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 (English version)	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 • Email Alias • Phone Number • Title/Department	CA Email Alias: info@actalis.it Does the email alias info@actalis.it include the people in your company who should receive correspondence from Mozilla in regards to root certificates? An email alias is requested so that more than one person in your organization will receive notifications in case the primary contact is out of the office or leaves the organization. CA Phone Number: +39-02-68825 Title / Department: If Mozilla needed to call your main phone number, what Title/Department should the Mozilla representative ask for?

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 will be filled in by Kathleen based on the information below.
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 / key length	2048
Test Website	https://portal-pte.actalis.it/ The test website loads fine in my Firefox browser until I enforce OCSP. Then I get an error: Invalid OCSP signing certificate in OCSP response. (Error code: sec_error_ocsp_invalid_signing_cert) Please try it in your Firefox browser. Note: RFC 2560, sections 2.2, 2.6, 3.2 and 4.2.2.2 define the requirements for the OCSP response signer's certificate and certificate chain. NSS enforces these requirements exactly.
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 any suspensions or revocations; after each new suspension or revocation.
OCSP Responder URL	http://ocsp.actalis.it SSL CPS section 4.10.2: Access to the CRL and OCSP possible service is available on a continuous (24 x 7), except if stopped for scheduled maintenance and in case of breakdowns. See also paragraph 9.16.
List or description of subordinate CAs operated by the CA organization associated with the root CA	Please provide a description of the CA-hierarchy for this root. What certificates are issued directly from this root? Are there any internally operated subordinate CAs for these roots?
For subordinate CAs operated by third parties, if any: General description of the types of third-party subordinates that exist, and what the general legal/technical arrangements are by which those subordinates are authorized, controlled, and audited.	Does this root have any subordinate CAs that are operated by external third parties? For the subordinate CAs that are operated by third parties, please provide a general description and explain how the CP/CPS and audits ensure the third parties are in compliance. Also, see https://wiki.mozilla.org/CA:SubordinateCA_checklist
List any other root CAs that have issued cross-signing certificates for this root CA	Has this root been involved in cross-signing with another root?
Requested Trust Bits	Websites (SSL/TLS) -- EKU=1.3.6.1.5.5.7.3.1, EKU=1.3.6.1.5.5.7.3.2 Email (S/MIME) -- EKU=1.3.6.1.5.5.7.3.4 Code Signing -- EKU=1.3.6.1.5.5.7.3.3
SSL Validation Type	OV

DV, OV, and/or EV	
EV policy OID(s)	Not EV
CP/CPS	Certification Practice Statement for SSL and Code Signing Certs (Italian): https://portal.actalis.it/cms/actalis/Info/Manuali/CPS_SSLServer_CodeSigning_v2 Please also provide the CPS for the email (S/MIME) certs.
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/ Audit statement: We will need an official statement from the auditor which includes when the last audit was performed, that it covered this root, and that the audit used the ETSI TS 101 456 criteria. I cannot read Italian… Is there a way on the CNIPA website to find the statement of accreditation for Actalis? Or can you provide a direct link if the CNIPA provide an online certificate or statement of Actalis having been audited/accredited? When audit statements are provided by the company requesting CA inclusion rather than having an audit report posted on the website such as cert.webtrust.org, the Mozilla process requires doing an independent verification of the authenticity of audit statements that have been provided.
Organization Identity Verification	Google Translations of the SSL CPS: (Please correct the following translation as necessary) 3 IDENTIFICATION AND AUTHENTICATION (I & A) 3.1 Regulation of naming The subject field of the certificate must contain easily understandable information to allow identification of the organization certificate holder. We do not allow pseudonyms or names of the actual-verse name (or other official title) of the Customer. The country component of the Subject field should contain the ISO 3166 two-letter code (eg "IT") that identifies the country where the group is established certificate holder. OrganizationName component of the Subject field must contain the official name (eg name to social) organization certificate holder. The name must be unique, ie must not lend itself to ambiguity. To resolve any ambiguity, the CA may require that the name is followed by the organization's tax code or other information useful for the purpose. In the case of SSL server certificate, the commonName component of the Subject field should contain the correct address of the web server (numeric or symbolic). A good example is "www.example.com". In the case of Code Signing certificate, the commonName component of the Subject field can count all-black one sentence, as proposed by the applicant, provided that this sentence is not likely to mislead the Relying Parties as to the identity of the owner and the purpose / functionality Software signed. An example is-strand is "ACME Code Signing".

