END USER TERMS AND CONDITIONS

CertDigital qualified certificates for electronic signatures and electronic seals – essential information for the subject of the certificate

We are sending you this document because you are about to become the subject of a qualified certificate issued by CENTRUL DE CALCUL S.A. (CertDigital). It summarises, in plain language, the Terms and Conditions for qualified certificates (TC-CERT) and the PKI Disclosure Statement (PDS), without replacing them; in case of discrepancy, TC-CERT and the contract prevail. Please read it before signing the contract and the "User Agreement" and keep this message. If the certificate is requested by your employer or by the legal person you represent, the obligations below apply to you personally. In case of discrepancy between this English version and the Romanian version, the Romanian version prevails.

1. Who issues the certificate

CENTRUL DE CALCUL S.A. (CertDigital brand), Str. Tudor Vladimirescu nr. 17, Târgu Jiu, Gorj County, Romania, tax identification number RO2163993, a qualified trust service provider listed in the Romanian Trusted List (https://trustedlist.adr.gov.ro/) and supervised by the Romanian Digitalization Authority (ADR). Contact: phone +40 253 214 767, office@certdigital.ro, suport@certdigital.ro; opening hours: Monday–Friday, 09:00–17:00 (Romanian time).

2. The certificate and its legal effect

The qualified certificate for electronic signatures (ETSI policy QCP-n-qscd) allows you to create qualified electronic signatures, which have the legal effect of a handwritten signature. The qualified certificate for electronic seals (QCP-l-qscd) allows the legal person to create qualified electronic seals, which enjoy the presumption of integrity and of correctness of origin of the data (Articles 25 and 35 of Regulation (EU) No 910/2014). The certificate is valid for at most 3 years. The applied policy and the identity verification method are indicated in the certificate. The certificate contains no transaction value limits.

3. Receiving and accepting the certificate

The private key is generated and remains in your token; CERTDIGITAL does not keep it and cannot recover it. The PIN and PUK codes are sent to you in a sealed envelope, separately from the token. **Changing the PIN before first use is mandatory.** On receipt, check the data in the certificate (at the counter, on the "Certificate Annex" document) and report any discrepancy immediately: the certificate is revoked and, where appropriate, a correct one is issued. **The certificate is deemed accepted on its first use or, if you have not sent any objection, 7 calendar days after it has been made available to you**, whichever occurs first.

4. Your obligations

– to provide accurate, complete and up-to-date data and to report any change without delay;
– to keep the token and the PIN/PUK codes under your sole control, not to disclose them and not to allow other persons to use them;
– if you generate your keys yourself, to use only the tokens and the CertDigital CSR application indicated by CERTDIGITAL;
– to use the certificate only for the permitted purposes (point 5) and only during its validity period;
– **to request revocation within 24 hours at most** of the loss or compromise of the token or of the codes, or of finding that the data in the certificate no longer correspond to reality, including when a professional authorisation included in the certificate ends, is suspended or is withdrawn (Article 26 of Law no. 214/2024);
– to stop using the private key immediately if it has been compromised, after the certificate has expired or has been revoked, or after you have been informed that the certification authority has been compromised;
– for seals: 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. Permitted and prohibited uses

The certificate is used to create the qualified electronic signatures (or seals) of the subject and to authenticate the subject. The certificate is not used: outside the purposes indicated in the certificate (keyUsage, extKeyUsage, 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 illegal activities. Use beyond these limits is not covered by the liability of CERTDIGITAL.

6. Revocation

You can request revocation 24/7 in the customer portal https://ca.certdigital.ro/ra-web/apps/ota/, after authentication, by e-mail bearing a qualified electronic signature sent to office@certdigital.ro, or in writing, at the registered office, during opening hours. The request is processed within 24 hours at most, and the revocation is published immediately through OCSP and in the next certificate revocation list (CRL). Revocation is free of charge, final and enforceable against third parties from its entry in the certificate register; you are informed without delay, with the reasons. CERTDIGITAL does not suspend certificates: where the law provides for suspension, the certificate is revoked and, if the reason ceases, a new certificate is issued free of charge on request, after identity verification.

7. Renewal

Renewal is performed only with a new key pair. Remote renewal, on the basis of the valid CertDigital qualified certificate, is allowed only once in a row; at the next renewal, the identity is verified again, by physical presence or with CERTDIGITAL KYC.

