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**	Information Verification In Process

Additional Case Information

Subject	Include new 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	http://www.sheca.com/policy/	**Verified?**	Verified
Organizational Type	Commercial Organization	**Verified?**	Verified
Organizational Type (Others)		**Verified?**	Not Applicable
Geographic Focus	China	**Verified?**	Verified
Primary Market / Customer Base	a) Business corporations registered in mainland China b) Government agencies of China(e.g.,tax bureau) c) Individual; China citizens(including citizens from Hong Kong, Macau and Taiwan) d) Servers of business corporations which have been registered in mainland China e) Software developers	**Verified?**	Verified
Impact to Mozilla Users	A large proportion of our customers are using Firefox as a daily browser	**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	1. NEED CA's response to each of the items listed in https://wiki.mozilla.org/CA:Recommended_Practices#CA_Recommended_Practices 1) Publicly Available CP and CPS: (please provide links)	**Verified?**	Need Response From CA

Recommended Practices	2) CA Hierarchy: CP Section 1.1.2 3) Audit Criteria: ??? 4) Document Handling of IDNs in CP/CPS: CP: section 3.2.2-3.2.3, CPS: section 3.2.5 5) Revocation of Compromised Certificates: CP: Section 5.7.3 6) Verifying Domain Name Ownership: ??? 7) Verifying Email Address Control: ??? 8) Verifying Identity of Code Signing Certificate Subscriber: 9) DNS names go in SAN: All DNS names go into SAN, and one primary DNS name maybe go into the Subject Common Name. 10) Domain owned by a Natural Person: ??? 11) OCSP: CP, CPS: Section 7.3 12) Network Security Controls: ???

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	2. NEED CA's response to each of the items listed in https://wiki.mozilla.org/CA:Problematic_Practices#Potentially_problematic_CA_practices 1) Long-lived DV certificates: Not applicable, SHECA does not issue any Long-lived DV certificates 2) Wildcard DV SSL certificates: Not applicable, SHECA does not issue any Wildcard DV SSL certificates 3) Email Address Prefixes for DV Certs: Not applicable 4) Delegation of Domain / Email validation to third parties: Not applicable. SHECA doesn't delegate any business part to third parties. 5) Issuing end entity certificates directly from roots: Not applicable. 6) Allowing external entities to operate subordinate CAs: Not allowed. 7) Distributing generated private keys in PKCS#12 files: Not support. 8) Certificates referencing hostnames or private IP addresses: Not applicable. SHECA does not issue certificates of this type. 9) Issuing SSL Certificates for Internal Domains: Not applicable 10) OCSP Responses signed by a certificate under a different root: OCSP Responses are signed by a certificate under the corresponding issuer of the supplied certificate in OCSP Requests. 11) SHA-1 Certificates: This root does not issue any SHA-1 Certificates. 12) Generic names for CAs: Not applicable 13) Lack of Communication With End Users: SHECA provides customer server hotline, email and official website to general publics including subscriber, relying parties 14) Backdating the notBefore date: No backdating of notBefore date – Certificates are valid from the issuing day.	**Verified?**	Need Response From CA

Root Case Record # 1

Root Case Information

Root Certificate Name	UCA Global G2 Root	**Root Case No**	R00000123
Request Status	Information Verification In Process	**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 Fingerprint	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.	**Verified?**	Verified
Root Certificate Download URL	http://www.sheca.com/download/getdownloadforpdf/126	**Verified?**	Verified
CRL URL(s)	SHECA Global G3 SSL CRL http://ldap2.sheca.com/root/ucaglobalg2.crl SHECA Global G3 CodeSigning CRL http://ldap2.sheca.com/root/ucaglobalg2.crl	**Verified?**	Verified
OCSP URL(s)	http://ocsp3.sheca.com/ocsp/sheca/sheca.ocsp	**Verified?**	Verified
Trust Bits	Email	**Verified?**	Verified
SSL Validation Type	OV	**Verified?**	Verified
EV Policy OID(s)	N/A	**Verified?**	Not Applicable
Root Stores Included In	Microsoft	**Verified?**	Verified
Mozilla Applied Constraints	None	**Verified?**	Verified

