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 (English version)	http://www.certsign.ro/certsign_en/
Organizational type. (E.g., whether the CA is operated by a private or public corporation, government agency, academic institution or consortium, NGO, etc.)	The CA is operated by a private corporation: SC CERTSIGN srl Romania
Primary market / customer base. (Which types of customers does the CA serve? Are there particular vertical market segments in which it operates? Does it focus its activities on a particular country or other geographic region?)	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.

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

Info Needed	Data	Status / Notes
Certificate Name	certSIGN ROOT CA	COMPLETE
Cert summary / comments	This root issues internally-operated subordinate CAs for different classes of certificates based on use and verification requirements.	COMPLETE
The root CA certificate URL Download into FireFox and verify	https://bugzilla.mozilla.org/attachment.cgi?id=359654 https://www.certsign.ro/certcrl/root.crt	COMPLETE
SHA-1 fingerprint.	fa:b7:ee:36:97:26:62:fb:2d:b0:2a:f6:bf:03:fd:e8:7c:4b:2f:9b	COMPLETE
Valid from	7/4/2006	COMPLETE
Valid to	7/4/2031	COMPLETE
Cert Version	3	COMPLETE
Modulus length	2048	COMPLETE
CRL	All CRLS:	I get the error ffffe009 when I try to load

• URL • update frequency for end-entity certificates	https://www.certsign.ro/certificate_digitale/lista_certificate_revocate_en.htm Root CRL: http://www.certsign.ro/certcrl/root.crl For Subordinated Authorities certificates (Classes 2-4) Class 2 CRL: http://crl.certsign.ro/class2.crl Qualified Class 3 CRL: http://www.certsign.ro/certcrl/qualified.crl Enterprise CA Class 3 CRL: http://www.certsign.ro/certcrl/enterprise.crl Class 4 CRL: http://crl.certsign.ro/class4.crl CPS section 4.10.4, Certificate Revocation Maximum Period: "within 24 hourse"	the CRLs into Firefox. Please see http://www.mozilla.org/projects/security/pki/nss/ref/ssl/sslerr.html If my calculation is correct, this error corresponds to error code -8183 which would be "Security library: improperly formatted DER-encoded message."
OCSP (if applicable) • OCSP Responder URL • Max time until OCSP responders updated to reflect end-entity revocation	http://ocsp.certisgn.ro	In Firefox when I set the validation option to treat the certificate as invalid if OCSP fails, I can successfully go to https://www.certsign.ro/certificate_digitale/lantul_de_incredere_en.htm However, I get the following error when trying to access other www.certsign.ro https sites like https://www.certsign.ro/certsign_en/ The OCSP server experienced an internal error. (Error code: sec_error_ocsp_server_error)
List or description of subordinate CAs operated by the CA organization associated with the root CA. (For	Hierarchy shown in section 1.1 of CPS. Root and sub-CAs can be downloaded from:	COMPLETE

example, this might include subordinate CAs created to issue different classes or types of end entity certificates: Class 1 vs. class 2 certificates, qualified vs. non-qualified certificates, EV certificates vs. non-EV certificates, SSL certificates vs. email certificates, and so on.) For internally-operated subordinate CAs the key is to confirm that their operation is addressed by the relevant CPS, and that any audit covers them as well as the root.	https://www.certsign.ro/certificate_digitale/lantul_de_incredere_en.htm certSIGN ROOT CA has the following sub-CAs: + certSIGN Demo CA Class 1 Used for demos and testing only, no ID checking performed + certSIGN CA Class 2 Simple certificates used for authentication, signing, and encryption. + certSIGN Qualified CA Class 3 Qualified Certificates + certSIGN Enterprise CA Class3 Trusted Encrypting Certificates used for SSL, code signing, VPN gateways. +certSIGN Non-Repudiation CA Class 4 CA Servers Certificates used for Time Stamping and OCSP. They are all internally operated and included in the CP, CPS, and audit.	
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. (For example, contractual arrangements should require third-party subordinates to operate in	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. At page 11 of CPS: "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)."	COMPLETE

