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 ROOT CA/RSA 05/2022

FOR MICROSOFT TRUSTED ROOT CERTIFICATE PROGRAM

No. PCEB-N 24/05/02

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 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 EU Qualified CA2/RSA 06/2022,
b) I.CA EU Qualified CA-SK/RSA 10/2022
c) I.CA TSA CA/RSA 06/2022,
d) I.CA Public CA/RSA 06/2022.

These subordinate CAs are issuing certificates for end users.

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 319 412-2 V2.3.1 (2023-09) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons

ETSI EN 319 412-3 V1.3.1 (2023-09) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons

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

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 Root CA/RSA 05/2022

Issuer	CN = I.CA Root CA/RSA 05/2022
Subject Distinguished Name	CN = **I.CA Root CA/RSA 05/2022** O = První certifikační autorita, a.s. SERIALNUMBER = NTRCZ-26439395 C = CZ
Certificate Serial Number	05 f5 e1 02
SHA-256 fingerprint (rca22_rsa.cer)	d279c01a12e8dd9a6230e459faa447ceb336998477338c2ee4135c96737418eb
Applied policy requirements	ETSI EN 319 411-1 V1.4.1 (2023-10) policies NCP, NCP+ ETSI EN 319 411-2 V2.5.1 (2023-10) policies QCP-n, QCP-n-qscd, QCP-l, QCP-l-qscd

B. I.CA EU Qualified CA2/RSA 06/2022

Issuer	CN = I.CA Root CA/RSA 05/2022
Subject Distinguished Name	CN = **I.CA EU Qualified CA2/RSA 06/2022** O = První certifikační autorita, a.s. SERIALNUMBER = NTRCZ-26439395 C = CZ
Certificate Serial Number	05 f5 e5 2a
SHA-256 fingerprint (2qca22_rsa.cer)	5f9147824201b2e23d8e128f99adb9ec11c495796960fa0faef05f901a347c66
Applied policy requirements	ETSI EN 319 411-2 V2.5.1 (2023-10) policies QCP-n, QCP-n-qscd, QCP-l, QCP-l-qscd ETSI EN 319 411-1 V1.4.1 (2023-10) policies NCP, NCP+

C. I.CA EU Qualified CA-SK/RSA 10/2022

Issuer	CN = I.CA Root CA/RSA 05/2022
Subject Distinguished Name	CN **= I.CA EU Qualified CA-SK/RSA 10/2022** O = První certifikační autorita, s.r.o. organizationIdentifier = NTRSK-54869099 C = SK
Certificate Serial Number	05 f5 e5 34
SHA-256 fingerprint (qcask22_rsa.cer)	a045f6acb1f2d0d190ee07dfb6f6611374338bae1905ecb21918c0d7b19496ee
Applied policy requirements	EN 319 411-2 V2.5.1 (2023-10) policies QCP-n-qscd, QCP-l-qscd

D. I.CA TSA CA/RSA 06/2022

Issuer	CN = I.CA Root CA/RSA 05/2022
Subject Distinguished Name	CN = **I.CA TSA CA/RSA 06/2022** O = První certifikační autorita, a.s. organizationIdentifier = NTRCZ-26439395 C = CZ
Certificate Serial Number	05 f5 e5 2b
SHA-256 fingerprint (2tsaca22_rsa.cer)	52b27152bd36bce43c76dd4f8e8068a39a2230ebcd21a354c27485d12ff6f9e1
Applied policy requirements	ETSI EN 319 411-2 V2.5.1 (2023-10) policy QCP-l

E. I.CA Public CA/RSA 06/2022

Issuer	CN = I.CA Root CA/RSA 05/2022
Subject Distinguished Name	CN = **I.CA Public CA/RSA 06/2022** O = První certifikační autorita, a.s. SERIALNUMBER = NTRCZ-26439395 C = CZ
Certificate Serial Number	05 f5 e5 27
SHA-256 fingerprint (pca22_rsa.cer)	df5baf6d7e1a7d14e9911c5b8c676ec6ebcad9354a74f4ac7314e133e07a94de
Applied policy requirements	ETSI EN 319 411-1 V1.4.1 (2023-10) 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. 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.