Bugzilla ID: 484171
Bugzilla Summary: Add I.CA 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.

General Information	Data
CA Name	I.CA První certifikační autorita, a.s. First certification authority
Website URL (English version)	http://www.ica.cz/gb/
Organizational type. (E.g., whether the CA is operated by a private or public corporation, government agency, academic institution or consortium, NGO, etc.)	General nature - commercial Primary geographical areas served: Czech Republic, Slovak Republic
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?)	První certifikační autorita, a.s. (First certification authority - I.CA), is the largest provider in the field of issuing and administrating the certificates in the Czech republic. It renders its services in the Slovak republic as well. There have been already more than million of issued certificates registered till today.

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

Info Needed	Data	Data
Certificate Name	I.CA - Qualified root certificate	I.CA - Standard root certificate
Cert summary / comments	To Do – based on info gathered below.	To Do – based on info gathered below.
The root CA certificate URL	http://www.ica.cz/userdata/pages/4/qica_root_20080311.der	http://www.ica.cz/userdata/pages/4/sica_root_20080311.der
SHA-1 fingerprint.	64:90:2a:d7:27:7a:f3:e3:2c:d8:cc:1d:c7:9d:e1:fd:7f:80:69:ea	ab:16:dd:14:4e:cd:c0:fc:4b:aa:b6:2e:cf:04:08:89:6f:de:52:b7
Valid from	2008-04-01	2008-04-01
Valid to	2018-04-01	2018-04-01
Cert Version	3	3
Modulus length / key length or type of signing key (if ECC)	2048	2048

CRL URL	http://qcrldp1.ica.cz/qica08.crl http://qcrldp2.ica.cz/qica08.crl http://qcrldp3.ica.cz/qica08.crl every 24 hours	http://scrldp1.ica.cz/sica08.crl http://scrldp2.ica.cz/sica08.crl every 25 hours
OCSP Responder URL	N/A	N/A
List or description of subordinate CAs operated by the CA organization associated with the root CA. (For 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.)	Please provide a diagram and/or description of the CA hierarchy. Including all of the intermediate CAs that chain up to this root. Indicate which of the sub-CAs are operated internally and which are operated by third parties. For internally-operated subordinate CAs the key is to confirm that their operation is addressed by the relevant CP/CPS, and that any audit covers them as well as the root.	Please provide a diagram and/or description of the CA hierarchy. Including all of the intermediate CAs that chain up to this root. Indicates which of the sub-CAs are operated internally and which are operated by third parties. For internally-operated subordinate CAs the key is to confirm that their operation is addressed by the relevant CP/CPS, and that any audit covers them as well as the root.
Subordinate CAs operated by third parties.	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?	Has this root been involved in cross-signing with another root?
Requested Trust Bits One or more of:	Email (S/MIME)	Websites (SSL/TLS) Email (S/MIME)

• Websites (SSL/TLS) • Email (S/MIME) • Code Signing		
If SSL certificates are issued within the hierarchy rooted at this root CA certificate: • DV – only the domain name referenced in the certificate is verified to be owned/controlled by the certificate subscriber. • OV – in addition to verifying the domain name, the value of the Organization attribute is verified to be that associated with the certificate subscriber. • EV -- Extended Validation Certificate		Do you perform identity/organization verification for all SSL certificates? Is it ever the case for SSL certs that the domain name is verified, but the identity/organization of the subscriber is not verified?
EV policy OID(s)	Not EV	Not EV
CP/CPS	CP in Czech http://www.ica.cz/userdata/pages/2/CP_QCv2.5.pdf	CP in Czech http://www.ica.cz/userdata/pages/2/CP_KC_21.pdf
Translations into English of sections of CP/CPS documents pertaining to: • Verification of Identity and Organization • Verification of ownership/control of domain name • Verification of ownership/control of	Please provide translations into English of the sections of the CP/CPS documents pertaining to: • Verification of Identity and Organization • Verification of ownership/control of domain name • Verification of ownership/control of email address • Section 7 of http://www.mozilla.org/projects/security/certs/policy/ • Potentially Problematic Practices, http://wiki.mozilla.org/CA:Problematic_Practices	Please provide translations into English of the sections of the CP/CPS documents pertaining to: • Verification of Identity and Organization • Verification of ownership/control of domain name • Verification of ownership/control of email address • Section 7 of http://www.mozilla.org/projects/security/certs/policy/ Potentially Problematic Practices, http://wiki.mozilla.org/CA:Problematic_Practices

email address • Section 7 of http://www.mozilla.org/projects/security/certs/policy/ • Potentially Problematic Practices, http://wiki.mozilla.org/CA:Problematic_Practices		
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.	Test cert	https://www.portalzp.cz/czspa00.phtml
AUDIT	Please see sections 8, 9, and 10 of http://www.mozilla.org/projects/security/certs/policy/ We need a publishable statement or letter from an auditor (who meets the policy requirements) that states that they have reviewed the practices as outlined in the CP/CPS for these roots, and that the CA does indeed follow these practices and meets the requirements of one of:	

	• ETSI TS 101 456 • ETSI TS 102 042 • WebTrust Principles and Criteria for Certification Authorities

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.
- 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.
- Verify identity info in code signing certs is that of subscriber
- Make sure it's clear which checks are done for which context (cert usage)
- All documents supplied as evidence should be publicly available and must be addressed in any audit. Any substantial omissions submitted afterwards may need to be confirmed by auditor, at Mozilla's discretion.

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

- Long-lived DV certificates
- Wildcard DV SSL certificates
    - individuals may receive wild card certificates, but the subscriber should be validated. The issue of concern is for domain control validated certificates where no additional verification has
      taken place. Subscribers for wild cards do not have to be organizations – they may be private persons, but the scope of validation matters for this type of certificates.
- Delegation of Domain / Email validation to third parties
    - I.CA website: In order to be able to satisfy all customers needs, it operates more then 300 registration authorities in the Czech and Slovak republic. These contact places enable ideal availability of the services.
- Issuing end entity certificates directly from roots
- Allowing external entities to operate unconstrained subordinate CAs
- Distributing generated private keys in PKCS#12 files
- Certificates referencing hostnames or private IP addresses
- OCSP Responses signed by a certificate under a different root
    - No OCSP

- CRL with critical CIDP Extension
    - CRLs imported into Firefox without error.
- Generic names for CAs

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