TLS BR Audit Attestation for

A-Trust GmbH

Reference: VIG-25-093-TLS-BR

"Wien, 2026-03-11"

To whom it may concern,

This is to confirm that "A-SIT, Secure Information Technology Center – Austria" has audited the CAs of the "A-Trust GmbH" without critical findings.

This present Audit Attestation Letter is registered under the unique identifier number "VIG-25-093-TLS-BR" covers multiple Root-CAs and consists of 13 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	2026-03-11T21:10:27+01:00
	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 f) knowledge of security policies and controls.

[1] https://akkreditierung-austria.gv.at/ (search for “A-SIT” or “0929”)

- 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):	A-Trust GmbH, Landstraßer Hauptstraße 1b, E02, 1030 Wien, Austria, registered under company registration number FN 195738a

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:	2024-12-15 to 2025-12-14
Point in time date:	none, as audit was a period of time audit
Audit dates:	2026-01-26 (on site) 2026-02-25 (remote)
Audit location:	A-Trust GmbH, Landstraßer Hauptstraße 1b, E02, 1030 Wien, Austria (office location)

Root 1: A-Trust-Root-07

Standards considered:	European Standards: • ETSI EN 319 411-1 V1.5.1 (2025-04) • ETSI EN 319 401 V3.1.1 (2024-06) CA Browser Forum Requirements: • Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, version 2.2.1 • 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:

- A-Trust PKI Disclosure Statement (PDS), version 1.6, as of 2024-10-24
- A-Trust Certificate Practice Statement for a.sign SSL advanced and a.sign SSL qualified certificates, version 2.6, as of 2025-05-14
- A-Trust Certificate Practice Statement for a.sign SSL advanced and a.sign SSL qualified certificates, version 2.6.1, as of 2026-01-26

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

Findings with regard to ETSI EN 319 401:
None

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 Certificates:
5.7.1.2 Mass Revocation Plans:

There is no assertion to a mass revocation plan in section 5.7.1 of the combined CP/CPS “A-Trust Certificate Practice Statement for a.sign SSL advanced and a.sign SSL qualified certificates, version 2.6”
This is fixed in “A-Trust Certificate Practice Statement for a.sign SSL advanced and a.sign SSL qualified certificates, version 2.6.1”

All non-conformities have been closed before the issuance of this attestation.

This Audit Attestation also covers the following incidents as described in the following.

- Bug 1972887, A-Trust: TLS non-compliance detected during linter implementation: https://bugzilla.mozilla.org/show_bug.cgi?id=1972887

The remediation measures taken by A-Trust GmbH as described on Bugzilla (see link above) have been checked by the auditors and properly addressed the incident.

Distinguished Name	SHA-256 fingerprint	Applied policy
C = AT O = A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH OU = A-Trust-Root-07 CN = A-Trust-Root-07	8AC552AD577E37AD2C6808D72AA331D6A96B4B3FEBFF34CE9BC0578E08055EC3	ETSI EN 319 411-1 V1.5.1, policy OVCP

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 O = A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH OU = a-sign-SSL-07 CN = a-sign-SSL-07	789E625AE7BF6B604DF93CA8EB99A30B0378A8F82A67562C66D8013926121529	ETSI EN 319 411-1 V1.5.1, OVCP

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

Root 2: A-Trust-Root-09

Standards considered:	European Standards: • ETSI EN 319 411-1 V1.5.1 (2025-04) • ETSI EN 319 401 V3.1.1 (2024-06) CA Browser Forum Requirements: • Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, version 2.2.1 • 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:

- A-Trust PKI Disclosure Statement (PDS), version 1.6, as of 2024-10-24
- A-Trust Certificate Practice Statement for a.sign SSL advanced and a.sign SSL qualified certificates, version 2.6, as of 2025-05-14
- A-Trust Certificate Practice Statement for a.sign SSL advanced and a.sign SSL qualified certificates, version 2.6.1, as of 2026-01-26

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

Findings with regard to ETSI EN 319 401:
None

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 Certificates:
5.7.1.2 Mass Revocation Plans:

There is no assertion to a mass revocation plan in section 5.7.1 of the combined CP/CPS “A-Trust Certificate Practice Statement for a.sign SSL advanced and a.sign SSL qualified certificates, version 2.6”
This is fixed in “A-Trust Certificate Practice Statement for a.sign SSL advanced and a.sign SSL qualified certificates, version 2.6.1”

All non-conformities have been closed before the issuance of this attestation.

