S/MIME Certificates

Certificate Policy

Version 3.1

Last revised: January 15, 2026

Andrea Sassetti
Firmato
digitalmente il
15/01/2026
15:18:51 CET

Via San Clemente 53 | 24036 Ponte S. Pietro (BG)
Tel +39-0575-050.350 | Fax +39-0575-862.350
www.actalis.it | info@actalis.it

CHANGE HISTORY

Version	Date	Author	Changes
1.0	11/11/2015	AS	First version.
1.1	27/12/2016	AS	Changed company address. Added S/MIME certificates for organizations.
1.2	07/10/2019	AS	§1.3 Clarified that email can only be validated by the CA. §1.7 Updated reference for OCSP protocol. §3.1 Clarifications on the EE naming rules. §3.2 Modified headings for better clarity. §4.2 Clarifications on certificate revocation. §7.2 Updated profile of intermediate CA. §7.3 Updated profile of EE certificate.
2.0	07/11/2023	AS	Document restructuring for better alignment with RFC3647. §1.3.2 and §4.1.2: Added provisions for Enterprise RAs. General document update for compliance with CABF Baseline Requirements for S/MIME Certificates.
2.1	28/08/2024	AS	Correction of typos. § 1.6 Updated acronyms for CAA records. § 1.7 Updated references for CAA records § 4.1 and § 4.2 Updated for compliance with CABF Requirements regarding CAA record processing. §7.2 Updated with details on reasonCodes.
2.2	07/03/2025	NP, AS	Restructured the CP in accordance with RFC 3647; $2.3 Specification regarding the frequency of CP updating; $4.2.2 Integration about CAA Record checks before issuance.
3.0	10/07/2025	NP, AS	Merger of the two previous separate S/MIME CPs into a single S/MIME covering all types of Actalis S/MIME certs. $7.1 Updating certs' profile to *multipurpose* generation.
3.1	15/01/2026	BS, NP, AS	$1.3, $7.1 Updates to the PKI infrastructure with the addition of new RootCA and SubCA certificates

CONTENTS

1 INTRODUCTION

Actalis S.p.A. (www.actalis.it) is a leading Italian Trust Service Provider (TSP) since 2002, offering all types of digital certificates and related management services, digital time stamping, certified electronic mail, digital signatures, and other solutions in the field of Public Key Infrastructures (PKI), as well as in other fields pertaining to information security.

1.1 Overview

A **Certificate** binds a *public key* (the public component of cryptographic key pair) to an identity, namely a set of information items that identifies an individual or an organization. Such entity, identified in the **Subject** field of the certificate, holds and uses the corresponding *private key*.

The certificate is generated and supplied to the Subject by a trusted third party known as **Certification Authority** (CA), and is *digitally signed* by the CA. The Subject is also referred to as **Subscriber**, in that it subscribes an agreement with the CA for the issuance and management of the certificate. As long as the certificate has not yet been issued, the Subscriber is referred to as **Applicant**. The term **Applicant Representative** (or **Requestor**) refers to the human agent that materially requests the certificate on behalf of the Applicant.

The reliability of the certificate also depends on the CA's identification and authentication procedures, the obligations and responsibilities between the CA and the Subscriber, and the CA's physical, operational and technical security controls. All these aspects are described in a public document called **Certification Practice Statement** (CPS) or **Certificate Policy** (CP), depending on the level of detail and broadness of scope (see RFC 3647).

This document is the Actalis' CP relevant to the issuance and management of Publicly-Trusted **S/MIME Certificates** according to the [SMBR], and is integrated by the related CPS for a number of aspects (e.g., physical, technical, and operational controls).

This CP is based on RFC 3647; however, some topics listed in RFC 3647 either are covered in the related CPS or Actalis makes no stipulation about them.

As regards the certificates governed by this CP, Actalis conforms to the current version of the **Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates** published at http://www.cabforum.org. In the event of any inconsistency between this CP and those Requirements, those Requirements [SMBR] shall take precedence over this document.

Actalis also conforms to the current version of the **Mozilla Root Store Policy** [MRSP], the **Microsoft Trusted Root Program** [MTRP], and the **Apple Root Certificate Program** [ARCP], to the extent that they are applicable.

1.2 Document name and identification

This document is the **Certificate Policy** for **S/MIME Certificates** issued by Actalis S.p.A.

1.3 PKI participants

1.3.1 Certification Authorities

The **Certification Authority** (CA) is **Actalis S.p.A.**, headquartered at Via S. Clemente 53, 24036 Ponte San Pietro (BG), Italy, enlisted in the Company Registry of Bergamo under #03358520967.

For certificates issued under this CP, Actalis acts as Root CA and as Issuing CA (through its issuing Certification Authorities/SubCAs), depending on the certificate type and the applicable hierarchy.

Actalis is currently issuing S/MIME certificates under a legacy, non-dedicated Root CA that will be phased out at a later date (for further details, see the [CPS]). In 2025, Actalis also created new Root CAs and SubCAs dedicated to S/MIME certificates; the inclusion of these new Root Cas in the relevant application root stores is currently underway.

1.3.1.1 Root Certification Authorities

At the date of revision of this CP, the existing Actalis' Root CAs are those identified below; for further details, see also chapter 7.

Subject DN	Subject Key ID (Hex)	notBefore	notAfter
CN = Actalis Authentication Root CA O = Actalis S.p.A./03358520967 L = Milan C = IT	52 d8 88 3a c8 9f 78 66 ed 89 f3 7b 38 70 94 c9 02 02 36 d0	22 September 2011	22 September 2030
CN=Actalis SMIME ECC Root CA 2025 O=Actalis S.p.A. C=IT	8d 6f bc f6 76 d1 ca 7d 86 dd ab d0 2a 96 99 c8 f1 63 b2 29	28 February 2025	22 February 2050
CN=Actalis SMIME RSA Root CA 2025 O=Actalis S.p.A. C=IT	f3 ef a2 39 aa 77 3b c2 ad 6a 9f fc 2e 58 00 fe 5b bf 47 51	28 February 2025	22 February 2050

1.3.1.2 Cross Certificates

At the date of revision of this CP, the existing Actalis Cross Certificates are those identified below; for further details, see also Chapter 7.

Subject DN	Subject Key ID (Hex)	notBefore	notAfter
CN = Actalis SMIME RSA Root CA 2025 O = Actalis S.p.A./03358520967 L = Milan C = IT	f3 ef a2 39 aa 77 3b c2 ad 6a 9f fc 2e 58 00 fe 5b bf 47 51	07 august 2025	22 september 2030

1.3.1.3 Subordinate Certification Authorities

At the date of revision of this CP, the SubCAs operated by Actalis for issuing S/MIME certificates are those identified below; for further details, see also Chapter 7.

Subject DN	Subject Key ID (Hex)	notBefore	notAfter
CN = Actalis Client Authentication CA G3 O = Actalis S.p.A. L = Ponte San Pietro S = Bergamo C =	BE 97 A9 AA 84 BF 80 BF 10 53 7D 09 32 F9 E1 2E 32 1B CF 77	6 Jul 2020	22 set 2030
CN = Actalis SMIME RSA CA 2025 O = Actalis S.p.A. L = Ponte San Pietro S = Bergamo C = IT	8d e8 af d2 e4 fe 55 20 49 3f f2 83 22 f0 a0 39 89 22 84 45	07 July 2025	05 July 2035

1.3.2 Registration Authorities

Registration Authorities (RAs) are the entities performing Identification and Authentication (I&A) of Applicants, their registration into the CA database, and transmission of certificate requests to the CA.

For certificates to be issued to individuals (**IV** and **SV** certificates), RA tasks may be performed by external organizations (e.g., employers) acting as "Enterprise RA" in compliance with the [SMBR].

For certificates to be issued to organizations (**OV** certificates), RA tasks are performed by Actalis. In all cases, email address validation shall be performed by Actalis only (it cannot be delegated).

