ACTALIS

www.actalis.it

Certification Practice Statement

SSL Server and Code Signing certificates

Version: 2.0.3

Date: 18 May 2010

Certification Practice Statement

SSL Server and Code Signing certificates

Written by:	Fulvio Parisi Auditing Manager		Date
Verified by:	Roberto Ravazza Registration Manager		Date
Verified by:	Rosalia Valsecchi Certification Manager		Date
Verified by:	Fabio Omenigrandi Production Manager		Date
Approved by:	Adriano Santoni Security Manager		Date

Document Code: CAACT-03-01-04

Distribution: PUBBLICA

REVISION INDEX

DATE	VERS.	PARAGRAPHS	CHANGES	AUTHOR
14 Dec. 2005	1	-	Initial release	FP
24 June 2009	2	all	Complete review of document in accordance with RFC 3647	FP, AS
19 Nov. 09	2.0.1	1.3.1	Changed name of President	AS
13 May 2010	2.0.2	3.4	Removed sentence referring to private IP addresses in certificates (that is not allowed)	AS
18 May 2010	2.0.3	4.2, 8.1, 8.2, 8.4, 8.5, 8.6, 9.5.2, 9.8	Clarifications and integrations related to RAs	AS
18 May 2010	2.0.3	1.3.1	Updated Actalis' address; corrected the given name of the President.	AS

LIST OF CONTENTS

1. INTRODUCTION

1.1 Overview

Actalis S.p.A. has been a leading provider, since 2002, of certification services accredited by CNIPA (Italian Authority for Informatics in the Public Administration) under the EU Signature Directive (Directive 1999/93/EC), and offers various types of certificates and relevant management services together with other services and solutions (www.actalis.it).

A certificate binds a public key to a set of information that identifies an entity (individual or organisation). This entity, the subscriber or owner of the certificate, possesses and utilises the corresponding public key. The certificate is generated and supplied to the owner by a trusted third party known as **Certification Authority** (CA). The certificate is digitally signed by the CA.

The reliability of a certificate, in other words the dependable association of a given public key with the identified subject, also depends on the CA's operating procedures, on the obligations and responsibilities between the certification authority and subscriber, and the CA's physical and logical security controls. These aspects are described in a public document: **Certification Practice Statement** (CPS).

This document is the Actalis CPS relevant to the issue and management of two types of certificates:

- SSL Server Certificate
- Code Signing Certificate

The structure and content of this CPS are compliant with the public specification [RFC 3647].

1.2 CPS Object Identifier

This CPS is indicated in the certificates with the following Object Identifier (OID): **1.3.159.1.4.1**

1.3 Participants to Public Key Infrastructure (PKI)

1.3.1 Certification Authority

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.

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

Company name:	**Actalis S.p.A.**
Registered Office:	**Via dell'Aprica, 18 – 20158 Milan, Italy**
Legal representative:	**Giovanni Utili** (President)
VAT Reg. No. and Tax Code:	**03358520967**
Telephone (switchboard):	**+39 02 68825.1**
DUNS number:	**440-489-735**
ISO Object Identifier (OID):	**1.3.159**
Corporate web site (information):	http://www.actalis.it
Certification service web site:	https://portal.actalis.it
E-mail address (information):	info@actalis.it
Directory server (certificate register):	ldap://ldap.actalis.it

1.3.2 Registration Authorities

The Registration Authority (RA) is a person, structure or organisation that is responsible for the following:

- collection and validation of certification requests and certificate management requests;
- registration of the applicant and organisation to which the same belongs;
- authorise issuance, by CA, of the certificate requested;
- provide the Client with the certificate and relevant information.

The RA activities are normally performed by Actalis, but in certain circumstances these can be delegated to other parties based on a specific "delegation agreement".

1.3.3 End users (subscribers)

The end users, namely the subscribers, of the certificates are organisations or entities requesting an SSL Server certificate or Code Signing certificate (digital signature of software code) and holding the private key.

The contract with the CA is normally stipulated by the subscriber as the client. Nonetheless the client (the entity which pays the certificate and its subsequent management by CA) may be allowed to act in the name of and on behalf of the subscriber of the certificate, a circumstance which must be demonstrated by the interested parties upon application (refer to section 3.2.2).

1.3.4 Relying parties

Relying Parties are recipients of a certificate who act on reliance on the information contained in the certificate. In the case of an SSL Server certificate, these are the users of the relevant web site. For Code Signing certificates, these are users of the signed software.

1.4 Use of certificates

The SSL Server certificate is used to activate the TSL/SSL protocol on a web site.

The Code Signing certificate is used for the digital signature of software (executable code).

Any other use of the certificates issued by Actalis in accordance with this CPS is strictly prohibited and shall bring about, as soon as Actalis gets aware, the immediate revocation of the certificate.

It is assumed that the client possesses the competence and instruments required to use the certificate. If this is not the case, Actalis is available to provide all the necessary assistance as consultancy.

1.5 Administration of CPS

This CPS is developed, reviewed, published and updated by Actalis.

For further information about this CPS, not found in this document, send an e-mail to the following address: cps-admin@actalis.it.

This CPS is approved by the Actalis' Security Manager, in full collaboration with Management, subject to consultation with the other company departments involved in the issuance of the service.

