Bugzilla ID: 562764
Bugzilla Summary: Add IDRBT root certificate

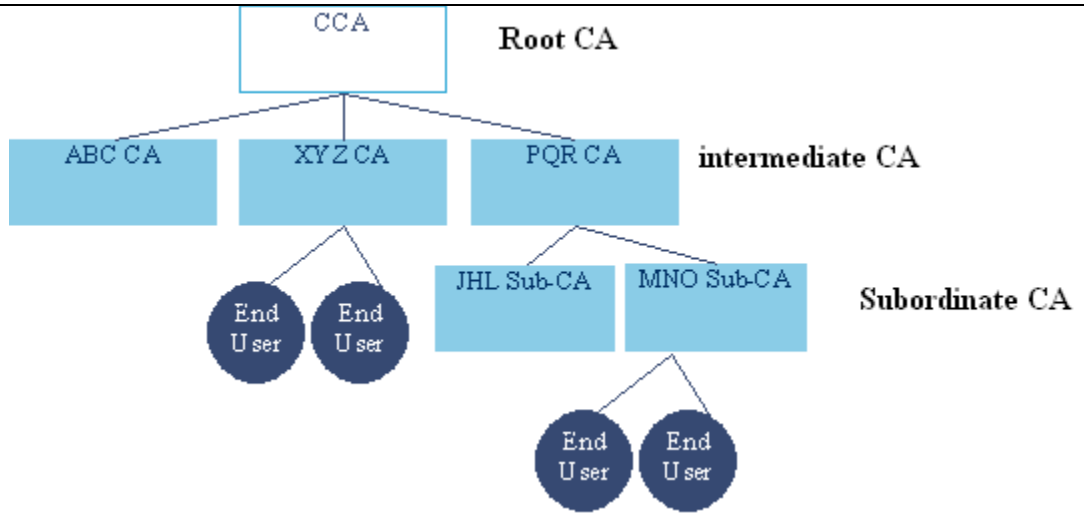
Mozilla CA certificate policy: http://www.mozilla.org/projects/security/certs/policy/
CA's are also encouraged to review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices.

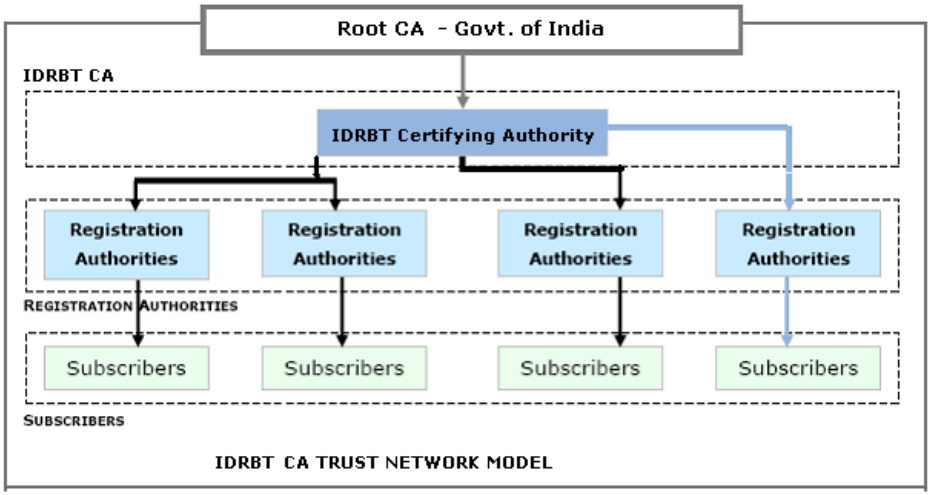
General Information	Data
CA Name	IDRBT
Website URL	http://idrbtca.org.in
Organizational type	Bank/Semi-Government
Primary market / customer base	IDRBT CA functions under the Services Wing of IDRBT, an autonomouos organization established by the Reserve Bank of India for the research and development in 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 CA 2011
Issuer Field	CN = CCA India 2011 O = India PKI C = IN
Subject Field	CN = IDRBT CA 2011 Object Identifier (2 5 4 51) = Castle Hills Object Identifier (2 5 4 9) = "Road No.1, Masab Tank, Hyderabad" ST = Andhra Pradesh Object Identifier (2 5 4 17) = 500057 OU = Certifying Authority O = Institute for Development and Research in Banking Technology 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/CA_Certificate_SHA2.cer
SHA-1 fingerprint	C4:76:9E:35:76:51:78:D4:DE:54:34:E6:B4:E2:58:15:E9:0D:0C:FE
Valid from	2011-03-11
Valid to	2016-03-11
Cert Version	3
Signature Algorithm	SHA-256
Modulus length / key length	2048
Test Website	https://services.idrbtca.org.in/
CRL URL	http://cca.gov.in/rw/resources/CCAIndia2011Latest.crl -- Error: Code:ffffe009 http://idrbtca.org.in/crl_2794.crl -- CRL imported correctly -- valid for 17 days? 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. 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. Required now as per the CA/Browser Forum's Baseline Requirements.
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	Currently not applicable. All the rules of CCA would apply.
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	Guidelines issued by CCA: http://cca.gov.in/cca/index.php India PKI CP Ver 1.1: http://cca.gov.in/cca/index.php?q=india_pki_cp_ver1.1.html CPS: http://cca.gov.in/cca/?q=cps.html FAQ: http://cca.gov.in/cca/?q=faq-page CCA sub-CAs: http://cca.gov.in/cca/?q=faq-page#n41
IDRBT CP/CPS	IDRBT Repository: http://idrbtca.org.in/repository.htm IDRBT CPS (English): http://idrbtca.org.in/CPS.html
Baseline Requirements	How is it indicated that IDRBT complies with the CA/Browser Forum's Baseline Requirements? Comment #13: Please add a comment in this bug to provide IDRBT's answers to the action items listed in Mozilla's January CA Communication: https://wiki.mozilla.org/CA:Communications#January_10.2C_2013
Response to CA Communications	Please provide response to this CA Communiction and action items: https://wiki.mozilla.org/CA:Communications#January_10.2C_2013
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) 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 Need 2012 or 2013 audit statement
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.
Email Address Ownership / Control	CPS section 4.1.2: E-mail verification is done by the way of sending the user-id to subscriber to enable the submission of the Certificate Signing Request to CA system. This ensures that the subscriber, who has requested for the certificate, also has the control over the e-mail mentioned in the request form.
Domain Name Ownership / Control	CPS section 4.1.2: Domain and E-mail validation are performed by the Registration Authority officials of Registration Authority offices of IDRBT CA. The Certifying Authority issues the digital certificates only after validating/verifying the Distinguished Name Details such as Common Name, E-mail id, Organization, Organization Unit, Postal Code of the Locality, State and Country in online requests digitally signed and released by the Registration Authority Officials. For obtaining Web Server (SSL) Certificate, the applicant is required to submit the application form with details of IP Address, URL/Domain name, the Custodian of the web Server, Department to which the server belongs, Official address, Contact Number and Physical Location of the Server etc to the Registration Authority. Only after proper verification of the details of Domain Name contained in the Common Name and Subject Alternative Name (SAN) mentioned in the application form by the subscriber are properly verified by the Registration Authority officials based on which the subscriber will be allotted a User Id to apply online for the Web Server Certificate. Before issuing SSL certificate, the authenticity of Applicant's registration, ownership or exclusive control of the Domain Name(s) to be listed in the SSL Certificate will be verified by the Certifying Authority that the domain name is registered with an Internet Corporation for Assigned Names and Numbers (ICANN) approved registrar or a registry listed by the Internet Assigned Numbers Authority (IANA). This process would help the Certifying Authority not to issue certificates for non-valid Top Level Domains (TLD). For GOV.IN the authenticity will be verified by the Certifying Authority from the registry maintained by National Informatics Centre (https://registry.gov.in/). CA also ensures the correctness of the furnished information by making NSLOOKUP query / WHOIS Lookup query as applicable, and in case of any doubt, the RA is advised to contact the applicant over phone, email or personal interaction for clarifications to resolve the matter. CA will further confirm that the Applicant is aware of its registration or exclusive

