SMIME BR and NetSec Audit Attestation for

První certifikační autorita, a.s.

Reference: PCEB-N 25/10/01

"Prague, 2025-10-16"

To whom it may concern,

This is to confirm that "TAYLLORCOX PCEB established by TAYLLORCOX s.r.o." has audited the CAs of the "První certifikační autorita, a.s" without critical findings.

This present Audit Attestation Letter is registered under the unique identifier number "PCEB-N 25/10/01" covers multiple Root-CAs and consists of 12 pages.

Kindly find here below the details accordingly.

In case of any question, please contact:

TAYLLORCOX PCEB established by TAYLLORCOX s.r.o.
Na Florenci 1055/35
110 00 Praha 1, Czech Republic
E-Mail: audit@tayllorcox.com
Phone: +420 725 536 797

With best regards,

Ing. Martin Dudek
Lead auditor

General audit information

Identification of the conformity assessment body (CAB) and assessment organization acting as ETSI auditor
• TAYLLORCOX PCEB established by TAYLLORCOX s.r.o., Na Florenci 1055/35, 110 00 Praha 1, Czech Republic, registered under company ID 0027902587. • Accredited by Český institut pro akreditaci, o.p.s. (Czech Accreditation Institute) under registration https://www.cai.cz/?subjekt=3239-tayllorcox-s-r-o&lang=en[1] for the certification of trust services according to “EN ISO/IEC 17065:2012” and “ETSI EN 319 403-1 V2.3.1 (2020-06)”. • Insurance Carrier (BRG section 8.2): Allianz pojišťovna, a.s., Ke Štvanici 656/3 186 00 Praha 8, Czech Republic, registered under company national ID 47115971. • Third-party affiliate audit firms involved in the audit: None.
Identification and qualification of the audit team
• Number of team members: 2 • Academic qualifications of team members: All team members have formal academic qualifications or professional training or extensive experience indicating general capability to carry out audits based on the knowledge given below and at least four years full time practical workplace experience in information technology, of which at least two years have been in a role or function relating to relevant trust services, public key infrastructure, information security including risk assessment/management, network security and physical security. • Additional competences of team members: • All team members have knowledge of 1) audit principles, practices and techniques in the field of CA/TSP audits gained in a training course of at least five days; 2) the issues related to various areas of trust services, public key infrastructure, information security including risk assessment/management, network security and physical security; 3) the applicable standards, publicly available specifications and regulatory requirements for CA/TSPs and other relevant publicly available specifications including standards for IT product evaluation; and 4) the Conformity Assessment Body's processes. Furthermore, all team members have language skills appropriate for all organizational levels within the CA/TSP organization; note-taking, report-writing, presentation, and interviewing skills; and relevant personal attributes: objective, mature, discerning, analytical, persistent and realistic. • Professional training of team members: See “Additional competences of team members” above. Apart from that are all team members trained to demonstrate adequate competence in: a) knowledge of the CA/TSP standards and other relevant publicly available specifications; b) understanding functioning of trust services and information security including network security issues; c) understanding of risk assessment and risk management from the business perspective;

[1] URL to the accreditation certificate hosted by the national accreditation body

d) technical knowledge of the activity to be audited; e) general knowledge of regulatory requirements relevant to TSPs; and f) knowledge of security policies and controls. • Types of professional experience and practical audit experience: The CAB ensures, that its personnel performing audits maintains competence on the basis of appropriate education, training or experience; that all relevant experience is current and prior to assuming responsibility for performing as an auditor, the candidate has gained experience in the entire process of CA/TSP auditing. This experience shall have been gained by participating under supervision of lead auditors in a minimum of four TSP audits for a total of at least 20 days, including documentation review, on-site audit and audit reporting. • Additional qualification and experience Lead Auditor: On top of what is required for team members (see above), the Lead Auditor a) has acted as auditor in at least three complete TSP audits; b) has adequate knowledge and attributes to manage the audit process; and c) has the competence to communicate effectively, both orally and in writing. • Special skills or qualifications employed throughout audit: None. • Special Credentials, Designations, or Certifications: All members are qualified and registered assessors within the accredited CAB. • Auditors code of conduct incl. independence statement: Code of Conduct as of Annex A, ETSI EN 319 403 or ETSI EN 319 403-1 respectively.
Identification and qualification of the reviewer performing audit quality management
• Number of Reviewers/Audit Quality Managers involved independent from the audit team: 1 • The reviewer fulfils the requirements as described for the Audit Team Members above and has acted as an auditor in at least three complete CA/TSP audits.