1.6 Definitions and acronyms

CA	Certification Authority
CCIAA	Chamber of Commerce, Industry, Crafts and Agriculture
CCTV (TVCC)	Closed Circuit TV
CNIPA	Italian Authority for Informatics in the Public Administration
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DN	Distinguished Name
DPC (CED)	Data Processing Centre
FIPS	Federal Information Processing Standard
HSM	Hardware Security Module
HTTP	Hyper-Text Transfer Protocol
I&A	Identification and Authentication
ISO	International Standards Organization
LDAP	Lightweight Directory Access Protocol
OCSP	On-line Certificate Status Protocol
OID	Object Identifier
PDF	Portable Document Format
PKI	Public Key Infrastructure
RA	Registration Authority
SSL	Secure Sockets Layer
TLS	Transport Layer Security
UPS	Uninterruptible Power Supply
VMD	Video Motion Detection

1.7 List of references

[DLGS196] Legislative Decree n.196 of 30 June 2003 “Personal data protection code”, published in the Supplemento Ordinario n.123 of the Gazzetta Ufficiale n.174 of 29 July 2003.

[RFC2251] Wahl, M., Howes, T., and S. Kille, "Lightweight Directory Access Protocol (v3)", RFC 2251, December 1997. (http://www.ietf.org/rfc/rfc2251.txt)

[RFC2314] Kaliski, B., "PKCS #10: Certification Request Syntax Version 1.5", RFC 2314, March 1998. (http://www.ietf.org/rfc/rfc2314.txt)

[RFC2560] Myers, M., R. Ankney, A. Malpani, S. Galperin and C. Adams, "Online Certificate Status Protocal - OCSP", June 1999. (http://www.ietf.org/rfc/rfc2560.txt)

[RFC2616] [RFC2616] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P. and T. Berners-Lee, "Hypertext Transfer Protocol, HTTP/1.1", RFC 2616, June 1999. (http://www.ietf.org/rfc/rfc2616.txt)

[RFC2818] Rescorla, E., "HTTP Over TLS", RFC 2818, May 2000. (http://www.ietf.org/rfc/rfc2818.txt)

[RFC3647] Chokhani, S., Ford, W., Sabett, R., Merrill, C., and S. Wu, "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", RFC 3647, November 2003. (http://www.ietf.org/rfc/rfc3647.txt)

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, May 2008. (http://www.ietf.org/rfc/rfc5280.txt)

[X.509] ITU-T Recommendation X.509 (2005) | ISO/IEC 9594-8:2005, Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks. (http://www.iso.ch)

2. PUBLICATIONS 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 CPS.

2.1 Repository management

The Actalis repository consists of:

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

The CA manages the repository and is directly responsible for the same.

2.2 Published information

As a minimum, the CA publishes the following documentation on its own web site:

- Certification Practice Statement (CPS)
- general terms and conditions of the service
- maximum fees charged for the service
- request forms

Furthermore, the CA publishes the certificates and the CRL on its own directory server.

For further information about the CRL refer to section 4.10.

2.3 Time and frequency of publications

The CPS and associated documentation are published in PDF format on the CA web site each time they are updated.

The certificates are published on the directory server as soon as they are issued.

For further information about the CRL refer to section 4.10.

2.4 Access control

Anyone can freely access the repository in read-only mode.

Access to the repository for the publication of new and updated information is only possible from work stations directly connected to the repository local network, subject to authentication.

3. IDENTIFICATION AND AUTHENTICATION (I&A)

3.1 Naming rules

The *subject* field of the certificate must contain information which is easy to understand and allows the subscriber organisation of the certificate to be identified. Pseudonyms or alternative names to the company name (or other official name) of the Client are not allowed.

The *country* component in the subject field must contain the ISO 3166 two-letter code (e.g. "IT" for Italy) which identifies the country to which the subscriber organisation of the certificate belongs.

The *organizatioName* component of the field must contain the official name (i.e. company name) of the certificate subscriber organisation. The name must be unique and not lead to ambiguity. In order to resolve a possible ambiguity, the CA may request that the name is followed by the tax code of the organisation or other useful information.

In the case of an SSL Server certificate, the *commonName* component of the subject field must contain the correct web server address (numeric or symbolic). A valid example is "www.example.com".

In the case of a Code Signing certificate, the *commonName* component of the subject field may contain any phrase whatsoever, proposed by the applicant, provided that it cannot lead Relying Parties to mistake the identity of the subscriber and the objectives/functionality of the signed software. A valid example is "ACME Code Signing".

The Clients shall not be able to use names in the certificate applications which violate the intellectual property rights of others. Actalis shall not be involved in any controversy whatsoever concerning the copyright of domain names, commercial names, commercial trademarks or services. Actalis reserves the right to reject the certificate application (or revoke an already issued certificate) in case of such a controversy.

3.2 Initial identity validation

3.2.1 Proving possession of private key

The proof-of-possession, by the applicant, of the private key corresponding to the requested certificate is based on the cryptographic verification of the CSR (Certificate Signing Request) sent to the CA. In fact the applicant must send its own public key to the CA in the form of a CSR in PKCS#10 format [RFC2314]. The CA shall verify that the digital signature in the CSR is valid.

Transmission of the CSR to the CA is normally done over the web (https://portal.actalis.it) or via electronic mail.

3.2.2 Authentication of organisation identity

Authentication of the identity of the applicant organisation includes in any case a lookup in the relevant CCIAA (Chamber of Commerce, Industry, Crafts and Agriculture) database. The name of the organisation declared by the client must correspond with the company name as registered in the chamber of commerce. In case of mismatch, the certificate application shall be rejected.

3.2.3 Authentication of individual identity

The individual identities indicated in the certificate application are verified over the phone, by contacting the person declared as "requestor" in the certificate application form.

