Certification Practice Statement

SSL Server and Code Signing certificates

Andrea Sassetti
Firmato
digitalmente il
09/07/2024
17:48:38 CEST

Version: 5.15

Date: Jul 09, 2024

Certification Practice Statement

SSL Server and Code Signing certificates

Approved by: Andrea Sassetti

Document Code: MGA_A_93

Distribution: PUBLIC

Change History

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
14 June 2011	2.0.4	1.3.1, 3.1, 4.1	Updated Actalis' legal representative. Clarified I&A and pre-issuance checks for wildcard and multi-SAN certificates	AS
28 Sep 2011	2.1.0	all	Transition to a 2-level CA hierarchy (Root CA, SubCA). Added details about management of CA keys. Clarified that two-factor authentication is required for all accounts allowing certificate issuance. Clarified that certificate serial numbers include at least 8 random bytes. SHA-256 used for certificate and CRL issuance. Updated minimum key lengths.	AS
6 Nov 2013	2.2.3	all	Alignment to Italian CPS v2.2.3	AS
13 Nov 2013	2.2.4	all	Updated name of Actalis CEO in §1.3.1. New section 4.13 on certificate problem reporting. Modified §1.3.2 to cover Enterprise RAs. Addedd OV profiles in §1.4 and in chapter 7. Modified §3.1 for more clarity. Clarifications in §3.3 regarding checks. Clarifications on the use CNames in CRL and OCSP URLs.	AS
14 Feb 2014	2.2.5	all	CAB Forum compliance made explicit at beginning of chapter 3. Clarification about IDNs.	AS
03 Sep 2014	2.2.6	3.1.1, 4.13, 6.33	Clarified that hostnames are not allowed in Code Signing certificates. Added phone number for certificate problem reporting. Keys of 1024-bits are not allowed anymore.	AS
20 Oct 2014	2.2.7	all	Added support of DV (Domain Validated) certificates. Added digital signature as a means to validate individual identities. Correction of typos and some clarifications.	AS
9 Dec 2014	2.3	all	Correction of typos.	AS
13 Mar 2015	2.4	various	New section 1.3.5 (Resellers). Corrections and clarifications in §1.4 (Use of certificates), §4.1 (Certificate application), and §4.9.6 (Procedure for suspension and revocation).	AS
26 Aug 2015	2.5	various	New §1.3.5 (Resellers). Corrections in §1.4 (Use of certificates), in §4.1 (Certificate application), and in 4.9.6 (Procedure for suspension and revocation). Clarifications	AS

			on the URLs of CRL and OCSP services. Clarifications on support and assistance. Additional ways to validate domain control. Some paragraphs moved or renamed for better clarity. Dedicated SubCA for EV-class certificates. Addedd CAB Forum Policy OIDs to some EE certificate profiles.	
22 March 2016	2.6	1.3.1, 4.13	Modified coversheet after organizational changes. Changed company address and phone numbers.	AS
05 August 2016	2.7	1.4, 3.4	Clarification on .onion domains. Clarification on CAA Records.	AS
06 October 2016	2.8	1.3, 7	Clarifications on CAs. Inclusion of cAIssuers in the AIA certificate extension. Dedicated SubCA for DV-class SSL Server certificates.	AS
24 July 2017	2.9	1.7, 3.2, 4.3	Changed from ETSI 102 042 to 319 411-1 in References. CAA Records are now checked. For EV certs, handwritten signature allowed if authenticated by notary. Clarifications on validation of authority and on non-verified subscriber information.	AS
28 Aug 2017	3.0	4.3, 7.3	Correction of typos. New paragraph 7.3 with OCSP profile.	AS
22 Jan 2018	4.0	All	Restructuring and revision of the entire document for easier comparison with RFC 3647 and CABF Baseline Requirements. Clarified that certain types of certificates may be issued to individuals. Disclosure of a new Subordinate CA for OV certificates. Removed references to EV Code Signing certificate, not currently offered.	AS
27 Apr 2018	4.1	3.1.1, 3.2.2.5, 4.3.1, 7.1.2.3	Clarified that DV- and EV-class SSL Server certificates may not contain IP addresses. Added mandatory Certificate Transparency for all classes of SSL Server certificates	AS
23 Mag 2018	5.0	1.4, 1.5, 1.7, 4.6, 7.1.2.3, 5, 6, 8, 9	Expanded chapter 4 for better clarity. Revised chapters 5, 6, 8, 9 for alignment with other Actalis' CPSes. Added QWACs (Qualified Web Authentication Certificates). Updated normative references.	AS
28 Feb 2019	5.1	1.3.1	New Legal representative	AS
23 May 2019	5.2	1.3.1.2, 3.2.2.5, 4.9.1.1, 7.1.2.3, 7.1.4.2.1	Aligned with current version of [BR] and [EVGL]. Updated list of Subordinate CAs. Clarifications on certificate profiles. Correction of typos.	AS
29 Aug 2019	5.3	7.1	Added paragraph on applicability of Determinazione AgID n.121/2019	FC
26 Sep 2019	5.4	4.9.1.1, 7.1.2.3	Clarification on the revocation by the CA in case of any non-compliance of certificates to the BR and/or the EVGL. Added support for ECC keys (P256/P384) in Subscriber certificates.	AS
08 Oct 2019	5.5	7.1.2.2	Clarifications on EKU in SubCA certificates for compliance with the Mozilla Root Store Policy	AS
22 Jan 2020	5.6	1.3.1.2, 1.5.2, 3.2.2.4, 4.2.2, 4.10.3, 4.12.1,	Updated table of SubCAs. Clarifications in §3.2.2.4. Moved text of former §4.13 to §1.5.2 for compliance with the BR, then removed §4.13. Repeated in §4.2.2 that	AS

		4.12.2, 4.13, 5.6.2, 6.2.3, 7.1.4.2, 7.1.2.3	internal names are not allowed. Added §4.10.3, §4.12.1, and §4.12.2 for compliance with RFC3647. Revisions and corrections in some certificate profiles. Clarified that key escrow is not provided.	
15 Jul 2020	5.7	4.1.2, 4.9.5, 6.1.5, 6.3.2, 9.11	Update and specification of how to request the certificate. Details on the time for revocation. Accuracy on algorithms and key length of the Holders. Maximum validity of SSL Server certificates reduced to 398 days. Clarifications on assistance.	AS
5 Oct 2020	5.8	1.3.1.2, 1.4.2, 3.2.2.4	Updated list of intermediate CAs. Added warning about ICA embedding and certificate pinning. Updated list of supported DCV methods (added ACME http-01)	AS
22 apr 2021	5.9	1.1, 1.7, 6.1.2, 6.1.3, 6.1.5, 6.2.1, 9.6.1, 9.6.3, 3.2.2.1	Inserted reference to Code Signing Baseline Requirements. Updates for Code Signing certificates. Inserted reference to list of approved incorporating agencies.	AS
14 jun 2021	5.10	3.2.2.4, 3.2.2.8 4.9.12	Alignment with Mozilla Root Policy. Adaptation to CABF Ballot SC45. Adaptation to CABF Ballot SC46. Specified how to report a compromised private key to the CA.	AS
29 apr 2022	5.11	3.2.2.1; 3.2.2.3; 7.1.4.2.1; 7.1.4.2.2	Identity validation update Alignment in chapter numbering Update of SAN and FQDN policies	AS
10 Oct 2022	5.12	4.1.2 4.9.1.1	Update of the procedures for signing the request for EV certificates. Update of the circumstances for the revocation of a Subscriber Certificate	AS
17 May 2023	5.13	1.3.1.2, 3.1, 4.1.2, 5.5.2, 6.1, 6.2, 6.8, 7.1.2, 7.1.3, 7.1.4, 7.2, 9.6.1	Correction of small typos. Updated the Subordinate Certification Authorities table. Removed references to the "organizational-UnitName" (OU) attribute. Added clarifications for Code Signing certificates' enrollment process. Corrected the QWAC certificate profile. Clarified that Subject may be empty in DV SSL certificates. Changed requirements for private key protection and verification in the case of Code Signing certificates. Added information about Actalis' TSA. Clarified usage of CRLReason in CRL entries. Updated algorithm object identifiers. Changed retention period for records archival.	AS
16 May 2024	5.14	1.3.1.2, 1.6, 3.2.2.9, 3.2.5, 4.2.1, 6.2.7.4, 7.1, 7.1.2.2	Annual revision of the document. Subordinate CA 'Actalis DV Server ACME CA G1' added. Adaptation to BR 2.0.4 and EVGL 2.0.1. Correction of typos. Clarification of Code Signing certificates	AS, EDF
09 July 2024	5.15	1.1, 2.1, 4.2.1, 4.10.1, 6.7, 7	Correction of typos and some clarifications.	AS, EDF

Table of Contents

1. Introduction

1.1 Overview

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

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

The reliability of a certificate, in particular the association - attested by the certificate - between a given public key and a given identity, also depends on the CA's operating procedures, the obligations and responsibilities of the CA and the certificate Subscriber, and the CA's physical and logical security controls. All these aspects are described in a public document called **Certification Practice Statement** (CPS).

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

- SSL Server certificates
- Code Signing certificates

The structure of this CPS conforms to the public specification [RFC 3647].

As regards the **SSL Server** certificates regulated by this CPS, Actalis conforms to the current version of the **Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates** and the **Guidelines for Issuance and Management of Extended Validation Certificates** published at http://www.cabforum.org. In the event of any inconsistency between this CPS and those documents, those documents take precedence.

As regards the **Code Signing** certificates regulated by this CPS, Actalis conforms to the current version of the **Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates** published at http://www.cabforum.org. If there is any inconsistency between this CPS and those Requirements, those Requirements take precedence.

1.2 Document Identification

This document is the **Certification Practice Statement** (**CPS**) applying to **SSL Server and Code Signing certificates** issued by **Actalis S.p.A.** Version and time of last revision are indicated on the first page. This document is published on Actalis' web site in two languages: Italian and English. In the event of any inconsistency between the two versions, the Italian version takes precedence.

Actalis also issues other types of certificates (e.g., SSL Client, S/MIME) in compliance with policies described in separate documents. Those policies may refer to this CPS for all common aspects (e.g., infrastructure, organization, physical and operational security, etc.).

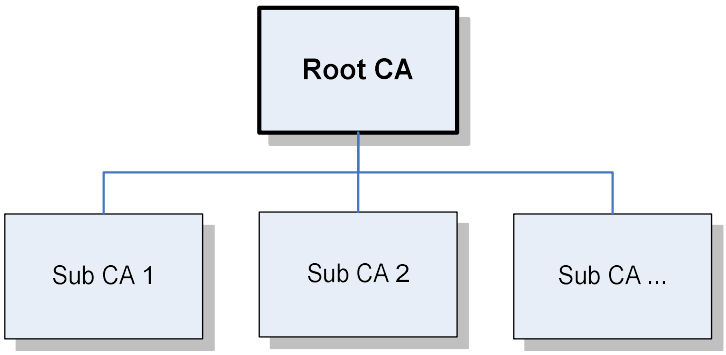
This CPS is published as a signed PDF document in order to ensure its origin and integrity.

1.3 PKI participants

1.3.1 Certification Authorities

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

The Actalis PKI (Public Key Infrastructure) that the SSL Server and Code Signing certificate issuance and management service is based upon is a two-level hierarchy, as shown in the following diagram:



The **Root CA** is used for issuing Sub CA certificates and related CRLs only, and is kept off-line when not in use, whereas end-entity certificates are issued by **Sub CA**s.

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

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

1.3.1.1 Root Certification Authorities

As anticipated, the role of Root CA is played by Actalis. As of the date of revision of this presente CPS, Actalis’ Root CA keys are those identified in the following table; for further details, see chapter 7.

Subject DN	Subject Key ID	notBefore	notAfter
CN = Actalis Authentication Root CA O = Actalis S.p.A./03358520967 L = Milan C = IT	52 d8 88 3a c8 9f 78 66 ed 89 f3 7b 38 70 94 c9 02 02 36 d0	22 September 2011	22 September 2030

1.3.1.2 Subordinate Certification Authorities

As of the date of revision of this CPS, the **Subordinate CAs run by Actalis** are those identified in the following table. For further details, see chapter 7.

Subject DN	Subject Key ID	notBefore	notAfter
CN = Actalis Organization Validated Server CA G3 O = Actalis S.p.A. L = Ponte San Pietro S = Bergamo C = IT	9F 8A B1 B5 F1 B1 DE 82 F4 27 7C BE 88 CD DE A9 43 81 A3 4B	6 Jul 2020	22 set 2030
CN = Actalis Extended Validation Server CA G3 O = Actalis S.p.A. L = Ponte San Pietro S = Bergamo C = IT	AB 41 73 F0 6F 50 D0 69 FD 73 17 AB 89 B3 6B 62 ED BD 7C 4B	6 Jul 2020	22 set 2030
CN = Actalis Domain Validation Server CA G3 O = Actalis S.p.A. L = Ponte San Pietro S = Bergamo C = IT	42 83 6D 80 7C 09 84 67 FD 80 57 AB F1 26 F5 77 C8 22 82 71	6 Jul 2020	22 set 2030
CN = Actalis DV Server ACME CA G1 O = Actalis S.p.A. L = Ponte San Pietro S = Bergamo C = IT	51 9A 91 1F D2 57 39 17 D9 B7 E2 26 83 BD 7B B4 B5 3F 38 8A	6 Jun 2023	22 Sep 2030
CN = Actalis Code Signing CA G2 O = Actalis S.p.A. L = Ponte San Pietro S = Bergamo C = IT	78 07 05 52 0B A3 D8 C8 4B 41 3D 4F CF 38 63 06 78 F0 A7 F3	6 Jul 2020	22 set 2030
CN = Actalis Client Authentication CA G1 O = Actalis S.p.A./03358520967 L = Milano S = Milano C = IT	7E 60 FC F8 6C A7 3D 3D D7 AE 93 A1 79 02 8F B3 74 29 3B F5	14 May 2015	14 May 2030
CN = Actalis Client Authentication CA G3 O = Actalis S.p.A. L = Ponte San Pietro S = Bergamo C = IT	BE 97 A9 AA 84 BF 80 BF 10 53 7D 09 32 F9 E1 2E 32 1B CF 77	6 Jul 2020	22 set 2030
CN = Actalis Time Stamping CA G1 O = Actalis S.p.A. L = Ponte San Pietro S = Bergamo C = IT	D7 9C 73 39 2D 7D F0 D9 E4 16 4A 50 23 53 00 6D 4E FD 11 A3	10 mar 23	22 set 2030

Subordinate CA certificates can be issued to **external CAs** (i.e. not run by Actalis), under an Actalis' Root CA, provided that the entities running those external CAs commit in writing to fully comply with CAB Forum's Baseline Requirements [BR], via a suitable **contract** with Actalis[1].

