Bugzilla ID: 476766
Bugzilla Summary: Add China Internet Network Information Center (CNNIC) 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	China Internet Network Information Center (CNNIC)
Website URL (English version)	http://www.cnnic.cn/en/index/index.htm (English Version) http://www.cnnic.cn/index.htm (Chinese Version)
Organizational type. (E.g., whether the CA is operated by a private or public corporation, government agency, academic institution or consortium, NGO, etc.)	non-profit organization CNNIC is not a Chinese Government organization. It is an organization that mainly operates Chinese top level domain name registration. CA is a new operation for CNNIC to protect Internet security.
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?)	China Internet Network Information Center (CNNIC), the state network information center of China, is a non-profit organization. CNNIC takes orders from the Ministry of Information Industry (MII) to conduct daily business, while it is administratively operated by the Chinese Academy of Sciences (CAS). The CNNIC Steering Committee, a working group composed of well-known experts and commercial representatives in domestic Internet community, supervises and evaluates the structure, operation and administration of CNNIC. The objective customers of the CNNIC root are domain owners from general public, including enterprise, government, organization, league, individual, etc. CNNIC's Main Business: 1． Operates and Administrates China's Domain Name Registry Service, ".CN" country code top level domain (ccTLD) and Chinese Domain Name (CDN) system. 2 As a National Internet Registry (NIR) of Asia-Pacific Network Information Center (APNIC), CNNIC initiated the IP Allocation Alliance, providing IP address and AS Number application services to domestic ISPs and users. 3． Responsible for setting up and maintain the state top level network catalogue database, providing information search services of Internet user, web address, domain name, AS number and so on.

	4． Carries out relevant technical researches and takes on technical projects of the state based on its administrative and working experiences on traditional network technologies. 5． Internet Survey and Relevant Information Services 6． International Liaison and Policy Research. As the national network information center (NIC), CNNIC maintains cooperative relationship with many International Internet Communities, working closely with NICs of other countries. 7． Secretariat of the Internet Policy and Resource Committee, Internet Society of China (ISC)

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

Info Needed	**Data**	**Status / Notes**
Certificate Name	CNNIC ROOT	COMPLETE
Cert summary / comments	There is one internally-operated subordinate CA named CNNIC SSL, which offers only SSL certificates. SSL certificates may be issued to general public, including enterprise, government, organization, league, individual, etc.	COMPLETE
The root CA certificate URL	http://www.cnnic.cn/uploadfiles/rar/2009/2/12/cnnicroot.rar	COMPLETE
SHA-1 fingerprint.	8b:af:4c:9b:1d:f0:2a:92:f7:da:12:8e:b9:1b:ac:f4:98:60:4b:6f	COMPLETE
Valid from	4/16/2007	COMPLETE
Valid to	4/16/2027	COMPLETE
Cert Version	3	COMPLETE
Modulus length	2048	COMPLETE
CRL URL update frequency for end-entity certificates	http://www.cnnic.cn/download/crl/CRL1.crl CPS Section 4.5.9 and 4.5.10: every 12 hours	COMPLETE
OCSP Responder URL (if applicable)	Not Applicable From CNNIC: We actually have OCSP server. But since now we only provide SSL certificates, we didn't release this to the public. CPS Section 4.5.11: “CNNIC Trusted Network Service Center provides the online inquiry service for certificate status (CSP). This service is available 7x24 hours every week except at most four (4) hours’ regular maintenance and emergency maintenance.”	COMPLETE
List or description of subordinate CAs	There is one internally-operated subordinate CA named CNNIC SSL, which offers only	COMPLETE

operated by the CA organization associated with the root CA. For internally-operated subordinate CAs the key is to confirm that their operation is addressed by the relevant CPS, and that any audit covers them as well as the root.	SSL certificates. SSL certificates may be issued to general public, including enterprise, government, organization, league, individual, etc. In the future, CNNIC plans to build other subordinate CAs to be used in other operations, like email certificate, code signing certificate, etc. The subordinate CA is included in the audit.	
For subordinate CAs operated by third parties, if any: General description of the types of third-party subordinates that exist, and what the general legal/technical arrangements are by which those subordinates are authorized, controlled, and audited.	None	COMPLETE
List any other root CAs that have issued cross-signing certificates for this root CA	None CPS Section 2.2.10: "CNNIC Trusted Network Service Center shall preserve the right to carry out certification with other Certificate by defining and determining proper reasons."	COMPLETE
Requested Trust Bits One or more of: Websites (SSL/TLS) Email (S/MIME) Code (Code Signing)	Websites (SSL/TLS)	COMPLETE
If SSL certificates are issued within the hierarchy rooted at this root CA certificate: Whether or not the domain name referenced in the certificate is verified to be owned/controlled by the certificate subscriber. (This is commonly referred to as a DV certificate.) Whether or not the value of the Organization attribute is verified to be that associated with the certificate subscriber in addition to verifying the	OV CPS Section 3.2 Requires proof of identification of the certificate applicant or organization representative. Enterprises, government organizations, institutions, etc. must provide the organization code certificate or legal person business license (each page affixed with an official seal). CPS Section 4.1.1.1: "The handlers for applying for domain name certificates must go to a Local Registration Authority of CNNIC Trusted Network Service Center designated by the CNNIC to submit applications."	COMPLETE