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

3.3 Further verifications by the CA

In the case of SSL Server certificates, the CA shall also lookup the WHOIS record to verify that the owner organisation of the domain is the same as the applicant. In the case when the details do not match the application shall be rejected. Nonetheless, it is possible that the owner organisation has

delegated the management of its domain to the party applying for the certificate. In this case, the application shall be accepted if a proof of such delegation is provided to the CA (i.e. copy of registration application for the domain sent to the manager by the owner organisation of the domain).

In the case of Code Signing certificates, it is not allowed that the certificate be requested by an organisation different than the one to which the certificate is to be attributed: client and subscriber must coincide.

The CA reserves the right to perform any further verification as required.

3.4 Information not verified by the CA

The CA does not verify the electronic mail address indicated in the application form.

In general, the CA does not verify the correctness of any information received from the applicant which is not intended to be used in security-sensitive fields of the certificate and which is not necessary for the issue and subsequent management (suspension, re-activation, revocation) of the certificate.

3.5 I&A for renewal applications

The renewal process is similar to the first issuance process. It consists in the generation of a new pair of keys, by the subscriber, to replace the expired pair and a request to the CA for a new certificate. The same identification and authentication processes (I&A) as used for first issuance are also followed for the renewal.

3.6 I&A for requests to suspend or revoke

The methods for identification and authentication of the requests to suspend or revoke a certificate depend on the channel which is used for the request:

- in order to be able to submit suspension or revocation requests through the CA services portal, it is necessary to "login" to the portal by means of a userid and password (these credentials are supplied to the client upon issuance of the certificate);
- in the case of suspension or revocation requests sent to the CA on paper, the procedures as described in paragraph 3.2.3 shall be followed.

4. CERTIFICATE MANAGEMENT OPERATIONAL REQUIREMENTS

4.1 Certificate application

The certificate application may take place in two different ways:

- by filling-out and submitting the on-line application form on the CA web site https://portal.actalis.it;
- by filling-out and sending the application form to the CA (via fax, e-mail, ordinary mail).

The certificate application shall at least include the following information:

- details of applicant organisation
- personal and contact details (e-mail, telephone) of applicant

- personal and contact details (e-mail, telephone) of a “technical reference”
- address of the web site to be included in the certificate (for the SSL Server certificates)
- value proposed for commonName field (for Code Signing certificates)

The certificate application must be accompanied by the **CSR** (Certificate Signing Request). In the case of an application on paper, the CSR can be subsequently sent to the CA via electronic mail, to the address provided by the registration manager.

The CSR is normally generated by the applicant organisation by its own means.

It is also possible to request a “wildcard” SSL Server certificate (i.e., valid for all web sites belonging to a specific domain) or a “multi-host” /”multi-domain” type (i.e., valid for various web sites, even on different domains). In these cases different procedures and specific fees are applied. For further information please contact the Actalis commercial offices.

4.2 Application processing

Upon receipt of the certificate application, the RA shall perform the following:

- insert the applicant data in the registration database;
- verify that the identification data contained in the CSR are coherent with that supplied in the application form;
- verify the identity of the applicant and possession of the private key corresponding to the CSR, as described in section 3.2;
- perform the additional verifications described in section 3.3.

Registration of the applicant consists in the storing, in the CA database, of the identification and contact data (telephone, e-mail) of the applicant organisation and person requesting the certificate (normally the legal representative, for example a director with powers of signature).

4.3 Issue of certificates

If the verifications above are successful, the CA shall generate the certificate, store it in its database and publish it on its own directory server (ldap://ldap.actalis.it).

Subsequently, the CA sends the following to the client via e-mail:

- subscriber certificate
- certificate of issuing CA
- accompanying documentation
- credentials (userid, password) for accessing the restricted area of the CA services portal (https://portal.actalis.it), for suspension/re-activation or revocation of the certificate.

At this point, if the certificate has not already been paid for, the CA will issue the invoice and submit this to the client.

4.4 Certificate acceptance

The certificate is intended as accepted after 30 days from the date of delivery, as certified by the date of the electronic mail message by means of which the same is sent to the client, if no notice is received to the contrary from the client.

Public use of the certificate (i.e. installation on a web site with public access, signature of executable code that can be downloaded from public access web sites), even if temporary, shall in any case imply acceptance of the certificate by the subscriber.

In the case when the certificate contains incorrect information due to an incorrect filling-out of the application form by the client, this shall in any case be paid for.

4.5 Use of key pairs and certificate

The subscriber shall use the private key:

- (Code Signing certificates) to digitally sign proprietary executable code (e.g. Java applets, dynamic libraries, etc.) and/or code for which the same is responsible;
- (SSL Server certificates) to activate the TLS/SSL protocol on its own web site, thereby allowing server authentication and encryption of the transactions with web browsers.

The relying parties shall use the certificate:

- (Code Signing certificates) to verify the integrity and origin of the executable code;
- (SSL Server certificates) to verify the identity of a web site and the organisation which manages the site, as well as to exchange the “session key” with the web server in a safe manner.

See also paragraph 1.4.

4.6 Certificate renewal

The certificate has an expiry date beyond which it is no longer valid. The reason for which the certificate has a limited duration is that the security of a pair of encryption keys could decrease over time or even be compromised, due to the effect of cryptanalytic techniques and attacks by criminals. For these reasons Actalis does not renew a certificate, unless the client generates a new pair of keys. Apart from this condition, the renewal process is the same as the first issue process.

4.7 Key re-generation

In the case when the final user (subscriber) decides to use a new key, the same shall request a new corresponding certificate.

4.8 Certificate modification

Since the certificate is signed by the issuing CA, it cannot be “modified”. Thus, to solve a possible certificate generation problem, it is necessary to issue a new one (and revoke the incorrect one for obvious security reasons).

