SMIME BR Audit Attestation for DigitalSign - Certificadora Digital, S.A.

Reference: 2025/13840

Thiene, 2025-09-22

To whom it may concern,

This is to confirm that CSQA Certificazioni Srl has audited the CAs of the the DigitalSign - Certificadora Digital, S.A." without critical findings.
This present Audit Attestation Letter is registered under the unique identifier number **2025/13840** covers multiple Root-CAs and consists of 12 pages.
Kindly find here below the details accordingly.

In case of any question, please contact:

CSQA Certificazioni S.r.l.

Via S. Gaetano, 74
36016 Thiene (VI), Italy
Email: csqa@csqa.it Phone:
+39 0445 313011

With best regards,

Firmato digitalmente da:
Bonato Pietro
Firmato il 08/10/2025 12:36
Seriale Certificato: 4385020
Valido dal 28/03/2025 al 28/03/2028
InfoCamere Qualified Electronic Signature CA

Pietro Bonato
Chief Executive Officer

This attestation is based on the template version 3.4 as of 2025-07-08, that was approved for use by ACAB'c.

General audit information

Identification of the conformity assessment body (CAB) and assessment organization acting as ETSI auditor
• **CSQA Certificazioni S.r.l.,** Via S. Gaetano, 74, 36016 Thiene (VI) registered under VAT 02603680246 • Accredited by the Italian National Accreditation Body (Accredia – www.accredia.it) under registration 014B for the certification of trust services according to "EN ISO/IEC 17065:2012" and "ETSI EN 319 403-1 V2.3.1 (2020-06)" and/or "ETSI EN 319 403-1 V2.3.1 (2020-06)" respectively. • Insurance Carrier (BRG section 8.2): Zurich Third-party affiliate audit firms involved in the audit: none.
Identification and qualification of the audit team
• Number of team members: 3 • Academic qualifications of team members: 1 All team members have formal academic qualifications or professional training or extensive experience indicating general capability to carry out audits based on the knowledge given below and at least four years full time practical workplace experience in information technology, of which at least two years have been in a role or function relating to relevant trust services, public key infrastructure, information security including risk assessment/management, network security and physical security. • Additional competences of team members: All team members have knowledge of 1) audit principles, practices and techniques in the field of CA/TSP audits gained in a training course of at least five days; 2) the issues related to various areas of trust services, public key infrastructure, information security including risk assessment/management, network security and physical security; 3) the applicable standards, publicly available specifications and regulatory requirements for CA/TSPs and other relevant publicly available specifications including standards for IT product evaluation; and 4) the Conformity Assessment Body's processes. Furthermore, all team members have language skills appropriate for all organizational levels within the CA/TSP organization; note-taking, report- writing, presentation, and interviewing skills; and relevant personal attributes: objective, mature, discerning, analytical, persistent and realistic. • Professional training of team members: See "Additional competences of team members" above. Apart from that are all team members trained to demonstrate adequate competence in: a) knowledge of the CA/TSP standards and other relevant publicly available specifications; b) understanding functioning of trust services and information security including network security issues; c) understanding of risk assessment and risk management from the business perspective;technical knowledge of the activity to be audited; d) general knowledge of regulatory requirements relevant to TSPs; and e) knowledge of security policies and controls. • Types of professional experience and practical audit experience: The CAB ensures, that its personnel performing audits maintains competence on the basis of appropriate education, training or experience; that all relevant experience is current and prior to assuming responsibility for performing as an auditor, the candidate has gained experience in the entire process of CA/TSP auditing. This experience shall have been gained by participating under supervision of lead auditors in a minimum of four TSP audits for a total of at least 20 days, including documentation review, on-site audit and audit reporting. • Additional qualification and experience Lead Auditor: On top of what is required for team members (see above), the Lead Auditor a) has acted as auditor in at least three complete TSP audits;

b) has adequate knowledge and attributes to manage the audit process; and
c) has the competence to communicate effectively, both orally and in writing.

Special skills or qualifications employed throughout audit: ISMS Auditor (ISO/IEC 27001)

- Special Credentials, Designations, or Certifications:

All members are qualified and registered assessors within the accredited CAB.

- Auditors code of conduct incl. independence statement:

Code of Conduct as of Annex A, ETSI EN 319 403 or ETSI EN 319 403-1 respectively.

Identification and qualification of the reviewer performing audit quality management
• Number of Reviewers/Audit Quality Managers involved independent from the audit team: 1 • The reviewer fulfils the requirements as described for the Audit Team Members above and has acted as an auditor in at least three complete CA/TSP audits.

