Bugzilla ID: 520557
Bugzilla Summary: Add Actalis Authentication CA G1 root 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	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 CA G1
Cert summary / comments	This CA directly issues end-entity certificates for SSL and Code Signing.
The root CA certificate URL	https://bugzilla.mozilla.org/attachment.cgi?id=405122
SHA-1 fingerprint	91:58:C5:EF:98:73:01:A8:90:3C:FD:AB:03:D7:2D:A1:D8:89:09:C9
Valid from	2009-06-23
Valid to	2022-06-24
Cert Version	3
Modulus length	2048
Test Website	https://portal-pte.actalis.it/
CRL URL	http://portal.actalis.it/Repository/AuthCA1/getCRL (Next Update: 30 hours) SSL CPS section 4.10.1: The CRL is regenerated and republished: at least every 6 hours, even in the absence of new suspensions or revocations; after each new suspension or revocation.

OCSP Responder URL	From Actalis: At this time, an OCSP responder address (although envisioned in the CPS) is not supposed to be included in our SSL Server certificates. Our OCSP service will be released next year, according to schedule.
CA Hierarchy	This CA directly issues end-entity certificates for SSL and Code Signing.
SubCAs Operated by 3rd parties	None
Cross-Signing	None
Requested Trust Bits	Websites (SSL/TLS) Code Signing
SSL Validation Type DV, OV, and/or EV	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_SSLServer_CodeSigning_v2.0.3_EN CPS for SSL and Code Signing Certs (Italian): http://portal.actalis.it/cms/actalis/Info/Manuali/CPS_SSLServer_CodeSigning_v2.0.3_IT
AUDIT	Audit Type: ETSI TS 101 456 Auditor: Centro Nazionale per L'Informatica nella Pubblica Amministrazione (CNIPA) Auditor website: http://www.cnipa.gov.it/site/it-IT/ (Stefano Arbia, arbia@cnipa.it) Audit statement (censored version): https://bugzilla.mozilla.org/attachment.cgi?id=414040 (2008.05.20) Actalis is listed as an accredited national certification service provider: http://ec.europa.eu/information_society/policy/esignature/eu_legislation/notification/italy/index_en.htm Actalis is listed as an Accredited Certifier on the CNIPA website: http://www.cnipa.gov.it/QCSP CPS Section 8.1 Frequency and reason for audit: The external audits performed CNIPA are carried out every 18 months. -- This root was created after the audit took place. Before inclusion we will need the updated audit that includes this root. However, we can proceed based on the current audit for now. Audit Criteria used by CNIPA http://www.cnipa.gov.it/site/_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.
Organization Identity Verification	CPS Section 3.2.2 Authentication of organisation identity 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 Authentication of individual identity 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 Further verifications by the CA 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. CPS Section 3.4 Information not verified by the CA The CA does not verify the electronic mail address indicated in the application form.
Identity of Code Signing Subscriber	CPS Section 3.3 Further verifications by the CA 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.

Potentially Problematic Practices	http://wiki.mozilla.org/CA:Problematic_Practices
	• Long-lived DV certificates
	  ○ SSL certs are OV
	  ○ CPS Section 7.1.2: 1 or 2 years depending on request
	• Wildcard DV SSL certificates
	  ○ SSL certs are OV
	  ○ 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-host" /"multi-domain" type (i.e., valid for various web sites, even on different domains). In these cases different procedures and specific fees are applied. For further in-formation please contact the Actalis commercial offices.
	  ○ From Actalis: Same as in the single-host case: the requestor must be the actual owner (or the formally delegated manager) of the involved domain(s)
	• Delegation of Domain / Email validation to third parties
	  ○ 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.
	  ○ 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. o CPS Section 8.4: Audits on external RAs aim at verifying the respect, by each audited RA, of the delegation agreement (see section 1.3.2). • Issuing end entity certificates directly from roots o **Yes, this root signs end-entity certs directly.** o From Actalis: Apart from the information already provided in the CPS, we have a detailed Security Plan in place that can only be disclosed (and has, in fact, been disclosed) to our national supervising authority (CNIPA). Let me know what additional information you would like to know. • 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 Comment #12: Actalis does not issue SSL certs with private IP addresses in them. • OCSP Responses signed by a certificate under a different root o OCSP is not supported as of today, but planned for the future. • CRL with critical CIDP Extension o CRL downloaded into Firefox browser without error. • Generic names for CAs o Root name is not generic