


# PKI Disclosure Statement (PDS)

# CertDigital

| **ISSUED BY:** | | | |
|---|---|---|---|
| **DEPARTMENT** | **NAME** | **SIGNATURE** | **DATE** |
| POLICY AND PROCEDURE MANAGEMENT | IT Security Officer | | _____ |

| **APPROVED BY:** | | | |
|---|---|---|---|
| **DEPARTMENT** | **NAME** | **SIGNATURE** | **DATE** |
| POLICY AND PROCEDURE MANAGEMENT | General Director | | _____ |

| **REVISION HISTORY:** | | | |
|---|---|---|---|
| **VERSION** | **AUTHOR** | **DESCRIPTION OF CHANGES** | **DATE:** |
| 1.0–1.6 | — | PKI Disclosure Statement for the G2, G3 and G4 generations (30.04.2017 – 01.11.2025; version 1.6: QPS service) | 01/11/2025 |
| 2.0 | IT Security Officer | Rewritten according to ETSI EN 319 411-1, Annex A: the G4 and G5 generations (subject certificates and service certificates of CERTDIGITAL QCA G5), the fixed addresses referred to by the QcPDS statement (en, ro), Law no. 214/2024; G2 expired, G3 withdrawn; replaces version 1.6 | 23/10/2026 |
| | | | |

# Contents

1. The document and contact information....4
1.1. Nature of the document....4
1.2. The provider and contact details....4
1.3. Revocation requests....5
2. Certificate types, identity verification and usage....6
2.1. Certification hierarchies....6
2.2. Subject certificates....6
2.3. Identity verification....7
2.4. Certificates for keys managed in a remote QSCD....7
2.5. CERTDIGITAL service certificates....8
2.6. Use, renewal and revocation....8
3. Reliance limits....10
4. Obligations of subjects and subscribers....11
5. Obligations of relying parties....12
6. Limited warranty and limitation of liability....13
7. Applicable documents....14
8. Personal data protection....15
9. Fees and refund policy....16
10. Applicable law, complaints and dispute resolution....17
11. Qualified status, conformity assessment and audit....18

# 1. The document and contact information

## 1.1. Nature of the document

This document is the PKI Disclosure Statement (PDS) of CENTRUL DE CALCUL S.A. (CertDigital brand, hereinafter "CERTDIGITAL"), drawn up according to the model in ETSI EN 319 411-1, Annex A. It summarises, for subjects, subscribers and relying parties, the main conditions under which CERTDIGITAL issues and manages the qualified certificates for electronic signatures and for electronic seals of the G4 and G5 generations, as well as the service certificates of CERTDIGITAL.

The document is a simplified information instrument. It does not replace the CertDigital Certification Services Policy, the certification practice statements (DPC CERTDIGITAL G4 and DPC CERTDIGITAL G5) or the Terms and Conditions for qualified certificates (TC-CERT), which contain all the information below in full and form part of the contract with the subject (chapter 7).

The QcPDS statement (ETSI EN 319 412-5) in the certificates issued by CERTDIGITAL QCA G5 refers to this document, published at fixed addresses:

– in English: https://www.certdigital.ro/repository/pds/certdigital_pds_en.pdf;

– in Romanian: https://www.certdigital.ro/repository/pds/certdigital_pds_ro.pdf.

In the certificates of the G4 generation, the QcPDS statement refers to the repository page, https://www.certdigital.ro/repository, from which this document is accessible. The English version has the same content as the Romanian version (ETSI EN 319 412-5, table 2); in the event of any discrepancy, the Romanian version prevails.

Version 2.0 replaces the PKI Disclosure Statement, version 1.6, which is kept in the repository archive (https://www.certdigital.ro/repository/arhiva/).

