SHECA Certification Practice Statement (CPS)

Version 3.8.0

Effective Date: April 30, 2025

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 https://www.sheca.com .

Version Control

Version	Released Date	Issuer
V3.8.0 (Current version)	April 30, 2025	SHECA Security Certification Committee
V3.7.9 (Previous version)	Nov 18, 2024	SHECA Security Certification Committee
V3.7.8 (Previous version)	May 21, 2024	SHECA Security Certification Committee
V3.7.7 (Previous version)	March 13, 2024	SHECA Security Certification Committee
V3.7.6 (Previous version)	August 23, 2023	SHECA Security Certification Committee
V3.7.5 (Previous version)	July 21, 2023	SHECA Security Certification Committee
V3.7.4 (Previous version)	June 12, 2023	SHECA Security Certification Committee
V3.7.3 (Previous version)	April 18, 2023	SHECA Security Certification Committee
V3.7.2 (Previous version)	April 18, 2022	SHECA Security Certification Committee
V3.7.1 (Previous version)	Nov 15, 2021	SHECA Security Certification Committee
V3.7 (Previous version)	June 18, 2021	SHECA Security Certification Committee
V3.6.9 (Previous version)	April 29, 2021	SHECA Security Certification Committee
V3.6.8 (Previous version)	August 11, 2020	SHECA Security Certification Committee
V3.6.7 (Previous version)	June 5, 2020	SHECA Security Certification Committee
V3.6.6 (Previous version)	April 30, 2020	SHECA Security Certification Committee
V3.6.5 (Previous 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**
V3.8.0	Update UniTrust Network Trust Service Hierarchy; Add CAA record check requirements according to S/MIME BR; Add Time Stamping certificate policy OID; Adjustment of wording
V3.7.9	Disclosure of newly issued Sub-CAs; Modify version as required by Baseline Requirements;

	Adjustment of wording
V3.7.8	Disclosure of 8 newly issued single-purpose Root CAs and 15 corresponding Sub-CAs; Disclosure of 12 newly issued Sub-CAs under UCA Global G2 Root; Add algorithm object identifiers of ECDSA; Modify version as required by Code Signing Baseline Requirements; Adjustment of wording
V3.7.7	Modify version as required by S/MIME Baseline Requirements; Disclosure of reissued corss-signed UCA Global G2 Root
V3.7.6	Modify version as required by Baseline Requirements; Add organization identification method; Adjust 9.16.3 Severability Requirements
V3.7.5	Disclosure of newly issued Sub-CAs Xinnet DV SSL /Xinnet OV SSL
V3.7.4	Information of reissued corss-signed UCA Global G2 Root
V3.7.3	Disclosure of newly issued Sub-CAs SHECA OV Server CA G7; Update Sub-CAs status; Update ARL/CRL renewal cycle
V3.7.2	Disclosure of newly issued Sub-CAs
V3.7.1	Information about disable partial Subordinate Roots Disclose special domain validation rules of China e-government extranet Add the authentication method of staff certificate Description of key recovery service
V3.7	Update ARL renewal cycle Key length of Code Signing and Timestamp certificate requirement
V3.6.9	Disclosure of new Sub-CAs Delete outdated domain validation methods listed in section 3.2.5 2(8)，(9) of last version
V3.6.8	Update name of supervision government agency Disclosure of LDAP address Power supply of server room
V3.6.7	Information of new Subordinate Root GlobalSign China CA for AATL
V3.6.6	Information of new Roots UniTrust Global Root CA R1, UniTrust Global Root CA R2, UniTrust Global Root CA R3 Delete outdated domain validation method listed in section 3.2.5 2(3) of last version Add new Identity authentication method Certificate renewal period adjustment Add an initial investigation reporting mechanism
V3.6.5	Information of new corss-signed UCA Global G2 Root SSL certificate validity changed SSL certificate domain validation method changed

V3.6.4	Information of new root certificate UniTrust PTC Root CA R1, UniTrust PTC Root CA R2 Modified Individual and Organizaiton Identity Certificate validation process
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 Verification Methodology modified to conform 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

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 website https://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(https://www.sheca.com).

Contents

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(MIIT) and State Cryptography Administration(SCA), 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, S/MIME Baseline Requirements and Code Signing Baseline Requirements 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 above Baseline Requirements, the latter 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.

1.1.2 The Relationship Between CPS and CP

Each certificate under the Unitrust NTSH is supported by a unique Certificate Policies (CP).The CP sets forth the requirements all participants of certificate services must meet under the UNTSH. Certification Practice Statement(CPS) is to mainly confirm the procedures, operation and control measures participants take for implementing and meeting the requirements of Certificate Policies while SHECA as a digital certificate operational service subject ,is providing digital certificate services, and to describe and specify the required conditions, operational procedures and established guidelines to provide digital certificate services in detail. Certificate Policies (CP) and Certification Practice Statement (CPS) are serving the UNTSH, decided the level scope, purpose of trust for digital certificates under the UNTSH. Certification practice statement (CPS) is subordinate to the Certificate Policies (CP), when elaborating the same theme; Certificate Policies (CP) is the benchmark.

Currently, "SHECA Certification Practice Statement (CPS)" only supports "Unit rust NTSH Certificate Policies." If there is a need, "SHECA Certification Practice Statement (CPS)" can support multiple Certificate Policies to be applied to different purposes or different Relying Party groups.

1.1.3 UniTrust Network Trust Service Hierarchy

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

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

PKI hierarchical architecture within Unitrust NTSH includes the following root CAs:

- **UCA Root**
- **UCA Root G2**
- **UCA Global G2 Root**
- **UCA Extended Validation Root**
- **UCA Root SM2**
- **UniTrust Global Root CA R1**
- **UniTrust Global Root CA R2**
- **UniTrust Global Root CA R3**

- **UCA Global Root**
- **UniTrust Global TLS RSA Root CA R1**
- **UniTrust Global TLS ECC Root CA R2**
- **UniTrust Global SMIME RSA Root CA R1**
- **UniTrust Global SMIME ECC Root CA R2**
- **UniTrust Global Code Signing RSA Root CA R1**
- **UniTrust Global Code Signing ECC Root CA R2**
- **UniTrust Global Time Stamping RSA Root CA R1**
- **UniTrust Global Time Stamping ECC Root CA R2**

UCA Global G2 Root is cross signed by **Certum Trusted Network CA**.

UniTrust Global TLS RSA Root CA R1 is cross signed by **UCA Global G2 Root**.

UniTrust Global TLS ECC Root CA R2 is cross signed by **UCA Global G2 Root**.

All intermediate certification authorities are subordinated to their roots. All the above root CAs and their sub CAs (including cross-signed CAs) are subject to Unitrust NTSH PKI hierarchical. Detailed information of the CA certificates is disclosed on SHECA's repository: https://www.sheca.com/repository/

1.2. Document Name and Identification

This document is "SHECA Certification Practice Statement (CPS)", referred to as SHECA CPS."SHECA CPS", "Shanghai CA CPS", "Shanghai CA Certification Practice Statement", "Shanghai CA Authentication Service White Paper", "SHECA White Paper", "SHECA Certification Business Statement," "Shanghai CA Authentication Business Statement ", "Shanghai CA Center CPS ","Shanghai CA Center Certification Practice Statement "and its similar expressions, no matter in what place, they should be seen as this document or the quote of this document. The CPS will be regularly updated based on the development of SHECA third-party electronic authentication services. Version number (such as "version 1.2" or "CPS1.2") should be indicated in the Certificate Practice Statement (CPS).

SHECA assigned a self-defined Object Identifier (OID) to this CPS: 1.2.156.112570.1.0.2.

The CPS defines the OID of the ssl certificates that compliance with the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates of the CA/B forum (www.cabforum.org) is:

1.2.156.1.112570.1.1.2.2

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

OID	Object
1.2.156.112570	UniTrust
1.2.156.112570.1	SHECA
1.2.156.112570.1.0	Policies
1.2.156.112570.1.0.1	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 2.23.140.1.4.2	TimeStamping Policy

1.2.156.112570.1.4.1	TimeStamping AATL Policy
1.2.156.112570.1.5	OCSP Policy
1.2.156.112570.1.9.1 2.23.140.1.5.1.3	Mailbox-validated SMIME Certificates Policy
1.2.156.112570.1.9.2 2.23.140.1.5.2.3	Organization-validated SMIME Certificates Policy
1.2.156.112570.1.9.3 2.23.140.1.5.3.3	Sponsor-validated SMIME Certificates Policy
1.2.156.112570.1.9.4 2.23.140.1.5.4.3	Individual-validated SMIME Certificates 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，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 S/MIME Certificate

Based on different security levels and authentication methods of the issued certificates, the S/MIME Certificates include: Mailbox-validated S/MIME Certificates, Sponsor-validated S/MIME Certificates, Individual-validated S/MIME Certificates and Organization-validated S/MIME Certificates. The Mailbox-validated S/MIME Certificate only verifies the ownership and control of the email address and does not verify the true identity of the email address owner, which can ensure the integrity of the email content without being read and tampered by others during the email transmission procedure. The Sponsor-validated S/MIME Certificate is the most common type of email certificates, often issued by an Enterprise to its employees, and the Subject includes organization details as well as attributes of the 'sponsored' individuals. The Individual-validated S/MIME Certificate specifically verifies the ownership and control of personal email address as well as the true identity of person to which the email belongs. The Organization-validated S/MIME Certificate verifies the ownership and control of the organization email address as well as the true identity of the organization to which the email address belongs.

S/MlME Certificates are mainly used for digital signature and encryption of e-mails. They can not only ensure the identity authenticity of the email sender, but also ensure that the email content is not read or tampered by others during the email transmission procedure and is verified by the email recipient so as to ensure its integrity.

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 Industry and Information Technology, SHECA develops the Certification Practice Statement (CPS) and appoints a special body - SHECA Security Certification Committee as an agency of policy administration.

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

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

1.5.2 Contact Person

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

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

Tel : 86-21-36393197

Fax :86-21-36393200

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

Postal Code: 200080

E-mail: policy@sheca.com

1.5.3 CPS Decision in Line With Strategy Agency

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

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

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

1.5.4 Release of the Certification Practice Statement

The release methods of CPS include:

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

https://www.sheca.com/repository

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

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

1.5.5 The Change and Release of Certificate Practice Statement

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

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

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

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

1.5.6 CPS Approval Procedure

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

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

1.6. Definitions and Abbreviations

1.6.1 SHECA

Abbreviation for Shanghai Electronic Certification Authority Center Co., Ltd

1.6.2 UNTSH

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

1.6.3 SHECA Security Certification Committee

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

1.6.4 The Electronic Certification Service Agency

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

1.6.5 Registration Authority

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

service agency.

1.6.6 Registration Authority Terminal

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

1.6.7 System Administrator

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

1.6.8 Entry Clerk

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

1.6.9 Reviewer

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

1.6.10 Certificate Producer

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

1.6.11 Certificate

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

1.6.12 Digital Certificate

Digital certificate is used for identifying the signatory as a digital signature that indicates the signer has the recognized signature data. The certificate involved in 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，decrypting，electronic 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. 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: https://www.sheca.com/repository/ to visit SHECA repository, or other communication methods specified by the SHECA at any time. SHECA can issue subscriber certificates and associated CRL information outside the SHECA repository. CPS prohibits anyone except those persons authorized by SHECA from visiting any confidential information CPS and / or SHECA declared (or other data maintained by the issuing authority) in repository.

2.2. Publication of Certificate Information

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

2.2.1.Directory Services

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

2.2.2.The Release of Announcements and Notifications

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

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

2.3. The Time and Frequency of Releasing

2.3.1 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 https://www.sheca.com and publish the latest CPS on SHECA repository, and list together with the original CPS in order to retrieve.

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

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

2.3.2 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.

Once complete issurance,certificate will be published on the directory server ldap2.sheca.com, wich can be checked using specific tools. Users can also check and obtain a certificate by visiting https://www.sheca.com.

2.3.3 Time and Frequency of the CRL Publishing

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

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

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

SHECA should release Certificate Revocation List of a sub-CA certificate (ARL) at least once every 7 months. If the root certificate is revoked, revocation information is published on the website in time. The difference between of the Sub-CA certificate ARL nextUpdate time (nextUpdate) and this update time (thisUpdate) of the root/intermediate root certificate ARL must be less than or equal to 10 months. If the root/Intermediate Root certificate is revoked, SHECA will publish the revocation information on the website.

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

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

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

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

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

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

2.4. Repository Access Control

2.4.1 SSL Channel

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

2.4.2 Rights Management and Security Audit Channel

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

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

3. 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 unique identifiers that identifies the users following the regulation of X.509. Screening name is included in the subject of each certificate, and the user uniquely identify items is included in the certificate extension item, which uniquely identifies the certificate subscriber's identity.

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

3.1.2 Need for Names to be Meaningful

User identification information used for identifying name must be clear, traceable and certainly representative significance, that does not allow to appear anonymous or pseudo-names etc. However, in e-government applications of some special requirements, SHECA can not only specify a special name for the user according to certain regulation but also contact uniquely the special name with a certain entity (individual, organization or device). Any particular naming must be approved by SHECA Security Certification Committee.

3.1.3 Anonymity or Pseudonymity of Subscribers

SHECA does not accept or allow any anonymity or pseudonymity only to accept a clear sense of the name as a unique identifier, expressly stated in this CPS. SHECA may specify a special name for the user according to certain regulation, unless being in certain e-government special requirements applications, and SHECA can also contact the special name with an only certain entity (individual, organization or device). Any particular naming must be approved by SHECA Security Certification Committee.

3.1.4 Rules for Interpreting Various Name Forms

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

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

Detailed description of the DN may refer to the latest version of CA/B Forum baseline requirements and guidelines for different kinds of certificates.

3.1.5 Uniqueness of Names

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

3.1.6 The Processing of Name Dispute

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

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

3.1.7 Naming Agencies

Naming agencies, the SHECA naming authority coordinates all SHECA Relative Distinguished Names issuance. SHECA naming agencies determine the naming convention of subject name of

SHECA repository, which may be due to the difference between certificate categories and issuing authorities. These naming conventions vary for the difference between certification issuance and re-issue / re-registration certificates.