Test Websites or Example Cert

Test Website URL (SSL) or Example Cert	https://ef-gb.wwwtrust.org/	**Verified?**	Need Response From CA
Test Website - Expired			
Test Website - Revoked			

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

Revocation Tested	No Errors	**Verified?**	Verified

CA/Browser Forum Lint Test	No Errors	**Verified?**	Verified
Test Website Lint Test	Test not currently available	**Verified?**	Not Applicable
EV Tested	No EV request	**Verified?**	Not Applicable

CA Hierarchy Information

CA Hierarchy	CP Section 1.1.2 http://www.sheca.com/download/getdownloadforpdf/162	**Verified?**	Verified
Externally Operated SubCAs	None	**Verified?**	Verified
Cross Signing	None	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	Not Applicable	**Verified?**	Not Applicable

Verification Policies and Practices

Policy Documentation	NEED: Languages that the CP/CPS and other documents are provided in.	**Verified?**	Need Response From CA
CA Document Repository		**Verified?**	Need Response From CA
CP Doc Language	English		
CP	http://www.sheca.com/download/getdownloadforpdf/162	**Verified?**	Verified
CP Doc Language	English		
CPS	http://www.sheca.com/download/getdownloadforpdf/160	**Verified?**	Verified
Other Relevant Documents		**Verified?**	
Auditor Name	Auditor:PricewaterhouseCoopers (PWC)	**Verified?**	Verified
Auditor Website	www.pwc.com	**Verified?**	Verified
Auditor Qualifications	https://cert.webtrust.org/ViewSeal?id=2045	**Verified?**	Verified
Standard Audit	NEED: for all root inclusion/change requests. Reference section 2 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date		**Verified?**	Need Response From CA
BR Audit	NEED: If requesting Websites trust bit, then also need a BR audit as described here: https://wiki.mozilla.org/CA:BaselineRequirements	**Verified?**	Need Response From CA
BR Audit Type		**Verified?**	Need Response From CA
BR Audit Statement Date		**Verified?**	Need Response From CA
EV Audit	No EV	**Verified?**	Not

			Applicable
EV Audit Type		**Verified?**	Not Applicable
EV Audit Statement Date		**Verified?**	Not Applicable
BR Commitment to Comply	NEED section in the CP/CPS that has the commitment to comply with the BRs as described in section 2.2 of version 1.3 of the CA/Browser Forum's Baseline Requirements.	**Verified?**	Need Response From CA
SSL Verification Procedures	CP: Sections 3.2.2-3.2.3,3.2.5 CPS: Sections 3.2.2-3.2.5,3.2.7 NEED: if Websites trust bit requested... Sections of CP/CPS that sufficiently describe the verification steps that are taken to confirm the ownership/control of the domain name to be included in the SSL/TLS cert. As per section 3 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices https://wiki.mozilla.org/CA:BaselineRequirements#CA_Conformance_to_the_BRs It is not sufficient to simply reference the section of the CA/Browser Forum's Baseline Requirements (BR) that lists the ways in which the CA may confirm that the certificate subscriber owns/controls the domain name to be included in the certificate. The CA's CP/CPS must specify which of those options the CA uses, and must include a reasonable description of the ways the CA can verify that the certificate subscriber owns/controls the domain name(s) to be included in the certificate. https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Domain_Name_Ownership	**Verified?**	Need Response From CA
EV SSL Verification Procedures	No EV request	**Verified?**	Not Applicable
Organization Verification Procedures	CP: Sections 3.2.2-3.2.3,3.2.5 CPS: Sections 3.2.2-3.2.5,3.2.7	**Verified?**	Verified
Email Address Verification Procedures	CP,CPS: Sections 3.2.2-3.2.3 NEED if Email trust bit requested... Sections of CP/CPS that sufficiently describe the verification steps that are taken to confirm the ownership/control of the email address to be included in the cert. As per section 4 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Email_Address_Control	**Verified?**	Need Response From CA
Code Signing Subscriber Verification Pro	Mozilla is no longer accepting requests to enable the Code Signing trust bit.	**Verified?**	Not Applicable
Multi-Factor Authentication	The multi-factor authentication mechanisms include username-password and USB-Key .The multi-factor authentication mechanisms apply to all accounts, including Root CA, SubCAs system and RA system.	**Verified?**	Verified
Network Security	CP, CPS: Section 6.7 SHECA maintains the network security controls which meets the CPA Canada WebTrustSM/TM for Certification Authorities WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security -Version 2.0.	**Verified?**	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	NEED URL to publicly disclosed subordinate CA certificates that chain up to certificates in Mozilla's CA program, as per Items #8, 9, and 10 of Mozilla's CA Certificate Inclusion Policy.	**Verified?**	Need Response From CA

