UniTrust Network Trust Service Hierarchy Certificate Policy/Certificate Practice Statement for Event Certificate

Version 1.1

January 17, 2020

18/F, JiaJie International Plaza,
No.1717,North Sichuan Road,
Shanghai, China
Tel: 86-21-36393100
Fax: 86-21-36393200
https://www.sheca.com

UniTrust Network Trust Service Hierarchy Certificate Policy/Certificate Practice Statement for Event Certificate

Location: Shanghai, North Sichuan Road 1717, JiaJie International Plaza F18
Postal Code: 200080
Tel: 86-21-36393197
E-mail: policy@sheca.com

Revision Control

Version	Effective Date	Author	Issuer	Notice
V1.0	December 13, 2019	Toria Chen	SHECA Security Certification Commission	Historical Version
V1.1	January 17, 2020	Toria Chen	SHECA Security Certification Commission	Current Version

Changes Description

Version	Description
V1.0	--
V1.1	Add Circumstances for Revoking a Subordinate CA Certificate

Notices

This document conforms to all or parts of the following standards:

- RFC3647: Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practice Statement Framework.
- RFC2459: Internet X.509 Public Key Infrastructure - Certificate and CRL Attribute
- RFC2560: Internet X.509 Public Key Infrastructure - Online Certificate Status Protocol-OCSP
- ITU-T X.509 V3（1997）: Information Technology - Open Systems Interconnection – Directory: Authentication Framework.
- RFC 5280: Internet X.509 Public Key Infrastructure - Certificate and CRL Structure
- GB/T 20518-2006: Information Security Technology - Public Key Infrastructure –Digital Certificate Format

This document has been submitted to the independent audit institution to perform assessment in accordance with AICPA / CICA WebTrust for Certification Authority. If this document complies with the above auditing standards，the result will be published at www.sheca.com.

Copyright Notices

For any request the copy of this document, please contact with Shanghai Electronic Certification Authority Center Co., Ltd.

Address: 18F, No.1717 North Sichuan Road, Shanghai, PRC(200080)
Tel :(021)36393100,
Fax :(021)36393200.
E-mail: cps@sheca.com.

For the latest version of this document, please visit our website http://www.sheca.com/repository, without further notice to specific individuals, businesses, governments and other social organizations.

SHECA Security Certification Committee is responsible for the interpretation of this document.

Note:
SHECA electronic certification service is to comply with the laws of the PRC. Any individual, institution or other organizations who violated the laws and influenced the SHECA electronic certification service, SHECA will retain all legal rights in order to maintain its interests.

The summary of main rights and obligations about SHECA CP/CPS

This summary is only a brief description of an important part of this document, for a complete discussion of the relevant provisions and other important terms and details please see the full text of the document.

1. The CPS file provides implementation and usage of SHECA electronic certification service. Electronic certification services include SHECA digital certificate issuance, management and authentication that cover the operational processes, operational management, operating environment, management policies, etc. within the entire life cycle of a digital certificate.

2. Notes to the certificate applicants:
(1) The applicant before applying for a certificate has been recommended to receive appropriate training in relevant aspects of digital certificates.
(2) From SHECA website and other channels you can get files about digital signatures, certificates and the CPS, certificate applicants can also take relevant training and learning.

3. SHECA provides different types of certificate, applicants should consult by themselves SHECA in order to determine which certificate is suitable for their needs.

4. Applicants must accept the certificate before using the certificate to establish communication with other people or guiding others to use the certificate. That an applicant received a certificate means that he/she had accepted the rights and obligations under this document, and had assumed corresponding responsibilities.

5. If you are a recipient or relying party of the digital signature or digital certificate, you must decide whether to trust it. Prior to this, SHECA suggests that you should check SHECA certificate directory services to ensure that the certificate is correct and valid, and verify that digital signature is generated by the certificate holder within the valid period of certificate, moreover the relevant information has not been changed.

6. The certificate holder agrees that, if it happens to compromise security of the private key, he/she should promptly notify the SHECA and its authorized certificate service agencies.

7. If the user has any comments and suggestions on editing later CPS version, please Email to:cps@sheca.com; or please mail to: 18F, 1717 North Sichuan Road, Shanghai, PRC (200080).

8. For more information please visit SHECA website (http://www.sheca.com).

Contents

1. Introduction

1.1 General Description

Shanghai Electronic Certification Authority Center Co., Ltd. (abbreviated as SHECA) is a third-party electronic certification service agency taking leading role in China, and who is the first to obtain licenses, with professional management, operation and technical supporting capabilities providing users with various types of digital certificate services and takes efforts to construct a harmonious, trusted network environment. Event certificate in this document is a special type of digital certificate that uses a one-time private key for an event. Event certificates are generally used for one-time event digital signatures, and the private key is destroyed after the signature, ensuring the authenticity of the identity of each signature participant, the integrity of information and the non-repudiation of the signature.

Certification Policy/ Certificate Practice Statement (referred to as this document in the following) is a set of naming rules that indicate the applicability of a certificate to a particular group and/or an application type with the same security requirements. "UniTrust Network Trust Service Hierarchy Certificate Policy/Certificate Practice Statement for Event Certificate", referred to as this document is an event certificate applied under UNTSH framework, for the use of UNTSH event certificate application, issuance, regulation, application, revocation, renewal and to provide related trust services including legal, technical requirements and norms for all participants. These specifications ensure the security and integrity of UNTSH certificates, and the single set of rules that apply consistently across UNTSH, provides the same trust guarantee under the UNTSH framework. This document is not a legal agreement between the parties, SHECA and UNTSH. Rights and obligations of the parties, SHECA and UNTSH depend on signed agreements.

This document conforms RFC3647, "Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practice Statement Framework", and GB/T 20518-2006, "Information Security Technology – Public Key Infrastructure – Digital Certificate Format".

1.1.1 Shanghai Electronic Certification Authority Center Co., Ltd. (SHECA)

Shanghai Electronic Certification Authority Center Co., Ltd. (abbreviated as SHECA, referred to as Shanghai CA) was founded in 1998. SHECA is the first professional third-party electronic certification authority of China and is also one of certification authorities with the most experience in operating nationwide, the most wide-ranging application and the largest user groups.

In April 2005, SHECA obtained the "Electronic Authentication Service Password Usage License" from the State Cryptography Administration; In September 2005, SHECA obtained the "Electronic Authentication Services License" from Ministry of Industry and Information Technology and became the first national qualification for operating the electronic certification service after the "Electronic Signature Law of the People's Republic of China" put into effect; In June 2008, SHECA obtained the international WebTrust Certification; In December 2008, SHECA was listed in the built-in root certificate of the Microsoft operating system, and is the first authority to achieve global electronic authentication services in China.

SHECA has a professional and strong Research and Development team, which is focusing on researching and developing required technologies, products and services to build the network trust system, and has a number of self-research, and proprietary core technologies, products and solutions.

SHECA established by law as a third-party electronic certification service agency, has constructed and operated the UniTrust NTSH. UniTrust NTSH is China's most influential agencies responsible for issuing and managing digital certificate and issued and managed digital certificates have been widely used.

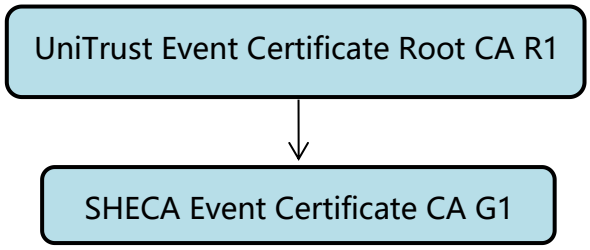
1.1.2 UniTrust Network Trust Service Hierarchy

UniTrust Network Trust Service Hierarchy (abbreviated as UNTSH) proposed the concept of digital certificate services "a card in hand, travel the world" , and UNTSH has issued digital certificates to participants involved in e-government, e-commerce, social services and other online business ,and can achieve cross-industrial, cross-regional electronic certification services.

Unitrust NTSH has a clear, complete PKI hierarchical architecture in order to achieve different needs for different applications of certification services. Unitrust NTSH includes root CA, sub-CA, the relevant Registration Authority (RA Centre), Registration Authority Terminal (RAT) and other authorized entities related with service, and those are service subjects at different levels within the Unitrust NTSH. All related certificate services and management within the Unitrust NTSH, completely, correctly and comprehensively perform and implement the document and the corresponding Certificate Policies.

The system of Certification Policy for Event Certificate:

UniTrust Event Certificate Root CA R1



UniTrust Event Certificate Root CA R1 Root key is 4096-bit, under which is SHECA Event Certificate CA G1 acting as the only sub-CAs under UCA Root-G2, responsible for issuing subscriber certificate of 2048-bit with RSA algorithm or 256 bits with the SM2 algorithm.

UniTrust Event Certificate Root CA R1 will expire on November 10, 2044 and will no longer issue any subordinate certificates since November 1, 2039.

1.2 Document Name and Identification

This document is “UniTrust Network Trust Service Hierarchy Certificate Policy/Certificate Practice Statement for Event Certificate”, abbreviated as “Certificate Policy/Certificate Practice Statement for Event Certificate”, this document defines the OID as: 1.2.156.112570.1.0.5.

All self-defined Object Identifier (OID) of SHECA is listed as below:

OID	Object
1.2.156.112570	UniTrust
1.2.156.112570.1	SHECA

1.2.156.112570.1.0	Policies
1.2.156.112570.1.0.5	UniTrust Network Trust Service Hierarchy Event Certificate Practice Statement (UNTSH Rapid CP)
1.2.156.112570.1.0.6	UniTrust Network Trust Service Hierarchy Timestamp Certificate Practice Statement (UNTSH Rapid CPS)
1.2.156.112570.1.2.4	Adobe Signing Policy
1.2.156.112570.1.2.5	Document Signing
1.2.156.112570.1.3	Client Certificates Policy
1.2.156.112570.1.4	TimeStamping Policy
1.2.156.112570.1.4.1	TimeStamping AATL Policy
1.2.156.112570.1.5	OCSP Policy

1.3 PKI Participants

1.3.1 Electronic Certification Service Authority (CA)

Electronic certification authority is the entity that issues certificates.

SHECA is electronic certificate authority established by law in charge of constructing and operating UNTSH. The structure of UNTSH is a multi-class model, and UNTSH has multiple entities that could issue certificates, including various root CA and subordinate CA. These CA could issue certificates. Generally, root CA only issues certificates to subordinate CA, and subordinate CA could issue certificates to end-user subscribers or other CA. The UNTSH CA issue certificates to all parties (hereafter called subjects or entities, including organizations, individuals and other subjects or entities that their identities are marked clearly could act as subjects or entities as claimed in this document) who participate in electronic government, electronic commerce and other affairs to ensure that the public key correspond with subject' s identity uniquely.

As the main operator, SHECA is responsible for editing and publishing UNTSH CP, publishing Certificate Revocation List and Certificate Trust Chain, and managing Certificate Life-Cycle, including Certificate Issuance, Revocation, Renewal, status check and verification, directory services etc. Also, SHECA manages all subordinate RAs and all certification service authority (Sub-CA).

1.3.2 Registration Authority (RA)

A Registration Authority is an entity that performs identification and authentication of certificate applicants for end-user certificates, initiates or passes along revocation requests for certificates for end-user certificates, and approves applications for renewal or re-keying certificates on behalf of a UNTSH CA. UNTSH RA could be either a subordinate part of CA, designated by SHECA, or independent of the CA, authorized and delegated by related agreements between SHECA and relevant organizations.

RA must perform certificate services under the approval and authorization of SHECA in accordance with the procedures and requirements of this document and corresponding CPS. SHECA must assess RA appropriately to confirm that the duty could be performed properly.

1.3.3 Subscribers

Subscribers, the entities that receive certificates from CA, include individuals, organizations or equipment accepting certificates from UNTSH. A subscribers represents the only entity in the certificate that is bound to the public key and has ultimate control over the corresponding private key that is unique to the public key in the certificate. Subscribers who use certificates within the scope of this document are willing and able to assume the obligations agreed upon by this document.
The subscriber is the electronic signer in an electronic signature application.

1.3.4 Relying Parties

Relying Party, under the SHECA certification service system, is an individual or entity that acts in reliance of any certificate holders who use certificates for online business and any entities that have reasonable confidence in the authenticity of certificate according to the SHECA CPS. A Relying party may, or may not also be a Subscriber. In this practice, a relying party is the entity who trusts the Certificate according to the mechanism of Certificate Policy for Event Certificate issued by SHECA.
To trust or verify a certificate, a relying party must verify information of certificate revocation, and review the certificate reasonably.

1.3.5 Other participants

Other participants refers to other entities who provide related service to CA certificate services system.
In the provision of certificate services, organizations that offer query and verification of organization or individual information and/or other extra information could be the cooperator assisting in verifying the information of certificate applications.
Some RAs are not approved by SHECA, but the organizations apply for certificates, verify certificate information and pay for certificate cost for a specific group, known as Certificate Advance Vendor. SHECA could provide certificate services required for specific users by entering into the agreement with Advance Vendor. The Advance Vendor and its specific certificate subscribers shall comply with the provisions of this document.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Usage

The event certificate issued by SHECA is widely used in the fields of enterprise information, e-government and e-commerce, and is used to prove the identity of the electronic signature, the integrity of the signed document data and to ensure whether the electronic signature has been modified.

1.4.2 Prohibited Certificate Usage

Event certificate can only be used to for electronic signature and authentication of certificate subscribers, and any non-compliant applications are not protected by this document.
The certificate issued by SHECA 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.

1.5 Policy Management

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 Information Industry, SHECA develops this document 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

Specialized agencies designated by the SHECA and staff take the responsibility for controlling the version of CPS strictly. If you have any problems, suggestions, questions, etc., about CPS, you could contact with the contact person.

Contact Person: Shanghai Electronic Certification Authority Center Co., Ltd. SHECA Strategy Development Center.

Tel: 86-21-36393197

Fax: 86-21-36393200

Address: 18F, 1717 North Sichuan Road, Shanghai, the People's Republic of China

Postal Code: 200080

E-mail: policy@sheca.com

1.5.3 CPS Decision in Line With Strategy Agency

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

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

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

1.5.4 CP/CPS Approval Procedure

This "Certificate Strategy for Event Certificate" is approved by the SHECA Security Certification Committee and published on the SHECA website.

SHECA will inform Ministry of Information Industry within 30 days after publishing this "Certificate Strategy for Event Certificate" which must be approved by the SHECA Security Certification Committee.

1.6 Definitions and Abbreviations

1.6.1 SHECA

Abbreviation for Shanghai Electronic Certification Authority Center Co., Ltd

1.6.2 UNTSH

An open key infrastructure constructed and operated by the Shanghai Electronic Certification Authority Center Co., Ltd. (abbreviated as SHECA) is referred to as UniTrust, and provides electronic certification services based on digital certificate. SHECA is established as third-party certification authority in accordance with the "Electronic Signature Law of the People's Republic of China" and is dedicated to create a harmonious environment for the network to provide Internet users with secure, reliable, trusted digital certificate services.

