Certificate Policy for

SSL Client & S/MIME Certificates

OID: 1.3.159.1.11.1

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	Released	Remarks
1.0	17/06/2013	First version.

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) 6
3.1 NAMING 6
3.2 INITIAL IDENTITY VALIDATION 7
3.2.1 Authentication of requestor identity 7
3.2.2 Proving possession of private key 7
3.3 I&A FOR RENEWAL REQUESTS 7
3.4 I&A FOR REVOCATION REQUESTS 7
4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 8
4.1 CERTIFICATE APPLICATION, PROCESSING AND ISSUANCE 8
4.2 CERTIFICATE REVOCATION AND SUSPENSION 8
4.2.1 Circumstances for Suspension and Revocation 8
4.2.2 Procedure for Suspension and Revocation 9
4.3 CERTIFICATE STATUS SERVICES 9
5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 9
5.1 PHYSICAL SECURITY CONTROLS 9
5.2 PROCEDURAL CONTROLS 10
5.3 PERSONNEL CONTROLS 10
5.4 AUDIT LOGGING 10
5.5 RECORDS ARCHIVAL 10
6 TECHNICAL SECURITY CONTROLS 10
6.1 KEY PAIR GENERATION AND INSTALLATION 10
6.2 PRIVATE KEY PROTECTION AND HSM CONTROLS 10
6.3 COMPUTER SECURITY CONTROLS 11
6.4 NETWORK SECURITY CONTROLS 11
7 CERTIFICATE, CRL, AND OCSP PROFILES 12
7.1 CA CERTIFICATE 12
7.2 END ENTITY CERTIFICATES 13
7.3 CERTIFICATE REVOCATION LISTS 14
7.4 OCSP PROFILE 14
8 COMPLIANCE AUDIT AND OTHER ASSESSMENT 14
9 OTHER BUSINESS AND LEGAL MATTERS 14
9.1 FEES 14
9.2 FINANCIAL RESPONSIBILITY 14
9.3 PRIVACY OF PERSONAL INFORMATION 14
9.4 GOVERNING LAW AND DISPUTE SETTLEMENT 14

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 **SSL Client and S/MIME certificates** issued by Actalis S.p.A. and is identified within certificates by the Object Identifier (OID) **1.3.159.1.11.1**.

This document is broadly based on RFC 3647; however, not all possible topics are covered. As to the topics not addressed in this document, 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 people needing one or more certificates for the purposes indicated in §1.4. Subscribers, however, must have a VAT number.

Registration Authorities (RAs) are entities performing I&A of Subscribers and their registration into the CA database for subsequent certificate issuance. By default, RA tasks are accomplished by the CA itself (Actalis). In some cases, also depending on the overall number of certificates to be issued to an organization, RA duties may be delegated to that organization (acting as an "**Enterprise RA**") on the basis of a specific agreement with the CA.

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 (and possibly other attributes) contained in the same certificate.

1.4 Certificate usage

Certificates issued under this CP are to be used for SSL/TLS client authentication, according to the TLS standard [TLS], and/or secure e-mail, according to the S/MIME standard [SMIME].

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

[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.

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

[RQFRM] CAACT-04-02-01 Richiesta Certificato SSL Client & SMIME

[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.

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.

The Actalis repository consists of:

- CA services web site (http://portal.actalis.it)
- LDAP directory server (ldap://ldap.actalis.it)

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

- Certificate Policy (CP) – this document
- request forms

Furthermore, the CA publishes certificates and CRLs on its LDAP directory server (see §4.2 for more information on CRLs).

3 IDENTIFICATION AND AUTHENTICATION (I&A)

3.1 Naming

The *commonName* component of the certificate's *subject* field may contain any string that concisely identifies the certificate owner (e.g. name and surname). It can be chosen at will by the RA, provided that it does not violate any third party rights nor does it lead to confusion regarding the certificate owner's identity. Also, all certificate owners shall have different commonNames. In case the RA does not specify a value for the *commonName*, a default value will be automatically generated by the CA.

The optional *organizatioName* component of the *subject* field shall contain the name (if applicable) of the organization that the certificate owner belongs to.

The *country* component of the *subject* field shall contain the ISO 3166 two-letter code (e.g. "IT" for Italy) of the country where the certificate owner (or his/her organization) resides.

Other components of the subject field may or may not be present.

