Bugzilla ID: 562764
Bugzilla Summary: Add IDRBT root certificate

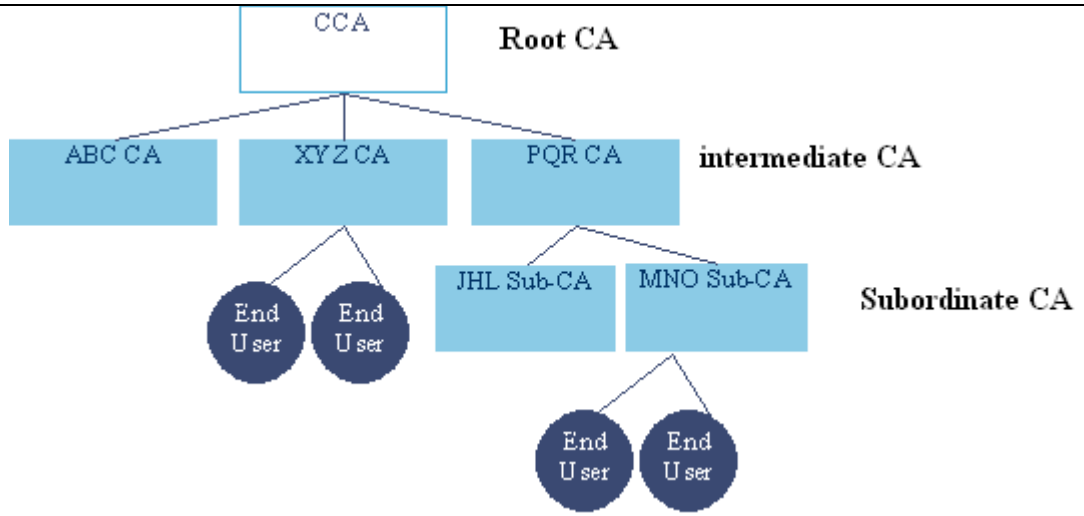
Mozilla CA certificate policy: http://www.mozilla.org/projects/security/certs/policy/
CA's are also encouraged to review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices.

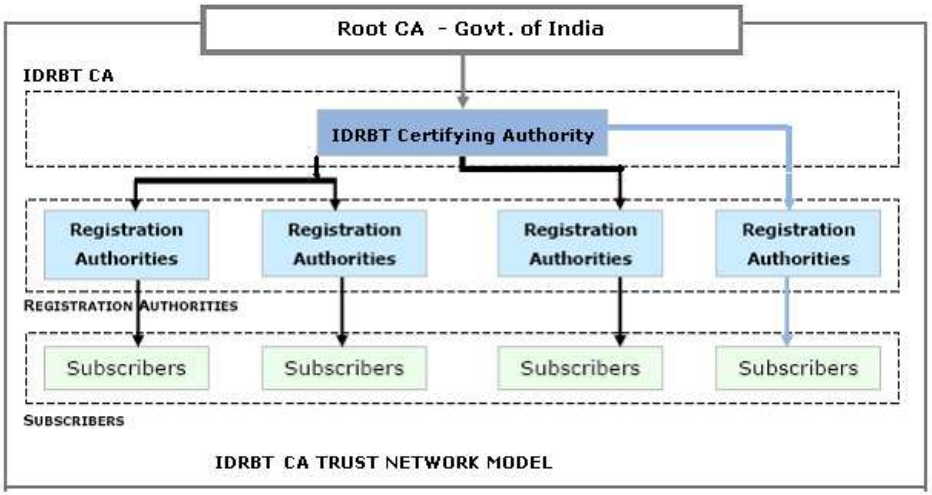
General Information	Data
CA Name	IDRBT
Website URL	http://idrbtca.org.in
Organizational type	Bank/Semi-Government
Primary market / customer base	IDRBT CA functions under the Services Wing of IDRBT, an autonomouos organization established by the Reserve Bank of India for the research and development in Banking Technology and registered as a Society under Andhra Pradesh (Telengana areas) Public Societies Registration Act, 1350 Fasli (Act 1 of 1235OF) with its registered office at IDRBT, Castle Hills, Road No.1, Masab Tank, Hyderabad – 500 057, India. IDRBT offers Certification Services primarily for the members of the INFINET; banks and Financial institutions in India.
CA Contact Information	CA Email Alias: cahelp@idrbt.ac.in CA Phone Number: 91-40-23534981 Title / Department: IDRBT 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	IDRBT CERTIFYING AUTHORITY
Issuer Field	CN = CCA India 2007 O = India PKI C = IN
Subject Field	ST = Andhra Pradesh E = cahelp@idrbt.ac.in L = Hyderabad CN = IDRBT CERTIFYING AUTHORITY OU = IDRBT CA O = INDIA PKI C = IN
Cert summary / comments	This CA is signed by CCA India, and is used to establish a trust chain from CCA to end entities in digital certificates issued by IDRBT CA to be used in PKI-enabled applications. IDRBT CA offers 3 distinct classes of certification services. Each class of certificate provides specific functionality and security features. The classes are: Class 1, Class 2, and Class 3.
Root Cert URL	http://idrbtca.org.in/download/IDRBTCA2007.cer

