Bugzilla ID: 957548
Bugzilla Summary: Enable EV for Actalis Authentication Root CA

CAs wishing to have their certificates included in Mozilla products must

1) Comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/)
2) Supply all of the information listed in http://wiki.mozilla.org/CA:Information_checklist.
    a. Review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices
    b. Review the Potentially Problematic Practices at https://wiki.mozilla.org/CA:Problematic_Practices

General information about the CA's associated organization

CA Company Name	Actalis S.p.A.
Website URL	http://www.actalis.it
Organizational type	Public corporation
Primark Market / Customer Base	Actalis is a public CA offering PKI services to 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). Actalis designs, develops, delivers and manages services and solutions for on-line security, digital signatures and document certification; develops and offers PKI-enabling components, supplies complete digital signature and strong authentication kits (including hardware and software), delivers ICT security consultancy and training
Inclusion in other major browsers	Yes. IE.
CA Primary Point of Contact (POC)	CA Email Alias: cps-admin@actalis.it POC direct email: adriano.santoni@actalis.it CA Phone Number: +39-02-68825.1 Title/Department: Certification Manager / Certification Authority

Technical information about each root certificate

Certificate Name	Actalis Authentication Root CA

Certificate Issuer Field	CN = Actalis Authentication Root CA
	O = Actalis S.p.A./03358520967
	L = Milan
	C = IT

Certificate Summary	This request is to enable EV treatment for the "Actalis Authentication Root CA" root certificate that was included in NSS via bug #520557. This root signs internally-operated subordinate CAs which sign end-entity certificates.
Root Cert URL	https://bugzilla.mozilla.org/attachment.cgi?id=563066
SHA1 Fingerprint	F3:73:B3:87:06:5A:28:84:8A:F2:F3:4A:CE:19:2B:DD:C7:8E:9C:AC
Valid From	2011-09-22
Valid To	2030-09-22
Certificate Version	3
Cert Signature Algorithm	SHA-256
Signing key parameters	4096

Test Website URL	https://ssltest-a.actalis.it:8443
CRL URL	http://portal.actalis.it/Repository/AUTH-ROOT/getLastCRL http://crl03.actalis.it/Repository/AUTH-G2/getLastCRL
OCSP URL	http://portal.actalis.it/VA/AUTH-ROOT http://ocsp03.actalis.it/VA/AUTH-G2 Our OCSP responses have an expiration time of 1 day, and our OSCP database is updated at least 15 mins.
Requested Trust Bits	Websites (SSL/TLS) Code Signing
SSL Validation Type	OV and EV
EV Policy OID(s)	1.3.159.1.17.1 EV Tested: https://bugzilla.mozilla.org/attachment.cgi?id=8357056
Non-sequential serial numbers in cert	All of our certificates contain 32 bits of random data in the serial number, as made clear in chapter 7 of our CPS (see details of each certificate profile).

CA Hierarchy information for each root certificate

CA Hierarchy	CPS Section 1.3.1: The Root CA is used for issuing Sub CA certificates only and is kept off-line when not in use, whereas end-users certificates are issued by Sub CAs. Within the framework of the service described in this document, both CA roles (Root CA and Sub CA) are played by Actalis S.p.A.
Externally Operated SubCAs	None
Cross-Signing	None
Technical Constraints on Third-party Issuers	CPS Section 1.3.1.2: There currently exists only one Sub CA, run by Actalis S.p.A. (see section 1.3.1). 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: · collection and validation of certification requests and certificate management requests; · registration of the applicant and organization to which the same belongs; · authorization of issuance, by the CA, of the certificate requested; 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	Actalis Policy Documents: http://portal.actalis.it/Info/cmsContent?cmsRef=actalis/Info/Manuali CPS for SSL and Code Signing Certs (English): http://portal.actalis.it/cms/translations/en/actalis/Info/Solutions/Documents/CPS_SSLServer_CodeSigning_v2.2.5_EN.pdf CPS for SSL and Code Signing Certs (Italian): http://portal.actalis.it/cms/actalis/Info/Solutions/Documents/CPS_SSLServer_CodeSigning_v2.2.5_IT.pdf