In the case when the issued certificate contains incorrect information due to errors committed by the CA or the RA (if this latter is a separate entity), the incorrect certificate shall be revoked and a correct one will be promptly issued without additional costs for the client and without asking the client for additional information.

In the case when the issued certificate contains incorrect information due to errors committed by the applicant (i.e. incorrect filling-out of one or more fields of the application form), the incorrect certificate shall be revoked.

4.9 Certificate suspension and revocation

The suspension of the certificate determines a temporary suspension of the validity of a certificate, starting from a given moment in time (date/time). Once a certificate has been suspended, it can be re-activated at any time.

Revocation determines the premature termination of the validity of a certificate, starting from a given moment in time (date/time). Revocation of a certificate is irreversible and not retroactive.

Implementation of the suspension or revocation consists in the generation and publication of a new CRL (Certificate Revocation List) which includes the serial number of the suspended or revoked certificate. The CRL is accessible to anyone needing to verify the certificate status (refer to section 4.10).

Re-activation consists in the generation and publication of a new CRL in which the serial number of the previously suspended certificate does not appear.

4.9.1 Reasons for suspension

The conditions which could cause a suspension are as follows:

- suspected compromise of private key;
- temporary interruption of the use of the certificate by the client;
- breaches of contract by the client (e.g. failure to pay).

4.9.2 Request for suspension

Suspension can be requested by the client and/or subscriber of the certificate or by the CA.

Under certain circumstances the subscriber *shall be obliged* to request suspension of the certificate (refer to paragraph 9.5.3).

Suspension can be performed directly by the CA when the same becomes aware of conditions which could compromise the reliability of the certificate or which constitute contractual non-fulfilments by the client.

4.9.3 Suspension procedure

Suspension can be requested by the subscriber on-line (refer to paragraph 4.9.6).

Following a period of 15 days after suspension the certificate will be re-activated automatically.

The certificate may also be re-activated by the user, at any moment in time, via the CA services web portal, subject to authentication.

4.9.4 Certificate revocation

The conditions which may cause a revocation request are as follows:

- registration errors;
- measures taken by authority;
- suspected compromise of private key;
- failure to comply with the CPS (i.e. this document);
- changes of the information included in the certificate (i.e. name of subscriber company);
- illegal activities by the certificate subscriber company;
- termination of activity by certificate subscriber company;
- requested by subscriber (i.e. motivated by discontinued use of the certificate);
- breach of contract by the client (e.g. failure to pay).

4.9.5 Revocation request

Revocation can be requested by the client and/or subscriber of the certificate or by the CA.

Under certain circumstances the subscriber *shall be obliged* to request revocation of the certificate (refer to paragraph 9.5.3).

Revocation can be performed directly by the CA when the same becomes aware of conditions which could compromise the reliability of the certificate or which constitute contractual non-fulfilments by the client.

4.9.6 Revocation procedure

Requests for suspension and revocation may be submitted to the CA through the Actalis services web portal at address https://portal.actalis.it. To access this function it is necessary to “login” to the portal, and thus the client will need the access credentials sent to him/her together with the certificate.

As an alternative, it is possible to use a paper request form signed by the client’s representative. The signed form may be delivered to the RA by hand or sent directly to the CA (via fax, ordinary mail, electronic mail).

The CA shall inform the client about the suspension or revocation by means of sending an e-mail to the address of the “technical manager” indicated in the application form.

4.9.7 Frequency of issue of CRL

See paragraph 4.10.1.

4.10 Certificate status information

The status of the certificates (active, suspended, revoked) is available to all interested parties through the publication of the Certificate Revocation List (CRL) in the format defined in the specification [RFC5280].

The CA reserves the right to provide an OCSP (On-line Certificate Status Protocol) service in compliance with the specification [RFC2560], the characteristics of which are not specified in this document.

4.10.1 Operational characteristics

The CRL can be accessed in two different ways:

- via LDAP protocol [RFC2251] on server ldap.actalis.it
- via HTTP protocol [RFC2616] on server portal.actalis.it

The LDAP and HTTP complete addresses for the CRL are inserted in the *CRLDistributionPoints* extension of the certificate.

The CRL is re-generated and re-published:

- at least every 6 hours, even in the absence of new suspensions or revocations;
- following each new suspension or revocation.

The OCSP server address is inserted in the *AuthorityInformationAccess* extension of the certificate.

The CRL and OCSP services can be accessed by anyone.

4.10.2 Service availability

Access to the CRL and OCSP service is continuously available (24 x 7), except in the cases of scheduled maintenance of the machines or in the case of faults. See also paragraph 9.16.

4.11 Contract termination

The service contract stipulated between the CA and client is intended as terminated:

- at the natural expiry date of the certificate, or...
- at the date when the certificate has been revoked (refer to section 4.9).

4.12 Key escrow and recovery

The term “key escrow” is intended as the consignation of the CA key pair to a trusted third party (e.g. notary public). Within the framework of the service provided by Actalis in accordance with this CPS, the escrowing of the CA key is not contemplated.

However, key recovery of the CA key is provided, in the case of unintentional cancellation of fault in the HSM. In order to allow key recovery, the CA keeps a backup CA key pair (refer to paragraph 6.8).

5. PHYSICAL AND OPERATIONAL SECURITY CONTROLS

The technological infrastructure, operating procedures, physical and logical security controls and personnel responsible for providing the service described in this CPS are the same as those used within the Actalis service for issuing qualified certificates (according to EU directive on electronic signatures).

5.1 Physical security

The Actalis electronic data centre DPC (CED) is located in the basement at the registered offices in Via Taramelli 26.

