Print this page

Mozilla - CA Program

Case Information

Case Number	00000083	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	Shanghai Electronic Certification Authority Co., Ltd. (SHECA)	**Request Status**	In Detailed CP/CPS Review

Additional Case Information

Subject	Include SHECA Roots	**Case Reason**	

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org /show_bug.cgi?id=1309797

General information about CA's associated organization

CA Email Alias 1			
CA Email Alias 2			
Company Website	https://www.sheca.com/repository	**Verified?**	Verified
Organizational Type	Commercial Organization	**Verified?**	Verified
Organizational Type (Others)		**Verified?**	Not Applicable
Geographic Focus	China	**Verified?**	Verified
Primary Market / Customer Base	SHECA issues certificates to business corporations, government agencies, and individuals in China, Hong Kong, Macau and Taiwan.	**Verified?**	Verified
Impact to Mozilla Users	A large proportion of our customers are using Firefox as a daily browser	**Verified?**	Verified

Required and Recommended Practices

Recommended Practices	https://wiki.mozilla.org /CA/Required_or_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. Publicly Available CP and CPS: Yes 2. Audit Criteria: CP/CPS section 8 3. Revocation of Compromised Certificates: CP/CPS section 4.9.1 4. Verifying Domain Name Ownership: CP/CPS section 3.2 5. Verifying Email Address Control: CP/CPS section 3.2 6. DNS names go in SAN: Yes 7. OCSP: CP/CPS section 7.3 8. Network Security Controls: CP/CPS section 6.7	**Verified?**	Verified

Forbidden and Potentially Problematic Practices

Potentially Problematic Practices	https://wiki.mozilla.org/CA/Forbidden_or_Problematic_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	1. Long-lived Certificates: CP/CPS sections 6.3.2, 6.3.3 2. Non-Standard Email Address Prefixes for Domain Ownership Validation: CP/CPS section 3.2 3. Issuing End Entity Certificates Directly From Roots: CP/CPS section 1.1.2 4. Distributing Generated Private Keys in PKCS#12 Files: CP/CPS section 3.2.1 5. Certificates Referencing Local Names or Private IP Addresses: CPS sections 3.2.5, 3.2.6 6. Issuing SSL Certificates for .int Domains: CP/CPS section 3.2 7. OCSP Responses Signed by a Certificate Under a Different Root: No 8. Issuance of SHA-1 Certificates: CPS Appendix.2 "Cryptographic Algorithms and Key Strengths" 9. Delegation of Domain / Email Validation to Third Parties: CP/CPS section 1.3.2	**Verified?**	Verified

Root Case Record # 1

Root Case Information

Root Certificate Name	UCA Global G2 Root	**Root Case No**	R00000123
Request Status	In Detailed CP/CPS Review	**Case Number**	00000083

Certificate Data

Certificate Issuer Common Name	UCA Global G2 Root
O From Issuer Field	UniTrust
OU From Issuer Field	
Valid From	2016 Mar 11
Valid To	2040 Dec 31
Certificate Serial Number	5ddfb1da5aa3ed5dbe5a6520650390ef
Subject	CN=UCA Global G2 Root, OU=null, O=UniTrust, C=CN
Signature Hash Algorithm	sha256WithRSAEncryption
Public Key Algorithm	RSA 4096 bits
SHA-1 Fingerprint	28:F9:78:16:19:7A:FF:18:25:18:AA:44:FE:C1:A0:CE:5C:B6:4C:8A
SHA-256 Fingerprint	9B:EA:11:C9:76:FE:01:47:64:C1:BE:56:A6:F9:14:B5:A5:60:31:7A:BD:99:88:39:33:82:E5:16:1A:A0:49:3C
Certificate ID	32:B9:15:B5:8C:BF:59:C7:21:C6:8E:35:BC:D2:37:F5:43:02:0B:A7:57:6D:27:2E:52:32:22:1E:EE:A1:21:72
Certificate Version	3

Technical Information about Root Certificate

Certificate Summary	There are two subordinate CAs signed by “UCA Global G2 Root” issuing SSL certificates and code signing certificates. - SHECA Global G3 SSL - SHECA Global G3 Code Signing	**Verified?**	Verified
Root Certificate Download URL	https://bugzilla.mozilla.org /attachment.cgi?id=8962973	**Verified?**	Verified
CRL URL(s)	http://ldap2.sheca.com /root/ucaglobalg2.crl http://ldap2.sheca.com/CA10011 /RA12050100/CRL23844.crl CP section 4.9.7, CPS section 4.9.8. 24 hours for EE CRL.	**Verified?**	Verified
OCSP URL(s)	http://ocsp3.sheca.com /ucaglobalg2root /ucaglobalg2root.ocsp	**Verified?**	Verified

	http://ocsp3.sheca.com/ocsp/sheca/sheca.ocsp CPS section 4.9.11		
Mozilla Trust Bits	Email; Websites	**Verified?**	Verified
SSL Validation Type	OV	**Verified?**	Verified
Mozilla EV Policy OID(s)	Not EV	**Verified?**	Not Applicable
Root Stores Included In	Microsoft	**Verified?**	Verified
Mozilla Applied Constraints	None	**Verified?**	Verified

