UniTrust Network Trust Service Hierarchy

Extended Validation Certification Practice Statement

Version 1.5.9

Valid from: July 25, 2025

Shanghai Electronic Certification Authority Co.Ltd

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

UniTrust Network Trust Service Hierarchy Extended Validation Certification Practice Statement

Address: 18/F, JaJie International Plaza, No.1717, North Sichuan Road, Shanghai, China

Postal Code: 200080

Tel: 86-21-36393197

E-mail: cps@sheca.com

Brand Explanation

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

Changing History Record of this document

Version	Valid date	Author	Issuer	Notes
V1.5.9	2025-07-25	Alice Shao	SHECA Security Authentication Committee	Current Version
V1.5.8	2025-04-30	Alice Shao	SHECA Security Authentication Committee	Previous Version
V1.5.7	2024-11-18	Alice Shao	SHECA Security Authentication Committee	Previous Version
V1.5.6	2024-07-01	Alice Shao	SHECA Security Authentication Committee	Previous Version
V1.5.5	2023-07-21	Celia Yu	SHECA Security Authentication Committee	Previous Version
V1.5.4	2023-06-12	Celia Yu	SHECA Security Authentication Committee	Previous Version
V1.5.3	2023-04-18	Celia Yu	SHECA Security Authentication Committee	Previous Version
V1.5.2	2022-04-18	Toria Chen	SHECA Security Authentication Committee	Previous Version
V1.5.1	2021-11-15	Toria Chen	SHECA Security Authentication Committee	Previous Version
V1.5	2021-6-18	Toria Chen	SHECA Security Authentication Committee	Previous Version
V1.4.9	2021-4-29	Toria Chen	SHECA Security Authentication Committee	Previous Version
V1.4.8	2020-8-11	Toria Chen	SHECA Security Authentication Committee	Previous Version
V1.4.7	2020-6-5	Toria Chen	SHECA Security Authentication Committee	Previous Version
V1.4.6	2020-4-30	Toria Chen	SHECA Security Authentication Committee	Previous Version
V1.4.5	2020-3-27	Toria Chen	SHECA Security Authentication Committee	Previous Version
V1.4.4	2019-5-29	Toria Chen	SHECA Security Authentication Committee	Previous Version
V1.4.3	2018-9-10	Toria Chen	SHECA Security Authentication Committee	Previous Version

V1.4.2	2018-8-31	Toria Chen	SHECA Security Authentication Committee	Previous Version
V1.4.1	2018-7-12	Toria Chen	SHECA Security Authentication Committee	Previous version
V1.4	2018-6-1	Toria Chen	SHECA Security Authentication Committee	Previous version
V1.3	2017-5-24	Ruby Xiong	SHECA Security Authentication Committee	Previous version
V1.2	2016-5-25	John Cui	SHECA Security Authentication Committee	Previous version
V1.1	2014-4-25	John Cui	SHECA Security Authentication Committee	Previous version
V1.0	2013-4-28	John Cui	SHECA Security Authentication Committee	Previous version

Changes Description

Version	Description
V1.5.9	Disclose tset web pages for EV certificates; Update initial identity validation requirements and methods; Update signature algorithm identifier; Update frequency and circumstances of assessment; Align paragraph structure with outline in RFC3647 section 6； Adjustment of wording;
V1.5.8	Update UniTrust EV PKI Hierarchy; Adjustment of wording
V1.5.7	Disclosure of newly issued Sub-CAs
V1.5.6	Update Sub-CAs status
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:

- RFC3647: Internet X.509 Public Key Infrastructure - Certificate Policies and Certificate business statement framework
- RFC6960: Internet X.509 Public Key Infrastructure - Online Certificate Status Protocol - OCSP
- ITU-T X.509 V3 (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework
- RFC5280: Internet X.509 Public Key Infrastructure - Certificate and CRL structure
- GB/T 26855-2011: Information Security Technology - Public Key Infrastructure - Framework for Certificate Policy and Certification Practice Statement
- GB/T 20518-2018: Information Security Technology - Public Key Infrastructure - Format of Digital Certificates
- GB/T 25056-2018: Information Security Technology - Cryptographic and Related Security Technical Specifications for Certificate Authority Systems
- GB/T 19713-2025: Cybersecurity Technology - Public Key Infrastructure - Online Certificate Status Protocol

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 UNTSH EV Certificate hierarchy (refer to Section 1.1.2) 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 EV CPS is formulated in accordance with UNTSH EV CP. SHECA doesn't set Affiliate, subcontractor, external RA or Enterprise RA that relate to EV Certificates. Subscriber, relying party and related entities use and trust certificate in accordance with this EV CPS and EV CP while performing obligations.

UNTSH EV Structure contains root CAs and subordinate CAs. EV Certificate services and management within UNTSH EV Structure should completely, accurately and comprehensively perform and implement the requirements of this document and EV CP.

1.1.2 UNTSH EV Certificate hierarchical structure

UNTSH EV Certificate hierarchical structure is as follows:

UCA Global G2 Root

- SHECA EV Server CA G2 (revoked)

UCA Extended Validation Root

- SHECA RSA Extended Validation Code Signing CA (revoked)
- SHECA RSA Extended Validation Server CA (revoked)
- SHECA EV Server CA G3
- SHECA EV Code Signing CA G2
- SHECA Extended Validation SSL CA (revoked)
- SHECA Extended Validation Code Signing CA (revoked)

- SHECA EV Code Signing CA G3
- SHECA EV TLS RSA CA C1
- SHECA EV TLS ECC CA C2

UniTrust Global Root CA R1 (ceased)

- SHECA EV Server CA 1A (revoked)
- SHECA EV Code Signing CA 1A (revoked)

UniTrust Global Root CA R2 (ceased)

- SHECA EV Server CA 2A (revoked)

UniTrust Global TLS RSA Root CA R1

- SHECA EV TLS RSA CA 1A

UniTrust Global TLS ECC Root CA R2

- SHECA EV TLS ECC CA 2A

UniTrust Global Code Signing RSA Root CA R1

- SHECA EV Code Signing RSA CA 1B

UniTrust Global Code Signing ECC Root CA R2

- SHECA EV Code Signing ECC CA 2A

Cross-signed Certificates:
UniTrust Global TLS RSA Root CA R1 is cross signed by **UCA Global G2 Root.**
UniTrust Global TLS ECC Root CA R2 is cross signed by **UCA Global G2 Root.**
UCA Global G2 Root is cross signed by **Certum Trusted Network CA**.

Detailed information and status of the above EV root CAs and sub-CAs is disclosed on SHECA's repository: https://www.sheca.com/repository/

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 object identifier (OID) of this document is 1.2.156.112570.1.0.4

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 the use is consistent with subject's identity that certificate represents. For example, Individual Certificate can not be used as Organizational or Equipment certificate, Organizational Certificate can not be used as Individual or Equipment Certificate, Equipment Certificate can not be used as Individual Certificate or Organizational Certificate. Any unmatched application hasn't the protection from the CPS.

The certificate usage is prohibited in such circumstances such as any violation of state laws, regulations and national security or legal consequences, or users legal results led by that by themselves. In particular, the certificate is not designed for, not intended for, nor authorized for using in application systems including personal injury, environmental damage and other applications, such as navigation or communication systems, traffic control systems or weapons control systems and so on.

1.5 Policy Administration

1.5.1 Organization Administering the Document

According to Electronic Signature Law of the People's Republic of China, Measures for Administration of Electronic Authentication Service and The Standard for Certification Practice Statement from Ministry of Industry and Information Technology, SHECA develops the Certification Practice Statement (CPS) and appoints a special body - SHECA Security Certification Committee as an agency of policy administration.

As an administration agency to develop all the policies under the SHECA certification system, SHECA Security Certification Committee consisting of members from management layer, directors of relevant departments (service, operational and technical departments, etc.) and staff in charge of writing corresponding CPS is responsible for auditing CPS and implementing inspection and supervision as the highest decision-making body.

As a CPS agency，SHECA Strategy Development Department is responsible for drafting the CPS ， is required to amend the report，and takes charge of external consultation services in this regard.

1.5.2 Contact Person

SHECA designated the strategy development department 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 strategy development department.

Contact: Shanghai Electronic Certification Authority Co.,Ltd. strategy development department.

