UniTrust Network Trust Service Hierarchy

Extended Validation Certification Practice Statement

Version 1.5.5

Valid from: July 21, 2023

Shanghai Electronic Certificate Authority Center Co.Ltd

18/F,JiaJie International Plaza, No.1717,North Sichuan Road, Shanghai,China

UniTrust Network Trust Service Hierarchy Extended Validation Certification Practice Statement

This Certification Practice Statement shall be executed in Chinese and English language in case of any discrepancy the Chinese text shall prevail.

Address: 18th. Floor, Jia Jie International Plaza, No. 1717, North Sichuan Road, 200080, Shanghai

Tel: 86-21-36393197

E-mail: policy@sheca.com

Brand Explanation

"UniTrust" and "协卡" are registered trademark of Shanghai Electronic Certificate Authority Center Co.Ltd, which are also the service identification of SHECA.

Changing History Record of this document

Version	Valid date	Author	Issuer	Notes
V1.5.5	07-21-2023	Celia Yu	SHECA Security Authentication Committee	Current Version
V1.5.4	06-12-2023	Celia Yu	SHECA Security Authentication Committee	Previous Version
V1.5.3	04-18-2023	Celia Yu	SHECA Security Authentication Committee	Previous Version
V1.5.2	04-18-2022	Toria Chen	SHECA Security Authentication Committee	Previous Version
V1.5.1	11-15-2021	Toria Chen	SHECA Security Authentication Committee	Previous Version
V1.5	06-18-2021	Toria Chen	SHECA Security Authentication Committee	Previous Version
V1.4.9	04-29-2021	Toria Chen	SHECA Security Authentication Committee	Previous Version
V1.4.8	08-11-2020	Toria Chen	SHECA Security Authentication Committee	Previous Version
V1.4.7	06-05-2020	Toria Chen	SHECA Security Authentication Committee	Previous Version
V1.4.6	04-30-2020	Toria Chen	SHECA Security Authentication Committee	Previous Version
V1.4.5	03-27-2020	Toria Chen	SHECA Security Authentication Committee	Previous Version
V1.4.4	05-29-2019	Toria Chen	SHECA Security Authentication Committee	Previous Version
V1.4.3	10-09-2018	Toria Chen	SHECA Security Authentication Committee	Previous Version
V1.4.2	31-08-2018	Toria Chen	SHECA Security Authentication Committee	Previous Version
V1.4.1	11-07-2018	Toria Chen	SHECA Security Authentication Committee	Previous version
V1.4	01-06-2018	Toria Chen	SHECA Security Authentication Committee	Previous version
V1.3	24-05-2017	Ruby Xiong	SHECA Security Authentication Committee	Previous version

V1.2	25-05-2016	John Cui	SHECA Security Authentication Committee	Previous version
V1.1	25-04-2014	John Cui	SHECA Security Authentication Committee	Previous version
V1.0	28-04-2013	John Cui	SHECA Security Authentication Committee	Previous version

Changes Description

Version	Description
V1.5.5	Disclosure of newly issued Sub-CAs Xinnet DV SSL /Xinnet OV SSL
V1.5.4	Information of reissued corss-signed UCA Global Root G2
V1.5.3	Disclosure of newly issued Sub-CAs SHECA OV Server CA G7; Update Sub-CAs status; Update CRL/ARL renewal cycle
V1.5.2	Disclosure of newly issued Subordinate Root CECloud Secure Server CA V1
V1.5.1	Information about disable partial Subordinate Roots Disclose special domain validation rules of China e-government extranet
V1.5	Update ARL renewal cycle Revise key length requirement of Code Signing and Timestamp certificate
V1.4.9	Disclosure of newly issued Sub-CAs Delete outdated domain validation method listed in section 3.2.4.1 2(8),(9) of last version
V1.4.8	Disclosure of LDAP address Power supply of server room
V1.4.7	Information of new Root UniTrust Global Root CA R1, UniTrust Global Root CA R2; Information of Root newly used for issuing EV certificates, UCA Global G2 Root Revise revocation mechanism
V1.4.6	Delete outdated domain validation method listed in section 3.2.5 2(3) of last version Revise revocation mechanism Add an initial investigation reporting mechanism
V1.4.5	Information of new cross-signed UCA Global G2 Root Certificate validity changed Certificate domain validation method changed
V1.4.4	Information of new root certificate UniTrust PTC Root CA R1, UniTrust PTC Root

	CA R2 Added Reason for Revoking Code Signing Certificate
V1.4.3	Added Changes Description
V1.4.2	Revise EV Certificate hierarchical structure Chart; Fix some translation errors
V1.4.1	Revised Data Source Accuracy, stated the 825 validity; IP Address Recognition and Identification; CAA Record Checking Requirement
V1.4	Modified UniTrust Network Trust Service Hierarchy; Added Object Identifier (OID); Modified Validation of Domain Name
V1.3	Revised Revocation Request Process and Who Can Request Revocation
V1.2	Revised Key Pair and Certificate Usage
V1.1	Added the Situation of Certificate Revocation Modified Revocation Process Added Appendix C CRL Format
V1.0	N.A.

Statements

The Certification Practice Statement (CPS) endorses in whole or in part the following standards:

Guidelines for the Issuance and Management of Extended Validation Certificates

RFC3647, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework.

RFC2459, Internet X.509 Public Key Infrastructure: Certificate and CRL Properties.

RFC2560, Internet X.509 Public Key Infrastructure: Online Certificate Status Protocol-OCSP.

ITU-T X.509 V3(1997): Information technology- Open Systems Interconnection- The Directory: Public-key and attribute certificate frameworks.

RFC5280, Internet X.509 Public Key Infrastructure: Certificate and CRL Profile.

GB/T 20518-2006: Information security technology- Public Key Infrastructure-Digital Certificate Format.

This CPS has been handed to the independent auditor for assessment. The auditing assessment report will be published on www.sheca.com and other corresponding website.

Table of Contents

1. Introduction

This document is the UniTrust Network Trust Service Hierarchy Extended Validation Certification Practice Statement (UNTSH EV CPS) of UniTrust Network Trust Service Hierarchy. UniTrust Network Trust Service Hierarchy is a Public Key Infrastructure established and operated by Shanghai Electronic Certification Authority Co., ltd, (SHECA), providing electronic authentication service based on digital certification. SHECA is the third party certification authority established according to 'Electronic Signature Law of People's Republic of China', devoted itself to creating harmonious network trust environment, providing secure, reliable and credible digital certification service.

UNTSH EV CPS explains the specific requirements SHECA shall obey when providing the certificate services that include, but not limited to, issuing, managing, revoking, and renewal certificate. UNTSH EV CPS is formulated by UniTrust Network Trust Service Hierarchy Extended Validation Certificates Policies (UNTSH EV CP), following the rule of 'Electronic Signature Law of People's Republic of China' and the requirements of UNTSH EV CP.

UNTSH CP is the principal statement of policy governing the UNTSH. It establishes the business, legal, and technical requirements for approving, issuing, managing, using, revoking, and renewing, digital Certificates within UNTSH and providing associated trust services. These requirements protect the security and integrity of the UNTSH EV Certificate, apply to all UNTSH EV Participants, and thereby provide assurances of uniform trust throughout the UNTSH EV. More information is available in UNTSH EV CP.

UNTSH operated by SHECA, contains users, subscribers and relying parties subjected to it. While the UNTSH EV CP sets forth requirements that UNTSH EV Participants must meet, this CPS describes the practices how SHECA and participants meet these requirements:

- securely managing the core infrastructure that supports the UNTSH, and
- issuing, managing, revoking, and renewing UNTSH EV Certificates in accordance with the requirements of the CP

This CPS conforms to RFC 3647 for Certificate Policy and Certification Practice Statement construction, also conforms to the current version of the CA/Browser Forum (CA/BROWSER FORUM) requirements published at www.cabforum.org including:

- Guidelines for the Issuance and Management of Extended Validation (EV) Certificates
- Guidelines for the Issuance and Management of Extended Validation (EV) Code-Signing Certificates
- Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates

In the event of any inconsistency between this document and those Requirement, those Requirements take precedence over this document. The EV Certificates SHECA issued under UNTSH EV CP conform to the CA/BROWSER FORUM Requirements. SHECA assert that all Certificates issued containing UNTSH EV CP and CPS identifier(s) are issued and managed in conformance with the CA/Browser Forum Requirements.

1.1 Overview

This CPS sets forth procedures which SHECA should follow to issue certificate, according to Guidelines for Extended Validation Certificates published by CA/Browser Forum which set forth the minimum requirements.

The CPS applies to EV ROOT CA, EV SSL CA, and EV Codesigning CA within UNTSH and related user, subscriber and replying party, etc. The CPS, as a single document, covers practices and procedures concerning the issuance and management of all EV Certificates. SHECA may publish Certificate Practices Statements that are supplemental to this CPS in order to conform to the specific policy requirements of Government, or other industry standards and requirements. These supplemental certificate policies shall applicable to subscribers for the certificates issued under the supplemental policies and their relying parties. The CPS is only one of a set of documents relevant to UNTSH. These other documents include:

- Subscriber Agreement

- CA/RA Operation Standard
- Relying Party Agreement
- Assessment and Audit Standard
- Other Related Agreement and Standard

The object of EV certificates which issued in accordance with the CPS, is various organizations applied for EV Certificate and validated the identity by SHECA. All UNTSH EV Certificate subscriber and relying party must decide how to use and trust certificate correspond related provisions of this CPS and CP.

EV SSL Certificates are used on the Internet SSL / TLS authentication, aiming to establish a secure communications pipeline through SSL/TLS protocol. The owner of the certificate may be displayed in a specific way, enabling the users to confirm the website is controlled by a trusted entity.

The primary purpose of EV SSL Certificate is to identify the legal identity that controls a website (EV SSL Certificate contained information such as institution name, business address, registered institution and registered code, etc., could reasonable guarantee that the website visited is owned and controlled by a legal entity), and enable encrypted channel (data encryption and transfer between user browser and website).

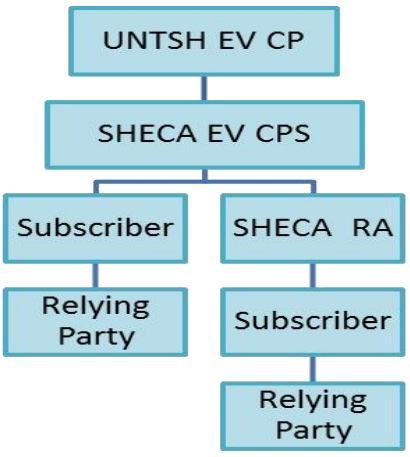
Secondly, by confirming an entity's legal and existence in reality, the EV Certificate help the entity get a legality statement to operate a website, while assist in proving solution to phishing and other forms of online fraud (making phishing and online identity fraud used SSL certificate more difficult, and can also assist in law enforcement investigation of phishing and other forms of online fraud).

In addition, EV SSL certificates only concerns the identity of the subject named in the certificate, not the subject's behavior. EV SSL Certificate do not provide any guarantee, statement or warranties on whether the entity is comply with law, regulation requirements, business integrity and the security of the business.

1.1.1 UNTSH Structure

The CPS is formulated in accordance with UNTSH EV CP. RA perform certificate application identification in comply with the CPS. Subscriber, relying party and related entities use and trust certificate in accordance with this CPS and EV CP while performing obligations.

UNTSH contains a root CA, subordinate CA, registration authority (RA), these entities are different service providers within UNTSH. EV Certificate services and management within UNTSH should complete, accurate and comprehensive meet the requirement of CPS and EV CP.



1.1.2 UNTSH EV Certificate hierarchical structure

UNTSH consists of six EV ROOT CAs

- UCA Global G2 Root

The length of UCA Global G2 Root's root key is 4096-bit, UCA Global G2 Root will expire on December 31, 2040 and will no longer issue any subordinate certificates since January 1, 2036.

Asseco Data System S.A.'s Root CA namely Certum Trusted Network CA issued a cross signing Root CA UCA Global G2 Root on Feburary 21th,2020, with validity from Feburary 21,2020 to Feburary 21,2025,which was revoked on 28 April 2023.

On 28 March 2023, Asseco Data Systems S.A.'s Root CA namely Certum Trusted Network CA reissued the cross-root certificate UCA Global G2 Root, valid from 28 March 2023 to 21 February 2025.

UCA Global G2 Root have 10 sub-CAs in use, 2 disabled sub-CAs, and 4 revoked sub-CAs.

Subordinate CA	Key Algorithm /length	Signing Algorithm	Issuing Certificates	Status
SHECA RSA Code Signing CA G3	RSA /2048	SHA-256 with RSA Encryption	Code Signing Certificates	Revoked
SHECA RSA Domain Validation Server CA G3	RSA /2048	SHA-256 with RSA Encryption	DV SSL Certificates	
SHECA RSA Organization Validation Server CA G3	RSA /2048	SHA-256 with RSA Encryption	OV SSL Certificates	
SHECA RSA Time Stamp Authority G1	RSA /2048	SHA-256 with RSA Encryption	Time Stamp Certificates	
SHECA SMIME CA G1	RSA /2048	SHA-256 with RSA Encryption	SMIME Certificates	In Use
SHECA DV Server CA G5	RSA / 2048	SHA-256 with RSA Encryption	DV SSL Certificates	
SHECA OV Server CA G5	RSA / 2048	SHA-256 with RSA Encryption	OV SSL Certificates	
SHECA EV Server CA G2	RSA / 2048	SHA-256 with RSA Encryption	EV SSL Certificates	
SHECA Code Signing CA G4	RSA / 3072	SHA-256 with RSA Encryption	Code Signing Certificates	
SHECA Time Stamping CA G2	RSA / 3072	SHA-256 with RSA Encryption	Time Stamp Certificates	
TrustAsia RSA DV TLS CA - S1	RSA / 2048	SHA-256 with RSA Encryption	DV SSL Certificates	
TrustAsia RSA OV TLS CA - S1	RSA / 2048	SHA-256 with RSA Encryption	OV SSL Certificates	
Xinnet DV SSL	RSA / 2048	SHA-256 with RSA Encryption	DV SSL Certificates	
Xinnet OV SSL	RSA / 2048	SHA-256 with RSA Encryption	OV SSL Certificates	
SHECA Global G3 SSL	RSA / 2048	SHA-256 with RSA Encryption	SSL Certificates	Disabled
SHECA Global G3 Code Signing	RSA / 2048	SHA-256 with RSA Encryption	Code Signing Certificates	

- UCA Extended Validation Root

The length of UCA Extended Validation Root's root key is 4096-bit, will expire on December 31, 2038 and will no longer issue any subordinate certificates since January 1, 2034, under which are 8 sub-CAs.

