



Key Generation Ceremony Report for Actalis SpA

Reference: 24985811

“Ponte San Pietro (BG), 2025-02-28”

To whom it may concern,

This is to confirm that “Bureau Veritas Italia SpA” has audited a key generation ceremony of “Actalis SpA”. The ceremony was followed in its entirety, completed successfully and without non-conformities in accordance with the applicable requirements.

This Key Generation Ceremony Report is registered under the unique identifier number “24985811” and consists of 13 pages.

Kindly find here below the details accordingly.

In case of any question, please contact:

Bureau Veritas Italia SpA
Viale Monza, 347
20126, Milano (MI) Italia
E-Mail: certificati@bureauveritas.com
Phone: +39 02.2709911

With best regards,


GLORIA FOCETOLA
Local technical Manager


ANDREA FILIPPI
Certification Service Line Manager

This attestation is based on the template version 3.3 as of 202y-mm-dd, that was approved for use by ACAB-c.

Bureau Veritas Italia SpA – P. IVA 11498640157 – Viale Monza, 347 – 20126 Milano (MI), Italia
page 1 of 18 pages

General audit information

Identification of the conformity assessment body (CAB) and assessment organization acting as ETSI auditor

- Bureau Veritas Italia SpA¹, Viale Monza 347, 20126 Milano, Italia, registered under IT11498640157
- Accredited by ACCREDIA under registration Annex expiry date 2027-05-24 link to Url (https://services.accredia.it/ppsearch/accredia_orgmask.jsp?ID_LINK=1733&area=310&PPSEARCH_ORG_SEARCH_MASK_ORG=0663&PPSEARCH_ORG_SEARCH_MASK_STANDARDS=2&PPSEARCH_ORG_SEARCH_MASK_SCHEMI_ALTRI_STD=&PPSEARCH_ODC_SEARCH_MASK_SETTORE_ACCR=&PPSEARCH_ORG_SEARCH_MASK_CITTA=&PPSEARCH_ORG_SEARCH_MASK_PROVINCIA=&PPSEARCH_ORG_SEARCH_MASK_REGIONE=&PPSEARCH_ORG_SEARCH_MASK_STATO=&PPSEARCH_ORG_SEARCH_MASK_SCOPO=&PPSEARCH_ORG_SEARCH_MASK_PDFACCREDITAMENTO=&submitBtn=Cerca) for the certification of trust services according 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>>>
- Third-party affiliate audit firms involved in the audit: None.

Identification and qualification of the audit team

- Number of team members: 1
- 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 work Milano 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:

¹ in the following termed shortly "CAB"

<ul style="list-style-type: none"> 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; 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. <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> 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: All team members are Accredia (NAB) certified lead auditor for CA/TSP audits. • 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.
<p>Identification and qualification of the reviewer performing audit quality management</p>
<ul style="list-style-type: none"> • 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.

<p>Identification of the CA / Trust Service Provider (TSP):</p>	<p>ACTALIS SpA, Via San Clemente, 53, Ponte San Pietro (BG), Italia, registered under IT03358520967</p>
---	---

<p>Type of audit:</p>	<p>Point in time audit of key and certificate generation ceremony</p>
<p>Point in time date:</p>	<p>2025-02-28</p>
<p>Audit location:</p>	<p>Ponte San Pietro (BG), HQ Arezzo (AR), operational site</p>

A key generation script has been prepared in accordance with the normative requirements and with the rules stated in the policy and practice statement documents of the certification service provider. During generation of the keys and certificates, this script has been followed.

In particular:

- The key generation ceremony was performed by 8 individuals of the CA Owner acting in Trusted Roles
- The key generation ceremony was observed by 1 individual of the Conformity Assessment Body with independence from the CA Owner
- Principles of multiparty control and split knowledge were observed.
- The CA key pairs were generated in a physically secured environment as described in the CA's CP / CPS.
- The CA key pairs were generated within cryptographic modules meeting the applicable technical and business requirements as disclosed in the CA's CP / CPS.
- CA key pair generation activities were logged.
- Effective controls were maintained to provide reasonable assurance that the private key was generated and protected in conformance with the procedures described in its CP / CPS and the Key Generation Script.

The key generation ceremony has been witnessed in person.

No non-conformities have been identified during the audit.

