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. CFCA's customers are throughout People's Republic of China, and it's in the leading position in Chinese CA industry for years in terms of business size, security and technology. There are more than 200 Chinese banks that are using CFCA's certificates to ensure the security of online banking trade.
Impact to Mozilla Users	CFCA is the top one of China's CAs, certificates issued by CFCA has accumulated over 50,000,000 for now, which accounts for more than 50% of the total amount of certificates issued in China. Certificate users of which using firefox requires CFCA's root certificate to be included in Mozilla's products.
Inclusion in other major browsers	Internet Explorer http://social.technet.microsoft.com/wiki/contents/articles/14945.windows-and-windows-phone-8-ssl-root-certificate-program-december-2012.aspx http://social.technet.microsoft.com/wiki/contents/articles/19217.windows-and-windows-phone-8-ssl-root-certificate-program-may-2013.aspx
CA Contact Information	CA Email Alias: gxzhao@cfca.com.cn CA Phone Number: 8610-83528031 Title / Department: Risk management supervisor/ Business management department

Technical information about each root certificate

Certificate Name	CFCA GT CA	CFCA EV ROOT
Certificate Issuer Field	CN = CFCA GT CA O = China Financial Certification Authority C = CN	CN = CFCA EV ROOT O = China Financial Certification Authority C = CN

Certificate Summary	This root certificate has signed internally-operated intermediate certificates that issue individual certificates, organization certificates, web server certificates and code signing certificates.	This root certificate has one internally-operated intermediate certificate that issues EV certificates.
Root Cert URL	https://bugzilla.mozilla.org/attachment.cgi?id=816416	https://bugzilla.mozilla.org/attachment.cgi?id=8356494
SHA1 Fingerprint	A8:F2:DF:E3:6A:E0:CC:2D:B9:DD:38:34:7D:30:AE:D9:55:1D:D2:5A	E2:B8:29:4B:55:84:AB:6B:58:C2:90:46:6C:AC:3F:B8:39:8F:84:83
Valid From	2012-08-21	2012-08-08
Valid To	2042-08-21	2029-12-31
Certificate Version	3	3
Certificate Signature Algorithm	SHA-256	SHA-256
Signing key parameters	2048	4096
Test Website URL	https://www.56zhifu.com I imported the root cert and browsed to this URL, and got the following error: The certificate is not trusted because no issuer chain was provided. (Error code: sec_error_unknown_issuer) Intermediate CA certificates are expected to be distributed to the certificate subjects (the holders of the private keys) together with the subjects' own certificates. Those subject parties (e.g. SSL servers) are then expected to send out the intermediate CA certificates together with their own certificates whenever they are asked to send out their certificates. That is required by SSL/TLS. Certificate authorities MUST advise their subscribers that all intermediate certificates should be installed in the servers containing the dependent subscriber certificates.	https://pub.cebnet.com.cn I imported the root cert and browsed to this URL, and got the following error: The response from the OCSP server was corrupted or improperly formed. (Error code: sec_error_ocsp_malformed_response) Please see https://wiki.mozilla.org/CA:Recommended_Practices#OCSP Please read section 4.2.2.2 "Authorized Responders" on pages 10-11 of RFC 2560. CAs that emit certificates for the general public must use a configuration that conforms to either rule 2 or 3. Please test in Firefox with preferences set to hard fail if OCSP fails.
CRL URL	http://crl.cfca.com.cn/gtoca/RSA/crl1.crl 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	http://ocsp.cfca.com.cn/ocsp/ Maximum expiration time of OCSP responses : 7 days	http://ocsp.cfca.com.cn/ocsp/ Maximum expiration time of OCSP responses : 7 days
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) Code Signing	Websites (SSL/TLS) Code Signing
SSL Validation	OV	EV

Type		
EV Policy OID(s)	N/A Not requesting EV treatment for this root.	2.16.156.112554.3 Please follow https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version and attach a screenshot to the bug that shows successful completion of the test.
Non-sequential serial numbers and entropy in cert	CFCA's end-entity certificates now have 8 bits of unpredictable random data in serial number.New end-entity certificates after 2014-2-15 will have 20 bits of unpredictable random data in serial number .	20 bits of unpredictable random data will be include in serial number of new end-entity certificates.