Unless an external CA is technically constrained in compliance with section 7.1.2.3, 7.1.2.4 and 7.1.2.5 of the [BR], such CA shall submit itself to a **compliance audit on an annual basis**, performed by a **qualified and independent auditor** according to chapter 8 of the [BR], and timely provide to Actalis the resulting audit statement every year. Lacking such audit statement, Actalis will revoke the SubCA certificate. Furthermore, Actalis reserves the right to revoke the SubCA certificate in case the related audit statement has major qualifications, at the sole judgement of Actalis.

1.3.2 Registration Authorities

The Registration Authority (RA) is a person or an organization that is responsible for:

- collection and validation of certification requests and certificate management requests;
- registration of the Applicant, and related information, into the RA database;
- authorization of issuance, by the CA, of the requested certificates.

For EV certificates, all RA activities shall generally be performed by Actalis only.

For DV and OV certificates only, the CA may delegate some RA tasks to Delegated Third Parties (DTP), except for the validation of domain / IP address ownership or control that remains the sole responsibility of the CA.

Organizations meeting the requirements for "Enterprise RAs" set forth in the [BR] may be enabled to operate as their own RA, limited to the domains and IP addresses they own or control.

1.3.3 Subscribers

Subscribers are those legal entities or individuals to whom Certificates are issued according to this CPS and who hold the private keys corresponding to their certificates. In particular:

- for OV and EV SSL Server certificates, the Subscriber may only be a legal entity (i.e., an organization);
- for DV SSL Server and Code Signing certificates, the Subscriber may be either a legal entity or an individual.

Except for DV SSL Server certificates, which by definition do not include Subject identity information, the Subscriber is the party identified in the Subject field of the certificate.

Prior to verification of identity and issuance of a certificate, any requesting Subscriber is defined as an **Applicant**. Once the Certificate is issued, the Applicant is referred to as the **Subscriber**.

The Customer, namely the individual or organization that purchases the certificate, is normally the Subscriber itself, but this is not a requirement (another entity may purchase the certificate on behalf of the Subscriber).

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 (for instance) the users of the relevant web site. For Code Signing certificates, these are typically the users of the signed software.

[1] Issuance of EV certificates by external SubCAs, under an Actalis' Root CA, is currently not allowed.

1.3.5 Resellers

Certificates may also be provided through Resellers (business partners), which in certain cases may also play the role of Registration Authorities, depending on the agreements with the CA.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

Certificates issued under this CPS may be used for the following purposes, depending on certificate type:

- **SSL Server certificates** may be used to enable the TLS/SSL protocol on one or more servers.
- **Code Signing certificates** may be used for validating digital signatures of executable code.

A list of major platforms and browsers where certificates issued according to this CPS are trusted can be found on Actalis' web site at the following URL: https://www.actalis.it/products/ssl-certificate.aspx. Applicants are supposed to review that list before requesting certificates.

The CA may also issue other types of certificates (e.g. SSL Client, S/MIME) that are not entirely regulated by this CPS, but in separate policy documents that refer to this CPS for the shared aspects (e.g. facility, management and operational controls, technical security controls, Root CAs, etc.).

It is assumed that the Applicant possesses the competence and tools necessary to request, install and use the certificate. Actalis can provide consultancy on request, as a separate service.

The following table shows the **classes** and **policies** of certificates issued under this CPS, and the applicable CAB Forum requirements. Each policy is identified by a specific **OID** (Object Identifier) under the Actalis arc **1.3.159**:

Class	Certificate policy	OID	CABF reqs.
EV	SSL Server EV (Extended Validation)	1.3.159.1.17.1	[BR], [EVGL]
OV	SSL Server Wildcard OV (Organization Validated)	1.3.159.1.19.1	[BR]
OV	SSL Server OV (Organization Validated)	1.3.159.1.20.1	[BR]
OV	Code Signing (Organization Validated)	1.3.159.1.21.1	[BR]
DV	SSL Server DV (Domain Validated)	1.3.159.1.22.1	[BR]
DV	SSL Server Wildcard DV (Domain Validated)	1.3.159.1.23.1	[BR]

The OID that identifies the certificate policy is contained in the *CertificatePolicies* certificate extension, as detailed in chapter 7. The same extension also contains the applicable policy OID defined by CAB Forum.

In the case of *qualified* certificates according to the eIDAS regulation (see par. 7.1), the CertificatePolicies extension also includes the relevant policy OID defined in ETSI EN 319 411-2.

1.4.2 Prohibited certificate uses

Any use of the certificate other than provided for in section 1.4.1 is forbidden and may result, as soon as Actalis is made aware of it, in the revocation of the certificate (see also section 4.9.1).

Actalis reserves the right to put in operation new subordinate i.e. intermediate CAs (ICAs) when needed according to its own determinations, and to stop issuing certificates from the old ones. In some circumstances, Actalis may also need to revoke certain ICAs before their natural expiration.

Actalis therefore strongly recommends that *ICA certificates not be embedded into applications and/or platforms*.

Actalis strongly discourages certificate "pinning" and does not consider it a sufficient reason to delay revocation.

Customers should not use certificates trusted for the web in contexts where there is no such need (e.g. on private networks), especially where a quick replacement of certificates is not viable.

Customers should keep in mind that any certificates trusted by the browsers must comply with all requirements of all applicable browser root policies, including the revocation periods recalled in section 4.9.1 of this CPS.

1.5 Policy administration

1.5.1 Organization administering the document

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

1.5.2 Contact person

For any enquiries about this CPS, please send e-mail to cps-admin@actalis.it.

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

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

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

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

- his/her full name;
- his/her phone number;
- description of the alleged problem;
- enough information to identify the certificate in question, such as:
  - for an SSL Server certificate: either the address of the web site where the certificate is installed, or the certificate hostname, starting validity date, and serial number;
  - for a Code Signing certificate: commonName (CN), starting validity date, and serial number.

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

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

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

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

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

1.5.3 Person determining CPS suitability for the policy

This CPS is approved by Actalis' CA services direction, after review by all internal stakeholders, taking into account the Requirements [BR] and Guidelines [EVGL], and the results and recommendations received from qualified auditors (see also section 8).

1.5.4 CPS approval procedures

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

1.6 Definitions and acronyms

AgID	Agenzia per l'Italia Digitale (Agency for a Digital Italy)
ARL	Authority Revocation List
CA	Certification Authority
CAA	CA Authorization (a type of DNS record)
CAB	Conformity Assessment Body
CP	Certificate Polilcy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DBA	Doing Business As (trade name)
DCV	Domain Control Validation
DN	Distinguished Name
DV	Domain (Control) Validated
ECC	Elliptic Curve Cryptography
eIDAS	Electronic Identification and Trust Services (Regulation EU n.910/2014)
EV	Extended Validation
FIPS	Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
gTLD	Generic TLD (Top-Level Domain)
HSM	Hardware Security Module
HTTP	Hyper-Text Transfer Protocol
I&A	Identification and Authentication
IDN	Internationalized Domain Name
ISMS	Information Security Managament System
ISO	International Standards Organization
OCSP	On-line Certificate Status Protocol
OID	Object Identifier
OV	Organization Validated
PDF	Portable Document Format
PKI	Public Key Infrastructure
RA	Registration Authority
SAN	Subject Alternative Names ()
SSL	Secure Sockets Layer (all over this CPS, SSL refers to TLS unless otherwise specified)
TLS	Transport Layer Security
TSL	Trust-services Status List
TSP	Trust Service Provider
UPS	Uninterruptible Power Supply
VMD	Video Motion Detection

Throughout this document, certain terms shall be interpreted according to the definitions provided in [BR] and [EVGL]. In particular (but not limited to) the following terms: Subscriber, Subject, Applicant, Applicant Representative, Affiliate, Certificate Requester, Certificate Approver, Contract Signer, Authorization Domain Name, Base Domain Name, Domain Contact, Domain Registrant, Enterprise RA, Internal Name, Reserved IP Address.

1.7 Normative 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)

[RFC6960] Santesson, S., Myers, M., Ankney, R., Malpani, A., Galperin, S., and C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", RFC 6960, June 2013. (http://www.ietf.org/rfc/rfc6960.txt)

[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)

[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)

[CT] Laurie, B., Kasper, E., “Certificate Transparency”, RFC 6962, June 2013. (http://www.ietf.org/rfc/rfc6962.txt)

[ETSI411-1] ETSI EN 319 411-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements, v1.1.1 (2016-02).

[ETSI411-2] ETSI EN 319 411-2: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates, v2.1.1 (2016-02).

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

[CSBR] CA/Browser Forum, “Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates”. (https://cabforum.org/working-groups/code-signing/documents/)

[EVGL] CA/Browser Forum, “Guidelines For The Issuance And Management Of Extended Validation Certificates”. (https://cabforum.org/working-groups/server/extended-validation/documents/)

[GDPR] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[ACME] Barnes, R., Hoffman-Andrews, J., McCarney, D., and J. Kasten, "Automatic Certificate Management Environment (ACME)", RFC 8555, March 2019. (https://www.rfc-editor.org/info/rfc8555)

2 Publications and repository responsibilities

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 Repositories

The Actalis repository is published on:

- the Actalis website (http://www.actalis.it and other Actalis websites therein referred to)

Actalis manages its repository and is directly responsible for it.

The repository is normally accessible on a continuous basis (7x24).

2.2 Publication of information

Actalis publishes at least the following documentation on its website:

- Certification Practice Statement (CPS)
- Root CA and SubCA certificates
- Terms & Conditions
- audit statements
- application forms

Actalis also publishes test web pages that allow Application Software Suppliers to test their software with Subscriber certificates that chain up to Actalis’ publicly trusted Root CAs.

2.3 Time or frequency of publications

This CPS and any associated documents are published on the CA web site each time they are updated.

This CPS is reviewed and updated at least every year, also to ensure that it conforms to the latest versions of CAB Forum Requirements and Guidelines [BR], [CSBR] and [EVGL], and other applicable standards and regulations.

See also section 4.10.

2.4 Access control on repositories

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

Access to the repository in write-mode (e.g., for the publication of new or updated information) is only possible from workstations / servers directly connected to the repository’s local network, subject to authentication.

3 Identification and Authentication (I&A)

The I&A procedures followed by Actalis comply with CAB Forum requirements. In particular, for all classes of certificates issued under this CPS, the CA performs at least the mandatory checks provided in [BR] and [CSBR]. In addition, for EV certificates, the CA also performs at least the additional checks required by the [EVGL].

3.1 Naming

3.1.1 Types of names

Certificates issued according to this CPS normally contain a non-null Distinguished Name (DN) compliant with the ITU-T X.500 standard (ISO/IEC 9594) in both the Subject and the Issuer fields.

The Subject field may be *empty* in DV (Domain Validated) certificates, e.g., when it cannot accommodate a very long FQDN (> 64 chars); in such a case, the Subject Alternative Name (SAN) extension is flagged as *critical*.

Furthermore, all the requirements set forth in the [BR], [CSBR] and [EVGL] shall be met.

In particular, all SSL Server certificates shall include entries in the Subject Alternative Name (SAN) extension, where each entry is either a Fully Qualified Domain Name (FQDN) or an IP address. However, IP addresses are not allowed in DV (Domain Validated) and EV (Extended Validation) SSL Server certificates.

3.1.1.1 Internal names and reserved IP addresses

Internal Names and/or Reserved IP Addresses (see the respective definitions in [BR]) are not allowed.

3.1.1.2 Internationalized domain names (IDNs)

No stipulation.

3.1.2 Need for names to be meaningful

Actalis inserts meaningful names in both the *subject* and the *issuer* fields of certificates, with the possible exception of the Subject field in DV certificates as previously noted.

3.1.3 Anonymity or pseudonymity of subscribers

Except for SSL Server certificates of class DV (Domain Validated), which by definition do not contain Subscriber identification information, in all other cases the certificate contains either the official (i.e. registered) name of the Subscriber or a verified DBA (Doing Business As) name.

3.1.4 Rules for interpreting various name forms

All name forms shall be interpreted according to the ITU-T X.500 (ISO/IEC 9594) and the RFC 5820 standards, also taking into account CAB Forum's Requirements [BR], [CSBR] and [EVGL] according to certificate type and class.

3.1.5 Uniqueness of names

No stipulation.

3.1.6 Recognition, authentication, and role of trademarks

Names that violate the intellectual property rights of others are not allowed into certificates. Actalis shall not be involved in any controversy whatsoever regarding the ownership 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 Method to prove 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 transmit its public key to the CA in the form of a CSR (Certificate Signing Request) in PKCS#10 format [RFC2314]. The CA shall verify that the digital signature in the CSR is valid.

3.2.2 Authentication of organization and domain identity

3.2.2.1 Identity

When the certificate is to include the name or address of an organization, the CA shall verify the identity and address of the organization, and that the address is the Applicant's address of existence or operation. This verification is done in compliance with the CAB Forum's requirements [BR], [CSBR] and [EVGL] according to certificate type and class.