Subordinate CA	Key Algorithm /length	Signing Algorithm	Issuing Certificates	Status
SHECA RSA Extended Validation Code Signing CA	RSA 2048	SHA-256 with RSA Encryption	EV Code Signing Certificates	Revoked

SHECA RSA Extended Validation Server CA	RSA 2048	SHA-256 with RSA Encryption	EV SSL Certificates	
SHECA OV Server CA G6	RSA 2048	SHA-256 with RSA Encryption	EV SSL Certificates	
SHECA EV Server CA G3	RSA 2048	SHA-256 with RSA Encryption	EV SSL Certificates	In Use
SHECA EV Code Signing CA G2	RSA 3072	SHA-256 with RSA Encryption	EV Code Signing Certificates	
SHECA OV Server CA G7	RSA 2048	SHA-256 with RSA Encryption	EV SSL Certificates	
SHECA Extended Validation SSL CA	RSA 2048	SHA-256 with RSA Encryption	EV SSL Certificates	Disabled
SHECA Extended Validation Code Signing CA	RSA 2048	SHA-256 with RSA Encryption	EV Code Signing Certificates	

- UCA Root SM2

The length of UCA Root SM2 root key is 256 bits, SM Signature with SM3 algorithm, UCA Root SM2 will expire on December 31, 2038 and will no longer issue any subordinate certificates since December 31, 2033,under which are 8 sub-CAs,

Subordinate CA	Key Algorithm /length	Signing Algorithm	Issuing Certificates	Status
UniTrust DV Secure Server	SM2 256	SM2 Signature with SM3	SM2 DV SSL Certificates	In Use
UniTrust OV Secure Server	SM2 256	SM2 Signature with SM3	SM2 OV SSL Certificates	
SHECA SM2	SM2 256	SM2 Signature with SM3	Individual Identity Certificate Organization Identity Certificate Device Certificate	
TrustAsia SM2 DV TLS CA - S1	SM2 256	SM2 Signature with SM3	SM2 DV SSL Certificates	
TrustAsia SM2 OV TLS CA - S1	SM2 256	SM2 Signature with SM3	SM2 OV SSL Certificates	
TrustAsia SM2 Identity CA - S1	SM2 256	SM2 Signature with SM3	Individual Identity Certificate Organization Identity Certificate	
SHECA SM2 Identity CA G1	SM2 256	SM2 Signature with SM3	Individual Identity Certificate	
CECloud Secure Server CA V1	SM2 256	SM2 Signature with SM3	SM2 SSL Certificates	

- UniTrust Global Root CA R1

The UniTrust Global Root CA R1 root key is 4096 bits, with RSA and SHA-384,. UniTrust Global Root CA R1 will expire on April 28, 2045 and on longer issue any subordinate certificates since April 28, 2040, which has 6 sub-CAs.

Subordinate CA	Key Algorithm /length	Signing Algorithm	Issuing Certificates	Status
SHECA DV Server CA 1A	RSA / 4096	SHA-384 with RSA Encryption	DV SSL Certificates	Ceased
SHECA OV Server CA 1A	RSA / 4096	SHA-384 with RSA Encryption	OV SSL Certificates	
SHECA EV Server CA 1A	RSA / 4096	SHA-384 with RSA	EV SSL Certificates	

		Encryption		
SHECA Code Signing CA 1A	RSA / 4096	SHA-384 with RSA Encryption	Code Signing Certificates	
SHECA EV Code Signing CA 1A	RSA / 4096	SHA-384 with RSA Encryption	EV Code Signing Certificates	
SHECA Time Stamping CA 1A	RSA / 4096	SHA-384 with RSA Encryption	Time Stamp Certificates	

- UniTrust Global Root CA R2

The UniTrust Global Root CA R2 root key is 384 bits, with ECDSA with ECDSA SHA-384. UniTrust Global Root CA R2 will expire on April 30, 2045 and no longer issue any subordinate certificates since April 20, 2040, which has 3 sub-CAs.

Subordinate CA	Key Algorithm /length	Signing Algorithm	Issuing Certificates	Status
SHECA DV Server CA 2A	ECC / NIST P-384	ECDSA Signature with SHA-384	ECC DV SSL Certificates	Ceased
SHECA OV Server CA 2A	ECC / NIST P-384	ECDSA Signature with SHA-384	ECC OV SSL Certificates	
SHECA EV Server CA 2A	ECC / NIST P-384	ECDSA Signature with SHA-384	ECC EV SSL Certificates	

- UniTrust Global Root CA R3

The UniTrust Global Root CA R2 root key is 256 bits, with SM2 with SM3. UniTrust Global Root CA R2 will expire on April 30, 2045 and no longer issue any subordinate certificates since April 20, 2040, which has 3 sub-CAs.

Subordinate CA	Key Algorithm /length	Signing Algorithm	Issuing Certificates	Status
SHECA DV Server CA 2A	ECC / NIST P-384	ECDSA Signature with SHA-384	SM DV SSL Certificates	Ceased
SHECA OV Server CA 2A	ECC / NIST P-384	ECDSA Signature with SHA-384	SM OV SSL Certificates	
SHECA EV Server CA 2A	ECC / NIST P-384	ECDSA Signature with SHA-384	SM EV SSL Certificates	

1.1.3 UNTSH EV Certificate Trust Hierarchy

UNTSH EV Subscriber Certificate issued has been performed strict identity validation by CA. All applicants are required to provide supporting documentation to SHECA to validate the reality. UNTSH do not issue EV Certificate to natural personal.

Judging from the level of confidence, EV subscriber certificates is consistent in trust, no differences in security levels.

1.2 Document Name and Identification

This document is UniTrust Network Trust Service Hierarchy Extended Validation Certification Practice Statement, abbreviated as UNTSH EV CPS.

The CPS object identifier (OID) is consistent with the OID of UniTrust Network Trust Service Hierarchy Extended Validation Certificates Policy (UNTSH EV CP), SHECA no longer assign an specialized object identifier (OID) to UNTSH EV CPS.

1.3 PKI Participants

1.3.1 Certification Authorities (CA)

The term Certification Authority (CA) is an umbrella term that refers to EV Root CA, EV SSL CA and EV Code signing CA, constructed and operated by SHECA. In addition, SHECA established Security Authentication Committee as the policy management administration of UNTSH.

(1) EV Root CA

EV Root CA is the highest certificate issuing authority, the trusted root of EV certificate in UNTSH. Its main responsibilities include:

- issue and manage root certificates and subordinate CA certificates
- manage and distribute relevant certificates, certificate revocation lists (CRL)
- manage and operate certificate repository

(2) EV SSL CA

The primary duties of EV SSL CA include:

- issue and manage subscriber EV SSL Certificates
- manage and distribute relevant subscriber certificates and certificate revocation list (CRL)
- manage and operate certificate repository

(3) EV Code signing CA

The primary duties of EV Code signing CA include:

- issue and manage subscribers EV Code signing certificates
- manage and distribute relevant subscriber certificates and certificate revocation list (CRL)
- manage and operate certificate repository

(4) Security Authentication Committee

SHECA Security Authentication Committee is policy management administration of UNTSH. Its major responsibilities include:

- Develop and publish Certificate Policy (CP)
- Develop and publish Certificate Practice Statement (CPS)
- Develop and publish operations standards
- Develop and publish service standards
- Supervise and guide operational services within UNTSH

1.3.2 Registration Authorities (RA)

A Registration Authority (RA) is an entity that performs identification and authentication of certificate applicants for subscriber EV Certificates, and performs information validation to assist CA in EV Certificate issuance.

SHECA, the EV Certificate Authority, serves as EV certificate RA itself without setting any other RA

1.3.3 Subscribers

Subscriber is a distinct entity name as the certificate subject which owns the EV Certificate and corresponding private key. The subscriber in this CPS refers to various organizations. SHECA only issues EV certificates to various organizations, but not to natural persons.

1.3.4 Relying Parties

A Relying Party is an individual or entity that uses the public key in certificate to verify the effectiveness of the entity's electronic signature. A Relying party may, or may not be a Subscriber within UNTSH.

Relying parties identify the domain name, the name of the software code and information about legal institutions according to the identity information contained in the certificate.

Relying parties should decide whether or not to trust the certificate or whether it can be used for specific purposes, based on the information contained in the certificate and considering the validation of certificate revocation information and so on.

1.3.5 Other Participants

Not applicable.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Usage

EV certificates issued by SHECA are mainly used to verify identity.

EV SSL Certificates, issued by the CPS, can be used to verify the identity of the domain name identified in the certificate, as well as the identity of the legal entity holding the domain name. EV Code signing certificate, issued by this CPS, can be used to verify the identity which providing or publishing the software. The information contained in EV certificates issued by SHECA is authentic, effective, and validated.

1.4.2 Prohibited Certificate Uses

Certificates shall be used only to the extent as described in Section 1.4.1. It is prohibited to use the EV Certificate in applications or business which may result in any personal injury or death, mental injury or hazards in the social order and public interests. EV Certificates shall be used only to the extent which is consistent with Electronic Signature Law and other applicable law.

CA Certificates shall not be used for any functions except CA functions. In addition, Subscriber Certificates shall not be used as CA Certificates.

1.5 Policy Administration

1.5.1 Organization Administering the Document

SHECA Security Authentication Committee is wholly responsible for developing, publishing, and modifying of CPS.

1.5.2 Contact Person

SHECA designated the Ministry of strategy development as the CPS contact, responsible for external communications of the CPS and other related matters. For any questions regarding this CPS, suggestions, questions, etc., you can contact the SHECA Ministry ofstrategy development.

Contact: Shanghai Electronic Certificate Authority Center Co.,Ltd Ministry of strategy development.

Tel : 86 -21-36393195

Fax : 86 -21-36393200

Address: 18th Floor, Jiajie International Plaza, No. 1717 North Sichuan Road, Shanghai, People's Republic of China

Postal Code: 200080

Email: policy@sheca.com

1.5.3 Person Determining CPS Suitability for the Policy

SHECA Security Authentication Committee determines the suitability and applicability of this CPS.

1.5.4 CPS Approval Procedures

Approval of this CPS and subsequent amendments shall be made by SHECA Security Authentication Committee.

According to 'Electronic Signature Law of People's Republic of China' and 'Electronic Authentication Service Management Policy', SHECA shall report to competent government organization after issuing the CPS.

1.6 Definitions and Acronyms

Refer to Appendix A.

2. Publication and Repository Responsibilities

2.1 Repositories

SHECA maintain repositories to enable the inquiry and download of corresponding information such as certificates, certificates revocation list (CRL), certification policy(CP), Certification Practice Statement(CPS), Related Agreements and Online Certificate Status Protocol (OCSP).

The website of repositories is https://www.sheca.com/repository

SHECA also offer the service of Online Certificate Status Protocol (OCSP) service.

2.2 Publication of Certificate Information

SHECA should public its CP, CPS, Subscriber Agreements, Relying Party Agreements, other agreements related to certificate usage and service, certificates, certificates revocation list and Online Certificate Status Protocol .,etc.

SHECA provide clear address and method. The certificates, certificate revocation lists and online status inquiry are released online, which is a part of Certificate Services.Once complete issurance,certificate will be published on the directory server ldap2.sheca.com, wich can be checked using specific tools. Users can also check and obtain a certificate by visiting https://www.sheca.com.

In addition, SHECA publishes certificate policy, certification practice statement, the related agreements in a fixed URL, .

2.3 Time or Frequency of Publication

This Certificate Policy shall be published through Repository on a 7x24 basis ,as soon as possible after the approval of SHECA Security Authentication Committee.

For subscriber certificates, SHECA should issue CRLs at least every 5 days, or within 24 hours after the subscriber certificate is revoked. The difference between the next update time (nextUpdate) field and this update time (thisUpdate) field of the subscriber certificate CRL must be less than or equal to 7 days.

For Sub-CA Certificates, a ARL should be published at least once every 6 months or within 24 hours after revoked. The difference between nextUpdate time (nextUpdate) and this update time (thisUpdate) of the root/intermediate root certificate ARL must be less than or equal to 10 months. If the root/Intermediate Root certificate is revoked, SHECA will publish the revocation information on the website.

2.4 Access control on repositories

Information published (include CP, CPS, Certificate, Certificate status and CRL) in the repository portion of the SHECA web site is publicly-accessible information. SHECA reserve the right to implement logical and physical security measures to prevent malicious access.

3. Identification and Authentication

3.1 Naming

3.1.1 Types of Names

EV Certificate name should comply with X.501 Distinguished Name (DN) guidance.

EV SSL Certificates and EV codesigning certificate naming rules and requirements must be recorded in the CPS and should in accordance with the requirements of part 9 in Guide publish by CA / Browser Forum on www.cabforum.org. Distinguished names of EV SSL Certificates and EV Code Signing certificate must contain the common name (CN =), the common name which has been verified should contain the domain name, email addresses, institution's legal name and etc.

- EV Subscribers Certificates Distinguished Names consist of the components specified in table below.

Name Prosperities	Explanation	If Required
Country (C)	Country Refers to the county name where the business operate	Y
Organization(O) Name	Organization Name Must be approved by government department	Y
Organization Unit(OU)	Name of department or subordinate unit	N
State or Province (S):	State or Province where the business operate	Y
Locality (L)	City Refer to the city where the business operate	Y
Common Name (CN)	Used to identify the subject in certificateEV SSL certificate: the domain name EV Codesigning certificate: institution name	Y

Business Category	Business Category Contains private organization, government organization, commercial entity, and non-commercial entity: • Private organization (V1.0,Cause 5.(b)) refers to individual business, individual-owned business, law firm and others lawfully registered and obtained the licenses. • Government organizationV1.0,Cause 5.(c) refer to government organizations and institution • Commercial entity V1.0,Cause 5.(d) refer to legally registered business entity • Non-commercial entity V1.0,Cause 5.(e) refer to social organization, non-government non-profit organization	Y
Jurisdiction Of Incorporation Local City Name	City name of Registered jurisdiction located	N
Jurisdiction Of Incorporation State Or Province Name	State, province, or autonomous region of Registered jurisdiction located	N
Jurisdiction Of Incorporation Country Name	Country of Registered jurisdiction of the located	N
Serial Number	Institution Registration Number Registration Number is assigned by Governance Department. If the institutions do not have the number, could fill the date of set up.	N
Street Address	Street address of the business premises	N
Postal Code	Postal Code of the business premises	N

- EV Root Distinguished Names is specified in table below

Distinguished Names （DN）	Explanation
Cuntry(C)	C=CN
Organization(O)	O=UniTrust
CommonNameCN)	CN= UCA Extented Validation root

- EV Server CA Certificate Distinguished Names is specified in below

Distinguished Name （DN）	Explanation
Country(C)	C=CN
Organization(O)	O= UniTrust
CommonName(CN)	CN= SHECA RSA Extended Validation Server CA

- EV Codesigning CA Certificate Distinguished Name is below

Distinguished Name （DN）	Explanation
Country(C)	C=CN
Organization(O)	O= UniTrust
CommonName(CN)	CN= SHECA RSA Extended Validation CodeSigning CA

3.1.2 Need for Names to be Meaningful

The distinguish name in the Subscriber certificate could identify the subject, domain name or the software Issuer, and could be distinguished by relying parties. Subject distinguished name should follow the requirements of law and rules.

