

Standard Audit Attestation for A-Trust GmbH

Reference: VIG-25-093

“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” covers multiple Root-CAs and consists of 18 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,



**placeholder for the
electronic signature
NR: 1**

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 0929¹ 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	
<ul style="list-style-type: none"> • 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:	<input type="checkbox"/> Point in time audit <input type="checkbox"/> Period of time, after x month of CA operation <input checked="" type="checkbox"/> 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:	<p>European Standards:</p> <ul style="list-style-type: none">• 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)• ETSI EN 319 421 V1.3.1 (2025-07)• ETSI TS 119 431-1 V1.3.1 (2024-12)• ETSI TS 119 461 V2.1.1 (2025-02)• ETSI TS 119 495 V1.7.1 (2024-07) <p>CA Browser Forum Requirements:</p> <ul style="list-style-type: none">• Guidelines for the Issuance and Management of Extended Validation Certificates, version 2.0.1• 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 <p>For the Trust Service Provider Conformity Assessment:</p> <ul style="list-style-type: none">• 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 Zertifikatsrichtlinie (Certificate Policy) für qualifizierte Zertifikate, version 1.3, as of 2025-12-01
- A-Trust Zertifizierungsrichtlinie (Certificate Practice Statement) für qualifizierte Zertifikate, version 1.3, as of 2025-12-01
- 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:

Audit Attestation "VIG-25-093", issued to "A-Trust GmbH"

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, policies NCP+, OVCP ETSI EN 319 411-2 V2.6.1, policies QCP-n-qscd, QCP-l-qscd, 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 O = A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH OU = a-sign-Premium-Enc-07 CN = a-sign-Premium-Enc-07	81687160EEBE0D05637113F132BEE01D2EC2BDA27073093DFC27944811259973	ETSI EN 319 411-1 V1.5.1, NCP+
C = AT O = A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH OU = a-sign-premium-mobile-07 CN = a-sign-premium-mobile-07	0F522765DB829D9AE9E6AF380A72443C9688B098BFBA2CEE17322F848BAD0511	ETSI EN 319 411-2 V2.6.1, QCP-n-qscd
C = AT O = A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH OU = a-sign-premium-mobile-seal-07 CN = a-sign-premium-mobile-seal-07	8EE2F003E3ADD19F76DB49247E4A3F3272316946124A4E520D78E43615D4CE34	ETSI EN 319 411-2 V2.6.1, QCP-l-qscd
C = AT O = A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH OU = a-sign-premium-seal-07 CN = a-sign-premium-seal-07	87E75615D6227A282528C13D3378F1AA53DFEF4ABFA1FB8ECCD6529DCADB5A1	ETSI EN 319 411-2 V2.6.1, QCP-l-qscd
C = AT O = A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH OU = a-sign-Premium-Sig-07 CN = a-sign-Premium-Sig-07	17D13622F3A190F41C0E9BE2BCC271B3E3686400B15A4BCF23F69DAA5DCE9E66	ETSI EN 319 411-2 V2.6.1, QCP-n-qscd

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
C = AT O = A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH OU = a-sign-SSL-EV-07a CN = a-sign-SSL-EV-07a	C76AD81BD29B66E24C8BA239267DDE6A0D9BB9C8867864733DA8A9C7F42AFC57	ETSI EN 319 411-2 V2.6.1, QEVCP-w
C = AT O = A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH OU = a-sign-premium-timestamping-07 CN = a-sign-premium-timestamping-07	395D12775B6EF12CC55FA28BB8991A6673A3D101751901CBCA4DC962213E7BAE	ETSI EN 319 421 V1.3.1