8. Certificate data and the public register

The certificate contains your identification data and, on request, the professional attributes verified by CERTDIGITAL (Government Emergency Ordinance no. 140/2020). The signature certificate also contains a fingerprint of the data of the verified

identity document, without the data in clear. The public register https://ca.certdigital.ro/registry shows the serial number, the issuer, the policy, the validity period and the status of the certificate; it does not display the personal numeric code. The full certificate can be downloaded from the register only with your consent, which you can withdraw at any time.

9. Information for those who rely on your signature

Recipients of signed documents check the status of the certificate at the time of signing (OCSP or CRL), the certification chain up to CERTDIGITAL ROOT CA G4 or CERTDIGITAL ROOT CA G5, the qualified status in the Trusted List, and validate the signature according to ETSI EN 319 102-1, taking into account the time-stamp, if any. Certificate status information is free of charge and available 24/7, including after expiry: G4 – http://ocsp.g4.certdigital.ro, http://crl.certdigital.ro/certdigital_qualified_g4.crl; G5 – http://ocsp.g5.certdigital.ro, http://crl.certdigital.ro/certdigital_qualified_g5.crl. At the written request of any person, CERTDIGITAL verifies, free of charge and within 30 days at most, a signature created with a certificate it has issued.

10. Record retention and personal data protection

CERTDIGITAL keeps the certificate, the documents and data used for identity verification (including the CERTDIGITAL KYC video recording), the applications, the revocation records and the event logs **for at least 10 years after the certificate ceases to be valid**. The data are processed for identity verification and for issuing and managing the certificate, on the basis of the contract and of legal obligations; biometric comparison is performed only with your explicit consent. The mandated partners who identify you at their counter process the data on behalf of CERTDIGITAL. You 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 Romanian data protection authority (ANSPDCP). Data protection officer: dpo@centruldecalcul.ro; details: https://www.certdigital.ro/protectia-datelor/.

11. Liability and insurance

CERTDIGITAL is liable for damage caused intentionally or negligently through a failure to comply with its obligations (Article 13 of Regulation (EU) No 910/2014; Article 30 of Law no. 214/2024); intention or negligence is presumed unless proven otherwise. CERTDIGITAL is not liable for damage resulting from use of the certificate beyond the limits in point 5, from failure to comply with the obligations in point 4, from the relying party's failure to check the status of the certificate, or from force majeure. Liability for intent or gross negligence is neither excluded nor limited; consumers also enjoy the protection of Law no. 193/2000. For each qualified certification service, CERTDIGITAL holds professional liability insurance of EUR 500,000.

12. Service availability and fees

OCSP and CRL: 24/7, with a target availability of 99.5% per year; website and document repository: 24/7, 99% per year; counter and support: Monday–Friday, 09:00–17:00. Planned interruptions are announced on the website at least 24 hours in advance. Fees are those in the list published at https://www.certdigital.ro/ or in the offer you received; revocation, certificate status information, consulting the register and verifying 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.

13. Complaints, disputes and applicable law

Complaints are sent to office@certdigital.ro; CERTDIGITAL replies within 30 days at most. If no amicable solution is reached, disputes with professionals fall under the jurisdiction of the courts of the registered office of CENTRUL DE CALCUL S.A. (Târgu Jiu); consumers may also apply to the courts of their domicile and use the alternative dispute resolution procedures (https://anpc.ro/sal). Romanian law applies, together with Regulation (EU) No 910/2014, as amended by Regulation (EU) 2024/1183, and Law no. 214/2024.

14. Conformity assessment and changes

The service is assessed at least once every 24 months by an accredited conformity assessment body (EN ISO/IEC 17065 and ETSI EN 319 403-1); the conformity assessment report is published in the document repository, and the qualified status can be checked in the Trusted List and in the EU Trust Services Dashboard (https://eidas.ec.europa.eu/efda/). Changes to the terms and conditions are published on the website at least 30 days before they enter into force; during this period you may raise objections or request the revocation of the certificate, free of charge.

15. Full documents

Full terms and conditions (TC-CERT, in Romanian): https://www.certdigital.ro/repository/termeni/certdigital_tc-cert_ro.pdf; PKI Disclosure Statement (PDS): https://www.certdigital.ro/repository/pds/certdigital_pds_en.pdf (in Romanian: https://www.certdigital.ro/repository/pds/certdigital_pds_ro.pdf); the certificate policy, DPC CERTDIGITAL G4 and G5 and the other public documents: https://www.certdigital.ro/repository/. For the certificates of the remote signing service (rQSCD), the Terms and Conditions of the remote QSCD management service also apply, and the provisions on the token and the PIN/PUK codes do not apply to these certificates.