Bugzilla ID: 511380
Bugzilla Summary: Add NIC Certifying Authority 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.

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

General Information	**Data**
CA Name	National Informatics Centre (NIC)
Website URL (English version)	http://nicca.nic.in
Organizational type	National Government CA
Primary market / customer base	National Informatics Centre (NIC), a premier IT Organisation of the Department of Information Technology, Govt. of India, has been instrumental in steering Information and Technology applications in various Government Departments at Central, State and District levels, facilitating improvement in Government services for the Public, wider transparency in Government functions, and improvement in decentralized planning and management. As the nodal IT organization in the country, NIC has established the Certifying Authority (NICCA) in May, 2003, under license from the CCA for issuance of Digital Signature Certificates. Since its inception, NICCA has played a major role to promote, develop and incorporate e-governance in the country.

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

Info Needed	**Data**
Certificate Name	NIC Certifying Authority
Cert summary / comments	NIC CA issues three classes of Digital Signatures to subscribers, based on the level of verification that is performed in regards to the identity of the certificate subscriber. The NIC CA directly signs Class 1, Class 2 and Class3 end-entity certificates which can be used for SSL, email, and document signing. The NIC CA also signs the E-passport Sub-CA which signs Class 1, Class 2 and Class3 end-entity certificates which can be used for SSL, email, and document signing. These Digital Signatures are issued based on verification procedures as stated in the Information Technology (IT) Act 2000, an Act which was passed by the Indian Parliament in June 2000.
The root CA certificate URL	NICCA Root Certificate: https://bugzilla.mozilla.org/attachment.cgi?id=397595 CCA Root Certificate: https://bugzilla.mozilla.org/attachment.cgi?id=397596
SHA-1 fingerprint.	48:22:82:4e:ce:7e:d1:45:0c:03:9a:a0:77:dc:1f:8a:e3:48:9b:bf
Valid from	2007-07-01

Valid to	2015-07-03
Cert Version	3
Modulus length / key length	2048
Test Website	https://nicca.nic.in
CRL URL	https://nicca.nic.in/crl_2783.crl NextUpdate: 7 days. CPS section 2.1.5: The publication of the CRL is scheduled, at least once in every week. The NICCA will immediately update and publish CRL after Suspension/Revocation of DSCs
OCSP Responder URL	None – OCSP is currently not provided
CA Hierarchy	Diagram: https://bug511380.bugzilla.mozilla.org/attachment.cgi?id=398631 When the NICCA root certificate alone is imported, it acts as the root. When the CCA root certificate is also imported, the NICCA certificate chains up to it. Comment #7: We (Mozilla) have the technical capability to treat any CA certificate as a trust anchor, whether it's a root or not. So, in cases where a root does not qualify under Mozilla's policy, or chooses not to apply, but a subordinate CA does qualify and does apply, it is feasible for Mozilla to go ahead an approve the cert for that subordinate CA to be treated like a root in Mozilla's trusted list. Now, some policy questions arise when considering such a case. For example: if a subordinate CA applies for admission to Mozilla's list, and its superior root CA does not apply, how long should Mozilla wait before deciding to go ahead and grant trust anchor status to the subordinate? Comment #9: in the Indian PKI regime, NICCA is not an intermediate CA or Sub-CA, in the real sense. This is further explained in the following lines wherein I have tried to present the Indian PKI model. -- The Government of India established the Controller of Certifying Authorities (CCA), under section 17 of the Information Technology (IT) Act 2000, an Act which was passed by the Indian Parliament in June 2000. The IT Act promotes the use of Digital Signatures for e-governance and e-Commerce through legal recognition to electronic records, and treats digital signatures at par with handwritten signatures. The Act defines the legal and administrative framework for establishment of a Public Key Infrastructure (PKI) in the country for creating trust in the electronic environment. The CCA (url : http://cca.gov.in) is the apex body to issue license and regulate the working of Certifying Authorities, in accordance with the provisions of the IT Act 2000. CCA has set up the The Root Certifying Authority of India (RCAI), which is at the root of trust in the hierarchical PKI established in the country. The Certifying Authorities, which meet the requisite criteria specified in the IT Act 2000, are issued licenses to operate by CCA and come under the RCAI. The Certifying Authorities (CAs) in turn issue certificates

