SHECA Certification Practice Statement (CPS)

Version 3.6.5

Effective Date:April 2, 2020

Shanghai Electronic Certification Authority Center Co.,Ltd.

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

Statement

The CPS conforms to the following criteria wholly or partially:

RFC3647: Internet X.509 Public Key Infrastructure – Certificate Policies and Certificate business statement framework

RFC2459:Internet X.509 Public Key Infrastructure – Certificate and CRL property

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

ITU-T X.509 V3 (1997): Information Technology-Open Systems Interconnection – The Directory: 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

The CPS has been submitted to the independent audit institution, which will assess the CPS in accordance with AICPA/ CICA WebTrust for Certification Authority. The CPS meets the requirements states in above standards and is published on the website http://www.sheca.com .

Version Control

Version	Released Date	Issuer
V3.6.5 (Current version)	April 2, 2020	SHECA Security Certification Committee
V3.6.4 (Previous version)	May 29, 2019	SHECA Security Certification Committee
V3.6.3 (Previous version)	Sept 10, 2018	SHECA Security Certification Committee
V3.6.2 (Previous version)	Aug 21, 2018	SHECA Security Certification Committee
V3.6.1 (Previous version)	July 12, 2018	SHECA Security Certification Committee
V3.6 (Previous version)	June 7,2018	SHECA Security Certification Committee
V3.5 (Previous version)	May24,2017	SHECA Security Certification Committee
V3.4.2.3 (Previous version)	May 25,2016	SHECA Security Certification Committee
V3.4.2.2 (Previous version)	Sept 18,2015	SHECA Security Certification Committee
V3.4.2.1 (Previous version)	Sept 1,2014	SHECA Security Certification Committee
V3.4.2 (Previous version)	April 29,2014	SHECA Security Certification Committee
V3.4.1 (Previous version)	April 8,2010	SHECA Security Certification Committee
V3.4 (Previous version)	April 23,2009	SHECA Security Certification Committee
V3.3 (Previous version)	March 26,2009	SHECA Security Certification Committee
V3.2 (Previous version)	March 18,2008	SHECA Security Certification Committee
V3.1 (Previous version)	July 1,2005	SHECA Security Certification Committee

Changes Description

Version	Change Description
9	Information of new corss-signed UCA Global G2 Root SSL certificate validity changed SSL certificate domain validation method changed
9	/v{}ŒE š]}v}(v ÁŒE}š Œš[] š hv]dŒE•šWd Z}}š Zíhv]dŒE•šWd Z}}š Zî D}][/v]À] µ o v KŒP v]Ì]š}v/ vš]šÇ Œš[] š Àd š]}v%ŒE ••
V3.6.3	Added Changes Description
V3.6.2	State the 825 days validity of data, document or validation SSL Certificate renewal process SSL Certificate re-key process Complement some reasons for revocation
V3.6.1	Added Root UCA Global G2; IP Address Verification; Added CAA Record checking requirement Stated 825 days validity of Data Source
V3.6	Modified UniTrust Network Trust Service Hierarchy; Deleted RAB related content Added Object Identifier (OID) Modified certificates maximum validity
V3.5	Revised Certificate Identification Verification process; Data Source Accuracy, added 825 days validity
V3.4.2.3	Administrative update/ clarifications
V3.4.2.2	Modified Fee of Issuance and Renewal
V3.4.2.1	Modified UniTrust Network Trust Service Hierarchy
V3.4.2	Email Verfication Methodology modified to comform with BR Revised Appendix Modified Email Validation Process
V3.4.1	Contact information of SHECA Changed
V3.4	Added English Version; Revised Certificate Identification Verification process; Revised content about Extended Key Usage
V3.3	Added the relationship between CPS and CP; Modified UniTrust Network Trust Service Hierarchy; Added Certificate Usage Limitation; Revised Record Archive Retention Time

V3.2	Added Appendix
V3.1	N.A.

Copyright Notices

Shanghai Electronic Certification Authority Center Co., Ltd. (abbreviated as SHECA) owns the copyright of this document. "SHECA" and its icons involved in this document are all exclusively owned by the Shanghai Electronic Certificate Authority Center Co., Ltd. and they are protected by copyright.

Any other individual and group can accurately and completely repost, paste or publish this document, but the above copyright notices and the main content in the previous paragraph should be marked on a prominent position in the beginning of each copy. Without the written consent of Shanghai Electronic Certification Authority Center Co., Ltd, any individuals and groups shall not in any way, any means (electronic, mechanical, photocopying, recording, etc.) repost, paste or publish the part of the CPS, and are not allowed to make modification to the document and repost.

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 the CPS, please visit our websitehttp://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 CPS.

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 CPS

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

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 a applicant received a certificate means that he/she had accepted the rights and obligations under the CPS, 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. Suggestions

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. General Description..... 12

1.1. Overview..... 12

1.2. Document Name and Identification..... 17

1.3. Electronic Certification Event Participants..... 19

1.4. Certificate Usage..... 23

1.5. Policy Management..... 25

1.6. Definitions and Abbreviations..... 28

2. Publication and Repository Management..... 30

2.1. Publication of Certificate Information..... 30

2.2. The Time and Frequency of Releasing..... 31

2.3. Repository Access Control..... 33

3. Authentication and Identification..... 33

3.1 Naming..... 33

3.2 Initial Identity Validation..... 36

3.3 Identification and Authentication of Re-key Requests..... 44

3.4 Identification and Authentication for Revocation Requests..... 45

3.5 Identification and Authentication of Authorized Service Organization.. 45

4. Operational Requirements of Certification Life Cycle..... 46

4.1 Certification Application..... 46

4.2 Certificate Application Processing..... 56

4.3 Certificate Issuance..... 58

4.4 Certificate Acceptance..... 60

4.5 The Key Pair and Certificate Usage..... 60

4.6 Certificate Renewal.....63

4.7 Certificate Key Renewal..... 65

4.8 Certificate Modification.....67

4.9 Certificate Revocation and Suspension.....69

4.10 Certificate Status Services.....76

4.11 Termination..... 77

4.12 Key Generation, Backup and Recovery.....77

4.13 Certificates and CRL Archiving.....78

5. Facility È Management and Operational Control.....79

5.1 Physical Control.....79

5.2 Procedural Control..... 81

5.3 Personnel Control.....84

5.4 Audit Logging Procedures..... 87

5.5 Record Archive.....89

5.6 Expiration Date of Root Certificate for Electronic Certification Services Agencies.....92

5.7 Key Changeover of Electronic Certification Services Agencies.....92

5.8 Compromise and Disaster Recovery.....92

5.9 CA or RA Termination..... 94

6. Technical Security Controls for Certification System.....95

6.1 Key Pair Generation and Installation..... 95

6.2 Private Key Protection and Cryptographic Module Engineering Controls 97

6.3 Other Aspects of Key Pair Management.....101

6.4 Activation Data..... 103

6.5 Security Controls of Computer..... 104

6.6 Technical Controls of Life Cycle..... 105

6.7 Security Controls of Network..... 106

6.8 Time-Stamping.....106

7. Certificates, Certificate Revocation Lists, and Online Certificate Status Protocol 107

7.1 Certificates..... 107

7.2 Certificate Revocation List.....110

7.3 Online Certificate Status Protocol..... 111

8. Compliance Audit and Other Assessments.....112

8.1 Frequency and Circumstance of the Assessment..... 112

8.2 The Qualifications of the Assessor.....113

8.3 Assessor's Relationship to Assessed Entity.....113

8.4 Assessment Content..... 114

8.5 Actions Taken as a Result of Deficiency.....114

8.6 Communications and Release of Results..... 115

9. Other Business and Legal Matters.....115

9.1 Fees.....115

9.2 Financial Responsibility.....117

9.3 Confidentiality of Business Information..... 117

9.4 Privacy of Personal Information.....119

9.5 Intellectual Property Rights.....120

9.6 Representations and Warranties..... 121

9.7 Disclaimers of Warranties..... 127

9.8 Limitations of Liability..... 128

9.9 Indemnities 128

9.10 Term and Termination..... 131

9.11 Individual Notices an Communications with Participants..... 132

9.12 Amendments..... 132

9.13 Dispute Resolution Provisions..... 134

9.14 Governing Law.....134

9.15 Compliance with Applicable Law.....134

9.16 General Provisions..... 134

9.17 All property of security information..... 135

Appendix.....136

1. Root Certificate..... 136

1.1. Root Certificates In Use..... 136

1.2. Root Certificates Out of Use..... 137

2. Cryptographic Algorithms and Key Strengths..... 138

2.1. Root Certificate..... 138

2.2. Sub-CA certificate.....138

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.

