

AUDIT STATEMENT REPORT

POLICY AND SECURITY REQUIREMENTS FOR TRUST SERVICE PROVIDERS ISSUING CERTIFICATES COMPLIANCE AUDIT

AUDIT DETAILS

Subject of audit: Certification Authority "CA Disig"
Company: **Disig, a.s.**
Location: Záhradnícka 151, 821 08 Bratislava, Slovak Republic
Contact person: Peter Miškovič
Standards: **ETSI EN 319 411-1 V1.2.2 (2018-04), ETSI EN 319 411-2 V2.2.2 (2018-04), CA/Browser Forum Baseline Requirements, v.1.7.4 (April 4, 2021)**

Lead auditor: Ján Matuška, CISA (#1081409), CISSP (#350884)
Date of audit: May 21, 2021
Audited time period: May 22, 2020 – May 21, 2021, period of time audit
Date of audit report: June 22, 2021
Main CA policy documents: CP CA Disig, version 5.5 (effective May 20, 2021)
CPS RA CA Disig, version 5.5 (effective May 20, 2021)

SUMMARY

Independent audit team has conducted and completed an audit of the Certification Authority "CA Disig" to assess its compliance with the following technical standards and specifications:

ETSI EN 319 411-1 V1.2.2 (2018-04) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements;

ETSI EN 319 411-2 V2.2.2 (2018-04) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates Part 2: Requirements for trust service providers issuing EU qualified certificates

Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates, v.1.7.4, adopted by the CA/Browser Forum as of April 5, 2021.

The main objective was to verify the level and effectiveness of existing controls within the infrastructure of Certification Authority "CA Disig" and to determine whether the Certification Authority meets the requirements of the above-mentioned standards.

The audit was conducted as a **full audit applying LCP, OVCP and NCP criteria of ETSI EN 319 411-1 (SSL trust bit), QCP-n and QCP-I criteria of ETSI EN 319411-2 (email trust bit) and the criteria of CA/Browser Forum Baseline Requirements.**

The examination was conducted in accordance with international and European Standards/Specifications, in particular with ETSI EN 319 403, V2.2.2.

The certification authorities that were in scope of the audit (root CAs and their subordinate CAs capable of issuing SSL certificates):

Name and distinguished name of CA	SHA256 Fingerprint
CA Disig Root R2 C=SK, L=Bratislava, O=Disig a.s., CN=CA Disig Root R2	E23D4A036D7B70E9F595B1422079D2B91EDFBB1FB651A0633EAA8A9DC5F80703
CA Disig R2I2 Certification Service C=SK, L=Bratislava, O=Disig a.s., CN=CA Disig R2I2 Certification Service	C96F24C45113FD91AE2F9E40E106653BFA0FFBCFA07E209524C844E7C8DA4148
CA Disig R2I3 Certification Service C=SK, L=Bratislava, O=Disig a.s., CN=CA Disig R2I3 Certification Service	239FFA86D71033BA255914782057D87E8421AEDD5910B786928B6A1248C3E341

The audit covered the relevant systems and processes used in the issuance of all Certificates that assert the certification policy CP CA Disig, version 5.5, OID = 1.3.158.35975946.0.0.0.1.1.

CA Policy documents that were referenced during the audit:

- Certificate Policy (CP CA Disig), version 5.5,
- Certificate Practice Statement Part: Registration Authority (CPS RA CA Disig), version 5.5,
- General Terms and Conditions for Providing and Using a Trusted Service, version 2.0.

CONCLUSION

According to the security audit compliance results based on ETSI EN 319 411-1 V1.2.2 and ETSI EN 319 411-2 V2.2.2 requirements and on the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates v.1.7.4, the audit team formulated the following statement:

„The audit team has confirmed that the requirements identified in the standards are met.“

The audit report states some minor findings without material impact on the security of the certification services. No evidence of significant violation of the Certification Authority policies, practices or procedures was found.

Ing. Ján Matuška
Lead auditor

Ing. Marcel Šlúch
Chief executive