The *SubjectAlternativeName* (SAN) extension of the certificate should contain the personal e-mail address of the certificate owner, or it may be impossible to use the certificate for S/MIME e-mail.

3.2 Initial Identity Validation

3.2.1 Authentication of requestor identity

First of all, the RA shall carefully check the certificate request form and its annexes for readability, completeness and consistency.

Then, unless the certificate requestor is present in person before the RA, the RA verifies the requestor's identity over the phone, by contacting the person who purportedly signed the certificate application form.

The RA reserves the right to perform further verifications in order to validate individual identities.

3.2.2 Proving possession of private key

The private cryptographic key corresponding to the public key within the certificate may, on request, be generated by the CA itself, and subsequently provided to the certificate owner in PKCS#12 format. Otherwise, before issuing the certificate the CA needs a proof that the applicant holds the private key corresponding to the public key to be included in the certificate. To that end, the applicant must send his/her public key to the CA in the form of a CSR in PKCS#10 format [CSR]. The CA shall verify that the digital signature in the CSR is valid, before issuing the certificate.

3.3 I&A for Renewal Requests

I&A for certificate renewal requests is done in the same way as for the first certificate issuance.

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 submit suspension or revocation requests through the CA services portal (https://portal.actalis..it) it is necessary for the Subscriber to login to the portal by means of suitable credentials supplied to him/her upon registration or issuance of the certificate;
- otherwise, the Subscriber can contact the CA Customer Care (contact details available on the CA services portal) 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 get an offer for certificates conforming to this CP, interested parties can inquire Actalis' sales department by calling phone nr. +39-02-68825.1 (PBX) or writing email to commerciale@actalis.it.

To apply for a certificate pursuant to this CP, after accepting the quote, the requestor shall fill in and submit to Actalis a **Certificate Request Form** conformant to the template [RQFRM], to be found on the CA services portal (https://portal.actalis.it). The form should then be sent to Actalis via e-mail at assistenza@actalis.it, or to the fax number +39-02-68825.223.

The RA shall then perform I&A according to §3.2 and subsequently register the user into the CA database by means of the suitable web-based application. Upon registration, the RA provides the user with personal credentials (such as user-id and password) allowing access to the CA services portal.

The user shall then access the CA services portal and request his/her certificate by following the on-screen instructions. The web-based certificate enrollment procedure then takes place, comprised of the following steps:

- generation of a suitable RSA key pair on the user PC;
- creation of a corresponding CSR and submission to the CA;
- generation of the corresponding certificate by the CA;
- certificate download and installation on the user PC.

Enterprise RAs are allowed to carry out the enrollment procedure on behalf of their users, provided they do not retain the user's private key nor his/her credentials for accessing the CA services portal.

4.2 Certificate Revocation and Suspension

4.2.1 Circumstances for Suspension and Revocation

The certificate shall be revoked in the following cases:

- registration errors (*);
- compromise of private key (*);
- failure to comply with this CP;
- loss of validity of some certificate data (*);
- termination of use of the certificate (*);
- breach of contract (e.g. failure to pay the due fee).

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 certificate owner or by initiative of the CA/RA.

The certificate owner may request suspension or revocation of his/her certificates by accessing the CA services portal (using the credentials that he/she was given at registration time), then following the on-screen instructions.

4.3 Certificate status services

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

- through the publication of a Certificate Revocation List (CRL) in the format defined in the specification [PROF];
- by providing an on-line certificate status service based on OCSP protocol in compliance with the specification [OCSP].

The CRL can be downloaded via both the LDAP protocol [LDAP] and the HTTP protocol [HTTP]. The LDAP and HTTP addresses of the CRL are inserted in the *CRLDistributionPoints* (CDP) extension of the certificate, while the OCSP server address is inserted in the *AuthorityInformationAccess* (AIA) extension of the certificate.

The CRL is regenerated and republished every 6 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

5.1 Physical Security Controls

All the main systems (computers, cryptographic hardware, network devices, etc.) used by Actalis for issuing and managing certificates according to this CP are housed in a physically secure data center located in Arezzo, Italy. Access to the data room is only allowed to authorized people and requires a suitable badge. The data center has redundant internet connectivity, redundant power supply systems, and is protected against fire and floods.

5.2 Procedural Controls

Actalis enforces a "separation of duties" principle in assigning responsibilities to the personnel employed in its CA services. In particular, the following roles are assigned to different people:

- Operations and Customer Care
- CA development and maintenance
- Information Security
- Internal Auditing

In addition, certain procedures require the involvement of several people and are recorded.