Root 1: Actalis Code Signing ECC Root CA 2025

<p>Standards considered: (Only with regard to key generation and key protection requirements)</p>	<p>European Standards:</p> <ul style="list-style-type: none">• ETSI EN 319 411-2 V2.6.0 (2024-12)• ETSI EN 319 411-1 V1.4.1 (2023-10)• ETSI EN 319 401 V3.1.1 (2024-06) <p>CA Browser Forum Requirements:</p> <ul style="list-style-type: none">• Guidelines for the Issuance and Management of Extended Validation Certificates, version 2.0.1• Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, version 2.1.3• Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, version 1.0.8• Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates, version 3.8• Network and Certificate System Security Requirements, version 2.0 <p>For the Trust Service Provider Conformity Assessment:</p> <ul style="list-style-type: none">• ETSI EN 319 403 V2.2.2 (2015-08)• ETSI EN 319 403-1 V2.3.1 (2020-06)• ETSI TS 119 403-2 V1.2.4 (2020-11)
---	---

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

- Certification Practice Statement, version 5.16, as of 15/01/2025

This report covers the generation of the key pair and certificate of the Root-CA referenced in the following table. No Sub-CAs were generated during the ceremony.

Distinguished Name	SHA-256 fingerprint of the certificate	Applied policy
Complete subject DN: CN = Actalis Code Signing ECC Root CA 2025 O = Actalis S.p.A. C = IT	SHA-256 fingerprint of the certificate: 7EF55518DE6350C3CC618A9837CBAD65DDB6EEF652F79DA71C69F6B8919D3A12	ETSI EN policy that this Root has been assessed against: ETSI EN 319 411-2 V2.6.0, QCP-w ETSI EN 319 411-1 V1.4.1, EVCP
	SHA-256 fingerprint of Subject Public Key Info	
	SHA-256 fingerprint of the subject public key info: 676C942869539B12CCF7F33F793F20C00FEDE7A801B0E1666DCDDEE60ABA59E6	

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 of the certificate	Applied policy
	SHA-256 fingerprint of Subject Public Key Info	

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

Root 2: Actalis Code Signing RSA Root CA 2025

<p>Standards considered: (Only with regard to key generation and key protection requirements)</p>	<p>European Standards:</p> <ul style="list-style-type: none">• ETSI EN 319 411-2 V2.6.0 (2024-12)• ETSI EN 319 411-1 V1.4.1 (2023-10)• ETSI EN 319 401 V3.1.1 (2024-06) <p>CA Browser Forum Requirements:</p> <ul style="list-style-type: none">• Guidelines for the Issuance and Management of Extended Validation Certificates, version 2.0.1• Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, version 2.1.3• Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, version 1.0.8• Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates, version 3.8• Network and Certificate System Security Requirements, version 2.0 <p>For the Trust Service Provider Conformity Assessment:</p> <ul style="list-style-type: none">• ETSI EN 319 403 V2.2.2 (2015-08)• ETSI EN 319 403-1 V2.3.1 (2020-06)• ETSI TS 119 403-2 V1.2.4 (2020-11)
---	---

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

- Certification Practice Statement, version 5.16, as of 15/01/2025

This report covers the generation of the key pair and certificate of the Root-CA referenced in the following table. No Sub-CAs were generated during the ceremony.

Distinguished Name	SHA-256 fingerprint of the certificate	Applied policy
Complete subject DN: CN = Actalis Code Signing RSA Root CA 2025 O = Actalis S.p.A. C = IT	SHA-256 fingerprint of the certificate: 041C6215F8DF4137DF0F3FC23A0009B46E75AC4619F811727076BAA8FE5008C9	ETSI EN policy that this Root has been assessed against: ETSI EN 319 411-2 V2.6.0, QCP-w ETSI EN 319 411-1 V1.4.1, EVCP
	SHA-256 fingerprint of Subject Public Key Info	
	SHA-256 fingerprint of the subject public key info: B4FD92CA4F91161770D9099E281B9CB1A41A05A5A44F516A5E155461BDBCDAC9	

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 of the certificate	Applied policy
	SHA-256 fingerprint of Subject Public Key Info	