1.6.3 SHECA Security Certification Committee

It is the agency for managing highest policies and is decision-making agency pursuant to CPS within the SHECA certification services system.

1.6.4 The Electronic Certification Service Agency

SHECA and authorized subordinate CA are called not only electronic certification service agency but also the certificate authority, which means they are the entities that issue the certificate.

1.6.5 Registration Authority

Registration Authority（RA）is responsible for processing service requests from certificate applicants and certificate subscribers, and submitting them to the certification authority for the end-use certificate applicant to establish registration process. RA is also responsible for identifying and verifying certificate applicants, initiating or transferring certificate revocation request, and approving certificate renewal or re-key request on behalf of the electronic certification service agency.

1.6.6 Registration Authority Terminal

As service subject facing directly with users within the architecture of SHECA certification service, RAT is the terminal organization offering the certificate services and through the CA or RA, is authorized to be engaged in various services.

1.6.7 System Administrator

System Administrator is responsible for not only installing, configuring and maintaining CA hardware and software system but also starting and stopping the CA server and managing the CA operator.

1.6.8 Entry Clerk

Entry clerk is responsible for the input of the information submitted by the applicant and help the user handle digital certificates application, revocation renewal and other procedures.

1.6.9 Reviewer

The reviewer is responsible for checking the information of certificate application and help the user handle digital certificates application, revocation， renewal and other procedures.

1.6.10 Certificate Producer

Certificate producer is responsible for downloading and producing the certificate for certificate applicant and submit it to the user.

1.6.11 Certificate

Certificate refers to an electronic signature certificate, the electronic documents issued by the electronic certification authority to prove the electronic signature, identity, qualification and other relevant information of the certificate holder.

1.6.12 Digital Certificate

Digital certificate is used for identifying the signatory as a digital signature that indicates the signer has the recognized signature data. The certificate involved in this document is the digital certificate, including signing certificate and encryption certificate.

1.6.13 Event Digital Certificate

Event digital certificate is a special type of digital certificate, designed by SHECA with patented technology for demand service or specific business scenarios. In the business process, the relevant information in the business scene (electronic documents, characteristics information of signature, handwriting, or other proof of information regarding signature behavior, etc.) is automatically associated with the extended domain of the digital certificate, and an event digital certificate is issued to ensure reliability of electronic signatures in the business process. The private key corresponding to the event digital certificate is generally used for only once, and is destroyed immediately after being used.

The digital certificate described in this document, without a special definition, refers to event digital certificate.

1.6.14 Reliable digital certificate

Personal identification that comply with the provisions of "Electronic Signature Signed Act" and related regulations.

1.6.15 Electronic Signature

Electronic signature, referred to as the signature, has the technical means of identifying signatory and showing the recognized signature data.

1.6.16 Digital Signature

The asymmetric encryption system is used for encrypting , decrypting , electronic data, to achieve an electronic signature. The Signature mentioned in the document is digital signature.

1.6.17 Electronic Signer

Electronic signatory is a person who holds electronic signature data created by electronic signature and implement electronic signatures in his own identity or on behalf of the person he represents.

1.6.18 The Relying Party on Electronic Signature

The relying party on electronic signature is the person who engages in the relevant activities.

1.6.19 Private Key (creation data of electronic signature)

In the course of the use of electronic signatures, private key is the data such as character, encoding associating reliably electronic signatures with electronic signatory.

1.6.20 Public Key (validation data of electronic signature)

Public key refers to the subscriber's validation data of electronic signature.

1.6.21 Subscribers

Certificate subject is issued a certificate.

1.6.22 Relying Parties

The receiver of the certificate, who relying this certificate and/or digital signature verified by this certificate. In this standard, "certificate users" and "relying parties" can be used interchangeably.

1.6.23 Certificate Advance Vendor

Certificate Advance Vendor is the group or organization who is able to bear all the certificate service fees for subsidiary and served subscribers or potential subscribers. It is also a special service point.

2. Publication and Repository Management

2.1 Publication of Certificate Information

SHECA will publish related information on http://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.

2.1.1 SHECA Repository

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: http://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.

2.1.2 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 http://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.

2.2 The Time and Frequency of Releasing

2.2.1 The Time and Frequency of the Certificate Practice Statement Releasing

SHECA will release the latest version of CP/CPS in time. Once amendments are approved, SHECA will post them on http://www.sheca.com and publish the latest CP/CPS on SHECA repository, and list together with the original CP/CPS in order to retrieve. This document should be updated at least for one-year period.
SHECA may change the CP/CPS, with the technological advancements, business development, application promotion and the objective requirements of laws and regulations. The releasing time and frequency of the CP/CPS will be independently decided by the SHECA. This publication should be immediate, efficient, and be consistent with the national laws and regulations.
The current CP/CPS is effective and is in the implementation of the state, before the SHECA releasing a new CP/CPS or any form of announcements, notices to modify, supply, adjust or update for CP/CPS. Only the SHECA has the right to change any form of the state.

2.2.2 The 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.

When certificates are published by the directory server, SHECA will issue a certificate successfully and release simultaneous. Users can also check and obtain a certificate by visiting http://www.sheca.com.

2.2.3 Time and Frequency of the CRL Publishing

Subscriber' s certificate of event certificate is immediately destroyed after a signature, therefore, the certificate revocation is actually not performed.

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 within 24 hours, and release Certificate Revocation List of a sub-CA certificate (ARL) at least once every three months. If the root certificate is revoked, revocation information is published on the website in time.

SHECA does not provide subscriber certificate CRL service for event certificate. SHECA ensures that revocation lists (CRL) of Sub-CA Certificate will be issued at least once every 3 months for intermediate root, unless it is specified. In case of emergency, SHECA can choose time and frequency of the certificate revocation list to publish.

2.2.4 The 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 http://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.

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

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

2.3 Repository Access Control

2.3.1 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).

2.3.2 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. Authentication and Identification

3.1 Naming

3.1.1 Type of Names

In order to distinguish from other applicants, Certification authority issues certificate in accordance with specific procedures to save the particular record of the certificate registration process, identify specific object identification. This name appeared with naming process, including the distinguished name and the unique identifiers included in certificate extension item, is able to identify a group of real-world entity.

The Subject Name of certificate generated and identified by SHECA uses the way of X.501 Distinguished Name (DN).

Each certificate subscriber has a distinguished name correspondingly, consists of the screening name and user uniquely identify items, following the regulation of X.509. Screening name is included in the subject of each certificate, and the user uniquely identify items is included in the certificate extension item, which uniquely identifies the certificate subscriber's identity.

As a third party certification authority trusted who is responsible for identifying the link between the public key and the named entities. This relationship will be confirmed unequivocally through a certificate. Naming could be solved by negotiating between SHECA and the applicant, which can also be completed by the applicant independently.

3.1.2 Need for Names to be Meaningful

User identification information used for identifying name must be clear, traceable and certainly representative significance, that does not allow to appear anonymous or pseudo-names etc.

3.1.3 Anonymity or Pseudonymity of Subscribers

SHECA does not accept or allow any anonymity or pseudonymity only to accept a clear sense of the name as a unique identifier.

3.1.4 Rules for Interpreting Various Name Forms

The certificates issued by SHECA certification service system, whose contents format of distinguished name DN is comply with naming regulation of the X.500. The following is a general identified naming regulation:

Distinguished Name（DN）	Contents	Content(demonstration)
1、Country（C）	The company's country name	C=CN
2、Organization（O）	Company Name	O=SHECA
3、Organization Unit（OU）	Unit or Department name	OU=Techonical Support Center
4、Common Name（CN）	Certificate holder’ s general common name	CN=Zhang Shan

The naming regulation of identifier is defined by the SHECA.

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.

3.1.6 The Processing of Name Dispute

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

When the subscriber or applicant's name is proved by the legal documents of the competent authorities that the name belongs to other subscribers or applicant, SHECA will cancel the right of 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.

3.1.7 Naming Agencies

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.

3.1.8 Recognition, Identification and Role of Trademark

The trademark information is allowed to be contained in subscriber's certificate, but cannot 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

When applicants of event certificate have signature behavior, certificate requests are produced such as applications' identification information, and information recorded during signature behavior by certificate applicants (including the certificate applicant's signature scene, signature action, signature content object, or signature content characteristic value, so that the signature behavior can be effectively restored afterwards). Information recorded for the signature behavior is bound to the identity information of the certificate applicant at the time of the certificate application. Therefore, the certificate applicant is considered as the only holder of the private key at the time of the signature.

3.2.2 Authentication of Organization Identity

Subscriber authentication of event certificate refers to the method of institutional identify authentication. The subscriber shall, before applying for the event certificate for the electronic signature, effectively prove the subscriber's identity, accept the relevant provisions of the event certificate application, and agree to assume the corresponding responsibility.

In the process of event certificate identification, CA or authorized registration authority accepts the subscriber's certificate application, reviews the subscriber's authenticity, collects and records the information of subscriber's identity and electronic signature behavior.

3.2.3 Authentication of Individual Identity

Subscriber authentication of event certificate refers to the method of individual identify authentication. Before applying for event certificate of electronic signature, subscriber's identify authentication should be verified, so that to effectively prove the subscriber's identity, to accept the relevant provisions of the event certificate application, and to agree to assume the corresponding responsibility.

In the process of event certificate identification, CA or authorized registration authority accepts the subscriber's certificate application, reviews the subscriber's authenticity, collects and records the information of subscriber's identity and electronic signature behavior.

If a subscriber rejects SHECA's authentication, it is considered an abandonment of the certificate application. SHECA states that SHECA may reject any application requests and has no obligation to specify for rejection.

3.2.4 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:

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

3.2.5 Non-Verified Subscriber information

Generally, this certificate identity information should be verified clearly and reliably, other information submitted by subscriber is non-verified subscriber information.

For non-verified subscriber information, SHECA will archive it in written or electronic form. SHECA will not promise the authenticity of such information and assume any liability and the obligation to settle disputes as this information is untrue or incomplete, etc.

3.2.6 Validation of Authority

When applicant entrusts others to take personal application or organization entrusts authorized person to apply for a certificate, SHECA and its authorized certificate services organization need to review the applicant's identity and eligibility, including the essential proof of identity and authorization, and verify and confirm with representative entity by telephone, letter or other way to review whether applicant has the right to represent the entity. SHECA and its authorized certificate services organization are responsible to verify the validation of authorized information, and to properly preserve authorized information.

SHECA and its authorized certificate services organization SHECA can connect the organization to verify an applicant's authorization (for example, verify the agent's job application or verify whether the applicant is the one who is in the application form) by the way of obtaining phone number and other contact information from a third -party. If SHECA cannot get all the required information from a third-party, it may require a third-party to carry out an investigation, or requiring certificate applicant to provide additional information and evidence material.

3.2.7 Criteria for Interoperation

Other certification services organization can interoperate with SHECA of non-UNTSH certification services system for cross-certification, single cross-certification or other forms of interoperation. But the CP/CPS of certificate services organization must meet the requirements of this document, and certificate services organization may sign the corresponding agreement with SHECA. SHECA will accept the information identified by the certifying authority of non-SHECA and issue the corresponding certificate based on content of the agreement. If there is no similar agreement between the two parties, SHECA will decide whether to accept the reviewed material with specific conditions and make a decision whether to accept. However, SHECA will not authorize any rights for electronic certification service agency via cross-certification. If there are provisions of national laws and regulations, SHECA will perform strictly.

3.3 Identification and Authentication of Re-key Requests

3.3.1 Identification and Authentication of Routine Re-key

The key for an event certificate only applies to one-time signature events, and there is no certificate re-key service.

3.3.2 Identification and Authentication for Re-key After Revocation

The key for an event certificate only applies to one-time signature events, and there is no after revocation certificate re-key service.

3.3.3 Identification and Authentication for Certificate Change

The key for an event certificate only applies to one-time signature events, and there is no certificate change service.

3.4 Identification and Authentication for Revocation Requests

Event Certificate only applies for one-time signature events. Certificate expires immediately after being used, and there is no certificate revocation service.

3.5 Identification and Authentication of Authorized Service Organization

SHECA will authorize external service organization to conduct event certificate business, when the external certification service organization meets related agreements of SHECA authorized service, and agrees to accept supervision and audit evaluation from SHECA.

1. The organization is required to provide following materials when applying for as a SHECA authorized organization:

- Original Business license, and a copy with official stamped seal, Original Organization Code Certificate, and a copy with official stamped seal or Original Legal Person's Registration of Institutions, and a copy with official stamped seal.
- Applicant’ s original ID, and a copy with official stamped seal.
- Application form of authorized service organizations with official stamped seal.

2. Processes of applying for SHECA authorized service organization:

- The applicant completes and signs the “SHECA Authorized Service Organization Application Form”, “SHECA Certificate Admission Operator Registration Form”, “SHECA Authorized Organization (CA Sub-Center) Service Agreement”, all with the official seal, and submitted to SHECA, and submitted a copy of the business license and signed operator's ID card with the official seal.
- SHECA will complete the “SHECA Authorized Service Assessment Form” based on actual situation.

If the applicant organization passes the assessment, the applicant should complete the “SHECA Sub-Center (Sub-CA) Certificate Acceptance Form”, “SHECA Server (RA) Certificate Acceptance Form”, “SHECA Authorized Service Organization Certificate Administrator Registration Form”, and then the applicant organization will be officially authorized by SHECA.

4. Operational Requirements of Certification Life Cycle

4.1 Certification Application

SHECA only accepts online certificate application. The steps requested by certificate application operation should be complied.

4.1.1 Formal Certificate

Formal certificate is ratified by Certificate Authority after submitting real information in accordance with the regulation and the process regulated in this document, and SHECA bears the obligations and responsibilities regulated in this document of such certificates. Applicants need to submit complete application form with personal handwritten signature or official seal according to the requirement of the certificate. The application form can be downloaded from the website or got from SHECA and its authorized service

authority.

SHECA issues certificates into Chinese, English and Chinese and English bilingual edition. The name of the Chinese version is the applicant's Chinese name; English version is the applicant's English name; the name of Chinese and English bilingual version can be the applicant's Chinese name or English name.

When applicants apply for the Chinese version certificate, if applicant is personal, the Chinese name on identification or (other legal personal documents) can be used as the certificate name; if applicant is a company, the Chinese name on business license or other legal organization registration document can be used as the certificate name. When applying for the English version certificate, individual can use the English name on passport or (other legal personal documents) as the certificate name; company should submit materials to prove the English name, if not, SHECA chooses business license or other legal organization registration document as proving material, from which the common English translation of Chinese names as the English name, and the specific company name should be Chinese phonetic alphabet of Chinese name or words in similar English pronunciation. As for the Chinese and English bilingual version, mainly using the Chinese name on legal documents, English name of the certificate is in accordance with the approach applied in English.

Event Certificates are divided into the following two categories:

1. Personal Event Certificate, an event certificate applied in an individual identity to sign a specific time, person, task, or content to effectively prove the reliability of the event.

