

QSCert, spol. s r. o., Management Systems Certification Body
Residence address: Klimentůvská 52, Nové Město, 110 00 Prague 1, Czech Republic
Postal address: E.P.Vojanského 1, 960 01 Zvolen, Slovak Republic
Accredited ISO/IEC 27001:2013, N. 677/2015 CZECH ACCREDITATION INSTITUTE

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 V1.2.0 (2017-08)**
CA/Browser Forum Baseline Requirements, v.1.5.7 (April 29, 2018)

Lead auditor: Ján Matuška, CISA (#1081409)
Date of audit: May 29, 2018
Audited time period: October 11, 2017 – May 29, 2018, period-of-time audit
Date of audit report: August 07, 2018
Main CA policy documents: CP CA Disig, version 5.1; CPS RA Disig, version 5.1

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 V1.2.0 (2017-08) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements,

Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.5.7, adopted by the CA/Browser Forum as of April 29, 2018.

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 above mentioned standards.

The audit was conducted as a **full audit applying NCP+ criteria of ETSI EN 319 411-1 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 (sha256RSA) C=SK, L=Bratislava, O=Disig a.s., CN=CA Disig Root R2	E2:3D:4A:03:6D:7B:70:E9:F5:95:B1:42:20:79:D2:B9:1E:DF:BB:1F:B6:51:A0:63:3E:AA:8A:9D:C5:F8:07:03
CA Disig R2I1 Certification Service (CERTIFICATE REVOKED ON MARCH 28, 2018) C=SK, L=Bratislava, O=Disig a.s., CN=CA Disig R2I1 Certification Service	AC:6E:48:D1:4A:31:D6:2C:B8:C1:52:2D:00:6A:AD:58:5A:89:26:36:D9:CD:2D:79:8C:B6:1E:A1:3B:49:57:BD
CA Disig R2I2 Certification Service C=SK, L=Bratislava, O=Disig a.s., CN=CA Disig R2I2 Certification Service	C9:6F:24:C4:51:13:FD:91:AE:2F:9E:40:E1:06:65:3B:FA:0F:FB:CF:A0:7E:20:95:24:C8:44:E7:C8:DA:41:48
CA Disig R2I3 Certification Service C=SK, L=Bratislava, O=Disig a.s., CN=CA Disig R2I3 Certification Service	23:9F:FA:86:D7:10:33:BA:25:59:14:78:20:57:D8:7E:84:21:AE:DD:59:10:B7:86:92:8B:6A:12:48:C3:E3:41
CA Disig Root R1 (sha1RSA) C=SK, L=Bratislava, O=Disig a.s., CN=CA Disig Root R1	F9:6F:23:F4:C3:E7:9C:07:7A:46:98:8D:5A:F5:90:06:76:A0:F0:39:CB:64:5D:D1:75:49:B2:16:C8:24:40:CE
CA Disig R1I1 Certification Service (CERTIFICATE REVOKED ON MARCH 28, 2018) C=SK, L=Bratislava, O=Disig a.s., CN=CA Disig R1I1 Certification Service	E1:AB:B0:FA:EA:A7:31:2F:2C:3E:04:1C:BD:2D:F0:3A:50:7E:34:6B:97:16:44:24:63:ED:61:10:6A:FF:69:47

The audit covered the relevant systems and processes used in the issuance of all Certificates that assert the certification policy CP CA Disig version 5.1,
OID = 1.3.158.35975946.0.0.0.1.1.

CA Policy documents that were referenced during the audit:

- CP CA Disig, version 5.1,
- CPS RA Disig, version 5.1,
- General Terms and Conditions for Providing and Using a Trusted Service, version 1.0.

CONCLUSION

According to the security audit compliance results based on ETSI EN 319 411-1 V1.2.0 requirements and on the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates v.1.5.7, the audit team formulated the following statement

„The audit team 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 Šluch
Chief executive