Free S/MIME Certificates

Certificate Policy

Version 2.2

Last revised: March 07, 2025

Andrea Sassetti
Firmato digitalmente il 07/03/2025 12:28:39 CET

Via S. Clemente 23 | 24036 Ponte S. Pietro (BG)
Tel +39-0575.050.350 | Fax +39-02-0575.862.350
www.actalis.it | info@actalis.it

CHANGE HISTORY

Version	Date	Author	Remarks
1.0	22/04/2015	AS	First version.
1.1	29/04/2016	AS	Changed company address.
1.2	07/10/2019	AS	Corrected typos. Updated references. Revised terminology.
2.0	12/09/2023	AS	Correction of typos. Updated sections 1, 3, 7 for compliance with CABF Baseline Requirements for S/MIME Certificates.
2.1	01/09/2024	AS	Correction of typos. Restructured chapters 4 and 7 in line with RFC3647. §1.6 Updated acronyms for CAA records. §1.7 Updated references for CAA records. §4.2 Added clarifications on CAA records processing. §7.2 Added details on revocation *reasonCodes*.
2.2	07/03/2025	NP, AS	Restructured this 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; $9.1 Integration about applied fees.

CONTENTS

1 INTRODUCTION

Actalis S.p.A. (www.actalis.it) is a leading Italian Certification Service Provider (CSP) since 2002, offering all types of certificates and related management services, digital time stamping, certified electronic mail, smart cards, 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 to a set of information that identifies an entity (be it an individual or an organization). This entity, the owner of the certificate, possesses and uses the corresponding private key. The certificate is generated and supplied to the owner by a trusted third party known as *Certification Authority* (CA), and is digitally signed by the CA. The reliability of a certificate also depends on the CA's operating procedures, on the obligations and responsibilities between the CA and Subscriber, and the CA's physical and technical security controls. All those 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). Certificate owners are also called *Subscribers* as they undersign a contract with the CA (of which the CP/CPS is an integral constituent) for certificate issuance and management. Since the CA provides a service to its subscribers, it is also called a *Certification Service Provider* (CSP).

This document is the Actalis' CP relevant to the issuance and management of "Free S/MIME" certificates which are Publicly Trusted **Mailbox-Validated** S/MIME certificates according to the [BR].

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

1.2 Document name and identification

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

1.3 PKI Partecipants

1.3.1 Certification Authorities

The **Certification Authority** (CA) is **Actalis S.p.A.**, with principal address at Via dell'Aprica 18, 20158 Milano, Italy, registered in the Registry of Enterprises of Milano under #03358520967.

Subscribers may be any individuals needing S/MIME certificates for the purposes indicated in §1.4.

1.3.2 Registration Authorities

Registration Authorities (RAs) are entities performing I&A of Subscribers and their registration into the CA database for subsequent certificate issuance. For this particular policy, RA tasks are performed by the CA itself (external RAs are not allowed).

Relying Parties (RP) 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 (his/her email address, in this particular case) contained in the same certificate.

1.3.3 Subscribers

Subscribers, as identified in the Subject field of certificates, may be either **organizations** or **individuals associated with an organization** (e.g., employees). Certificates issued according to this CP are not provided to private individuals.

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 Partecipants

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 with the CA.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

Certificates issued under this CP are mainly intended for **secure e-mail** according to the **S/MIME** standard [SMIME]. In some context, they may also be used for SSL/TLS client authentication [TLS], depending on the target systems' requirements.

Note: It is assumed that Subscribers already have the competence and instruments required to 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

BR	Baseline Requirements
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
LDAP	Lightweight Directory Access Protocol
MV	Mailbox-Validated
OID	Object Identifier
PKI	Public Key Infrastructure
RA	Registration Authority
S/MIME	Secure MIME
SSL	Secure Sockets Layer
TLS	Transport Layer Security

1.7 List of references

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

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

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

[IMF] RFC 5322: "Internet Message Format", October 2008.

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

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

[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.

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

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

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

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

[CPS] Certification Practice Statement - SSL Server and Code Signing certificates (https://www.actalis.it/documenti-en/cps_for_ssl_server_and_code_signing_en.aspx)

[T&C] SSL Client and S/MIME Certificates – Terms & Conditions (https://www.actalis.it/area-download.aspx)

2 PUBLICATION AND REPOSITORY RESPONSABILITY

2.1 Repositories

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.

Actalis also publishes revocation information as described in §4.10.

2.2 Publication of certification information

As specified in §1.1, this CP is structured in accordance with RFC 3647 and Actalis will adhere to the latest published version of the [SMBR].