accordance with some CPS/CP. Technical arrangements might include name constraints, not allowing them to create their own subordinates, etc.)		
List any other root CAs that have issued cross-signing certificates for this root CA	None	COMPLETE
Requested Trust Bits One or more of: • Websites (SSL/TLS) • Email (S/MIME) • Code (Code Signing)	Websites Email Code	COMPLETE
If SSL certificates are issued within the hierarchy rooted at this root CA certificate: • Whether or not the domain name referenced in the certificate is verified to be owned/controlled by the certificate subscriber. (This is commonly referred to as a DV certificate.) • Whether or not the value of the Organization attribute is verified to be that associated with the certificate subscriber in addition to verifying the domain name. (This is commonly referred to as an OV certificate.) • Whether verification of the certificate subscriber conforms to the Extended Validation Certificate Guidelines issued by the CAB Forum. (This is commonly referred to as an EV certificate.)	OV As per CPS Section 3.1.7 and 3.1.8 From certSIGN: For all the certificates we issue we perform this check. The difference is that for those issued with certSIGN CA Class 2 we don't ask the subscriber to appear in person at the RA but to send a copy of ID by fax or email. For all the other types of certificates presence is mandatory. Please check table Table 3.1.8 from CPS, page 53.	COMPLETE
If EV certificates are issued within the	Not EV.	COMPLETE

hierarchy rooted at this root, the EV policy OID(s) associated with those EV certificates.		
Example certificate(s) issued within the hierarchy rooted at this root, including the full certificate chain(s) where applicable. • For SSL certificates this should also include URLs of one or more web servers using the certificate(s). • There should be at least one example certificate for each of the major types of certificates issued, e.g., email vs. SSL vs. code signing, or EV vs. OS vs. DV. • Note: mainly interested in SSL, so OK if no email example.	https://www.certsign.ro/certsign_en/ https://www.certsign.ro/certificate_digitale/lantul_de_incredere_en.htm	COMPLETE
CP/CPS • Certificate Policy URL • Certificate Practice Statement(s) (CPS) URL (English or available in English translation)	CP: http://www.certsign.ro/certsign_en/files/CP_certSIGN_EN_v1.0.pdf CPS: http://www.certsign.ro/certsign_en/files/CPS_certSIGN_EN_v1.2.pdf CP and CPS are at the bottom of each page of this site: http://www.certsign.ro/certsign_en/	COMPLETE
AUDIT: The published document(s) relating to independent audit(s) of the root CA and any CAs within the hierarchy rooted at the root. (For example, for WebTrust for CAs audits this would be the "audit report and management assertions" document available from the	Auditor: Ernst & Young Auditor website: www.ey.com Audit: From certSIGN: Details about them can be obtain from the Ernst and Young auditor. More precisely from Mr Gabriel Apostu - Partner, Business and Risk Advisory Services,, at Ernst & Young SRL, Premium Plaza Building, 3rd Floor, 63-69 Dr. Iacob	Please provide link to audit, or attach to bug.

webtrust.org site or elsewhere.)	Felix Street, Sector 1, 011033 Bucharest, Romania; Tel: +40 (0) 21 402 4000, Fax: +40 (0) 21 310 7193, www.ey.com 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	

Review CPS sections dealing with subscriber verification
(section 7 of http://www.mozilla.org/projects/security/certs/policy/)

- Verify the domain referenced in an SSL cert is owned/controlled by the subscriber. In addition to verification of subscriber's legal identity.
    - I found IV/OV verification and uniqueness of domain name requirement in CPS, but I could not find how the RA verifies that the domain name is owned/controlled by the subscriber.
- Verify the email account associated with the email address in the cert is owned by the subscriber. In addition to verification of subscriber's legal identity.
    - Via email: "For all certificates we issue we check if the subscriber has control of the email account associated with email address in the certificate."
    - I need to find this in the CPS.
- Verify identity info in code signing certs is that of subscriber
    - Code signing certs are class 3, and identity is verified in person as per CPS Section 3.1.7 and 3.1.8
- Make sure it's clear which checks are done for which context (cert usage)

Flag Problematic Practices (COMPLETE)
(http://wiki.mozilla.org/CA:Problematic_Practices)

- Long-lived DV certificates
    - SSL certs are OV
    - CPS page 113, Table 6.3.2.2: SSL certificates are issued only with certSIGN Enterprise Class 3 CA. That means that the maxium usage period for an SSL certificate is of 1 year.
- Wildcard DV SSL certificates
    - Not applicable.

- Delegation of Domain / Email validation to third parties
  - Not applicable.
- Issuing end entity certificates directly from roots
  - Not applicable. Root issues sub-CAs only.
- Allowing external entities to operate unconstrained subordinate CAs
  - All sub-CAs are internally operated.
  - 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
    - At page 11 of CPS: "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
  - 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 Table 1.1 Types of certificates from CPS page 12.
- Certificates referencing hostnames or private IP addresses
  - 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
  - OCSP response is signed by a cert under this root.
- CRL with critical CIDP Extension
  - Not applicable

Verify Audits
(Sections 8, 9, and 10 of http://www.mozilla.org/projects/security/certs/policy/)
- Validate contact info in report, call to verify that they did indeed issue this report.
- For EV CA's, verify current WebTrust EV Audit done.
- Review Audit to flag any issues noted in the report