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 2024

I.CA ROOT CA/RSA 05/2022

NO. PCEB-N 24/05/02

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/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 policies QCP-n, QCP-n-qscd, QCP-l, QCP-l-qscd

Part II: Conformity evaluation of service

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

and

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

PART III: AUDIT INFORMATION

1.1 Audit period

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

Audit period start date: 10/05/2023

Audit period end date: 09/05/2024

1.2 Audit scope

1.2.1 "HIERARCHICAL CERTIFICATE ISSUING AND MANAGEMENT SYSTEM"

Compliance with:

1. ETSI EN 319 411-2 V2.5.1 (2023-10) policies:
    a) QCP-n: certificate policy for EU qualified certificate issued to natural persons (for advanced electronic signatures)
    b) QCP-n-qscd: certificate policy for EU qualified certificates issued to natural persons with private key related to the certified public key in a QSCD (for qualified electronic signatures)
    c) QCP-l: certificate policy for EU qualified certificate issued to legal persons (for advanced electronic seals)
    d) QCP-l: certificate policy for EU qualified certificate issued to legal persons (for advanced electronic seals) + PSD2
    e) QCP-l-qscd: certificate policy for EU qualified certificate issued to legal persons with private key related to the certified public key in a QSCD (for qualified electronic seals)
    f) QCP-l-qscd: certificate policy for EU qualified certificate issued to legal persons where the private key and the related certificate reside on a QSCD (for qualified electronic seals) + PSD2
2. ETSI EN 319 411-1 V1.4.1 (2023-10) policies:
    a) NCP: Normalized Certificate Policy
    b) NCP+: Normalized Certificate Policy requiring a secure cryptographic device

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.

1.2.2 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 V2.3.1 (2021-05) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
2. 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 (policies NCP, NCP+)
3. 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 (policies QCP-n, QCP-n-qscd, QCP-l, QCP-l-qscd)
4. ETSI EN 319 412-1 V1.5.1 (2023-09) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
5. 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
6. 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
7. ETSI EN 319 412-5 V2.4.1 (2023-09) 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 V1.4.3 (2023-08) Electronic Signatures and Infrastructures (ESI); Cryptographic Suites

1.3.2 I.CA's information security risk analysis

1. 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
2. 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
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/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
Policy and practice statement documents of the TSP (versions valid within audit period)	"Certifikační politika kořenové kvalifikované certifikační autority (algoritmus RSA)" „The Root Certification Authority Certificate Policy (RSA Algorithm)“ "Certifikační prováděcí směrnice (algoritmus RSA)" “The Certification Practice Statement (RSA Algorithm)” “Certifikační politika vydávání certifikátů OCSP respondérů (algoritmus RSA)” “The Certificate Policy for Issuing Certificates for OCSP Responders (RSA Algorithm)“

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
Policy and practice statement documents of the TSP (versions valid within	“Certifikační politika vydávání kvalifikovaných certifikátů pro elektronické podpisy (algoritmus RSA)” “Certifikační politika vydávání systémových certifikátů (algoritmus RSA)” “Certifikační politika vydávání kvalifikovaných certifikátů pro elektronické

audit period)	pečetě (algoritmus RSA)" "Certifikační politika vydávání kvalifikovaných certifikátů pro elektronické pečetě PSD2[1] (algoritmus RSA)" "Certifikační politika vydávání kvalifikovaných certifikátů pro elektronické podpisy na dálku (algoritmus RSA)" "Certifikační politika vydávání kvalifikovaných certifikátů pro elektronické pečetě na dálku (algoritmus RSA)" "Certifikační politika vydávání kvalifikovaných certifikátů pro elektronické podpisy prostřednictvím NKČR (algoritmus RSA)" "Certifikační politika vydávání certifikátů OCSP respondérů (algoritmus RSA)" "Certifikační prováděcí směrnice (algoritmus RSA)"

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
Policy and practice statement documents of the TSP (versions valid within audit period)	"Certifikační politika vydávání kvalifikovaných certifikátů pro elektronické podpisy dle legislativy SR (algoritmus RSA)" "Certifikační politika vydávání kvalifikovaných mandátních certifikátů dle legislativy SR (algoritmus RSA)" "Certifikační politika vydávání kvalifikovaných certifikátů pro elektronické pečetě dle legislativy SR (algoritmus RSA)" "Certifikační politika vydávání kvalifikovaných certifikátů pro vzdálené podepisování dle legislativy SR (algoritmus RSA) (algoritmus RSA)" "Certifikační politika vydávání certifikátů OCSP respondérů dle legislativy SR (algoritmus RSA)" "Certifikační prováděcí směrnice (algoritmus RSA)"

[1] ETSI TS 119 495 V1.6.1 (2022-11) Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Certificate Profiles and TSP Policy Requirements for Open Banking.

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
Policy and practice statement documents of the TSP (versions valid within audit period)	"Certifikační politika vydávání kvalifikovaných certifikátů pro elektronickou pečeť systému TSA2 (algoritmus RSA)" "Certifikační politika vydávání certifikátů OCSP respondérů (algoritmus RSA)" "Certifikační prováděcí směrnice (algoritmus RSA)"

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+
Policy and practice statement documents of the TSP (versions valid within audit period)	"Certifikační politika vydávání komerčních certifikátů (algoritmus RSA)" "Certifikační politika vydávání komerčních technologických certifikátů (algoritmus RSA)" „Certifikační politika vydávání komerčních certifikátů pro systém elektronické identifikace (algoritmus RSA)" "Certifikační politika vydávání certifikátů OCSP respondérů (algoritmus RSA)" "Certifikační prováděcí směrnice (algoritmus RSA)"

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 3.4 as of 20/04/2023, I.CA

Scope of the information security management system (ISMS):

"Rozsah ISMS - důvěryhodné systémy", version 6.1 as of 30/04/2024, I.CA

Information security risk assessment and treatment:

"Analýza rizik - Důvěryhodné systémy Závěrečná zpráva", version 1.8 as of 30/04/2024, I.CA

"Výběr protiopatření - důvěryhodné systémy", version 2.1 as of 01/11/2023, I.CA

"Zbytková rizika - důvěryhodné systémy", version 3.1 as of 01/11/2023, 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. 2211217661, valid until 20.11.2025.

1.5 Audit workflow

Schedule of audit:

Date	Activity
13.5.2024	Stage 1 audit – verification of I.CA's documentation Location: Office of Auditor (TAYLLORCOX PCEB)
16.5.2024	Stage 2 audit – on site audit Location: Headquarters and operational premises of I.CA company
17.5.2024	Qualifying Attestation Letter, Audit Statement Report 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 V1.3.1 (2023-03) "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

1.6 QUALIFYING ATTESTATION LETTER

The Qualifying Attestation Letter is a separate annex to this report. It was issued together with this report and contains the same identifier PCEB-N 24/05/02.

Part IV: Audit conclusion

Auditor confirms that the examination of I.CA's "Hierarchical certificate issuing and management system" supporting RSA algorithm (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 and, where applicable, has considered all current requirements of ETSI TS 119 495.
.

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 V1.4.1 (2023-10) 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 V2.5.1 (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.

Part V: Signature and confirmation of audit report

Signature of lead auditor:

Ing. Martin Dudek

Praha: 21/05/2024