UniTrust Network Trust Service Hierarchy

Extended Validation Certificates Policies

Version 1.3

Valid from: 24-05-2017

Shanghai Electronic Certificate Authority Center Co.Ltd

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

UniTrust Network Trust Service Hierarchy Extended Validation Certificates Policies

Any company or individual who requires this document can contact the strategy development department of Shanghai Electronic Certificate Authority Center Co.

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

Tel: 86-21-36393195

E-mail: policy@sheca.com

Brand Explanation

"UniTrust" is registered trademark of Shanghai Electronic Certificate Authority Center Co., which is also the service identification of SHECA.

Changing History Record of this document

Version	Valid date	Author	Issuer	Notes
V1.3	24-05-2017	Ruby Xiong	SHECA Security Authentication Committee	Current version
V1.2	25-05-2016	John Cui	SHECA Security Authentication Committee	Previous version
V1.1	25-04-2014	John Cui	SHECA Security Authentication Committee	Previous version
V1.0	28-04-2013	John Cui	SHECA Security Authentication Committee	Previous version

Statements:

CP endorses in whole or in part the following standards:

Guidelines For The Issuance And Management Of Extended Validation Certificates

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

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

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

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

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

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

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

Table of Contents

1. Introduction

1.1 Overview

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

This document is named as UniTrust Network Trust Service Hierarchy Extended Validation Certificates Policies(UNTSH EV CP), which is based on 'Guidelines For The Issuance And Management Of Extended Validation Certificates' (EV Guidelines) issued by CA/Browser Forum and relative rules issued by National electronic certification services competent authorities, applicable to all EV digital certificate issued and managed by UNTSH.

As EV Certificate Supreme policy and the basis of management, and operation for EV certificates throughout the UNTSH, and setting a limit and basic provisions for right obligations relationship of the participation parties, this CP clarifies the framework of UNTSH EV certificate and related service of operation process, requirements of business, technology and legal for security and full to implement these process.

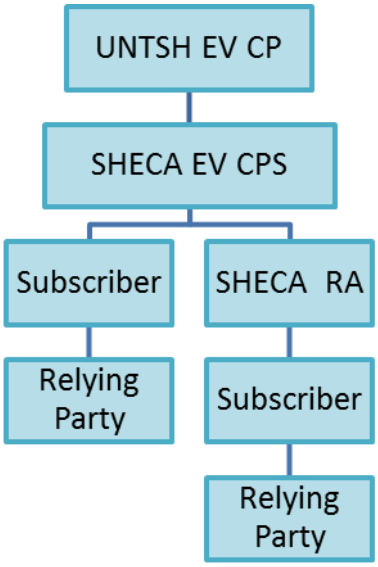
SHECA as a certification authority (CA), generates and operates EV root certificates, EV sub CA certificate, and issues subscriber certificates under the constraints of the CP. SHECA EV Certification Practice Statement (CPS) be bound by the CP, gives details on SHECA as Electronic verification service agencies providing certificates, how to provide certificates and the corresponding administration, operation and security measures. All UNTSH certificates of subscribers and relying parties must use and trust the certificate referring to the provisions of the CP and CPS.

This CP is continuously audited by an independent third party, and SHECA posts the audit reports on www.sheca.com.

1.1.1 UNTSH Structure

The CP is the supreme UNTSH EV certificate policy. The certificate Authorities of UNTSH develops CPS according to CP. RA perform certificate application identification in comply with the CP and EV CPS. Subscriber, relying party and related entities use and trust certificate in accordance with this CPS and EV CP while performing obligations.

