Certificate Policy and Certification Practice Statement

S/MIME Certificates

Version: **1.0**

Date: **June 19, 2026**

Approved by: Andrea Sassetti

Document code: MODAC_A_67

Distribution: PUBLIC

Sassetti
Andrea
21.06.2026
16:55:05
UTC

Table of Contents

1 INTRODUCTION

1.1 Overview

Actalis S.p.A., a company of the Aruba S.p.A. group, is a leading provider of certification services since 2002, accredited by AgID under the European Directive on Electronic Signatures, then under the European Regulation EU n.910/2014 ("eIDAS"). Actalis offers several types of certificates and related management services, as well as other trust services and solutions (https://www.actalis.it).

The reliability of a certificate, in particular the association - attested by the certificate - between a given public key and a given identity, critically depends on the CA's operating procedures, the obligations and responsibilities of the CA and the certificate Subscriber, and the CA's physical, technical, and operational security controls. All these aspects are described in a public document called Certification Practice Statement (CPS) and/or a separate document called Certificate Policy (CP), according to [RFC 3647], or a combined document.

This document is the Actalis' combined CP/CPS relevant to the issuance and management of **S/MIME certificates**. This CPS is structured according to the outline set forth in section 6 of [RFC 3647], as may be amended by the CA/Browser Forum's S/MIME Baseline Requirements..

Actalis conforms to the latest published versions of: CAB Forum's Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates (https://www.cabforum.org), the CCADB Policy (https://www.ccadb.org/policy), the Mozilla Root Store Policy, the Apple Root Program, and the Microsoft Root Program. In the event of any inconsistency between this CPS and those documents, those documents take precedence.

1.2 Document Name and Identification

This document is the **Certificate Policy and Certification Practice Statement** (hereinafter referred to only as CPS) applying to **S/MIME certificates** issued by **Actalis S.p.A.** Version and time of last revision are indicated on the first page.

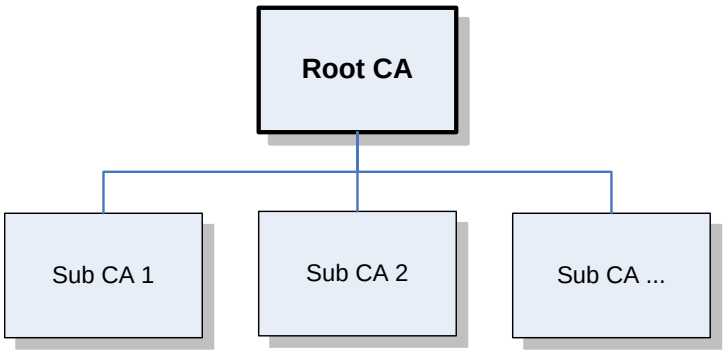
This CPS is published as a signed PDF document in order to ensure its origin and integrity.
Actalis also publishes this CPS in Markdown, to facilitate transparency, reviewability, version comparison, and change tracking. Where this CPS is published in multiple formats, Actalis ensures that the official text is consistent across formats and clearly identifies the authoritative version in the event of discrepancy. The authoritative version is the document in pdf format.

1.3 PKI participants

1.3.1 Certification Authorities

The Certification Authority (CA) is the trusted third party who issues the certificates and signs them with its own private key (CA key). Furthermore, the CA manages the status of the certificates.

The Actalis PKI (Public Key Infrastructure), on which the S/MIME certificate issuance and management service is based, is a two-level hierarchy, as shown in the following diagram:



The **Root CA** is used for issuing Sub CA certificates and related CRLs only, and is kept off-line when not in use. The **Sub CAs** are the CAs that issue end-user certificates.

In particular, to date there are:

- A *legacy* hierarchy based on the single multi-purpose Root CA *"Actalis Authentication Root CA",* included in the main root certificate stores, currently in use. Under this single Root CA, various SubCAs operate that issue different types of certificates (TLS Server, Code Signing, S/MIME, etc.);
- New hierarchies based on *single-purpose* Root CAs detailed below, which are currently not included in the main root certificate stores. These hierarchies are intended to replace the legacy structure, forming the basis for the structured migration of certificates. The new hierarchies are specific to the type of certificate (TLS Server, Code Signing, S/MIME, etc.).

Some of the Root CAs on which the new hierarchies are based have been cross-certified by the *multi-purpose* Root CA, thus allowing the issuance of certificates also using the subordinate CAs under these new Root CAs.

Within the framework of the service described in this document, the role of Root CA is played by the Italian company Actalis S.p.A. (hereinafter referred to as "Actalis"), identified as follows:

Company name:	**Actalis S.p.A.**
Registered Office:	**Via San Clemente 53 – 24036 Ponte S. Pietro (BG) – ITALY**
Legal representative:	**Massimiliano Carollo** (Chief Executive Officer)
VAT Reg. No. and Tax Code:	**03358520967**
Telephone (switchboard):	**+39 0575 050.350**
DUNS number:	**440-489-735**
ISO Object Identifier (OID):	**1.3.159**
Company web site:	https://www.actalis.it
Company e-mail address:	info@actalis.it

1.3.1.1 Root Certification Authorities

At the date of revision of this CPS, 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 CPS, 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 CPS, 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 = IT	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
CN = Actalis SMIME ECC CA 2025 O = Actalis S.p.A. L = Ponte San Pietro	49 2f 9b 45 15 a1 5c e6 79 9f c6 39 ff 6e f7 18 47 ec 5d 29	07 July 2025	05 July 2035

S = Bergamo C = IT			

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 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 CPS according to the [SMBR] terminology:

- **Mailbox-Validated (MV)** – 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 CPS 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.

1.5 Policy administration

1.5.1 Organization administering the document

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

1.5.2 Contact person

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

1.5.2.1 Problem reporting

Actalis makes available to all interested parties (Subscribers, Relying Parties, Application Software Suppliers, law enforcement, etc.) two communication channels through which certificate problems can be reported to the CA at any time (24x7):

- the mailbox **cert-problem@actalis.it**, which the CA commits to timely read during working hours only (9 AM to 5 PM on Italian working days);
- the telephone number **+39-0575-050.376**, at which Actalis commits to answer at all times (24x7x365).

These channels cannot be used to request technical assistance of any kind, but only to report problems (such as misissuance, use of the certificate for unlawful purposes, etc.) that may warrant the revocation of the involved certificates.

