Free S/MIME Certificates

Certificate Policy

Version 1.0 – Last revised: June 5, 2015

Via dell'Aprica 18 | 20158 Milano
Tel +39-02-68825.1 | Fax +39-02-68825.223
www.actalis.it | info@actalis.it

CHANGE HISTORY

Version	Date	Author	Remarks
1.0	22/04/2015	AS	First version.

CONTENTS

1 INTRODUCTION

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

1.1 Overview and terminology

A *certificate* binds a public key to a set of information that identifies an entity (be it an individual or an organization). This entity, the owner of the certificate, possesses and uses the corresponding private key. The certificate is generated and supplied to the owner by a trusted third party known as *Certification Authority* (CA), and is digitally signed by the CA. The reliability of a certificate also depends on the CA's operating procedures, on the obligations and responsibilities between the CA and Subscriber, and the CA's physical and technical security controls. All those aspects are described in a public document called *Certification Practice Statement* (CPS) or *Certificate Policy* (CP), depending on the level of detail and broadness of scope (see RFC 3647). Certificate owners are also called *Subscribers* as they undersign a contract with the CA (of which the CP/CPS is an integral constituent) for certificate issuance and management. Since the CA provides a service to its subscribers, it is also called a *Certification Service Provider* (CSP).

1.2 Policy Identification

This document is the **Certificate Policy** for **Free S/MIME certificates** issued by Actalis S.p.A. and is identified within certificates by the Object Identifier (OID) **1.3.159.1.24.1**.

This document is broadly based on RFC 3647; however, not all topics found in RFC 3647 are addressed in this document. As regards 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.**, with principal address at Via dell'Aprica 18, 20158 Milano, Italy, registered in the Registry of Enterprises of Milano under #03358520967.

Subscribers, who will become **certificate owners**, may be any individuals needing one or more certificates for the purposes indicated in §1.4.

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

Relying Parties (RP) are all entities that rely on the accuracy of the binding between the subject's public key distributed via a certificate and the Subject's identity (his/her email address, in this particular case) contained in the same certificate.

1.4 Certificate usage

Certificates issued under this CP are mainly intended for **secure e-mail**, according to the **S/MIME** standard [SMIME]. However, they can also be used for **SSL/TLS client authentication** [TLS].

Note: It is assumed that Subscribers already have the competence and instruments required to use their certificates. Otherwise, Actalis is available to offer the necessary consultancy.

1.5 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

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

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

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

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

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

[OCSP] RFC 2560: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", June 1999.

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

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
- web-based certificate request form

3 IDENTIFICATION AND AUTHENTICATION (I&A)

3.1 Naming

Certificates issued according to this policy do not contain the personal identity of the Subscriber, like e.g. name and surname, but only his/her email address. The CA makes no attempt to find out the requestor's identity and does not provide any warranty that the certificate owner is a specific person. The only warranty provided is that the CA, before issuing the certificate, has made a reasonable effort to verify that the requestor was able to access to the email address included in the certificate.

The **commonName** component (CN) of the certificate's Subject field contains the subscriber's email address conformant to RFC 5322 and subsequent updates.

No other components are present in the certificate's Subject field.

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

3.2 Initial Identity Validation

3.2.1 Authentication of requestor identity

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

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

3.2.2 Proving possession of private key

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

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

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

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

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

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

Upon submission of the certificate request form, the CA shall issue the certificate and send this latter to the Subscriber via email.

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

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 certificate owner **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.

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 2560 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) certificate 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.

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), and are generated by the CA itself by means of a procedure ensuring an adequate key quality, then sent to the Subscriber in a secure way.

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 = Milano 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>

On a temporary basis, Actalis may use one of the already existing subordinate CAs (e.g. those used for issuing SSL Server and Code Signing certificates). Please refer to [SSLCPS] for further details.

7.3 End-Entity certificates

The profile of end entity certificates is as follows:

Base field	**Value**	
Version	V3 (2)	
SerialNumber (hex)	<8 random bytes>	
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)	
Issuer	<Subject of the Subordinate CA – see §7.2>	
Validity	notBefore = <issuance time> notAfter = <12 months later>	
Subject	CN = <email address of the subscriber>	
SubjectPublicKeyInfo	<public RSA key of length 1024 to 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)		<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 clients are expected to conform to the [OCSP] specification. OCSP requests need not be signed or otherwise authenticated. OCSP responses returned by the CA conform the "Basic" profile as defined in the [OCSP] specification.

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 provided for free (that is, at no charge). However, *not more than 1 certificate request per year is accepted for each unique email address*.

At any rate, *Actalis does not promise to issue the certificate*, or to make it available to the requestor within any particular time.

9.2 Correspondence and technical support

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

Actalis does not commit to provide technical support to Subscribers, for certificates issued according to this CP. However, Actalis will try and provide assistance, only via e-mail, on a "best effort" basis. To request assistance, e-mail should be sent to client-certs@actalis.it providing the following information:

- name and surname of the user;
- a clear description of the alleged problem;
- description of the user's computing environment (at least: operating system name and version, browser name and version, email application name and version).

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 legislation (Legislative Decree n.196 of 2003).

9.5 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 Milano (IT).

END OF DOCUMENT