Tel : 86 -21-36393197

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

Postal Code: 200080

Email: cps@sheca.com

Release of the Certification Practice Statement

The release methods of CPS include:

1、the electronic means, publishing in SHECA repository, Website address :

https://www.sheca.com/repository

2、the electronic way, by e-mail, e-mail address: getcps@sheca.com

3、in writing, issued by the SHECA Strategy Development Department. Address:18F, 1717 North Sichuan Road, Shanghai ,PRC ; Post code : 200080

1.5.3 Person Determining CPS Suitability for the Policy

CPS Decision in Line With Strategy Agency

As a competent department for electronic certification services, the Ministry of Industry and Information Technology issued "The Standard for Certification Practice Statement". SHECA has developed this CPS and submitted the MIIT for record. As the body for administrating the highest policy, SHECA Security Certification Committee is a decision-making organization in line with CPS policy which is responsible for approving and deciding whether the CPS meets the corresponding provisions of CP.

SHECA ensures that the CPS it develops and releases, the execution, interpretation, translation and effectiveness are in line with laws and regulations of PRC.

Strategy Development Department, as the authentication service department, is responsible for daily supervision and inspection of CPS implementation, and ensures that operation within the SHECA certification service system conforms to the requirements of the CPS.

Change of CPS

SHECA has the right to conduct scheduled and unscheduled revise to CPS. Scheduled revise is twice a year to check whether the CPS is consistent with the latest Guidelines, Baseline Requirement, latest S/MIME Baseline Requirements and Minimum Requirements for Code Signing Certificates of CA/Browser Forum, if not, CPS must be revised accordingly. Unscheduled revise to CPS happens when company business adjusts or CA/Browser Forum modifies the Guidelines, Baseline Requirement and Minimum Requirements for Code Signing Certificates which leads to the necessary change of CPS. Modified CPS will be recorded by MIIT within the prescribed time according to the requirements of Measures for Administration Electronic Authentication Service.

If the following situations occur, this CPS must be modified:

- The encryption technology develops significantly enough to affect the effectiveness of existing CPS.
- The certificate policy changes significantly
- The standards of relevant certification business shall be renewed.
- Certification system and relevant management regulations take significant upgrade or changes.
- The requirements of laws and regulations and competent department requirement.
- There is some important deficiency in the existing CPS.

For the revision of the CPS will take effect in release after seven days. Unless before the seven days, SHECA publishes a cancel revision notice in the same way.

However, if SHECA issues a amendment, and if the amendment is not entried into force timely, it will result in all or part of SHECA certification system damage, then the amendment should be immediate taken into effect from the date of release.

SHECA Security Certification Committee will research proposal report about modification provided by the Strategy Development Department prior to any changes in the CPS， and then it will make the final decision.

SHECA will announce the changed CPS on the website after the resolution forms. The changes of the CPS will take immediate effect from the released date of and the modifications of the CPS will replace any conflict and specified terms of the previous version.

SHECA will strictly control on version of CPS. Modified version will be published on SHECA website (https://www.sheca.com).

1.5.4 CPS Approval Procedures

After drafted by Strategy Development Department, the CPS is submitted to SHECA security certification Committee to audit. If the CPS will be modified because of changes in standards, improvements in technology, enhancements in security mechanism， changes in operating environment and the requirements of laws and regulations , the proposal report about modification will be submitted by Strategy Development Department, then would be audited by the SHECA Security Certification Commission to. After approved by the Committee, SHECA will publish it on the website: https://www.sheca.com.

Under the provisions of the "Electronic Signature Law of the People's Republic of China", "Measures for administration of Electronic Authentication Services" , SHECA should announce to the MIIT after publishing the CPS .

1.6 Definitions and Acronyms

Refer to Appendix A.

2. Publication and Repository Responsibilities

2.1 Repositories

SHECA repository is open to the public, it can store, retrieve certificates and its related information. SHECA repository includes but is not limited to the following: CP, CPS and other policy documents like the current and historical versions of the documents, certificates, CRL, and other information published from time to time by the SHECA. SHECA repository will not change any notification about certificate and certificate revocation that are published by the authority, but describe the above content accurately.

Deal with any related matter about SHECA, SHECA must use its repository as the main and the formal repository.

SHECA repository will release timely information about the certificate, CPS revision , revocation notice and so on that must remain consistence with the CPS and the relevant laws and regulations .You can via Web: https://www.sheca.com/repository/ to visit SHECA repository, or other communication methods specified by the SHECA at any time. SHECA can issue subscriber certificates and associated CRL information outside the SHECA repository. CPS prohibits anyone except those persons authorized by SHECA from visiting any confidential information CPS and / or SHECA declared (or other data maintained by the issuing authority) in repository.

2.2 Publication of Certificate Information

SHECA will publish related information on https://www.sheca.com； The site is the foremost, most timely, most authoritative channel releasing all the information. SHECA will publish the new information in time. Only SHECA is empowered to deal with old information on the site.

2.2.1 Directory Services

SHECA will release a copy of the certificate at the same time， when the subscriber accepts a certificate. The issuing authority also announces the certificate revoked within the valid period SHECA issues the certificate and the related information of certificate revocation through directory services. Users obtain these information by visiting the SHECA's directory server .It also provides services of online certificate status check, certificate revocation lists check services， etc.

2.2.2 The Release of Announcements and Notifications

SHECA will releases the Certification Practice Statement, Certificate Policies, business processes, technology and the changes of product timely by the form of bulletins and notification on website https://www.sheca.com, meanwhile, SHECA will also release in other possible forms.

SHECA will publish possible effective measure to protect the private key of certificate holder according to the new technological developments.

2.3 Time or Frequency of Publication

2.3.1 Time and Frequency of Certificate Practice Statement Releasing

SHECA will release the latest version of Certificate Practice Statement (CPS) in time. Once amendments to the CPS are approved, SHECA will post them on https://www.sheca.com and publish the latest CPS on SHECA repository, and list together with the original CPS in order to retrieve.

SHECA may change the CPS, with the technological advancements, business development, application promotion and the objective requirements of laws and regulations. The releasing time and frequency of the CPS will be independently decided by the SHECA. This publication should be immediate, efficient, and be consistent with the national laws and regulations. The CPS should be updated at least for one-year period.

The current CPS is effective and is in the implementation of the state, before the SHECA releasing a new CPS or any form of announcements, notices to modify, supply, adjust or update for CPS. Only the SHECA has the right to change any form of the state.

2.3.2 Time and Frequency of Certificates Releasing

Issuing authority will publish copy of the certificate in SHECA repository or one or more other repository decided by the SHECA and its issuing certificate authority, once the subscribers accept the certificate. Subscribers can also publish their certificates issued by SHECA in other repository.

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://issp.sheca.com/Query/CertQuery.

2.3.3 Time and Frequency of the CRL Publishing

Issuing authority must immediately issue revocation notice in SHECA repository, after the revocation of the certificate issued. SHECA will publish one or more of the following: publishing a list of certificates revoked which can be obtained through a secure channel.

The requester can instantaneously view and obtain the state as well as the effectiveness of a certificate through the OCSP. SHECA can also provide follow-up services, after the requirements are met. When the specified certificate is revoked, SHECA will notify the service requester in accordance with the agreement.

All CRL will be released by the SHECA directory server. SHECA should release Certificate Revocation List (CRL) of a subscriber certificate at least once every 5 days or within 24 hours after the subscriber certificate is revoked. The difference of the subscriber certificate CRL between the next update time (nextUpdate) and this update time (thisUpdate) must be less than or equal to 7 days.

SHECA should release Certificate Revocation List of a sub-CA certificate (ARL) at least once every 7 months. If the root certificate is revoked, revocation information is published on the website in time. The difference between of the Sub-CA certificate ARL 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.

In case of emergency, SHECA can choose time and frequency of the certificate revocation list to publish.

2.3.4 Time and Frequency of Announcement，Notification and Other Information Releasing

Once there is a need to publish notification and announcement related to electronic authentication service for some reason, SHECA will release these information on website https://www.sheca.com in time.

The release of such information is at irregular intervals. SHECA ensures that the information will be released at the first time.

2.3.5 The Releasing Time and Frequency of Customer Service, Business Structure, Market Development and Other Information

SHECA will publish related information on the website https://www.sheca.com at any time.

2.3.6 Tset Web Pages for EV Certificates

SHECA MUST host test Web pages that allow Application Software Suppliers to test their software with EV Certificates that chain up to each EV Root Certificate. At a minimum, SHECA MUST host separate Web pages using certificates that are Valid, Revoked, and Expired.

ROOT	Test Web Page
UCA Extended Validation Root	https://rsaevg3.good.sheca.com https://rsaevg3.revoked.sheca.com

	https://rsaevg3.expired.sheca.com
UniTrust Global TLS ECC Root CA R2	https://eccev2a.good.sheca.com https://eccev2a.revoked.sheca.com https://eccev2a.expired.sheca.com
UniTrust Global TLS RSA Root CA R1	https://rsaev1a.good.sheca.com https://rsaev1a.revoked.sheca.com https://rsaev1a.expired.sheca.com

2.4 Access Controls on Repositories

2.4.1 SSL Channel

Hypertext Transfer Protocol (HTTPS) was used to access to sensitive information with Secure Sockets Layer protocol (SSL), In order to achieve access to the safe mode of records (must use an SSL-enabled browser).