Organizations meeting the requirements for "Enterprise RAs" set forth in the [SMBR] may be enabled to operate as their own RA, on request, limited to the email domains they own or control. This shall be subject to the stipulation of a suitable agreement between such organizations and Actalis in compliance with the [SMBR].

Depending on the quantity of certificates to be managed, specific customer needs and other factors, Actalis may enable Enterprise RAs to request certificates via a specific web-based application allowing greater autonomy and faster processes.

1.3.3 Subscribers

Subscribers may be either **organizations** or **individuals**. In the case of individuals, they may be identified in in the Subject field of certificates as private persons or affiliated with some organization.

1.3.4 Relying Parties

Relying Parties (RPs) are all entities that rely on the accuracy of the binding between the Subject's public key distributed via a certificate and the Subject's identity contained in the same certificate.

1.3.5 Other Participants

Certificates may also be provided through Resellers (business partners), which in certain cases may also play the role of Registration Authorities, depending on the agreements in place with Actalis.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

Four types of S/MIME certificates are covered by this CP according to the [SMBR] terminology:

- **Mailbox-Validated (OV)** – issued to natural or legal person, contains only an email address;
- **Individual-Validated (IV)** - issued to a natural person, contains the subscriber's individual identity (personal name) in addition to an email address;
- **Organization-Validated (OV)** – issued to an organization (legal person), contains the subscriber's organization identity in addition to an email address;
- **Sponsor-Validated (SV)** – issued to an individual (natural person) associated with an organization (legal person), contains both an individual identity (personal name) and an organization's identity in addition to an email address.

All these types of certificates are *mainly* intended for **signing and/or encrypting email messages according** to the **S/MIME** standard [SMIME], typically by means of a suitable email application.

A non-committal list of supported email clients can be found on the Actalis' website at the following URL: https://guide.actalis.com/smime/documentation. Applicants are supposed to review that list before requesting Actalis' S/MIME certificates.

Subscribers are allowed to use the Certificates to sign and/or encrypt data in different ways and for different purposes (i.e., not necessarily according to the S/MIME standard); however, Actalis declines all responsibility for any inconvenience that Subscribers may encounter in that case.

Certificates issued under this CP can also be used for SSL/TLS client authentication [TLS], depending on the target environment; however, Actalis declines all responsibility for any inconvenience that Subscribers may encounter in that case.

Note: It is assumed that Applicants have the competence and the tools required to request, install, and use their Certificates. Otherwise, Actalis is available to offer the necessary consultancy.

1.4.2 Prohibited certificate uses

Any use of the Certificate other than allowed in section 1.4.1 is discouraged and may result in the revocation of the Certificate by Actalis (see also section 4.9.1), depending on the security impact of the use being made of the Certificate.

See also [CPS] for additional provisions.

1.5 Policy administration

1.5.1 Organization administering the document

This CP is drafted, revised, approved, published and maintained by Actalis S.p.A.

1.5.2 Contact person

For any questions regarding this CP, please write to ca-admin@actalis.it.

For instructions on how to submit a Certificate Problem Report or revocation request, please refer to section 1.5.2 of the reference [CPS].

1.5.3 Person determining CP suitability for the policy

This CP is approved by Actalis' CA services direction, after review by all internal stakeholders, taking into account the Requirements [SMBR].

1.5.4 CP approval procedures

Approval of this CP follows the procedures defined in the company's Quality Management System. This CP is reviewed and updated at least yearly.

1.6 Definitions and acronyms

ARL	Authority Revocation List
CA	Certification Authority (see CSP)
CAA	Certification Authority Authorization
CABF	CA/Browser Forum
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSP	Certification Service Provider (see CA)
CSR	Certificate Signing Request
HSM	Hardware Security Module
HTTP	Hyper-Text Transfer Protocol
I&A	Identification and Authentication
ICA	Intermediate CA
IV	Individual-Validated
LDAP	Lightweight Directory Access Protocol
LEI	Legal Entity Identifier
MV	Mailbox-Validated
OID	Object Identifier
OV	Organization-Validated
PKI	Public Key Infrastructure
RA	Registration Authority
S/MIME	Secure MIME
SSL	Secure Sockets Layer
SV	Sponsor-Validated
TLS	Transport Layer Security

1.7 References

[BR] CA/Browser Forum: "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" (https://cabforum.org/baseline-requirements-documents/)

[SMBR] CA/Browser Forum: "Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates" (https://cabforum.org/smime-br/)

[CAA] RFC 9495: "Certification Authority Authorization (CAA) Processing for Email Addresses", October 2023.

[CPS] Certification Practice Statement - SSL Server and Code Signing certificates (https://www.actalis.com/cps-for-ssl-server-and-code-signing)

[CSR] RFC 2314: "PKCS #10: Certification Request Syntax Version 1.5", March 1998.

[HTTP] RFC 2616: "Hypertext Transfer Protocol -- HTTP/1.1", June 1999.

[LDAP] RFC 4511: "Lightweight Directory Access Protocol (LDAP) - The Protocol", June 2006.

[MRSP] Mozilla Root Store Policy (https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy)

[MTRP] Microsoft Trusted Root Program (https://docs.microsoft.com/en-us/security/trusted-root/program-requirements)

[ARCP] Apple Root Certificate Program (https://www.apple.com/certificateauthority/ca_program.html)

[OCSP] RFC 6960: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", June 2013.

[LOCSP] RFC 5019: "The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments", September 2007.

[PFW] RFC 3647: "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", November 2003.

[PFX] RFC 7292: "PKCS #12: Personal Information Exchange Syntax v1.1", July 2014.

[PROF] RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", May 2008.

[XUPD] RFC 6818, "Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", January 2013.

[SMIME] RFC5751: "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification", January 2010.

[T&C] S/MIME Certificates – Terms & Conditions (https://www.actalis.it/documenti-en/sslclient_smime_termsconditions.aspx)

[TLS] RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2", August 2008.

[eIDAS] Regulation (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in

the internal market and repealing Directive 1999/93/EC and subsequent amendments (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02014R0910-20241018)

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

See §4.9 and §4.10 for details on revocation information.

2.2 Publication of certification information

Actalis publishes this CP, the related CPS, Terms and Conditions, Subscriber Agreements, and other relevant documentation in the Repository below, freely accessible by anyone on a 24x7 basis:

https://www.actalis.com/legal-repository.aspx.

2.3 Time or frequency of publication

This CP is reviewed and updated at least once every 365 days, also to ensure that it conforms to the latest versions of applicable CAB Forum Requirements and other applicable standards and regulations.

As to the time and frequency of CRL publication, see §4.9.7.

2.4 Access controls on repositories

The Actalis Repository is freely accessible by anyone in read-only mode. Only authorized users and systems can write to it, and suitable controls are in place to prevent unauthorized writes.

3 IDENTIFICATION AND AUTHENTICATION (I&A)

3.1 Naming

See section 7.1.4.

3.1.1 Types of names

Actalis issues Certificates with non-null subject DNs complying with ITU X.500.

Actalis does not issue pseudonymous Certificates.

In any case, §3.1.1 of the [SMBR] applies.

3.1.2 Need for names to be meaningful

As per §3.1.2 of the [SMBR].

3.1.3 Anonymity or pseudonymity of subscribers

Pseudonyms are not supported.

3.1.4 Rules for interpreting various name forms

As per §3.1.4 of the [SMBR].

3.1.5 Uniqueness of names

No stipulation.

3.1.6 Recognition, authentication, and role of trademarks

No stipulation.

3.2 Initial Identity Validation

The CA SHALL authenticate the identity attributes of the Subject and their control over the Mailbox Addresses to be included in the S/MIME Certificate according to the requirements of the following sections:

Certificate Type	Mailbox Control	Organization Identity	Individual Identity
Mailbox-validated	Section 3.2.2	N/A	N/A
Organization-validated	Section 3.2.2	Section 3.2.3	N/A
Sponsor-validated	Section 3.2.2	Section 3.2.3	Section 3.2.4
Individual-validated	Section 3.2.2	N/A	Section 3.2.4

3.2.1 Method to prove possession of private key

When the Subscriber's private key is generated by Applicant, this latter shall send its public key to the CA as a CSR (Certificate Signing Request) in PKCS#10 format, as part of the certificate request. In this case the CA, before issuing the certificate, shall check that the CSR is cryptographically valid. See also §6.1.2 for further details.

