Mozilla - CA Program

Case Information

Case Number	00000067	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	Actalis	**Request Status**	Initial Request Received

Additional Case Information

Subject	Enable Email Trust Bit for Actalis Authentication Root CA	**Case Reason**	

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org /show_bug.cgi?id=1176188

General information about CA's associated organization

CA Email Alias 1	cps-admin@actalis.it		
CA Email Alias 2			
Company Website	http://www.actalis.it/	**Verified?**	Verified
Organizational Type	Public Corporation	**Verified?**	Verified
Organizational Type (Others)		**Verified?**	Not Applicable
Geographic Focus	Italy	**Verified?**	Verified
Primary Market / Customer Base	Actalis CA has a wide number of customers, mainly banks and local government. Actalis is a Qualified certification service provider according to the EU Signature Directive (Directive 1999/93/EC).	**Verified?**	Verified
Impact to Mozilla Users	This root is already trusted for secure email on other platforms.	**Verified?**	Verified

Response to Mozilla's list of Recommended Practices

Recommended Practices	https://wiki.mozilla.org /CA:Recommended_Practices#CA_Recommended_Practices	**Recommended Practices Statement**	I have reviewed Mozilla's list of Recommended Practices, and confirm that we follow those practices, with exceptions and clarifications noted in the text box below.
CA's Response to Recommended Practices	* Document Handling of IDNs in CP/CPS - CPS section 3.3.1.1: As of the date of revision of this CPS, Internationalized Domain Names (IDN) are not allowed: all FQDNs to be inserted in the certificate must therefore be comprised of ASCII characters only. * Revocation of Compromised Certificates - CPS section 4.9.4 * DNS names go in SAN - We meet this requirement; this is	**Verified?**	Verified

made clear in §3.1.1 and in chapter 7 of our CPS
* Domain owned by a Natural Person - We do not issue certs to natural persons; this is documented in §1.3.3 of our CPS

Response to Mozilla's list of Potentially Problematic Practices

Potentially Problematic Practices	https://wiki.mozilla.org/CA:Problematic_Practices#Potentially_problematic_CA_practices	**Problematic Practices Statement**	I have reviewed Mozilla's list of Potentially Problematic Practices, and confirm that we do not do those practices, with exceptions and clarifications noted in the text box below.
CA's Response to Problematic Practices	* SSL certs are OV or EV * CPS section 4.1: It is also possible to apply for a “wildcard” SSL Server certificate	**Verified?**	Verified

Root Case Record # 1

Root Case Information

Root Certificate Name	Actalis Authentication Root CA	**Root Case No**	R00000091
Request Status	Need Information from CA	**Case Number**	00000067

Additional Root Case Information

Subject	Turn on Email Trust Bit for Actalis Authentication Root CA root cert

Technical Information about Root Certificate

O From Issuer Field	Actalis S.p.A./03358520967	**Verified?**	Verified
OU From Issuer Field		**Verified?**	Verified
Certificate Summary	Requesting that the email trust bit be turned on for the "Actalis Authentication Root CA" root certificate that was included via Bugzilla Bug #520557, and enabled for EV via Bugzilla Bug #957548.	**Verified?**	Verified
Root Certificate Download URL	Already included	**Verified?**	Not Applicable
Valid From	2011 Sep 22	**Verified?**	Verified
Valid To	2030 Sep 22	**Verified?**	Verified
Certificate Version	3	**Verified?**	Verified
Certificate Signature Algorithm	SHA-256	**Verified?**	Verified
Signing Key Parameters	4096	**Verified?**	Verified
Test Website URL (SSL) or Example Cert	https://ssltest-a.actalis.it:8443	**Verified?**	Verified

