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/?subjekt=3239-tayllorcox-s-r-o&lang=en)
Address: Na Florenci 1055/35, Praha 1 - Nové Město, CZ 110 00, info@tayllorcox.com

QUALIFYING ATTESTATION LETTER
RSA ALGORITHM

FOR MICROSOFT TRUSTED ROOT CERTIFICATE PROGRAM

NO. PCEB-N 21/05/01

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)
Ing. Radek Nedvěd (Head of CAB)

Identification of the trust service provider (CA name):

První certifikační autorita, a.s. (hereinafter also I.CA)
Identification No.: 264 39 395
Podvinný mlýn 2178/6
Praha 9 - Libeň
CZ 190 00
Czech Republic

Identification of the audited Root CA (CN):

1) **I.CA Root CA/RSA**

(see chapter 1.3.1 A. for details)

2021.05.18
06:27:09 +02'00'

Praha, 18/05/2021

Ing. Martin Dudek
Lead auditor

Part I: Audit information

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

The audit period covered the period 10/05/2020 to 09/05/2021.

1.1 Audit scope

1.1.1 "HIERARCHICAL CERTIFICATE ISSUING AND MANAGEMENT SYSTEM"

The hierarchical structure of the system consists of off-line root certification authority (I.CA Root CA/RSA) issuing certificates for subordinate CAs (I.CA SSL EV CA/RSA, I.CA SSL CA/RSA, I.CA Qualified CA/RSA, I.CA Qualified 2 CA/RSA, I.CA TSACA/RSA and I.CA Public CA/RSA), 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

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

ETSI EN 319 412-1 V1.4.1 (2020-06) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures

ETSI EN 319 412-2 V2.2.1 (2020-07) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons

ETSI EN 319 412-3 V1.2.1 (2020-07) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons

ETSI EN 319 412-4 V1.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates

ETSI EN 319 412-5 V2.3.1 (2020-04) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements

as well as

ETSI EN 319 401 V2.2.1 (2018-04) 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 1.7.4

CA/Browser Forum: "**Guidelines For The Issuance And Management Of Extended Validation Certificates**", version 1.7.5

1.3 Audit targets

1.3.1 CERTIFICATION SERVICES PROVIDED BY HIERARCHICAL STRUCTURE OF I.CA CAs

A. I.CA Root CA/RSA

Issuer	CN = I.CA Root CA/RSA
Subject Distinguished Name	CN = **I.CA Root CA/RSA** O = První certifikační autorita, a.s. SERIALNUMBER = NTRCZ-26439395 C = CZ
Certificate Serial Number	05 f5 e1 00
SHA-256 fingerprint	d3 d6 07 a9 ff 24 a1 95 23 b6 da 9d 2c 64 94 46 f8 78 8c b9 6d 9f d1 30 97 2e 12 0c 13 67 77 30
Applied policy requirements	ETSI EN 319 411-1 V1.2.2 (2018-04) policies NCP, NCP+, DVCP, OVCP, EVCP ETSI EN 319 411-2 V2.2.2 (2018-04) policies QCP-l, QCP-n, QCP-l-qscd, QCP-n-qscd, QCP-w

B. I.CA SSL EV CA/RSA

Issuer	CN = I.CA Root CA/RSA
Subject Distinguished Name	CN = **I.CA SSL EV CA/RSA 10/2017** O = První certifikační autorita, a.s. organizationIdentifier = NTRCZ-26439395 C = CZ
Certificate Serial Number	05 f5 e4 fe
SHA-256 fingerprint	75 f5 c8 db 96 b8 e2 14 8a 6a 95 8a 47 83 11 f0 5c 75 8f b7 d9 6d 5b 8b c0 4e 5b 9d 35 9c 3b 09
Applied policy requirements	ETSI EN 319 411-1 V1.2.2 (2018-04) policy EVCP ETSI EN 319 411-2 V2.2.2 (2018-04) policy QCP-w