3.2.2 Validation of mailbox authorization or control

The CA SHALL verify that the Applicant controls the email account associated with the Mailbox Address referenced in the Certificate (or has been authorized by the email account holder to act on the account holder's behalf) by one of the following methods:

- by verifying the Applicant's control over the domain portion of the Mailbox Address using one of the methods allowed by the CAB Forum's Baseline Requirements [BR], in compliance with §3.2.2.1 of the [SMBR];
- by sending an email message containing a **unique Random Value** to the Mailbox Address and receiving a confirming response utilizing the same Random Value, in compliance with §3.2.2.2 of the [SMBR].

In any case, §3.2.2 of the [SMBR] applies.

3.2.3 Authentication of organization identity

For **OV** and **SV** certificates issued under this CP, Actalis shall collect, verify, and retain evidence supporting the following identity attributes for the Organization:

- formal name of the Legal Entity (as registered);
- address of the Legal Entity (main place of business);
- Jurisdiction of Incorporation or Registration of the Legal Entity;
- unique identifier and type of identifier for the Legal Entity.

The unique identifier shall be included in the Certificate *subject:organizationIdentifier* attribute as specified in §7.1.4.2.2 in compliance with the [SMBR].

All these data shall be verified by Actalis by querying reliable independent information sources like e.g., the applicable jurisdiction's company registry, or a governmental database of public agencies, or a LEI data reference, in compliance with §3.2.8 of the [SMBR]. Where such sources are not usable, Actalis may accept a suitable Attestation (e.g., a Lawyer's letter) in line with §3.2.8 of the [SMBR].

3.2.4 Authentication of individual identity

For **IV** and **SV** certificates, the Applicant's identity shall be verified in compliance with section 3.2.4 of the [SMBR]. Actalis (or an Enterprise RA on Actalis' behalf) shall collect, verify, and retain evidence supporting at least the following identity attributes for the individual Applicant:

- given name(s) and surname(s), which shall be current names;
- ID unique identification number, issuer, and validity period.

In order to collect these data, any of the methods described in §3.2.4.1 of the [SMBR] can be employed, depending on the certificate request channel and other factors. Normally, Actalis requires the Applicant to show a government-issued physical identity document bearing the holder's photo, such as passport or identity card. Other kinds of IDs are not accepted.

For physical ID document validation, Actalis may apply automated techniques and/or manual processes that involve accessing authoritative sources to verify the authenticity of ID documents, depending on the certificate request channel and other factors. In particular circumstances, Actalis may perform individual identity validation based on a qualified digital signature [eIDAS] compliant of the Applicant placed on a certificate application form.

Organizations enabled to act as Enterprise RAs are allowed to use their own records as evidence of individual identity verification, subject to the provisions of the related agreement with Actalis.

Validation of the Individual identities shall in any case conform to §3.2.4 of the [SMBR].

3.2.5 Non-verified subscriber information

Actalis does not include in Publicly-Trusted S/MIME Certificates any Subscriber information that has not been verified in accordance with [SMBR].

3.2.6 Validation of authority

For OV and SV certificates, before commencing to issue a Certificate regulated by this CP, Actalis shall use a Reliable Method of Communication to verify the authenticity of the Applicant Representative's certificate request, in line with §3.2.6 of the [SMBR]. To this end, Actalis will normally use one of the following methods:

- Applicant's confirmation by telephone;
- Applicant's confirmation by certified email;
- Applicant's Qualified Electronic Signature (QES) on the certificate application form;
- formal purchase order on the Applicant's organization headed paper;
- a suitable Attestation (e.g., a Lawyer's letter) in line with §3.2.8 of the [SMBR].

Other methods may also be used, depending on the circumstances.

For further details, please refer to §3.2.5 of the [CPS].

3.2.7 Criteria for interoperation

The provisions of §3.2.7 of the [SMBR] apply.

3.2.8 Reliability of verification sources

The provisions of §3.2.8 of the [SMBR] apply.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for re-key request

No stipulation.

3.3.2 Identification and authentication for re-key after revocation

No stipulation.

3.4 Identification and authentication for revocation request

I&A for revocation requests depends on how the request is made and by whom:

- depending on the certificate request channel, the Subscriber can request the revocation of their certificate online, on a 24x7 basis, by accessing:
    - the Actalis' portal, using the authentication credentials provided to them upon issuance of the certificate; or,
    - a Reseller's portal, using the related authentication credentials;
- an Enterprise RA can request the revocation of their own certificates, in the circumstances indicated in this CP, either interactively from an Actalis portal, or programmatically by calling an appropriate API, subject to strong authentication of the operator/caller.
- a Reseller can request the revocation of certificates they ordered, in the circumstances indicated in this CP, by calling an appropriate API, subject to strong client authentication.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can submit a certificate application

No stipulation.

4.1.2 Enrollment process and responsibilities

The certificate request process details vary depending on whether it takes place on the CA website, a Reseller's, or the Actalis' portal for Enterprise RAs. However, the CA shall always obtain the following from the Applicant:

- a Certificate Request; and
- an executed Subscriber Agreement and/or Terms of Use.

The Certificate Request may include a CSR (PKCS#10 object) or not, depending on the certificate request channel and Applicant's preferences. See section 6.1.2 for further details.

The Terms of Use shall be executed by Applicants as part of the certificate request procedure, except for Enterprise RAs which must adhere to Actalis' Terms of Conditions upon entering into the related agreement with Actalis.

In any cases, the provisions of §4.1.2 of [SMBR] apply.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

Upon receipt of a certificate application via any of the channels/methods described in §4.1, all the verifications described in §3.2 and not yet done are performed either automatically, where feasible and allowed, or manually by a Validation Specialist, in compliance with the [SMBR], according to the certificate type and the specific verification to be done.

Actalis may reuse previous validations and/or supporting evidence for additional certificates to be issued to the same Applicant, to the extent that is permitted by §4.2.1 of the [SMBR].

4.2.2 Approval or rejection of certificate applications

Starting from March 15, 2025, prior to issuing a certificate that includes a Mailbox Address, Actalis retrieves and processes CAA Resource Records [CAA] according to section 4.2.2.1 of the [SMBR]. In particular, Actalis SHALL process the "issuemail" property tag as specified in RFC 9495.

The domain identifier to be used in CAA records to authorize the Actalis CA is "actalis.it".

Actalis also logs the results of all CAA records checking.

4.2.3 Time to process certificate applications

No stipulation.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

If all the previous steps (see §4.2) completed successfully, the CA system:

- if the Applicant has sent a CSR, checks that the CSR is well-formed and does not contain unexpected data, the CSR signature is valid, the key algorithm and size meet the applicable constraints, and the Public Key in the CSR is not affected by known weaknesses;
- otherwise, generates a suitable Key Pair for the Applicant;

Next, the CA system generates the Certificate, stores it into its database, and makes it available to the requester in ways that depends on how the certificate was requested (see §4.1).

When the Subscriber' Private Key is generated by the CA, the Certificate is made available as a PKCS#12 file whose protection password is provided to the Subscriber over a different channel (e.g., via HTTPS or SMS). See also §6.1.2 for additional details.

4.3.2 Notification to subscriber by the CA of issuance of certificate

When an Enterprise RA is not involved, the CA normally sends the Certificate to Subscriber via email. This email sending may be omitted if the certificate request was submitted by a Reseller that runs its own certificate management portal for its own customers.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

No stipulation.

4.4.2 Publication of the certificate by the CA

No stipulation.

4.4.3 Notification of certificate issuance by the CA to other entities

No stipulation.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

See sections 1.4 and 9.6.3.

