

# **SMIME BR Audit Attestation for GLOBALTRUST operated by e-commerce monitoring GmbH**

**Reference: VIG-25-035-SMIME-BR**

“Wien, 2025-06-27”

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-25-035-SMIME-BR” covers multiple Root-CAs and consists of 11 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](mailto: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 0929<sup>1</sup> 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;

---

<sup>1</sup> <https://akkreditierung-austria.gv.at/> (search for "A-SIT" or "0929")

<p>e) general knowledge of regulatory requirements relevant to TSPs; and f) knowledge of security policies and controls.</p> <ul style="list-style-type: none"> <li>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.</li> <li>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"> <li>a) has acted as auditor in at least three complete TSP audits;</li> <li>b) has adequate knowledge and attributes to manage the audit process; and</li> <li>c) has the competence to communicate effectively, both orally and in writing.</li> </ul> </li> <li>Special skills or qualifications employed throughout audit: None.</li> <li>Special Credentials, Designations, or Certifications: All members are qualified and registered assessors within the accredited CAB.</li> <li>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.</li> </ul>
--

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:	<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:	2024-04-01 to 2025-03-31
Point in time date:	none, as audit was a period of time audit
Audit dates:	2025-04-29 (on site) 2025-06-26 (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:	<div>European Standards:<ul style="list-style-type: none"><li>ETSI EN 319 411-1 V1.4.1 (2023-10)</li><li>ETSI EN 319 401 V3.1.1 (2024-06)</li><li>ETSI TS 119 411-6 V1.1.1 (2023-08)</li></ul></div> <div>CA Browser Forum Requirements:<ul style="list-style-type: none"><li>Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, version 1.0.8</li><li>Network and Certificate System Security Requirements, version 2.0.3</li></ul></div> <div>For the Trust Service Provider Conformity Assessment:<ul style="list-style-type: none"><li>ETSI EN 319 403-1 V2.3.1 (2020-06)</li><li>ETSI TS 119 403-2 V1.3.1 (2023-03)</li></ul></div>
-----------------------	--

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

- GLOBALTRUST Certificate Policy, version 3.3, as of 2024-10-22 (OID-Number: 1.2.40.0.36.1.1.8.1)
- GLOBALTRUST Certificate Practice Statement, version 3.0c, as of 2025-03-25 (OID-Number: 1.2.40.0.36.1.2.3.1)
- GLOBALTRUST Company Certificate Practice Statement, version 1.0d, as of 2024-02-19 (OID-Number: 1.2.40.0.36.1.1.999.999)

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

Findings with regard to ETSI EN 319 401:

6.3 Information security policy

Documentation of information security policy shall be improved to reflect all changes resulting from the takeover by the new owner. [REQ-6.3-06X]

7.9 Vulnerabilities and Incident management

Documentation of incident response and reporting procedures shall be improved to apply the incident response policy of the new owner. [REQ-7.9.2-06X, REQ-7.9.3-03X]

7.14 Supply chain

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

Findings with regard to ETSI EN 319 411-1:

None.

Findings with regard to ETSI EN 319 411-2:

None.

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.

Audit Attestation "VIG-25-035-SMIME-BR", issued to "GLOBALTRUST operated by e-commerce monitoring GmbH"

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
CN=GLOBALTRUST 2015 O=e-commerce monitoring GmbH OU=GLOBALTRUST Certification Service C=AT ST=Wien L=Wien	416B1F9E84E74C1D19B23D8D7191C6AD81246E641601F599132729F507BEB3CC	ETSI EN 319 411-1 V1.4.1, policies LCP, NCP, NCP+

**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
CN=GLOBALTRUST 2015 CLIENT 1 O=e-commerce monitoring GmbH OU=GLOBALTRUST Certification Service C=AT ST=Wien L=Wien	ED1E061A00B8E0F4C8409C63CBADD21550A4CEB6BB0D678A8A88973DE8ACB86E	ETSI EN 319 411-1 V1.4.1, LCP 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, Sponsor-validated – Multipurpose (2.23.140.1.5.3.2)
CN=GLOBALTRUST 2015 COMPANY CLIENT 1 O=e-commerce monitoring GmbH C=AT ST=Wien L=Wien	EFCF30EFEFD471867EBA62E42ADD6F698243FE315887B9D2486EB84CD2BC3EA1	ETSI EN 319 411-1 V1.4.1, LCP, NCP, NCP+