Identification of the CA / Trust Service Provider (TSP):	**DigitalSign - Certificadora Digital, S.A.**, Largo Pe. Bernardino Ribeiro Fernandes, 26 - 4835 NESPEREIRA, Portugal https://www.digitalsign.pt/en/

Type of audit:	☐ Point in time audit ☐ Period of time, after x month of CA operation ☒ Period of time, full audit
Audit period covered for all policies:	2024-06-27 to 2025-06-26
Point in time date:	none, as audit was pot audit
Audit dates:	2025-07-14 to 2025-07-23 (remote and on site)
Audit location:	Largo Pe. Bernardino Ribeiro Fernandes, 26 – 4835-489 NESPEREIRA, Portugal Avenida da Igreja, 367 - 4835-507 NESPEREIRA, Portugal RIBA D'AVE DATA CENTER, Rua Cruzeiro dos Chãos - 4765-341 Santa Maria Oliveira, Portugal

Root 1: DIGITALSIGN GLOBAL ROOT RSA CA

Standards considered:	European Standards: • ETSI EN 319 411-2, 2.5.1 (2023-10) • ETSI TS 119 411-6 V1.1.1 (2023-08) • ETSI EN 319 411-1, V1.4.1 (2023-10) • ETSI EN 319 401, V2.3.1 (2021-05) • ETSI EN 319 412-2 V2.3.1 (2023-09) • ETSI EN 319 412-3 V1.3.1 (2023-09) • ETSI EN 319 412-5 V2.4.1 (2023-09) • ETSI TS 119 441 v1.2.1 (2023-10) • ETSI TS 119 442 v1.1.1 (2019-02) • ETSI EN 319 102-1 v1.3.1 (2021-11) • ETSI TS 119 102-2 v1.4.1 (2023-06) • ETSI EN 319 421 V1.1.1 (2016-03) • ETSI EN 319 422 V1.1.1 (2016-03) • ETSI TS 119 511 v.1.1.1 (2019-06) • ETSI TS 119 512 v.1.1.1 (2020-01) • ETSI TS 119 461 V2.1.1 (2025-02) CA Browser Forum Requirements: • Baseline Requirements for the Issuance and Management of Publicly‐Trusted TLS Server Certificates, version 2.1.5 • Network and Certificate System Security Requirements, version 2.0.5 • Baseline Requirements for the Issuance and Management of Publicly‐Trusted S/MIME Certificates, version 1.1.10 Browser Policy Requirements: • Mozilla Root Store Policy, section 6.1.3 regarding mass revocation plans and testing thereof For the Trust Service Provider Conformity Assessment: • ETSI EN 319 403 V2.2.2 (2015-08) • ETSI EN 319 403-1 V2.3.1 (2020-06) • ETSI TS 119 403-2 V1.3.1 (2023-03)

The audit was based on the following policy and practice statement documents of the CA / TSP:

- Certification Practice Statement - Version 1.11 – 16/07/2025
- Certification Profile List - Version 1.8 - 06/12/2024
- PKI Disclosure Statement - Version 3.3 - 16/07/2025
- Timestamp Policy and TSA Practice Statement - Version 2.3 – 01/08/2024
- Signature Validation Service Policy and Practice Statements - Version 1.0 - 29/09/2022
- Preservation Service Policy and Practice Statements - Version 1.0 - 16/06/2025

One minor non-conformities have been identified during the audit.

- 1 23/07/2025 NC_I [ETSI EN 319 401] REQ-7.9-10 - REQ-7.9-11 Regarding the VA/PT, there is a lack of documentation of the vulnerability management process, a priority/severity scale, and resolution deadlines defined in the remediation plan
- All non-conformities have been closed before the issuance of this attestation.

- This Audit Attestation also covers the following incidents as documented under: No incident detected during the period.

Distinguished Name	SHA-256 fingerprint	Applied policy
CN= DIGITALSIGN GLOBAL ROOT RSA CA, O=DigitalSign Certificadora Digital, C=PT	82BD5D851ACF7F6E1BA7BFCBC53030D0E7BC3C21DF772D858CAB41D199BDF595	ETSI EN 319 411-2 V2.5.1, QCP-n;QCP-n-qscd;QCP-l;QCP-l-qscd ETSI EN 319 411-1 V1.4.1, LCP;NCP;NCP+ ETSI EN 319 421 V1.1.1, Time-stamp

Table 1: Root-CA 1 in scope of the audit

The TSP named the Sub-CAs that have been issued by the aforementioned Root-CA, that are listed in the following table and that have been covered in this audit.