Regardless of the communication channel used, the problem reporter must provide at least the following information, or the communication will be ignored:

- his/her full name;
- description of the alleged problem;
- enough information to unambiguously identify the certificate in question, such as the certificate fingerprint, or the certificate issuer and serial number.

Such communications may be made in Italian or English; other languages are not handled.

The CA is committed to take charge of *proper communications* within 24 hours, start investigating the reported problem, and take the necessary measures, depending on the problem severity[1]. The priority assigned to the problem will depend on:

- the nature of the alleged problem;
- the identity of the reporter (reports received by a Court or law enforcement agents will be handled with higher priority than other messages);
- the law and/or regulations relevant for the alleged problem (e.g., reports of illegal acts will be handled with higher priority than other messages).

If the reported problem does exist, the CA will decide on a case-by-case basis the measures to be taken (e.g., revocation of the certificate) and will notify the reporter by e-mail.

Note: those who send unwanted messages (spam) will be prosecuted according to applicable laws.

1.5.3 Person determining CPS suitability for the policy

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

1.5.4 CPS approval procedures

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

[1] Those who send unwanted messages (spam) will be prosecuted according to applicable laws.

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/Multipurpose Internet Mail Extensions
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.

[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.

[X509] 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.

[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 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 CPS 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.

3.1.2 Need for names to be meaningful

Personal Names SHALL be a meaningful representation of the Subject's name as verified in the identifying documentation or Enterprise RA records.

3.1.3 Anonymity or pseudonymity of subscribers

Pseudonyms are not supported.

3.1.4 Rules for interpreting various name forms

The name forms used in Certificate Subject DNs and Issuer DNs conform to a subset of those defined and documented in RFC 2253 and ITU-T X.520.

As regards non-ASCII character substitution and geographic names, Actalis respects the provisions of section 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 CPS, 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.

Actalis also verifies that the status of the Organization is not designated by labels such as "ceased," "inactive," "invalid," "not current," or the equivalent.

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].

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].

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 CPS, 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.

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 CPS, 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 CPS, 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

Either the Applicant (i.e., the future Subscriber) or a natural person authorized to request certificates on behalf of the Applicant (i.e., an Applicant Representative) may submit certificate requests, in compliance with the requirements described in par. 3.2.5.

Resellers may submit certificate requests on behalf of Applicants, pursuant to Actalis' reseller contract.

Actalis maintains an internal database of all previously revoked certificates and previously rejected certificate requests due to suspected phishing or other fraudulent usage or concerns. Actalis uses this information to identify subsequent suspicious certificate requests.

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 and 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

Actalis examines the Certification Authority Authorization (CAA) DNS Resource Records as specified in RFC 9495. If such records are found and do not allow Actalis to issue S/MIME certificates, the certificate application SHALL be rejected.

In particular, Actalis looks for the "issuemail" property tag as specified in RFC 9495. Where the Relevant RRSet contains any "issuemail" Property Tags, Actalis recognizes the issuer-domain-name "**actalis.it**", in the related Property Values, as granting authorization for S/MIME certificates issuance by Actalis.

Actalis also implements MPIC as per §4.2.2.2 of the CABF S/MIME Baseline Requirements, and performs DNSSEC validation on all DNS queries associated with CAA record lookups performed by the Primary Network Perspective in compliance with 4.2 of the [SMBR].

Actalis logs the results of the CAA checks.

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 section 4.2) are completed successfully, the CA system:

- checks that the CSR (*) is well-formed and does not contain unexpected data;
- checks that the CSR (*) is cryptographically valid according to section 3.2.1;
- checks that the algorithm and size of the key from CSR (*) meet the applicable constraints;
- checks that the key found in the CSR (*) is not a known “weak key” (see §6.1.1.3);
- performs a linting of the tbsCertificate, using linters broadly adopted by the industry, in order to minimize the risk of incorrect issuance.

(*) If a CSR was sent by Applicant; otherwise, the CA 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

Actalis notifies Subscriber of the issuance of a Certificate either via email and/or through delivery, depending on the certificate request channel, whether an Enterprise RA or a Reseller is involved, and specific configurations or preferences.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

Actalis considers the certificate accepted after 30 days from the date of notification and/or delivery (see 4.3.2), unless otherwise communicated by the Subscriber.

Public use of the certificate (i.e., using it for exchanging S/MIME email), even if temporary, shall in any case imply acceptance of the certificate by the Subscriber.
In the event that the certificate is issued with incorrect information in it due to incorrect completion of the application form by the requestor, the certificate must nonetheless be paid for.

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 this 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 CPS 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, a Reseller, 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

Actalis does not support the suspension of S/MIME Subscriber Certificates.

Where circumstances require that an S/MIME Subscriber Certificate no longer be trusted, Actalis SHALL revoke the Certificate in accordance with Section 4.9.1 of this CPS.

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

For the management of its CA infrastructure, Actalis makes use of the data center services provided by its holding company, Aruba S.p.A., who takes responsibility for the housing, Internet connectivity, physical and network security of all Actalis' systems. The data center service provided is ISO/IEC 27001 certified.

5.1 Physical controls

5.1.1 Site location and construction

All computer systems used for the provision of Actalis' CA services are housed in highly secure data centers owned and managed by the Actalis' holding company, Aruba S.p.A. In particular, Actalis maintains at least two full PKI infrastructures at separate locations, for redundancy, plus a third one at a distant location (> 300 km), for disaster recovery purposes. All these data centers are located on the Italian territory.

5.1.2 Physical access

At all the CA facilities, the following controls are in place:

- physical **access control system**, so that access to the facility is possible only to those who need, upon registration at the reception, and that access to the technical rooms is allowed only to authorized employees;
- **passive anti-intrusion systems** such as grids, bulletproof glass, armored doors, motorized gates;
- **active anti-intrusion systems** such as CCTV and VMD.

5.1.3 Power and air conditioning

All data centers hosting Actalis' CA services are equipped with:

- fully redundant power supply systems, to guarantee the continuity of electric power supply in every predictable condition;
- ventilation and air conditioning systems (HVAC) to ensure optimal climatic conditions for the regular operation of servers hosted in the data center.

5.1.4 Water exposures

All data centers hosting Actalis' CA services are equipped with flood detection and protection systems.

5.1.5 Fire prevention and protection

All the data centers hosting Actalis' CA services are equipped with fire detection and suppression systems compliant with the applicable laws and standards; fire detectors are also present on all floors of the building. For the details of specific data centers, see par. 5.1.1.