2.4.2 Rights Management and Security Audit Channel

SHECA sets up access control and security auditing measures to ensure that the one authorized by SHECA can write and modify the SHECA related information published online.

SHECA can make implementation to access control certain SHECA information related in order to ensure that only SHECA certificate holders have the right to read the information, when it is necessary. SHECA can decide whether to take the rights management.

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	Y

	Must be approved by government department	
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
eJurisdiction 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

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

All certificate holders' names are required to be unique. SHECA identifies certificate holders according to the name. When the same name appears, the first applicant is preferential, the other applicant name should be identified through the difference followed by the unique identification code.

The first applicant applies for the registration is priority in use, when the subscriber or applicant uses the same name. SHECA has no rights and obligations to deal with the related dispute, and the relevant users can apply to the relevant authorities to resolve.

When the subscriber or applicant's names are proved by the legal documents of the competent authorities that they are belong to other subscribers or applicant, SHECA will cancel the right of previous subscriber to use the name immediately and revoke the user certificate. The subscriber must assume legal liability of the resulting. It is not SHECA's responsibility to verify the legitimacy of subscriber or applicant.

Naming agencies, the SHECA naming authority coordinates all SHECA Relative Distinguished Names issuance. SHECA naming agencies determine the naming convention of subject name of SHECA repository, which may be due to the difference between certificate categories and issuing authorities. These naming conventions vary for the difference between certification issuance and re-issue / re-registration certificates.

SHECA naming agencies have the right to specify the name of Relative Distinguished Names (RDN) and the certificate serial number in the certificate issued by SHECA. When naming agencies specify relative distinguished names, the relevant certificates about screening name will be asked to provide, or inquiries to the appropriate agency to determine whether the subscriber has the right to use the appropriate distinguished name.

3.1.6 Recognition, Authentication, and Role of Trademarks

The trademark information is allowed to be contained in subscriber's certificate, but can not be used for identifying individuals, organization or device. 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.

Any certificate applicants are prohibited from using names in their certificate applications that infringe upon the Intellectual Property Rights of others. SHECA does not verify or arbitrate whether a certificate applicant has intellectual property rights over the name appearing in a certificate application. SHECA does not resolve any dispute concerning the ownership of any domain name, trade name, trademark, or service mark, or ensure for the uniqueness of this right. 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

SHECA must verify that the applicant has the legitimacy and correctness of the private key. SHECA may verify the applicant's private key at least by one of the following methods:

1、If a subscriber requests a certificate using its private key to sign on the application information, SHECA and its authorized service agencies must verify the correctness, legality and uniqueness of the public key and private key as well as the applicant identity information.

2、SHECA and its authorized service agencies provide the applicant with certificate initialization information for completing the certificate request (such as a password envelope). When the certificate applicant is applying for a certificate or certain certificate operations, the applicant must use the initialization information to ensure the applicant is the legitimate owner of the private key. Initialization information is generally safely delivered to the certificate applicant off-line.

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.

3.2.2.1 Overview

This part sets forth Verification Requirements and Acceptable Methods of Verification for each such Requirement.

Verification Requirements – Overview

EV certificates are only offered to government department, enterprises, institutions, social organizations and other institutions. SHECA must identify and verify the following:

1. Verify Applicant's existence and identity, including;

A. Verify the Applicant's legal existence and identity (as more fully set forth in Section 3.2.2.2),

B. Verify the Applicant's physical existence (business presence at a physical address), and

C. Verify the Applicant's operational existence (business activity).

2. Verify the Applicant is a registered holder, or has control, of the Domain Name(s) to be included in the EV Certificate;

3. Verify a reliable means of communication with the entity to be named as the Subject in the Certificate;

4. Verify the Applicant's authorization for the EV Certificate, including;

A. Verify the name, title, and authority of the Contract Signer, Certificate Approver, and Certificate Requester,

B. Verify that a Contract Signer signed the Subscriber Agreement or that a duly authorized Applicant Representative acknowledged and agreed to the Terms of Use; and

C. Verify that a Certificate Approver has signed or otherwise approved the EV Certificate Request.

Acceptable Methods of Verification – Overview

As a general rule, SHECA is responsible for taking all verification steps reasonably necessary to satisfy each of the Verification Requirements set forth in the subsections below. The Acceptable Methods of Verification set forth in each of Sections 3.2.2 through 3.2.14 (which usually include alternatives) are considered to be the minimum acceptable level of verification required of SHECA. In all cases, however, SHECA is responsible for taking any

additional verification steps that may be reasonably necessary under the circumstances to satisfy the applicable Verification Requirement.

Disclosure of Verification Sources

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

3.2.2.2 Verification of Applicant's Legal Existence and Identity

Verification Requirements

To verify the Applicant's legal existence and identity, SHECA MUST do the following.

1.Private Organization Subjects

Legal Existence: Verify that the Applicant is a legally recognized entity, in existence and validly formed (e.g., incorporated) with the Incorporating or Registration Agency in the Applicant's Jurisdiction of Incorporation or Registration, and not designated on the records of the Incorporating or Registration Agency by labels such as “inactive”, “invalid”, “not current”, or the equivalent.

Organization Name: Verify that the Applicant's formal legal name as recorded with the Incorporating or Registration Agency in the Applicant's Jurisdiction of Incorporation or Registration matches the Applicant's name in the EV Certificate Request.

Registration Number: Obtain the specific Registration Number assigned to the Applicant by the Incorporating or Registration Agency in the Applicant's Jurisdiction of Incorporation or Registration. Where the Incorporating or Registration Agency does not assign a Registration Number, SHECA SHALL obtain the Applicant's date of Incorporation or Registration.

Registered Agent: Obtain the identity and address of the Applicant's Registered Agent or Registered Office (as applicable in the Applicant's Jurisdiction of Incorporation or Registration).

2.Government Entity Subjects

Legal Existence: Verify that the Applicant is a legally recognized Government Entity, in existence in the political subdivision in which such Government Entity operates.

Entity Name: Verify that the Applicant's formal legal name matches the Applicant's name in the EV Certificate Request.

Registration Number: SHECA MUST attempt to obtain the Applicant's date of incorporation, registration, or formation, or the identifier for the legislative act that created the Government Entity. In circumstances where this information is not available, SHECA MUST enter appropriate language to indicate that the Subject is a Government Entity.

3.Business Entity Subjects

Legal Existence: Verify that the Applicant is engaged in business under the name submitted by the Applicant in the Application.

Organization Name: Verify that the Applicant's formal legal name as recognized by the Registration Agency in the Applicant's Jurisdiction of Registration matches the Applicant's name in the EV Certificate Request.

Registration Number: Attempt to obtain the specific unique Registration Number assigned to the Applicant by the Registration Agency in the Applicant's Jurisdiction of Registration. Where the Registration Agency does not assign a Registration Number, SHECA SHALL obtain the Applicant's date of Registration.

Principal Individual: Verify the identity of the identified Principal Individual.

4.Non-Commercial Entity Subjects (International Organizations)

Legal Existence: Verify that the Applicant is a legally recognized International Organization Entity.

Entity Name: Verify that the Applicant's formal legal name matches the Applicant's name in the EV Certificate Request.

Registration Number: SHECA MUST attempt to obtain the Applicant's date of formation, or the identifier for the legislative act that created the International Organization Entity. In circumstances where this information is not available,SHECA MUST enter appropriate language to indicate that the Subject is an International Organization Entity.

Acceptable Method of Verification

1.Private Organization Subjects

Unless verified under subsection (6), all items listed in Section 3.2.2.2.1 (1) MUST be verified directly with, or obtained directly from, the Incorporating or Registration Agency in the Applicant's Jurisdiction of Incorporation or Registration. Such verification MAY be through use of a Qualified Government Information Source operated by, or on behalf of, the Incorporating or Registration Agency, or by direct contact with the Incorporating or Registration Agency in person or via mail, e-mail, Web address, or telephone, using an address or phone number obtained directly from the Qualified Government Information Source, Incorporating or Registration Agency, or from a Qualified Independent Information Source.

2.Government Entity Subjects

Unless verified under subsection (6), all items listed in Section 3.2.2.2.1 (2) MUST either be verified directly with, or obtained directly from, one of the following:

I. a Qualified Government Information Source in the political subdivision in which such Government Entity operates;

II. a superior governing Government Entity in the same political subdivision as the Applicant (e.g. a Secretary of State may verify the legal existence of a specific State Department), or

III. from a judge that is an active member of the federal, state or local judiciary within that political subdivision.

Any communication from a judge SHALL be verified in the same manner as is used for verifying factual assertions that are asserted by an Attorney as set forth in Section 3.2.2.11.1.

