Mozilla - CA Program

Case Information

Case Number	00000006	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owners/Certificate Name	China Financial Certification Authority (CFCA)	**Request Status**	CA Action Items from Discussion

Additional Case Information

Subject	Include CFCA (China Financial Certification Authority) EV root	**Case Reason**	New Owner/Root inclusion requested

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org /show_bug.cgi?id=926029

General information about CA's associated organization

Company Website	http://www.cfca.com.cn/	**Verified?**	Verified
Organizational Type	Public Corporation	**Verified?**	Verified
Organizational Type (Others)	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.	**Verified?**	Verified
Geographic Focus	People's Republic of China	**Verified?**	Verified
Primary Market / Customer Base	CFCA SSL Certificates can be used in the areas such as online banking, e-commence, e-politic, enterprise informatization and public services and so on. There are more than 200 Chinese banks that are using CFCA's certificates to ensure the security of online banking trade.	**Verified?**	Verified
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.	**Verified?**	Verified

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	* Revocation of Compromised Certificates: CPS section 4.8.1 * EV can be bought only by organisation	**Verified?**	Verified

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	* 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. * 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)	**Verified?**	Verified

Root Case Record # 1

Root Case Information

Root Case No	R00000009	**Case Number**	00000006
Request Status	CA Action Items from Discussion	**Root Certificate Name**	CFCA EV ROOT

Additional Root Case Information

Subject	Include CFCA EV ROOT

Technical Information about Root Certificate

O From Issuer Field	China Financial Certification Authority	**Verified?**	Verified
OU From Issuer Field		**Verified?**	Verified
Certificate Summary	This root certificate has one internally-operated intermediate certificate that issues EV certificates.	**Verified?**	Verified
Root Certificate Download URL	https://bugzilla.mozilla.org/attachment.cgi?id=8356494	**Verified?**	Verified
Valid From	2012 Aug 08	**Verified?**	Verified
Valid To	2029 Dec 31	**Verified?**	Verified
Certificate Version	3	**Verified?**	Verified
Certificate Signature Algorithm	SHA-256	**Verified?**	Verified
Signing Key Parameters	4096	**Verified?**	Verified
Test Website URL (SSL) or Example Cert	https://pub.cebnet.com.cn	**Verified?**	Verified

CRL URL(s)	http://crl.cfca.com.cn/evrca/RSA/crl1.crl http://crl.cfca.com.cn/evoca/RSA/crl1.crl	**Verified?**	Verified
OCSP URL(s)	http://ocsp.cfca.com.cn/ocsp/	**Verified?**	Verified
Trust Bits	Websites	**Verified?**	Verified
SSL Validation Type	EV	**Verified?**	Verified
EV Policy OID(s)	2.16.156.112554.3	**Verified?**	Verified
EV Tested	// CN=CFCA EV ROOT,O=China Financial Certification Authority,C=CN "2.16.156.112554.3", "CFCA EV OID", SEC_OID_UNKNOWN, { 0x5C, 0xC3, 0xD7, 0x8E, 0x4E, 0x1D, 0x5E, 0x45, 0x54, 0x7A, 0x04, 0xE6, 0x87, 0x3E, 0x64, 0xF9, 0x0C, 0xF9, 0x53, 0x6D, 0x1C, 0xCC, 0x2E, 0xF8, 0x00, 0xF3, 0x55, 0xC4, 0xC5, 0xFD, 0x70, 0xFD }, "MFYxCzAJBgNVBAYTAkNOMTAwLgYDVQQKDCdDaGluYSBGaW5hbmNpYWwgQ2VydGlm" "aWNhdGlvbiBBdXRob3JpdHkxFTATBgNVBAMMDENGQ0EgRVYgUk9PVA==", "GErM1g==", Success!	**Verified?**	Verified
Root Stores Included In	Microsoft	**Verified?**	Verified
Mozilla Applied Constraints	None	**Verified?**	Verified

Digital Fingerprint Information

SHA-1 Fingerprint	E2:B8:29:4B:55:84:AB:6B:58:C2:90:46:6C:AC:3F:B8:39:8F:84:83	**Verified?**	Verified
SHA-256 Fingerprint	5C:C3:D7:8E:4E:1D:5E:45:54:7A:04:E6:87:3E:64:F9:0C:F9:53:6D:1C:CC:2E:F8:00:F3:55:C4:C5:FD:70:FD	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	CFCA EV ROOT has one internally-operated subordinate CA -- CFCA EV OCA	**Verified?**	Verified
Externally Operated SubCAs	None, and none planned.	**Verified?**	Verified
Cross Signing	None, and none planned.	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	Not applicable.	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	http://www.cfca.com.cn/us/us-12.htm	**Verified?**	Verified
CA Document Repository	http://www.cfca.com.cn/us/us-12.htm	**Verified?**	Verified
CP Doc Language	Chinese		
CP	http://www.cfca.com.cn/us/us-12.htm	**Verified?**	Verified
CP Doc Language	Chinese		
CPS	http://www.cfca.com.cn/file/CFCA-1403-CPS-en.rar	**Verified?**	Verified

Other Relevant Documents		**Verified?**	Not Applicable
Auditor Name	PricewaterhouseCoopers	**Verified?**	Verified
Auditor Website	http://www.pwccn.com/home/eng/index.html	**Verified?**	Verified
Auditor Qualifications	http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx	**Verified?**	Verified
Standard Audit	https://cert.webtrust.org/SealFile?seal=1788&file=pdf	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	12/5/2014	**Verified?**	Verified
BR Audit	https://cert.webtrust.org/SealFile?seal=1787&file=pdf	**Verified?**	Verified
BR Audit Type	WebTrust	**Verified?**	Verified
BR Audit Statement Date	12/5/2014	**Verified?**	Verified
EV Audit	https://cert.webtrust.org/SealFile?seal=1786&file=pdf	**Verified?**	Verified
EV Audit Type	WebTrust	**Verified?**	Verified
EV Audit Statement Date	12/5/2014	**Verified?**	Verified
BR Commitment to Comply	CPS sections 1.1 and 9.17	**Verified?**	Verified
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, address, and country of the applicant, but also the IP and the compliance of CSR. The procedures are as follows: 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 the IP is allocated by the ISP to the applicant.	**Verified?**	Verified
EV SSL Verification Procedures	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: …	**Verified?**	Verified

Organization Verification Procedures	CPS section 3.2.2	**Verified?**	Verified
Email Address Verification Procedures	Not requesting Email trust bit for this root.	**Verified?**	Verified
Code Signing Subscriber Verification Pro	Not requesting Code Signing trust bit for this root.	**Verified?**	Verified
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	**Verified?**	Verified
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	**Verified?**	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	https://www.cfca.com.cn/file/EVSSL.zip	**Verified?**	Verified