TLS EV Audit Attestation for

Buypass AS

Reference: AAL-CT016-2500902-TLS-EV

The Hague, 12 February 2026

To whom it may concern,

This is to confirm that Attestic B.V., also operating under the trade name “Attestic Certification”, has audited the CAs of Buypass AS without critical findings.

This present Audit Attestation Letter is registered under the unique identifier number AAL-CT016-2500902-TLS-EV covers multiple Root-CAs and consists of 7 pages.

Kindly find here below the details accordingly.

In case of any question, please contact:

Attestic Certification
Zeestraat 70
2518 AC The Hague, The Netherlands
E-Mail: info@attestic.eu
Phone: -

With best regards,

Maarten de Boer
General Director

General audit information

Identification of the conformity assessment body (CAB) and assessment organization acting as ETSI auditor
• Attestic B.V., also operating under the trade name "Attestic Certification", Zeestraat 70, 2518 AC The Hague, The Netherlands, registered under Dutch Trade Register number: 95187499 • Accredited by Dutch Accreditation Council (RvA) under C710[1] for the certification of trust services according to "EN ISO/IEC 17065:2012" and "ETSI EN 319 403-1 V2.3.1 (2020-06)". • Insurance Carrier (BRG section 8.2): AIG Europe S.A., Netherlands branche is providing the professional liability insurance coverage • Third-party affiliate audit firms involved in the audit: None.
Identification and qualification of the audit team
• Number of team members: 2 • 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

[1] https://www.rva.nl/en/alle-geaccrediteerden/c710/

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: 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):	Buypass AS, Gullhaug Torg 2D, 0484 Oslo, Norway, registered under NO 983 163 327

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:	2024-11-01 to 2025-10-31
Point in time date:	none, as audit was a period of time audit
Audit dates:	2025-11-03 to 2025-11-06 (remote) 2025-11-10 to 2025-11-14 (onsite) 2025-11-17 to 2025-11-19 (remote) 2025-11-24 to 2025-11-28 (onsite) 2025-12-03 to 2025-12-04 (remote)
Audit location:	Oslo and Gjøvik, Norway

Root 1: Buypass Class 3 Root CA

Standards considered:	European Standards: • ETSI EN 319 411-2 V2.6.1 (2025-06) • ETSI EN 319 411-1 V1.5.1 (2025-04) • ETSI EN 319 401 V3.1.1 (2024-06) CA Browser Forum Requirements: • Guidelines for the Issuance and Management of Extended Validation Certificates, version 2.0.1 • Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates, version 2.1.7 • Network and Certificate System Security Requirements, version 2.0.5 Browser Policy Requirements: • Mozilla Root Store Policy • Mozilla Root Store Policy, section 6.1.3 regarding mass revocation plans and testing thereof • Microsoft Trusted Root Program, Program Requirements • Google Chrome Root Program Policy • Apple Root Certificate Program Other: • None For the Trust Service Provider Conformity Assessment: • 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 - Buypass Class 3 SSL Certificates v14.5, dated: 2024-01-26 (effective date: 2024-01-26)
- Certification Practice Statement - Buypass Class 3 SSL Certificates v14.6, dated: 2024-11-07 (effective date: 2024-11-07)
- Certification Practice Statement - Buypass Class 3 SSL Certificates v14.7, dated: 2025-01-15 (effective date: 2025-01-15)
- Certification Practice Statement for Buypass TLS Certificates v1.0, dated 2025-01-20 (effective date: 2025-01-30)
- Certification Practice Statement for Buypass TLS Certificates v1.1, dated 2025-03-30 (effective date: 2025-03-30)
- Certification Practice Statement for Buypass TLS Certificates v2.0, dated 2025-08-29 (effective date: 2025-09-08)

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

Findings with regard to ETSI EN 319 401:

7.13 Compliance

Documentation and implementation of compliance auditing on support processes shall be improved. [REQ-7.13-02]

7.14 Supply Chain

Documentation and implementation of Supply Chain Policy shall be improved. [7.14.1, 7.14.2, 7.14.3]

Findings with regard to ETSI EN 319 411-1:
None.

Findings with regard to ETSI EN 319 411-2:
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.

To the best of our knowledge, no incidents have occurred within this Root-CA's hierarchy during the audited period.

Distinguished Name	SHA-256 fingerprint	Applied policy
CN=Buypass Class 3 Root CA,O=Buypass AS-983163327,C=NO	EDF7EBBCA27A2A384D387B7D4010C666E2EDB4843E4C29B4AE1D5B9332E6B24D	ETSI EN 319 411-2 V2.6.1, QEVCP-w ETSI EN 319 411-1 V1.5.1, EVCP

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= Buypass Class 3 CA 2,O=Buypass AS-983163327,C=NO	DAA0435407FA44C28AB939E6823813605779093873A96649AD6E03B05D28626C	ETSI EN 319 411-2 V2.6.1, QEVCP-w ETSI EN 319 411-1 V1.5.1, EVCP

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

Modifications record

Version	Issuing Date	Changes
Version 1	2026-01-29	Initial attestation
Version 2	2026-02-12	Amended attestation: additional practices documents added.

End of the audit attestation letter.