Corporate S/MIME Certificates

Certificate Policy

Version 1.2

Last revised: October 07, 2019

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

CHANGE HISTORY

Version	Date	Author	Remarks
1.0	11/11/2015	AS	First version.
1.1	27/12/2016	AS	Changed company address. Added S/MIME certificates for organizations.
1.2	07/10/2019	AS	§1.3 Clarified that email can only be validated by the CA. §1.7 Updated reference for OCSP protocol. §3.1 Clarifications on the EE naming rules. §3.2 Modified headings for better clarity. §4.2 Clarifications on certificate revocation. §7.2 Updated profile of intermediate CA. §7.3 Updated profile of EE certificate.

CONTENTS

1 INTRODUCTION 4
1.1 OVERVIEW AND TERMINOLOGY 4
1.2 POLICY IDENTIFICATION 4
1.3 PARTICIPANTS TO PKI 4
1.4 CERTIFICATE USAGE 5
1.5 POLICY ADMINISTRATION 5
1.6 DEFINITIONS & ACRONYMS 5
1.7 LIST OF REFERENCES 6
2 PUBLICATION AND REPOSITORY 6
3 IDENTIFICATION AND AUTHENTICATION (I&A) 7
3.1 NAMING 7
3.2 INITIAL IDENTITY VALIDATION 7
3.2.1 Certificates for organizations 7
3.2.2 Certificates for individuals 8
3.3 I&A FOR RENEWAL REQUESTS 9
3.4 I&A FOR REVOCATION REQUESTS 9
4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 9
4.1 CERTIFICATE APPLICATION, PROCESSING AND ISSUANCE 9
4.1.1 Certificates for organizations 9
4.1.2 Certificates for individuals 10
4.2 CERTIFICATE REVOCATION AND SUSPENSION 11
4.2.1 Circumstances for Suspension and Revocation 11
4.2.2 Procedure for Suspension and Revocation 11
4.3 CERTIFICATE STATUS SERVICES 12
4.4 KEY ESCROW AND RECOVERY 12
5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 12
5.1 PHYSICAL SECURITY CONTROLS 12
5.2 PROCEDURAL CONTROLS 12
5.3 PERSONNEL CONTROLS 12
5.4 AUDIT LOGGING 12
5.5 RECORDS ARCHIVAL 12
6 TECHNICAL SECURITY CONTROLS 13
6.1 KEY PAIR GENERATION AND INSTALLATION 13
6.2 PRIVATE KEY PROTECTION AND HSM CONTROLS 13
6.3 COMPUTER SECURITY CONTROLS 13
6.4 NETWORK SECURITY CONTROLS 13
7 CERTIFICATE, CRL, AND OCSP PROFILES 14
7.1 ROOT CA CERTIFICATE 14
7.2 SUBORDINATE CA CERTIFICATE 14
7.3 END-ENTITY CERTIFICATES 15
7.4 CERTIFICATE REVOCATION LISTS 16
7.5 OCSP PROFILE 16
8 COMPLIANCE AUDIT AND OTHER ASSESSMENT 16
9 OTHER BUSINESS AND LEGAL MATTERS 16
9.1 FEES 16
9.2 CORRESPONDENCE AND TECHNICAL SUPPORT 16
9.3 FINANCIAL RESPONSIBILITY 17
9.4 PRIVACY OF PERSONAL INFORMATION 17
9.5 OBLIGATIONS AND GUARANTEES 17
9.6 DISCLAIMERS OF WARRANTIES 18
9.7 GOVERNING LAW AND DISPUTE SETTLEMENT 18

1 INTRODUCTION

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

1.1 Overview and terminology

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

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

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

1.2 Policy Identification

This document is the Certificate Policy for **Corporate S/MIME certificates** issued by Actalis S.p.A. and is identified within certificates by the Object Identifier (OID) **1.3.159.1.25.1**.

This document is broadly based on RFC 3647; however, not all topics found in RFC 3647 are addressed in this document. With reference to the topics not addressed here nor in any referenced documents, Actalis does not commit to do anything in particular, or in any particular way.

