Bugzilla ID: 520557
Bugzilla Summary: Add Actalis Authentication Root CA certificate

CAs wishing to have their certificates included in Mozilla products must comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/) and must supply the information necessary to determine whether or not the policy's requirements have been satisfied, as per http://wiki.mozilla.org/CA:Information_checklist.

CA's are also encouraged to review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices.

General Information	Data
CA Name	Actalis S.p.A.
Website URL	http://www.actalis.it
Organizational type	Public corporation
Primary 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.
CA Contact Information	CA Email Alias: cps-admin@actalis.it CA Phone Number: +39-02-68825.1 Title/Department: Certification Manager / Certification Authority

For Each Root CA whose certificate is to be included in Mozilla (or whose metadata is to be modified)

Info Needed	Data
Certificate Name	Actalis Authentication Root CA
Issuer	CN = Actalis Authentication Root CA O = Actalis S.p.A./03358520967 L = Milan C = IT
Cert summary / comments	This root signs internally-operated subordinate CAs which sign end-entity certificates.
The root CA certificate URL	https://bugzilla.mozilla.org/attachment.cgi?id=563066
SHA-1 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
Cert Version	3
Certificate Signature Algorithm	SHA256
Signing key parameters	4096 bit
Test Website	https://portal-pte.actalis.it/
CRL URL	http://portal.actalis.it/Repository/AUTH-ROOT/getLastCRL http://portal.actalis.it/Repository/AUTH-G2/getLastCRL (NextUpdate: 24 hours) SSL CPS section 4.10.1: The CRL is re-generated and re-published at least every 24 hours
OCSP Responder URL	http://portal.actalis.it/VA/AUTH-G2

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.
SubCAs Operated by 3rd parties	None
Cross-Signing	None
Requested Trust Bits	Websites (SSL/TLS) Code Signing
SSL Validation Type	OV
EV policy OID(s)	Not EV
CP/CPS	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/actalis/Info/Manuali/CPS_certificati_SSL_server_e_Code_Signing_v2.1.0_EN.pdf CPS for SSL and Code Signing Certs (Italian): http://portal.actalis.it/cms/actalis/Info/Manuali/CPS_certificati_SSL_server_e_Code_Signing_v2.1.0_IT
AUDIT	Audit Type: ETSI TS 101 456 Auditor: DigitPA Auditor website: http://www.digitpa.gov.it/ (Stefano Arbia, arbia@cnipa.it) Audit statement: https://bugzilla.mozilla.org/attachment.cgi?id=598788 (2012.02.13) Actalis is an accredited national certification service provider: http://www.digitpa.gov.it/firme-elettroniche/qcsp-english https://applicazioni.cnipa.gov.it/TSL/IT_TSL_HR.pdf The auditor, DigitPA, is our national supervising body according to EU directive. See here: http://ec.europa.eu/information_society/policy/esignature/eu_legislation/notification/italy/index_en.htm Audit Criteria: http://www.digitpa.gov.it/firma-digitale/certificatori-accreditati (see PDF document "Linee guida per la vigilanza sui certificatori qualificati") http://www.digitpa.gov.it/sites/default/files/linee%20guida%20per%20la%20vigilanza%20sui%20certificatori%20qualificati%20v1.2.pdf Section 1.3: These Guidelines are structured in accordance with the schedule of the technical specifications ETSI TS 101 456 and ETSI Technical Report TR 102 437. CPS Section 8.1: The external audits performed DigitPA are carried out every 18 months as provided by Circolare CNI-PA n.52 of 2007. Actalis, however, commits to do what is necessary so that a conformity audit be done at least every 12 months, if necessary by engaging an external independent auditor so to enforce the annual periodicity.
Organization Identity Verification	CPS Section 3.2.2: Authentication of the identity of the applicant organisation includes in any case a lookup in the relevant CCIAA (Chamber of Commerce, Industry, Crafts and Agriculture) database. The name of the organisation declared by the client must correspond with the company name as registered in the chamber of commerce. In case of mismatch, the certificate application shall be rejected. CPS Section 3.2.3: The individual identities indicated in the certificate application are verified over the phone, by contacting the person declared as “requestor” in the certificate application form. CA reserves the right to perform further verifications in order to validate individual identities.

Domain Name Ownership / Control	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).
Email Address Ownership / Control	Not applicable. Note requesting email trust bit at this time.
Identity of Code Signing Subscriber	See CPS Sections 3.2.2 and 3.2.3. CPS Section 3.3: In the case of Code Signing certificates, it is not allowed that the certificate be requested by an organisation different than the one to which the certificate is to be attributed: client and subscriber must coincide.
Multi-factor Authentication	CPS Section 6.11: Multi-factor authentication is required for all CMS and WebRA/WebCA accounts capable of directly causing certificate issuance. … For performing most of the operations listed above the RA operator uses a specific type of account on the Certificate Management System. Such type of account requires strong two-factor authentication for logon. All security-relevant operations – e.g. authorization of certificate issuance – require the RA operator's digital signature (smartcard-based) and are traced to the audit log.
Network Security	Comment #56 -- Confirmed completion of the actions listed in #7 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices
Potentially Problematic Practices	http://wiki.mozilla.org/CA:Problematic_Practices • Long-lived DV certificates o SSL certs are OV o CPS Section 7.1.3: 1, 2, or 3 years depending on request • Wildcard DV SSL certificates o SSL certs are OV o CPS section 4.1: It is also possible to request 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 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. • Delegation of Domain / Email validation to third parties o CPS Section 1.3.2: The RA activities are normally performed by Actalis, but in certain circumstances these can be delegated to other parties based on a specific "delegation agreement". In such a case, suitable technical controls restrict the external RA to authorize certificates only for a specific set of domain names that the external RA has registered or has been authorized to act for. o CPS Secton 4.2: the RA shall perform the following: ▪ insert the applicant data in the registration database; ▪ verify that the identification data contained in the CSR are coherent with that supplied in the application form; ▪ verify the identity of the applicant and possession of the private key corresponding to the CSR, as described in section 3.2; ▪ perform the additional verifications described in section 3.3. ▪ … For performing most of the operations listed above the RA operator uses a specific type of account on the Certificate Management System. Such type of account requires strong

	two-factor authentication for logon. All security-relevant operations – e.g. authorization of certificate issuance – require the RA operator's digital signature (smartcard-based) and are traced to the audit log. o CPS Section 8.4: Audits on external RAs aim at verifying the respect, by each audited RA, of the delegation agreement • Issuing end entity certificates directly from roots o This new root only signs internally-operated intermediate certificates. • Allowing external entities to operate unconstrained subordinate CAs o There are no sub-CAs operated by external entities. • Distributing generated private keys in PKCS#12 files o 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 o See above. • OCSP Responses signed by a certificate under a different root o N/A • CRL with critical CIDP Extension o CRL downloaded into Firefox browser without error. • Generic names for CAs o Root name is not generic