4.5.2 Relying party public key and certificate usage

No stipulation.

4.6 Certificate renewal

No stipulation.

4.6.1 Circumstance for certificate renewal

No stipulation.

4.6.2 Who may request renewal

No stipulation.

4.6.3 Processing certificate renewal requests

No stipulation.

4.6.4 Notification of new certificate issuance to subscriber

No stipulation.

4.6.5 Conduct constituting acceptance of a renewal certificate

No stipulation.

4.6.6 Publication of the renewal certificate by the CA

No stipulation.

4.6.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.7 Certificate re-key

In the event that the Subscriber wishes their Certificate to contain a different public key, the Subscriber should request revocation of their current Certificate and apply for a new one.

4.7.1 Circumstance for certificate re-key

No stipulation.

4.7.2 Who may request certification of a new public key

No stipulation.

4.7.3 Processing certificate re-keying requests

No stipulation.

4.7.4 Notification of a new certificate issuance to subscriber

No stipulation.

4.7.5 Conduct constituting acceptance of a re-key certificate

No stipulation.

4.7.6 Publication of the re-key certificate by the CA

No stipulation.

4.7.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.8 Certificate modification

4.8.1 Circumstance for certificate modification

In the event that the Subscriber wishes their Certificate to contain different Subject information, the Subscriber should request revocation of their current Certificate and apply for a new one.

4.8.2 Who may request certificate modification

No stipulation.

4.8.3 Processing certificate modification requests

No stipulation.

4.8.4 Notification of new certificate issuance to subscriber

No stipulation.

4.8.5 Conduct constituting acceptance of modified certificate

No stipulation.

4.8.6 Publication of the modified certificate by the CA

No stipulation.

4.8.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for revocation

4.9.1.1 Reasons for revoking a subscriber certificate

Actalis shall revoke the certificate **within 24 hours** if one or more of the following occurs:

- the Subscriber requests in writing that Actalis revoke the Certificate;
- the Subscriber notifies Actalis that the original Certificate Request was not authorized and does not retroactively grant authorization (*);
- Actalis obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise; (*)
- Actalis is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate;
- Actalis obtains evidence that the validation of domain authorization or mailbox control for any Mailbox Address in the Certificate should not be relied upon.

Actalis shall revoke the certificate **within 5 days** if one or more of the following occurs:

- the Certificate no longer complies with the requirements of §6.1.5 and §6.1.6;
- Actalis obtains evidence that the Certificate was misused;
- Actalis is made aware that the Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use;
- Actalis is made aware of any circumstance indicating that use of an email address or Fully-Qualified Domain Name in the Certificate is no longer legally permitted (e.g., a court or arbitrator has revoked the right to use an email address or Domain Name, a relevant licensing or services agreement between the Subscriber has terminated, or the account holder has failed to maintain the active status of the email address or Domain Name);
- Actalis is made aware of a material change in the information contained in the Certificate;
- Actalis is made aware that the Certificate was not issued in accordance with these CP and/or the referenced CPS (*);

- Actalis determines or is made aware that any of the information appearing in the Certificate is inaccurate (*);
- Actalis' right to issue Certificates under the [SMBR] expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository;
- revocation is required by this CP and/or the referenced CPS; or
- Actalis CA is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed.

In the cases marked with an asterisk (*), the Subscriber **must** promptly request revocation of their certificate as soon as they become aware of the circumstance.

4.9.1.2 Reasons for revoking a subordinate CA certificate

The provisions of §4.9.1.2 of the [SMBR] apply.

4.9.2 Who can request revocation

The Subscriber, an Enterprise RA, or Actalis can initiate revocation. Additionally, Subscribers, Relying Parties, Application Software Suppliers, and other third parties may submit Certificate Problem Reports (see section 1.5.2) informing Actalis of reasonable cause to revoke a Certificate.

4.9.3 Procedure for revocation request

For Mailbox-Validated certificates, certificate suspension is not supported, for the other types the suspension or revocation may occur on request of the Subscriber, or an Enterprise RA, or a Reseller, or the CA itself, depending on circumstance.

Subscribers may request suspension or revocation of their own certificates by accessing an Actalis' web site and following the on-screen instructions. The address of the suitable web site is included in the same mail by which the certificate is sent to the user, or is provided on the Actalis' main website.

Enterprise RAs enabled to the dedicated Actalis' portal (see §1.3.2.1) can also request certificate suspension or revocation through that portal.

4.9.4 Revocation request grace period

No stipulation.

4.9.5 Time within CA must process the revocation request

The provisions of §4.9.5 of the [SMBR] apply.

4.9.6 Revocation checking requirement for relying parties

No stipulation.

Note: Since a Certificate may be revoked for the reasons listed in §4.9, Relying Parties should check the revocation status of all Certificates that contain a CDP or OCSP pointer.

4.9.7 CRL issuance frequency

The provisions of §4.9.7 of the [SMBR] apply. In particular, the CRL is regenerated and republished every 24 hours, even in the absence of new certificate status changes after the last CRL issuance.

4.9.8 Maximum latency for CRLs

No stipulation.

4.9.9 On-line revocation/status checking availability

The status of certificates is made available to all Relying Parties in two ways:

- by publishing a Certificate Revocation List (CRL) compliant with RFC 5820;
- by providing an on-line certificate status service based on the OCSP protocol, in compliance with RFC 6960 and RFC 5019.

The HTTP address of the CRL is inserted in the CRL Distribution Points (CDP) certificate extension, instead the OCSP responder address is inserted in the Authority Information Access (AIA) extension.

The CRL is regenerated and republished every 24 hours, even in the absence of new certificate status changes after the last CRL issuance.

The CRL and OCSP services can be freely accessed by anyone.

The provisions of §4.9.9 of the [SMBR] also apply.

4.9.10 On-line revocation checking requirements

The provisions of §4.9.10 of the [SMBR] apply.

4.9.11 Other forms of revocation advertisements available

No stipulation.

4.9.12 Special requirements re key compromise

See §4.9.1.

4.9.13 Circumstances for suspension

No Stipulation.

4.9.14 Who can request suspension

No Stipulation.

4.9.15 Procedure for suspension request

No Stipulation.

4.9.16 Limits on suspension request

No Stipulation.

4.10 Certificate status services

See §4.9.9.

4.10.1 Operational characteristics

Revocation entries on a CRL or OCSP Response shall not be removed until after the Expiry Date of the revoked Certificate.

4.10.2 Service availability

As per §4.10.2 of the [SMBR].

4.10.3 Optional features

No stipulation.

4.11 End of subscription

The contract between Actalis and the Subscriber ends when the Subscriber's certificate expires or is revoked, whichever comes first.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

No stipulation.

4.12.2 Session key encapsulation and recovery policy and practices

No stipulation.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

All facility, management, and operations controls applying to this certificate policy are exactly the same as those documented in [CPS], except where otherwise specified hereafter.

5.1 Physical Security Control

5.1.1 Site location and construction

Same as documented in [CPS].

5.1.2 Physical access

Same as documented in [CPS].

5.1.3 Power and air conditioning

Same as documented in [CPS].

5.1.4 Water exposures

Same as documented in [CPS].

5.1.5 Fire prevention and protection

Same as documented in [CPS].

5.1.6 Media storage

Same as documented in [CPS].

5.1.7 Waste disposal

Same as documented in [CPS].

5.1.8 Off-site backup

Same as documented in [CPS].

5.2 Procedural Controls

5.2.1 Trusted roles

Same as documented in [CPS].

5.2.2 Number of persons required per task

Same as documented in [CPS].

5.2.3 Identification and authentication for each role

Same as documented in [CPS].

5.2.4 Roles requiring separations of duties

Same as documented in [CPS].

5.3 Personnel Controls

5.3.1 Qualification, experience, and clearance requirements

The personnel employed in the Actalis' certification services has the necessary qualifications, experience, and have undergone suitable training.