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

3.1.1 Types of names

Certificates issued according to this policy do not contain the Subscriber's personal identity, like e.g., forename and surname, but only his/her email address. The CA does not attempt to determine the Applicant's identity and does not warranty that the Subscriber is a specific person. The only warranty provided is that the CA, before issuing the certificate, has made a reasonable effort to verify that the Applicant controls the email account associated with the email address included in the certificate.

The **commonName** component (CN) of the certificate's Subject field contains the Subscriber's email address. No other attributes are included in the Subject field.

The **SubjectAlternativeName** (SAN) extension of the certificate contains the Subscriber's e-mail address, with the same value as in the **commonName** component of the Subject field.

3.1.2 Need for names to be meaningful

As descripted in §3.1.1 of this CP.

3.1.3 Anonymity or pseudonymity of subscribers

Pseudonyms are not supported.

3.1.4 Rules for interpreting various name forms

As descripted in §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 only element of the Applicant's identity that is collected and verified by the CA is the Applicant's email address. This is checked by sending a **random code** to the email address specified by the requestor into the on-line certificate request form, then asking the requestor to enter such code before the certificate request is accepted. The requestor's ability to enter the correct code is considered proof that the specified email address exists and the Applicant has access to it.

No other identity information (e.g., forename, surname, affiliation, etc.) are collected or verified by the CA, as they are not inserted into the certificate.

3.2.1 Method to prove possession of private key

The private cryptographic key corresponding to the public key within the certificate is generated by the CA (with a suitable algorithm, size, etc.) and subsequently sent to the subscriber in PKCS#12 format [PFX], via email, thereby ensuring that the subscriber does possess the private key.

The CA does not retain the Subscriber's private key after having sent it to the Subscriber.

The password needed to import the PKCS#12 file is provided to the Subscriber out-of-band (via web, over a secure TLS channel), therefore protecting it from unwanted disclosure to third parties. The CA does not retain such password; therefore, the legitimate Subscriber – assuming that he/she keeps such password confidential – remains the only person able to decrypt the PKCS#12.

3.2.2 Authentication of organization identity

Certificates issued according to this CP do not contain any organization identity.

3.2.3 Authentication of individual identity

Certificates issued according to this CP do not contain the Subscriber's personal identity, like e.g., forename and surname, but only his/her email address.

3.2.4 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].

3.2.5 Validation of authority

No stipulation.

3.2.6 Criteria for interoperation

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

3.3 Identification and Authentication for re-key requests

3.3.1 Identification and authentication for re-key request

Certificate "renewal" in the strict sense is not provided for. If the Subscriber would like to obtain a new certificate before the current certificate expires, he/she will have to proceed in the same way as for the first certificate issuance. The processing and checks made by the CA are always the same.

3.3.2 Identification and authentication for re-key after revocation

No stipulation.

3.4 Identification and authentication for Revocation Requests

I&A for certificate revocation requests depends on the way the request is made:

- in order to request certificate revocation through the CA web site, it is necessary for the Subscriber to login to the CA portal by means of the suitable credentials supplied to him/her upon issuance of the certificate;
- otherwise, the Subscriber can contact the CA Customer Care (contact details available on the CA web site) and request the revocation of the certificate; in that case, the Subscriber must prove its identity by providing the information that Customer Care agent will be asking of him/her.

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

To apply for a certificate pursuant to this CP, after accepting the quote, the Applicant shall fill in and submit a **web-based request form** to be found on the CA web site.

Before the Applicant can actually submit the certificate request form to the CA, he/she must read and accept this Certificate Policy and the Terms & Conditions; both documents are made available for download in the same web form. Acceptance by the Applicant is expressed through the "point & click" method, as permitted by Italian and European legislation on distance contracts.

Furthermore, before the certificate request is accepted, the CA shall perform I&A according to §3.2.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

Upon receipt of a certificate application with 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 paragraph 4.2.2.1 of the [SMBR].

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 the previous steps (see §4.2) are completed successfully, the CA system generates a suitable Key Pair for the Applicant;

Next, the CA system generates the Certificate, stores it into its database, and send this latter to the Subscriber via email.

The certificate is sent to the Subscriber requestor together with the corresponding private key, both bundled into a PKCS#12 file [PFX]. The password needed to decipher the PKCS#12 file is shown to the requestor in the browser, at the end of the certificate request procedure. It is up to the Subscriber to keep that password confidential and protect it from unwanted loss. See 3.2.2 for additional details.

4.3.2 Notification to subscriber by the CA of issuance of certificate

No stipulation.

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

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 Revocation

The certificate shall be revoked in the following cases:

- request errors
- non-compliance with this CP
- compromise of the private key (*)

- termination of use of the certificate (*)
- loss of validity of some certificate data (*)
- infringement of the applicable Terms & Conditions.

In the cases marked with asterisk (*), the Subscriber **must** promptly request revocation of his/her certificate as soon as the circumstance occurs.

