UniTrust Network Trust Service Hierarchy Certificate Policies (UNTSH CP)

Version 1.5.6

Effective Date: May 21, 2024

Shanghai Electronic Certificate Authority Center Co., ltd

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

《UniTrust Network Trust Service Hierarchy Certificate Policies》

Any organization or individual who requires this document could contact with Strategy Development Department of Shanghai Electronic Certification Authority Co., ltd.

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

Revision History

Version	Effective Date	Author	Issuer	Notice
V1.5.6	May 21, 2024	Alice Shao	SHECA Security Certification Commission	Current Version
V1.5.5	March 13, 2024	Alice Shao	SHECA Security Certification Commission	Previous Version
V1.5.4	November 23, 2023	Alice Shao	SHECA Security Certification Commission	Previous Version
V1.5.3	July 19, 2023	Celia Yu	SHECA Security Certification Commission	Previous Version
V1.5.2	June 12, 2023	Celia Yu	SHECA Security Certification Commission	Previous Version
V1.5.1	April 18, 2023	Celia Yu	SHECA Security Certification Commission	Previous Version
V1.5.0	April 18, 2022	Toria Chen	SHECA Security Certification Commission	Previous Version
V1.4.9	November 15, 2021	Toria Chen	SHECA Security Certification Commission	Previous Version
V1.4.8	June 18,2021	Toria Chen	SHECA Security Certification Commission	Previous Version
V1.4.7	April 29,2021	Toria Chen	SHECA Security Certification Commission	Previous Version
V1.4.6	August 11,2020	Toria Chen	SHECA Security Certification Commission	Previous Version
V1.4.5	June 5,2020	Toria Chen	SHECA Security Certification Commission	Previous Version
V1.4.4	April 30,2020	Toria Chen	SHECA Security Certification Commission	Previous Version
V1.4.3	April 2,2020	Toria Chen	SHECA Security Certification Commission	Previous Version
V1.4.2	May 29,2019	Toria Chen	SHECA Security Certification Commission	Previous Version
V1.4.1	Sept 10,2018	Toria Chen	SHECA Security Certification Commission	Previous Version
V1.4	Aug 31,2018	Toria Chen	SHECA Security Certification Commission	Previous Version
V1.3	June 7,2018	Toria Chen	SHECA Security Certification Commission	Previous version
V1.2	May 24,2017	Ruby Xiong	SHECA Security Certification Commission	Previous version
V1.1.3	May 25,2016	John Cui	SHECA Security Certification Commission	Previous version

V1.1.2.1	Septemper 1,2014	John Cui	SHECA Security Certification Commission	Previous version
V1.1.2	April 25,2014	John Cui	SHECA Security Certification Commission	Previous version
V1.1.1	April 8,2010	John Cui	SHECA Security Certification Commission	Previous version
V1.1	April 23,2009	John Cui	SHECA Security Certification Commission	Previous version
V1.0	March 26,2009	John Cui	SHECA Security Certification Commission	Previous version

Changes Description

Version	Description
V1.5.6	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 algorithmobject identifiers of ECDSA; Modify version as required by Code Signing Baseline Requirements; Adjustment of wording
V1.5.5	Modify version as required by S/MIME Baseline Requirements; Disclosure of reissued corss-signed UCA Global G2 Root
V1.5.4	Wording adjustment
V1.5.3	Disclosure of newly issued Sub-CAs Xinnet DV SSL /Xinnet OV SSL
V1.5.2	Information of reissued corss-signed UCA Global G2 Root
V1.5.1	Disclosure of newly issued Sub-CAs SHECA OV Server CA G7; Update Sub-CAs status; Update ARL /CRL renewal cycle
V1.5.0	Disclosure of newly issued Sub-CAs
V1.4.9	Information about disable partial Subordinate Roots Add the authentication method of staff certificate Description of key recovery service
V1.4.8	Update ARL renewal cycle Rrevise key length requirement of Code Signing and Timestamp certificate
V1.4.7	Disclosure of newly issued Sub-CAs
V1.4.6	Update name of supervision government agency
V1.4.5	Information of new subordinate root GlobalSign China CA for AATL
V1.4.4	Information of new Roots UniTrust Global Root CA R1, UniTrust Global Root CA R2, UniTrust Global Root CA R3 Add an initial investigation reporting mechanism
V1.4.3	Publish new corss-signed UCA Global G2 Root SSL certificate validity changed
V1.4.2	Information of new root certificate UniTrust PTC Root CA R1, UniTrust PTC Root CA R2

	Modified Individual and Organizaiton Identity Certificate validation process
V1.4.1	Added Changes Description
V1.4	Stated that SSL certificate do not issue test certificate Update renewal process of SSL and Code signing certificate Complete all BR required revocations reasons
V1.3	Modified UniTrust Network Trust Service Hierarchy; Added Object Identifier (OID); Algorithm Object Identifiers
V1.2	Modified UniTrust Network Trust Service Hierarchy; Added the Situation of Certificate Revocation; Revised Archive Record Retention Time Modified certificate and key pair validity
V1.1.3	Added Root UCA Global G2
V1.1.2.1	Stated External RA must not issue SSL and code signing Certificates
V1.1.2	Added Guidance; UniTrust Network Trust Service Hierarchy; Added the Situation of Certificate Revocation; Deleted Appendix B Certificate Format
V1.1.1	Contact information of SHECA Changed Deleted Appendix C CRL Format
V1.1	Added the Situation of Certificate Revocation Revised the Process of Revocation Request Added Appendix C CRL Format
V1.0	N.A.

Notices

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

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

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

Contents

1. Introduction

UniTrust Network Trust Service Hierarchy is an open public key infrastructure (called UniTrust) constructed and operated by Shanghai Electronic Certification Authority Co., ltd (acronymed SHECA), which provides electronic certification services based on digital certificate. SHECA, established as the third-party electronic certification authority in accordance with "People's Republic of China Electronic Signature Law ", is committed to create harmonious network environment and to provide secure, reliable, trustworthy digital certificate services.

This document called UniTrust Network Trust Service Hierarchy Certificate Policies(acronymed UNTSH CP), is UniTrust digital certificate service policy statement that is applied to all digital certificates issued and managed by UNTSH and its relevant participants. Certificate Policies is a named rule set used for indicating the adaptability of certificate for a specific body and(or)the application type that has the similar security requirements. Relying Party utilizes Certificate Policies to determine whether the certificate (and its binding)is trustworthy enough or not, or whether it is applied to a specific application. This CP sets forth business, legal and technical requirements and specifications for certificate application, issuance, management, usage, revocation, renewal and related trust services provided for all participants within the UNTSH. These specifications protect the security and integrity of certificate service and comprise a single set of rules that apply consistently UNTSH-wide, therefore offering assurances of uniform trust throughout the UNTSH. The CP is not a legal agreements between SHECA and UNTSH participants ;rather, contractual rights and obligations between SHECA and UNTSH participants are established by means of agreements with such participants.