Actalis will normally query:

- for private organizations, the relevant company registry for the applicable jurisdiction or an equivalent private or governmental source of organization information meeting the requirements of §3.2.2.7;
- for public entities, the relevant official index or registry of public entities for the applicable jurisdiction.

In the event that the consultation of the above sources is not possible, or returns incomplete or obsolete information about the Applicant (e.g. registered identity and brands, address, phone numbers, contact persons, etc.), Actalis may accept an Attestation Letter signed by a lawyer, government official, or other reliable third party customarily relied upon for such information in the Applicant's jurisdiction, attesting to that information. Jointly with this document, it will also be necessary to make a copy of the license or different document proving the role of the third party available. This information must be written in Italian or, if in a different language, it must also be written in English.

Other information sources meeting the requirements of section 3.2.2.7 (see below) may also be used, at Actalis' sole discretion, depending on circumstances, to corroborate the information obtained from the above sources.

For EV SSL Server certificates, the approved information sources used for validating the Applicant's identity are those published on the Actalis website at the following address:
https://www.actalis.it/documenti-en/actalis-approved-incorporation-agencies.aspx.

The name of the Applicant must match the organization name resulting from such lookups. In case of mismatch (except for negligible differences like e.g. uppercase/lowercase, non-meaningful diacritics, or punctuation), unless the Applicant can provide an explanatory evidence, the certificate application will be rejected. Any ambiguity must be solved by the Applicant.

The CA may use the same information sources to also verify the Applicant's address(es). When the claimed Applicant' address cannot be verified in that way, the Applicant will be required to provide to the CA a utility bill, or a bank or credit card statement reporting the Applicant's full address. Other forms of evidence may also be accepted by the CA, subject to a case-by-case evaluation by the CA.

The information gathered by the CA include at least:

- actual existence and status of the Applicant organization
- legal (i.e. registered) name of the Applicant organization
- full address of the Applicant organization's head office and operation sites
- the Applicant organization's registration number issued by the relevant jurisdiction
- the Applicant organization's VAT and/or fiscal code or equivalent (where applicable)
- the Applicant organization general phone and/or fax number(s), if available
- the Applicant organization general email address(es), if available

As a rule, should the CA not be able to collect the above information by itself, the Applicant will be required to provide it to the CA, subject to the subsequent CA's evaluation of the trustworthiness of the provided information in view of the minimal requirements set forth in the [BR], [CSBR], and [EVGL].

3.2.2.2 DBA/Tradename

If the Subject the certificate is to include a DBA or trade name (not applicable to DV-class SSL Server certificate), the CA shall verify the Applicant's right to use the DBA/trade name with at least one of the criteria provided for in [BR], [CSBR] or [EVGL] according to certificate type and class.

3.2.2.3 Verification of country

When the certificate Subject is to include a country code (not applicable to DV-class SSL Server certificates), the CA shall verify the country using one of the methods provided for in section 3.2.2.3 of the [BR].

3.2.2.4 Validation of Domain Authorization or Control

Prior to issuing an **SSL Server** certificate, the CA shall verify that **each FQDN** to be included in the certificate **either is owned or controlled by the Applicant** or an affiliate thereof (e.g. parent or subsidiary). These checks (also referred to as Domain Control Validation or DCV) are done by one of the following methods:

- The CA confirms, by directly querying the Domain Name Registrar, that the Applicant is the Domain Registrant. This method may only be used if the Base Domain Name is registered by Aruba S.p.A. (that is the Actalis' holding company). This method is implemented in compliance with §3.2.2.4.12 of [BR].
- The CA sends a Random Value via e-mail to a Domain Contact (found in the WHOIS record of the Authorization Domain Name) and receives a confirming response utilizing the Random Value. This method is implemented in compliance with §3.2.2.4.2 of [BR].
- The CA sends a Random Value via e-mail to an address obtained by pre-pending "admin@", or "administrator@", or "webmaster@", or "hostmaster@", or "postmaster@" to the Authorization Domain Name, and receives a confirming response utilizing the Random Value. This method is implemented in compliance with §3.2.2.4.4 of [BR].
- The CA asks the Applicant to publish a file on the HTTP server at the target FQDN, under the "/.well-known/pki-validation" directory, containing a Random Value provided by the CA, and then confirms the presence of such file, with the expected contents. As of December 1, 2021, this method

cannot be used for wildcard FQDNs and does not cover subdomains of the validated domain. This method is implemented in compliance with §3.2.2.4.18 of [BR].

- The CA asks the Applicant to publish a file on the HTTP server at the target FQDN, under the "/.well-known/acme-challenge" directory, according to section 8.3 of RFC8555 [ACME], containing the value provided by the CA, and then confirms the presence of such file, with the expected contents. As of December 1, 2021, this method cannot be used for wildcard FQDNs and does not cover subdomains of the validated domain. This method is implemented in compliance with §3.2.2.4.19 of [BR].
- The CA asks the Applicant to insert a TXT record, containing a Random Value provided by the CA, into the DNS information of the Authorization Domain Name, and then confirms the presence of such record with the expected contents. This method is implemented in compliance with §3.2.2.4.17 of [BR].
- The CA confirms that the Applicant controls an IP address returned from a DNS lookup for A or AAAA records for the FQDN in line with section 3.2.2.5. This method may not be used for wildcard FQDNs. This method is implemented in compliance with §3.2.2.4.8 of [BR].

Note: in the above list of DCV methods, the “Authorization Domain Name” is obtained by pruning zero or more components from the requested FQDN, up to and excluding a public suffix or registry-controlled label.

In all cases, the DCV is done in full compliance with section 3.2.2.4 of the [BR], and no DCV methods are employed by the CA other than those provided for in the [BR].

The particular DCV method used for a given FQDN may depend on circumstances, on the certificate requestor’s preferences. The range of supported DCV methods may vary depending on the certificate request channel.

3.2.2.5 Authentication for an IP Address

Prior to issuing an **SSL Server** certificate, the CA shall verify that **all IP addresses** to be included in the certificate (excluding DV and EV certificates that may not contain IP addresses) **are controlled by the Applicant** or an affiliated thereof (e.g. holding or subsidiary). These checks are done by one of the following methods:

- the Applicant demonstrate practical control over the IP Address by publishing a file on the HTTP server at the target IP, under the "/.well-known/pki-validation" directory, containing a Random Value provided by the CA; the CA confirms the presence of such file, with the expected contents;
- the CA sends a Random Value via e-mail to an IP Address Contact, obtained by consulting the Internet Assigned Numbers Authority (IANA) or a Regional Internet Registry (RIPE, APNIC, ARIN, AfriNIC, LACNIC), and receives a confirming response utilizing the Random Value;
- performing a reverse-IP address lookup and then verifying control over the resulting Domain Name according to section 3.2.2.4.

3.2.2.6 Wildcard Domain Validation

Prior to issuing an **SSL Server** certificate, if the certificate is to include a **wildcard FQDN** in the Subject commonName (CN) or in the Subject Alternative Name extension, the CA shall determine if the wildcard character would fall within the label immediately to the left of a registry-controlled or public suffix; in such a case, the CA shall reject the certificate request unless the Applicant proves its rightful control of the entire Domain Namespace. For this verification, Actalis consults the Public Suffix List published at https://publicsuffix.org/.

3.2.2.7 Data Source Accuracy

Prior to using any data source as a Reliable Data Source, the CA shall evaluate the source for its reliability, accuracy, and resistance to alteration or falsification, according to section 3.2.2.7 of the [BR].

3.2.2.8 CAA Records

As part of the issuance process, the CA shall check for a CAA record for each dNSName in the Subject Alternative Name extension of the certificate to be issued, according to the procedure in RFC 6844 and in section 3.2.2.8 of the [BR]. The CAs shall not issue the certificate unless either (1) the certificate request is consistent with the applicable CAA Resource Record set or (2) an exception applies. The CA's CAA identifying domain is "**actalis.it**".

3.2.2.9 Further verifications

For EV-class certificates, the CA shall also verify:

- **physical existence** of the Applicant (or an affiliate thereof) in line with section 11.4 of [EVGL];
- **operational existence** of the Applicant (or an affiliate thereof) in line with section 11.6 of [EVGL].

For the second item, Actalis will normally check that the Applicant has been in existence for at least 3 years, by querying reliable information sources (see 3.2.2.1), or ask the Applicant to prove possession of a demand deposit (or equivalent) bank account. To that aim, the Applicant may provide to the CA a letter of bank reference, dated and signed by the bank, on the bank's headed paper.

Actalis may reject the certificate request in the event that problematic situations (e.g. bankruptcy proceedings, disputes, insolvency, etc.) are found regarding the Applicant or an Applicant Representative.

3.2.3 Authentication of individual identity

For certificates containing Subject Identity Information, if the Applicant is a natural person the CA shall verify the Applicant's name, Applicant's address, and the authenticity of the certificate request in compliance with section 3.2.2 of the [BR]. To that aim, Actalis will normally:

- verify the Applicant's name using a legible copy, which discernibly shows the Applicant's face, of at least one currently valid government-issued photo ID (passport, drivers license, military ID, national ID, or equivalent document type) and will inspect the copy for any indication of alteration or falsification;
- verify the Applicant's address using a form of identification that Actalis determines to be reliable, such as a government ID, utility bill, or bank or credit card statement. Actalis may rely on the same government-issued ID that was used to verify the Applicant's name;
- verify the certificate request with the Applicant using a reliable method of communication.

3.2.4 Non-verified subscriber information

The CA does not verify the following Subscriber information:

- Organizational Unit name (except for checking that it's not misleading);
- information not needed for Subscriber identification purposes;
- email addresses specified in certificate application forms;

In general, the CA does not verify the correctness of any information received from the Applicant that is not intended to be included in security-sensitive fields of the certificate and is not necessary for the issuance and subsequent management (e.g. revocation) of the certificate.

3.2.5 Validation of authority

For certificates containing Subject Identity Information, if the Applicant is an organization the CA shall use a Reliable Method of Communication to verify the authenticity of the Applicant Representative's certificate request, in line with CAB Forum's [BR], [CSBR] or [EVG} according to certificate type and class.

The CA may use the sources listed in section 3.2.2.1 to verify the Reliable Method of Communication.

Actalis will normally use one the following validation methods:

- By telephone: a CA validation specialist contacts the Applicant by telephone, through the Applicant organization's general phone number (previously found in a reliable source of information) and asks confirmation that the certificate request received from Applicant Representative is authentic.
- By on-line authentication: the Applicant Representative sends the certificate request to the CA via a web site or web service that requires on-line authentication using personal credentials provided to the Applicant Representative after a suitable identification procedure by the CA.
- By certified email: the Applicant specifies the name and contact details of its Representative(s) in an email message sent to the CA via a certified email service[2] (or an equivalent service), from the Applicant's certified email address (which must be found in a reliable information source);
- By digital signature: the Applicant sends to the CA a certificate application form, including the name and contact details of the Applicant Representative(s), as a digitally signed document; the signature must be a *qualified electronic signature* (according to EU legislation) and the signer's certificate must be valid (not expired nor revoked) and clearly ascribable to the Applicant.
- By formal purchase order: the name and contact details of the Applicant Representative are provided to the CA in attachment to a formal purchase order issued directly by the Applicant, written on the Applicant's headed paper, including complete identifying data of the Applicant and sent to the CA by the Applicant's purchasing department.

For EV certificates, the CA shall verify the Name, Title, and Authority (Agency) of Contract Signer and Certificate Approver according to section 11.8 of the [EVGL]. To the aim of this verification, Actalis will normally rely on a suitable representation from the Contract Signer, based on a template provided by Actalis, which must be signed according to section 4.1.2.

3.2.6 Criteria for interoperation

The CA shall disclose all cross certificates that identify the CA as the Subject, provided that the CA arranged for or accepted the establishment of the trust relationship.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

Re-keying a certificate may routinely occur in two cases:

- when a Subscriber wishes to replace an existing certificate with a new one (with same or different details) containing a different key; or

[2] One such service is the Italian "Posta Elettronica Certificata" (PEC).

- when a Subscriber wishes to renew a certificate that is about to expire, that is, obtain a new certificate with the same details of the one that is about to expire; in this case, the CA requires that the new certificate contains a new key.

In both cases, the CA may request the Subscriber to pass the same identification and authentication procedures used for the initial certificate issuance, depending on the age of the validation data used for the initial certificate issuance (in view of the requirements set forth in [BR], [CSBR] and [EVGL]) and on the request channel.

3.3.2 Identification and authentication for re-key after revocation

After a certificate has been revoked, the Subscriber wishing a new certificate must generate a new key pair and follow all the normal identification and authentication procedures as in the initial certificate issuance.

3.4 Identification and authentication for revocation requests

See section 4.9.3.

4 Certificate management operational requirements

4.1 Certificate application

4.1.1 Who can submit a certificate application

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

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

4.1.2 Enrollment process and responsibilities

The certificate enrollment process includes the following mandatory steps:

- generating a suitable key pair;
- submitting to Actalis a certificate application form;
- delivering to Actalis the public key of the key pair;
- agreeing to and/or signing the applicable Subscriber Agreement;
- paying the applicable fees (depending on certificate class, type, etc.).

All the above steps are the responsibility of the Applicant, except for the Payment which may possibly be made by another entity.

In the case of Code Signing certificates, the generation of the Applicant's key pair is performed by Actalis upon request, as part of the certificate enrollment process that applies in that case.

The order and the exact way in which these steps are carried out may vary, depending on chosen request channel, but all the steps have to be completed (with the possible exception of the payment which can be deferred,

depending on the customer and the amount due, subject to approval by Actalis' sales department) *before* the certificate request is taken charge of by the CA.

For DV and OV SSL Server certificates and Code Signing certificates, the following Applicant roles are required, as defined in the [BR], and enforced within the enrollment process:

- Applicant
- Applicant Representative

For EV SSL Server certificates, the following additional Applicant roles are required, as defined in the [EVGL], and enforced within the enrollment process:

- Certificate Requester
- Certificate Approver
- Contract Signer (the natural person who signs the Subscriber Agreement EV - see below)

The Applicant may authorize one individual to occupy two or more of the above roles, and/or may authorize more than one individual to occupy any of these roles.

