



CONFORMITY DECLARATION

WE HEREBY DECLARE THAT THE COMPANY

ACTALIS SPA

Via San Clemente, 53
24036 Ponte San Pietro (BG), ITALY

IS COMPLIANT

for issuing and management of:

SSL Certificates of EV/OV/DV classes,
Code Signing certificates and
S/MIME Certificates

in accordance with:

ETSI EN 319 411-1 (v 1.1.1 – 2016/02)
ETSI EN 319 411-2 (v. 2.1.1 – 2016/02)
ETSI EN 319 412-4 (v 1.1.1 – 2016/02)

and

CA/Browser Forum Baseline Requirements
(Version 1.5.7 April 29, 2018)
CA/Browser Forum EV Guidelines
(Version 1.6.8 March 09, 2018)

This declaration is valid only referred to full audit report ZIG: 60576646 as of June 05, 2018

Certificate n° IT281959

Date of issuance: June 05, 2018



ANDREA FILIPPI – Local Technical Manager



**ANNEX TO THE CONFORMITY DECLARATION n° IT281959
ISSUED BY BUREAU VERITAS ITALIA
AUDIT REPORT ZIG 60576646 June 05, 2018**

Audit Requirements

The audit requirements are defined in the following technical specification:

- ETSI EN 319 411-1 (v 1.1.1 – 2016/02)
- ETSI EN 319 411-2 (v. 2.1.1 – 2016/02)
- ETSI EN 319 412-4 (v 1.1.1 – 2016/02)

and

- CA/Browser Forum Baseline Requirements
(Version 1.5.7 April 29, 2018)
- CA/Browser Forum EV Guidelines
(Version 1.6.8 March 09, 2018)

The applicable ETSI certification policies are: DVCP, OVCP, EVCP, LCP, NCP

The audit object is the following Actalis's Certification Authority services:

- Issuing and management of SSL Server certificate of EV, OV, DV classes
- Issuing and management of Code Signing certificates
- Issuing and management of S/MIME certificates

Actalis Certification Practice Statement: 4.1 as of 27/04/2018
Certificate Policy for S/MIME: LCP
Certificate Policy for Code Signed: NCP
Observation period: June 06, 2017 – June 05, 2018

Audit result

- The audit object fulfills all applicable requirements from the audit criteria, as detailed in Full Audit (Stage 2) report ZIG #60576646 June 05, 2018
- All requirements for a CA Practice according to rules and standards together with the therein demanded measures are implemented in terms of the selected Certificate Policy.
- The audited CA takes the responsibility for the requirements fulfillment.
- The CA provides the certification service according to the definitions of the Certificate Practice Statement rel 4.1 as of April 27, 2018.
- The Certificate Policy is part of an effective certificate policy management with regulations concerning responsibilities, communication and PDCA cycle.

Root CA

Subject DN	Subject Key ID	SHA256 fingerprint
CN = Actalis Authentication Root CA	52 d8 88 3a c8	55:92:60:84:EC:96:3A:64:B9:6E:2A:
O = Actalis S.p.A./03358520967	9f 78 66 ed 89	BE:01:CE:0B:A8:6A:64:FB:FE:BC:C7:
L = Milan	f3 7b 38 70 94	AA:B5:AF:C1:55:B3:7F:D7:60:66
C = IT	c9 02 02 36 d0	

Intermediate CAs (issuing CAs)

Subject DN	Subject Key ID	SHA256 fingerprint
CN = Actalis Authentication CA G3 O = Actalis S.p.A./03358520967 L = Milano S = Milano C = IT	AA AA FD CA 8C 1D 4D F1 2E 83 E1 06 FC FA 8E EA 0E 23 AE 3D	A1:D2:5D:28:94:1F:AF:C0:C2:A6:EB: 9E:59:6A:54:78:6E:73:1D:0A:4A:8E: 32:1D:B9:F1:CF:2C:24:FD:D6:09
CN = Actalis Organization Validated Server CA G1 O = Actalis S.p.A./03358520967 L = Ponte San Pietro S = Bergamo C = IT	23 B4 CC 8E BE 20 F9 24 D5 A9 90 A5 0A 26 39 8E D5 95 05 96	36:51:F9:B3:6A:1D:A9:83:20:0C:6E: E4:EF:CE:CF:A4:DE:FC:05:94:66:68: 9D:AA:1A:6D:B6:84:A5:4C:9E:7B
CN = Actalis Extended Validation Server CA G1 O = Actalis S.p.A./03358520967 L = Milano S = Milano C = IT	61 C1 E4 86 1E 4D 6D 74 74 BC D9 97 3B 31 71 78 CB 3F 9F DC	49:42:AD:04:41:21:8A:EC:22:DA:C4: 17:AC:49:9D:7D:E4:C5:4E:CB:D3:D3: :35:F3:4A:5F:8B:06:8F:6E:6C:96
CN = Actalis Domain Validation Server CA G1 O = Actalis S.p.A./03358520967 L = Ponte San Pietro S = Bergamo C = IT	1B 42 7F 5C 45 7E FF 7E 1E 1E 41 9C F3 AD AE 35 C6 65 EB C5	FD:98:B4:0E:B9:4A:AC:09:76:22:17: 9F:1E:3A:CD:DA:CD:3F:3C:95:27:CD: :69:74:DC:36:14:D0:9A:D3:7A:AE
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	AB:DE:EC:53:14:90:98:F8:A0:B0:7E: FD:97:2B:34:5A:89:BE:DE:8E:DE:69: 75:E6:1B:E9:5E:E0:26:DA:7E:FA

Summary of the audit requirements

The ETSI specification contains the following:

5.1 General requirements

The CA maintains compliant documentation and statement structure

5.2 Certification Practice Statement requirements

The CA maintains a compliant presentation of policies and practices, along with complete CA hierarchy, signature algorithms and parameters employed.

5.3 Certificate Policy name and identification

The CA maintains certificates CP identifier. The identifiers for the certificate policies specified in the present document are listed above.

5.4 PKI participants

The CA ensures specific roles to all involved parties (CA itself, subscribers, subjects, others identified by the CA)

5.5 Certificate usage

The CA ensures that the policies (listed above) place no constraints on the user community and applicability of the certificate.

6.1 Publication and repository responsibilities



The CA ensures dissemination life cycle, that makes certificates available to subscribers, subjects and relying parties.

6.2 Identification and authentication

The CA ensures requirements for naming in certificates, verification of the identity of the subscriber and subject, updating due to change to the subject's attributes, revoking certificates

6.3 Certificate Life-Cycle operational requirements

The CA ensures that certificate life cycle is maintained under controlled conditions

6.4 Facility, management, and operational controls

The CA ensures physical, procedural, personnel, environmental and logical security conditions

6.5 Technical security controls

The CA ensures that key pairs life cycle is maintained under controlled conditions, including all technical conditions for network and computer security

6.6 Certificate, CRL, and OCSP profiles

The CA ensures that certificates, CRL profile and OCSP profile meet the specified requirements

6.7 Compliance audit and other assessment

The CA ensures full availability to third-party auditing activities and ensures full collaboration at all stages

6.8 Other business and legal matters

The CA ensures that all applicable organizational, financial and legal topics are fulfilled

6.9 Other provisions

The CA provides the capability to allow third parties to check and test all the certificate types; the CA allows use of such capability even to visual impaired people

The CA ensures impartiality and privacy compliance where applicable for all certificate life cycle activities



ANDREA FILIPPI – Local Technical Manager