If Client can not be used in certification applications names that infringe intellectual property rights of others. Actalis remains foreign to any dispute concerning the ownership of domain names, nor does it seek to resolve disputes regarding the ownership of names of domain, trade names, trademarks or service. Actalis reserves the right to reject an application for certification and to revoke a certificate in the face of such a dispute.

3.2 Initial Identity Validation

3.2.1 Proof of possession of private key

The proof of possession by the applicant, the private key corresponding to the certificate request is based on the cryptographic verification of CSR (Certificate Signing Request) sent to the CA. The applicant, in fact, must send your public key to the CA form of CSR in PKCS # 10 [RFC2314]. The CA verifies that the digital signature contained in the CSR is valid.

Sending the CSR to the CA is usually done via web (https://portal.actalis.it) or via email.

3.2.2 Authentication of the applicant organization

The verification of identity of the applicant organization includes in each case the consultation of the database of the CCIAA (Chamber of Commerce, Industry and Handicraft). The name of the organization declared by the client must match the name that results from an overview. In the case of mismatch, the certificate request is rejected.

3.2.3 Authentication of individual identity

Individual identities listed in the certificate request is verified by telephone, by contacting the person listed as "applicant" in the certificate request form.

CA reserves to make further checks in ways not predetermined.

3.3 Further tests conducted by the CA

In the case of certificates for SSL Server, the CA also consults the WHOIS records to verify that the organization owns the domain is the same as applying for the certificate. In the case of non-correspondence, the certificate request is rejected. However, it is possible that the holder of the domain organization he has entrusted the management to the person requesting the certificate. In this case, the request is accepted on condition that the CA provides the evidence of those expectations (ie copy of the request for registration of the domain addressed by the organization to the domain owner operator).

In the case of Code Signing certificates, it is admitted that the certificate is requested by an organization other than that which it must be awarded the certificate means a client and owner must coincide.

The CA reserves the right to conduct additional testing in ways not predetermined.

3.4 Information not verified by the CA

The CA does not verify the e-mail addresses indicated in the application form.

If requested inclusion in the SSL certificate server in a private IP address (ie not achievable from the public Internet), the CA does not verify the correctness of that address.

In general, the CA does not verify the accuracy of information received by the applicant which are not intended to be included in critical fields of the certificate (for safety) and are not necessary for the issuance and subsequent management (sleep, wake, revocation) of the certificate.

4. REQUIREMENTS OPERATIONAL MANAGEMENT CERTIFICATES

4.1 Certificate Request

The certificate request can be done in two ways:

- through the completion and submission of online application form (web form) available on the website https://portal.actalis.it;
- by filling in and sending to the CA (by fax, email, regular mail) to request special application form downloadable from the same website.

The certificate request includes at least the following information:

- identification of the applicant organization
- identifying information and contact details (email, phone) of the applicant
- identifying information and contact details (email, phone) of a "technical reference"
- web site address for inclusion in the certificate (for SSL Server Certificates)
- proposed value for the field commonName (for Code Signing Certificate)

The certificate request must be accompanied by the CSR (Certificate Signing Request). In the case of a request on paper, CSR can be sent to the CA thereafter for electronic mail address designated by the head of the recording.

CSR is normally generated by the applicant's own resources.

You can also request an SSL server type "wildcard" (ie valid for all websites on a specific domain certificates) or a 'multi-host "/" multi-domain "(ie valid for mol-ning, websites even on different domains). In such cases, the procedures in the different specific rates. For more information contact the business direction of Actalis.

4.2 Processing requests

Upon receipt of an application for certification, the RA performs the following activities:

- provides a census of the applicant in the registration database;
- verify that the identifying information contained in the CSR are consistent with those provided in the application form;
- verifying the identity of the applicant and his possession of the private key corresponding to the CSR, as described in section 3.2.