Root Case Record # 2

Root Case Information

Root Certificate Name	UCA Extended Validation Root	**Root Case No**	R00000135
Request Status	Information Verification In Process	**Case Number**	00000083

Certificate Data

Certificate Issuer Common Name	UCA Extended Validation Root
O From Issuer Field	UniTrust
OU From Issuer Field	
Valid From	2013 Mar 28
Valid To	2038 Dec 31
Certificate Serial Number	79d26410e23fbd258f6ea2b11853db30
Subject	CN=UCA Extended Validation Root, OU=null, O=UniTrust, C=CN
Signature Hash Algorithm	sha1WithRSAEncryption
Public Key Algorithm	RSA 4096 bits
SHA-1 Fingerprint	B9:C9:F5:8B:3B:BE:F5:75:E2:B5:83:28:77:0E:7B:00:76:C4:0B:5E
SHA-256 Fingerprint	2C:E0:D4:0F:6D:D2:AB:24:63:40:33:4D:A2:A1:E5:2D:AD:63:79:F4:18:F8:9E:0F:B7:7A:C3:9A:6F:CB:DD:7B
Certificate Fingerprint	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	http://www.sheca.com/download/getdownloadforpdf/73	**Verified?**	Verified
CRL URL(s)	EV SSL certificates CRL http://ldap2.sheca.com/root/ucaevsub.crl	**Verified?**	Verified
OCSP URL(s)	http://ocsp3.sheca.com/ocsp/sheca/sheca.ocsp	**Verified?**	Verified
Trust Bits	Websites	**Verified?**	Verified
SSL Validation Type	EV	**Verified?**	Verified
EV Policy OID(s)	1.2.156.112570.1.1.3	**Verified?**	Verified
Root Stores Included In	Microsoft	**Verified?**	Verified
Mozilla Applied Constraints	None	**Verified?**	Verified

Test Websites or Example Cert

Test Website URL (SSL) or Example Cert	https://ef-gb.wwwtrust.org/	**Verified?**	Need Response From CA
Test Website - Expired			

Test Website - Revoked	

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

Revocation Tested	No Error	**Verified?**	Verified
CA/Browser Forum Lint Test	Certificate not found	**Verified?**	Verified
Test Website Lint Test	Test not currently available	**Verified?**	Not Applicable
EV Tested	NEED: If EV treatment is being requested, then provide successful output from EV Testing as described here https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version	**Verified?**	Need Response From CA

CA Hierarchy Information

CA Hierarchy	CP Section 1.1.2 http://www.sheca.com/download/getdownloadforpdf/166	**Verified?**	Verified
Externally Operated SubCAs	None	**Verified?**	Verified
Cross Signing	None	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	Not Applicable	**Verified?**	Not Applicable