To apply for a personal event certificate, you need to submit the following materials:

• Application form filled in and signed by the applicant as required,

• Subscriber agreement filled in and signed by the applicant as required.

2. Institutional Event Certificate, an event certificate applied in an institutional identity to sign a specific time, person, task, or content to effectively prove the reliability of the event.

To apply for an institutional event certificate, you need to submit the following materials:

- Application form filled in and stamped with the official seal as required,
- Manager’ s power of attorney that is completed and stamped as required,
- Business license with official seal,
- Subscriber agreement filled in and stamped with the official seal as required,
- If the institution applicant holds a reliable unit identity certificate, only the subscriber agreement filled in and stamped with the official seal is required.

4.1.2 Certificate Application Entity

The entities involved in the certificate application process include:

1. Certificate applicants, including individuals, enterprises, institutions, government agencies, social organizations, people's organizations and other organizations. Any legitimate organizations, individuals and the subject of having a clear identity and ownership may apply for digital certificates to ensure that online transactions and online administrative operations are safe and reliable.

2. SHECA authorized service agencies, as well as the corresponding system, system administrators, operators, etc.

3. The electronic certification service agencies, including SHECA and SHECA authorized sub-CA and so on.

4. Subscribers issued certificate by issuing authority, do not depend whether to accept their certificates.

5. Key generators, including electronic certification service agencies and users choosing the key generator, including but not limited to USB key, IC card, card encryption, encryption machine and other hardware providers and IE and so on.

6. Manage department, including the department defined by the "Electronic Signatures Law of PRC", "Measures for Administration of Electronic Authentication Services", "Measures for Administration of Electronic Authentication Service Password" and other department.

4.1.3 Application Process and Responsibility

SHECA only accepts online certificate application.

4.1.3.1 Application Process

1. Individual applicant

a. CA performs real-name authentication for the applicant through face recognition, bank card verification, mobile phone SMS verification or reliable personal identification. If the real-name certification fails, CA will refuse to issue a certificate to the applicant and file the failed information.

b. If the real-name certification is passed, CA will ask the applicant to enter the certificate application information online.

c. CA requires the applicant to confirm and sign the subscriber agreement online.

d. CA issues a certificate based on the certificate request.

e. The applicant accepts and downloads the certificate.

2. Institutional applicant

(1) Holding a reliable agency identity certificate

a. Verify the authenticity of the applicant's identity certificate online. If the verification fails, the CA will refuse to issue a certificate to the user and archive the failed information.

b. After the verification is passed, the applicant organization needs to fill out and agree to the subscriber agreement online.

c. CA issues a certificate based on the certificate request.

d. The applicant accepts and downloads the certificate.

(2) Not holding a reliable agency identity certificate

a. CA performs real-name authentication for the agent through face recognition. If the real-name certification fails, the CA will refuse to issue a certificate to the applicant and file the failed information.

b. If the real-name certification is passed, the CA agency will ask the agent to upload and submit the application documents with the official seal.

c. CA manually verifies the reliability of the relevant information. If the verification fails, the next step will be refused and the failure information will be directly returned.

d. After the verification is passed, the applicant organization must complete and agree to the subscriber agreement online.

e. CA issues a certificate based on the certificate request.

f. The applicant accepts and downloads the certificate.

4.1.3.2 The Responsibility of the Participating Entities

1. The Responsibility of Electronic Authentication Service Agencies

Electronic certification service agencies should bear these responsibilities: ensure that the private key within their electronic signature certification service providers is stored and protected safely in SHECA, and security mechanisms by SHECA established and carried out meet national policy need.

Electronic authentication service agencies may audit and manage its authorized service agencies to ensure the safety and reliability throughout the application process.

Electronic certification service agencies provide safe and reliable operation for CA system. SHECA doesn't bear reparation responsibility of operational failure or delay caused by objective accidents or other force majeure event. To express clearly, these events include strikes or other labor disputes, riots, civil unrest, supplier actions, intended or not, force majeure, war, fire, explosion, earthquake, flood or other disasters.

2. The responsibility of certificate applicants

Certificate applicants must strictly comply with requirements about the ownership of private key and certificate applications related hold safely:

The certificate applicants commit that all the statements and information filled in the application form must be complete, accurate, true and correct, for inspection and verification of issuing authority. Moreover the certificate applicant is willing to undertake legal liability arising from any false information provided, false information and other acts. As the application selves reasons causing that issuing authority is unable to correctly issue the certificate that the applicant should bear the loss and liability.

Before applicants applying for or accepting the certificate and its related services, they need to know the regulations of this document and policies related with the certificate. Before SHECA receiving applications, it considers that applicants have already known the content of this document, and promise to comply with restrictions by the certificate holder using certificate.

3. The responsibility of subscriber

When SHECA recognizes the applicant's application and issues a certificate for applicant, certificate applicant becomes a subscriber, no matter what certificate is or not received by applicant

Subscribers must ensure that the certificate is used as intended application purpose.

SHECA only inform, but does not require certificate applicants comply with security measures SHECA proposed. Subscribers can choose any secret measures that they think.

4. The responsibility of the relying party

The relying party trusts the certificates issued by SHECA and sub-CA, must ensure comply with and carry out the following terms:

(A) The relying party is familiar with the terms of this document and policies, laws certificate related, understands the purpose and restrictions of certificates using.

(B) Before the relying party trusts the certificates issued by SHECA and its sub-CA, they must have a reasonable review, including but not limited to: check whether the certificate is valid, check effective CRL SHEC announced to obtain the certificate status. SHECA thinks that the relying party always follows this provision. Once the relying party violates the terms and brought to SHECA losses because of negligence or otherwise, SHECA will reserve the right to take appropriate legal action.

(C) All relying parties must recognize that their behavior of trusting the certificate means that they have

acknowledged and understood the relevant regulations of this document, including the terms of exemption, rejection and limit obligation.

5. Responsibility of Key Generator Provider

Once the certificate applicants choose certain key generator, it indicates that the applicant trusts security and reliability of key pair generated by the generator. SHECA does not provide any form of guarantee, and has no responsibility and right to deal with dissension.

6. The Competent Authorities

SHECA commits that it will provide a third-party electronic authentication services in accordance with strictly laws and regulations of national authorities and meet the requirements of a written request from competent department.

4.2 Certificate Application Processing

4.2.1 The implementation of Identification and Authentication

SHECA and its authorized certificate service agencies have rights and responsibilities to identify reasonably for applicant identity. For security and audit requirements, the certificate application form should be recorded the name, signature, date of verification and validation results of identifier.

Upon receipt of subscriber's certificate application, the issuing agencies shall complete the following identification work as the pre-conditions of subscriber's certificate issued:

- Verify that the certificate applicant has accepted the terms of the subscriber agreement.
- Verify the identity of the certificate applicant as required by the event certificate.
- Confirm the certificate applicant is the legal owner of private key that matching with the public key contained in the certificate (such as asking subscriber to guarantee, etc.).
- Confirm the information contained in the certificate is accurate except unauthenticated subscriber information.
- Confirm any trustee applying for a certificate in behalf of their organizations, and has been represented by the organization's legal authority.
- Confirm legitimacy and authority of the identity of the consignor and the consignee.

After the issuance of the certificate, SHECA will no longer bear the responsibility to continue to monitor and investigate the accuracy of the certificate, unless it is noticed the certificate has been damaged described in this document.

SHECA retains the right to update identification procedures and requirements. The identification procedures and requirements renewed will be published on http://www.sheca.com, and you can also obtain it via the following address:

18F, No.1717, north Sichuan Road, Shanghai, People's Republic of China (200080)

Shanghai Electronic Certificate Authority Center Co., Ltd.

SHECA Customer Service Center

The auditors of SHECA and its authorized service agencies audit reasonably and prudently for the applicant identification and approve or reject.

4.2.2 Certificate Approval and Rejection

SHECA and its authorized service agencies receive the certificate applications then identify the application information and identity information completely, effectively, reliably and truly, and if it is accurate, they will approve the applications. SHECA and its authorized service agencies issue a certificate for the applicant in accordance with the provisions of CPS to prove that they have approved the applicant's certificate request.

The certificate application was authorized, if the following conditions occur:

- The application satisfy fully the clause 3.2 about the subscriber's identification information and identification requirements.
- Applicant accepts or does not opposed to the content or requirements of the subscriber's agreement
- Applicant has paid in accordance with the provisions, except other provisions.

When SHECA and its authorized certification service agencies are in the identification process, if the applicant fails to successfully identify, SHECA will reject the applicant's certificate application and notify applicant failure. SHECA has the right to refuse to explain the reason for the failure, and does not need to notify the applicant except for a clear legal requirement. If it is the third-party information which led to identification failure, SHECA will provide this third-party contact information for applicants to inquire. SHECA uses the same method that the applicant submits a certificate application to the SHECA to notify the applicant that his or her certificate application is failure.

SHECA can also refuse an applicant certificate in its sole discretion, and does not need any explanation, and does not have obligations and liability of any loss or costs. Unless the applicant of the certificate has submitted fraudulent or falsified information, after SHECA refusing to issue a certificate, SHECA would immediately return the cost that the applicant pays for the certificates.

If the following circumstances happened, SHECA may refuse the certificate request:

- The application does not meet the terms of the previous 3.2 Information on the identity of subscribers and identification requirements.
- The applicant cannot provide the required identity documents or other supporting documents that is needed.
- The applicant cannot accept or against the relevant content and requirements of the subscriber's agreement.
- The applicant has not or cannot pay the appropriate fees.
- RA or CA considers that the approval of the application will bring the dispute, legal disputes or losses to the CA.

The certificate applicant who is rejected could then apply again.

4.2.3 Time of Processing the Certificate Application

Event certificate application is processed immediately.

4.3 Certificate Issuance

4.3.1 The Behavior of Electronic Certification Services Agencies

and Registered Agencies When Issuing the Certificate

Upon an applicant submitting a certificate application, despite the fact that he or she doesn't accept the certificate, but still regarded as the subscriber who has agreed to receive a certificate from the issuing authority.

When the issuing authority approves the certificate request, it will issue a certificate. The release of certificate means SHECA formally approved the final certification application.

4.3.2 Notification to subscribers by Electronic Certification Services Agencies and Registered Agencies

The event certificate is used to identify and prove the electronic signature behavior of the subscriber. After the certificate authority approves the certificate application, the certificate issuing certificate will be issued to the subscriber and directly applied to the corresponding electronic signature. If the subscriber successfully completes the electronic signature, it is deemed that the SHECA certificate is successfully issued, and SHECA no longer advertises the certificate to the subscriber in other ways.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

After the event certificate is issued and the certificate is applied to the corresponding electronic signature, it is deemed to agree to accept the certificate.

4.4.2 Publication of the Certificate by Electronic Certification Services Agencies

Once the subscriber accepts the certificate, SHECA will publish one or more copies of the certificate in its repository, directory services and other repository. Subscribers can also publish their certifications in other places.

Subscriber and the relying party can query their own or other subscriber certificates through HTTP.

If the subscriber submits written application, CA cannot publish the subscriber's certificate information to any public information repository.

4.4.3 Notification to other entities when Electronic Certification Services Agencies issues the certificate

With regard to the issue of event certificates from SHECA, SHECA does not advertise other entities.

4.5 The Key Pair and Certificate Usage

4.5.1 The Subscriber Private Key and Certificate Usage

After submitting a certificate application and accepting a certificate issued by a CA, the subscriber is deemed to have agreed to abide by the terms and rights of the CA agency and the relying party. Subscribers can use their certificate and the private key that corresponds to the certificate. The certificate can be used only based on this document and the relevant provisions of the CP/CPS. Subscribers can only use the private

key and certificate in the proper range of applications which is consistent with the contents of the certificate (if the usage and purpose of the certificate is defined in some fields, this certificate will be used only in this range, such as key usage). All acts must be consistent with the requirements of the subscriber agreement.

The event certificate is only applied to the corresponding electronic signature behavior of the subscriber. The subscriber can only use the private key and the certificate in the electronic signature. The subscriber can perform the electronic signature operation using the corresponding private key only after accepting the relevant certificate. The private key will be destroyed after completing the electronic signature math operation, and then the subscriber must stop using the private key corresponding to the certificate.

When using electronic signature information and electronic signature issued by SHECA, participants have the rights and obligations provided by this document. Participants (the issuing authority, the certificate subscriber and relying party) agree to abide by this document, UNTSH CP/CPS and SHECA agreement. Any usage of certification and private keys beyond the provisions of this document, SHECA will not bear any resulting consequences.

If the usage and purpose of the certificate is defined in some fields, this certificate will be used only in this range. The person who takes any actions beyond certificate marked the usage scope bear the responsibility. Beyond any usage scope, SHECA does not bear any responsibilities and obligations arising therefore.

4.5.2 The Relying Party Public Key and Certificate Usage

Before trusting the certificates and signatures, the relying party should make due diligence and reasonable judgments independently:

- Whether the certificate issued by a trusted CA.
- For any given purpose, the certificate is used appropriately; whether the certificate is used against this document, CPS or the relevant laws and regulations. After the acception of certificate, the subscriber is fully responsible of the appropriate use of the certificate.
- When the certificate is used whether it is consistent with the content included (if the usage and the purpose of the certificate is defined, this certificate will only be allowed to use within this range, such as key usage).

Unless provided in this document, certificate from the issuing authority is not any commitment of power or privilege. The relying party only trusts certificate and the public key contained in the certificate within the limits prescribed in this document and makes this decision.

If the usage and purpose of the certificate is defined in some fields, this certificate will be used only in this range. This relying party must make reasonable judgments, and the person who takes any actions beyond certificate marked the usage scope bear the responsibility. Beyond any usage scope, SHECA does not bear any responsibilities and obligations arising therefore.

4.6 Certificate Renewal

The event certificate is only used for the subscriber's specific one-time electronic signature behavior, and there is no certificate update service.

4.7 Certificate Key Renewal

The event certificate key is destroyed after it has been used once, and there is no certificate key update service.

4.8 Certificate Modification

The event certificate is only used for the subscriber's specific one-time electronic signature behavior, and there is no certificate modification service.

4.9 Certificate Revocation and Suspension

The event certificate is only used for the subscriber's specific one-time electronic signature behavior, and there is no certificate revocation and suspension service.

4.10 Certificate Status Services

The event certificate is only used for the subscriber's specific one-time electronic signature behavior. Once the certificate is used once, it will be invalid. According to the agreement of the relying party, the status query service can be provided to the relying party.

4.11 Termination

The termination of the event certificate subscription means that when the subscriber completes the electronic signature using the digital certificate, the service time of the certificate ends.

4.12 Key Generation, Backup and Recovery

4.12.1 Signature Key Generation, Backup and Recovery Strategies and Actions

After the subscriber's signature key pair is generated by the signature device and executed, the signature is immediately destroyed and the signature key is not stored.

5. Facility, Management and Operational Control

5.1 Physical Control

The physical control and security policies, authentication service system complied with by SHECA and subordinate authorized service agency is in a secure building which has independent hardware and software operating environment. Only authorized operators can enter into the appropriate area to operate based on the related security practices. Root key of SHECA in the environment of maximum security strength avoid the operation destroying or operating unauthorized.