## 1.2. The provider and contact details

| Item | Information |
|---|---|
| Qualified trust service provider | CENTRUL DE CALCUL S.A. (CertDigital brand), Str. Tudor Vladimirescu nr. 17, Târgu Jiu, Gorj County, postal code 210132, Romania; Trade Register number J1991000103187; EUID ROONRC.J1991000103187; tax identification number RO2163993 |
| Contact | tel. +40 253 214 767; e-mail office@certdigital.ro; https://www.certdigital.ro/; opening hours: Monday–Friday, 09:00–17:00 |
| Technical support / sales | suport@certdigital.ro / sales@certdigital.ro |
| Data protection officer (DPO) | dpo@centruldecalcul.ro |
| Document repository | https://www.certdigital.ro/repository/ |
| Certificate register | https://ca.certdigital.ro/registry |
| Certificates of the authorities | G4: the addresses in DPC CERTDIGITAL G4, section 2.1; G5: http://certs.certdigital.ro/certdigital_root_g5.crt · http://certs.certdigital.ro/certdigital_qualified_g5.crt |

| Item | Information |
|---|---|
| Certificate status information | G4: OCSP http://ocsp.g4.certdigital.ro · CRL http://crl.certdigital.ro/certdigital_qualified_g4.crl; G5: OCSP http://ocsp.g5.certdigital.ro · CRL http://crl.certdigital.ro/certdigital_qualified_g5.crl |
| Supervisory body | Romanian Digitalization Authority (Autoritatea pentru Digitalizarea României, ADR), www.adr.gov.ro |

## 1.3. Revocation requests

The revocation of a certificate can be requested 24 hours a day, 7 days a week, through the customer portal https://ca.certdigital.ro/ra-web/apps/ota/, after authentication. The request can also be sent by e-mail bearing a qualified electronic signature, to office@certdigital.ro, or in writing, at the registered office, during working hours.

Revocation can be requested by the subject, by the subscriber who obtained the certificate, by the legal representative of the legal person that is the subject, by a court or by ADR; CERTDIGITAL may also revoke a certificate on its own initiative. The request is processed within 24 hours at most, and revocation is free of charge and final (section 2.6).

# 2. Certificate types, identity verification and usage

## 2.1. Certification hierarchies

| Generation | Root authority | Authority issuing the subject certificates and the service certificates |
|---|---|---|
| G4 | CERTDIGITAL ROOT CA G4 | CERTDIGITAL QUALIFIED CA G4 |
| G5 | CERTDIGITAL ROOT CA G5 (RSA 4096, valid for 25 years) | CERTDIGITAL QCA G5 (RSA 4096, valid for 15 years) |

The issuing authority is indicated in each certificate. The hierarchies, the certificates of the authorities and of the services and the supported policies are described in the document CertDigital PKI hierarchy (IER-PKI v7.0).

The G3 generation (CertDigital ROOT CA G3 and its subordinate authorities) no longer issues certificates. The G3 certificates issued remain valid until they expire, on 02.05.2027 at the latest, under the conditions of the G3 generation documents, kept in the repository archive. The certificates of the G2 generation have expired.

## 2.2. Subject certificates

| Certificate | ETSI policy (EN 319 411-2) | CERTDIGITAL identifier | Legal effect |
|---|---|---|---|
| Qualified certificate for electronic signatures (natural person, including a natural person associated with a legal person) | QCP-n-qscd (0.4.0.1941 12.1.2) | 1.3.6.1.4.1.47898.4.1.{1,2}.{1,4,6}.1 (G4); 1.3.6.1.4.1.47898.5.1.{1,2}.{1,4,6}.1 (G5) | A qualified electronic signature has the equivalent legal effect of a handwritten signature (Article 25(2) of the eIDAS Regulation). |
| Qualified certificate for electronic seals (legal person) | QCP-l-qscd (0.4.0.1941 12.1.3) | 1.3.6.1.4.1.47898.4.1.{1,2}.{1,4,6}.2 (G4); 1.3.6.1.4.1.47898.5.1.{1,2}.{1,4,6}.2 (G5) | A qualified electronic seal enjoys the presumption of integrity of the data and of correctness of the origin of the data to which it is linked (Article 35(2) of the eIDAS Regulation). |

The CERTDIGITAL identifier indicates:

– the device (1 = the subject's token);

– the key generation (1 = by the subject, with the CertDigital CSR application; 2 = by CERTDIGITAL);

– the identity verification method (1 = physical presence; 4 = CERTDIGITAL KYC; 6 = qualified CERTDIGITAL certificate, on renewal);

– the type of subject (1 = natural person; 2 = legal person).