The certificate request is normally made through the submission of an online form (web form) on the website of the CA itself or on the website of a Reseller. In special cases where this method cannot be followed, you can submit an off-line application form (e.g., via email) to the CA (available on the CA portal).

Enterprise RAs can request certificates via a specific web-based application hosted by Actalis.

The certificate application always includes the following information:

- type, class, and duration (validity) of the requested certificate
- for SSL Server certificates, FQDN(s) and/or IP address(es) to be included in the certificate
- (except for DV SSL Server certificates) value of the proposed Subject DN
- name and contact details of one or more Technical Contacts

Only for OV and EV-class certificates, the following information must also be provided:

- details of the Applicant organization (official name, registration number, address, etc.)
- name and contact details of a suitable Organizational Contact

The certificate application includes, as a mandatory step, the Applicant's express acceptance of a Subscriber Agreement (also named "Terms and Conditions") that includes this CPS by reference. Depending on the certificate class and the particular application procedure or channel, the Applicant may agree these terms in different ways, such as:

- by "point and click" on a web form (in conformance to European legislation on distance contracts);
- by expressly confirming acceptance in writing to Actalis (possibly via email);
- by a hand-written signature,
- by a digital signature.

When an actual signature is required, it must be made by a suitably authorized person.

EV Certificate requests must be submitted by an authorized Certificate Requester and approved by a suitable Certificate Approver according to the [EVGL]. The certificate request must be accompanied by a dedicated signed Subscriber Agreement from a suitable Contract Signer according to the [EVGL]. The EV Subscriber Agreement must be signed in one of the following ways:

- by a handwritten signature made before an Actalis representative (who counter-signs as a witness, after checking the identity of the signatory by examining a valid identity document of the same and keeping a scan thereof);
- by a handwritten signature with a copy of a valid government-issued photo ID of the signatory; in this case, the original handwritten document and the copy of the government ID must be sent to Actalis by e-mail, from an e-mail address related to a domain under control of the Applicant, then sent to Actalis by post;
- by a handwritten signature authenticated by a notary or another person whose commission under applicable law includes authority to authenticate the execution of a signature on a document; (*)
- by a valid *qualified electronic signature* compliant with European regulations.

(*) In this case, the authenticated copy of the Subscriber Agreement must be sent to the CA in original. The certificate request will not be processed until Actalis has received and verified such original.

Before accepting the Subscriber Agreement, the Applicant or Applicant Representative is supposed to review all aspects of the Actalis' CA service by reading the documentation published on the CA web site.

The certificate application form and the Subscriber Agreement are available in Italian and English language. Actalis does not commit to support other languages.

The certificate application form must be accompanied or followed by a suitable Certificate Signing Request file (CSR) conformant to section 3.2.1.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

Upon receipt of a certificate application, all the verifications previously described (see chapter 3 and the previous sections of chapter 4) are performed either automatically, to the extent that is possible and allowed, and/or by a Validation Specialist when necessary or mandatory, in compliance with the [BR], [CSBR] and [EVGL] according to certificate type and class.

Depending of the age and applicability of the already available validation data, the CA may re-use previous validations (documents, data, etc.) for additional certificates to be issued to the same Applicant, to the extent that is permitted by the [BR], [CSBR] and [EVGL] according to certificate type and class.

The CA also checks that the information contained in the CSR (e.g. Subject DN, FDQNs and/or IP addresses) are consistent with those supplied in the certificate application form and with the type of certificate requested, and rejects the request in case of conflicts or anomalies.

The CA also checks the relevant CAA records (if any) according to paragraph 3.2.2.8 of the [BR]. The domain identifier to be used in the CAA records to authorize the Actalis CA is "actalis.it".

For EV SSL Server certificates, Actalis enforces the principle of Separation of Duties to ensure that no one person can single-handedly validate and authorize the issuance of an EV Certificate, in compliance with section 14.1.3 of the [EVGL]. In particular, the "Final Cross-Correlation and Due Diligence" (see section 3.2.2.13 of EVGL) is carried out by a different validation specialist than the one(s) who performed the previous validation steps.

Once the essential I&A steps are successfully completed, the CA will normally send to the Applicant Representative, via email, the authentication credentials needed to login to the CA portal, for the possible submission of revocation requests.

4.2.2 Approval or rejection of certificate applications

Approval of certificate applications requires the successful completion of all validation steps described so far, in full compliance with all CA policies. However, a few additional checks are performed by Actalis:

- Certificates containing internal names will not be issued.
- Certificates containing a new gTLD under consideration by ICANN will not be issued.
- Certificates for domains with ".onion" in their right-most label will not be issued.
- Actalis will reject certificate requests for domains that, at the time of issuance, are reported as risky (e.g. because of phishing or malware) by widely used domain reputation services.
- Actalis maintains a list of high-profile domains and will block the issuance of certificates containing any of those domains, in order to mitigate the associated risks. Before such requests can be approved, the Applicant will be required to provide extra information to corroborate its right to use such domain(s).

4.2.3 Time to process certificate applications

No stipulation.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

If the previous steps (see section 4.2) are completed successfully, the CA system:

- checks that the CSR is well-formed and does not contain unexpected data;
- checks that the CSR is cryptographically valid according to section 3.2.1;
- checks that the key found in the CSR is not a known "weak key" (see CVE-2008-0166);
- checks the relevant CAA Records (if any) according to section 3.2.2.8 of the [BR].

If all the above checks are successful, the CA generates the certificate, stores it into its database, and eventually sends to the Applicant an e-mail containing at least:

- the Subscriber certificate (or a link to it);
- the certificate of the Issuing CA (or a link to it).

All of the above operations are performed automatically for Subscriber certificates, normally.

All SSL Server certificates issued after 30 April 2018 MUST be compliant with Certificate Transparency requirements according to [CT]. When an SSL Server certificate is to be issued, a precertificate is first generated and

registered in a number of CT-logs according to Chromium CT Policy. Each CT-log returns a signed certificate timestamp (SCT) as a proof of inclusion. Then, the final certificate is generated wherein the SCTs are embedded as an extension (OID 1.3.6.1.4.1.11129.2.4.2).

In case of a Subordinate CA certificate, however, the certificate issuance requires a suitably authorized individual (i.e., the CA system operator, system officer, or PKI administrator) to deliberately issue a direct command in order for the Root CA to perform the certificate signing operation.

4.3.2 Notification to subscriber by the CA of issuance of certificate

The Subscriber will normally be notified via email of the successful issuance of the certificate, either by the CA directly or by an RA and/or Reseller where applicable, provided that the email address supplied to the CA for that purpose by the Applicant Representative or Certificate Requester is valid.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

The CA intends the certificate as accepted after 30 days from the date of delivery, as attested by the date of the electronic mail message sent to the Subscriber, barring any notice to the contrary from the Subscriber.

Public use of the certificate (i.e., its installation on a website with public access, publication on a public website of executable code signed by that certificate), even if temporary, shall in any case imply acceptance of the certificate by the Subscriber.

In the event that the certificate is issued with incorrect information in it due to incorrect completion of the application form by the requestor, the certificate must nonetheless be paid for.

4.4.2 Publication of the certificate by the CA

As regards Root CA and Subordinate CA certificates, see paragraph 2.2

No stipulation as regards end entity certificates.

4.4.3 Notification of certificate issuance by the CA to other entities

For all new SSL Server certificates, the CA submits the pre-certificate to at least two different Certificate Transparency (CT) logs according to RFC6962.

4.5 Key pair and certificate usage

The Subscriber shall use the private key:

- (Code Signing certificates) to digitally sign their own executable code (e.g., PE files, Java applets, dynamic libraries, etc.) and/or code for which the Subscriber is responsible;
- (SSL Server certificates) to activate the TLS/SSL protocol on their own servers, thereby allowing TLS server authentication and session encryption of the transactions with clients.

The relying parties shall use the certificate to:

- (Code Signing certificates) verify the integrity and origin of the executable code;
- (SSL Server certificates) verify the identity of a server and (depending on certificate class) the organization which controls the server, as well as to exchange the “session key” safely with the server.

See also paragraph 1.4.

4.6 Certificate renewal

Renewal of a certificate means the issuing of a new certificate containing the same Subject identifying information (according to the certificate class) and the same domains and IP addresses (according to the type of certificate) that are found in a certificate already issued and not yet expired or revoked.

The CA makes a reasonable effort to inform the Subscriber about the forthcoming expiration of their certificates, by periodically sending emails to the Technical Contact. The warning emails are sent, normally, starting from 30 days before the expiry of the certificate.

4.6.1 Circumstance for certificate renewal

Same as described in par. 4.1.1.

4.6.2 Who may request renewal

Same as described in par. 4.1.2.

4.6.3 Processing certificate renewal requests

Same as described in par. 4.1.3.

4.6.4 Notification of new certificate issuance to subscriber

Same as described in par. 4.1.4.

4.6.5 Conduct constituting acceptance of a renewal certificate

Same as described in par. 4.1.5.

4.6.6 Publication of the renewal certificate by the CA

Same as described in par. 4.1.6.

4.6.7 Notification of certificate issuance by the CA to other entities

Same as described in par. 4.1.7.

4.7 Certificate re-key

Certificate re-keying implies the issuance of a new certificate, with a new public key and a new serial number, but with the same Subject information found in the current certificate, provided this latter is not expired or revoked (otherwise, the normal first-issuance procedures are followed).

Key regeneration is a mandatory step if certificate renewal is required, but may also be required following the compromise of the current key or for other reasons at the discretion of the CA.

Certificate re-keying may be requested by the Subscriber, or by an RA, or by the CA, depending on circumstances.

Normally, the procedure for processing a key regeneration request is the same as in the new certificate issuance case. If the evidences previously collected during the I&A phase (see section 3.2) are still valid, the CA can process the request without necessarily redoing I&A; in this case, an authenticated request by the Subscriber is sufficient.

4.8 Certificate modification

Certificate modification implies issuing a new certificate to the same Subscriber, with the same or a different public key, but with different identification information (e.g. parts of Subject or SubjectAlternativeNames) than are found in the old certificate.

Certificate modification may be requested by the Subscriber, or by an RA, or by the CA, depending on the case.

When the old certificate contains incorrect information due to errors committed by the CA or RA, that incorrect certificate will be revoked and a correct one will be issued without additional charges for the customer.

When the old certificate contains incorrect information due to errors committed by the Applicant (e.g. incorrect inputs in one or more fields of the request form), that incorrect certificate will be revoked and the Subscriber may request a new certificate.

Normally, the procedure for modifying a certificate is the same as for issuing a new certificate. Depending on the case, a new I&A (see Section 3.2) may be necessary, either complete or partial.

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. Suspension is not supported for certificates issued under this CPS.

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.

Implementation of revocation consists in the generation and publication of a new CRL (Certificate Revocation List) that includes the serial number of the revoked certificate, and update of the OCSP responder database (see section 4.10 for more details on certificate status services).

4.9.1 Circumstances for revocation

4.9.1.1 Reasons for Revoking a Subscriber Certificate

The CA shall revoke a certificate **within 24 hours** if one or more of the following events occurs:

- the Subscriber requests in writing that the CA revoke the certificate;
- the Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization;
- the CA obtains evidence that the Subscriber's private key (corresponding to the public key in the certificate) has suffered a key compromise;
- the CA is made aware that the domain control validation for any of the FQDNs and/or IPs contained in the certificate should not be relied upon.

The CA shall revoke a certificate **within 5 days** if one or more of the following events occurs:

- the certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6 of the [BR];
- the CA is made aware that the certificate was misused (e.g. for unlawful purposes);

- the CA is made aware that the Subscriber has violated one or more of its material obligations under the Terms & Conditions of the service and/or this CPS;
- the CA is made aware that use of a FQDN or IP address in the certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a domain name registrant's right to use the domain name, the domain name registrant has failed to renew the domain name, etc.);
- the CA is made aware that a wildcard certificate has been used to authenticate a fraudulently misleading subordinate FQDN;
- the CA is made aware of a material change in the information contained in the certificate;
- the CA is made aware that the certificate has any non-compliance with this CPS and/or with the [BR] requirements and/or the [EVGL] guidelines (where applicable), regardless of the impact of such non-compliance on the security and/or the correct working of the certificate;
- the CA determines that any of the information appearing in the certificate is inaccurate or misleading (e.g. the Subscriber organization no longer exists, or is indicated ambiguously in the certificate);
- the CA's right to issue certificates under the [BR] expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP repository;
- the CA is made aware of a demonstrated or proven method that exposes the Subscriber's private key to compromise, or methods have been developed that can easily calculate it based on the public key, or if there is clear evidence that the specific method used to generate the private key was flawed.
- compromise of the private key of the subordinate CA used for issuing the certificate;
- breach of contract by the client (e.g. failure to pay for the certificate);
- a court order to revoke the certificate.

If an EV certificate is requested, by means of a handwritten signature, the CA will revoke the certificate for the following circumstances:

- failure to send, within 30 days from the issue of the certificate, the original documentation together with the copy of the government ID;
- incorrectness of the documentation compared to the original copy sent in advance by e-mail.

Before revoking a certificate, the CA will make a reasonable effort to warn to the affected Subscriber of the imminent revocation, compatibly with the maximum revocation times indicated above. However, the CA shall immediately revoke the certificate *without a prior notice* in the following cases:

- the certificate is being used for any kind of criminal activity (e.g. "phishing" attacks, "man-in-the-middle" attacks, malware distribution, etc.);
- the certificate was erroneously issued with CA = TRUE in its KeyUsage extension.

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

Actalis shall meet the requirements set forth in section 4.9.1.2 of the [BR].

4.9.2 Who can request revocation

Revocation can be requested by (depending on circumstances):

- the Subscriber;

- the issuing Certificate Authority;
- the Registration Authority;
- a court of law.

