

Bugzilla ID: 562764

Bugzilla Summary: Add IDRBT root certificate

Mozilla CA certificate policy: <http://www.mozilla.org/projects/security/certs/policy/>

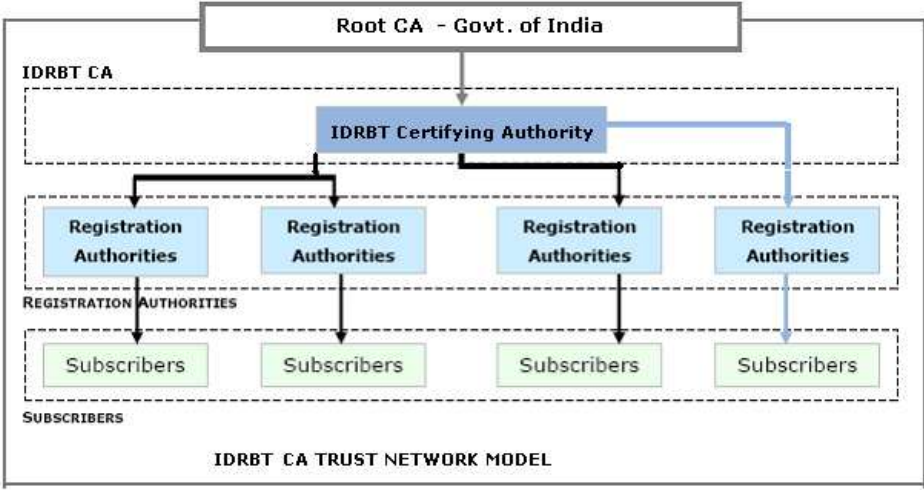
CA's are also encouraged to review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices.

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 autonomous 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: idrbtca@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
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 Error on trying to go to website in Firefox browser (IDRBT CA has been imported into my browser) services.idrbtca.org.in uses an invalid security certificate. The certificate is only valid for 10.0.65.60 (Error code: ssl_error_bad_cert_domain)

CRL URL	https://services.idrbtea.org.in/Subscriber/Subscriber/Download/downloadCRL.jsp (30 days) I did not find information in the IDRBT CPS about the CRL issuance frequency for end-entity certificates.
OCSP Responder URL	
CCA CA Hierarchy	<p>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.</p> <p>The CA model will be based on the following principles (effective from Jan 2011)</p> <ul style="list-style-type: none"> • 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 <div data-bbox="651 706 1722 1209" data-label="Diagram"> <pre> graph TD CCA[CCA] --- ABC[ABC CA] CCA --- XYZ[XYZ CA] CCA --- PQR[PQR CA] ABC --- EU1((End User)) ABC --- EU2((End User)) XYZ --- JHL[JHL Sub-CA] XYZ --- MNO[MNO Sub-CA] PQR --- JHL PQR --- MNO JHL --- EU3((End User)) JHL --- EU4((End User)) MNO --- EU5((End User)) MNO --- EU6((End User)) </pre> </div> <p>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</p>

IDRBT CA Hierarchy	<p>IDRBT CA does not currently have any subordinate CAs.</p>  <p>The diagram illustrates the IDRBT CA Trust Network Model. At the top is the Root CA - Govt. of India. Below it is the IDRBT CA, which contains the IDRBT Certifying Authority. This authority is connected to four Registrars (Registration Authorities). These Registrars are then connected to their respective Subscribers. The entire structure is labeled as the IDRBT CA TRUST NETWORK MODEL.</p> <p>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.</p>
Externally Operated Sub-CAs	<p>Currently None IDRBT CPS section 1.3.1: On advice of the CCA, IDRBT CA may include Subordinate CA also.</p>
Cross-Signing	<p>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.</p>
Requested Trust Bits	<p>Websites (SSL/TLS) Email (S/MIME) Code Signing</p>
SSL Validation Type DV, OV, and/or EV	<p>OV</p>
EV policy OID(s)	<p>Not EV</p>

CCA CP/CPS	<p>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</p>
IDRBT CP/CPS	<p>IDRBT CPS (English): http://idrbtca.org.in/Download/IDRBT-CPS-v3.1.pdf IDRBT CP for Offline Users (English): http://idrbtca.org.in/Download/IDRBT-CPO-v1.2.pdf</p>
AUDIT	<p>Audit Type: 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 Audit Document URL(s): Confidential</p> <p>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</p> <p>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 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:</p> <ul style="list-style-type: none"> • ETSI TS 101 456 • ETSI TS 102 042 • WebTrust Principles and Criteria for Certification Authorities <p>My understanding is that the IT Act 2000 criteria are equivalent to the WebTrust for CAs audit criteria. Is this true? Is there public documentation to state or support this claim?</p>
Organization Identity Verification	<p>Identity Verification procedures are described in section 3.1.2 of the IDRBT CPS.</p> <p>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.</p> <p>IDRBT CPS Section 4.1.2 has a table of the information that must be verified for each class and usage of certificate.</p> <p>IDRBT CPS Section 4.2 lists the items that the RA shall validate.</p>

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 (SSL) 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.

	<p>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.</p> <p>The Class 3 Certificate is intended to use for Digital Signature, Encryption of messages, Object signing and Secure Web Server.</p> <p>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.</p>
<p>Domain Name Ownership / Control</p>	<p>SSL Certificates are Class 3, which means that the identity/organization are verified as described in sections 3 and 4 of the IDRBT CPS.</p> <p>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</p> <p>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.</p>
<p>Email Address Ownership / Control</p>	<p>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.</p> <p>Please see https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Email_Address_Control</p> <p>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.</p>
<p>Identity of Code Signing Subscriber</p>	<p>Code Signing are Class 3, which means that the identity/organization are verified as described in sections 3 and 4 of the IDRBT CPS.</p>
<p>Potentially Problematic Practices</p>	<p>Please review the list of Potentially Problematic Practices (http://wiki.mozilla.org/CA:Problematic_Practices). Identify the ones that are and are not applicable. For the ones that are applicable, please provide further information.</p> <p>Long-lived DV certificates SSL cert are OV</p> <p>Wildcard DV SSL certificates SSL certs are OV</p> <p>Email Address Prefixes for DV SSL Certs SSL certs are OV</p>

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

?

Certificates referencing hostnames or private IP addresses

Yes, SSL certs may be issued for IP addresses.

Issuing SSL Certificates for Internal Domains

?

OCSP Responses signed by a certificate under a different root

?

CRL with critical CIDP Extension

?

Generic names for CAs

CA name includes IDRBT.