Such verification MAY be by direct contact with the appropriate Government Entity in person or via mail, e-mail, Web address, or telephone, using an address or phone number obtained from a Qualified Independent Information Source.

3.Business Entity Subjects

Unless verified under subsection (6), Items listed in Section 3.2.2.2.1 (3) (A) through (C) above, MUST be verified directly with, or obtained directly from, the Registration Agency in the Applicant's Jurisdiction of Registration. Such verification MAY be performed by means of a Qualified Government Information Source, a Qualified Governmental Tax Information Source, or by direct contact with the Registration Agency in person or via mail, e-mail, Web address, or telephone, using an address or phone number obtained directly from the Qualified Government Information Source, Qualified Governmental Tax Information Source or Registration Agency, or from a Qualified Independent Information Source. In addition, SHECA MUST validate a Principal Individual associated with the Business Entity pursuant to the requirements in subsection (4), below.

4.Principal Individual

A Principal Individual associated with the Business Entity MUST be validated in a face-to-face setting. SHECA MAY rely upon a face-to-face validation of the Principal Individual performed by the Registration Agency, provided that SHECA has evaluated the validation procedure and concluded that it satisfies the requirements of the Guidelines for face-to-face validation procedures. Where no face-to-face validation was conducted by the Registration Agency, or the Registration Agency's face-to-face validation procedure does not satisfy the requirements of the Guidelines, SHECA SHALL perform face-to-face validation.

A. Face-To-Face Validation: The face-to-face validation MUST be conducted before either an employee of SHECA, a Latin Notary, a Notary (or equivalent in the Applicant's jurisdiction), a Lawyer, or Accountant (Third-Party Validator). The Principal Individual(s) MUST present the following documentation (Vetting Documents) directly to the Third-Party Validator:

i. A Personal Statement that includes the following information:

1. Full name or names by which a person is, or has been, known (including all other names used);

2. Residential Address at which he/she can be located;

3. Date of birth; and

4. An affirmation that all of the information contained in the Certificate Request is true and correct.

ii. A current signed government-issued identification document that includes a photo of the Individual and is signed by the Individual such as:

1. A passport;

2. A driver's license;

3. A personal identification card; or

4. A military ID.

iii. At least two secondary documentary evidences to establish his/her identity that include the name of the Individual, one of which MUST be from a financial institution.

1. Acceptable financial institution documents include:

a. A major credit card, provided that it contains an expiration date and it has not expired’

b. A debit card from a regulated financial institution, provided that it contains an expiration date and it has not expired,

c. A mortgage statement from a recognizable lender that is less than six months old,

d. A bank statement from a regulated financial institution that is less than six months old.

2. Acceptable non-financial documents include:

a. Recent original utility bills or certificates from a utility company confirming the arrangement to pay for the services at a fixed address (not a mobile/cellular telephone bill),

b. A copy of a statement for payment of a lease, provided that the statement is dated within the past six months,

c. A certified copy of a birth certificate,

d. A local authority tax bill for the current year,

e. A certified copy of a court order, such as a divorce certificate, annulment papers, or adoption papers.

The Third-Party Validator performing the face-to-face validation MUST:

i. Attest to the signing of the Personal Statement and the identity of the signer; and

ii. Identify the original Vetting Documents used to perform the identification. In addition, the Third-Party Validator MUST attest on a copy of the current signed government-issued photo identification document that it is a full, true, and accurate reproduction of the original.

B. Verification of Third-Party Validator: SHECA MUST independently verify that the Third-Party Validator is a legally-qualified Latin Notary or Notary (or legal equivalent in the Applicant's jurisdiction), lawyer, or accountant in the jurisdiction of the Individual's residency, and that the Third-Party Validator actually did perform the services and did attest to the signature of the Individual.

C. Cross-checking of Information: SHECA MUST obtain the signed and attested Personal Statement together with the attested copy of the current signed government-issued photo identification document. SHECA MUST review the documentation to determine that the information is consistent, matches the information in the application, and identifies the Individual. SHECA MAY rely on electronic copies of this documentation, provided that:

i. SHECA confirms their authenticity (not improperly modified when compared with the underlying original) with the Third-Party Validator; and

ii. electronic copies of similar kinds of documents are recognized as legal substitutes for originals under the laws of SHECA's jurisdiction.

5.Non-Commercial Entity Subjects (International Organization)

Unless verified under subsection (6), all items listed in Section 3.2.2.2.1 (4) MUST be verified either:

A. With reference to the constituent document under which the International Organization was formed; or

B. Directly with a signatory country's government in which SHECA is permitted to do business. Such verification may be obtained from an appropriate government agency or from the laws of that country, or by verifying that the country's government has a mission to represent it at the International Organization; or

C. Directly against any current list of qualified entities that CA/Browser Forum may maintain at www.cabforum.org.

D. In cases where the International Organization applying for the EV Certificate is an organ or agency - including a non-governmental organization of a verified International Organization, then SHECA may verify the International Organization Applicant directly with the verified umbrella International Organization of which the Applicant is an organ or agency.

6.Verified Professional Letter

SHECA may rely on a Verified Professional Letter to establish the Applicant's information listed in (1)-(5) above if:

the Verified Professional Letter includes a copy of supporting documentation used to establish the Applicant's legal existence, such as a certificate of registration, articles of incorporation, operating agreement, statute, or regulatory act, and

SHECA confirms the Applicant's organization name specified in the Verified Professional Letter with a QIIS or QGIS.

3.2.2.3 Verification of Applicant's Legal Existence and Identity - Assumed Name

Assumed name is not allowed for application of EV certificates from SHECA.

3.2.2.4 Verification of Applicant's Physical Existence

Address of Applicant's Place of Business

1.Verification Requirements: To verify the Applicant's physical existence and business presence, SHECA MUST verify that the physical address provided by the Applicant is an address where the Applicant or a Parent/Subsidiary Company conducts business operations (not, for example, a mail drop or P.O. box, or 'care of' (C/O) address, such as an address for an agent of the Organization), and is the address of the Applicant's Place of Business.

2. Acceptable Methods of Verification

A. Place of Business in the Country of Incorporation or Registration

i. For Applicants whose Place of Business is in the same country as the Applicant's Jurisdiction of Incorporation or Registration and whose Place of Business is NOT the same as that indicated in the relevant Qualified Government Information Source used in Section 3.2.2.2 to verify legal existence:

1. For Applicants listed at the same Place of Business address in the current version of either at least one QGIS (other than that used to verify legal existence), QIIS or QTIS, SHECA MUST confirm that the Applicant's address, as listed in the EV Certificate Request, is a valid business address for the Applicant or a Parent/Subsidiary Company by reference to such QGIS, QIIS, or QTIS, and MAY rely on the Applicant's representation that such address is its Place of Business;

2. For Applicants who are not listed at the same Place of Business address in the current version of either at least one QIIS or QTIS, SHECA MUST confirm that the address provided by the Applicant in the EV Certificate Request is the Applicant's or a Parent/Subsidiary Company's business address, by obtaining documentation of a site visit to

the business address, which MUST be performed by a reliable individual or firm. The documentation of the site visit MUST:

a. Verify that the Applicant's business is located at the exact address stated in the EV Certificate Request (e.g., via permanent signage, employee confirmation, etc.),

b. Identify the type of facility (e.g., office in a commercial building, private residence, storefront, etc.) and whether it appears to be a permanent business location,

c. Indicate whether there is a permanent sign (that cannot be moved) that identifies the Applicant,

d. Indicate whether there is evidence that the Applicant is conducting ongoing business activities at the site (not that it is just, for example, a mail drop, P.O. box, etc.), and

e. Include one or more photos of

i. the exterior of the site (showing signage indicating the Applicant's name, if present, and showing the street address if possible), and

ii. the interior reception area or workspace.

ii. For all Applicants, SHECA MAY alternatively rely on a Verified Professional Letter that indicates the address of the Applicant's or a Parent/Subsidiary Company's Place of Business and that business operations are conducted there.

iii. For Government Entity Applicants, SHECA MAY rely on the address contained in the records of the QGIS in the Applicant's jurisdiction.

iv. For Applicants whose Place of Business is in the same country as the Applicant's Jurisdiction of Incorporation or Registration and where the QGIS used in Section 3.2.2.2 to verify legal existence contains a business address for the Applicant, SHECA MAY rely on the address in the QGIS to confirm the Applicant's or a Parent/Subsidiary Company's address as listed in the EV Certificate Request, and MAY rely on the Applicant's representation that such address is its Place of Business.

B. Place of Business not in the Country of Incorporation or Registration: SHECA MUST rely on a Verified Professional Letter that indicates the address of the Applicant's Place of Business and that business operations are conducted there.

