Standard Audit Attestation for

Česká pošta s.p. (hereinafter PostSignum)

Reference: PCEB-N 26/10/01

"Prague, 2026-10-23"

To whom it may concern,

This is to confirm that "TAYLLORCOX PCEB established by TAYLLORCOX s.r.o." has audited the CAs of the "Česká pošta s.p. (hereinafter PostSignum)" without critical findings.

This present Audit Attestation Letter is registered under the unique identifier number "PCEB-N 26/10/01" covers a single Root-CA and consists of 10 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
186 00 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, 186 00 Praha 8, Czech Republic, registered under ID 0027902587 • Accredited by Český institut pro akreditaci, o.p.s. (Czech Accreditation Institute) under registration https://www.cai.cz/en/?subjekt=3239-tayllorcox-s-r-o[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):	Česká pošta s.p. (hereinafter PostSignum), Politických vězňů 909/4, 255 99 Praha 1, Czech Republic, registered under No.: 47114983

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:	2025-10-23 to 2026-10-22
Point in time date:	none
Audit dates:	2026-10-09 (remote) 2026-10-22 (on site)
Audit location:	CAB office – validation of TSP documentation, TSP office – Olšanská 38/9, 130 00 Praha 3

Root 1: PostSignum Root QCA 4

Standards considered:	European Standards: • ETSI EN 319 411-2 V2.6.1 (2025-06) • ETSI EN 319 411-1 V1.5.1 (2024-12) • ETSI EN 319 401 V3.2.1 (2026-01) CA Browser Forum Requirements: • Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, version 2.3.1 • Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, version 1.0.16 • 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:

- Certifikační politika PostSignum Root QCA pro certifikáty podřízených CA

Version	Release Date	Effective from	Effective until
Version 1.1.5	2025-05-07	2025-05-07	2026-05-07
Version 1.1.6	2026-05-07	2026-05-07	
…	…	…	…

- Certifikační politika PostSignum Public CA pro komerční osobní certifikáty

Version	Release Date	Effective from	Effective until
Version 4.1.4	2025-08-15	2025-08-15	2026-08-14
Version 4.1.5	2026-08-14	2026-08-14	
…	…	…	…

- Certifikační politika PostSignum Public CA pro komerční serverové certifikáty

Version	Release Date	Effective from	Effective until
Version 4.0.4	2025-08-15	2025-08-15	2026-08-14
Version 4.0.5	2026-08-14	2026-08-14	
…	…	…	…

- Certifikační politika PostSignum Public CA pro komerční doménové certifikáty

Version	Release Date	Effective from	Effective until
Version 5.0.4	2025-08-15	2025-08-15	2026-03-10
Version 5.1.0	2026-02-10	2026-03-10	
…	…	…	…

- Certifikační prováděcí směrnice pro úlohu Komerční certifikační autorita České pošty, s.p. PostSignum VCA

Version	Release Date	Effective from	Effective until
Version 4.1.2	2025-08-15	2025-08-15	2026-08-14
Version 4.1.3	2026-08-14	2026-08-14	
…	…	…	…

- Certifikační politika PostSignum Qualified CA pro kvalifikované certifikáty pro elektronický podpis

Version	Release Date	Effective from	Effective until
Version 2.1.4	2025-08-15	2025-08-15	2026-08-14
Version 2.1.5	2026-08-14	2026-08-14	
…	…	…	…

- Certifikační politika PostSignum Qualified CA pro kvalifikované certifikáty pro elektronickou pečeť

Version	Release Date	Effective from	Effective until
Version 2.0.4	2025-08-15	2025-08-15	2026-08-14
Version 2.0.5	2026-08-14	2026-08-14	
…	…	…	…

- Certifikační politika PostSignum Qualified CA pro certifikáty OCSP

Version	Release Date	Effective from	Effective until
Version 4.1.0	2025-08-15	2025-08-15	2026-08-14
Version 4.1.1	2026-08-14	2026-08-14	
…	…	…	…

- Certifikační politika PostSignum VCA pro certifikáty OCSP

Version	Release Date	Effective from	Effective until
Version 4.1.0	2025-08-15	2025-08-15	2026-08-14
Version 4.1.1	2026-08-14	2026-08-14	
…	…	…	…

- Certifikační prováděcí směrnice pro úlohu Kvalifikovaná certifikační autorita České pošty, s.p. PostSignum QCA