SHA-1 fingerprint	64:3C:C0:FC:C7:E5:E5:C5:E6:F7:D9:3E:79:57:57:2C:AE:75:86:2C
Valid from	2007-07-16
Valid to	2015-07-04
Cert Version	3
Modulus length / key length	2048
Test Website	https://services.idrbtca.org.in/
CRL URL	http://idrbtca.org.in/crl.crl CPS section 4.6.9, CRL Issuance Frequency: …IDRBT CA will make every effort to publish new CRL in every last working day of the week. When I try to import the CRL, http://idrbtca.org.in/crl.crl, into my Firefox browser, I get thee error: Error Importing CRL to local Database. Error Code:ffffe009 ffffe009 is equivalent to -8183, "Security library: improperly formatted DER-encoded message." It means that the reply contained anything other than a valid DER-encoded CRL. Typical Resolution: Change encoding from PEM to DER.
OCSP Responder URL	None. OCSP is currently not provided.
CCA CA Hierarchy	In order to facilitate greater flexibility to Certifying Authorities, the CCA allowed the creation of subordinate-CAs. As per this model, an intermediate Certifying Authority can create a subordinate-CA to meet his business-branding requirement. However the subordinate-CA will be part of the same legal entity as the CA. It is also necessary that the subordinate-CA will be in the same infrastructure of intermediate CA. The CA model will be based on the following principles (effective from Jan 2011) • The intermediate CAs MUST NOT have more than ONE level of subordinate -CAs • The subordinate-CA MUST use a subordinate-CA certificate issued by the intermediate CA for issuing end entity certificates • The subordinate-CA must necessarily use the intermediate-CAs infrastructure for issuing certificate • The subordinate-CAs operations shall be subject to same audit procedures as the intermediate CA • The certificate policies of the subordinate-CA must be same as of the intermediate CA's certificate policies

	 There are currently seven intermediate CAs under the Root CA of India. Though intermediate CAs have subordinate CA under that, they are all physically located in the same physical infrastructure of intermediate CAs. The subordinated CAs are allowed mainly for operational management. The intermediate CAs and its subordinate CAs have single CPS. The Audit is as per security guidelines mentioned in the Information Technology ACT. Strict measures are taken by Root CA to monitor the compliance of CPS, and recommendations specified in the Information Technology Act
IDRBT CA Hierarchy	IDRBT CA does not currently have any subordinate CAs.

	 IDRBT CPS section 1.3.1: After verification of the credentials of the RA by IDRBT CA, the RA will be issued a Class 3 Certificate from IDRBT CA in person. The RA Office will verify the credentials of the subscribers as mentioned in the section 4.1.2 of this CPS and will approve the certificate request and release the request to IDRBT CA Office for the issuance of the certificate. Under the IT Act all functions of RA are subsumed within the IDRBT CA. IDRBT CA is responsible for all actions of RAs including correctness of the subscriber information given by RA which is incorporated using contractual Master Agreement.
Externally Operated Sub-CAs	Currently None IDRBT CPS section 1.3.1: On advice of the CCA, IDRBT CA may include Subordinate CA also.
Cross-Signing	Currently None IDRBT CPS section 4.12: IDRBT CA will undergo Cross-certification with other operating CAs as per the Rules and Regulations to Certifying Authorities, by CCA, Ministry of Communication and Information Technology.
Technical Constraints on Third-party Issuers	Please describe the technical constraints that are in place for all third-parties (CAs and RAs) who can directly cause the issuance of certificates. See #4 of https://wiki.mozilla.org/CA:Information_checklist#CA_Hierarchy_information_for_each_root_certificate
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) Code Signing
SSL Validation Type DV, OV, and/or EV	OV

