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
ELLIPTIC CURVE CRYPTOGRAPHY (ECC)

FOR MICROSOFT TRUSTED ROOT CERTIFICATE PROGRAM

NO. PCEB-N 22/05/02

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/ECC 12/2016**

(see chapter 1.3.1 A. for details)

Praha, 18/05/2022
(correction of audit period - 06/06/2022)

Ing. Martin Dudek
Lead auditor

Part I: Audit information

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

The audit period covered the period from 10/05/2021 to 09/05/2022.

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/ECC 12/2016) issuing certificates for subordinate CAs:

a) I.CA Qualified 2 CA/ECC 06/2019,
b) I.CA Public CA/RSA 12/2016.

These subordinate CAs are issuing certificates for end users.

1.2 Used audit standards

ETSI EN 319 411-1 V1.3.1 (2021-05) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements

ETSI EN 319 411-2 V2.4.1 (2021-11) 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 V1.4.4 (2021-05) 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 319 412-5 V2.3.1 (2020-04) 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

1.3 Audit targets

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

A. I.CA ROOT CA/ECC 12/2016

Issuer	CN = I.CA Root CA/ECC 12/2016
Subject Distinguished Name	CN = **I.CA Root CA/ECC 12/2016** O = První certifikační autorita, a.s. organizationidentifier = NTRCZ-26439395 C = CZ
Certificate Serial Number	05 f5 e1 01
SHA-256 fingerprint	b8 69 21 48 ff 49 c3 79 9f a2 34 7a e2 8b cc 52 89 62 35 12 b6 7d c1 91 70 45 2a de 24 ba 51 d5
Applied policy requirements	ETSI EN 319 411-1 V1.3.1 (2021-05) policies NCP, NCP+ ETSI EN 319 411-2 V2.4.1 (2021-11) policies QCP-n, QCP-n-qscd, QCP-l, QCP-l-qscd

B. I.CA QUALIFIED 2 CA/ECC 06/2019

Issuer	I.CA Root CA/ECC 12/2016
Subject Distinguished Name	CN = **I.CA Qualified 2 CA/ECC 06/2019** O = První certifikační autorita, a.s. organizationidentifier = NTRCZ-26439395 C = CZ
Certificate Serial Number	05 f5 e5 09
SHA-256 fingerprint	b7 fa c2 7a a6 88 e9 73 6c b6 3b bb 0c 8a a4 01 75 f6 a3 ea 6e 25 14 d7 34 31 1d ca c9 b5 a5 45
Applied policy requirements	ETSI EN 319 411-2 V2.4.1 (2021-11) policies QCP-n, QCP-n-qscd, QCP-l, QCP-l-qscd

C. I.CA Public CA/ECC 12/2016

Issuer	CN = I.CA Root CA/ECC 12/2016
Subject Distinguished Name	CN = **I.CA Public CA/ECC 12/2016** O = První certifikační autorita, a.s. organizationidentifier = NTRCZ-26439395 C = CZ
Certificate Serial Number	05 f5 e4 f0
SHA-256 fingerprint	a6 8f 0d e7 8d b7 c0 2a 78 bb 44 cc 46 92 9e 67 88 39 c8 93 54 0c 09 3f c7 41 3e 9e 31 25 a6 96
Applied policy requirements	ETSI EN 319 411-1 V1.3.1 (2021-05) 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 of the company První certifikační autorita, a.s. 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.