This document is targeted at:

- UNTSH certification service providers who have to operate in terms of their own Certification Practices Statement (CPS) that complies with the requirements laid down by the CP

- UNTSH certificate Subscribers who need to understand how they are authenticated, what their rights and obligations are as UNTSH subscribers and how they are protected under the UNTSH

- Relying parties, who need to understand how much trust to place in a UNTSH certificate or a digital signature using that certificate

The CP does not govern any services outside the UNTSH. For example, SHECA establishes the internal CA for some enterprises or organizations who are responsible for operating.

The CP meets the requirements of structure and content in Certificate Policies and Certification

Practice Statement RFC3647 from The Internet Engineering Task Force (called IETF),and makes appropriate changes in accordance with Chinese laws and regulations together with operational requirements of SHECA.
SHECA conforms to the latest version of CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly – Trusted Certificates, Guidelines For The Issuance And Management Of Extended Validation Certificates, and Minimum Requirements for Code Signing Certificates published at www.cabforum.org .In the event that a discrepancy arises between interpretations of this document and standards, the standards shall govern.

1.1. Overview

As the highest policy, this CP provides a basis of management, operation and specification for certifications within the entire UNTSH, and determines a limitative range and basic provisions for the relationships of rights and obligations between the UNTSH participants. The CP establishes UNTSH root certificate framework, life-cycle, usage, reliance and managerial role, responsibility, procedure, as well as related subjects ' duties. As a operator of root certificate, SHECA manages the classes of root certificates under the UNTSH. The CP sets forth the operational procedures of all certificates and its relevant services under the UNTSH, and gives the business, technical and legal requirements to perform these procedures in security and integrity.

As a Certification Authority (CA), SHECA generates root certificates and subordinate certificates under the restriction of the CP, and issues certificates to subscribers. Registration Authorities (RAs) are entities which authenticate certificate requests under the UNTSH, and SHECA acts as an RA. Enterprises and organization also act as RAs, authenticating certificate requests for their relevant users by entering into contractual relationship with SHECA. Based on different types and application scope, Digital Certificates may be used by Subscribers to secure websites, digitally sign code, digitally sign documents and e-mails, and other different applications. Relying Party could decide whether to trust a certificate in accordance with the requirements of the relying party’s obligation in this CP. SHECA Certification Practice Statement elaborates the certificate SHECA as a electronic certification authority provides, and how to provide certificate and take corresponding managerial, operational and security measures. All certificate subscribers and relying parties under the UNTSH must refer to the provisions of the CP and its relevant CPS in order to determine the usage and reliability of certificate.

This CP shall be audited continuously by an independent third party, and SHECA will publish audit results at www.sheca.com.

1.1.1. UNTSH Framework

The CP is the highest strategy, certification authority (CA)under the UNTSH formulates CPS in accordance with CP.RA authenticates certificate requests according to the CP and its related

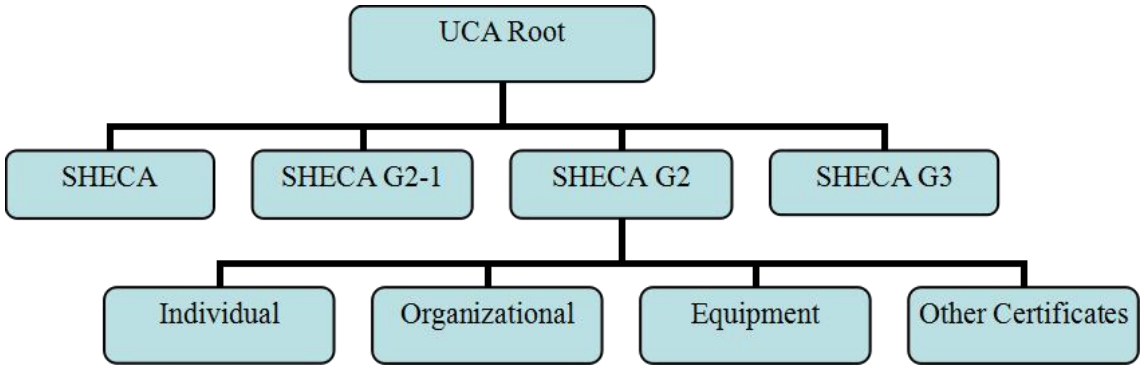
CPS,and subscribers,relying parties along with other correlative entities determine the usage, whether to trust it and other related obligations of certificate on the basis of the CP and its related CPS.UNTSH includes root CA,Subordinate CA,related RA, Registration Authority Terminal and other relevant authorized service entities,and those entities are service subjects at different classes within UNTSH. All services and management related with certificates within UNTSH perform and implement the requirements of the CP and its corresponding CPS in integrity, accuracy and entirety.

1.1.2. UNTSH Structure of Certificate Classes

UNTSH has 18 root certificates at present.All of them are self-issued, operated and managed by SHECA. Each root certificate authorizes subordinate certificate authorities to issue certificates to subscribers.

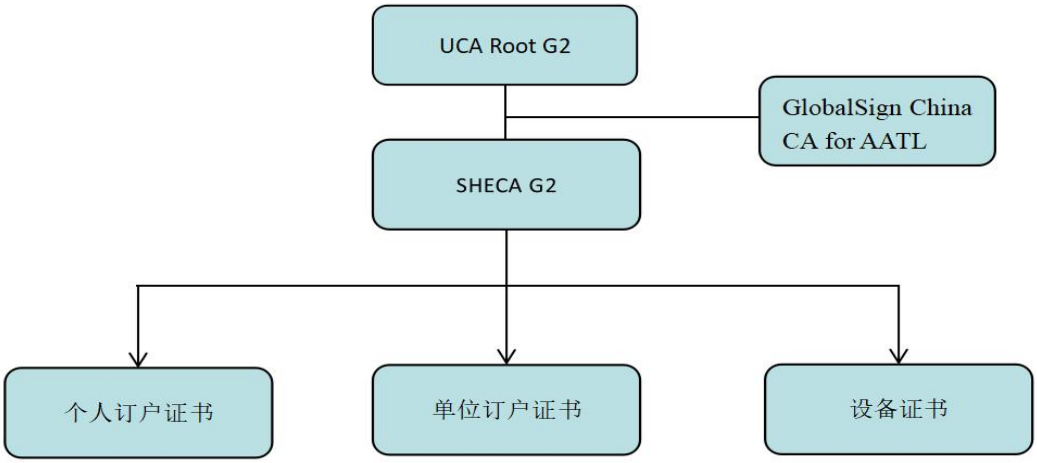
The structure of classes of PKI within UNTSH is as follows:

- UCA Root



The length of UCA Root root key is 2048-bit.There are four sub-CAs under UCA Root-G2, including: (1) SHECA G2 is responsible for issuing the 1024-bit or 2048-bit certificate individual certificates, organization certificates, equipment certificates and other certificates with RSA algorithm, and is forbidden to sign SSL certificates. (2)SHECA, SHECA G2-1 and SHECA G3no longer issue any subscriber certificates.
UCA Root will expire on December 31, 2029 and it will issue no subordinate certificates since January 1, 2025.

- UCA Root G2



The length of UCA Root G2 root key is 2048-bit, under which is two subordinate CAs.
Sub-CA SHECA G2 is responsible for issuing 2048-bit individual subscribers, organizational certificates, equipment certificates and other certificates; Sub-CA GlobalSign China CA for AATL is responsible for issuing 2048-bit document-signing certificates. On 26 December 2023, Sub-CA SHECA G2 was reissued to renew the validity period.
UCA Root G2 will expire on December 31, 2036 and will no longer issue any subordinate certificates since January 1, 2032.