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

3.1.8 Recognition, Identification and Role of Trademark

The trademark information is allowed to be contained in subscriber's certificate, but can not be used for identifying individuals, organization or device. If the trademark is in the certificate information, subscriber should provide documentary proof for SHECA trademark registration party, and this requirement is not and should not be considered that SHECA will judge and decide the ownership of the trademark.

Any certificate applicants are prohibited from using names in their certificate applications that infringe upon the Intellectual Property Rights of others. SHECA does not verify or arbitrate whether a certificate applicant has intellectual property rights over the name appearing in a certificate application. SHECA does not resolve any dispute concerning the ownership of any domain name, trade name, trademark, or service mark, or ensure for the uniqueness of this right. SHECA is entitled, without liability to any certificate applicant, to reject or suspend any certificate application because of such dispute.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

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

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

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

3.2.2 Authentication of Organization and Domain Identity

SHECA has set up a procedure to verify the certificate applicant's identity, including but is not limited to verifying the user's identity documents, investigating through a public database and

verifying the user's postal address.

SHECA will firstly require the applicant to state for the authenticity of the submitted material, and the applicant bears the corresponding legal responsibility. SHECA will verify the material following the provisions of this CPS. SHECA may also take additional or extra methods for the verification.

If the applicant refuses the verification requirements of SHECA, then he or she will be deemed as forfeiting the qualification of certificate application. Meanwhile, SHECA states that it may refuse any application, and doesn't have an obligation for providing the reason.

3.2.2.1 Authentication of the Organization Identity

The authentication processes of organization identity are different as there are different types of certificates for application. SHECA can follow the corresponding requirements of each different certificate to validate, such as proving the validity of e-mail, quering credible database to verify the authenticity, distinguishing materials face to face and other methods applicants can obtain a clear identity information. The corresponding certificate application process sets different identification procedure. The signature of applicants themselves or the applicants who are fully authorized is in the certificate application form.

When applying for an organization certificate, the applicant shall designate the certificate application representative to endow lawful authority, and the certificate application representative signs on the application form express accepting the relevant provisions of the certificate application and undertakes the corresponding responsibility. SHECA and its certification services organization audit whether certificate applicant's representative meets the requirements.

The authentication of organizations as follows:

SHECA or registered institution, registration authority terminal and other certification services must examine documents submitted by applicants, and applicants are required to provide a valid certificate of the existence of the organization or server for SHECA, including but not limited to business license etc. The applicant has obligation to ensure that application materials are real and effective, and bears the related legal liability. SHECA shall determine that the organization exists by using at least one third party identity proofing service or database, or alternatively, organizational documentation issued by or filed with the applicable government agency or competent authority that confirms the existence of the organization. SHECA shall confirm by telephone or comparable procedure to the Certificate Applicant that the organization has authorized the Certificate Application, and that the person submitting the Certificate Application on behalf of the Certificate Applicant is authorized to do so. If SHECA can not get all the required information from a third-party, it may require a third-party to conduct an investigation or to require certificate applicants to provide additional information and evidence material.

If an applicant already hold an identity certificate issued by SHECA before apply for another one, SHECA and it's registry authorities can authenticate the identity of applicant by verifying the applicant's possession of the held identity certificate. Such as, using the identity certificate to log in the online service platform of SHECA.

When the domain name, device name or e-mail address is used as the contents of the certificate subject to apply for a certificate, it is also needed to verify reasonably whether the organization

has the right, such as querying a third-party databases and sending a confirmation e-mail and so on.

For batch application applied by one organization of organization identity certificates, which issue to internal departments, subsidiaries and other affiliates controlled by applicant, the organization shall serve as the only applicant.

Except the case of authentication by identity certificate issued by SHECA, applicant representative shall submit copy of ID card, batch application form with organization seal, and the information of subjects.

If the subject is an independent legal entity, and subject identity information is to include organization license number, the validation process avobe shall be followed, otherwise refet to <<Validation guideline for Individual and Organization Identity Certificate>> .

If SHECA or registered institution, receiving registration authority terminal or other certificate service organization has been identified in advance the identity of the certificate applicant, SHECA and its certification services organization can rely on evidence provided by the applicant.

This identification is usually conducted face to face. It is acceptable that the applicant sends the material for identification by post. However through such a way, SHECA will require the applicant to provide additional identification information and proof, and identify by the assisted way of the phone, a third-party surveying, postal address that a reasonable investigation SHECA considered.

SHECA and its authorized certificate services organization save all the organization application materials within the prescribed time, and the limit period is decided by the laws, policies, requirements of administrative department or SHECA itself.

If an organization applies staff certificates for its internal employees,organizations or other unincorporated organizations, The certificate holder's information entered in the certificate shall be subject to the content provided and by the organization， which has obligation to assure the application materials are real and effective. Staff certificates should only be used for identification within the organization.

For Sponsor-validated and Organization-validated S/MIME certificates, SHECA or RA shall collect and retain evidence supporting the following identity attributes for the Organization:

1. Formal name of the Legal Entity;
2. A registered Assumed Name for the Legal Entity (if included in the Subject);
3. An organizational unit of the Legal Entity (if included in the Subject);
4. An address of the Legal Entity (if included in the Subject);
5. Jurisdiction of Incorporation or Registration of the Legal Entity; and
6. Unique identifier and type of identifier for the Legal Entity.

SHECA or RA shall verify the full legal name and an address (if included in the Certificate Subject) of the Legal Entity Applicant using documentation provided by, or through communication with, at least one of the following:

1. A government agency in the jurisdiction of the Legal Entity’ s creation, existence, or

recognition;

2. A Legal Entity Identifier (LEI) data reference;

3. A site visit by the CA or a third party who is acting as an agent for the CA; or

4. An Attestation which includes a copy of supporting documentation used to establish the Applicant’s legal existence, such as a certificate of registration, articles of incorporation, operating agreement, statute, or regulatory act.

SHECA or RA may use the same documentation or communication described in 1 through 4 above to verify both the Applicant’s identity and address.

If an LEI data reference is used, SHECA or RA shall verify that the RegistrationStatus is ISSUED and the EntityStatus is ACTIVE. SHECA shall only allow use of an LEI if the ValidationSources entry is FULLY_CORROBORATED. An LEI shall not be used if ValidationSources entry is PARTIALLY_CORROBORATED, PENDING, or ENTITY_SUPPLIED_ONLY.

When SHECA uses third-party attestation letters to authenticate organization identities, SHECA has relevant controls to ensure:

1. This attestation letter is issued by a trusted third party;

2. A copy of documentation supporting the fact to be attested is attached to the attestation letter;

3. Realness of the attestation letter is confirmed through a trustworthy communication method.

3.2.2.2.Authentication of DBA/Tradename

Not applicable.

3.2.2.3.Verification of Country

If the certificate subject contains an option of country, SHECA shall verify the country using one or more of the following ways:

(1) Confirming the host country by checking the IP address displayed by the DNS record.

(2) The CCTLD of the requested domain name.

(3) Query government agencies or other trusted third-party data sources to confirm the country where the applicant's address is located through the methods in this CPS 3.2.2.1

SHECA SHOULD implement a process to screen proxy servers in order to prevent reliance upon IP addresses assigned in countries other than where the Applicant is actually located.

3.2.2.4.Domain Recognition and Identification

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

1. SHECA should confirm the requested domain name is not in the form of .onion. SSL

Certificate issuance for a domain name in the form of .onion is not allowed by SHECA;

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

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

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

(3) Confirming the Applicant's control over the FQDN by confirming the presence of a Random Value or Request Token for either in a DNS CNAME, TXT or CAA record for either 1) an Authorization Domain Name; or 2) an Authorization Domain Name that is prefixed with a Domain Label that begins with an underscore character. This method should be performed in accordance with BR Section 3.2.2.4.7;

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

(5) Confirming the Applicant's control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value. The Random Value MUST be sent to a DNS CAA Email Contact. The relevant CAA Resource Record Set MUST be found using the search algorithm defined in RFC 8659, Section 3. This method should be performed in accordance with BR Section 3.2.2.4.13;

(6) Confirming the Applicant's control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value. The Random Value MUST be sent to a DNS TXT Record Email Contact for the Authorization Domain Name selected to validate the FQDN. This method should be performed in accordance with BR Section 3.2.2.4.14;

(7) An Agreed - Upon Change to the Website by the Applicant placing an agreed-upon Request Token or Request Value in the "/.well - known/pki-validation" directory, performed in accordance with BR Section 3.2.2.4.18;

The request token or random value contained in the contents of a file should conform to:

a. The entire Request Token or Random Value MUST NOT appear in the request used to retrieve the file;

b. The CA MUST receive a successful HTTP response from the request (meaning a 2xx HTTP status code must be received).

The file containing the Request Token or Random Number:

a. is located on the Authorization Domain Name;

b. is located under the "/.well-known/pki-validation" directory

c. is retrieved via either the "http" or "https" scheme, and

d. MUST be accessed over an Authorized Port (80 or 443).

e. the HTTP response code for redirects must be 302, 307, 308, and redirect to a resource URL with "http" or "https". The number of redirects cannot exceed five times.

(8) Confirming the Applicant’s control over a FQDN by validating domain control of the FQDN using the ACME HTTP Challenge method defined in Section 8.3 of RFC 8555, performed in accordance with BR Section 3.2.2.4.19;

The request token or random value contained in the contents of a file should conform to:

a. The entire Request Token or Random Value MUST NOT appear in the request used to retrieve the file;

b. The CA MUST receive a successful HTTP response from the request (meaning a 2xx HTTP status code must be received).

The file containing the Request Token or Random Number:

a. is located on the Authorization Domain Name;

b. is located under the "/.well-known/pki-validation" directory

c. is retrieved via either the "http" or "https" scheme, and

d. MUST be accessed over an Authorized Port (80 or 443).

e. the HTTP response code for redirects must be 302, 307, 308, and redirect to a resource URL with "http" or "https". The number of redirects cannot exceed five times.

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

All of the above methods for validation, except No. 4 IP Address (BR Section 3.2.2.4.8) may be used for Wildcard Certificate Domain Name validation.

3.2.2.5 IP Address Recognition and Identification

According to the requirements of CA/Browser Forum, SHECA does not issue a certificate for a Reserved IP Address marked by IANA or non-routable internal domain names. SHECA shall confirm the applicant's ownership of or control over the IP address using one of the following authentication methods.

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

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

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

(1) Agreed-Upon Change to Website: confirming the Applicant’s control over the requested IP Address by confirming the presence of a Request Token or Random Value contained in the content of a file or webpage in the form of a meta tag under the “/.well-known/pki-validation” directory, performed in accordance with Baseline Requirements Section 3.2.2.5.1.

The request token or random value contained in the contents of a file should conform to:

a. The entire Request Token or Random Value MUST NOT appear in the request used to retrieve the file;

b. The CA MUST receive a successful HTTP response from the request (meaning a 2xx HTTP status code must be received).

The file containing the Request Token or Random Number:

a. is located on the Authorization Domain Name;

b. is located under the "/.well-known/pki-validation" directory

c. is retrieved via either the "http" or "https" scheme, and

d. MUST be accessed over an Authorized Port (80 or 443).

e. the HTTP response code for redirects must be 302, 307, 308, and redirect to a resource URL with "http" or "https". The number of redirects cannot exceed five times.

(2) Email, Fax, SMS, or Postal Mail to IP Address Contact: Confirming the Applicant’s control over the IP Address by sending a Random Value via email, fax, SMS, or postal mail and then receiving a confirming response utilizing the Random Value, performed in accordance with Baseline Requirements Section 3.2.2.5.2.

(3) Reverse Address Lookup: Confirming the Applicant’s control over the IP Address by obtaining a Domain Name associated with the IP Address through a reverse-IP lookup on the IP Address and then verifying control over the FQDN using a method permitted under Section 3.2.2.4., performed in accordance with Baseline Requirements Section 3.2.2.5.3.

(4) ACME method for IP Addresses: Confirming the Applicant’s control over the IP Address by validating domain control of the FQDN using the ACME HTTP Challenge method.

The request token or random value contained in the contents of a file should conform to:

a. The entire Request Token or Random Value MUST NOT appear in the request used to retrieve the file;

b. The CA MUST receive a successful HTTP response from the request (meaning a 2xx HTTP status code must be received).

The file containing the Request Token or Random Number:

a. is located on the Authorization Domain Name;

b. is located under the "/.well-known/pki-validation" directory

c. is retrieved via either the "http" or "https" scheme, and

d. MUST be accessed over an Authorized Port (80 or 443).

e. the HTTP response code for redirects must be 302, 307, 308, and redirect to a resource URL with "http" or "https". The number of redirects cannot exceed five times.

The random value used in the above validation methods remains valid for no more than 30 days from the time of creation.

3.2.2.6 Wildcard Domain Validation

In common circumstance, if a wildcard falls within the lable immediately to the left of a registry-controlled or public suffix, SHECA must refuse the issuance unless the applicant proves its rightful control of the entire Domain Namespace.

At the same time, SHECA should review section3.2.2.4 in this CPS to confirm that the domain name in the right position of the wildcard is in valid registration and is controlled by the applied organization.

If necessary, SHECA may take other methods for validating the ownership of the domain such as consulting a public suffix list （ http://publicsuffix.org/ ）maintained by Mozilla, during this process, the applicant has the obligation to provide assistance to SHECA.

3.2.2.7 Data Source Accuracy

Prior to using any data source as a Reliable Data Source, SHECA evaluates the source for its reliability, accuracy, and resistance to alteration or falsification. That is SHECA will consider the following during its evaluation:

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

Data source of SSL certificates, if obtained no more than 398 days, can be revalidated.

For S/MIME certificates, SHECA may reuse completed validations and/or supporting evidence performed in accordance within the following limits: Completed validation of mailbox authorization or control shall be obtained no more than 398 days prior to issuing the certificate. Completed validation of organization identity or individual identity shall be obtained no more than 825 days prior to issuing the certificate.

