Bugzilla ID: 607208
Bugzilla Summary: Add CNNIC EV 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	China Internet Network Information Center (CNNIC)
Website URL	http://www.cnnic.cn/en/index/index.htm (English Version) http://www.cnnic.cn/index.htm (Chinese Version)
Organizational type	CNNIC is a non-profit organization, which is administrated by Computer Network Information Center of Chinese Academy of Sciences.
Primary market / customer base	The objective customers are domain owners from general public, including enterprise, government, organization, league, individual, etc. 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	China Internet Network Information Center EV Certificates Root
Cert summary / comments	
Root Cert URL	https://bugzilla.mozilla.org/attachment.cgi?id=486481 http://www.cnnic.cn/download/cert/CNNICEVROOT.cer
SHA-1 fingerprint	4F:99:AA:93:FB:2B:D1:37:26:A1:99:4A:CE:7F:F0:05:F2:93:5D:1E
Valid from	2010-08-31
Valid to	2030-08-31
Cert Version	3
Modulus length	2048
Test Website	https://evdemo.cnnic.cn/
CRL URL	End-entity: http://www.cnnic.cn/download/evcrl/crl1.crl (NextUpdate: 12 hours) CPS Section 4.5.9 and 4.5.10: CRL of intermediate root every 12 hours
OCSP Responder URL	http://ocspev.cnnic.cn EV CPS Section 2.13.1, Max expiration time of OCSP response: every 12 hours
CA Hierarchy	Currently there is one internally-operated subordinate CA named CNNIC EV SSL, which offers only EV Certificates. CNNIC EV SSL Cert: http://www.cnnic.cn/download/cert/CNNICEVSSL.cer From CNNIC: The extent and nature of subordinate CAs 1) We offer all kinds of domains from general public, including enterprise, government, organization, league, individual, etc. 2) Whether or not subordinate CAs can create their own subordinates I'm not sure what this means. Do you plan to have other subCAs under this root in the future? If yes, please describe the subCAs that will eventually chainup to this root.
Externally operated subCAs	Currently none. Do you plan to have any externally-operated subCAs under this root in the future? If yes, please describe.
Cross-Signing	Currently none. Any planned for this root?
Requested Trust Bits	Websites (SSL/TLS)
SSL Validation Type	DV, OV, and/or EV Will only EV certs be issued under this root? Or do you also plan to issue non-EV certs under this root?

EV policy OID(s)	1.3.6.1.4.1.29836.1.10
CP/CPS	CNNIC Trusted Network Service Center: http://tns.cnnic.cn CNNIC Policy Documents: http://www.cnnic.cn/html/Dir/2007/04/29/4568.htm CNNIC Trusted Network Service Center EV CPS (English): http://www.cnnic.cn/uploadfiles/pdf/2010/9/10/141005.pdf CNNIC Trusted Network Service Center CPS (English): http://www.cnnic.cn/uploadfiles/20100414/CNNIC_CPS_V2_07_EN.pdf
AUDIT	Audit Type: WebTrust CA Auditor: Ernst & Young Auditor Website URL: http://www.ey.com/global/content.nsf/China_E/home Audit Report and Management's Assertions: https://cert.webtrust.org/ViewSeal?id=1071 (2010.05.31) Next WebTrust CA audit will include this root and it's sub-CAs. Correct? Audit Type: WebTrust EV Auditor: Ernst & Young Auditor Website URL: http://www.ey.com/global/content.nsf/China_E/home Audit Report and Management's Assertions: https://cert.webtrust.org/ViewSeal?id=1079 (2010.09.08) From CNNIC: The extent and nature of audits performed against subordinate CAs 1) subordinate CAs are included within the audit 2) subordinate CAs are subject to third-party audit 3) once a year
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." EV CPS Section 4.6.1: Verification of legal existence and identity of applicant EV CPS Section 4.6.3: Verification on physical operation address and contact telephone EV CPS Section 4.6.4: Verification on existence of applicant operation EV CPS Section 4.6.6: Verification on name, title, and authority of manager and operator
Domain Name Ownership / Control	As per sections 3.2 and 4.1 of the CPS, the Local Registration Authority performs a domain name registration information inquiry (whois), 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 owns this domain name. Then 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. EV CPS Section 4.1.1: Single domain name EV certificate LRA does preliminary verification by obtaining via whois the domain name register material and comparing the information with that of the application. Then the RA at CNNIC also checks the application information by comparing it to information from whois. Then the RA reviewer sends an email to the certificate applicant with the first 13 bits of the reference number (from the RA system) and the RA reviewer will also call the certificate applicant on the phone to provide the last 13 bits of the reference number. The certificate applicant must be able to provide the full reference number or application is rejected. EV CPS Section 4.1.2: Multiple domain name EV Certificate EV CPS Section 4.6.5: Verification on domain names of applicant
Email Address Ownership / Control	Not applicable. Not requesting email trust bit.
Identity of Code Signing Subscriber	Not applicable. Not requesting code signing trust bit.

Potentially Problematic Practices	http://wiki.mozilla.org/CA:Problematic_Practices
	• 1.1 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.
	• 1.2 Wildcard DV SSL certificates
	  ○ Wildcard SSL certs are OV (See CPS Section 3.2.2)

	• 1.3 Email Address Prefixes for DV Certs
	  ○ Not applicable. SSL certs are either OV or EV. Correct?
	• 1.4 Delegation of Domain / Email validation to third parties
	  ○ CPS Section 2.1.2 and 3.2.2: 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.
	• 1.5 Issuing end entity certificates directly from roots
	  ○ No. The root only signs sub-CAs. The sub-CA issues the end-entity certs.
	• 1.6 Allowing external entities to operate subordinate CAs
	  ○ Is there provision for having externally-operated subCAs in the future?
	• 1.7 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."
	• 1.8 Certificates referencing hostnames or private 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.
	• 1.9 Issuing SSL Certificates for Internal Domains
	  ○ ?
	• 1.10 OCSP Responses signed by a certificate under a different root
	  ○ Test website has OCSP URI in the AIA, and the page loads into the Firefox browser with OCSP enforced.
	• 1.11 CRL with critical CIDP Extension
	  ○ CRL downloaded without error into Firefox browser.
	• 1.12 Generic names for CAs
	  ○ CN has "China Internet Network Information Center" in it.