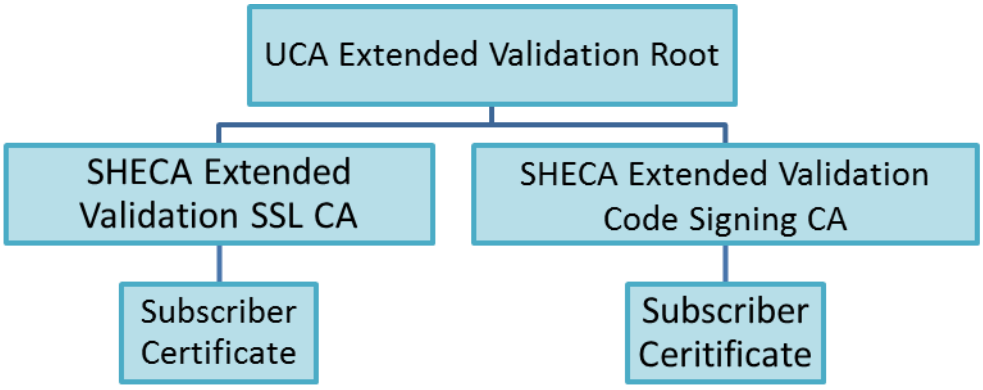
UNTSH contains a root CA, subordinate CA, registration authority (RA), these entities are different service providers within UNTSH. EV Certificate services and management within UNTSH should complete, accurate and comprehensive meet the requirement of CPS and EV CP.



1.1.2 UNTSH EV Certificate hierarchical structure

UNTSH consists of one EV ROOT CA called UCA Extended Validation Root, two subordinate CA called SHECA Extended Validation SSL CA and SHECA Extended Validation Code Signing CA issuing subscriber EV SSL certificate and EV Code signing Certificate.

UNTSH PKI hierarchical structure：



1.1.3 UNTSH EV Certificate Trust Hierarchy

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

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

1.2 Document Name and Identification

This document is UniTrust Network Trust Service Hierarchy Extended Validation Certificates Policies, abbreviated as UNTSH EV CP.

The CP object identifier (OID) is1.2.156.112570.149.

1.3 PKI Participants

1.3.1 Certification Authorities (CA)

CA is issuing entity, responsible for the issuance of the EV certificate, operating and management constructed and operated by SHECA.

Main responsibility of CA includes:

- issue and manage certificates.
- manage and distribute relevant certificates, certificate revocation lists (CRL)
- manage and operate certificate repository
- develop and distribute relevant policies, CPS and Specifications

1.3.2 Registration Authorities (RA)

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

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

1.3.3 Subscribers

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

1.3.4 Relying Parties

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

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

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

1.3.5 Other Participants

None.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Usage

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

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

1.4.2 Prohibited Certificate Uses

EV Certificates issued by SHECA shall be used only to the extent as described in Section 1.4.1. It is prohibits to use the EV Certificate in applications or business which may result in any personal injury or death, mental injury or hazards in the social order and public interests.

EV Certificates shall be used only to the extent which is consistent with Electronic Signature Law and other applicable law.

1.5 Policy Administration

1.5.1 Organization Administering the Document

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

1.5.2 Contact Person

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

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

Tel : 86 -21-36393195

Fax : 86 -21-36393200

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

Postal Code: 200080

Email: policy@sheca.com

1.5.3 Person Determining CP Suitability for the Policy

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

1.5.4 CP Approval Procedures

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

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

1.6 Definitions and Acronyms

Refer to Appendix A.

2. Publication and Repository Responsibilities

2.1 Repositories

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

The website of repositories is the following:www.sheca.com

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

2.2 Publication of Certificate Information

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

SHECA provide clear address and method. The certificates, certificate revocation lists and online status inquiry are released by online way, which is a part of Certificate Services.

In addition, SHECA publishes certificate policy, certification practice statement, the related agreements in a fixed URL, www.sheca.com/repository .

2.3 Time or Frequency of Publication

This Certificate Policy shall be published in repository as soon as possible after the approval of SHECA Security Authentication Committee.

SHECA should issue CRLs for Subscribers Certificates at least every 24 hours, ARL for Sub-CA Certificate every 3 months and Root-CA Certificate every year. Information should be published on website timely if a Root-CA certificate is revoked.

2.4 Access control on repositories

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

3. Identification and Authentication

3.1 Naming

3.1.1 Types of Names

EV Certificate contains an X.501 Distinguished Name (DN) in the Issuer and Subject fields.

EV SSL Certificates, EV code signing (Code Signing) certificate naming rules and requirements should clearly documented in CPS and compliant with the requirements of part 9 in Guide publish by CA / Browser Forum on www.cabforum.org. Distinguished names of EV SSL Certificates, EV Code Signing certificates' distinguished name must contain the common name (CN =), identified common name should contain the domain name, email addresses, institution's legal name and etc.