Identification of the CA / Trust Service Provider (TSP):	**První certifikační autorita, a.s.** Podvinný Mlýn 2178/6 Praha 9 - Libeň CZ 190 00 Identification No.: 264 39 395

Type of audit:	☐ Point in time audit ☐ Period of time, after x month of CA operation ☒ Period of time, full audit
Audit period covered for all policies:	2024-09-01 to 2025-08-31
Point in time date:	None
Audit dates:	2025-10-03 to 2025-10-06 (offline) 2025-10-07 to 2025-10-08 (on site)

Audit location:	CAB office – validation of TSP documentation (offline), První certifikační autorita, a.s. - providing evidence for audit purposes (on site)

Root 1: I.CA Root CA/RSA 05/2022

Standards considered:	European Standards: • ETSI EN 319 411-2 V2.5.1 (2023-10) • ETSI TS 119 411-6 V1.1.1 (2023-08) • ETSI EN 319 411-1 V1.4.1 (2023-10) • ETSI EN 319 401 V3.1.1 (2024-06) CA Browser Forum Requirements: • Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, version 1.0.11 • Network and Certificate System Security Requirements, version 2.0.5 For the Trust Service Provider Conformity Assessment: • ETSI EN 319 403-1 V2.3.1 (2020-06) • ETSI TS 119 403-2 V1.3.1 (2023-03)

The audit was based on the following policy and practice statement documents of the CA / TSP:

- Root Qualified Certification Authority Certificate Policy (RSA Algorithm), version 1.173, as of 2025-04-20
- Certifikační politika kořenové kvalifikované certifikační autority (algoritmus RSA), version 1.173, 2025-04-20
- Certification Practice Statement (RSA Algorithm), version 1.74, as of 2025-04-25
- Certifikační prováděcí směrnice (algoritmus RSA), version 1.74, 2025-04-25
- Certificate Policy for Issuing Certificates for OCSP Responders (RSA Algorithm), version 1.142, as of 2024-02-26
- Certifikační politika vydávání certifikátů OCSP respondérů (algoritmus RSA), version 1.142, 2024-02-26
- Certificate Policy for Issuing Qualified Certificates for Electronic Signatures (RSA Algorithm), version 1.185, as of 2025-08-16
- Certifikační politika vydávání kvalifikovaných certifikátů pro elektronické podpisy (algoritmus RSA), version 1.185, 2025-08-16
- Certificate Policy for Issuing Qualified Certificates for Electronic Seals (RSA Algorithm), version 1.044, as of 2025-08-16
- Certifikační politika vydávání kvalifikovaných certifikátů pro elektronické pečetě (algoritmus RSA), version 1.044, 2025-08-16
- Certificate Policy for Issuing Qualified Certificates for Electronic Seals PSD2 (RSA Algorithm), version 2.153, as of 2024-08-26
- Certifikační politika vydávání kvalifikovaných certifikátů pro elektronické pečetě PSD2 (algoritmus RSA), version 2.153, 2025-08-16
- Certificate Policy for Issuing Qualified Certificates for Remote Electronic Signatures (RSA Algorithm), version 1.023, as of 2025-08-16
- Certifikační politika vydávání kvalifikovaných certifikátů pro elektronické podpisy na dálku (algoritmus RSA), version 1.023, 2025-08-16

- Certificate Policy for Issuing Qualified Certificates for Remote Electronic Seals (RSA Algorithm), version 1.033, as of 2025-08-16
- Certifikační politika vydávání kvalifikovaných certifikátů pro elektronické pečetě na dálku (algoritmus RSA), version 1.033, 2025-08-16
- Certificate Policy for Issuing Qualified Certificates for Electronic Signatures through NKČR (RSA Algorithm), version 1.013, as of 2025-08-16
- Certifikační politika vydávání kvalifikovaných certifikátů pro elektronické podpisy prostřednictvím NKČR (algoritmus RSA), version 1.013, 2025-08-16
- Certificate Policy for Issuing Commercial Certificates (RSA Algorithm), version 1.176, as of 2025-08-16
- Certifikační politika vydávání komerčních certifikátů (algoritmus RSA), version 1.176, 2025-08-16
- Certificate Policy for Issuing Commercial Technological Certificates (RSA Algorithm), version 1.144, as of 2025-08-16
- Certifikační politika vydávání komerčních technologických certifikátů (algoritmus RSA), version 1.144, 2025-08-16
- Certificate Policy for Issuing Electronic Identification System Commercial Certificates (RSA Algorithm), version 1.034, 2025-08-16
- Certifikační politika vydávání komerčních certifikátů pro systém elektronické identifikace (algoritmus RSA), version 1.034, 2025-08-16
- Certificate Policy for Issuing Qualified Certificates for Electronic Signatures According to the Legislation of the Slovak Republic (RSA Algorithm), version 1.004, as of 2025-08-16
- Certifikační politika vydávání kvalifikovaných certifikátů pro elektronické podpisy dle legislativy SR (algoritmus RSA), version 1.004, 2025-08-16
- Certificate Policy for Issuing Qualified Mandate Certificates According to the Legislation of the Slovak Republic (RSA Algorithm), version 1.006, as of 2025-08-16
- Certifikační politika vydávání kvalifikovaných mandátních certifikátů dle legislativy SR (algoritmus RSA), version 1.006, 2025-08-16
- Certificate Policy for Issuing Qualified Certificates for Electronic Seals According to the Legislation of the Slovak Republic (RSA Algorithm), version 1.002, as of 2025-08-16
- Certifikační politika vydávání kvalifikovaných certifikátů pro elektronické pečetě dle legislativy SR (algoritmus RSA), version 1.002, 2025-08-16
- Certificate Policy for Issuing Qualifies Certificates for Remote Signing According to the Legislation of the Slovak Republic (RSA Algorithm), version 1.003, as of 2025-08-16
- Certifikační politika vydávání kvalifikovaných certifikátů pro vzdálené podepisování dle legislativy SR (algoritmus RSA), version 1.003, 2025-08-16
- Certifikační politika vydávání certifikátů OCSP respondérů dle legislativy SR (algoritmus RSA), version 1.00, 2022-10-15