C. I.CA SSL CA/RSA

Issuer	CN = I.CA Root CA/RSA
Subject Distinguished Name	CN = **I.CA SSL CA/RSA 07/2015** O = První certifikační autorita, a.s. SERIALNUMBER = NTRCZ-26439395 C = CZ
Certificate Serial Number	05 f5 e4 ea
SHA-256 fingerprint	92 a4 46 d2 78 94 31 22 7f f4 b3 34 18 9a a5 a7 b9 30 20 08 ac 37 47 e9 68 c6 ae 68 ad 7a eb 66
Applied policy requirements	ETSI EN 319 411-1 V1.2.2 (2018-04) policies DVCP, OVCP

D. I.CA Qualified CA/RSA

Issuer	CN = I.CA Root CA/RSA
Subject Distinguished Name	CN = **I.CA Qualified CA/RSA 07/2015** O = První certifikační autorita, a.s. SERIALNUMBER = NTRCZ-26439395 C = CZ
Certificate Serial Number	05 f5 e4 ec
SHA-256 fingerprint	de 2e a0 58 39 b8 2d ca 52 83 a6 04 c7 d8 df f9 47 f5 46 95 bb b4 da fb 96 48 40 b1 e6 11 da 7e
Applied policy requirements	EN 319 411-2 V2.2.2 (2018-04) policies QCP-n-qscd, QCP-l-qscd

E. I.CA Qualified 2 CA/RSA

Issuer	CN = I.CA Root CA/RSA
Subject Distinguished Name	CN = **I.CA Qualified 2 CA/RSA 02/2016** O = První certifikační autorita, a.s. SERIALNUMBER = NTRCZ-26439395 C = CZ
Certificate Serial Number	05 f5 e4 ee
SHA-256 fingerprint	07 6a bc 22 69 32 7e ef 50 0a 0c 57 52 72 62 ba c8 31 f9 d2 df 4e f2 d4 39 e7 4c e1 70 36 aa 3a
Applied policy requirements	ETSI EN 319 411-2 V2.2.2 (2018-04) policies QCP-n, QCP-n-qscd, QCP-l, QCP-l-qscd ETSI EN 319 411-1 V1.2.2 (2018-04) policies NCP, NCP+

F. I.CA TSACA/RSA

Issuer	CN = I.CA Root CA/RSA
Subject Distinguished Name	CN = **I.CA TSACA/RSA 05/2017** O = První certifikační autorita, a.s. organizationIdentifier = NTRCZ-26439395 C = CZ
Certificate Serial Number	05 f5 e4 f4
SHA-256 fingerprint	4a b8 bc 60 61 74 3e 09 80 bf d1 21 37 0a 88 c5 11 c4 f2 9e b4 bc 08 97 65 88 6b 64 c7 91 f7 68
Applied policy requirements	ETSI EN 319 411-2 V2.2.2 (2018-04) policy QCP-l

G. I.CA Public CA/RSA

Issuer	CN = I.CA Root CA/RSA
Subject Distinguished Name	CN = **I.CA Public CA/RSA 07/2015** O = První certifikační autorita, a.s. SERIALNUMBER = NTRCZ-26439395 C = CZ
Certificate Serial Number	05 f5 e4 eb
SHA-256 fingerprint	97 38 4d 1e 5a a6 37 ac 60 1b 19 89 37 15 9f e8 b3 9a 2f d2 9f e4 1a 86 a0 93 0b 65 60 76 6a 71
Applied policy requirements	ETSI EN 319 411-1 V1.2.2 (2018-04) policies NCP, NCP+

Part II: Audit conclusion

The audit was completed successfully without critical findings.

As a part of the process of continuous improvement of provided services, the company První certifikační autorita, a.s., was assessed for the compliance of the internal implementation of Information Security Management System (ISMS) with the requirements of ISO/IEC 27001:2013 by the independent external audit last year. The scope of ISMS includes the usage of all internal systems used on the provision of trust services within the meaning of the eIDAS Regulation (Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC) activities. The result of the audit is Certificate No. 1912059861, valid until 20.11.2022.

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

TAYLLORCOX PCEB,
TAYLLORCOX s.r.o.
Na Florenci 1055/35
Praha 1 - Nové Město
CZ 110 00
Czech Republic
phone: +420 222 553 101
e-mail: martin.dudek@tayllorcox.com; info@tayllorcox.com

The Auditor uploads results of audit to the TAYLLORCOX PCEB project storage.
Qualifying Attestation Letter is also available on the website https://pceb.tayllorcox.cz/Documents.html.