5.1.6 Media storage

On the topic of media storage, the procedures set by Actalis' ISMS apply.

5.1.7 Waste disposal

On the subject of waste disposal, the CA applies the provisions of current regulations.

5.1.8 Off-site backup

Backups are stored at a different site than that of data origin, thus ensuring the possibility of restoration in any foreseeable condition.

5.2 Procedural controls

Actalis maintains a Security Plan, including a Risk Assessment, which analyses the CA assets, the threats they are exposed to, and describes the various technical, physical and procedural controls deployed so to adequately mitigate the risks. The risk assessment is reviewed at least yearly.
Furthermore, Actalis has defined an inventory of assets (hardware and software) as required by the policy and the company procedure.

5.2.1 Trusted roles

Actalis has defined and formally assigned the following trusted roles within the CA service regulated by this CPS:

- Security Officer: responsible for implementation and management of security procedures;
- System Administrator: responsible for installation, configuration and maintenance of CA systems;
- System Operator: responsible for the day-to-day operation of CA systems;
- System Auditor: responsible for checking the reviewing record archives and audit logs;
- Internal Auditor: responsible for performing self-audits (see section 8.7) and other assessments;
- Validation Specialist: responsible for performing the information verification duties specified by this CPS (in particular, those described in section 3);
- Registration & Revocation Officer: responsible for verifying the information needed to issue certificates and approving certificate requests; also responsible for certificate status changes (e.g. revocations).

Some persons may hold multiple roles provided that this does not prejudice the security and trustworthiness of the PKI and is not prohibited by applicable regulations and standards.

Trusted roles are appointed by senior management. A list of personnel appointed to trusted roles is maintained and reviewed annually, and made available to auditors.

5.2.2 Number of persons required per task

Management of the CA private keys (key generation, backup, restore, deletion, etc.) requires at least two persons in trusted roles ("dual control") and must take place in a physically protected environment.

5.2.3 Identification and authentication for each role

All the trusted roles listed in par. 5.2.1 and, in general, all the Actalis staff use appropriate identification and authentication systems for accessing Actalis' computer systems.

In particular, with regard to the physical access to data rooms and cabinets that contain the CA systems, identification and authentication takes place by means of restricted access.

As regards the logical access to the CA systems, identification is based on the account name and relative password or through a two-factor authentication system where necessary. In particular, access to any account that allows direct issuance of certificates requires strong authentication (multi-factor).

5.2.4 Roles requiring separation of duties

Persons holding any of the trusted roles listed in par. 5.2.1 cannot have other roles within the CA services, except for Validation Specialists and Registration & Revocation Officers. See also section 5.2.2

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

Actalis ensures that the personnel assigned to its CA services are adequately competent for the tasks assigned to them, based on appropriate education, training, skills, and experience, and that they are free from conflicts of interest that may compromise the necessary impartiality and respect of the procedures. In particular, with reference to the trusted roles, the required characteristics and skills are described in the "job description" company document.

In the case of new recruitments, Actalis always reserves the right to assess what type of training is necessary in relation to the tasks to be assigned, the existing qualifications and experience, and provides where necessary for the inclusion of the resource in a training plan.

5.3.2 Background check procedures

For the definition of the shortlist of candidates, both for technical and administrative areas, Actalis uses both the curricula sent directly to it through the appropriate channels (e.g. website) and those provided by external recruiters. For each candidate, the accuracy of the information contained in the CV (e.g. education, masters, specific training courses, etc.) is verified. External recruiters contracted by Actalis also have the obligation to request references, for each potential candidate, before submitting their CVs to Actalis. Furthermore, all candidates, once the selection phase is completed, must provide their certificate of good conduct (extract from the judicial record) or an equivalent declaration to the Human Resources office.

5.3.3 Training requirements

The staff in charge of the CA services is adequately trained for the tasks that they perform. Actalis provides staff with initial training at the time of recruitment, including courses held by external teachers when deemed necessary, and training on the job.

The staff involved in the verification of information (Validation Specialists) are trained on at least the following topics: Public Key Infrastructures (PKI), identification and authentication policies and procedures, common threats to information verification procedures, and CAB Forum Requirements. The records of this training, which is provided at least yearly, are kept and made available to the auditors on request.

5.3.4 Retraining frequency and requirements

For all personnel working in the CA service, the need for new training is assessed at least once per year (or in advance, in case new developments/services), so as to ensure that all personnel are always able to perform their tasks satisfactorily and competently. Furthermore, training on information security matters is held annually for all staff.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

In the case of unauthorized actions and/or violations of company (or Group) policy and/or procedures, Actalis reserves the right to activate the disciplinary procedure provided for in the employment contract, after having assessed the nature and the severity of the violation and its impact on company operations, whether it was the first occurrence, whether the employee had been adequately trained, etc.

5.3.7 Independent contractor requirements

Any independent contractor or Delegated Third Party's personnel involved in the issuance of Certificates shall be fully subject to this CPS, including training and skills requirements (see section 5.3.3), sanctions (see section 5.3.6), document retention and event logging requirements (see section 5.4.1).

Non-employees (e.g. consultants) are required to sign a confidentiality agreement (NDA) before starting collaboration with Actalis and possibly accessing confidential data.

5.3.8 Documentation supplied to personnel

Personnel in trusted roles are provided with the documentation necessary to perform their duties, depending on their role (see section 5.2.1). In particular, Validation Specialists are provided with this CPS, CAB Forum's Baseline Requirements, and detailed instructions on how to properly perform the identification and authentication activities and issue certificates, plus the manuals of the CA/RA applications they use.

5.4 Audit logging procedures

5.4.1 Types of events recorded

The CA and any Delegated Third Parties shall record all the details related to certificate requests, issuances, and subsequent management (e.g. revocation), and make these records available to the CA auditors. For each event, information shall be recorded about event type, date and time of occurrence, the associated data (depending on event type), the personnel involved (if applicable), and possibly other information depending on event type.

At least the following events shall be logged, in line with section 5.4.1 of the [SMBR]:

- CA key lifecycle management events;
- CA and Subscriber certificate life cycle management events;
- Security events (e.g. accesses to PKI systems, PKI and security system actions performed, security profile changes, entries to and exits from the CA facility, relevant activities on routers and firewalls, in particular with regard to its configurations etc.).