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

Root 3: Actalis SMIME ECC Root CA 2025

<p>Standards considered: (Only with regard to key generation and key protection requirements)</p>	<p>European Standards:</p> <ul style="list-style-type: none">• ETSI EN 319 411-2 V2.6.0 (2024-12)• ETSI EN 319 411-1 V1.4.1 (2023-10)• ETSI EN 319 401 V3.1.1 (2024-06) <p>CA Browser Forum Requirements:</p> <ul style="list-style-type: none">• Guidelines for the Issuance and Management of Extended Validation Certificates, version 2.0.1• Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, version 2.1.3• Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, version 1.0.8• Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates, version 3.8• Network and Certificate System Security Requirements, version 2.0 <p>For the Trust Service Provider Conformity Assessment:</p> <ul style="list-style-type: none">• ETSI EN 319 403 V2.2.2 (2015-08)• ETSI EN 319 403-1 V2.3.1 (2020-06)• ETSI TS 119 403-2 V1.2.4 (2020-11)
---	---

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

- Certification Practice Statement, version 5.16, as of 15/01/2025

This report covers the generation of the key pair and certificate of the Root-CA referenced in the following table. No Sub-CAs were generated during the ceremony.

Distinguished Name	SHA-256 fingerprint of the certificate	Applied policy
Complete subject DN: CN = Actalis SMIME ECC Root CA 2025 O = Actalis S.p.A. C = IT	SHA-256 fingerprint of the certificate: 3347EEA8149CD3F6B7796CCAAD234ADA294372F7B1EA49F87F5ADB11C8581624	ETSI EN policy that this Root has been assessed against: ETSI EN 319 411-1 V1.4.1, NCP+, LCP ETSI EN 319 411-2 V2.6.0, QCP-n-qscd, QCP-l-qscd
	SHA-256 fingerprint of Subject Public Key Info	
	SHA-256 fingerprint of the subject public key info: 2FB67486570ADD6622A2F3E08E9BE8D9A018B3241A70D7C243168BBCEE174BF8	

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 of the certificate	Applied policy
	SHA-256 fingerprint of Subject Public Key Info	

Table 6: Sub-CA's issued by the Root-CA 3 or its Sub-CA's in scope of the audit

Root 4: Actalis SMIME RSA Root CA 2025

<p>Standards considered: (Only with regard to key generation and key protection requirements)</p>	<p>European Standards:</p> <ul style="list-style-type: none">• ETSI EN 319 411-2 V2.6.0 (2024-12)• ETSI EN 319 411-1 V1.4.1 (2023-10)• ETSI EN 319 401 V3.1.1 (2024-06) <p>CA Browser Forum Requirements:</p> <ul style="list-style-type: none">• Guidelines for the Issuance and Management of Extended Validation Certificates, version 2.0.1• Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, version 2.1.3• Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, version 1.0.8• Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates, version 3.8• Network and Certificate System Security Requirements, version 2.0 <p>For the Trust Service Provider Conformity Assessment:</p> <ul style="list-style-type: none">• ETSI EN 319 403 V2.2.2 (2015-08)• ETSI EN 319 403-1 V2.3.1 (2020-06)• ETSI TS 119 403-2 V1.2.4 (2020-11)
---	---

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

- Certification Practice Statement, version 5.16, as of 15/01/2025

This report covers the generation of the key pair and certificate of the Root-CA referenced in the following table. No Sub-CAs were generated during the ceremony.

Distinguished Name	SHA-256 fingerprint of the certificate	Applied policy
Complete subject DN: CN = Actalis SMIME RSA Root CA 2025 O = Actalis S.p.A. C = IT	SHA-256 fingerprint of the certificate: F1B7C8A8F447B395786E325AF0A7571203F3812400FF1905FCA7726B858FC44A	ETSI EN policy that this Root has been assessed against: ETSI EN 319 411-1 V1.4.1, NCP+, LCP ETSI EN 319 411-2 V2.6.0, QCP-n-qscd, QCP-l-qscd
	SHA-256 fingerprint of Subject Public Key Info	
	SHA-256 fingerprint of the subject public key info: 7E9653B325D0E74E82F2C53E71F71BAE85C56D8A58F67B366A3382A25EE1BC7F	

Table 7: Root-CA 4 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 of the certificate	Applied policy
	SHA-256 fingerprint of Subject Public Key Info	