5.1.1 Site Location and Construction

The host house of SHECA authentication system is in Shanghai Telecom Building, and backup room located in Shanghai Big Data Center Disaster Recovery Center has four physical protection layers to monitor and manage physical channel. Host and backup rooms of SHECA are equipped with shock-proof, fireproof, waterproof temperature control systems, access control systems, video surveillance systems and alarm systems to ensure continuity and reliability of certification services. The construction and management of all rooms is in strict accordance with the requirements of SHECA. In principle, machine room is prohibited to visit, only person authorized by SHECA can enter into the site and the area authorized. The high-security monitoring technology was made in generator room, including video, fingerprint, access control and other security management tools to ensure the security of the physical channel. Entering into SHECA generator

room, there are time-limited access control system. All-weather automatic monitoring is carried out in computer room.

Monitoring Record documents includes the records of all traces of channel in the engine room.

All personnel authorized by the SHECA acts in restricted areas accompanying with SHECA staff. List of personnel authorized by SHECA is sent to SHECA operation responsible departments to ensure that only personnel authorized by SHECA can enter the room. For the visitors who want to enter the SHECA room, only after the corresponding approval, accompanied by the SHECA authorized employees can enter the SHECA room.

All authorized service agencies by SHECA, including the registered agencies, RAT certificate service systems must be protected to ensure that only employees authorized can enter the system to operate. SHECA administrator is responsible for setting and checking privileges of registration agencies, RAT administrator. The privileges and responsibilities of registered agencies and RAT operator are made provision in the operation agreement.

5.1.2 Physical Access

Operators enter the room, through the IC card access control system and fingerprint identification system; operators enter and leave shielded room, engine room and other important system areas also together with two or more person, and 24-hour video surveillance.

When the operator enters the work area, he or she must access through fingerprint verification and inspection.

5.1.3 Power and Air Conditioning

CA supplying power is fully protected with using an uninterruptible power supply (UPS) to avoid power fluctuations. Dual power is used when the single power supplied is damaged, which can automatically switch to maintain the system normal operation.

CA air conditioning system uses a separate air conditioning system and ventilation equipment to ensure that the temperature and humidity is controlled within the operation scope to ensure system stability.

SHECA maintains according to the provisions of the telecommunications facilities.

5.1.4 Water Exposures

The place SHECA CA system in is an enclosed building, and taking measures of a raised floor to prevent flood erosion.

5.1.5 Fire Prevention and Protection

Machine room is adopted fire-resistant materials with the central fireproof control equipment and automatic sprinkler system to avoid the threat of fire. SHECA establishes fire prevention and protection and other emergency response measures through coordination with professional fire departments, and the machine room passes the fire test from the national authorities.

5.1.6 Media Storage

The storage medium system used is in anti-magnetic, anti-static interference circumstance, safe and reliable protection, against harm and destruction produced possibly from such as temperature, humidity, and magnetic and other environmental changing.

5.1.7 Waste Disposal

Hardware devices, storage devices, encryption devices used by SHECA, are abandoned, involving in sensitive and confidential information eliminated safely and completely.

The documents、 materials and storage media containing sensitive and confidential information before disposal have been a special measures to ensure that the information cannot be recovered and read.

All the procession behavior will be recorded in order to meet the needs of the review, and all the destruction behavior shall follow the relevant laws and regulations.

5.1.8 Off-site Backup

System backup: CA system has the off-site system backup, preventing the system cannot work properly because of uncertainties. When the main system cannot work properly, the backup system will be put into use to continue to provide certification services.

Data backup: SHECA has the off-site data backup at the same time. The operation of off-site backup is made in the disaster recovery plan of SHECA. Security requirements for medium of SHECA off-site data backup are corresponded with backup standards and procedures of SHECA.

5.2 Procedural Control

5.2.1 Trusted Roles

Certificate services have the requirements of high reliability and high security. The employees, third-party services, consultant and so on who should be recognized as credible persons can work in a credible position, in order to ensure that reliable personnel management. SHECA have all the right to use or control staff, third parties service personnel (collectively, the "staff") that may affect such operations (including repository restrictive operations for SHECA) as the issuance of the certificate, usage, management and revocation, considered as credible role in this document.

SHECA clearly defines the key functions positions for CA, including

1. The administrator of the application system,
2. The administrator of the operating system,
3. The administrator of the database system,
4. The administrator of the network system,
5. Entry staffs,
6. Auditors,
7. The key control group,
8. Safety Executive Group,
9. Other personnel.

Arrangements for these posts are to ensure share a clear responsibility and establish an effective security mechanism to ensure the safety of internal management and operations.

SHECA in accordance with this document and authorized agreement creates the management practices of authorized certification services organization (RA, RAT and others), standardizes the certification service organization and the operation of service systems management staff and operator. Take full account of

security constraints during a related software designed.

Responsibility of authorized certification service organization by SHECA is divided reasonably to ensure responsibilities and obligations management and implementation through the systems and technology.

5.2.2 Number of Persons Required per Task

CA and RA should establish, maintain and enforce strict control process, and establish measures of duties segregation, based on job requirements and arrangement to implement the safety mechanism of mutual restraint, mutual supervision to ensure that sensitive operation is completed by a number of credible personnel.

Tactics and control procedures of duties segregation are based on the requirements of actual duties. For the certification business, the most important sensitive operations is visiting and managing CA cryptographic equipment, distribution and management of key material and protection of key password. These operations must require more credible personnel to accomplish together. The sensitive internal control processes require two credible personnel at least to participate, have their own independent physical or logical control facilities, and the process of CA key equipment life cycle is required strictly to participate together by more credible personnel. Key control will be separated physical and logical, such as the personnel having critical equipment physical authority cannot hold logic authority, and vice versa.

SHECA ensure that a single person cannot touch, export, restore, update or revoke the private key stored by SHECA. At least three persons together may have the operation of any CA key generation and key recovery, by a technology of secret key segmentation and synthesis for participating operators.

For identification and issuance of the certificate application, it requires two credible personnel at least to operate.

For manipulation of critical systems data and important system, it needs one person to operate, at the same time one person to monitor at least.

SHECA has a clear labor division for its operation and functions related operation, the security mechanism of mutual restraint, mutual supervision.

SHECA usually arranges one person to operate, the other one to monitor and record for operations and maintenance of critical system.

5.2.3 Identification and Authentication of Each Role

For all personnel seeking to become Trusted Persons, verification and authentication of identity is performed strictly to ensure that it can meet the requirements for the job duties. Mainly including:

- Each role should be defined according to actual needs and be distributed with rights and requirements as well as background demands.
- In order to meet the requirement for the role, background investigation should be conducted for personnel seeking to be included as certain role.
- Security token and proper rights should be assigned to trusted roles.

Before the credible background checking, firstly the person's authenticity and reliability of physical identity is confirmed, and identity is further confirmed through the background checking procedures in CPS.

All serving officers in SHECA must be certified then given to the required system operation cards, access cards, password, operating certificate, operating accounts and other security tokens, according to the job nature and position right. For the employees using security tokens, SHECA will record completely all the

operating behavior.

All SHECA employees must ensure that:

- Security tokens issued only directly belongs to personal or organization.
- Security tokens issued does not allow to share.
- SHECA systems and processes control operator authority by identifying the different token.

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 requests, key recovery requests or renewal requests, or enrollment information.
- The issuance, or revocation of Certificates, including personnel having access to restricted portions of the repository.
- The handling of Subscriber information or requests.
- The generation, issuing or destruction of a CA certificate.
- The personnel of system on-line or off-line.
- The personnel of mastering important password key.
- Management staff and operator of key and cryptographic equipment.

The acceptance of the certificate services is completed by two roles entry clerks and auditors.

For the root key operation, three or more of the root key administrator simultaneously on the scene, can carry out the operation.

When SHECA system encountering emergency and need to joint repair, one SHECA personnel at least on the scene, repair personnel accompanying with SHECA personnel, may carry out licensing operation, and all operations, modifications retain records.

When the non-SHECA employees because of physical fix, fire, high power failures, etc., need enter the machine room to repair something, they must be approved, firstly with the identity confirmed. Then repair personnel is agreed to complete the repair of the agreed parts by SHECA while under accompanying and guardian of stuff of SHECA.

5.3 Personnel Control

5.3.1 Qualifications, Experience, and Clearance Requirements of No-fault

Personnel seeking to become Trusted Persons must present proof of the required background, qualifications, experience and other conditions, and is able to submit the appropriate documents.

- Various operators of certification business systems in SHECA must have the characteristics of credibility and high enthusiasm, other part-time work without affecting their jobs. And they don't have the irresponsible experience of certification business operation, and there is no lawlessness record.

- System operators must have relevant work experience in authentication systems or obtaining related training in SHECA.
- Managers must have practical certificate authentication experience and many years of experience in systems management and operation.

5.3.2 Background Check Procedures

The personnel operating as trusted role need to take a rigorous background investigation process, generally re-investigate again within five years. Background investigation must comply with laws and regulations, and survey content, survey method and officer engaging in the investigation shall not violate the laws and regulations.

According to the work characteristics of different credible position, background checks should include but are not limited to the following:

- Identification, such as personal identity cards, passports, permanent residence booklet, etc.
- Education, degrees and other qualifications.
- Resume, including education, training experience, work experience and reference related.
- No crime evidence.

Background investigations should use legal ways as much as possible background information verification by relevant organizations, departments for staff. The person assessment is worked out by certification organization's human resources department and security personnel.

Employees in SHECA need to have study period of three-month, and employees of key and core position after pass the study period, they also need an additional study period. According to the inspection results Employees are arranged for relevant work or fired. According to the need for staff, SHECA conduct the training of responsibilities, job, technology, policy, legal, security and other aspects.

SHECA will conduct strictly the background investigation for staff in key positions. Background investigation need to verify the materials and procedures, including but not limited to the following:

- Verify the authenticity of the previous work record.
- Verify the authenticity of identity.
- Verify education, degrees and other authenticity of credentials.
- Check no criminal evidence and confirm without a criminal record.
- See whether there is a serious dishonesty in the work through appropriate channels.

In the background investigation, if SHECA finds the following circumstances, SHECA can refuse qualifications of trusted personnel:

- There is fabricating facts or information.
- With evidence of the unreliable staff.
- There are some criminal record or fact.
- Use illegal identification or education, qualifications.
- The behavior of serious dishonesty in the work.

The check of certification service manager and operator staff authorized by SHECA can refer to the way of trusted employees examination by SHECA, on this basis, increasing visits and training provision, but not

contrary to this document and the corresponding CP/CPS, licensing agreements and requirement of public certificate services specifications by SHECA.

SHECA establishes the rules of process management regulation, and under which employees are restrained by contract, not allowed to disclose sensitive information of SHECA certificate service.

All employees sign confidentiality agreements with SHECA and go on working in similar with SHECA after expiration of the agreements 2 years.

If necessary, SHECA can complete background investigation on employee collaborate with relevant government departments and investigative organizations.

5.3.3 Requirements of the Training

The following training is offered by SHECA to staff:

- SHECA security management strategy.
- Job responsibilities.
- PKI basic knowledge.
- The software description of SHECA authentication system used.
- Control system of authentication and management on SHECA.
- Identity authentication, auditing policy and procedures.
- Disaster recovery and business continuity procedures.
- Authentication policy, the policy of this document and related standards and procedures Common threats in regards to authentication procedure, including phishing and other social engineering actions.
- Electronic authentication and other relevant laws and regulations.
- Other training.

SHECA shall record the staff training and archive the record, and assure the personnel have qualified skill as required prior to work.

5.3.4 Retraining Frequency and Requirements

SHECA may require employees to continue training to adapt new change, according to SHECA strategy adjustment, system updates, etc.

The company Safety management strategy should be training at least once a year.

Related personnel for authentication system operations should be trained relevant skills and knowledge at least once a year.

For the cases of authentication system upgrade, new systems implementation and the progress of PKI / CA and cryptographic technological etc., SHECA needs to arrange appropriate training accordingly.

5.3.5 Job Rotation Cycle and the Sequence

The operation and maintenance personnel have different responsibilities with the employees who design and develop system in SHECA certification system, separation of both positions, and in order to ensure safety the latter cannot become the former that means developing staff and running staff are in duty segregation.

In order to meet the certification system operational needs and job adaptation, SHECA will select suitable candidates according to the situation in the rotation of different positions. But this rotation shall not violate the principle of the position separation above.

5.3.6 Penalties for Unauthorized Actions

When SHECA employee is suspected or has carried out unauthorized operations, such as abusing right under the unauthorized situation or using SHECA system beyond the limits of authority or conducting the ultra-operation, after SHECA get information to suspend immediately that personnel entered work of certification services within the system on SHECA. According to the severity, SHECA can take criticism education, and implement including the submission to judicial authority.

Once any one of above happens, SHECA suspends or terminates immediately the personnel's security token.

5.3.7 Requirements of Independent Contractor

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

In order to continue normal security operation for authentication system running, employees should be provided with the relevant document, at least, including the following:

- System software and hardware documentation for the operation, cryptographic equipment documentation for the operation, WWW services for operating documentation.
- The operating instructions manual for authentication system itself.
- CP/CPS, electronic certification business rules and related protocols and specifications.
- Internal operating files, including backup manual, disaster recovery programs.
- Job descriptions.
- Company-related training materials.
- The standards of relevant safety management.

5.4 Audit Logging Control

5.4.1 Types of Event Recorded

SHECA must record the events of operating system-related with the CA and RA. These records whether handwritten, or electronic format must include date of the event, content of the event, time of the event, entities of event-related, including but are not limited to:

1. Information of certificate subscriber service application and revocation, such as the application form, agreement, identity information and other relevant information.

2. Generation, storage, recovery, archiving, destruction, transportation and migration for CA key.

3. All kinds of service system key pair for generation, built-in, changes and other records of success and failure in the authentication system.

4. The log files generated from the authentication system daily operation.

5. Form of passing in and going out the control area of SHECA and its authorized agencies, record of security token passing in and going out sensitive areas, work logs of machine room, records of system maintenance daily, surveillance video, etc.

7. The records of system software and hardware devices on the line, replacement and off-line and other.

8. Specifications and records related work of among CA、RA、RAT.

9. SHECA also records the events not directly related with the system, such as visiting records of physical access, personnel changes.

10. Record of credible personnel management, including account application record of network access, an application record of application, change, creation for the system permissions, personnel changes in circumstances.

11. System security events, including: activity of successful or unsuccessful access to the CA system network, unauthorized access attempts and access for CA system network, unauthorized access attempts and access for the system files, security, sensitive documents or records of read, write or delete, system crashes, hardware failures and other anomalies.

12. Security events of firewall and intrusion detection system recording.

5.4.2 Frequency of Processing Log

SHECA periodically reviews the log records, putting on records for the behavior of the record reviewed. Reviews should be conducted not less than two times in 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

SHECA carries out strictly the measures of physical and logical access control to ensure that only personnel authorized by SHECA can close to the records reviewed. These records are strictly protected, and strictly prohibited of the operations of unauthorized access, read, modify, and delete.