5.4.2 Frequency of processing log

The relevant events are collected by the systems that generate them and are transmitted to the centralized log management system. On the log management system, events are automatically classified and stored locally in order to allow them to be consulted. On a daily basis, local data are copied to the long-term storage system (see Section 5.4.4).

5.4.3 Retention period for audit log

The CA shall retain audit logs for at least 10 years.

5.4.4 Protection of audit log

Audit logs are periodically stored on a remote long-term archival system based on WORM-type (Write-Once, Read Many) or equivalent technology. The “live” copy of the audit log is protected from tampering by multiple security measures.

5.4.5 Audit log backup procedures

The storage where the audit log is archived (see section 5.4.4) is replicated on two data centers hosted in separate facilities.

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

Audit logs are periodically examined for anomalies by personnel in trusted roles. Anomalies indicating possible security breaches are reported and investigated. Security incidents are handled according to section 5.7.1.

Vulnerability assessments of the CA networks and systems are done at least annually by qualified third parties. See also section 6.7.

A comprehensive a risk assessment is conducted at least annually (see also section 5.2).

5.5 Records archival

5.5.1 Types of records archived

The CA keeps at least the following information related to the request, issuance and revocation of certificates:

- certificate requests, including CSRs;
- details of applicants and applicant representatives;
- any further documentation supplied by applicants;
- verifications performed by the CA and the results thereof;
- certificate revocation requests.

5.5.2 Retention period for archive

Archived records are kept for at least 10 years past the certificates' expiration or revocation dates.

5.5.3 Protection of archive

Archives are protected from unauthorized modification or destruction by strong security controls. To this end, a document preservation service is used complying with the Italian regulations (Legislative Decree No. 82/2005: "Codice dell'Amministrazione Digitale" and subsequent amendments and additions) and accredited by AgID.

5.5.4 Archive backup procedures

Archives are backed up by the preservation system referred to in paragraph 5.5.3.

5.5.5 Requirements for time-stamping of records

All archived records are time-stamped at the date and time of creation or occurrence, with a date and time reference obtained from a trusted time source (see section 6.8).

5.5.6 Archive collection system (internal or external)

No stipulation.

5.5.7 Procedures to obtain and verify archive information

The retention system referred to in paragraph 5.5.3 allows searching for archived information on the basis of the associated metadata, as well as its recovery and the verification of its integrity.

5.6 Key changeover

5.6.1 Root CA

No stipulation.

5.6.2 Subordinate CA

At least 2 years before the end of the validity of the current certification key (Subordinate CA key), a new key pair will be generated and the corresponding certificate will be made available to Subscribers and Relying Parties as described in section 6.1.4. From that moment on, Subscriber certificates and related CRLs will be signed with the new Sub CA key.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

The Actalis' Information Security Management System (ISMS), compliant with ISO/IEC 27001, also includes incident and compromise handling procedures. The management of an information security incident is handled by following a multi-stage procedure coordinated by an internal committee (Committee for Security and Crisis Management, later on "Committee") composed of figures of various responsibilities and members of the senior management. The process is articulated into several phases described below:

- Detection: phase in which any person (employee, collaborator or any interested party) who detects a possible incident communicates it to the Committee. The Committee ensures that the report is as detailed as possible and that those who have encountered the problem do not take any action autonomously.
- Identification and analysis: the Committee takes charge of the report and assesses whether it is actually a security incident. If so, it evaluates its severity and proceeds with the following phases. Otherwise, it just closes the incident.
- Containment: in this phase, the harmful effects caused by the incident are contained as much as possible, in order to prevent them from spreading to other areas of the organization.
- Collection of evidence: phase in which the evidence is sought for and collected in order to attach it to the documentation of the incident in case of possible legal consequences or for the need to proceed with more in-depth investigations. All the evidences are collected following guidelines which aim to guarantee a correct and reliable collection.
- Removal and Recovery: phase in which the cause of the damage is removed and the systems affected are reactivated, through the recovery procedures, allowing the systems and users to return to work.
- Incident closure and Notification: once the recovery phase is over, the incident is closed. In this phase, the incident closure is notified to the involved managers.

Actalis shall publicly disclose and/or respond to incident reports in Bugzilla (https://bugzilla.mozilla.org/), regardless of perceived impact. Reports shall be submitted in accordance with the current version of the CCADB incident report format and timelines.

Disaster management is regulated by the Actalis' Business Continuity Plan (BCP) which covers all items listed in paragraph 5.7.1 of the [SMBR]. See also section 5.1.

Actalis also undertakes to maintain a complete and actionable plan for mass-revocation events, carrying out annual tests of the plan and incorporating the lessons learned in order to continually improve its preparedness for mass revocation over time.

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

Actalis implements a Business Continuity Plan for the CA service in order to ensure that the corruption or loss of one or more computers cannot cause any disruption to the CA platform. In particular, all the critical components of the system are redundant both locally, in the single data center, and between the primary and secondary data centers. Actalis also implements specific backup plans to guarantee that there is no loss of software and/or data.

5.7.3 Entity private key compromise procedures

The CA's private key is the single most critical resource of the CA; as such, it is protected by a set of multi-layered security measures, as other critical CA resources. In case of compromise (loss of confidentiality) of the CA key, after assessment of the incident, Actalis will execute the following plan (not necessarily in this order):

- notify the national supervisory body (AgID);
- notify the conformity assessment body (CAB);
- publish a well-visible information note on the CA website;
- notify the Application Software Suppliers with whom Actalis has a Root Certificate distribution
  agreement in place;
- notify any Delegated Third Parties (DTPs) and other interested parties to the extent possible;
- revoke of all certificates that were issued with the compromised key.

Finally, unless the CA is to be terminated, a new CA key pair will be generated and the new CA public key will be disseminated as described in section 6.1.4.

5.7.4 Business continuity capabilities after a disaster

Actalis are deployed in two geographically distant facilities (see section 5.1), each of which is capable of operating the CA systems independently. In the event that a disaster entirely disables one facility, Actalis' CA operations will fail over to another facility. See also section 5.7.1.

5.8 CA or RA termination

The activities that will be carried out if Actalis decides, for any reason, to cease its certification service are described below.