3.2.2.8 Certification Authority Authorization(CAA)

For the SSL certificates, SHECA will do CAA record check based on RFC 8649 for each dNSName in the subject alias extension of the certificate before the certificate is issued. For the SMIME certificates, SHECA will do CAA record check based on RFC 9495 for each Mailbox Address prior to issuing a certificate that includes a Mailbox Address.

SHECA will issue the certificate to the certificate applicant within 8 hours of checking the CAA record. If more than 8 hours have elapsed, SHECA will conduct a new CAA check.

The SHECA shall process the property tags of"issue","issuewild","issuemail" and "iodef" as specified in RFC 8659 and RFC 9495: if the "issue","issuewild" ,"issuemail" tags exist and do not contain “sheca.com”，the CA will not issue the corresponding certificate if the iodef tag appears in the CAA record, the CA will communicate with the applicant and then decide whether to issue the certificate.The CA is permitted to treat a record lookup failure as permission to issue if：

1) The failure is outside the SHECA's infrastructure:

2) The lookup has been retried at least once,

3) the domain's zone does not have a DNSSEC validation chain to the ICANN root.

The CA documents potential issuance that was prevented by CAA record in sufficient detail to provide feedback to the CA/Browser forum on the circumstances.

3.2.2.9 Validation of Mailbox Authorization or Control

This section defines the permitted processes and procedures for confirming the Applicant’ s control of Mailbox Addresses to be included in issued Certificates. SHECA verifies that Applicant controls the email accounts associated with all Mailbox Fields referenced in the Certificate or has been authorized by the email account holder to act on the account holder’ s behalf. SHECA does not delegate the verification of mailbox authorization or control.

SHECA’ s CP/CPS specifies the procedures that SHECA employs to perform this verification. SHECA maintains a record of which validation method, including the relevant version number from the TLS Baseline Requirements or S/MIME Baseline Requirements, was used to validate every domain or email address in issued Certificates.

Completed validations of Applicant authority MAY be valid for the issuance of multiple Certificates over time. In all cases, the validation SHALL have been initiated within the time period specified in the relevant requirement (such as Section 4.2.1) prior to Certificate issuance.

Note: Mailbox Fields MAY be listed in Subscriber Certificates using rfc822Name or otherNames of type id-on-SmtpUTF8Mailbox in the subjectAltName extension. Mailbox Fields MAY be listed in Subordinate CA Certificates via rfc822Name in permittedSubtrees within the nameConstraints extension.

For all S/MIME certificates, authentication of the Applicant’ s ownership or control of all requested mailbox SHECA uses one of the following methods:

- Validating authority over mailbox via domain

SHECA confirms the Applicant has been authorized by the email account holder to act on the account holder’s behalf by verifying the entity’s control over the domain portion of the Mailbox Address to be used in the Certificate. For purposes of domain validation, the term Applicant includes the Applicant’s Parent Company, Subsidiary Company, or Affiliate. SHECA uses only the approved methods in Section 3.2.2.4 of the TLS Baseline Requirements to perform this verification.

- Validating control over mailbox via email

SHECA confirms the Applicant’s control over each Mailbox Field to be included in a Certificate by sending a Random Value via email and then receiving a confirming response utilizing the Random Value.

The verification process is as below,

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

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

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

Control over each Mailbox Address is confirmed using a unique Random Value. The Random Value is sent only to the email address being validated and not shared in any other way.

The Random Value is unique in each email. The Random Value remains valid for use in a confirming response for no more than 24 hours from its creation. SHECA specifies a shorter validity period for Random Values in its CP and/or CPS.

The Random Value is reset upon each instance of the email sent by SHECA to a Mailbox Address, however all relevant Random Values sent to that Mailbox Address remain valid for use in a confirming response within the validity period described in this Section. In addition, the Random Value are reset upon first use by the user if intended for additional use as an authentication factor following the Mailbox Address verification.

- Validating applicant as operator of associated mail server(s)

SHECA does not support this validation method.

3.2.3 Authentication of Individual Identify

Authentication of individual identity differs according to the types of certificates applied. SHECA can validate information follow the corresponding requirements for each different certificate, such as by proving the validity of e-mail, querying credible database to verify the authenticity, distinguishing materials face to face and other ways that applicants can obtain a clear identity information. The process of the corresponding certificate application provides a different authentication procedure. The signature of applicants themselves or the applicants who are fully authorized is in the certificate application form.

1. Prove the validity of e-mail. Review and identify the real existence of the certificate holder's

e-mail address to identify and distinguish individual identity.

2. Query the credible information database. Check and confirm necessary personal characteristics in the credibility database to identify personal identification. The Credible database was chosen and decided by the SHECA, including existing SHECA database and other third-party database.

3. Face-to-face identification. Individual applicant's identification and authentication can be conducted by one of the following methods:

SHECA and its authorized certificate service organization will compare the applicants themselves with two of Identification (original and copy). Identification must be a valid identity card or passport document.

If SHECA or registration authority terminal has clearly confirmed the identity of individual applicants, SHECA or its authorized certificate services organization can trust the existing certificate.

4. SHECA can also obtain information from a third-party to verify the identity of the individual applicant. If SHECA can not get all the required information from a third-party, it may require a third-party to conduct an investigation or to require certificate applicants to provide additional information and evidence material.

5. SHECA also supports the way through the post as identification. But for this way, SHECA will require the applicant to provide additional identification information and proof, and identify by the assisted way of the phone, a third-party surveying, postal address that a reasonable investigation SHECA considered.

6. For an application in the name of an individual identity, it also need to submit proof of its organization material .

7. When the domain name, device name or e-mail address is used as the contents of the certificate subject to apply for a certificate, you also need to verify reasonably whether the applicant has the right, such as request for domain ownership documents, ownership certificate, querying a third-party databases and sending a confirmation e-mail and so on.

8. For internal organiztion-individual certificates, which are only used within the organization, the organization shall apply as the only applicants while the final users are staffs.

9.If an applicant already hold an identity certificate issued by SHECA before apply for another one, SHECA and it’s registry authorities can authenticate the identity of applicant by verifying the applicant’s possesion of the held identity certificate. Such as, using the identity certificate to log in the online service platform of SHECA.

Except method no.9, applicant representative shall submit copy of his/her ID card, batch application form with organization seal, and the information of individual identity. If the individual identity information is to include ID number, the validation process for Individual Identity Certificate shall be followed, otherwise refet to <<Validation guideline for Individual and Organization Identity Certificate>>.

Applicant must bear the responsibility for the authenticity of materials. SHECA and its authorized certificate services organization after a limited audit according to the law ,which does not bear the applicant's identity document (such as ID cards, etc.) to identify the obligation of the legality.

SHECA and its authorized certificate services organization save the detail information for certificate holders which is filled out in the application form.

For SV and IV S/MIME certificates, SHECA, RA, or Enterprise RA shall collect and retain evidence supporting the following identity attributes for the Individual Applicant:

1. Given name(s) and surname(s), which SHALL be current names;
2. Title (if used);
3. Address (if displayed in Subject); and
4. Further information as needed to uniquely identify the Applicant.

Pseudonym is not accepted by SHECA for individual identity validation. SHECA shall comply with applicable data protection legislation in the gathering and retention of evidence relating to Individual identity supporting this Requirement in accordance with S/MIME BR Section 9.4.

SHECA shall obtain consent to collect personal information (privacy statement consent) during the S/MIME individual validation certificate issuance process.

3.2.4 Non-Verified Subscriber information

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

3.2.5 Validation of Authority

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

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

3.2.6 Criteria for Interoperation

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

Other certification services organization can interoperate with SHECA of non-UNTSH certification services system. But the CPS of certificate services organization must meet the requirements of UNTSH CP, and certificate services organization may sign the corresponding agreement with SHECA. SHECA will accept the information identified by the certifying authority

of non-SHECA and issue the corresponding certificate based on content of the agreement. If there is no similar agreement between the two parties, SHECA will decide whether to accept the reviewed material with specific conditions and make a decision whether to accept.

If there are provisions of national laws and regulations, SHECA will perform strictly

3.3 Identification and Authentication of Re-key Requests

Prior to the expiration of an existing subscriber's certificate, it is necessary for the subscriber to obtain a new certificate to maintain continuity of certificate usage. After the key expires, the user can choose to update (re-generate a pair of public key and private key), and apply to issuing authority for re-issue certificate, which is called the certificate re-key. Subscribers can also choose to retain the original key, and to apply to issue organization for a new certificate. Subscribers may request a new certificate for an existing key pair (technically defined as “renewal”).

Generally speaking, both "Rekey" and "Renewal" are commonly described as "Certificate Renewal", focusing on the fact that the old certificate is being replaced with a new certificate and not emphasizing whether or not a new key pair is generated. In addition to some possible specific applications, whether the certificate renewal generates new key pair is not usually the key point. But SHECA usually requires subscribers to use the new key pair when certificate is renewed. When subscribers concern the key's security, they must re-register, and generate a new key pair and apply to issue authority for a new certificate. In this case, the subscriber will not be allowed to use the old key pair in order to consider risk management and security when re-applying for a certificate.

If the certificate information related changes, subscribers can choose to keep the original key or new key to re-issue certificate. If subscribers choose to retain the original key pair, subscribers need to ensure that its key pair is safe.

If there are provisions of national laws and regulations about key management and renewal, SHECA will perform strictly.

3.3.1 Identification and Authentication of Routine Re-key

Routine re-key procedures ensure that t subscribers can use the existing private key to sign the requests for updating. Issuing authority will authenticate and identify the accuracy, legitimacy, uniqueness of user request information contained, the users signature and public key.

Identification and authentication of routine re-key including:

- Subscribers sign the application information, and CA verifies the signature with its original certificate's public key.
- If subscriber registration information has not changed, CA issues a new certificate based on subscriber original registration information.

Subscribers can also choose the initial certificate application process to re-key conventionally, submit the appropriate certificate in accordance with requirements of the application and identification information. In any case, the means of initial identification can be used for identifying means of the re-key processing.

If there are provisions of national laws and regulations about key management and renewal, SHECA will perform strictly.

3.3.2 Identification and Authentication for Re-key After Revocation

Re-key/renewal after revocation is not permitted. Subscribers must re-identify and re-register, and generate a new key pair to apply to re-issuance a certificate for SHECA.

3.4 Identification and Authentication for Revocation Requests

SHECA and its authorized certificate services agency need to verify identification on-site for revocation request of certificates. Subscribers need to submit the same material, certificate and private key with applying for certificate to SHECA and its authorized certificate services agency.

SHECA will verify identification for the identity of the applicant by reasonable means, such as by telephone, mail, and other third-party proof, if not on-site auditing because of constraints,

If the judiciary proposes revocation according to the law, SHECA directly regards judiciary written revocation request as the basis on identification documents, not to conduct other forms of identification.

SHECA ensure that the identification of the revocation request will undergo reasonably.

3.5 Identification and Authentication of Authorized Service Organization

For the various certificate service agencies who are authorized to join in, including registry RA and RAT, SHECA assigns a unique number and the operation authority and manages the number.

SHECA issues a digital certificate for each RA as the unique identity of RA in the certificate system. CA identities the identification of RA based on RA's signature in order to determine whether the institution is recognized by SHECA, what authority and whether it accepted all kinds of service requests and service information SHECA uploading.

SHECA issues a digital certificate for the operator of each perspective center and service registration authority terminal, and the operator of the same perspective center and service registration authority terminal is assigned to an operation group. The operation group number is the number of perspective center and service registration authority terminal. CA (including the RA) identifies identification according to the signature of the perspective center and service registration authority terminal to determine whether the perspective center and registration authority terminal is accredited by SHECA, what authority , and whether it accepted all kinds of service requests and service information SHECA uploading.

4. Operational Requirements of Certification Life Cycle

The whole process of certification life cycle according to the announced CPS is introduced under the SHECA certification system, which including the implementation of the certificate application, issuance, management, updating, revocation etc. Each party's responsibilities and obligations are also elaborated involved during the process.

In order to meet the users' need for electronic signature and other network security services technology, SHECA digital certificates can support secure e-commerce, secure e-government and other general secure services. To this end, as the trusted third-party, SHECA and its authorized issuing authority complete all the process of certificate service to meet the numerous, open, widely distributed users on a variety of communications and information security needs.

4.1 Certification Application

SHECA accepts two modes of certificate application, the offline and online. According to the certificate type of the applications, SHECA takes different application registration process, but the steps requested by certificate application operation should be complied.

4.1.1 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.

4.1.2 Certificate Type

Currently, SHECA provides two types of certificate which include formal certificate and test certificate.

4.1.2.1 Test Certificate

Test certificate is made by registration authority terminal of SHECA. SHECA does not assume any responsibility for the validity of the certificate. Test certificate is only for users testing. SHECA recommends that subscribers do not use any test certificate to prove their true identity in order to avoid unnecessary losses and disputes.

SHECA does not save or publish the information filled out in test certificate application, nor assuming any liability arise from information leakage.

SHECA has strict requirements on the test certificate. Its user name must be in English "test" or Chinese "测试" at the beginning, and the expiration date sets in 3 months.

SHECA do not issue SSL test certificates for customers.

4.1.2.2 Formal Certificate

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

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

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

applied in English.

1. Personal Certificate

(A) Personal certificate---SHECA personal certificate is signed by SHECA containing personally identifiable information and personal public key file, which format follows international standard of the x.509. Personal certificate is used to sign the certificate holder during the exchange of information, electronic signatures, e-government, e-commerce and other Internet activities and guarantee security and integrity of information in the transmission which can be stored in the hard drive, USB Key, IC card and other medium.

Applicants applying for personal certificate, required to submit the following information:

- A written application form filled out and signed by applicants as required
- Personal ID card (or Military ID, passport or student card or other valid identification documents) and a copy of the original; if SHECA and registration authority terminal verify the identity of individual applicants by phone, mail, third-party, or other means expressly confirm, applicants can submit copies of identification documents, identity documents by fax, mail, etc. without submitting the originals.
- If it is entrusted to handle, it is required to submit the applicant and the client's documents, and copies of the above, and a written authorization signed by the client who applies for a certificate.

