**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>.
   1. Review the Recommended Practices at <https://wiki.mozilla.org/CA:Recommended_Practices>
   2. 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](mailto:cps-admin@actalis.it)  POC direct email: [adriano.santoni@actalis.it](mailto: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>  Maximum expiration time of OCSP responses  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 and entropy in cert | http://www.mozilla.org/projects/security/certs/policy/MaintenancePolicy.html  “9. We expect CAs to maintain current best practices to prevent algorithm attacks against certificates. As such, the following steps will be taken: …  - all new end-entity certificates must contain at least 20 bits of unpredictable random data (preferably in the serial number).”  The purpose of adding entropy is to help defeat a prefix-chosen collision for non collision resistant hash functions. Using SHA256 without entropy isn't a problem in a near future. However, the Mozilla Policy doesn't say that; the entropy is mandatory for all new certificates, the used hash function isn't taken into consideration.  This isn't a blocker for an inclusion request if SHA1 is forbidden in the CA hierarchy. However, the CP/CPS must clearly state that SHA1 isn’t an acceptable hash algorithm for certificates in this hierarchy.  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 | No external third-party issuers.  CPS Section 1.3.2: The RA activities are performed by Actalis. |

**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_v2.2.3_EN.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) | 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: In the case of SSL Server certificates, the CA shall also verify that IP addresses and domains to be included in the certificate are controlled by the requesting organization. In the event that any of such domains or IP address turn are managed by a different entity, the applicant must provide to the CA an evidence that such entity was formally delegated to manage those domains and/or IP addresses on behalf of their owner.  The previous English translation of the CPS said: “CPS Section 3.3: In the case of SSL Server certificates, the CA shall also lookup the WHOIS record to verify that the owner organisation of the domain is the same as the applicant. In the case when the details do not match the application shall be rejected. Nonetheless, it is possible that the owner organisation has delegated the management of its domain to the party applying for the certificate. In this case, the application shall be accepted if a proof of such delegation is provided to the CA (i.e. copy of registration application for the domain sent to the manager by the owner organisation of the domain).”  Why was information removed about how domain ownership is verified?  At the time when you checked, there was an unwanted mismatch between the Italian and English version of our CPS; however, both were being updated. We have just published version 2.2.5 of our CPS, where this fundamental check is clearly described in §3.1.1 in both versions (Italian and English) of the document.  English version:  <http://portal.actalis.it/cms/translations/en/actalis/Info/Solutions/Documents/CPS_SSLServer_CodeSigning_v2.2.5_EN.pdf>  Italian version:  <http://portal.actalis.it/cms/actalis/Info/Solutions/Documents/CPS_SSLServer_CodeSigning_v2.2.5_IT.pdf> |
| EV  SSL Verification Procedures | See chapter 3 of our CPS (see URL above) that we have restructured and clarified. Look for “EV” in the text.  Let me know if you think that something is missing or not sufficiently clear. |
| Email Address Verification Procedures | Not applicable. Not requesting the email trust bit. |
| Code Signing Subscriber Verification Procedures | CPS section 3.2.2 and 3.2.3.  CPS Section 3.3: In the case of Code Signing certificates, the certificate cannot be requested by organizations other than the one to which the certificate is to be attributed: customer and subscriber must coincide. |
| 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](https://wiki.mozilla.org/CA:Recommended_Practices#Publicly_Available_CP_and_CPS) | See above. |
| [CA Hierarchy](https://wiki.mozilla.org/CA:Recommended_Practices#CA_Hierarchy) | See above. |
| [Audit Criteria](https://wiki.mozilla.org/CA:Recommended_Practices#Audit_Criteria) | See above. |
| [Document Handling of IDNs in CP/CPS](https://wiki.mozilla.org/CA:Recommended_Practices#Document_Handling_of_IDNs_in_CP.2FCPS) | We do not support IDNs at this time: this is documented in §3.3.1.1 of our CPS (see URL above). |
| [Revocation of Compromised Certificates](https://wiki.mozilla.org/CA:Recommended_Practices#Revocation_of_Compromised_Certificates) | CPS section 4.9.4 |
| [Verifying Domain Name Ownership](https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Domain_Name_Ownership) | See above. |
| [Verifying Email Address Control](https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Email_Address_Control) | N/A |
| [Verifying Identity of Code Signing Certificate Subscriber](https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Identity_of_Code_Signing_Certificate_Subscriber) | See above. |
| [DNS names go in SAN](https://wiki.mozilla.org/CA:Recommended_Practices#DNS_names_go_in_SAN) | We meet this requirement; this is made clear in §3.1.1 and in chapter 7 of our CPS (see URL above). |
| [Domain owned by a Natural Person](https://wiki.mozilla.org/CA:Recommended_Practices#Domain_owned_by_a_Natural_Person) | We do not issue certs to natural persons; this is documented in §1.3.3 of our CPS (see URL above). |
| [OCSP](https://wiki.mozilla.org/CA:Recommended_Practices#OCSP) | tested |

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

|  |  |
| --- | --- |
| [Long-lived DV certificates](https://wiki.mozilla.org/CA:Problematic_Practices#Long-lived_DV_certificates) | SSL certs are OV  CPS Section 7.1.3: 1, 2, or 3 years depending on request |
| [Wildcard DV SSL certificates](https://wiki.mozilla.org/CA:Problematic_Practices#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](https://wiki.mozilla.org/CA:Problematic_Practices#Email_Address_Prefixes_for_DV_Certs) | SSL certs are OV. |
| [Delegation of Domain / Email validation to third parties](https://wiki.mozilla.org/CA:Problematic_Practices#Delegation_of_Domain_.2F_Email_validation_to_third_parties) | CPS Section 1.3.2: The RA activities are performed by Actalis.  We have introduced the possibility of delegating RA activities for OV-class certificates only, and only to “Enterprise RAs” – i.e., customers requesting certificates for their own domains (pre-verified). |
| [Issuing end entity certificates directly from roots](https://wiki.mozilla.org/CA:Problematic_Practices#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](https://wiki.mozilla.org/CA:Problematic_Practices#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](https://wiki.mozilla.org/CA:Problematic_Practices#Distributing_generated_private_keys_in_PKCS.2312_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](https://wiki.mozilla.org/CA:Problematic_Practices#Certificates_referencing_hostnames_or_private_IP_addresses) | See above. |
| [Issuing SSL Certificates for Internal Domains](https://wiki.mozilla.org/CA:Problematic_Practices#Issuing_SSL_Certificates_for_Internal_Domains) | See above. |
| [OCSP Responses signed by a certificate under a different root](https://wiki.mozilla.org/CA:Problematic_Practices#OCSP_Responses_signed_by_a_certificate_under_a_different_root) | N/A |
| [CRL with critical CIDP Extension](https://wiki.mozilla.org/CA:Problematic_Practices#CRL_with_critical_CIDP_Extension) | N/A |
| [Generic names for CAs](https://wiki.mozilla.org/CA:Problematic_Practices#Generic_names_for_CAs) | Root name is not generoic |
| [Lack of Communication With End Users](https://wiki.mozilla.org/CA:Problematic_Practices#Lack_of_Communication_With_End_Users) | Certificate problem reporting procedures are now documented in §4.13 of our CPS (see URL above). |
| [Backdating the notBefore date](https://wiki.mozilla.org/CA:Problematic_Practices#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. |