5.3.2 Background check procedures

Same as documented in [CPS].

5.3.3 Training requirements

Same as documented in [CPS].

5.3.4 Retraining frequency and requirements

Same as documented in [CPS].

5.3.5 Job rotation frequency and sequence

No stipulation

5.3.6 Sanction for unauthorized actions

Same as documented in [CPS].

5.3.7 Independent contractor requirements

Same as documented in [CPS].

5.3.8 Documentation supplied to personnel

Same as documented in [CPS].

5.4 Audit logging procedures

5.4.1 Types of events recorded

Same as documented in [CPS].

5.4.2 Frequency of processing audit log

Same as documented in [CPS].

5.4.3 Retention period for audit log

Same as documented in [CPS].

5.4.4 Protection of audit log

Same as documented in [CPS].

5.4.5 Audit log backup procedures

Same as documented in [CPS].

5.4.6 Audit collection system (internal vs. external)

No stipulation.

5.4.7 Notification to event-causing subject

No stipulation.

5.4.8 Vulnerability assessments

Same as documented in [CPS].

5.5 Records archival

5.5.1 Types of record archived

The CA and each Delegated Third Party archive all audit data, certificate application information including all data used for verifying the identity of applicants, documentation supporting certificate applications and documentation related to the security of their Certificate Systems, Certificate Management Systems, Root CA Systems and Delegated Third Party Systems.

5.5.2 Retention period for archive

Archives are kept for at least 3 years.

5.5.3 Protection of archive

Same as documented in [CPS].

5.5.4 Archive backup procedures

Same as documented in [CPS].

5.5.5 Requirements for time-stamping of records

Same as documented in [CPS].

5.5.6 Archive collection system (internal or external)

No stipulation.

5.5.7 Procedures to obtain and verify archive information

Same as documented in [CPS].

5.6 Key changeover

No stipulation.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

Same as documented in [CPS].

5.7.2 Computing resources, software, and/or data are corrupted

Same as documented in [CPS].

5.7.3 Entity private key compromise procedures

Same as documented in [CPS].

5.7.4 Business continuity capabilities after a disaster

Same as documented in [CPS].

5.8 CA or RA termination

Same as documented in [CPS].

6 TECHNICAL SECURITY CONTROLS

All facility, management, and operations controls applying to this certificate policy are exactly the same as documented in [CPS], except where otherwise specified hereafter.

6.1 Key pair generation and installation

6.1.1 Key pair generation

6.1.1.1 CA key pair generation

The key pairs of the CA are generated and handled as documented in [CPS].

6.1.1.2 RA key pair generation

No stipulation.

6.1.1.3 Subscriber key pair generation

The provisions of §6.1.1.3 of the [SMBR] apply. See also §6.1.2 below.

6.1.2 Private key delivery to subscriber

Depending on the specific certificate request procedure or channel used, the Subscriber's Private Key may be generated by CA on request by the Applicant. In such a case, the private key is provided to the Subscriber together with the corresponding certificate within a single PKCS#12 file [PFX].

The private key within the PKCS#12 file is encrypted by a password-based encryption algorithm ensuring at least 128 bits of cipher strength, using a random password of suitable length and complexity, in accordance with the [SMBR].

The password needed to decipher the PKCS#12 file is provided to the Subscriber in such a way as to prevent unauthorized parties to get hold of both the PKCS#12 file and the related password. If the password is provided on-line, a TLS channel is used; otherwise, it is delivered via a separate communication channel (e.g., SMS).

Actalis does not archive the PKCS#12 files generated for Subscribers nor the related passwords.

6.1.3 Public key delivery to certificate issuer

No stipulation.

6.1.4 CA public key delivery to relying parties

No stipulation.

6.1.5 Key sizes

The provisions of §6.1.5 of the [SMBR] apply.

6.1.6 Public key parameters generation and quality checking

The provisions of §6.1.6 of the [SMBR] apply.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

The provisions of §6.1.7 of the [SMBR] apply.

6.2 Private Key Protection and Cryptographic Module Engineering controls

The CA private keys are generated and handled as documented in [CPS].

6.2.1 Cryptographic module standards and controls

Same as documented in [CPS].

6.2.2 Private key (n out of m) multi-person control

Same as documented in [CPS].

6.2.3 Private key escrow

Same as documented in [CPS].

6.2.4 Private key backup

Same as documented in [CPS].

6.2.5 Private key archival

Same as documented in [CPS].

6.2.6 Private key transfer into or form a cryptographic module

Same as documented in [CPS].

6.2.7 Private key storage on cryptographic module

Same as documented in [CPS].

6.2.8 Method of activating private key

Same as documented in [CPS].

6.2.9 Method of deactivating private key

Same as documented in [CPS].

6.2.10 Method of destroying private key

Same as documented in [CPS].

6.2.11 Cryptographic module rating

Same as documented in [CPS].

6.3 Other aspects of key pair management

6.3.1 Public key archival

No stipulation.

6.3.2 Certificate operational periods and key pair usage periods

The provisions of §6.3.2 of the [SMBR] apply.

6.4 Activation data

6.4.1 Activation data generation and installation

Same as documented in [CPS].

6.4.2 Activation data protection

Same as documented in [CPS].

6.4.3 Other aspects of activation data

Same as documented in [CPS].

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

Same as documented in [CPS].

6.5.2 Computer security rating

Same as documented in [CPS].

6.6 Life cycle technical controls

6.6.1 Security development controls

Same as documented in [CPS].

6.6.2 Security management controls

Same as documented in [CPS].

6.6.3 Life cycle security controls

Same as documented in [CPS].

6.7 Network security controls

Same as documented in [CPS].

6.8 Time-stamping

No stipulation.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

7.1.1 Version number(s)

Certificates are of type X.509 v3.

7.1.2 Certificate content and extensions

7.1.2.1 Root CA certificates

For the legacy Root CA profile, please refer to [CPS].
The certificates of the new dedicated Root CAs have the following profile:

Field	Value
Version	V3 (2)
SerialNumber	<includes at least 8 pseudo-random bytes>
Signature	ecdsa-with-SHA384 (1.2.840.10045.4.3.3)

Issuer	CN = Actalis SMIME ECC Root CA 2025 O = Actalis S.p.A. C = IT	
Validity	<According to section 6.3.2>	
Subject	CN = Actalis SMIME ECC Root CA 2025 O = Actalis S.p.A. C = IT	
SubjectPublicKeyInfo	<ECC public key of 384 bits>	
SignatureValue	<Root CA signature>	
Extension	**Critical?**	**Value**
Basic Constraints	True	CA=true
AuthorityKeyIdentifier (AKI)		<SHA1- of the public key>
SubjectKeyIdentifier (SKI)		<SHA1- of the public key>
KeyUsage	True	keyCertSign, cRLSign
ExtendedKeyUsage (EKU)		<not included>
CertificatePolicies		<not included>
SubjectAlternativeName (SAN)		<not included>
AuthorityInformationAccess (AIA)		<not included>
CRLDistributionPoints (CDP)		<not included>

Field	**Value**	
Version	V3 (2)	
SerialNumber	<includes at least 8 pseudo-random bytes>	
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)	
Issuer	CN = Actalis SMIME RSA Root CA 2025 O = Actalis S.p.A. L = Ponte San Pietro ST = Bergamo C = IT	
Validity	<According to section 6.3.2>	
Subject	CN = Actalis SMIME RSA Root CA 2025 O = Actalis S.p.A. L = Ponte San Pietro ST = Bergamo C = IT	
SubjectPublicKeyInfo	<RSA public key of 4096 bits>	
SignatureValue	<Root CA signature>	
Extension	**Critical?**	**Value**
Basic Constraints	True	CA=true
AuthorityKeyIdentifier (AKI)		<SHA1- of the public key>

