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: https://www.cai.cz/?subjekt=3239-tayllorcox-s-r-o&lang=en)
Company address: Na Florenci 1055/35, Praha 1 - Nové Město, CZ 110 00, audit@tayllorcox.com

AUDIT STATEMENT REPORT

I.CA ETSI ASSESSMENT 2026

I.CA ROOT CA/RSA 05/2022

I.CA ROOT CA/ECC 05/2022

I.CA TLS ROOT CA/RSA 05/2022

I.CA ROOT CA/RSA

NO. PCEB-N 26/07/06

Part I: Basic information

Conformity assessment body (CAB, auditor name):

TAYLLORCOX PCEB,
TAYLLORCOX s.r.o.
Identification No.: 279 02 587
Křižíkova 2136/2a
Praha 8
CZ 186 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 CAs:

Subject Distinguished Name	CN = **I.CA Root CA/RSA 05/2022** O = První certifikační autorita, a.s. organizationIdentifier = NTRCZ-26439395 C = CZ
Certificate Serial Number	05 f5 e1 02
SHA-256 fingerprint (rca22_rsa.der)	d279c01a12e8dd9a6230e459faa447ceb336998477338c2ee4135c96737418eb
Applied policy requirements	ETSI EN 319 411-1 V1.5.1 (2025-04) NCP, NCP+ policies ETSI EN 319 411-2 V2.6.1 (2025-06) QCP-n, QCP-n-qscd, QCP-l, QCP-l-qscd policies

Subject Distinguished Name	**CN = I.CA Root CA/ECC 05/2022** O = První certifikační autorita, a.s. organizationidentifier = NTRCZ-26439395 C = CZ
Certificate Serial Number	05 f5 e1 03
SHA-256 fingerprint (rca22_ecc.der)	3808ce3e961ca532682ffb8708b544e8f175aa065601a45902df92128fc38532
Applied policy requirements	ETSI EN 319 411-1 V1.5.1 (2025-04) NCP, NCP+ policies ETSI EN 319 411-2 V2.6.1 (2025-06) QCP-n, QCP-n-qscd, QCP-l, QCP-l-qscd policies

Subject Distinguished Name	**CN=I.CA TLS Root CA/RSA 05/2022** O=První certifikační autorita, a.s. organizationIdentifier=NTRCZ-26439395, C=CZ
Certificate Serial Number	05 f5 e5 2e
SHA-256 fingerprint (rcatls22_rsa.der)	f9a17a00e5c294ba9614a715819af57f3fd48cc413453fbb8a5fc7e97964e2bc
Applied policy requirements	ETSI EN 319 411-1 V1.5.1 (2025-04) NCP, NCP+, DVCP, OVCP, EVCP policies ETSI EN 319 411-2 V2.6.1 (2025-06) QCP-n, QCP-n-qscd, QCP-l, QCP-l-qscd, QEVCP-w policies

Subject Distinguished Name	**CN=I.CA Root CA/RSA** O=První certifikační autorita, a.s. serialNumber=NTRCZ-26439395, C=CZ
Certificate Serial Number	05 f5 e1 00
SHA-256 fingerprint (rca15_rsa.der)	d3d607a9ff24a19523b6da9d2c649446f8788cb96d9fd130972e120c13677730
Applied policy requirements	ETSI EN 319 411-1 V1.5.1 (2025-04) NCP, NCP+ policies ETSI EN 319 411-2 V2.6.1 (2025-06) QCP-n, QCP-n-qscd, QCP-l, QCP-l-qscd policies

Part II: Conformity evaluation of service

ETSI EN 319 411-1 V1.5.1 (2025-04) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements

ETSI EN 319 411-2 V2.6.1 (2025-06) 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 TS 119 411-6 V1.1.1 (2023-08) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 6: Requirements for Trust Service Providers issuing publicly trusted S/MIME certificates.