The certificates are issued to the public (natural persons and legal persons). They are valid for at most 3 years and contain the QcCompliance, QcSSCD, QcType and QcPDS statements (ETSI EN

319 412-5). The subjects' keys are 2048-bit RSA keys for certificates issued until 28.02.2027 and ECDSA keys on the NIST P-256 curve for certificates issued from 01.03.2027.

The key pair is generated in the subject's cryptographic device, the certified Century Longmai mToken CryptoID token (qualified signature and seal creation device; FIPS 140-3, security level 3, CMVP certificate no. 4845): either by CERTDIGITAL, on issuance, or by the subject, with the CertDigital CSR application. The private key never leaves the device. CERTDIGITAL does not keep, archive or recover the subjects' private keys.

## 2.3. Identity verification

Before issuing a qualified certificate, CERTDIGITAL verifies the identity of the subject and, where applicable, the attributes of the legal person, by one of the following methods:

a) **by physical presence**, before a CERTDIGITAL registration operator, with the original identity card, passport or residence permit (Article 24(1a)(d) of the eIDAS Regulation; Article 16(3)(a) of Law no. 214/2024);

b) **remotely, with the CERTDIGITAL KYC solution**: a video recording made by the subject, with automated verification of the identity document and of the person, followed by the review of the recording by a CERTDIGITAL operator within 24 hours at most. The solution is entered by ADR in the list of third parties performing remote identity verification by video means. The biometric comparison of the facial image is performed only with the explicit consent of the subject;

c) **on the basis of a valid qualified CERTDIGITAL certificate**, issued after identity verification by one of the methods in points a) or b), for renewal only (Article 24(1a)(b) of the eIDAS Regulation).

For Romanian citizens, the validity of the identity document is checked through the National Interoperability Platform. For seal certificates and for subjects associated with a legal person, the existence of the legal person and the capacity of the representative are also verified. From 19.08.2027, identity verification also complies with Commission Implementing Regulation (EU) 2025/1566 (ETSI TS 119 461 V2.1.1).

## 2.4. Certificates for keys managed in a remote QSCD

The certificates associated with keys generated and managed by CERTDIGITAL in a remote qualified device have the identifiers 1.3.6.1.4.1.47898.4.2.2.{1,4,6}.{1,2} in the G4 generation and 1.3.6.1.4.1.47898.5.2.2.{1,4,6}.{1,2} in the G5 generation, the identifier 1.3.6.1.4.1.47898.11.1.1 and the EUSPv2 policy (0.4.0.19431.1.1.4). They are additionally subject to the Terms and Conditions of the remote QSCD management service (TC-rQSCD) and to the Policy and practice statement of the service (PDP-rQSCD v2.0).

## 2.5. CERTDIGITAL service certificates

For the trust services of CERTDIGITAL, CERTDIGITAL QCA G5 issues qualified certificates for electronic seals whose subject is CENTRUL DE CALCUL S.A. The keys of these certificates are generated in a key ceremony and kept in the CERTDIGITAL cryptographic module. Each certificate is used only for the service indicated:

