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

I.CA TLS ROOT CA/RSA 05/2022

FOR MICROSOFT TRUSTED ROOT CERTIFICATE PROGRAM

NO. PCEB-N 24/05/03

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 TLS Root CA/RSA 05/2022**

(see chapter 1.3.1 A. for details)

Praha, 21/05/2024

Ing. Martin Dudek
Lead auditor

Part I: Audit information

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

The audit period covered the period 10/05/2023 to 09/05/2024.

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 05/2022) issuing certificates for subordinate CAs:

a) I.CA TLS EV CA/RSA 06/2022,
b) I.CA TLS DV/OV CA/RSA 06/2022,

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 V1.4.1 (2023-10) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements

ETSI EN 319 411-2 V2.5.1 (2023-10) 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 V1.5.1 (2023-09) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures

ETSI EN 319 412-4 V1.3.1 (2023-09) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates

ETSI EN 319 412-5 V2.4.1 (2023-09) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements

as well as

ETSI EN 319 401 V2.3.1 (2021-05) 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 from 1.8.6 to 2.0.4

CA/Browser Forum: "Guidelines for the Issuance and Management of Extended Validation Certificates", version from 1.8.0 to 2.0.1

ETSI TS 119 312 V1.4.3 (2023-08) Electronic Signatures and Infrastructures (ESI); Cryptographic Suites

1.3 Audit targets

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

A. I.CA TLS Root CA/RSA 05/2022

Issuer	CN = I.CA TLS Root CA/RSA 05/2022
Subject Distinguished Name	CN = **I.CA TLS Root CA/RSA 05/2022** O = První certifikační autorita, a.s. SERIALNUMBER = NTRCZ-26439395 C = CZ
Certificate Serial Number	05 f5 e1 04
SHA-256 fingerprint (rca22_rsa.cer)	f9a17a00e5c294ba9614a715819af57f3fd48cc413453fbb8a5fc7e97964e2bc
Applied policy requirements	ETSI EN 319 411-1 V1.4.1 (2023-10) policies NCP, NCP+, DVCP, OVCP, EVCP ETSI EN 319 411-2 V2.5.1 (2023-10) policies QCP-l, QCP-n, QCP-l-qscd, QCP-n-qscd (based on EN 319411-1, NCP, NCP+), QEVCP-w (based on EN 319411-1, EVCP)

B. I.CA TLS EV CA/RSA 06/2022

Issuer	CN = I.CA TLS Root CA/RSA 05/2022
Subject Distinguished Name	CN = **I.CA TLS EV CA/RSA 06/2022** O = První certifikační autorita, a.s. SERIALNUMBER = NTRCZ-26439395 C = CZ
Certificate Serial Number	05 f5 e5 2f
SHA-256 fingerprint (qcw22_rsa.cer)	b9ef51a5f69a974f8d290b0a75fb253b7339053002aecb6516a270ea88aef4ed
Applied policy requirements	ETSI EN 319 411-1 V1.4.1 (2023-10) policy EVCP ETSI EN 319 411-2 V2.5.1 (2023-10) policies QCP-l, QCP-n, QCP-l-qscd, QCP-n-qscd (based on EN 319411-1, NCP, NCP+), QEVCP-w (based on EN 319411-1, EVCP)

C. I.CA TLS DV/OV CA/RSA 06/2022

Issuer	CN = I.CA TLS Root CA/RSA 05/2022
Subject Distinguished Name	CN = **I.CA TLS DV/OV CA/RSA 06/2022** O = První certifikační autorita, a.s. SERIALNUMBER = NTRCZ-26439395 C = CZ
Certificate Serial Number	05 f5 e5 2e

SHA-256 fingerprint (sca22_rsa.cer)	15448c743b75dcc18d782728037226b6f339ac288c1b8fecba5892556e5879ee
Applied policy requirements	ETSI EN 319 411-1 V1.4.1 (2023-10) policies DVCP, OVCP, NCP, NCP+

Part II: Audit conclusion

The audit was completed successfully without critical findings.

Due to technical reasons, the deployment of the updated software package was delayed and 33 certificates were issued, which did not take into account the requirement of the CABforum document "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates", version 2.0.0, effective from 15.9.2023, to designate the basicConstraits extension as critical. The mentioned certificates are gradually revoked and new ones are issued in the correct profile, with units of pieces remaining at the audit date.

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. 2211217661, valid until 20.11.2025.

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.