Before the actual termination:

- at least 60 days before the scheduled termination date, an information note will be sent to all customers of the CA service (and other services that include the CA services), as well as to the supervisory body (AgID), the conformity assessment body (CAB), and other subjects with whom the CA has stipulated agreements in this regard;
- with a minimum notice of 60 days, an informative note will be published on the CA website, in order to make the information available also to Relying Parties;
- with a minimum notice of 60 days, the CA will send a notice to all possible sub-contractors and Delegated Third Parties (RAs), informing them that at the end of the deadline they will no longer be authorized to perform activities related to the certificate issuance service;
- the responsibility for the preservation of evidences (certificate requests, event log, etc.) will be transferred to another reliable subject that can guarantee preservation for an adequate time. The responsibility to publish on its website the public key of the ceased CA will also be transferred to such entity;
- the destruction of private certification keys as well as of the attached cryptographic material will be planned.

On the termination date:
the private certification keys as well as the annexed key restoration material (if any) will be destroyed (by logical deletion) and the transaction will be recorded.

6 TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

6.1.1.1 CA key pair generation

Generation of all CA key pairs (Root CAs and subordinate CAs) takes place in a physically secured environment, following a documented procedure that requires the joint intervention of two different people in Trusted Roles under the principles of "*dual control*" and "*split-knowledge*". All CA key pairs are generated inside HSMs (Hardware Security Modules) meeting the requirements of section 6.2.1. Execution of the procedure is witnessed by an internal auditor and by an independent qualified auditor; the activity is recorded in a report which is archived on the liability of the Director of Certification Services.

6.1.1.2 RA key pair generation

No stipulation.

6.1.1.3 Subscriber key pair generation

The CA or a Delegated Third-Party MAY generate the Private Key on behalf of the Subscriber.

Actalis shall reject a certificate request for a Public Key that does not meet the requirements set forth in sections 6.1.5 and 6.1.6 or that corresponds to an industry-demonstrated weak Private Key, such as a "Debian weak key" (https://wiki.debian.org/SSLkeys) or one affected by the ROCA

(https://github.com/crocs-muni/roca) or the Close Primes (https://fermatattack.secvuln.info/) vulnerabilities.

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 required to decrypt the PKCS#12 file is provided to the subscriber in such a way as to prevent unauthorized third parties from getting 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

For RSA key pairs, Actalis SHALL ensure that:

- the modulus size, when encoded, is at least 2048 bits; and
- the modulus size, in bits, is evenly divisible by 8.

For ECDSA key pairs, Actalis SHALL ensure that:

- the key represents a valid point on the NIST P-256, P-384, or P-521 elliptic curve.

Algorithms other than RSA and ECDSA are not currently supported.

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

6.2.1 Cryptographic module standards and controls

All CA private keys (both Root CAs and issuing CAs) shall be generated, stored and used only in HSMs (Hardware Security Modules) possessing a security evaluation according to FIPS PUB 140-2 Level 3 (or higher), FIPS PUB 140-3 Level 3 (or higher) and/or Common Criteria (namely ISO/IEC 15408) at EAL 4 or higher.

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

See section 5.2.2.

6.2.3 Private key escrow

Actalis does not escrow its CA private keys to any third parties nor does it provide such a service for Subscriber keys.

6.2.4 Private key backup

For guaranteeing continuity of service, Actalis keeps encrypted backup copies of its CA keys on removable media. The backup copy is kept in a safe place that is different from the location of the operational copy. Backup and restore procedures require the joint intervention of at least two people ("dual control") in trusted roles.

6.2.5 Private key archival

No stipulation beyond what is provided for in the [SMBR].

6.2.6 Private key transfer into or from a cryptographic module

When CA private keys are transferred between HSMs (e.g., for redundancy or backup purposes) they are encrypted prior to leaving HSMs and unwrapped only inside destination HSMs. CA private keys never exist in plain text form outside of HSMs. Actalis does not generate CA keys for external subordinate CAs.

6.2.7 Private key storage on cryptographic module

Private Keys corresponding to CA Keys MUST be stored in accordance with [SMBR] section 6.2.7.

6.2.8 Method of activating private key

CA private keys are only activated by authorized persons, using the mechanisms provided by the HSM manufacturer. Activation data and devices are protected from loss or disclosure to unauthorized people.

Subscribers are responsible for protecting their private keys. Subscribers are supposed to use a strong password or an equivalent authentication method to prevent unauthorized access or use of their private keys.

6.2.9 Method of deactivating private key

CA private keys are de-activated by authorized persons, using the mechanisms provided by the HSM manufacturer.

6.2.10 Method of destroying private key

CA private keys shall be destroyed when they are no longer needed. CA keys are only destroyed by authorized persons in trusted roles, using the mechanisms provided by the HSM manufacturer.

Subscribers shall securely destroy their private keys when they are no longer needed (e.g. when the corresponding certificates expire or are revoked) by suitable methods depending on the type of media where the private keys are stored (e.g. storage media or HSMs).

6.2.11 Cryptographic module rating

See section 6.2.1.

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

Subscriber certificates have a maximum validity period of 825 days.

6.4 Activation data

Activation data refers to data that are required to activate private keys within HSMs. Examples include, but are not limited to, PINs, passphrases, and fragments of private keys used in a split-knowledge scheme.

6.4.1 Activation Data Generation and Installation

Activation data are generated and used following information security best practices and, where applicable, the procedures provided by the HSM manufacturers.

6.4.2 Activation Data Protection

6.4.2.1 CA keys

Activation data are protected by physical (e.g. storage on removable media), logical (e.g. encryption), and procedural measures (e.g. assignment to persons in trusted roles), in compliance with the company's information security policy and the "dual control" requirement (see par. 6.1.1.1).

6.4.2.2 Subscriber keys

Activation data are protected by the Subscriber so to prevent their disclosure to any unauthorized parties. For further important details on this topic, see paragraph 9.6.3.

6.4.3 Other Aspects of Activation Data

Root CA keys are normally kept in a non-operational state, except when needed for issuing or revoking Subordinate CA certificates or generating CRLs.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

The computers used in the CA services run operating systems of proven quality and reliability, configured in such a way as to prevent unauthorized and/or improper use of resources (data, applications, communication channels, etc.).

Where possible and where such functionality is not provided by the operating system itself, anti-malware systems are installed in order to mitigate the risk of "infections" and security attacks. Furthermore, for the same reason, the recommended security patches are installed from time to time.

Computers are subject to a "hardening" procedure aimed at removing or disabling unneeded functionalities, in a specific way on each computer according to the role it plays in the infrastructure.

Privileged access to computers (i.e. as " Administrator") is limited to personnel who actually need it and who have been appointed "System Administrator" in compliance with current legislation.