A complete history of QTSP published documentation is available on its website https://www.ica.cz/Certification-policy.

No major or minor non-conformities have been identified during the audit.

Findings with regard to ETSI EN 319 401:
None.

Findings with regard to ETSI EN 319 411-1:
None.

Findings with regard to ETSI EN 319 411-2:
None.

Findings with regard to ETSI TS 119 411-6:
None.

Findings with regard to CA Browser Forum Requirements:
None.

All non-conformities have been closed before the issuance of this attestation.

To the best of our knowledge, no incidents have occurred within this Root-CA’s hierarchy during the audited period.

- No Bugs on audit scope were found

Distinguished Name	SHA-256 fingerprint	Applied policy
CN=I.CA Root CA/RSA 05/2022 O=První certifikační autorita, a.s. organizationIdentifier=NTRCZ-26439395 C=CZ	SHA-256 fingerprint of the certificate: rca22_rsa.der D279C01A12E8DD9A6230E459FAA447CEB336998477338C2EE4135C96737418EB	ETSI EN 319 411-2 V2.5.1, QCP-l, QCP-n, QCP-l-qscd, QCP-n-qscd ETSI EN 319 411-1 V1.4.1, NCP, NCP+

Table 1: Root-CA 1 in scope of the audit

The TSP named the Sub-CAs that have been issued by the aforementioned Root-CA, that are listed in the following table and that have been covered in this audit.

Distinguished Name	SHA-256 fingerprint	Applied policy
CN=I.CA EU Qualified CA2/RSA 06/2022 O=První certifikační autorita, a.s. organizationIdentifier=NTRCZ-26439395 C=CZ	SHA-256 fingerprint of the certificate: 2qca22_rsa.der 5F9147824201B2E23D8E128F99ADB9EC11C495796960FA0FAEF05F901A347C66	ETSI EN 319 411-2 V2.5.1, QCP-l, QCP-n, QCP-l-qscd, QCP-n-qscd ETSI EN 319 411-1 V1.4.1, NCP, NCP+
CN=I.CA Public CA/RSA 06/2022 O=První certifikační autorita, a.s. organizationIdentifier=NTRCZ-26439395 C=CZ	SHA-256 fingerprint of the certificate: pca22_rsa.der DF5BAF6D7E1A7D14E9911C5B8C676EC6EBCAD9354A74F4AC7314E133E07A94DE	ETSI EN 319 411-1 V1.4.1, NCP, NCP+
CN=I.CA EU Qualified CA-SK/RSA 10/2022 O=První certifikační autorita, s.r.o. organizationIdentifier=NTRSK-54869099 C=SK	SHA-256 fingerprint of the certificate: qcask22_rsa.der A045F6ACB1F2D0D190EE07DFB6F6611374338BAE1905ECB21918C0D7B19496EE	ETSI EN 319 411-2 V2.5.1, QCP-l-qscd, QCP-n-qscd

