Bugzilla ID:
Bugzilla Summary: Add SHECA Root Certificates

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	Shanghai Electronic Certification Authority Co., Ltd.(SHECA)
Website URL	www.sheca.com(Chinese)
Organizational type	Commercial
Primark Market / Customer Base	Shanghai Electronic Certification Authority Co., Ltd.(SHECA) is a Shanghai-based commercial company and is one of the biggest Certification Authorities in China. SHECA is a national recognized CA and operates under China's Electronic Signature Law. SHECA's customers include individuals and companies from mainland China, Taiwan and Hong Kong. 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; China citizens (individuals)or business corporations registered in mainland China
Impact to Mozilla Users	A large proportion of our customers are using Firefox as a daily browser, we really want our root certificates be included.
Inclusion in other major browsers	Yes. Our UCA Root and UCA Global Root are already included in Adobe , Microsoft and Chrome. And we are applying for Java and Opera.
CA Primary Point of Contact (POC)	POC direct email: xiongyuanyuan@sheca.com CA Email Alias: cuijiuqiang@sheca.com CA Phone Number: +86 021-36393199

Technical information about each root certificate

Info Needed	**Data1**	**Data2**
Certificate Name	UCA Global G2 Root	UCA Extended Validation Root
Certificate Issuer Field	CN = UCA Global G2 Root O = Shanghai Electronic Certification Authority Co., Ltd.. C = CN	CN = UCA Extended Validation Root O = Shanghai Electronic Certification Authority Co., Ltd.. C = CN
Certificate Summary	There are two subordinate CAs signed by "UCA Global G2 Root" issuing SSL certificates and code signing certificates.	There are two subordinate CAs signed by "UCA Extended Validation Root" issuing SSL certificates and code signing

		certificates.
Mozilla Applied Constraints	No limit.	No limit.
Root Cert URL	http://www.sheca.com/download/getdownloadforpdf/126	http://www.sheca.com/download/getdownloadforpdf/73
SHA1 Fingerprint	28 f9 78 16 19 7a ff 18 25 18 aa 44 fe c1 a0 ce 5c b6 4c 8a	a3 a1 b0 6f 24 61 23 4a e3 36 a5 c2 37 fc a6 ff dd f0 d7 3a
Valid From	2016-03-11	2015-03-13
Valid To	2040-12-31	2038-12-31
Certificate Version	3	3
Certificate Signature Algorithm	SHA256RSA	SHA256RSA
Signing key parameters	4096	4096
Test Website URL(SSL) Example Certificate (non-SSL)	https://ef-gb.wwwtrust.org	https://ef-EV.sheca.com
CRL URL	SHECA Global G3 SSL CRL http://ldap2.sheca.com/root/ucaglobalg2.crl SHECA Global G3 CodeSigning CRL http://ldap2.sheca.com/root/ucaglobalg2.crl	EV SSL certificates CRL http://ldap2.sheca.com/root/ucaevsub.crl EV Code signing certificates CRL http://ldap2.sheca.com/root/ucaevsub.crl
OCSP URL (Required now for end-entity certs)	http://ocsp3.sheca.com/ocsp/sheca/sheca.ocsp	http://ocsp3.sheca.com/ocsp/sheca/sheca.ocsp
Requested Trust Bits	Email(S/MIME),Websites(SSL/TLS) and Code Signing	Websites(SSL/TLS) and Code Signing
SSL Validation Type	OV	EV
EV Policy OID(s)	N/A	EV SSL server certificates policy OID: 1.2.156.112570.1.1.3 EV code signing certificates policy OID: 1.2.156.112570.1.1.3
Non-sequential serial numbers and entropy in cert	A 16-Byte(more than 20 bits) Random serial number is used in each end-entity certificate. Also entropy has been added to all the certificates.	A 16-Byte(more than 20 bits) Random serial number is used in each end-entity certificate. Also entropy has been added to all the certificates.
Response to Recent CA Communication(s)		

CA Hierarchy information for each root certificate

CA Hierarchy	See CP Section 1.1.2	See CP Section 1.1.2
Externally Operated SubCAs	None.	None.
Cross-Signing	None.	None.
Technical Constraints on Third-party Issuers	Not Applicable.	Not Applicable.