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	CFCA EV ROOT has one internally-operated subordinate CA -- CFCA EV OCA
Externally Operated SubCAs	CFCA GT CA has no Externally Operated subCA.	CFCA EV root has no Externally Operated subCA.
Cross-Signing	N/A	N/A
Technical Constraints on Third-party Issuers	N/A	N/A

Verification Policies and Practices

Policy Documentation	CFCA Document repository: **Please provide URL to where the policy documentation can be found on the CFCA website.** CPS (English): https://bug926029.bugzilla.mozilla.org/attachment.cgi?id=816212
Audit	Audit Type: WebTrust for CA and EV Auditor: PricewaterhouseCoopers Audit Report: https://cert.webtrust.org/SealFile?seal=1606&file=pdf (2013.10.31) EV Audit Report: https://cert.webtrust.org/SealFile?seal=1607&file=pdf (2013.10.31)

Baseline Requirements (SSL)	CFCA conforms to the Baseline_Requirements_V1_1_6 of the CA/Browser Forum Guidelines for Issuance and Management of Extended Validation Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and those Guidelines, those Guidelines take precedence over this document. Was this text added to the CPS? Need to see new version of the CPS. Need BR audit statement. 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 3.2.2.3-6 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	CPS section 3.2.2.5: The applicants of other types of certificates also undergo identity verification. For Email Certificate, CFCA only issue certificates to domain name email that can be verified through WHOIS. CFCA verifies the validity of the email address and determines whether it's legitimate through appropriate channels.
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. I did not find text in the CPS that said which procedures apply to Code Signing certificates issuance. Section 3.2.2.3 is about authentication of SSL certificate subscriber identity. It doesn't appear to say anything about code signing certs.
Multi-factor Authentication	For each account that can access the certificate issuance system, we use usbkey model SJK1232 in the

	procedure of authorization, this measure is apply to all accounts that can cause the approval and/or issuance of end-entity certificates
Network Security	CPS sections 5 and 6 CFCA maintain network security controls that meet the Network and Certificate System Security Requirements published at http://www.cabforum.org

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	N/A
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	For Multi-domain certificate each domain will containing the Fully-Qualified Domain Name or an iPAddress containing the IP address of a server, meet the CA/Browser Forum Baseline Requirements.
Domain owned by a Natural Person	CFCA's follow this patternO = name of the person in the form as displayed in its IDOU = the string "natural person" EV can be bought only by organisation
OCSP	See above.

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

Long-lived DV certificates	CFCA doesn't issue DV certs. issues OV and EV certs.
Wildcard DV SSL certificates	CFCA doesn't issue DV certs. issues OV and EV certs.
Email Address Prefixes for DV Certs	CFCA doesn't issue DV certs. issues OV and EV certs.
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	CFCA issuing certificates using internally- - operated subordinate CAs
Allowing external entities to operate subordinate CAs	CFCA do not allow external entities to operate subordinate CAs
Distributing generated private keys in PKCS#12 files	CFCA will not generate the key pairs for their subscriber or any signer or SSL certificates.
Certificates referencing hostnames or	Yes.

private IP addresses	See CPS section 3.2.2.3 , 3.2.2.4, certificate hostname not resolvable through the public DNS will not pass our verification.And CFCA will not accept private IP addresses. (OV accept public IP, EV don't accept IP)
Issuing SSL Certificates for Internal Domains	See above
OCSP Responses signed by a certificate under a different root	CFCA's OCSP responses conform to RFC 2560, And passed BVT test using Firefox 26CFCA's OSCP sign cert is under same root .
CRL with critical CIDP Extension	CFCA issues full CRLs, but not partitioned CRLs, and never put critical CIDP extensions into full CRLs.
Generic names for CAs	Our CA name include “CFCA”
Lack of Communication With End Users	CFCA has 7*24 hour hotline(8610-4008809888) for end users.