- UCA Global G2 Root

The length of UCA Global G2 Root's root key is 4096-bit, UCA Global G2 Root will expire on December 31, 2040 and will no longer issue any subordinate certificates since January 1, 2036.
Asseco Data System S.A.'s Root CA namely Certum Trusted Network CA issued a cross signing Root CA UCA Global G2 Root on February 21th,2020, with validity period from February 21,2020 to February 21,2025,which was revoked on 28 April 2023.
On 28 March 2023, Asseco Data Systems S.A.'s Root CA namely Certum Trusted Network CA reissued the cross-root certificate UCA Global G2 Root, valid from 28 March 2023 to 21 February 2025.
On 8 January 2024, Asseco Data Systems S.A.'s Root CA namely Certum Trusted Network CA reissued the cross-root certificate UCA Global G2 Root, valid from 8 January 2024 to 6 January 2029.
UCA Global G2 Root have 16 sub-CAs in use, and 2 disabled sub-CAs.and 4 revoked sub-CAs.

Subordinate CA	Key Algorithm /length	Signing Algorithm	Issuing Certificates	Status
SHECA RSA Code Signing CA G3	RSA / 2048	SHA-256 with RSA Encryption	Code Signing Certificates	Revoked
SHECA RSA Domain Validation Server CA G3	RSA / 2048	SHA-256 with RSA Encryption	DV SSL Certificates	
SHECA RSA Organization Validation Server CA G3	RSA / 2048	SHA-256 with RSA Encryption	OV SSL Certificates	

SHECA RSA Time Stamp Authority G1	RSA / 2048	SHA-256 with RSA Encryption	Time Stamp Certificates	
SHECA DV Server CA G5	RSA / 2048	SHA-256 with RSA Encryption	DV SSL Certificates	In Use
SHECA OV Server CA G5	RSA / 2048	SHA-256 with RSA Encryption	OV SSL Certificates	
SHECA EV Server CA G2	RSA / 2048	SHA-256 with RSA Encryption	EV SSL Certificates	
SHECA Code Signing CA G4	RSA / 3072	SHA-256 with RSA Encryption	Code Signing Certificates	
SHECA Time Stamping CA G2	RSA / 3072	SHA-256 with RSA Encryption	Time Stamp Certificates	
TrustAsia RSA DV TLS CA - S1	RSA / 2048	SHA-256 with RSA Encryption	DV SSL Certificates	
TrustAsia RSA OV TLS CA - S1	RSA / 2048	SHA-256 with RSA Encryption	OV SSL Certificates	
SHECA SMIME CA G1	RSA / 2048	SHA-256 with RSA Encryption	SMIME Certificates	
Xinnet DV SSL	RSA / 2048	SHA-256 with RSA Encryption	DV SSL Certificates	
Xinnet OV SSL	RSA / 2048	SHA-256 with RSA Encryption	OV SSL Certificates	
SHECA Global G3 SSL	RSA / 2048	SHA-256 with RSA Encryption	SSL Certificates	Disabled
SHECA Global G3 Code Signing	RSA / 2048	SHA-256 with RSA Encryption	Code Signing Certificates	
JoySSL DV Secure Server CA	RSA / 3072	SHA-384 with RSA Encryption	DV SSL Certificates	In Use
JoySSL OV Secure Server CA	RSA / 3072	SHA-384 with RSA Encryption	OV SSL Certificates	
KeepTrust DV RSA TLS CA G1	RSA / 3072	SHA-384 with RSA Encryption	DV SSL Certificates	
KeepTrust OV RSA TLS CA G1	RSA / 3072	SHA-384 with RSA Encryption	OV SSL Certificates	
ZoTrus RSA DV SSL CA	RSA / 3072	SHA-384 with RSA Encryption	DV SSL Certificates	
ZoTrus RSA OV SSL CA	RSA / 3072	SHA-384 with RSA Encryption	OV SSL Certificates	

- UCA Extended Validation Root

The length of UCA Extended Validation Root's root key is 4096-bit, will expire on December 31, 2038 and will no longer issue any subordinate certificates since January 1, 2034, under which are 8 sub-CAs.

Subordinate CA	Key Algorithm /length	Signing Algorithm	Issuing Certificates	Status
SHECA RSA Extended Validation Code Signing CA	RSA 2048	SHA-256 with RSA Encryption	EV Code Signing Certificates	Revoked
SHECA RSA Extended Validation Server CA	RSA 2048	SHA-256 with RSA Encryption	EV SSL Certificates	
SHECA OV Server CA G6	RSA 2048	SHA-256 with RSA Encryption	EV SSL Certificates	
SHECA OV Server CA G7	RSA 2048	SHA-256 with RSA Encryption	EV SSL Certificates	In Use
SHECA EV Server CA G3	RSA 2048	SHA-256 with RSA Encryption	EV SSL Certificates	
SHECA EV Code Signing CA G2	RSA 3072	SHA-256 with RSA Encryption	EV Code Signing Certificates	
SHECA Extended Validation SSL CA	RSA 2048	SHA-256 with RSA Encryption	EV SSL Certificates	Disabled
SHECA Extended Validation Code Signing CA	RSA 2048	SHA-256 with RSA Encryption	EV Code Signing Certificates	

- UCA Root SM2

The length of UCA Root SM2 root key is 256 bits, SM Signature with SM3 algorithm, UCA Root

SM2 will expire on December 31, 2038 and will no longer issue any subordinate certificates since December 31, 2033,under which are 8 sub-CAs,

Subordinate CA	Key Algorithm /length	Signing Algorithm	Issuing Certificates	Status
UniTrust DV Secure Server	SM2 256	SM2 Signature with SM3	SM2 DV SSL Certificates	In Use
UniTrust OV Secure Server	SM2 256	SM2 Signature with SM3	SM2 OV SSL Certificates	
SHECA SM2	SM2 256	SM2 Signature with SM3	Individual Identity Certificate Organization Identity Certificate Device Certificate	
TrustAsia SM2 DV TLS CA - S1	SM2 256	SM2 Signature with SM3	SM2 DV SSL Certificates	
TrustAsia SM2 OV TLS CA - S1	SM2 256	SM2 Signature with SM3	SM2 OV SSL Certificates	
TrustAsia SM2 Identity CA - S1	SM2 256	SM2 Signature with SM3	Individual Identity Certificate Organization Identity Certificate	
SHECA SM2 Identity CA G1	SM2 256	SM2 Signature with SM3	Individual Identity Certificate	
CECloud Secure Server CA V1	SM2 256	SM2 Signature with SM3	SM2 SSL Certificates	

- UniTrust Global Root CA R1

The UniTrust Global Root CA R1 root key is 4096 bits, with RSA and SHA-384,. UniTrust Global Root CA R1 will expire on April 28, 2045 and on longer issue any subordinate certificates since April 28, 2040, which has 6 sub-CAs.