SHECA developed this document -- "SHECA Certification Practice Statement (CPS)" (hereinafter referred to as "the CPS"). The CPS accepts the "UniTrust Network Trust Service Hierarchy Certificate Policies" (referred to as "UniTrust NTSH certificate policies"), elaborates SHECA following the requirements of "UniTrust NTSH certificate policies" ,carries out the digital certificate service processes, controlling, management and supporting activities, and provides a digital certificate application, issuance, renewal, revocation, management and other business processes, methods, standards and norms to follow, and the corresponding services, technical measures, rights and obligations agreement, legal protection and so on.

1.1. Overview

SHECA in strict accordance with legal provisions such as the "Electronic Signature Law of the People's Republic of China" and the requirements of Ministry of Industry and Information Technology and State Cryptography Administration, has recommended, designed, constructed and operated the UniTrust Network Trust Service Hierarchy(abbreviated as UniTrust NTSH). UniTrust NTSH provides reliable digital certificates and related services to customers, constructs the trusted relationship based on all kinds of information interaction and trading activities on Internet, to assure the authenticity, privacy, and integrity of participant’s identity and the non-repudiation of behaviors.

The CPS was edited mainly based on "Certification Practice Statement (Trial)" released by Ministry of Industry and Information Technology and following the "Electronic Signature Law of the People’s Republic of China” "Measures for Administration of Electronic Authentication Services","Measures for Administration of Electronic Authentication Service Password "and other laws and regulations. This document is in line with "UniTrust NTSH Certificate Policies" , implemented and achieved provisions and requirements of the"UniTrust NTSH Certificate policies" ,and is applicable for all the CAs operated and managed by Unitrust hierarchy including the root CA and its sub-CA. All the CA-signed certificates within UniTrust hierarchy includes self-signed root certificates, sub -CA certificates and user certificates, are in accordance with operation and management , and performance of related rights and obligations as provided in this document.

The CPS elaborates the activities of SHECA in issuing and managing digital certificates, together with operating and maintaining certificate service facilities, and provides the norms to be followed in practical work and operation. The CPS elaborates the process of the entire certification business,

supervises its implementation, and provides legal constraints and reminds the parties to produce, use certificates, and validate certificates within the scope in terms of the CPS.

As a documentation providing practical application and operation, the CPS is suitable for SHECA, and the various types of registered institutions, services branches, service points and other institutions authorized by SHECA, all staff of SHECA, all related entities and their employees, certificate subscribers and relying parties. All these subjects must fully understand and implement the provisions of the SHECA CPS and enjoy the corresponding rights and assume the corresponding responsibilities and obligations. SHECA and its authorized service organizations of various kinds make commitments: be pursuant to the provisions of the CPS, issuing a certificate, in the case that the certificate is valid, to ensure that the certificate can be associated an entity with a clear identity uniquely, and its public key can correspond with an entity with a definite identity uniquely.

SHECA conforms to the latest version of CA/Browser Forum Baseline Requirements, guidelines and Minimum Requirements for Code Signing Certificates for the Issuance and Management of Publicly – Trusted Certificates published at www.cabforum.org .In the event that a discrepancy arises between interpretations of this document and Baseline Requirement, the Baseline Requirement, guidelines and Minimum Requirements for Code Signing Certificates shall govern.

The CPS announced the basic position and views of SHECA upon certificate service to the public, any organizations, institutions, groups and individuals related with SHECA must completely understand and accurately interpret its content.

1.1.1 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.

1.2.156.112570.1.0	Policies
1.2.156.112570.1.0.1	UniTrust Network Trust Service Hierarchy Certificate Policies (UNTSHCP)
1.2.156.112570.1.0.2	Certification Practice Statement
1.2.156.112570.1.0.3	EV Certificate Policy
1.2.156.112570.1.0.4	EV Certification Practice Statement
1.2.156.112570.1.1	SSL Server Certificates Policy
1.2.156.112570.1.1.1 2.23.140.1.2.1	Domain Validation SSL Certificates Policy
1.2.156.112570.1.1.2 2.23.140.1.2.2	Organization Validation SSL Certificates Policy
1.2.156.112570.1.1.3 2.23.140.1.1	Extended Validation SSL Certificates Policy
1.2.156.112570.1.2	Object Signing Policy
1.2.156.112570.1.2.1 2.23.140.1.4.1	Code Signing Policy
1.2.156.112570.1.2.2 2.23.140.1.3	Extended Validation Code Signing Policy
1.2.156.112570.1.2.3	Windows Kernel Mode Code Signing Policy
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. Electronic Certification Event Participants

1.3.1 Electronic Certification Service Authority

SHECA was established by law as electronic certification service authority (CA), constructing and operating UNTSH. As a trusted third party, UNTSH has a number of entities issuing the certificates, including the different root CAs and sub-CAs, the issuing entity as CA can also issue the certificates. Root CA can only issue sub-CA certificates, sub-CA can issue end- user certificates or other CA certificates. Under the UNTSH CA issues digital certificates to other types of participants involved in e-government, e-commerce and other online business (hereinafter referred to as subjects or entities, organizations, individuals and any other entities who have a clear identity can become the subject or entity as this CPS claimed), to ensure that the public key can uniquely correspond with the subject's identity.

SHECA has established a perfect operational mechanism of the CA and the tight security control mechanisms, and has generated the independent key pair and self-issued root CA certificate (ROOT CA). SHECA can issue operational sub-CA certificate at the next lower level based on certificate development strategy, certificate application strategy and the related authorization and agreements. SHECA must renews root CA key pair, through the procedures specified by national competent authorities, law and policy etc, after approved by SHECA Security certification Committee. SHECA Security Certification Committee as SHECA digital certificate policy-making body shall decide SHECA root CA and the operational sub-CA Re-Key Pair and switchable strategies and actions.

Every certificate SHECA issued is binding with the public key each entity applying for the certificate. SHECA promises that the certificate issued within the valid period will use the directory server and Certificate Revocation Lists server and it will publish information and status of the certificate that can be disclosed.

Based on business requirements, SHECA builds interconnection with other CAs which is not involved in the SHECA certification system. Interconnection refers to two certification authorities that are of complete independence, and use their CPSs respectively to establish mutual trust so that mutual customers can achieve mutual authentication. When SHECA needs to build interconnection with a CA, it means that the certificate a CA issued has been trusted, SHECA will review CPS, related certificate business documents, commitment and operational procedures. If all

institutions, which are trusting SHECA, are willing to accept the certificates issued by CA who has interconnection with SHECA, they must examine their own practical specification and other related certificate business documents. Interconnection does not mean that SHECA approved or offer other rights for non-SHECA agencies of independence.

1.3.2 Registration Authority

A Registration Authority (RA) 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 CA. SHECA itself is both a CA and a RA, also has authorized a number of external RAs. In addition to establishing the registration process for end-user certificate applicant, RA also manages and serves subordinate agencies, including Registration Authority Terminal (RAT). Each RA can be divided into multiple RATs following the industry, administrative region and other factors to offer services to the end users. RA should follow authorization from the CPS and SHECA to establish the appropriate RAT.