CRL URL(s)	http://portal.actalis.it/Repository/AUTH-ROOT/getLastCRL http://crl03.actalis.it/Repository/AUTH-G3/getLastCRL	**Verified?**	Verified
OCSP URL(s)	http://portal.actalis.it/VA/AUTH-ROOT http://ocsp03.actalis.it/VA/AUTH-G3 OCSP responses have an expiration time of 1 day	**Verified?**	Verified
Revocation Tested	http://certificate.revocationcheck.com/ssltest-a.actalis.it No errors.	**Verified?**	Verified
Trust Bits	Code; Email; Websites	**Verified?**	Verified
SSL Validation Type	OV; EV	**Verified?**	Verified
EV Policy OID(s)	1.3.159.1.17.1	**Verified?**	Verified
EV Tested	// CN=Actalis Authentication Root CA,O=Actalis S.p.A./03358520967,L=Milan,C=IT "1.3.159.1.17.1", "Actalis EV OID", SEC_OID_UNKNOWN, { 0x55, 0x92, 0x60, 0x84, 0xEC, 0x96, 0x3A, 0x64, 0xB9, 0x6E, 0x2A, 0xBE, 0x01, 0xCE, 0x0B, 0xA8, 0x6A, 0x64, 0xFB, 0xFE, 0xBC, 0xC7, 0xAA, 0xB5, 0xAF, 0xC1, 0x55, 0xB3, 0x7F, 0xD7, 0x60, 0x66 }, "MGsxCzAJBgNVBAYTAklUMQ4wDAYDVQQHDAVNaWxhbjEjMCEGA1UECgwaQWN0YWxp" "cyBTLnAuQS4vMDMzNTg1MjA5NjcxJzAlBgNVBAMMHkFjdGFsaXMgQXV0aGVudGlj" "YXRpb24gUm9vdCBDQQ==", "VwoRl0LE48w=", Success!	**Verified?**	Verified
Root Stores Included In	Apple; Google; Microsoft; Mozilla	**Verified?**	Verified
Mozilla Applied Constraints	None	**Verified?**	Verified

Digital Fingerprint Information

SHA-1 Fingerprint	F3:73:B3:87:06:5A:28:84:8A:F2:F3:4A:CE:19:2B:DD:C7:8E:9C:AC	**Verified?**	Verified
SHA-256 Fingerprint	55:92:60:84:EC:96:3A:64:B9:6E:2A:BE:01:CE:0B:A8:6A:64:FB:FE:BC:C7:AA:B5:AF:C1:55:B3:7F:D7:60:66	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	The Actalis Authentication Root CA currently has one subordinate CA that is internally-operated. This root signs internally-operated intermediate certificates that sign end-entity certificates. CPS section 1.3.1: 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 CAs.	**Verified?**	Verified
Externally Operated SubCAs	None. CPS section 1.3.1: Within the framework of the service described in this document, both CA roles (Root CA and Sub CA) are played by Actalis	**Verified?**	Verified
Cross Signing	None.	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	CPS Section 1.3.1.2: There currently exists only one Sub CA, run by Actalis	**Verified?**	Verified

	The feasibility and opportunity of activating additional Sub CAs, run by other organizations, will be evaluated later on, taking into account the requirements and constraints imposed by the applicable laws, business practices, and security policies (including those enforced by browser vendors). CPS Section 1.3.2: The Registration Authority (RA) is a person, structure or organization that is responsible for: ... For certificates of class EV (Extended Validation), the RA activities are performed by Actalis only. For certificates of class OV (Organization Validated), RA activities can be performed by the Customer as an “Enterprise RA”, if the conditions are met, limited to Internet domains controlled by the Customer.