Subordinate CA	Key Algorithm /length	Signing Algorithm	Issuing Certificates	Status
SHECA DV Server CA 1A	RSA / 4096	SHA-384 with RSA Encryption	DV SSL Certificates	ceased
SHECA OV Server CA 1A	RSA / 4096	SHA-384 with RSA Encryption	OV SSL Certificates	
SHECA EV Server CA 1A	RSA / 4096	SHA-384 with RSA Encryption	EV SSL Certificates	
SHECA Code Signing CA 1A	RSA / 4096	SHA-384 with RSA Encryption	Code Signing Certificates	
SHECA EV Code Signing CA 1A	RSA / 4096	SHA-384 with RSA Encryption	EV Code Signing Certificates	
SHECA Time Stamping CA 1A	RSA / 4096	SHA-384 with RSA Encryption	Time Stamp Certificates	

- UniTrust Global Root CA R2

The UniTrust Global Root CA R2 root key is 384 bits, with ECDSA with ECDSA SHA-384. UniTrust Global Root CA R2 will expire on April 30, 2045 and no longer issue any subordinate certificates since April 20, 2040, which has 3 sub-CAs.

Subordinate CA	Key Algorithm /length	Signing Algorithm	Issuing Certificates	Status
SHECA DV Server CA 2A	ECC / NIST P-384	ECDSA Signature with SHA-384	ECC DV SSL Certificates	ceased
SHECA OV Server CA 2A	ECC / NIST P-384	ECDSA Signature with SHA-384	ECC OV SSL Certificates	
SHECA EV Server CA 2A	ECC / NIST P-384	ECDSA Signature with SHA-384	ECC EV SSL Certificates	

- UniTrust Global Root CA R3

The UniTrust Global Root CA R2 root key is 256 bits, with SM2 with SM3. UniTrust Global Root CA R2 will expire on April 30, 2045 and no longer issue any subordinate certificates since April 20, 2040, which has 3 sub-CAs.

Subordinate CA	Key Algorithm /length	Signing Algorithm	Issuing Certificates	Status
SHECA DV Server CA 2A	ECC / NIST P-384	ECDSA Signature with SHA-384	SM DV SSL Certificates	ceased
SHECA OV Server CA 2A	ECC / NIST P-384	ECDSA Signature with SHA-384	SM OV SSL Certificates	
SHECA EV Server CA 2A	ECC / NIST P-384	ECDSA Signature with SHA-384	SM EV SSL Certificates	

- UniTrust Global TLS RSA Root CA R1

UniTrust Global TLS RSA Root CA R1 key algorithm/length is RSA/4096, signing algorithm is sha384RSA, expiry date is March 37, 2039. It has 3 sub-CAs.

Subordinate CA	Key Algorithm /length	Signing Algorithm	Issuing Certificates	Status
SHECA DV TLS RSA CA 1A	RSA/3072	sha384RSA	RSA DV SSL Certificates	In Use
SHECA OV TLS RSA CA 1A	RSA/3072	sha384RSA	RSA OV SSL Certificates	
SHECA EV TLS RSA CA 1A	RSA/3072	sha384RSA	RSA EV SSL Certificates	

- UniTrust Global TLS ECC Root CA R2

UniTrust Global TLS ECC Root CA R2 key algorithm/length is ECDSA_P384, signing algorithm is sha384ECDSA, expiry date is March 37, 2039. It has 3 sub-CAs.

Subordinate CA	Key Algorithm /length	Signing Algorithm	Issuing Certificates	Status
SHECA DV TLS ECC CA 2A	ECDSA_P384	sha384ECDSA	ECC DV SSL Certificates	In Use
SHECA OV TLS ECC CA 2A	ECDSA_P384	sha384ECDSA	ECC OV SSL Certificates	
SHECA EV TLS ECC CA 2A	ECDSA_P384	sha384ECDSA	ECC EV SSL Certificates	

- UniTrust Global SMIME RSA Root CA R1

UniTrust Global SMIME RSA Root CA R1 key algorithm/length is RSA/4096, signing algorithm is sha384RSA, expiry date is March 37, 2039. It has 3 sub-CAs.

Subordinate CA	Key Algorithm /length	Signing Algorithm	Issuing Certificates	Status
SHECA MV SMIME RSA CA 1A	RSA/3072	sha384RSA	RSA MV SMIME Certificates	In Use
SHECA IV SMIME RSA CA 1A	RSA/3072	sha384RSA	RSA IV SMIME Certificates	

SHECA OV SMIME RSA CA 1A	RSA/3072	sha384RSA	RSA OV SMIME Certificates	

- UniTrust Global SMIME ECC Root CA R2

UniTrust Global SMIME ECC Root CA R2 key algorithm/length is ECDSA_P384, signing algorithm is sha384ECDSA, expiry date is March 37, 2039. It has 3 sub-CAs.

Subordinate CA	Key Algorithm /length	Signing Algorithm	Issuing Certificates	Status
SHECA MV SMIME ECC CA 2A	ECDSA_P384	sha384ECDSA	ECC MV SMIME Certificates	In Use
SHECA IV SMIME ECC CA 2A	ECDSA_P384	sha384ECDSA	ECC IV SMIME Certificates	
SHECA OV SMIME ECC CA 2A	ECDSA_P384	sha384ECDSA	ECC OV SMIME Certificates	

- UniTrust Global Code Signing RSA Root CA R1

UniTrust Global Code Signing RSA Root CA R1 key algorithm/length is RSA/4096, signing algorithm is sha384RSA, expiry date is March 37, 2039.

- UniTrust Global Code Signing ECC Root CA R2

UniTrust Global Code Signing ECC Root CA R2 key algorithm/length is ECDSA_P384, signing algorithm is sha384ECDSA, expiry date is March 37, 2039. It has 2 sub-CAs.

Subordinate CA	Key Algorithm /length	Signing Algorithm	Issuing Certificates	Status
SHECA Code Signing ECC CA 2A	ECDSA_P384	sha384ECDSA	ECC Code Signing Certificates	In Use
SHECA EV Code Signing ECC CA 2A	ECDSA_P384	sha384ECDSA	ECC EV Code Signing Certificates	

- UniTrust Global Time Stamping RSA Root CA R1

UniTrust Global Time Stamping RSA Root CA R1 key algorithm/length is RSA/4096, signing algorithm is sha384RSA, expiry date is March 37, 2039.

- UniTrust Global Time Stamping ECC Root CA R2

UniTrust Global Time Stamping ECC Root CA R2 key algorithm/length is ECDSA_P384, signing algorithm is sha384ECDSA, expiry date is March 37, 2039. It has 1 sub-CA.

Subordinate CA	Key Algorithm /length	Signing Algorithm	Issuing Certificates	Status
SHECA Time Stamping ECC CA 2A	ECDSA_P384	sha384ECDSA	ECC Time Stamping Certificates	In Use

- UCA Root-G1

UCA Root-G1 no longer issues any certificates since January 1, 2009.

- UCA Global Root

UCA Global Root no longer issues any certificates since April 27, 2017.

1.1.3. UNTSH certificate trust level

UNTSH shall issue certificates through strict identification. All subjects: individual, organization or facility and so on, must offer materials to confirm its actual existence. Besides, for organization certificates and facility certificates, authorization documents of the organization are required as well.