(B) Personal E-mail certificate---personal email certificate is used to encrypt and sign operations in personal communication of important contents by the e-mail .With a certificate to encrypt e-mail content and attachments, only the designated recipient can read the message, which can ensure that the message in transit will not be stolen and tampered. E-mail signed with a certificate is not tampered during transmission, and the receiver may confirm the message sender, which ensures non-repudiation of messages.

Applicants applying for personal E-mail certificate, required to submit the following information:

- Applicants fill in and sign a written application form (in triplicate)
- Original personal ID card (or military ID, student ID, passport, etc.)
- A copy of personal ID card (or military ID, student ID, passport, etc.)
- If it is entrusted to handle, it is required to submit the applicant and the client's documents, and copies of the above, and a written authorization signed by the client who applies for a certificate.
- SHECA confirm subscriber’s e-mail address by requiring the subscriber to be able to answer a challenge-response e-mail to that address. As a means of verifying whether the applicant control the E-mail, the verification message include arithmetical operation, question about the user identity information etc. Applicant should reply to the email within the prescribed period. SHECA decide whether to issue a certificate to the applicant in accordance with the e-mail reply.

2. Organization certificate

(A) Organization Identity certificate---- SHECA organization Identity certificate is signed by

SHECA containing organization identity information, which stands for the holders of organization during the exchange of information, electronic signatures, e-government, e-commerce and other Internet activities status, awarded to enterprises, government departments, community groups and other organizations. Certificate can be stored in the hard drive, USB Key, IC card and other types of medium.

When applying for organization identity certificate, the following information should be required:

- Applicants fill in , sign and seal a written application form
- The original and photocopy of applicant's valid certificate (business license or other valid documents recognized by national laws) with official seal; If SHECA or RA have already confirmed the identity of applicant through phone, post, third-party verification or other means, the applicant may only submit a photocopy of the supporting documents by fax, post or other means without original documents.
- A copy and the original of identity card (or military ID, student ID, passport and other valid documents) of entrusted applicant representative.

(B) Organization E-mail certificate---SHECA organization Email certificate is signed by SHECA for marking unit E-mail identity of a certificate holder .Certificate holder encrypts and signs operations on the contents of the letter by e-mail .

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 398 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.

4.1.3 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 server.

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 https://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 responsibilities to identify reasonably for applicant identity. For security and audit requirements, the certificate application form should be recorded the name, signature, date of verification and validation results of identifier.

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

- Verify that the certificate applicant has accepted the terms of the subscriber agreement.
- According to the type of certificate applied by applicant, verify the identity of the applicant in accordance with the different types of certificate authentication.
- Confirm the certificate applicant is the legal owner of private key that matching with the public key contained in the certificate (adopt different recognition methods according to different types of certificate, such as ask subscriber to guarantee, etc.).
- Confirm the information contained in the certificate is accurate except unauthenticated subscriber information.
- Confirm any trustee applying for a certificate in behalf of their organizations, and has been represented by the organization's legal authority.
- Confirm legitimacy and authority of the identity of the consignor and the consignee.

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

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

SHECA retains the right to update identification procedures and requirements. The identification procedures and requirements renewed will be published on https://www.sheca.com , and you can

also obtain it via the following address:

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

Shanghai Electronic Certificate Authority Center Co., Ltd.

SHECA Customer Service Center

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

4.2.2 Certificate Approval and Rejection

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

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

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

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

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

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

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

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

The certificate applicant who is rejected could then apply again.

SHECA perform CAA (Certificate Authority Authorization) Record Check in issuance process, and remain record in authentication checklist, based on RFC 8659 (for TLS certificates) and RFC 9495 (for S/MIME certificates). If the S/MIME Certificate includes more than one Mailbox Address, then SHECA SHALL perform the above procedure for each Mailbox Address.

SHECA accepts the following CAA record: sheca.com

When the CAA record is set as sheca.com then it takes the following form:

- standard SSL certificates: domain.name IN CAA 0 issue “sheca.com”
- wildcard SSL certificates: domain.name IN CAA 0 issuewild “sheca.com”
- S/MIME certificates: domain.name IN CAA 0 issuemail “sheca.com”

4.2.3 Time of Processing the Certificate Application

SHECA will identify and review the certificate information submitted by the applicant and make a decision for approval or rejection in 7 working days.

4.3 Certificate Issuance

4.3.1 Issuing the Certificate

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

When the issuing authority approves the certificate request, it will issue a certificate by means of HTTP and LDAP for subscriber. The release of certificate means SHECA formally approved the final certification application.

4.3.1.1 Manual authorization of certificate issuance for Root CAs

Certificate issuance by the Root CA SHALL require an individual authorized by SHECA (i.e. the

CA system operator, system officer, or PKI administrator) to deliberately issue a direct command in order for the Root CA to perform a certificate signing operation.

4.3.1.2 Linting of to-be-signed Certificate content

For SSL certificates, due to the complexity involved in implementing Certificate Profiles that conform to these Requirements, it is considered best practice for the CA to implement a Linting process to test the technical conformity of each to-be-signed artifact prior to signing it. When a Precertificate has undergone Linting, it is not necessary for the corresponding to-be-signed Certificate to also undergo Linting, provided that SHECA has a technical control to verify that the to-be-signed Certificate corresponds to the to-be-signed Precertificate in the manner described by RFC 6962, Section 3.2. Effective 2024-09-15, SHECA SHOULD implement such a Linting process. Effective 2025-03-15, SHECA SHALL implement such a Linting process.

Methods used to produce a certificate containing the to-be-signed Certificate content include, but are not limited to:

1. Sign the tbsCertificate with a "dummy" Private Key whose Public Key component is not certified by a Certificate that chains to a publicly-trusted CA Certificate; or

2. Specify a static value for the signature field of the Certificate ASN.1 SEQUENCE.

SHECA may implement its own certificate Linting tools. SHECA uses the Linting tools that have been widely adopted by the industry (see https://cabforum.org/resources/tools/).

4.3.1.3 Linting of issued Certificates

SHECA uses a Linting process to test each issued SSL Certificate.

4.3.2 The Behavior of Electronic Certification Service Agencies and Registered Agencies When Issuing the Certificate

When the certificate application is approved, the applicant will receive a marked items that containing the application password, referred to application password (such as passwords or password card envelopes, bar codes, encrypted digital streams, etc.) to ensure apply for a certificate safely.

SHECA and its authorized service agencies will issue the password to the applicant, which fully meets the following conditions:

- Comply with application procedures of SHECA certificate;
- Pay a certificate fee according to the regulation;
- SHECA and its authorized service agencies have approved the application;

The registered agencies have accomplished the registration of applications and operation of certificate in accordance with this CPS and SHECA relevant operation agreement, and send the licensing information and user data to the certification agencies.

After the certificate agencies receive application information and verify the legitimacy of the applicant's identity and the integrity, validity and reliability of the certificate application information, if they are all correct, then the applicant will be issued the certificate.

If the applicant applies for a signed certificate, then:

1、 The applicant sends to SHECA a public key. SHECA will establish a secure channel with the applicant through the network, and the applicant upload the public key to CA agencies. SHECA supports PKCS10 standard certificate request.

2、SHECA confirm the authenticity of the certificate requesting. SHECA issues the corresponding certificates, once confirmed.

If the certificate applicant applies for encryption certificate, then:

1、When the applicant applies for a signing certificate, he or she can also apply for encryption certificate simultaneously.

2、When SHECA receives the request of applying for encryption certificate, SHECA will obtain encryption key pairs from the corresponding national key management ,and issue the certificate to the user.

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

4.3.3 Notification of Electronic Authentication Services and Registry to Subscribers

The way of sending password can be divided into the following ways, according to SHECA different application objects:

1、Notify the applicant face to face(such as the applicant gets certificate from RAT, etc.);

2、 Notify via e-mail;

3、 Notify via postal letters;

4、 Notice via the confirmed safety channel ;

5、 Other safe and practical manner SHECA considered.

SHECA does not have the obligations of installing the certificate on-site for users .If the applicant needs, SHECA can go to install but need to charge the appropriate services. SHECA and its authorized service agencies support hotline services. Hotline telephone and mail is announced by SHECA and its authorized service agencies.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

When the applicant completes the application process, and SHECA and its authorized service agencies deliver the certificate, a way to obtain the certificate, or the password associated with the certificate to the applicant, which means that the applicant accepts the certificate. After subscribers receive digital certificate, the private key should be kept properly with the corresponding certification.

The following acts are considered that subscribers receive a certificate:

- Subscribers have received a medium containing certificate
- Subscribers download or install the certificate to a local storage medium through the network , such as the local PC, IC card, USB Key, mobile hard drive or other removable storage medium
- Subscribers receive a way of obtaining certificate , and do not object certificate or the contents of the certificate
- Subscribers object certificate or content of certificate operation failure

4.4.2 Publication of the Certificate by the CA

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

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

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

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

After the subscriber accepts certificate, SHECA will not specifically notice to the registrar, registration authority terminal, the competent departments and other entities , and these entities can obtain subscriber's certificates and related information by quering the directory service or SHECA database .

4.5 The Key Pair and Certificate Usage

4.5.1 The Subscriber Private Key and Certificate Usage

The subscribers use their certificates and the corresponding private key, only the subscribers agree

and accept the subscriber's agreement requirements (for example, sign a subscriber agreement). The certificate can be used only based on the CPS and the relevant provisions of the CP. Subscribers can only use the private key and certificate in the proper range of applications which is consistent with the contents of the certificate (if the usage and purpose of the certificate is defined in some fields, this certificate will be used only in this range, such as key usage). All acts must be consistent with the requirements of the subscriber agreement.

When the subscribers use the certificate, they must keep and store the private key associated with the certificate in order to avoid the loss, disclosure, alteration, or embezzled. Any person who uses the certificate must check the validity of the certificate, including whether the certificate is revoked, expiration and it is issued by the right authority and so on.

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

The certificate issued by SHECA only indicates that certificate holders who apply for a certificate identity, and verifies the signature made by private key corresponding certificate holder the public key .Thus, by signing and verifying signature, SHECA can ensure the authenticity of the certificate holder's identity, the integrity of information and the information non-repudiation etc. If the certificate holder uses the certificate for any other purposes, SHECA will not bear any responsibilities and obligations arising therefrom.

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

4.5.2 The Relying Party Public Key and Certificate Usage

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

- Whether the certificate issued by a trusted CA
- For any given purpose, the certificate is used appropriately; whether the certificate is used against the CP, CPS or the relevant laws and regulations. SHECA and RA are not responsible and can not assess whether the subscriber certificate is used appropriately.
- When the certificate is used whether it is consistent with the content included (if the usage and the purpose of the certificate is defined , this certificate will only be allowed to use within this range, such as key usage)
- Checking the certificate status of all certificates and certificate chain, whether it is in the period, or it has been revoked. If the subscriber certificate or any certificate of the certificate chain has been revoked, the relying party must know whether the signature is made before revoked

Unless provided in this CPS, certificate from the issuing authority is not any commitment of

power or privilege. The relying party only trusts certificate and the public key contained in the certificate within the limits prescribed in this CPS and makes this decision.

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

4.5.3 Signature and Verification

Signature can only be created under the following situations:

- Created in certificate valid period
- The signature is verified exactly through the chain of certificates
- Relying party doesn't find or noticed the behavior contrary to the CPS requirements
- Relying party complies with all provisions of the CPS

The usage of certificates does not mean that subscriber can act on any individual interests or have the rights to take any special action. Certification can be indicated only that the subscriber's identity and the subscriber's signature is verified.

The signature verification confirms that the signature is created by the signer's private key corresponding to private key contained in the certification, and after the signature is created, the information of the signature has not been changed.

This validation will be conducted by the way of CPS prescribed, and authentications are as follows:

1、Confirmed the certificate chain of the signature verification - to verify the signature firstly you should confirm that the selected certificate chain is the best match with the digital signature certificate chain. There are possibly more than one valid certificate chain (eg:cross validation),from a given certificate to an acceptable root certificate. If there are multiple certificate chains between the acceptable root certificates, the person who selects or confirms the signature certificate chain may have different choices. In this case, the person who verifies the digital signature has better make the choice for the end of the "higher trust level" of a CA or an end in the root certificate chain of SHECA.

2、Checking SHECA or other agencies repository to view the certificate of certificate chain whether it is revoked. Certificate may be revoked and is no longer valid， during the signature created period ,. You can check the revocation status or view the latest certificate chain provided in the Certificate Revocation List (CRL) to verify the certificate status.

3、When the signature is verified, the range of a signed message should be determined and you should know exactly what data has been signed.

4、Determine the scope and the purpose of the signer. Issuing authority may limit to the use of private key which is corresponding with its issued certification. These limitations will be accompanied by a certificate or displayed in the reference information of the certificate, and as a warning to the recipient that in some cases it is unreasonable to trust the certificate. The warning and restrictions of certificate was checked to ensure the rational use of the certificate.

SHECA solemnly points out:

- If the relying party trusts the signature which can not be verified, then all risks should be borne by themselves.
- And relying parties don't have the right to make any assumptions about the digital signature whether it is valid.
- This means that any reliance on the signature must be judged reasonably and properly.
- Under the following conditions, the receiving party who received the information by subscriber's signature can trust subscriber's bound signature:
- Signature is created by the legal validity of the certificate use and the signature can be verified through a valid certificate chain.
- The relying party trusts the digital signature reasonably. If you need additional guarantee to trust the signatures, the relying party must obtain these assurances then trust the signature reasonably.
- Of course, whether to trust the final decision of verified signature will be verified independently by the authenticator.

4.6 Certificate Renewal

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

For individual or institution identity certificate, when certificate renewal, the subscriber no longer needs to submit a certificate registration information, only submits sufficient information which can identify the original certificate, such as subscriber distinguished name, certificate serial number, etc. Using the private key of the original certificate signature for the renewal application information containing of the public key. To ensure that the certificate and key are safe and reliable, SHECA sets for the validity period of the certificate issuance, usually one year. Before the expiry date of the certificate and whithin 3 months after expiry, the certificate subscribers can choose to retain the original key to update the certificate by issuing authority. Subscribers must ensure that the private key held by them is safe and reliable.

For SSL certificate and code signing certificate, SHECA perform identification and authentication process of new application for renewal request, please refer to section 3.2 for details.

