Standard Audit Attestation for

Financijska agencija

Reference: PCEB-N 26/02/02

"Prague, 2026-02-18"

To whom it may concern,

This is to confirm that "TAYLLORCOX PCEB established by TAYLLORCOX s.r.o." has audited the CAs of the "Financijska agencija" without critical findings.

This present Audit Attestation Letter is registered under the unique identifier number "PCEB-N 26/02/02" 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
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 V2.2.2 (2015-08)” / “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):	Financijska agencija, Ulica grada Vukovara 70 10000 Zagreb - HR, registered under No. (OIB): 85821130368

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:	2025-06-03 to 2026-02-06
Point in time date:	none
Audit dates:	2026-02-06 to 2026-02-06 (remote) 2026-01-12 to 2026-01-16 (on site)
Audit location:	CAB office – validation of TSP documentation, TSP office – Koturaška ul. 43, 10000 Zagreb

Root 1: Fina Root CA

Standards considered:	European Standards: • ETSI EN 319 411-2 V2.5.1 (2023-10) • ETSI EN 319 411-1 V1.4.1 (2023-10) • ETSI EN 319 401 V3.1.1 (2024-06) • ETSI EN 319 421 V1.3.1 (2025-07) CA Browser Forum Requirements: • Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, version 2.1.8 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) • ETSI TS 119 403-3 V1.1.1 (2019-03)

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

- Certificate Profiles Aligned With The Regulation (EU) No 910/2014 (eIDAS), Version 2.14., Effective date: 09 January, 2026.
- Certificate Profiles Aligned With The Regulation (EU) No 910/2014 (eIDAS), version 2.15, Effective date: 09 February, 2026
- Certificate Policy and Certification Practice Statement for Fina Root CA, Version 2.10, Effective date: 24 November 2025
- Certificate Policy for Qualified Certificates for Electronic Signatures and Seals, Version 2.6, Effective date: 24 November 2025
- Certificate Policy for Qualified Certificates for Electronic Signatures and Seals, Version 2.7, Effective date: 09 February 2026
- Certificate Policy for Non-qualified Certificates, Version 2.0, Effective date: 24 November 2025
- Certificate Policy for Non-qualified Certificates, Version 2.1, Effective date: 09 February 2026
- Certificate Policy for Qualified Certificates for Website Authentication, Version 1.8, Effective date: 24 November 2025
- Certificate Policy for Certificates for Website Authentication, Version 1.13, Effective date: 24 November 2025
- Certification Practice Statement for Qualified Certificates for Electronic Signatures and Seals, Version 2.6, Effective date: 24 November 2025
- Certification Practice Statement for Qualified Certificates for Electronic Signatures and Seals, Version 2.7, Effective date: 09 February 2026
- Certification Practice Statement for Non-Qualified Certificates, Version 2.0, Effective date: 24 November 2025

- Certification Practice Statement for Non-Qualified Certificates, Version 2.1, Effective date: 09 February 2026
- Certification Practice Statement for Qualified Certificates for Website Authentication, Version 1.8, Effective date: 24 November 2025
- Certification Practice Statement for Certificates for Website Authentication, Version 1.13, Effective date: 24 November 2025
- Qualified Time-Stamp Policy, Version 1.10, Effective date: 09 February 2025
- Qualified Time-Stamping Practice Statement, Version 1.10, Effective date: 09 February 2025

CP/CPS can be found: https://www.fina.hr/finadigicert/regulativa-dokumenti-i-potvrde-o-sukladnosti

In the following areas, non-conformities have been identified throughout the audit:

Findings with regard to ETSI EN 319 401:
None.

Findings with regard to ETSI EN 319 411-1:
GEN-6.6.1-01: The certificate issuing software was blocking the ability to select a value for “Subject Country” other than “HR”. Correction implemented and validated during the audit. New CP issued effective 2026-02-09.

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.

The audit verified the measures taken for the incident "Financial Agency (Fina): Incorrectly issued certificates", which is reported as bug 1986968 on Bugzilla (1986968 - Financijska agencija (Fina): Mis-issued certificates).

The incident timeline and subsequent action plan were verified.

Shortcut of incident timeline:

2019-06-10 00:00 UTC-02 Certification Practice Statement for Certificates for Website Authentication ver. 1.4 came into force with the regulated possibility of issuing test certificates for the purpose of internal tests of the production CA environment

2024-02-18 11:07 Issuing of first internal test certificate for IP address 1.1.1.1

2025-09-03 14:03:36 Initial notice received in Fina sent from the owner of IP address 1.1.1.1 about several certificates issued for that IP address.

…

2025-09-16 13:00 Email from the Croatian Supervisory Body in charge of eIDAS Regulation has been received with confirmation of proposed measures and request for performing an eIDAS conformity assessment by Conformity Assessment Body as soon as possible.

Action Items:

1) Decision on banning the issuance of certificates – presented **Completed**
2) Employee training on requirements and procedures for providing trust services (part 1) – verified by interviews with relevant employees **Completed**
3) Audit and non-conformities management procedure for the area of providing trust services - realised **Completed**
4) New version of CPS (Certification Practice Statement for Certificates for Website Authentication, Ver. 1.13) issued with an effective date of 24.11.2025 **Completed**
5) Procedure for Issuing Production Certificates for Testing the Fina PKI System – presented **Completed**
6) Employee training on requirements and procedures for providing trust services (part 2) – relevant persons have been trained in the first part (this is an improvement in training), will be implemented in the week of 9. 2. 2026. Not necessary for the closure of the incident. **Delayed**
7) Internal audit according to eIDAS regulation, ETSI 319 411-1, ETSI 319411-2 and the Baseline Requirements document – presented during audit. **Completed**
8) eIDAS conformity assessment by CAB (external full audit in full scope) according to eIDAS regulation, ETSI norms and the Baseline Requirements document – performed in the week from 12. 1. 2026 to 16. 1. 2026. Final result and report were issued on 6. 2. 2026 after implementation of all agreed measures. **Completed**
9) Setting up the linting process – risk level explained and accepted **Completed**

Distinguished Name	SHA-256 fingerprint	Applied policy
CN = Fina Root CA O = Financijska agencija C = HR	5AB4FCDB180B5B6AF0D262A2375A2C77D25602015D96648756611E2E78C53AD3	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, LCP ETSI EN 319 411-1 V1.4.1, OVCP 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 ETSI EN 319 411-2 V2.5.1, QCP-w-psd2

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 = Fina RDC 2015 O = Financijska agencija C = HR	857BFCE43B1BB4601FF4543B46D3FB2E213BF9B4FEEB6F13BE9EF45C04FF6F8B	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, LCP ETSI EN 319 411-1 V1.4.1, OVCP 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 ETSI EN 319 411-2 V2.5.1, QCP-w-psd2
CN = Fina RDC 2020 O = Financijska agencija C = HR	4140B70629FDA4B8A36FD53FB0AA53237157869931B8B2308FD05DF3FF7D78AB	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 319 411-2 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 ETSI EN 319 411-2 V2.5.1, QCP-w-psd2
CN = Fina RDC 2025 O = Financijska agencija C = HR	ECD2605CFE4A0B27ABEB670513850CB048E486815CCE4BDFBF698AD82403C2FE	ETSI EN 319 411-1 V1.4.1, NCP ETSI EN 319 411-1 V1.4.1, LCP

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	2026-02-18	Initial attestation Audit period from the end of the last audited period (AAL issued by CAB Bureau Veritas) to the end of the extraordinary audit.

End of the audit attestation letter.