3.2.2.5 Verified Method of Communication

Verification Requirements

To assist in communicating with the Applicant and confirming that the Applicant is aware of and approves issuance, SHECA MUST verify a telephone number, fax number, email address, or postal delivery address as a Verified Method of Communication with the Applicant.

Acceptable Methods of Verification

To verify a Verified Method of Communication with the Applicant, SHECA MUST:

A. Verify that the Verified Method of Communication belongs to the Applicant, or a Parent/Subsidiary or Affiliate of the Applicant, by matching it with one of the Applicant's Parent/Subsidiary or Affiliate's Places of Business in:

i. records provided by the applicable phone company;

ii. a QGIS, QTIS, or QIIS; or

iii. a Verified Professional Letter; and

B. Confirm the Verified Method of Communication by using it to obtain an affirmative response sufficient to enable a reasonable person to conclude that the Applicant, or a Parent/Subsidiary or Affiliate of Applicant, can be contacted reliably by using the Verified Method of Communication.

3.2.2.6 Verification of Applicant's Operational Existence

Verification Requirements

SHECA MUST verify that the Applicant has the ability to engage in business by verifying the Applicant's, or Affiliate/Parent/Subsidiary Company's, operational existence. SHECA MAY rely on its verification of a Government Entity's legal existence under Section 3.2.2.2 as verification of a Government Entity's operational existence.

Acceptable Methods of Verification

To verify the Applicant's ability to engage in business, SHECA MUST verify the operational existence of the Applicant, or its Affiliate/Parent/Subsidiary Company, by:

1. Verifying that the Applicant, Affiliate, Parent Company, or Subsidiary Company has been in existence for at least three years, as indicated by the records of an Incorporating Agency or Registration Agency;

2. Verifying that the Applicant, Affiliate, Parent Company, or Subsidiary Company is listed in either a current QIIS or QTIS;

3. Verifying that the Applicant, Affiliate, Parent Company, or Subsidiary Company has an active current Demand Deposit Account with a Regulated Financial Institution by receiving authenticated documentation of the Applicant's, Affiliate's, Parent Company's, or Subsidiary Company's Demand Deposit Account directly from a Regulated Financial Institution; or

4. Relying on a Verified Professional Letter to the effect that the Applicant has an active current Demand Deposit Account with a Regulated Financial Institution.

3.2.2.7 Verification of Applicant's Domain Name

Domain Recognition and Identification is implemented compliance with section 3.2.2.4 of UniTrust CPS.

SHECA SHALL NOT issue certificates for onion or arpa domain names. For each Fully-Qualified Domain Name listed in a Certificate, SHECA SHALL confirm that, as of the date the Certificate was issued, the Applicant (or the Applicant's Parent Company, Subsidiary Company, or Affiliate, collectively referred to as “Applicant” for the purposes of this section) either is the Domain Name Registrant or has control over the FQDN using a procedure specified in Section 3.2.2.4 of the Baseline Requirements.

Mixed Character Set Domain Names: EV Certificates MAY include Domain Names containing mixed character sets only in compliance with the rules set forth by the domain registrar. SHECA MUST visually compare any Domain Names with mixed character sets with known high risk domains. If a similarity is found, then the EV Certificate Request

MUST be flagged as High Risk. SHECA must perform reasonably appropriate additional authentication and verification to be certain beyond reasonable doubt that the Applicant and the target in question are the same organization.

3.2.2.8 Verification of Name, Title, and Authority of Contract Signer and Certificate Approver

Verification Requirements

For both the Contract Signer and the Certificate Approver, SHECA MUST verify the following.

1. Name, Title and Agency: SHECA MUST verify the name and title of the Contract Signer and the Certificate Approver, as applicable. SHECA MUST also verify that the Contract Signer and the Certificate Approver are agents representing the Applicant.

2. Signing Authority of Contract Signer: SHECA MUST verify that the Contract Signer is authorized by the Applicant to enter into the Subscriber Agreement (and any other relevant contractual obligations) on behalf of the Applicant, including a contract that designates one or more Certificate Approvers on behalf of the Applicant.

3. EV Authority of Certificate Approver: SHECA MUST verify, through a source other than the Certificate Approver him- or herself, that the Certificate Approver is expressly authorized by the Applicant to do the following, as of the date of the EV Certificate Request:

A. Submit, and, if applicable, authorize a Certificate Requester to submit, the EV Certificate Request on behalf of the Applicant; and

B. Provide, and, if applicable, authorize a Certificate Requester to provide, the information requested from the Applicant by SHECA for issuance of the EV Certificate; and

C. Approve EV Certificate Requests submitted by a Certificate Requester.

Acceptable Methods of Verification – Name, Title and Agency

Acceptable methods of verification of the name, title, and agency status of the Contract Signer and the Certificate Approver include the following.

1.Name and Title: SHECA MAY verify the name and title of the Contract Signer and the Certificate Approver by any appropriate method designed to provide reasonable assurance that a person claiming to act in such a role is in fact the named person designated to act in such role.

2.Agency: SHECA MAY verify the agency of the Contract Signer and the Certificate Approver by:

A. Contacting the Applicant using a Verified Method of Communication for the Applicant, and obtaining confirmation that the Contract Signer and/or the Certificate Approver, as applicable, is an employee;

B. Obtaining an Independent Confirmation From the Applicant (as described in Section 3.2.2.11.4), or a Verified Professional Letter verifying that the Contract Signer and/or the Certificate Approver, as applicable, is either an employee or has otherwise been appointed as an agent of the Applicant; or

C. Obtaining confirmation from a QIIS or QGIS that the Contract Signer and/or Certificate Approver is an employee of the Applicant.

SHECA MAY also verify the agency of the Certificate Approver via a certification from the Contract Signer (including in a contract between SHECA and the Applicant signed

by the Contract Signer), provided that the employment or agency status and Signing Authority of the Contract Signer has been verified.

Acceptable Methods of Verification – Authority

Acceptable methods of verification of the Signing Authority of the Contract Signer, and the EV Authority of the Certificate Approver, as applicable, include:

1. Verified Professional Letter: The Signing Authority of the Contract Signer, and/or the EV Authority of the Certificate Approver, MAY be verified by reliance on a Verified Professional Letter;

2. Corporate Resolution: The Signing Authority of the Contract Signer, and/or the EV Authority of the Certificate Approver, MAY be verified by reliance on a properly authenticated corporate resolution that confirms that the person has been granted such Signing Authority, provided that such resolution is

i. certified by the appropriate corporate officer (e.g., secretary), and

ii. SHECA can reliably verify that the certification was validly signed by such person, and that such person does have the requisite authority to provide such certification;

3. Independent Confirmation from Applicant: The Signing Authority of the Contract Signer, and/or the EV Authority of the Certificate Approver, MAY be verified by obtaining an Independent Confirmation from the Applicant (as described in Section 3.2.2.11.4);

4. Contract between CA and Applicant: The EV Authority of the Certificate Approver MAY be verified by reliance on a contract between SHECA and the Applicant that designates the Certificate Approver with such EV Authority, provided that the contract is signed by the Contract Signer and provided that the agency and Signing Authority of the Contract Signer have been verified;

5. Prior Equivalent Authority: The signing authority of the Contract Signer, and/or the EV authority of the Certificate Approver, MAY be verified by relying on a demonstration of Prior Equivalent Authority.

A. Prior Equivalent Authority of a Contract Signer MAY be relied upon for confirmation or verification of the signing authority of the Contract Signer when the Contract Signer has executed a binding contract between SHECA and the Applicant with a legally valid and enforceable seal or handwritten signature and only when the contract was executed more than 90 days prior to the EV Certificate application. SHECA MUST record sufficient details of the previous agreement to correctly identify it and associate it with the EV application. Such details MAY include any of the following:

i. Agreement title,

ii. Date of Contract Signer's signature,

iii. Contract reference number, and

iv. Filing location.

B. Prior Equivalent Authority of a Certificate Approver MAY be relied upon for confirmation or verification of the EV Authority of the Certificate Approver when the Certificate Approver has performed one or more of the following:

i. Under contract to SHECA, has served (or is serving) as an Enterprise RA for the Applicant, or

ii. Has participated in the approval of one or more certificate requests, for certificates issued by SHECA and which are currently and verifiably in use by the Applicant. In this case SHECA MUST have contacted the Certificate Approver by phone at a previously validated phone number or have accepted a signed and notarized letter approving the certificate request.

6. QIIS or QGIS: The Signing Authority of the Contract Signer, and/or the EV Authority of the Certificate Approver, MAY be verified by a QIIS or QGIS that identifies the Contract Signer and/or the Certificate Approver as a corporate officer, sole proprietor, or other senior official of the Applicant.

