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

Column1	Column2
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. Furthermore, CFCA has passed Webtrust audit, it meets Mozilla's requirements of root certificate inclusion.
Inclusion in other major browsers	Internet Explorer
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（GT）

Certificate Name	CFCA GT CA
Certificate Issuer Field	CN = CFCA GT CA O = China Financial Certification Authority C = CN
Certificate Summary	This root certificate issues Individual Certificate, Organization Certificate, Web Server Certificate and Code Signing Certificate.
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
Test Website URL	https://www.56zhifu.com
CRL URL	http://crl.cfca.com.cn/gtoca/RSA/crl1.crl
OCSP URL	http://ocsp.cfca.com.cn/ocsp/
	http://gtc.cfca.com.cn/gtoca/gtoca2.cer
	Maximum expiration time of OCSP responses : 7 days
Requested Trust Bits	websites, email, code signing
SSL Validation Type	OV
EV Policy OID(s	N/A
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 .

Technical information about each root certificate（EV）

Certificate Name	CFCA EV ROOT
Certificate Issuer Field	CN = CFCA EV ROOT O = China Financial Certification Authority C = CN
Certificate Summary	This root certificate issues EV certificates.
Root Cert URL	https://bugzilla.mozilla.org/attachment.cgi?id=8356494
SHA1 Fingerprint	E2:B8:29:4B:55:84:AB:6B:58:C2:90:46:6C:AC:3F:B8:39:8F:84:83
Valid From	2012---08---08
Valid To	2029---12---31
Test Website URL	https://pub.cebnet.com.cn
CRL URL	http://crl.cfca.com.cn/evoca/RSA/crl1.crl
OCSP URL	http://ocsp.cfca.com.cn/ocsp/
	http://gtc.cfca.com.cn/evoca/evoca.cer
	Maximum expiration time of OCSP responses : 7 days
Requested Trust Bits	websites,code signing
SSL Validation Type	EV
EV Policy OID(s	2.16.156.112554.3
Non---sequential serial numbers and entropy in cert	20 bits of unpredictable random data will be include in serial number of new end-entity certificates.

CA Hierarchy information for each root certificate（GT）

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.
Externally Operated SubCAs	CFCA GT CA has no Externally Operated subCA.
Cross---Signing	N/A
Technical Constraints on Third---party Issuers	N/A

CA Hierarchy information for each root certificate（EV）

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

Verification Policies and Practices （GT）	
Policy Documentation	https://bug926029.bugzilla.mozilla.org/attachment.cgi?id=816212
Audit	Audit Type: WebTrust for CA Auditor: PricewaterhouseCoopers Audit Report: https://cert.webtrust.org/ViewSeal?id=1606
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.
Organization Verification	CPS section 3.2.2.2
SSL Verification Procedures	CPS section 3.2.2.3-6
Email Address Verification Procedures	CPS section 3.2.2.5
Code Signing Subscriber Verification Procedures	CPS section 3.2.2.3
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	CFCA maintain network security controls that meet the Network and Certificate System Security Requirements published at http://www.cabforum.org
Verification Policies and Practices （EV）	
Policy Documentation	https://bug926029.bugzilla.mozilla.org/attachment.cgi?id=816212
Audit	Audit Type: WebTrust EV for CA Auditor: PricewaterhouseCoopers Audit Report: https://cert.webtrust.org/ViewSeal?id=1607
Baseline Requirements (SSL)	CFCA conforms to the EV SSL Certificate Guidelines Version 1.4.3 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.
Organization Verification	CPS section 3.2.2.2
SSL Verification Procedures	CPS section 3.2.2.3-6
Email Address Verification Procedures	CPS section 3.2.2.5
Code Signing Subscriber Verification Procedures	CPS section 3.2.2.4
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	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 （GT）	
Publicly Available CP and CPS	https://bug926029.bugzilla.mozilla.org/attachment.cgi?id=816212
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.
Audit Criteria	WebTrust Principles and Criteria for Certification Authorities 2.0 From http://www.webtrust.org/ https://cert.webtrust.org/ViewSeal?id=1606
Document Handling of IDNs in CP/CPS	N/A
Revocation of Compromised	CPS section 4.8, CFCA will revoke certificates with private keys that are known to be compromised, or for which verification of subscriber information is known to be invalid.
Verifying Domain Name Ownership	CPS section 3.2.2.3-6
Verifying Email Address Control	CPS section 3.2.2.5
Verifying Identity of Code Signing Certificate Subscriber	CPS section 3.2.2.3
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 pattern O = name of the person in the form as displayed in its ID OU = the string "natural person"
OCSP	http://ocsp.cfca.com.cn/ocsp/
	http://gtc.cfca.com.cn/gtoca/gtoca2.cer
Network Security Controls	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 （EV）	
Publicly Available CP and CPS	https://bug926029.bugzilla.mozilla.org/attachment.cgi?id=816212
CA Hierarchy	CFCA EV ROOT has one internally---operated subordinate CA --- CFCA EV OCA
Audit Criteria	WebTrust for Certification Authorities - Extended Validation Audit Criteria Version 1.4 From http://www.webtrust.org/ https://cert.webtrust.org/ViewSeal?id=1607
Document Handling of IDNs in CP/CPS	N/A

Revocation of Compromised	CPS section 4.8, CFCA will revoke certificates with private keys that are known to be compromised, or for which verification of subscriber information is known to be invalid.
Verifying Domain Name Ownership	CPS section 3.2.2.3-6
Verifying Email Address Control	CPS section 3.2.2.5
Verifying Identity of Code Signing Certificate Subscriber	CPS section 3.2.2.4
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	EV can be bought only by organisation
OCSP	http://ocsp.cfca.com.cn/ocsp/
	http://gtc.cfca.com.cn/gtoca/gtoca2.cer
Network Security Controls	CFCA maintain network security controls that meet the Network and Certificate System Security Requirements published at http://www.cabforum.org

Response to Mozilla's list of Potentially 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	Domain and Email validation will be incorporated into the issuing CAs procedures .Delegation of domain/email validation to third parties can't be done without CFCA
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 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	See CPS section 3.2.2.3 , 3.2.2.4 , CFCA will not issue SSL Certificates for Internal Domains.
OCSP Responses signed by a certificate under a different root	CFCA's OCSP responses conform to RFC 2560, And passed BVT test using Firefox 26 CFCA'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.