3.1.2 Need for Names to be Meaningful

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

3.1.3 Anonymity or Pseudonymity of Subscribers

Subscribe certificate is not permitted to use anonymity or pseudonyms.

3.1.4 Rules for Interpreting Various Name Forms

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

3.1.5 Uniqueness of Names

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

3.1.6 Solution of Naming Dispute

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

3.1.7 Recognition, Authentication, and Role of Trademarks

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

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

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

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

The certificate applicant must demonstrate that it rightfully holds the private key corresponding to the public key to be listed in the Certificate. The method to prove possession of a private key shall be PKCS #10, another cryptographically equivalent demonstration, or another SHECA-approved method.

3.2.2 Authentication of Organization Identity

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

3.2.3 Authentication of Individual Identity

SHECA does not accept any individual EV Certificates application.

3.2.4 Non-Verified Subscriber information

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

3.2.5 Validation of Authority

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

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

3.2.6 Criteria for Interoperation

No stipulation.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

Subscriber should re-applicant the certificate as descript in Section 3.2 before the EV certificate expires.

3.3.2 Identification and Authentication for Re-key After Revocation

Subscriber should re-applicant the certificate as descript in Section 3.2 with regenerated key pair after the revocation of EV Certificate

3.4 Identification and Authentication for Revocation Request

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

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application?

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

4.1.2 Enrollment Process and Responsibilities

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

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

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

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

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

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

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

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

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

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

4.2.2 Approval or Rejection of Certificate Applications

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

If the laws and regulations clearly prohibit certain application, or which SHECA considered a high-risk, SHECA should reject the application.

4.2.3 Time to Process Certificate Applications

SHECA should complete processing certificate applications within a reasonable time.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

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

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

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

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

The following conduct constitutes certificate acceptance:

- Downloading or installing a Certificate.
- Fail to object to the certificate or its content.

4.4.2 Publication of the Certificate by the CA

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

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

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

Subscribers shall protect their private keys from unauthorized use and don't use expired or revoked certificate. Private key can't be archived.

4.5.2 Relying Party Public Key and Certificate Usage

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

Reliance on a certificate must be reasonable under the circumstances. If the circumstances indicate a need for additional assurances, the Relying Party must obtain such assurances for such reliance to be deemed reasonable.

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

- Certificates are appropriate for any particular purpose, and these used to determine if the certificate has not been the CP prohibits or restricts, SHECA has no responsibility to assess whether the certificate has been properly used
- That the certificate is being used in accordance with the *KeyUsage* field extensions included in the certificate.
- The status of the certificates in the certificate should be verified. If any of the certificate in the Certificate Chain has been revoked, the Relying Party should judge independently whether the digital signature is signed prior to the revocation.

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

4.6 Certificate Renewal

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

4.6.1 Circumstances for Certificate Renewal

SHECA doesn't the updated service of EV Certificates.

4.6.2 Who May Request Renewal

Not applicable.

4.6.3 Processing Certificate Renewal Requests

Not applicable.

4.6.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Not applicable.

4.6.6 Publication of the Renewal Certificate by the CA

Not applicable.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.7 Certificate Rekey

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

4.7.1 Circumstances for Certificate Rekey

Certificate key renewal refers to requirements in Section 3.3.1.

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

4.7.2 Who May Request Rekey

Subscribers are the subjects of certificate re-key application.

4.7.3 Processing Certificate Rekey Requests

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

Certificate issuance is in accordance with Section 4.3.

4.7.4 Notification of New Certificate Issuance to Subscriber

Refer to Section 4.3.2

4.7.5 Conduct Constituting Acceptance of a Rekey Certificate

Refer to Section 4.4

4.7.6 Publication of the Rekey Certificate by the CA

Refer to Section 4.4.2.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

Refer to Section 4.4.3.

4.8 Certificate Modification

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

4.8.1 Circumstances for Certificate Modification

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

4.8.2 Who May Request Certificate Modification

Not applicable.

4.8.3 Processing Certificate Modification Requests

Not applicable.

4.8.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Not applicable.