7. Contract Signer's Representation/Warranty: Provided that SHECA verifies that the Contract Signer is an employee or agent of the Applicant, SHECA MAY rely on the signing authority of the Contract Signer by obtaining a duly executed representation or warranty from the Contract Signer that includes the following acknowledgments:

A. That the Applicant authorizes the Contract Signer to sign the Subscriber Agreement on the Applicant's behalf,

B. That the Subscriber Agreement is a legally valid and enforceable agreement,

C. That, upon execution of the Subscriber Agreement, the Applicant will be bound by all of its terms and conditions,

D. That serious consequences attach to the misuse of an EV certificate, and

E. The contract signer has the authority to obtain the digital equivalent of a corporate seal, stamp or officer's signature to establish the authenticity of the company's Web site.

Pre-Authorized Certificate Approver

Where SHECA and Applicant contemplate the submission of multiple future EV Certificate Requests, then, after SHECA:

1. Has verified the name and title of the Contract Signer and that he/she is an employee or agent of the Applicant; and

2. Has verified the Signing Authority of such Contract Signer in accordance with one of the procedures in Section 3.2.2.8.3.

SHECA and the Applicant MAY enter into a written agreement, signed by the Contract Signer on behalf of the Applicant, whereby, for a specified term, the Applicant expressly authorizes one or more Certificate Approver(s) designated in such agreement to exercise EV Authority with respect to each future EV Certificate Request submitted on behalf of the Applicant and properly authenticated as originating with, or otherwise being approved by, such Certificate Approver(s).

Such an agreement MUST provide that the Applicant shall be obligated under the Subscriber Agreement for all EV Certificates issued at the request of, or approved by, such Certificate Approver(s) until such EV Authority is revoked, and MUST include mutually agreed-upon provisions for:

i. authenticating the Certificate Approver when EV Certificate Requests are approved,

ii. periodic re-confirmation of the EV Authority of the Certificate Approver,

iii. secure procedures by which the Applicant can notify SHECA that the EV Authority of any such Certificate Approver is revoked, and

iv. such other appropriate precautions as are reasonably necessary.

3.2.2.9 Verification of Signature on Subscriber Agreement and EV Certificate Requests

Both the Subscriber Agreement and each non-pre-authorized EV Certificate Request MUST be signed. The Subscriber Agreement MUST be signed by an authorized Contract Signer. The EV Certificate Request MUST be signed by the Certificate Requester submitting the document, unless the Certificate Request has been pre-authorized in line with Section

3.2.2.8.4. If the Certificate Requester is not also an authorized Certificate Approver, then an authorized Certificate Approver MUST independently approve the EV Certificate Request. In all cases, applicable signatures MUST be a legally valid and contain an enforceable seal or handwritten signature (for a paper Subscriber Agreement and/or EV Certificate Request), or a legally valid and enforceable electronic signature (for an electronic Subscriber Agreement and/or EV Certificate Request), that binds the Applicant to the terms of each respective document.

1. Signature: SHECA MUST authenticate the signature of the Contract Signer on the Subscriber Agreement and the signature of the Certificate Requester on each EV Certificate Request in a manner that makes it reasonably certain that the person named as the signer in the applicable document is, in fact, the person who signed the document on behalf of the Applicant.

2. Approval Alternative: In cases where an EV Certificate Request is signed and submitted by a Certificate Requester who does not also function as a Certificate Approver, approval and adoption of the EV Certificate Request by a Certificate Approver in accordance with the requirements of Section 3.2.2.10 can substitute for authentication of the signature of the Certificate Requester on such EV Certificate Request.

3.2.2.10 Verification of Approval of EV Certificate Request

In cases where an EV Certificate Request is submitted by a Certificate Requester, before SHECA issues the requested EV Certificate, SHECA MUST verify that an authorized Certificate Approver reviewed and approved the EV Certificate Request.

3.2.2.11 Verification of Certain Information Sources

SHECA adopts the following verified information source:

1.Verified Legal Opinion according to section 3.2.2.11.1 of EV Guidelines

2.Verified Accountant Letter according to section 3.2.2.11.2 of EV Guidelines

3.Face-to-Face Validation according to section 3.2.2.11.3 of EV Guidelines

4.Independent Confirmation From Applicant according to section 3.2.2.11.4 of EV Guidelines

5.Qualified Independent Information Source according to section 3.2.2.11.5 of EV Guidelines

6.Qualified Government Information Source according to section 3.2.2.11.6 of EV Guidelines

7.Qualified Government Tax Information Source according to section 3.2.2.11.7 of EV Guidelines

3.2.2.12 Other Verification Requirements

The High Risk Certificate requirements of Section 4.2.1 of the Baseline Requirements apply equally to EV Certificates.

SHECA MUST verify whether the Applicant, the Contract Signer, the Certificate Approver, the Applicant's Jurisdiction of Incorporation, Registration, or Place of Business:

A. Is identified on any government denied list, list of prohibited persons, or other list that prohibits doing business with such organization or person under the laws of the country of SHECA's jurisdiction(s) of operation; or

B. Has its Jurisdiction of Incorporation, Registration, or Place of Business in any country with which the laws of SHECA's jurisdiction prohibit doing business.

SHECA MUST NOT issue any EV Certificate to the Applicant if either the Applicant, the Contract Signer, or Certificate Approver or if the Applicant's Jurisdiction of Incorporation or Registration or Place of Business is on any such list.

SHECA MUST take reasonable steps to verify with government denied lists and export regulations.

SHECA verifying an Applicant using information of the Applicant's Parent, Subsidiary, or Affiliate, when allowed under Section 3.2.2.4.1, Section 3.2.2.5, Section 3.2.2.6.1, or Section 3.2.2.7.1, MUST verify the Applicant's relationship to the Parent, Subsidiary, or Affiliate. Acceptable methods of verifying the Applicant's relationship to the Parent, Subsidiary, or Affiliate.

3.2.2.13 Final Cross-Correlation and Due Diligence

1. The results of the verification processes and procedures outlined in these Guidelines are intended to be viewed both individually and as a group. Thus, after all of the verification processes and procedures are completed, SHECA MUST have a person who is not responsible for the collection of information review all of the information and documentation assembled in support of the EV Certificate application and look for discrepancies or other details requiring further explanation.

2. SHECA MUST obtain and document further explanation or clarification from the Applicant, Certificate Approver, Certificate Requester, Qualified Independent Information Sources, and/or other sources of information, as necessary, to resolve those discrepancies or details that require further explanation.

3. SHECA MUST refrain from issuing an EV Certificate until the entire corpus of information and documentation assembled in support of the EV Certificate Request is such that issuance of the EV Certificate will not communicate factual information that SHECA knows, or the exercise of due diligence should discover from the assembled information and documentation, to be inaccurate,. If satisfactory explanation and/or additional documentation are not received within a reasonable time, SHECA MUST decline the EV Certificate Request and SHOULD notify the Applicant accordingly.

4. In case where some or all of the documentation used to support the application is in a language other than SHECA's normal operating language, SHECA or its Affiliate MUST perform the requirements of this Final Cross-Correlation and Due Diligence section using employees under its control and having appropriate training, experience, and judgment in confirming organizational identification and authorization and fulfilling all qualification requirements contained in Section 5.3.2. When employees under the control of SHECA do not possess the language skills necessary to perform the Final Cross-Correlation and Due Diligence a CA MAY:

A. Rely on language translations of the relevant portions of the documentation, provided that the translations are received from a Translator; or

B. When SHECA has utilized the services of an RA, SHECA MAY rely on the language skills of the RA to perform the Final Cross-Correlation and Due Diligence, provided that the RA complies with Section 3.2.2.13, Subsections (1), (2) and (3). Notwithstanding the

foregoing, prior to issuing the EV Certificate, SHECA MUST review the work completed by the RA and determine that all requirements have been met; or

C. When SHECA has utilized the services of an RA, SHECA MAY rely on the RA to perform the Final Cross-Correlation and Due Diligence, provided that the RA complies with this section and is subjected to the Audit Requirements of Section 8.1.1 and Section 8.2.

In case of EV Certificates to be issued in compliance with the requirements of Section 1.3.2, the Enterprise RA MAY perform the requirements of this Final Cross-Correlation and Due Diligence section.

3.2.2.14 Requirements for Re-use of Existing Documentation

For each EV Certificate Request, including requests to renew existing EV Certificates, SHECA MUST perform all authentication and verification tasks required by these Guidelines to ensure that the request is properly authorized by the Applicant and that the information in the EV Certificate is still accurate and valid. This section sets forth the age limitations on for the use of documentation collected by SHECA.