5.4.5 Backup Procedures of Audit Log

SHECA ensures that all records of review and the summary of review in accordance with standards and procedures on SHECA are backed up. Following the nature and requirements of the record, it needs real-time, daily, weekly, monthly and annual and other forms of backup, using a variety of on-line and off-line backup tools.

5.4.6 Audit Collection System

SHECA audits collection systems, including the objects involved:

- Certificate management system.

- Certificate issuing system.
- Certificate accepted and approval system.
- Backup and recovery system.
- Access and control systems (including firewalls).
- Customer service system.
- Security system of website, database.
- other systems by SHECA considering necessary to review.

SHECA conducts collection and review for the system log to meet the system's safe operation needs using the mode of automatic and manual combination.

5.4.7 Notification of Abnormal Events

When operation of the authentication system has affected safety control, the security officers must be informed, and measures should be taken. If the operation affects the system seriously, which leads to SHECA providing abnormal services on certificate, SHECA will announce to user by website and other way.

If attack phenomenon is found during the review in SHECA, SHECA will record the attack behavior and retrospect the attacker within the law. SHECA reserves the right to take appropriate counter measures. According to the attacker's behavior, SHECA takes the measures including cutting off the open services for attacker, submitting the judiciary to deal with. Whether to notify the attacker or the perpetrators, it is decided by SHECA.

5.4.8 Weakness 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. 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 Record Archive

5.5.1 Types of Records Archived

SHECA follows the records (including but not limited to) for archiving:

1. System constructed and upgraded documentation of SHECA.

2. Certificate application for information, information of certificate service approved and rejected, the certificate subscriber agreement and so on.

3. Log data of system operating and certificate authentication service, the key upgraded for certificate authentication system, and the information updated, etc.

4. The electronic certification service rules, the services specification and operational protocols, and management regulation.

5. Data of the system database.

6. Records of personnel passing in and out, and records of third-party personnel service.

7. Video surveillance.

8. Employee information, including background investigation, hiring, training, etc.

9. Various external, internal document of the review and assessment.

5.5.2 Retention Period of Archiving Records

In addition to the deadline of preserve by laws and regulations and proposed of the certificate authority, SHECA develops about third-party electronic authentication related for operating information archived for at least the following.

1. The business rules of the electronic authentication, certificate policy, forms of the user application information and related agreements, subscriber applications, renewals, expired and revoked certificates should be kept for at least 7 years after the end of the certificate validation.

As for those e-government electronic certification services for government departments, the related documents and information should be kept for at least 10 years.

2. The service records of the certificate user's certificate application, query, and revocation should be saved for at least 7 years after the validation of the certificate.

3. The subscriber's certificate, key and changes of related information are saved 7 years at least.

4. The certificate and key of certification authority, and related change information are saved 20 years at least.

5. Video surveillance content is stored in local hard disk in the system for one month. Video surveillance content in the surveillance system is backed up weekly. Backup content must be kept for one year, in accordance with the provisions to archive a year later.

6. Other information is retained for 5 years at least.

7. Records of business management is retained not less than 2 years

8. If the time is different with the provisions of laws and policies, the longer time between them is chosen.

In addition, SHECA can decide the information regular archive period without an explanation and interpretation, under the premise without violating the laws and regulations and the provisions of the competent authorities.

5.5.3 Archive File Protection

Archive content is ensured not only physical security measures, but also cryptography guarantees, which ensure that the archive document can be saved effectively and long-term. Only authorized personnel can close and access the archive content in accordance with the specific security way.

In addition to legal requirements and the certification practices need, no person gets freely.

SHECA protects files information related to avoid the threat of harsh environment such as temperature, humidity and strong magnetic and other damage to ensure that the content of archiving content within the period of provision, meets the needs of any legitimate requirement for reading and using. For information

deemed necessary, SHECA will take the way of off-site backup to save.

The identification information and basic information of the application and user saved by SHECA, any unrelated third parties can't get them by non-governmental authorities or the judiciary to apply through legal means.

5.5.4 Backup Procedures of Archive File

All the documents and data archived, usually is stored in the main storage site on SHECA. Really necessary, it will also be saved the backup in its offsite. Database archived generally is accepted the physical or logical isolation for approach, not exchanging information with the outside world.

Only authorized personnel can conduct the operation for reading the file in the supervision of the case. SHECA makes sure that it prohibits deletion or modification for backup and files, or other inappropriate operations in the security mechanism.

The files and data to be continued and saved are backed up and archived on SHECA backup strategy.

When the authentication system is leaded to abnormal operation because of unusual circumstances, in accordance with SHECA recovery strategy, the system can be recovered by these data archived.

5.5.5 Requirements for Time-Stamping of Records

All the archive contents above have time stamp, for example, the time recorded automatically by the system, or the time marked manually by the operator. The time doesn't take the time stamp based on the encryption manner.

5.5.6 Archiving Collection System

SHECA authentication system operational information related from the SHECA internal staff or the security controls internal system is generated and collected in accordance with operation for manual and automatic conducted, and is managed and classified by the people with the relevant authority.

5.5.7 Procedures to Obtain and Verify Archive Information

Only authorized Trusted Personnel are able to obtain access to the archive. The integrity of the information is verified when it is restored. During the archiving period, all the records accessed must verify the consistency in the return.

5.6 Expiration Date of Root Certificate for Electronic Certification Services Agencies

Valid of SHECA root certificate for a maximum is not more than 25 years, and any certificate validity issued by root certificate including the sub-CA certificate, the subscriber certificate, is shorter than the valid of root certificate. Any subscribers certificate validity issued by sub-CA certificate, is shorter than the sub-CA certificate validity.

The validity of root certificate and sub-CA certificate is introduced clearly in the certificate.

5.7 Key Changeover of Electronic Certification Services Agencies

Prior to the expiration of certificate, SHECA will replace the root key in accordance with the provisions of this

document, and generate a new certificate. When making a generation for key, specifications of SHECA key management is followed strictly. CA key replacement must comply with the following principles:

1. The new certificates isn't issued before the end of the lower certificate life cycle, which ensure that all subordinate certificates are all expired as the CA certificate expiration.

2. CA continues to issue CRLs signed with the original CA private key until the expiration date of the last Certificate issued using the original key pair has been reached.

3. CA key generation and management conform to key regulations strictly.

4. Release the new CA certificate timely.

5. The entire transition process is safe and smooth, which did not appear a vacuum of trust and confidence.

6. As for the CA certificate of external authorized orgnizations (sub-CA), key replacement is not available. To replace the key or update the CA certificate, external authorized orgnizations have to follow the certification application procedures.

5.8 Compromise and Disaster Recovery

SHECA assigns a reliable damage and disaster recovery plan to deal with the system problems by unexpected incidents, in order to enable to regain certification system operation in the shortest time when the situation of abnormal or disaster appears.

5.8.1 Incident and Compromise Handling Procedures

When SHECA is attacked, the following happens, a communication network resources are destroyed, computer system of equipment cannot provide normal services, software is damaged, the database is tampered or disaster because of force majeure. SHECA will imply recovery according to disaster recovery plan. Specific work depends on SHECA disaster recovery plan.

5.8.2 Computing Resources, Software and / or Data Corruption

In the event of the corruption of computing resources, software, and/or data, such an occurrence is reported to SHECA, incident handling procedures are enacted, follows SHECA system backup and recovery operations manuals and conducts the system recovery operations to enable authentication system to resume normal operations in accordance with backed-up data within the system or off-site backed-up data.

When the authentication system hardware device is damaged, SHECA can follow system backup and recovery operations manuals to start the backup hardware, and related operating system backed-up and authentication system to restore system operation.

Recovery process should be completed by SHECA as soon as possible, if not to complete the recovery process within 6 hours, and the accident led to the certificate services without operation, then SHECA should start off-site backup mechanism to restore certificate services within 24 hours.

5.8.3 SHECA Private Key Compromise Procedures

When SHECA root private key appears damage, missing, leaking, cracking, tampering or unauthorized used by third parties, SHECA should:

1. SHECA reports immediately to the electronic authentication service management office and other government departments through the website and other public media to notice for subscribers, and takes measures to protect t users' interests.

2. SHECA revokes immediately all the certificates issued, and updates CRL and OCSP information for certificate subscriber and relying party to query. Meanwhile, SHECA generates immediately a new key pair and self-issues a new root certificate.

3. SHECA Re-issues lower certificates and lower sub-CA certificate for operating in accordance with this document about provision of a certificate issued after the new root certificate is issued.

4. After the new root certificate issued by SHECA, it will be immediately published by SHECA repository, directory server, HTTP, etc.

When private key of SHECA sub-CA appears damaged, missing, leaking, cracking, tampering or doubt for unauthorized used by third parties, SHECA should:

1. Sub-CA reports immediately to the SHECA and generates a new key pair and certificate request to apply a new certificate issued by SHECA.

2. SHECA reports immediately to the electronic authentication service management office and other government departments through the website and other public media to notice for subscribers, and takes measures to protect t users' interests.

3. All the certificates issued by the sub-CA are revoked immediately to update information on OCSP for certificate subscriber and relying party to query.

4. Subscriber certificate is re-issued in accordance with this document about provision of a certificate issued after the new sub-CA certificate is issued.

5. After the new root certificate is issued, it will be immediately published by the SHECA repository, directory server, HTTP, etc. for distribution.

When private key for subscriber certificate appears damaged, missing, leaking, cracking, tampering or doubt for unauthorized used by third parties, the subscriber should follow the provision with this document, applying for certificate revocation firstly and following the provisions to re-apply the new certificate.

5.8.4 Continuity Capabilities on Business after a Disaster

In order to avoid the authentication business intermission because of the sudden disaster, SHECA develops a comprehensive continuity plan on business, and establishes the corresponding backup system for off-site disaster, hardware and software, data storage, and user certificates information required for the operation, business practices and disaster recovery documentation provided by certification, leaving an appropriate distance from safe place of existing operational systems to establish backup system and backup files.

The conduct training and testing of disaster recovery plan is conducted for authentication business recovery system of off-site disaster recovery center, according to demand a year at least, and updating the recovery plans and disaster recovery file immediately and saving the corresponding archive record in accordance with changes of the actual situation. In order to ensure when abnormal disaster appears, SHECA certification system can recover system for operation and service delivery within 24 hours at most, which will minimize the risks.

5.9 CA or RA Termination

If SHECA discontinues operations for any reason, SHECA will report to competent authorities in accordance with relevant laws and regulations, and operates on the basis of legal procedures, including:

1. Before the deadline of the laws and regulations provisions, SHECA notices the competent authorities, the certificate holder and all other related entities.

2. Arrange the business to undertake.

- Save all of the operational information related to certification service, including certificates, user information, system files, CP/CPS, norms and agreements.
- Stop the related operation services.
- Clear system root key.

When certification service agencies authorized by SHECA discontinues service for any reason, SHECA deals with related business matters and other matters in accordance with the signing agreement. Termination of service for any reason, SHECA will operate in accordance with the RA operation agreement to undertake the business matters and other matters.

If any of following circumstances occurs, SHECA should revoke the subordinate CA or RA, and revoke the subordinate CA or RA certificate within 7 days:

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

2. SHECA obtains evidence that the Certificate was misused;

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

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

misleading;

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

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

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

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

6. Technical Security Controls for Certification System

6.1 Key Pair Generation of SHECA Event Certificate

Key pair is the critical part for electronic signatures security mechanism. The corresponding provisions are created in the CPS to ensure generation, transmission, installation for the key pair with confidentiality, integrity and non-repudiation.

6.1.1 Key Pair Generation

1. Root Key Generation of Event Certificate

The root key pair of SHECA is generated by devices approved and licensed by the National Password Authority. At present, part of the encryption machines purchased by SHECA are fully compliance with the FIPS140-2 standard. Other encryption machines comply with the requirements of the national password

management regulations and partially comply with the relevant provisions of the FIPS140-2 standard. The event certificate root key is generated by the national secret standard encryption machine and complies with the requirements of FIPS 140-2 in terms of key generation, key operation and key protection. Since FIPS140-2standard is not recognized and supported by the State Commercial Cryptography Administration of China, and the government has strict regulatory requirements for cryptography products, the standards for key generation, key operation and key protection are following requirements of FIPS140-2, while other parts are following the relevant provisions of state encryption management, which are equivalent to the standard of FIPS140-2.

When the key pair is being generated by SHECA, there must be at least three management personnel with authorization for key management and co-operate the hardware encryption machine to generate a key pair. No person alone can generate a root key pair. Any operations related to private key is operated inside the encryption machine and the private key cannot be exported in the form of plain text or cipher text.

2. Sub-CA Key Pair Generation of Event Certificate

The sub-CA key pair of the event certificate refers to the intermediate root key issued by the SHECA event certificate root key controlled by the SHECA self-operated or external CA sub-center that has signed the authority agreement with SHECA. The event certificate sub-CA key also conforms to the FIPS140-2 standard, and the key pair generation requirement is consistent with the SHECA root key. There must be more than 3 authorized key management personnel and operators at the same time.

3. Generation of subscribers signing key pair

The signing key pair of the subscriber certificate is generated by a Hardware Security Module (HSM) that complies with the national key management standard, to ensure that its key generation process is safe and reliable. SHECA has implemented security and confidentiality measures in technology, business processes and management.

4. Generation of Encryption Key Pair of the Subscriber

Encryption key pair is generated by the appropriate state management institutions and transmitted in the safe way.

6.1.2 Private Key Delivery to the Subscribers

The subscriber's signature key pair is generated and maintained by HSM.

6.1.3 Public Key Delivery to Certificate Issuer

Certificate subscribers apply for a certificate by the public key to SHECA, the public key within the requested information obtaining the protection of subscribers private key signature, user's authentication and message integrity, and transferring by the way of safety and reliability.

The reply message of certificate issued successfully is protected by the electronic signatures and message integrity, transferring by the way of safety and reliability.

6.1.4 CA Public Key Delivery to Relying Parties

Public key of SHECA is included in the root CA certificate self-signed by SHECA, through the website http://www.sheca.com to publish. SHECA supports on-line delivery the public-key or the way of downloading from SHECA to deliver the public key for the certificate subscriber and relying party's to query.

In addition, CA also supports the way of built-in browser and the software agreement (such as S/MIME) to

distribute public key to the relying party.

6.1.5 Key Length

The RSA key length of the subscriber certificate of the SHECA event certificate shall be RSA 2048 bits or more, and the key using the SM2 algorithm shall correspond to 256 bits.

The root key length of the SHECA event certificate is RSA 4096 bits and SM2 256.

SHECA will fully comply with the specifications and requirements for the length of key that is issued by national laws and regulations, government authorities and others.

6.1.6 Public Key Parameters Generation and Quality Checking

Public key parameters must be used the generation of encryption equipment approved and permitted by national password authorities, such as encryption machine, encryption card, USB Key, IC card, and follow generation norms and standards of these devices. Of course, SHECA considers that built-in protocols, algorithms for these devices meet already sufficient level of security requirements.