Table 2: Sub-CA’s issued by the Root-CA 1 or its Sub-CA’s in scope of the audit

Root 2: I.CA Root CA/ECC 05/2022

Standards considered:	European Standards: • ETSI EN 319 411-2 V2.5.1 (2023-10) • ETSI TS 119 411-6 V1.1.1 (2023-08) • ETSI EN 319 411-1 V1.4.1 (2023-10) • ETSI EN 319 401 V3.1.1 (2024-06) CA Browser Forum Requirements: • Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, version 1.0.11 • Network and Certificate System Security Requirements, version 2.0.5 For the Trust Service Provider Conformity Assessment: • ETSI EN 319 403-1 V2.3.1 (2020-06) • ETSI TS 119 403-2 V1.3.1 (2023-03)

The audit was based on the following policy and practice statement documents of the CA / TSP:

- Root Certification Authority Certificate Policy (EC Cryptography), version 1.053, as of 2025-04-20
- Certifikační politika kořenové certifikační autority (kryptografie EC), version 1.053, 2025-04-20
- Certification Practice Statement (EC Cryptography), version 1.07, as of 2025-04-25
- Certifikační prováděcí směrnice (kryptografie EC), version 1.07, 2025-04-25
- Certificate Policy for Issuing Certificates for OCSP Responders (EC Cryptography), version 1.022, as of 2024-02-26
- Certifikační politika vydávání certifikátů OCSP respondérů (kryptografie EC), version 1.022, 2024-02-26
- Certificate Policy for Issuing Qualified Certificates for Electronic Signatures (EC Cryptography), version 1.065, as of 2025-08-16
- Certifikační politika vydávání kvalifikovaných certifikátů pro elektronické podpisy (kryptografie EC), version 1.065, 2025-08-16
- Certificate Policy for Issuing Qualified Certificates for Electronic Seals (EC Cryptography), version 1.034, as of 2025-08-16
- Certifikační politika vydávání kvalifikovaných certifikátů pro elektronické pečetě (kryptografie EC), version 1.034, 2025-08-16
- Certificate Policy for Issuing Commercial Certificates (EC Cryptography), version 1.066, as of 2025-08-16
- Certifikační politika vydávání komerčních certifikátů (kryptografie EC), version 1.166, 2025-08-16
- Certificate Policy for Issuing Commercial Technological Certificates (EC Cryptography), version 1.034, as of 2025-08-16
- Certifikační politika vydávání komerčních technologických certifikátů (kryptografie EC), version 1.034, 2025-08-16

No major or minor non-conformities have been identified during the audit.

Findings with regard to ETSI EN 319 401:
None.

Findings with regard to ETSI EN 319 411-1:
None.

Findings with regard to ETSI EN 319 411-2:
None.

Findings with regard to ETSI TS 119 411-6:
None.

Findings with regard to CA Browser Forum Requirements:
None.

All non-conformities have been closed before the issuance of this attestation.

To the best of our knowledge, no incidents have occurred within this Root-CA’s hierarchy during the audited period.

- No Bugs on audit scope were found

Distinguished Name	SHA-256 fingerprint	Applied policy
CN=I.CA Root CA/ECC 05/2022 O=První certifikační autorita, a.s. organizationIdentifier=NTRCZ-26439395 C=CZ	SHA-256 fingerprint of the certificate: rca22_ecc.der 3808CE3E961CA532682FFB8708B544E8F175AA065601A45902DF92128FC38532	ETSI EN 319 411-2 V2.5.1, QCP-l, QCP-n, QCP-l-qscd, QCP-n-qscd ETSI EN 319 411-1 V1.4.1, NCP, NCP+

Table 3: Root-CA 2 in scope of the audit

The TSP named the Sub-CAs that have been issued by the aforementioned Root-CA, that are listed in the following table and that have been covered in this audit.

Distinguished Name	SHA-256 fingerprint	Applied policy
CN=I.CA EU Qualified CA2/ECC 06/2022 O=První certifikační autorita, a.s. organizationIdentifier=NTRCZ-26439395 C=CZ	SHA-256 fingerprint of the certificate: 2qca22_ecc.der A7CDF7F580EA9016FD3AE07F642F5FB58A971224E6C4E92A498A33537B2034C8	ETSI EN 319 411-2 V2.5.1, QCP-l, QCP-n, QCP-l-qscd, QCP-n-qscd
CN=I.CA Public CA/ECC 06/2022 O=První certifikační autorita, a.s. organizationIdentifier=NTRCZ-26439395 C=CZ	SHA-256 fingerprint of the certificate: pca22_ecc.der 8F1924E14752D2264D905508AB3C48E2EAEA860C9843573A96A347AEAED0CCAF	ETSI EN 319 411-1 V1.4.1, NCP, NCP+

Table 4: Sub-CA’s issued by the Root-CA 2 in scope of the audit

Modifications record

Version	Issuing Date	Changes
Version 1	2025-10-16	Initial attestation

End of the audit attestation letter.