Member of TAYLLORCOX UK Ltd. 75 King William St., EC4N, London, UK
TAYLLORCOX PCEB, CAB No. 3239, accredited in accordance with ČSN EN ISO/IEC 17065:2013 by Czech Accreditation Institute (Certificate of accreditation No.: 91/2020, 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

AUDIT STATEMENT REPORT - I.CA ETSI ASSESSMENT 2021

ELLIPTIC CURVE CRYPTOGRAPHY (ECC)

NO. PCEB-N 21/05/02

Part I: Basic information

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:

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 V1.2.2 (2018-04) policies NCP, NCP+, ETSI EN 319 411-2 V2.2.2 (2018-04) policies policies QCP-n, QCP-n-qscd, QCP-l, QCP-l-qscd

Part II: Conformity evaluation of service

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

and

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

PART III: AUDIT INFORMATION

1.1 Audit period

The audit was performed as **full annual audit**, the audit period covered:

Audit period start date: 10/05/2020

Audit period end date: 09/05/2021

1.2 Audit scope

1.2.1 "HIERARCHICAL CERTIFICATE ISSUING AND MANAGEMENT SYSTEM"

compliance with:

1. ETSI EN 319 411-2 V2.2.2 (2018-04) policies:
    a) QCP-n Policy for EU qualified certificate issued to a natural person (for advanced electronic signatures)
    b) QCP-n-qscd Policy for EU qualified certificate issued to a natural person where the private key and the related certificate reside on a QSCD (for qualified electronic signatures)
    c) QCP-l Policy for EU qualified certificate issued to a legal person (for advanced electronic seals)
    d) QCP-l-qscd Policy for EU qualified certificate issued to a legal person where the private key and the related certificate reside on a QSCD (for qualified electronic seals)
2. ETSI EN 319 411-1 V1.2.2 (2018-04) policies:
    a) NCP: Normalized Certificate Policy
    b) NCP+: Enhanced Normalized Certificate Policy requiring a secure cryptographic device

The system consists of off-line root certification authority (I.CA Root CA/ECC 12/2016) issuing certificates for subordinate CAs (I.CA Qualified 2 CA/ECC 06/2019 and I.CA Public CA/ECC 12/2016), these subordinate CAs are issuing certificates for end users.

1.2.2 INFORMATION SECURITY RISK ANALYSIS

Information security risk analysis of trustworthy systems supporting "Hierarchical certificate issuing and management system" performed as a part of ETSI EN 319 411-1 and ETSI EN 319 411-2 requirements.

1.3 Audit requirements

1.3.1 Certification services provided by I.CA hierarchical structure of I.CA CAs

1. ETSI EN 319 401 V2.2.1 (2018-04) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
2. 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 (policies NCP, NCP+)
3. 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 (policies QCP-n, QCP-n-qscd, QCP-l, QCP-l-qscd)
4. ETSI EN 319 412-1 V1.4.1 (2020-06) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
5. 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
6. 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
7. ETSI EN 319 412-5 V2.3.1 (2020-04) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements
8. CEN/TS 419261 March 2015 Security requirements for trustworthy systems managing certificates and timestamps
9. ETSI TS 119 312 V1.3.1 (2019-02) Electronic Signatures and Infrastructures (ESI); Cryptographic Suites

1.3.2 I.CA's information security risk analysis

1. 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
2. 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
3. ISO/IEC 27002:2013 Information technology Security techniques - Information security management systems -Code of practice for information security controls

1.4 Audit targets

1.4.1 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 V1.2.2 (2018-04) policies NCP, NCP+ ETSI EN 319 411-2 V2.2.2 (2018-04) policies QCP-n, QCP-n-qscd, QCP-l, QCP-l-qscd
Policy and practice statement documents of the TSP (versions valid within audit period)	"Certifikační politika kořenové certifikační autority (kryptografie EC)" "The Root Qualified Certification Authority Certification Policy (EC Cryptography)" "Certifikační prováděcí směrnice (kryptografie EC)" " The Certification Practice Statement (EC Cryptography)"