Test Websites or Example Cert

Test Website - Valid	https://ef-gb.wwwtrust.org	**Verified?**	Verified
Test Website - Expired	https://ex-gb.wwwtrust.org		
Test Website - Revoked	https://re-gb.wwwtrust.org		
Example Cert			
Test Notes			

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

Revocation Tested	https://certificate.revocationcheck.com/ef-gb.wwwtrust.org OK	**Verified?**	Verified
CA/Browser Forum Lint Test	https://crt.sh/?caid=36110&opt=cablint,zlint,x509lint&minNotBefore=2016-03-12 OK	**Verified?**	Verified
Test Website Lint Test	See above	**Verified?**	Verified
EV Tested	N/A	**Verified?**	Not Applicable

CA Hierarchy Information

CA Hierarchy	CP/CPS section 1.1.2 This root has two internally-operated subCAs.	**Verified?**	Verified
Externally Operated SubCAs	None	**Verified?**	Verified
Cross Signing	None	**Verified?**	Verified

Technical Constraint on 3rd party Issuer	CPS section 1.3.2: SHECA does not allow external RAs to issue SSL certs.	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	Documents are in Chinese, and some are translated into English. The SHECA repository website cert chains up to the UCA Extended Validation Root cert, so must import that root first: https://bugzilla.mozilla.org/attachment.cgi?id=8962974 Also, I ran into problems accessing the CP/CPS documents directly from the links below, but I was able to access the documents by going to the repository page and clicking the links from there.	**Verified?**	Verified
CA Document Repository	https://www.sheca.com/repository	**Verified?**	Verified
CP Doc Language	English		
CP	https://assets-cdn.sheca.com/documents/unitrust-certificate-policy-en-v1.2.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	https://assets-cdn.sheca.com/documents/sheca-certificate-practice-statement-en-v3.5.pdf	**Verified?**	Verified
Other Relevant Documents		**Verified?**	Not Applicable
Auditor (New)	PwC - PricewaterhouseCoopers International Limited	**Verified?**	Verified
Auditor Location (New)	China	**Verified?**	Verified
Standard Audit	https://cert.webtrust.org/SealFile?seal=2262&file=pdf	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	6/16/2017	**Verified?**	Verified
BR Audit	https://cert.webtrust.org/SealFile?seal=2263&file=pdf	**Verified?**	Verified
BR Audit Type	WebTrust	**Verified?**	Verified
BR Audit Statement Date	6/16/2017	**Verified?**	Verified

EV SSL Audit	N/A	**Verified?**	Not Applicable
EV SSL Audit Type		**Verified?**	Not Applicable
EV SSL Audit Statement Date		**Verified?**	Not Applicable
BR Commitment to Comply	CPS section 1.1, CP section 1.	**Verified?**	Verified
BR Self Assessment	https://bugzilla.mozilla.org/attachment.cgi?id=8872017	**Verified?**	Verified
SSL Verification Procedures	CPS sections 3.2.5, 3.2.6, 3.2.7 CP section 3.2.3	**Verified?**	Verified
EV SSL Verification Procedures	N/A	**Verified?**	Not Applicable
Organization Verification Procedures	CPS sections 3.2.2, 3.2.3, 3.2.4, 3.2.11 CP sections 3.2.2, 3.2.3, 3.2.5	**Verified?**	Verified
Email Address Verification Procedures	CPS section 3.2.8 CP section 3.2.3	**Verified?**	Verified
Code Signing Subscriber Verification Pro	Mozilla is no longer accepting requests to enable the Code Signing trust bit.	**Verified?**	Not Applicable
Multi-Factor Authentication	CP/CPS section 5	**Verified?**	Verified
Network Security	CP/CPS section 6.7	**Verified?**	Verified

Root Case Record # 2

Root Case Information

Root Certificate Name	UCA Extended Validation Root	**Root Case No**	R00000135
Request Status	In Detailed CP/CPS Review	**Case Number**	00000083

Certificate Data

Certificate Issuer Common Name	UCA Extended Validation Root
O From Issuer Field	UniTrust
OU From Issuer Field	
Valid From	2015 Mar 13

Valid To	2038 Dec 31
Certificate Serial Number	4fd22b8ff564c8339e4f345866237060
Subject	CN=UCA Extended Validation Root, OU=null, O=UniTrust, C=CN
Signature Hash Algorithm	sha256WithRSAEncryption
Public Key Algorithm	RSA 4096 bits
SHA-1 Fingerprint	A3:A1:B0:6F:24:61:23:4A:E3:36:A5:C2:37:FC:A6:FF:DD:F0:D7:3A
SHA-256 Fingerprint	D4:3A:F9:B3:54:73:75:5C:96:84:FC:06:D7:D8:CB:70:EE:5C:28:E7:73:FB:29:4E:B4:1E:E7:17:22:92:4D:24
Certificate ID	FD:EE:D5:B2:F5:81:8F:96:D7:9C:0E:6A:FD:BB:B6:90:2B:5E:E6:E3:88:38:62:6A:E6:3D:0D:9E:4F:1F:3C:05
Certificate Version	3