From level of trust, certificates issued by each root CA under the UNTSH are in common use. All certificates could be trusted, no difference in security levels and no specific level of trust. However, different type of certificate, for diverse certificate subjects, the corresponding application requirements are different, as a result, all certificates should be used appropriately.

1.2. Document Name and Identification

This document is the UniTrust Network Trust Service Hierarchy Certificate Policies, called UNTSH CP for short. No Object Identifier (OID) is assigned to it by SHECA. (OID) 为 1.2.156.112570.1.0.1.

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

OID	Obeject
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 (UNTSH CP)
1.2.156.112570.1.0.2	Certification Practice Statement
1.2.156.112570.1.0.3	EV Certificate Policy
1.2.156.112570.1.0.4	EV Certification Practice Statement
1.2.156.112570.1.1	SSL Server Certificates Policy
1.2.156.112570.1.1.1 2.23.140.1.2.1	Domain Validation SSL Certificates Policy
1.2.156.112570.1.1.2 2.23.140.1.2.2	Organization Validation SSL Certificates Policy
1.2.156.112570.1.1.3 2.23.140.1.1	Extended Validation SSL Certificates Policy
1.2.156.112570.1.2	Object Signing Policy
1.2.156.112570.1.2.1 2.23.140.1.4.1	Code Signing Policy
1.2.156.112570.1.2.2 2.23.140.1.3	Extended Validation Code Signing Policy
1.2.156.112570.1.2.3	Windows Kernel Mode Code Signing Policy
1.2.156.112570.1.2.4	Adobe Signing Policy

1.2.156.112570.1.2.5	Document Signing
1.2.156.112570.1.3	Client Certificates Policy
1.2.156.112570.1.4	TimeStamping Policy
1.2.156.112570.1.4.1	TimeStamping AATL Policy
1.2.156.112570.1.5	OCSP Policy
1.2.156.112570.1.9.1 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. PKI Participants

1.3.1. Electronic Certification Authorities

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

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

1.3.2. RA

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

independent of the CA, authorized and delegated by related agreements between SHECA and relevant organizations.

RA must perform certificate services under the approval and authorization of SHECA in accordance with the procedures and requirements of the CP and corresponding CPS. SHECA must assess RA appropriately to confirm that the duty could be performed properly.
Especially, the external RA do not involve SSL certificate and code signing certificate. SHECA would not authorize the external RA to validate the information which supplied to apply for a SSL/code signing certificate and issue a SSL/code signing certificate.

1.3.3. Subscribers

Subscribers, the entities that receive certificates from CA, include individuals and organizations accepting certificates from UNTSH. Subscribers are always not applicants, in this case, applicants need to ensure that they have obtained explicit and appropriate authorization. Individual is divided into natural person and person in organization. Organization contains all kinds of government organizations, enterprises and institutions and other social organizations, generally speaking, an organization has the status of a legal person and organization code. For equipment certificates, due to the particularity of the main body involved in certificates, subscribers are usually organizations or individuals that have the equipment assuming the corresponding obligations.

In the applications of electronic government affairs, because of some requirements of specific applications, a government agency applies for certificates for some specific groups of users, and it may be inconvenient or unavailable for the government agency to provide detailed, integral information about identification of users. For such users, the government agency need to offer a description of subscriber's identity, and assure the authenticity of their identities and submit it to SHECA in written form.

1.3.4. Relying Parties

A Relying Party is an individual or entity that acts in reliance of a certificate and/or use a public key to verify a digital signature. A Relying Party mayor may not also be a subscriber.

To trust or verify a certificate, a relying party must verify information of certificate revocation, including Certificate Revocation List (CRL), query, OCSP check and other queries. Relying Party must trust a certificate after reviewing reasonably.

1.3.5. Other participants

In the provision of certificate services, organizations that offer query and verification of organization or individual information and/or other extra information could be the cooperator assisting in verifying the information of certificate applications.

Some RAs are not approved by SHECA, but the organizations apply for certificates, verify certificate information and pay for certificate cost for a specific group, known as Certificate Advance Vendor. SHECA could provide certificate services required for specific users by entering into the agreement with Advance Vendor. The Advance Vendor and its specific certificate subscribers shall comply with the provisions of this CP.

1.4. Certificate Usage

Under the circumstances where the CP or CPS describes the different levels of assurance, this stipulation could describe different type of applications applicable or non-applicable for different levels of assurance.

1.4.1. Appropriate Certificate Usages

UNTSH Subscriber certificate is universal certificate, which has appropriate application in accordance with different type. For example, individual certificates are used for signing and encrypting e-mail, personal online banking business etc, and organization certificate is applied to B2B transactions, online tax declaration etc, facility certificate is applied to identify facilities, encrypt information channels etc. In addition to the difference between certificate applications due to different subjects, subscriber certificates within UNTSH could be widely applied to electronic government, electronic commerce affairs or other social activities to authenticate identity, electronic signing etc. Except for the restrict of law, regulations and national policies.

UNTSH Subscriber certificates could meet the following security requirements in term of the function:

- Identification-to ensure that the identity of certificate holder subject to trust services of SHECA is legitimate.

- Verifying the integrity of messages to ensure whether messages are modified during delivery, and whether messages sent are consistent with ones received as digital certificates and digital signatures are used.

- Verifying digital signatures –Verifying digital signatures that is the evidence of Non-repudiation of transactions trust body. It must be pointed out that for any electronic communications or transactions, non-repudiation should be ruled based on the laws and the measures for solving disputes.

- Confidentiality of information transmission-confidentiality ensures that messages delivered between senders and receiver are confidential, and will not be disclosed to

others who are not authorized legally. But SHECA shall not assume corresponding responsibilities and obligations for confidential incidents. For any direct and indirect damages and losses led by confidentiality purposes, SHECA shall not assume responsibilities.

Subscribers, Relying Parties and other subjects could judge by themselves on the basis of the actual needs to decide using corresponding and appropriate certificates, understand the types of application, the range of application, and select their own applications.

1.4.1.1.Identity Certificate Usage

Identity certificates is divided into identity certificates I and identity certificates II, identifying various types of organizations, individuals and facilities, could be applied to all kinds of electronic government, electronic commerce affairs and other social activities, such as, online transactions, payment, reporting, management, business, access control and other applications.

Identity Certificates I only use a pair of key-pair for signing, verifying signatures, encrypting and decrypting information.

Identity Certificates II use two pairs of key-pair, one is signature key pair used to sign and verify signatures; the other is encryption key pair used to encrypt and decrypt information.

1.4.1.2.E-mail Certificate Usage

Based on different security levels and authentication methods of the issued certificates, the Email Certificates include: Mailbox-validated Email Certificates, Sponsor-validated Email Certificates, Individual-validated Email Certificates and Organization-validated Email Certificates. The Mailbox-validated Email 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 Email 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 Email 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 Email 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.
The S/MlME Email 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.

1.4.1.3.Code Signing Certificate Usage

Code Signing Certificate authenticates the source or owner of the software code, only is applied to various types of code digital signatures, must not be applied to various types of transactions, payment, encryption and other applications.

Subscribers for code signing certificate must not use code signing certificates to sign malicious software, virus code, software infringement, hacker software.