4.6.1 The Situation of Certificate Renewal

Prior to the expiration of an existing subscriber's certificate, SHECA will make reasonable efforts to send a certificate renewal prompt to the certificate subscriber or certificate application trustee, suppliers or agents. Reasonable efforts including but not limited, site prompts, the system prompts, writing prompts, E-mail notification or other means, but SHECA and its authorized service agencies take any of the above methods of hints or notices which may be reasonable efforts.

Effective data of user certificate issued by SHECA is from the time when the certificate is issued. SHECA will send certificate holders the renewal notice or the appropriate information, a month

before the expiry of the certificate.

Meanwhile, SHECA also accepts update requests made by subscribers, and do some update processing for their certifications.

4.6.2 Who May Request Renewal

All subscribers hold certificates issued by SHECA , including individuals, enterprises, institutions, government agencies, social organizations, people's organizations and other organizations, etc., they all can request to update their various types of certificates, before the validity of the certificate is about to expire.

4.6.3 Processing Certificate Renewal Requests

SHECA and its authorized service agencies provide two means, online and offline renewal. Certificate holder can choose the appropriate update strategy. For certificate renewal, SHECA need ensure that the person requesting the certificate update is the subscriber. When SHECA issues new certificate, the applicant can be asked to update the original private key or use the same process of issuing the initial certificate to identify. Usually, when the certificate is updated, subscribers can use the existing private key to sign the update request, and the issuing authority will verify and identify the signature and public key of the user, user information contained certificate renewal requests correctly, legally, uniquely:

- Subscriber signs the application information, and CA verifies signature by the original certification public key
- Subscriber's registration information has not changed, and CA issues a new certificate based on their original registration information

When updating the certificate online, the subscribers must fill out the update request, and in accordance with SHECA and its authorized certification service requirements, sign the update request information with the current private key and submit to the issuing authority. After the issuing authority receives update requests, it issues a new certificate, when the identity and request information of the applicant are confirmed.

When updating the certificate offline, the subscriber can give update request to SHECA and its authorized service agencies in accordance with the original application process. Issuing authority will identify and verify certificate renewal application in accordance with the original application process .Certifying authority will issue a new certificate after it has recognized and approved the update application.

4.6.4 Notification of New Certificate Issuance to Subscriber

Before subscribers update certificates, they should ensure that the upcoming key is safe and reliable. Once this reliability can not be confirmed, SHECA and its authorized service agencies recommend subscribers to directly select the certificate key updating.

4.6.5 The Behavior Constitutes Acceptance of the Certificate

Renewal

When the updating requests online or offline submitted by subscribers are approved , SHECA and its authorized service agencies deliver the certificate or the way of obtaining the certificate, or the password associated with the certificates to the subscriber, which means the subscriber has accepted the certificate . When the subscribers receive digital certificate, private key should be kept safely.

4.6.6 Publication of the Renewal Certificate by the CA

Once the subscriber accepts the certificate renewal , SHECA will issue copies of the certificate in its repository, directory services and other one or more repository decided by the SHECA . Subscribers can also publish their certificates in other place.

After new certificates are issued, SHECA and its authorized service agencies can revoke the old certificate according to subscribers' requirements.

4.6.7 The Notices From Electronic Certification Authority to Other Entities

After subscribers receive updated certificate, SHECA will not notice the registration agencies, registration authority terminal, competent departments and other entities, which can obtain subscribers' updated certificate and related information by querying the directory service or SHECA information repository.

4.7 Certificate Key Renewal

When the subscriber or other participants need to generate a new key and issue the new certificate for new public key, the user can select the certificate key renewal service. For some security reasons, SHECA recommends subscribers update key at the same time while updating certificate

After the expiration of the certificate, when the certificate key is updated, the subscriber needn't submit the registration certificate, and submit sufficient information that can identify the original certificate, such as subscriber's distinguished name, certificate serial number, the certificate key renewal signature of the original certificate's corresponding private key, and send a new public key for applying a new certificate.

For SSL certificate and code signing certificate, the application process is the same as new application, please refer to section 4.1, identification and authentication process of new application , please refer to section 3.2.

4.7.1 Circumstances for Certificate Re-Key

If the following circumstances happen, the subscriber must select the certificate key renewal:

- Certificate expires and the key also expires

- Certificate key pair has been leaded, stolen, tampered or safely is not exit for other reason
- After the certificate is revoked , a new certificate is needed

In addition, any certificates under the SHECA structure, including RA, certificate operators, etc., must be updated after the expiration of the certificate key.

Subscriber whose certificate is about to expire, should update the certificate key to obtain a new certificate for security reasons.

4.7.2 Who May Request Certification of a New Public Key

All subscribers hold certificates issued by SHECA, including individuals, enterprises, institutions, government agencies, social organizations, people's organizations and other organizations, etc. may request a certificate key update service.

4.7.3 Certificate Key Update Request Processing

SHECA and its authorized service agencies provide online and offline update means. Usually, when the certificate key is updated, subscribers can submit the related information of original certificate, such as the certificate distinguished name, certificate serial number, the certificate key renewal signature of the original certificate's corresponding private key to identify their status. Issuing authority will verify and identify the user information of the user's renewal request correctly, legally and uniquely. Including:

- Subscribers submit information to verify their identity ,then CA identifies it
- Subscribers sign to the certificate key renewal request by the original certificate corresponding private key , and CA verifies their signature
- Subscriber registration information doesn't change, then CA issues a new certificate based on their original registration information.

Online updating the certificate----The subscriber must fill out the online renewal request , and sign the update request information of the new generated public key by the current private key, in accordance with SHECA and its authorized certification service requirements, then submit it to the issuing authority . After SHECA and its authorized service agencies receive the certificate key update request and identify the identity of the applicant and request information, they issue new certificate for the applicant. The certificate's public key is a new public key submitted by the applicant.

Offline updating the certificate----The subscriber submits certificate renewal request to SHECA and its authorized service agencies in accordance with the original application process, and submit public key newly generated. SHECA and its authorized service agencies identify and verify certificate renewal application in accordance with the certificate application process. After issuing authority recognize and approve the update application, they issue a new certificate for the applicant, and certificate public key is new public key submitted by the applicant.

4.7.4 Notification of Updating the Certificate key

When subscribers select the certificate key update, encrypted information and data to be updated

certificate should be proper treated (such as backup certificate and key to be updated, or using an existing certificate encrypted file to decrypt t, and reasonable disposition subscriber thought), then the certificate can be updated.

If the subscriber does not properly handle the certificate but update key directly may result in the original encrypted information and data that can not be decrypted. SHECA will not bear any responsibility for the result of the possible loss.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

After subscribers' certificate key updating request submitting or a certificate offline key updating request submitting is approved, SHECA and its authorized service agencies delivered the certificate itself, or the way of obtaining the certificate, or the password associated with the certificate to subscribers, which means the subscriber accepts the certificate. After subscriber receives digital certificate, the private key corresponding to the certificate should be kept safely.

4.7.6 Publication of the Re-Keyed Certificate by the CA

Once the subscriber receives the Re-Keyed certificate, SHECA will issue copies of the certificate in its repository, directory services and other one or more repositories decided by the SHECA. Subscribers can also publish their updated certificate in other places .

After new certificate is issued, SHECA and its authorized service agencies can revoke the old certificate according to subscriber's requirements.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

After subscribers receive key updates certificates, SHECA will not specifically notice the registration authority, registration authority terminal, the competent departments and other entities for special notice, and these entities can obtain subscribers' updated certifications and related information by querying the directory service or SHECA information repository.

4.8 Certificate Modification

In the validity of the certificate, when the certificate information is changed, the subscriber or other participants may choose to change the certification, preserve the public key and apply for a new certificate. SHECA will provide a re-certification once the information submitted by the applicant identified and verified. Only in the period, subscribers can change the certificate. When the subscriber information contained in the certificate is changed, the subscriber must apply for certificate change to ensure that it does not affect the relying party's trust.

When the subscriber information is changed, which is enough to affect the identity changes of the certificate held by the subscriber, the subscriber has the obligation to report for the SHECA.

4.8.1 The Circumstances of Certificate Modification

When the modification of the subscriber or other participant information results in physical status changes, the user must make changes to the original certificate and re-apply for certification after the certificate is revoked. Including:

- Subscriber's name, telephone, address and other information changes
- Subscriber changes because of organizational restructuring and other reasons
- Other information changes

If information contained in the certificate changes that may affect and modify the rights and obligations of subscribers. The subscriber can not apply for the certificate change, only can revoke the certificate then re-apply for a new certificate.

The process and conditions of certificate changing is the same with and certificate application.

4.8.2 Who May Request Certificate Modification

All subscribers hold certificates issued by SHECA , including individuals, enterprises, institutions, government agencies, social organizations, people's organizations and other organizations, etc., when their certificate information changes , resulting in physical status changes, they may request to certificate modification service.

4.8.3 The Processing of Certificate Modification Requests

SHECA and its authorized service agencies can provide online and offline changing.

Changing the certificate online----The subscriber must fill out the change request online , and in accordance with SHECA requirements , uses the private key in corresponding public key to sign the modification request information, then submit to the issuing authority .When the certificate authority receives the certificate modification request , after they identify and verify the identity of the applicant and request information , issue a new certificate ,and the original public key is still used .

Changing the certificate offline----The subscribers should fill out the certificate application form to the SHECA and its authorized service agencies in accordance with the original application process. SHECA and its authorized certification service agency identify and verify certification changed application according to the original application process. After issuing authority recognizes and approves application, it will issue a new certificate, and certificate's public key is the original applicant public key.

Currently, the only way is changing the certificate offline.

4.8.4 The Notification of Certificate Change

After the certificate is changed, the certificate is valid from the day it is changed till the original expiration date .

Before subscribers change the certificate, they should ensure that the certificate key pair is safe

and reliable. Once this reliability can not be confirmed, then SHECA recommends subscribers to select directly the certificate key updating.

4.8.5 The Behavior Constitutes Acceptance of Certificate Change

After a certificate modification request submitted by the subscribers online or offline is approved, SHECA and its authorized service agencies will deliver the certificate, a way of obtaining the certificate or the password associated with the certificates to the subscriber, which means that subscribers accept the certificate. After subscribers receive digital certificate, the private key corresponding to the certificate should be kept properly.

4.8.6 The Release of Electronic Certification Service Agency to Change the Certificate

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

After new certificate is issued, the old certificate will be revoked within 24 hours, which is released by CRL.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

After subscribers accept the certificate modification, SHECA will not devoted to the RA, RAT, the competent departments and other entities for special notification, these entities can obtain modification certificates and related information by querying the directory service or SHECA information repository .

4.9 Certificate Revocation and Suspension

Subscriber, the electronic certification service agencies and law or government authority departments can request certificate revocation.

After the certificate is revoked, the certificate holder may re-apply for a digital certificate to SHECA or its authorized certificate services agencies, and the procedure is the same with the first application procedure. The private key with the corresponding public key contained in the certificate is revoked, unless destroyed, should be protected by subscriber ate key in a credible method in the preservation.

All certificate revocation application forms and other formats are saved by the SHECA and its authorized certificate service agencies.

Currently, SHECA does not provide certificate suspension services. Once these services are provided, SHECA will announce it through the website, etc.

4.9.1 The Situation of Certificate Revocation

4.9.1.1 Reasons for Revoking a Subscriber Certificate

1、SHECA and it's Registry Authorities will revoke the Subscriber Certificates within 24 hours if any of the following circumstances occurs:

- Subscriber (or authorized proxy) requests to revoke certificate, and CA make sure the request is from the subscriber;
- Because the certificate is improper used in violation of the main and important obligations of national laws and regulations;
- SHECA is made aware that the original certificate request was not authorized and does not retroactively grant authorization;
- SHECA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise, or no longer comply with the requirements of key size and key parameters setting and quality check in section 6.1.5 and section 6.1.6;
- SHECA is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate;
- SHECA obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address or mailbox control for any Mailbox Address in the Certificate should not be relied upon;
- SHECA has reasonable assurance that a Certificate was used to sign Suspect Code.

2、SHECA and it's Registry Authorities will revoke the Subscriber Certificates within 5 days if any of the following circumstances occurs:

- The Certificate no longer complies with the requirements of Section 6.1.5 and Section 6.1.6;
- SHECA obtains evidence that the certificate is improperly used;
- It is discovered and confirmed that a certificate is not issued in accordance with UniTrust CP and/or CPS;
- Subscriber information in the certificate has material modification;
- Revocation according the requirement of CP/CPS;
- SHECA determines that any of the information appearing in the Certificate is inaccurate or misleading or subscriber provides false or deceptive material in application;
- SHECA is made aware that a Subscriber has violated one ore more of its material obligations under the Subscriber Agreement or Terms of Use;
- The subscriber didn't perform the obligation of payment;
- Continuity of using the certificate will cause harm to SHECA business credit and trust mode;
- The change, revocation or dismiss of subscriber legal identification;
- Evolution of technologies or standards may lead to unacceptable risk for the relying party or

software providers;

- SHECA's right to issue SSL Certificate under Bseline Requirements expires or is revoked or terminated, unless SHECA has made arrangements to continue maintaining the CRL/OCSP Repository;
- SHECA is made aware of any circumstance indicating that use of an email address or Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g., a court or arbitrator has revoked the right to use an email address or Domain Name, a relevant licensing or services agreement between the Subscriber has terminated, or the account holder has failed to maintain the active status of the email address or Domain Name);
- SHECA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
- SHECA is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed.
- Requirements to revoke the certificate according to related laws and regulations.

Note:

SHECA MAY delay revocation based on a request from Application Software Suppliers where immediate revocation has a potentially large negative impact to the ecosystem.

SHECA has no obligation to public the reason of certificate revoked.

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

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

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

1. The Subordinate CA requests revocation in writing;

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

3. SHECA obtains evidence that the Subordinate certificate's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the Sections 6.1.5 and 6.1.6 of Baseline Requirements (including S/MIME BR and Code Signing BR);

4. SHECA obtains evidence that the Certificate was misused;

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

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

misleading;

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

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

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

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

4.9.2 Who Can Request Revocation

The following subject can request revocation:

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

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

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

4.9.3 The Process of Revocation Request

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

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

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

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

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

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

(3) SHECA shall decide whether revocation or other appropriate action is warranted during two workdays. If the revocation request is from an Application Software Supplier, SHECA should inform the Application Software Supplier whether or not SHECA will revoke the certificate within 2 business days.

