



Standard Audit Attestation for
MULTICERT Serviços de Certificação
Electrónica, S.A

Reference: ALLMULTICERT2026v1

14/04/2026

To whom it may concern,

This is to confirm that BSI has audited the CAs of the **MULTICERT Serviços de Certificação Electrónica, S.A** without critical findings.

This present Audit Attestation Letter is registered under the unique identifier number **MULTIC-0048019368-000** covers multiple Root-CAs and consists of 9 pages.

Kindly find here below the details accordingly.

In case of any question, please contact:

BSI Group The Netherlands B.V.
Say Building, John M. Keynesplein 9
1066 EP Amsterdam
The Netherlands
E-Mail: gary.pattison@bsigroup.com
Phone: +44 07920 502741

With best regards,

Gary Pattison
Certification Team Leader

This attestation is based on the template version 3.5 as of 2026-03-09, 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

- BSI Group The Netherlands B.V., Say Building, John M. Keynesplein 9, 1066 EP, Amsterdam, The Netherlands registered under 33264284
- Accredited by Raad voor Accreditatie (RvA) under registration C646 - Raad voor Accreditatie for the certification of trust services according to "EN ISO/IEC 17065:2012" and "ETSI EN 319 403 V2.2.2 (2015-08)" / "ETSI EN 319 403-1 V2.3.1 (2020-06)".
- Insurance Carrier (BRG section 8.2):
- Third-party affiliate audit firms involved in the audit: None.

Identification and qualification of the audit team

- Number of team members: 1
- Academic qualifications of team members:
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;
 - d) technical knowledge of the activity to be audited;
 - e) general knowledge of regulatory requirements relevant to TSPs; and
 - f) 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: None. - 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: 2 - 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):	MULTICERT Serviços de Certificação Electrónica, S.A, Estrada de Alfragide, 67 2610-008 Amadora Portugal Registered under VAT 505767457
--	--

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:	2025-04-01 to 2026-03-31
Point in time date:	Not Applicable
Audit dates:	2026-05-18 – Porto (on site) 2026-05-19 – (remote) 2026-05-20 – Amadora (on site) 2026-05-21 – Amadora (on site) 2026-05-22 – (remote) 2026-05-27 – (remote) 2026-06-01 – Viseu (on site) 2026-06-03 – (remote) 2026-06-08 – (remote)



Audit Attestation ALLMULTICERT2026v1, issued to MULTICERT

	2026-06-08 – (remote) 2026-06-09 – (remote) 2026-06-09 – (remote) 2026-06-11 – (remote) 2026-06-12 – (remote) 2026-06-22 – Porto (on site)
Audit location:	• Amadora - Portugal • Porto - Portugal • Viseu – Portugal • Lisbon – Portugal • Coimbra – Portugal



Root 1: MULTICERT Root Certification Authority 01

Standards considered:	European Standards: • ETSI EN 319 401 V3.2.1 • ETSI EN 319 411-1 V1.5.1 • ETSI EN 319 411-2 V2.6.1 • ETSI EN 319 421 V1.3.1 • ETSI TS 119 495 V1.7.1 For the Trust Service Provider Conformity Assessment: • ETSI EN 319 403 V2.2.2 • ETSI EN 319 403-1 V2.3.1 • ETSI TS 119 403-2 V1.3.1
-----------------------	---

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

- Multicert Certification Practice Statement, version 19.0, dated 2025-12-15
- Multicert Certificate Policy, version 13.0, dated 2025-12-15
- Declaração de Práticas de Validação Cronológica, version 9.0, dated 2025-12-15.

In the following areas, non-conformities have been identified throughout the audit:

1. Findings with regard to ETSI EN 319 401:

- 7.6 – Physical Security
 - REQ-7.6-02 / REQ-7.6-03 / REQ-7.6-04 / REQ-7.6-09 / REQ-7.6-13
 1. Following an assessment of the implementation of the CCTV system, lack of redundancy coverage was identified in the coverage of sensitive areas on Level 3 in both data centres.
 2. It has not been demonstrated that the cameras' connectivity utilises redundant cable routes and redundant LAN switches.
- 7.8 – Network Security
 - REQ-7.8-12:
 1. Although redundant routers and redundant cable routes are used in both Data Centres, there is only one service provider for interconnection with external networks.