4.8.6 Publication of the Modified Certificate by the CA

Not applicable.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.9 Certificate Revocation and Suspension

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

4.9.1 Circumstances for Revocation

Occurrence of the following circumstances, the subscriber certificate may be revoked:

- Subscribers hang the request of withdrawal
- Within the validity period, the information contained in the subscriber certificate changes, exists errors or mistakes or inconsistent with the actual information of subscriber, fake information in a certificate request, or a certificate request has not been validly licensed
- Subscriber information in EV SSL certificate is substantially changed
- After certificate insurance, fake information is found by SHECA in the application materials provided by EV SSL certificate subscriber
- The application of certificate is not authorized or can't be traced to the authorization
- Subscriber doesn't use EV SSL certificate according to CP/CPS or the agreement, or changes the usage of EV SSL certificate; they use this certificate to fishing, cheat or other crimes.

- Private key of subscribers is confirmed or suspected to be cracked, damaged, lost, or tampered
- Certificate is not used properly, or is misused or used in illegal ways
- Subscribers violates the obligations of CP and CPS, Subscriber Agreement and other provisions, representations or warranties, or subscribers cannot fulfill the obligations specified in the relevant agreement
- SHECA terminates operation and has not arranged other EV certificate issuing authorities to offer revoke services; or SHECA no longer have the rights or qualifications to issue EV SSL certificates
- Subscribers failed to fulfill the obligation to pay
- Continuity of using the certificate will cause harm to SHECA
- Private key of SHECA EV Root or EV sub CA certificate exists security risk or SHECA no longer have the right to issue EV certificates or qualifications, or SHECA found issuance of a certificate does not comply with the guide or SHECA EV certificate policy
- Evolution of technologies or standards may lead to unacceptable risk for the relying party or software providers.
- Judgments of the judiciary leads that the certificate subject information does not remain effective or continue to be trusted, or the relevant provisions of laws and regulations or requirements

4.9.2 Who Can Request Revocation

The following entities may require certification 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

Only SHECA may revoke root certificate or subordinate CA certificate

4.9.3 Procedure for Revocation Request

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

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

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

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

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

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

(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

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

4.9.5 Time within Which CA Must Process the Revocation Request

SHECA shall take reasonable steps after receiving the revocation request, and can't be delayed.

4.9.6 Revocation Checking Requirements for Relying Parties

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

4.9.7 CRL Issuance Frequency

For subscribers certificate, SHECA should issue and publish certificate revocation list at least every 24 hours, for the sub-CA certificate, at least every three months, for the root CA certificate, the certificate revocation list must be published once a year .

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

4.9.8 Maximum Latency for CRLs

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

4.9.9 On-Line Revocation/Status Checking Availability

SHECA provide online certificate status inquiry service (OCSP) certificates to subscribers and relying parties. OCSP availability complies with requirements in Section 13 of Guide issued by CA / Browser Forum via www.cabforum.org.

4.9.10 On-Line Revocation Checking Requirements

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

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation

4.9.12 Special Requirements Related to Key Compromise

When private key of SHECA CA certificate is suspected or actual damage scenarios occurs, all participants of UNTSH should be told through reasonable efforts.

4.9.13 Circumstances for Suspension

SHECA does not support suspension of EV Certificates.

4.9.14 Who Can Request Suspension

Not applicable

4.9.15 Procedure for Suspension Request

Not applicable

4.9.16 Limits on Suspension Period

Not applicable

4.10 Certificate Status Services

4.10.1 Operational Characteristics

The Status of public certificates can be queried via CRL, LDAP directory and via an OCSP responder. Such certificate status services should request a reasonable response time for queries and concurrent processing capabilities.

4.10.2 Service Availability

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

4.10.3 Operational Features

Refer to Section 4.9.9 and 4.9.11.

4.11 End of Subscription

When SHECA EV Root certificate or EV CA certificate validity ends, certificate revocation, SHECA end its operations, all SHECA would mean the termination of service of the certificate was issued, unless the law provides otherwise.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

EV private keys are never escrowed. SHECA does not offer Key Recovery Services to Subscribers.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5. Facility, Management, and Operational Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

CA and RA operations are conducted within a physically protected environment, and prevent and check unauthorized usage, access or disclosure to the sensitive information or system.

