Bugzilla ID: 470756
Bugzilla Summary: add certsign's root ca cert

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.

General Information	**Data**
CA Name	certSIGN
Website URL	http://www.certsign.ro/certsign_en/
Organizational type	private corporation
Primary market / customer base	certSIGN is operated by SC CERTSIGN srl, a private corporation. certSIGN is a company member of UTI Group and an accredited supplier of certification services. certSIGN solutions are developed integrally in Romania.
CA Contact Information	CA Email Alias: office@certSIGN.ro CA Phone Number: 00 40 311 99 04

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

Info Needed	**Data**
Certificate Name	certSIGN ROOT CA
Cert summary / comments	This root issues internally-operated subordinate CAs for different classes of certificates based on use and verification requirements.
The root CA certificate URL	https://bugzilla.mozilla.org/attachment.cgi?id=359654
SHA-1 fingerprint.	fa:b7:ee:36:97:26:62:fb:2d:b0:2a:f6:bf:03:fd:e8:7c:4b:2f:9b
Valid from	7/4/2006
Valid to	7/4/2031
Cert Version	3
Modulus length	2048
Test Website	https://www.certsign.ro/certsign_en/
CRL • URL • update frequency for end-entity certificates	All CRLS: https://www.certsign.ro/certificate_digitale/lista_certificate_revocate_en.htm Root CRL: http://www.certsign.ro/certcrl/root.crl Class 2 CRL: http://crl.certsign.ro/class2.crl (NextUpdate: 48 hours) Qualified Class 3 CRL: http://www.certsign.ro/certcrl/qualified.crl (NextUpdate: 48 hours) Enterprise CA Class 3 CRL: http://www.certsign.ro/certcrl/enterprise.crl (NextUpdate: 48 hours) Class 4 CRL: http://crl.certsign.ro/class4.crl (NextUpdate: 48 hours) CPS section 4.10.5: The CRL's availability period is of 48 hours and it is updated daily.

OCSP (if applicable)	http://ocsp.certisgn.ro
List or description of subordinate CAs operated by the CA organization	Hierarchy shown in section 1.1 of CPS. There are four Certification Authorities, immediately subordinated to certSIGN ROOT CA: + certSIGN CA Class 2: Simple certificates used for authentication, signing, and encryption. + certSIGN Qualified CA Class 3: Qualified Certificates + certSIGN Enterprise CA Class 3: Certificates used for SSL, code signing, VPN gateways. + certSIGN Non-Repudiation CA Class 4: CA Servers Certificates used for Time Stamping and OCSP. Sub-CAs can be downloaded from: https://www.certsign.ro/certificate_digitale/lantul_de_incredere_en.htm certSIGN Demo CA Class 1 is a selfsigned authority which issue only demo certificates.
Sub-CAs operated by third parties	No sub-CAs are operated by third parties. From certSIGN: We have not and we will not issue CA certificates for third parties directly under the root. However, certSIGN Non-Repudiation CA Class 4 could issue certificates for CA servers that might be operated by a third party. CPS Section 1.1: "For the time being, certSIGN does not have a mutual agreement with another certificate issuing authority. If this situation will change the users will be informed by publishing the new version of the Certification Policy (CP) and of the Certification Practice Statement (CPS)."
cross-signing	None
Requested Trust Bits	Websites Email Code
For SSL: DV, OV, and/or EV	OV CPS Table 1.1: SSL certs are issued under the Enterprise CA Class 3 sub-CA. CPS Table 3.1.8: For Class 3 and Class 4 certs the subscriber has to appear in person at the RA or a public notary.
EV policy OID(s)	Not EV
CP/CPS	Certification Policy in English: http://www.certsign.ro/certsign_en/files/certSIGN_CP_EN_v1.0.pdf Certification Practice Statement in English: http://www.certsign.ro/certsign_en/files/certSIGN_CPS_EN.pdf CP and CPS are at the bottom of each page of this site: http://www.certsign.ro/certsign_en/
AUDIT	Audit Type: Webtrust CA Auditor: Ernst & Young Auditor website: www.ey.com Audit: https://bug470756.bugzilla.mozilla.org/attachment.cgi?id=361730 (2008-11-15) There are 3 audits performed on this root: 1) An audit performed once at every three years by an independent auditor and requested by the Romanian law for us to be able to issue qualified certificates

	2) an annual audit performed by BSI for conformity with ISO 27001 3) an annual audit performed by E&Y for WebTrust for CA conformity > From: Gabriel.Apostu@ro.ey.com <Gabriel.Apostu@ro.ey.com> > Subject: Re: Confirming the Authenticity of certSIGN Audit Report > To: kathleen95014@yahoo.com > Date: Friday, February 13, 2009, 1:22 AM > Dear Ms Wilson, > I confirm that E&Y has issued the report you have pointed out. We have > performed audit work as per Webtrust for CA criteria and issued our report. > Thank you, > Ernst & Young ® > Ernst & Young SRL > Gabriel Apostu | Partner | Business and Risk Advisory Services
Organization Identity Verification	CPS Section 3.1.7, Authentication of Legal Entity’s Identity The authentication of a legal entity’s identity is done either by personal attendance of the authorized representative of the legal entity to the Registration Authority, or, by personal attendance of the authorized representative of the Registration Authority at the legal entity’s headquarters (mentioned in the request). The authorized representatives of the institution regardless the certificate level they are requesting are bind to present upon the request of the Registration Authority the following documents: - Certified copy “in compliance with the original” of the registration certificate of the company; - Copy of utility invoice (phone, others) issued to the company; - Documents to attest the solicitor’s identity (identity card or passport) and the authorization attesting that he is representing the company; - Purchasing request; - Template statement of the domain’s titular (in case of WEB certificates when the certificate solicitor is not the owner of the domain he wants to secure). The procedure performed by RA of checking the legal entity’s identity and its authorized representative’s identity consists of (see as well Table 3.1.8): - Checking the documents rendered by the Subscriber, - Checking the request, that consists of: o Checking the compliance of the data mentioned in the request with those from the documents rendered, o (optional) checking the proof of private key possession (if the request supposes a key pair to create an electronic signature) and the fact that the Distinctive Name is the right one,

