TLS BR Audit Attestation for

Actalis SpA

Reference: PCEB-N 26/04/04

"Prague, 2026-04-02"

To whom it may concern,

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

This present Audit Attestation Letter is registered under the unique identifier number "PCEB-N 26/04/04" covers multiple Root-CAs and consists of 13 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):	Actalis SpA, Via San Clemente, 53, Ponte San Pietro (BG), Italia registered under No. (OIB): IT03358520967

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:	2025-06-07 to 2026-03-31
Point in time date:	None
Audit dates:	2026-03-26 to 2026-04-02
Audit location:	CAB office – validation of TSP documentation, TSP office – Ponte San Pietro (BG), HQ – online

Root 1: Actalis Authentication Root CA

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 2.0.1 • Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates, version 2.2.5 • Network and Certificate System Security Requirements, version 2.0.5 Browser Policy Requirements: • Mozilla Root Store Policy, section 6.1.3 regarding mass revocation plans and testing thereof 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:

- Certification Practice Statement, SSL Server and Code Signing certificates, version 5.21 as of 2026-03-15
- Certification Practice Statement, OPERATIVE MANUAL FOR THE "AgID CA" SERVICE, version 9.0 as of 2025-07-10

CP/CPS can be found: https://www.actalis.com/legal-repository

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:
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.
• https://bugzilla.mozilla.org/show_bug.cgi?id=1973238

• https://bugzilla.mozilla.org/show_bug.cgi?id=1982646

• https://bugzilla.mozilla.org/show_bug.cgi?id=2012157

Distinguished Name	SHA-256 fingerprint	Applied policy
CN = Actalis Authentication Root CA O = Actalis S.p.A./03358520967 L = Milan C = IT	55926084EC963A64B96E2ABE01CE0BA86A64FBFEBCC7AAB5AFC155B37FD76066	ETSI EN 319 411-1, V1.5.1, ETSI EN 319 411-2 V2.6.1, 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 = Actalis Authentication CA G3 O = Actalis S.p.A./03358520967 L = Milano S = Milano C = IT	A1D25D28941FAFC0C2A6EB9E596A54786E731D0A4A8E321DB9F1CF2C24FDD609	ETSI EN 319 411-2 V2.6.1, OVCP
CN = Actalis Organization Validated Server CA G3 O = Actalis S.p.A. L = Ponte San Pietro S = Bergamo C = IT	931AAA1EC9B2BA0FA59A82302F4F830628C86D9B2D2A50A4D1B2CE895C4CC648	ETSI EN 319 411-2 V2.6.1, OVCP
CN = Actalis Extended Validation Server CA G3 O = Actalis S.p.A. L = Ponte San Pietro S = Bergamo C = IT	124EAAF26F570C4FB4D89F5D61078F15B885345FCAF0C57F3477D8C63B5AB26F	ETSI EN 319 411-1, V1.5.1, ETSI EN 319 411-2 V2.6.1, EVCP, QCP-w
CN = Actalis Domain Validation Server CA G3 O = Actalis S.p.A. L = Ponte San Pietro S = Bergamo C = IT	3450B6D38290C3CA5D7BB38B71495BBF72C6D0C44DBA292245F9BCA9843A9FFF	ETSI EN 319 411-2 V2.6.1, DVCP
= Actalis Code Signing CA G2 O = Actalis S.p.A. L = Ponte San Pietro S = Bergamo C = IT	8CC827CEA1CD8DB79AEB7CD4BEEAE36658AF7B4C0606C257B7538AB1E710BC6A	ETSI EN 319 411-2 V2.6.1, NCP

CN = Actalis Client Authentication CA G1 O = Actalis S.p.A./03358520967 L = Milano S = Milano C = IT	ABDEEC53149098F8A0B07EFD972B345A89BEDE8EDE6975E61BE95EE026DA7EFA	ETSI EN 319 411-2 V2.6.1, LCP
CN = Actalis Client Authentication CA G3 O = Actalis S.p.A. L = Ponte San Pietro S = Bergamo C = IT	BB4D3EE661E5029409DB6740B9951494A7F22A7BC0FDC1A1900C07A4781F1419	ETSI EN 319 411-2 V2.6.1, LCP
CN = Actalis Time Stamping CA G1 O = Actalis S.p.A. L = Ponte San Pietro S = Bergamo C = IT	AA0CA7B6C6A4DD5335761A7213801B3D2D1829CDD0A72F4587F8830804A03B7E	N/A
CN=AgID CA1; OU=Area Soluzioni per la Pubblica Amministrazione; O=Agenzia per l'Italia Digitale; C=IT; L=Roma	790EC428504A61F273E4FCF7FFD4D56991EDC02D4402FBBD8914E149FA278C1D	ETSI EN 319 411-2 V2.6.1, LCP
CN = AgID CA SSL SERVER OU = Area Soluzioni per la Pubblica Amministrazione O = Agenzia per l'Italia Digitale C = IT, L = Roma	8B7ED5358484781F4C08376B183B018C957908CAAC32AA72ACD02E51707A58A7	ETSI EN 319 411-2 V2.6.1, OVCP
CN = Actalis DV Server ACME CA G1, O = Actalis S.p.A., L = Ponte San Pietro, S = Bergamo, C = IT	C0A9FB425D0EDEBC72BC6C47AD3D3A2B68245ED1D59A5883BF19CE9F8C4DED1F	ETSI EN 319 411-2 V2.6.1, DVCP

