Key Generation Ceremony Report for

A-Trust GmbH

Reference: VIG-25-085-KeyGen-SMIME

"Wien, 2025-12-29"

To whom it may concern,

This is to confirm that "A-SIT, Secure Information Technology Center – Austria" has audited a key generation ceremony of "A-Trust GmbH". The ceremony was followed in its entirety, completed successfully and without non-conformities in accordance with the applicable requirements.

This Key Generation Ceremony Report is registered under the unique identifier number "VIG-25-085-KeyGen-SMIME" and consists of 7 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	2025-12-29T15:20:43+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

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

Type of audit:	Point in time audit of key and certificate generation ceremony
Point in time date:	2025-08-13 (Root-CA) 2025-10-28 (Sub-CA)
Audit location:	A-Trust GmbH, Landstraßer Hauptstraße 1b, E02, 1030 Wien, Austria (remote)

A key generation script has been prepared in accordance with the normative requirements and with the rules stated in the policy and practice statement documents of the certification service provider. During generation of the keys and certificates, this script has been followed.

In particular:

- The key generation ceremony was performed by 2 individuals of the CA Owner acting in Trusted Roles
- The key generation ceremony was observed in physical presence by 1 individual of the CA Owner

- The key generation ceremony was observed remotely by 2 individuals of the Conformity Assessment Body with independence from the CA Owner
- Principles of multiparty control and split knowledge were observed.
- The CA key pairs were generated in a physically secured environment as described in the CA’s CPS.
- The CA key pairs were generated within cryptographic modules meeting the applicable technical and business requirements as disclosed in the CA’s CPS.
- CA key pair generation activities were logged.
- Effective controls were maintained to provide reasonable assurance that the private key was generated and protected in conformance with the procedures described in its CPS and the Key Generation Script.

The key generation ceremony has been witnessed remotely.

No non-conformities have been identified during the audit.

Root 1: a-sign-Root-SMIME-01

Standards considered: (Only with regard to key generation and key protection requirements)	European Standards: • ETSI TS 119 411-6 V1.1.1 (2023-08) • 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 S/MIME Certificates, version 1.0.12 • 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 Certificate Practice Statement for a.sign SSL advanced, a.sign SSL qualified and a.sign Mail certificates, version 2.6, as of 2025-05-14
- A-Trust Certificate Practice Statement for a.sign Mail certificates, version 1.1, as of 2025-10-23

This report covers the generation of the key pairs and certificates of the Root-CA and Sub-CAs referenced in the following tables.

Distinguished Name	SHA-256 fingerprint of the certificate	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+
	SHA-256 fingerprint of Subject Public Key Info	
	BC0322C022AB7F950B9C320FE6139CFCE3A894847640B90E5FE448D0471A1163	

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 of the certificate SHA-256 fingerprint of Subject Public Key Info	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)
	9CD0131F5B86FAF31F74BAA3ED8FF7762C7C02FE72A823EBA38503DB4DE4D114	

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

Modifications record

Version	Issuing Date	Changes
Version 1	2025-12-29	Initial attestation

End of the audit attestation letter.