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

6.1 Key Pair Generation and Installation

The key pair used by the CA to sign certificates and CRLs is an RSA key pair with a module of at least 2048 bits. Such key is generated and kept inside a high quality Hardware Security Module (HSM) – see also §6.2.

The key pairs of Subscribers (certificate owners) must be RSA key pairs with a module of 1024 to 2048 bits and a public exponent of 0x10001 (65537).

6.2 Private Key Protection and HSM Controls

The HSM used by the CA (see §6.1) has a FIPS PUB 140-2 Level 3 security certification. Private keys within it are protected by a PIN. HSM activation, configuration and CA key generation is only possible for authorized personnel using special tokens.

6.3 Computer Security Controls

The operating systems used by the CA for management of certificates have been certified according to ITSEC (E2-HIGH) or other equivalent criteria. They are configured so that all users are required to identify themselves by means of a username and password or, for more critical systems, via the use of a smartcard and corresponding PIN.

6.4 Network Security Controls

Access to the CA servers is protected by high quality firewalls which guarantee an adequate filtering of the incoming connections. In order to strengthen protection, the entire certification management infrastructure is split-up into an external network, internal network and a De-Militarized Zone (DMZ). Also, a security assessment is periodically carried out to check for vulnerabilities.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 CA certificate

The profile of the CA certificate is as follows:

Base field	**Value**	
Version	V3 (2)	
SerialNumber (hex)	<8 bytes>	
Signature	sha1WithRSAEncryption (1.2.840.113549.1.1.11)	
Issuer	CN = Actalis e-Business CA G1 OU = Authentication Service Provider O = Actalis S.p.A./03358520967 C = IT	
Validity	from 9 May 2011 to 9 May 2023	
Subject	CN = Actalis e-Business CA G1 OU = Authentication Service Provider O = Actalis S.p.A./03358520967 C = IT	
SubjectPublicKeyInfo	<public RSA key of length ≥ 2048 bits>	
SignatureValue	<signature value>	
Extension	**Critical?**	**Value**
Basic Constraints	True	CA=True
AuthorityKeyIdentifier (AKI)		KeyID=<SHA1 hash of public key>
SubjectKeyIdentifier (SKI)		<SHA1 hash of public key>
KeyUsage	True	keyCertSign, cRLSign
ExtendedKeyUsage (EKU)		-
CertificatePolicies		(optional)
SubjectAlternativeName (SAN)		-
AuthorityInformationAccess (AIA)		-
CRLDistributionPoints (CDP)		(optional)

7.2 End entity certificates

The profile of end entity certificates is as follows:

Base field	**Value**	
Version	V3 (2)	
SerialNumber (hex)	<8 random bytes>	
Signature	sha1WithRSAEncryption (1.2.840.113549.1.1.11)	
Issuer	CN = Actalis e-Business CA G1 OU = Authentication Service Provider O = Actalis S.p.A./03358520967 C = IT	
Validity	notBefore = <issuance time> notAfter = <1 to 3 years later>	
Subject	CN = <chosen by the Registration Authority> O = <optional; name of the owner's organization> C = <country where the certificate owner resides>	
SubjectPublicKeyInfo	<public RSA key of length 1024 to 2048 bits>	
SignatureValue	<CA signature value>	
Extension	**Critical?**	**Value**
Basic Constraints		-
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 >
AuthorityInformationAccess (AIA)		<URL of OCSP responder>
CRLDistributionPoints (CDP)		<HTTP URL of the CRL>, <LDAP URL of the CRL>

7.3 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.

7.4 OCSP profile

OCSP client are required to be conformant to the [OCSP] specification. OCSP requests need not be signed or otherwise authenticated. OCSP responses returned by the CA are conformant to the "Basic" profile as defined in the [OCSP] specification.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENT

The infrastructure and procedures being used by Actalis for issuing certificates under this CP are periodically audited by Actalis' internal auditor; results are presented to the Direction. If necessary, remedial actions are taken to ensure adherence to this policy and the reliability and correctness of operations.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

The fees due to Actalis for certificate issuance and management according to this CP are negotiated on a per-Customer basis and may vary depending on the total number of certificates ordered and other factors. Please contact Actalis' sales department (commerciale@actalis.it) to get a quote.

9.2 Financial Responsibility

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

9.3 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).

9.4 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).