	- Checking the authorization and identity of the representative of the legal entity that submits the request (including applications for certification as Certification Authority) on behalf of this entity. - Checking for certificates to be used for SSL-enabled servers, that the domain referenced in the certificate is registered by the entity submitting the certificate request or by that that has authorized the usage of domain by the entity submitting the request. This is done be means of whois service provided by ROTLD at www.rotld.ro - Verification that the email account associated with the email address in the certificate is controlled by the subscriber. The certificate request cannot be made/validated in the RA software application if the subscriber does not validate his email account. *The Registration Authority is committed to check the correctness and the authenticity of all data rendered in a request (see Table 3.1.8, Chapter 3.1.9).*
Domain Name Ownership / Control	CPS section 3.1.7, Authentication of Legal Entity's Identity • The authorized representatives of the institution regardless the certificate level they are requesting are bind to present upon the request of the Registration Authority the following documents: o Template statement of the domain's titular (in case of WEB certificates when the certificate solicitor is not the owner of the domain he wants to secure)..." • The procedure performed by RA of checking the legal entity's identity and its authorized representative's identity consists of (see as well Table 3.1.8): o Checking for certificates to be used for SSL-enabled servers, that the domain referenced in the certificate is registered by the entity submitting the certificate request or by that that has authorized the usage of domain by the entity submitting the request. This is done be means of whois service provided by ROTLD at www.rotld.ro. o The Registration Authority is committed to check the correctness and the authenticity of all data rendered in a request (see Table 3.1.8, Chapter 3.1.9).
Email Address Ownership / Control	CPS section 3.1.7, Authentication of Legal Entity's Identity The procedure performed by RA of checking the legal entity's identity and its authorized representative's identity consists of (see as well Table 3.1.8): • Verification that the email account associated with the email address in the certificate is controlled by the subscriber. The certificate request cannot be made/validated in the RA software application if the subscriber does not validate his email account. • The Registration Authority is committed to check the correctness and the authenticity of all data rendered in a request (see Table 3.1.8, Chapter 3.1.9). CPS section 3.1.8, Authentication of Natural Entity's Identity The procedure for natural entities realized in front of the Registration Authority consist of: • Verification that the email account associated with the email address in the certificate is

	controlled by the subscriber. The certificate request cannot be made/validated in the RA software application if the subscriber does not validate his email account.
Identity of Code Signing Subscriber	Code signing certs are class 3, and identity is verified in person as per CPS Section 3.1.7 and 3.1.8
Potentially Problematic Practices	http://wiki.mozilla.org/CA:Problematic_Practices) • Long-lived DV certificates o SSL certs are OV o CPS Table 6.3.2.2: SSL certificates are issued only with certSIGN Enterprise Class 3 CA. That means that the maximum usage period for an SSL certificate is of 1 year. • Wildcard DV SSL certificates o Not found. • Delegation of Domain / Email validation to third parties o CPS Section 2.1.2 Registration Authority Obligations o CPS Section 2: Between CERTSIGN and local authorities there are concluded contracts when these parties play the role of a Certification Authority's agent that operates within CERTSIGN's domain. Based on such an agreement a Registration Authority may conclude contracts of certification service providing with Subscribers on behalf of CERTSIGN. In well-founded cases the Registration Authorities may conclude contracts on their own behalf with Subscribers for services provided by the Registration Authorities. certSIGN Certification Authority can register and issue a certificate to any external entity that plays the role of subordinate Certification Authority, provided that the registration and issuance of the certificate are based on an agreement concluded between the two parties. • Issuing end entity certificates directly from roots o Root issues sub-CAs only. • Allowing external entities to operate unconstrained subordinate CAs o All sub-CAs are currently internally operated. o From certSIGN: We have not and we will not issue CA certificates for third parties directly under the root. However, certSIGN Non-Repudiation CA Class 4 could issue certificates for CA servers that might be operated by a third party ▪ CPS Section 1.1: "For the time being, certSIGN does not have a mutual agreement with another certificate issuing authority. If this situation will change the users will be informed by publishing the new version of the Certification Policy (CP) and of the Certification Practice Statement

	(CPS)." • Distributing generated private keys in PKCS#12 files o The only certificates that are not issued on tokens/smartcards and are intended to be used by persons (apart from those for web servers, VPN servers, CA, TSA or OCSP servers) are some of Class 2, but they are only generated by the subscriber. See CPS Table 1.1. • Certificates referencing hostnames or private IP addresses o All certificates are issued only after the subscribers sign the Terms and conditions of services use. In this way is their responsibility to use the certificate issued to them only for the scope intended. • OCSP Responses signed by a certificate under a different root o OCSP response is signed by a cert under this root. o Test website loads into Firefox browser without error with OCSP enforced. • CRL with critical CIDP Extension o CRLs download into Firefox without error. • Generic names for CAs o Root name is not generic.