Certificate suspension is not supported for certificates governed by this CP.

The CA will revoke the certificate within 5 days if it discovers that the certificates have any non-compliance with this CP. In case the CA becomes aware that the certificate has major defects impacting security (e.g., it was mistakenly issued with CA=true in its KeyUsage extension) or it is being used for criminal purposes (e.g., distribution of malware, phishing, etc.), the CA will revoke the certificate within 24 hours.

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

Certificate suspension is not supported for certificates governed by this CP.

Certificate revocation may occur on request of the Subscriber or by initiative of the CA itself, depending on circumstance.

The Subscriber may request revocation of his/her certificates by accessing the CA web site (using the credentials that were sent to him/her upon certificate issuance), and then following the on-screen instructions. The exact address of the web site is included in the same mail by which the certificate is sent to the user.

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 CRLDistributionPoints (CDP) certificate extension, instead the OCSP responder address is inserted in the AuthorityInformationAccess (AIA) extension.

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

4.10.1 Operational characteristics

The status of certificates (active, suspended, revoked) is made available to all Relaying Parties in two ways:

- through the publication of a Certificate Revocation List (CRL) conformant to the RFC 5820 standard [PROF];
- by providing an on-line certificate status service based on OCSP protocol, in compliance with the RFC 6960 standard [OCSP].

4.10.2 Service availability

The HTTP address of the CRL is inserted in the CRLDistributionPoints (CDP) certificate extension, while the OCSP responder address is inserted in the AuthorityInformationAccess (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.

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 applying to Actalis' **SSL Server and Code Signing Certificates** [CPS], except where otherwise specified hereafter.

5.1 Physical Security Controls

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

5.4.1 Types of events recorded

Same as documented in [CPS].

5.4.2 Frequency of processing 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 procedures

Same as documented in [CPS].

5.4.6 Audit log backup procedures

No stipulation.

5.4.7 Notification to event-causing subject

No stipulation.

5.4.8 Vulnerability Assessment

Same as documented in [CPS].

5.5 Records Archival

5.5.1 Types of records archived

The CA and each Delegated Third Party archive all audit data, certificate application information, 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

Same as documented in [CPS].

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 those applying to Actalis' **SSL Server and Code Signing Certificates** [CPS], except where otherwise specified hereafter.

6.1 Key pair generation and Installation

6.1.1 Key pair generation

Same as documented in [CPS].

6.1.2 Private key delivery to subscriber

Same as documented in [CPS].

6.1.3 Public key delivery to certificate issuer

Same as documented in [CPS].

6.1.4 CA public key delivery to relying parties

Same as documented in [CPS].

6.1.5 Key sizes

Same as documented in [CPS].

6.1.6 Public key parameters generation and quality checking

Same as documented in [CPS].

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

Same as documented in [CPS].

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

Same as documented in [CPS].

6.3.2 Certificate operational periods and key pair usage periods

Certificates issued under this CP and the corresponding private keys shall have a maximum operational period of 1 year (or 365 days).

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

Same as documented in [CPS].

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 extensions

7.1.2.1 Root CA certificate

The Root CA certificate is the same used for **SSL Server and Code Signing certificates**. Please refer to [CPS] for further details.

7.1.2.2 Subordinate CA certificate

The certificate of the subordinate CA, used to sign end-entity certificates, has 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	<10 years>	
Subject	CN = Actalis Client Authentication CA G***N*** 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, pathLenConstraint=0
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 address of this Policy>
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>

7.1.2.3 End-Entity certificates

The profile of end entity 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	notBefore = <Issuance time> notAfter = <12 months later>	
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 legacy (2.23.140.1.5.1.1)
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>

7.1.3 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 **SubjectAlternativeName** (SAN) extension always contains the Subscriber's **Mailbox Address** as verified by the CA. No other SAN forms are inserted into the certificate.

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 extentions

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]

- unspecified (0);
- keyCompromise (1);
- affiliationChanged (3);
- superseded (4);
- cessationOfOperation (5);
- privilegeWithdrawn (9).

7.3 OCSP profile

7.3.1 Version number(s)

The profile of OCSP responses complies with section 7.3.1 of the [BR].

OCSP clients are expected to conform to the [OCSP] specification. OCSP requests need not be signed or otherwise authenticated.

7.3.2 OCSP extensions

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

8 COMPLIANCE AUDIT AND OTHER ASSESSMENT

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

Certificates issued according to this policy are provided for free (that is, at no charge) only for the first year. However, *not more than 1 certificate per year is provided for each unique email address*.

After the first year, certificates are priced depending on volumes, duration (validity period), and any possible customer-specific requirements and other factors.

At any rate, *Actalis does not commit to issue the certificate* nor to make it available to the requestor within any particular time.

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 Privacy of Personal 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