Version	Release Date	Effective from	Effective until
Version 4.3.2	2025-08-15	2025-08-15	2026-08-14
Version 4.3.3	2026-08-14	2026-08-14	
…	…	…	…

- Certifikační politika PostSignum Qualified CA pro certifikáty TSA

Version	Release Date	Effective from	Effective until
Version 1.6.4	2025-08-15	2025-08-15	2026-08-14
Version 1.6.5	2026-08-14	2026-08-14	
…	…	…	…

- Prováděcí směrnice pro úlohu Autorita časových razítek České pošty, s.p. PostSignum TSA

Version	Release Date	Effective from	Effective until
Version 3.0.4	2025-08-15	2025-08-15	2026-08-14
Version 3.0.5	2026-08-14	2026-08-14	
…	…	…	…

CP/CPS can be found: https://www.postsignum.cz/certifikacni_politiky.html

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.

This Audit Attestation also covers the following incidents as described in the following.

- Bug 2016722, PostSignum
  Incident description: Mis-issued certificate
  https://bugzilla.mozilla.org/show_bug.cgi?id=2016722

- Bug 2021239, PostSignum
  Incident description: Length Subject organizationName
  https://bugzilla.mozilla.org/show_bug.cgi?id=2021239

The remediation measures taken by Česká pošta s.p. (hereinafter PostSignum) as described on Bugzilla (see link above) have been checked by the auditors and properly addressed the incident.

Distinguished Name	SHA-256 fingerprint	Applied policy
CN = PostSignum Root QCA 4, O = Česká pošta, s.p., C = CZ	AC7F7862E685C7A7D9826A58EA32D183D4893FCC8F8FD6D900C9769A987E77F0	ETSI EN 319 411-1 V1.4.1, NCP ETSI EN 319 411-1 V1.4.1, NCP+ ETSI EN 319 411-1 V1.4.1, OVCP ETSI EN 319 411-1 V1.4.1, DVCP ETSI EN 319 411-2 V2.5.1, QCP-n ETSI EN 319 411-2 V2.5.1, QCP-n-QSCD ETSI EN 319 411-2 V2.5.1, QCP-l ETSI EN 319 411-2 V2.5.1, QCP-l-QSCD ETSI EN 319 411-2 V2.5.1, QCP-w

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 = PostSignum Public CA 4, O = Česká pošta, s.p., 2.5.4.97 = NTRCZ-47114983, C = CZ	E4272DFA3FBC48C90929518A0482BA3D9EB9C94A3CD397139F0ECDF2475955F6	ETSI EN 319 411-1 V1.4.1, NCP ETSI EN 319 411-1 V1.4.1, NCP+
CN = PostSignum Public CA 5, O = Česká pošta, s.p., 2.5.4.97 = NTRCZ-47114983, C = CZ	78C0BAD095E13547B7E5646D38453393818B2972D09B2144311B65D7EBB8B9CA	ETSI EN 319 411-1 V1.4.1, NCP ETSI EN 319 411-1 V1.4.1, NCP+ ETSI EN 319 411-1 V1.4.1, OVCP ETSI EN 319 411-1 V1.4.1, DVCP
CN = PostSignum Qualified CA 4, O = Česká pošta, s.p., 2.5.4.97 = NTRCZ-47114983, C = CZ	4779BA66C768FE7E5A5BB74A225FA8B69CD6942AF481355630E5AD78B34DFF2B	ETSI EN 319 411-2 V2.5.1, QCP-n ETSI EN 319 411-2 V2.5.1, QCP-n-QSCD ETSI EN 319 411-2 V2.5.1, QCP-l ETSI EN 319 411-2 V2.5.1, QCP-l-QSCD ETSI EN 319 411-2 V2.5.1, QCP-w
CN = PostSignum Qualified CA 5, O = Česká pošta, s.p., 2.5.4.97 = NTRCZ-47114983, C = CZ	BD0636ABC7F7501899C3FBD00AE071BB070B3E82ECAFF9A27F6E1FB1E7E2A2EA	ETSI EN 319 411-2 V2.5.1, QCP-n ETSI EN 319 411-2 V2.5.1, QCP-n-QSCD ETSI EN 319 411-2 V2.5.1, QCP-l ETSI EN 319 411-2 V2.5.1, QCP-l-QSCD ETSI EN 319 411-2 V2.5.1, QCP-w

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	2026-10-23	Initial attestation
…	…	…
…	…	…

End of the audit attestation letter.