3.1.3 Anonymity or Pseudonymity of Subscribers

Applicants are not permitted to use anonymity or pseudonyms when apply certificates.

3.1.4 Rules for Interpreting Various Name Forms

Various Name Forms in Subscribe Certificates are interpreted by ITU-T X.520 standards.

3.1.5 Uniqueness of Names

SHECA ensures that Subject Distinguished Name (DN) of the Subscriber is unique within the domain of UNTSH. It is possible for a Subscriber to have two or more certificates with the same Subject DN.

SHECA will verify the uniqueness of the Chinese and English name and domain name the applicants submit.

3.1.6 Solution of Naming Dispute

SHECA does not assume responsibility for the naming dispute during the certificate application. When there is a dispute, the subscriber should propose the application of solutions to judicial bodies or authorities by themselves.

Typically, when there is name dispute, SHECA solves it according to the manner of earlier application earlier serve.

3.1.7 Recognition, Authentication, and Role of Trademarks

If the trademark is in the certificate information, subscriber should provide documentary proof for SHECA trademark registration party, and this requirement is not and should not be considered that SHECA will judge and decide the ownership of the trademark.

SHECA respects the applicant's trademark and other intellectual property, but does not have the obligation to recognize and validate trademarks and other intellectual property rights.

Certificate Applicants are prohibited from using names in their Certificate Applications that infringe upon the Intellectual Property Rights of others. SHECA, however, does not verify whether a Certificate Applicant has Intellectual Property Rights in the name appearing in a Certificate Application, or otherwise resolve any dispute concerning the ownership of any domain name, or trademark. SHECA is entitled, without liability to any Certificate Applicant, to reject or suspend any Certificate Application because of such dispute.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

The public key and related private key of EV Certificate are produced by users.

The certificate applicant must demonstrate that it rightfully holds the private key corresponding to the public key to be listed in the Certificate. The method to prove possession

of a private key shall be PKCS #10, another cryptographically equivalent demonstration, or another SHECA-approved method.

3.2.2 Authentication of Organization Identity

SHECA EV certificate application service is only available to institutional subscribers. Institutional identity authentication and audit shall compliance with guidance published by CA / Browser Forum on www.cabforum.org. Meanwhile, according to Mozilla Verification Requirements, when certificate application contains internationalized domain names (IDNs), SHECA verifies the identity of owner of domain to detect whether the IDNs homographic spoofing occurs.

1. Identification requirements

EV certificates are only offered to government department, enterprises, institutions, social organizations and other institutions. The applicant organization must have the following roles:

- Certificate Requester: the handling personnel of the applying unit;
- Certificate Approver: the person in charge of the applicant unit;
- Contract Signer: The signer of the application agreement.

SHECA must identify and verify the following:

- Institutions must exist legally
- Certificate applicant's name and entity name are consistent
- Certificate Application operator must be authorized by applicant

2. Identification methods

(1) Identification of organization

- Verify relevant documents such as organization registration code certificate, industrial and commercial business license, social organizations registration certificate, registration certificate of other institutions, etc.
- Verify name, registration information and other information submitted by the applicant is consistent by inquiring third-party database
- Verify business operation location
- Verify telephone and other contact

(2) Identification of certificate application Operator

- Verify ID card, passports and other personal identity documents
- Verify bank card, phone bill and other evidence
- Verify the authorization documents certification
- confirm the identity and authority of the relevant personnel with HR department via telephone

(3) Domain name reorganization

- Verify the domain name holder information through "Whois".

(4) Separation of duties for EV authentication

- After all verification processes and procedures are completed, SHECA will have a person who is not responsible for collecting information to review all the information and documents collected to support the EV certificate application, and approve the issuance of the EV certificate.

3.2.3 Authentication of Individual Identity

SHECA does not accept any individual EV Certificates application.

3.2.4 Domain Recognition and Identification

If the certificate name is a domain name, SHECA requires the applicant to provide additional evidence material of domain name in addition to the written materials submitted by the applicant to audit. SHECA must proceed the following procedure while performing verification,

3.2.4.1. Validation of Domain Name

1. SHECA should confirm the requested domain name is not in the form of .onion. SSL Certificate issuance for a domain name in the form of .onion is not allowed by SHECA;

2. Authentication of domain name by one of the following methods:

(1). Validating the Applicant as a Domain Contact directly with the Domain Name Registrar. Provided that SHECA has:

a. Authenticated the Applicant's identity as required by the Baseline Requirements Section 3.2.2.1 or EV Guideline Section 11.2.

b. Authenticated the authority of the Applicant Representative/Certificate Approver as required by the Baseline Requirements section 3.2.5 or EV Guidelines Section 11.8.

c. Respectively, performed in accordance with BR Section 3.2.2.4.1;

d. Since August 1,2018, SHECA will stop use this method for validation and completed validations using this method will NOT be used for the issuance of certificates.

(2). Validating the applicant's control over the Domain Name by sending a Random Value via email, fax, SMS, or postal mail, to the Domain Contact and receiving a confirmation utilizing the Random Value, performed in accordance with BR Section 3.2.2.4.2;

(3).Constructed Email to Domain Contact establishing the Applicant's control over the FQDN by sending an e-mail including a Random Value created by using 'admin', 'administrator', 'webmaster', 'hostmaster' or 'postmaster' as the local part followed by the ("@") sign, followed by an Authorization Domain name, and receiving a confirming response using the Random Value, performed in accordance with BR Section 3.2.2.4.4;

(4). Relying upon a Domain Authorization Document that attests to the authority of the Applicant to request a Certificate for the Domain Name, provided that the Domain Authorization Document substantiates that it came from the Domain Contact and that (i) it is dated on or after the domain validation request or (ii) the WHOIS data has not materially changed since a previously provided Domain Authorization Document was provided, performed in accordance with BR Section 3.2.2.4.5;

Since August 1,2018, SHECA will stop use this method for validation and completed validations using this method will NOT be used for the issuance of certificates.

(5). An Agreed-Upon Change to the Website by the Applicant placing an agreed-upon Request Token or Request Value in the "/.well-known/pki-validation" directory, performed in accordance with BR Section 3.2.2.4.6;

(6). DNS Change by confirming the presence of a Random Value or Request Token in a DNS CNAME, TXT, or CAA record for either an Authorization Domain Name or an Authorization Domain Name prefixed with a label that begins with an underscore character, performed in accordance BR Section 3.2.2.4.7;

(7). IP Address - by confirming the Applicant's control over the FQDN through control of an IP address returned from a DNS lookup for A or AAAA records for the FQDN, performed in accordance with BR Section 3.2.2.4.8;

(8). For the domain names of Shanghai E-government Extranet, which are in form of "sh.cegn.cn", given the fact that Shanghai Big Data Center is the government administration of Shanghai E-government Extranet, that is to say the actual controller. SEHCA accept its official sealed application documents as the verification material.

The Random Value used in the methods listed above shall remain valid for no more than 30 days from its creation.

All of the above methods for validation, except No. 8 IP Address (BR Section 3.2.2.4.8) may be used for Wildcard Certificate Domain Name validation.

3.2.5 IP Address Recognition and Identification

If the certificate name is an IP address, SHECA requires the applicant to provide evidence of the IP address in addition to the written materials submitted by the applicant for verification. SHECA also needs to inquire of the appropriate IP address registrar service organization or other third-party database to determine whether the applicant has the right to use the IP address. SHECA must proceed the following procedure while performing verification,

1 SHECA should confirm the requested IP address is not a reserved IP address. EV SSL Certificate issuance for a reserved IP address is not allowed by SHECA.

2 SHECA must Confirm Applicant has control over the IP address by either:

1) Having the Applicant demonstrate practical control over the IP address by making an agreed - upon change to information found on an online Web page identified by a uniform resource identifier containing the IP address;

2) Obtaining documentation of IP address assignment from the Internet Assigned Numbers Authority (IANA) or a Regional Internet Registry (RIPE, APNIC, ARIN, AfriNIC, LACNIC); or

3) Performing a reverse - IP address lookup and then verifying control over the resulting Domain Name under Section 3.2.4..

3.2.6 Email Address Verification

When an email address is applied as one of the contents presented in the subject of the requested certificate, SHECA must verify the effectiveness and ownership of the email address before the issuance of the certificate. The verification process shows below,

1 After the applicant finishes and submits the CSR file, automation system of SHECA will perform detection to the CSR file, once an email address is detected, an email including a Random Value will be sent to the applicant. The Random Value shall be unique in each email.

2 The applicant must reply the email as a response with the Random Value to confirm the effectiveness and ownership of the email address.

3 SHECA receives the response and shall make sure the received Random Value is the same with the sent one.

The confirming email MAY be re-sent in its entirety, including the re-use of the Random Value, provided that its entire contents and recipient shall remain unchanged. The Random Value shall remain valid for use in a confirming response for no more than 30 days from its creation.

3.2.7 Data Source Accuracy

Prior to using any data source as a Reliable Data Source, SHECA evaluates the source for its reliability,

accuracy, and resistance to alteration or falsification. That is SHECA will consider the following during its evaluation:

1. The age of the information provided,
2. The frequency of updates to the information source,
3. The data provider and purpose of the data collection,
4. The public accessibility of the data availability, and
5. The relative difficulty in falsifying or altering the data.

Data source of EV SSL certificates required with re-verification as indicated by the EV Guidelines and/or EV Code Signing Guidelines.

3.2.8 Non-Verified Subscriber information

All the information about subscribers in EV Certificates should be verified.

3.2.9 Validation of Authority

Whenever an individual's name is associated with an Organization name in a certificate in such a way to indicate the individual's affiliation or authorization to act on behalf of the Organization:

- Determines that the Organization exists by using at least one third party identity proofing service or database, or alternatively, organizational documentation issued by or filed with the applicable government that confirms the existence of the organization, and
- Using telephone, confirmatory postal mail, or comparable procedure to verify the employment with the Organization of the individual submitting the Certificate Application and, when appropriate, his/her authority to act on behalf of the Organization.

3.2.10 Criteria for Inter-operation

No stipulation.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

As time goes on, the risk of private key lose and decipher increase. Subscriber should regularly re-key the certificate to ensure the security of the private key.

Subscriber should re-apply the certificate as descripted in Section 3.2 before the EV certificate expires.

3.3.2 Identification and Authentication for Re-key After Revocation

Subscriber should re-apply the certificate as descripted in Section 3.2 with re-generated key pair after the revocation of EV Certificate.

3.4 Identification and Authentication for Revocation Request

When the revocation has been requested by the Certificate's Subscriber, SHECA will verify the request by contacting the Certificate Application using the registered information.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application?

Any representative of an Organization or authorized agents can be the applicants of EV Certificates.

4.1.2 Enrollment Process and Responsibilities

EV certificate enrollment operations conform to the requirements issued by CA / Browser Forum (CA / Browser Forum) via www.cabforum.org .

Applicants should understand the subscriber agreement, agreed matters in CP and CPS, especially content with regard to the scope of the certificate, rights, obligations and guarantees.

Applicants should submit EV Certificate application form and the relevant evidential documents to SHECA, which means that the applicant has understood and accepted the above content.

Applicants should generate public and private key pair, PKCS # 10 by themselves and submit certificate request file to SHECA.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

(1) The representatives of institutions or designated agent as EV certificate applicant submit certification application

(2) The applicant submits a certificate application form, identity documents. Public key and PKCS # 10 certificate request file is generated and submitted to SHECA

(3) SHECA performs identity authentication and verification process in accordance with the section 3.2.

(4) SHECA verify application materials submitted by the applicant, according to the results to decide whether to accept, reject or require the applicant to submit relevant supplementary materials

(5) The issuance process is entered after SHECA accepted the application.

Besides, since September 2017, SHECA perform CAA(Certificate Authority Authorization) Record Check in issuance process, and remain record in authentication checklist.

Authorized CAA Records of SHECA are: sheca.com, imtrust.cn and wwwtrust.cn.

4.2.2 Approval or Rejection of Certificate Applications

After identification and authentication in Section 4.2.1, if the user meets the corresponding requirements, it is considered that SHECA has accepted the certificate request, the applicant becomes the EV certificate subscriber of SHECA; otherwise the certificate request should be rejected.

If the application is clearly prohibit the by laws and regulations, or is a SHECA considered high-risk, SHECA should reject the application,

SHECA creates and maintains certificates high risk applicants list according to the list published by the anti-phishing Alliance, antivirus vendors or related Union, government agencies responsible for network security services, or information disclosed in public reports by media. SHECA will check the list before accepting certificate application. For applicants in the list, SHECA will refuse its application directly, or request additional application materials, fund guarantees to prove that their certificates will not be misused or unlawful use. Issued certificates will be reviewed according to the list on a regular basis, once a holder of the certificate appears in the list, SHECA has the right to revoke the certificate, or adopt appropriate mechanisms for careful handling.

For those organizations is prohibited engaging in commercial activities or public activities by laws and regulations, national government departments, industry regulators, SHECA has the right to refuse issuing an EV certificate. In addition, if the certificate applicants restricted by relevant laws and regulations, the State or local government, SHECA can reject their participation in the EV certificate request.

4.2.3 Time to Process Certificate Applications

SHECA should complete processing certificate applications within a reasonable time.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

CA will generate and issue certificates after the certificate application is approved. CA generates and issues a certificate to the applicant based on the information which has been approved in the certificate application. Operation of issuing certificates is in compliance with requirements of guidance issued by CA / Browser Forum through www.cabforum.org .

(1) Submit the request documents self-generated in PKCS # 10 formats on application date to the CA in reliable manner

(2) CA verify that the request does come from the applicant

(3) Confirm the integrity of the PKCS # 10 format request file in the way verifying the digital signature.

(4) Check whether the name and other information in request file is consistent with the validated name in the application form.

(5) The subscriber certificate should be issued after verification.

(6) Upon completion of the issuance of the certificate, subscribers will be informed offline or online to download or receive it.

Besides, certificate issuance by the Root CA shall require an individual authorized by the CA system administrator of SHECA to deliberately issue a direct command in order for the Root CA to perform a certificate signing operation.