Additionally, Subscribers, Relying Parties, Application Software Suppliers, and other third parties may submit Certificate Problem Reports (in accordance with the circumstances described in Section 4.9.1 and in the manner described in Section 1.5.2.) informing the issuing CA of reasonable cause to revoke the certificate.

Under certain circumstances the Subscriber *must* request revocation of its certificate (see §9.6.3).

4.9.3 Procedure for revocation request

Requests for revocation can be submitted directly to the CA, through the CA portal. In the event that the certificate was provided through a reseller or through an RA, revocation of the certificate may also be requested through the reseller's or RA. In any case, before revocation of a certificate can be requested, it is necessary to authenticate to the relevant web site / service with the credentials that were provided to the Subscriber for that purpose at the time of certificate issuance.

As an alternative, it is possible to fill out a revocation request form (downloadable from the Actalis' web site), signed by the Subscriber. The signed form must then be sent directly to the CA (e.g. via ordinary mail, or rather e-mail). Before carrying out the revocation, the CA will check that the request is authentic. Revocation requests submitted to the CA in this way are handled on working days only.

For revocation requests submitted on-line, certificates shall be revoked within 24 hours.

Regardless of whom requested the certificate revocation, the CA shall normally inform the Subscriber about the effected revocation via an e-mail message sent to the "technical contact" specified in the application form.

4.9.4 Revocation request grace period

There is no grace period associated with certificate revocation requests. The Subscriber is expected to request revocation of its certificate as soon as circumstances requiring revocation (see §4.9.1) are confirmed.

4.9.5 Time within which CA must process the revocation request

Properly authenticated revocation requests received from Subscribers are processed within 24 hours provided that the request is made with the expected on-line procedure (see section 4.9.3).

In case of certificate problem reports that may require revocation (as described at 1.5.2), investigation on the alleged problem will begin within 24 hours of receiving the problem report. Once decided that certificate revocation is warranted, it will be carried out within 24 hours.

4.9.6 Revocation checking requirement for relying parties

See section 9.6.4.

4.9.7 CRL issuance frequency

See paragraph 4.10.1.

4.9.8 Maximum latency for CRLs

CRLs are published right after having been generated. The latency between generation time and publication time may depend on the load of the CA's processing systems; it is typically a few minutes and does not exceed 60 minutes.

4.9.9 On-line revocation/status checking availability

See sections 4.10 and 7.3.

4.9.10 On-line revocation checking requirements

The CA shall support an OCSP capability using the GET method for all certificates issued.

Except for CAs that are technically constrained in line with section 7.1.5, the CA's OCSP responders shall not respond with a "good" status when queried about a certificate that has not been issued.

The CA shall update the information provided via OCSP in compliance with the [BR] and [CSBR].

4.9.11 Other forms of revocation advertisements available

Actalis allows for OCSP stapling.

4.9.12 Special requirements related to key compromise

No particular requirement in case of key compromise detected by the Subscriber. In this case, the Subscriber is supposed to promptly request Actalis to revoke their certificate (see section 9.6.3).

Subjects *other* than the Subscriber can report the compromise of the key of an Actalis certificate (not expired and not revoked) using one of the following methods to demonstrate that they possess or control the private key in question:

- Create a text file containing the phrase "This key is compromised" (or a similar phrase), then sign the file with the private key that you want to report as compromised and send the signed file to Actalis (§).
- Create, with the private key that you want to report as compromised, a CSR that includes the text "This key is compromised" (or a similar phrase) in the commonName, then send the CSR to Actalis (§).
- Send to Actalis (§) the private key that you want to report as compromised. However, this method is *not recommended for safety reasons*.
- Send to Actalis (§) references to sources of information on vulnerabilities and/or security incidents that allow to verify the compromise.

(§) Send to cert-problem@actalis.it specifying "Key compromise" as the subject.

Actalis may, at its discretion, also allow other methods to demonstrate possession or control of a private key.

4.9.13 Circumstances for suspension

Not applicable.

4.9.14 Who can request suspension

Not applicable.

4.9.15 Procedure for suspension request

Not applicable.

4.9.16 Limits on suspension period

Not applicable.

4.10 Certificate status services

In general, the status of certificates (active or revoked) is made available to all interested parties via:

- the publication of Certificate Revocation Lists (CRL);
- the provision of an OCSP (On-line Certificate Status Protocol) service.

4.10.1 Operational characteristics

The CRL can be accessed:

- via HTTP protocol according to [RFC2616]

The addresses (URLs) of 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 revocations;
- following each new revocation.

The address (URL) of the OCSP responder is inserted in the *AuthorityInformationAccess* certificate extension.

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

The ARL, namely the list of revoked SubCA certificates, is re-generated and re-published:

- at least every 3 months, even in the absence of new revocations;
- following each new revocation.

Revocation entries in CRLs and OCSP responses shall not be removed until after the expiry date of the revoked certificates.

4.10.2 Service availability

Access to the CRL and OCSP service shall be continuously available (24 x 7), except in the case of system faults or other unexpected events. See also section 17.1.

For both CRL and OCSP, the response time shall be ten seconds or less under normal operating conditions.

4.10.3 Optional features

No stipulation.

4.11 End of subscription

The contract between the CA and the Subscriber ends when the Subscriber's certificate expires or is revoked, whichever comes first.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

Not applicable.

4.12.2 Session key encapsulation and recovery policy and practices

Not applicable.

5 Facility, management, and operational controls

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

5.1 Physical controls

5.1.1 Site location and construction

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

- primary data center ("IT1") located in Arezzo (AR);
- secondary data center ("IT2") located in Arezzo (AR);
- disaster recovery data center ("IT3") located in in Ponte S. Pietro (BG).

The main features the data centers mentioned above, e.g. construction, Internet connectivity, power supply, air conditioning, security, etc., can be found at https://datacenter.aruba.it.

The following figure shows the geographical location of the three sites. The site "IT3" (disaster recovery) of Ponte S. Pietro (BG), near Milan, is about 300 km from the primary and secondary sites in Arezzo:

Figure 1: Location of the CA production sites

5.1.2 Physical access

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

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

5.1.3 Power and air conditioning

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

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

5.1.4 Water exposures

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

5.1.5 Fire prevention and protection

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

5.1.6 Media storage

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

5.1.7 Waste disposal

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

5.1.8 Off-site backup

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

5.2 Procedural controls

Actalis maintains a Security Plan, including a Risk Assessment, which analyses the CA assets, the threats they are exposed to, and describes the various technical, physical and procedural controls deployed so to adequately mitigate the risks. The risk assessment is reviewed at least yearly.

5.2.1 Trusted roles

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

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

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

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

5.2.2 Number of persons required per task

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

Issuance of EV certificates shall require the participation of at least two validation specialists.

5.2.3 Identification and authentication for each role

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

In particular, with regard to the physical access to data rooms and cabinets that contain the CA systems, identification and authentication takes place via personal badge with PIN.

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

5.2.4 Roles requiring separation of duties

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

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

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

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

5.3.2 Background check procedures

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

5.3.3 Training requirements

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

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

5.3.4 Retraining frequency and requirements

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

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

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

5.3.7 Independent contractor requirements

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

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

5.3.8 Documentation supplied to personnel

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

5.4 Audit logging procedures

5.4.1 Types of events recorded

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

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

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

5.4.2 Frequency of processing log

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

5.4.3 Retention period for audit log

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

5.4.4 Protection of audit log

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

5.4.5 Audit log backup procedures

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

5.4.6 Audit collection system (internal vs. external)

No stipulation.

5.4.7 Notification to event-causing subject

No stipulation.

5.4.8 Vulnerability assessments

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

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

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

5.5 Records archival

5.5.1 Types of records archived

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

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

5.5.2 Retention period for archive

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

5.5.3 Protection of archive

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

5.5.4 Archive backup procedures

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

5.5.5 Requirements for time-stamping of records

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

5.5.6 Archive collection system (internal or external)

No stipulation.

5.5.7 Procedures to obtain and verify archive information

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

5.6 Key changeover

5.6.1 Root CA

No stipulation.

5.6.2 Subordinate CA

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

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

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

- Detection: phase in which any person (employee, collaborator or any interested party) who detects a possible incident communicates it to the Committee. The Committee ensures that the report is as detailed as possible and that those who have encountered the problem do not take any action autonomously.

- Identification and analysis: the Committee takes charge of the report and assesses whether it is actually a security incident. If so, it evaluates its severity and proceeds with the following phases. Otherwise, it just closes the incident.
- Containment: in this phase, the harmful effects caused by the incident are contained as much as possible, in order to prevent them from spreading to other areas of the organization.
- Collection of evidence: phase in which the evidence is sought for and collected in order to attach it to the documentation of the incident in case of possible legal consequences or for the need to proceed with more in-depth investigations. All the evidences are collected following guidelines which aim to guarantee a correct and reliable collection.
- Removal and Recovery: phase in which the cause of the damage is removed and the systems affected are reactivated, through the recovery procedures, allowing the systems and users to return to work.
- Incident closure and Notification: once the recovery phase is over, the incident is closed. In this phase, the incident closure is notified to the involved managers.

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

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

Actalis implements a Business Continuity Plan for the CA service in order to ensure that the corruption or loss of one or more computers cannot cause any disruption to the CA platform. In particular, all the critical components of the system are redundant both locally, in the single data center, and between the two IT1 and IT2 data centers. Actalis also implements specific backup plans to guarantee that there is no loss of software and/or data.

5.7.3 Entity private key compromise procedures

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

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

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

5.7.4 Business continuity capabilities after a disaster

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

5.8 CA or RA termination

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

Before the actual termination:

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

On the termination date:

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

6 Technical security controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

6.1.1.1 CA key pair generation

Generation of all CA key pairs (Root CAs and subordinate CAs) takes place in a physically secured environment, following a documented procedure that requires the joint intervention of two different people (“dual control”) in trusted roles. All CA key pairs are generated inside HSMs (Hardware Security Modules) meeting the requirements of section 6.2.1. Execution of the procedure is witnessed by an internal auditor and is recorded in a report which is kept by the Security Officer.

6.1.1.2 RA key pair generation

No stipulation.

6.1.1.3 Subscriber key pair generation

For SSL certificates, the Subscriber’s key pairs shall be generated by the Subscriber itself.

The CA shall reject a certificate request for a public key that does not meet the requirements set forth in sections 6.1.5 and 6.1.6 or if it is a known weak key (such as a "Debian weak key", see http://wiki.debian.org/SSLkeys).

For Code Signing certificates, the Subscriber's Private Keys MUST be generated, stored, and used in compliance with the requirements in section 6.2.7.

6.1.2 Private Key delivery to subscriber

See paragraph 6.1.1.3.

6.1.3 Public key delivery to certificate issuer

The Applicant must submit its public key to the issuing CA in the form of a Certificate Signing Request (CSR) conforming to the PKCS#10 standard [RFC2314].

6.1.4 CA public key delivery to relying parties

Root CA public keys are distributed at least in these ways:

- by publication in the CA repository (in the form of self-signed certificates);
- by inclusion in the lists of trusted Root CAs ("root stores") managed and distributed by software suppliers, such as operating system and/or browser vendors;
- via the Trust-service Status List (TSL) that is published on the AgID website.

Subordinate CA (i.e. issuing CA) public keys, in the form of certificates signed by the Root CA, are provided to Subscribers, together with the Subscriber certificate, and are published in the CA repository.

6.1.5 Key sizes

Root CAs shall use an RSA key pair with a module size of 4096 bit.

Subordinate CAs (i.e. issuing CAs) shall use an RSA key pair with a module size of at least 2048 bits.

Subscriber keys shall be either:

- RSA keys with a module size of at least 2048 bits (up to 4096),
- or ECC keys of type NIST P-256 or P-384.

Effective from June 1, 2021, RSA keys used for Code Signing shall have a module size of at least 3072 bits.

6.1.6 Public key parameters generation and quality checking

The CA shall confirm that public keys meet the requirements set forth in section 6.1.6 of the [BR].

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

Root CA private keys MUST NOT be used to sign Certificates except in the cases listed in §6.1.7 of the [BR]

See also section 7.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

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

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

See section 5.2.2.

6.2.3 Private Key escrow

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

6.2.4 Private Key backup

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

6.2.5 Private Key archival

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

6.2.6 Private Key transfer into or from a cryptographic module

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

6.2.7 Private Key storage on cryptographic module

6.2.7.1 Private key storage for CA keys

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

6.2.7.2 Private key storage for Timestamp Authorities

Actalis' Timestamp Authority protects its signing keys according to [CSBR] section 6.2.7.

6.2.7.3 Private key storage for Signing Services

The Actalis' Code Signing Service ensures that Subscribers' Private Keys are generated, stored, and used in a secure environment that meets the requirements of [CSBR] section 6.2.7.

6.2.7.4 Subscriber Private Key protection and verification

For Private Keys corresponding to **SSL certificates**, the requirements in [BR] section 6.2 are applied.

For Private Keys corresponding to **Code Signing certificates**, the following requirements are applied:

Actalis normally issues Code Signing certificates only for private keys generated, stored and used through the **Actalis' Code Signing Service** (see also section 6.2.7.3).

At its own discretion, Actalis may in some circumstances issue Code Signing certificates on personal cryptographic devices (e.g. smartcards or similar) that comply at least with FIPS 140 Level 2, Common Criteria EAL 4+, or equivalent security criteria.

6.2.8 Method of activating private key

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

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

6.2.9 Method of deactivating private key

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

6.2.10 Method of destroying private key

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

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

6.2.11 Cryptographic Module Rating

See section 6.2.1.

6.3 Other aspects of key pair management

6.3.1 Public key archival

See section 5.5

6.3.2 Certificate operational periods and key pair usage periods

Certificates and private keys shall have a *maximum* operational period according to the following table:

Type	Priv. key usage period	Certificate validity period
Root CA	18 years	20 years
Subordinate CA	12 years	15 years
Subscriber – DV SSL Server	No stipulation	Max 398 days
Subscriber – OV SSL Server	No stipulation	Max 398 days
Subscriber - EV SSL Server	No stipulation	Max 398 days
Subscriber – Code Signing	No stipulation	Max 39 months

See also section 7.1.