RA has the responsibility to keep customer's data, which could not be allowed to be disclosed to any organization or individual who has nothing to do with certificate application, and to be used for commercial interests. RA must get the authorization from SHECA to operate sub-CA, be engaged in all kinds of certificate services and expand corresponding subordinate service agencies based on authorization. Various government agencies, enterprises, institutions can apply to become a Registration Authority under the architecture of SHECA certification service system.

Especially, the external RAs do not involve SSL certificate and code signing certificate. SHECA would not authorize the external RAs to validate the information which supplied to apply for a SSL/code signing certificate and issue a SSL/code signing certificate.

In accordance with the nature of the applying organization, expectation of certificate development, the site and personnel, SHECA will decide to issue letter of authorization qualified by Security Certification Committee after performing a reasonable auditing assessment for the agency, in order to authorize it as a Registration Authority.

1.3.3 CA RAT

Registration Authority Terminal is abbreviated as RAT.

After examinating SHECA and its authorized organization, SHECA and its authorized organizations may authorize a particular organization or entity as RAT in charge of processing and approving digital certificates applications, revocation and inquiry and other certificate services. Application procedures, handling process and processing requirements must be consistent with the CPS SHECA is implementing and license agreement between SHECA and RAT.RAT is responsible for providing information of certificate services for SHECA CA agency (covering SHECA and Sub CA) or the RA, including the name of the application entity, legal identification which indicates its identity and any legal documentation SHECA requires, contact information (mailing address, e-mail box, telephone) and so on. On the basis of this information, RAT provides certificate application, certificates manufacture, signature key generation, certificate check, certificate revocation, certificate renewal and other authorized services for application entities or

according to the requirements of the application entity, provides any other services and technical supporting SHECA published, which are in line with the CPS. RAT takes legal responsibility relevant to affording certificate services, including but not limited to the CPS and the relevant content set forth in licensing agreements.

Depending on whether the RAT will bear the cost for a certificate applicant, RAT can be divided into advancing-type RAT and non-advancing-type RAT. Unless otherwise stated, RAT usually refers to non-advancing-type RAT.

If RAT meets and achieves the requirements SHECA performs certificate advancing services, and obtains the authorization from SHECA and other authorized agencies, RAT of this type could be called advancing-type RAT.

If a RAT does not bear the cost for the certificate applicant (different from advancing-type RAT), this RAT is called non-advancing-type of RAT.

SHECA will decide to issue letter of authorization qualified by Security Certification Committee according to the nature of application organization, expectation of certificate development, site and personnel and so on, after performing a reasonable auditing assessment for those who apply directly to the SHECA, in order to authorize them as Registration Authorities.

Registration Authority could make decisions upon whether to authorize those who apply to be RAT to Registration Authority, and shall not violate policies and strategies of SHECA.

1.3.4 Certificate Advance Vendor

Certificate Advance Vendor is groups or organizations who are able to bear all certificate service fees for subsidiary and served subscribers or potential subscribers. According to the provisions of CPS, other terms SHECA published, or related laws and policies. Certificate Advance Vendor has the right to ban all or part of certificate services offered to the certificate holder, and whose fees is born by the vendor, including but not limited to cancelling the holders' certificates. Certificate Advance Vendor must pre-book the number of certificates, pre-pay all certificate fees in accordance with the agreement with SHECA and enjoy certain preferential policies based on the provisions of SHECA. Certificate Advance Vendor is required to take all the responsibilities of the authenticity of the certificate holder's identity whose fees were born by the vendor.

1.3.5 Subscribers

Subscriber, namely the certificate holder, is the entity who receive the certificates from SHECA, including individuals, organizations or, infrastructure components such as trusted servers or other devices used to secure communications within an Organization and other subject or entity who has applied for or has owned digital certificate issued by SHECA , and any other objects who have defined identification and hold various certificates issued by SHECA , including any individuals, matters and organizations of entities or non-entity

Subscriber is divided into two types: (a) the pre-paid certificate holder whose certificate fees is paid by Certificate Advance Vendor; or (b) the own-paying certificate holder who bears the certificate fees by himself.

Before applying for certificates, subscribers have been advised to receive appropriate training of

the usage of electronic authentication technology. Subscribers can get documents and learning materials relevant to electronic signatures, certificates, PKI from SHECA, and based on the actual situation, SHECA will provide these documents through the website, training activities, and promotional material. SHECA provide different types of certificates, and certificate subscribers shall decide the certificate he/she/it requires. Subscribers agree that they shall promptly notify the issuing authority in case of compromising the private key security.

1.3.6 Relying Party

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.

SHECA makes a commitment for a relying party that in addition to unverified subscriber's information, all the information in the certificate or in reference to the certificate is accurate. All issuing certificate authorities within the framework of SHECA certification system comply fully with all provisions of SHECA CPS to issue certificates.

Relying party should trust reasonably certificate and related digital signature. If you need extra assurance when you trust digital signature, the relying party will not reasonably trust the digital signature until he/she/it obtains these assurances.

Relying Party of SHECA certificate subscriber enjoy a variety of the corresponding rights that SHECA CPS provides, including certificate protection offered by SHECA as well as the interests involved in the CPS. Except SHECA assures the authenticity of certificates issued by the SHECA, relying party of non-SHECA subscribers trust and related signatures, SHECA shall assume no other obligations and responsibilities.

1.3.7 Certificate Applicant

Certificate Applicant, each entity who is certificate subscriber expecting to be SHECA or its subordinate CA , and, according to the type of certificate they want, they should provide the necessary information specified by CPS of SHECA and complete the application process.

If the certificate applicant cannot provide the required information for SHECA, the application process will be delayed or terminated. That certificate applicant submits a certificate application; means that all certificate applicants has authorized SHECA to conduct investigation of security. All of these investigations must be pursuant to the requirements of laws and regulations such as relevant privacy and data protection, and the applicants agree to assist SHECA or its authorized organizations to adopt the means that the latter deems it is appropriate and consistent with the CPS in order to determine all the facts, environment and other relevant information.

If the certificate application has passed the all necessary procedures of identification specified by Issuing Certificate Authority, SHECA will issue certificate to applicant in accordance with CPS to prove that SHECA has approved the applicant's certificate request. If the applicant fails to pass the identification, SHECA will reject the applicant's certificate application and notify the applicant of the failure, at the same time provide the reasons of failure for the applicant (except prohibited by law). Rejected certificate application could make an application again.

SHECA and its authorized service authorities issue certificates only after the certificate applicant's consent. Once applicant submits the certificate application, despite the fact that he has not accepted the certificate yet, but it is still regarded that the subscriber has agreed to accept the certificate from the issuing authority. Meanwhile the issuing authority could refuse to issue certificates to any entities on the basis of the independent judgment and therefore does not bear any responsibility and obligation for any loss or costs caused by this.

1.3.8 Other Participants

Other entities not mentioned above who can provide certificate services within the entire SHECA and its service system, such as third-party authentication authority SHECA selected, PKI application technology service provider and so on.

1.4. Certificate Usage

1.4.1 Formal Certificate and Testing Certificate

SHECA provides the formal certificate and test certificate in the SHECA certification services system.

Applicants for formal certificate must go through the specified physical identification and procedures of authentication that SHECA required; usually it is valid for one year.

Applicants for test certificate can make an online application; usually it is valid for no more than three months. Test certificate can only be used to test whether it adapts to application system and how well the purpose of the technical could be achieved, and cannot be used for any formal purpose. SHECA don not provide test certificate for SSL certificate in particular.

Whether it is a formal certificate or test certificate, any organization or individual involved in certificate issuance, application, acceptance, operation, management or usage should be familiar with the terms, conditions, requirements, recommendations, rights and interests and so on in the Certificate Policies of SHECA.

