TLS EV Audit Attestation for

GLOBALTRUST operated by e-commerce monitoring GmbH

Reference: VIG-26-069-TLS-EV

"Wien, 2026-06-26"

To whom it may concern,

This is to confirm that "A-SIT, Secure Information Technology Center – Austria" has audited the CAs of the "GLOBALTRUST operated by e-commerce monitoring GmbH" without critical findings.

This present Audit Attestation Letter is registered under the unique identifier number "VIG-26-069-TLS-EV", covers multiple Root-CAs and consists of 10 pages.

Kindly find here below the details accordingly.

In case of any question, please contact:

A-SIT, Secure Information Technology Center – Austria
Seidlgasse 22/9
1030 Wien, Austria
E-Mail: office@a-sit.at
Phone: +43 1 503 19 63 - 0

With best regards,

SIGNATURE INFORMATION	Signatory	Herbert Leitold
	Date/Time-UTC	2026-06-26T20:22:54+02:00
	Verification	Information about the verification of the electronic signature can be found at: https://www.signaturpruefung.gv.at

Herbert Leitold, Director

General audit information

Identification of the conformity assessment body (CAB) and assessment organization acting as ETSI auditor
• A-SIT, Secure Information Technology Center – Austria, Seidlgasse 22/9, 1030 Wien, Austria, registered under association registration number ZVR: 948166612 • Accredited by Akkreditierung Austria under registration ID 0929[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): Generali Versicherung AG • 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://akkreditierung-austria.gv.at/ (search for “A-SIT” or “0929”)

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):	GLOBALTRUST operated by e-commerce monitoring GmbH, Lamezanstraße 4-8, 1230 Wien, Austria, registered under “Handelsgericht Wien, Company registration number FN 224536 a”

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:	none, as audit was a period of time audit
Audit dates:	2026-04-28 (remote) 2026-06-09 (remote)
Audit location:	e-commerce monitoring GmbH (c/o AUSTRIA CARD-Plastikkarten und Ausweissysteme Gesellschaft m.b.H.), Lamezanstraße 4-8, 1230 Wien, Austria (office location)

Root 1: GLOBALTRUST 2015

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 V3.2.1 (2026-01) 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 2.2.6 • Network and Certificate System Security Requirements, version 2.0.5 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:

- GLOBALTRUST Certificate Policy (OID-Number: 1.2.40.0.36.1.1.8.1)

Version	Release Date	Effective from	Effective until
Version 3.3	2024-10-22	2024-10-22	

- GLOBALTRUST Certificate Practice Statement (OID-Number: 1.2.40.0.36.1.2.3.1)

Version	Release Date	Effective from	Effective until
Version 3.0b	2024-02-16	2024-02-16	2025-04-29
Version 3.0c	2025-03-25	2025-04-30	

- GLOBALTRUST Company Certificate Practice Statement (OID-Number: 1.2.40.0.36.1.1.999.999)

Version	Release Date	Effective from	Effective until
Version 1.0d	2024-02-19	2024-02-19	

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

Findings with regard to ETSI EN 319 401:

7.11 Business continuity management

Test plans for disaster recovery and crisis management should be improved and implemented precisely (the last test of the restart and recovery procedures after a disaster was more than one year ago). [REQ-7.11.2-06, REQ-7.11.3-03]

7.14 Supply chain

Documentation and implementation of the register of suppliers and their agreements shall be improved. [REQ-7.14.3-11, REQ-7.14.3-12]

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

Findings with regard to ETSI EN 319 411-2:
None.