CA/Browser Forum:

- Network and Certificate System Security Requirements, version 2.0.5
- Guidelines for the Issuance and Management of Extended Validation Certificates, version 2.0.2
- Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, version 2.2.6
- Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, version 1.0.14

PART III: AUDIT INFORMATION

1.1 Audit period

The Standard, TLS-BR, TLS-EV audits were performed as **full annual audit** (including Guidelines for the Issuance and Management of Extended Validation Certificates, Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates and Network and Certificate System Security Requirements), the audit period covered:

Audit period start date: 10/05/2025

Audit period end date: 09/05/2026

1.2 Audit scope

1.2.1 "HIERARCHICAL CERTIFICATE ISSUING AND MANAGEMENT SYSTEM"

1.2.1.1 ROOT CERTIFICATION AUTHORITY (I.CA ROOT CA/RSA 05/2022)

1. ETSI EN 319 411- V2.6.1 (2025-06) policies:
    a) QCP-n: certificate policy for EU qualified certificate issued to natural persons
    b) QCP-n: certificate policy for EU qualified certificate issued to natural persons as amended by ETSI TS 119 411-6
    c) 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
    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 as amended by ETSI TS 119 411-6
    e) QCP-l: certificate policy for EU qualified certificate issued to legal persons
    f) QCP-l: certificate policy for EU qualified certificate issued to legal persons as amended by ETSI TS 119 411-6
    g) QCP-l: certificate policy for EU qualified certificate issued to legal persons + PSD2
    h) QCP-l: certificate policy for EU qualified certificate issued to legal persons + PSD2 as amended by ETSI TS 119 411-6
    i) 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
    j) 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 as amended by ETSI TS 119 411-6
    k) 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 + PSD2
    l) 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 + PSD2 as amended by ETSI TS 119 411-6
2. ETSI EN 319 411-1 V1.5.1 (2025-04) policies:
    a) NCP: Normalized Certificate Policy
    b) NCP: Normalized Certificate Policy as amended by ETSI TS 119 411-6
    c) NCP+: Normalized Certificate Policy requiring a secure cryptographic device
    d) NCP+: Normalized Certificate Policy requiring a secure cryptographic device as amended by ETSI TS 119 411-6

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 TSA CA/RSA 06/2022 (no S/MIME certificates)
c) I.CA Public CA/RSA 06/2022
d) I.CA EU Qualified CA-SK/RSA 10/2022

These subordinate CAs are issuing certificates for end users.

1.2.1.2 ROOT CERTIFICATION AUTHORITY (I.CA ROOT CA/ECC 05/2022)

1. ETSI EN 319 411-2 V2.6.1 (2025-06) policies:

    a) QCP-n: certificate policy for EU qualified certificate issued to natural persons
    b) QCP-n: certificate policy for EU qualified certificate issued to natural persons as amended by ETSI TS 119 411-6
    c) 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
    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 as amended by ETSI TS 119 411-6
    e) QCP-l: certificate policy for EU qualified certificate issued to legal persons
    f) QCP-l: certificate policy for EU qualified certificate issued to legal persons as amended by ETSI TS 119 411-6
    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
    h) 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 as amended by ETSI TS 119 411-6

2. ETSI EN 319 411-1 V1.5.1 (2025-04) policies:

    a) NCP: Normalized Certificate Policy
    b) NCP: Normalized Certificate Policy as amended by ETSI TS 119 411-6
    c) NCP+: Normalized Certificate Policy requiring a secure cryptographic device
    d) NCP+: Normalized Certificate Policy requiring a secure cryptographic device as amended by ETSI TS 119 411-6

The system consists of off-line root certification authority (I.CA Root CA/ECC 05/2022) issuing certificates for subordinate CAs:

a) I.CA EU Qualified CA2/ECC 06/2022
b) I.CA Public CA/ECC 06/2022

These subordinate CAs are issuing certificates for end users.

1.2.1.3 ROOT CERTIFICATION AUTHORITY (I.CA TLS ROOT CA/RSA 05/2022)

1. ETSI EN 319 411-2 V2.6.1 (2025-06) 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
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
e) QCP-l: certificate policy for EU qualified certificate issued to legal persons
f) 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

2. ETSI EN 319 411-1 V1.5.1 (2025-04) 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.

1.2.1.4 ROOT CERTIFICATION AUTHORITY (I.CA ROOT CA/RSA)

1. ETSI EN 319 411-2 V2.6.1 (2025-06) policies:

a) QCP-n: certificate policy for EU qualified certificate issued to natural persons
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
c) QCP-l: certificate policy for EU qualified certificate issued to legal persons
d) QCP-l: certificate policy for EU qualified certificate issued to legal persons + 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
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
g) QEVCP-w: certificate policy for EU qualified website authentication certificates based on EVCP

2. ETSI EN 319 411-1 V1.5.1 (2025-04) policies:

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

The system consists of off-line root certification authority (I.CA Root CA/RSA) issuing certificates for subordinate CAs:

a) I.CA TSACA/RSA 05/2017 (no S/MIME certificates)
b) I.CA TSA CA/RSA 03/2022 (no S/MIME certificates)

These subordinate CAs issued certificates for system TSA.