1.3 Participants to PKI

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

Subscribers may be any **individuals** or **organizations**. Individuals will typically (but need not) be employees of some organization that plays the role of RA (see below).

Registration Authorities (RAs) are entities performing I&A of Subscribers and possibly their registration into the CA database, to allow the subsequent certificate issuance. For certificates to be issued to individuals, RA tasks can be performed by an external organization (e.g. the employer). For certificates to be issued to organizations, RA tasks are performed by the CA itself. In all cases, email address validation is directly performed by the CA (it cannot be delegated).

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.

1.4 Certificate usage

Certificates issued under this CP are mainly intended for **securing email** according to the **S/MIME** standard [SMIME]. In some contexts, they could also be used for SSL/TLS client authentication [TLS], depending on the target environment.

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.

1.5 Policy administration

This CP is drafted, revised, approved, published and maintained by Actalis. For any questions regarding this CP, please write to ca-admin@actalis.it.

1.6 Definitions & Acronyms

CA	Certification Authority (see CSP)
CMS	Certificate Management System
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSP	Certification Service Provider (see CA)
CSR	Certificate Signing Request
HSM	Hardware Security Module
HTTP	Hyper-Text Transfer Protocol
I&A	Identification and Authentication
LDAP	Lightweight Directory Access Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
RA	Registration Authority
S/MIME	Secure MIME
SSL	Secure Sockets Layer
TLS	Transport Layer Security

1.7 List of references

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

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

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

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

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

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

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

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

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

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

[SSLCPS] Certification Practice Statement - SSL Server and Code Signing certificates (https://www.actalis.it/documenti-en/cps-for-ssl-server-and-code-signing.pdf)

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

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

2 PUBLICATION AND REPOSITORY

The term "repository" refers to a combination of on-line archives or registers containing information of public interest regarding the issuance and management of certificates described in this CP.

Actalis' repository consists of:

- Actalis' web site (http://www.actalis.it)
- Actalis' LDAP directory server (ldap://ldap.actalis.it)

From Actalis' main web site, the user may be directed to other Actalis' web sites, depending on the specific information sought. From now on, we refer to the final web site by "the CA web site".

The CA publishes at least the following documentation on its web site:

- Certificate Policy (CP) – this document
- Terms & Conditions for this CA service
- certificate request form(s)

3 IDENTIFICATION AND AUTHENTICATION (I&A)

3.1 Naming

Certificates issued under this CP always contain an email address and the identity of an organization (full name and registration number). Certificates issued to individuals may also contain an individual identity (e.g. forename and surname).

More precisely:

- the optional **commonName** component (CN) of the Subject field may contain, on request of the Applicant, the Subscriber's common name (e.g. forename and surname for individuals, or a service/device name in case of organizations) as verified by the RA; this field may not contain a string which is or resembles a DNS domain name;
- the **organizationName** component (O) of the Subject field contains the full registered name of the Subscriber's organization, where applicable, as verified by the RA;
- the optional **organizationalUnitName** component (OU) of the Subject field may contain, on request of the Applicant, an organizational unit name (e.g. department, division, etc.); this information is not verified by the CA;
- the **countryName** component (C) of the certificate's Subject field contains the ISO 3166 2-letter code of the country where the Subscriber's organization is headquartered.

Other components MAY be present in the certificate's Subject field in compliance with RFC 5280 and subject to verification by the RA, depending on specific projects and customers.

The **SubjectAlternativeName** (SAN) extension contains the Subscriber's **email address** as verified by the CA. No other SAN forms are inserted into the certificate.

3.2 Initial Identity Validation

3.2.1 Certificates for organizations

3.2.1.1 Validation of Applicant identity

For certificates to be issued to organizations, a **certificate request form** must be filled in, signed by a suitable Applicant Representative, and submitted to the CA. The Applicant Representative's identity (and consequently the authenticity of the request) is then verified in different ways, depending on how the request form is signed:

1) If the request form is signed by hand, the signature shall:
   - either be witnessed and counter-signed by an RA operator,
   - or verified by an RA operator via a telephone call to the alleged signatory, using a telephone number obtained from a reliable and independent source;
2) If the request form is digitally signed, the RA operator shall check that the signature certificate is a valid qualified e-signature certificate according to EU legislation; if so, the requestor's identity is obtained from that certificate; otherwise, the request shall be rejected.

