



tayllorcox.com
ensure your ict certification

TAYLLORCOX s.r.o.

Member of TAYLLORCOX UK Ltd. 75 King William St., EC4N, London, UK
TAYLLORCOX PCEB, certification body No. 3239, accredited in accordance with ČSN EN ISO/IEC 17065:2013
by Czech Accreditation Institute (website: www.cai.cz/en/Subjekt.aspx?ID=11346)
Address: Na Florenci 1055/35, Praha 1 - Nové Město, CZ 110 00, info@tayllorcox.com

QUALIFYING ATTESTATION LETTER

FOR MICROSOFT TRUSTED ROOT CERTIFICATE PROGRAM

NO. PCEB-N 18/07/01

Conformity assessment body (CAB, auditor name):

TAYLLORCOX PCEB,
TAYLLORCOX s.r.o.
Identification No.: 279 02 587
Na Florenci 1055/35
Praha 1 - Nové Město
CZ 110 00
Czech Republic

Audit team: Ing. Martin Dudek (Lead auditor)
Nebojša Živković (Auditor)

Identification of the trust service provider (CA name):

Ministry of Public Administration,
Trust Service Authority of Slovenia SI-TRUST
Tax No. : 91838983
Registration No. : 2482762000

Tržaška 21
1000 Ljubljana
Slovenia

Identification of the audited Root CA (CNs):

1) SI-TRUST Root

(see chapter 1.4.1, A. for details)

Ljubljana / Prague, 16/07/2018

Martin Dudek
Lead Auditor



1.1 Part I: Audit information

The audit was performed as **full annual audit**.

The audit period covered the period from 31/05/2017 to 30/05/2018.

1.2 Audit scope

1.2.1 "HIERARCHICAL CERTIFICATE ISSUING AND MANAGEMENT SYSTEM"

The hierarchical structure of the system consists of off-line root certification authority (**SI-TRUST Root**) issuing certificates for subordinate CAs (SIGOV-CA, SIGEN-CA, SI-PASS CA), these subordinate CAs are issuing certificates for end users.

The TSP assured that no other non-revoked Sub-CA's technically capable of issuing SSL/TLS certificates have been issued by this Root-CA.

1.3 Used audit standards

ETSI EN 319 411-1 V1.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.

ETSI EN 319 411-2 V2.1.1 (2016-02) 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

as well as

ETSI EN 319 401 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers

CA/Browser Forum: "**Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates**", version 1.5.7



1.4 Audit targets

1.4.1 CERTIFICATION SERVICES PROVIDED BY HIERARCHICAL STRUCTURE OF SI-TRUST ROOT

A. SI-TRUST Root

Issuer	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SI-TRUST Root
Subject Distinguished Name	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SI-TRUST Root
Certificate Serial Number	90AE 7776 0000 0000 571D D06F
SHA-256 fingerprint	FAD5 4081 1AFA E0DC 767C DF65 72A0 88FA 3CE8 493D D82B D10A 9A67 3B86 AB4E 8124
Applied policy requirements	ETSI EN 319 411-1 V1.1.1 (2016-02) policies NCP ETSI EN 319 411-2 V2.1.1 (2016-02) policies QCP-l, QCP-n, QCP-l-qscd, QCP-n-qscd, QCP-w

B. SIGOV-CA

Issuer	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SI-TRUST Root
Subject Distinguished Name	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SIGOV-CA
Certificate Serial Number	A0E3 6B67 0000 0000 571D D0E9
SHA-256 fingerprint	9863 73DD A59F D093 84B0 A47C 8E31 55AB 7424 ECDA 5DD8 2DB2 E2A4 3FBD 7591 434E
Applied policy requirements	ETSI EN 319 411-1 V1.1.1 (2016-02) policies NCP ETSI EN 319 411-2 V2.1.1 (2016-02) policies QCP-l, QCP-n, QCP-l-qscd, QCP-n-qscd, QCP-w

Issuer	c=si, o=state-institutions, ou=sigov-ca
Subject Distinguished Name	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SI-TRUST Root
Certificate Serial Number	B16D 3159 0000 0000 571D D0EA
SHA-256 fingerprint	BE73 A04F 7A02 AEE2 D35C 3ADB 7AEF A2FA 2FF3 334D 920A 4FFD 24CD D751 FDAA 4C1D
Applied policy requirements	ETSI EN 319 411-1 V1.1.1 (2016-02) policies NCP ETSI EN 319 411-2 V2.1.1 (2016-02) policies QCP-n, QCP-n-qscd



C. SIGEN-CA

Issuer	c=si, o=state-institutions, ou=sigen-ca
Subject Distinguished Name	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SI-TRUST Root
Certificate Serial Number	A668 BD51 0000 0000 571D D0E8
SHA-256 fingerprint	E016 01D8 F0D6 9434 E699 735C 4F34 8FC1 5FB4 8F2C 2B20 03FE E0F5 4A90 E819 48FD
Applied policy requirements	ETSI EN 319 411-1 V1.1.1 (2016-02) policies NCP ETSI EN 319 411-2 V2.1.1 (2016-02) policies QCP-n

Issuer	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SI-TRUST Root
Subject Distinguished Name	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SIGEN-CA G2
Certificate Serial Number	28C3 981D 0000 0000 571D D0E7
SHA-256 fingerprint	7950 15CA ACA7 4715 D341 120D 3F0E FD19 2A03 2F1C 0039 1797 F54E F998 0804 A175
Applied policy requirements	ETSI EN 319 411-1 V1.1.1 (2016-02) policies NCP ETSI EN 319 411-2 V2.1.1 (2016-02) policies QCP-l, QCP-n, QCP-w

D. SI-PASS CA

Issuer	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SI-TRUST Root
Subject Distinguished Name	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SI-PASS-CA
Certificate Serial Number	9D0E 9E3A 0000 0000 571D D10C
SHA-256 fingerprint	B394 3BD0 C0FF B4B4 1CD9 E1AD E986 ABE3 3583 12D6 AA6C 5DD2 45BB 7B0D 63A5 F851
Applied policy requirements	ETSI EN 319 411-1 V1.1.1 (2016-02) policies NCP ETSI EN 319 411-2 V2.1.1 (2016-02) policies QCP-n, QCP-n-qscd



Part II: Audit conclusion

The audit was completed successfully without critical findings.

In case of any question, please contact directly local Auditor on address:

TAYLLOR & COX d.o.o,
Ljubljanska 12f
1236 Trzin
Slovenia
phone: +386 (0)1 777 98 92
e-mail: nebojsa.zivkovic@tayllorcox.si

The Auditor uploads results of audit to the TAYLLORCOX PCEB project storage.

Qualifying Attestation Letter is also available on the TSP website:

https://www.si-trust.gov.si/dokumenti/MS_QualifyingAttestationLetter - SITRUST - 2018.pdf