6.5.2 Computer security rating

No stipulation.

6.6 Life cycle technical controls

6.6.1 System Development Controls

The development of software systems used to support the trust services provided by Actalis, including the CA service, be it carried out by Actalis itself or on behalf of Actalis by contractors, respects the company's Quality Management System (QMS), compliant with the UNI EN ISO 9001 standard: 2015.
For software provided by third parties for the execution of its CA activities, Actalis provides for continuous monitoring of software versioning and upgrades in order to guarantee the highest quality of the services offered.

6.6.2 Security Management Controls

Actalis has in place an Information Security Management System (ISMS), compliant with the ISO/IEC 27001 standard, covering all company areas, including those involved in the development and provision of the CA service. Among the other provisions of the ISMS, all equipment and software used for Actalis' trust services (including CA services) is deployed and updated following a documented change management process.

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 Network security controls

Access to the CA on-line hosts is protected by high quality firewalls that guarantee an adequate filtering of the incoming connections and implement intrusion detection functionalities. Before the firewalls, a series of routers that implement suitable ACLs (Access Control List) constitute further protection. All the communication ports of the certification servers that are not used are disabled. Only those ports

are active which support the protocols and functions required for the operation and functionality of the service.

In order to strengthen the filter against unwanted communications, the entire certification system is split-up into an external zone, internal zone and a De-Militarized Zone (DMZ). Sensitive systems are deployed on the internal zone and cannot be directly accessed from the external zone.

The Root CA systems are located on networks that are physically separated from all other CA infrastructures.

Actalis performs at least an annual security assessment to verify the possible presence of network vulnerabilities, making use of independent specialists.

Actalis also complies with the requirements of the "Network and Certificate System Security Requirements" published on https://cabforum.org/working-groups/netsec/ .

6.8 Time-Stamping

The time reference used by Actalis, with which the CA processing systems are kept synchronized, is obtained from a high precision device that guarantees a difference of no more than one second with respect to UTC time.

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

7.1.2.1.1 Legacy hierarchy

Below is the profile of the *multi-purpose* Root CA certificate:

Field	Value
Version	V3 (2)
SerialNumber	1
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	from September 22, 2011 to September 22, 2030
Subject	CN = Actalis Authentication Root CA O = Actalis S.p.A./03358520967 L = Milano C = IT
SubjectPublicKeyInfo	<RSA public key of 4096 bits>
SignatureValue	<Root CA signature>
Extension	**Value**
Basic Constraints	critical: CA=true
AuthorityKeyIdentifier (AKI)	<not included>
SubjectKeyIdentifier (SKI)	52:D8:88:3A:C8:9F:78:66:ED:89:F3:7B:38:70:94:C9:02:02:36:D0
KeyUsage	critical: keyCertSign, cRLSign
ExtendedKeyUsage (EKU)	<not included>
CertificatePolicies	<not included>
SubjectAlternativeName (SAN)	<not included>
AuthorityInformationAccess (AIA)	<not included>
CRLDistributionPoints (CDP)	<not included>

7.1.2.1.2 New hierarchies

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	<Subordinate CA signature algorithm>	
Issuer	<Subject of the Subordinate CA>	
Validity	<According to section 6.3.2>	
Subject	CN = <Email address of the Subscriber>	
SubjectPublicKeyInfo	<According to sections 6.1.5 and 6.1.6>	
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 (for RSA keys only)
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	<Subordinate CA signature algorithm>
Issuer	<Subject of the Subordinate CA>
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	<According to sections 5.1.5 and 6.1.6>
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 (for RSA keys only)
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	<Subordinate CA signature algorithm>
Issuer	<Subject of the Subordinate CA>
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	<According to sections 6.1.5 and 6.1.6>
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 (for RSA keys only)
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	<Subordinate CA signature algorithm>	
Issuer	<Subject of the Subordinate CA>	
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	<According to sections 6.1.5 and 6.1.6>	
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 (for RSA keys only)
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

Certificates are normally signed using one of the following algorithms:

Algorithm name	Object Identifier
sha256WithRSAEncryption	1.2.840.113549.1.1.11
sha512WithRSAEncryption	1.2.840.113549.1.1.13
ecdsa-with-SHA256	1.2.840.10045.4.3.2
ecdsa-with-SHA384	1.2.840.10045.4.3.3

CRLs and OSCP responses are signed using one of the following algorithms:

Algorithm name	Object Identifier
sha256WithRSAEncryption	1.2.840.113549.1.1.11
sha512WithRSAEncryption	1.2.840.113549.1.1.13
ecdsa-with-SHA256	1.2.840.10045.4.3.2
ecdsa-with-SHA384	1.2.840.10045.4.3.3

7.1.4 Name forms

The forms of the names are those specified in section 3.1.1.

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

Actalis includes the relevant CAB Forum reserved policy OID in Subscriber certificates, in the *CertificatePolicies* extension, in conformance to §7.1.6 of the [SMBR].

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

Actalis issues CRLs in compliance with [X509] and section 7.2 of the [SMBR].

7.2.1 Version number(s)

Actalis issues version 2 CRLs.

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).

As described in §4.9.13 Actalis does not support the suspension of S/MIME Subscriber Certificates.

7.3 OCSP profile

Actalis issues OCSP responses in compliance with [OCSP] and section 7.3 of the [SMBR].

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 CPS, 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 services regulated by this CPS shall be based on the latest version of ETSI TS 119 411-6, which includes normative references to ETSI EN 319 401, ETSI EN 319 411-1 and ETSI EN 319 411-2.

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 result of the audit carried out by the CAB is communicated to the company management and to the heads of the organizational structure in charge of providing the CA service. The result of the audit (i.e. the Audit Report or Audit Statement) is also communicated to the national Supervisory Body (AgID).
Actalis shall make the Audit Report publicly available as an authoritative, text-searchable English-language PDF document within 3 months of the end of the audit period.

The Audit Report MUST contain at least the information required by the CCADB Policy.

The result of internal audits or second-party audits is communicated to the company management, to the heads of the organizational structure responsible for providing the CA service and, where applicable, to the involved external entity/organization.

8.7 Self-audits

Actalis monitors adherence to this CPS and to CABF Requirements [SMBR], and controls the quality of its services, by performing self-audits at least quarterly on a randomly selected sample that includes a

minimum of the greater of thirty (30) Certificates or three percent (3%) of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken.