SubjectKeyIdentifier (SKI)		<SHA1- of the public key>
KeyUsage	True	keyCertSign, cRLSign
ExtendedKeyUsage (EKU)		<not included>
CertificatePolicies		<not included>
SubjectAlternativeName (SAN)		<not included>
AuthorityInformationAccess (AIA)		<not included>
CRLDistributionPoints (CDP)		<not included>

7.1.2.2 Cross Certificates

Actalis' Cross Certificates have the following profile:

Field	**Value**	
Version	V3 (2)	
SerialNumber	<includes at least 8 pseudo-random bytes>	
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)	
Issuer	CN = Actalis Authentication Root CA O = Actalis S.p.A./03358520967 L = Milano C = IT	
Validity	<According to section 6.3.2>	
Subject	CN = Actalis SMIME RSA Root CA 2025 O = Actalis S.p.A. C = IT	
SubjectPublicKeyInfo	<RSA public key of 4096 bits>	
SignatureValue	<Root CA signature>	
Extension	**Critical?**	**Value**
Basic Constraints	True	CA=true
AuthorityKeyIdentifier (AKI)		<Same value as the Root CA SKI extension>
SubjectKeyIdentifier (SKI)		<public key SHA1-digest>
KeyUsage	True	keyCertSign, cRLSign
ExtendedKeyUsage (EKU)		clientAuth (1.3.6.1.5.5.7.3.2), emailProtection (1.3.6.1.5.5.7.3.4)
CertificatePolicies		PolicyOID = 2.5.29.32.0 (anyPolicy)
SubjectAlternativeName (SAN)		<not included>
AuthorityInformationAccess (AIA)		<HTTP address of OCSP responder>
CRLDistributionPoints (CDP)		<HTTP address to access the ARL>

7.1.2.3 Subordinate CA certificates

The certificates of the subordinate CAs, used to sign end-entity certificates, have the following profile:

Field	Value	
Version	V3 (2)	
SerialNumber	<includes at least 8 pseudo-random bytes>	
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)	
Issuer	CN = Actalis Authentication Root CA O = Actalis S.p.A./03358520967 L = Milano C = IT	
Validity	<According to section 6.3.2>	
Subject	CN = Actalis Client Authentication CA GN O = Actalis S.p.A. L = Ponte San Pietro ST = Bergamo C = IT	
SubjectPublicKeyInfo	<RSA public key of 4096 bits>	
SignatureValue	<Root CA signature>	
Extension	**Critical?**	**Value**
Basic Constraints	True	CA=true
AuthorityKeyIdentifier (AKI)		<Same value as the Root CA SKI extension>
SubjectKeyIdentifier (SKI)		<public key SHA1-digest>
KeyUsage	True	keyCertSign, cRLSign
ExtendedKeyUsage (EKU)		clientAuth (1.3.6.1.5.5.7.3.2), emailProtection (1.3.6.1.5.5.7.3.4)
CertificatePolicies		PolicyOID = 2.5.29.32.0 (anyPolicy), CPS-URI = <HTTP link to Actalis' legal repository>
SubjectAlternativeName (SAN)		<not included>
AuthorityInformationAccess (AIA)		<HTTP address of OCSP responder>
CRLDistributionPoints (CDP)		<HTTP address to access the ARL>, <LDAP address to access the ARL>

Field	Value
Version	V3 (2)
SerialNumber	<includes at least 8 pseudo-random bytes>
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	CN = Actalis SMIME RSA Root CA 2025 O = Actalis S.p.A. L = Ponte San Pietro ST = Bergamo C = IT
Validity	<According to section 6.3.2>

Subject	CN = Actalis SMIME RSA CA 2025 O = Actalis S.p.A. L = Ponte San Pietro ST = Bergamo C = IT	
SubjectPublicKeyInfo	<RSA public key of 4096 bits>	
SignatureValue	<Root CA signature>	
Extension	**Critical?**	**Value**
Basic Constraints	True	CA=true
AuthorityKeyIdentifier (AKI)		<Same value as the Root CA SKI extension>
SubjectKeyIdentifier (SKI)		<public key SHA1-digest>
KeyUsage	True	keyCertSign, cRLSign
ExtendedKeyUsage (EKU)		clientAuth (1.3.6.1.5.5.7.3.2), emailProtection (1.3.6.1.5.5.7.3.4)
CertificatePolicies		PolicyOID = 2.5.29.32.0 (anyPolicy) CPS-URI = <HTTP link to Actalis' legal repository>
SubjectAlternativeName (SAN)		<not included>
AuthorityInformationAccess (AIA)		ocsp: <HTTP address of OCSP responder> caIssuers: <HTTP address of the Root CA >
CRLDistributionPoints (CDP)		<HTTP address to access the ARL>

Field	**Value**	
Version	V3 (2)	
SerialNumber	<includes at least 8 pseudo-random bytes>	
Signature	ecdsa-with-SHA384 (1.2.840.10045.4.3.3)	
Issuer	CN = Actalis SMIME ECC Root CA 2025 O = Actalis S.p.A. L = Ponte San Pietro ST = Bergamo C = IT	
Validity	<According to section 6.3.2>	
Subject	CN = Actalis SMIME ECC CA 2025 O = Actalis S.p.A. L = Ponte San Pietro ST = Bergamo C = IT	
SubjectPublicKeyInfo	<ECC public key of 384 bits>	
SignatureValue	<Root CA signature>	
Extension	**Critical?**	**Value**
Basic Constraints	True	CA=true
AuthorityKeyIdentifier (AKI)		<Same value as the Root CA SKI extension>

SubjectKeyIdentifier (SKI)		<public key SHA1-digest>
KeyUsage	True	keyCertSign, cRLSign
ExtendedKeyUsage (EKU)		clientAuth (1.3.6.1.5.5.7.3.2), emailProtection (1.3.6.1.5.5.7.3.4)
CertificatePolicies		PolicyOID = 2.5.29.32.0 (anyPolicy) CPS-URI = <HTTP link to Actalis' legal repository>
SubjectAlternativeName (SAN)		<not included>
AuthorityInformationAccess (AIA)		ocsp: <HTTP address of OCSP responder> caIssuers: <HTTP address of the Root CA >
CRLDistributionPoints (CDP)		<HTTP address to access the ARL>

7.1.2.4 Subscriber certificates

All subscriber certificates comply with the [SMBR] provisions for "Multipurpose Generation".

7.1.2.4.1 Mailbox Validated (MV)

The profile of MV subscriber certificates is as follows:

Base field	**Value**	
Version	V3 (2)	
SerialNumber (hex)	<Includes at least 8 pseudo-random bytes>	
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)	
Issuer	<Subject of the Subordinate CA – see §7.2>	
Validity	<According to section 6.3.2>	
Subject	CN = <Email address of the Subscriber>	
SubjectPublicKeyInfo	<Public RSA key of length 2048 bits>	
SignatureValue	<Subordinate CA signature value>	
Extension	**Critical?**	**Value**
Basic Constraints	True	cA=FALSE
AuthorityKeyIdentifier (AKI)		KeyID=<SHA1 hash of the CA public key>
SubjectKeyIdentifier (SKI)		<SHA1 hash of Subject public key>
KeyUsage	True	digitalSignature, keyEncipherment
ExtendedKeyUsage (EKU)		clientAuth (1.3.6.1.5.5.7.3.2), emailProtection (1.3.6.1.5.5.7.3.4)
CertificatePolicies		CABF mailbox-validated multipurpose (2.23.140.1.5.1.2)
SubjectAlternativeName (SAN)		rfc822Name=<Email address of the Subscriber>
AuthorityInformationAccess (AIA)		id-ad-ocsp: <URL of OCSP responder> id-ad-caIssuers: <URL of Issuing CA>
CRLDistributionPoints (CDP)		<HTTP URL of the CRL>

7.1.2.4.2 Organization Validated (OV)

The profile of OV subscriber certificates is as follows:

