

**Zentrum für sichere Informationstechnologie – Austria
Secure Information Technology Center – Austria**



Seidlgasse 22 / 9, 1030 Wien
Tel.: +43 1 503 19 63–0
Fax: +43 1 503 19 63–66

Inffeldgasse 16a, 8010 Graz
Tel.: +43 316 873-5514
Fax: +43 316 873-5520

<https://www.a-sit.at>

DVR: 1035461

E-Mail: office@a-sit.at
ZVR: 948166612

UID: ATU60778947

**Audit Attestation for
A-Trust Gesellschaft für Sicherheitssysteme im
elektronischen Datenverkehr GmbH**

Reference: VIG-22-089

Vienna, 2023-02-23

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 Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH” without critical findings.

This present Audit Attestation Letter is registered under the unique identifier number “VIG-22-089” and consists of << 8 >> 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: 0001

Herbert Leitold, Director

This attestation is based on the template version 2.9 as of 2022-04-04, that was approved for use by ACAB-c.



<p>Identification of the conformity assessment body (CAB) and assessment organization acting as ETSI auditor:</p>	<ul style="list-style-type: none"> • A-SIT, Secure Information Technology Center – Austria¹, Seidlgasse 22/9, 1030 Wien, Austria registered under association registration number ZVR: 948166612 • Accredited by Akkreditierung Austria under registration ID 0929² for the certification of trust services according to “EN ISO/IEC 17065:2012” and “ETSI EN 319 403-1 V2.3.1 (2020-06)” respectively. • Insurance Carrier (BRG section 8.2): Generali Versicherung AG • Third-party affiliate audit firms involved in the audit: none.
<p>Identification and qualification of the audit team:</p>	<ul style="list-style-type: none"> • Number of team members: 1 Lead Auditor, 1 Auditor • 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 <ol style="list-style-type: none"> 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: <ol style="list-style-type: none"> 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;

¹ in the following termed shortly “CAB“

² <https://akkreditierung-austria.gv.at/> (search for “A-SIT” or “0929”)

	<p>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.</p> <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> 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.
<p>Identification and qualification of the reviewer performing audit quality management:</p>	<ul style="list-style-type: none"> • Number of Reviewers/Audit Quality Managers involved independent from the audit team: 1 Reviewer • 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.
<p>Identification of the CA / Trust Service Provider (TSP):</p>	<p>A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH, Landstraßer Hauptstraße 1b, E02, 1030 Wien, Austria registered under Company registration number FN 195738a</p>
<p>Type of audit:</p>	<p><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</p>

Audit period covered for all policies:	2021-12-15 to 2022-12-14
Point in time date:	none, as audit was pot audit
Audit dates:	2023-01-23 (on site)
Audit location:	A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH, Landstraßer Hauptstraße 1b, E02, 1030 Wien, Austria (office location) Both data centres used by A-Trust, located in Vienna, Austria

Standards considered:	<p>European Standards:</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> ETSI EN 319 411-2, V2.4.1 (2021-11) <input checked="" type="checkbox"/> ETSI EN 319 411-1, V1.3.1 (2021-05) <input checked="" type="checkbox"/> ETSI EN 319 401, V2.3.1 (2021-05) <input checked="" type="checkbox"/> ETSI EN 319 421, V1.1.1 (2016-03) <p>CA Browser Forum Requirements:</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> EV SSL Certificate Guidelines, version 1.8.0 <input checked="" type="checkbox"/> Baseline Requirements, version 1.8.6 <p>For the Trust Service Provider Conformity Assessment:</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> ETSI EN 319 403 V2.3.1 (2020-06) <input checked="" type="checkbox"/> ETSI TS 119 403-2 V1.2.4 (2020-11)
-----------------------	--

