TLS BR Audit Attestation for

Disig, a.s.

Reference: 1705/24-2

"Zvolen, 21st June 2024"

To whom it may concern,

This is to confirm that QSCert, spol. s r.o. has audited the CAs of the Disig, a.s. without critical findings.

This present Audit Attestation Letter is registered under the unique identifier number 1705/24-2 covers a single Root-CA and consists of 7 pages.

Kindly find here below the details accordingly.

In case of any question, please contact:

QSCert spol. s r.o.
E.P.Voljanského 1
960 01 Zvolen, Slovakia
E-Mail: qscert@qscert.sk
Phone: +421 455 400 718

With best regards,

Mr. Marcel Šlúch managing director	*Name_2* Title

General audit information

Identification of the conformity assessment body (CAB) and assessment organization acting as ETSI auditor
• QSCert spol. s r.o., E.P.Voljanského 1, Zvolen, Slovakia, registered under 36040631 (national business register)   • Accredited by Slovak National Accreditation Service (SNAS) under registration P-049[1]for the certification of trust services according to “EN ISO/IEC 17065:2012” and “ETSI EN 319 403 V2.2.2 (2015-08)” / “ETSI EN 319 403-1 V2.3.1 (2020-06)”. • Insurance Carrier (BRG section 8.2): PREMIUM Insurance Company Limited • 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;

[1] https://ais.snas.sk/ReportServer?%2FwebReports%2FCertificateDetail&rs%3ACommand=Render&rc%3AToolbar=false&CertificateID=568&LanguageID=sk&URI=https%3A%2F%2Fais.snas.sk

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. • 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):	Disig, a.s., Záhradnícka 151, Bratislava, Slovakia registered under company registration 35 975 946

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:	2023-04-22 to 2024-04-18
Point in time date:	none, as audit was a period of time audit
Audit dates:	2024-04-19 (on site)
Audit location:	Disig, a.s., Záhradnícka 151, Bratislava, Slovakia

Root 1: &CA_Disig_Root_R2

Standards considered:	European Standards: • ETSI EN 319 411-2 V2.5.1 (2023-10) • ETSI EN 319 411-1 V1.4.1 (2023-10) • ETSI EN 319 401 V2.3.1 (2021-05) CA Browser Forum Requirements: • Baseline Requirements for TLS Server Certificates, version 2.0.3 Browser Policy Requirements: • Apple Root Certificate Program (2023-08-15) • Chrome Root Program (2024-01-16) • Microsoft Trusted Root Program (2023-11-28) • Mozilla Root Store Policy, version 2.9 (2023-09-01) 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 V1.3.1 (2023-03)

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

1. Certificate Policy for issuing TLS certificate, version 6.0, as of 2024-02-01
2. Certificate Practice Statement for issuing TLS certificates Part: Registration Authority, version 6.0, as of 2024-02-01

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

Findings with regard to ETSI EN 319 401:

Opportunity for improvement #1:

It is recommended to increase the frequency of business continuity testing.

Opportunity for improvement #2:

It is recommended to increase the frequency of vulnerability scanning.

Opportunity for improvement #3:

It is recommended to increase the frequency of penetration testing.

Findings with regard to ETSI EN 319 411-1:

None.

Findings with regard to ETSI EN 319 411-2:

None.

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

- Bug 1888104, TSP Name: TLS certificate with basicConstraints not marked as critical https://bugzilla.mozilla.org/show_bug.cgi?id=1888104

- Bug 1889672, TSP Name: Certificates with incorrect Subject attribute order https://bugzilla.mozilla.org/show_bug.cgi?id=1889672

The remediation measures taken by Disig, a.s. as described on Bugzilla (see link above) have been checked by the auditors and properly address the incident.

Distinguished Name	SHA-256 fingerprint	Applied policy
Complete subject DN: CN = CA Disig Root R2, O = Disig a.s., C = SK	SHA-256 fingerprint of the certificate: E23D4A036D7B70E9F595B1422079D2B91EDFBB1FB651A0633EAA8A9DC5F80703	ETSI EN policy that this Root has been assessed against: ETSI EN 319 411-1 V1.4.1, LCP, OVCP, NCP ETSI EN 319 411-2 V2.5.1, QCP-n, QCP-l

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
C = SK, L = Bratislava, O = Disig a.s., CN = CA Disig R2I2 Certification Service	C96F24C45113FD91AE2F9E40E106653BFA0FFBCFA07E209524C844E7C8DA4148	ETSI EN 319 411-1 V1.4.1 LCP, OVCP, NCP ETSI EN 319 411-2 V2.5.1, QCP-n, QCP-l

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

Modifications record

Version	Issuing Date	Changes
Version 1	2024-06-21	Initial Attestation

End of the audit attestation letter.