Audit Attestation for

Halcom d.d.

Reference: AAL1743672201rev01

"Ljubljana, 2023-06-06"

To whom it may concern,

This is to confirm that "Bureau Veritas d.o.o." has audited the CAs of the "Halcom d.d." without critical findings.

This present Audit Attestation Letter is registered under the unique identifier number "AAL1743672201rev01" covers a single Root-CA and consists of 7 pages.

Kindly find here below the details accordingly.

In case of any question, please contact:

Bureau Veritas d.o.o.
Linhartova cesta 49a
1000 Ljubljana, Slovenia
E-Mail: eidas-slovenia@bureauveritas.com
Phone: +38614757670

With best regards,

Digitally signed by MARKO KOREN
Date: 2023.06.22 09:47:34 +02'00'

Marko Koren
LTM

BUREAU VERITAS, d.o.o. Linhartova cesta 49A, 1000 LJUBLJANA 14

Digitally signed by BORUT MLAKAR
Date: 2023.06.22 09:49:22 +02'00'

Borut Mlakar
Certification Manager

General audit information

Identification of the conformity assessment body (CAB) and assessment organization acting as ETSI auditor
• Bureau Veritas d.o.o., Linhartova cesta 49a, 1000 Ljubljana, Slovenia, https://www.bureauveritas.si/sites/g/files/zypfnx291/files/media/document/AAL1743672201rev01.pdf registered under company_registration no.: 5000939000 • Accredited by Slovenska Akreditacija (SA) https://www.slo-akreditacija.si/?lang=en# under registration accreditation_registration : http://www.slo-akreditacija.si/acreditation/bureau-veritas-d-o-o-3/ [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): Zavarovalnica Triglav • 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;

[1] URL to the accreditation certificate hosted by the national accreditation body

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.

- 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):	Halcom d.d., Tržaška cesta 118, 1000 Ljubljana, Slovenia, registered under company_registration No: 5556511000

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:	2022-06-01 to 2023-05-31
Point in time date:	none, as audit was a period of time audit
Audit dates:	2023-05-30 to 2023-05-31 (on site)
Audit location:	Halcom d.d., Tržaška cesta 118, 1000 Ljubljana, Slovenia Pošta Slovenije d.o.o., Cesta v Mestni log 81, 1000 Ljubljana, Slovenia T2 d.o.o., Brnčičeva ulica 41, 1231 Ljubljana-Črnuče, Slovenia

Root 1: Halcom Root Certificate Authority

Standards considered:	European Standards: ☒ ETSI EN 319 411-2 V2.2.1 (2021-05) ☒ ETSI EN 319 411-1 V1.3.1 (2021-05) ☒ ETSI EN 319 401 V2.4.1 (2018-04) CA Browser Forum Requirements: ☒ EV SSL Certificate Guidelines, version 1.7.9 ☒ Baseline Requirements, version 1.8.4 For the Trust Service Provider Conformity Assessment: ☒ ETSI EN 319 403 V2.2.2 (2015-08) ☒ ETSI EN 319 403-1 V2.3.1 (2020-06) ☒ ETSI TS 119 403-2 V1.2.4 (2020-11)

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

1. Halcom Root Certificate Authority, version 08, as of 2023-06-15
2. Halcom CA PO e-signature 1, version 07, as of 2023-06-15
3. Halcom CA PO e-signature 2, version 01, as of 2023-06-15
4. Halcom CA PO e-seal 1, version 07, as of 2023-06-15
5. Halcom CA PO e-seal 2, version 01, as of 2023-06-15
6. Halcom CA web 1, version 07, as of 2023-06-15
7. Halcom CA TSA 1, version 06, as of 2023-06-15
8. Halcom CA TS 5, version 03, as of 2023-06-15
9. Halcom CA FO e-signature 1, version 07, as of 2023-06-15
10. Halcom CA FO e-signature 2, version 01, as of 2023-06-15
11. Certificate Practise Statement, version 09, as of 2023-06-15