In case the RA has any doubts on the signatory's agency (i.e. his/her authorization to request certificates on behalf the applicant), it is up to the Applicant to provide suitable evidence thereof.

In any case, the official name, legal address, company registration number and other data of the Applicant shall be verified by the RA by querying reliable independent information sources like e.g. the applicable jurisdiction's company registry or a governmental database of public agencies.

3.2.1.2 Validation of Applicant email address

The CA shall verify that the requesting organization controls the email address to be included in the requested Certificate by one of the following methods:

- by performing domain control validation over the email domain using one of the methods allowed by the CAB Forum's Baseline Requirements [BR];
- by sending an email message containing a random value to the email address to be included in the Certificate and receiving the same random value from the certificate requestor via a different channel, showing that the requestor has access to that email address.

3.2.1.3 Proving possession of private key

Proof of possession, by the requestor, of the private key corresponding to the public key to be certified is based on different mechanisms depending on the specific certificate request procedure:

- either the requestor shall send its public key to the CA as a CSR in PKCS#10 format, together with the certificate request form (in this case the CA, before issuing the certificate, checks that the CSR is cryptographically valid);
- or, the public key is provided to the requestor by the CA together with the corresponding private key (see section 3.2.2.3 for more details).

3.2.2 Certificates for individuals

3.2.2.1 Validation of applicant identity

Applicant identity (except the Applicant's email address) shall be verified by the RA in a reliable way, e.g. by a face to face procedure including the examination of a personal identification document, or by an online procedure requiring the Applicant to authenticate itself and subsequent lookup of previously verified identification data, or other similarly secure procedure. The applicant email shall be verified directly by the CA as described in §3.2.2.2 below.

To request the certificate, a web-based certificate request form must be suitably filled in by the Applicant and submitted to the CA web site (see §4.1.2). The data to be entered in the request form include the Applicant's **email address** (see next paragraph) and a "**voucher**" code used to lookup the other identity information (e.g. commonName, etc.) previously verified by the RA.

3.2.2.2 Validation of the Applicant email address

The Applicant's email address to be inserted into the certificate is verified by the CA via a **challenge-response** method. The submission of the web-based certificate request form (see §4.1.2) requires that the requestor also enters a unique "**verification code**" sent by the CA to the Applicant's claimed

email address. If the verification code inserted into the request form does not match the one generated by the CA, the request form is rejected. The requestor's capability to enter the correct verification code in the certificate request form proves that the Applicant's email address does exist and the requestor has access to it.

3.2.2.3 Proving possession of private key

The private cryptographic key corresponding to the public key within the certificate is generated by the CA itself and subsequently sent to the subscriber in **PKCS#12** format [PFX], via email, thereby insuring that the subscriber possesses the private key. The PKCS#12 file is enciphered by a strong password-based encryption (PBE) algorithm, using a random password of suitable length.

The password needed to decipher the PKCS#12 file is provided to the Subscriber out-of-band (over a secure TLS channel), therefore protecting it from unwanted disclosure to third parties. The CA does not retain such password, so the Subscriber (who is supposed to keep its password confidential) remains the only person able to decipher the PKCS#12 file and access the private key within.

3.3 I&A for Renewal Requests

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

3.4 I&A for Revocation Requests

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

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

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application, Processing and Issuance

4.1.1 Certificates for organizations

To request the Certificate, the Applicant Representative (Requestor) must fill in and submit to the CA a certificate request form. Depending on the case, the Requestor may have to also attach a suitable CSR (containing an RSA public key with a modulus length of 2048 bits) to the form.