Verification Policies and Practices

Policy Documentation	CP : http://www.sheca.com/download/getdownloadforpdf/162 CPS: http://www.sheca.com/download/getdownloadforpdf/160	EV CP: http://www.sheca.com/download/getdownloadforpdf/166 EV CPS: http://www.sheca.com/download/getdownloadforpdf/165
Audits	Audit Type: WebTrust for CA Auditor: PWC Auditor Website:www.pwc.com URL to Audit Report and Management's Assertions: https://cert.webtrust.org/ViewSeal?id=2045 https://cert.webtrust.org/ViewSeal?id=2047	Audit Type: WebTrust for CA Auditor: PWC Auditor Website:www.pwc.com URL to Audit Report and Management's Assertions: https://cert.webtrust.org/ViewSeal?id=2048
Baseline Requirements (SSL)	See point-in-time audit report attached.	See point-in-time audit report attached.
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	EV CP,EV CPS: Sections 3.2.2-3.2.3,3.2.5
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	EV CP,EV CPS: Sections 3.2.2-3.2.3,3.2.5
Email Address Verification Procedures	CP,CPS: Sections 3.2.2-3.2.3	According to CP and CPS Section 3.2.6, we don't provide Email Address Verification.
Code Signing Subscriber Verification Procedures	CP: Sections 3.2.2-3.2.3,3.2.5 CPS: Sections 3.2.2-3.2.5,3.2.7	EV CP,EV CPS: Sections 3.2.2-3.2.3,3.2.5
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.	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.

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.	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.

Response to Mozilla's CA Recommended Practices (https://wiki.mozilla.org/CA:Recommended_Practices)

Publicly Available CP and CPS	See above.	See above.	
CA Hierarchy	See above.	See above.	
Audit Criteria	See above.	See above.	
Document Handling of IDNs in CP/CPS	CP: section 3.2.2-3.2.3 CPS: section 3.2.5	EV CP, EV CPS: section 3.2.2	
Revocation of Compromised Certificates	CP: Section 5.7.3 CPS: Section 5.8.3	EV CP,EV CPS: Section 5.7.3	
Verifying Domain Name Ownership	See above.	See above.	
Verifying Email Address Control	See above.	See above.	
Verifying Identity of Code Signing Certificate Subscriber	See above.	See above.	
DNS names go in SAN	All DNS names go into SAN, and one primary DNS name maybe go into the Subject Common Name.	All DNS names go into SAN, and one primary DNS name maybe go into the Subject Common Name.	
Domain owned by a Natural Person	See above.	See above.	
OCSP	CP, CPS: Section 7.3	EV CP, EV CPS: Section 7.3	

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

Long-lived DV certificates	Not applicable, SHECA does not issue any Long-lived DV certificates.	Not applicable, SHECA does not issue any Long-lived DV certificates.
Wildcard DV SSL certificates	Not applicable, SHECA does not issue any Wildcard DV SSL certificates.	Not applicable, SHECA does not issue any Wildcard DV SSL certificate.
Email Address Prefixes for DV Certs	Not applicable.	Not applicable.
Delegation of Domain / Email validation to third parties	Not applicable. SHECA doesn't delegate any business part to third parties.	Not applicable. SHECA doesn't delegate any business part to third parties.

Issuing end entity certificates directly from roots	Not applicable.	Not applicable.
Allowing external entities to operate subordinate CAs	Not allowed.	Not allowed.
Distributing generated private keys in PKCS#12 files	Not support.	Not support.
Certificates referencing hostnames or private IP addresses	Not applicable. SHECA does not issue certificates of this type.	Not applicable. SHECA does not issue certificates of this type.
Issuing SSL Certificates for Internal Domains	Not applicable.	Not applicable.
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.	OCSP Responses are signed by a certificate under the corresponding issuer of the supplied certificate in OCSP Requests.
SHA-1 Certificates	This root does not issue any SHA-1 Certificates.	This root does not issue any SHA-1 Certificates.
Generic names for CAs	Not applicable.	Not applicable.
Lack of Communication With End Users	SHECA provides customer server hotline, email and official website to general publics including subscriber, relying parties.	SHECA provides customer server hotline, email and official website to general publics including subscriber, relying parties.
Backdating the notBefore date	No backdating of notBefore date – Certificates are valid from the issuing day.	No backdating of notBefore date – Certificates are valid from the issuing day.