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

Root 2: Actalis TLS Server RSA Root CA 2025

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 2.0.1 • Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates, version 2.2.5 • Network and Certificate System Security Requirements, version 2.0.5 Browser Policy Requirements: • Mozilla Root Store Policy, section 6.1.3 regarding mass revocation plans and testing thereof 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:

- Certification Practice Statement, SSL Server and Code Signing certificates, version 5.21 as of 2026-03-15
- Certification Practice Statement, OPERATIVE MANUAL FOR THE "AgID CA" SERVICE, version 9.0 as of 2025-07-10

CP/CPS can be found: https://www.actalis.com/legal-repository

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:
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.
• https://bugzilla.mozilla.org/show_bug.cgi?id=1973238

• https://bugzilla.mozilla.org/show_bug.cgi?id=1982646

• https://bugzilla.mozilla.org/show_bug.cgi?id=2012157

Distinguished Name	SHA-256 fingerprint	Applied policy
CN=Actalis TLS Server RSA Root CA 2025; O=Actalis S.p.A.; C=IT	6D0E47DFDE7CF48308CD4C6C1517DD1AF033DCC72BB0501C04268B03B58A9085	ETSI EN 319 411-1 v. 1.5.1, ETSI EN 319 411-2 v.2.6.1, DVCP, OVCP, EVCP, QEVCP-w

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=Actalis Domain Validated TLS Server RSA CA 2025; O=Actalis S.p.A.; L=Ponte San Pietro; ST=Bergamo; C=IT	C511EF2F15EF7681EEADFF97F1E90596270EADB71BDA8F847AB36FFF15DC6264	ETSI EN 319 411-1 V. 1.5.1, DVCP
CN=Actalis Organization Validated TLS Server RSA CA 2025; O=Actalis S.p.A.; L=Ponte San Pietro; ST=Bergamo; C=IT	BAE1C37CEE8621A3016AE4E76E36204949DA3160BCE5AE56CF4003860EE3B2CD	ETSI EN 319 411-1 V. 1.5.1, OVCP
CN=Actalis Extended Validation TLS Server RSA CA 2025; O=Actalis S.p.A.; L=Ponte San Pietro; ST=Bergamo; C=IT	8FA40E1594EB493E5D2954F577BB50473A3512F2D203A99B402BBCB608AED73B	ETSI EN 319 411-1 V. 1.5.1, ETSI EN 319 411-2 V.2.6.1, EVCP, QEVCP-w

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

Root 3: Actalis TLS Server ECC Root CA 2025

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 2.0.1 • Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates, version 2.2.5 • Network and Certificate System Security Requirements, version 2.0.5 Browser Policy Requirements: • Mozilla Root Store Policy, section 6.1.3 regarding mass revocation plans and testing thereof 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:

- Certification Practice Statement, SSL Server and Code Signing certificates, version 5.21 as of 2026-03-15
- Certification Practice Statement, OPERATIVE MANUAL FOR THE "AgID CA" SERVICE, version 9.0 as of 2025-07-10

CP/CPS can be found: https://www.actalis.com/legal-repository

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:
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.
• https://bugzilla.mozilla.org/show_bug.cgi?id=1973238

• https://bugzilla.mozilla.org/show_bug.cgi?id=1982646

• https://bugzilla.mozilla.org/show_bug.cgi?id=2012157

Distinguished Name	SHA-256 fingerprint	Applied policy
CN=Actalis TLS Server ECC Root CA 2025; O=Actalis S.p.A.; C=IT	4EFAADA2543E1E02666998574B3BAD96AE264088FA5917F75D32E7A609D1869C	ETSI EN 319 411-1 V. 1.5.1, ETSI EN 319 411-2 V.2.6.1, DVCP, OVCP, EVCP, QEVCP-w

Table 5: Root-CA 3 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=Actalis Domain Validated TLS Server ECC CA 2025; O=Actalis S.p.A.; L=Ponte San Pietro; ST=Bergamo; C=IT	E102A52A016B025B31C749A9A0A7F4650E1227AFA27C27E9A37C846AD42FA8B0	ETSI EN 319 411-1 V. 1.5.1, DVCP
CN=Actalis Organization Validated TLS Server ECC CA 2025; O=Actalis S.p.A.; L=Ponte San Pietro; ST=Bergamo; C=IT	E7929CDA1A88D2E94016A3F2D52BE95DB1C28C178C425B4303A82E3E29293544	ETSI EN 319 411-1 V. 1.5.1, OVCP
CN=Actalis Extended Validation TLS Server ECC CA 2025; O=Actalis S.p.A.; L=Ponte San Pietro; ST=Bergamo; C=IT	12D8FBFFEB27481EB0EECD032336D6D1E2B1A678A9B1018E653E7FC253D929A5	ETSI EN 319 411-1 V. 1.5.1, ETSI EN 319 411-2 V.2.6.1, EVCP, QEVCP-w

Table 6: Sub-CA’s issued by the Root-CA 3 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	2026-04-02	Initial attestation
Version 1.1	2026-04-02	Revison of CAB Baseline Requirements list
Version 2	2026-04-21	Revison of report, changed period of audit

End of the audit attestation letter.