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 ETSI EN 319 401 V3.1.1 (2024-06) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
2. ETSI EN 319 411-1 V1.5.1 (2025-04) 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 V2.6.1 (2025-06) 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 V1.6.1 (2025-06) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
5. ETSI EN 319 412-2 V2.4.1 (2025-06) 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 319 412-4 V1.4.1 (2025-06) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Part 4: Certificate profile for web site certificates
8. ETSI EN 319 412-5 V2.5.1 (2025-06) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements
9. ETSI TS 119 411-6 V1.1.1 (2023-08) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 6: Requirements for Trust Service Providers issuing publicly trusted S/MIME certificates
10. ETSI TS 119 461 V2.1.1 (2025-02) Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects
11. CEN/TS 419261 March 2015 Security requirements for trustworthy systems managing certificates and timestamps
12. ETSI TS 119 312 V1.5.1 (2024-12) Electronic Signatures and Infrastructures (ESI); Cryptographic Suites
13. Guidelines for the Issuance and Management of Extended Validation Certificates, version 2.0.2
14. Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates, version 2.2.6

1.3.2 I.CA's information security risk analysis

1. ETSI EN 319 411-1 V1.5.1 (2025-04) 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 V2.6.1 (2025-06) 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 27002:2022 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. organizationIdentifier = NTRCZ-26439395 C = CZ
Certificate Serial Number	05 f5 e1 02
SHA-256 fingerprint (rca22_rsa.der)	d279c01a12e8dd9a6230e459faa447ceb336998477338c2ee4135c96737418eb
Applied policy requirements	ETSI EN 319 411-1 V1.5.1 (2025-04) NCP, NCP+ policies ETSI EN 319 411-2 V2.6.1 (2025-06) QCP-n, QCP-n-qscd, QCP-l, QCP-l-qscd policies
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)“

a. 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. organizationIdentifier = NTRCZ-26439395 C = CZ
Certificate Serial Number	05 f5 e5 2a
SHA-256 fingerprint (2qca22_rsa.der)	5f9147824201b2e23d8e128f99adb9ec11c495796960fa0faef05f901a347c66

Applied policy requirements	ETSI EN 319 411-1 V1.5.1 (2025-04) NCP, NCP+ policies ETSI EN 319 411-2 V2.6.1 (2025-06) QCP-n, QCP-n-qscd, QCP-l, QCP-l-qscd policies
Policy and practice statement documents of the TSP (versions valid within audit period)	"Certifikační politika vydávání kvalifikovaných certifikátů pro elektronické podpisy (algoritmus RSA)" "Certifikační politika vydávání kvalifikovaných certifikátů pro elektronické 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)"

b. 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.der)	a045f6acb1f2d0d190ee07dfb6f6611374338bae1905ecb21918c0d7b19496ee
Applied policy requirements	ETSI EN 319 411-2 V2.6.1 (2025-06) QCP-n-qscd, QCP-l-qscd policies
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 V1.8.1 (2026-04) Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Certificate Profiles and TSP Policy Requirements for Open Banking.

c. 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.der)	52b27152bd36bce43c76dd4f8e8068a39a2230ebcd21a354c27485d12ff6f9e1
Applied policy requirements	ETSI EN 319 411-2 V2.6.1 (2025-06) QCP-l policy
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)"

d. 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. organizationIdentifier = 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 V1.5.1 (2025-04) NCP, NCP+ policies
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)"

B. I.CA ROOT CA/ECC 05/2022

Issuer	CN = I.CA Root CA/ECC 05/2022
Subject Distinguished Name	CN = **I.CA Root CA/ECC 05/2022** O = První certifikační autorita, a.s. organizationidentifier = NTRCZ-26439395 C = CZ
Certificate Serial Number	05 f5 e1 03
SHA-256 fingerprint (rca22_ecc.der)	3808ce3e961ca532682ffb8708b544e8f175aa065601a45902df92128fc38532
Applied policy requirements	ETSI EN 319 411-1 V1.5.1 (2025-04) NCP, NCP+ policies ETSI EN 319 411-2 V2.6.1 (2025-06) QCP-n, QCP-n-qscd, QCP-l, QCP-l-qscd policies
Policy and practice statement documents of the TSP (versions valid within audit period)	"Certifikační politika kořenové certifikační autority (kryptografie EC)" "The Root Certification Authority Certificate Policy (EC Cryptography)" "Certifikační prováděcí směrnice (kryptografie EC)" " The Certification Practice Statement (EC Cryptography)" “Certifikační politika vydávání certifikátů OCSP respondérů (kryptografie EC)” “The Certificate Policy for Issuing Certificates for OCSP Responders (EC Cryptography)“