This Audit Attestation also covers the following incidents as described in the following.

- Bug 1972887, A-Trust: TLS non-compliance detected during linter implementation: https://bugzilla.mozilla.org/show_bug.cgi?id=1972887

The remediation measures taken by A-Trust GmbH as described on Bugzilla (see link above) have been checked by the auditors and properly addressed the incident.

Distinguished Name	SHA-256 fingerprint	Applied policy
C = AT O = A-Trust GmbH OU = A-Trust-Root-09 CN = A-Trust-Root-09	7A38F708A35A31E42E1CF3220F9A2D273E7666354618B2464657D43D8E77ADC2	ETSI EN 319 411-1 V1.5.1, policy OVCP

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 = A-Trust GmbH OU = a-sign-SSL-09 CN = a-sign-SSL-09	D341A34A41EEF9C54F9849095FAE8E73C9A9CDC39511C3E142506C17245F0A25	ETSI EN 319 411-1 V1.5.1, OVCP

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

Root 3: A-Trust-Root-10

Standards considered:	European Standards: • ETSI EN 319 411-1 V1.5.1 (2025-04) • ETSI EN 319 401 V3.1.1 (2024-06) CA Browser Forum Requirements: • Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, version 2.2.1 • 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:

- A-Trust PKI Disclosure Statement (PDS), version 1.6, as of 2024-10-24
- A-Trust Certificate Practice Statement for a.sign SSL advanced and a.sign SSL qualified certificates, version 2.6, as of 2025-05-14
- A-Trust Certificate Practice Statement for a.sign SSL advanced and a.sign SSL qualified certificates, version 2.6.1, as of 2026-01-26

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

Findings with regard to ETSI EN 319 401:
None

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 Certificates:
5.7.1.2 Mass Revocation Plans:

There is no assertion to a mass revocation plan in section 5.7.1 of the combined CP/CPS “A-Trust Certificate Practice Statement for a.sign SSL advanced and a.sign SSL qualified certificates, version 2.6”
This is fixed in “A-Trust Certificate Practice Statement for a.sign SSL advanced and a.sign SSL qualified certificates, version 2.6.1”

All non-conformities have been closed before the issuance of this attestation.

This Audit Attestation also covers the following incidents as described in the following.

- Bug 1972887, A-Trust: TLS non-compliance detected during linter implementation: https://bugzilla.mozilla.org/show_bug.cgi?id=1972887

The remediation measures taken by A-Trust GmbH as described on Bugzilla (see link above) have been checked by the auditors and properly addressed the incident.

Distinguished Name	SHA-256 fingerprint	Applied policy
C = AT O = A-Trust GmbH CN = A-Trust-Root-10	3F1F25C7326D48E5FE501F1EDE5CE654317D0D06EDBEE93A001FFF4D8C7EB091	ETSI EN 319 411-1 V1.5.1, policy OVCP

Table 5: Root-CA 3 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 = A-Trust GmbH CN = a-sign-SSL-10	0B93CFA8918A56C98422FAEA6850C7ABCF1B683AAD6908BC9FD8352A4A7A1B75	ETSI EN 319 411-1 V1.5.1, OVCP

Table 6: Sub-CAs issued by the Root-CA 3 or its Sub-CAs in scope of the audit

Modifications record

Version	Issuing Date	Changes
Version 1	2026-03-11	Initial attestation

End of the audit attestation letter.