Access to the technical room is only permitted to authorised personnel subject to identification through an access badge and corresponding PIN.

There are passive anti-intrusion systems fitted on the inside and outside of the building such as bars, bullet-proof glasses, steel reinforced doors, motorised gates and CCTV and VMD anti-intrusion control systems.

The computer control room, manned continuously 24 hours a day, is fitted with a centralised alarm system.

The fire-prevention system is realised in compliance with UNI 9795 Norm. The fire detections sensors are installed on all floors of the building.

The entire building is provided with static and dynamic uninterruptable Power Supply units, and in particular:

- UPS units to guarantee power supply to all the systems connected until the emergency generator starts or, when this is not available, for at least one hour;
- emergency generator (diesel generator set) to guarantee continuous power supply even for several days.

An additional guarantee is provided by withdrawing medium voltage from two different power supply stations.

5.2 Procedural controls

Actalis maintains a Security Plan which analyses the assets and describes the technical and organisational controls aimed at assuring an adequate level of security for the operations.

All the standard operational procedures are documented and included in the Actalis Quality Management System, certified in accordance with ISO 90001 Standard.

5.3 Personnel controls

Personnel involved in the service have at least 5 years of working experience in the definition, development and management of PKI services and have been adequately trained on the procedures and tools to be used during the various operational phases.

5.4 Event logging

The main events relevant to the certificate lifecycle operations, including the requests for certification, suspension or revocation etc., are registered on paper or in electronic form. Furthermore, events like the following are also recorded: logical access to the certificate management system, operations carried out by Actalis personnel, presence of visitors at areas where certification activities are performed etc.

For each event, information is logged about the type, date and time of occurrence and, if available, other information useful to identify those involved in the event and the outcome of the operations.

All this information constitutes the audit log. The files of this audit log are transferred on a daily basis to a permanent backup support.

5.5 Data retention and archival

The CA keeps the following information related to the certificate issuing and management processes:

- requests for the issuing of certificates

- documentation supplied by the applicants
- CSR (Certificate Signing Request) supplied by the applicants
- personal details of the applicants and subscribers (when the two are different)
- results of verifications performed by the CA (Chamber of Commerce Enquiries, WHOIS Records)
- suspension or revocation requests
- all certificates issued

5.6 Renewal of CA key

Within 90 days before the end of the period of validity of the current certification key, Actalis will generate a new CA key pair and distribute this to the users in accordance with the methods described in section 6.2.1. From this moment on, the new certificates and the new CRLs shall be signed with the new key.

5.7 Backup copy

A backup copy of data, applications, audit log and any other file necessary for a complete recovery of the service is performed on a daily basis.

Data backup is made to magneto-optical disks which are kept in a reinforced steel cabinet located in a different area to where the backup operations are performed.

5.8 Compromise and disaster recovery

The term “compromise” is intended as the violation of one or more of the binding conditions necessary for providing the service while “disaster” is intended as a damaging event, the consequences of which determine the unavailability of the service under normal conditions. Following a compromise or disaster, special procedures shall be applied for the recovery of the certification services.

These procedures are described in detail in the Security Plan (confidential document, which can be viewed at the offices of Actalis upon request by the client).

In any case, recovery after compromise or disaster takes place for the following situations:

- faults in one or more of the computer resources used to provide the certification services;
- compromise (i.e., compromise of security by disclosure to unauthorised third parties or the loss) of one or more private certification keys.

6. TECHNICAL SECURITY CONTROLS

The technological infrastructure, operating procedures, physical and logical security controls and personnel responsible for providing the service described in this CPS are the same as those used for the Actalis service for issuing qualified certificates (according to the EU directive on electronic signatures).

6.1 Key generation

6.1.1 CA keys

The key pair used by the CA to sign the certificates and CRLs is generated inside a high quality HSM (Hardware Security Module), with a security certification in accordance with FIPS PUB 140-2 Level 3.

6.1.2 Subscriber keys

The applicant normally generates its own key pairs by his/her own means.

6.2 Distribution of public key

6.2.1 CA keys

As a minimum, the CA public key is distributed in the following ways:

- by means of publication on the CA directory server (ldap://ldap.actalis.it)
- by means of publication on the CA web site (https://portal.actalis.it)

6.2.2 Subscriber keys

The public key of the certificate requestor is supplied to the CA in the form of a Certificate Signing Request (CSR) in compliance with PKCS#10 [RFC2314].

6.3 Key size

6.3.1 CA keys

To sign the client certificates and the CRLs, Actalis uses keys having a module size of 2048 bit.

6.3.2 Subscriber keys

The module of subscriber keys shall have a size comprised between 1024 and 2048 bit.

6.4 Parameters generation and key quality

6.4.1 CA keys

The CA uses a cryptographic key pair generated with the RSA algorithm, with a public exponent equal to 65537 (Hex 0x10001).

6.4.2 Subscriber keys

Normally, the certificate subscriber uses a cryptographic key pair generated with the RSA algorithm.

The CA does not undertake to certify user keys generated with other algorithms (e.g. DSA, ECDSA).

6.5 Key usage (X.509v3 extension)

The CA certificate includes KeyUsage extension with the appropriate values which indicate the purpose of the private key:

- keyCertSign (sign certificates)
- cRLSign (sign CRLs)

6.6 Protection of private key

The key pair used by the CA to sign the certificates and CRLs is kept inside a high quality HSM (Hardware Security Module), provided with a security certification in accordance with FIPS PUB 140-2 Level 3.

6.7 Security Standard for cryptograph modules

The HSMs (Hardware Security Modules) used by the CA shall be provided with a security certification in accordance with FIPS PUB 140-2 Level 3.