1.4.1.4.Security Website Certificate Usage

Security website certificate identifies Websites or web servers, could be used to prove the identity or qualification of the site and offer SSL-encrypted channel. It must not be used in signing and verifying diverse types of transactions and payment.

1.4.2. Prohibited Certificate Uses

Certificates shall be used only to the extent the use is consistent with the subjects represented by certificate. For example, individual certificates could not be used as organization certificates and facility certificates, organization certificates could not be used as individual certificates and facility certificates, facility certificates could not be used as individual certificates and organization certificates. Any applications that do not conform to this stipulation will not obtain the protection from the CP.

Certificates are prohibited from using in any violation of national laws, regulations or destroying national security, otherwise users assume the legal results led by that by themselves. In particular, certificates are not designed for, not intended for, not authorized for using in application systems involved in personal injury, environmental destruction and so on, such as navigation or communication systems, traffic control systems or weapons control systems etc.

1.5. Policy Administration

1.5.1. Organization Administering the Document

As the operator of UNTSH, SHECA established SHECA Safety Certification Committee which is responsible for formulating, maintaining and interpreting the CP as the agency of policy administration. SHECA Safety Certification Committee contains at least one member from SHECA management layer, two directors taking charge of operational services, and one member participating in editing policies directly. A member from the management layer is the principal of SHECA Safety Certification Committee.

AS all members of SHECA Safety Certification Committee manage and approve certificate policies, they are entitled to one vote decision. If there are two voting results, the principal of Safety Certification Committee has a double-vote decision.

Strategy Development Department of SHECA as the agency of Safety Certification Committee in charge of daily operation,responsible for drafting the CP and submitting the modification report according to requirements and its external consulting services.

1.5.2. Contact Person

SHECA designates Strategy Development Department as contact person of the CP,specializing in external communication and other related matters.If you have any problems,suggestions,questions etc about the CP,you can contact with SHECA Strategy Development Department.

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

Tel:86-21-36393197
Tax:86-21-36393200
Location:18F, No.1717, North Sichuan Road, Shanghai, China
Postal Code:200080
E-mail:policy@sheca.com

1.5.3. Person Determining CP Suitability for the Policy

SHECA Security Certification Committee determines the suitability and applicability of this CP.SHECA Security Certification Committee as the highest policy administration agency, is the agency that approves and decides whether the CPS of SHECA or another CA corresponds with the CP or not.
Strategy Development Department as the policy department designated by SHECA Security Certification Committee,takes charge of supervising and inspecting daily implementation according to CPS to ensure that operational services performed by CA in accordance with its CPS conform to the requirements of the CP.

1.5.4. CP Approval Procedure

This CP is approved by SHECA Security Certification Committee,including revising and changing the version.

If the CP needs to be modified due to changes in standards, improvements in technology, enhancements in security mechanism, changes in operating environments and requirements of laws and regulations, Strategy Development Department submits the modify report to SHECA Security Certification Committee. Approved by the committee, it will be published by SHECA on www.sheca.com.

According to the provisions of "People's Republic of China Electronic Signature Law" and "Electronic Authentication Services management measures", SHECA will inform Ministry of Industry and Information Technology after publishing the CPS.

1.6. Definitions and Acronyms

See Appendix A.

2. Publication and Repository Responsibilities

2.1. Repositories

SHECA establish and maintain a publicly accessible online repository, publishing the Certificate Policy (CP), Certification Practices Statement (CPS), correlative agreements, certificates, Certificate Revocation List (CRL), Online Certificate Status Protocol(OCSP) and so on. SHECA's repository, should contain two types of information which could be published by different means, one is about certificate as a part of certificate services and certificate status check etc,and the other is about certificate policies and related documents etc.

SHECA are responsible for maintaining a publicly accessible online repository and disclose it in CPS and other documents

2.2. Publication of Certificate Information

SHECA needs to publish information which includes Certificate policies, Certification Practice Statement, and agreements related with certificate usage and service, certificates, Certificate Revocation List, Online Certificate Status Protocol etc.

SHECA provides clear location and way of access to the repository,issues certificates, Certificate Revocation list and Online Certificate Status Protocol, the information issuing is a part of certificate services.

Moreover,SHECA publishes Certificate Policies,Certification Practice Statement,related agreements and so on at www.sheca.com/repository.

2.3. Time or Frequency of Publication

SHECA issue timely Certificate Policies, Certification Practice Statement, certificate services, related agreements and other documents, as well as its revision in these documents.
For subscriber certificates, SHECA should issue CRLs at least every 5 days, or within 24 hours after the subscriber certificate is revoked. The difference between the next update time (nextUpdate) field and this update time (thisUpdate) field of the subscriber certificate CRL must be less than or equal to 7 days.

For Sub-CA Certificates, a ARL should be published at least once every 7 months or within 24 hours after revoked. The difference between nextUpdate time (nextUpdate) and this update time (thisUpdate) of the root/intermediate root certificate ARL must be less than or equal to 10 months. If the CA or Sub-CA Certificate is revoked, SHECA will publish the revocation information on the website.
SHECA ought to issue certificates to make users accessible to download, check and use within the specific time in the CP or corresponding CPS.

2.4. Access Controls on Repositories

SHECA does not control access to CP, CPS, certificates, certificate status information and CRL, but any interrelated parties who require access to certificates, certificate status information and certificate revocation list should abide by the CP and related CPS. SHECA retains the right of taking access-control measures.

SHECA shall implement controls to prevent unauthorized persons from adding, deleting, or modifying repository entries.

3. Identification and Authentication

This stipulation describes the process in which certificate applicants and/ or other attributes are identified for end users before certificates are issued. For the entities expecting to be CA, RA or other PKI operations, this stipulation formulates the process in which their identities are verified and acceptance criteria. And this stipulation describes how to authenticate Re-Key requesters and revocation requesters. In addition, this stipulation specifies naming rules, including admission of the trademarks in some names.

3.1. Naming

Unless where indicated otherwise in this CP, the relevant CPS or the content of the digital certificate, names appearing in Certificates issued under UNTSH are authenticated.

3.1.1. Type of Names

Naming should abide by X.500.Subscribers certificates should contain an X.501 distinguished name in the subject name field.

3.1.2. Need for Names to be Meaningful

The subscriber's name must be meaningful, usually contains the semantics which could be understood, and could confirm the identity of individuals, organizations or facilities in the certificate subjects. In the applications of electronic government affairs which have some special requirements, SHECA is allowed to assign the special names to users on the basis of the certain rule, moreover, SHECA could associate the special name with the certain entity (individual, organization or facility) uniquely. Any special name should be authorized by SHECA Security Certification Committee.

3.1.3. Anonymity or Pseudonymity of Subscribers

Subscriber certificates are not allowed to use anonymous or pseudonyms, but in some applications of electronic government affairs, SHECA is allowed to assign the special names to users on the basis of the certain rule, moreover, SHECA could associate the special name with the certain entity (individual, organization or facility) uniquely. Any special name should be authorized by SHECA Security Certification Committee.

3.1.4. Rules for Interpreting Various Name Forms

UNTSH subscriber certificates explain the different names in accordance with X.500 rules.

3.1.5. Uniqueness of Names

The names of UNTSH subscriber certificates must be unique in the trust domain of CA. Uniqueness of names mean that a name could correspond with the unique entity (individual, organization or facility).If two names are the same, the name gives priority to the first applicant.

