

TLS EV Audit Attestation for

První certifikační autorita, a.s.

Reference: PCEB-N 26/07/04

"Prague, 2026-07-23"

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 26/07/04" covers a single Root-CA and consists of 8 pages.

Kindly find here below the details accordingly.

In case of any question, please contact:

TAYLLORCOX PCEB established by TAYLLORCOX s.r.o.
Křižíkova 2136/2a
19800 Praha 8, Czech Republic
E-Mail: audit@tayllorcox.com
Phone: +420 725 536 797

With best regards,

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., Křižíkova 2136/2a, 19800 Praha 8, 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-ro&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, 190 00 Praha 9 - Libeň, Czech Republic, registered under company ID 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:	2025-05-10 to 2026-05-09
Point in time date:	None
Audit dates:	2026-06-26 to 2026-07-08 (remote) 2026-07-22 to 2026-07-23 (on site)
Audit location:	CAB office – validation of TSP documentation (remote), První certifikační autorita, a.s. - providing evidence for audit purposes (on site)

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

Standards considered:	European Standards: - ETSI EN 319 411-2 V2.6.1 (2025-06) - ETSI EN 319 411-1 V1.5.1 (2025-04) - ETSI EN 319 401 V3.1.1 (2024-06) CA Browser Forum Requirements: - 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 - 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 for TLS Certificates Certificate Policy (RSA Algorithm)

Version	Release Date	Effective from	Effective until
Version 1.003	2025-04-20	2025-04-20	2026-04-19
Version 1.004	2026-04-20	2026-04-20	

- Certification Practice Statement (RSA Algorithm)

Version	Release Date	Effective from	Effective until
Version 1.74	2025-04-25	2025-04-25	2026-04-24
Version 1.75	2026-04-25	2026-04-25	

- Certificate Policy for Issuing Certificates for TLS OCSP Responders (RSA Algorithm)

Version	Release Date	Effective from	Effective until
Version 1.000	2024-02-26	2024-02-26	

- Certificate Policy for Issuing Qualified Certificates for Website Authentication to Legal Persons (RSA Algorithm)

Version	Release Date	Effective from	Effective until
Version 1.083	2025-04-23	2025-04-23	2026-04-22
Version 1.084	2026-04-23	2026-04-23	

- Certificate Policy for Issuing Qualified Certificates for Website Authentication to Legal Persons PSD2 (RSA Algorithm)

Version	Release Date	Effective from	Effective until
Version 1.193	2025-04-23	2025-04-23	2026-04-22
Version 1.194	2026-04-23	2026-04-23	

A history of QTSP published documentation is available on its website

<https://www.ica.cz/en/certification-policies>.

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.

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 were found within the audit scope.

Distinguished Name	SHA-256 fingerprint	Applied policy
CN=I.CA TLS Root CA/RSA 05/2022, O=První certifikační autorita, a.s., organizationIdentifier=NTRCZ-26439395, C=CZ	SHA-256 fingerprint of the certificate: rcats22_rsa.der F9A17A00E5C294BA9614A715819AF57F3FD48CC413453FBB8A5FC7E97964E2BC	ETSI EN 319 411-2 V2.6.1, QCP-I, QCP-n, QCP-I-qscd, QCP-n-qscd (based on ETSI EN 319 411-1 V1.5.1, NCP, NCP+), QEVCP-w (based on ETSI EN 319 411-1 V1.5.1, EVCP) ETSI EN 319 411-1 V1.5.1, NCP, NCP+, DVCP, OVCP, EVCP

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 TLS EV CA/RSA 06/2022 O=První certifikační autorita, a.s. organizationIdentifier=NTRCZ-26439395 C=CZ	SHA-256 fingerprint of the certificate: qcw22_rsa.der B9EF51A5F69A974F8D290B0A75FB253B7339053002AECB6516A270EA88AEF4ED	ETSI EN 319 411-2 V2.6.1, QCP-I, QCP-n, QCP-I-qscd, QCP-n-qscd (based on ETSI EN 319 411-1 V1.5.1, NCP, NCP+), QEVCP-w (based on ETSI EN 319 411-1 V1.5.1, EVCP) ETSI EN 319 411-1 V1.5.1, EVCP

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

Key pairs without a corresponding certificate ("parked keys")

None.

Modifications record

Version	Issuing Date	Changes
Version 1	2026-07-23	Initial attestation
...	...	...

End of the audit attestation letter.