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:	<p>European Standards:</p> <ul style="list-style-type: none">• 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)• ETSI EN 319 421 V1.3.1 (2025-07)• ETSI TS 119 431-1 V1.3.1 (2024-12)• ETSI TS 119 461 V2.1.1 (2025-02)• ETSI TS 119 495 V1.7.1 (2024-07) <p>CA Browser Forum Requirements:</p> <ul style="list-style-type: none">• Guidelines for the Issuance and Management of Extended Validation Certificates, version 2.0.1• 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 <p>For the Trust Service Provider Conformity Assessment:</p> <ul style="list-style-type: none">• 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 Zertifikatsrichtlinie (Certificate Policy) für qualifizierte Zertifikate, version 1.3, as of 2025-12-01
- A-Trust Zertifizierungsrichtlinie (Certificate Practice Statement) für qualifizierte Zertifikate, version 1.3, as of 2025-12-01
- 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, policies NCP+, OVCP ETSI EN 319 411-2 V2.6.1, policies QCP-n-qscd, QCP-l-qscd, 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 = A-Trust GmbH OU = a-sign-Premium-Enc-09 CN = a-sign-Premium-Enc-09	8A07DED8FC86B9A28A2BF84547A8A47946775494CC42263AF9DBF0F1958492E4	ETSI EN 319 411-1 V1.5.1, NCP+
C = AT O = A-Trust GmbH OU = a-sign-premium-mobile-09 CN = a-sign-premium-mobile-09	2F64DE538D980F3B3E811EC946FB7D323EDB7047A32CB138CA9442EBBCE7349F	ETSI EN 319 411-2 V2.6.1, QCP-n-qscd
C = AT O = A-Trust GmbH OU = a-sign-premium-mobile-seal-09 CN = a-sign-premium-mobile-seal-09	417B27A708669DEFCA9E90F3675455A82C2BE69929E32A2D2F9F55648BA871A9	ETSI EN 319 411-2 V2.6.1, QCP-l-qscd
C = AT O = A-Trust GmbH OU = a-sign-premium-seal-09 CN = a-sign-premium-seal-09	66FC1F07F506BB00938AA3B20FED680FAAD51226A2CB6B3E86AD60A0FA921A68	ETSI EN 319 411-2 V2.6.1, QCP-l-qscd
C = AT O = A-Trust GmbH OU = a-sign-Premium-Sig-09 CN = a-sign-Premium-Sig-09	B900E04138E0555147C98B728B2DF0028FCACCE798F10CC8FA4A4A9E56532CD9	ETSI EN 319 411-2 V2.6.1, QCP-n-qscd
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

C = AT O = A-Trust GmbH OU = a-sign-SSL-EV-09 CN = a-sign-SSL-EV-09	9AAD0918FBE3D382DB7E0EBFFEEAB4F380C9A9B4F55492F945C7F3C9D7B28308	ETSI EN 319 411-2 V2.6.1, QEVCP-w
C = AT O = A-Trust GmbH OU = a-sign-premium-timestamping-09 CN = a-sign-premium-timestamping-09	840DE0FA36DF2C715E7459EF854E5C6AE32D73081A31DEAD6A6D48A6A060ACCB	ETSI EN 319 421 V1.3.1
C = AT O = A-Trust GmbH OU = EU-Identity-mobile-09 CN = EU-Identity-mobile-09	6BD15368EA1589E8C84121A540DE96D8C4785085D326EE028663C223C24087C0	ETSI EN 319 411-2 V2.6.1, QCP-n-qscd

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:	<p>European Standards:</p> <ul style="list-style-type: none">• 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)• ETSI EN 319 421 V1.3.1 (2025-07)• ETSI TS 119 431-1 V1.3.1 (2024-12)• ETSI TS 119 461 V2.1.1 (2025-02)• ETSI TS 119 495 V1.7.1 (2024-07) <p>CA Browser Forum Requirements:</p> <ul style="list-style-type: none">• Guidelines for the Issuance and Management of Extended Validation Certificates, version 2.0.1• 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 <p>For the Trust Service Provider Conformity Assessment:</p> <ul style="list-style-type: none">• 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 Zertifikatsrichtlinie (Certificate Policy) für qualifizierte Zertifikate, version 1.3, as of 2025-12-01
- A-Trust Zertifizierungsrichtlinie (Certificate Practice Statement) für qualifizierte Zertifikate, version 1.3, as of 2025-12-01
- 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, policies NCP+, OVCP ETSI EN 319 411-2 V2.6.1, policies QCP-n-qscd, QCP-l-qscd, QEVCP-w