Validation For Existing Subscribers

If an Applicant has a currently valid EV Certificate issued by SHECA, a CA MAY rely on its prior authentication and verification of:

1. The Principal Individual verified under Section 3.2.2.2.2 (4) if the individual is the same person as verified by SHECA in connection with the Applicant's previously issued and currently valid EV Certificate;

2. The Applicant's Place of Business under Section 3.2.2.4.1;

3. The Applicant's Verified Method of Communication required by Section 3.2.2.5 but still MUST perform the verification required by Section 3.2.2.5.2 (B);

4. The Applicant's Operational Existence under Section 3.2.2.6;

5. The Name, Title, Agency and Authority of the Contract Signer, and Certificate Approver, under Section 3.2.2.8; and

6. The Applicant's right to use the specified Domain Name under Section 3.2.2.7, provided that SHECA verifies that the WHOIS record still shows the same registrant as when SHECA verified the specified Domain Name for the initial EV Certificate.

Re-issuance Requests

A CA may rely on a previously verified certificate request to issue a replacement certificate, so long as the certificate being referenced was not revoked due to fraud or other illegal conduct, if:

1. The expiration date of the replacement certificate is the same as the expiration date of the EV Certificate that is being replaced, and

2. The Subject Information of the Certificate is the same as the Subject in the EV Certificate that is being replaced.

Age of Validated Data

1. Except for reissuance of an EV Certificate under Section 3.2.2.14.2 and except when permitted otherwise in Section 3.2.2.14.1, the age of all data used to support issuance of an EV Certificate (before revalidation is required) SHALL NOT exceed the following limits:

A. Legal existence and identity – 398 days;

B. Assumed name – 398 days;

C. Address of Place of Business – 398 days;

D. Verified Method of Communication – 398 days;

E. Operational existence – 398 days;

F. Domain Name – 398 days;

G. Name, Title, Agency, and Authority – 398 days, unless a contract between SHECA and the Applicant specifies a different term, in which case, the term specified in such contract controls. For example, the contract MAY include the perpetual assignment of EV roles until revoked by the Applicant or CA, or until the contract expires or is terminated.

2. The 398-day period set forth above SHALL begin to run on the date the information was collected by SHECA.

3. SHECA MAY reuse a previously submitted EV Certificate Request, Subscriber Agreement, or Terms of Use, including use of a single EV Certificate Request in support of multiple EV Certificates containing the same Subject to the extent permitted under Section 3.2.2.9 and Section 3.2.2.10.

4. SHECA MUST repeat the verification process required in these Guidelines for any information obtained outside the time limits specified above except when permitted otherwise under Section 3.2.2.14.1.

3.2.3 Authentication of Individual Identity

SHECA does not accept any individual EV Certificates application.

3.2.4 Non-Verified Subscriber information

Subscriber information that has not been verified in accordance with Baseline Requirements is not included in certificates.

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.

3.2.5 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.

3.2.6 Criteria for Inter-operation

SHECA SHALL disclose all Cross-Certified Subordinate CA Certificates that identify SHECA as the Subject, provided that SHECA arranged for or accepted the establishment of the trust relationship.

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 described 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 described 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 is: sheca.com

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 SHECA 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 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:

- Subscriber (or authorized proxy) request to revoke certificate, and CA make sure the request is from the subscriber;
- Because the certificate is improper used in violation of the main and important obligations of national laws and regulations;
- SHECA is made aware that the original certificate request was not authorized and does not retroactively grant authorization;
- Certificate's private key is lost, stolen, tampered, unauthorized disclosure or damaged, or no longer comply with the requirements of key size and key parameters setting and quality check in section 6.1.5 and section 6.1.6;
- SHECA is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate;
- SHECA obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address in the Certificate should not be relied upon.
- 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 SHECA's Certificate Policy or Certification Practice Statement;
- 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;
- Revocation is required by SHECA'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 certificate is substantially changed
- After certificate insurance, fake information is found by SHECA in the application materials provided by EV certificate subscriber
- The application of certificate is not authorized or can't be traced to the authorization
- Subscriber doesn't use EV certificate according to CP/CPS or the agreement, or changes the usage of EV 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 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. The Subordinate CA requests revocation in writing;

2. The Subordinate CA notifies the SHECA that the original certificate request was not authorized and does not retroactively grant authorization;

3. 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 Sections 6.1.5 and 6.1.6 of Baseline Requirements (including S/MIME BR and Code Signing BR);

4. SHECA obtains evidence that the Certificate was misused;

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

6. SHECA determines that any of the information appearing in the Certificate is inaccurate or

misleading;

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

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

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

10. 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 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 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 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 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.

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 subscriber certificates under UNTSH EV Certificate hierarchical structure (refer to section 1.1.2), 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 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-Certified Subordinate CA Certificates;

3.Certificates for infrastructure purposes (administrative role certificates, internal CA operational device certificates); and

4.Certificates for OCSP Response verification.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 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	398 days
EV CodeSigning certificate	No stipulation	39 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 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 CA / Browser Forum 'Guidelines for the Issuance and Management of Extended Validation Certificates'.

7.1.3 Algorithm Object Identifiers

Keys and hash algorithms for SHECA's EV certificates meet the requirement specified in the CA/B Forum Baseline Requirements and the Applicable EV Guidelines.

7.1.3.1 SubjectPublicKeyInfo

The following requirements apply to the subjectPublicKeyInfo field within a Certificate or Precertificate. No other encodings are permitted.

7.1.3.1.1 RSA

SHECA indicates an RSA key using the rsaEncryption (OID: 1.2.840.113549.1.1.1) algorithm identifier, and it is an explicit NULL. SHECA shall not use a different algorithm to indicate an RSA key.

SHECA shall not use sha1RSA algorithm for the publicly trusted certificates.

7.1.3.1.2 ECDSA

SHECA indicates an ECDSA key using the id-ecPublicKey (OID: 1.2.840.10045.2.1) algorithm identifier. The parameters must use the namedCurve encoding.

For P-384 keys, the namedCurve is secp384r1 (OID: 1.3.132.0.34).

7.1.3.2 Signature Algorithm Identifier

All objects signed by SHECA Private Key conform to these requirements on the use of the AlgorithmIdentifier or AlgorithmIdentifier-derived type in the context of signatures.

In particular, it applies to all of the following objects and fields:

The signatureAlgorithm field of a Certificate or Precertificate.

The signature field of a TBSCertificate (for example, as used by either a Certificate or Precertificate).

The signature Algorithm field of a CertificateList

The signature field of a TBSCertList

The signature Algorithm field of a BasicOCSPResponse.

No other encodings are permitted for these fields.

7.1.3.2.1 RSA

SHECA uses the following RSA signature algorithms and encodings:

SHA-256 with RSA, (OID) 1.2.840.113549.1.1.11

SHA-384 with RSA, (OID) 1.2.840.113549.1.1.12

SHA-512 with RSA, (OID) 1.2.840.113549.1.1.13

7.1.3.2.2 ECDSA

SHECA uses the following ECDSA signature algorithms and encodings:

SHA-256 with ECDSA, (OID) 1.2.840.10045.4.3.2

SHA-384 with ECDSA, (OID) 1.2.840.10045.4.3.3

SHA-512 with ECDSA, (OID) 1.2.840.10045.4.3.4

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 CA / Browser Forum EV 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

SHECA CRL profile conforms to RFC 5280. CRLs containing revocation information about EV TLS and EV Code Signing Certificates conform to the CA/B Forum Baseline Requirements.

SHECA issues regularly CRL for the user to query.

7.2.1 Version Number(s)

SHECA issues X 509 V2 version of CRLs.

7.2.2 CRL and CRL Entry Extensions

If a CRL entry reasonCode extension is present, the reason must indicate the most appropriate reason for revocation of the certificate. Refer to the UniTrust CPS Section 7.2.2 for the usage of CRL entry extensions.

Users can download the CRL through the URL indicated in CRL extensions issued by SHECA.

7.3 OCSP Profile

SHECA provides users OCSP (Online Certificate Status Inquiry Service), and the OCSP response issued complies with the RFC6960 standard.OCSP, as an effective supplement to CRL, facilitates certificate users to query certificate status information in time.

7.3.1 Version Number(s)

RFC6960 defines the OCSP V1.

7.3.2 OCSP Extensions

SHECA's OCSP Extensions are consistent with RFC6960.

The singleExtensions of an OCSP response shall not contain the reasonCode (OID 2.5.29.21) CRL entry extension.

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 has a currently valid WebTrust Seal of Assurance for CAs. Before issuing EV Certificates, SHECA and its Root CA MUST successfully complete a point-in-time readiness assessment audit against the WebTrust EV Program.

SHECA MUST complete any required point-in-time readiness assessment no earlier than twelve (12) months prior to issuing an EV Certificate.

