Print this page

Mozilla - CA Program

Case Information

Case Number	00000087	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	China Internet Network Information Center (CNNIC)	**Request Status**	Initial Request Received

Additional Case Information

Subject	CNNIC ROOT	**Case Reason**	New Owner/Root inclusion requested

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org/show_bug.cgi?id=1312957

General information about CA's associated organization

CA Email Alias 1	anyin@cnnic.cn		
CA Email Alias 2			
Company Website	http://www.cnnic.cn	**Verified?**	Verified
Organizational Type	Government Agency	**Verified?**	Verified
Organizational Type (Others)	N/A	**Verified?**	Not Applicable
Geographic Focus	China	**Verified?**	Verified
Primary Market / Customer Base		**Verified?**	Need Response From CA
Impact to Mozilla Users		**Verified?**	Need Response From CA

Response to Mozilla's list of Recommended Practices

Recommended Practices	https://wiki.mozilla.org/CA:Recommended_Practices#CA_Recommended_Practices	**Recommended Practices Statement**	I have reviewed Mozilla's list of Recommended Practices, and confirm that we follow those practices, with exceptions and clarifications noted in the text box below.
CA's Response to Recommended Practices	1. NEED CA's response to each of the items listed in https://wiki.mozilla.org/CA:Recommended_Practices#CA_Recommended_Practices 1) Publicly Available CP and CPS: CPS: http://www.cnnic.cn/jczyfw/fwqzs/CNNICfwqzsywgz/201206/W020161026393737627803.pdf CP: http://cnnic.cn/jczyfw/fwqzs/CNNICfwqzsywgz/201206/W020160421527397195222.pdf CA only have English version for CPS. 2) CA Hierarchy: in CPS section 1.3.1 3) Audit Criteria: in CPS section 8 4) Document Handling of IDNs in CP/CPS: CAdoesn't have specific process for IDNs in CP/CPS. So far, the only IDNs CNNIC issue certificate is .中国（.China) and the cert is for domain CNNIC owns. 5) Revocation of Compromised Certificates: in CPS section 4.8.1 6) Verifying Domain Name Ownership: in CPS section 3.2.2 7) Verifying Email Address Control: in CPS section 3.1.1	**Verified?**	Need Response From CA

8) Verifying Identity of Code Signing Certificate Subscriber: in CPS section 3.1.1
9) DNS names go in SAN: in CPS section 3.1.1
10) Domain owned by a Natural Person: in CPS section 3.2.3 and section 4.2.1
11) OCSP: in CPS section 7.3
12) Network Security Controls: in CPS section 6.7, we also perform the Network security refer to internal documents <CNNIC CA security management policy and regulations> which will be check in WebTrust annual audit. Since it's have Chinese version only, we can provide an English version which include major network security control.

Response to Mozilla's list of Potentially Problematic Practices

Potentially Problematic Practices	https://wiki.mozilla.org/CA:Problematic_Practices#Potentially_problematic_CA_practices	**Problematic Practices Statement**	I have reviewed Mozilla's list of Potentially Problematic Practices, and confirm that we do not do those practices, with exceptions and clarifications noted in the text box below.
CA's Response to Problematic Practices	2. NEED CA's response to each of the items listed in https://wiki.mozilla.org/CA:Problematic_Practices#Potentially_problematic_CA_practices 1) Long-lived DV certificates: None 2) Wildcard DV SSL certificates: None 3) Email Address Prefixes for DV Certs: None 4) Delegation of Domain / Email validation to third parties: None 5) Issuing end entity certificates directly from roots: None 6) Allowing external entities to operate subordinate CAs: None 7) Distributing generated private keys in PKCS#12 files: None 8) Certificates referencing hostnames or private IP addresses: None 9) Issuing SSL Certificates for Internal Domains: None 10) OCSP Responses signed by a certificate under a different root: None 11) SHA-1 Certificates: Stopped issue SHA-1 certificates from September 28th, 2016. 12) Generic names for CAs: None 13) Lack of Communication With End Users: None 14) Backdating the notBefore date: None	**Verified?**	Need Clarification From CA

Root Case Record # 1

Root Case Information

Root Certificate Name	CNNIC ROOT	**Root Case No**	R00000129
Request Status	Initial Request Received	**Case Number**	00000087