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

SHECA shall inform the subscriber of the issuance of a certificate by phone or e-mail.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

The following conduct constitutes certificate acceptance:

- Download or install a Certificate.
- Fail to object to the certificate or its content.

After a certificate is received, the subscriber should do the following procedures:
(1) Confirm the consistency of the certificate content and application information
(2) Confirm the correctness of certificate contents
(3) Verify whether the public key information in certificate is the same with the content in PKCS # 10 certificate request
(4) Verify the validity and legitimacy of the certificate with CA certificate
If exception is found by implementing of the above process, the subscriber should inform SHECA immediately to revoke the certificate and renew the request for issuance.
After receiving the applied certification, subscriber must confirm fully understand and agreement to the rights and obligations of certificate usage, if not, the certificate shall be deemed rejected, SHECA should revoke the certificate.

4.4.2 Publication of the Certificate by the CA

All the Certificates will be published in a publicly accessible repository.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Use of the Private Key corresponding to the public key in the certificate shall only be permitted once the Subscriber has agreed to the Subscriber Agreement and accepted the certificate. Certificates are used in accordance with the Subscriber Agreement, the provisions of the CP and CPS, and must be used consistent with the purpose defined in the key usage extension in certificate.

Subscribers shall protect their private keys from unauthorized use and don’t use expired or revoked certificates. Subscriber private key can’t be archived.

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties shall agree to the terms of the applicable Relying Party Agreement as a condition of relying on the certificate.

Relying Party should rely on a certificate under reasonable circumstances. If the circumstances indicate additional assurances are required, the Relying Party must obtain assurances for such reliance to be deemed reasonable.

Before any act of reliance, Relying Parties shall independently assess:

- Certificates should be used properly under specific situation, and could not be used for any forbidden or limited situation identified by CPS. SHECA has no responsibility to assess whether the certificate has been properly used
- The certificate is being used in accordance with the *KeyUsage* field extensions included in the certificate.
- The status of the certificates in the certificate should be verified. If any of the Certificates in the Certificate Chain has been revoked, the Relying Party should judge independently whether the digital signature is signed prior to the revocation.

After evaluation, if the relying party assumes the certificate is properly used, then the relying party should use the proper software and hardware to perform digital signature verification or other decryption operations, as dependent on the conditions of the certificate. These operations include the identification and validation of the certificate chain and all digital signatures in certificate chain.

Before relying party trust certificates issued by SHECA, at least the following should be operated to determine whether trust the certificate or not:
(1) Obtain the EV Root Certificates of SHECA
(2) Check whether the certificate and the subscriber's certificate is in validity period
(3) Check whether the certificate is valid digital signature
(4) Check whether the certificate is revoked
(5) Verify the digital signature contained in the subscriber certificate with public key of certificate.
(6) Check whether the subscriber certificate is revoked.
If these operations fail validation, which means that subscribers certificate that relying parties obtained is not issued by SHECA, or the certificate has expired, or if the certificate has been revoked, or the certificate digital signature cannot be authenticated, relying party should not trust the subscriber certificate.

4.6 Certificate Renewal

Certificate renewal is the issuance of a new certificate to the subscriber without changing the public key or any other information in the certificate.

4.6.1 Circumstances for Certificate Renewal

SHECA doesn't provide the certificate renewal service.

4.6.2 Who May Request Renewal

No stipulation.

4.6.3 Processing Certificate Renewal Requests

No stipulation.

4.6.4 Notification of New Certificate Issuance to Subscriber

No stipulation.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

No stipulation.

4.6.6 Publication of the Renewal Certificate by the CA

No stipulation.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.7 Certificate Re-key

Certificate re-key is the application for the issuance of a new certificate that certifies the new public key without changing of information in the certificates from the SHECA.

4.7.1 Circumstances for Certificate Re-key

Certificate re-key refers to requirements in Section 3.3.1.

Revoked certificate cannot be applied for the certificate re-key, which can only be applied for a new certificate in accordance with the initial application for a certificate in Section 3.2.

4.7.2 Who May Request Re-key

Subscribers are the subjects of certificate re-key application.

4.7.3 Processing Certificate Renewal Requests

Identification and Authentication for Re-key Requests is in accordance with Section 3.3.

Certificate issuance is in accordance with Section 4.3.

4.7.4 Notification of New Certificate Issuance to Subscriber

Refer to Section 4.3.2

4.7.5 Conduct Constituting Acceptance of a Renewal Certificate

Refer to Section 4.4

4.7.6 Publication of the Re-key Certificate by the CA

Refer to Section 4.4.2.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

Refer to Section 4.4.3.

4.8 Certificate Modification

Certificate modification refers to the application for the issuance of a new certificate due to changes in the information in an existing certificate (other than the subscriber's public key).

4.8.1 Circumstances for Certificate Modification

SHECA does not offer EV certificate modification service. If the name of certificate subject or any information contained is changed, the certificate should be revoked according to the provisions of 4.9, and the subscriber shall apply for issuance certificate in accordance with the provisions of 4.1, 4.2, 4.3, 4.4.

4.8.2 Who May Request Certificate Modification

No stipulation.

4.8.3 Processing Certificate Modification Requests

No stipulation.

4.8.4 Notification of New Certificate Issuance to Subscriber

No stipulation.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

No stipulation.

4.8.6 Publication of the Modified Certificate by the CA

No stipulation.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.9 Certificate Revocation and Suspension

Certificate revocation and status query operations comply with Part 13 of guidance requirements issued by CA / Browser Forum via www.cabforum.org .

4.9.1 Circumstances for Revocation

4.9.1.1 Reasons for Revoking a Subscriber Certificate

In any of the following circumstances, the subscriber certificate should be revoked in 24 hours:

- Subscribers request to withdrawal
- SHECA obtains evidence that the Certificate was misused;
- SHECA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully- Qualified Domain Name;
- SHECA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's Certificate Policy or Certification Practice Statement;
- SHECA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository;
- Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement;
- Within the validity period, the information contained in the subscriber certificate changes, exists errors or mistakes, or is inconsistent with the actual information of subscriber
- Subscriber information in EV SSL certificate is substantially changed
- After certificate insurance, fake information is found by SHECA in the application materials provided by EV SSL certificate subscriber
- The application of certificate is not authorized or can't be traced to the authorization
- Subscriber doesn't use EV SSL certificate according to CP/CPS or the agreement, or changes the usage of EV SSL certificate; they use this certificate to fishing, cheat or other crimes.
- Private key of subscribers is confirmed or suspected to be cracked, damaged, lost, or tampered
- Subscribers violates the obligations of CP and CPS, Subscriber Agreement and other provisions, representations or warranties, or subscribers cannot fulfill the obligations specified in the relevant agreement
- Subscribers failed to fulfill the obligation to pay
- Continuity of using the certificate will cause harm to SHECA business credit and trust mode
- The change, revocation or dismiss of subscriber legal identification
- Private key of SHECA EV Root or EV sub CA certificate exists security risk or being cracked or blabbed

- SHECA found that the issuance of EV subscriber certificates does not comply with the guide or SHECA EV certificate policy; Or believe that the information displayed in the EV certificate is not correctly
- SHECA terminates operation and has not arranged other EV certificate issuing authorities to offer revoke services; or SHECA no longer have the rights or qualifications to issue EV SSL certificates
- Evolution of technologies or standards may lead to unacceptable risk for the relying party or software providers.
- Judgments of the judiciary, such as the domain name in the certificate, the certificate subject information does not remain effective or continue to be trusted
- When SHECA obtains evidence or is made aware that the subscriber has suspect Code in their signed software object, the Code Singning Certificate should be revoked;
- The relevant provisions of laws and regulations or requirements

  When these conditions occur, the relevant certificate should be revoked and posted to the certificate revocation list. The revoked certificate must be contained in CRL till the expiration of certificate validity.

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

In any of the following circumstances, the Subordinate CA Certificate should be revoked in 7 days:

1. SHECA obtains evidence that the Subordinate certificate's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Sections 6.1.5 and 6.1.6;

2. SHECA obtains evidence that the Certificate was misused;

3. SHECA is made aware that the Certificate was not issued in accordance with the applicable requirements such as Certificate Policy or Certification Practice Statement;

4. SHECA determines that any of the information appearing in the Certificate is inaccurate or misleading;

5. SHECA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;

6. SHECA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless SHECA has made arrangements to continue maintaining the CRL/OCSP Repository;

7. Revocation is required by SHECA's Certificate Policy and/or Certification Practice Statement; or

8. The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties.

4.9.2 Who Can Request Revocation

The following subject can request revocation:

- Certificates subscriber,Representative who is authorized legally by Certificates subscriber or business entity who pays for the certificate with proper authorization
- SHECA
- The courts, government and other public power department

Other parties may report suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates, in the first instance, by email to report@sheca.com.

Only SHECA can revoke root certificate or sub-CA certificate.

4.9.3 Procedure for Revocation Request

As for the certificate revocation application, SHECA shall handle it in accordance with the following process:

(1) Certificate Subscriber representative or designated agent could apply certificate revocation in the following ways:

- Online application(only for subscribers with USB KEY):log in on http://issp.sheca.com/ with the USB KEY and apply for certificate revocation
- Email: report @sheca.com
- Fax 021 -36393200
- Tel 021 -36393196
- site application: SHECA's service locations

(2) During the valid period of the certificate, SHECA should begin an investigation within 24 hours after receive the revocation request. SHECA performs identification and verification for certificate revocation request according to the following rules.

a) For subscribers with USB KEY, just log in on http://issp.sheca.com/ with the USB KEY and submit the certificate revocation request online.

b) For subscribers with no USB KEY, Certificate Subscriber representative or designated agent must go to one of the service locations of SHECA and submit the certificate revocation request together with essential proof of identity and authorization. If there is no service location available for the subscriber, the request may be submitted (by the person who was responsible for the certificate application is preferred) via telephone or email, SHECA stuff shall perform identification verification of the individual and the organization via telephone.

(3) SHECA shall decide whether revocation or other appropriate action is warranted during two workdays.

If a software provider request to revoke the certificate, SHECA should inform the software supplier within 2 workdays after receiving the request whether the certificate revocation is required.
If SHECA confirmed that the revocation of the certificate will have an unreasonable impact on other customers after an investigation, SHECA should recommend the software provider to take additional measures.

(4) After the certificate has been revoked, SHECA should publish it to the certificate revocation list

Any revocation application that is not requested from the subscriber, should be approved appropriately before proceeding.

When Root certificate or sub CA certificate's private key encounters severe security risk, the certificate can be directly revoked after approved by competent authorities.

SHECA establishes and maintains 7 * 24 hours online service for Certificate Problem Reports and Acceptance mechanism.

Subscriber should immediately inform SHECA when private key appears or is suspected leak, break or abused within 24 hours. SHECA shall, within 24 hours after receiving the

subscribers report, make the investigation and decide whether revocation or other appropriate action is needed and provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate Problem Report.

SHECA establishes and maintains 7 * 24 hours of EV Certificate Problem Reports and accepted mechanism. Subscriber, relying party, application software vendors or other third parties may report and complain to SHECA when they have discovered certificate problem, the private key leaking risk, certificates of abuse, or other related fraud, leakage. Report as follows:

- Email: report @sheca.com
- Fax 021 -36393200
- Tel 021 -36393196

After receiving the report or complaint, SHECA will investigate and detect the report within 24 hours and decide whether to revoke or take other appropriate procedure based on investigation results. If an software provider requests a certificate revocation, SHECA should inform the software provider whether the certificate revocation is required based on the results of investigation within 2 workdays after receiving the request. Identification and investigation include, but not limited to, the following:

- Speaker identification
- The nature and cause of the problem
- Number of occurrences and the frequency of corresponding problem
- Re-examine business processes such as certificate issuance, etc.
- Follow CP / CPS, subscriber agreement and other relevant specifications
- Follow relevant laws and regulations

In addition, when SHECA finds that the Code Signing certificates with the malicious software involved are issued, it shall:

- Contact the software publisher in 1 working day and request a response within 72 hours;
- Within 72 hours, SHECA shall make sure the number of relevant stakeholders affected by the current accident;
- If SHECA receives a response from the software publisher, SHECA and the software publisher should make a joint decision about the reasonable time of revoking the certificate;
- If SHECA did not receive responses from the software publisher, SHECA shall inform the software publisher that the certificate will be revoked in 7 days, unless there is a documented evidence indicate that the certificate revocation will make a huge effect to the public.

4.9.4 Revocation Request Grace Period

Certificate revocation request should be made within a reasonable period of time, SHECA is not mandatory on this.

However, based on the perspective of protecting subscribers' interest, the subscriber should apply for revoking certificate immediately when the event could cause certificate revocation

occurs. If private key has been suspected or confirmed cracked, leaked or others which could affect security, subscriber should request to revoke certificate within 24 hours.

4.9.5 Time within Which CA Must Process the Revocation Request

After receiving the revocation request, CA should take reasonable steps to deal with, and shall not delay.

Usually, SHECA should start the investigation within 24 hours and decide whether revocation or other appropriate action is warranted during two workdays based on at least the following criteria:

1. The nature of the alleged problem;

2. The number of Certificate Problem Reports received about a particular Certificate or Subscriber;

3. The entity making the complaint (for example, a complaint from a law enforcement official that a Web site is engaged in illegal activities should carry more weight than a complaint from a consumer alleging that she didn't receive the goods she ordered); and

4. Relevant legislation.

4.9.6 Revocation Checking Requirements for Relying Parties

Before trusting UNTSH EV certificate, Relying Party need to check the certificate status, including inquiries certificate revocation list by www.sheca.com (http mode), checking certificate status through the Online Certificate Status Protocol (OCSP) mode inquiries and so on.

Relying Parties should assess the risk, responsibility and relevant consequences to determine the interval time to inquiry (or download) certificate revocation list.

Before using the certificate revocation list, relying party need to verify whether the certificate revocation list is signed by SHECA (verifying digital signature in certificate revocation list), and check whether the CA certificate is revoked.

4.9.7 CRL Issuance Frequency

SHECA updates and publishes Certificate Revocation lists (CRLS/ARLs) according to the following rules.

For root/intermediate root certificates, publish a CRL at least every 6 months, or publish an ARL within 24 hours of a root/intermediate root certificate being revoked. The difference between nextUpdate time (nextUpdate) and this update time (thisUpdate) of the root/intermediate root certificate ARL must be less than or equal to 10 months. If the root/Intermediate Root certificate is revoked, SHECA will publish the revocation information on the website.

For subscribers certificate, SHECA should issue and publish the CRL at least every 5 days, or within 24 hours after the subscriber certificate is revoked. The difference between the next update time (nextUpdate) field and this update time (thisUpdate) field of the subscriber certificate CRL must be less than or equal to 7 days.