EV policy OID(s)	Not EV
CCA CP/CPS	Root CA CPS: http://cca.gov.in/rw/pages/rcai_cps.en.do Steps to become CA: http://cca.gov.in/rw/pages/becoming_ca_suppdoc.en.do FAQ : http://cca.gov.in/rw/pages/faqs.en.do CCA sub-CAs: http://cca.gov.in/rw/pages/ca_certificates_2007.en.do
IDRBT CP/CPS	IDRBT Repoistory: https://services.idrbtca.org.in/ IDRBT CPS (English): http://idrbtca.org.in/CPS.html IDRBT CP for Offline Users (English): http://idrbtca.org.in/Download/IDRBT-CPO-v1.2.pdf
AUDIT	Audit Type: WebTrust CA equivalent, based on Controller of Certifying Authorities (CCA) for the Government of India Information Technology Act 2000, Rules, Regulation & Guidelines Auditor: M/s Digital Age Strategies Pvt. Ltd., Bangalore (Present Auditor) Auditor Website: http://www.digitalage.co.in/home/default.aspx Letter from Auditor: https://bugzilla.mozilla.org/attachment.cgi?id=472254 (2010.02.09) – need updated audit. CCA Approved Auditors List: http://cca.gov.in/rw/pages/auditors.en.do CCA Audit Criteria: http://cca.gov.in/rw/pages/auditors_auditcriteria.en.do Information Technology Act: http://cca.gov.in/rw/pages/it_act.en.do Rules: http://cca.gov.in/rw/pages/rules.en.do Act Modification: http://cca.gov.in/rw/resource/actmod_nov02.pdf IT Act Regulations: http://cca.gov.in/rw/pages/regulations.en.do According to CCA Approved Auditors List (http://cca.gov.in/rw/pages/auditors.en.do) the contacts for the auditor M/s Digital Age Strategies Pvt. Ltd. are: digitalageaudit@airtelmail.in / chinwik@gmail.com 9/13: I have sent email to these addresses to confirm the authenticity of the audit letter that was attached to the bug. 9/26/2011: I did not receive a response.
Organization Identity Verification	Identity Verification procedures are described in section 3.1.2 of the IDRBT CPS. CPS Section 3.2.8, Authentication of organizational identity: The RA needs to verify that an entity belongs to the set of entities that the IDRBT CA recognizes as qualified to become and end user. A Representative of an organization should come with a letter authorizing him/her to represent the organization for the given purpose. IDRBT CPS Section 4.1.2 has a table of the information that must be verified for each class and usage of certificate. IDRBT CPS Section 4.2 lists the items that the RA shall validate.

	Snippets from IDRBT CPS Section 2.11: **Class 1** certificates are issued only to individuals. Class 1 certificates confirm that a user's name (or alias) and e-mail address form a distinct subject name within the IDRBT CA repository. Class 1 certificates are added to his/her set of available certificates in the directory services. They are used primarily for digital signature, to enhance the security of environments. Class 1 Encryption Certificates are used for e-mail purposes. RA verifies the name, e-mail address, organization and the postal address in the request. The verification of the certificate request of this class represent a simple check of the certainty of the subject name within the IDRBT CA repository, plus a limited verification of the address, other personal information and e-mail address. **Class 2** certificates are issued to individuals and to the servers used in financial transactions. The RA basis it on the verification of the applicant form and the certificate request. RA verifies the name, e-mail address and the postal address in the request. Class 2 Certificate processes utilize various procedures to obtain probative evidence of the identity of individual applicants. These validation procedures provide stronger assurance of an applicant's identity. The Class 2 Certificate is used for Digital Signature and Encryption. **Class 3** Certificates are issued to Individuals as well as Servers. Class 3 Certificates provide important assurances of the identity of individual subscribers by requiring their personal (physical) appearance before an RA. All the personal details (as mentioned in section 4.1.2) will be physically verified by the RA office and after confirmation of facts it will recommend the issuance of the certificate. Class 3 Certificates for Secure Server will help web servers to enable secure communications through the use of Secure Sockets Layer (SLL) technology. As a matter of practice, IDRBT CA issues Class 3 certificates to web servers. IDRBT CA Secure Server Certificate boosts the credibility and scope of website with today's strongest encryption available for secure communications. Along with the application form the authorized person must give the domain name or the Server IP address on which it needs the Certificate. The domain name must be registered and the proof must also be accompanied with the application. Class 3 certificates are issued either for one year validity period or two years validity period as per choice of the subscriber.