Certificate Data

Certificate Issuer Common Name	CNNIC ROOT
O From Issuer Field	CNNIC
OU From Issuer Field	
Valid From	2007 Apr 16
Valid To	2027 Apr 16
Certificate Serial Number	49330001
Subject	CN=CNNIC ROOT, OU=null, O=CNNIC, C=CN
Signature Hash Algorithm	sha1WithRSAEncryption
Public Key Algorithm	RSA 2048 bits
SHA-1 Fingerprint	8B:AF:4C:9B:1D:F0:2A:92:F7:DA:12:8E:B9:1B:AC:F4:98:60:4B:6F
SHA-256 Fingerprint	E2:83:93:77:3D:A8:45:A6:79:F2:08:0C:C7:FB:44:A3:B7:A1:C3:79:2C:B7:EB:77:29:FD:CB:6A:8D:99:AE:A7

Certificate Fingerprint	6C:6D:AE:76:36:8E:4B:FF:D1:32:EF:02:32:75:C7:E8:6A:64:BA:D3:BB:69:D8:ED:4E:A0:1F:46:CC:71:6F:D6
Certificate Version	3

Technical Information about Root Certificate

Certificate Summary	CNNIC ROOT is used for OV and DV SSL certificate issuance. Now only CNNIC SHA256 SSL is used to issue SSL is used to issue SHA256 OV SSL for entity customer.	**Verified?**	Verified
Root Certificate Download URL	http://www.cnnic.cn/download/cert/CNNICROOT.cer	**Verified?**	Verified
CRL URL(s)	http://crl.cnnic.cn/download/rootsha2crl/CRL1.crl	**Verified?**	Verified
OCSP URL(s)	http://ocspcnnicroot.cnnic.cn http://ocspsha2ssl.cnnic.cn/	**Verified?**	Verified
Trust Bits	Websites	**Verified?**	Verified
SSL Validation Type	DV; OV	**Verified?**	Verified
EV Policy OID(s)	NA	**Verified?**	Not Applicable
Root Stores Included In	Microsoft	**Verified?**	Verified
Mozilla Applied Constraints	NEED: Mozilla has the ability to name constrain root certs; e.g. to *.gov or *.mil. CAs should consider if such constraints may be applied to their root certs. https://dxr.mozilla.org/mozilla-central/source/security/nss/lib/certdb/genname.c#1551	**Verified?**	Need Response From CA

Test Websites or Example Cert

Test Website URL (SSL) or Example Cert	NEED: - If requesting Websites trust bit: URL to a website whose SSL cert chains up to this root. Note that this can be a test site. - If requesting Email trust bit: attach an example cert to the bug.	**Verified?**	Need Response From CA
Test Website - Expired			
Test Website - Revoked			

Test Results (When Requesting the SSL/TLS Trust Bit)

Revocation Tested	No Errors	**Verified?**	Verified
CA/Browser Forum Lint Test	ERROR: CA certificates must set keyUsage extension as critical ERROR: Unallowed key usage for RSA public key	**Verified?**	Need Response From CA
Test Website Lint Test	Test not currently available	**Verified?**	Not Applicable
EV Tested	No EV request	**Verified?**	Not Applicable

CA Hierarchy Information

CA Hierarchy	NEED: A description of the PKI hierarchy rooted at or otherwise associated with this root CA certificate. - List and/or describe all of the subordinate CAs that are signed by this root. - Identify which of the subordinate CAs are internally-operated; e.g. list the subordinate CAs that operated by the CA organization associated with the root CA. For example, this might include subordinate CAs created to issue different classes or types of end entity certificates to the general public: Class 1 vs. class 2 certificates, qualified vs. non-qualified certificates, EV certificates vs. non-EV certificates, SSL certificates vs. email certificates, and so on. - It might also include subordinate CAs operated for the benefit of specific third parties. In this case note that we do not require that the CA submit a	**Verified?**	Need Response From CA