3.1.6. Recognition, Authentication, and Role of Trademarks

A subscriber certificate is allowed to contain the information of trademarks, which could not be used to identify individual, organization, or facility. Certificate applicants should not use names that infringe upon intellectual property rights of others. SHECA does not judge and determine whether certificate applicants have the intellectual property of names, and is not responsible for any dispute about domain names, trademarks and other intellectual property. SHECA has no right, and no obligation to refuse or question any certificate request which causes dispute about intellectual property.

As the name submitted by an applicant contains trademark, the applicant is required to submit a trademark registration document (the well-known trademarks could not be required), but this requirement is not or should not be deemed that SHECA shall judge and decide the ownership of the trademark.

3.2. Initial Identity Validation

3.2.1. Method to Prove Possession of Private Key

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, another cryptographically equivalent demonstration, or another SHECA-required method containing the initial information submitted by SHECA(key storage medium assigned and the password involved in its corresponding password envelope)etc.

3.2.2. Authentication of Organization Identity

Any organization (government agencies, enterprise and institutions, etc.), applies for organization certificates, facility certificates and e-mail certificates in the name of the organization, the identity of the organization and other enrollment information should be identified strictly,including:

- Any material offered by the third party proving the existence of organization, for example the legal information (organization code certificate, Industry and Commercial Business License and other information), and other legal material offered by the recognized authority.

- Confirming the authenticity of the information about organization and whether applicants has obtained adequate authorization and other information required to be validated by telephone, postal letter, material required or other similar means.

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 request for validation of Domain Authorization or control.

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

Applicant representative shall submit copy of ID card, batch application form with organization seal, and the information of certificate subjects.

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.

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>> .

SHECA could also require other methods and information to authenticate the identity of organization for UNTSH subscriber certificates.

3.2.3. Authentication of Individual Identity

For individual indentity certificate,comprising identity certificate,e-mail certificate,code signing certificate,domain-name certificate etc., and users must confirm the real identity of the individual applicant while applying for certificate.

- Individuals should submit their legal identification, including ID card, military ID or other equivalent identification information.
- The authenticity of information about the identity could be validated via face to face review, telephone, postal letter and other means.
- For an application in the name of an individual identity, it also need to submit proof of its organization material.
- For ones who delegate others to apply for certificates, they need to submit the documents proving the adequate authorization.

SHECA can also obtain information from the third party to identify the applicants, if SHECA is unable to obtain the required information from the third party, SHECA could delegate the third party to investigate, or require applicants to afford extra information and materials.

When the domain name, device name 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 pass the domain name control verification defined in the CPS of SHECA or providing ownership documents.

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

Applicant representative shall submit copy of 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>>.

SHECA could also require other methods and information to authenticate the identity of organization for UNTSH subscriber certificates.

3.2.4. Non-Verified Subscriber information

Generally, this certificate identity information should be verified clearly and reliably, and the information stated to be non-verified in the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly – Trusted Certificates, Guidelines For The Issuance And Management Of Extended Validation Certificates, and Minimum Requirements for Code Signing Certificates in the application is not required to verify.

3.2.5. Validation of Authority

Confirmation of the authorization includes the following two aspects:

- Confirming commission and authorization, as individual delegates others or organization delegates others to apply for a type of certificate, need to confirm the authorization from the consignor and identity material from the consignee.
- When the application information from individual applicant contains organization information (governmental agency,enterprise and institution),it needs to confirm that the organization exists and the applicant is a member of the organization.

If SHECA is unable to obtain the required information from the third party, SHECA could delegate the third party to investigate, or require applicants to afford extra information and evidentiary materials.

3.2.6. Criteria for Interoperation

SHECA may provide interoperation services that allow a non-UNTSH CA to be able to interoperate with the UNTSH but the non-UNTSH CA must meet the following conditions:

- Enters into a contractual agreement with SHECA
- Operates under a CPS that meets SHECA's CP
- Accepting the assessment and annual compliance assessment from SHECA

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

3.3. Identification and Authentication for Re-key Requests

For this, SHECA requires subscribers to generate a pair of new key replacing the key pair of expired certificate, which is called re-key. But, at many times, subscribers ask for maintaining the key pair of expired certificate while obtaining a new certificate, SHECA issues new certificates to users using the existing key pair, which is called certificate renewal.

Generally,both "re-key" 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 specific applications,it is not the point that the new key pair has generated in the certificate renewal. But SHECA often requires the subscriber to use the new key pair in the certificate renewal.

3.3.1. Identification and Authentication for Routine Re-key

For route Re-Key after the expiration of certificate, subscriber could sign the renewal request using the original private key. Issuing Certificate Authority shall validate and verify the accuracy,legitimacy,uniqueness of user's signature, public key, and the user's information in the certificate-renewal request.

Identification and Authentication of route re-key including:

- Subscribers shall sign the application information, CA verifies the signature with the public key of the original certificate.
- If subscriber's registered information does not change, CA issues a new certificate based on original registration.

Subscriber can also choose the initial certificate application process to conduct route re-key, in accordance with requirements submitting corresponding information regarding to application and identification. In any case, SHECA could verify the identity of the subscriber in accordance with the identification and authentication requirements of an original certificate application when there is a re-key request.

3.3.2. Identification and Authentication for Re-key After Revocation

Re-key after revocation is not permitted if the revocation occurred. Subscriber use the same procedure verifying the original identity to apply for certificate, including re-identification and re-registration,and generating a new key pair to apply for a new certificate.

3.4. Identification and Authentication for Revocation Request

Certificate revocation request could be from subscribers, and also could come from CA or RA. While applying for suspension of the application, subscribers need to submit the equivalent identity information, certificate and private key applying for certificate to authenticate identity. If it is unable to audit on site due to the limitation of conditions, CA or RA will validate and verify the applicant's identity through the reasonable ways, for instance by telephone, postal delivery, the materials submitted by the third parties .If the judiciary requires the revocation based on laws, CA or RA will regard the written revocation request from the judiciary as the basis for validation, and will not verify the revocation request in other ways.

In case of emergency or under special circumstances subscriber can revoke their certificate by themselves. In this situation,subscriber need to sign the revocation request using the private key activating by password of certificate private key,and CA will verify the signature.CA or RA could validate revocation by telephone,fax,postal letter.

SHECA ensure that it will be reasonable to verify the revocation request.

The certificate revocation request from CA must be allowed by its administrative agencies or supervising agencies.

4. Certificate Life-Cycle Operational Requirements

4.1. Certificate Application

UNTSH provides formal certificates and test certificates. The formal certificates is the certificate applicant obtains after submitting the authenticate applicant information and approved by UNTSH certification authority in accordance with the provisions and procedures in the CP and its corresponding CPS,and certification authority will be responsible for warranting the authenticity of formal certificate. The certificate referred to this CP or CPS ,is usually formal certificate, unless it is demonstrated test certificate. Test certificate is only provided for user to test, CA has no responsibility for warranting the authenticity of certificate, and will provide no relevant warranty. User should not and cannot be allowed to apply test certificate in any occasion when there is a request of proving authenticate identity.