Table 8: Sub-CA's issued by the Root-CA 4 or its Sub-CA's in scope of the audit

Root 5: Actalis TLS Server ECC Root CA 2025

<p>Standards considered: (Only with regard to key generation and key protection requirements)</p>	<p>European Standards:</p> <ul style="list-style-type: none">• ETSI EN 319 411-2 V2.6.0 (2024-12)• ETSI EN 319 411-1 V1.4.1 (2023-10)• ETSI EN 319 401 V3.1.1 (2024-06) <p>CA Browser Forum Requirements:</p> <ul style="list-style-type: none">• Guidelines for the Issuance and Management of Extended Validation Certificates, version 2.0.1• Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, version 2.1.3• Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, version 1.0.8• Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates, version 3.8• Network and Certificate System Security Requirements, version 2.0 <p>For the Trust Service Provider Conformity Assessment:</p> <ul style="list-style-type: none">• ETSI EN 319 403 V2.2.2 (2015-08)• ETSI EN 319 403-1 V2.3.1 (2020-06)• ETSI TS 119 403-2 V1.2.4 (2020-11)
---	---

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

- Certification Practice Statement, version 5.16, as of 15/01/2025

This report covers the generation of the key pair and certificate of the Root-CA referenced in the following table. No Sub-CAs were generated during the ceremony.

Distinguished Name	SHA-256 fingerprint of the certificate	Applied policy
Complete subject DN: CN = Actalis TLS Server ECC Root CA 2025 O = Actalis S.p.A. C = IT	SHA-256 fingerprint of the certificate: 4EFAADA2543E1E02666998574B3BAD96AE264088FA5917F75D32E7A609D1869C	ETSI EN policy that this Root has been assessed against: ETSI EN 319 411-1 V1.4.1, EVCP ETSI EN 319 411-2 V2.6.0, QCP-w
	SHA-256 fingerprint of Subject Public Key Info	
	SHA-256 fingerprint of the subject public key info: CCA4EB68C98622E2264879B61562EAD139559C91FE6B6AB3081EB19631426855	

Table 9: Root-CA 5 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 of the certificate	Applied policy
	SHA-256 fingerprint of Subject Public Key Info	

Table 10: Sub-CA's issued by the Root-CA 5 or its Sub-CA's in scope of the audit

Root 6: Actalis TLS Server RSA Root CA 2025

<p>Standards considered: (Only with regard to key generation and key protection requirements)</p>	<p>European Standards:</p> <ul style="list-style-type: none">• ETSI EN 319 411-2 V2.6.0 (2024-12)• ETSI EN 319 411-1 V1.4.1 (2023-10)• ETSI EN 319 401 V3.1.1 (2024-06) <p>CA Browser Forum Requirements:</p> <ul style="list-style-type: none">• Guidelines for the Issuance and Management of Extended Validation Certificates, version 2.0.1• Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, version 2.1.3• Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, version 1.0.8• Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates, version 3.8• Network and Certificate System Security Requirements, version 2.0 <p>For the Trust Service Provider Conformity Assessment:</p> <ul style="list-style-type: none">• ETSI EN 319 403 V2.2.2 (2015-08)• ETSI EN 319 403-1 V2.3.1 (2020-06)• ETSI TS 119 403-2 V1.2.4 (2020-11)
---	---

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

- Certification Practice Statement, version 5.16, as of 15/01/2025

This report covers the generation of the key pair and certificate of the Root-CA referenced in the following table. No Sub-CAs were generated during the ceremony.

Distinguished Name	SHA-256 fingerprint of the certificate	Applied policy
Complete subject DN: CN = Actalis TLS Server RSA Root CA 2025 O = Actalis S.p.A. C = IT	SHA-256 fingerprint of the certificate: 6D0E47DFDE7CF48308CD4C6C1517DD1AF033DCC72BB0501C04268B03B58A9085	ETSI EN policy that this Root has been assessed against: ETSI EN 319 411-1 V1.4.1, EVCP ETSI EN 319 411-2 V2.6.0, QCP-w
	SHA-256 fingerprint of Subject Public Key Info	
	SHA-256 fingerprint of the subject public key info: 8F94CEDD9A5C168BE13D0511F67E92664E89876224CEF12F7FCEB91A67F8E6F0	

Table 31: Root-CA 6 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 of the certificate	Applied policy
	SHA-256 fingerprint of Subject Public Key Info	

Table 14: Sub-CA's issued by the Root-CA 6 or its Sub-CA's in scope of the audit

Key #	Subject Public Key Info Field Hash (SHA-256)
1	
2	
3	
4	

Table 13: Key pairs generated without issuance of a corresponding certificate

Modifications record

Version	2025-02-28	Changes
Version 1	2025-02-28	Initial attestation

End of the audit attestation letter.