If SHECA determine that revocation will have an unreasonable impact on customer, SHECA will propose an alternative course of action to the Application Software Supplier, based on the investigation,

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

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

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

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

4.9.4 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.

4.9.5 Time Within Which CA Must Process the Revocation Request

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

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

1. The nature of the alleged problem;

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

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

4. Relevant legislation..

4.9.6 Revocation Checking Requirements for Relying Parties

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.

4.9.7 CRL Issuance Frequency

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

SHECA should release Certificate Revocation List of a sub-CA certificate (ARL) at least once every 7 months. If the root certificate is revoked, revocation information is published on the website in time. The difference between of the Sub-CA certificate ARL nextUpdate time (nextUpdate) and this update time (thisUpdate) of the root/intermediate root certificate ARL must be less than or equal to 10 months. If the root/Intermediate Root certificate is revoked, SHECA will publish the revocation information on the website.

4.9.8 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.

4.9.9 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. OCSP responses MUST either:

1. Be signed by the CA that issued the Certificates whose revocation status is being checked, or

2. Be signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked. In this case, the OCSP signing Certificate MUST contain an extension of type id-pkix-ocsp-nocheck, as defined by RFC6960.

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

4.9.10 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.

4.9.11 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.

4.9.12 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.

4.9.13 Circumstances for Suspension

Not applicable.

4.9.14 Who Can Request Suspension

Not applicable.

4.9.15 Procedure for Suspension Request

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

4.9.17 Problem Reporting and Processing Mechanism

SHECA should set up and maintain a 7*24h problem reporting and processing mechanism. Any subscriber, relying party, software supplier or other third party who 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 investigation process within 24 hours to the related certificate and provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate Problem Report. Also, 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.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

Regarding a revoked certificate, SHECA does not delete its revocation records from OCSP server; SHECA does not delete its revocation records from CRL until the certificate expires.

SHECA provides two access to certificate status check services:

1、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、OCSP ----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.

The response time is no more than 10 seconds (no more than 3 seconds for the CRL response time for EV certificates; The response time here does not include the time-consuming of obtaining data slowly due to reasons such as the subscriber network.).

SHECA SHALL maintain an online 24x7 Repository that application software can use to automatically check the current status of all unexpired Certificates issued by the CA.

SHECA SHALL maintain a continuous 24x7 ability to respond internally to a high-priority Certificate Problem Report, and where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a Certificate that is the subject of such a complaint.

4.11 Termination

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

1、After 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、In 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 strategy are decided by this agency.

To recover the private key, the subscriber needs to submit application material which should be the same of new application. The entry staff verifies the subscriber information, confirms that the key applied for recovery belongs to the applicant, then type in the application data for key recovery. The auditor reviews the application data and recover the key. The system must keep audit log of all operations and results. The Entry staff and auditor should not be the same person . the applicant need to pay for the restoration fee.

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 backup room located in SHECA building has three physical protection layers to monitor and manage physical channel. Host and backup rooms of SHECA are equipped with shock-proof, fireproof, waterproof temperature control systems, access control systems, video surveillance systems and alarm systems to ensure continuity and reliability of certification services. The construction and management of all rooms is in strict accordance with the requirements of SHECA. In principle, machine room is prohibited to visit, only person authorized by SHECA can enter into the site and the area authorized. The high-security monitoring technology was made in generator room, including video, fingerprint, access control and other security management tools to ensure the security of the physical channel. Entering into SHECA generator room, there are time-limited access control system. All-weather automatic monitoring is carried out in computer room.

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

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

5.1.2 Physical Access

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

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

5.1.3 Power and Air Conditioning

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

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

SHECA maintains according to the provisions of the telecommunications facilities.

5.1.4 Water Exposures

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

5.1.5 Fire Prevention and Protection

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

5.1.6 Media Storage

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

5.1.7 Waste Disposal

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

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

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

5.1.8 Off-site Backup

1. System backup

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

2. Data backup

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

5.2 Procedural Control

5.2.1 Trusted Roles

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

SHECA clearly defines the key functions positions for CA, including

1. The administrator of the application system

2. The administrator of the operating system

3. The administrator of the database system

4. The administrator of the network system

5. RA administrator

6. Entry staffs

7. Auditors

8. The key control group

9. Safety Executive Group

10. Other personnel

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

SHECA in accordance with this CPS and authorized agreement creates the management practices of authorized certification services organization (RA, RAT and others), standardizes the certification service organization and the operation of service systems management staff and operator. Take full account of security constraints during a related software designed. Responsibility of authorized certification service organization by SHECA is divided reasonably to ensure responsibilities and obligations management and implementation through the systems and technology.

5.2.2 Number of Persons Required per Task

CA and RA should establish, maintain and enforce strict control process, and establish measures of

duties segregation, based on job requirements and arrangement to implement the safety mechanism of mutual restraint, mutual supervision to ensure that sensitive operation is completed by a number of credible personnel.

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

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

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

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

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

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

5.2.3 Identification and Authentication of Each Role

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

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

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

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

will record completely all the operating behavior.

All SHECA employees must ensure that:

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

5.2.4 Roles Requiring Separation of Duties

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

- The validation of information in Certificate Applications;
- The acceptance, rejection, or other processing of Certificate Applications, revocation requests, key recovery requests or renewal requests, or enrollment information;
- The issuance, or revocation of Certificates, including personnel having access to restricted portions of the repository;
- The handling of Subscriber information or requests
- The generation, issuing or destruction of a CA certificate
- The personnel of system on-line or off-line
- The personnel of mastering important password key Management staff and operator of key and cryptographic equipment
- The acceptance of the certificate services is completed by two roles entry clerks and auditors.

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

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

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

5.3 Personnel Control

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

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

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

2. System operators must have relevant work experience in authentication systems or obtaining related training in SHECA.

3. Managers must have practical certificate authentication experience and many years of experience in systems management and operation.

5.3.2 Background Check Procedures

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

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

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

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

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

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

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

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

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

The check of certification service manager and operator staff authorized by SHECA can refer to the way of trusted employees examination by SHECA , on this basis, increasing visits and training provision, but not contrary to the CPS and the corresponding CP, licensing agreements and requirement of public certificate services specifications by SHECA.

SHECA establishes the rules of process management regulation, and under which employees are restrained by contract, not allowed to disclose sensitive information of SHECA certificate service. All employees sign confidentiality agreements with SHECA and go on working in similar with SHECA after expiration of the agreements 2 years.

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

5.3.3 Requirements of the Training

The following training is offered by SHECA to staff:

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

SHECA shall record the staff training and archive the record, and assure the personnel have qualified skill as required 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、RA、RAT .

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

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

personnel changes in circumstances.

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

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

5.4.2 Frequency of Processing Log

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

5.4.3 Retention Period for Audit Log

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

5.4.4 Protection of Audit Log

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

5.4.5 Backup Procedures of Audit Log

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

5.4.6 Audit Collection System

SHECA audits collection systems, including the objects involved:

- Certificate management system
- Certificate issuing system
- 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 the period of provision, meets the needs of any legitimate requirement for reading and using .For information deemed necessary, SHECA will take the way of off-site backup to save.

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

5.5.4 Backup Procedures of Archive File

All the documents and data archived, usually is stored in the main storage site on SHECA. Really necessary, it will also be saved the backup in its offsite. Database archived generally is accepted the physical or logical isolation for approach, not exchanging information with the outside world. Only authorized personnel can conduct the operation for reading the file in the supervision of the case. SHECA makes sure that it prohibits deletion or modification for backup and files, or other inappropriate operations in the security mechanism.

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

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

5.5.5 Requirements for Time-Stamping of Records

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

5.5.6 Archiving Collection System

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

5.5.7 Procedures to Obtain and Verify Archive Information

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

5.6 Key Changeover of Electronic Certification Services Agencies

Valid of SHECA root certificate for a maximum is not more than 30 years, and any certificate validity issued by root certificate including the sub-CA certificate , the subscriber certificate , is shorter than the valid of root certificate. Any subscribers certificate validity issued by sub-CA certificate, is shorter than the sub-CA certificate validity.

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

Prior to the expiration of certificate, SHECA will replace the root key in accordance with the provisions of UNTSH CP, and generate a new certificate. When making a generation for key, specifications of SHECA key management is followed strictly. CA key replacement r must comply with the following principles:

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

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

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

4. Release the new CA certificate timely.

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

5.7 Compromise and Disaster Recovery

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

5.7.1. Incident and Compromise Handling Procedures

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

5.7.2. 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.

5.7.3. 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.

5.Take reasonable efforts to promptly inform users and relying parties which include Asseco Data Systems S.A..

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.

5.7.4. 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.

5.8 CA or RA Termination

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

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

2. Arrange the business to undertake.

- Save all of the operational information related to certification service, including certificates, user information, system files, 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

6.1.1.1. CA Key pair Generation

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.

For CA Key Pairs that are either used as a CA Key Pair for a Root Certificate or used as a CA Key Pair for a Subordinate CA Certificate, SHECA SHALL: prepare and follow a Key Generation Script, have a Qualified Auditor witness the CA Key Pair generation process or record a video of the entire CA Key Pair generation process, and have a Qualified Auditor issue a report opining that the CA followed its key ceremony during its Key and Certificate generation process and the controls used to ensure the integrity and confidentiality of the Key Pair.

6.1.1.2. RA Key Pair Generation

No stipulations.

6.1.1.3. Subscriber Key Pair Generation

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.

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

SHECA SHALL reject a certificate request if one or more of the following conditions are met:

1. For SSL/ CS/ SMIME certificates, the Key Pair does not meet the requirements set forth in corresponding CA/B Forum BR Section 6.1.5 and/or Section 6.1.6;

2. There is clear evidence that the specific method used to generate the Private Key was flawed;

3. SHECA is aware of a demonstrated or proven method that exposes the Applicant's Private Key to compromise;

4. SHECA has previously been notified that the Applicant's Private Key has suffered a Key Compromise using its procedure for revocation request;

5. For SSL/ CS/ SMIME certificates, the Public Key corresponds to an industry-demonstrated weak Private Key.

6. SHECA or authorized third parties can generate private keys on behalf of subscribers (for S/MIME certificates).

For requests submitted on or after November 15, 2024, at least the following precautions SHALL be implemented for SSL certificates:

In the case of Debian weak keys vulnerability (https://wiki.debian.org/SSLkeys), SHECA SHALL reject all keys found at https://github.com/cabforum/Debian-weak-keys/ for each key type (e.g. RSA, ECDSA) and size listed in the repository. For all other keys meeting the requirements of CA/B Forum BR Section 6.1.5, with the exception of RSA key sizes greater than 8192 bits, SHECA SHALL reject Debian weak keys.

In the case of ROCA vulnerability, SHECA SHALL reject keys identified by the tools available at https://github.com/crocs-muni/roca or equivalent.

In the case of Close Primes vulnerability (https://fermatattack.secvuln.info/), SHECA SHALL reject weak keys which can be factored within 100 rounds using Fermat's factorization method.

If the Subscriber Certificate will contain an extKeyUsage extension containing either the values id-kp-serverAuth [RFC5280] or anyExtendedKeyUsage [RFC5280], SHECA SHALL NOT generate a Key Pair on behalf of a Subscriber, and SHALL NOT accept a certificate request using

a Key Pair previously generated by SHECA.

Other Concerns:

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

2. For SSL, Code Signing, S/MIME, EV SSL and EV Code Signing certificates, 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. SHECA should record the delivery of the key pairs. But in case of the loss, leakage of this key pair, SHECA does not assume any responsibility and obligation.

Parties other than the Subscriber SHALL NOT archive the Subscriber Private Key without authorization by the Subscriber.

SHECA or authorized third parties shall not store subscriber private keys in plain text.

If SHECA or any of its designated RAs become aware that a Subscriber’s Private Key has been communicated to an unauthorized person or an organization not affiliated with the Subscriber, then SHECA SHALL revoke all certificates that include the Public Key corresponding to the communicated Private Key.

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 https://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. Algorithm Type and Key Length

For RSA key pairs, SHECA shall ensure that the modulus size, when encoded, is at least 2048 bits, and ensure that the modulus size, in bits, is evenly divisible by 8.

For ECDSA key pairs, SHECA shall ensure that the key represents a valid point on the NIST P‑256, NIST P‑384 or NIST P‑521elliptic curve.

The size of SM2 key is 256 bits.

Since June 1,2021, the size of RSA key of codesigning certificate or timestamp certificate should be 3072 bits or more.

The SHECA key pair length is RSA 2048 bits, RSA 4096 bits, ECDSA NIST P‑256, ECDSA NIST P‑384 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.

RSA: SHECA SHALL confirm that the value of the public exponent is an odd number equal to 3 or more. Additionally, the public exponent SHOULD be in the range between 2^16 + 1 and 2^256 - 1. The modulus SHOULD also have the following characteristics: an odd number, not the power of a prime, and have no factors smaller than 752. [Source: Section 5.3.3, NIST SP 800-89]

ECDSA: SHECA SHOULD confirm the validity of all keys using either the ECC Full Public Key Validation Routine or the ECC Partial Public Key Validation Routine. [Source: Sections 5.6.2.3.2 and 5.6.2.3.3, respectively, of NIST SP 800-56A: Revision 2]

6.1.7. Key Usage Purposes

Private Keys corresponding to Root Certificates MUST NOT be used to sign Certificates except in the following cases:

1. Self-signed Certificates to represent the Root CA itself;
2. Certificates for Subordinate CAs and Cross-Certified Subordinate CA Certificates;
3. Certificates for infrastructure purposes (administrative role certificates, internal CA operational device certificates); and

4. Certificates for OCSP Response verification.

Intermediate CA keys are generally used to issue the following certificates and CRLs:

1 Subscriber certificate;

2 PKI system function certificates for specific purposes (such as OCSP certificates);

3 Subscriber CRLs.

Subscriber keys can be used to provide security services such as message encryption and signing.