6.4 Activation data

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

6.4.1 Activation Data Generation and Installation

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

6.4.2 Activation Data Protection

6.4.2.1 CA keys

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

6.4.2.2 Subscriber keys

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

6.4.3 Other Aspects of Activation Data

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

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

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

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

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

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

6.5.2 Computer security rating

No stipulation.

6.6 Life cycle technical controls

6.6.1 System Development Controls

The development of software systems used to support the trust services provided by Actalis, including the CA service, be it carried out by Actalis itself or on behalf of Actalis by contractors, respects the company's Quality Management System (QMS), compliant with the UNI EN ISO 9001 standard: 2015.

6.6.2 Security Management Controls

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

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 Network security controls

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

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

Security assessments, to verify the presence of any network vulnerabilities, are carried out at least annually by independent experts.

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

6.8 Time-stamping

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

Actalis also operates a Time-Stamping Authority (TSA) intended for use in signing software when used in conjunction with Actalis Code Signing certificates. No guarantee is offered, and no liability will be accepted for any use of the Actalis TSA other than for signing software in combination with Code Signing certificates.

The Actalis TSA service, compliant with RFC3161 and with the applicable requirements in [CSBR], is available at the following URL: http://timestamp.actalis.com

7 Certificate, CRL and OCSP profiles

7.1 Certificate profile

All certificates issued under this CPS conforms to the public specification [RFC5280], which is based on the ITU-T x.509v3 standard (equivalent to ISO/IEC 9594-8:2005) and to the European norms ETSI EN 319-411 and ETSI EN 319 412 (applicable parts).

Unless otherwise requested by the interested parties, qualified certificates according to the eIDAS regulation also comply with the AgID recommendations aimed at fostering the interoperability and use of online services in the Italian context (AgID Determination n.121/2019, and subsequent amendments and additions). Application of the said recommendations is normally declared through the inclusion, in the CertificatePolicies extension (OID 2.5.29.32), of an additional PolicyIdentifier item with value agIDcert (OID 1.3.76.16.6), except where this indication is redundant or inapplicable in view of the requirements of the intended application context.

7.1.1 Version number(s)

All certificates shall be of type X.509 v3.

7.1.2 Certificate content and extensions

All certificates conform to the [RFC 5280] public specification and to the CA/Browser Forum's [BR], [CSBR] or [EVGL] according to certificate type and class.

7.1.2.1 Root CA Certificates

The profile of the Root CA certificate is as follows:

Field	Value
Version	V3 (2)
SerialNumber (hex)	57:0A:11:97:42:C4:E3:CC
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	CN = Actalis Authentication Root CA O = Actalis S.p.A./03358520967 L = Milano C = IT
Validity	from September 22, 2011 to September 22, 2030
Subject	CN = Actalis Authentication Root CA O = Actalis S.p.A./03358520967 L = Milano C = IT
SubjectPublicKeyInfo	<RSA public key of 4096 bits>
SignatureValue	<Root CA signature>
Extension	**Value**
Basic Constraints	critical: CA=true
AuthorityKeyIdentifier (AKI)	<included, KeyID>
SubjectKeyIdentifier (SKI)	52:D8:88:3A:C8:9F:78:66:ED:89:F3:7B:38:70:94:C9:02:02:36:D0
KeyUsage	critical: keyCertSign, cRLSign
ExtendedKeyUsage (EKU)	<not included>
CertificatePolicies	<not included>
SubjectAlternativeName (SAN)	<not included>
AuthorityInformationAccess (AIA)	<not included>
CRLDistributionPoints (CDP)	<not included>

7.1.2.2 Subordinate CA Certificates

7.1.2.2.1 Sub CAs for DV-class certificates

The profile of Sub CA certificates is as follows:

Field	**Value**
Version	V3 (2)
SerialNumber	< includes at least 8 pseudo-random bytes>
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	<Subject DN Root CA>
Validity	<According to section 6.3.2>
Subject	CN = Actalis Domain Validation Server CA G***N*** O = Actalis S.p.A. L = Ponte San Pietro S = Bergamo C = IT
SubjectPublicKeyInfo	<RSA public key of at least 2048 bits>
SignatureValue	<Root CA signature>
Extension	**Value**
Basic Constraints	critical: CA=true
AuthorityKeyIdentifier (AKI)	<Same value as the Root CA SKI extension>
SubjectKeyIdentifier (SKI)	<public key SHA1-digest>
KeyUsage	critical: keyCertSign, cRLSign
ExtendedKeyUsage (EKU)	< serverAuth + clientAuth>
CertificatePolicies	PolicyOID = 2.5.29.32.0 (anyPolicy) CPS-URI = <HTTP address of this CPS>
SubjectAlternativeName (SAN)	<not included>
AuthorityInformationAccess (AIA)	<HTTP address of OCSP responder>
CRLDistributionPoints (CDP)	<HTTP address to access the ARL>

7.1.2.2.2 Sub CAs for DV-class certificates - ACME

Field	Value
Version	V3 (2)
SerialNumber	< includes at least 8 pseudo-random bytes >
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	< Subject DN Root CA >
Validity	< According to section 6.3.2>
Subject	CN = Actalis DV Server ACME CA G***N*** O = Actalis S.p.A. L = Ponte San Pietro S = Bergamo C = IT
SubjectPublicKeyInfo	< RSA public key of at least 2048 bits >
SignatureValue	< Root CA signature >
Extension	**Value**
Basic Constraints	critical: CA=true
AuthorityKeyIdentifier (AKI)	< Same value as the Root CA SKI extension >
SubjectKeyIdentifier (SKI)	< public key SHA1-digest >
KeyUsage	critical: keyCertSign, cRLSign
ExtendedKeyUsage (EKU)	serverAuth + clientAuth
CertificatePolicies	PolicyOID = 2.5.29.32.0 (anyPolicy) CPS-URI = < HTTP address of this CPS >
SubjectAlternativeName (SAN)	< not included >
AuthorityInformationAccess (AIA)	< HTTP address of OCSP responder >
CRLDistributionPoints (CDP)	< HTTP address to access the ARL >

7.1.2.2.3 Sub CAs for OV-class certificates

The profile of Sub CA certificates is as follows:

Field	**Value**
Version	V3 (2)
SerialNumber	< includes at least 8 pseudo-random bytes>
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	<Subject DN Root CA>
Validity	<According to section 6.3.2>
Subject	CN = Actalis Organization Validated Server CA G***N*** O = Actalis S.p.A. L = Ponte San Pietro ST= Bergamo C = IT
SubjectPublicKeyInfo	<RSA public key of 2048 bits>
SignatureValue	<Root CA signature>
Extension	**Value**
Basic Constraints	critical: CA=true
AuthorityKeyIdentifier (AKI)	<Same value as the Root CA SKI extension>
SubjectKeyIdentifier (SKI)	<public key SHA1-digest>
KeyUsage	critical: keyCertSign, cRLSign
ExtendedKeyUsage (EKU)	< serverAuth + clientAuth >
CertificatePolicies	PolicyOID = 2.5.29.32.0 (anyPolicy) CPS-URI = <HTTP address of this CPS>
SubjectAlternativeName (SAN)	<not included>
AuthorityInformationAccess (AIA)	<HTTP address of OCSP responder>
CRLDistributionPoints (CDP)	<HTTP address to access the ARL>

7.1.2.2.4 Sub CAs for EV-class certificates

The profile of Sub CA certificates is as follows:

Field	**Value**
Version	V3 (2)
SerialNumber	< includes at least 8 pseudo-random bytes>
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	<Subject DN Root CA>
Validity	<According to section 6.3.2>
Subject	CN = Actalis Extended Validation Server CA G***N*** O = Actalis S.p.A. L = Ponte San Pietro ST = Bergamo C = IT
SubjectPublicKeyInfo	<RSA public key of at least 2048 bits>
SignatureValue	<Root CA signature>
Extension	**Value**
Basic Constraints	critical: CA=true
AuthorityKeyIdentifier (AKI)	<Same value as the Root CA SKI extension>
SubjectKeyIdentifier (SKI)	<public key SHA1-digest>
KeyUsage	critical: keyCertSign, cRLSign
ExtendedKeyUsage (EKU)	< serverAuth + clientAuth >
CertificatePolicies	PolicyOID = 2.5.29.32.0 (anyPolicy) CPS-URI = <HTTP address of this CPS>
SubjectAlternativeName (SAN)	<not included>
AuthorityInformationAccess (AIA)	<HTTP address of OCSP responder>
CRLDistributionPoints (CDP)	<HTTP address to access the ARL>

7.1.2.2.5 Sub CAs for Code Signing certificates

The profile of Sub CA certificates is as follows:

Field	**Value**
Version	V3 (2)
SerialNumber	< includes at least 8 pseudo-random bytes>
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	<Subject DN Root CA>
Validity	<According to section 6.3.2>
Subject	CN = Actalis Code Signing CA G***N*** O = Actalis S.p.A. L = Ponte San Pietro ST = Bergamo C = IT
SubjectPublicKeyInfo	<RSA public key of at least 2048 bits>
SignatureValue	<Root CA signature>
Extension	**Value**
Basic Constraints	critical: CA=true
AuthorityKeyIdentifier (AKI)	<Same value as the Root CA SKI extension>
SubjectKeyIdentifier (SKI)	<public key SHA1-digest>
KeyUsage	critical: keyCertSign, cRLSign
ExtendedKeyUsage (EKU)	codeSigning
CertificatePolicies	PolicyOID = 2.5.29.32.0 (anyPolicy) CPS-URI = <HTTP address of this CPS>
SubjectAlternativeName (SAN)	<not included>
AuthorityInformationAccess (AIA)	<HTTP address of OCSP responder>
CRLDistributionPoints (CDP)	<HTTP address to access the ARL>

7.1.2.3 Subscriber Certificates

7.1.2.3.1 SSL Server DV

The SSL Server DV certificate is issued with the following profile:

Field	Value
Version	V3 (2)
SerialNumber	<includes at least 8 random bytes>
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	<DN of issuing CA>
Validity	<According to section 6.3.2>
Subject	CN = <one of the IP addresses or FQDNs contained in the SAN extension>
SubjectPublicKeyInfo	<According to section 6.1.5>
SignatureValue	<Sub CA signature>
Extension	**Value**
Basic Constraints	<absent>
AuthorityKeyIdentifier (AKI)	<Same value as the Sub CA SKI extension>
SubjectKeyIdentifier (SKI)	<public key SHA1-digest>
KeyUsage	critical: digitalSignature, keyEncipherment (only for RSA keys)
ExtendedKeyUsage (EKU)	serverAuth (1.3.6.1.5.5.7.3.1), clientAuth (1.3.6.1.5.5.7.3.2)
CertificatePolicies	PolicyOID = 1.3.159.1.22.1 PolicyOID = 2.23.140.1.2.1 CPS-URI = <HTTP address of this CPS>
SubjectAlternativeName (SAN)	<One or more IP addresses and/or FQDNs>
AuthorityInformationAccess (AIA)	<HTTP address of OCSP responder> <HTTP address of the issuing CA certificate>
CRLDistributionPoints (CDP)	<HTTP address to access the CRL>
EmbeddedSCTList (1.3.6.1.4.1.11129.2.4.2)	List of Signed Certificate Timestamps according to RFC 6962 [CT]

In case the certificate was requested for a FQDN like www.<domain>, the SAN extension will also contain <domain> (without the “www” label) provided that Domain Control Validation is carried out on <domain> (and not on www.<domain>). For instance, in a certificate requested for *www.example.com* the SAN extension could contain two items: *www.example.com* and *example.com*.

7.1.2.3.2 SSL Server DV Wildcard

The Wildcard SSL Server DV certificate is issued with the following profile:

Field	Value
Version	V3 (2)
SerialNumber	<includes at least 8 random bytes>
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	<DN of issuing CA>
Validity	<According to section 6.3.2>
Subject	CN = <Wildcard FQDN, also contained in the SAN extension>
SubjectPublicKeyInfo	<According to section 6.1.5>
SignatureValue	<Sub CA signature>
Extension	**Value**
Basic Constraints	<if included, is critical and contains CA=FALSE>
AuthorityKeyIdentifier (AKI)	<Same value as the Sub CA SKI extension>
SubjectKeyIdentifier (SKI)	<public key SHA1-digest>
KeyUsage	critical: digitalSignature, keyEncipherment (only for RSA keys)
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.**23**.1 PolicyOID = 2.23.140.1.2.1 CPS-URI = <HTTP address of this CPS>
SubjectAlternativeName (SAN)	<Same wildcard FQDN as in the Subject.CN field, and possibly further FQDNs>
AuthorityInformationAccess (AIA)	<HTTP address of OCSP responder> <HTTP address of the issuing CA certificate>
CRLDistributionPoints (CDP)	<HTTP address to access the CRL>
EmbeddedSCTList (1.3.6.1.4.1.11129.2.4.2)	List of Signed Certificate Timestamps according to RFC 6962 [CT]

Note: the SAN extension also contains the domain name obtained by removing the wildcard character ('*') from the wildcard FQDN. For instance, in a certificate issued for *.example.com, the SAN extension contains both *.example.com and example.com.