Findings with regard to Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates:
5.7.1.2 Mass Revocation Plans:

There is no assertion to a mass revocation plan in section 5.7.1 of the “GLOBALTRUST Certificate Policy, version 3.3”
This will be fixed in “GLOBALTRUST Certificate Policy, version 3.3a”

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
C=AT ST=Wien L=Wien O=e-commerce monitoring GmbH OU=GLOBALTRUST Certification Service CN=GLOBALTRUST 2015	416B1F9E84E74C1D19B23D8D7191C6AD81246E641601F599132729F507BEB3CC	ETSI EN 319 411-1 V1.5.1, policy EVCP ETSI EN 319 411-2 V2.6.1, policy QEVCP-w

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
C=AT ST=Wien L=Wien O=e-commerce monitoring GmbH CN=GLOBALTRUST 2015 SERVER EV 2	3A014BEF9DE8E25AE4A685A5CA351EDD2B110EB8CDE33E17B829509D78FC5E4A	ETSI EN 319 411-1 V1.5.1, EVCP
C=AT ST=Wien L=Wien O=e-commerce monitoring GmbH OU=GLOBALTRUST Certification Service CN=GLOBALTRUST 2015 SERVER QUALIFIED 1	4B9235A7FEA69307129E842F392BF28E98C6F6084660ABC44855654FA5099805	ETSI EN 319 411-2 V2.6.1, QEVCP-w (including all EVCP requirements)
C=AT ST=Wien L=Wien O=e-commerce monitoring GmbH OU=GLOBALTRUST Certification Service CN=GLOBALTRUST 2015 SERVER QUALIFIED EV 1	23EA405BB51D89CA5B67504C0F7193FA51B77C831774094D59937503FF716369	ETSI EN 319 411-2 V2.6.1, QEVCP-w (including all EVCP requirements)

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

Root 2: GLOBALTRUST 2020

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 V3.2.1 (2026-01) 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 2.2.6 • Network and Certificate System Security Requirements, version 2.0.5 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:

- GLOBALTRUST Certificate Policy (OID-Number: 1.2.40.0.36.1.1.8.1)

Version	Release Date	Effective from	Effective until
Version 3.3	2024-10-22	2024-10-22	

- GLOBALTRUST Certificate Practice Statement (OID-Number: 1.2.40.0.36.1.2.3.1)

Version	Release Date	Effective from	Effective until
Version 3.0b	2024-02-16	2024-02-16	2025-04-29
Version 3.0c	2025-03-25	2025-04-30	

- GLOBALTRUST Company Certificate Practice Statement (OID-Number: 1.2.40.0.36.1.1.999.999)

Version	Release Date	Effective from	Effective until
Version 1.0d	2024-02-19	2024-02-19	

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

Findings with regard to ETSI EN 319 401:

7.11 Business continuity management

Test plans for disaster recovery and crisis management should be improved and implemented precisely (the last test of the restart and recovery procedures after a disaster was more than one year ago). [REQ-7.11.2-06, REQ-7.11.3-03]

7.14 Supply chain

Documentation and implementation of the register of suppliers and their agreements shall be improved. [REQ-7.14.3-11, REQ-7.14.3-12]

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

Findings with regard to ETSI EN 319 411-2:
None.

Findings with regard to Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates:
5.7.1.2 Mass Revocation Plans:

There is no assertion to a mass revocation plan in section 5.7.1 of the “GLOBALTRUST Certificate Policy, version 3.3”
This will be fixed in “GLOBALTRUST Certificate Policy, version 3.3a”

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
C=AT O=e-commerce monitoring GmbH CN=GLOBALTRUST 2020	9A296A5182D1D451A2E37F439B74DAAFA267523329F90F9A0D2007C334E23C9A	ETSI EN 319 411-1 V1.5.1, policy EVCP ETSI EN 319 411-2 V2.6.1, policy QEVCP-w

Table 3: Root-CA 2 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
C=AT O=e-commerce monitoring GmbH CN=GLOBALTRUST 2020 SERVER EV 1	A5B27D844A0ECB68F1D065723202A2F07C667DE96B84E68A9AF234669397D6C4	ETSI EN 319 411-1 V1.5.1, EVCP
C=AT O=e-commerce monitoring GmbH CN=GLOBALTRUST 2020 SERVER QUALIFIED EV 1	FE95A24E7F94978E58D99350AB7AB789774A987CD25187C128C191D207523BB1	ETSI EN 319 411-2 V2.6.1, QEVCP-w (including all EVCP requirements)

Table 4: Sub-CAs issued by the Root-CA 2 or its Sub-CAs in scope of the audit

Modifications record

Version	Issuing Date	Changes
Version 1	2026-06-26	Initial attestation

End of the audit attestation letter.