Audit Attestation ALLMULTICERT2026v1, issued to MULTICERT

2. Replication between data centres is currently supported by just one router; there is no equipment redundancy.
 3. There are no redundancies in the physical fibre-optic connectivity with Multicert's communications routers in Data Centre.
- REQ-7.8-13 / REQ-7.8-23
 1. Penetration tests and vulnerability scans are not being carried out on all internal Level 3 and Level 4 networks.
- 7.11 – Business Continuity
 - REQ-7.11-1-02 / REQ-7.11.1-03
 1. Although there is a manual procedure in place for issuing or revoking certificates, it has become evidenced that the system responsible for sending SMS messages does not have site redundancy, which prevents certificate lifecycle operations from being carried out.
2. Findings with regard to ETSI EN 319 411-1: None.
 3. Findings with regard to ETSI EN 319 411-2: None.
 4. Findings with regard to ETSI EN 319 421: None.

For all non-conformities, remediation has been scheduled within three months after the onsite audit at latest and will be covered by a corresponding audit.

During the audit period Multicert didn't report any incident on Bugzilla.



Audit Attestation ALLMULTICERT2026v1, issued to MULTICERT

Distinguished Name	SHA-256 fingerprint	Applied policy
CN=MULTICERT Root Certification Authority 01 O=MULTICERT - Serviços de Certificação Electrónica S.A. C=PT	604D32D036895AED3BFEFAEB727C009EC0F2B3CDFA42A1C71730E6A72C3BE9D4	ETSI EN 319 401 v3.2.1 ETSI EN 319 411-1 v1.5.1: LCP, NCP, NCP+ ETSI EN 411-2 v2.6.1: QCP-n, QCP-n-qscd, QCP-l, QCP-l-qscd, QNCP-w-gen ETSI TS 119 495 v1.7.1 ETSI EN 319 421 v1.3.1

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=MULTICERT Trust Services Certification Authority 005 OU=Certification Authority O=MULTICERT - Serviços de Certificação Electrónica S.A. C=PT	48A153E21E1B8C64DCBDCBA034DAB2EF8527A779A1BA2AA238ACC48A2C6FCACF	ETSI EN 319 411-1 v1.5.1: LCP, NCP, NCP+ ETSI EN 319 411-2 v2.6.1: QCP-n, QCP-n-qscd, QCP-l, QCP-l-qscd
CN=MULTICERT Trust Services Certification Authority 002 OU=Certification Authority O=MULTICERT - Serviços de Certificação Electrónica S.A. C=PT	82CFDAE3A70B6E375A96ED3CFC912E81A020104A8BA886272B5963ADECA24411	ETSI EN 319 411-1 v1.5.1: LCP, NCP, NCP+ ETSI EN 319 411-2 v2.6.1: QCP-n, QCP-n-qscd, QCP-l, QCP-l-qscd



Audit Attestation ALLMULTICERT2026v1, issued to MULTICERT

CN= MULTICERT QWAC Certification Authority 005 OU=Certification Authority O=MULTICERT - Serviços de Certificação Electrónica S.A. C=PT	35A1FAA8C81125666D26F0A6E864DDEAA70431CC1570DC883CF147CD196E4AB6	ETSI EN 319 411-1 v1.5.1: NCP+ ETSI EN 319 411-2 v2.6.1: QNCP-w-gen
CN=MULTICERT Timestamping Certification Authority 005 OU=Certification Authority O=MULTICERT - Serviços de Certificação Electrónica S.A. C=PT	E8627AC236183A420E1513839ACEEEF833D27A45512717A9BAFDE8506BB5C1CF	ETSI EN 319 411-1 v1.5.1 ETSI EN 319 411-2 v2.6.1 ETSI EN 319 421 v1.3.1
CN=MULTICERT Advanced Certification Authority 001 OU=Certification Authority O=MULTICERT - Serviços de Certificação Electrónica S.A. C=PT	EF72A054691F855D52A31988439B75BDE49F03899ADF0EBC142CB96E3483D6F7	ETSI EN 319 411-1 v1.5.1: LCP, NCP, NCP+
CN= MULTICERT Advanced Certification Authority 005 OU=Certification Authority O=MULTICERT - Serviços de Certificação Electrónica S.A. C=PT	24EDD4E503A8D3FDB5FFB4AF66C887359901CBE687A5A0760D10A08EED99A7C3	ETSI EN 319 411-1 v1.5.1: LCP, NCP, NCP+

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



to MULTICERT

Audit Attestation ALLMULTICERT2026v1, issued

Modifications record

Version	Issuing Date	Changes
Version 1	2026-07-17	Validated Attestation Letter

End of the audit attestation letter.