5.1.2 Physical Access

Access to each of the physical security layer should be auditable and controllable to ensure that only authorized personnel gets access.

5.1.3 Power and Air Conditioning

The secure facilities of CA and RA are equipped with backup diesel generator and UPS to ensure continuous, uninterrupted access to electric power. Besides, the facility room is equipped with independent air conditioning systems to control temperature and relative humidity.

5.1.4 Water Exposures

The secure facilities of CA and RA can prevent flooding or other damage caused by the flooding via construction, equipment and feasible measures.

5.1.5 Fire Prevention and Protection

The server room is decorated with fire-resistant materials, with a smoke alarm system, automatic gas fire extinguishing system.

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

5.1.6 Media Storage

CA and RA should protect back up critical system data or sensitive information of magnetic storage media for protection to avoid damage caused by water, fire, or other physical factors, and take protective measures to prevent, detect, and prevent the media from unauthorized use, access or disclosure.

5.1.7 Waste Disposal

CA and RA should conduct waste (file, media or other waste) disposal procedure, preventing unauthorized use, visit or disclosure of sensitive and confidential information.

5.1.8 Off-Site Backup

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

5.2 Procedural Controls

5.2.1 Trusted Roles

Employees, contractors and consultants who is designated as the credibility of the management infrastructure should be regarded as trusted personnel in trusted positions, and must meet the requirements of the CP.

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

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

Trusted Persons include, but are not limited to:

- customer service personnel

- system administration personnel
- designated engineering personnel
- Executives that are designated to manage infrastructural trustworthiness.

5.2.2 Number of Persons Required per Task

CA and RA must establish, maintain and enforce rigorous control procedures to ensure segregation of duties based on job responsibilities and to ensure that multiple Trusted Persons are required to perform sensitive tasks. Policy and control procedures are in place to ensure segregation of duties based on job responsibilities. The most sensitive tasks, such as access to and management of CA cryptographic hardware (cryptographic signing unit or CSU) and associated key material, require multiple Trusted Persons.

These internal control procedures are designed to ensure that at a minimum, two trusted personnel are required to have either physical or logical access to the device. Access to CA cryptographic hardware is strictly enforced by multiple Trusted Persons throughout its lifecycle, from incoming receipt and inspection to final logical and/or physical destruction. Once a module is activated with operational keys, further access controls are invoked to maintain split control over both physical and logical access to the device. Persons with physical access to modules do not hold “Secret Shares” and vice versa.

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

5.2.3 Identification and Authentication for Each Role

CA and RA should take strict role authorization and identity for all staff that will become the trusted roles by required identity documents, smart card or USB Key token or other authentication password ways.

Identification should include human resources and security screening and background investigation process in accordance with this CP.

For all personnel seeking to become Trusted Persons, verification of identity should be performed by CA and RA by devices such as ID, smart cards or USB key or identity password verification.

5.2.4 Roles Requiring Separation of Duties

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

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

5.3 Personnel Controls

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

5.3.1 Qualifications, Experience, and Clearance Requirements

SHECA operators of certification business systems must have credible, high characteristic enthusiasm, no part-time sexual influential Certificate Services, no irresponsible record in certificate services and no poor record of lawlessness.

System operator, certificate management or internal control person must have relevant experience, relevant knowledge and technology of certificate service.

5.3.2 Background Check Procedures

SHECA certificate Services practitioners should be on board after background check and business capacity investigation according to background check standard. Generally, based on job requirements, operational capacity survey should be conducted every two years for each appropriate staff as the basis of qualification.

Background check must comply with legal and regulatory requirements, conducted by the HR department and the business units separately according to the survey content.

5.3.3 Training Requirements

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

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

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

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

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

5.3.4 Retraining Frequency and Requirements

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

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

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

5.3.7 Independent Contractor Requirements

In limited circumstances of human resource or special requirements, CA and RA can use independent contractors or consultants to fill Trusted Positions 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.

5.3.8 Documentation Supplied to Personnel

SHECA provides its employees the requisite training and other documentation needed to perform their job responsibilities competently and satisfactorily.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

CA and RA log the following audit events, manually or automatically, including the date and time the event occurred and the entity or person caused the event.

