://www.adr.gov.ro>).

### 10.3 Soluționarea disputelor

Disputele dintre QSIGN și titulari/relying parties se soluționează amiabil; în caz de eșec, sunt supuse instanțelor competente din România, cu excepția cazurilor în care părțile convin asupra unei modalități alternative de soluționare (mediere, arbitraj). Litigiile cu autoritățile

(ADR, ANSPDCP, DNSC) se soluționează conform procedurilor administrative aplicabile, cu posibilitatea contestării în contencios administrativ.

## 11. Licențe TSP, mărci și audit

- QSIGN va opera, după acordarea statutului calificat de către ADR, pe baza Deciziei Președintelui ADR conform art. 7 alin. (2) Anexa 1 la Ordinul MEDAT 102/2026 și va fi inclus în Lista sigură națională (Trusted List) și — prin LOTL — în Lista listelor sigure UE.
- Mărcile, logo-urile și siglele QSIGN sunt protejate; utilizarea de către terți a Marcii de încredere UE (UE Trust Mark) pentru servicii calificate este permisă numai după obținerea statutului calificat și exclusiv pentru serviciile listate, conform art. 23 eIDAS și Reg. de punere în aplicare (UE) 2015/806.
- QSIGN este auditat la fiecare 24 de luni — și ad-hoc la solicitarea ADR — de către un Conformity Assessment Body (CAB) acreditat conform Reg. (CE) 765/2008 și ETSI EN 319 403-1. Raportul de evaluare a conformității este transmis ADR în 5 zile lucrătoare de la primire (Anexa 4, Decizia 162/2026); un sumar (fără detalii confidențiale de securitate) este publicat în repository și în raportul anual de transparență.
- Lista standardelor declarate îndeplinite (ETSI EN 319 401, 411-1, 411-2, 412/1–5, 421, 422, TS 119 461, TS 119 511, EN 419 221-5, EN 419 241-2) este publicată separat (QSIGN-Lista-Standarde-v1.0).

## 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	_____