Verification Policies and Practices

Policy Documentation	NEED: Languages that the CP/CPS and other documents are provided in.	**Verified?**	Need Response From CA
CA Document Repository		**Verified?**	Need Response From CA
CP Doc Language	English		
CP	http://www.sheca.com/download/getdownloadforpdf/166	**Verified?**	Verified
CP Doc Language	English		
CPS	http://www.sheca.com/download/getdownloadforpdf/165	**Verified?**	Verified
Other Relevant Documents		**Verified?**	Not Applicable
Auditor Name	Auditor:PricewaterhouseCoopers (PWC)	**Verified?**	Verified
Auditor Website	www.pwc.com	**Verified?**	Verified
Auditor Qualifications	https://cert.webtrust.org/ViewSeal?id=2048	**Verified?**	Verified
Standard Audit	NEED: for all root inclusion/change requests. Reference section 2 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date		**Verified?**	Need Response From CA

BR Audit	NEED: If requesting Websites trust bit, then also need a BR audit as described here: https://wiki.mozilla.org/CA:BaselineRequirements	**Verified?**	Need Response From CA
BR Audit Type		**Verified?**	Need Response From CA
BR Audit Statement Date		**Verified?**	Need Response From CA
EV Audit	NEED only if requesting EV treatment	**Verified?**	Need Response From CA
EV Audit Type		**Verified?**	Need Response From CA
EV Audit Statement Date		**Verified?**	Need Response From CA
BR Commitment to Comply	NEED section in the CP/CPS that has the commitment to comply with the BRs as described in section 2.2 of version 1.3 of the CA/Browser Forum's Baseline Requirements.	**Verified?**	Need Response From CA
SSL Verification Procedures	CP: Sections 3.2.2-3.2.3,3.2.5 CPS: Sections 3.2.2-3.2.5,3.2.7 NEED: if Websites trust bit requested... Sections of CP/CPS that sufficiently describe the verification steps that are taken to confirm the ownership/control of the domain name to be included in the SSL/TLS cert. As per section 3 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices https://wiki.mozilla.org/CA:BaselineRequirements#CA_Conformance_to_the_BRs It is not sufficient to simply reference the section of the CA/Browser Forum's Baseline Requirements (BR) that lists the ways in which the CA may confirm that the certificate subscriber owns/controls the domain name to be included in the certificate. The CA's CP/CPS must specify which of those options the CA uses, and must include a reasonable description of the ways the CA can verify that the certificate subscriber owns/controls the domain name(s) to be included in the certificate. https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Domain_Name_Ownership	**Verified?**	Need Response From CA
EV SSL Verification Procedures	EV CP,EV CPS: Sections 3.2.2-3.2.3,3.2.5 NEED: If EV verification is performed, then provide URLs and section/page number information pointing directly to the sections of the CP/CPS documents that pertain to EV and describe the procedures for verifying the ownership/control of the domain name, and the verification of identity, existence, and authority of the organization to request the EV certificate. The EV verification documentation must meet the requirements of the CA/Browser Forum's EV Guidelines, and must also provide information specific to the CA's operations.	**Verified?**	Need Response From CA
Organization Verification Procedures	EV CP,EV CPS: Sections 3.2.2-3.2.3,3.2.5	**Verified?**	Verified
Email Address Verification Procedures	According to CP and CPS Section 3.2.6, CA doesn't provide Email Address Verification.	**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	The multi-factor authentication mechanisms include username-password and USB-Key .The multi-factor authentication mechanisms apply to all accounts, including Root CA, SubCAs system and RA system.	**Verified?**	Verified
Network Security	EV CP, EV CPS: Section 6.7 SHECA maintains the network security controls which meets the CPA Canada WebTrustSM/TM for Certification Authorities WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security-Version 2 .0.	**Verified?**	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	NEED URL to publicly disclosed subordinate CA certificates that chain up to certificates in Mozilla's CA program, as per Items #8, 9, and 10 of Mozilla's CA Certificate Inclusion Policy.	**Verified?**	Need Response From CA