7.1.2.3.3 SSL Server OV

The SSL Server OV certificate is issued with the following profile:

Field	Value
Version	V3 (2)
SerialNumber	<includes at least 8 random bytes>
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	<DN of issuing CA>
Validity	<According to section 6.3.2>
Subject	C = <Two-letter code of country where the Subscriber is based> ST = <State or province where Subscriber is based> L = <Locality where Subscriber is based > O = <Registered name or DBA of Subscriber> CN = <One of the IP addresses or FQDNs contained in the SAN>
SubjectPublicKeyInfo	<According to section 6.1.5>
SignatureValue	<Sub CA signature>
Extension	**Value**
Basic Constraints	<absent>
AuthorityKeyIdentifier (AKI)	<Same value as the Sub CA SKI extension>
SubjectKeyIdentifier (SKI)	<public key SHA1-digest>
KeyUsage	critical: digitalSignature, keyEncipherment (only for RSA keys)
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.**20**.1 PolicyOID = 2.23.140.1.2.2 CPS-URI = <HTTP address of this CPS>
SubjectAlternativeName (SAN)	<One or more IP addresses and/or FQDNs>
AuthorityInformationAccess (AIA)	<HTTP address of OCSP responder> <HTTP address of the issuing CA certificate>
CRLDistributionPoints (CDP)	<HTTP address to access the CRL>
EmbeddedSCTList (1.3.6.1.4.1.11129.2.4.2)	List of Signed Certificate Timestamps according to RFC 6962 [CT]

In case the certificate was requested for a FQDN like www.<domain>, the SAN extension will also contain <domain> (without the “www” label) provided that Domain Control Validation is carried out on <domain> (and not on www.<domain>). For instance, in a certificate requested for *www.example.com* the SAN extension could contain two items: *www.example.com* and *example.com*.

7.1.2.3.4 SSL Server OV Wildcard

The Wildcard SSL Server OV certificate is issued with the following profile:

Field	**Value**
Version	V3 (2)
SerialNumber	<includes at least 8 random bytes>
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	<DN of issuing CA>
Validity	<According to section 6.3.2>
Subject	C = <Two-letter code of country where the Subscriber is based> ST = <State or province where Subscriber is based> L = <Locality where Subscriber is based > O = <Registered name or DBA of Subscriber> CN = <One of the IP addresses or FQDNs contained in the SAN>
SubjectPublicKeyInfo	<According to section 6.1.5>
SignatureValue	<Sub CA signature>
Extension	**Value**
Basic Constraints	<if included, is critical and contains CA=FALSE>
AuthorityKeyIdentifier (AKI)	<Same value as the Sub CA SKI extension>
SubjectKeyIdentifier (SKI)	<public key SHA1-digest>
KeyUsage	critical: digitalSignature, keyEncipherment (only for RSA keys)
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.**19**.1 PolicyOID = 2.23.140.1.2.2 CPS-URI = <HTTP address of this CPS>
SubjectAlternativeName (SAN)	<Same wildcard FQDN as in the Subject.CN field, and possibly further FQDNs>
AuthorityInformationAccess (AIA)	<HTTP address of OCSP responder> <HTTP address of the issuing CA certificate>
CRLDistributionPoints (CDP)	<HTTP address to access the CRL>
EmbeddedSCTList (1.3.6.1.4.1.11129.2.4.2)	List of Signed Certificate Timestamps according to RFC 6962 [CT]

Note: the SAN extension also contains the domain name obtained by removing the wildcard character ('*') from the wildcard FQDN. For instance, in a certificate issued for *.example.com, the SAN extension contains both *.example.com and example.com.

7.1.2.3.5 SSL Server EV

The SSL Server EV certificate is issued with the following profile:

Field	**Value**
Version	V3 (2)
SerialNumber	<includes at least 8 random bytes>
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	<DN of issuing CA>
Validity	<According to section 6.3.2>
Subject	C = <Two-letter code of country where Subscriber is based> ST = <State or province where Subscriber is based> L = <Locality where Subscriber is based> O = <Subscriber's registered name or DBA > CN = <One of the IP addresses or FQDNs contained in the SAN> serialNumber = <Subscriber's VAT number or an equivalent> businessCategory = <Organization type, according to [EVGL]>
SubjectPublicKeyInfo	<According to section 6.1.5>
SignatureValue	<Sub CA signature>
Extension	**Value**
Basic Constraints	<absent>
AuthorityKeyIdentifier (AKI)	<Same value as the Sub CA SKI extension>
SubjectKeyIdentifier (SKI)	<public key SHA1-digest>
KeyUsage	critical: digitalSignature, keyEncipherment (only for RSA keys)
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.**17**.1 PolicyOID = 2.23.140.1.1 CPS-URI = <HTTP address of this CPS>
SubjectAlternativeName (SAN)	<One or more IP addresses and/or FQDNs>
AuthorityInformationAccess (AIA)	<HTTP address of OCSP responder> <HTTP address of the issuing CA certificate>
CRLDistributionPoints (CDP)	<HTTP address to access the CRL>
EmbeddedSCTList (1.3.6.1.4.1.11129.2.4.2)	List of Signed Certificate Timestamps according to RFC 6962 [CT]

In case the certificate was requested for a FQDN like www.<domain>, the SAN extension will also contain <domain> (without the "www" label) provided that Domain Control Validation is carried out on <domain> (and not on www.<domain>). For instance, in a certificate requested for *www.example.com* the SAN extension could contain two items: *www.example.com* and *example.com*.

7.1.2.3.6 Qualified Website Authentication Certificate

The qualified SSL Server certificate ("Qualified Website Authentication Certificate"), variant of the SSL Server EV certificate, is issued with the following profile:

Field	**Value**
Version	V3 (2)
SerialNumber	<includes at least 8 random bytes>
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	<DN of issuing CA>
Validity	<According to section 6.3.2>
Subject	C = <Two-letter code of country where Subscriber is based> ST = <State or province where Subscriber is based> L = <Locality where Subscriber is based> STREET=<street where Subscriber is based > O = <Subscriber's registered name or DBA > CN = <One of the IP addresses or FQDNs contained in the SAN> serialNumber = <Subscriber's VAT number or an equivalent> joiCountryName=< code of the country where the Subscriber is registered> businessCategory = <Organization type, according to [EVGL]> organizationIdentifier = <according to [EVGL]>
SubjectPublicKeyInfo	<According to section 6.1.5>
SignatureValue	<Sub CA signature>
Extension	**Value**
Basic Constraints	<absent>
AuthorityKeyIdentifier (AKI)	<Same value as the Sub CA SKI extension>
SubjectKeyIdentifier (SKI)	<public key SHA1-digest>
KeyUsage	critical: digitalSignature, keyEncipherment (only for RSA keys)
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.**17**.1 PolicyOID = 2.23.140.1.1 PolicyOID = 0.4.0. 194112.1.4 (QCP-w) CPS-URI = <HTTP address of this CPS>
SubjectAlternativeName (SAN)	<One or more IP addresses and/or FQDNs, according to [EVGL]>
AuthorityInformationAccess (AIA)	<HTTP address of OCSP responder> <HTTP address of the issuing CA certificate>
CRLDistributionPoints (CDP)	<HTTP address to access the CRL>
QCStatements	id-etsi-qcs-QcCompliance id-etsi-qcs-QcPDS id-etsi-qcs-QcType
cabfOrganizationIdentifier	<according to [EVGL]>
EmbeddedSCTList (1.3.6.1.4.1.11129.2.4.2)	List of Signed Certificate Timestamps according to RFC 6962 [CT]

7.1.2.3.7 Code Signing

The Code Signing certificate is issued with the following profile:

Field	Value
Version	V3 (2)
SerialNumber	<includes at least 8 random bytes>
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	<DN of issuing CA>
Validity	<According to section 6.3.2>
Subject	C = <Two-letter code of country where the Subscriber is based> ST = <State or province where Subscriber is based> L = <Locality where Subscriber is based > O = <Registered name or DBA of Subscriber> OU = <optional> CN = <Same value as the O field>
SubjectPublicKeyInfo	<According to section 6.1.5>
SignatureValue	<Sub CA signature>
Extension	**Value**
Basic Constraints	<absent>
AuthorityKeyIdentifier (AKI)	<Same value as the Sub CA SKI extension>
SubjectKeyIdentifier (SKI)	<public key SHA1-digest>
KeyUsage	critical: digitalSignature
ExtendedKeyUsage (EKU)	critical: codeSigning (1.3.6.1.5.5.7.3.3)
CertificatePolicies	PolicyOID = 1.3.159.1.**21**.1 PolicyOID = 2.23.140.1.4.1 CPS-URI = <HTTP address of this CPS>
SubjectAlternativeName (SAN)	<Optional; may not contain FQDNs or IP addresses>
AuthorityInformationAccess (AIA)	<HTTP address of OCSP responder> <HTTP address of the issuing CA certificate>
CRLDistributionPoints (CDP)	<HTTP address to access the CRL>

7.1.2.4 All certificates

The CA may include in the certificate further information (e.g. additional extensions and/or additional extension fields or values), provided that such additional information:

1) fully complies with both the [RFC 5280] and CAB Forum Requirements and Guidelines; and
2) cannot mislead Relying Parties about the certificate information verified by the CA.

7.1.3 Algorithm object identifiers

Certificates are normally signed using one of the following algorithms:

Algorithm name	Object Identifier
sha256WithRSAEncryption	1.2.840.113549.1.1.11

OSCP responses are signed using one of the following algorithms:

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

7.1.4 Name forms

7.1.4.1 Issuer Information

The content of the certificate Issuer DN field shall match the Subject DN of the Issuing CA to support name chaining as specified in [RFC 5280], section 4.1.2.4.

7.1.4.2 Subject Information in Subscriber certificates

By issuing the Certificate, the CA represents that it followed the procedures set forth in this CPS to verify that, as of the Certificate's issuance date, all of the Subject Information was accurate. The CA shall not include a Domain Name or IP Address in a Subject attribute except as specified in section 3.2.2.4 or section 3.2.2.5.

7.1.4.2.1 Subject Alternative Name Extension

For all **SSL Server** certificates, the following rule applies:

- The ***SubjectAlternativeNames*** (**SAN**) extension must contain at least one item. Each of the items in this extension must be an IP address or an FQDN that the Subscriber either owns or controls. Internal server names or reserved IP addresses are not allowed. See also section 3.1.1.

This extension is marked *critical* in case the Subject DN is empty.

The underscore character ("_") is not allowed in FQDNs.

7.1.4.2.2 Subject Distinguished Name Fields

For **DV SSL Server** certificates, the following rules apply:

- The **commonName** attribute (OID 2.5.4.3) of the Subject DN must contain a single IP address or Fully Qualified Domain Name (FQDN) among those contained in the SAN extension (see previous section). If a FQDN is too long to fit (> 64 chars), this attribute will be omitted resulting in an empty Subject DN.
- No other Subject DN attributes shall be present.
- The Subject field may be empty in DV SSL Server certificates, e.g., when it cannot accommodate a very long FQDN (longer that 64 characters).

For **OV SSL Server and Code Signing certificates**, the following rules apply:

- The ***commonName*** (OID 2.5.4.3) attribute of the Subject DN:
  - in an SSL Server certificate, must contain one single IP address or Fully Qualified Domain Name (FQDN) among those contained in the SAN extension (see previous section);
  - in a Code Signing certificate, must contain the same value as the **organizationName** attribute;
- The ***organizationName*** attribute (OID 2.5.4.10) of the Subject DN must contain the name or DBA (Doing Business As) of the Subscriber. For an SSL Server certificate, it must be the entity that either owns or controls all the FQDNs and/or IP addresses included in the certificate.

- The ***localityName*** attribute (OID 2.5.4.7) of the Subject DN must contain the name of the locality (e.g., city) where the Subscriber is located (main place of business).
- The ***stateOrProvinceName*** attribute (OID 2.5.4.8) of the Subject DN must contain the name of the province (for Italian organizations) or Region/State (for foreign organizations) where the Subscriber's principal place of business is located.
- The ***countryName*** attribute (OID 2.5.4.6) of the Subject DN must contain the ISO 3166 two-letter code (e.g., "IT") of the country where the Subscriber's principal place of business is located.

For **EV SSL Server certificates,** the following additional rules also apply:

- The **businessCategory** attribute (OID 2.5.4.15) of the Subject DN must contain the Subscriber's organization type (either "Private Organization" or "Government Entity").
- The ***serialNumber*** attribute (OID 2.5.4.5) of the Subject DN must contain the VAT Number or other official registration number of the Subscriber.
- The ***jurisdictionOfIncorporationCountryName*** attribute (OID 1.3.6.1.4.1.311.60.2.1.3) of the Subject DN must contain the two-letter ISO 3166 code of the country where the Subscriber's organization was registered or incorporated.
- The ***streetAddress*** attribute (OID 2.5.4.9) of the Subject DN must contain the address (e.g., street name and building number) of the Subscriber's main place of business.

For **Qualified Website Authentication Certificates (QWACs),** the following additional rules also apply:

- The ***organizationIdentifier*** attribute (OID 2.5.4.97) of the Subject DN must be populated according to the [EVGL].

Note: in the case of QWACs, the **cabfOrganizationIdentifier** extension (OID 2.23.140.3.1) is also added to the certificate (see also paragraph 7.1.2.3.6) and is populated according to the [EVGL].

7.1.4.3 Subject Information in Subordinate CA certificates

By issuing a Subordinate CA Certificate, Actalis represents that it followed the procedure set forth in this CPS to verify that, as of the certificate's issuance date, all of the Subject Information was accurate.

7.1.5 Name constraints

Actalis may issue, subject to a contractual agreement, Subordinate CA certificates to external entities, signed by an Actalis' root CA key. In such a case, the Subordinate CA certificate will be technically constrained in compliance with section 7.1.5 of the [BR].

7.1.6 Certificate policy object identifier

See section 1.4.

7.1.7 Usage of Policy Constraints extension

Not applicable.

7.1.8 Policy qualifiers syntax and semantics

See section 7.1.

7.1.9 Processing semantics for the critical Certificate Policies extension

Not applicable.

7.2 CRL profile

The CRLs shall conform to public specification [RFC 5280].

The version of CRL is v2 (1).

Besides the mandatory information, the CRLs also contain:

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

CRLs are signed with the sha256WithRSAEncryption algorithm (OID 1.2.840.113549.1.1.11).

Associated with each CRL entry, the *reasonCode* extension is used to indicate the reason of revocation.