Verification Policies and Practices

Policy Documentation	Documents are provided in Italian and English.	**Verified?**	Verified
CA Document Repository	http://www.actalis.it/area-download.aspx	**Verified?**	Verified
CP Doc Language	Italian		
CP	http://www.actalis.it/area-download.aspx	**Verified?**	Verified
CP Doc Language	Italian		
CPS	https://www.actalis.it/documenti-en/cps-for-ssl-server-and-code-signing.aspx	**Verified?**	Verified
Other Relevant Documents	NEED: CP/CPS for email certs	**Verified?**	Need Response From CA
Auditor Name	IMQ	**Verified?**	Verified
Auditor Website	http://www.img.it/	**Verified?**	Verified
Auditor Qualifications	NEED: URLs to prove ETSI accreditation status for IMQ	**Verified?**	Need Response From CA
Standard Audit	http://www.actalis.it/documenti-en/actalisca_audit_statement.pdf	**Verified?**	Verified
Standard Audit Type	ETSI TS 102 042	**Verified?**	Verified
Standard Audit Statement Date	9/23/2014	**Verified?**	Verified
BR Audit	http://www.actalis.it/documenti-en/actalisca_audit_statement.pdf	**Verified?**	Verified
BR Audit Type	ETSI TS 102 042	**Verified?**	Verified
BR Audit Statement Date	9/23/2014	**Verified?**	Verified
EV Audit	http://www.actalis.it/documenti-en/actalisca_audit_statement.pdf	**Verified?**	Verified
EV Audit Type	ETSI TS 102 042	**Verified?**	Verified
EV Audit Statement Date	9/23/2014	**Verified?**	Verified
BR Commitment to Comply	CPS section 1.1	**Verified?**	Verified

SSL Verification Procedures	CPS section 3.3.1: For SSL Server certificates, the CA verifies that all FQDNs and IP address to be included in the certificate are under the control of the Applicant organization, or his parent organization. These checks are carried out by dif-ferent methods, depending on the case and the certificate class: - by means of WHOIS queries (+ reverse DNS lookups for IP addresses) to reliable DNS information sources. - by querying the relevant DNS Registrars or governmental domain registration agencies, as appropriate; - by communicating with the domain administrator via e-mail, using an e-mail address obtainned by pre-pending a “admin”, “administrator”, “webmaster”, “hostmaster”, or “postmaster” to the domain name (this latter is obtained by pruning zero or more components from the requested FQDN). Should one or more of those FQDNs and/or IP addresses be managed by an entity other than the Applicant or their parent organization, the Applicant is required to provide evidence to the CA that they have been formally delegated by the domains’ owner to manage those domains and/or IP addresses.	**Verified?**	Verified
EV SSL Verification Procedures	CPS section 3.3.2 For EV-class certificates	**Verified?**	Verified
Organization Verification Procedures	CPS section 3.2.2 and 3.2.3 describe authentication of organization and individual identity.	**Verified?**	Verified
Email Address Verification Procedures	NEED: the sections of the CP/CPS documents that describe the procedures for verifying that the email address to be included in the certificate is owned/controlled by the certificate subscriber, as per item #4 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA
Code Signing Subscriber Verification Pro	CPS section 1.3.3: Certificate Owners or Subscribers are organizations or agencies requesting an SSL Server certificate or Code Signing certificate and holding the corresponding private key. In particular, with reference to §7.2 of [EVCG], Actalis issues certificates to following types of organizations: - Private Organization - Government Entity In this CPS, the term “Owner” refers to the entity named “Subject” or “Subscriber” in [BR] and [EVCG]. In all cases the certificate Owner shall be an organization, not a natural person. CPS section 1.4: Actalis issues EV and OV Code Signing certs. Authentication of organization and individual identity is described in sections 3.2.2 and 3.2.3 of the CPS. CPS section 3.1.1: The commonName (OID 2.5.4.3) component of the Subject field: … – for a Code Signing certificate, may contain any string chosen by requestor, provided that it is not misleading about the certificate owner’s identity or about the certificate purpose	**Verified?**	Verified
Multi-Factor Authentication	CPS Section 4.2: The procedure for certificate issuance enforces a “dual control” requirement, in that it always requires two different operators to be completed: - RA operator (RAO) - CA operator (CAO) … For performing the operations listed above, the RAO logs on to Actalis’ CA system by means of a strong (i.e. two-factor) authentication.	**Verified?**	Verified
Network Security	CPS section 6	**Verified?**	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	http://www.actalis.it/area-download.aspx	**Verified?**	Verified