For the sub-CA certificate, at least every 6 months, the validity of ARL is 10 months. If the root/Intermediate Root certificate is revoked, SHECA will publish the revocation information on the website.

CRL issuance frequency should comply with the requirements of Section 13 that CA / Browser Forum published on www.cabforum.org.

4.9.8 Maximum Latency for CRLs

CRLs are posted to the repository within a commercially reasonable time after generation. This is generally done automatically within minutes of generation.

4.9.9 On-Line Revocation/Status Checking Availability

SHECA provide online certificate service protocol (OCSP) to subscribers and relying parties. OCSP's availability complies with requirements in RFC6960 and/or RFC5019.

SHECA provides OCSP services at: http://ocsp3.sheca.com/Sheca/sheca.ocsp

4.9.10 On-Line Revocation Checking Requirements

Effective 1 January 2013, SHECA supports an OCSP capability using the GET method for Certificates issued in accordance with these Requirements.

1 For the status of Subscriber Certificates:

SHECA maintains real-time update of information provided via an Online Certificate Status Protocol. OCSP responses from this service have a maximum expiration time of one hour.

2 For the status of Subordinate CA Certificates:

SHECA shall update information provided via an Online Certificate Status Protocol at least 1) every 12 months and 2) within 24 hours after revoking a Subordinate CA Certificate.

If the OCSP responder receives a request for status of a certificate that has not been issued, the responder will not respond with a "good" status. SHECA monitors the responder for such requests as part of security response procedures.

Effective 1 August 2013, OCSP responders for SHECA which are not Technically Constrained in line with BR Section 7.1.5 will not respond with a "good" status for such certificates.

A relying party must check the status of a certificate before relying on that certificate. The Relying Party shall check Certificate status by OCSP instead of checking the CRLs.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12 Special Requirements Related to Key Compromise

SHECA uses commercially reasonable efforts to notify UNTSH participants if it discovers, or have reason to believe, that there has been a compromise of SHECA private key.

When these situations occur, SHECA should follow the procedures below:

(1) Generate new CA key pairs and issue a new corresponding CA certificates

(2) Revoke all issued certificates, use the new CA key issuing certificate revocation lists, which contains all issued and unexpired certificates (including revoked certificate before CA Key compromise)

(3) Use reasonable efforts to inform the subscriber and relying party

(4) Issue new certificate to subscribers

(5) Deliver the new CA certificate to subscribers

(6) Issue new subscriber certificate using the new CA key

The subscriber should inform SHECA to revoke subscriber certificate within 24 hours if the subscriber private key is suspected or confirmed to be cracked.

4.9.13 Circumstances for Suspension

SHECA does not provide suspension service for EV Certificates.

4.9.14 Who Can Request Suspension

Not applicable

4.9.15 Procedure for Suspension Request

Not applicable

4.9.16 Limits on Suspension Period

Not applicable

4.10 Certificate Status Services

4.10.1 Operational Characteristics

The Status of public certificates can be queried via CRL, LDAP directory and via an OCSP responder. Such certificate status services could response timely while having strong concurrent processing capabilities.

4.10.2 Service Availability

Certificate status services must maintain 24x7 availability, which in accordance with the requirements of Section 13 issued by CA/Browser Forum on www.cabforum.org

4.10.3 Operational Features

Refer to Section 4.9.9 and 4.9.11.

4.11 End of Subscription

When SHECA EV Root certificate or EV sub-CA certificate un-valid, revoked, or SHECA end its operations, it means the termination of service for the certificate issued, unless there are other provisions in laws and regulations.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

SHECA should not escrow any subscriber's EV private keys. SHECA does not provide Key Recovery Services.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5. Facility, Management, and Operational Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

CA and RA operations are conducted within a physically protected environment, situated in China Telecom Building, conforming to the facility standards of storage of critical and sensitive information.

With physical security measures such as security barriers, entry controls and CCTV, unauthorized person can be prevented from access to related facility, preventing and checking unauthorized usage, access or disclosure to the sensitive information or system.

5.1.2 Physical Access

Access to each of the physical security layer should be auditable and controllable to ensure that only authorized personnel gets access. SHECA takes the following measures for CA computer room access:

(1) Set the multi-layer entrance guard system, personnel checks, smart cards or fingerprint for identification, of which at least two layers must simultaneously have two or more persons through identity and access control examinations before entering

(2) Record in and out of computer room with 24-hour video surveillance equipment.

(3) Password devices for CA private key backup should be stored in safe with video surveillance systems and a key to a safe and password are kept by two persons separately.

(4) All important hardware, software and other equipment are under protection of video surveillance systems. Any key management operations must be carried out by two or more persons.

5.1.3 Power and Air Conditioning

Electricity of CA server room is supplied by Uninterruptible Power Supply(UPS) provided by of Shanghai Telecom North District Power Center. The UPS is equipped with two different power supply channels to guarantee uninterrupted power supply and using diesel engine as a backup.

The facility room is equipped with independent air conditioning systems to control temperature and relative humidity with periodical preservation and test.

5.1.4 Water Exposures

The server room is located inside the High airtight building. Except for the access doors, all the exterior walls are made of concrete. Server room floor is raised to effectively prevent flooding or other damage caused by the flooding.

5.1.5 Fire Prevention and Protection

The server room is decorated with fire-resistant materials, with a smoke alarm system, automatic gas fire extinguishing system. Once upon a fire is detected, these facilities can be automatically triggered to put out fire.

Fire protection measures should meet the requirements of the National Fire regulations.

5.1.6 Media Storage

SHECA use safe with electromagnetic shielding, anti-static equipment, fire-resistant as well as anti-magnetic features which protect back up critical system data or sensitive information of magnetic storage media from damage caused by water, fire, or other physical factors. It also takes protective measures to prevent, detect, and prevent the media from unauthorized use, access or disclosure.

5.1.7 Waste Disposal

When hardware, storage devices, and other cryptographic devices SHECA using are abandoned, sensitive and confidential information should be physically shredded safely and completely.

Special measures should be taken when deal with file and storage media which contains sensitive and confidential information to guarantee sensitive information can’t be restored and read.

All processing behavior will be recorded and rigorously validated. And appropriate documentation should be retained.

Actions of destruction of all classified materials follow the relevant National laws and regulations.

5.1.8 Off-Site Backup

SHECA takes secure offsite backup and maintains critical system data or any other sensitive information (including audit data) backup:

- Offsite backup server room is equipped with the appropriate equipment, when daily operations is not working properly due to external factors, the backup system can provide continuous operation ability.
- CA operation related backup data is stored in temperature and humidity control environment with magnetic, anti-static, video surveillance and physical access control measures.
- Establish a disaster recovery plan, and conduct regular drill accordingly, in order to maintain the availability of backup facilities

5.2 Procedural Controls

5.2.1 Trusted Roles

In order to ensure the reliability and security of UNTSH certificate service, personnel in SHECA with rights to use or control the operation which might affect the issuance, use, management, and revocation of certificates (including restrictive operations to SHECA information base) should be trusted persons.

Trusted Persons include all employees, contractors, and consultants that have access to or control following authentication or cryptographic operations which may have materially impact:

- the validation of information in Certificate Applications;
- the acceptance, rejection, or other processing of Certificate applications, revocation, renewal, or enrollment information;
- the issuance, or revocation of Certificates, including personnel having access to restricted portions of its repository, handling subscriber information or requests
- Access, manage, and maintain critical systems or sensitive data

Trusted Persons include, but are not limited to:

- customer service personnel,
- certificate business operations personnel,
- system administration personnel,
- database management and operations personnel,
- designated engineering personnel,
- key management and operations personnel,
- Internal audits and evaluations officer
- Executives that are designated to manage infrastructural trustworthiness.

5.2.2 Number of Persons Required per Task

CA and RA must establish, maintain and enforce rigorous control procedures to ensure segregation of duties based on job responsibilities and to ensure that multiple Trusted Persons are required to perform sensitive tasks. Policy and control procedures are in place to ensure segregation of duties based on job responsibilities. The most sensitive tasks, such as access to

and management of CA cryptographic hardware (cryptographic signing unit or CSU) and associated key storage material, require multiple Trusted Persons.

These internal control procedures are designed to ensure that at a minimum, two trusted personnel are required to have either physical or logical access to the device. Access to CA cryptographic hardware is strictly enforced by multiple Trusted Persons throughout its lifecycle, from incoming receipt and inspection to final logical and/or physical destruction. Once a module used for key management is activated, further access controls (include physical and logical access to the device) are invoked to maintain split. Persons with physical access to modules cannot hold "Secret Shares" and vice versa.

To ensure that a single person can't obtain, export, restore, update, abolished the private key is stored, at least three(3) personnel using key segmentation and synthesis technology which is confidential can perform CA key generation and recovery.

Other operations such as the validation and issuance of certificate, require the participation of at least two (2) Trusted Persons, or a combination of at least one trusted person and an automated validation and issuance process. Manual operations for Key Recovery may optionally require the validation of two (2) authorized Administrators.

Operations of key system data and maintenance of key systems requires at least one operator and one monitor.

In case of emergency the system needs repair by external person, at least one SHECA staff should be at the scene, all permitted operations or modifications should be recorded by SHECA staff.

5.2.3 Identification and Authentication for Each Role

For all personnel seeking to become Trusted Persons, verification of identity should be performed by CA and RA to ensure their satisfying job responsibility. Including:

- Set different roles according to the actual requirements and permissions of its division, and set background requirements according to different roles
- Conduct background checks to meet trusted role requirements
- Issue access devices and grant access to the required facilities for the Trusted Role.

Before conducting credible investigations, the authenticity and reliability of the physical identity should be confirmed firstly, and further background checks need to follow the strict requirements of the CPS.

Trusted Persons will be accessed to Security Token according to job nature and position rights such as system operation card, access card, login password, operating certificate, account after passing identification and authentication. For security token staff, all operating behaviors will be recorded by SHECA.

All SHECA staffs must ensure that:

- Issued security tokens only belonged to individuals or organizations directly
- Issued security token is not allowed to be shared
- Access of SHECA systems and procedures controlled by identifying different token

Operations performed according to business needs should be recorded to ensure the auditability of certificate of service-related jobs and the system can make the appropriate security threat and risk assessment.

5.2.4 Roles Requiring Separation of Duties

Roles requiring Separation of duties include (but are not limited to)

- the validation of information in Certificate Applications;

- the acceptance, rejection, or other processing of Certificate Applications, revocation or renewal requests, or enrollment information;
- the issuance, or revocation of Certificates;
- the access to restricted or sensitive information;
- the handling of Subscriber information or requests;
- the generation, issuing or destruction of a CA certificate;
- the visiting, management and prevention of key system or sensitive data;
- the loading or offline of a CA to a Production environment;
- the management and operation of password setting;

5.3 Personnel Controls

Personnel controls are in accordance with the requirements in Section 14.1 issued via www.cabforum.org by CA/Browser Forum.

5.3.1 Qualifications, Experience, and Clearance Requirements

Personnel seeking to become Trusted Persons present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities competently and satisfactorily, proof of not taking part-time which influent current Certificate Services, as well as proof of any government clearances and non-bad credit record.

- Operators of certification business systems must have credible, high characteristic enthusiasm, no part-time job which has influence on current Certificate Services, no experience of due diligence issue or irresponsible record in certificate services and no poor record of lawlessness.
- System operator must have relevant experience of certificate operating system, or obtain training provided by SHECA.
- Managers must have practical experience in certification operation and years of experience in system management operation.

5.3.2 Background Check Procedures

Certificate Services practitioners should be on board after background check and business capacity investigation according to background check standard. Generally, based on job requirements, business capacity investigation should be conducted once every two years for each appropriate staff

Background check must comply with legal and regulatory requirements including content, method, and the investigation officer activities. Background check must be conducted by HR and the business department separately according to the content.

According to the characteristics of different Trusted Role, background checks should include (but not limited to) the following:

- Proof of identity, such as identity cards, passports, household register, etc.
- Educational degree and other qualifications.
- Resume, including education, training experience, work experience and relevant references.
- Search of criminal records (local, state or provincial, and national)

Background check should use legal means to verify the personnel background information through relevant organizations, departments. Staffs from HR department and security management conduct the assessment together.

SHECA employees have a 3-month observation period, and the key and core staffs have additional observation period after that. SHECA would arrange work or dismissal based on

the results of the inspection. SHECA would organize training including responsibilities, jobs, technology, policy, legal, security and other aspects according to requirements.

Prior to commencement of employment in a Key Role, SHECA conducts background checks which include (but are not limited to) the following:

- Confirmation of previous employment,
- Confirmation of identity,
- Confirmation of the educational degree obtained,
- Search of criminal records (local, state or provincial, and national),
- Search of serious dishonest working actions by appropriate method

The factors revealed in a background check that may be considered grounds for rejecting candidates for Trusted Positions generally include (but are not limited to) the following:

- Misrepresentations made by the candidate,
- Highly unfavorable or unreliable professional references,
- Certain criminal convictions
- Using illegal identification or qualifications, proof of qualification
- Seriously dishonest behavior in work

SHECA establishes process management rules which bind employees not to reveal sensitive information of SHECA Certificate Services system. All employees should sign confidentiality agreement with SHECA, and are not allowed engaging in similar work as SHECA two years after the contract expires.

If necessary, SHECA can cooperates with the relevant government departments and investigative agencies to complete background checks on employees.

5.3.3 Training Requirements

CA and RA provide its personnel with training regularly for employees qualified for their job. Training programs are tailored to the individual's responsibilities, specific situations and include the following as relevant:

- UNTSH safety guidelines and mechanisms
- Using versions of hardware and software
- Responsibilities of all personnel
- Incident and Compromise reporting and handling
- Disaster recovery and business continuity procedures.

To ensure the competency of employees, SHECA provides its personnel necessary pre-job training and on job training, including but not limited to, the following:

- Job responsibilities
- UNTSH Certificate Policy (CP) and Certification Practice Statement(CPS)
- Electronic Signature Low and Related laws and regulations
- Authentication system hardware functions and modules
- Operational policies and procedures
- Basic knowledge of Certificate and Key and operating instructions
- Disaster recovery and business continuity procedures

- Requirements for security management strategy

System administrators and certification operators would be appropriately trained for critical updates or upgrades of authentication system, as well as the new system being on-line.

It would be recorded after training.

5.3.4 Retraining Frequency and Requirements

CA and RA provides refresher training continuously to enhance their capability. The extent and frequency of training is required to ensure that such personnel maintain the level of proficiency to perform their job responsibilities competently and satisfactorily.

The training of corporate security management strategy should be conducted at least once a year.

Operators of UniTrust Network Trust Service should take relevant skills and knowledge training at least once a year.

