



Audit Attestation for

Disig, a.s.

Reference: 1705/23-1

Bratislava, 2023-06-02

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 "1705/23-1" and consists of 6 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,

ePodpis:
Marcel
Šlúch

Signature_1
Title

Signature_2
title

General audit information

Identification of the conformity assessment body (CAB) and assessment organization acting as ETSI auditor
<ul style="list-style-type: none">• QSCert spol. s r.o., E.P.Vojňanského 1, Zvolen, Slovakia registered under 36040631 (national business register)• Accredited by Slovak National Accreditation Service (SNAS) under registration P-049: https://ais.snas.sk/ReportServer?%2FwebReports%2FCertificateDetail&rs%3ACommand=Render&rc%3AToolbar=false&CertificateID=568&LanguageID=sk&URI=https%3A%2F%2Fais.snas.sk for the certification of trust services according to "EN ISO/IEC 17065:2012" and "ETSI EN 319 403 V2.3.1 (2015-08)" and/or "ETSI EN 319 403-1 V2.3.1 (2020-06)" respectively.• 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
<ul style="list-style-type: none">• Number of team members: 1• 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<ol style="list-style-type: none">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; and4) 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:<ol style="list-style-type: none">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;

<ul style="list-style-type: none"> 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. <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> 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	
<ul style="list-style-type: none"> • 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:	<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:	2022-04-23 to 2023-04-21
Point in time date:	none, as audit was pot audit
Audit dates:	2023-04-21 to 2023-04-21 (on-site)
Audit Location:	Disig, a.s., Záhradnícka 151, Bratislava, Slovakia

Root 1: &CA_Disig_Root_R2

Standards considered:	<p>European Standards:</p> <ul style="list-style-type: none"><input checked="" type="checkbox"/> ETSI EN 319 411-2, V2.4.1 (2021-11)<input checked="" type="checkbox"/> ETSI EN 319 411-1, V1.3.1 (2021-05)<input checked="" type="checkbox"/> ETSI EN 319 401, V2.3.1 (2021-05) <p>CA Browser Forum Requirements:</p> <ul style="list-style-type: none"><input type="checkbox"/> EV SSL Certificate Guidelines, version 1.7.1<input checked="" type="checkbox"/> Baseline Requirements, version 1.8.7 <p>Browser Policy Requirements:</p> <ul style="list-style-type: none"><input checked="" type="checkbox"/> Apple Root Certificate Program (2022-10-01)<input checked="" type="checkbox"/> Chrome Root Program (2023-01-06)<input checked="" type="checkbox"/> Microsoft Trusted Root Program (2021-12-02)<input checked="" type="checkbox"/> Mozilla Root Store Policy, version 2.8.1 (2023-02-15) <p>For the Trust Service Provider Conformity Assessment:</p> <ul style="list-style-type: none"><input type="checkbox"/> ETSI EN 319 403 V2.2.2 (2015-08)<input checked="" type="checkbox"/> ETSI EN 319 403-1 V2.3.1 (2020-06)<input checked="" type="checkbox"/> ETSI TS 119 403-2 V1.3.1 (2023-03)
-----------------------	---

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

1. Certificate Policy, version 5.8, as of 2023-04-20
2. Certificate Practice Statement Part: Registration Authority, version 5.8, as of 2022-10-01

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.

Distinguished Name	SHA-256 fingerprint	Applied policy and OID
Complete subject DN: CN = CA Disig Root R2, O = Disig a.s., C = SK	SHA-256 fingerprint of the certificate: E23D4A036D7B70EE9F595B1422079D2B91EDFBB1FB651A0633EAA8A9DC5F80703	ETSI EN policy that this Root has been assessed against: ETSI EN 319 411-1 V1.3.1, LCP, OVCP, NCP ETSI EN 319 411-2 V2.4.1, QCP-n, QCP-I

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 OID	EKU
C = SK, L = Bratislava, O = Disig a.s., CN = CA Disig R2/2 Certification Service	C96F24C45113FD91AE2F9E40E106653BF A0FFBCFA07E209524C844E7C8DA4148	ETSI EN 319 411-1 V1.3.1 LCP, OVCP, NCP ETSI EN 319 411-2 V2.4.1, QCP-n, QCP-I	not defined
C = SK, L = Bratislava, O = Disig a.s., CN = CA Disig R2/3 Certification Service	239FFA86D71033BA255914782057D87E8421AEDD5910B786928B6A1248C3E341	ETSI EN 319 411-1 V1.3.1 LCP, OVCP, NCP ETSI EN 319 411-2 V2.4.1 QCP-n, QCP-I	not defined
C = SK, L = Bratislava, O = Disig a.s., CN = CA Disig R2/5 Certification Service	90BA720B376FEB9FDCF8A1037A5316FB493B5ACF656AD79C6839008BD43343FDD	ETSI EN 319 411-1 V1.3.1 LCP, OVCP, NCP ETSI EN 319 411-2 V2.4.1 QCP-n, QCP-I	emailProtection clientAuth ocspSigning

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

This attestation is based on the template version 3.0 as of 2023-02-20, that was approved for use by ACAB-c.

Modifications record

Version	Issuing Date	Changes
Version 1	2023-06-02	Initial attestation

End of the audit attestation letter.