	to the general public and others in accordance with the CA's CPS. As on date, there are eight CAs that are operating under RCAI in India and NICCA is one of them. CCA, which is the apex regulatory body under the well established hierarchical PKI regime in the country, issues license to operate as a CA under its domain only after overseeing and ensuring the compliance of the "Technical Requirements" and "Operating Standards" under the IT Act 2000, by the participating CA. These standards are at par with the existing international practices and a comparison between the audit program requirements of CCA and WebTrust shows a clear equivalence. -- Controller of Certifying Authorities (CCA) is the government Licensing and Regulatory Authority, which has been set up under the Information Technology (IT) Act 2000. The IT Act was passed by the Indian Parliament in June 2000 and defines the legal and administrative framework for establishment of a PKI in the country. The Act requires that for a Digital Signature Certificate to be valid in an Indian court of law, it has to be issued by a Certifying Authority which has been licensed to operate by the CCA. CCA has set up the The Root Certifying Authority of India (RCAI), which is at the root of trust in the well established hierarchical PKI system in the country. The CCA issues license to a Certifying Authority only after overseeing and ensuring the compliance of the "Technical Requirements" and "Operating Standards" under the IT Act 2000, by the participating CA. These standards are at par with the existing international practices and a comparison between the audit program requirements of CCA and WebTrust shows a clear equivalence. As on date, there are eight CAs that are operating under RCAI in India and NICCA is one of them. So in the Indian PKI hierarchy, CCA operates a root CA, but technically it is a licensing body whose end entity is a CA only. It may please be noted that CCA does not issue certificates to individuals. Only the licensed CAs in India issue certificates to the general public and others, in accordance with the respective CA's CPS. The point in Comment #7 for inclusion of CCA's Certificate is well taken. It may be reiterated here that CCA is a facilitator for the proliferation of PKI technology in India and NICCA would approach CCA in due course with a request for enrolment of CCA's Certificate in the firefox browser.
List or description of subordinate CAs operated by the CA organization associated with the root CA.	The NIC CA directly signs Class 1, Class 2 and Class3 end-entity certificates which can be used for SSL, email, and document signing. The NIC CA also signs the E-passport Sub-CA which signs Class 1, Class 2 and Class3 end-entity certificates which can be used for SSL, email, and document signing. Sub-CAs may be created for different organizations and agencies, for ease of operations and management. The sub-CAs would be created purely in a technical context, to be part of the NICCA's technical infrastructure. The keys created for the sub-CAs will be located only on NICCA's technical infrastructure.

	Sub-CAs can issue Certificates only in the specified domain for which the sub-CA has been created. Agencies for whom the Sub-CAs are created have to be reflected in the corresponding certificate as ‘NICCA – Sub-CA for <name of agency for whom Sub-CA has been set up>’. Sub-CAs cannot create their own subordinates. The certificate issuing authority for the Sub-CA always remains only with NICCA.
SubCAs operated by 3rd parties	The keys created for Sub-CAs are located only on NICCA’s technical infrastructure.
Cross-signing	None
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) Code Signing
If SSL certificates are issued within the hierarchy rooted at this root CA certificate: DV, OV, and/or EV	DV (Class 1), OV(Class 2 and 3) Comment #14: > My interpretation of the current CPS is that all three of the class/verification levels can be used > for issuing SSL Certs. Is this correct? Yes
EV policy OID(s)	Not EV
CP/CPS	The following documents are all in English. Certificate Practice Statement of NIC CA: http://nicca.nic.in/pdf/niccacps.pdf Overview of Information Technology Act 2000: http://nicca.nic.in/index.jsp Details of Information Technology Act 2000: http://nicca.nic.in/pdf/itact2000.pdf Digital Signature Certificate Request Form: http://nicca.nic.in/pdf/DSC-Request-Form.pdf The NICCA authenticates entities requesting a Certificate, with the help of the RA setup at the concerned Government organization and with the help of the NIC Coordinator of that organization. (Detailed procedure given in the Digital Signature Certificate Request Form)
	The Policy Overview section in the CPS describes how the identity of the certificate subscriber is verified depending on the class/assurance level. ***Class-1 Certificate*** **OID 2.16.356.100.1.4.3.1** ***Category*** Issued to the Individual from Govt., PSU/Statutory Bodies, Government Registered Companies and Web Servers/Servers. ***Suggested Usage*** Signing certificate primarily be used for signing personal emails and encryption certificate is to be used for encrypting digital emails and SSL certificate is used to establish secure communications through the use of secure socket layer (SSL)