The record consists of the applicant in the storage, the CA database, the identification data and contact information (phone,

	email) of the applicant organization and the person requesting the certificate (usually a legal representative, eg. A manager with appropriate powers signature). 4.3 Issue of Certificate If the checks referred to in the previous section are exceeded, the CA generates the certificate, stores it in its database and publishes on its directory server (ldap://ldap.actalis.it). The CA then sends to the customer by e-mail: • certificate holder • certificate of issuing CA • accompanying documentation • the credentials (userid, password) to access the private area of the CA service portal (https://portal.actalis.it) for the suspension / reactivation or revocation of the certificate. At this point, if the certificate has already been paid, the CA issued the invoice and send it to the customer. 4.4 Acceptance of the certificate The certificate is accepted by the customer will undoubtedly spent 30 days from the date of delivery as indicated by the date of the email by which it is sent to the customer, without any communication to the contrary by the customer. The public use of the certificate (eg. Installation on a web site with public access, signature of executable code downloaded from websites with public access), even if temporary, in any case implies the acceptance of the certificate by the holder. If the certificate contains inaccurate information due to incorrect filling in the form of re-requested by the customer, it should in any case be paid.
Domain Name Ownership / Control	Google Translation of SSL CPS section 3.3, Further tests conducted by the CA: In the case of certificates for SSL Server, the CA also consults the WHOIS records to verify that the organization owns the domain is the same as applying for the certificate. In the case of non-correspondence, the certificate request is rejected. However, it is possible that the holder of the domain organization he has entrusted the management to the person requesting the certificate. In this case, the request is accepted on condition that the CA provides the evidence of those expectations (ie copy of the request for registration of the domain addressed by the organization to the domain owner operator).
Email Address Ownership / Control	section 7 of http://www.mozilla.org/projects/security/certs/policy/: We consider verification of certificate signing requests to be acceptable if it meets or exceeds the following requirements: • for a certificate to be used for digitally signing and/or encrypting email messages, the CA takes reasonable measures to verify that the entity submitting the request controls the email account associated with the email address referenced in the certificate *or* has been authorized by the email account holder to

	act on the account holder's behalf; Please provide translations into English of the sections of the CP/CPS documents that describe the procedures for verifying that the email account associated with the email address in the cert is owned/controlled by the subscriber. Please also list the corresponding document(s) and section or page numbers containing the original text.
Identity of Code Signing Subscriber	Google Translation of SSL CPS section 3.3, Further tests conducted by the CA: (Please correct translation if needed) In the case of Code Signing certificates, it is admitted that the certificate is requested by an organization other than that which it must be awarded the certificate means a client and owner must coincide.
Potentially Problematic Practices	Please review the list of Potentially Problematic Practices (http://wiki.mozilla.org/CA:Problematic_Practices). Identify the ones that are and are not applicable. . For the ones that are applicable, please provide further information and translations into English of the CP/CPS where relevant. • Long-lived DV certificates o SSL certs are OV o How long can SSL certs be valid for? • Wildcard DV SSL certificates o SSL certs are OV o SSL CPS section 4.1: You can also request an SSL server type "wildcard" (ie valid for all websites on a specific domain certificates) or a 'multi-host "/" multi-domain "(ie valid for mol-ning, websites even on different domains). In such cases, the procedures in the different specific rates. For more information contact the business direction of Actalis. o Please provide further info about verification or what's allowed. • Delegation of Domain / Email validation to third parties o ? • Issuing end entity certificates directly from roots o This appears to be the case. Need info on CA hierarchy. o If this is the case, need more info about how the root is kept secure since it cannot be offline. • Allowing external entities to operate unconstrained subordinate CAs o ? • Distributing generated private keys in PKCS#12 files o SSL CPS section 3.2.1: The applicant, in fact, must send your public key to the CA form of CSR in PKCS # 10 [RFC2314]. • Certificates referencing hostnames or private IP addresses o ? • OCSP Responses signed by a certificate under a different root o ?

	• CRL with critical CIDP Extension o CRL downloaded into Firefox browser without error. • Generic names for CAs o Root name is not generic