Appropriate training needed to be arranged for upgrades authentication system, using the new system, PKI / CA and password technological advances, etc.

5.3.5 Job Rotation Frequency and Sequence

No stipulation

5.3.6 Sanctions for Unauthorized Actions

CA and RA shall establish, maintain and implement policies of unauthorized conduct penalty. Disciplinary actions may include measures up to and including termination and are commensurate with the frequency and severity of the unauthorized actions.

Typically, when an employee is suspected or has been carried out unauthorized operations, such as abuse of rights without authorization, exceeding authority or unauthorized using SHECA system operation, SHECA forbids that employee entering workplace once receiving information. According to the severity of the circumstances, take actions of education, expulsion, submitting Judiciary treatment, etc.

Once detecting unauthorized behavior, security token should be revoked or terminated.

5.3.7 Independent Contractor Requirements

In limited circumstances of human resource or special requirements, CA and RA can use independent contractors or consultants to fill Trusted Persons as long as it meets the following conditions:

- No suitable Trusted Person and independent contractors or consultants can take this role.
- Independent contractor or consultant can be trusted as a trusted employee

Otherwise, independent contractors and consultants are permitted access to secure facilities only to the extent they are escorted and directly supervised by Trusted Persons at all times.

In addition to signing confidentiality agreement, independent contractors or consultants should take training of necessary knowledge and safety regulations to comply with SHECA specifications strictly.

5.3.8 Documentation Supplied to Personnel

SHECA provides its employees the requisite training and other documentation needed to perform their job responsibilities competently and satisfactorily, including at least:

- CA system operation documentation
- Key equipment operating documentation
- Certificate Services Guide and related specifications

- CP, CPS, and related specifications
- Internal operating documents, including backup manual, disaster recovery programs
- Job descriptions
- Company related training materials
- Safety regulations

For sensitive and confidential documents, SHECA strictly limits range of personnel and specify confidentiality requirements and take appropriate measures.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

CA and RA manually or automatically log the following events:

- The type of event,
- The result of event,
- The date and time the event occurred,
- The entity or person caused the event.

SHECA records logs and events types, including but not limited to the following:

- Running event, including but not limited to Key generation of CA and Sub CA; System go live and off-line; System and application startup and shutdown; CA Key and information change, Password equipment life-cycle-related events; CA private key activation data manipulation and physical access logs; Changes and maintenance of system configuration including key, activation data or Media Destruction of Personal Information
- Certificate life cycle event, including but not limited to issuing, renewal, re-key, revocation, suspended;
- Certificate applicant identity documents and Identity verification audit records (including verification content, time, methods and etc.)
- Certificate format adjustments or changes
- CP, CPS modification
- Trusted Person events, including but not limited to logon and logoff attempts, password creation, Delete and Set, User system rights chance, and related personnel changes
- Abnormal and accident reports
- Read and write operations of certificate and information repository
- Certificate generation policy changes, such as changing validity
- Physical and Environmental Management
- Security events
- Audit events

5.4.2 Frequency of Processing Log

SHECA reviews audit logs monthly or quarterly to verify real time alerts of significant security and operational events according to the operational requirements. Actions taken based on audit log reviews are also documented.

Review is carried out not less than twice a year.

5.4.3 Retention Period for Audit Log

SHECA shall retain any audit logs generated for at least seven years. In the event that there are laws and regulations defining rules for this point, the rules in laws and regulations shall govern.

5.4.4 Protection of Audit Log

Audit logs are protected avoid unauthorized viewing, modification, reading, deletion, or other tampering in order to make sure:

- Only authorized person can read audit logs
- Only authorized person can backup audit logs
- Using logical access control to save currently exist and archived electronic audit records, and store in non-rewritable discs or other media which cannot be modified
- Audit records in paper and other media are stored in a safe place

5.4.5 Audit Log Backup Procedures

Incremental backups of audit logs are created daily and full backups are performed weekly.

SHECA takes real-time, daily, weekly, monthly, yearly or other forms of backup, using online or offline backup tool which depends on the nature and requirements of the records.

5.4.6 Audit Collection System

No stipulation.

5.4.7 Notification to Event-Causing Subject

Where an event is logged by the audit collection system, no notice is required to be given to the individual, organization, device, or application that caused the event.

5.4.8 Vulnerability Assessments

Events recorded in the audit section is used to monitor system vulnerabilities, logical security vulnerability assessment data can be recorded in real time, daily, monthly, and annual basis.

SHECA performs regular vulnerability assessments at least annually, which focus on internal and external threats facing. Based on the assessment results and the implementation of regular audit of system log, the safety control measures related to system operation should be timely adjusted in order to minimize the risk of system operation. Including:

- Vulnerability Assessment of operating system
- Vulnerability Assessment of physical facilities
- Vulnerability Assessment of Certificate System
- Vulnerability Assessment of network

5.5 Records Archival

5.5.1 Types of Records Archived

CA and RA need to archive records including, but are not limited to the following types:

- Audit data collected in Section 5.4;
- Documentation of certificate system construction and upgrade;
- CP, CPS and related specifications
- Certificate
- Background survey
- Audit assessment data
- Certificate application information
- Certificate application documentation

- Certificate lifecycle information

5.5.2 Retention Period for Archive

The minimum retention period for archive certificates is 7 years. Related certificate requests and verification documentation's retention periods are calculated after the certificate had expired or revoked.

5.5.3 Protection of Archive

All archived records need to take appropriate physical and logical access controls to ensure that only authorized trusted persons get access.

Archived content is protected by both physical security measures and cryptographic techniques to ensure long term valid storage. Only authorized staff could access in a specific security way. No one get free access to obtain it without legal requirements and certification practices.

SHECA protects related information files from threats of harsh environments, such as the destruction of temperature, humidity and strong magnetic force, etc., in order to ensure that the archives in the specified period meet any legitimate using requirement. For critical data, SHECA will use off-site backup to save.

The identity information of applicants, subscribers and authentication data which SHECA preserves can't be accessed to any unrelated third parties without lawful means from governmental authority or the judiciary.

5.5.4 Archive Backup Procedures

Electronic filing system-generated records should be regularly backed up with backup files off-site storage.

Paper materials need to be preserved in the secure facility.

5.5.5 Requirements for Time-Stamping of Records

Archiving records must retain time information, but such time information isn't recorded on cryptographic-based like Digital timestamp.

Archive of electronic records (such as certificates, certificate revocation lists, etc.) shall contain date and time information using the date and time of computer operating system. All computer systems are regularly checked to ensure the accuracy and reliability of date and time information in electronic records.

Archived hard copy records date and time information if necessary. Written records of the date and time cannot be changed freely, and any changes must be confirmed with the auditor's signature.

5.5.6 Archive Collection System

All filing related to certification services are performed by internal staff in accordance with privileges and responsibilities. Audit logs are generated by the internal system and the relevant documentation of certificate system operation is collected and managed by relevant persons with permission.

5.5.7 Procedures to Obtain and Verify Archive Information

Only authorized Trusted Personnel is able to obtain access to the archives. The integrity of the information is verified when filing. During archiving, all borrowed records must be verified the consistency in return.

Archived data can be obtained only after formal authority with written application. Auditors are responsible for archiving data verification. The authenticity of the document and the date of the issuer of written document must be verified. The digital signature of electronic documents should be verified or in cryptography way.

5.6 Key Changeover

To reduce the risk of CA private key cracked, SHECA regularly updates CA certificate private key.

The maximum lifetime of CA signing key does not exceed 30 years, which is equivalent to the corresponding validity of certificates. When generating a new key pair, SHECA will issue a new CA certificate and timely release it, so that subscribers and relying parties can obtain it timely.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

SHECA establishes accidents and damage processing procedures, which focus on accident investigation, incident response and handling. According to the disaster recovery plan, backup information should be properly preserved and could be used effectively to recovery services as soon as possible in the event of damage.

5.7.2 Computing Resources, Software, and/or Data Are Corrupted

SHECA develops recovery process for broken systems and data, and does the corresponding drill annually.

In the event of the corruption of computing resources, software, and/or data, it must be reported to the Security Management Department. Incident handling procedures are enacted. If necessary, disaster recovery procedures will be enacted.

If the CA's computer equipment is destroyed or run out, but the CA private key is not damaged, then databases and knowledge repository recovery and backup systems should be resumed in priority to quickly re-implement functions of issuance, revocation and management of certificates.

5.7.3 Entity Private Key Compromise Procedures

In case a CA private key is compromised, lost, destroyed or suspected to be compromised, all the issued certificates should be revoked and CA should take reasonable efforts to notify subscribers and relying parties in time.

5.7.4 Business Continuity Capabilities after a Disaster

CA and RA should develop, build, test, maintain and execute a disaster recovery plan when necessary to mitigate the effects of any manual or natural catastrophes. Disaster recovery plan should clarify conditions of activation plan, acceptable system outage and system recovery time. Business continuity is compliance with requirements in Section 16 of guide that CA / Browser Forum (CA / Browser Forum) published by www.cabforum.org.

In the event of a natural disaster or other catastrophe, if certificate status services couldn’t be recovered in a 24-hour, CA will open offsite backup lab facilities to provide the certificate status service within 24 hours after the opening.

5.8 CA or RA Termination

When SHECA terminates the service, in accordance with the "Electronic Signature Law" and the relevant provisions of the deal, it should notify national authorities and users within the specified time, and make reasonable arrangements to undertake business matters.

When termination is required, SHECA will take actions to minimize disruption to system operation by reasonable arrangements to transfer business to other legitimate certificate authority to continue.

Arising from the business end, contract termination, company consolidation, company integration which leads that certificate services could not be maintained, SHECA will process according to the following:

(1) Before the deadline of laws and regulations, notify the responsibility authorities, certificate holders and all other related parties.

(2) Three months prior to the termination of service, the termination of service and the fact that other related certificate authority would undertake the business will be notified to subscribers and published in the knowledge repository.

(3) Arrange business undertaking and transfer certificates, keys, etc. to the relevant undertaking agency.

(4) Transfer relevant data such as CP, CPS, operations manuals, subscriber agreement, knowledge repository, user application documents, audit records and other documents to undertaking agency.

(5) Clear CA key.

(6) Formally declare the notice to subscribers that certificate business was transferred to undertaking agency.

When business is terminated, rights and obligations will be handled in accordance with the subscriber agreement.

5.9 Data Security

Data security is compliance with section 16 of guides issued by the CA / Browser Forum through www.cabforum.org.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

CA key pair is generated by device with approval and permission of the national competent authority. Due to strict requirements for cryptographic products and systems, SHECA should comply with relevant state regulations during key generation, management, storage, backup and recovery. Besides, SHECA should follow CNS 15135, ISO 19790, or Hardware CA key generation and management regulations FIPS140-2 standard, and use standard hardware devices to generate and manage CA keys.

CA key generation process needs to be carried out under independent third party impartial witness and they should issue witness report.

Subscriber key pair is generated by the subscriber's own servers or other devices built-in key generation mechanism.

For certificates issued by UCA Global G2 Root and UCA Extended Validation Root, SHECA must not generate key pair for subscribers.

6.1.2 Private Key Delivery to Subscriber

Key pairs are generated by the end-user Subscriber, private key delivery to a Subscriber is not applicable.

6.1.3 Public Key Delivery to Certificate

Public key is submitted to CA for certification electronically through the use of PKCS#10 Certificate Signing Request in secure and reliable way.

6.1.4 CA Public Key Delivery to Relying Parties

SHECA makes public key published in the knowledge base as well as web page for Subscribers and Relying Parties to download/query .In addition, SHECA also provides such new certificates to relying parties for inclusion in new browser or the software agreement (such as S / MIME) .

6.1.5 Key Sizes

RSA Key length (for both CA root key and subscriber key) is 2048 bit. Since June 1st,2021,the key length of codesigning and timestamp certificates should be at least 3072 bits.

These requirements are in accordance with the requirements in Section 6.1.5 of reference issued by CA/Browser Forum via www.cabforum.org.

6.1.6 Public Key Parameters Generation and Quality Checking

According to national competent authority, CA key pair is generated by approved encryption device, and public key parameters generation and quality checking are controlled by the corresponding device.

6.1.7 Key Usage Purposes

The Root CA keys of SHECA are not used to sign certificates except in the following states:

1 Self-signed certificates to represent the Root CA itself

2 Certificates for Subordinate CAs and Cross Certificates

3 Certificates for Infrastructure purposes

Subscriber Certificate version issued by SHECA is X509 v3. It contains KeyUsage extension. If SHECA specify the use of issued certificate in KeyUsage extension, subscribers should use the certificate in accordance with the specified purpose.

Subscriber Certificate KeyUsage extension contains digitalSignature, keyEncipherment, dataEncipherment and keyAgreement.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

SHECA has implemented password modules approved and licensed by National code authorities as private key generation and protection equipment, and on this basis following CNS 15135, ISO 19790 or FIPS140-2 level 3 hardware cryptographic modules required, the modules requires function of multi-control.

Please find details from hardware product information provided by the device manufacturer with production qualification required by national code authorities.

6.2.2 Private Key (n out of m) Multi-Person Control

1. SHECA adopts multi-person control strategy to generate, use and deactivate the private key (m out of n)

CA private key generation, activation, backup and recovery operations take multi-control strategy which is in n out of m (m> n, n> = 3) way. Use the "secret segment" technique to write private key protection information separately in devices such as IC cards, holding by three or more trusted personnel approved by SHECA safety certification Committee, and store it in a secure and controllable environment.

Protection of smart cards or smart-password key related to private key information, as well as passwords protection should be controlled by independent management, and stored in a safely controlled environment.

2. The private key of the subscriber certificate should be controlled by the subscriber

The private key of the subscriber certificate should be controlled by the subscriber and responsible for its safety. If a specify individual is required to manage the private key, the specify person must be effectively authorized in order to prevent the private key from being

leaked, damaged, lost, or used unauthorized. When the private key occurs the security problems above, the subscriber has an obligation to immediately inform SHECA.

6.2.3 Private Key Escrow

SHECA private keys are not escrowed. Escrow of private keys for end user subscribers is not served.

6.2.4 Private Key Backup

SHECA CA private key backup performed in the following way:

(1) Keys are stored in hardware cryptographic modules, in accordance with specified in section 6.2.2, backup in a multiple controlled manner after private key encryption, and encryption key protection information is stored separately in multiple smart cards using secret-division technique. Smart card is hold by different personnel.

(2) Smart card storing cryptographic key information is placed in a security environment with the dual control and sealed for safekeeping by security personnel.

(3) Hardware cryptographic module storing backup private keys is placed inside a controlled environment with strict security. At least two persons hold safe correlation token separately.