| Certificate | Use | Policies |
|---|---|---|
| CERTDIGITAL TSA G5 | signing qualified time stamps (extKeyUsage timeStamping) | QCP-l-qscd (0.4.0.194112.1.3) and 1.3.6.1.4.1.47898.5.2.2.1.2 |
| CERTDIGITAL QPS SERVICE G5 | qualified preservation of qualified electronic signatures and seals | QCP-l-qscd, 1.3.6.1.4.1.47898.5.2.2.1.2 and 1.3.6.1.4.1.47898.10.1 |
| CERTDIGITAL QESVAL SERVICE G5 | qualified validation of qualified electronic signatures and seals | QCP-l-qscd, 1.3.6.1.4.1.47898.5.2.2.1.2 and 1.3.6.1.4.1.47898.9.1 |
| CERTDIGITAL QEARCH SERVICE G5 | qualified electronic archiving | QCP-l-qscd, 1.3.6.1.4.1.47898.5.2.2.1.2 and 1.3.6.1.4.1.47898.12.1 |
| CERTDIGITAL QLEDGERS SERVICE G5 | qualified electronic ledgers | QCP-l-qscd, 1.3.6.1.4.1.47898.5.2.2.1.2 and 1.3.6.1.4.1.47898.13.1 |
| CERTDIGITAL QERDS SERVICE G5 | qualified electronic registered delivery | QCP-l-qscd, 1.3.6.1.4.1.47898.5.2.2.1.2 and 1.3.6.1.4.1.47898.14.1 |
| CERTDIGITAL QREM SERVICE G5 | qualified registered electronic mail (extKeyUsage emailProtection) | QCP-l-qscd, 1.3.6.1.4.1.47898.5.2.2.1.2 and 1.3.6.1.4.1.47898.14.1 |
| CERTDIGITAL QEAA SERVICE G5 | qualified electronic attestation of attributes (ECDSA P-256 key) | QCP-l-qscd, 1.3.6.1.4.1.47898.5.2.2.1.2 and 1.3.6.1.4.1.47898.15.1 |

These certificates contain the QcCompliance, QcSSCD, QcType eSeal and QcPDS statements, with the same addresses as the subject certificates, and are valid for 5 years; the CERTDIGITAL TSA G5 certificate is valid for 3 years and its key is used for at most 2 years. The CERTDIGITAL OCSP G5 certificate, valid for 3 years, signs only OCSP responses; it is not a qualified certificate and contains no QC statements. The service certificates issued by CERTDIGITAL QUALIFIED CA G4 are described in IER-PKI v7.0; their QcPDS statement refers to the repository page.

## 2.6. Use, renewal and revocation

The qualified certificate for electronic signatures is used to create and validate the qualified electronic signatures of the natural person who is the subject and to authenticate that person; the qualified certificate for electronic seals, to create and validate the qualified electronic seals of the legal person that is the subject and to authenticate that legal person. The certificates are not used:

– outside the purposes indicated in the keyUsage and extKeyUsage extensions and in the certificate policy;

– after expiry or revocation;

– to issue certificates or revocation lists;

– in control systems of critical installations, where a failure may cause death, injury or serious environmental damage;

– for unlawful activities.

The certificate is deemed accepted by the subject on its first use or, in the absence of an objection, 7 calendar days after it has been made available. Renewal is performed only with the generation of a new key pair; remote renewal, on the basis of the valid qualified CERTDIGITAL certificate, is allowed only once consecutively.

Revocation is published immediately through the OCSP service and is included in the next CRL, issued within 24 hours at the latest. The subject is informed without delay, with the reasons. CERTDIGITAL does not offer certificate suspension: where the law provides for suspension (Article 17(1) of Law no. 214/2024), the certificate is revoked. The public certificate register (https://ca.certdigital.ro/registry) indicates, for each certificate, its status and, where applicable, the date, time and reason of revocation.

## 3. Reliance limits

The certificates contain no transaction value limits (they do not contain the QcLimitValue statement). The limits of use are those in section 2.6 and are indicated in the certificate by the keyUsage and extKeyUsage extensions, by the certificate policy and by the validity period.

CERTDIGITAL keeps the certificates issued, the documents and data used for identity verification (including the video recordings made with CERTDIGITAL KYC), the requests, the revocation records and the relevant event logs for at least 10 years after the end of the validity of the certificate (Article 16(2) of Law no. 214/2024; Article 24(2)(h) of the eIDAS Regulation). If the activity is terminated, the records are kept and made available according to the Service termination plan.

The certificate status information services (OCSP and CRL) are available 24 hours a day, 7 days a week, with a target availability of 99.5% per year. Certificate status information is free of charge and remains available after the certificates have expired (Article 24(4) of the eIDAS Regulation).