Public key parameters quality is also checked through the encryption equipment approved and permitted by the national password authorities, such as encryption machine, encryption card, USB Key, IC cards. Of course, SHECA considers that built-in protocols, algorithms for these devices meet already sufficient level of security requirements.

6.1.7 Key Usage Purposes

Certificate issued by SHECA is X.509 version 3, contains key usage extension. If the key usage of certificate issued is defined in key usage extension, the certificate subscriber must use the key according to the key usage defined.

All the keys usage must follow this document.

The event certificate subscriber's signing key can be used to provide security services, identity authentication, non-repudiation and information integrity, etc., for signing legally binding electronic documents and electronic transaction data.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Standards and Controls of Cryptographic Module

The cryptographic equipment used by CA institutions is a product approved by the relevant state departments, and its interfaces, protocols, keys and physical security must comply with relevant national regulations.

All of the applied host encryption servers obtained the national commercial password product model certificate. Its main features include:

1. Key generation: It can generate 4096-bit or 2048-bit RSA key, and it can generate more symmetric key (the communication key).The speed of generating the key is fast with the physical noise source as a random number.

2. Key storage: It can store and generate the RSA key and the communication key. Keys are stored in security, and illegal one cannot get the key.

3. Rights management: It can initialize the administrators and operators, and is responsible for the judgment of administrators and operator' s right. Administrator password uses the separating permission key management mechanism.

4. Key backup: On meeting permissions the keys and other important information in the host encryption server encrypted backups to other storage medium and can be imported into the host server with same type according to need.

5. Key generation and output: When generating RSA key pair which can be output encryption devices, the key pair is already encrypted.

6. Physical noise source random number generator chip with hardware generates random numbers.

7. Using the IC card to store PIN and using IC password card to distinguish the administrator and operator identity, the password using the key management mechanism of separate permission.

8. When the client host invokes the host server encryption to invoke business, it is necessary to pass it with shake hands, and it is means that it requires to pass the authentication password, and verifies the compatibility of version number.

9. Key encrypted is stored in electronic storage devices, and is not allow the key output by the way of plain text, appears on disk and memory in clear text.

6.2.2 Private Key Multi-Person Control

1. SHECA uses multi-person control to activate, use, and stop private. (n out of m)

SHECA private key accepts multi-control strategy (means n out of m strategies, m> n, n> = 3).At present SHECA uses five persons to control, at least three or more key control personnel to complete generation and segmentation procedures on common. SHECA system has established appropriate security mechanisms with the technology to limit the generation operation. The key management personnel with authority holds respectively a separate password. All the information related private key, such as controlling the IC card, protecting PIN code etc. should be controlled by different managers.

2. Private Key of subscriber certificate should be controlled by Subscriber

Private Key of subscriber certificate should be controlled and secured by Subscriber, if specific person are assigned to manage private key, the one should be effectively authorized to prevent private keys from being compromised, damaged, lost, or used unauthorized.

Sub-CAs are obligated to inform SHECA in the first place in any of these circumstances.

6.2.3 Private Key Escrow

Protection, management, archiving, backup, escrow etc. of encrypted private key are regulated and decided by the Shanghai Key Management Center (KM). Since the subscriber certificate private key of the event certificate is destroyed after use, the subscriber certificate private key is stored in the hardware security module.

6.2.4 Private Key Backup

In order to ensure ongoing operations, electronic certification service agencies must create backup of the CA private key for disaster recovery. Such keys are stored in encrypted form within hardware cryptographic modules and associated key storage devices Backup of the private key in encrypted form is stored in the hardware cryptographic module, and cryptographic modules used for CA private key storage meet the

requirements of 6.2.1. CA private key is copied to backup for hardware cryptographic module to meet the requirements of 6.2.6.

For subscribers signing certificate, if the private key is stored in the software code module, it is proposed that subscribers backup the private key, the backup private key using the password for access control authorized to prevent unauthorized modification or disclosure.

For the subscriber encryption certificate, since the event certificate private key is destroyed after use, no backup is performed.

6.2.5 Private Key Archival

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

6.2.6 Private Key Transfer into or from a Cryptographic Module

SHECA private key backup is run strictly in accordance with procedure and strategies specified by SHECA, in addition, any imported and exported operations not to be allowed. When CA key pair is backed up to another hardware cryptographic module, by the way of the encrypted form to transmit between the modules, and made a authentication before the transmitting to prevent the CA private key from being lost, stolen, modified, disclosure non-authorized, used unauthorized.

SHECA does not provide subscriber for the way that private key derived from the hardware cryptographic module and does not allow this operation.

6.2.7 Private Key Storage on Cryptographic Module

Private keys held on hardware cryptographic modules shall be stored in encrypted form which is approved and permitted by the national encryption department, and all the private key stored in the cryptographic modules are stored in the form of cipher text.

The private key of the subscriber certificate is invalidated once it is signed.

6.2.8 Method of Activating Private Key

The private key can only be activated after password authentication by the subscriber. SHECA’ s private key is stored in a hardware encryption module, the activation data is parted in accordance with 6.2.2. It must take at least three authorization from the authorized management personnel to activate the private key of SHECA. Any unauthorized person must not be allowed to access, use or activate the private key.

6.2.9 Method of Deactivating Private Key

Once the private key is activated, unless the state is removed, the private key is always active. In the use of some private key, private key is activated each time, only for one operation, if it needs for a second, it must be activated again.

SHECA removed the way of the private key active statement, including exit, power off, remove token / key and automatic freeze. Any unauthorized person must not make relevant operations.

6.2.10 Method of Destroying Private Key

SHECA private key is no longer used, after the public key corresponding to private key is expired or revoked, there are no residuals remains in the encryption device. Meanwhile, all the PIN code, IC card, dynamic tokens for activating private key also must be destroyed or recovered. Archival operations for private key follows the provisions of this document to deal with.

The event certificate subscriber private key is destroyed after once signed.

6.2.11 Cryptographic Module Rating

SHECA uses the products approved and permitted by the national encryption department, and accepts various standards, specifications, assessment, evaluation certification and other requirements published by the national encryption department. SHECA selects the module according to product performance, efficiency, suppliers' qualifications and other aspects.

6.2.12 Transportation of keys

Not applicable.

6.2.13 Transmission of keys

Not applicable.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

The public key in the subscriber certificate includes the public key in the signed certificate, which is periodically archived by the CA.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The validity period of the event certificate key pair is different from the validity period of the certificate. The validity period of the private key is from the issuance of the certificate to the first use of the certificate for digital signature. The validity period of the public key is generally the same as the validity period of the certificate.

The certificate operation period is the same as the validity period included in the certificate. For subscriber certificates, the validity period is no longer than 3 years. For CA certificates, the maximum validity period is no more than 30 years.

Type	Key Pair Usage Period	Certificate Validation Period
Root Certificate(issued before 2018)	30 years	30 years
Root Certificate(issued on or after 2018)	25 years	25 years
Subordinate CA Certificate	25 years	25 years
Subscribe Certificate	Private key: destroyed after usage Public key: 3 years	3 years
Time-stamping Certificate	15 months	135 months

OCSP Certificate	12 months	12 months

6.4 Activation Data

6.4.1 Generation and Installation of Activation Data

Activation data of CA private key must follow the requirements of the key activation data segmentation and key management methods to make a strict production, distribution and usage.

6.4.2 Protection of Activation Data

For the activation data of CA private key, must be segmented according to reliable way to administer by different people, and administer must meet the requirements of segmentation.

6.4.3 Other Aspects of Activation Data

When the activation data of the private key is not needed, it should be destroyed and protected from theft, leakage or unauthorized use in the process. The result of the destruction is that some or all of the activation data cannot be obtained directly or indirectly through the residual information or media. For example, a sheet with a password recorded must be shredded.

6.5 Security Controls of Computer

6.5.1 Specific Computer Security Technical Requirements

Information security management of SHECA certification system agrees "Certificate Authentication System Encryption Security Technical Specifications" published by State Encryption Administration, "Electronic Authentication Service Management Approach" published by Ministry of Industry and Information Technology, standards of information security in ISO17799 and security standards of other relevant information. SHECA draws up comprehensive and perfect security management strategies and standard, has implementation, review and record within operations.

The main security technologies and control measures include:

- Identification and authentication management.
- Access rights control of resources and information.
- Security audit and log.
- Material backup and preservation for safeguard.
- Decentralization of personnel's responsibilities, classification for the role of the CA job to establish secure distributed and contained mechanisms.
- Internal operation control procedures.
- Recovery mechanism of disaster backup.
- Personal computer security management.
- Encryption mechanism of Information transmission.

Through strict security controls to ensure that the system of CA software and data files is safe and reliable without unauthorized access. In addition, the certification authorities should only allow necessary personnel with work requirements to access the certificate server, and the general application user has not account in

the certificate server. Core system must be separated physically with other systems and the production system separated with other system for logic isolation.

6.5.2 Computer Security Rating

SHECA certification business systems pass the relative evaluation, review and certification of the

State Cryptography Administration, China National Information Security Evaluation Center, the Shanghai Information Security Evaluation Center and other departments.

6.6 Technical Controls of Life Cycle

6.6.1 Development Controls of System

SHECA development control includes credible personnel management, development environment security management, product design and development assessment, the use of reliable development tools, production systems designed to meet the requirements of redundancy, fault tolerance and modularity. Software design and development process follow the following principles:

Verification and review of third-party

The security risk analysis and reliability design

Meanwhile, the software development specifications developed by SHECA refers to national relevant standards, implements strictly relevant planning and development control in the implementation.

6.6.2 Controls of Security Management

Information security management of SHECA authentication system follows strictly the relevant operation management specification of the Ministry of Industry and Information Technology, the State Encryption Administration and other departments and SHECA security management strategy to operate.

The usage of SHECA authentication system is under strict controls, and all the systems may use through rigorous testing and verifying. Any modifications and upgrades will be recorded for reference and make a version control, functional test and record. SHECA also carries out regular and irregular inspection and test for certification systems.

SHECA accepts the strict management system to control and monitor system configuration to prevent unauthorized modification.

Hardware devices are safety checked before from procurement to on-line to identify whether the device is compromised and the existence of security holes. The procurement and installation of encryption equipment is in a more strict security control mechanism to carry out inspection, installation and acceptance.

After all the hardware and software equipment of SHECA authentication systems are upgraded, SHECA must confirm whether the information for affecting authenticate business security is in waste equipment during the process.

6.6.3 Security Control of Lifetime

No stipulation.

6.7 Security Controls of Network

SHECA authentication system accepts the protection of multi-level firewall and network control systems and implies perfect access control technology.

Authentication system only opens the relevant operation functions with the certificate application, checking the certificate to operate by network for users.

In order to ensure network security, SHECA authentication system installs firewall, intrusion detection, security auditing, virus protection system, and update the version of firewall, intrusion detection, security audits, virus protection system, as much as possible to reduce the risk from the network.

6.8 Time-Stamping

All kinds of system log and operations log of authentication system should contain a corresponding time record. The time record does not need to accept the technology of digital time-stamping based on password encryption.

7. Certificates, Certificate Revocation Lists, and Online Certificate Status Protocol

7.1 Certificates

The SHECA certificate detailed format meets the international standards and follows the ITU-T X.509 V3 (1997): information technology-- open systems interconnection--the directory: authentication framework (June 1997) standard and RFC 5280: Internet X.509 public key infrastructure certificate and CRL structure (May 2008).

7.1.1 Version

Certificate issued by SHECA is in line with X.509 V3 certificate format. The version information is stored in the attribute column of certificate version.

7.1.2 Certificate Extensions

In addition to the certificate standard items and standard extensions, SHECA also uses private extensions defined by SHECA itself.

- Key Usage

Key is used for electronic signatures, non-repudiation, key encryption, data encryption, key agreement, certificate signature verification, CRL signature validation, only encryption and only decryption.

	Event Certificate (Subscribe Certificate)	CA Certificate
0 digitalSignature	√	√
1 nonRepudiation	×	×
2 keyEncipherment	×	×
3 dataEncipherment	×	×
4 keyAgreement	×	×
5 keyCertSign	×	√
6 cRLSign	×	√

7 encipherOnly	×	×
8 decipherOnly	×	×

- Certificate policy

Certificate policy issued by SHECA is in line with the X.509 certificate format, which is stored in the attribute column of certificate policy.

- Basic restrictions

Basic restriction is used to identify the certificate holder's identity, such as final users.

- Extended Key Usage

The event certificate should be configured with the following extended key usage:

	Event Certificate (Subscribe Certificate)
Document signing (1.3.6.1.4.1.311.10.3.12)	√
Adobe PDF signing (1.2.840.113583.1.1.5)	√

- CRL Distribution Points

The extension of CRL distribution point contains a URL which can obtain CRL and is used to verify the certificate status.

- Serial number

The serial number in all the certificates issued by SHECA is random.

- Private extensions

Event certificates support the following private extensions:

Signature extension: Signature Extension, should contain the contents of the signature related evidence, such as sound, image, and so on.

7.1.3 Algorithm Object Identifiers

The cryptographic algorithm identifiers of certificates issued by SHECA include sha256RSA or SM3.

Algorithm object identifier used by SHECA is in accordance with ISO object identifier (OID) management standards. For example:

1. Signing Algorithm

- SHA256withRSAEncryption OBJECT IDENTIFIER : {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)}
- SM3withSM2Encryption OBJECT IDENTIFIER : {iso(1) member-body(2) cn(156) ccstc(10197) sm-scheme(1) sm3WithSM2Encryption(501)}

2. Digest Algorithm

- sha256 OBJECT IDENTIFIER : {joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) hashAlgs(2) sha256(1)}

- sm3 OBJECT IDENTIFIER：{iso(1) member-body(2) cn(156) ccstc (10197) sm-scheme(1) sm3(401)}

3. Asymmetric Algorithm

- RSAEncryption OBJECT IDENTIFIER : {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) rsaEncryption(1)}
- SM2Encryption OBJECT IDENTIFIER : {iso(1) member-body(2) cn(156) ccstc(10197) sm-scheme(1) sm2Encryption(301)}

4. Symmetric algorithms

This document recommends the use of the symmetric algorithm approved by the state cryptography administration department.

7.1.4 Name Forms

The certificates are issued by SHECA, whose format and content of name form meets the X.501 distinguished name format.

The X.500 DN of the subject is the unique name of the X.500 directory under the C=CN namespace, and the encoding of each attribute uses UTF8String.

The subject's X.500 DN supports multiple levels of O and OU in the following format:

C=CN;

O=××;

OU= ××;

CN=××;

7.1.4.1 C (Country) should be the country where the certificate is located, optional

7.1.4.2 O (Organization) shall be the full name of the name of the province, autonomous region or municipality where the certificate entity or the entity to which the certificate belongs, optional

7.1.4.3 OU (Organization Unit) should be the full name of the name of the certificate entity or the unit to which the certificate body belongs.

