



QUALIFYING ATTESTATION LETTER

FOR MICROSOFT TRUSTED ROOT CERTIFICATE PROGRAM

Identification of the trust service provider (CA name):

Ministry of Public Administration, Trust Service Authority of Slovenia SI-TRUST

Tržaška 21, 1000 Ljubljana, Slovenia

Conformity assessment body (CAB, auditor name):

SIQ Ljubljana

Mašera-Spasićeva ulica 10, 1000 Ljubljana, Slovenia

CAB Ref. No.: 3150-0021/10-0024 accredited in accordance with SIST EN ISO/IEC17065:2012 by Slovenian Accreditation. Information on current accreditation status is available at the SA website, www.slo-akreditacija.si

Audit team:

mag. Miha Ozimek (Lead auditor)

Andrej Gornik (Auditor)

PIT PN036-2021

Qualifying attestation letter date: 05.12.2022

Created:

Miha Ozimek

A handwritten signature in black ink, appearing to be 'Miha Ozimek', is located below the printed name.

1. AUDIT INFORMATION

The audit was performed as full annual audit. The audit period covers the period from 2021-05-21 to 2022-05-22. All changes from 2021-05-21 until 2022-12-05 were checked during the audit and are applicable with EIDAS and ETSI standards as stated in the QUALIFYING ATTESTATION LETTER FOR MICROSOFT TRUSTED ROOT CERTIFICATE PROGRAM NO. PCEB-N 20/06/01 (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).

1.1 Audit scope

"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.

1.2 Used audit standards and legislation

REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

ETSI standards:

EN 319 401 General Policy Requirements for Trust Service Providers

EN 319 411 Policy and security requirements for Trust Service Providers issuing certificates

319 411-1 General requirements

319 411-2 Requirements for trust service providers issuing EU qualified certificates

EN 319 421 Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps

EN 319 412 Certificate Profiles

319 412-1 Overview and common data structures

319 412-2 Certificate profile for certificates issued to natural persons

319 412-3 Certificate profile for certificates issued to legal persons

319 412-4 Certificate profile for web site certificates issued to organisations

319 412-5 QCStatements

EN 319 422 Time-stamping protocol and electronic time-stamp profiles

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

All ETSI standards versions are valid on 05.12.2022.

1.3 Audit targets

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

- SI-TRUST eID Podpis

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 eID Podpis
Certificate Serial Number	60CC E65C 0000 571D D226
SHA-256 fingerprint	0228 7E94 B50D 1FDA 51A0 B91B C3B2 E928 8B04 D174 BE0B E416 C06A 35BC 2792 F51C
Applied policy requirements	ETSI EN 319 411-1 policies NCP ETSI EN 319 411-2 policies QCP-n-qscd

- 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 policies NCP ETSI EN 319 411-2 policies QCP-l, QCP-n, QCP-l-qscd, QCP-n-qscd, QCP-w

- 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 policies NCP ETSI EN 319 411-2 policies QCP-l, QCP-n, QCP-l-qscd, QCP-n-qscd, QCP-w

- SIGEN-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=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 policies NCP ETSI EN 319 411-2 policies QCP-I, QCP-n, QCP-w

- 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 policies NCP ETSI EN 319 411-2 policies QCP-n, QCP-n-qscd

2. AUDIT CONCLUSION

The audit was completed successfully without critical findings.

SIQ Ljubljana
Mašera-Spasičeva ulica 10
1000 Ljubljana
Slovenia

Email: infosec@siq.si
Phone number: +386 1 4778 343