domain name. (This is commonly referred to as an OV certificate.) Whether verification of the certificate subscriber conforms to the Extended Validation Certificate Guidelines issued by the CAB Forum. (This is commonly referred to as an EV certificate.)		
If EV certificates are issued within the hierarchy rooted at this root, the EV policy OID(s) associated with those EV certificates.	Not EV	COMPLETE
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.	https://www.enum.cn/	COMPLETE
CP/CPS Certificate Policy URL Certificate Practice Statement(s) (CPS) URL (English or available in English translation)	Policies of the CNNIC Trusted Network Service Center http://www.cnnic.cn/html/Dir/2007/04/29/4568.htm English CPS of the CNNIC Trusted Network Service Center http://www.cnnic.cn/uploadfiles/pdf/2008/11/18/142721en.pdf	COMPLETE
AUDIT: The published document(s) relating to independent audit(s) of the root CA and any CAs within the hierarchy rooted at the root.	Audit Type: WebTrust CA Auditor Website URL: http://www.ey.com/global/content.nsf/China_E/home Audit Report: http://cert.webtrust.org/ViewSeal?id=805	COMPLETE 8/8/2008

Review CPS sections dealing with subscriber verification (COMPLETE)
(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.
  - CPS Section 3.2:
    - The inputer at the Local Registration Authority carries out preliminary examination. Through the domain name registration information inquiry (whois), the inputer gets the information of the domain name registrar of the domain name certificate application, checks whether the domain name registrar is consistent with the domain name certificate applicant, and determines whether the domain name certificate applicant indeed has this domain name through preliminary examination.
    - The RA auditor checks whether the legal domain name subscriber is consistent with the certificate applicant (also using the whois function), and whether the information is true, and compares it with the application information in the RA system. The RA auditor confirms the information with the director and the handler respectively through telephone.
- 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.
  - Not Applicable
- Verify identity info in code signing certs is that of subscriber
  - Not Applicable
- Make sure it's clear which checks are done for which context (cert usage)

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

- Long-lived DV certificates
  - CPS Section 6.3.3: The usage period of the domain name certificates of CNNIC Trusted Network Service Center is one (1) year.
- Wildcard DV SSL certificates
  - CPS Section 1.3.4: Wildcard domain certificate: CN is a domain name whose format is *.xxx.xxx.
  - Comment #5: Wildcard SSL Certificates indeed have some weakness, so we only issue this type certificate to appliers whose identities have been validated with organizational validation. In addition, the subscribers of this type have to sign a contract to promise that their sub-domains are really belonging to them. This will be update in CPS in March 2009.
- Delegation of Domain / Email validation to third parties
  - Local Registration Authorities are used.
- Issuing end entity certificates directly from roots
  - Not applicable.
- Allowing external entities to operate unconstrained subordinate CAs
  - Not applicable.
- Distributing generated private keys in PKCS#12 files

    - CPS Section 3.3: CNNIC Trusted Network Service Center verifies that a certificate applicant has a private key corresponding to the certificate public key by using the certificate request in PKCS#10 attached with a digital signature.
- Certificates referencing hostnames or private IP addresses
    - Comment #5: For single domain and wildcard domain certificates, the name is hostnames, not IP addresses. For Multi-domain Certificates, the name is composed by each domain name and the serial number designated by CNNIC, also not IP addresses.
    - CPS Section 3.1.1: the entity names of the certificates issued by CNNIC Trusted Network Service Center may be domain names or the serial numbers designated by CNNIC Trusted Network Service Center. Naming meets the X.500 regulations on distinguished names.
    - CPS Section 3.1.2: The names included in the certificates issued by CNNIC Trusted Network Service Center shall be composed of the domain names or the serial number automatically generated by CNNIC Trusted Network Service Center…
- OCSP Responses signed by a certificate under a different root
    - Not applicable
- CRL with critical CIDP Extension
    - CRL downloaded successfully into Firefox.

Verify Audits (COMPLETE)
(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.
    - Posted on cert.webtrust.org
- For EV CA's, verify current WebTrust EV Audit done.
    - Not EV
- Review Audit to flag any issues noted in the report
    - No issues noted in report.