6.2.5 Private Key Archival

SHECA private key will be securely retained after encrypted. SHECA does not archive Private Keys.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

CA's private key is generated and stored in a hardware cryptographic module. The private key is imported to another hardware cryptographic module only when performing backup and recovery. Import and Export activities should follow 6.2.2 and 6.2.4 requirements.

6.2.7 Private Key Storage on Cryptographic Module

CA private keys shall be stored in encrypted form within hardware cryptographic devices.

6.2.8 Method of Activating Private Key

CA private keys are stored in a hardware cryptographic module, and there must be 3 or more authorized persons activate the private key by inserting their IC cards and entering the correct password after identification.

Provisions related to processes should be in accordance with Section 5.2.

6.2.9 Method of Deactivating Private Key

The activated private keys are deactivated upon logging off their system after Identification or automatically deactivate after predetermined time in order to avoid the private key being used illegally.

6.2.10 Method of Destroying Private Key

After the expiration of CA private key, SHECA Safety Certification Commission authorizes multiple persons to execute zeroing function of hardware cryptographic module to destroy the private keys and physically destroy hardware cryptographic module. All IC cards used to activate and backup private key should be destroyed as well.

6.2.11 Cryptographic Module Rating

SHECA uses password encryption products approved and licensed by national code authority, and selects the hardware for cryptographic modules as needed referring to the CNS 15135, ISO 19790 or relevant provisions of FIPS 140-2 (level 3).

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

After the CA certificate (including the root CA certificate and sub-CA certificate) expires, the certificate should be archived, including the public key contained in the certificate.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

Certificate validity period should be clearly recorded in the CPS, which is in accordance with the requirements in Section 9.4 of reference issued via www.cabforum.org by CA/Browser Forum.

The validity of the public and private key is consistent. The validity period of CA certificate is consistent with the key pair's, and the validity period of subscriber certificate can be less than its key pair's. When subscriber certificate's using periods have expired, the original key in the key pair validity period can be used to apply for renewal of the certificate.

The key pair usage period and certificate validation period are set as following:

Type	**Key Pair Usage Period**	**Certificate Validation Period**
Root certificate	30 years	30 years
Subordinate CA certificate	25 years	25 years
EV SSL certificate	No stipulation	27 months
EV CodeSigning certificate	No stipulation	39 months
Time-Stamping certificate	15 months	15 months

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

CA private key activation data must be generated from several smart cards according to requirement of key activation data segmentation and key management, and it should be kept in Duty Separation way.

The activation data on smart card is read and written by card reader, and protective password with a smart card (Pin code) is used for activated data access authentication.

6.4.2 Activation Data Protection

CA private key activation data must be managed by different trusted personnel after IC card within activate data segmented in a reliable way, and the smart card PIN code should be set.

Smart card Pin code cannot be recorded on any paper or other media. If entered incorrectly 3 times, the card will lock automatically. When the transfer of smart card occurs, the new holder must reset the Pin code.

Subscriber private keys should be used to protect passwords or PIN-protected private key.

6.4.3 Other Aspects of Activation Data

No stipulation

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

Computer equipment used for SHECA certificate system is managed and operated by identification and authentication, audit, role access control, information transmission encryption, physical access control, network access control and other ways according to the "certificate authentication system password and its relevant safety specification" published by State Cryptography Administration, "Electronic Authentication Service Management Policy" published by the Ministry of industry and information technology of the, reference ISO17799 information security standards, as well as other relevant information security standards.

System security meets guide section 16.5 requirements published by CA / Browser Forum through www.cabforum.org.

Typically, SHECA takes the following controls of Certificate management system through the relevant operating systems, related hardware and software equipment and management measures:

(1) Using identification to login

(2) Providing customized access control

(3) Having security audit capability

(4) Limitations to certificate services and role-based access control

(5) Identification of reliable role and identity

(6) Ensuing communication and database security.

(7) Safe and reliable pipeline associated with roles and identity

(8) Program integrity and security control.

6.5.2 Computer Security Rating

Computers and other equipment SHECA certificate system used have passed the assessment of State Cryptography Administration, China National Information Security Testing Evaluation Center, Shanghai Information Security Evaluation Center, or the assessment of other third-party organizations. (TCSEC C2)

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

Development program Control of SHECA certification systems include trusted personnel management, development environment and safety management, product design and development evaluation, process control, reliable development tools, and the production system designed to meet the redundancy, fault-tolerant, modular requirements.

System development follows the ISO27001 specification.

All of core development devices have strict security precautions and means of killing malicious code, and irrelevant hardware and software are not allowed to be installed or developed.

6.6.2 Security Management Controls

Information security management of the system is strictly followed the requirement of National information technology authorities, State Cryptography Administration and SHECA safety management strategy.

Use of the system has strict control measures and all systems are rigorously tested and verification before using. Any modifications and upgrades will be recorded with version

control, functional testing. SHECA inspects and tests authentication system regularly and irregularly.

Operating system uses a strict management system to control and monitor the system configuration and change in order to prevent unauthorized modification.

6.6.3 Life Cycle Security Controls

No stipulation

6.7 Network Security Controls

SHECA uses network security management of multilevel firewall, intrusion detection, security auditing, anti-virus, and strict access control permissions to ensure that only authorized personnel can operate after identification. Systems with different security levels are strictly divided into internal and external networks, and set access permissions and controls, respectively.

Certificate system must be managed and operated by authorized operators after rigorous authentication.

To protect against network intrusions and damages, installation and configuration of firewall, intrusion detection, anti-virus systems and etc. are used to enhance network security.

Certificate system and the internal database server is only connected to the internal network and isolated by firewall. Only internal devices are allowed connection and only authorized personnel or the system gets access to visit after identification.

6.8 Time-Stamping

No stipulation

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

7.1.1 Version Number(s)

SHECA issues EV certificates in compliance with X.509 Version 3

7.1.2 Certificate Extensions

The extension of EV certificate is in compliance with RFC 5280 and requirement of 'Guidelines for the Issuance and Management of Extended Validation Certificates'.

EV SSL certificate policy extension meets the requirements of section 9.7 published by CA / Browser Forum Guidelines www.cabforum.org.

7.1.3 Algorithm Object Identifiers

SHECA Certificates uses the following algorithms object identifier(OID):

sha256withRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}

sha-1WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}

7.1.4 Name Forms

SHECA issues EV certificates with Name Forms and Content comply with X.501 (Distinguished Name; DN) and RFC 5280 regulation, and the requirements in Section 7.1.4 of CA/B Forum Baseline Requirements

7.1.5 Name Constraints

SHECA uses the nameConstraints extension as needed.

7.1.6 Certificate Policy Object Identifier

SHECA EV Certificates contain the Certificate Policies extension object identifier for the Certificate Policy（Certificate Policies）

The object identifier meets the requirements of section 9.3 published by CA / Browser Forum Guidelines through www.cabforum.org.

7.1.7 Usage of Policy Constraints Extension

SHECA uses the policyConstraints extension as needed.

7.1.8 Policy Qualifiers Syntax and Semantics

SHECA uses the limit extensions (policyConstraints) syntax as needed.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation

7.2 CRL Profile

7.2.1 Version Number(s)

SHECA issues X 509 V2 version of CRLs.

7.2.2 CRL and CRL Entry Extensions

No stipulation

7.3 OCSP Profile

7.3.1 Version Number(s)

Version 1 of the OCSP specification is defined by RFC2560.

7.3.2 OCSP Extensions

OCSP extensions comply with RFC 2560 specifications.

8. Compliance Audit and Other Assessments

As an operating subject of UNTSH, SHECA performs consistency audits and operation assessments quarterly to ensure the reliability, security and controllability of certification services. In addition to internal audit and assessment, SHECA also hires an independent auditing firm in accordance with WebTrust audit for external assessment.

8.1 Frequency and Circumstances of Assessment

SHECA conducts an external audits and evaluations at least once a year and executes internal audits and evaluations on a quarterly basis.

Audit operations should be clearly documented in CPS, and to the requirements should be compliance with requirements in section 17 of guide published by CA / Browser Forum through www.cabforum.org.

8.2 Identity/Qualifications of Assessor

When conducting internal assessment audit, SHECA requires that evaluators should have related knowledge of CA and information security audit with more than two years of relevant experience. Meanwhile evaluators should be familiar with the CP and CPS-related norms, knowledge of computer, network and information security and practical work experience and so on.

SHECA should choose a professional institution with national or internationally recognized qualification, with good reputation and wealth of practical experience to conduct an external audit.

8.3 Assessor's Relationship to Assessed Entity

When conducting internal audits, auditor and audited entity is in independent relationship, and no interest can affect the objectivity of the evaluation. Auditor should be independent and impartial, objective approach to audit and evaluations.

When conducting an external audit, the audit organization should be entrusted with SHECA and no interest could affect the objectivity and independence of the assessment.

8.4 Topics Covered by Assessment

SHECA audit conducted mainly includes the following:

- Draw up and publish CP/CPS or not;
- Certificate operations and services comply with CP / CPS or not;
- CPS complies with the provisions of CP or not;
- Certificate and key life cycle management
- Physical and environmental security controls
- Business continuity management

When carrying out internal audits and evaluations, in addition to the audit of certificate issuance and operational safety audit, the following must also be audited:

- For all issued EV certificates in the audit period, randomly select at least 5% certificates to double check identity audit.
- For all issued EV certificates in the audit period, randomly select at least 10% certificates to compare with high risk applicants list.
- Training record of trusted personnel associated with EV certificates issued in audit period.

In addition, when conducting internal audit, it is important to set up risk assessment team, to assess the risk of overall business activity of the EV certificate, to identify internal and external threats and its potential prejudice, to analyze and evaluate of existing and extend of current policies, processes, and systems for risk control, to prepare risk assessment report and propose appropriate security control measures. Upon completion of the evaluation, assessment result should be reported to the SHECA safety certification Committee.

8.5 Actions Taken as a Result of Deficiency

After the completion of internal and external audits, SHECA must check for missing or insufficient based on the results of the assessment, propose changes and preventive measures, and track improvements.

SHECA may conduct follow-up rectification as needed.

8.6 Communications of Results

After audit assessment, SHECA audit results will be announced via www.sheca.com website, but specific audit information would not be disclosed.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

SHECA is entitled to charge end-user Subscribers for the issuance and renewal of certificate.

Fees for issuance, renewal of certificate and any associated are made clear to end-user on SHECA's website www.sheca.com or specified in the agreement signed by subscriber and SHECA.

9.1.2 Certificate Access Fees

Free of charge.

9.1.3 Revocation or Status Information Access Fees

Free of charge.

9.1.4 Fees for Other Services

No stipulation.

9.1.5 Refund Policy

If for any reason a subscriber request refund after the completion of certificate application and before the certificate's issuance, the residual interest-free payment would be reimbursed to subscriber after deducting handling cost for certificate application.

If for any reason a subscriber request refund after the certificate's issuance, the residual interest-free payment would be reimbursed to subscriber after proportional deduction of certificate usage in month spent (Any fraction of one month thereof charge of one month) and handling cost.

9.2 Financial Responsibility

9.2.1 Liability

SHECA would bear the liability in accordance to following:

1. SHECA shall not be liable to indemnity to any loss to end-user, unless loss is caused by SHECA's faults failing to follow SHECA EV Certificate Policy (CP), Certificate Practice Statement (CPS) and any related operation guidance.
2. SHECA shall not be liable to indemnity to any loss caused by force majeure event (e.g. earthquakes), or other circumstances SHECA does not bear responsibility.
3. If the damage to end-user is due to personnel fault or willful act during certificate application, issuance, renewal and revocation breaking the requirement of SHECA EV Certificate Policy (CP), Certificate Practice Statement (CPS) and any related laws and regulations.
4. For any legal dispute arising from using the subscriber certificate during the period of certificate revocation applicant and certificate revocation coming into force (the time in CRL shall be the time of revocation), while SHECA doesn't break the CPS, CP and any related laws and regulations, SHECA shall not be liable to indemnity to any loss caused.
5. SHECA shall not be liable to indemnity to any loss if and when subscribers using fake or wrong certificate, or even using forged document to apply for certificate.
6. Temporal limits of liability follow the appropriate laws and regulation.
7. SHECA would engage an independent third-party financial audit annually to ensure having sufficient cash asset prepared for compensating potential end-user loss.
8. SHECA would purchase third-party insurance as needed. Otherwise, SHECA would be liable to the loss by own fund following guidelines issued by the CA / Browser through http://www.cabforum.org .

9.2.2 Other Assets

SHECA has enough cash asset as financial guarantee for compensation arising from certification operation.

9.2.3 Insurance or Warranty Coverage for End-Entities

See section 9.2.1

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The following records shall be kept confidential and private:

1. Agreement, envelope and commercial agreements between subscribers, other relevant party and SHECA;
2. Private Key and relevant active data;
3. Subscriber's personally information submitted when applying for a certificate;
4. System operation and management logs and records
5. Audit records
6. System and network configuration data
7. System operation management documentation
8. Others documents which SHECA clearly defines as confidential

9.3.2 Information Not Within the Scope of Confidential Information

Certificate policy (CP), Certificate Practice Statement (CPS), the certificate application forms, certificates and CRL, external audit evaluation results, etc. are not considered confidential and private information.

9.3.3 Responsibility to Protect Confidential Information

Except as otherwise required by law, national authorities or written authorization by subscriber, SHECA shall secure confidential and private information from compromise and disclosure to third parties.

If the judiciary requires SHECA to provide related documentation for treatment of certificate disputes, SHECA shall conform to legal procedures.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

SHECA respects all users and their privacy, and in accordance with laws and regulations on the protection of personal privacy information.

9.4.2 Information Treated as Private

Eliminating the information already included in the certificate, subscriber's essential information and identification including telephone number, address are considered is treated as private.

9.4.3 Information Not Deemed Private

All information made public in a certificate is deemed not private

9.4.4 Responsibility to Protect Private Information

SHECA shall secure the private information from compromise and disclosure to third parties and shall comply with all local privacy laws in jurisdiction.

9.4.5 Notice and Consent to Use Private Information

SHECA shall have no obligation to inform and obtain consent of subscriber when using subscriber information within the scope of certification service, so as when SHECA follows laws, regulations, and requirement of court and government.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

SHECA shall be entitled to disclose confidential and private information with the following exceptions:

- Applicant should submit a written application with consent from related government department
- Court and government department submit a written application for conducting any legal dispute arising from using the subscriber certificate
- An arbitration organization with competent jurisdiction submits a written applicant.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property rights

1. SHECA retain all intellectual property rights in and to SHECA private key, certificate issued, CRL, CP/CPS and other relevant documents.
2. Subscribers retain all intellectual property rights in and to subscriber private key pairs. SHECA will own intellectual right on Certificate once the public key is signed by SHECA to issue the certificate. Subscriber and relying party only have the certificate-use right.
3. SHECA does not guarantee intellectual property rights set forth in the certificate name.