1.4.2 Certificate Assurance Level

All subscriber certificates issued by SHECA need to be strictly identified. All application subjects, whether individuals, organizations, equipment, etc., must provide supporting materials to confirm its real existence. While applying for equipment certificates or organization certificate, applicants should provide not only supporting materials but also authorization documents. From level of trust, all subscriber certificates issued by the root CA are in common use, all subscriber certificates could be trusted, no difference in security levels, no specific level of trust. However, different types of certificates, because of the different subject, the corresponding application requirements are also different, so they should be properly applied to appropriate use.

1.4.3 Appropriate Certificate Usage

From the function, certificates issued by SHECA meet the following security needs, unless required, SHECA usually does not achieve the function:

- Identification--to ensure that the identity of the certificate holder to trust services of SHECA is legitimate.
- Verifying the integrity of messages --to ensure whether the information in the transmission process has been tampered, and whether messages sent are completely consistent with ounces received as digital certificates and digital signatures are used.
- Verifying digital signatures-- Validating digital signatures that are the evidence that the two trusted parties conduct a transaction without repudiation. It must be pointed out that for any electronic communications or transactions, non-repudiation should be ruled based on laws and dispute resolution.
- The confidentiality of SHECA certificate.--confidentiality ensures that messages delivered between senders and receipts are confidential and will not disclosed to other parties who are not authorized legally. But SHECA takes no appropriate responsibility for confidential events. For all the damage and loss caused by confidentiality purposes directly or indirectly, SHECA shall not assume responsibilities.

Certificates issued by SHECA are general certificate which are not subject to a limitation for particular purpose and scope, it also can be applied in e-government, e-commerce, social management and other online businesses in order to achieve authentication, electronic signature and other purposes. According to the different type of certificate, the certificate has its appropriate application. For example, individual certificate is used for sending signing and encrypting e-mail, personal online banking business, etc., organization certificate is used for B2B transactions, online tax declaration, equipment certificate is used to identify equipment, encrypt information channel. But there are exceptions because of limitation by laws, regulations and national policies. Certificate applicants, subscribers È relying parties and other subjects could decide the appropriate type of certificate according to actual needs and independent judgment to understand the type of application, the range of application so that they can choose their own way of application . Any usage of certificate beyond the terms of the CPS and the CP will not be protected by CPS, and SHECA will not provide any warranty or assurance for it.

1.4.3.1 The Usage of Identity Certificates

Identity certificate is divided into the identity certificate I, identity certificate II ,used for identify types of organizations, individuals and equipment, and which can be applied to various types of e-government, e-commerce and other society information activities such as various types of online transactions, payment, reporting, management, business, access control and other applications.

Identity Certificate I only uses a key pair for signing, verifying the signature, encrypting and decrypting information.

Identity certificate II owns two key pairs. One is used for signing and verifying signature and the other one is used for encrypting and decrypting information.

1.4.3.2 The Usage of E-mail Certificate

E-mail certificate identifies the user's e-mail address and is mainly used for e-mail digital signature, encryption and non-commercial, government-affair access control , which shall not be used for various types of transactions, payment and other applications requiring explicit authentication.

1.4.3.3 The Usage of Code Signing Certificate

Code signing certificate identifies the source or owner of the software code, which can only be used for various types of digital signature and not be used for various types of transactions, payment, encryption and other applications.

Code signing certificate subscribers must promise not to use code signing certificate for signing malicious software, virus code, software infringement and the hacker software.

1.4.3.4 SSL Certificate Usage

SSL certificate identifies the Web site or Web server which can be used to prove the identity or qualification of site and to provide SSL-encrypted channel, and it must not be used for signing and verifying types of transactions or payment of the signature or verification.

Unless specifically stated in this CPS, SHECA has no responsibility for additional economic compensation of any usage of the certificate.

1.4.4 Prohibited Certificate Usage

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

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

1.5. Policy 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 the Certification Practice Statement (CPS) and appoints a special body - SHECA Security Certification Committee as an agency of policy administration.

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

As a CPS agency ÈSHECA Strategy Development Department is responsible for drafting the CPS È is required to amend the report Èand 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

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 Èrenewal 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 CPS is the digital certificate, including signing certificate and encryption certificate.

1.6.13 Electronic Signature

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

1.6.14 Digital Signature

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

1.6.15 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.

1.6.16 The Relying Party on Electronic Signature

The relying party on electronic signature is the person who engages in the relevant activities which is based on his trust in the electronic certificate or electronic signature.

1.6.17 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.

1.6.18 Public Key (validation data of electronic signature)

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

1.6.19 Subscribers

Subscriber is the entity receiving the certificate from the electronic certification authority, known as certificate holders. In the applications of electronic signature, subscriber is an electronic signatory.

1.6.20 Relying Party

A Relying Party is an individual or entity that acts in reliance of a certificate and/or a digital signature issued by CA. A Relying party may, or may not also be a Subscriber.

1.6.21 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 Directory Services

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

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

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

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

2.2.2 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

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

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

All CRL will be released by the SHECA directory server. SHECA should release Certificate Revocation List (CRL) of a subscriber certificate at least once 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 ensures that various types of certificate revocation lists (CRL) will be issued at least once every 24 hours, 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 ÈNotification 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 anonxhano A

SHECA confirms whether the applicants have the E-mail by sending mail, and issues their certificates on basis of e-mail replying. However, this process does not mean that SHECA can deem that the applicant is really legal ownership of the E-mail. SHECA has no obligation and doesn't need to confirm E-mail belonging to the applicant. SHECA ensures that applicant's information is applied for E-mail certificate applications and whether information is correspondence with the E-mail Certificates information SHECA will not resolve, because of E-mail ownership causing dispute. SHECA will provide help in accordance with the requirements of the relevant departments, but this is not an obligation of commitment. Organization E-mail certificate, required to submit the same information as Organization Identity certificate:

(C) Department certificate--- according to different needs of each unit, awarded to a department for using and used to prove the identity of the digital certificate of the department, which is called the department certificate.

Applying for department certificate is required to submit the same information as Organization Identity certificate.

(D) Position certificate--- The position certificate is used to identify holder's identity when in the network communication, containing basic information, the public key and SHECA signatures of the certificate holder, which can be stored in various media, one of the unit certificates.

Applying for position certificate is required to submit same information as Organization Identity certificate.

3. SSL Certificate

SSL Certificate is also called a security cite certificate or a web server certificate. SSL certificate binding with the site's IP address and domain, can guarantee the authenticity of the site and not faked. The users are safe in the network communications, by the client browser and web server to establish the SSL security channel to ensure.

Applying for SSL certificate is required to submit the following information:

- Applicants fill in and sign (or seal) a written application form
- Applicants' (individual or organization) original identification material and photocopy or digital scan (the specific requirements mentioned as individual and organization certificates requirements above).
- Applicants must submit a written commitment documents about the domain name (or IP address of the Internet), including the usage of domain ownership information and assurance to indicate that the domain name (or IP address) belonging to all applicants, and the certificate is legitimate used. SHECA will take appropriate way to assess applicants for the domain ownership, please refer to Section 3.2.5.
- If it is entrusted to handle, which is required to submit an original and copy or digital scan of identification documents of an application and the trustee and a letter of attorney signed by the applicant.

For data source of SSL certificate, if the date of obtaining data or document estimated reliable does not exceed 825 days and the certificate is still within valid period, then the data and

document can be revalidated.

4. Code signing certificate

(A) Personal code-signing certificate applied by a personal identification is used to sign software code, in order to effectively prevent tampering, identity theft by other such owners. The software is downloaded that code signing, which ensures that the source of the software and software is integrity.