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

SHECA SHALL implement physical and logical safeguards to prevent unauthorized certificate issuance. Protection of the CA Private Key outside the validated system or device specified in BR Section 6.2.7 MUST consist of physical security, encryption, or a combination of both, implemented in a manner that prevents disclosure of the Private Key. SHECA SHALL encrypt its Private Key with an algorithm and key-length that, according to the state of the art, are capable of withstanding cryptanalytic attacks for the residual life of the encrypted key or key part.

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.

1. 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.

If the Issuing CA generated the Private Key on behalf of the Subordinate CA, then the Issuing CA SHALL encrypt the Private Key for transport to the Subordinate CA. If the Issuing CA becomes aware that a Subordinate CA’s Private Key has been communicated to an unauthorized person or an organization not affiliated with the Subordinate CA, then the Issuing CA SHALL revoke all certificates that include the Public Key corresponding to the communicated Private Key.

6.2.7 Private Key Storage on Cryptographic Module

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

Subscriber's private key is stored in the USB key medium meeting the regulations of the national password administration, and all the private key stored in the USB key are stored in the form of cipher text. For the private key generated by software cryptographic 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.

For code signing certificates and EV code signing certificates, Subscriber ’ s Private Key is generated, stored, and used in a suitable Hardware Crypto Module (USB key) with a unit design form factor certified as conforming to at least FIPS 140-2 Level 2, in accordance with Section 6.2.7.4 of Code Signing Baseline Requirements.

Regarding USB Key Lifecycle Management, SHECA provides the USB Key in accordance with relevant provision of national encryption management as the generation subscribers' signature key and storage devices for user. SHECA ensures that the certificate applicant obtains the USB Key to meet the management and application requirements of certificate and private key:

- USB Key is kept properly before the certificate applicant getting, including procurement, inventory, distribution and other management by implement strict standards.
- USB Key must pass the password authentication before it can be used.
- The private key stored in USB Key can not be exported and stored in the form of cipher text.
- Once the USB Key Certificate is issued to the applicant, it will be held by the certificate subscriber, and by controlled and owned completely by the subscribers.
- SHECA provides subscribers a year warranty of USB Key.
- During the updating the certificate, subscribers may not replace the USB Key.
- After subscribers certificate is lost, revoked or updated, subscribers deals with their own USB Key. SHECA is not responsible for the destruction or reclamation of subscribers' USB Key.

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, encryption card, encryption machine,

or other forms of hardware module, the subscriber can further protect through password, fingerprint, IC card, etc. If the subscriber's computer is installed with appropriate driver, and the USB Key, smart cards are plugged into the appropriate device, after the input of password or fingerprint, the private key will be activated.

6.2.9 Method of Deactivating Private Key

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

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

Subscriber removed the way of the private key active statement decided its own , such as exit, power off, remove token / key, automatic freeze and so on. Subscriber own must bear the risk and responsibility for removing the private key active statement.

6.2.10 Method of Destroying Private Key

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

Subscriber's private key is used no longer, or the public key corresponding to private key expired or revoked, the method of destruction is determined by the subscribers .The subscriber must ensure to log off effectively the private key, and bear the relevant responsibility. Preservation and archiving involved of key expired, the subscriber must follow the provisions of this CPS.

6.2.11 Cryptographic Module Rating

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

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Operation process, security measures, preservation deadline and strategy kept of public key archival is in accordance with certificates. Public key archival requirements refers to the relevant provisions of 5.5 in the CPS.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The usage period of public keys and private keys is related to validity period of certificate, but it is not completely consistent. For the certificate signing used, the private key can only be used for digital signatures within the certificate validity period, the use period of private key not exceeding the validity period of the certificate. However, in order to ensure signature information within the certificate validity period can be verified, the usage period of public keys can surpass validity period of certificate. For encryption certificate, the public key can only be used for encrypted information within the validity period of certificate, the use period of private key not exceeding the validity period of the certificate. However, in order to ensure information encrypted can be used to unlock the information within the validity period of certificate, the usage period of private keys can surpass validity period of certificate. Certificate authentication used, the private key and public key can be used within the validity period of certificate. When a certificate has multiple usages, the usage period of public keys and private keys is a combination of the above.

The certificate operating period is in accordance with the validity period contained within the certificate. The table below shows the validity period for subscriber certificates and CA certificates.

In addition to attention, after the end of the validity for whether subscriber certificate or CA certificate, under the circumstances of ensuring safety, is allowed to use the original key pair to update the certificate. But the key pair can not be used indefinitely. The key pair usage period and certificate validation period are set as following:

Type	**Key Pair Usage Period**	**Certificate Validation Period**
Root certificate (issued before 2018)	30 years	30 years
Root certificate (issued on or after 2018)	25 years	25 years
Subordinate CA certificate	25 years	25 years
DV SSL certificate (issued on or before September 1th, 2020)	No stipulation	825 days
DV SSL certificate (issued after September 1th, 2020)	No stipulation	398 days
OV SSL certificate (issued on or before September 1th, 2020)	No stipulation	825 days
OV SSL certificate (issued after September 1th, 2020)	No stipulation	398 days

EV SSL certificate (issued on or before September 1th, 2020)	No stipulation	825 days
EV SSL certificate (issued after September 1th, 2020)	No stipulation	398 days
CodeSigning certificate	No stipulation	39 months
EV CodeSigning certificate	No stipulation	398 days
Other types of subscriber certificate	No stipulation	No stipulation
Time-Stamping Certificate	15 months	135 months
OCSP Certificate	3 years	3 years
S/MIME Certificate (strict/ multipurpose generation)	15 years	825 days
S/MIME Certificate (legacy generation)	15 years	1185 days

6.4 Activation Data

6.4.1 Generation and Installation of Activation Data

In order to protect the security of private keys, certificates subscriber generating and installing activation data must ensure safety and reliability, so as to avoid the private key compromised, stolen, used unauthorized, tampered or disclosed without authorization.

Activation data of CA private key must follow the requirements of the key activation data segmentation and key management methods to make a strict production, distribution and usage. Activation data for subscribers' private key , including passwords for downloading the certificate (provided in the form of the password envelope), USB Key, landing passwords of IC card, must generate randomly in the safe and reliable environment.

Activation data generated by SHECA, including passwords for downloading the certificate (provided in the form of the password envelope), USB Key, landing passwords of IC card , must generate randomly in the safe and reliable environment .The activation data are delivered to subscribers by the safety and reliability way, such as offline in person to submit, post courier, etc. For activation data of non-single usage, SHECA suggests users to modify by themselves.

All the passwords protected should not be guessed easily, and should follow the following principles:

- Eight characters at least
- Contain one character and one number at least
- Contain one lowercase letter at least
- Not contain many same characters
- And operator's name can not be the same
- Can not use birthdays, telephone numbers
- The longer substring in the user name information

6.4.2 Protection of Activation Data

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

Subscriber activation data must be properly safeguarded or destroyed, and can not be got by others. If the certificate subscriber uses a password or PIN to protect private key, the subscriber should take good care of password or PIN to prevent the leakage or theft. If the certificate subscriber uses biological characteristics to protect the private key, the subscriber should also take attention to prevent its biological characteristics from illegal obtaining. Meanwhile, in order to meet the safe requirements of business systems, activation data should always be modified.

6.4.3 Other Aspects of Activation Data

When activation data of the private key is transferred, they should be protected from loss, theft, modification, unauthorized disclosure, or unauthorized usage during the transmission.

The private key activation data no usage should be destroyed, and protect them from lost theft, disclosure or unauthorized use during the process. The destruction result can not be obtained directly or indirectly some or all of the activation data by the remnants information and medium, such as paper recorded passwords must be crushed.

Considering safety reasons, the provisions for the life cycle of the application certificate subscriber activating data stated as follows:

1. The certificate password applied for subscribers, becomes invalid after the application is successful.

2. The password used to protect the password of the private key, or IC card, USB Key, could be modified by subscriber at any time based on business application , and should be modified after three months the using period .

6.5 Security Controls of Computer

6.5.1 Specific Computer Security Technical Requirements

Information security management of SHECA certification system agrees " Certificate

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

The main security technologies and control measures include:

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

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

6.5.2 Computer Security Rating

SHECA certification business systems pass the relative evaluation, review and certification of the State Cryptography Administration, China National Information Security Evaluation Center, the Shanghai Information Security Evaluation Center and other departments.

6.6 Technical Controls of Life Cycle

6.6.1 Development Controls of System

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

Verification and review of third-party

The security risk analysis and reliability design

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

If SHECA uses Linting software developed by third parties, it SHOULD monitor for updated versions of that software and plan for updates no later than three months from the release of the update.

SHECA MAY perform Linting on the corpus of its unexpired, un-revoked Subscriber Certificates whenever it updates the Linting software.

6.6.2 Controls of Security Management

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

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

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

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

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

6.6.3 Security Control of Lifetime

No stipulation.

6.7 Security Controls of Network

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

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

In order to ensure network security, SHECA authentication system installs firewall, intrusion detection, security auditing, virus protection system, and update the version of firewall, intrusion

detection, security audits, virus protection system , as much as possible to reduce the risk from the network.

6.8 Time-Stamping

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

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

7.1 Certificates

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

7.1.1 Version

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

7.1.2 Certificate Extensions

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

1、the certificate extensions

- Key Usage

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

	SSL Certificate	Code Signing Certificate	Timestamp Certificate	CA Certificate
0 digitalSignature	√	√	√	×
1 nonRepudiation	×	×	×	×
2 keyEncipherment	√	×	×	×
3 dataEncipherment	×	×	×	×
4 keyAgreement	×	×	×	×

5 keyCertSign	×	×	×	√
6 CRLSign	×	×	×	√
7 encipherOnly	×	×	×	×
8 decipherOnly	×	×	×	×

For S/MIME certificates, the key usage should be set as the table below (SHECA issues strict generation S/MIME certificates only).

Generation	rsaEncryption	id-ecPublicKey	id-Ed25519 and id-Ed448
Strict	For signing only, bit positions SHALL be set for digitalSignature and MAY be set for nonRepudiation. For key management only, bit positions SHALL be set for keyEncipherment. For dual use, bit positions SHALL be set for digitalSignature and keyEncipherment and MAY be set for nonRepudiation.	For signing only, bit positions SHALL be set for digitalSignature and MAY be set for nonRepudiation. For key management only, bit positions SHALL be set for keyAgreement and MAY be set for encipherOnly or decipherOnly. For dual use, bit positions SHALL be set for digitalSignature and keyAgreement and MAY be set for nonRepudiation and for encipherOnly or decipherOnly (only if keyAgreement is set).	Bit positions SHALL be set for digitalSignature and MAY be set for nonRepudiation.
Multipurpose and Legacy	For signing only, bit positions SHALL be set for digitalSignature and MAY be set for nonRepudiation. For key management only, bit positions SHALL be set for keyEncipherment and MAY be set for dataEncipherment.	For signing only, bit positions SHALL be set for digitalSignature and MAY be set for nonRepudiation. For key management only, bit positions SHALL be set for keyAgreement and MAY be set for encipherOnly or decipherOnly.	Bit positions SHALL be set for digitalSignature and MAY be set for nonRepudiation.

	For dual use, bit positions SHALL be set for digitalSignature and keyEncipherment and MAY be set for nonRepudiation and dataEncipherment.	For dual use, bit positions SHALL be set for digitalSignature and keyAgreement and MAY be set for nonRepudiation and for encipherOnly or decipherOnly (only if keyAgreement is set).	

The key usage for other types of certificates are set based on demand which is compliant with RFC5280.

- netscape certificate type

The extension is used to declare the approbatory type of certificate approved for a relying party who uses netscape. The extension is declared as the following key usage: SSL client authentication, SSL server authentication, S / MIME, the object signature and so on.

- Certificate policy

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

- Basic restrictions

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

- Precertificate Poison

The Precertificate MUST contain the Precertificate Poison extension (OID: 1.3.6.1.4.1.11129.2.4.3). This extension MUST have an extnValue OCTET STRING which is exactly the hex-encoded bytes 0500, the encoded representation of the ASN.1 NULL value, as specified in RFC 6962, Section 3.1.

- Extended Key Usage

	SSL Certificate	Code Signing Certificate	Timestamp Certificate
Server Authentication **1.3.6.1.5.5.7.3.1**	√	×	×
Client Authentication **1.3.6.1.5.5.7.3.2**	√	×	×
Code Signing **1.3.6.1.5.5.7.3.3**	×	√	×

Secure e-mail **1.3.6.1.5.5.7.3.4**	×	×	×
Time stamp **1.3.6.1.5.5.7.3.8**	×	×	√

For S/MIME certificates, the extended key usage should be set as the table below. The values id-kp-serverAuth, id-kp-codeSigning, id-kp-timeStamping, and anyExtendedKeyUsage SHALL NOT be present. In parctice, SHECA only issues strict generation S/MIME certificates.

Generation	KeyPurposeId
Strict	id-kp-emailProtection (**1.3.6.1.5.5.7.3.4**) SHALL be present. Other values SHALL NOT be present.
Multipurpose and Legacy	id-kp-emailProtection (**1.3.6.1.5.5.7.3.4**) SHALL be present. Other values MAY be present.

The extended key usage for other types of certificates are set based on demand which is compliant with RFC5280.

- CRL Distribution Points

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

- Serial number

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

2、Private extensions

The content of private extensions refers to about certificate custom extension instructions in CPS appendix.

7.1.3 Algorithm Object Identifiers

Keys and hash algorithms for SHECA's TLS/ Code Signing/ Time Stamp/ SMIME certificates meet the requirement specified in the CA/B Forum Baseline Requirements and the Applicable Requirements.

7.1.3.1 SubjectPublicKeyInfo

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

7.1.3.1.1 RSA

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

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

7.1.3.1.2 ECDSA

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

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

7.1.3.1.3 SM2

SHECA uses sm2Encryption (OID1.2.156.10197.1.301).

7.1.3.2 Signature AlgorithmIdentifier

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

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

The signatureAlgorithm field of a Certificate or Precertificate.

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

The signature Algorithm field of a CertificateList

The signature field of a TBSCertList

The signature Algorithm field of a BasicOCSPResponse.