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-Premium-Enc-10	C5B06D7A1F37CB06B6F1C29ED54B0164DB3440ABDA6A174E3DED6B4DE7089C57	ETSI EN 319 411-1 V1.5.1, NCP+
C = AT O = A-Trust GmbH CN = a-sign-premium-mobile-10	50FDED1CC8DF74C813200CA71E6E3B0856E7E81D6334FA93B70AF53537DEAC40	ETSI EN 319 411-2 V2.6.1, QCP-n-qscd
C = AT O = A-Trust GmbH CN = a-sign-premium-mobile-seal-10	3B4BFBB73FE7270ECA451B5CA73DBF693292F0FAEA68BDB5C9831799BDFBB4D0	ETSI EN 319 411-2 V2.6.1, QCP-l-qscd
C = AT O = A-Trust GmbH CN = a-sign-Premium-Once-10	C2308EA574134D78B5F41CEEFAA5DA3FE9E7CCF7E9E5B9C1C2D23D61B8EFA6E1	ETSI EN 319 411-2 V2.6.1, QCP-n-qscd
C = AT O = A-Trust GmbH CN = a-sign-premium-seal-10	9923037B3185575370305D1B93815DE0A508F3FC3EF4F159F782C02F91534004	ETSI EN 319 411-2 V2.6.1, QCP-l-qscd
C = AT O = A-Trust GmbH CN = a-sign-Premium-Sig-10	437651ABEA4835D0ADC583131B6EE6D7462BA770B04F5BCBBA6082273FD109E7	ETSI EN 319 411-2 V2.6.1, QCP-n-qscd
C = AT O = A-Trust GmbH CN = a-sign-premium-timestamping-10	E7C65D949023E16997D4BA13A6F7CCB4C72FBCBCB172AA79B3B75D72D4F82B3A	ETSI EN 319 421 V1.3.1
C = AT O = A-Trust GmbH CN = a-sign-SSL-10	0B93CFA8918A56C98422FAEA6850C7ABCF1B683AAD6908BC9FD8352A4A7A1B75	ETSI EN 319 411-1 V1.5.1, OVCP
C = AT O = A-Trust GmbH CN = a-sign-SSL-EV-10	997D1E997512A8A320CDA2C24DB9D2AAB468D283C8A430136507A49FBEBCC705	ETSI EN 319 411-2 V2.6.1, QEVCP-w

C = AT O = A-Trust GmbH CN = EU-Identity-mobile-10	97DA26F808DBED28ECD9A7193A5B86969F6468012A58CFE97D44CE07A4D9F16B	ETSI EN 319 411-2 V2.6.1, QCP-n-qscd
--	--	---

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

Root 4: a-sign-Root-SMIME-01

Standards considered:	<p>European Standards:</p> <ul style="list-style-type: none">• ETSI EN 319 411-1 V1.5.1 (2025-04)• ETSI TS 119 411-6 V1.1.1 (2023-08)• ETSI EN 319 401 V3.1.1 (2024-06) <p>CA Browser Forum Requirements:</p> <ul style="list-style-type: none">• Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, version 1.0.12• Network and Certificate System Security Requirements, version 2.0.5 <p>For the Trust Service Provider Conformity Assessment:</p> <ul style="list-style-type: none">• 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 Certificate Practice Statement for a.sign Mail certificates, version 1.1, as of 2025-10-23

No major or minor non-conformities have been identified during the audit.

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-sign-Root-SMIME-01	7B06AE19E4085CB0B1A24BE8677BCD6CF40A93E5B660500021D6E38243EB6EC4	ETSI EN 319 411-1 V1.5.1, policies LCP, NCP, NCP+

Table 7: Root-CA 4 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-mail-01	CA09C1168A1D4469FFBBA1D59300FC476B701BA31EDED841DD47CDF312990E79	ETSI EN 319 411-1 V1.5.1, policies LCP, NCP, NCP+ ETSI TS 119 411-6 V1.1.1, Mailbox-validated Multipurpose (2.23.140.1.5.1.2) ETSI TS 119 411-6 V1.1.1, Mailbox-validated Strict (2.23.140.1.5.1.3) ETSI TS 119 411-6 V1.1.1, Organization-validated Multipurpose (2.23.140.1.5.2.2) ETSI TS 119 411-6 V1.1.1, Organization-validated Strict (2.23.140.1.5.2.3) ETSI TS 119 411-6 V1.1.1, Sponsor-validated Multipurpose (2.23.140.1.5.3.2) ETSI TS 119 411-6 V1.1.1, Sponsor-validated Strict (2.23.140.1.5.3.3) ETSI TS 119 411-6 V1.1.1, Individual-validated Multipurpose (2.23.140.1.5.4.2) ETSI TS 119 411-6 V1.1.1, Individual-validated Strict (2.23.140.1.5.4.3)

Table 8: Sub-CAs issued by the Root-CA 4 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.