	complete customer list; rather we are interested in the general type and nature of the third-party arrangements		
Externally Operated SubCAs	NEED: - If this root has any subordinate CA certificates that are operated by external third parties, then provide the information listed in the Subordinate CA Checklist,https://wiki.mozilla.org/CA:SubordinateCA_checklist - If the CA functions as a super CA such their CA policies and auditing don't apply to the subordinate CAs, then those CAs must apply for inclusion themselves as separate trust anchors.	**Verified?**	Need Response From CA
Cross Signing	NEED: - List all other root certificates for which this root certificate has issued cross-signing certificates. - List all other root certificates that have issued cross-signing certificates for this root certificate. - If any such cross-signing relationships exist, it is important to note whether the cross-signing CAs' certificates are already included in the Mozilla root store or not.	**Verified?**	Need Response From CA
Technical Constraint on 3rd party Issuer	NEED: CP/CPS documentation describing the technical and contractual controls over any 3rd party who may issue certs in this CA Hierarchy. This includes external RAs as well as External subCAs. References: - section 7.1.5 of version 1.3 of the CA/Browser Forum's Baseline Requirements - https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/inclusion/ - https://wiki.mozilla.org/CA:CertificatePolicyV2.1#Frequently_Asked_Questions	**Verified?**	Need Response From CA

Verification Policies and Practices

Policy Documentation	NEED: Languages that the CP/CPS and other documents are provided in.	**Verified?**	Need Response From CA
CA Document Repository		**Verified?**	Need Response From CA
CP Doc Language	Chinese		
CP	http://cnnic.cn/jczyfw/fwqzs/CNNICfwqzsywgz/201206/W020160421527397195222.pdf	**Verified?**	Verified
CP Doc Language	Chinese		
CPS	http://www.cnnic.cn/jczyfw/fwqzs/CNNICfwqzsywgz/201206/W020161026393737627803.pdf	**Verified?**	Verified
Other Relevant Documents	No	**Verified?**	Not Applicable
Auditor Name	E&Y	**Verified?**	Verified
Auditor Website	:http://www.ey.com/	**Verified?**	Verified
Auditor Qualifications		**Verified?**	Verified
Standard Audit	NEED: for all root inclusion/change requests. Reference section 2 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date		**Verified?**	Need Response From CA
BR Audit	NEED: If requesting Websites trust bit, then also need a BR audit as described here: https://wiki.mozilla.org/CA:BaselineRequirements	**Verified?**	Need Response From CA
BR Audit Type		**Verified?**	Need Response From CA
BR Audit Statement Date		**Verified?**	Need Response From CA

EV Audit	NEED only if requesting EV treatment	**Verified?**	Not Applicable
EV Audit Type		**Verified?**	Not Applicable
EV Audit Statement Date		**Verified?**	Not Applicable
BR Commitment to Comply	NEED section in the CP/CPS that has the commitment to comply with the BRs as described in section 2.2 of version 1.3 of the CA/Browser Forum's Baseline Requirements.	**Verified?**	Need Response From CA
SSL Verification Procedures	NEED: if Websites trust bit requested... Sections of CP/CPS that sufficiently describe the verification steps that are taken to confirm the ownership/control of the domain name to be included in the SSL/TLS cert. As per section 3 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices https://wiki.mozilla.org/CA:BaselineRequirements#CA_Conformance_to_the_BRs It is not sufficient to simply reference the section of the CA/Browser Forum's Baseline Requirements (BR) that lists the ways in which the CA may confirm that the certificate subscriber owns/controls the domain name to be included in the certificate. The CA's CP/CPS must specify which of those options the CA uses, and must include a reasonable description of the ways the CA can verify that the certificate subscriber owns/controls the domain name(s) to be included in the certificate. https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Domain_Name_Ownership	**Verified?**	Need Response From CA
EV SSL Verification Procedures	No EV request	**Verified?**	Not Applicable
Organization Verification Procedures	NEED: CP/CPS sections that describe identity and organization verification procedures for cert issuance.	**Verified?**	Need Response From CA
Email Address Verification Procedures	NEED if Email trust bit requested... Sections of CP/CPS that sufficiently describe the verification steps that are taken to confirm the ownership/control of the email address to be included in the cert. As per section 4 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Email_Address_Control	**Verified?**	Need Response From CA
Code Signing Subscriber Verification Pro	Mozilla is no longer accepting requests to enable the Code Signing trust bit.	**Verified?**	Not Applicable
Multi-Factor Authentication	NEED CA response (and corresponding CP/CPS sections/text) to section 6 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA
Network Security	NEED CA response (and corresponding CP/CPS sections/text) to section 7 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	NEED URL to publicly disclosed subordinate CA certificates that chain up to certificates in Mozilla's CA program, as per Items #8, 9, and 10 of Mozilla's CA Certificate Inclusion Policy.	**Verified?**	Need Response From CA