CA should record in CPS of logs and events types:

- Running event, including but not limited to Key generation of CA and Sub CA; System and application startup and shutdown; CA Key and information change, Password equipment life-cycle-related events; CA private key activation data manipulation and physical access logs; Changes and maintenance of system configuration including key, activation data or Media Destruction of Personal Information
- Certificate life cycle event, including but not limited to issuing, renewal, rekey, revocation, suspended;
- Trusted Person events, including but not limited to logon and logoff attempts, password creation, Delete and Set, User system rights chance, and related personnel changes
- Incident reports, including but not limited to, unauthorized logon attempts to system and network
- Read and write operations of certificate and information repository
- Certificate generation policy changes, such as changing validity
- Physical and Environmental Management

5.4.2 Frequency of Processing Log

Certification organizations should review audit logs regularly in order to verify real time alerts of significant security and operational events. Actions taken based on audit log reviews are also documented.

Review is carried out not less than twice a year.

5.4.3 Retention Period for Audit Log

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

5.4.4 Protection of Audit Log

Audit logs are protected avoid unauthorized viewing, modification, reading, deletion, or other tampering.

5.4.5 Audit Log Backup Procedures

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

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

5.4.6 Audit Collection System

No stipulation.

5.4.7 Notification to Event-Causing Subject

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

5.4.8 Vulnerability Assessments

Events are 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.

5.5 Records Archival

5.5.1 Types of Records Archived

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

- Audit data collected in Section 5.4;
- Certificate application information
- Certificate application documentation
- Certificate lifecycle information

5.5.2 Retention Period for Archive

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

5.5.3 Protection of Archive

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

5.5.4 Archive Backup Procedures

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

Paper materials need to be preserved in the secure facility.

5.5.5 Requirements for Time-Stamping of Records

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

5.5.6 Archive Collection System

All filing related to certification services are performed by internal staff in accordance with privileges and responsibilities.

5.5.7 Procedures to Obtain and Verify Archive Information

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

5.6 Key Changeover

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

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

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

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

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

5.7.3 Entity Private Key Compromise Procedures

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

5.7.4 Business Continuity Capabilities After a Disaster

CA and RA should develop, build, test, maintain and execute a disaster recovery plan when necessary to mitigate the effects of any manual or natural catastrophes. Disaster recovery plan should clarify conditions of activation plan, acceptable system outage and system recovery time.

Business continuity should be clearly documented in CPS, and compliant with requirements in Section 16 of guide that CA / Browser Forum (CA / Browser Forum) published by www.cabforum.org.

5.8 CA or RA Termination

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

5.9 Data Security

Data security should be clearly documented in CPS, and compliant with section 16 of guides issued by the CA / Browser Forum through www.cabforum.org.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

CA key pair is generated by device with approval and permission of the national competent authority. Due to strict requirements for cryptographic products and systems, SHECA should comply with relevant state regulations during key generation, management, storage, backup

and recovery. Besides, SHECA should follow CNS 15135, ISO 19790, or Hardware CA key generation and management regulations FIPS140-2 standard, and use standard hardware devices to generate and manage CA keys.

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

6.1.2 Private Key Delivery to Subscriber

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

6.1.3 Public Key Delivery to Certificate

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

6.1.4 CA Public Key Delivery to Relying Parties

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

6.1.5 Key Sizes

Key length should be clearly documented in CPS, and compliant with the requirements in Section 9.5 of reference issued by CA/Browser Forum via www.cabforum.org .

6.1.6 Public Key Parameters Generation and Quality Checking

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

6.1.7 Key Usage Purposes

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

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

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

Specific refer to hardware product information provided by the device manufacturer with production qualification required by national code authorities.

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

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

6.2.3 Private Key Escrow

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

6.2.4 Private Key Backup

According to specified in 6.2.2, SHECA backups CA private key in encryption way, and encryption key to protect the information is stored in the secret-division multiple smart cards with multi- held separately. Back up the private key of the CA hardware cryptographic modules meets the requirements of section 6.2.6.