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

1. A-Trust PKI Disclosure Statement (PDS), version 1.4, as of 2022-05-02
2. A-Trust Anwendungsvorgabe (Certificate Policy) für qualifizierte Zertifikate a.sign premium (a-sign-premium CP), version 1.4.3, as of 2022-11-22
3. A-Trust Zertifizierungsrichtlinie (Certificate Practice Statement) für qualifizierte Zertifikate a.sign premium (a-sign-premium CPS), version 1.4.6, as of 2022-12-16
4. A-Trust Anwendungsvorgabe (Certificate Policy) für qualifizierte Zertifikate a.sign premium mobile (a-sign-premium-mobile CP), version 1.1.5, as of 2022-11-22
5. A-Trust Zertifizierungsrichtlinie (Certificate Practice Statement) für qualifizierte Zertifikate a.sign premium mobile (a-sign-premium-mobile CPS), version 1.1.6, as of 2022-11-22
6. A-Trust Anwendungsvorgabe (Certificate Policy) für qualifizierte Zertifikate a.sign premium mobile seal (a-sign-premium-mobile-seal CP), version 1.0.3, as of 2022-11-22
7. A-Trust Anwendungsvorgabe (Certificate Policy) für qualifizierte Zertifikate a.sign premium seal (a-sign-premium-seal CP), version 1.0.2, as of 2022-11-22
8. A-Trust Certificate Practice Statement for a.sign SSL advanced and a.sign SSL qualified certificates (a-sign-ssl & a-sign-ssl-ev CPS), version 2.2, as of 2022-11-22
9. A-Trust Anwendungsvorgabe (Certificate Policy) für qualifizierte Zeitstempel (a-sign-premium-timestamping CP), version 1.0.4, as of 2022-12-14
10. A-Trust Zertifizierungsrichtlinie (Certificate Practice Statement) für qualifizierte Zeitstempel (a-sign-premium-timestamping CPS), version 1.0.4, as of 2022-12-12

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

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

Distinguished Name	SHA-256 fingerprint	Applied policy and OID
CN = A-Trust-Root-07 OU = A-Trust-Root-07 O = A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH C = AT	8AC552AD577E37AD2C6808D72AA331D6A96B4B3FEBFF34CE9BC0578E08055EC3	ETSI EN 319 411-1 V1.3.1, policies NCP+, OVCP ETSI EN 319 411-2 V2.4.1, policies QCP-n-qscd, QCP-l-qscd, QEVCP-w

Table 1: Root-CA 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 and OID	EKU
CN = a-sign-Premium-Enc-07 OU = a-sign-Premium-Enc-07 O = A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH C = AT	81687160EEBE0D05637113F132BEE01D2EC2BDA27073093DFC27944811259973	ETSI EN 319 411-1 V1.3.1, NCP+	not defined
CN = a-sign-premium-mobile-07 OU = a-sign-premium-mobile-07 O = A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH C = AT	0F522765DB829D9AE9E6AF380A72443C9688B098BFBA2CEE17322F848BAD0511	ETSI EN 319 411-2 V2.4.1, QCP-n-qscd	not defined
CN = a-sign-premium-mobile-seal-07 OU = a-sign-premium-mobile-seal-07 O = A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH C = AT	8EE2F003E3ADD19F76DB49247E4A3F3272316946124A4E520D78E43615D4CE34	ETSI EN 319 411-2 V2.4.1, QCP-l-qscd	not defined
CN = a-sign-premium-seal-07 OU = a-sign-premium-seal-07 O = A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH C = AT	87E75615D6227A282528C13D3378F1AA53DFEF4ABFA1FB8ECCD6529DCADB5A1	ETSI EN 319 411-2 V2.4.1, QCP-l-qscd	not defined

This attestation is based on the template version 2.9 as of 2022-04-04, that was approved for use by ACAB-c.

CN = a-sign-Premium-Sig-07 OU = a-sign-Premium-Sig-07 O = A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH C = AT	17D13622F3A190F41C0E9BE2BCC271B3E3686400B15A4BCF23F69DAA5DCE9E66	ETSI EN 319 411-2 V2.4.1, QCP-n-qscd	not defined
CN = a-sign-SSL-07 OU = a-sign-SSL-07 O = A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH C = AT	789E625AE7BF6B604DF93CA8EB99A30B0378A8F82A67562C66D8013926121529	ETSI EN 319 411-1 V1.3.1, OVCP	not defined
CN = a-sign-SSL-EV-07a OU = a-sign-SSL-EV-07a O = A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH C = AT	C76AD81BD29B66E24C8BA239267DDE6A0D9BB9C8867864733DA8A9C7F42AFC57	ETSI EN 319 411-2 V2.4.1, QEVCP-w	not defined
CN = a-sign-premium-timestamping-07 OU = a-sign-premium-timestamping-07 O = A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH C = AT	395D12775B6EF12CC55FA28BB8991A6673A3D101751901CBCA4DC962213E7BAE	ETSI EN 319 421 V1.1.1	not defined

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

Modifications record

Version	Issuing Date	Changes
Version 1	2023-02-23	Initial attestation

End of the audit attestation letter.