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

A-SIT

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

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

https://www.a-sit.at

DVR: 1035461 ZVR: 948166612 UID: ATU60778947

SMIME BR Audit Attestation for

GLOBALTRUST operated by e-commerce monitoring GmbH

Reference: VIG-24-034-SMIME-BR

"Wien, 2024-08-28"

To whom it may concern,

This is to confirm that "A-SIT, Secure Information Technology Center – Austria" has audited the CAs of "GLOBALTRUST operated by e-commerce monitoring GmbH" with critical findings.

This present Audit Attestation Letter is registered under the unique identifier number "VIG-24-034-SMIME-BR", covers a single Root-CA and consists of 10 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	2024-08-28T14:30:31+02:00
	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):	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:	☐ Point in time audit ☐ Period of time, after x month of CA operation ☒ Period of time, full audit
Audit period covered for all policies:	2023-09-01 to 2024-03-31
Point in time date:	none, as audit was a period of time audit
Audit dates:	2024-04-19 (on site) 2024-05-03 (remote) 2024-06-04 (remote) 2024-06-14 (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 2020

Standards considered:	European Standards: • ETSI EN 319 411-1 V1.4.1 (2023-10) • ETSI EN 319 401 V2.3.1 (2021-05) • ETSI TS 119 411-6 V1.1.1 (2023-08) CA Browser Forum Requirements: • Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, version 1.0.3 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:

- GLOBALTRUST Certificate Policy, version 3.2a, as of 2024-02-16 (OID-Number: 1.2.40.0.36.1.1.8.1)
- GLOBALTRUST Certificate Practice Statement, version 3.0b, as of 2024-02-16 (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:

5 Risk assessment

The risk assessment shall be revised within the review cycle. In particular, risk treatment measures related to the takeover by the new owner (AUSTRIA CARD-Plastikkarten und Ausweissysteme Gesellschaft m.b.H.) should be addressed. [REQ-5-04]

7.2 Human resources

The TSP shall use resources with senior experience provided by the new owner to improve TSP’s processes (in particular incident reporting, internal auditing and development). The use of resources provided by the new owner shall be appropriately documented. [REQ-7.2-02, REQ-7.2-06, REQ-7.2-10]

7.6 Physical and environmental security

The TSP shall provide documentation of integration into the infrastructure of the new owner. [REQ-7.6-01]

7.8 Network security

The TSP shall provide documentation of integration into the infrastructure of the new owner and take this into account in future vulnerability scans and penetration tests. [REQ-7.8-13, REQ-7.8-14]

7.9 Incident management

The TSP shall improve the incident response processes and provide sufficient resources to reduce response times and the time for implementing remediation measures. [REQ-7.9-05, REQ-7.9-07, REQ-7.9-11]

Findings with regard to ETSI EN 319 411-1:
6.3 Certificate Life-Cycle operational requirements
Monitoring of CRL issuance shall be improved. [CSS-6.3.9-05]

Findings with regard to ETSI EN 319 411-2:
None.

All major non-conformities have been closed before the issuance of this attestation. For all minor non-conformities, remediation has been scheduled within three months after the onsite audit at latest and will be covered by a corresponding audit.

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

- Bug 1815534, e-commerce monitoring GmbH: SCT in precertificate: https://bugzilla.mozilla.org/show_bug.cgi?id=1815534
- Bug 1830536, e-commerce monitoring gmbh: certificate issued with two pre-certificates: https://bugzilla.mozilla.org/show_bug.cgi?id=1830536
- Bug 1862004, e-commerce monitoring GmbH: Delayed revocation: https://bugzilla.mozilla.org/show_bug.cgi?id=1862004
- Bug 1883711, e-commerce monitoring gmbh: precertificate validity does not match leaf certificate: https://bugzilla.mozilla.org/show_bug.cgi?id=1883711
- Bug 1888371, e-commerce monitoring GmbH: CRLs with mismatched issuer: https://bugzilla.mozilla.org/show_bug.cgi?id=1888371

The remediation measures taken by e-commerce monitoring GmbH as described on Bugzilla (see links above) have been checked by the auditors and properly addressed the incident. During the audit, the TSP was able to credibly demonstrate that the incident response processes will be improved with the support of human resources with senior experience provided by the new owner. The long-term effectiveness of the measures will be rechecked at the next regular audit.

