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 2023

I.CA TLS ROOT CA/RSA 05/2022

NO. PCEB-N 23/07/01

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 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 (rcatls22_rsa.cer)	f9a17a00e5c294ba9614a715819af57f3fd48cc413453fbb8a5fc7e97964e2bc
Applied policy requirements	ETSI EN 319 411-1 V1.3.1 (2021-05) policies NCP, NCP+, DVCP, OVCP, EVCP ETSI EN 319 411-2 V2.4.1 (2021-11) 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)

Part II: Conformity evaluation of service

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

and

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

PART III: AUDIT INFORMATION

This report fully replaces report No. PCEB-N 23/05/05. Certificate No. PCEB-N 23/05/05 remains valid.

1.1 Audit period

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

Audit period start date: 10/05/2022

Audit period end date: 09/05/2023

1.2 Audit scope

1.2.1 "HIERARCHICAL CERTIFICATE ISSUING AND MANAGEMENT SYSTEM"

compliance with:

1. ETSI EN 319 411-2 V2.4.1 (2021-11) policies:
    a) QEVCP-w: certificate policy for EU qualified website authentication certificates based on EVCP
    b) QEVCP-w: certificate policy for EU qualified website authentication certificates based on EVCP + PSD2
    c) QCP-n: certificate policy for EU qualified certificate issued to natural persons (for advanced electronic signatures)
    d) 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)
    e) QCP-l: certificate policy for EU qualified certificate issued to legal persons (for advanced electronic seals)
    f) QCP-l: certificate policy for EU qualified certificate issued to legal persons (for advanced electronic seals) + PSD2
    g) 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)
    h) 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 V1.3.1 (2021-05) policies:
    a) DVCP: Domain Validation Certificate Policy for TLS/SSL certificates

b) OVCP: Organizational Validation Certificate Policy for TLS/SSL certificates
c) EVCP: Extended Validation Certificate Policy for TLS/SSL certificates
d) NCP: Normalized Certificate Policy
e) NCP+: Normalized Certificate Policy requiring a secure cryptographic device

The system consists of off-line root certification authority (I.CA TLS 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 assures that no other non-revoked Sub-CA's technically capable of issuing SSL/TLS certificates have been issued by this Root-CA.

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.

1.2.3

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 V1.3.1 (2021-05) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements (policies NCP, NCP+, DVCP, OVCP, EVCP)
3. 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 (policies QCP-n, QCP-n-qscd, QCP-l, QCP-l-qscd, QEVCP-w)
4. 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 (policy QCP-w-psd2)
5. ETSI EN 319 412-1 V1.4.4 (2021-05) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
6. 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
7. 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
8. ETSI EN 319 412-4 V1.2.1 (2021-11) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates

9. ETSI EN 319 412-5 V2.3.1 (2020-04) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements
10. CA/Browser Forum: "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates", version 1.8.6
11. CA/Browser Forum: "Guidelines for the Issuance and Management of Extended Validation Certificates", version 1.8.0
12. CEN/TS 419261 March 2015 Security requirements for trustworthy systems managing certificates and timestamps
13. ETSI TS 119 312 V1.4.2 (2022-02) Electronic Signatures and Infrastructures (ESI); Cryptographic Suites

1.3.2 I.CA's information security risk analysis

1. ETSI EN 319 411-1 V1.3.1 (2021-05) 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 V2.4.1 (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
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 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 V1.3.1 (2021-05) policies NCP, NCP+, DVCP, OVCP, EVCP ETSI EN 319 411-2 V2.4.1 (2021-11) 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)
Policy and practice statement documents of the TSP (versions valid within audit period)	"Certifikační politika kořenové certifikační autority pro TLS certifikáty (algoritmus RSA)" „The Root Certification Authority for TLS Certificates Certification Policy (RSA Algorithm)“ "Certifikační prováděcí směrnice (algoritmus RSA)" “The Certification Practice Statement (RSA Algorithm)”

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 V1.3.1 (2021-05) policy EVCP ETSI EN 319 411-2 V2.4.1 (2021-11) 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)
Policy and practice statement documents of the TSP (versions valid within audit period)	"Certifikační politika vydávání kvalifikovaných certifikátů pro autentizaci internetových stránek právnickým osobám (algoritmus RSA)" "Certifikační politika vydávání kvalifikovaných certifikátů pro autentizaci internetových stránek právnickým osobám PSD2[1] (algoritmus RSA)" "Certifikační politika vydávání certifikátů OCSP respondérů (algoritmus RSA)" "Certifikační prováděcí směrnice (algoritmus RSA)"

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 V1.3.1 (2021-05) policies DVCP, OVCP, NCP, NCP+
Policy and practice statement documents of the TSP (versions valid within audit period)	"Certifikační politika vydávání SSL certifikátů (algoritmus RSA)" "Certifikační politika vydávání certifikátů OCSP respondérů (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

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 5.9 as of 11/04/2023, I.CA

Information security risk assessment and treatment:

"Analýza rizik - Důvěryhodné systémy Závěrečná zpráva", version 1.6 as of April 2023, I.CA

"Výběr protiopatření - důvěryhodné systémy", version 2.0 as of 14/04/2023, I.CA

"Zbytková rizika - důvěryhodné systémy", version 3.0 as of 19/04/2023, 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
5.5.2023	Stage 1 audit – verification of I.CA's documentation Location: Office of Auditor (TAYLLORCOX PCEB)
16.5.2023	Stage 2 audit – on site audit Location: Headquarters and operational premises of I.CA company
18.5.2023	Qualifying Attestation Letter, Audit Statement Report Location: Office of Auditor (TAYLLORCOX PCEB)
19.7. – 20.7.2023	According to ALV's request, compliance with the NCP, NCP+, QCP-l, QCP-n, QCP-l-qscd, QCP-n-qscd standards was re-verified and their addition to the respective output reports.
21.7.2023	Qualifying Attestation Letter, Audit Statement Report The change compared to Report No. PCEB-N 23/05/05 is the listing of all standards that CAs meet, not just those that CAs use. 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 23/07/01.

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 and CA/Browser Forum Requirements.

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 V1.3.1 (2021-05) 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 V2.4.1 (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.

Part V: Signature and confirmation of audit report

Signature of lead auditor:

Ing. Martin Dudek

Prague: 21/07/2023