7.1.4.4 CN (Common Name) shall be the name of the subject of the certificate.

7.1.5 Name Constraints

The certificate is issued by SHECA, whose identifier name cannot be anonymous or pseudo-name, must have a definite name.

7.1.6 Certificate Policy Object Identifier

The certificate is issued by SHECA in accordance with the X.509 standard, whose policy object identifier is stored in the relevant topic of certificate policy. Please refer to Section 1.2 in this document.

7.1.7 The Usage of Policy Constraints Extensions

No stipulation.

7.1.8 The Syntax and Semantics of Policy Qualifiers

No stipulation.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2 Certificate Revocation List

The event certificate does not issue a CRL, and all the subscriber certificate private keys are destroyed after being signed; the ARL is issued only for the intermediate root certificate (sub-CA).

7.2.1 Version Number

SHECA currently issues ARL of X.509 V2 version, the version number was stored in the columns of ARL version format.

7.2.2 CRL and CRL Entry Extensions

No stipulation.

7.2.3 Download CRL

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

7.3 Online Certificate Status Protocol

SHECA provides users OCSP (Online Certificate Status Inquiry Service), and it is convenience for the certificate user to query certificate status information in time.

7.3.1 Version number

RFC2560 defines the OCSP V1.

7.3.2 OCSP Extensions

No stipulation.

7.3.3 The Request and Response of OCSP

An OCSP request contains the following data:

- Protocol Version.
- Service Request.
- Target certificate identifier.
- An optional extension may be handled by OCSP responder.

After receiving a request, OCSP server response to the following tests:

- Information correctly formatted.
- The response server is configured to provide the requested services.
- The request contains the information needed by response server. If any pre-conditions are not met, the OCSP server will generate an error message. Otherwise, it returns a determinate response.

All determinate response is encrypted digital signature by SHECA certificate issuer. The main response status includes that the certificate is valid, revoked, and unknown. The response message consists of the

following components:

- Reply syntax version.
- Response server name.
- Reply to the request client certificate.
- Optional extensions.
- Signature Algorithm object identifiers.
- The signature after replying message hash.

If an error occurs, OCSP server will return an error message, which doesn't contain certificate key signature issued by SHECA. Error messages include:

- Malformed Request.
- Internal Error.
- Try later.
- Signature required.
- Unauthorized.

8. CA Compliance Audit and Other Assessments

8.1 Frequency and Circumstance of the Assessment

The audit is to check and confirm whether CA conducts business in accordance with this document and its security policy, and finds the risks which may exists. According to the needs of the work, the audit assessment is organized regularly.

8.2 The Qualifications of the Assessor

The internal auditor is composed of internal personnel of CA, and the qualification of the external auditor is determined by a third party.

8.3 Assessor's Relationship to Assessed Entity

Assessor and Assessed Entity are independent, there is no business, financial transactions, or any other interest could affect the objectivity of the assessment.

8.4 Assessment Content

The assessment content include: human resource, engine room physical security, security operations management, key security and operational services, customer service and so on.

8.5 Actions Taken as a Result of Deficiency

For the deficiencies found in the audit, CA will prepare a solution based on the contents of the audit report and clarify the actions taken. CA will quickly resolve the issues in accordance with international practices and relevant laws and regulations.

8.6 Communications and Release of Results

CA generally do not publish the results of the assessment unless the law explicitly required.

For CA related parties, CA will release the evaluation results in accordance with the signed agreement.

9. Other Business and Legal Matters

9.1 Fees

SHECA charges subscribers for certificate. The subscribers have the obligation to pay SHECA under prices SHECA published or specified in agreement signed by SHECA.

The price of the certificate and related services will be published on the website http://www.sheca.com. Published price will effect in accordance with SHECA specified time, if there isn't specified effective time, it will be effect after seven days from the date of price publication. SHECA can also notify subscribers the change of prices in other ways. If the price is not published, the price agreed with the subscriber shall prevail.

If the price specified in SHECA agreement is different from the one published, the agreement price prevail.

9.1.1 Certificate Issuance and Renewal Fees

The fees of SHECA issuing certificates are published in the website http://www.sheca.com for user to query.

The announcement price is approved by the Shanghai Price Bureau.

If the price specified in SHECA agreement is different from the one published, the agreement price prevail.

9.1.2 Certificate Inquire Fees

At present SHECA doesn't charge for certificate inquiring. Unless the user asks for special demand, which need SHECA pays extra charge, and SHECA will charge to negotiate with users.

If charging policy of the certificate query has any change, SHECA will promptly posts on the website http://www.sheca.com.

9.1.3 Revocation or Status Information Access Fees

SHECA currently does not charge any fees for certificate status inquiry. Once charging policy changes, SHECA will promptly post this change on website http://www.sheca.com.

If the specified price signed in SHECA agreement is different from the price published, the agreement price prevails.

9.1.4 Fees for Other Services

1. When the user requests to SHECA for CPS or other paper related documents, SHECA needs to charge fee for postage and handling.

2. If SHECA provides these services of the certificate recovery, key escrow, signature key backup and recovery services, then SHECA will release related costs in time for user to query. If the specified price signed in SHECA agreement is different from the price published, then the agreement price prevail.

3. Other services cost that SHECA will or may provide will be released.

9.1.5 Refund Policy

Fees charged subscribers by SHECA, except the certificate application fee can be refunded because of

specific reasons, SHECA does not refund any fees.

In the process of the certificate operation and the certificate issued, SHECA complies with strict operating procedures and policies. If SHECA violates its responsibilities under this document or other material obligations, subscribers can request SHECA to revoke certificates and refund. After SHECA revokes subscribers certificate, SHECA will full refund immediately to subscribers that apply for the certificate. Subscribers need to fill out a refund application form and submit to SHECA and its authorized service agencies to request a refund.

Refund policy does not limit users to obtain other reparation.

After accomplishing refund, SHECA shall investigate its legal responsibility, if subscriber continues to use the certificate.

9.1.6 Capacity to Pay

Certificate services agencies authorized by SHECA should have financial ability to maintain its operations and fulfill its responsibilities, and it should afford to subscribers, relying parties who caused risks.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

SHECA shall determine the insurance policy according to business development, which includes but is not limited:

1. The fire of building and hardware facilities and other accident insurance.

2. Certificate Liability Insurance, the insurance coverage all subscriber’ s certificate issued by SHECA according to this document.

At present, SHECA cannot provide third-party insurance.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty for Terminal Entities

Currently, SHECA can't provide third-party insurance. SHECA will release insurance policy promptly on its website http://www.sheca.com.

Once certificate subscriber accepts SHECA certificate, or accepts certificate services by accomplishing agreement, which means that the subscriber has accepted the requirements and constraints of SHECA about insurance and warranty.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

1. Confidential information includes the agreement, letters and business agreement etc. between SHECA and its authorized certificate service authority, SHECA and subscriber, SHECA and other participants offering certificate services, SHECA and its correlative entities. Unless laws has clear provisions and SHECA offers explicitly written permission, generally confidential information is not allowed to be published without the other’ s permission.

2. The private key corresponding to subscriber holder public key is confidential, and certificate subscriber keeps the private key properly complying with the provisions of this document and could not publish it to any third-party which are not authorized. If certificate subscriber discloses the private key, all responsibilities shall be borne by subscriber.

3. Confidential information contains auditing report, audit results of SHECA or its relevant entities and other related information, and confidential information could not be disclosed to any one, except for the authorized and trusted personnel. These information could not be used in other functions but audit or laws and regulations.

4. Under the circumstance where the information related with SHECA certification system operation has been designated, and the information could only be offered to the personnel authorized by SHECA, but the authorization does not mean the information is open to public. For SHECA, all information involved in system operation shall be within the scope of confidentiality.

5. Unless the law provides explicitly, SHECA has no obligations to, and shall not publish or disclose any information excluding the information contained in subscriber' s certificate; also, when SHECA signs agreement with its authorized certification authority, or other relevant entities, above all shall be regarded as the requirements to meet.

9.3.2 Information not Within the Scope of Confidential Information

1. The application process, application procedure, application operation and other information related with certificate could be opened. And SHECA could utilize the information including the above information transmitted to the third party to handle application business.

2. Non-confidential information includes relevant subscriber information involved in certificate. The subscriber information involved in certificate could be opened.

3. Certificate and the public key contained in certificate are afforded for users to publish, check and verify.

4. The information of certification revocation is open to public, and SHECA shall publish the information on directory server.

5. The non-confidential information above could not be used by any unauthorized third-party, and SHECA and information holder shall reserve relevant rights of the information.

9.3.3 Responsibility to Protect Confidential Information

SHECA, any subscriber, relevant entities and parties involved in certification business, shall have the obligations to assume appropriate responsibility of keeping confidential information in accordance with this document.

When facing with any requirements of laws and regulations or any demands for undergoing legal process of court and other agencies, SHECA must review confidential information in this document, and could publish the relevant confidential information to law-enforcing department according to requirements of laws, regulations, or court judgments. SHECA shall not assume any responsibility. The reveal shall not be regarded as a breach of confidential requirement and obligations.

When confidential-information holder requires SHECA to publish or reveal all his/her/its own confidential information due to some causes, SHECA shall satisfy his/her/its requirements; Also, SHECA shall require the holder' s application and authorization in writing to express his/her/its own will of publishing or revealing.

If compensatory obligations shall be involved in the behavior of revealing confidential information, SHECA shall not assume any damage related with it or caused by the publishing of confidential information. The confidential-information holder shall assume compensatory responsibilities related with it or caused by the opening confidential information.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

SHECA respects for all users and their privacy, if there is an announcement associated with this explicit privacy protection laws (such as the Personal Information Protection Law), it will automatically be referenced in this document and its privacy protection will become a fundamental basis to perform.

Anyone who choose to use any services of SHECA, has agreed to accept SHECA about the privacy statement.

9.4.2 Information Treated as Private

As SHECA manages and uses relevant information offered by subscriber, in addition to the information in the certificate, the basic information and identification information shall be considered as privacy, and the information shall not be published without subscriber’ s agreement or the legal requirements of laws and regulations and other agencies.

9.4.3 Information Not Deemed Private

All information made public in a certificate held by subscriber and the status information of the certificate etc., is deemed not private, and shall not be regarded as privacy information.

9.4.4 Responsibility to Protect Private Information

SHECA, any subscriber, relevant entities and the participants involved in certification business, shall have the obligations to assume corresponding responsibilities of protecting privacy information according to the provisions of this CPS.

At the request of laws and regulations or in any court and the public power sector through legal procedures or the owner or the information written authorization, SHECA can release to specific objects about the relevant privacy information. SHECA do not assume any responsibility, and such disclosure cannot be considered as a violation of privacy obligations. If this privacy disclosure leads to any loss, SHECA should not bear any responsibility.

9.4.5 Notice and Consent to Use Private Information

Any subscriber information SHECA obtaining within the scope of certification business can only be used for identifying, managing and serving subscribers. As using the information, no matter the privacy is involved or not, SHECA has no obligations to notify subscribers, and doesn't get subscriber consent.

Under any requirements of laws and regulations, and demands for undergoing the legal process of other agencies, or under the circumstance where private information holder submits the written authorization to certain object for publishing the information, SHECA has no obligations to notify subscriber, and to obtain the consent from the subscriber.

If certification authority and registration authority shall apply user’ s private information to other purposes beyond the functions agreed between two sides, CA and RA shall notify subscriber to obtain his/her/its agreement and authorization, and the agreement and authorization shall be archived with the form (such as

fax, letter, e-mail etc.).

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

SHECA shall be entitled to disclose Confidential/Private Information if, in good faith, SHECA believes that:

- Submitting the application through the legal process required by relevant agencies pursuant to the provisions of laws and regulations.
- Court and other agencies handle the legal application submitted because of the dispute of using certificate.
- The formal application of arbitration agency with legal jurisdiction.
- Certificate subscriber authorization in writing.

9.4.7 Other Information Disclosure Circumstances

If certificate subscriber shall authorize SHECA to offer the private information to certain object in writing, SHECA could afford the information to the object designated by subscriber. Not written authorized by the subscriber himself, SHECA will reject any disclosure request of third parties.

In addition to the legitimate request of government regulations and the relevant departments, and all written authorization information, or other than SHECA legitimate purposes, SHECA currently doesn't exist any other private information disclosure circumstances.

9.5 Intellectual Property Rights

1. The statement of SHECA owning the intellectual property rights.

SHECA holds and reserves all software offered by SHECA, and all system, intellectual property rights including ownership, name right, interest-sharing rights etc. SHECA shall determine certificate service software system used by entities related with SHECA, to assure the compatibility and intercommunication.

According to the provisions of this document, all copyright, trademark and other intellectual property rights involved in all certificates and software, system, documents offered by SHECA belongs to SHECA, these intellectual property rights including all relevant documents, CP, CPS, standard document and user manual and so on. Relevant entities within SHECA certification system could use interrelated documents and manuals, and have the responsibilities and obligations to make some suggestions of amendment, after obtaining the agreement from SHECA.

The intellectual property rights of key which was generated by subscriber belongs to the subscriber, but the public key becomes certificate through the issuance of SHECA, that is to say, SHECA owns the intellectual property rights of the certificate, and shall only provide the right to use for certificate subscriber and relying party.

Without the written agreement of SHECA, users could not use or accept any names, trademark, transaction form or its confused name, trademark, form of transaction or business title.

2. The statement of SHECA using other intellectual property rights

The software and hardware equipment, supporting facility and relevant operation manuals used by SHECA in the certification business system, intellectual property rights belong to related suppliers, SHECA ensure that it is legal to own corresponding rights, and SHECA shall not infringe the third party rights on purpose absolutely.

SHECA respects the registered trademark stored in "DN" of certificate, but the ownership of registered

trademark is not assured. If the Certificate subscriber' s registered trademark has been occupied by the former applicant, disputes settlement resulted from registered trademark and intellectual property rights is not in the SHECA responsibility.

9.6 Representations and Warranties

Unless SHECA makes special agreement in the agreement, if the provisions of this document conflict with the relevant provisions of other SHECA developed, the user must accept the constraints of the document. When the signing agreement is only binding both sides between SHECA and other parties, including subscribers, if the agreement is not agreed upon the content, then both sides should implement the provisions of this document. If the agreement is different from the provisions of the document, then the two sides should implement the agreement.

9.6.1 CA Representations and Warranties

1. SHECA warrants that

- Create Certificate Practice Statement (CPS) and other necessary specifications institutional system, for certification services.
- Provide infrastructure and certification services and comply with the provisions of this document within related provisions of this document.
- SHECA ensure that the private key will be safely stored and protected, the establishment and implementation of SHECA security mechanisms is in line with national policy.
- And activities related with certification business are in line with laws, regulations and department requirements.
- The relationship between SHECA and subscriber as well as the relationship between the subscriber and relying party is not the relationship between the agent and the principals. Certificate subscriber and relying party haven't the right to let SHECA assume fiduciary responsibilities with the methods of contract form or other ways. SHECA cannot express, implied or otherwise, contrary to the provisions of the above statements.