9.6 Representations and Warranties

9.6.1 Representations and Warranties of Subscriber's EV Certificate

Within the period of subscriber's EV certificate validity, SHECA warrants specifically include, but are not limited to:

1. Legal existence. From the date of issuance of Subscriber's EV Certificate, SHECA has confirmed that the subject specified in EV Certificate is a valid organization registered in government authority.
2. Identity. From the date of issuance of Subscriber's EV Certificate, SHECA has confirmed that the legal name of the subject specified in EV Certificate consistent with the name recorded by government authority.
3. The right to uses the domain name. From the date of issuance of Subscriber's EV Certificate, SHECA has confirmed the subject specified in EV Certificate has the ownership or exclusive use rights by taking all the necessary and reasonable measure following the relevant clause in Guidelines for the issuance and management of extended validation certificates.
4. EV Certificate Authorization. SHECA has confirmed the subject specified in EV Certificate authorized the issuance of the EV Certificate by taking all the necessary and reasonable measure following the relevant clause in Guidelines for the issuance and management of extended validation certificates.
5. The accuracy of the information. From the date of issuance of Subscriber's EV Certificate, SHECA has taken all necessary and reasonable measures to verify that all information contained in the EV Certificate is accurate.
6. Subscriber Agreement. The application representative of the subject specified in EV certificate has signed a subscriber agreement or accepts the term of use.
7. The certificate status. SHECA maintain an online 24x7 Repository which can be used to check the latest status of all certificate issued by SHECA following the requirement of Guidelines for the issuance and management of extended validation certificates.

8. Revocation. According to the Guidelines for the issuance and management of extended validation certificates, SHECA shall revoke the certificate when a circumstance under which a certificate may or must be revoked happens.

9.6.2 CA Representations and Warranties

SHECA as CA and RA warrants that:

1. SHECA provide certification services in accordance with laws and regulations
2. SHECA accepts and processes certificate requests, renewal, revocation request in accordance with the Certificate Policy (CP) and the Certification Practice Statement (CPS).
3. Subscriber information is accurately identified before the issuance of the EV Certificate by SHECA.
4. SHECA would keep subscribers' application and relevant materials.
5. SHECA shall inform the national authorities and subscribers timely when CA key pair occurs security problems.
6. SHECA would publish the certificates and CRL as required.
7. SHECA would supply subscriber relevant agreements and notice the rights and obligations when subscriber applies for EV Certificate.
8. SHECA guarantees the safety of its private key.
9. SHECA maintains effective and reliable operational systems and security management in accordance with the requirements of national authorities
10. SHECA guarantees all information contained in the EV Certificate is accurate without error.

The Root CA and CA's guarantee and liability should be specified in the CA's Certification Practice Statement (CPS) as required by Section 18 and 7.1 published by CA/Browser Forum on www.cabforum.org.

9.6.3 RA Representations and Warranties

See section 9.6.2 requirements.

9.6.4 Subscriber Representations and Warranties

SHECA only provide EV Certificate services to organization instead of individual users. The organizations should comply with following rules when apply and use EV Certificate:

1. Applicant must understand and agree the requirements of CP/CPS and relevant agreement when apply for a EV Certificate,
2. All information and documents in the Certificate Application the Subscriber submitted are true and authentic,
3. Their private key is protected, using the certificate in accordance with restriction requirement in CP/CPS and laws.
4. Applicant should ensure the accurate of information contained in EV Certificate while accept it, also should validate the correspondence of public key and private key in EV Certificate.
5. Subscriber should notify SHECA when the relevant information in the certificate changes occurred.
6. Subscriber should inform SHECA in due time when the private key is lost, leakage or others, and apply for certificate revocation as required. Meanwhile the subscriber should

bear the risk and liability arising from using of the certificate before the certificate's revocation status published.

7. Timely renewal certificate in accordance with SHECA provisions,
8. Accept all statements, changes, renewal and upgrades disclosed by SHECA bases on regulation and technology development,
9. For the interest of SHECA and EV certificates' relying party, subscriber should commit and guarantee statements required by Subscriber Agreement.

9.6.5 Relying Party's Representations and Warranties

When relying party trust any EV certificates issued by SHECA, he should adhere to:

1. Accepting or using a EV Certificate issued by SHECA, means the relying party understands and agrees to provision related to responsibilities and obligations disclosed in CP/CPS, and only trusts the certificate within the scope of CP/CPS.
2. Getting SHECA Root Certificate and certificate chain before decide whether to trust a subscriber EV Certificate,
3. Relying party should verify the certificate, including checking the latest valid CRL published by SHECA, checking whether the certificate is revoked, checking the reliability of the certificates in certificate chain, checking the validity of the certificate, and others that could affect the validity of the certificate
4. Choose safe and reliable computer and operation systems to rely EV Certificate issued by SHECA, and bear the loss caused by computer environment and operation systems.

9.6.6 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

To the extent permitted by applicable law, SHECA isn't subject to liability when:

1. SHECA is faultless when issuing EV Certificate,
2. Losses are caused by force majeure,
3. Losses caused within the reasonable time SHECA take to revoke the certificate after receiving the revocation request.

9.8 Limitations of Liability

SHECA has limited liability to the extent permitted by applicable law, subscriber agreement and CPS when subscriber and relying party claim damage caused by certificate issuance and usage.

9.9 Indemnities

SHECA would compensate subscriber or relying party if the damage is caused by SHECA.

Subscriber should compensate CA, relying party if the damage is due to itself.

Relying party should compensate SHECA for SHECA losses caused by it.

According to this CP, CPS, subscriber agreements, and other documents are required to specify the scope of compensation, limits, indemnity and so on.

9.10 Term and Termination

9.10.1 Term

This CPS shall come into force as of date of issue with detailed version number and date of issuance, and the old version will automatically become null and void.

9.10.2 Termination

The CPS will remain in force until replaced by a new version.

9.10.3 Effect of Termination and Survival

After the termination of the CPS, clauses related to confidential and private information, intellectual property, as well as provisions related to compensation and limited liability still stands until the expire and revoke of the final certificate.

9.11 Individual Notices and Communications with Participants

Unless specified by agreement between the parties or regulations, SHECA shall commercially reasonable methods to communicate with subscribers, such as e-mail, phone, fax, website, etc.

9.12 Amendments

9.12.1 Procedure for Amendment

SHECA is responsible for formulating and modifying the CPS, and should review the content at least once a year.

SHECA would timely revise the CPS according to the legal and regulatory requirements, OID changes, and relevant international standards.

The revised version will be filed in accordance with the provisions of the national authorities and published in repository.

9.12.2 Notification Mechanism and Period

SHECA has the right to revise any of the terms, conditions and clauses without prior notice other parties.

SHECA would publish the revised version on www.sheca.com and repository. If modification of this CPS is placed in SHECA repository, it is equivalent changes to the CPS.

If the applicant and subscriber do not request to revoke the certificate within 7 days of publication of amendment, it's considered that the applicant and subscriber agree to the amendment. Then all the amendment comes into force immediately.

Nevertheless, amendment which impacts the security of SHECA Trust Service will be effective immediately.

9.12.3 Circumstances Under Which CPS Must be changed

If any of the following situations occurs, SHECA MUST revise the CPS:

- Significant development in Cryptography which could affect the validity of the existing CPS
- Relevant Standard updated
- Major upgrades and changes to Trust Service and regulations
- The requirement by laws and government authority
- The current CPS has a major drawback.

9.12.4 Object Identifier change

When the amendment occurs, the corresponding object identifier does not change, only update the version identification code.

9.13 Dispute Resolution Provisions

Disputes among UniTrust Network Trust Service participants shall be resolved pursuant to provisions in the applicable agreements among the parties or applicable laws.

9.14 Governing Law

SHECA operations UNTSH system, all of its certificate service activities are governed and construed by the relevant laws and regulations in the People's Republic of China.

The implementation, interpretation, translation and validity of this CPS shall apply to laws of People's Republic of China regardless *c*ontract or other choice of law provisions, and without the requirement to establish a commercial nexus in China.

9.15 Compliance with Applicable Law

The CPS must comply with the "People's Republic of China Electronic Signature Law", "Electronic Authentication Service Password Management Policy" and "Electronic Authentication Service Management Policy."

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation

9.16.2 Assignment

No stipulation

9.16.3 Severability

In the event that a clause or provision of this CPS is held to be unenforceable by amendment or other reasons, the remainder of the CPS shall remain valid.

9.16.4 Enforcement

No stipulation

9.16.5 Force Majeure

To the extent permitted by applicable law, this CPS and Subscriber Agreements and other Agreements shall include a force majeure clause protecting all participants.

9.17 Other Provisions

No stipulation.

Appendix A Acronyms and Definition

SHECA

Abbreviation for Shanghai Electronic Certificate Authority Center Co.,Ltd.

UniTrust Network Trust Service Hierarchy

UniTrust Network Trust Service Hierarchy is a Public Key Infrastructure established and operated by Shanghai Electronic Certification Authority Co., Ltd, (SHECA), and providing electronic certification service based on digital certification. SHECA is the third party electronic certification service authority established according to 'Electronic Signature Law of People's Republic of China', devoted itself to creating harmonious network trust environment, providing secure, reliable and credible digital certification service.

SHECA Security Authentication Committee

The highest policy management authority ensures the consistence of CPS within the SHECA UniTrust Network Trust Service Hierarchy.

Certificate Authority

SHECA and its authorized subordinate CA which issue the certificate is call Certificate Authority.

Registration Authority

Any Legal Entity that is responsible for processing certificate applicants' and subscribers' request which shall be submitted to CA. It is responsible for identification and authentication of subjects of Certificates, initiating or transferring certificate revocation request, approving certificate renewal and re-key request represented CA.

Registration Authority Terminal

Registration Authority Terminal (RAT) is the terminal to process authorized certificate service which directly facing the client within the SHECA UniTrust Network Trust Service Hierarchy.

Electronic Certificate

Electronic signing certificate use digital signatures to identify the identity of the signatory and indicating the signatory's authentication.

Electronic Signature

A technical method abbreviated as a signature can identify the identity of signatory and indicate the signatory's authentication of signature data.

Digital Signature

A kind of Electronic Signature use asymmetric cryptography encryption system to encrypt and decrypt electronic data. Signature mentioned in the CPS is digital signature.

Electronic Signatory

The personnel owned the electronic signature data make the electronic signature by himself/herself or as the representative.

Electronic Signature Relying Party

It is the personnel trust electronic signature or electronic signature certificate in relative activities.

Private Key (Electronic Signature Creation Data)

The characters or codes create reliably linkage between electronic signature and electronic

signatory in the electronic signature application.

Key (Electronic Signature Verification Data)

It is the data subscribers used to verify the electronic signature.

Subscriber

The entity receive certificate from electronic certificate authority, called the certificate owner. In the electronic signature application, the subscriber is Electronic Signatory

Relying Party

An entity relies on the truth of certificate. In the electronic signature application is named electronic signature relying party. Relying party may, or may not be a subscriber.

Appendix B Terminology and Abbreviations

AICPA	American Institute of Certified Public Accountants, Inc.
ANS	American National Standard
CA	Certification Authority
CC	Common Criteria
CCITSE	Common Criteria for Information Technology Security Evaluation
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
FIPS	Federal Information Processing Standard
ISO/IEC	the International Organization for Standardisation, The International Electrotechnical Commission
ITSEC	Information Technology Security Evaluation Criteria
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificates Status Protocol
OID	Object Identifier
OECD	Organization for Economic Co-operation and Development
PMA	Policy Management Authority
PIN	Personal Identification number
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
RA	Registration Authority
RCA	Root Certification Authority
RSA	Rivest,Shamir,Adleman(encryption algorithm)
TCSEC	Trusted Computer System Evaluation Criteria
URL	Universal Resources Location

SSL	Secure Socket Layer
EV	Extended Validation

EV Certificates Required Certificate Extensions

1. Root CA Certificate

Root Certificates MUST be of type X.509 v3

(a) *basicConstraints*

This extension MUST appear as a critical extension. The cA field MUST be set true. The pathLenConstraint field SHOULD NOT be present.

(b) *keyUsage*

This extension MUST be present and MUST be marked critical. Bit positions for keyCertSign and cRLSign MUST be set. The others bit positions should not be set.

(c) certificatePolicies

This extension SHOULD NOT be present.

(d) extendedKeyUsage

This extension MUST NOT be present.

All other fields and extensions MUST be set in accordance with RFC 5280.

2. Subordinate CA Certificate

(a) *certificatePolicies*

This extension MUST be present and SHOULD NOT be marked critical. The policy OID MUST contain OID of UNTSH EV Policy.

(b) *cRLDistributionPoint*

This extension MUST be present and MUST NOT be marked critical. It MUST contain the HTTP URL ofthe CA's CRL service.

(c) *authorityInformationAccess*

It MUST NOT be marked critical, and it MUST contain the HTTP URL of the Issuing SHECA's OCSP responder

(d) *basicConstraints*

This extension MUST be present and MUST be marked critical. The cA field MUST be set true. The pathLenConstraint field MAY be present.

(e) *keyUsage*

This extension MUST be present and MUST be marked critical. Bit positions for keyCertSign and cRLSign MUST be set. The others bit positions should not be set.

All other fields and extensions MUST be set in accordance with RFC 5280.

3. Subscriber Certificate

(a) *certificatePolicies*

This extension MUST be present and SHOULD NOT be marked critical. The policy OID MUST contain OID of UNTSH EV Policy.

certificatePolicies:policyIdentifier (Required)

EV policy OID

certificatePolicies:policyQualifiers:policyQualifierId (Required)

id-qt 2 [RFC 5280]

certificatePolicies:policyQualifiers:qualifier (Required)

URI to the Certificate Practice Statement

(b) ***cRLDistributionPoint***

This extension SHOULD NOT be marked critical. It MUST contain the HTTP URL of the SHECA's CRL service.

(c) ***authorityInformationAccess***

It MUST NOT be marked critical, and it MUST contain the HTTP URL of the Issuing SHECA's OCSP responder

(d) ***basicConstraints*** (optional)

If present, the CA field MUST be set false.

(e) ***keyUsage*** (optional)

If present, bit positions for keyCertSign and cRLSign MUST NOT be set.

(f) ***extKeyUsage***

Either the value id-kp-serverAuth [RFC5280] or id-kp-clientAuth [RFC5280] or both values MUST be present. Other values SHOULD NOT be present.

(g) ***SubjectAltName***

This extension is marked as FALSE, fulfilled according to RFC 5280.

All other fields and extensions MUST be set in accordance with RFC 5280.