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

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 and OID
CN = Halcom Root Certificate Authority, O = Halcom d.d., C = SI	D7BA3F4FF8AD05633451470DDA3378A3491B90005E5C687D2B68D53647CFDD66	ETSI EN 319 411-2 V2.2.2, QCP-I-qscd

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 = Halcom CA FO e-signature 1, O = Halcom d.d., C = SI	24709797CD505CD70F27B2A6A013AF7455155CF7BA3E9AB6ACF03ABB12B8045B	[ETSI EN 319 411-1 V1.2.2] Policy: NCP; NCP+ [ETSI EN 319 411-2 V2.2.2] Policy: QCP-n; QCP-n-qscd;	Client Authentication, Document Signing, Secure Email
CN = Halcom CA PO e-signature 1, O = Halcom d.d., C = SI	6616DA2DC8C81CD1D5ACB8664D8715E07925915B1130D0D2284604620FABFA98	[ETSI EN 319 411-1 V1.2.2] Policy: NCP+ [ETSI EN 319 411-2 V2.2.2] Policy: QCP-n-qscd	Client Authentication, Document Signing, Secure Email
CN = Halcom CA PO e-seal 1, O = Halcom d.d., C = SI	7B1D60647E7DAB721BCE21BD2EC8D2AF281207B01474B1A47BF5CF772A311D9D	[ETSI EN 319 411-1 V1.2.2] Policy: NCP, NCP+ [ETSI EN 319 411-2 V2.2.2] Policy: QCP-l; QCP-l-qscd	Server Authentication, Client Authentication, Document Signing
CN = Halcom CA web 1, O = Halcom d.d., C = SI	D12DF63569F0F814514C2E29C93A9A133A4CBAA92D3046F8C6BC2D9D6F66F087	[ETSI EN 319 411-1 V1.2.2] Policy: LCP, NCP, DVCP, OVCP [ETSI EN 319 411-2 V2.2.2] Policy: QCP-w	Server Authentication, Client Authentication
CN = Halcom CA TSA 1, O = Halcom d.d., C = SI	A2FE481DBD77689629828DA50957B55B0D2CC4960601B3CB04E60C1DC3BC246C	[ETSI EN 319 411-1 V1.2.2] Policy: NCP+ [ETSI EN 319 411-2 V2.2.2] Policy: QCP-n-qscd; QCP-lqscd	Time Stamping
CN = Halcom CA FO e-signature 2, O = Halcom d.d., C = SI	B2FDA13F819007E924A5FF453FB4A450C2D3451FDB432CED4ABD34532D4477C2	[ETSI EN 319 411-1 V1.2.2] Policy: NCP; NCP+ [ETSI EN 319 411-2 V2.2.2] Policy: QCP-n; QCP-n-qscd;	Client Authentication, Document Signing, Secure Email

CN = Halcom CA PO e-signature 2, O = Halcom d.d., C = SI	4436A54D37BF9934B2FF7AAF235B77D95BAA0839BA7E5FFE9640EFC6655860CF	[ETSI EN 319 411-1 V1.2.2] Policy: NCP+ [ETSI EN 319 411-2 V2.2.2] Policy: QCP-n-qscd	Client Authentication, Document Signing, Secure Email
CN = Halcom CA PO e-seal 2, O = Halcom d.d., C = SI	5AE7385644A83ED2E18C66ECB80993EA17941CCE26D1ED6285DF83CB35BA24BA	[ETSI EN 319 411-1 V1.2.2] Policy: NCP, NCP+ [ETSI EN 319 411-2 V2.2.2] Policy: QCP-l; QCP-l-qscd	Server Authentication, Client Authentication, Document Signing

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

Modifications record

Version	Issuing Date	Changes
Version 1	2023-06-06	Initial attestation
…	…	…

End of the audit attestation letter.