Applying for an individual code signing certificate is required to submit the following information:

- Applicants are required to fill in and sign a written application form
- A copy and the original of personal ID card (or military ID, student ID, passport and other valid identification documents); if SHECA and registration authority terminal have confirmed the identity of individual applicants by phone, mail, third-party verification or other ways. Applicants can submit copies of identification documents by fax, mail, etc. without having to submit the originals of identity documents.
- Applicants must commit through written documents that the code certificate will not be used for any malicious or illegal purposes.
- If it is entrusted to handle, it is required to submit original and copy of the above applicant and client, and a letter signed by the client.

(B) Organization code signing certificate applied by the organization name is used to sign software code, in order to effectively prevent tampering, identity theft by other such owners. The software is downloaded that code signing, which ensures that the source of the software and software is integrity.

Applying for organization code signing certificate is required to submit the following information:

- Applicants fill in ,sign and seal a written application form
- the original (original or copy) and copy of business license or other legal organization registration documents.
- The applicant's original business license (original or copy) and copy, if a business license isn't here, the valid original documents (original or copy) optional in the a written application form ; currently recognized valid documents as follows: business license, registration institutions legal certificate , other social groups registration certificate, national laws recognized valid documents. If SHECA and the registration authority terminal have identified by phone, mail, and other third-party verification, or confirm identity of the unit applicant by other way, the applicant can submit copies of all documents by fax, mail, etc. without having to submit original documents.
- Applicants must commit the code certificate will not be used for any malicious or illegal purposes.
- A copy and the original of identity card (or military ID, student ID, passport and other valid documents) of entrusted applicant
- A letter of attorney to entrusted applicant (to be stamped with official seal).When

submitting the application form, applicants stamped with official seal after the applicant signs the application form , which means written authorization for the commission applicant is made .

5.Device Certificate

(A) Equipment certificate is issued to various types of non-web application servers, and is used to achieve encryption, electronic signatures of application servers identity and application .Application server certificate can be stored in the hard disk, IC card, encryption machines, cards and other types of encryption devices.

Applying for a server certificate may be required to submit the following information:

- Applicants fill in and sign (or seal) a written application form
- Applicants (individual or organization) identification material or the copies(the specific requirements mentioned as individual and organization certificates requirements above).
- Applicants must fill in the ownership declaration documents about a application server to show that the application server belongs to all applicants.
- If it is entrusted to handle, it is required to submit an original and copy of identification documents of the applicant and the agent, and a letter of attorney signed by the applicant.

(B) Internet equipment certificate is issued to various types of VPN gateways, network access equipment in order, and is used to record the device identity, and achieve the encryption, electronic signatures of the application. Such certificates can be stored in the hard disk, IC card, encryption machines, cards and other types of encryption devices. Specific application requirements please see the SSL certificate.

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, including RA, RAT and advance certificate providers, 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 The Registration Process and Responsibilities

4.1.3.1 Registration Process

Offline certificate application process

1. The certificate applicant brings all relevant evidence document to RAT of certification services agencies or submits application online to RAT), and fills in the application form.

2. The RAT audit authenticity of identity related to the certificate applicant. If authentication fails, RAT will refuse to issue certificates for applicant, and save information not passed.

3. If the authentication passes, RAT entries and audits certificate application information by service system, and signs by operator's certificate, then encrypts the certificate by the higher level RA, and submits the information to the RA.

4. When RA receives information submitted from RAT, verifies the signature after decryption, then transfers information to CA .If authentication is not passed, then the next step is refused, and failure is returned directly.

5. RAT gives out a password envelopes to the certificate applicant.

6. RA sends the certificate application data of the applicants to CA.

7. CA issues certificate in accordance with the certificate request.

8. Applicants accept and download the certificate.

For online application, SHECA requires:

SHECA supports online certificate requests. When the security and authentication is good, the applicant may submit their application information by fax or network. Applicants personally need not go to SHECA and its authorized service for physical authentication. This mode of application is for testing certificate applications, the certificate renewal application, and the applicant group identified by SHECA.

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.

Electronic certification service agencies require certificate subscriber to update certificate timely to ensure the reliability of the certificate, with technical progress and development.

2. The Responsibilities of RA

RA obtains SHECA authorization in accordance with procedures , follows the operation agreements of CPS and SHECA and other SHECA published standards and procedures to receive and process the applicant's certificate services requests, and sets up and manages various types of subordinate receiving agency based on authorization , including RA, RAT and so on.

RA must follow the service acceptance, systems operation and management practices created by SHECA, and SHECA will continue to improve and release timely relevant norms and standards. RA has right to decide whether to provide appropriate services for applicants, according to the CPS and practice statement published by SHECA. RA must meet establishes a reasonable mechanism to ensure the credibility safe and reliable of information transmission of all certificate services (such as applications, renewals, suspension, etc.), according to SHECA requirements and SHECA proposes mandatory standards.

According to SHECA requirements and specifications, RA determines setting up methods, management methods and audit methods of the certificate services agency, and these methods shall not conflict, contradiction or inconsistent with SHECA published relevant provisions must be written and published in the form of documents.

According to the provisions of the CPS, RA ensures that its operating system is in a secure physical environment, and has appropriate safety management measures. RA must be able to provide all the data and backup of certificate services, and in accordance with SHECA requirements to ensure information transfer security between the subordinate certificate service institutions. Importantly, RA promises it carries out strictly obligations to save application data for subscribers, and bears the legal responsibility therefore.

Electronic certification service agencies manage RA in accordance with this CPS and licensing agreements, including Service qualification examination and standardize inspection. Electronic certification service agencies have the final disposal right for servicing applicants. Electronic certification service agencies have the right to review the information of the applicant. All the losses are assumed by the RA, because of the applicant's qualification certificate checking lax.

RA must keep all the applicant information and does not leak to any unrelated third parties. RA must manage all kinds of application forms, certificate storage medium, passwords envelopes, etc. safely, reliably, strictly to ensure their adequate protection.

RA must accept SHECA supervision and audit for its operations, and act in concert with SHECA's audit requirements.

3. The responsibility of RAT

RAT obtains SHECA and higher level RA authorization in accordance with procedures ,

follows this CPS and related operation agreements and other SHECA published standards and procedures, receives and processes the applicant's certificate service requests.

RAT must follow the service acceptance, systems operation and management practices created by the electronic certification service providers and superior RA, and electronic certification service providers and superior RA will continue to improve and release timely relevant norms and standards . According to the CPS, superior RA, SHECA publishing specifications, RAT has right to decide whether to apply for a appropriate certificate services for applicants, according to SHECA requirements and SHECA proposes mandatory standards.

According to the provisions of the CPS, RAT ensures the security of its operating system is in the physical environment, and has the appropriate safety and quarantine measures. RAT must meet establishes a reasonable mechanism to ensure the credibility safe and reliable of information transmission of all certificate services (such as applications, renewals, suspension, etc.), according to SHECA requirements and SHECA proposes mandatory standards.

Electronic certification service agencies and superiors RA manage RAT in accordance with this CPS and licensing agreements, including Service qualification examination and standardize inspection. Electronic certification service agencies have the final disposal right for servicing applicants. Electronic certification service agencies have the right to review the information of the applicant.

RAT has responsible for the authenticity of the information of certificate applicants, no matter whether the application is accepted or not. All the losses are assumed by the RAT, because of the applicant's qualification certificate checking lax.

RAT must keep all the information of applicant and doesn't reveal to any unrelated third-party. RAT must manage all kinds of application forms, certificate storage media, passwords envelopes, etc. safely, reliably, strictly to ensure their adequate protection.

RAT must accept SHECA the supervision and audit of its operations, and act in concert with SHECA's audit requirements.

4. The responsibility of the advance vendor

Advance vendors are required to bear all the cost of the certificate, and pay off according to the manner provided by SHECA.

The behavior of advances vendors , that means he or she is willing and able to take the provisions of CPS and SHECA relevant agreement, guarantee authenticity on the identity of the applicant .