Submission of the request form requires express acceptance, by the requestor, of the applicable Terms and Conditions, and consequently of this Certificate Policy, and other clauses that may be required by law (e.g. privacy policy, etc.).

The CA then performs I&A according to §3.2.1. After all I&A checks are passed successfully, the CA issues the certificate and sends it to the Subscriber via email.

4.1.2 Certificates for individuals

Certificates pursuant to this CP can be issued to individuals on request of some organization playing the role of **Registration Authority** (see §1.3). In such case, the said organization is responsible for ensuring that the registration data sent to the CA (see below) are true and accurate. In the following, such organization is also referred to as (the) "RA".

First of all, the RA must send to the CA a **list of the individuals** to whom certificates are to be issued. For each individual, the following data must be provided in the list:

- personal email address
- (optional) common name (e.g. forename and surname)
- (optional) organizational unit name
- (optional) organization name
- (optional) company registration number (mandatory if previous field is present)

The list can contain an optional organization name because the organization with which a person is affiliated need not be the same organization acting as RA. When not specified, the organization name and registration number included in the certificate are those of the RA.

The list must be sent to the CA as a file in CSV format (or another format to be agreed with the CA) in a way that ensures the integrity and origin of the information, e.g. via certified email or as a digitally signed attachment to an ordinary email message.

The said file must be sent directly to the CA by a suitable officer or division of the RA organization.

Regardless of any prior agreement, by sending such file to the CA, the RA acknowledges to have read and to accept this Certificate Policy and the Terms & Conditions published on the CA web site.[1]

Upon receiving the said list from the RA, and after checking that the list is correctly formatted and contains proper data, the CA generates and shares with the RA a unique "**voucher**" code. The RA is then required to disclose such code to all the individuals in the list (and only to them).

At that point, all the people who received the voucher code from their RA can proceed with the certificate request procedure like follows. To request his/her certificate, the Requestor must fill in and submit a **web-based request form** to be found on the CA web site. The requestor must enter the following data in the web form:

- the "voucher" code
- the Requestor's email address
- the email address verification code (see §3.2.2.2)

[1] https://www.actalis.it/products/certificates-for-secure-electronic-mail.aspx

Submission of the request form requires express acceptance, by the Requestor, of the applicable Terms and Conditions, and consequently of this Certificate Policy, and other clauses that may be required by law (e.g. privacy policy, etc.).

Upon submission of the request form, the CA performs I&A according to §3.2. If all checks are passed, the CA issues the certificate and sends it to the Subscriber via email.

The certificate is sent to the Subscriber in bundle with the corresponding private key (an RSA public key with a modulus length of 2048 bits) as a PKCS#12 file [PFX]. The password needed to decipher the PKCS#12 file is shown to the Subscriber within the browser, over a secure TLS channel, at the end of the request procedure. It is up to the Subscriber to keep that password confidential.

4.2 Certificate Revocation and Suspension

4.2.1 Circumstances for Suspension and Revocation

The certificate shall be revoked in the following cases:

- request errors
- non-compliance with this CP
- compromise of the private key (*)
- termination of use of the certificate (*)
- loss of validity of some certificate data (*)
- infringement of the applicable Terms & Conditions.

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

Certificate suspension is justified in the following cases:

- suspected compromise of private key;
- temporary interruption of certificate use.

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

4.2.2 Procedure for Suspension and Revocation

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

The Subscriber may request suspension or revocation of his/her certificates by accessing the CA web site (using the credentials that were sent to him/her upon certificate issuance), and then following

the on-screen instructions. The exact address of the web site is included in the same mail by which the certificate is sent to the user.

4.3 Certificate status services

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

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

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

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

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

4.4 Key Escrow and Recovery

Depending on the specific customer and contract, the CA may provide a key recovery service.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

All facility, management, and operations controls applying to this certificate policy are exactly the same as those applying to Actalis' **SSL Server and Code Signing Certificates** [SSLCPS], except where otherwise specified hereafter.

5.1 Physical Security Controls

Same as documented in [SSLCPS].

5.2 Procedural Controls

Same as documented in [SSLCPS].