2. SHECA warrants to subscribers

Unless otherwise provided in this document or otherwise agreed between the issuing authority and subscribers, SHECA warrants to subscribers named in the certificate:

- Without misrepresentation that issuing authority knows or deriving from the issuing agency in the certificate.
- When generating the certificate, certification agencies will not lead to data conversion errors, it means they will not cause that certification agencies receive inconsistent information in the certificate because the issuing agency errors.
- Certification agencies issue certificates to subscribers, which is in line with all the substantive requirements of this document.
- The issuing agencies will inform subscribers any events, which will fundamentally affect the validity and reliability of the certificate.

These statements are only to guarantee the subscribers interests, and not for the benefit of any other party or other parties enforcing. If the issuing authority's behavior meet the legal and relevant provisions of the

document, which shall be deemed that the issuing agency make a reasonable effort as described above.

3. The issuing authority warrants to the relying party

The issuing authority warrants to the relying parties who trust the signature (the signature can be verified by the public key contained in the certificate) reasonably in accordance with this document:

- In addition to unauthenticated subscriber information, all the information in certificate or certificate merger reference to is accurate.
- The issuing authority is in full compliance with the provisions of the CPS to issue certificate.

4. SHECA warrants about the publication

By releasing certificate in public, issuing authorities prove to the relying party of SHECA repository and reasonably depending on certificate information: the issuing agency has issued subscriber a certificate, and subscriber has accepted the certificate in accordance with the provisions of this document.

9.6.2 RA Representations and Warranties

After obtaining SHECA authorization according to the procedures of authorization, RA and external authorized organization (sub-CA) warrant that:

- Follow the license agreement of this document and SHECA and other specifications and procedures published by SHECA, receive and process the applicant's certificate service requests, and manage all subordinate certification services agencies based on authorization including RAT, etc.
- RA and sub-CA must follow the norms, systems operation and management requirements created by SHECA. According to specifications published by the SHECA or in this document, RA and sub-CA have the right to decide whether to provide appropriate services for applicants.
- In accordance with SHECA requirements and specifications to determine the setting up mode, management and audit methods of subordinate certificate service institution, the determination of these methods must be published with written documents, which covers and shall not conflict, contradict or inconsistent with relevant provisions published by SHECA.
- According to the provisions of this document to ensure operating system in the security physical environment, and have the appropriate safety management and quarantine measures. Sub-CA must ensure that CA system, key management center and engine room meet the requirements of the relevant sections of this document. RA must be able to provide certificate services and backup data, and in accordance with SHECA requirements to ensure that information transfer between the subordinate services agencies is safe. RA promises to imply strictly the obligation of providing privacy security to users, and is willing to bear the legal responsibility therefore.
- Accept that SHECA manages RA and sub-CA under this document and licensing agreements, including the qualification standards and service performance review
- Recognize SHECA has the final discretion service to applicants for all certificates service requests.
- Shall not reject any statement, change, update, upgrade from SHECA, including but not limited to strategy, standards and modification and deletion of certification service.
- Provide the necessary technical advice for subscribers to protect subscribers to successfully apply for and use certificates.

9.6.3 Other Related Services Agency Representations and

Warranties

RAT Warrants:

- Provide certification services and its own management, RAT must complies with the relevant provisions of this document and the authorized operation agreement.
- As Certificate Services agencies authorized, accept authority qualification and management assessment.
- Private information will be kept confidentiality, regardless whether this application is approved.
- Comply with all provisions of this document, fulfill the responsibility of identification and services.
- Shall not reject statement, change, update, upgrade from SHECA, including but not limited to modification of strategy, standards and additions and deletions of certification services.
- Provide necessary technical advice to subscribers, enable subscribers to successfully apply for and use certificates.

9.6.4 Subscriber Representations and Warranties

Once subscriber accepting a certificate issued by the issuing authority, from the moment of acceptance until the end of the validation of the certificate, if the subscriber does not notice, then the subscriber is considered reasonably trust all information contained in the certificate and made the following guarantees:

- All statements and information filled in the certificate application form must be complete, accurate, true and correct, and can be examined and verified by SHECA and its authorized service agencies, and subscriber is willing to take legal responsibility for any false, forged information.
- If there is an agent, then both subscriber and the agent take jointly responsibility. Subscriber is responsible for notifying SHECA and its authorized certification service agencies about any false statements or omissions the agent makes.
- The private key signature corresponding to public key contained in the certificate is the subscribers own signature, during the signing, and the certificate is valid and has been accepted by the subscriber (the certificate has not expired, revoked).
- The one unauthorized has never visited the subscriber's private key.
- Subscriber warrants to the issuing authority that all the relevant information contained in the certificate is true. If the subscriber finds some errors in the certificate, but does not notify the issuing authority, then the issuing authority regards subscriber information as true.
- Subscriber only use certificate for the authorized or other lawful purpose in line with the provisions of this document.
- Subscriber ensures that they don't take the business worked by the issuing agency (or similar institutions), such as use the private key in corresponding with public key contained in the certificate to sign any certificates (or certified in any other form of public key) or certificate revocation list, unless the subscriber and the issuing authority have a written agreement.
- Once accepts certificate, it means that subscriber is aware of and accept all the terms and conditions in this document, and are aware of and accept the corresponding subscriber agreement.

- Once accepts certificate, the subscriber should assume the following responsibilities, always maintains control of their private key, uses trustworthy systems, and takes reasonable precautions to prevent the loss, disclosure, alteration, or unauthorized use of the private key.
- Once accepts certificate, it means that subscriber agrees to the following liability and losses resulted from SHECA direct or indirect action: Subscriber (or authorized agent) states falsely or incorrectly the facts. Subscriber fails to disclose key facts, and the intentional or unintentional misstatement or omission of the subscriber caused any trust of SHECA and the relying party of its certificate to deceive; subscriber does not use the necessary and reasonable measures to prevent the private key from compromised, lost, disclosure, alteration, or unauthorized used. If it causes any liability, loss and all costs associated with litigation, the subscriber will pay financial compensation.
- Shall not reject any statement, change, update, upgrade from SHECA, including but not limited to strategy, standards, and modification and deletion of certification services.

9.6.5 Relying Party Representations and Warranties

When the relying party trust any certificates issued by SHECA, it means to ensure:

- Relying party is familiar with the terms of this document, and understands the purpose of the certificates usage.
- Before the relying party trusts certificates issued by SHECA, relying party inspects and audits reasonably, including: checking the latest CRL announced by SHECA, verifying whether the certificate is revoked; checking all the certificates reliability appeared in the certificate trust path; checking the validity of the certificate; and checking other information that could affect the validity of the certificate.
- The relying party is willing to compensate SHECA for the losses caused and bear the resulting loss of self or others, due to negligence or otherwise violating the terms of a reasonable inspection.
- The trust behavior to certificates indicates that relying party has accepted all the provisions of this CPS, particularly the disclaimer, rejection, and the terms of the limiting liability.
- The relying party shall not reject any statement, change, update, upgrade published from SHECA, including but not limited to modification of strategy, additions and deletions of certification services.

9.6.6 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 document.
- 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 this document 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 document, 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 this document and SHECA.

9.9 Indemnities

9.9.1 The Scope of Compensation

Compensation generated in the certification activities based on the provisions of this document, unless it is otherwise prescribed by any law or regulation.

1. Indemnification by SHECA

- When issuing the certificate, if not in accordance with the provisions of this document for processing or in violation the requirement of laws and regulations causing the certificate subscriber losses, SHECA should bear the liability.
- Because the operator is malicious, willful or negligent, who is not in accordance with the provisions of this CPS to certificate request of the issuance and revocation resulting in the loss of the certificate subscriber, SHECA should compensate the loss of subscribers.
- Because of SHECA root key problems, resulting in subscriber certificate problems, SHECA should compensate related losses.
- Certificate subscribers or others who have the right to request for the certificate revocation, during the period that SHECA publishing the certificate revocation information, if the certificate is used for illegal transactions or arising from transactions disputes, once SHECA conducts relevant operation in accordance with this document, SHECA will not assume any liability for damages.
- The retroactive expiration date of subscriber compensation is operated in accordance with relevant laws and regulations.

2. Indemnification by register authorities (including RAT)

- If the register authorities and their operators do not take good care of subscriber's registration and authentication-related private information, causing subscriber information leakage, fraud, tampering with or resulting in any loss, the register authorities shall bear liability for damages.
- Because of the operator intentionally malicious or negligent and doesn't transact certificate registration service in accordance with the provisions of this document, or violation of laws and regulations that causing subscribers loss, register authorities should compensate the users direct loss, and other collateral damage and the correlation compensation.
- System or software errors caused because of registry, if register authorities haven't sent subscriber certificate request, revocation, and renewal requests information to SHECA within this document specified time, which led to the loss of subscribers or relying parties, register authorities should pay all liability for damages.
- The compensation retroactive expiration date is operated in accordance with relevant laws and regulations.

3. Indemnification by subscribers

- When subscribers apply for registration certificate, due to deliberate, negligent or malicious provide false information, leading to SHECA and its authorized service providers or third party suffered damage, the subscriber should compensate for all damage liability.
- Subscribers private key leakage, loss, knowing the private key has been leaked, lost caused due to intentionally or negligently don't tell SHECA and its authorized service agencies, and don't give others to use, which causes suffered damage of SHECA and its authorized service agencies, third-party, the subscriber shall bear all liability for damages.
- The behavior of subscribers using the certificate or a relying party trusting certificates, which violating this document and related practices norms, or certificate is used for non-business scope of this document, the subscriber or relying party shall bear all liability for damages.

- When subscribers use or trust certificate, if not in accordance with this document to audit reasonable, resulting in SHECA and its authorized service agencies or a third party suffering damage, subscriber should assume all liability for damages.
- Subscriber or other entity who is entitled to request for certificate revocation, during the period that SHECA publishes the certificate revocation information, if the certificate is used for illegal transactions or arising from transactions disputes, once SHECA conducts relevant operation in accordance with this document, subscriber will assume any liability for damages.
- If there are provisions in the agreement between SHECA and otherwise compensations, subscribers refer to its regulations.

9.9.2 Limit of Compensation

The total liability of SHECA and its authorized issuing authority for all parties (including but not limited to subscribers, the applicant, and recipient or relying party) cannot exceed the cap on the amount of compensation of these certificates as described following:

All total about signature and transaction processing of a particular certificate, SHECA and its authorized certification service authority for any person (or other entity), the aggregate compensation of the specific certificate should be limited to an amount not exceeding the certificate price in the agreement.

The limitation of terms applies to some form of damage, including but not limited to any person or entity (including but not limited to subscribers, the certificate applicant, recipient or relying party) because trust or use the certificate of SHECA issuance, management, use or revocation or certificate is expired due to direct, compensatory, indirect, special, consequential, exemplary or incidental damages.

The terms also apply to other responsibilities, such as contractual liability, tort liability or other form of responsibility. Each certificate limits compensation regardless of signature, transaction processing or other claims related to the compensation number. When compensation limit is exceeded, unless there is a judgment by the law or arbitration rule, the available limits of liability will be assigned to the first party who is the first to claim compensation. SHECA has no responsibility for the payment of higher than compensation limit for each certificate, regardless of the sum of compensation limit higher than the limits of liability how to distribute between the claimants.

9.10 Term and Termination

9.10.1 Term

This document 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.

Since the necessary reasons, SHECA may declare early to end the validity of this document after obtaining the approval of the national authorities.

9.10.2 Termination

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

9.11 Individual Notices a 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 document, 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 Certificate Authority Center 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

SHECA has the right to revise this document. SHECA has the right to publish revision results with the form of revised edition of this document on http://www.sheca.com, or in SHECA repository.

9.12.1 Procedure for Amendment

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

This document must be revised through the approval and verification of SHECA Security Certification Committee - the highest policy management agency of SHECA after Strategy Development Center puts forward the revision report。After the revised CP/CPS shall be published formally, should be submitted to information industry department to record.

9.12.2 Notification Mechanism and Period

SHECA has the right to revise and modify any terminology, conditions and clauses of this document within the proper time, and shall not notify any party in advance.

SHECA publishes the revision results on www.sheca.com and SHECA repository. If modification of this document is placed in SHECA repository (check www.sheca.com), it equals to modify this document. These

modifications shall take place of any conflicting and designated terms in the original version of this document.

All CP/CPS modification in writing to subscribers should be send according to the following rules:

- If the recipient is company or other organization, the message is sent to the address recorded in SHECA and its authorization certificate service agencies.
- If the recipient is personal, the message is sent to the address recorded in application.
- These notifications may be sent by express delivery or registered letter
- SHECA can send the message to subscribers by e-mail or other way, and the e-mail is defined when the subscribers apply for a certificate.

9.12.3 Comment Period

If certificate applicant and subscriber have not decided to revoke the certificate within 7 days after revision was published, they shall be deemed to agree the revision, and all revision and modification shall take effect.

9.12.4 Circumstance under Which CPS Must Be Modified

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

- The encryption technology develops significantly enough to affect the effectiveness of existing CP/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 CP/CPS.

For the revision of the CP/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 an amendment, and if the amendment is not come 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.

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 this document and the law, and find other solutions.

9.14 Governing Law

This document 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 document 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

All participants of electronic certification activities must conform "Electronic Signature Law of People's Republic of China", "Electronic Certification Services Management Measures", "Electronic Certification Service Encryption Management Measures" and other laws and regulations of People's Republic of China.

9.16 General Provisions

9.16.1 Entire Agreement

This document 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 cannot be verbal amended, given up, supplied, modified or ended.

When this document 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 this document.
- The contract shows expressly the relevant parties to replace this document matters, or the provisions of this document are prohibited to be 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

If any clause or application of this document is invalid or unenforceable in any reason or in any scope, the remainder of this document shall remain valid. Relevant parties understand and agree the limitation of liability, warranties or other terms or restrictions exemption or exclusion of damages specified in this document are individual provisions independent of the other terms of the and implementation.

9.16.4 Enforcement

Not applicable.

9.16.5 Force Majeure

In the extent permitted by applicable law, subscriber agreement and CP/CPS 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 this document 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 All property of security information

Unless otherwise agrees, the following - information and data related security is considered to parties'

property, indicated as the following:

- Certificate: Certificate is SHECA's property. Unless those certificates that isn't in any directory or repository without SHECA expressed written permission, the certificate can be a complete non-exclusive, royalty-free reproduction and distribution. On copyright notice, you can consult to SHECA.
- CP/CPS: This document is SHECA private property.
- Distinguished name: distinguished name is owned by all the named entities.
- Private key: Private key is owned by private subscribers (or their representative organizations, agencies or any other entities), regardless of the medium of storage and protection being used.
- Public key: Public key is owned by subscribers (or their representative organizations, agencies or any other entities), regardless of the medium of storage and protection being used.
- SHECA public key: The public key owned by SHECA is SHECA's property, and SHECA is allowed to use these public key.
- SHECA private key: Private key is SHECA's private property, whether partial or whole.