6.8 Backup and recovery of private key

For the purpose of guaranteeing continuity of service, the CA keeps an encrypted backup copy of keys on removable support media. The backup copy is kept in a safe place which is different than the location of the operational copy (inside the HSM).

6.9 Key activation data

The CA activation PIN for the HSM is only known by the personnel responsible for operational management of the service, under the responsibility of the Certification Manager.

6.10 Computer security requirements and controls

The operating systems used by the CA for management of the certificates are provided with a security certification in accordance with ITSEC Level E2 HIGH or equivalent. The operating systems are configured so that the user is always required to identify him/herself by means of a username and password or, in the case of more critical systems, via the use of a smartcard and corresponding PIN. The access events are logged as described in section 5.4.

6.11 Network security

Access to the CA on-line hosts is protected by high quality firewalls which guarantee an adequate filtering of the incoming connections. Before the firewalls, a series of routers which implement suitable ACLs (Access Control List) constitute further protection. All the communication ports of the certification servers which 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 communications the entire certification system is split-up into an external area, internal area and a Data Management Zone (DMZ).

Actalis carries out an annual security assessment to verify the presence of any network vulnerabilities by involving independent experts.

6.12 Clock synchronisation

All the computer systems used by the CA are synchronised with a time server which in turn is synchronized from an external GPS satellite network.

7. CERTIFICATE AND CRL PROFILES

7.1 Certificate profile

The certificates conforms to the ISO/IEC 9594-8:2005 [X.509] standard and to the [RFC 5280] public specification.

7.1.1 CA certificate

The profile of the issuing CA certificate is as follows:

Field	Value
Version	V3 (2)
SerialNumber	1
Signature	sha-1WithRSAEncryption (1.2.840.113549.1.1.5)
Issuer	CN = Actalis Authentication CA G1 O = Actalis S.p.A./03358520967 L = Milan, Italy C = IT
Validity	from 23 June 2009 to 25 June 2022
Subject	CN = Actalis Authentication CA G1 O = Actalis S.p.A./03358520967 L = Milan, Italy C = IT
SubjectPublicKeyInfo	<public key RSA algorithm 2048 bit>
SignatureValue	<CA signature>
Extension	**Value**
Basic Constraints	critical: CA=true, PathLen=0
AuthorityKeyIdentifier (AKI)	<not included>
SubjectKeyIdentifier (SKI)	01 BB D6 9B 56 B4 7E E6 C5 58 DD 2C 98 F4 CA 72 F6 5F 33 86
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 SSL Server certificate

The SSL Server certificate is issued with the following profile:

Field	Value
Version	V3 (2)
SerialNumber	<unique whole number>
Signature	sha-1WithRSAEncryption (1.2.840.113549.1.1.5)
Issuer	<DN of issuing CA>
Validity	<1 or 2 years depending on request>
Subject	countryName = <ISO 3166 two-letter code of country where the subscriber organisation resides> organizationName = <name of subscriber organisation> organizationalUnitName = <optional> commonName = <web server address>
SubjectPublicKeyInfo	<public key RSA algorithm 1024 or 2048 bit>
SignatureValue	<CA signature>
Extension	**Value**
Basic Constraints	<not included>
AuthorityKeyIdentifier (AKI)	<issuing CA SKI extension value>
SubjectKeyIdentifier (SKI)	<public key digest SHA1>
KeyUsage	critical: digitalSignature, keyEncipherment
ExtendedKeyUsage (EKU)	serverAuth (1.3.6.1.5.5.7.3.1), clientAuth (1.3.6.1.5.5.7.3.2)
CertificatePolicies	PolicyOID = 1.3.159.1.4.1 CPS-URI = <HTTP address of CPS>
SubjectAlternativeName (SAN)	<normally not included>
AuthorityInformationAccess (AIA)	<OCSP server address, optional>
CRLDistributionPoints (CDP)	<HTTP address to access the CRL> <LDAP address to access the CRL>

The CA reserves the right to include further information and/or extensions in the certificate provided that this is in compliance with the public specification [RFC5280] and by safeguarding the functionality of the certificate for the proposed usage.

7.1.3 Code Signing certificate

The Code Signing certificate is issued with the following profile:

Field	Value
Version	V3 (2)
SerialNumber	<unique whole number>
Signature	sha-1WithRSAEncryption (1.2.840.113549.1.1.5)
Issuer	<DN of issuing CA>
Validity	<1 or 2 years depending on request>
Subject	countryName = <ISO 3166 two-letter code of country where subscriber organisation resides> organizationName = <name of subscriber organisation> organizationalUnitName = <optional> commonName = <value proposed by subscriber>
SubjectPublicKeyInfo	<public key RSA algorithm 1024 or 2048 bit>
SignatureValue	<CA signature>
Extension	**Value**
Basic Constraints	<not included>
AuthorityKeyIdentifier (AKI)	< issuing CA SKI extension value>
SubjectKeyIdentifier (SKI)	<public key digest SHA1>
KeyUsage	digitalSignature
ExtendedKeyUsage (EKU)	codeSigning (1.3.6.1.5.5.7.3.3)
CertificatePolicies	PolicyOID = 1.3.159.1.4.1 CPS-URI = <HTTP address of CPS>
SubjectAlternativeName (SAN)	<subscriber e-mail address>
AuthorityInformationAccess (AIA)	<OCSP server address, optional>
CRLDistributionPoints (CDP)	<HTTP address to access the CRL> <LDAP address to access the CRL>

The CA reserves the right to include further information and/or extensions in the certificate provided that this in compliance with the public specification [RFC5280] and by safeguarding the functionality of the certificate for the proposed usage.