5. 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.

Certificate applicants must carefully read and understand the CPS listed or recommended by the SHECA or security measures to fully understand the importance of private key saving, to ensure the security of the private key.

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

6. 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.

Subscribers must ensure private key is safe. SHECA only inform, but does not require certificate applicants comply with security measures SHECA proposed. Subscribers can choose any secret measures that they think. At the same time, SHECA states that SHECA does not undertake all the responsibilities for problems caused by the subscriber keeping private key , unless the subscriber can legally prove that the primary responsibility of such problems coming from the issuing authority.

Once any crisis occurs that lead to security, including loss of subscribers' private key, forgotten or compromised, and other non-listed occasions, the subscriber should immediately notify SHECA to take measures. If the subscriber knows the private key is in some problems and without noticing SHECA timely , and led losses to SHECA , the relevant certificate authority services agencies, other subscribers and certificate relying party losses, the subscriber must bear the corresponding liability.

7. 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 the CPS 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 the CPS, including the terms of exemption, rejection and limit obligation.

8. The obligation of directory service

SHECA publishes subscriber's certificate and CRL the certificate associated in the directory

erver.

SHECA publishes and updates directory service of certificate and CRL at least every 24 hours, adjust and publish the time interval according to relevant laws, policies, requirements and certification service requirements. SHECA will publish the adjustment through the website http://www.sheca.com.

9. 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.

10. 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

finds there might be problems with the certificate, or finds or doubts there is private key leak or certificate abuse, or finds other related certificate malpractice, leak and abuse or other misbehavior can report or complain to SHECA. Details for reporting show below.

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

After accepting the report or complaint, SHECA will launch an audit and investigation process within 24 hours to the related certificate and inform the reporter and related other parties whether or not it will revoke the certificate within 2 business days. The investigation includes but is not limited to the following,

- The reporter's identity authentication
- The nature and the cause of the problem reported
- The number of times and the frequency of the problem reported
- The re-examination of the certificate issuing process and other related business processes.
- The conformance to CP/CPS and subscriber agreement.
- The conformance to related laws and regulations.

Besides, when SHECA is made aware of incidents involving malware, the following actions will be taken by SHECA.

- Within 1 business day of being made aware of the incident, SHECA contacts the software publisher and requests a response within 72 hours.
- Within 72 hours of being made aware of the incident, SHECA determines the volume of relying parties impacted.
- If a response is received from the publisher, SHECA and publisher determine a 'reasonable date' for revocating the CodeSigning certificate.
- If no response is received from the publisher, SHECA notifies the publisher that the certificate will be revoked in 7 days unless it has documented evidence that this will cause significant impact to the general public.

4.9.5 Revocation Request Grace Period

Revocation requests shall be submitted as promptly as possible within a commercially reasonable time. If the delay happens due to objective reasons, it should not exceed 8 hours. If it is in the grace period, subscribers did not timely request revocation, SHECA will not bear any loss or responsibility resulting from subscribers don't request timely revocation.

4.9.6 Time Within Which CA Must Process the Revocation Request

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

delay.

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

1. The nature of the alleged problem;

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

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

4. Relevant legislation..

4.9.7 Revocation Checking Requirements for Relying Parties

As public information, relying parties can get Certificate revocation list (CRL) in the Certificate Extensions of acquired certificates, or, query certificate state by the website: https://www.sheca.com website or query through the Online Certificate Status Protocol (OCSP).

Before the relying party trusts the certificate, they should take the initiative to check the status of certificate according to the latest CRL which based on SHECA and its sub-CA.

Meanwhile, they also need to verify the reliability and integrity of the CRL to ensure that it is published by SHECA and its authorized sub-CA, including digital signature of SHECA and its authorized sub-CA.

4.9.8 CRL Issuance Frequency

SHECA updates and publishes certificate revocation list (CRL) every 24 hours. For the sub-CA certificate, it is issued or published once at least every three months, annually for the root CA certificate.

SHECA may decide to shorten the time of generating and updating CRL.

4.9.9 Maximum Latency for CRLs

CRL is effective after revocation request approved within 24 hours. CRL can come into effect immediately in special emergency circumstances (without regarding network conditions, the time difference because of the network factors is allowed) . It means SHECA will publish the revoked certificate in the CRL.

SHECA promises to publish the certificate revocation list within 24 hours after revocation act happens.

4.9.10 The Availability of Online Status Queries

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

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

4.9.11 Online Status Query Requirements

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

1 For the status of Subscriber Certificates:

SHECA maintains real-time update of information provided via an Online Certificate Status Protocol. OCSP responses from this service have a minimum expiration of 8 hours and maximum expiration time of 7 days.

2 For the status of Subordinate CA Certificates:

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

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

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

Users can freely inquire status online. SHECA doesn't set any read permissions. If the relying parties can not query the CRL, then they can query certificate status through the OCSP or by visiting the website.

4.9.12 Other Forms of Revocation Advertisements Available

In addition to CRL mode of X.509 V2 format, SHECA does not provide other methods of the revocation information dissemination.

4.9.13 Special Requirements of Key Damage

If the subscriber finds or suspects that the key security is damaged, the certificate should be revoked immediately.

If SHECA own key is damaged, or due to the SHECA's reason f users' key is also damaged, SHECA will revoke the certificate actively and immediately and issue the certificate real-time to CRL. SHECA take responsibility for the subscribers' losses caused by key damage, and SHECA will issue new certificates in time.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

SHECA provides two access to certificate status check services:
1 Ã CRL ----CRL is published by the directory server ,and its credibility and security is to be

guaranteed by SHECA and its authorized issuing authority via CA certificate's signature . CRL only provides periodic certificate status inquiry. Now SHECA publishes CRL once every 24 hours.

Users need to download the CRL to the locality and verify, including legality verification and checking whether the CRL contains the serial number of the certificate to be tested.

2 ÃOCSP ----The user can inquire the status of certificates through the OCSP . OCSP provides real-time queries of certificate status information.

4.10.2 Service Availability

Certificate Status Services must be available in 7X24 hours. Without scheduled interruption, SHECA should ensure that CRL and OCSP inquiry is in use. Once exception circumstance happens, the user can query by http to obtain certificate status information.

4.11 Termination

The following conditions shall be deemed that the user terminated to use the certificate services provided by SHECA:

1 ÃAfter the expiration of the certificate, the certificate subscriber no longer extends the period of the certificate or reapplies for a certificate then it will automatically terminate SHECA services.

2 ÃIn the validity of the certificate, the subscriber terminates service certificate.

Once the user terminates to use SHECA certificate authentication services in the validity of certificate, after SHECA approves his or her request for termination, the subscriber's certificate will be revoked real-time, and released in accordance with the CRL distribution strategy.

4.12 Key Generation, Backup and Recovery

4.12.1 Signature Key Generation, Backup and Recovery Strategies and Actions

In order to ensure the security and uniqueness of subscribers' signature private key, SHECA will suggest subscribers to operate their keys generation and backup, and even operate the recovery themselves if the key is lost.

However, if the subscriber request SHECA to generate user keys for them, SHECA may perform signature key generation for user. SHECA shall not be liable for any loss caused by the loss of the signature private key.

SHECA will take strict measures to ensure the safety of the user key generation and follow relevant regulations of the State Commercial Cryptography Administration of China which is equivalent to FIPS 140-2 Level 2. SHECA won't keep any copies of user's private key.

SHECA does not provide services of hosting and recovery for subscriber’s private key.

4.12.2 Encryption Key Generation, Backup and Recovery Strategies and Actions

The user's encryption key is generated by the designated key management agency which is set up by the state. All the encryption key generation, backup and recovery strategy are decided by this agency.

4.13 Certificates and CRL Archiving

After the certificate is expired or revoked, user information and certificates data are reserved not less than 7years.