No other encodings are permitted for these fields.

7.1.3.2.1 RSA

SHECA uses the following two RSA signature algorithms and encodings:

- SHA-256 with RSA, (OID) 1.2.840.113549.1.1.11;
- SHA-384 with RSA, (OID) 1.2.840.113549.1.1.12.

7.1.3.2.2 ECDSA

SHECA uses the SHA-384 with ECDSA signature algorithms and encodings, (OID) 1.2.840.10045.4.3.3.

7.1.3.2.3 SM2

SHECA uses SM3withSM2Encryption signature algorithm (OID: 1.2.156.10197.1.501).

7.1.4 Name Forms

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

Each Certificate includes a unique serial number. Optional subject fields in a certificate either

contain verified information or are left empty. Certificates cannot contain metadata such as '.', '-' and ' ' characters or and/or any other indication that the value/field is absent, incomplete, or not applicable.

S/MIME Enterprise RAs may include optional attributes in the certificate as specified in Section 7.1.4.2.5 of the S/MIME Requirements. The Enterprise RA must validate this information using the process described in Section 3.

7.1.5 Name Constraints

The certificate is issued by SHECA, whose identifier name cannot be anonymous or pseudo-name, must have a definite name. SHECA can specify a special name for the user in accordance with certain rules and link uniquely the special name to a defined entity (individual, unit or device) in some special requirements e-government applications. Any particular name must be approved by SHECA Security Certification Committee.

Technically Constrained Subordinate CA certificates are issued with an extended key usage extension. The extension does not include the anyExtendedKeyUsage key usage purpose. The extended key usage may contain values permitted by the Applicable Requirements but, in addition to other values, may only include one of the following: serverAuth, code signing, emailProtection or timestamping.

7.1.6 Certificate Policy Object Identifier

An object identifier (OID) is a unique number that identifies an object or policy. OIDs are included as appropriate in certificates, including the relevant OIDs required by the CA/Browser Forum.

The certificate is issued by SHECA in accordance with the X.509 standard, whose policy object identifier is stored in the relevant topic of certificate policy.

SHECA discloses the OIDs included in publicly trusted certificates used. Please refer to this CPS Section 1.2.

7.1.7 The Usage of Policy Constraints Extensions

No stipulation.

7.1.8 The Syntax and Semantics of Policy Qualifiers

No stipulation.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2 Certificate Revocation List

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

SHECA issues regularly CRL for the user to query.

7.2.1. Version Number

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

7.2.2. CRL and CRL Entry Extensions

If a CRL entry reasonCode extension is present, the reason must indicate the most appropriate reason for revocation of the certificate. The CRLReason for a revoked CA cannot be unspecified (0) or certificateHold(6). Certificates may be revoked with one of the following reason codes, in order of preference when multiple reason codes are applicable:

- keyCompromise (1),
- CACompromise (2), which is only used for Sub CAs,
- privilegeWithdrawn (9);
- cessationOfOperation (5)
- affiliationChanged (3),
- superseded (4)
- unspecified (0), in which case the reasonCode entry extension is omitted.

7.2.2.1. CRL reasonCode Extension Entries

The following is a description of each of these reason codes and circumstances where SHECA or a subscriber will be obligated to use it for their revocation circumstances:

7.2.2.1.1. keyCompromise

The CRLReason keyCompromise is used if:

• SHECA obtains verifiable evidence that the certificate subscriber’s private key corresponding to the public key in the certificate suffered a key compromise; or

• SHECA is made aware of a demonstrated or proven method that exposes the certificate subscriber’s private key to compromise; or

• There is clear evidence that the specific method used to generate the private key was flawed; or

• SHECA is made aware of a demonstrated or proven method that can easily compute the certificate subscriber’s private key based on the public key in the certificate (such as a Debian weak key, see https://wiki.debian.org/TLSkeys); or

• The certificate subscriber requests that SHECA revoke the certificate for this reason, with the

scope of revocation being described below.

If the entity requesting revocation for keyCompromise can demonstrate possession of the certificate’s private key, then SHECA will revoke all instances of that key across all subscribers.

If the entity requesting revocation cannot demonstrate possession of the certificate’s private key, then SHECA may revoke all certificates associated with that subscriber that contain that public key.

If SHECA obtains verifiable evidence of private key compromise for a certificate whose CRL entry does not contain a reasonCode extension or has a reasonCode extension with a non-keyCompromise reason, SHECA may update the CRL entry to enter keyCompromise as the CRLReason in the reasonCode extension. Additionally, SHECA may update the revocation date in a CRL entry when it is determined that the private key of the certificate was compromised prior to the revocation date that is indicated in the CRL entry for that certificate.

7.2.2.1.2. privilegeWithdrawn

The CRLReason privilegeWithdrawn is used for subscriber-side infractions that do not compromise the certificate’s private key, such as when the certificate subscriber provided misleading information in their certificate request or has breached a non-waived breach of the subscriber agreement or terms of use.

CRLReason privilegeWithdrawn is used when:

- SHECA obtains evidence that the certificate was misused; or
- SHECA is made aware that the certificate subscriber has violated one or more of its material obligations under the subscriber agreement or terms of use; or
- SHECA is made aware that a wildcard certificate has been used to authenticate a fraudulently misleading subordinate fully‐qualified domain name; or
- SHECA is made aware of a material change in the information contained in the certificate; or
- SHECA determines or is made aware that any of the information appearing in the certificate is inaccurate; or
- SHECA is made aware that the original certificate request was not authorized and that the Subscriber does not retroactively grant authorization.

7.2.2.1.3. cessationOfOperation

The CRLReason cessationOfOperation is used when a website with the certificate is shut down prior to the expiration of the certificate or the subscriber no longer owns or controls the domain name in the certificate.

CRL cessationOfOperations is used when:

- The certificate subscriber will no longer be using the certificate because they are discontinuing their website; or
- SHECA is made aware of any circumstance indicating that use of a fully‐qualified domain name or IP address in the certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a domain name registrant’s right to use the domain name, a relevant licensing or services agreement between the domain name registrant and the applicant has terminated, or the domain

name registrant has failed to renew the domain name).

• The certificate subscriber has requested that their certificate be revoked for this reason; or

• SHECA received verifiable evidence that the certificate subscriber no longer controls, or is no longer authorized to use, all of the domain names in the certificate.

7.2.2.1.4. affiliationChanged

CRLReason affiliationChanged indicates that the subject’ s name or other subject identity information in the certificate has changed but there is no evidence that the certificate’s private key was compromised.

CRLReason affiliationChanged is used when:

• The certificate subscriber has requested that their certificate be revoked for this reason; or

• SHECA replaced the certificate due to changes in the certificate’ s subject information and the CA has not replaced the certificate for the other reasons: keyCompromise, superseded, cessationOfOperation, or privilegeWithdrawn.

7.2.2.1.5. superseded

The CRLReason superseded is used when:

• The certificate subscriber has requested a new certificate to replace an existing certificate; or

• SHECA obtains reasonable evidence that the validation of domain authorization or control for any fully‐qualified domain name or IP address in the certificate should not be relied upon; or

• SHECA revoked the certificate for compliance reasons such as the certificate does not comply with the SHECA Public Trust CP/CPS, the CA/B Forum’ s Baseline Requirements, or the Mozilla Root Store Policy. Unless the keyCompromise CRLReason is being used, the CRLReason superseded must be used when:

• The certificate subscriber has requested that their certificate be revoked for this reason; or

• SHECA revoked the certificate due to domain authorization or compliance issues other than those related to keyCompromise or privilegeWithdrawn.

7.2.3. Download CRL

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

7.3 Online Certificate Status Protocol

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

7.3.1. Version number

RFC6960 defines the OCSP V1.

7.3.2. OCSP Extensions

SHECA's OCSP Extensions are consistent with RFC6960.

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

7.3.3. The Request and Response of OCSP

An OCSP request contains the following data:

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

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

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

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

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

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

- Malformed Request
- Internal Error
- Try later
- Signature required
- unauthorize

8. Compliance Audit and Other Assessments

SHECA, as the operating body of UNTSH, conducts internal consistency audits and operational assessments on a quarterly basis, and takes at least 3% of SSL digital certificates for assessment each time to ensure the reliability, security and controllability of the certificate service..

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

2、In 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 performs an internal assessment audit annually. 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、SHECA employs an independent auditing firm, according to the audit rules of WebTrust to CA , annual external audits and assesses.

4、SHECA 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、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、During 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、If 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、The 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、 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、SHECA accepts the assessment of any content in accordance with requirements and specifications raised by information industry department.

2、SHECA 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、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、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、After 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、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、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 https://www.sheca.com.

2、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、 After the assessment from a third-party auditor firm is completed, the audit results will be published by the website https://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 https://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 https://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 https://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 https://www.sheca.com.

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

9.1.4 Fees for Other Services

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

2、If SHECA provides these services of the certificate recovery, key escrow, signature key backup

and recovery services , then SHECA will release related costs in time for user to query . If the specified price signed in SHECA agreement is different from the price published, then the agreement price prevail.

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

9.1.5 Refund Policy

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

9.6.5 Relying Party Representations and Warranties

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

- Relying party is familiar with the terms of this CPS, and understands the purpose of the certificates usage.
- Before the relying party trusts certificates issued by SHECA , relying party inspects and

audits reasonably, including: checking the latest CRL announced by SHECA , verifying whether the certificate is revoked; checking all the certificates reliability appeared in the certificate trust path ; checking the validity of the certificate; and checking other information that could affect the validity of the certificate.

- The relying party is willing to compensate SHECA for the losses caused and bear the resulting loss of self or others ,due to negligence or otherwise violating the terms of a reasonable inspection,.
- The trust behavior to certificates indicates that relying party has accepted all the provisions of this CPS, particularly the disclaimer, rejection, and the terms of the limiting liability.
- The relying party shall not reject any statement, change, update, upgrade published from SHECA, including but not limited to modification of strategy, additions and deletions of certification services.

9.6.6 Representations and Warranties of Other Participants

Advance vendor warrants:

- Advance vendor is required to bear all the cost of the certificate and pays all according to the provisions provided by SHECA.
- Advance business's behavior of advance vendor means advance vendor is willing and able to assume responsibility of guaranteeing applicant authenticity based on this CPS.
- Advance vendor shall not reject any statement, change, update, upgrade from SHECA, including but not limited to modification of strategy, standards and additions and deletions of certification services .

9.7 Disclaimers of Warranties

SHECA can't bear liability in the following circumstances:

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

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

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

4. If the applicant provide intentionally or unintentionally incomplete, unreliable or outdated, including but not limited to forgery, tampering, false information, but applicant also provides the necessary review documents based on the normal process and gets digital certificates issued by SHECA. The legal problems, the applicant result from above should be assumed full

responsibility for the economic disputes, and SHECA doesn't assume the legal and economic responsibility associated with the content of the certificate, but can provide investigation and evidence based on victim's Investigation and proof help.

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

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

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

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

9.8 Limitations of Liability

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

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

9.9 Indemnities

9.9.1 The Scope of Compensation

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

1. Indemnification by SHECA

- When issuing the certificate, if not in accordance with the provisions of the CPS for processing or in violation the requirement of laws and regulations causing the certificate subscriber losses, SHECA should bear the liability.
- Because the operator is malicious, willful or negligent, who is not in accordance with the provisions of this CPS to certificate request of the issuance and revocation resulting in the loss of the certificate subscriber, SHECA should compensate the loss of subscribers.

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

2. Indemnification by register authorities (including RAT)

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

3. Indemnification by subscribers

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

suffering damage, subscriber should assume all liability for damages.

- Subscriber or other entity who is entitled to request for certificate revocation, during the period that SHECA publishes the certificate revocation information, if the certificate is used for illegal transactions or arising from transactions disputes, once SHECA conducts relevant operation in accordance with this CPS , subscriber will assume any liability for damages.
- If there are provisions in the agreement between SHECA and otherwise compensations, subscribers refer to its regulations.

9.9.2 Limit of Compensation

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

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

1. Individual certificate, no more than RMB 2,000

2. Unit certificate, no more than RMB 50,000

3. Device certificate, no more than RMB 80,000

4. The SSL certificate, no more than RMB 100,000

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

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

9.10 Term and Termination

9.10.1 Term

This CPS is effective since it is published, version number and release date shall be specified by

the document, as new version is published, and takes effect, the original version shall lose effectiveness automatically.

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

9.10.2 Termination

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

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

9.10.3 Effect of Termination and Survival

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

9.11 Individual Notices an Communications with Participants

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

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

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

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

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

Sent to others from SHECA via the following address:

The latest address in SHECA’s postal record

9.12 Amendments

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

9.12.1 Procedure for Amendment

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

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

9.12.2 Notification Mechanism and Period

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

SHECA publishes the revision results on www.sheca.com and SHECA repository.If modification of this CPS is placed in SHECA repository (check www.sheca.com), it equals to modify this CPS. These modifications shall take place of any conflicting and designated terms in CPS original version.

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

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

9.12.3 Comment Period

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

9.12.4 Circumstance under Which CPS Must Be Modified

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

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

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

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

9.13 Dispute Resolution Provisions

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

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

9.14 Governing Law

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

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

9.15 Compliance with Applicable Law

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

9.16 General Provisions

9.16.1 Entire Agreement

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

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

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

9.16.2 Assignment

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

9.16.3 Severability

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

SHECA also (prior to issuing a certificate under the modified requirement) notify the CA/Browser Forum of the relevant information newly added to its CPS by sending a message to questions@cabforum.org and receiving confirmation that it has been posted to the Public Mailing List and is indexed in the Public Mail Archives available at https://cabforum.org/pipermail/public/ (or such other email addresses and links as the Forum may designate), so that the CA/Browser Forum may consider possible revisions to these Requirements accordingly.

An appropriate change in practice, modification to the SHECA’s CPS and a notice to the CA/Browser Forum, as outlined above, must be made within 90 days.

9.16.4 Enforcement

Not applicable.

9.16.5 Force Majeure

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

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

9.17 All property of security information

Unless otherwise agrees, the following - information and data related security is considered to parties property, indicated as the following:

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