	Assurance Level Provides minimum level of assurance. Subscriber's identity is proved only with help of Distinguished Name - DN and hence provides limited assurance of the identity. **Verification Process** Simply Checks for the certainty of the details given in the DSC Request Form as authenticated by Head of Office ***Class-2 Certificate*** **OID 2.16.356.100.1.4.3.2** ***Category*** Issued to the Individual from Govt., PSU/Statutory Bodies, Government Registered Companies and Web Servers/Servers. ***Suggested Usage*** In addition to the 'suggested usage' mentioned in class I, the class II Signing certificate may also be used for digital signing, code signing, authentication for VPN Client, web form signing, smart card logon, user authentication, single sign-on and signing involved in e-procurement/e-governance applications. In addition to the 'suggested usage' mentioned in class I, the class II Encryption certificate may also be used for encryption involved in e-procurement/e-governance applications. SSL certificate is used to establish secure communications through the use of secure socket layer (SSL). **Assurance Level** Provides higher level of assurance confirming the details submitted in the DSC Request Form, including photograph and documentary proof in respect of at least one of the identification details. **Verification Process** Checks for the certainty of the details given in the DSC Request Form as authenticated by Head of Applicant's Organisation, which is further authenticated by HOD/SIO/DIO/ NICCoordinator. Applicant's Organisation utilizes various procedures to obtain evidence in respect of identity of the applicants by way of documentary evidence of one of the items under point no 8 (Identification details), resulting in stronger assurance level. ***Class-3 Certificate*** **OID 2.16.356.100.1.4.3.3** ***Category*** Issued to individuals from Government entities/Head of the Institutions, Statutory/Autonomous bodies, Government registered Companies ***Suggested Usage*** In addition to the 'suggested usage' mentioned in class-1, class- 2 & class-3. Signing certificate may also be used for digital signing for discharging his/her duties as per official designation and also encryption certificate may also be used for encryption requirement as per his/her official capacity. **Assurance Level** Provides highest level of assurances, as verification process is very stringent. **Verification Process** In addition to the verification process required for the class II certificates, the subscriber's of class III certificates are required to be personally present with some proof of identity at NICCA/RA, for issuance of DSC.
AUDIT	Audit Type: WebTrust CA Equivalent Auditor: India Controller of Certifying Authorities (CCA) Auditor Website: http://cca.gov.in Audit Statement: The audit report is not publicly available but a statement from the auditor stating when the last audit was performed and that the audit included all of the criteria for WebTrust CA, can be obtained at short notice, depending upon requirement.

Yes, that would be a great help in showing that the audit meets the requirements of the Mozilla CA Policy.

Comment #14: We will submit the statement from auditor as soon as the above issues are resolved.

CPS:

2.7.1. Frequency of Entity Compliance Audit

The NICCA shall get its operations audited as per Rule 31 of the Rules under the IT Act.

2.7.2. Identity/Qualifications of Auditor

The compliance audits shall be carried out by one of the empanelled Auditors duly authorized by the CCA.