5.3 Personnel Controls

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

5.4 Audit Logging

For the purpose of maintaining a secure environment, the CA logs all relevant events such as certificate lifecycle operations, attempts to access the system, and requests made to the system. Audit logs are subject to random checks by Actalis' internal auditor.

5.5 Records Archival

The CA archives all audit data, certificate application information, and documentation supporting certificate applications; archives are kept for at least 3 years.

6 TECHNICAL SECURITY CONTROLS

All facility, management, and operations controls applying to this certificate policy are exactly the same as those applying to Actalis' **SSL Server and Code Signing Certificates** [SSLCPS], except where otherwise specified hereafter.

6.1 Key Pair Generation and Installation

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

The key pairs of Subscribers shall be RSA key pairs with a module of 2048 bits and a public exponent of 0x10001 (65537). Subscriber key pairs may be generated by the CA itself, with a procedure ensuring adequate key quality, and provided to the Subscriber in a secure way (see §3.2.2.3).

6.2 Private Key Protection and HSM Controls

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

The Subscriber's private key shall be protected by at least a PIN or password.

6.3 Computer Security Controls

Same as documented in [SSLCPS].

6.4 Network Security Controls

Same as documented in [SSLCPS].

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Root CA certificate

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

7.2 Subordinate CA certificate

The certificate of the subordinate CA, used to sign end-entity certificates, has the following profile:

Field	**Value**	
Version	V3 (2)	
SerialNumber	<includes at least 8 pseudo-random bytes>	
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)	
Issuer	CN = Actalis Authentication Root CA O = Actalis S.p.A./03358520967 L = Milano C = IT	
Validity	<10 years>	
Subject	CN = Actalis Client Authentication CA G***N*** O = Actalis S.p.A./03358520967 L = Ponte San Pietro ST = Bergamo C = IT	
SubjectPublicKeyInfo	<RSA public key of 2048 bits>	
SignatureValue	<Root CA signature>	
Extension	**Critical?**	**Value**
Basic Constraints	True	CA=true, pathLenConstraint=0
AuthorityKeyIdentifier (AKI)		<Same value as the Root CA SKI extension>
SubjectKeyIdentifier (SKI)		<public key SHA1-digest>
KeyUsage	True	keyCertSign, cRLSign
ExtendedKeyUsage (EKU)		clientAuth (1.3.6.1.5.5.7.3.2), emailProtection (1.3.6.1.5.5.7.3.4)
CertificatePolicies		PolicyOID = 2.5.29.32.0 (anyPolicy), CPS-URI = <HTTP address of this Policy>
SubjectAlternativeName (SAN)		<not included>
AuthorityInformationAccess (AIA)		<HTTP address of OCSP responder>
CRLDistributionPoints (CDP)		<HTTP address to access the ARL>, <LDAP address to access the ARL>

7.3 End-Entity certificates

The profile of end entity certificates is as follows:

Base field	Value	
Version	V3 (2)	
SerialNumber (hex)	<includes at least 8 pseudo-random bytes>	
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)	
Issuer	<Subject of the Subordinate CA – see §7.2>	
Validity	notBefore = <issuance time> notAfter = <12, 24, or 36 months later, depending on contract>	
Subject	[CN = <subscriber's common name>] O = <full name of subscriber's organization> [OU = <organizational unit name>] serialNumber = <organization's registration number> C = <ISO 3166 country code of subscriber's organization >	
SubjectPublicKeyInfo	<public RSA key of length 2048 bits>	
SignatureValue	<Subordinate CA signature value>	
Extension	**Critical?**	**Value**
Basic Constraints	True	cA=FALSE
AuthorityKeyIdentifier (AKI)		KeyID=<SHA1 hash of the CA public key>
SubjectKeyIdentifier (SKI)		<SHA1 hash of Subject public key>
KeyUsage	True	digitalSignature, keyEncipherment
ExtendedKeyUsage (EKU)		clientAuth (1.3.6.1.5.5.7.3.2), emailProtection (1.3.6.1.5.5.7.3.4)
CertificatePolicies		OID of this policy (see §1.2)
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>

7.4 Certificate Revocation Lists

The profile of CRLs is conformant to the reference standard [PROF] with the following remarks:

- CRL syntax version is v2 (1);
- The reasonCode extension is present in all revokedCertificates entries;
- The AuthorityKeyIdentifier (AKI) and CRLNumber extensions are present.