CRL files are archived in CD-ROM, the archive period is 7 years.

5. Facility, Management and Operational Control

5.1 Physical Control

The physical control and security policies, authentication service system complied with by SHECA 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 c

- Other training

SHECA shall record the staff training and archive the record, and assure the personnel have qualified skill as required in the Baseline Requirement 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 can not 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 and related agreements and norms
- 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 Procedures

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 and destruction 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. CRL's operational records.

6. Form of passing in and going out SHECA region, 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 ÃRA ÃRAT .

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
- directory 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 unnormal services on certificate, SHECA will announce to users 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, certificate and CRL 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

Subscriber's private key and certificate signature encryption key are stored by the subscribers themselves. Responsibility related for the preservation is undertaken by subscribers themselves.

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 d

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 the CPS 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 CRL and OCSP for certificate subscriber and relying party to query.

4. Subscriber certificate is re-issued in accordance with the CPS 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 the CPS, 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.

5.9CA 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, 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.

6. Technical Security Controls for Certification System

6.1 Key Pair Generation and Installation

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. Generation of root key pair

SHECA's root key pairs are generated by the equipment approved and licensed by the State Commercial Cryptography Administration of China. Currently, part of the encryption server is completely compliant with FIPS140-2 while they others in accordance with relevant provisions of state encryption management. 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 personnels 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 can not be exported in the form of plain text or cipher text.

2. Generation of subscribers signing key pair

Generation of subscriber siging key pair should be performed by subscribers. Each signing certificate subscribers can choose freely key pair generated by the equipment of state cryptography administration department approving and licensing, such as encryption machine, encryption card, USB Key, IC card. Subscriber should ensure the security and realiability of the generation process. Before the choice of these devices, users may consult in advance system compatibility and acceptance related towards SHECA. SHECA did not promise to accept all types of the password generation equipment. The subscribers may be provided the USB Key by SHECA in accordance with the relevant provisions of the state encryption management as the device for key generation and storage, and offering relevant guidance.

SHECA generally doesn't offer proxy service of key pair generation, The Subscribers certificate key pair generation must follow country's laws and policies. SHECA supports multiple generation method for multiple modes of signature key pair, certificate applicants may select according to their needs. No matter what way, the security the key pair generated should be guaranteed.

SHECA has implemented security measures in technology, business processes and management.

3. Generation for Encryption Key Pair of the Subscriber

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

4. Certificate subscribers have the responsibilities and obligations to protect the private key security, and assume the legal liability as this.

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

6.1.2 Private Key Delivery to the Subscribers

The private key of SHECA certificate authentication system is generated in the system initial phase. Private key delivered to a Subscriber is not applicable..

SHECA normally does not offer or generate signing key pair for subscribers. But if the applicant provides written application asking SHECA to sign the key pairs and after the application is approved by SHECA, SHECA will generate the key pairs on behalf of the applicant, and make sure to take adequate measures to ensure key security while delivering the key pairs to the applicant who performs the certificate application. But in case of the loss, leakage of this key pair, SHECA does not assume any responsibility and obligation.

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 size of key which SHECA supports is 1024 bits or more, and the size of RSA key for the publicly trusted subscriber certificates should be 2048 bits or more. The size of SM2 key is 256 bits.
The SHECA key pair length is RSA 2048 bits, RSA 4096 bits and SM2 256bits.

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.

Key Usage Purposes

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

1 Self-signed certificates to represent the Root CA itself

2 Certificates for Suboardinate CAs and Cross Certificates

3 Certificates for Infrastructure 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 the CPS and the CP-related.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Standards and Controls of Cryptographic Module

SHECA uses the host approved and permitted by the national state cryptography administrative department. The standards, usage and controls of cryptographic module meet national relevant provisions, and some parts follow related provisions for FIPS140-2 standard, mainly in the aspects of generation for key, operation for key and protection for key following FIPS140-2 requirements.

As FIPS140-2standard is not recognized and supported by the state cryptography administration department, country has strict regulatory requirements for cryptography products. Therefore, SHECA only consults FIPS140-2 standards and chooses autonomous encryption devices, under the state encryption management consent, may specifically reference to the information provided by equipment manufacturers.

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 can not 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: It can use number 0 or number 6 key in the host encryption server to generate RSA key pair which can be output encryption devices and 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 Control

1.SHECA uses multi-person control to activate, use, 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. Subscriber are obligated to inform SHECA in the first place in any of these circumstances.

6.2.3 Private Key Escrow

SHECA does not offer private key escrow service.

Protection, management, archiving, backup, escrow etc. of encrypted private key are regulated and decided by the Shanghai Key Management Center (KM). Certificate subscribers can communicate with the appropriate national authorities on encrypted private key trusteeship problem.

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 subscribers encryption certificate, the protection, management, archiving, backup, escrow etc. of encrypted private key are regulated and decided by the appropriate state key management department .Certificate subscribers can communicate with the appropriate national authorities on private key backup problem.

6.2.5 Private Key Archival

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

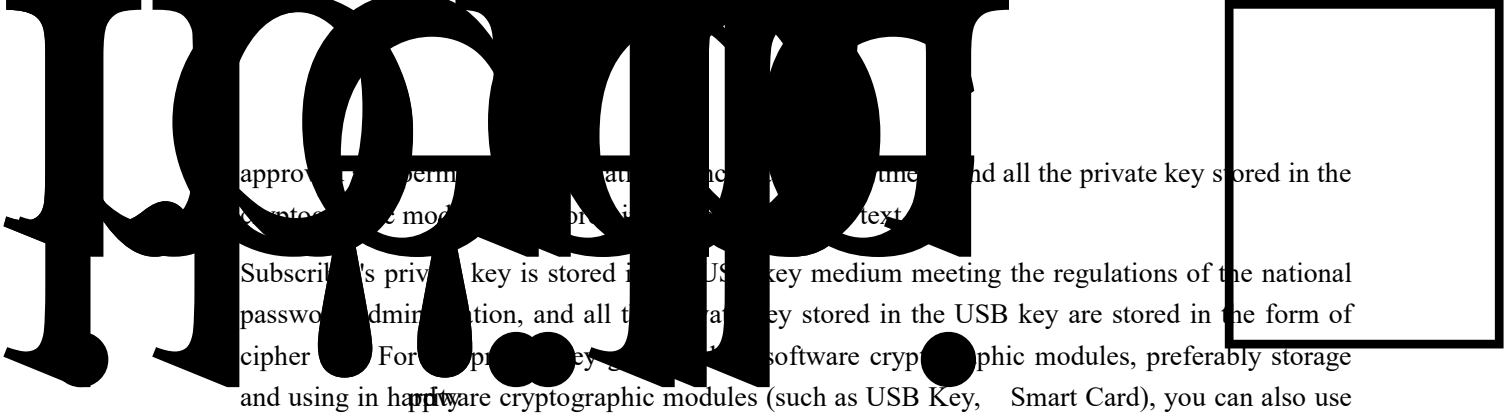
6.2.6 Private Key Transfer into or from a Cryptographic Module

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. As for the private key stored in the software code module, and if subscribers are willing to bear the relevant risks, the subscriber can choose the way of import and export, the operation using password protection and other control measures authorized access.

6.2.7 Private Key Storage on Cryptographic Module

Private keys held on hardware cryptographic modules shall be stored in encrypted form which is



approv[illegible] perm[illegible] at[illegible] nc[illegible] time [illegible] nd all the private key stored in the [illegible] mod[illegible] pr[illegible] text.

Subscri[illegible]'s priv[illegible] key is stored i[illegible] US[illegible] key medium meeting the regulations of the national passwo[illegible] dmin[illegible]tion, and all t[illegible] ey stored in the USB key are stored in the form of cipher [illegible] For [illegible] pr[illegible] ey [illegible] software cryp[illegible]phic modules, preferably storage and using in hardware cryptographic modules (such as USB Key, Smart Card), you can also use specific software code modules with security measures.