6.2.5 Private Key Archival

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

6.2.6 Private Key Transfer Into or From a Cryptographic Module

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

6.2.7 Private Key Storage on Cryptographic Module

CA private keys held on hardware cryptographic modules shall be stored in encrypted form.

6.2.8 Method of Activating Private Key

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

6.2.9 Method of Deactivating Private Key

The activated private keys are deactivated upon logging off their system after Identification or automatically deactivate after predetermined time.

6.2.10 Method of Destroying Private Key

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

6.2.11 Cryptographic Module Rating

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

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

CA public key (including the root CA certificate and sub-CA certificate) should be archived.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

Certificate validity period should be clearly documented in the CPS and compliant with the requirements in Section 9.4 of reference issued via www.cabforum.org by CA/Browser Forum.

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

According to the different key length, key pair validity varies accordingly:

- 4096 bit CA key, up to 30 years
- 2048 bit CA key, up to 27 years
- 2048 bit subscriber key, up to 27 months

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

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

6.4.2 Activation Data Protection

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

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

6.4.3 Other Aspects of Activation Data

No stipulation

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

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

System security should be clearly documented on CPS and compliant with section 16.5 requirements published by CA / Browser Forum (CA / Browser Forum) through www.cabforum.org.

6.5.2 Computer Security Rating

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

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

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

6.6.2 Security Management Controls

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

Use of the system has strict control measures and all systems are rigorously tested to verify before using. Any modifications and upgrades will be recorded with version control, functional testing and records. SHECA inspects and tests authentication system regularly and irregularly.

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

6.6.3 Life Cycle Security Controls

No stipulation

6.7 Network Security Controls

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

6.8 Time-Stamping

No stipulation

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

7.1.1 Version Number(s)

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

7.1.2 Certificate Extensions

SHECA issues EV certificates in compliance with RFC 5280 and requirement of 'Guidelines for the Issuance and Management of Extended Validation Certificates'. See in particular annexes: certificate format specification.

EV SSL certificate extension should be clearly documented in CPS and compliant with section 9.3 published by CA / Browser Forum Guidelines (CA / Browser Forum) through www.cabforum.org.

7.1.3 Algorithm Object Identifiers

SHECA Certificates uses the following algorithms(OID):

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

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

7.1.4 Name Forms

SHECA issues EV certificates with Name Forms and Content comply with X.501 （Distinguished Name；DN）following RFC 5280 regulation.

7.1.5 Name Constraints

SHECA uses the nameConstraints extension as required.

7.1.6 Certificate Policy Object Identifier

Where the Certificate Policies extension is used, SHECA EV Certificates contain the object identifier for the Certificate Policy（certificatePolicies）

The object identifier should be clearly documented in CPS and compliant with section 9.3 published by CA / Browser Forum Guidelines (CA / Browser Forum) through www.cabforum.org.

7.1.7 Usage of Policy Constraints Extension

SHECA uses the policyConstraints extension as required.

7.1.8 Policy Qualifiers Syntax and Semantics

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

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation

7.2 CRL Profile

7.2.1 Version Number(s)

SHECA issues X 509 V2 version of CRLs.

7.2.2 CRL and CRL Entry Extensions

No stipulation

7.3 OCSP Profile

7.3.1 Version Number(s)

Version 1 of the OCSP specification is defined by RFC2560.

7.3.2 OCSP Extensions

OCSP extensions comply with RFC 2560 specifications.

8. Compliance Audit and Other Assessments

8.1 Frequency and Circumstances of Assessment

SHECA conducts an internal and external audits and evaluations at least once a year.

Audit operations should be clearly documented in CPS, and compliantwith requirements in section 15 of guide published by CA / Browser Forum (CA / Browser Forum) through www.cabforum.org.

8.2 Identity/Qualifications of Assessor

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

When conducting an external audit, audit assessment should choose a professional institution with national or internationally recognized qualification, with good reputation and wealth of practical experience.

8.3 Assessor's Relationship to Assessed Entity

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

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

8.4 Topics Covered by Assessment

SHECA audit conducted mainly includes the following:

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

8.5 Actions Taken as a Result of Deficiency

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

SHECA conducts follow-up rectification as needed.