7.5 OCSP profile

OCSP responses returned by the CA conform to the "Basic" profile as defined in the [OCSP] specification.

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

8 COMPLIANCE AUDIT AND OTHER ASSESSMENT

Compliance audits and other assessments applying to this certificate policy are the same as those applying to Actalis' **SSL Server and Code Signing Certificates** [SSLCPS].

9 OTHER BUSINESS AND LEGAL MATTERS

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

9.1 Fees

Certificates issued according to this policy are priced depending on volumes, duration of the validity period, any possible custom-specific requirements and other factors. Quotes will be provided to interested parties on request.

9.2 Correspondence and technical support

Actalis accepts correspondence related to this CP, to be sent with the methods indicated at §1.5, and will normally respond within two working days.

Actalis does not commit to provide technical support to Subscribers unless expressly provided for in the contract. However, Actalis will try to provide assistance, via email, on a "best effort" basis. To request assistance, an email should be sent to client-certs@actalis.it including the following information:

- name, surname, and affiliation of the sender;
- a clear and detailed description of the alleged problem;
- a description of the computing environment where the alleged problem occurs (e.g. operating system name and version, browser name and version, email application name and version, type of internet connectivity, networking restrictions, etc.).

Requests not containing the above information will be silently discarded.

9.3 Financial Responsibility

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

9.4 Privacy of Personal Information

All personal information collected by Actalis for the purpose of issuing certificates shall be handled in full compliance with the Italian and EU legislation.

9.5 Obligations and guarantees

The **Certification Authority** shall:

- operate the certification service in compliance with this CP;
- take reasonable measures to ensure that Subscribers hold the private keys corresponding to their certificates;
- take reasonable measures to verify that, at the time when a certificate is issued, the requestor has control of the email account associated with the email address included in the certificate or has been authorized by the email account holder to act on its behalf;
- guarantee processing of personal data in compliance with applicable law.

Registration Authorities shall:

- read and accept this CP before or upon requesting the CA to issue certificates;
- collect and verify the accuracy and truthfulness of the personal data of individuals to whom certificates are to be issued;
- promptly inform the CA if any of the data provided to the CA (e.g. email addresses, personal names, organization names, etc.) are subsequently found to be no longer valid, for instance in the case where some Subscriber no longer has access to the work mailbox and/or are not anymore employed by their previous organization.

Subscribers shall:

- read and accept this CP before or upon requesting the certificate;
- request the certificate in the way described in this CP;
- provide true and accurate information to the CA (possibly via an RA);
- ensure confidentiality of secret codes (e.g. passwords) provided to them by the CA;
- adopt suitable measures to avoid unwanted disclosure of secret codes (e.g. the passwords provided to individual subscribers) obtained from the CA;
- adopt suitable measures to avoid compromise of their own private keys;
- install and start using their certificate only after having checked that it contains correct information;

- use the certificate only in the ways and for the purposes provided for in this CP;
- never use their private keys for issuing other certificates in turn;
- in the event of confirmed compromise of any of their own private keys, immediately request revocation of the corresponding certificates and immediately stop using those certificates;
- promptly request revocation of their certificate in the case when any of the information contained in their certificate (i.e. organization name, email address etc.) is no longer valid.

Relying Parties are required 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 §4.3;
- only rely on certificates which are not expired, nor suspended nor revoked.

9.6 Disclaimers of warranties

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

9.7 Governing Law and Dispute Settlement

This CP is subject to Italian laws.

All disputes deriving from, or related to the present CP shall be subject to the Italian jurisdiction and shall be settled by the Courts of Bergamo (IT).

END OF DOCUMENT