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 V2.2.2 (2018-04) policies QCP-n, QCP-n-qscd, QCP-l, QCP-l-qscd
Policy and practice statement documents of the TSP (versions valid within audit period)	“Certifikační politika vydávání kvalifikovaných certifikátů pro elektronické podpisy (kryptografie EC)” “Certifikační politika vydávání kvalifikovaných certifikátů pro elektronické pečetě (kryptografie EC)” “Certifikační politika vydávání certifikátů OCSP respondérů (kryptografie EC)” "Certifikační prováděcí směrnice (kryptografie EC)"

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 V1.2.2 (2018-04) policies NCP, NCP+
Policy and practice statement documents of the TSP (versions valid within audit period)	“Certifikační politika vydávání komerčních certifikátů (kryptografie EC)” “Certifikační politika vydávání komerčních technologických certifikátů (kryptografie EC)” “Certifikační politika vydávání certifikátů OCSP respondérů (kryptografie EC)” "Certifikační prováděcí směrnice (kryptografie EC)"

1.4.2 I.CA's information security risk analysis

The target of audit, the I.CA's Information security risk analysis of trustworthy systems supporting "Hierarchical certificate issuing and management system", is described by the information contained in the internal, I.CA classified, documentation:

Approach to the information security risk assessment and treatment:

"Přístupy k posuzování a ošetřování rizik bezpečnosti informací - důvěryhodné systémy", version 3.3 as of 27/09/2019, I.CA

Scope of the information security management system (ISMS):

"Rozsah ISMS - důvěryhodné systémy", version 5.5 as of 08/02/2021, I.CA

Information security risk assessment and treatment:

"Analýza rizik - Důvěryhodné systémy Závěrečná zpráva", version 1.2 as of February 2021, I.CA

"Výběr protiopatření - důvěryhodné systémy", version 1.6 as of 09/02/2021, I.CA

"Zbytková rizika - důvěryhodné systémy", version 2.6 as of 11/02/2021, I.CA

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.

1.5 Audit workflow

Schedule of audit:

Date	Activity
07/05/2021, 10/05/2021,	Stage 1 audit – verification of I.CA's documentation Location: Office of Auditor (TAYLLORCOX PCEB)
11/05/2021	Stage 2 audit – on site audit Location: Headquarters and operational premises of I.CA company
12/05/2021 – 14/05/2021	Audit Statement Report, Qualifying Attestation Letter Location: Office of Auditor (TAYLLORCOX PCEB)

Methodology:

1. ETSI EN 319 403-1 V2.3.1 (2020-06) "Electronic Signatures and Infrastructures (ESI); Trust Service Provider
   Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers"
2. ETSI TS 119 403-2 V1.2.4 (2020-11) "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 2: Additional requirements for Conformity Assessment Bodies auditing Trust Service Providers that issue Publicly-Trusted Certificates"
3. ETSI TS 119 403-3 V1.1.1 (2019-03) "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 3: Additional requirements for conformity assessment bodies assessing EU qualified trust service providers"
4. ISO/IEC 17065:2012 Conformity assessment - Requirements for bodies certifying products, processes and services.

Documentation and procedures:
Policies and practices that rule the provision and operation of the certification services
Policies and practices to the information security risk assessment and treatment

Part IV: Audit conclusion

Auditor confirms that the examination of I.CA's "Hierarchical certificate issuing and management system" supporting EC Cryptography (chapter 1.4.1) and "Information security risk analysis of its supporting trustworthy systems" (chapter 1.4.2) was conducted in accordance with ETSI standards, in particular EN 319411-1, EN 319411-2, EN 319 403-1, TS 119 403-2, TS 119 403-3.

The results of examination based on auditor's observations, review of relevant documentation (including web www.ica.cz) and test of administrative and operational procedures and implemented respective controls concluded to the auditor's statement that audited certification services of the company První certifikační autorita, a.s.

comply

with requirements of 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 and of 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.

Part V: Signature and confirmation of audit report

Signature of lead auditor:

Ing. Martin Dudek

Praha: 18/05/2021