a. I.CA EU QUALIFIED CA2/ECC 06/2022

Issuer	I.CA Root CA/ECC 05/2022
Subject Distinguished Name	CN = **I.CA EU Qualified CA2/ECC 06/2022** O = První certifikační autorita, a.s. organizationidentifier = NTRCZ-26439395 C = CZ
Certificate Serial Number	05 f5 e5 2c
SHA-256 fingerprint (2qca22_ecc.der)	a7cdf7f580ea9016fd3ae07f642f5fb58a971224e6c4e92a498a33537b2034c8
Applied policy requirements	ETSI EN 319 411-2 V2.6.1 (2025-06) QCP-n, QCP-n-qscd, QCP-l, QCP-l-qscd policies
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 kvalifikovaných certifikátů pro systém ZameKEP” “Certificate Policy for Issuing Qualified Certificates for ZameKEP System” “Certifikační politika vydávání certifikátů OCSP respondérů (kryptografie EC)” "Certifikační prováděcí směrnice (kryptografie EC)"

b. I.CA Public CA/ECC 06/2022

Issuer	CN = I.CA Root CA/ECC 05/2022
Subject Distinguished Name	CN = **I.CA Public CA/ECC 06/2022** O = První certifikační autorita, a.s. organizationidentifier = NTRCZ-26439395 C = CZ
Certificate Serial Number	05 f5 e5 28
SHA-256 fingerprint (pca22_ecc.der)	8f1924e14752d2264d905508ab3c48e2eaea860c9843573a96a347aeaed0ccaf
Applied policy requirements	ETSI EN 319 411-1 V1.5.1 (2025-04) NCP, NCP+ policies
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)"

C. 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. organizationidentifier = NTRCZ-26439395 C = CZ
Certificate Serial Number	05 f5 e1 04
SHA-256 fingerprint (rca22_rsa.der)	f9a17a00e5c294ba9614a715819af57f3fd48cc413453fbb8a5fc7e97964e2bc
Applied policy requirements	ETSI EN 319 411-1 V1.5.1 (2025-04) NCP, NCP+, DVCP, OVCP, EVCP policies ETSI EN 319 411-2 V2.6.1 (2025-06) QCP-l, QCP-n, QCP-l-qscd, QCP-n-qscd policies (based on EN 319411-1, NCP, NCP+), QEVCP-w policy (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 Certificate Policy (RSA Algorithm)“ "Certifikační prováděcí směrnice (algoritmus RSA)" “The Certification Practice Statement (RSA Algorithm)” “Certifikační politika vydávání certifikátů OCSP respondérů TLS (algoritmus RSA)” “Certificate Policy for Issuing Certificates for TLS OCSP Responders (RSA Algorithm)“

a. 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. organizationidentifier = NTRCZ-26439395 C = CZ
Certificate Serial Number	05 f5 e5 2f
SHA-256 fingerprint (qcw22_rsa.der)	b9ef51a5f69a974f8d290b0a75fb253b7339053002aecb6516a270ea88aef4ed
Applied policy requirements	ETSI EN 319 411-1 V1.5.1 (2025-04) EVCP policy ETSI EN 319 411-2 V2.6.1 (2025-06) QCP-l, QCP-n, QCP-l-qscd, QCP-n-qscd policies (based on EN 319411-1, NCP, NCP+), QEVCP-w policy (based on EN 319411-1, EVCP)
Policy and practice	“Certifikační politika vydávání kvalifikovaných certifikátů pro autentizaci

statement documents of the TSP (versions valid within audit period)	internetových stránek právnickým osobám (algoritmus RSA)" "Certifikační politika vydávání kvalifikovaných certifikátů pro autentizaci internetových stránek právnickým osobám PSD2[2] (algoritmus RSA)" "Certifikační politika vydávání certifikátů OCSP respondérů TLS (algoritmus RSA)" "Certifikační prováděcí směrnice (algoritmus RSA)"

b. 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. organizationidentifier = 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 V1.5.1 (2025-04) DVCP, OVCP, NCP, NCP+ policies
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 TLS (algoritmus RSA)" "Certifikační prováděcí směrnice (algoritmus RSA)"