7.2 CRL profile

The CRLs are compliant with the with the ISO/IEC 9594-8:2005 [X.509] International Standard and public specification [RFC 5280].

Besides the mandatory information, the CRLs also contain:

- *nextUpdate* (date for next issue of CRL)
- *cRLNumber* (sequential number of CRL)

Moreover, in correspondence with each item of the CRL there is a *reasonCode* extension to indicate the reasons for suspension or revocation.

8. COMPLIANCE AUDIT

The technological infrastructure, operating procedures, physical and logical security controls and personnel responsible for providing the service described in this CPS are the same as those used for the Actalis service for issuing qualified certificates according to the EU directive on electronic signatures.

Actalis is a qualified certification service provider, accredited by CNIPA. Consequently, Actalis is subject to a *periodic conformity assessment* ("supervision") by CNIPA and is also obliged to carry out *periodic internal audits*.

8.1 Frequency and reason for audit

The external audits performed CNIPA are carried out every 18 months.

The internal audits are carried out in accordance with a schedule which provides different periods (from monthly to annual) for the various technical-operational aspects of the CA service.

Audits on external RAs are carried out at least once per year.

8.2 Identity and qualification of inspectors

The internal audits are carried out by the Actalis Auditing Manager, qualified as security auditor in accordance with ISO 27001 Standard ("Information technology - Security techniques - Information security management systems - Requirements").

Audits on external RAs are carried out by Actalis' Auditing Manager.

8.3 Relationship between CA and Inspectors

There is no relationship between the CA and CNIPA which can influence the outcome of the audits in favour of Actalis.

The Actalis Auditing Manager is an employee reporting directly to management and is therefore independent from the organisational structure responsible for providing the CA service.

8.4 Audit activities

The purpose of the audit carried out by CNIPA is to verify, from a technical and organisational point of view, the compliance of the CA service provided by Actalis with applicable law. The CNIPA auditing is based on Guide Lines conformant to the European standard ETSI TS 101 456 ("Policy requirements for certification authority issuing qualified certificates").

The main objective of the internal audit is to verify the integrity of the audit log and compliance of the CA operating procedures.

Audits on external RAs aim at verifying the respect, by each audited RA, of the delegation agreement (see section 1.3.2).

8.5 Actions related to non-compliances

In the case of non-compliances, the CNIPA will ask the CA to adopt the necessary corrective measures within a certain period of time, under penalty of suspension or revocation of the accreditation.

Regarding external RAs: in the event that an RA is found not to comply with the delegation agreement, a period of time is agreed between Actalis and the RA wherein the non-compliances must be resolved. Should the RA fail to resolve the problems within the established deadline, Actalis revokes the RA credentials that are necessary to gain access to Actalis' on-line registration services. Further actions are then negotiated between Actalis and the offending RA. In the event that Actalis has suffered any damage as a consequence of the RA's misconduct, section 9.8 applies.

8.6 Notification of audit results

The result of the audits carried out by CNIPA is shared with the CA in question through the issue of an audit report.

The result of the internal audit is submitted to Management and the various managers of the organisational structure responsible for providing the CA service.

9. GENERAL TERMS AND CONDITIONS

The "general terms and conditions of service" are supplied to the user in a separate document, to be accepted during the application phase, which is available from the CA web site (refer to 2.2).

In the case of a discrepancy between the content of this CPS and the separate document "general terms and conditions of service", the CPS will have precedence in law.

9.1 Service fees

The *maximum* service fees are published on the CA web site: http://portal.actalis.it.

Different conditions may be negotiated case by case, in accordance with the volumes requested.

Service fees are subjected to change without prior notification.

9.2 Financial responsibility

Actalis has stipulated a particular insurance policy to cover risks and possible damages deriving from the provision of the certification service.

9.3 Privacy of personal data

Actalis is the processor of the personal data collected during the identification and registration phase of parties requesting the certificates, and shall be obliged to process such information with the maximum confidentiality and in compliance with the provisions of Italian Ministerial Decree 196/2003 [DLGS196].

In the case when the identification and registration of the users take place at a delegated (RA) structure, the latter is qualified as the "autonomous correlated data controller".

9.3.1 Information pursuant to Legislative Decree 196/03

Actalis, processor of the personal data provided by the subscriber, informs the subscriber that, pursuant to Ministerial Decree 196/2003 [DLGS196], this personal data shall be processed by means of paper archives and information systems suitable to guarantee the security and confidentiality in conformance with the aforesaid Decree.

The information supplied by the applicant falls into two categories: mandatory and optional. The mandatory information is necessary for the carrying out of the service; failure by the subscriber to provide this information will not allow the contract to be concluded. Please note that publication of the certificate will cause the information contained in the certificates to be distributed to third parties, also in countries outside of the European Union. The optional information is used to assist in the service; failure by the subscriber to provide this information will not prevent the contract to be concluded.

The information provided by the applicant is processed exclusively for the purpose of issuing and renewing the certificates, and can be communicated to companies providing consultancy and technical assistance to Actalis. In relation to this data processing, the applicant shall be able to exercise the rights pursuant to the Decree [DLGS196].

9.3.2 Archives containing personal data

The archives containing personal data are:

- registration database
- paper archive

The aforementioned archives are managed by the registration manager and are suitably protected against unauthorised access.

9.3.3 Privacy protection measures

As a certifier, Actalis processes personal data and information in compliance with the provisions of Ministerial Decree 196 [DLGS196] and subsequent modifications and amendments, by putting into place security measures which, as a minimum, are in compliance with Chapter II ("Minimum security measures") of the Decree. In particular Actalis:

- develops and maintains a "data security plan" (DPS)
- adopts suitable measures to control access to the archives
- adopts suitable procedures for management of authentication credentials
- keeps a permanent audit log of access to the archives
- performs periodic backup of data for recovery purposes.