CN=Deutscher Bundestag 01 O=Deutscher Bundestag C=DE	24582E6A3089A8FF7F223685949CFDBEAB264A71A51C8B117C96F819F96AEEE3	ETSI EN 319 411-1 V1.4.1, LCP, NCP, NCP+ 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 2: Sub-CAs issued by the Root-CA 1 or its Sub-CAs in scope of the audit

Root 2: GLOBALTRUST 2020

Standards considered:	<div>European Standards:<ul style="list-style-type: none"><li>ETSI EN 319 411-1 V1.4.1 (2023-10)</li><li>ETSI EN 319 401 V3.1.1 (2024-06)</li><li>ETSI TS 119 411-6 V1.1.1 (2023-08)</li></ul></div> <div>CA Browser Forum Requirements:<ul style="list-style-type: none"><li>Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, version 1.0.8</li><li>Network and Certificate System Security Requirements, version 2.0.3</li></ul></div> <div>For the Trust Service Provider Conformity Assessment:<ul style="list-style-type: none"><li>ETSI EN 319 403-1 V2.3.1 (2020-06)</li><li>ETSI TS 119 403-2 V1.3.1 (2023-03)</li></ul></div>
-----------------------	--

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

- GLOBALTRUST Certificate Policy, version 3.3, as of 2024-10-22 (OID-Number: 1.2.40.0.36.1.1.8.1)
- GLOBALTRUST Certificate Practice Statement, version 3.0c, as of 2025-03-25 (OID-Number: 1.2.40.0.36.1.2.3.1)
- GLOBALTRUST Company Certificate Practice Statement, version 1.0d, as of 2024-02-19 (OID-Number: 1.2.40.0.36.1.1.999.999)

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

Findings with regard to ETSI EN 319 401:

6.3 Information security policy

Documentation of information security policy shall be improved to reflect all changes resulting from the takeover by the new owner. [REQ-6.3-06X]

7.9 Vulnerabilities and Incident management

Documentation of incident response and reporting procedures shall be improved to apply the incident response policy of the new owner. [REQ-7.9.2-06X, REQ-7.9.3-03X]

7.14 Supply chain

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

Findings with regard to ETSI EN 319 411-1:

None.

Findings with regard to ETSI EN 319 411-2:

None.

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.



Audit Attestation "VIG-25-035-SMIME-BR", issued to "GLOBALTRUST operated by e-commerce monitoring GmbH"

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
CN=GLOBALTRUST 2020 O=e-commerce monitoring GmbH C=AT	9A296A5182D1D451A2E37F439B74DAAFA267523329F90F9A0D2007C334E23C9A	ETSI EN 319 411-1 V1.4.1, policy LCP

**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
CN=GLOBALTRUST 2020 CLIENT 1 O=e-commerce monitoring GmbH C=AT	6DCA83EF586C940A2040ABDD900CAF0E00A014851F7F9C46EBA20BEDCC07BED7	ETSI EN 319 411-1 V1.4.1, LCP 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, Sponsor-validated – Multipurpose (2.23.140.1.5.3.2)
CN=GLOBALTRUST 2020 COMPANY CLIENT 1 O=e-commerce monitoring GmbH C=AT	B868C8A09F1766D3289CE2CAC27488254A7310996C1B049C42C9EADD1A5ED621	ETSI EN 319 411-1 V1.4.1, LCP, NCP, NCP+
CN=Deutscher Bundestag 02 O=Deutscher Bundestag C=DE	7D4065500370F9D657EED83CFBC754BD7898F412FAB1994E92DEB4E3B0483D0E	ETSI EN 319 411-1 V1.4.1, LCP, NCP, NCP+ 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 4: Sub-CAs issued by the Root-CA 2 or its Sub-CAs in scope of the audit**

Audit Attestation "VIG-25-035-SMIME-BR", issued to "GLOBALTRUST operated by e-commerce monitoring GmbH"

### **Modifications record**

<b>Version</b>	<b>Issuing Date</b>	<b>Changes</b>
Version 1	2025-06-27	Initial attestation

**End of the audit attestation letter.**