8.6 Communications of Results

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

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

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

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

9.1.2 Certificate Access Fees

SHECA does not charge a fee as a condition of making a Certificate available in a repository or otherwise making Certificates available to Relying Parties.

9.1.3 Revocation or Status Information Access Fees

SHECA does not charge a fee as a condition of making the CRLs required by the CP available in a repository or otherwise available to Relying Parties.

9.1.4 Fees for Other Services

No stipulation.

9.1.5 Refund Policy

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

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

9.2 Financial Responsibility

9.2.1 Liability

SHECA would bear the liability in accordance to following:

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

9.2.2 Other Assets

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

9.2.3 Insurance or Warranty Coverage for End-Entities

See section 9.2.1

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The following records shall be kept confidential and private:

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

9.3.2 Information Not Within the Scope of Confidential Information

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

9.3.3 Responsibility to Protect Confidential Information

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

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

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

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

9.4.2 Information Treated as Private

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

9.4.3 Information Not Deemed Private

All information made public in a certificate is deemed not private

9.4.4 Responsibility to Protect Private Information

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

9.4.5 Notice and Consent to Use Private Information

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

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

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

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

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property rights

1. SHECA retain all intellectual property rights in and to SHECA private key, certificate issued, CRL, CP/CPS and other relevant documents.
2. Subscribers retain all intellectual property rights in and to subscriber private key pairs. SHECA will own intellectual right on Certificate once the public key is signed by

SHECA to issue the certificate. Subscriber and relying party only have the certificate-use right.

3. SHECA does not guarantee intellectual property rights set forth in the certificate name.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

SHECA as CA and RA warrants that:

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

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

9.6.2 RA Representations and Warranties

See section 9.6.1 requirements.

9.6.3 Subscriber Representations and Warranties

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

1. Applicant must understand and agree the requirements of CP/CPS and relevant agreement when apply for a EV Certificate,
2. All information and documents in the Certificate Application the Subscriber submitted are true and authentic,
3. Their private key is protected, using the certificate in accordance with restriction discloses in CP/CPS and laws.
4. Applicant should ensure the accurate of information contained in EV Certificate while accept it, also should validate the correspondence of public key and private key in EV Certificate.
5. Subscriber should notify SHECA when the relevant information in the certificate changes occur.

6. Subscriber should inform SHECA in due time when the private key is lost, leakage or others, and apply for certificate revocation as required. Meanwhile the subscriber should bear the risk and liability arising from using of the certificate before the certificate's revocation status published.
7. Timely renewal certificate in accordance with SHECA provisions,
8. Accept all statements, changes, renewal and upgrades disclosed by SHECA bases on regulation and technology development,

9.6.4 Relying Party's Representations and Warranties

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

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

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

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

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

9.8 Limitations of Liability

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

9.9 Indemnities

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

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

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

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

9.10 Term and Termination

9.10.1 Term

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

9.10.2 Termination

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

9.10.3 Effect of Termination and Survival

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

9.11 Individual Notices and Communications with Participants

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

9.12 Amendments

9.12.1 Procedure for Amendment

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

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

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

9.12.2 Notification Mechanism and Period

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

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

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

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

9.12.3 Circumstances Under Which CP Must be changed

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

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

9.12.4 Object Identifier change

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

9.13 Dispute Resolution Provisions

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

9.14 Governing Law

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

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

9.15 Compliance with Applicable Law

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

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation

9.16.2 Assignment

No stipulation

9.16.3 Severability

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

9.16.4 Enforcement

No stipulation

9.16.5 Force Majeure

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

9.17 Other Provisions

No stipulation.

Appendix A The Definitions and Glossary

SHECA

Abbreviation for Shanghai Electronic Certificate Authority Center Co., Led

UniTrust Network Trust Service Hierarchy

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

SHECA Security Authentication Committee

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

Certificate Authority

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

Registration Authority

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

Registration Authority Terminal

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

Electronic Certificate

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

Electronic Signature

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

Digital Signature

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

Electronic Signatory

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

Electronic signature relying party

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

Private Key (Electronic Signature Creation Data)

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

signatory in the electronic signature application.

Key (Electronic Signature Verification Data)

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

Subscriber

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

Relying Party

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