2.7.3. Topics covered by Audit

The NICCA shall be audited on the following:

- Security policy and planning
- Physical security
- Technology evaluation
- NICCA's services administration
- NICCA CPS.
- Compliance to NICCA's CPS
- Contracts/agreements
- Requirements under the IT Act, Rules, Regulations and Guidelines.

2.7.4. Auditors Relationship with NICCA

The auditor shall be independent of NICCA and shall not be software or hardware vendor or any service provider of NICCA. They shall not have any current or planned financial, legal or any other relationship, other than that of an auditor and the audited party. The auditor should be one of the empanelled auditors duly authorized by the CCA.

2.7.5. Actions taken as a Result of Deficiency

The NICCA shall take immediate and appropriate actions determined by the significant exceptions and deficiencies identified during the compliance audit, in order to rectify such deficiencies.

2.7.6. Communication of Results

A copy of the results of the compliance audit shall be submitted to the CCA's office, as required by Rule 31 of the Information Technology (Certifying Authorities) Rules, 2000.

Certificate 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 could not find any text in the CPS or DSC Request Form that explains the steps taken to verify that the certificate subscriber owns/controls the domain name to be referenced in the certificate.

    - Comment #14: The verification procedure will be specific to class-verification levels and is elaborated in the NICCA CPS ver-4.4, which is expected to be available in about a week's time.
- 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.
    - Comment #11: E-mail verification is done by the way of sending the user-id/password to the end-user to enable the submission of the Certificate Signing Request to NICCA system. This ensures that the person who has requested for the certificate, also has the control over the e-mail mentioned in the request form.
    - Comment #14: NICCA issues Certificates to the subscribers in the Government, PSUs, Statutory Bodies, and Govt. Registered Companies in India. All details filled by the applicant in the DSC Application form, inclusive of E-mail, are authenticated by the "Head of Office or JS (Admn.) for Government Sector/Superior Authority for Banking Sector of Applicant/ Company Secretary of Govt. Registered Companies, " before being formally submitted to NICCA for processing. This is given in the "Verification Process" in CPS. The procedure mentioned in Comment #11 for verification of Emails is documented and internal to NICCA and additionally ensures that the person who has requested for the certificate, also has the control over the e-mail mentioned in the request form.
- 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.

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

- Long-lived DV certificates
    - SSL certs are OV
    - CPS: Certificates issued will normally be valid for a maximum period of two years from the date of issue, but may vary from case to case at the discretion of NICCA.
- Wildcard DV SSL certificates
    - ?
- Delegation of Domain / Email validation to third parties
    - CPS section 1.4. Registration Authorities: At present NICCA functions through State/District office of NIC. Although verification of credentials of the applicants are carried out by the head of respective organizations/departments. The NICCA may also function through Registration Authorities (RAs) in each organization interested in having Digital Certificates issued to its employees. The head of office of the organization or any person authorized by the organization may function as the RA. These RAs have complete charge of the authentication and validation of each Subscriber within the organization.
- Issuing end entity certificates directly from roots
    - The NIC CA issues end-entity certificates directly, so this item is applicable if the NIC CA is included in Mozilla as a trust anchor root.
- Allowing external entities to operate unconstrained subordinate CAs

    - If sub-CAs are issued for third parties, those sub-CAs will still be operated by the NIC. Sub-CAs cannot create their own subordinates. The certificate issuing authority for the Sub-CA always remains only with NIC.
- Distributing generated private keys in PKCS#12 files
    - CPS:
        - The applicant has to submit certificate request in PKCS#10 format to NICCA for issuing web server certificate.
        - Subscribers will generate their key pair using a trustworthy method.
        - Since the time of creation of their private and public key pair, Subscribers are personally and solely responsible for the confidentiality and integrity of their private keys.
- Certificates referencing hostnames or private IP addresses
    - ?
- OCSP Responses signed by a certificate under a different root
    - Not applicable – OCSP not provide.
- CRL with critical CIDP Extension
    - CRL imported into Firefox without error.
- Generic names for CAs
    - CA names doesn't seem to be too generic.