SHECA MUST undergo a complete audit under such scheme within ninety (90) days of issuing the first EV Certificate.

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

During the period in which SHECA issues EV Certificates, SHECA MUST strictly control its service quality by performing ongoing self audits against a randomly selected sample of at least three percent of the EV Certificates it has issued in the period beginning immediately after the last sample was taken.

Audit operations should be clearly documented in CPS, and the requirements should be compliant with requirements of guidance 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.

SHECA SHOULD make its audit report publicly available no later than three months after the end of the audit period. If there is a delay greater than three months and if so requested by an Application Software Supplier, SHECA MUST provide an explanatory letter signed by its auditor.

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 Insurance coverage

SHECA shall determine the insurance policy according to business development.

Currently, SHECA self-insures for liabilities arising from its performance and obligations under this CPS.

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.

9.2.2 Other Assets

SHECA ensures it has sufficient financial strength to maintain normal operations, fulfill corresponding obligations, and reasonably assume responsibilities to subscribers and relying parties.

9.2.3 Insurance or Warranty Coverage for End-Entities

If SHECA is judicially determined to bear compensation and/or indemnification liabilities, it will assume the corresponding compensation liabilities in accordance with the ruling of the relevant arbitration institution or the judgment of the court.

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

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.

9.6.1 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 SHECA's Certification Practice Statement (CPS) as required by CA/Browser Forum on www.cabforum.org.

9.6.2 RA Representations and Warranties

See section 9.6.1 requirements.

9.6.3 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.

9.6.4 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.

9.6.5 Representations and Warranties of Other Participants

Advance vendor warrants:

Advance vendor is required to bear all the cost of the certificate and pays all according to the provisions provided by SHECA.

Advance business's behavior of advance vendor means advance vendor is willing and able to assume responsibility of guaranteeing applicant authenticity based on this CPS.

Advance vendor shall not reject any statement, change, update, upgrade from SHECA, including but not limited to modification of strategy, standards and additions and deletions of certification services .

9.7 Disclaimers of Warranties

SHECA can't bear liability in the following circumstances:

1. Don't assume any liability of an objective accidents or other force majeure event caused by failure or delay .These events include, but are not limited to, labor disputes, a party of transaction behavior intended or not, strikes, riots, disturbances, war, fire, explosion, earthquake, flood or other catastrophe.

2. Due to equipment failures, line break caused by reason out of SHECA, leading to error, delay, interruption or failure of the issuance of digital certificates, SHECA doesn't assume any liabilities.

3. No information in the CPS can be implied or construed, and SHECA must assume other obligations or other acts promised by SHECA , including but not assume any guarantees and obligations of any other form, and no guarantee for a particular purpose.

4. If the applicant provide intentionally or unintentionally incomplete, unreliable or outdated, including but not limited to forgery, tampering, false information, but applicant also provides the necessary review documents based on the normal process and gets digital certificates issued by SHECA. The legal problems, the applicant result from above should be assumed full responsibility for the economic disputes, and SHECA doesn't assume the legal and economic responsibility associated with the content of the certificate, but can provide investigation and evidence based on victim's Investigation and proof help.

5. SHECA does not assume legal liability for any other unauthorized person or organization on behalf of the SHECA compiling, publishing or distributing unreliable information.

6. For certificates, signatures or any other transaction or design services to use, issuance, authorization, execution, or refuse provided under this CPS, resulting in or relating to any indirect, special nature, with nature, or consequential damages, or any loss of profits, loss of data or other indirect, consequential or punitive damages, whether reasonably foreseeable, SHECA will not assume responsibility, even if SHECA had been warned of the possibility of such damage.

7. SHECA has clearly defined the scope of various types of certificates , if the certificates subscriber uses certificates for other purposes which is not allowed, and SHECA does not assume any responsibility, regardless of whether the usage causing any losses.

8. In the extent permitted by law, according to the law, policy, and the victim's request, SHECA provides truthfully e-government, e-commerce or other network operations based on non-repudiation electronic signatures, but SHECA is not required to bear the responsibilities outside legal or policy.

9.8 Limitations of Liability

Under the "Corporate Law of the PRC ""Electronic Signature Law of the PRC" and other laws and regulations, as a limited liability company established by law , SHECA assumes any responsibility and obligation limited liability within the law .

SHECA doesn't assure and perform any further obligations, in any party agreement between CPS and SHECA.

SHECA MUST NOT limit its liability to Subscribers or Relying Parties for legally recognized and provable claims to a monetary amount less than two thousand US dollars per Subscriber or Relying Party per EV server Certificate.

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 is effective since it is published, version number and release date shall be specified by the document, as new version is published, and takes effect, the original version shall lose effectiveness automatically.

9.10.2 Termination

This CPS as amended from time to time shall remain in force until it is replaced by a new version.

If the subscribers end the usage of their certificates, or a relying party end the trust of certificates, the subscriber certificate has been revoked and not re-apply for a certificate, then in addition to CPS provisions of the audit, archiving, confidential information, privacy, intellectual property, compensation and limited liability, for the subscriber or relying party, the CPS will no longer binding to them. If SHECA has other agreement, then operates in accordance with the provisions of the agreement.

9.10.3 Effect of Termination and Survival

After this CPS terminates, the audit, confidential information, privacy protection, archiving, intellectual property involved in this CPS, and indemnification and limited responsibility involved in terms shall exist effectively.

9.11 Individual Notices and Communications with Participants

Unless there are special provisions in laws and regulations or agreement, SHECA shall communicate with each other with the reasonable way, and shall not take individual way.

Whenever any person intends or requires to publish any services, specifications, operation of the notice, demand or request mentioned in this CPS, this information will be communicated in documents.

Written communications must be delivered with written documentation by the courier service, or by registered mail confirmation, accompanied by return mail and write back. Mailing address is as following:

18F, NO.1717， Sichuan North Road ,Shanghai, People's Republic of China (200080) Shanghai Electronic Certification Authority Co., Ltd.

If participants send notification to SHECA by e-mail, then it will be valid only when SHECA receives written confirmation materials within 24 hours after SHECA received e-mail notification.

Sent to others from SHECA via the following address:

The latest address in SHECA's postal record

9.12 Amendments

9.12.1 Procedure for Amendment

Through the authorization of SHECA Security Certification Committee, SHECA Strategy Development Department shall review this CPS once a year at least, to ensure that CPS meets the requirements of national laws and regulations, and satisfy the actual requirements of certification business operation.

This CPS must be revised through the approval and verification of SHECA Security Certification Committee ——the highest policy management agency of SHECA after Strategy Development Department puts forward the revision report.

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 OID Must be changed

No stipulation.

9.13 Dispute Resolution Provisions

As an expert agency of certificate dispute resolution, SHECA Security Certification Commission expert group collect relevant evidence to promote dispute resolution, coordination the relationship between SHECA and the parties, and as a final writer of controversial recommendation report.

Whether the expert group complete the proposed report and convey recommendations, and how ruling decisions to form and does not prevent SHECA, parties and other stakeholders to take consistent way related to the CPS and the law ,and find other solutions.

9.14 Governing Law

This CPS accepts “Electronic Signatures Laws of People's Republic of China”, “Electronic Certificate Service Management Measures” and other laws and regulations of jurisdiction and explanation of People's Republic of China.

No matter choose of contracts or other clauses or whether commercial relationship is established in People's Republic of China, the implementation, explanation, interpretation, effectiveness of this CPS shall apply to the laws of People's Republic of China. Choice of law is to ensure that all subscribers have uniform procedures and interpretation, regardless of where they live and where to use the certificate.

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

The CPS impacts directly on SHECA terms and provisions of rights and obligations, unless issued by the affected parties through the information or documents identified, or other provided, otherwise can not be verbal amended, given up, supplied, modified or ended.

When the CPS and other rules, norms or agreements conflicts, all parties involved in certification activities will be bound by the provisions of this CPS, but except the following:

- Signing before the effective date of the CPS.
- The contract shows expressly the relevant parties to replace the CPS matters, or the provisions of this CPS are prohibited to performed by law.

9.16.2 Assignment

The responsibility and obligation between CA, subscriber and relying party could not be assigned to other parties.

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

In the extent permitted by applicable law, subscriber agreement and CPS formulated in accordance with the CP shall include force majeure clause to protect each party. SHECA isn't responsible for the following force majeure events, the violation, delay or inability to perform that CPS regulated beyond its ability to control.

Force majeure including war, terrorist attacks, strikes, epidemics, natural disasters, fires, earthquakes, supplier or vendor failures, paralysis of the Internet or other infrastructure and other natural disasters.

9.17 Other Provisions

No stipulation.

Appendix A Acronyms and Definition

SHECA

Abbreviation for Shanghai Electronic Certification Authority 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.`