Bugzilla ID: 926029
Bugzilla Summary: CFCA (China Financial Certification Authority) root CA

CAs wishing to have their certificates included in Mozilla products must

1) Comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/)
2) Supply all of the information listed in http://wiki.mozilla.org/CA:Information_checklist.
    a. Review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices
    b. Review the Potentially Problematic Practices at https://wiki.mozilla.org/CA:Problematic_Practices

General information about the CA's associated organization

CA Company Name	China Financial Certification Authority (CFCA)
Website URL	http://www.cfca.com.cn/
Organizational type	Established on June 29, 2000, China Financial Certification Authority (CFCA) is a national authority of security authentication approved by the People's Bank of China and state information security administration. CFCA is a critical national infrastructure of financial information security and one of the first certification service suppliers granted a certification service license after the release of the Electronic Signature Law of the People's Republic of China.
Primark Market / Customer Base	SSL Certificates can be used in the areas such as online banking, e-commence, e-politic, enterprise informatization and public services and so on. Does the CA focus its activities on a particular country or other geographic region?
Impact to Mozilla Users	Why does this CA need to have their root certificate directly included in Mozilla's products, rather than being signed by another CA's root certificate that is already included in NSS?
Inclusion in other major browsers	Does this CA have root certificates included in any other major browsers? If yes, which? If no, why not?
CA Contact Information	CA Email Alias: CA Phone Number: Title / Department: An official representative of the CA must submit and/or participate in the root inclusion request. According to Mozilla's CA Certificate Inclusion Policy: "To request that its certificate(s) be added to the default set a CA should submit a formal request by submitting a bug report into the mozilla.org Bugzilla system ... **The request must be made by an authorized representative of the subject CA**..." If the CA contracts to another organization to help with the root inclusion request, the official representative of the CA must clarify that relationship in the bug, and must provide clear information about who the ongoing points-of-contact will be for the CA.

Technical information about each root certificate

Certificate Name	CFCA GT CA
Certificate Issuer Field	CN = CFCA GT CA O = China Financial Certification Authority C = CN
Certificate Summary	
Root Cert URL	https://bugzilla.mozilla.org/attachment.cgi?id=816416
SHA1 Fingerprint	A8:F2:DF:E3:6A:E0:CC:2D:B9:DD:38:34:7D:30:AE:D9:55:1D:D2:5A
Valid From	2012-08-21
Valid To	2042-08-21
Certificate Version	3
Certificate Signature Algorithm	SHA-256
Signing key parameters	2048
Test Website URL	Please provide a URL to a website (may be a test website) whose SSL cert chains up to this root.
CRL URL	URL CPS section 4.8.7: CRL information issued by OCA2 and EV OCA will be updated within 24 hours; while that by OCA21 within three hours.
OCSP URL (Required now)	OCSP URI in the AIA of end-entity certs Maximum expiration time of OCSP responses Baseline Requirement #13.2.2: "The CA SHALL update information provided via an Online Certificate Status Protocol..." BR Appendix B regarding authorityInformationAccess in Subordinate CA Certificate and Subscriber Certificate: "With the exception of stapling .... this extension MUST be present ... and it MUST contain the HTTP URL of the Issuing CA's OCSP responder"
Requested Trust Bits	One or more of: Websites (SSL/TLS) Email (S/MIME) Code Signing
SSL Validation Type	e.g. DV, OV, and/or EV CPS section 2.4: CFCA maintains the internal database that includes previously revoked certificates (including EV Certificates) and previously rejected certificate requests, due to suspected phishing or other fraudulent usage. This information is used to flag new EV Certificate Requests of the corresponding applicants as of significant risks.
EV Policy OID(s)	If requesting EV: https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version It looks like there is a separate root for EV. Do you want to have that EV root be part of this inclusion request?
Non-sequential serial numbers and entropy in cert	http://www.mozilla.org/projects/security/certs/policy/MaintenancePolicy.html "9. We expect CAs to maintain current best practices to prevent algorithm attacks against certificates. As such, the following steps will be taken: ... - all new end-entity certificates must contain at least 20 bits of unpredictable random data (preferably in the serial number)."

	The purpose of adding entropy is to help defeat a prefix-chosen collision for non collision resistant hash functions. Using SHA256 without entropy isn't a problem in a near future. However, the Mozilla Policy doesn't say that; the entropy is mandatory for all new certificates, the used hash function isn't taken into consideration. This isn't a blocker for an inclusion request if SHA1 is forbidden in the CA hierarchy. However, the CP/CPS must clearly state that SHA1 isn't an acceptable hash algorithm for certificates in this hierarchy.