For SSL Certificates issued on or after October 1, 2022, when an SSL certificate is revoked for one of the following reasons, the specified CRLReason is included in the reasonCode extension of the corresponding CRL entry. Otherwise, the CRLReason code is omitted:

- keyCompromise
- privilegeWithdrawn
- cessationOfOperation
- affiliationChanged
- superseded.

7.3 OCSP profile

The OSCP service shall conform to public specification [RFC6960].

OCSP responses are not signed with the private key of the issuing CA, but rather with a specific key of the OCSP responder. Therefore, the OCSP responder's certificate contains the **ocspSigning** (OID 1.3.6.1.5.5.7.3.9) key purpose in its ExtendedKeyUsage extension. The OCSP responder's certificate also contains the **id-pkix-ocsp-nocheck** (OID 1.3.6.1.5.5.7.48.1.5) extension.

OCSP responses conforms to the "pkix-ocsp-basic" profile (OID 1.3.6.1.5.5.7.48.1.1).

7.3.1 Version number(s)

The version of OCSP responses is v1 (0).

7.3.2 OCSP extensions

OCSP responses contain the Nonce extension (OID 1.3.6.1.5.5.7.48.1.2).

8 Compliance audits and other assessments

Actalis shall issue certificates and operate its PKI in accordance with applicable law and comply with CAB Forum's requirements [BR] and guidelines [EVGL].

8.1 Frequency or circumstances of assessment

The compliance of the Actalis' CA services to this CPS, to Regulation (EU) No. 910/2014 ("eIDAS"), to the applicable ETSI standards and to the [BR] and [EVGL] requirements is verified on an annual basis by an accredited Conformity Assessment Body (CAB).

Moreover, always on an annual basis, an internal auditing activity is performed on the CA services that also takes into account aspects related to information security, applicable data protection rules and internal policies and procedures.

8.2 Identity and qualification of assessor

Compliance audits on the CA are carried out by a Conformity Assessment Body (CAB) accredited in compliance with Regulation (EC) no. 765/2008, through personnel that is qualified and competent on the subject of conformity assessments, according to the ETSI EN 319 403 norm, of Trust Service Providers and the related trust services provided under the eIDAS Regulation. Any second part audits are also performed by accredited bodies in compliance with Regulation (EC) no. 765/2008.

8.3 Assessor's relationship to assessed entity

The Assessment Bodies (CABs) that perform audits on the CA service, and possibly on the external RAs that collaborate with the CA, have no relation with Actalis.

The internal auditor does not belong to the organizational structure that deals with CA activities.

8.4 Topics covered by assessment

External audits shall evaluate, based on the ETSI EN 319 411-1 and ETSI EN 319 411-2 norms, the compliance with the [BR], [CSBR] and [EVGL], and the proper operation of the CA as described in this CPS, including any Delegates Third Parties (DTPs) that are not "Enterprise RA", with the exception of any "technically constrained" subordinated CAs (see par. 1.3.1).

Non-compliant DTPs cannot continue to perform the functions delegated to them until the non-conformities have been completely remediated.

8.5 Actions taken as a result of deficiency

The actions resulting from any non-compliance detected during audits (failure to meet the requirements defined in the regulations, standards, and applicable procedures) depend on the nature and severity of the non-compliance detected, on the rules for the management of non-compliances defined by the Assessment Body (CAB) and/or the internal non-conformity management procedures.

In general, if a substantive non-compliance results from an audit, Actalis will develop a plan to remedy this non-compliance as quickly as possible. This plan could result in changes to CA certification policies and/or practices, and/or to the CA software. The plan will be presented to the Actalis direction for approval, and then to any third parties with whom Actalis has commitments in this regard.

8.6 Communication of results

The result of the audit carried out by the CAB is communicated to the company management and to the heads of the organizational structure in charge of providing the CA service. The result of the audit is also communicated to the national Supervisory Body (AgID) by sending to them the audit report issued by the CAB.

The CA publishes the result of the audit within three months of the end of the audit period.

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

8.7 Self-audits

During the period in which the CA issues certificates, the CA shall monitor adherence to this CPS (and linked documents if any) and to the [BR], [CSBR]and [EVGL] requirements, and strictly control its service quality, by performing self-audits on at least a quarterly basis. Self-audits shall be carried out against a randomly selected sample of at least three percent of the certificates issued in the period beginning immediately after the last sample was taken.

9 Other business and legal matters

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

9.1 Service fees

9.1.1 Certificate issuance or renewal fees

The maximum service fees are published on the CA web site.

Different conditions may be negotiated case by case, depending on volumes requested.

Service fees are subject to change without notice.

9.1.2 Certificate access fees

Not applicable.

9.1.3 Revocation or status information access fees

Access to certificate status services (CRL, OCSP) is free and open to everybody.

9.1.4 Fees for other services

No stipulation.

9.1.5 Refund policy

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

9.2 Financial responsibility

9.2.1 Insurance coverage

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

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

Please refer to par. 9.2.1.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

The following information is considered and treated as confidential:

- all information supplied to the CA by Applicants, except that intended to be included in Certificates;

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

9.3.2 Information not within the scope of confidential information

All information that must be public for compliance with applicable law (see section 9.15) and regulations (including CAB Forum's Requirements and Guidelines), or on explicit request from the Subscriber, is considered non-confidential. In particular, the following information is considered non-confidential:

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

9.3.3 Responsibility to protect confidential information

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

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

9.4 Privacy of personal information

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

9.4.1 Privacy plan

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

9.4.2 Information treated as private

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

9.4.3 Information not deemed private

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

9.4.4 Responsibility to protect private information

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

9.4.5 Notice and consent to use private information

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

9.4.6 Disclosure pursuant to judicial or administrative process

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

9.4.7 Other information disclosure circumstances

Not applicable.

9.5 Intellectual property rights

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

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

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

9.6 Representations and warranties

9.6.1 CA Representations and Warranties

By issuing a Certificate, the CA makes certain warranties to the following Certificate Beneficiaries:

- the Subscriber;
- all Application Software Suppliers (e.g. certain web browser and/or operating system vendors) who have a Root Certificate distribution agreement in place with Actalis;
- all Relying Parties who reasonably rely on a valid certificate.

In general, Actalis undertakes to operate, in all material aspects, in compliance with this CPS.

More specifically, Actalis represents and warrants to the Certificate Beneficiaries that:

- [for SSL Server certificates] at the time of issuance, the CA followed the procedure described in this CPS for verifying that the Applicant either had the right to use, or had control of, the Domain Name(s) and IP address(es) listed in the Certificate's Subject field and subjectAltName extension (or, only in the case of Domain Names, was delegated such right or control by someone who had such right to use or control);

- at the time of issuance, the CA followed the procedures described in this CPS for verifying that the Subject authorized the issuance of the Certificate and that the Applicant Representative was authorized to request the Certificate on behalf of the Applicant;
- at the time of issuance, the CA followed the procedures described in this CPS for verifying the accuracy of all Subject information contained in the Certificate;
- [for Code Signing certificates] at the time of issuance, the CA followed a procedure for reducing the likelihood that the information contained in the organizationalUnitName attribute of the Certificate's Subject would be misleading;
- if the Certificate contains Subject Identity Information, the CA verified the identity of the Applicant in accordance with the procedures described in this CPS;
- in the case of EV certificates, the CA has confirmed with the Incorporating or Registration Agency in the Subject's Jurisdiction of incorporation or Registration that, as of the date the Certificate was issued, the Subject named in the Certificate legally exists as a valid organization or entity in the Jurisdiction of Incorporation or Registration;
- if the CA and Subscriber are not affiliated, the Subscriber and CA are parties to a legally valid and enforceable Subscriber Agreement that satisfies the [BR] or the [EVGL] (depending on certificate class), or, if the CA and Subscriber are the same entity or are affiliated, the Applicant Representative acknowledged the Terms of Use;
- the CA maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates;
- the CA will revoke the Certificate for any of the reasons specified in this CPS;
- for Code Signing certificates, at the time of issuance the CA provided the Subscriber with documentation on how to securely store and prevent the misuse of private keys associated with the certificates.

9.6.2 RA Representations and Warranties

RAs must ensure their full compliance with the contract signed with the CA, in particular (but not only) to:

- accurate and secure I&A (authentication identification) of Applicants;
- diligent preservation of all the collected evidence (unless it is the responsibility of the CA, according to the specific contract stipulated with the RA), for the entire duration of the contract;
- proper use of the tools and transmission channels that the CA makes available to them.

9.6.3 Subscriber Representations and Warranties

Prior to the issuance of a Certificate, the CA shall obtain either the Applicant's agreement to a Subscriber Agreement with the CA, or the Applicant's acknowledgement of the Terms of Use. As part of the Subscriber Agreement or Terms of Use, the Applicant shall make the commitments and warranties listed below.

The Applicant represents and warrants to:

- read, understand and fully accept this CPS;
- request the certificate by the methods prescribed in this CPS;
- provide the CA with true, accurate and complete information at all times;
- ensure confidentiality of secret codes (e.g. passwords) received from the CA;

- take all reasonable measures to avoid compromise of its private keys;
- in particular, for Code Signing key pairs:
  - generate, store and use the key pairs within a hardware cryptographic device that meets or exceed the requirements as defined in §6.2.11 of this CPS; and,
  - keep the said hardware cryptographic device physically separate from the device (e.g. PC) that hosts the code signing function until a signing session is begun;
- install and start using the certificate only after checking that it contains correct information;
- use the certificate only in the ways and for the purposes provided for in this CPS;
- never use its private keys, for no reason whatsoever, for issuing other certificates in turn;
- in the event of confirmed compromise of any of its private keys, immediately request revocation of the corresponding certificates and immediately stop using those certificates;
- in the event of CA compromise, immediately stop using its certificates;
- immediately request revocation of a certificate in the event that 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;
- respond within 24 hours to requests by the CA related to possible improper use of certificates or possible key compromises;
- upon revocation of their certificate(s), immediately stop using the revoked certificates, and:
  - in the case of Code Signing certificates: immediately remove the signed software from the web sites on which it is published;
  - in the case of SSL Server certificates: immediately remove the certificate from the servers on which it is installed.
- stop using certificates upon their expiration.

Moreover, the Subscriber shall:

- in case of Code Signing certificates: not sign malicious software (malware) and not describe the signed software in a misleading way with respect to its real functionality and purpose;
- in case of SSL Server certificates: install the certificate only on the servers that are accessible at the subjectAlternativeName(s) listed in the Certificate and operate those servers only in the ways allowed by this CPS and for lawful purposes only.

Subscribers acknowledge and accept that the CA, if made aware that a Subscriber's certificate is being used for unlawful purposes (e.g. phishing, Man-In-The-Middle attacks, distribution of malware, etc.) or for issuing other certificates, will revoke that Certificate immediately and without any notice.

9.6.4 Relying Party Representations and Warranties

The term "Relying Parties" refers to all those entities (other than Subscribers) that rely on certificates for taking decisions (such as making information or resources available to the Subscriber, use the information or resources obtained from the Subscriber, etc.).

Each Relying Party, prior to relying on an Actalis certificate, represents and warrants that it:

- has made a reasonable effort to acquire a sufficient understanding of certificates and PKIs;
- has read, understands, and agrees to this CPS, including section 9.8 (limitations of liability);
- has verified the status of the certificate by one of the means described in section 4.10;
- will NOT rely on a certificate that is expired or revoked.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of warranties

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

9.8 Limitations of liability

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

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

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

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

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

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

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

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

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

9.9 Indemnities

9.9.1 Indemnification by CAs

The CA shall abide by section 9.9.1 of the [BR] towards Application Software Suppliers who have a Root Certificate distribution agreement in place with Actalis.

9.9.2 Indemnification by Subscribers

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

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

9.10 Term and termination

9.10.1 Term

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

9.10.2 Termination

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

9.10.3 Effect of termination and survival

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

9.11 Individual notices and communications with participants

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

Requests for assistance related to the CA service herein described (e.g. technical questions, problems installing the certificate, certificate not received, etc.) can be addressed to Actalis only when the involved certificates have

been purchased directly from Actalis. When the involved certificates have instead been purchased from a re-seller, assistance must be requested to that reseller. The terms for requesting assistance are published on the CA's website as well as on the certificate purchase and/or request portal.

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

9.12 Amendments

9.12.1 Procedure for amendment

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

9.12.2 Notification mechanism and period

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

9.12.3 Circumstances under which OID must be changed

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

9.13 Dispute resolution provisions

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

9.14 Governing law

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

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

9.15 Compliance with applicable law

The main applicable laws are listed below:

- Regulation (EU) 2014/910 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93 / EC (also "eIDAS").
- Legislative Decree March 7, 2005, No. 82: "Codice dell'Amministrazione Digitale", G.U. n.112 of 16 May 2005, and subsequent amendments and integrations (also "CAD").
- Legislative Decree 30 June 2003, n. 196: " Codice in materia di protezione dei dati personali ", G.U. n. 174 of 29 July 2003, and subsequent amendments and integrations.

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data, as well as on the free movement of such data and repealing Directive 95/46/EC (also “General Data Protection Regulation” or GDPR).

9.16 Miscellaneous provisions

9.16.1 Entire agreement

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

9.16.2 Assignment

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

9.16.3 Severability

The CA will abide by section 9.6.13 of the [BR], if applicable, and to the general Terms and Conditions published on the CA website.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

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

9.16.5 Force majeure

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

9.17 Other provisions

9.17.1 Service levels

The CA guarantees the following minimum service levels:

Metric	Objective	Measurement basis
CRL and OCSP availability (24 x 7)	99.8 %	annual
CA website availability (24 x 7)	99.8 %	annual
Certificate issuing time	max 5 working days in 95% of all cases	annual
Time for certificate revocation (when requested on-line)	max 2 minutes in 95% of all cases	annual
Time for certificate revocation (when requested by e-mail, ordinary mail or fax)	max 6 hours in 95% of all cases	annual