Limited to the service provided as in accordance with this CPS, the certifier does not process "confidential data" or "legal data" pursuant to article 4 of the Decree [DLGS196].

9.4 Intellectual property rights

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

The subscriber of the certificate keeps all the rights on its own commercial marks (brand name) and its own domain name.

With regards to the property rights of other data and information, the applicable law shall be applied.

9.5 Obligations and guarantees

9.5.1 Certification Authority

The CA shall:

- operate in compliance with this CPS;
- identify the applicants as described in this CPS;
- issue and manage the certificates as described in this CPS;
- provide an efficient suspension and revocation service for the certificates;
- guarantee that the subscriber, at the time when the certificate is issued, did possess the corresponding private key
- timely inform about any eventual compromise of its own private key;
- provide clear information about the procedures and requirements of the service;
- provide a copy of this CPS to anyone requesting the same;
- guarantee processing of personal data in compliance with applicable law;
- provide an efficient and reliable information service about the status of the certificates.

9.5.2 Registration Authority

In the case when the RA is an entity external to Actalis, the obligations of the RA are defined in the special delegation agreement. In any case, the RA shall:

- identity certificate requestors as described in section 3.2;
- perform the additional verifications described in section 3.3.

9.5.3 End users (subscribers)

End users, subscribers of the certificates, shall:

- read, understand and fully accept this CPS;
- request the certificate by the methods prescribed in this CPS;
- provide the CA with precise and true information during the registration phase;
- adopt appropriate technical and organisational measures to avoid compromise of their own private keys;
- guarantee the confidentiality of the reserved codes received from the CA;
- immediately request suspension of the certificate in the case of suspected compromise of their own private keys;
- immediately request revocation of the certificate in the case of confirmed compromise of their own private key;
- immediately request revocation of the certificate in the case when any of the information contained in the certificate (i.e. company name, web site address etc.) is no longer valid;
- immediately inform the CA, after issue and up to expiry or revocation of the certificate, of any changes in the information supplied during the application phase;
- stop using the certificate subsequent to its revocation, and shall also:
  - in the case of Code Signing certificates: immediately remove the signed software from the web site on which it is published;
  - in the case of SSL Server certificates: immediately remove the certificate from the web site on which it is installed.

Moreover, the subscribers of certificates shall:

- in the case of Code Signing certificates: not sign malicious software (e.g. spyware) and not describe the signed software in a misleading way with respect to its real functionality and purpose;
- in the case of SSL Server certificates: exclusively install the certificate on the proper web sites (as indicated in the certificate) and operate those web sites only for the purposes permitted by applicable law.

9.5.4 Relying parties

The relying parties, in other words all parties (different from the subscriber) who rely on the certificates issued according to this CPS, are required to:

- spend a reasonable effort to acquire a sufficient understanding of certificates and PKIs;
- verify the status of the certificates issued by Actalis according to this CPS, by accessing the information services described in section 4.10;
- only rely on a certificate which has not expired, or been suspended or revoked.

9.6 Exclusions

The CA has no further obligations and shall not be obliged to guarantee anything more than what is described in this CPS (refer to section 9.5.1) or prescribed by applicable law.

9.7 Limitations

The CA declines any responsibility for damages suffered by anyone due to the non-fulfilment, by the client or third parties, of one or more parts of this CPS.

The CA declines any responsibility for damages suffered by the client due to non-reception of communications from the CA as a consequence of an incorrect e-mail address supplied during the application phase.

Without prejudice to the mandatory provisions of law, Actalis shall only be held responsible, for any reason whatsoever deriving from this CPS, in the cases of malice or gross negligence.

9.8 Compensation

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

- false declarations in the certification request;
- failure to provide information about essential matters and facts due to negligence or with the objective of deceiving Actalis;
- use of names (for example, domain names, brand names) in violation of intellectual property rights.

RAs shall pay compensation of any damages suffered by Actalis as a consequence of their non respecting the delegation agreement and this CPS (see section 8.5).

9.9 Duration and termination

This CPS shall enter into force at the time it is published in the repository (refer to chapter 2) and shall remain in force until the time it is replaced with a new version.

9.10 Correspondence

Actalis accepts correspondence related to this CPS, to be sent with the methods indicated in paragraph 1.5, and shall respond within five working days.

9.11 Amendments

Actalis reserves the right to modify this CPS at any time whatsoever without prior notification.

9.12 Resolution of disputes

Any controversies deriving from this CPS between Actalis and the clients of the service shall be deferred to an arbitration committee. The seat of the arbitration shall be in Milan, Italy.

9.13 Applicable law

This CPS is subject to Italian Law and as such 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.

9.14 Compliance with applicable law

At the revision date of this CPS, Actalis is not aware of any legislation relevant to the services described herein. In any case this CPS shall be subject to applicable laws.

9.15 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.

9.16 Service levels

The CA services shall at least comply with the following service levels:

Application	Objective	Measurement basis
Directory server availability (24 x 7)	99.8 %	annual
Web portal availability (24 x 7)	99.8 %	annual
Certificate issuing time	max 5 working days in 95% of all cases	annual
Certificate suspension or revocation time (request through the CA web portal)	max 2 minutes in 95% of all cases	annual
Certificate revocation time (against request by fax, e-mail, ordinary mail)	max 3 working days in 95% of all cases	annual

Different service level may be negotiated case by case, according to certificate volumes.