	control of the Domain Name.
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	CPS section 5, Physical, Procedural, and Personnel Security Controls CPS section 5.2, Procedural Controls CPS section 5.2.2: The duties to be performed by each of the trusted personnel in the IDRBT CA Organizational structure are defined in such a manner that no single person would take control of the certificate issuance/revocation process.
Network Security	CPS section 6, Technical Security Controls
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 Domain and E-mail validation are performed by the Registration Authority. Certifying Authority also issues the digital certificates only after validating/verifying the Distinguished Name Details such as Common Name, E-mail id, Organization, Organization Unit, Postal Code of the Locality, State and Country in digitally signed online requests released by the Registration Authorities. Relevant Reference sections in CPS: Domain validation Section 4.1.2 Certificate application information and communication E-mail validation Section 9.1 Subscriber Application form & Section 2.11.1 & 2.11.2 Class 1 Certificates & Class 2 Certificates 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 Relevant Reference sections in CPS: Section 4.3 Certificate issuance

	Section 6.1.2 Private key delivery to entity Section 2.12.2 Encryption certificate Section 9.4 Subscriber Agreement Certificates referencing hostnames or private IP addresses Yes, SSL certs may be issued for IP addresses. Issuing SSL Certificates for Internal Domains Comments from IDRBT CA: There are no certificates that have been issued within CA hierarchy which have .int domain name in the Common Name and/or as DNS Name in the SubjectAlternativeName. Validate all Data included in Certificates Relevant Reference sections in CPS: Section 3.1.2 End Entity Initial Registration, Section 3.1.2.1 Identity Verification, Section 3.1.2.2 Post Identity Verification and Section 4.1.2. Certificate Application Information and Communication Authentication includes the following: 1. The identity of the person performing the identity verification; 2. A signed declaration by that person that he or she verified the identity of the applicant; 3. The applicant shall present one photo ID. The applicant shall also present a document as a proof of residential address. 4. Unique identifying numbers from the Identifier (ID) of the verifier and from an ID of the applicant; 5. The date and time of the verification; and 6. A declaration of identity signed by the applicant using a handwritten signature or equivalent per Indian Laws. For Class 3 certificates, identity shall be established by in-person proofing before the RA, to confirm identities; information provided shall be verified to ensure legitimacy. A trust relationship between the RA and the applicant which is based on an in-person antecedent may suffice as meeting the in-person identity proofing requirement. 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.