	Class 3 Certificate processes make use of various procedures to obtain strong confirmation of the identity of individual applicants as well as the server. These validation procedures provide stronger guarantee of an applicant's identity. Utilizing validation procedure by the Registration Authorities boosts the practical uses and trustworthiness of Class 3 Certificates. The Class 3 Certificate is intended to use for Digital Signature, Encryption of messages, Object signing and Secure Web Server. IDRBT CPS section 4.1.2: In case of Class 3 application the applicant/subscriber should present before RA of the bank where customer has account or is employee of the bank for personal verification.
Domain Name Ownership / Control	Please see: https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices "We rely on publicly available documentation and audits of those documented processes to ascertain that the CA takes reasonable measures to confirm the identity and authority of the individual and/or organization of the certificate subscriber." And item #3, "SSL Verification Procedures". SSL Certificates are Class 3, which means that the identity/organization are verified as described in sections 3 and 4 of the IDRBT CPS. The CPS states that the subscriber must provide proof of domain registration. However, I do not see a description of the steps that are taken to confirm that the domain registration information provided by the subscriber is authentic. Please see https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Domain_Name_Ownership There needs to be public-facing and audited documentation (such as in the CPS) about steps that are taken to verify that the SSL certificate subscriber owns/controls the domain name to be included in the certificate. Comment #5: The official authorized by the organization to apply for SSL Certificate should enclose the proof of registration of domain name along with the application form in order to get a digital certificate for the domain name. Does anyone verify the authenticity of the "proof of registration of domain name" that is provided by the organization?
Email Address Ownership / Control	Please see: https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices "We rely on publicly available documentation and audits of those documented processes to ascertain that the CA takes reasonable measures to confirm the identity and authority of the individual and/or organization of the certificate subscriber." And item #4, "Email Address Verification Procedures". The CPS states that the RA should verify the e-mail address. However, it doesn't provide any information about the steps that should be taken to confirm that the certificate subscriber owns/controls the email address to be included in the

	certificate. Please see https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Email_Address_Control There needs to be public-facing and audited documentation (such as in the CPS) about steps that are taken to verify that the certificate subscriber owns/controls the email address to be included in the certificate. Comment #5: E-mail verification is done by sending user id and password across e-mail to the end-user to enable submission of Digital certificate Request to IDRBT. This ensures that the official who has requested for digital certificate also has the ownership/control over the e-mail address. Subscribers are personally and solely responsible for the confidentiality and integrity of their private keys. Is this documented in the CPS?
Identity of Code Signing Subscriber	Code Signing are Class 3, which means that the identity/organization are verified as described in sections 3 and 4 of the IDRBT CPS.
Multi-factor Authentication	Please confirm that multi-factor authentication is required for all accounts capable of directly causing certificate issuance. See # 6 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices
Network Security	Please confirm that you have performed the actions listed in #7 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices
Potentially Problematic Practices	http://wiki.mozilla.org/CA:Problematic_Practices Long-lived DV certificates SSL cert are OV, and are valid for one or two years. Wildcard DV SSL certificates SSL certs are OV Email Address Prefixes for DV SSL Certs SSL certs are OV Delegation of Domain / Email validation to third parties CPS Section 2.1.2: RA Obligations Issuing end entity certificates directly from roots No Allowing external entities to operate unconstrained subordinate CAs No

	Distributing generated private keys in PKCS#12 files Comment #5: The file containing the private key, public key and the digital certificate can be downloaded by logging in to the Secured site of IDRBT using the user id and password provided to the end-entity. The file is also protected by a password. What types of certificates does this apply to? Certificates referencing hostnames or private IP addresses Yes, SSL certs may be issued for IP addresses. Issuing SSL Certificates for Internal Domains Comment #5: SSL Certificates have NOT been issued for internal domains SO FAR. Is this allowed? If yes, then what procedures are in place to verify that the certificate subscriber owns the right to use the domain? Is this documented in the CPS? OCSP Responses signed by a certificate under a different root OCSP not provided. CRL with critical CIDP Extension No Generic names for CAs CA name includes IDRBT.