# 4. Obligations of subjects and subscribers

The subject and, where applicable, the subscriber have the following obligations:

– to provide accurate, complete and up-to-date data and to communicate any change without delay;

– to read the terms and conditions (TC-CERT) before concluding the contract; a subscriber that contracts certificates for its employees or representatives ensures that they read them;

– to keep the cryptographic device and the activation data (PIN and PUK codes) under their sole control and not to disclose them;

– when generating the keys themselves, to use only the cryptographic devices and the CertDigital CSR application indicated by CERTDIGITAL;

– to check the data in the certificate on receipt and to report any discrepancy immediately;

– to use the certificate only for the permitted purposes (section 2.6) and only during its validity period;

– to request the revocation of the certificate within 24 hours at most of the loss or compromise of the device or of the activation data, or of finding that the data in the certificate no longer correspond to reality (Article 26 of Law no. 214/2024);

– to stop immediately and permanently using the private key if it is compromised, as well as after the certificate has expired or been revoked or after being informed that the certification authority has been compromised;

– for seal certificates: the legal person that is the subject designates the persons who use the seal, notifies the end of their capacity and is responsible for the use of the seal.

## 5. Obligations of relying parties

Before relying on a certificate or on a signature or seal created with it, the relying party:

– checks the status of the certificate at the time of signing, through OCSP or the most recent CRL (section 1.2);

– checks the certification path up to the root authority (CERTDIGITAL ROOT CA G4 or CERTDIGITAL ROOT CA G5, depending on the issuing authority), using the certificates of the authorities published by CERTDIGITAL (section 1.2);

– checks the qualified status of the service in the Romanian Trusted List (https://trustedlist.adr.gov.ro/);

– complies with the limits of use indicated in the certificate (keyUsage, extKeyUsage, certificate policy) and in this document;

– validates the signature or seal according to ETSI EN 319 102-1 (for example, through a validation service) and takes into account the time stamp, where available, to establish the time of signing.

At the written request of any person, accompanied by the signed document, CERTDIGITAL checks free of charge whether the signature or seal was created with a certificate issued by CERTDIGITAL, the status of the certificate at the time of signing and the integrity of the signature, and communicates the result within 30 days at most (Article 11(2) of Law no. 214/2024). This check is not a qualified validation service.

## 6. Limited warranty and limitation of liability

CERTDIGITAL is liable, in accordance with Article 13 of the eIDAS Regulation and Article 30 of Law no. 214/2024, for damage caused intentionally or negligently to any natural or legal person, including subjects and relying parties, due to a failure to comply with its obligations. The intention or negligence of CERTDIGITAL is presumed, unless CERTDIGITAL proves that the damage occurred without its intention or negligence.

CERTDIGITAL is not liable for damage resulting from:

– the use of the certificate beyond the limitations notified in advance and recognisable to third parties (Article 13(2) of the eIDAS Regulation; Article 15(5) of Law no. 214/2024);

– the subject's failure to comply with its obligations (chapter 4);

– the relying party's failure to check the status of the certificate and the status in the Trusted List;

– force majeure.

Liability for damage caused intentionally or by gross negligence is neither excluded nor limited (Article 1355 of the Romanian Civil Code); in relations with consumers, Law no. 193/2000 applies.

For each of the two qualified certification services (qualified certificates for electronic signatures and qualified certificates for electronic seals), CENTRUL DE CALCUL S.A. holds a separate professional liability insurance policy, with a limit of liability of EUR 500,000 for the insured period (Article 12(6) of Law no. 214/2024); in each policy, ADR is an additional insured party.

# 7. Applicable documents

The following documents apply together with this document and are published in the repository https://www.certdigital.ro/repository/:

| Document | Version |
|---|---|
| CertDigital Certification Services Policy | 2.0 |
| Certification Practice Statement of CERTDIGITAL ROOT CA G4 and CERTDIGITAL QUALIFIED CA G4 (DPC CERTDIGITAL G4) | 2.0 |
| Certification Practice Statement of CERTDIGITAL ROOT CA G5 and CERTDIGITAL QCA G5 (DPC CERTDIGITAL G5) | 1.0 |
| Terms and Conditions for qualified certificates (TC-CERT) | 2.0 |
| Contract for the provision of qualified certification services (CTR-CERT) | 2.0 |
| General policies of the trust service provider | 2.0 |
| CertDigital PKI hierarchy and supported policies (IER-PKI) | 7.0 |
| Policy and practice statement of the remote QSCD management service (PDP-rQSCD) and the terms and conditions of the service (TC-rQSCD) | 2.0 and 1.0 |
| Policies and practice statements of the services that use the G5 service certificates: PDP-QTST, PSPPS (QPS), PDP-QESVal, PDP-QEArch, PDP-Ledgers, PDP-QERDS (QeRDS and QREM), PDP-QEAA | 2.0; 1.1; 1.0 (the others) |
| Personal data protection policy | 2.1 |
| Service termination plan | 2.0 |