This Audit Attestation also covers the following key-lifecycle events:

- 2023-06-24: Backup and Restore of HSM-partitions (including keys intended for use in a CA Certificate, location: office)
- 2023-07-04: Backup and Restore of HSM-partitions (including keys intended for use in a CA Certificate, location: datacenter)
- 2023-10-24: Backup and Restore of HSM-partitions (including keys intended for use in a CA Certificate, location: datacenter)

All key-lifecycle events were performed in compliance with the standards ETSI EN 319 401, V2.3.1, ETSI EN 319 411-1, V1.4.1, ETSI EN 319 411-2, V2.5.1 and ETSI EN 319 421, V1.2.1 as well as the CA Browser Baseline Requirements, version 2.0.2 and EV SSL Certificate Guidelines, version 1.8.1.

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 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 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)

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

Root 2: GLOBALTRUST 2015

Standards considered:	European Standards: • ETSI EN 319 411-1 V1.4.1 (2023-10) • ETSI EN 319 401 V2.3.1 (2021-05) • ETSI TS 119 411-6 V1.1.1 (2023-08) CA Browser Forum Requirements: • Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, version 1.0.3 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:

- GLOBALTRUST Certificate Policy, version 3.2a, as of 2024-02-16 (OID-Number: 1.2.40.0.36.1.1.8.1)
- GLOBALTRUST Certificate Practice Statement, version 3.0b, as of 2024-02-16 (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:

5 Risk assessment

The risk assessment shall be revised within the review cycle. In particular, risk treatment measures related to the takeover by the new owner (AUSTRIA CARD-Plastikkarten und Ausweissysteme Gesellschaft m.b.H.) should be addressed. [REQ-5-04]

7.2 Human resources

The TSP shall use resources with senior experience provided by the new owner to improve TSP’s processes (in particular incident reporting, internal auditing and development). The use of resources provided by the new owner shall be appropriately documented. [REQ-7.2-02, REQ-7.2-06, REQ-7.2-10]

7.6 Physical and environmental security

The TSP shall provide documentation of integration into the infrastructure of the new owner. [REQ-7.6-01]

7.8 Network security

The TSP shall provide documentation of integration into the infrastructure of the new owner and take this into account in future vulnerability scans and penetration tests. [REQ-7.8-13, REQ-7.8-14]

7.9 Incident management

The TSP shall improve the incident response processes and provide sufficient resources to reduce response times and the time for implementing remediation measures. [REQ-7.9-05, REQ-7.9-07, REQ-7.9-11]

Findings with regard to ETSI EN 319 411-1:
6.3 Certificate Life-Cycle operational requirements
Monitoring of CRL issuance shall be improved. [CSS-6.3.9-05]

Findings with regard to ETSI EN 319 411-2:
None.

All major non-conformities have been closed before the issuance of this attestation. For all minor non-conformities, remediation has been scheduled within three months after the onsite audit at latest and will be covered by a corresponding audit.

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

- Bug 1815534, e-commerce monitoring GmbH: SCT in precertificate: https://bugzilla.mozilla.org/show_bug.cgi?id=1815534
- Bug 1830536, e-commerce monitoring gmbh: certificate issued with two pre-certificates: https://bugzilla.mozilla.org/show_bug.cgi?id=1830536
- Bug 1862004, e-commerce monitoring GmbH: Delayed revocation: https://bugzilla.mozilla.org/show_bug.cgi?id=1862004
- Bug 1883711, e-commerce monitoring gmbh: precertificate validity does not match leaf certificate: https://bugzilla.mozilla.org/show_bug.cgi?id=1883711
- Bug 1888371, e-commerce monitoring GmbH: CRLs with mismatched issuer: https://bugzilla.mozilla.org/show_bug.cgi?id=1888371

The remediation measures taken by e-commerce monitoring GmbH as described on Bugzilla (see link above) have been checked by the auditors and properly addressed the incident.
During the audit, the TSP was able to credibly demonstrate that the incident response processes will be improved with the support of human resources with senior experience provided by the new owner. The long-term effectiveness of the measures will be rechecked at the next regular audit.

This Audit Attestation also covers the following key-lifecycle events:

- 2023-06-24: Backup and Restore of HSM-partitions (including keys intended for use in a CA Certificate, location: office)
- 2023-07-04: Backup and Restore of HSM-partitions (including keys intended for use in a CA Certificate, location: datacenter)
- 2023-10-24: Backup and Restore of HSM-partitions (including keys intended for use in a CA Certificate, location: datacenter)

All key-lifecycle events were performed in compliance with the standards ETSI EN 319 401, V2.3.1, ETSI EN 319 411-1, V1.4.1, ETSI EN 319 411-2, V2.5.1 and ETSI EN 319 421, V1.2.1 as well as the CA Browser Baseline Requirements, version 2.0.2 and EV SSL Certificate Guidelines, version 1.8.1.

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, 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 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

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

Modifications record

Version	Issuing Date	Changes
Version 1	2024-07-22	Initial attestation
Version 1.1	2024-08-28	Root Globaltrust 2015 added

End of the audit attestation letter.