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	http://www.cnnic.cn/en/index/index.htm
Organizational type	Non-profit organization. CNNIC is not a Chinese Government organization. It is an organization that mainly operates Chinese top level domain name registration.
Primary market / customer base	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)
CA Contact Information	CA Email Alias: service@cnnic.cn CA Phone Number: 86-10-58813000 Title/Department: Trusted Network Service Center

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

Info Needed	**Data**
Certificate Name	CNNIC ROOT
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.
Root CA cert URL	http://www.cnnic.cn/uploadfiles/rar/2009/2/12/cnnicroot.rar
SHA-1 fingerprint.	8b:af:4c:9b:1d:f0:2a:92:f7:da:12:8e:b9:1b:ac:f4:98:60:4b:6f
Valid from	4/16/2007
Valid to	4/16/2027
Cert Version	3
Modulus length	2048
Test Website	https://www.enum.cn/
CRL URL	http://www.cnnic.cn/download/crl/CRL1.crl Next Update: 12 hours CPS Section 4.5.9 and 4.5.10: every 12 hours
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.
List or description of subordinate CAs operated by the CA organization	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. In the future, CNNIC plans to build other subordinate CAs to be used in other operations, like email certificate, code signing certificate, etc.
Sub CAs operated by third parties	None
cross-signing	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."
Requested Trust Bits	Websites (SSL/TLS)
If SSL: DV, OV, and/or EV	OV
EV policy OID(s)	Not EV
CP/CPS	Policies of the CNNIC Trusted Network Service Center: http://www.cnnic.cn/html/Dir/2007/04/29/4568.htm CPS translated into English: http://www.cnnic.cn/uploadfiles/pdf/2009/7/3/163452.pdf
AUDIT	Audit Type: WebTrust CA Auditor: Ernst & Young Auditor Website URL: http://www.ey.com/global/content.nsf/China_E/home Audit Report: https://cert.webtrust.org/ViewSeal?id=935 (2009.05.31)

Organization Identity Verification	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." CPS Section 4.1.1.2: "Documents used to prove the certificate subscriber organizations, handlers (subscribers) and identity of handlers are explained in Section 3.2 of this CPS, and applicants shall carry out application operations according to Section 3.2 of this CPS. After the Registration Authority of CNNIC Trusted Network Service Center completed the procedure of verifying identity, it emails the first thirteen numbers of the reference number and authorization code to handler and sends the last three number of these two code through cellphone. And make a paper 'certificate on approval for CNNIC SSL Certificates' via a safe mailing method to the certificate application handler." CPS Section 4.1.2.1: "The steps for issuing and accepting single domain and wildcard domain certificates are as follows: The certificate application handler generates a certificate request CSR in the Web server. The certificate application handler accesses the CNNIC certificate download page, submits the CSR and puts in the reference number and the authorization code. CNNIC Trusted Network Service Center system automatically checks the completeness of the CSR. CNNIC Trusted Network Service Center issues a certificate and the certificate application handler downloads it and then installs it."
Domain Name Ownership / Control	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.
Email Address Control	Not Applicable – Not requesting Email trust bit.
Code Signing	Not Applicable – Not requesting Email trust bit.
Potentially Problematic Practices	http://wiki.mozilla.org/CA:Problematic_Practices • Long-lived DV certificates o 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 o Wildcard SSL certs are OV (See CPS Section 3.2.2) o 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. • Delegation of Domain / Email validation to third parties o Local Registration Authorities are used for input of data and preliminary examination. The RA auditor at the CNNIC Registration Authority verifies the data and re-checks domain name ownership. • Issuing end entity certificates directly from roots o No. The root only signs sub-CAs. The sub-CA issues the end-entity certs. • Allowing external entities to operate unconstrained subordinate CAs o No. Only one sub-CA exists, and it is internally operated. • Distributing generated private keys in PKCS#12 files o 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 o 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. o 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. • OCSP Responses signed by a certificate under a different root o OCSP not currently provided. • CRL with critical CIDP Extension o CRL downloaded without error into Firefox browser. • Generic names for CAs o Root name is not generic.