Base field	Value	
Version	V3 (2)	
SerialNumber (hex)	<includes at least 8 pseudo-random bytes>	
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)	
Issuer	<Subject of the Subordinate CA – see §7.1.2.2>	
Validity	<According to section 6.3.2>	
Subject	CN = <same as the O attribute> O = <full registered name of Subscriber > organizationIdentifier = <Subscriber's registration reference according to a registration scheme allowed by [SMBR]> L = <locality of the Subscriber> ST = <state or province of the Subscriber> C = <ISO 3166 country code of Subscriber>	
SubjectPublicKeyInfo	<public RSA key of length 2048 bits>	
SignatureValue	<Subordinate CA signature value>	
Extension	**Critical?**	**Value**
Basic Constraints	True	cA=FALSE
AuthorityKeyIdentifier (AKI)		KeyID=<SHA1 hash of the CA public key>
SubjectKeyIdentifier (SKI)		<SHA1 hash of Subject public key>
KeyUsage	True	digitalSignature, keyEncipherment
ExtendedKeyUsage (EKU)		clientAuth (1.3.6.1.5.5.7.3.2), emailProtection (1.3.6.1.5.5.7.3.4)
CertificatePolicies		CABF organization-validated multipurpose (2.23.140.1.5.2.2)
SubjectAlternativeName (SAN)		rfc822Name=<email address of the subscriber>
AuthorityInformationAccess (AIA)		caIssuers: <URL of the issuing CA> ocsp: <URL of OCSP responder>
CRLDistributionPoints (CDP)		<HTTP URL of the CRL>

7.1.2.4.3 Sponsor Validated (SV)

The profile of SV subscriber certificates is as follows:

Base field	Value
Version	V3 (2)
SerialNumber (hex)	<includes at least 8 pseudo-random bytes>
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	<Subject of the Subordinate CA – see §7.1.2.2>
Validity	<According to section 6.3.2>

Subject	CN = <Personal Name (e.g., Name and Surname)> givenName =<Subscriber's forename> surname = <Subscriber's surname> O = <full registered name of Subscriber's organization> organizationIdentifier = <Subscriber's registration reference according to a registration scheme allowed by [SMBR]> L = <locality of the Subscriber's organization> ST = <state or province of the Subscriber's organization> C = <ISO 3166 country code of Subscriber's organization>	
SubjectPublicKeyInfo	<public RSA key of length 2048 bits>	
SignatureValue	<Subordinate CA signature value>	
Extension	**Critical?**	**Value**
Basic Constraints	True	cA=FALSE
AuthorityKeyIdentifier (AKI)		KeyID=<SHA1 hash of the CA public key>
SubjectKeyIdentifier (SKI)		<SHA1 hash of Subject public key>
KeyUsage	True	digitalSignature, keyEncipherment
ExtendedKeyUsage (EKU)		clientAuth (1.3.6.1.5.5.7.3.2), emailProtection (1.3.6.1.5.5.7.3.4)
CertificatePolicies		CABF sponsor-validated multipurpose (2.23.140.1.5.3.2)
SubjectAlternativeName (SAN)		rfc822Name=<email address of the subscriber>
AuthorityInformationAccess (AIA)		caIssuers: <URL of the issuing CA> ocsp: <URL of OCSP responder>
CRLDistributionPoints (CDP)		<HTTP URL of the CRL>

7.1.2.4.4 Individual Validated (IV)

The profile of IV subscriber certificates is as follows:

Base field	**Value**
Version	V3 (2)
SerialNumber (hex)	<includes at least 8 pseudo-random bytes>
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	<Subject of the Subordinate CA – see §7.1.2.2>
Validity	<According to section 6.3.2>
Subject	CN = <Personal Name (e.g., Name and Surname)> givenName =<Subscriber's forename> surname = <Subscriber's surname> L = <Locality of the Subscriber > (optional) ST = <State or province of the Subscriber> (optional) C = <ISO 3166 country code of Subscriber >
SubjectPublicKeyInfo	<public RSA key of length 2048 bits>
SignatureValue	<Subordinate CA signature value>

Extension	Critical?	Value
Basic Constraints	True	cA=FALSE
AuthorityKeyIdentifier (AKI)		KeyID=<SHA1 hash of the CA public key>
SubjectKeyIdentifier (SKI)		<SHA1 hash of Subject public key>
KeyUsage	True	digitalSignature, keyEncipherment
ExtendedKeyUsage (EKU)		clientAuth (1.3.6.1.5.5.7.3.2), emailProtection (1.3.6.1.5.5.7.3.4)
CertificatePolicies		CABF individual-validated multipurpose (2.23.140.1.5.4.2)
SubjectAlternativeName (SAN)		rfc822Name=<email address of the subscriber>
AuthorityInformationAccess (AIA)		caIssuers: <URL of the issuing CA> ocsp: <URL of OCSP responder>
CRLDistributionPoints (CDP)		<HTTP URL of the CRL>

7.1.2.5 All certificates

Further Subject attributes and/or extensions may be present in Subscriber certificates, in compliance with RFC5280 and the [SMBR], subject to verification by the CA, depending on specific projects and customers. See also section 3.1.

7.1.3 Algorithm object identifiers

The provisions of §7.1.3 of the [SMBR] apply.

7.1.4 Name forms

Attribute values are encoded according to RFC 5280.

7.1.4.1 Name encoding

The provisions of §7.1.4.1 of the [SMBR] apply.

7.1.4.2 Subject information - subscriber certificates

The provisions of §7.1.4.2 of the [SMBR] apply.

7.1.4.3 Subject information - root certificates and subordinate CA certificates

The provisions of §7.1.4.3 of the [SMBR] apply.

7.1.5 Name constraints

Actalis may issue, subject to a contractual agreement, Subordinate CA certificates to external entities, signed by an Actalis' root CA key. In such a case, the Subordinate CA certificate will be technically constrained in compliance with section 7.1.5 of the [SMBR].

7.1.6 Certificate policy object identifier

The provisions of §7.1.6 of the [SMBR] apply.

7.1.7 Usage of Policy Constraints extension

No stipulation.

7.1.8 Policy qualifiers syntax and semantics

No stipulation.

7.1.9 Processing semantics for the critical Certificate Policies extension

No stipulation.

7.2 CRL Profile

7.2.1 Version number(s)

Actalis issues CRLs compliant with [PROF] and section 7.2.1 of the [SMBR].

7.2.2 CRL and CRL entry extensions

Depending on the cause of revocation, CRL entries may contain one of the following reasonCodes in their CRLReason extension, according to section 7.2 of the [SMBR]:

- keyCompromise (1);
- affiliationChanged (3);
- superseded (4);
- cessationOfOperation (5);
- certificateHold (6);
- privilegeWithdrawn (9).

7.3 OCSP profile

7.3.1 Version number(s)

The provisions of §7.3.1 of the [SMBR] apply.

7.3.2 OCSP extensions

The provisions of §7.3.2 of the [SMBR] apply.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

Actalis shall issue certificates and operate its PKI in accordance with the applicable law, shall comply with the [SMBR], and shall comply with the audit requirements described hereafter.

8.1 Frequency or circumstances of assessment

The compliance of the Actalis' CA services to this CP, to Regulation (EU) No. 910/2014 ("eIDAS"), to the applicable ETSI standards and to the [SMBR] requirements is verified on an annual basis by an accredited Conformity Assessment Body (CAB). Moreover, always on an annual basis, an internal auditing activity is performed on the CA services that also takes into account aspects related to information security, applicable data protection rules and internal policies and procedures.

8.2 Identity and qualification of assessor

Audits on the CA are carried out by a Conformity Assessment Body (CAB) accredited in compliance with Regulation (EC) no. 765/2008, through personnel qualified and competent on the subject of conformity assessments, according to the ETSI EN 319 403 norm, of Trust Service Providers and the related trust services provided under the eIDAS Regulation. Any second part audits are also performed by accredited bodies in compliance with Regulation (EC) no. 765/2008.

8.3 Assessor's relationship to assessed entity

The Assessment Bodies (CABs) that perform audits on the CA service, and possibly on the external RAs that collaborate with the CA, have no relationship with Actalis. The internal auditor does not belong to the organizational structure that deals with CA activities.