## 8. Personal data protection

The data controller is CENTRUL DE CALCUL S.A. (CertDigital). The identification and contact data of the subject and of the representatives, the copy of the identity document and, for remote identification, the video recording are processed for identity verification and for the issuance and management of the certificate, on the basis of the contract and of legal obligations (Article 6(1)(b) and (c) of Regulation (EU) 2016/679; the eIDAS Regulation; Law no. 214/2024). The biometric comparison in CERTDIGITAL KYC is performed only with the explicit consent of the subject. The data are kept for at least 10 years after the end of the validity of the certificate.

The certificate contains the identification data of the subject, which are published in the certificate register; the register does not display the personal numeric code, and the full certificate can be downloaded from the register only with the consent of the subject. Signature certificates also contain the extension 1.3.6.1.4.1.47898.30.1, which links the certificate to the verified identity document through a fingerprint of its data, without the data in clear.

Data subjects have the right of access, rectification, erasure (within the limits of the law), restriction, portability and objection, as well as the right to lodge a complaint with the National Supervisory Authority for Personal Data Processing (ANSPDCP). Data protection officer: dpo@centruldecalcul.ro. Details: the Personal data protection policy, published at https://www.certdigital.ro/protectia-datelor/.

## 9. Fees and refund policy

The fees for the services are those in the price list published on the website https://www.certdigital.ro/ or in the offer sent on request (Article 11(3)(b) of Law no. 214/2024). Certificate status information (OCSP, CRL), consultation of the certificate register, revocation and the verification of a signature at the request of a third party are free of charge. Refunds are made according to the contract and, for consumers, according to Government Emergency Ordinance no. 34/2014.

## 10. Applicable law, complaints and dispute resolution

The services are provided in accordance with Regulation (EU) No 910/2014, as amended by Regulation (EU) 2024/1183, with the applicable implementing acts (including Commission Implementing Regulation (EU) 2025/1943), with Law no. 214/2024, with Order no. 102/2026 of the Minister of Economy, Digitalisation, Entrepreneurship and Tourism (MEDAT) and with Regulation (EU) 2016/679. The complete list of the legal acts and standards applied is in DPC CERTDIGITAL G4 and in DPC CERTDIGITAL G5, section 9.15. The contract is governed by Romanian law.

Complaints are sent to office@certdigital.ro, and CERTDIGITAL replies within 30 days at most. If no amicable solution is reached, disputes with professionals fall within the jurisdiction of the courts of the registered office of CENTRUL DE CALCUL S.A. (Târgu Jiu). Consumers may apply to the competent courts according to the law, including those of their domicile, and may use the alternative dispute resolution (ADR) procedures provided by Government Ordinance no. 38/2015 (National Authority for Consumer Protection, ANPC – https://anpc.ro/ce-este-sal/). The supervisory body is the Romanian Digitalization Authority.

## 11. Qualified status, conformity assessment and audit

CENTRUL DE CALCUL S.A. is a qualified trust service provider, entered in the Romanian Trusted List (https://trustedlist.adr.gov.ro/), for the services of issuing qualified certificates for electronic signatures and for electronic seals. The qualified status can be checked in the Trusted List and in the EU Trust Services Dashboard (https://eidas.ec.europa.eu/efda/).

The services are assessed at least every 24 months by a conformity assessment body accredited in accordance with Commission Implementing Regulation (EU) 2025/2162 (EN ISO/IEC 17065 supplemented by ETSI EN 319 403-1) (Article 20 of the eIDAS Regulation); the conformity assessment report is published at https://www.certdigital.ro/repository/conformitate/. CERTDIGITAL carries out an internal audit every year.