Distinguished Name	SHA-256 fingerprint	Applied policy
CN = DIGITALSIGN QUALIFIED CA G1 O = DigitalSign Certificadora Digital C = PT	27BB49D206B6DEC161EBB8EA739530E90AC68498D2EEA05A7ED9603D1DCE0FD5	ETSI EN 319 411-2 V2.5.1, QCP-n;QCP-n-qscd;QCP-l;QCP-l-qscd
CN = DIGITALSIGN QUALIFIED TSA CA G1 O = DigitalSign Certificadora Digital C = PT	2BB402D903E1C15743E99806D1D046CFBF45E37DDD312607566F464996E20750	ETSI EN 319 421 V1.1.1, Time-stamp
CN = DIGITALSIGN CA G1 O = DigitalSign Certificadora Digital C = PT	951B523C9B7FD59AF6FAE2E054D97F2B9371A41DF752D63295B3BB93F3C5059C	ETSI EN 319 411-1 V1.4.1, LCP;NCP;NCP+
CN = DIGITALSIGN TSA CA G1 O = DigitalSign Certificadora Digital C = PT	38BD3C34D9D93D71F8F331556756CB4BE152E1C99B50EB177F8A68E8D01F5CD6	ETSI EN 319 421 V1.1.1, Time-stamp

Table 2: Sub-CA’s issued by the Root-CA 1 or its Sub-CA’s in scope of the audit

Root 2: Sub-CA's issued by the Root-CA or its Sub-CA's in scope of the audit

Standards considered:	European Standards: • ETSI EN 319 411-2, 2.5.1 (2023-10) • ETSI TS 119 411-6 V1.1.1 (2023-08) • ETSI EN 319 411-1, V1.4.1 (2023-10) • ETSI EN 319 401, V2.3.1 (2021-05) • ETSI EN 319 412-2 V2.3.1 (2023-09) • ETSI EN 319 412-3 V1.3.1 (2023-09) • ETSI EN 319 412-5 V2.4.1 (2023-09) • ETSI TS 119 441 v1.2.1 (2023-10) • ETSI TS 119 442 v1.1.1 (2019-02) • ETSI EN 319 102-1 v1.3.1 (2021-11) • ETSI TS 119 102-2 v1.4.1 (2023-06) • ETSI EN 319 421 V1.1.1 (2016-03) • ETSI EN 319 422 V1.1.1 (2016-03) • ETSI TS 119 511 v.1.1.1 (2019-06) • ETSI TS 119 512 v.1.1.1 (2020-01) • ETSI TS 119 461 V2.1.1 (2025-02) CA Browser Forum Requirements: • Baseline Requirements for the Issuance and Management of Publicly‐Trusted TLS Server Certificates, version 2.1.5 • Network and Certificate System Security Requirements, version 2.0.5 • Baseline Requirements for the Issuance and Management of Publicly‐Trusted S/MIME Certificates, version 1.1.10 Browser Policy Requirements: • Mozilla Root Store Policy, section 6.1.3 regarding mass revocation plans and testing thereof For the Trust Service Provider Conformity Assessment: • ETSI EN 319 403 V2.2.2 (2015-08) • ETSI EN 319 403-1 V2.3.1 (2020-06) • ETSI TS 119 403-2 V1.3.1 (2023-03)

The audit was based on the following policy and practice statement documents of the CA / TSP:

- Certification Practice Statement - Version 1.11 – 16/07/2025
- Certification Profile List - Version 1.8 - 06/12/2024
- PKI Disclosure Statement - Version 3.3 - 16/07/2025
- Timestamp Policy and TSA Practice Statement - Version 2.3 – 01/08/2024
- Signature Validation Service Policy and Practice Statements - Version 1.0 - 29/09/2022
- Preservation Service Policy and Practice Statements - Version 1.0 - 16/06/2025

One minor non-conformities have been identified during the audit.

- 1 23/07/2025 NC_I [ETSI EN 319 401] REQ-7.9-10 - REQ-7.9-11 Regarding the VA/PT, there is a lack of documentation of the vulnerability management process, a priority/severity scale, and resolution deadlines defined in the remediation plan

All non-conformities have been closed before the issuance of this attestation. This Audit Attestation also covers the following incidents as documented under: No incident detected during the period.

Distinguished Name	SHA-256 fingerprint	Applied policy
CN=DIGITALSIGN GLOBAL ROOT ECDSA CA, =DigitalSign Certificadora Digital, C=PT	261D7114AE5F8FF2D8C7209A9DE4289E6AFC9D717023D85450909199F1857CFE	ETSI EN 319 411-2 V2.5.1, QCP-n;QCP-n-qscd;QCP-l;QCP-l-qscd ETSI EN 319 411-1 V1.4.1, LCP;NCP;NCP+ ETSI EN 319 421 V1.1.1, Time-stamp

Table 3: Root-CA in scope of the audit

The TSP named the Sub-CAs that have been issued by the aforementioned Root-CA, that are listed in the following table and that have been covered in this audit.