Technical Information about Root Certificate

Certificate Summary	There are two subordinate CAs signed by “UCA Extended Validation Root” issuing SSL certificates and code signing certificates.	**Verified?**	Verified
Root Certificate Download URL	https://bugzilla.mozilla.org/attachment.cgi?id=8962974	**Verified?**	Verified
CRL URL(s)	http://ldap2.sheca.com/root/ucaevsub.crl http://ldap2.sheca.com/CA81/RA12050100/CRL28438.crl CP section 4.9.7, CPS section 4.9.8. 24 hours for EE CRL.	**Verified?**	Verified
OCSP URL(s)	http://ocsp3.sheca.com/evroot/ev.ocsp http://ocsp3.sheca.com/ocsp/sheca/sheca.ocsp CPS section 4.9.11	**Verified?**	Verified
Mozilla Trust Bits	Websites	**Verified?**	Verified
SSL Validation Type	EV	**Verified?**	Verified
Mozilla EV Policy OID(s)	2.23.140.1.1	**Verified?**	Verified
Root Stores Included In	Microsoft	**Verified?**	Verified

Mozilla Applied Constraints	None	**Verified?**	Verified

Test Websites or Example Cert

Test Website - Valid	https://ef-EV.sheca.com	**Verified?**	Verified
Test Website - Expired	https://ex-EV.sheca.com		
Test Website - Revoked	https://re-EV.sheca.com		
Example Cert			
Test Notes			

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

Revocation Tested	https://certificate.revocationcheck.com/ef-ev.sheca.com OK	**Verified?**	Verified
CA/Browser Forum Lint Test	https://crt.sh/?caid=36111&opt=cablint,zlint,x509lint&minNotBefore=2015-03-14 OK	**Verified?**	Verified
Test Website Lint Test	See above	**Verified?**	Verified
EV Tested	ev-checker exited successfully: Success!	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	CP/CPS section 1.1.2 This root has two internally-operated subCAs.	**Verified?**	Verified
Externally Operated SubCAs	None	**Verified?**	Verified
Cross Signing	None	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	CP/CPS section 1.3.2: SHECA does not allow external RAs to issue EV certs.	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	Documents are in Chinese, with some translated into English The SHECA website cert chains up	**Verified?**	Verified

	to this UCA Extended Validation Root cert, so must import the root first: https://bugzilla.mozilla.org/attachment.cgi?id=8962974 Also, I ran into problems accessing the CP/CPS documents directly from the links below, but I was able to access the documents by going to the repository page and clicking the links from there.		
CA Document Repository	https://www.sheca.com/repository	**Verified?**	Verified
CP Doc Language	English		
CP	https://assets-cdn.sheca.com/documents/unitrust-ev-certificate-policy-en-v1.3.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	https://assets-cdn.sheca.com/documents/unitrust-ev-certificate-practice-statement-en-v1.3.pdf	**Verified?**	Verified
Other Relevant Documents		**Verified?**	Not Applicable
Auditor (New)	PwC - PricewaterhouseCoopers International Limited	**Verified?**	Verified
Auditor Location (New)	China	**Verified?**	Verified
Standard Audit	https://cert.webtrust.org/SealFile?seal=2262&file=pdf	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	6/16/2017	**Verified?**	Verified
BR Audit	https://cert.webtrust.org/SealFile?seal=2263&file=pdf	**Verified?**	Verified
BR Audit Type	WebTrust	**Verified?**	Verified
BR Audit Statement Date	6/16/2017	**Verified?**	Verified
EV SSL Audit	https://cert.webtrust.org/SealFile?seal=2264&file=pdf	**Verified?**	Verified
EV SSL Audit Type	WebTrust	**Verified?**	Verified
EV SSL Audit Statement Date	6/16/2017	**Verified?**	Verified
BR Commitment to Comply	CPS section 1	**Verified?**	Verified
BR Self Assessment	https://bugzilla.mozilla.org/attachment.cgi?id=8872017	**Verified?**	Verified

SSL Verification Procedures	CPS sections 3.2.4, 3.2.5	**Verified?**	Verified
EV SSL Verification Procedures	CP/CPS section 3.2	**Verified?**	Verified
Organization Verification Procedures	CPS sections 3.2.2, 3.2.9 CP sections 3.2.2, 3.2.5	**Verified?**	Verified
Email Address Verification Procedures	CPS section 3.2.6	**Verified?**	Verified
Code Signing Subscriber Verification Pro	Mozilla is no longer accepting requests to enable the Code Signing trust bit.	**Verified?**	Not Applicable
Multi-Factor Authentication	CP/CPS section 5	**Verified?**	Verified
Network Security	CP/CPS section 6.7	**Verified?**	Verified