Audits	Audit Type: ETSI TS 102 042 V2.2.1 with reference to EV Guidelines v1.3 Auditor: IMQ, http://www.imq.it/ Audit Statement: http://portal.actalis.it/cms/translations/en/actalis/Info/Solutions/Documents/ActalisCA_Audit_Statement.pdf (2013.10.18) Received from auditor Oct 28, 2013: "I confirm that IMQ issued the audit statement attached to the URL in your email."
Baseline Requirements (SSL)	In the audit statement: "During the Certification Authority audit it was also verified that the above-mentioned certification services meet the requirements of the following specification: "Baseline Requirements for then Issuance and Management of Publicly-Trusted Certificates", v.1.1…" CPS section 1.1: Within the Certification Authority services herein described, Actalis conforms to version 1.1 of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document. Furthermore, with regard to certificate types denoted by "EV" (see section 1.2), Actalis conforms to version 1.3 of the CA/Browser Forum Guidelines for Issuance and Management of Extended Validation Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and those Guidelines, those Guidelines take precedence over this document.
Organization Verification Procedures	CPS section 3.2.2 – Authentication of organization identity CPS section 3.2.3 – Authentication of individual identity
Non-EV SSL Verification Procedures	CPS section 3.3.1: For SSL Server certificates, the CA verifies that all Internet domains and IP address to be included in the certificate are under the direct control of the applicant organization. These checks are carried out through WHOIS queries and/or reverse DNS lookups, or by querying the relevant governmental do-main registration agencies, as appropriate. Should one or more of those domains and/or IP addresses be managed by an entity other than the applicant, this latter is required to provide evidence to the CA that they have been formally delegated by the legitimate owner to manage those domains and/or IP addresses.
EV Verification Procedures	CPS section 3.3.2 For EV-class certificates For private organizations, the CA also collects and evaluates the following information: · address of registered office · starting date of organization's activity · business purpose (objects) · board members · proprietor(s) or shareholders · transfers of property or shares · powers and representatives · protests, insolvency or other negative facts For government entities, the CA also collects and evaluates the following information: · address of main office · names and roles of top managers In both cases, the CA verifies that the certificate application was authorized by a manager of the applicant with adequate powers of attorney.

	The CA also verifies that all the address components (country, stateOrProvince, locality, streetAddress) to be included in the certificate match the address where the registered office of the applicant organization is actually located. All the above checks are carried out by querying the relevant chamber of commerce database (for private organizations) or the appropriate governmental database (for governmental entities).
Email Address Verification Procedures	Not applicable. Not requesting the email trust bit.
Code Signing Subscriber Verification Procedures	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
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.
Network Security	CPS section 6

Response to Mozilla's CA Recommended Practices (https://wiki.mozilla.org/CA:Recommended_Practices)

Publicly Available CP and CPS	See above.
CA Hierarchy	See above.
Audit Criteria	See above.
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
Verifying Domain Name Ownership	See above.
Verifying Email Address Control	N/A

Verifying Identity of Code Signing Certificate Subscriber	See above.
DNS names go in SAN	We meet this requirement; this is 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
OCSP	tested

Response to Mozilla's list of Potentially Problematic Practices (https://wiki.mozilla.org/CA:Problematic_Practices)

Long-lived DV certificates	SSL certs are OV or EV CPS Section 7.1.4: 1, 2, or 3 years depending on request
Wildcard DV SSL certificates	SSL certs are OV CPS section 4.1: It is also possible to apply for a “wildcard” SSL Server certificate (i.e., valid for all web sites belonging to a specific domain) or a multi-SAN SSL Server certificate (wherein two or more SAN values are present specifying several hostnames and/or domain names for which the same certificate will be used). In such cases, the same I&A procedures apply: the CA always checks that the requestor actually owns or controls the domains and/or IP addresses to be included in the certificate and that the requestor is an existing organization based on latest chamber of commerce records or other applicable reliable source of information.
Email Address Prefixes for DV Certs	SSL certs are OV.
Delegation of Domain / Email validation to third parties	CPS Section 1.3.2: The Registration Authority (RA) is a person, structure or organization that is responsible for: · collection and validation of certification requests and certificate management requests; · registration of the applicant and organization to which the same belongs; · authorization of issuance, by the CA, of the certificate requested; 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.
Issuing end entity certificates directly from roots	CPS section 1.3.1: The Root CA is used for issuing Sub CA certificates only and is kept off-line when not in use, whereas end-entity certificates are issued by Sub CAs.
Allowing external entities to operate subordinate CAs	CPS section 1.3.1.2: There currently exists only one Sub CA, run by Actalis S.p.A. (see section 1.3.1). 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).
Distributing generated private keys in PKCS#12 files	CPS section 3.2.1: the applicant must send its own public key to the CA in the form of a CSR in PKCS#10 format [RFC2314]
Certificates referencing hostnames or private IP addresses	See above.
Issuing SSL Certificates for Internal Domains	See above.

OCSP Responses signed by a certificate under a different root	N/A
CRL with critical CIDP Extension	N/A
Generic names for CAs	Root name is not generic
Lack of Communication With End Users	Certificate problem reporting procedures are now documented in §4.13 of our CPS
Backdating the notBefore date	We do not backdate our certificates. Our CA automatically sets the notBefore date/time very close – almost identical – to the date/time when the certificate was issued.