Distinguished Name	SHA-256 fingerprint	Applied policy
CN = DIGITALSIGN QUALIFIED CA V1 O = DigitalSign Certificadora Digital C = PT	4A2B2B0F8429A77E23BCAB8FFA253F4C21368CB4AA2A78DBC5D417C6D1D0E105	ETSI EN 319 411-2 V2.5.1, QCP-n;QCP-n-qscd;QCP-l;QCP-l-qscd
CN = DIGITALSIGN QUALIFIED TSA CA V1 O = DigitalSign Certificadora Digital C = PT	BD2318F64DCC529238BCC71C94948F7B9479A36E30DDA65A520A356F9EFB5AD9	ETSI EN 319 421 V1.1.1, Time-stamp
CN = DIGITALSIGN CA V1 O = DigitalSign Certificadora Digital C = PT	C18C8DE10A7B02AB2A700F3E95EE53501DC015012FAAC197B2D64BF2EE6DFE77	ETSI EN 319 411-1 V1.4.1, LCP;NCP;NCP+
CN = DIGITALSIGN TSA CA V1 O = DigitalSign Certificadora Digital C = PT	C811BD06D09F43F003C496F7C28B9D5D6477EFEDFFE169B418A5B7B48B6BB9D6	ETSI EN 319 421 V1.1.1, Time-stamp

Table 4: Sub-CA’s issued by the Root-CA or its Sub-CA’s in scope of the audit

Root 3: Sub-CA’s issued by the Root-CA or its Sub-CA’s in scope of the audit

Standards considered:	European Standards: • ETSI EN 319 401, V2.3.1 (2021-05) • ETSI EN 319 421 V1.1.1 (2016-03) • ETSI EN 319 422 V1.1.1 (2016-03) For the Trust Service Provider Conformity Assessment: • ETSI EN 319 403 V2.2.2 (2015-08) • ETSI EN 319 403-1 V2.3.1 (2020-06) • ETSI TS 119 403-2 V1.3.1 (2023-03)

The audit was based on the following policy and practice statement documents of the CA / TSP:

- Certification Practice Statement - Version 1.11 – 16/07/2025
- Certification Profile List - Version 1.8 - 06/12/2024
- PKI Disclosure Statement - Version 3.3 - 16/07/2025
- Timestamp Policy and TSA Practice Statement - Version 2.3 – 01/08/2024

- One minor non-conformities have been identified during the audit.
  1 23/07/2025 NC_I [ETSI EN 319 401] REQ-7.9-10 - REQ-7.9-11 Regarding the VA/PT, there is a lack of documentation of the vulnerability management process, a priority/severity scale, and resolution deadlines defined in the remediation plan
- All non-conformities have been closed before the issuance of this attestation.
- This Audit Attestation also covers the following incidents as documented under: No incident detected during the period.

Distinguished Name	SHA-256 fingerprint	Applied policy
CN = QuoVadis Root CA 3 G3, O = QuoVadis Limited, C = BM	88EF81DE202EB018452E43F864725CEA5FBD1FC2D9D205730709C5D8B8690F46	--

Table 5: Root-CA in scope of the audit

The TSP named the Sub-CAs that have been issued by the aforementioned Root-CA, that are listed in the following table and that have been covered in this audit.

Distinguished Name	SHA-256 fingerprint	Applied policy
CN = QuoVadis Enterprise Trust CA 3 G3, O = QuoVadis Limited, C = BM	DA5462526A0C2E9852A86186B025390158759CDCA6AE21F09F713CA6ACCDD1F1	--
CN = C = GB, O = British Telecommunications plc, CN = BT Class 2 DigiCert PKI Platform CA	843782303040BFB33576766E1700696DE0FC14887BE293D7265EB59ECE4ED9CC	--

Table 6: Intermediate CA in scope of the audit

The TSP named the Sub-CAs that have been issued by the aforementioned Root-CA, that are listed in the following table and that have been covered in this audit.

Distinguished Name	SHA-256 fingerprint	Applied policy
CN = DigitalSign Qualified CA - G4 OU = Class 2 DigiCert PKI Platform Individual Subscriber CA O = DigitalSign - Certificadora Digital C = PT	41678B8897E635DEA03B6E48565E267BA5AAC3B8F4DC4B74B7A0A9748CFDD35E	ETSI EN 319 421 V1.1.1, Time-stamp

Table 7: Sub-CA’s issued by the Root-CA or its Sub-CA’s in scope of the audit

Modifications record

Version	Issuing Date	Changes
Version 1	2025-09-22	Initial attestation

End of the audit attestation letter.