Actalis also uses a linting process to verify the technical accuracy of Certificates within the selected sample set, independently of previous linting performed on the same Certificates.

9 OTHER BUSINESS AND LEGAL MATTERS

The general Terms and Conditions of the CA service herein described are provided to customers as a separate document, to be accepted at application time, published on the CA web site (see par. 2.2).

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 and Conditions published on the CA website.

9.2 Financial responsibility

9.2.1 Insurance coverage

Actalis maintains a special insurance with a major insurance company to cover the risks related to the provision of its certification services and other trust services. In particular, the insurance provides for a single limit per claim and per insurance period of EUR 15,000,000 (fifteen million Euros). The insurance company has at least an "A" rating in the Best's Insurance Guide.

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

Please refer to par. 9.2.1.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

The following information is considered and treated as confidential:

- all information supplied to the CA by Applicants, except that intended to be included in Certificates;
- all communications between the CA and Applicants or Subscribers;
- any confidential codes provided to Subscribers by the CA or RA (such as the credentials necessary to login to the CA or RA websites);
- all information collected by the CA within the vetting process (identification and authentication);
- all contracts between the CA and other parties, including Subscribers, Application Software Suppliers, Delegated Third Parties (e.g. Resellers and Registration Authorities), subcontractors, etc.;
- all the private information of the CA (such as CA private keys, CA systems' accounts, passwords and other authentication credentials, business continuity and disaster recovery plans, internal procedures, internal infrastructure documentation, risk assessment reports, financial transaction records, etc.);
- the audit logs of the CA systems.

9.3.2 Information not within the scope of confidential information

including CAB Forum's Requirements and Guidelines), or on explicit request from the Subscriber, is considered non-confidential. In particular, the following information is considered non-confidential:

- all Certificates issued under this CPS;
- all Certificate Revocation Lists (see section 4.10);
- this CPS and other Actalis documents herein referred to;
- the status of Certificates provided via the OCSP service (see section 4.10);
- all information that the Applicant requested the CA to make public;
- all information obtainable from public information sources;
- any information that is already in the public domain.

9.3.3 Responsibility to protect confidential information

Actalis ensures that all confidential information is adequately protected from unauthorized access and from the risk of loss due to disasters (see section 5.7).

All confidential information is processed by the CA in compliance with applicable laws, in particular Legislative Decree no. 196/03 [DLGS196] and Regulation (EU) 2016/679 [GDPR].

9.4 Privacy of personal information

Actalis is the controller of the personal information collected during the identification and registration phase of parties requesting certificates under this CPS, and shall process such information ensuring their confidentiality and in compliance with the Italian Legislative Decree n.196/2003 [DLGS196].

9.4.1 Privacy plan

Regarding privacy, the CA complies with current laws, in particular Legislative Decree no. 196/03 [DLGS196] and Regulation (EU) 2016/679 [GDPR]. The protection of personal data is part of the Actalis' Information Security Management System (ISMS), compliant with ISO/IEC 27001.

9.4.2 Information treated as private

Please refer to the definition of personal data pursuant to current laws, in particular Legislative Decree no. 196/03 [DLGS196].

9.4.3 Information not deemed private

Non-personal data are those that do not fall within the definition in par. 9.4.2. Please also refer to par. 9.3.2.

9.4.4 Responsibility to protect private information

Actalis is the "data controller" for personal data pursuant to Legislative Decree no. 196/03 [DLGS196].

9.4.5 Notice and consent to use private information

The notice on the processing of personal data, pursuant to Legislative Decree no. 196/03 [DLGS196], is published on the CA website. The certificate request implies the Applicant's consent to the processing of personal data by the CA, in accordance with such notice.

9.4.6 Disclosure pursuant to judicial or administrative process

The Subscriber's personal data may be disclosed to the police, judicial authorities, information and security bodies or other public entities, pursuant to Legislative Decree no. 196/2003 [DLGS196], if that is required for the purposes of defense or security of the State or prevention, detection or repression of crimes.

9.4.7 Other information disclosure circumstances

Not applicable.

9.5 Intellectual property rights

This CPS is the property of Actalis who reserves all rights associated with the same.

The Subscriber keeps all the rights on its own commercial marks (brand names) and its own domain names.

Concerning the property rights of other data and information, the applicable law shall be applied.

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 CPS, 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 CPS, 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 CPS, 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 CPS, 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 CPS.

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 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 CPS 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 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 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of warranties

Except as expressly stated in this CPS or in a separate agreement with a Subscriber, Actalis does not make any further representations or warranties regarding its CA services. See also the Terms and Conditions published on the Actalis website.

9.8 Limitations of liability

The obligations and responsibilities of Actalis are exclusively those defined in this document and the service supply Contract. In case of violation or non-performance attributable to Actalis, in the event that the same has shown that said violation or non-fulfillment have occurred without malice or negligence, the same will not respond for an amount higher than the amount paid by the Customer for the Service, ordered or renewed, affected by the harmful event referred to the month in which said

event occurred, remaining in this case expressly excluded, now by then, any other indemnity or compensation to the Customer for direct or indirect damages of any nature and species.

Subject to the foregoing, without prejudice to the assumptions provided for by law, in no other case, for any reason and/or reason, can Actalis be held liable towards the Customer, or to other parties, directly or indirectly, connected or connected to the Customer for damages, direct or indirect, data loss, violation of third party rights, delays, malfunctions, interruptions, total or partial, which must be verified against the provision of the Service, where directly or indirectly connected, or arising from:

a) causes of force majeure, fortuitous events, catastrophic events (for example, but not limited to: fires, explosions, strikes, riots, etc.); and/or

b) tampering or interventions on the Service or on the equipment carried out by the Customer and/or by third parties not authorized by Actalis.

Actalis will not, in any case, be held liable for the use made of the Service in relation to critical situations involving, without limitation, specific risks for the safety of persons, environmental damage, specific risks in relation to mass transport services, the management of nuclear and chemical plants and medical devices; in such cases, Actalis is available to evaluate and negotiate with the Customer a specific "mission critical" agreement with the respective "SLA" (Service Level Agreements).

Actalis makes no warranty on the validity and effectiveness, even probative, of the Service or any data, information, message, document or document associated with it or otherwise entered, communicated, transmitted, stored or in any way processed by the Service itself:

a) when the Customer intends to use them or assert them in States or legal systems other than the Italian one, with the exception, with regard to European Union member States, for the Certificates issued on the basis of this document;

b) for their secrecy and/or integrity (in the sense that any violations of the latter are, of course, detectable by the User or the recipient through the appropriate verification procedure).

