Response to Mozilla's list of Recommended Practices

3)Audit Criteria

PWC performs WebTrust auditing for SHECA annually based on the Criteria for Certification Authorities Version 2.0 as well as other criterias including but are not limited to 'Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates', 'Baseline Requirements for the Issuance and Management Of Publicly-Trusted Code Signing Certificates', 'Guidelines For The Issuance And Management Of Extended Validation Certificates', 'Guidelines For The Issuance And Management Of Extended Validation Code Signing Certificates' and 'NETWORK AND CERTIFICATE SYSTEM SECURITY REQUIREMENTS'.

As for Auditing Reports and Management's Assertions, please see:

https://cert.webtrust.org/SealFile?seal=2045&file=pdf

6)Verifying Domain Name Ownership

CPS: Sections 3.2.5

7)Verifying Email Address Control

CPS: Sections 3.2.8

10） Domain owned by a Natural Person

SHECA doesn't issue certificate to a Natural Person.

12） Network Security Controls

CP, CPS: Section 6.7 & EV CP, EV CPS: Section 6.7

SHECA takes effective controls for risk. Besides PWC performs WebTrust audit for SHECA according to the AICPA/CICA Trust Services Principles and Criteria for Certification Authorities Version 2.0 and 'NETWORK AND CERTIFICATE SYSTEM SECURITY REQUIREMENTS'.

Response to Mozilla's list of Potentially Problematic Practices

1)Long-lived DV certificates:No, SHECA doesn't issue DV certificates.

2)Wildcard DV SSL certificates: No, SHECA doesn't issue DV certificates.

3)Email Address Prefixes for DV Certs: No, SHECA doesn't issue DV certificates.

4)Delegation of Domain/Email validation to third parties:No, SHECA doesn't delegate validation to any third party.

5)Issuing end entity certificates directly from roots:No.

6)Allowing external entities to operate subordinate CAs:No.
7)Distributing generated private keys in PKCS#12 files:No. CPS6.2.3
8)Certificates referencing hostnames or private IP addresses:No.
9)Issuing SSL Certificates for Internal Domains:No.
10)OCSP Responses signed by a certificate under a different root:No.OCSP Respnses signed by a certificate under the same root.
11)SHA-1 Certificate:SHECA doesn't issue SHA-1 certificate.
12)Generic names for CAs:No.
13)Lack of Communication With End Users: SHECA is contactable by, and accept and act upon complaints made by, those relying on their assertions of identity and is responsive to members of the general public, including people who have not purchased products from SHECA.
14)Backdating the notBefore date:No. All certificates issued by SHECA are valid from the issuing day.

Verification Policies and Practices

Certificate Name	UCA Global G2 Root	UCA Extended Validation Root
Policy Documentation	CP(Chinese Version) : http://www.sheca.com/download/getdownloadforpdf/187 CP(English Version) : http://www.sheca.com/download/getdownloadforpdf/188 CPS(Chinese Version) : http://www.sheca.com/download/getdownloadforpdf/183 CPS (English Version): http://www.sheca.com/download/getdownloadforpdf/184	EV CP(Chinese Version) : http://www.sheca.com/download/getdownloadforpdf/189 EV CP(English Version): http://www.sheca.com/download/getdownloadforpdf/190 EV CPS(Chinese Version) : http://www.sheca.com/download/getdownloadforpdf/185 EV CPS(English Version): http://www.sheca.com/download/getdownloadforpdf/186
CA Document Repository	http://www.sheca.com/policy	http://www.sheca.com/policy
Standard Audit	https://cert.webtrust.org/SealFile?seal=2048&file=pdf	https://cert.webtrust.org/SealFile?seal=2048&file=pdf
Standard Audit	May27,2016	May27,2016

Statement Date		
BR Audit	https://cert.webtrust.org/SealFile?seal=2048&file=pdf	https://cert.webtrust.org/SealFile?seal=2048&file=pdf
BR Audit Type	WebTrust	WebTrust
BR Audit Statement Date	May27,2016	May27,2016
EV Audit	NA	https://cert.webtrust.org/SealFile?seal=2048&file=pdf
EV Audit Type	NA	WebTrust
EV Audit Statement Date	NA	May27,2016
BR Commitment to Comply	CPS:Section1.1 SHECA conforms to the latest version of CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly – Trusted Certificates published at www.cabforum.org.	CPS:Section1.1 SHECA conforms to the latest version of CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly – Trusted Certificates published at www.cabforum.org.
SSL Verification Procedures	CPS: Sections 3.2.2-3.2.8,3.2.11 Prior to the issuance of an SSL certificate, SHECA performs the verification of ownership of the domain name and the identity,existence,and authority of the organization to request the certificate by : 1. obtaining a signed Authorization Letter provided by the Domain Name Register 2. checking through Whois if the Applicant is the entity to whom the domain name is registered and if the information recorded is in accordance with what is presented by the Applicant; if the Applicant is not the registrant of the domain, a valid Domain Authorization	NA

	Letter for the requested domain must be presented; 3. verifying the organization identity through business registration repositories or taxation registration reporsitories; 4. obtaining a signed Organization Authorization Letter;	
EV SSL Verification Procedures	NA	EV CP,EV CPS: Sections 3.2.2-3.2.6,3.2.9 Prior to the issuance of an EV Server certificate, SHECA performs the verification of ownership of the domain name and the identity,existence,and authority of the organization to request the EV certificate by : 1. obtaining a signed Authorization Letter provided by the Domain Name Register 2. checking through Whois if the Applicant is the entity to whom the domain name is registered and if the information recorded is in accordance with what is presented by the Applicant; if the Applicant is not the registrant of the domain, a valid Domain Authorization Letter for the requested domain must be presented; 3. verifying the organization identity through business registration repositories or taxation registration reporsitories, and checking the detail business and operation information presented in the record or checking the physical place in person; 4. obtaining a signed Organization Authorization Letter;
Email Address Verification	Not requesting Email trust bit.	Not requesting Email trust bit.

Procedures		

Test Websites or Example Cert

Certificate Name	UCA Global G2 Root	UCA Extended Validation Root
Test Website URL(SSL) Example Certificate (non-SSL)	https://ef-gb.wwwtrust.org https://ex-gb.wwwtrust.org https://re-gb.wwwtrust.org	https://ef-EV.sheca.com https://ex-EV.sheca.com https://re-EV.sheca.com

Link to Publicly Disclosed and Audited subordinate CA Certificates

Certificate Name	UCA Global G2 Root	UCA Extended Validation Root
Publicly Disclosed & Audited subCAs	http://www.sheca.com/download/getdownloadforpdf/127	http://www.sheca.com/download/getdownloadforpdf/193