D. I.CA ROOT CA/RSA

Issuer	CN = I.CA Root CA/RSA
Subject Distinguished Name	CN = **I.CA Root CA/RSA** O = První certifikační autorita, a.s. serialNumber = NTRCZ-26439395 C = CZ
Certificate Serial Number	05 f5 e1 00
SHA-256 fingerprint (rca22_rsa.der)	d3d607a9ff24a19523b6da9d2c649446f8788cb96d9fd130972e120c13677730
Applied policy requirements	ETSI EN 319 411-1 V1.5.1 (2025-04) NCP, NCP+ policies ETSI EN 319 411-2 V2.6.1 (2025-06) QCP-n, QCP-n-qscd, QCP-l, QCP-l-qscd policies
Policy and practice	"Certifikační politika kořenové kvalifikované certifikační autority (algoritmus

[2] 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

statement documents of the TSP (versions valid within audit period)	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)“

a. I.CA TSACA/RSA 05/2017

Issuer	CN = I.CA Root CA/RSA
Subject Distinguished Name	CN = **I.CA TSACA/RSA 05/2017** O = První certifikační autorita, a.s. serialNumber = NTRCZ-26439395 C = CZ
Certificate Serial Number	05 f5 e4 f4
SHA-256 fingerprint (tsaca17_rsa.der)	4ab8bc6061743e0980bfd121370a88c511c4f29eb4bc089765886b64c791f768
Applied policy requirements	ETSI EN 319 411-2 V2.6.1 (2025-06) QCP-l policy
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)"

b. I.CA TSACA/RSA 03/2022

Issuer	CN = I.CA Root CA/RSA
Subject Distinguished Name	CN = **I.CA TSACA/RSA 03/2022** O = První certifikační autorita, a.s. serialNumber = NTRCZ-26439395 C = CZ
Certificate Serial Number	05 f5 e5 22
SHA-256 fingerprint (tsaca22rsa.der)	6ab6349834712b0d898c5700fe4e1a9c203c5b98fef57187101689081997f27f
Applied policy requirements	ETSI EN 319 411-2 V2.6.1 (2025-06) QCP-l policy
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)"

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 3.5 as of 11/11/2024, I.CA

Scope of the information security management system (ISMS):

"Rozsah ISMS - důvěryhodné systémy", version 6.3 as of 25/04/2025, I.CA

Information security risk assessment and treatment:

"Analýza rizik - Důvěryhodné systémy Závěrečná zpráva", version 2.0 as of 25/04/2025, I.CA

"Výběr protiopatření - důvěryhodné systémy", version 2.4 as of 20/10/2025, I.CA

"Zbytková rizika - důvěryhodné systémy", version 3.4 as of 22/10/2025, 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 27001:2022 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. 2511214271, valid until 20.11.2028.

1.5 Audit workflow

Schedule of audit:

Date	Activity
2026-06-26 to 2026-07-08	Stage 1 audit – verification of I.CA's documentation Location: Office of Auditor (TAYLLORCOX PCEB)
2026-07-22 to 2026-07-23	Stage 2 audit – on site audit Location: Headquarters and operational premises of I.CA company
2026-07-23	Qualifying Attestation Letters Location: Office of Auditor (TAYLLORCOX PCEB)
2026-07-31	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 LETTERS

The Qualifying Attestation Letters are a separate annex to this report. It was issued together with this report and contains the identifier PCEB-N 26/07/02 (Standard), PCEB-N 26/07/03 (TLS BR), PCEB-N 26/07/04 (TLS EV) and PCEB-N 26/07/05 (SMIME).

Part IV: Audit conclusion

Auditor confirms that the examination of I.CA's "Hierarchical certificate issuing and management system" supporting RSA and ECC algorithms (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, ETSI TS 119 411-6 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 V1.5.1 (2025-04) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements, of ETSI EN 319 411-2 V2.6.1 (2025-06) 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 and of ETSI TS 119 411-6 V1.1.1 (2023-08) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 6: Requirements for Trust Service Providers issuing publicly trusted S/MIME certificates.

Part V: Signature and confirmation of audit report

Signature of lead auditor:



Ing. Martin Dudek

Praha: 2026-07-31