Actalis does not assume, in any case, any responsibility for the information, data, contents entered or transmitted and, in any case, processed by the Customer through the Service and in general for the use made by the same Service and reserves the right to adopt any initiative and action, to protect their rights and interests, including the communication, to the subjects involved, of the data useful for identifying the Customer.

9.9 Indemnities

9.9.1 Indemnification by CAs

The CA shall abide by section 9.9 of the [SMBR] towards Application Software Suppliers who have a Root Certificate distribution agreement in place with Actalis.

9.9.2 Indemnification by Subscribers

Subscribers shall pay compensation of any damages suffered by Actalis in the following cases:

- false declarations in the certification request;
- failure to provide information to the CA about essential matters and facts due to negligence or with the objective of deceiving the CA;
- use of names (for example, domain names, brand names) in violation of intellectual property rights;
- use of certificates for unlawful purposes and/or for purposes not allowed by this CPS.

9.10 Term and termination

9.10.1 Term

The Contract begins on the date of acceptance by the Contracting Party and ends on the expiry date of the certificate issued by Actalis; in case of renewal of the certificate itself, the validity of the Contract is deferred until the expiry date of the renewed certificate. In any case, the validity of the Contract will cease as a consequence of the revocation, for whatever reason, of the certificate.

9.10.2 Termination

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

9.10.3 Effect of termination and survival

In the case of contract termination, the certificate of the Subscriber is revoked by the CA.

9.11 Individual notices and communications with participants

Actalis accepts correspondence related to this CPS, to be sent with the methods indicated in section 1.5.2. Senders are invited to digitally sign their communications, if possible, or use another reliable communication method. Valid communications will be reviewed and replied to as appropriate in a timely manner.

Requests for assistance related to the CA service herein described (e.g. technical questions, problems installing the certificate, certificate not received, etc.) can be addressed to Actalis only when the involved certificates have been purchased directly from Actalis. When the involved certificates have instead been purchased from a reseller, assistance must be requested to that reseller. The terms for requesting assistance are published on the CA's website as well as on the certificate purchase and/or request portal.

Problems related to already issued certificates must be reported to Actalis as described in section 1.5.2.

9.12 Amendments

9.12.1 Procedure for amendment

The CA reserves the right to make changes to this CPS at any time, without notice, due to technical or organizational reasons or regulatory changes. Each new version of the CPS repeals and replaces the previous versions.

9.12.2 Notification mechanism and period

This CPS is reviewed by the CA and, if necessary, updated at least once per year, even in the absence of regulatory changes. The new versions of the CPS are published on the CA website.

9.12.3 Circumstances under which OID must be changed

This CPS applies to various certificate policies (see paragraph 1.4), each identified by a specific OID. Revision of the CPS does not in itself imply the modification of those OIDs.

9.13 Dispute resolution provisions

If the Subscriber or the Applicant of the certificate is a Professional pursuant to Legislative Decree no. n.206/2005 ("Consumer Code"), any dispute deriving from the Contract will be deferred to the judgment of an Arbitration Board composed of three members, one of whom is appointed by Actalis, one appointed by the Contractor, and the third, who will act as President, appointed by the first two. Should one of the Parties fail to appoint its Arbitrator within 20 days of receiving the notice of appointment of Arbitrator sent by the other Party, that second Arbitrator shall be appointed, at the request of the latter Party, by the President of the Court of Arezzo. Similarly, if the two Arbitrators appointed by the Parties do not reach an agreement on the appointment of the third Arbitrator within 20 days from the appointment of the second Arbitrator, the third Arbitrator shall be appointed by the President of the Court of Arezzo upon request of the most diligent Party. The arbitration will be of a ritual nature and the Arbitrators will judge according to the law in accordance with the provisions of articles 806 and following of the Code of Civil Procedure.
The Arbitration will be held in Arezzo.

9.14 Governing law

This CPS is subject to Italian Law and as such it shall be interpreted and carried out. For that not expressly prescribed in this CPS, the applicable law shall prevail.

Other contracts in which this CPS is incorporated by means of reference, may contain distinct and separate clauses with respect to applicable law.

9.15 Compliance with applicable law

The main applicable laws are listed below:

- Regulation (EU) 2014/910 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 (also "eIDAS").
- Legislative Decree March 7, 2005, No. 82: "Codice dell'Amministrazione Digitale", G.U. n.112 of 16 May 2005, and subsequent amendments and integrations (also "CAD").

- Legislative Decree 30 June 2003, n. 196: " Codice in materia di protezione dei dati personali ", G.U. n. 174 of 29 July 2003, and subsequent amendments and integrations.
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data, as well as on the free movement of such data and repealing Directive 95/46/EC (also “General Data Protection Regulation” or GDPR).

9.16 Miscellaneous provisions

9.16.1 Entire agreement

This CPS, which may or may not be supplemented by general or specific Terms and Conditions signed by the Applicant, constitutes the discipline that regulates the use of the certificate by the Subscriber and regulates the relationship between Subscriber and CA. The certificate application implies the full and unconditional acceptance of this CPS by the Applicant.

9.16.2 Assignment

Please refer to the general Terms and Conditions published on the CA website.

9.16.3 Severability

The CA will abide by section 9.16.3 of the [SMBR], if applicable, and to the general Terms and Conditions published on the CA website.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

Please refer to the general Terms and Conditions published on the CA website.

9.16.5 Force majeure

Actalis shall not be responsible for the failure to carry out the obligations assumed herein in the case when such non-fulfilment is due to causes not attributable to Actalis, such as – for instance, but not limited to – act of providence, unforeseen technical problems completely out of any form of control, intervention by the authority, force majeure, natural disasters, industrial actions including company strikes – inclusive of those at the premises of parties which are used for the execution of the activities associated with the services described herein, and other causes attributable to third parties.

APPENDIX A – CHANGE HISTORY

DATE	VERS.	PARAGRAPHS	CHANGES	AUTHOR
19-Jun-2026	1.0	All	First version obtained by merging the previous S/MIME Certificate Policy v3.1 with the common parts of the general CPS (which covered all types of Actalis publicly trusted certificates) to obtain a combined CP-CPS, self-consistent and focused on S/MIME certificates only.	AS, FM, NP