8.4 Topics covered by assessment

The audits performed on the CA are based on "ETSI EN 319 411-1 v1.3.1 or newer" or "ETSI EN 319 411-2 v2.4.1 or newer", which includes normative references to ETSI EN 319 401, and the [SMBR].

8.5 Actions taken as a result of deficiency

The actions resulting from any non-compliance detected during audits (failure to meet the requirements defined in the regulations, standards, and applicable procedures) depend on the nature and severity of the non-compliance detected, on the rules for the management of non-compliances defined by the Assessment Body (CAB) and/or the internal non-conformity management procedures. In general, if a substantive non-compliance results from an audit, Actalis will develop a remedy plan as quickly as possible. This plan could result in changes to CA certification policies and/or practices, and/or to the CA software. The plan will be presented to the Actalis direction for approval, and then to any third parties with whom Actalis has commitments in this regard.

8.6 Communication of results

The provisions of §8.6 of the [SMBR] apply.

8.7 Self-audits

The provisions of §8.7 of the [SMBR] apply.

9 OTHER BUSINESS AND LEGAL MATTERS

For more details on legal matters related to certificates issued under this CP, the reader is referred to the Terms & Conditions [T&C] published on the CA web site.

9.1 Fees

9.1.1 Certificate issuance or renewal fees

The fees charged by Actalis for certificate issuance or renewal depend on several factors, such as the certificate type, the validity period, the total number of certificates purchased by the same client, whether the client is a private person or an organization, the certificate request channel, the involvement of a Reseller, etc. Quotes will be provided to interested parties on request.

9.1.2 Certificate access fees

Not applicable

9.1.3 Revocation or status information access fee

Access to certificate status services (CRL, OCSP) is free and open to everybody.

9.1.4 Fees for other services

No stipulation.

9.1.5 Refund policies

Please refer to the General Terms & Conditions published on the CA website.

9.2 Financial responsibility

9.2.1 Insurance coverage

Actalis is suitably insured against the risks related to its certification services.

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

Please refer to [CPS].

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

Please refer to [CPS].

9.3.2 Information not within the scope of confidential information

Please refer to [CPS].

9.3.3 Responsibility to protect confidential information

Please refer to [CPS].

9.4 Privacy of personal information

9.4.1 Privacy plan

The Actalis' privacy policy is published at the following address:
https://www.actalis.it/documenti-en/sslclient_smime_privacy_information.aspx

9.4.2 Information treated as private

The provisions of §9.4.2 of the [SMBR] apply.

9.4.3 Information not deemed private

No stipulation

9.4.4 Responsibility to protect private information

The provisions of §9.4.4 of the [SMBR] apply.

9.4.5 Notice and consent to use private information

The provisions of §9.4.5 of the [SMBR] apply.

9.4.6 Disclosure pursuant to judicial or administrative process

No stipulation.

9.4.7 Other information disclosure circumstances

No stipulation.

9.5 Intellectual property rights

Actalis S.p.A. and Aruba S.p.A. own the intellectual property rights in Actalis' services, including the certificates, trademarks used in providing the services, and this CP. Subscribers keep all the rights on their own trademarks, brand names, and their own domain names. Private Keys and Public Keys remain the property of the Subscribers who rightfully hold them.

9.6 Representations and warranties

9.6.1 CA representations and warranties

By issuing a Certificate, Actalis makes the following warranties to all beneficiaries:

- **Right to Use Mailbox Address**: at the time of issuance, the CA implemented and followed a procedure, as documented in this CP, for verifying that the Applicant either had the right to use, or had control of, the Mailbox Addresses included in the Certificate (or was delegated such right or control by someone who had such right to use or control);
- **Authorization for Certificate**: at the time of issuance, the CA implemented and followed procedure, as documented in this CP, for verifying that the Subject authorized the issuance of the Certificate and that the Applicant Representative is authorized to request the Certificate on behalf of the Subject;
- **Accuracy of Information**: at the time of issuance, the CA implemented and followed a procedure, as documented in this CP, for verifying the accuracy of all of the information contained in the Certificate;
- **Identity of Applicant**: at the time of issuance, the CA implemented and followed a procedure, as documented in this CP, to verify the identity of the Applicant in accordance with §3.2 and §7.1.4.2.2 of the [SMBR];
- **Subscriber Agreement**: the Subscriber has accepted a legally valid and enforceable Subscriber Agreement or Terms of Use that meets the [SMBR];
- **Status**: the CA maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (Valid or Revoked) of all unexpired Certificates;

- **Revocation**: the CA will revoke the Certificate for any of the reasons specified in the [SMBR] and §4.9.1 of this CP.

9.6.2 RA representations and warranties

Before allowing any entity to act as **Registration Authority** (RA), Actalis will stipulate with that entity a specific *agreement* including at least the following obligations for the RA:

- read and accept all the provisions of this CP and the related CPS;
- collect, verify, and archive suitable evidence corroborating the identity of Applicants, in compliance with the [SMBR], in particular the Applicants' Personal Names (given names and surnames);
- promptly request the revocation of certificates, issued at their request, which include inaccurate or no longer valid Subject identity data (e.g., personal names, email addresses, etc.).

9.6.3 Subscriber representations and warranties

Actalis shall require, as part of the Subscriber Agreement or Terms of Use, that the Applicant make the following commitments and warranties:

- **Accuracy of Information**: provide true and accurate information to the CA or RA;
- **Protection of Private Key**: adopt suitable measures to avoid compromise of their own private keys, including the adoption of suitable measures to avoid unwanted disclosure of secret codes (e.g., the passwords) obtained from the CA or the RA;
- **Acceptance of Certificate**: install and start using the certificate only after having checked that it contains correct information;
- **Use of Certificate**: use the certificate only in the ways and for the purposes provided for in this CP and in compliance with all applicable laws;
- **Reporting and Revocation**: promptly request revocation of the Certificate, and cease using it and its associated Private Key…
  - if there is any actual or suspected misuse or compromise of the Subscriber's Private Key,
  - or if any information in the Certificate is or becomes incorrect or inaccurate;
- **Termination of Use of Certificate**: promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise;
- **Responsiveness**: respond to the CA's instructions concerning Key Compromise or Certificate misuse within a specified time period.
- **Acknowledgment and Acceptance**: acknowledge and accept that the CA is entitled to revoke the Certificate immediately if the Applicant were to violate the terms of the Subscriber Agreement or Terms of Use, or if revocation is required by this CP and/or the related CPS, or by the [SMBR].

9.6.4 Relying party representations and warranties

Relying Parties are supposed to:

- make a reasonable effort to acquire a sufficient understanding of certificates and PKIs;
- verify the status of certificates by accessing the information services described in §4.10;
- only rely on certificates that are not expired, suspended or revoked.

9.6.5 Representation and warranties of other participants

No stipulation.

9.7 Disclaimers of warranties

The CA has no further obligations and shall not be obliged to guarantee anything more than what is expressly described in this CP or prescribed by applicable law.

9.8 Limitations of liability

Please refer to [CPS].

9.9 Indemnities

Please refer to [CPS].

9.10 Term and termination

9.10.1 Term

Please refer to [CPS].

9.10.2 Termination

Please refer to [CPS].

9.10.3 Effect of termination and survival

Please refer to [CPS].

9.11 Individual notices and communications with participants

Please refer to [CPS].

9.12 Amendments

9.12.1 Procedure for amendment

Please refer to [CPS].

9.12.2 Notification mechanism and period

Please refer to [CPS].

9.12.3 Circumstances under which OID must be changed

Please refer to [CPS].

9.13 Dispute resolution provisions

Please refer to [CPS].

9.14 Governing law

Please refer to [CPS].

9.15 Compliance with applicable law

Please refer to [CPS].

9.16 Miscellaneous provisions

9.16.1 Entire agreement

Please refer to [CPS].

END OF DOCUMENT