6.2.8 Method of Activating Private Key

SHECA assumes that the private key can only be activated after password authentication by the subscriber, unless the subscriber has asked for a change for the method of activating the private key, and is willing to assume the responsibility after the change.

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 personnels to activate the private key of SHECA. Any unauthorized person must not be allowed to access, use or activate the private key.

For the private key stored in the subscriber's computer software code module, the subscriber should take reasonable measures to protect the physical security of the computers in order to prevent other users without the authorization using the subscriber's computer as well as the relevant private key. If the private key is stored in software code module without password protection, then the loading of software cryptographic module means the activation for private key. If you use password to protect private key, after software code module is loaded, you need to input the password to activate the private key.

For the private key stored in such as a USB Key, smart cards, en"ibib

- 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. Compliance Audit and Other Assessments

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

8.1 Frequency and Circumstance of the Assessment

1 ÃSHECA accepts the assessment and inspection authorities once a year under the "Electronic Signature Law", "Electronic Authentication Services" and other requirements.

2 ÃIn accordance with the requirements of national authorities , relevant national standards and the operations and services of the CPS provisions , internal evaluation and auditing standards created by SHECA ,SHECA at least perform an internal assessment audit. Audit contents towards authorized agencies mainly include spot check of certificate formats and validation prcedures.

RA, RAT and other SHECA authorized certification service agencies must follow the CPS and the corresponding CP, and accept all of its processes and operations audit by SHECA, test whether it is compliance with this CPS and related to SHECA license agreement or other publicity of the trust service policy . SHECA assess the affiliates generally once a year. In the licensing agreement SHECA and all agencies clearly define this. Auditors are appointed according to requirement by

SHECA, who should be familiar with related knowledge of SHECA norms and trust services, understand the basic safe knowledge, and perform audit according to SHECA norms, agreement to provide services, to make conclusion on SHECA and other authorized agencies independently and impartially .

3 ÃSHECA employs an independent auditing firm, according to the audit rules of WebTrust to CA , annual external audits and assesses.

4 ÃSHECA performs risk assessment annually to discriminate threats from internal and external, and estimates the possibility of occurrence of the threats and the loss that may be caused. Meanwhile, SHECA estimates if the current company policy, technologies, systems and other related measures are able to cover all the risks.

8.2 The Qualifications of the Assessor

1 Ã SHECA unconditionally receives the assessment from information industry department. SHECA is implemented evaluation by those who have the qualification and experience which depend on the competent departments.

2 ÃDuring the internal assessment audit, SHECA requires a assessment staff at least have the related knowledge of certification and information security audit, more than two years relevant experience and are familiar with the norms of the CPS, and should have a knowledge and practical experience of computer, network and information security . Internal assessment is organized and implemented by SHECA Strategy Development Department.

3 ÃIf SHECA deems that it is necessary to hire external auditors to implement internal assessment, then the auditors should have the following qualifications:

- Must be licensed, the rating agencies have a business license , a good reputation in the industry;
- Understand computer information security system, communications network security requirements, PKI technology, standards and operations
- Have the expertise and tools to check the system performance.

8.3 Assessor's Relationship to Assessed Entity

1 ÃThe external auditors (information industry department or its delegated entities) and SHECA are independent , there is no business, financial transactions, or any other interest could affect the objectivity of the assessment, and assessors should evaluate SHECA with independent, impartial and objective attitude .

2 Ã It is relationship independent between SHECA internal assessors and the object evaluated , without any interest enough to affect the objectivity of the assessment, and assessors should evaluate object with independent, impartial and objective attitude .

SHECA could choose a professional, impartial, objective and professional audit rating agencies as needed to assist internal evaluation.

8.4 Assessment Content

1 Ã SHECA accepts the assessment of any content in accordance with requirements and specifications raised by information industry department.

2 ÃSHECA internal assessment audit include:

- Whether SHECA develops and publishes CPS
- Whether SHECA develops the relevant practices and operation agreement in accordance with CPS
- Whether it operates in accordance with CPS and related business practices and operational protocols
- Service Integrity: the key and certificate life cycle safety management, certificate revocation operation, safe operation of business systems, business practices review
- Physical and environmental security controls: information security management, personnel security controls, security control of building facilities , security controls of hardware and software equipment and storage medium , system and network security control, security controls of system development and maintenance, disaster recovery and backup system management , audit and archive security management .

3 Ã The third-party auditor firm audits independently SHECA in accordance with WebTrust specification requirements for CA .

8.5 Actions Taken as a Result of Deficiency

1 Ã After the information industry department assessment has completed, SHECA must inspect deficiencies and shortcomings based on the results of the assessment . According to the requirements of its proposed rectification, SHECA submits modification and prevention measures and corrective plans, and accept its review of the corrective plan as well as reassess the situation.

2 ÃAfter SHECA completes the internal assessment , the auditors need to list the detailed list of all the problem projects . The auditors and the object evaluated should discuss the issue and the written results should be noticed to SHECA Safety Certification Commission and the person evaluated for further processing.

The object evaluated must inspect deficiencies based on the results of assessment, submit

modifications and preventive measures and corrective plans, and accept the assessment of the corrective plan and the evaluation of rectification once again.

3 Ã After the assessment from a third-party auditor firm is completed, SHECA will rectify in accordance with its work reports and accept the audit and evaluation once again.

If the authentication agencies confirms that the accident and no action found in the audit will result in threat immediately to the consistency or integrity of certificate security system,then the certification agencies will develop corrective action plans within 30 days and execute within reasonable time.

8.6 Communications and Release of Results

1 Ã After the assessment , the information industry authority will deal with assessment results in accordance with laws and regulations . The audit results will be published by the website http://www.sheca.com.

2 Ã After SHECA's internal assessment result is defined by the object relevant person evaluating , result will be treated as confidential information to handle. Only the object evaluated and the auditor as well as SHECA Safety Certification Committee can understand. Non-certified by the SHECA security committee approval or authorized by object evaluated, the auditors can not disclose to any other unrelated third parties. If necessary, the notification method of assessment results associated with SHECA entities, which will be stipulated in agreement SHECA and evaluated entity.

3 Ã After the assessment from a third-party auditor firm is completed, the audit results will be published by the website http://www.sheca.com.
Any third-party notices the assessment results or similar information to evaluation entity , which must be clear in advance that the purpose and manner of notice will be shown to SHECA and obtain SHECA consent, except otherwise provided by law; SHECA retains the legal authority in this area.

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

2 ÃIf 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 ÃOther 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 and renewal fees 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 CPS 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 CPS.

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 CPS 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 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 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 CPS.

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 CPS, 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 CPS 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 can not 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 CPS, 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 interrelative 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 CPS conflict with the relevant provisions of other SHECA developed, the user must accept the constraints of the CPS .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 CPS. If the agreement is different from the provisions of the CPS, 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 within related CPS provisions, comply

with the provisions of this CPS.

- 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 can not express, implied or otherwise, contrary to the provisions of the above statements.

2. SHECA warrants to subscribers

Unless otherwise provided in this CPS 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 CPS.
- The certification agencies will revoke the certificate timely according to the provisions of the CPS.
- 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 CPS, 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 CPS:

- 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 publishment

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 the CPS.

9.6.2 RA Representations and Warranties

After obtaining SHECA authorization according to the procedures of authorization, RA warrants that:

- Follow the license agreement of CPS 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 must follow the norms, systems operation and management requirements created by SHECA. According to specifications published by the SHECA and CPS, RA has 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 the CPS to ensure operating system in the security physical environment, and have the appropriate safety management and quarantine

measures. 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 under CPS 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 services .
- 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 the CPS 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 CPS, 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 the CPS.
- 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 the CPS, 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