CA Hierarchy information for each root certificate

CA Hierarchy	CFCA GT CA has two internally-operated subordinate CAs: - CFCA OCA2 – issues SSL, Code Signing, Email, VPN, and Device certificates. - CFCA GT OCA21 – issues pre-generated certificates, individual certificates, organization certificates
Externally Operated SubCAs	If this root has subCAs that are operated by external third parties, then provide the information listed here: 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.
Cross-Signing	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.
Technical Constraints on Third-party Issuers	Describe the technical constraints that are in place for all third-parties (CAs and RAs) who can directly cause the issuance of certificates. See #4 of https://wiki.mozilla.org/CA:Information_checklist#CA_Hierarchy_information_for_each_root_certificate

Verification Policies and Practices

Policy Documentation	CFCA Document repository: Please provide URL to where the policy documentationg is online. CPS (English): https://bugzilla.mozilla.org/attachment.cgi?id=816212
Audit	Audit Type: WebTrust for CA Auditor: PricewaterhouseCoopers Audit Report: https://cert.webtrust.org/SealFile?seal=1388&file=pdf (2012.11.02)
Baseline Requirements (SSL)	The document(s) and section number(s) where the "Commitment to Comply" with the CA/Browser Forum Baseline Requirements may be found, as per BR #8.3. Audits performed after January 2013 need to include verification of compliance with the CA/Browser Forum Baseline Requirements if SSL certificates may be issued within the CA hierarchy, and the audit statement shall indicate the results.
Organization Verification Procedures	CPS sections 3.2.2.1, 3.2.2.2, 3.2.2.3, and 3.2.2.4
SSL Verification Procedures	CPS section 3.2.2.3: Applications for SSL Certificates can only be submitted to CFCA, who accepts applications from both organizations and individuals. CFCA verifies not only the ID of the applicant, but also the IP and the compliance of CSR. The procedures are as follow:

	CFCA performs a WHOIS inquiry on the internet for the domain name supplied by the applicant, to verify that the applicant is the entity to whom the domain name is registered. Where the WHOIS record indicates otherwise, CFCA will ask for a letter of authorization, or email to the register to inquiry whether the applicant has been authorized to use the domain name. To verify the public IP, the subscriber can supply a sealed paper document or email from the ISP showing that the IP is allocated by the ISP to the applicant. CPS section 3.2.2.4: Applications for EV SSL Certificates can only be submitted to CFCA. The subject must be the domain name of the web server, not the IP address. The domain name must not contain wildcards. The applicants can only be private organizations, business entities, government entities and non-commercial entities and should meet the following requirements: ...
Email Address Verification Procedures	If you are requesting to enable the Email Trust Bit, then provide (In English and in publicly available documentation) all the information requested in #4 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices
Code Signing Subscriber Verification Procedures	CPS section 3.2.4: When a person applies for a certificate on behalf of the organization subscriber, enough proofs should be obtained to verify that the person is authorized. CFCA is obliged to verify that authorization, and store the authorization information.
Multi-factor Authentication	Confirm that multi-factor authentication is required for all accounts capable of directly causing certificate issuance. See # 6 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices
Network Security	Confirm that you have performed the actions listed in #7 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices CPS sections 5 and 6

Response to Mozilla's CA Recommended Practices (https://wiki.mozilla.org/CA:Recommended_Practices)

Publicly Available CP and CPS	See above
CA Hierarchy	See above
Audit Criteria	See above
Document Handling of IDNs in CP/CPS	???
Revocation of Compromised Certificates	CPS section 4.8.1
Verifying Domain Name Ownership	See above
Verifying Email Address Control	See above
Verifying Identity of Code Signing Certificate Subscriber	See above
DNS names go in SAN	???
Domain owned by a Natural Person	???
OCSP	???

Response to Mozilla's list of Potentially Problematic Practices (https://wiki.mozilla.org/CA:Problematic_Practices)

Long-lived DV certificates	???
Wildcard DV SSL certificates	???
Email Address Prefixes for DV Certs	If DV SSL certs, then list the acceptable email addresses that are used for verification.
Delegation of Domain / Email validation to third parties	CPS section 1.3.2: The RA function of the OCA2 and EV OCA system under the CFCA Global Trust System is performed by CFCA internally. The RA function of the OCA21 can be delegated to other organizations according to relevant norms.
Issuing end entity certificates directly from roots	No. See above.
Allowing external entities to operate subordinate CAs	???
Distributing generated private keys in PKCS#12 files	???
Certificates referencing hostnames or private IP addresses	Yes. CPS section 3.1.2: For SSL Certificate, the CN can be the domain name or external IP owned by the subscriber. It's identified and verified with the other information of the subscriber. Please see https://wiki.mozilla.org/CA:Communications#July_30.2C_2013
Issuing SSL Certificates for Internal Domains	See above
OCSP Responses signed by a certificate under a different root	???
CRL with critical CIDP Extension	???
Generic names for CAs	No. See above
Lack of Communication With End Users	