UNTSH certificate authority verify the identification of applicant, but do not verify other information contained in the test certificate. UNTSH strictly formulates certificate identification and valid period. The user name in test certificate must begin with English word "test" or Chinese word "测试", the valid period is 3 months. Test certificate do not apply to SSL certificates.

The application for formal certificate should be authenticated strictly, and perform the identification process depending on different types of certificate. On the basis of different applicants, certificate subject and functions, at present the certificate within UNTSH could be divided into three types, including individual certificates(containing individual identity certificate, individual e-mail certificate ,individual code signing certificate),organization certificates(organization identity certificate, organization e-mail certificate, department certificate, position certificate)and facility certificate(security website certificate, facility identity certificate and Internet facility certificate).The reliable verification process and identifying requirements shall be established in terms of various certificate in accordance with the CPS formulated by CP.

4.1.1. People Submitting a Certificate Application

Below is a list of people who may submit certificate applications:

- Any individual who is the subject of the certificate, the delegates must provide reliable authorized supporting documentation.
- Any authorized representative of a government agency, enterprise and institution, or other social organization.
- Any authorized representative of a CA.

- Any authorized representative of an RA.

4.1.2. Enrollment Process and Responsibilities

4.1.2.1. The Responsibilities of Applicant

All end-user certificate subscribers shall manifest assent to the relevant subscriber agreement that contains representations and warranties. All end-user certificate subscribers shall undergo an enrollment process consisting of:

- Completing a certificate application and providing true, reliable and integrated identity information.
- Generate the key pair or submit the application of authorization for generating the key pair
- Delivering his, her, or its public key to the CA
- Demonstrating possession and/or exclusive control of the private key.

For applicants applying for the certificate of RA and CA, they must sign the agreement with SHECA, deliver corresponding supporting documentation. The name and content of the certificate depend on SHECA.

4.1.2.2. The Process of application and registration

Applicant will send certificate request to RA, and RA will verify and sign the request, and then send the result to CA.CA validates the RA signature after receiving the request and issues the end-user subscriber certificate. In the whole enrollment process, it is necessary to take enough measures to ensure that:

- RA must identify the information of application and the identity of applicant.
- While RA is sending certificate request to CA, it ensure that the security, confidentiality, integrity in the process of transmission.

4.2. Certificate Application Processing

4.2.1. Performing Identification and Authentication Functions

An RA shall perform identification and authentication of all required Subscriber information in terms of Section 3.2.The RA shall authenticate in a reasonable manner.

4.2.2. Approval or Rejection of Certificate Applications

An RA will approve an application for a certificate if the following criteria are met:

- 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

An RA will reject an application for a certificate if the following criteria are met:

- 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

4.2.3. Time to Process Certificate Applications

CA and RA begin processing certificate applications within a reasonable time of receipt, no matter it is approved or not. There is no time stipulation to complete the processing of an application for SHECA, but usually the processing should be completed within 7 work ways, unless the otherwise indicated in the relevant Subscriber agreements, CPS or other agreements for this.

4.3. Certificate Issuance

4.3.1. CA Actions during Certificate Issuance

After the application is approved, CA will verify the signature in RA certificate request, and will issue subscriber certificate. When CA issues the certificate, the content of certificate is based on the subscriber information of certificate approved request.

4.3.2. Notifications to Subscriber by the CA of Issuance of Certificate

CAs issuing Certificates to end-user Subscribers shall, either directly or through an RA, notify Subscribers that they have created such Certificates, and provide Subscribers with access to the Certificates by notifying them that their Certificates are available and the means for obtaining them. Certificates shall be made available to end-user Subscribers, either by allowing them to download them from a web site or via a message sent to the Subscriber containing the Certificate or other conventional means to notify them how to get certificates .

4.4. Certificate Acceptance

4.4.1. Conduct Constituting Certificate Acceptance

The following conduct constitutes certificate acceptance:

- Subscriber accepts the medium containing certificate
- Subscriber downloads a certificate or installs a certificate to a local storage medium through network, such as the local computer, IC card, USB Key, mobile hard drive or other mobile storage medium.
- Subscriber accepts the means of obtaining certificate, and shall not object to certificate

or the contents of the certificate.

- Subscriber objects certificate or content of certificate operation failure

4.4.2. Publication of the Certificate by the CA

CA will publish certificate to a publicly accessible repository that subscriber may visit, including LDAP directory publishing, HTTP means publishing etc.

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 Certification Issuance by the CA to Other Entities

While issuing certificate, CA maybe send the certificate to RA approving the certificate. But usually, CA 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 querying the directory service or SHECA database.

If laws and regulations have other requirements, CA shall notify and operate according to their provisions.

4.5. key Pair and Certificate Usage

4.5.1. Subscriber Private Key and Certificate usage

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

After the expiration of certificate or certificate is revoked, subscriber must stop using private key.

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.

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. Any use of certificate and its corresponding private key is beyond SHECA will not be responsible for any result caused by this Any usage of certification and private keys beyond the terms of the CP and relevant CPS, as well as Subscriber Agreement, SHECA will not bear any resulting consequences.

4.5.2. Relying Party Public Key and Certificate Usage

Relying party may relay on UNTSH subscriber certificate in the application of proper internal only under the circumstance where relying parties assent to the terms of the CP. Prior to trust the certificate and signatures, relying party shall make appropriate efforts and reasonable judgment independently. 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 .

Before taking any action of reliance on UNTSH certificate, relying party shall independently assess and judge:

- Whether the certificate is issued by trustworthy CA.

- For any given purpose, the certificate should be used appropriately. Whether the certificate is used against the CP, CPS or the relevant laws and regulations should be determined. SHECA and RA is 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 ey 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. Any risk caused by reliance on certificate shall be undertaken by relying party independently, unless it can be turned out to be the mistakes made by CA or RA.

After judging whether the certificate is appropriate applied, Relying Party should utilize the appropriate software and/or hardware to perform digital signatures verification or other required operations.

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. When certificate renewal, the subscriber no longer needs to submit certificate registration information, only submits sufficient information which can identify the original certificate, such as subscriber distinguished name, certificate serial number etc. Use the private key of the original certificate to sign for the renewal application information containing of the public key.

4.6.1. Circumstance for Certificate Renewal

Every certificate has its valid period, when valid period of certificate expires, subscriber need to obtain a renewed certificate to continue to use certificate.

If the certificate expires, subscriber could still obtain a new certificate by certificate renewal, unless the certificate is compromised.

4.6.2. Who May Request renewal

Only the following persons could require certificate re-key:

- The individual certificate subscriber, if the subscriber authorizes others to do, the authorization documents is required to provide.
- The authorized representative for an organization certificate.
- Individual for a facility certificate, the authorized representative for a facility certificate.

4.6.3. Processing Certificate Renewal Requests

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

Subscriber could also choose the general process of certificate application to perform certificate re-key, and submit corresponding certificate application and confirmation documents in accordance with requirements. In any case, SHECA could use the way of initial certificate application as a means of identification in the certificate renewal.

4.6.4. Notification of New Certificate Issuance to Subscriber

See section 4.3.2

4.6.5. Conduct Constituting Acceptance of a Renewal Certificate

See section 4.4.1

4.6.6. Publication of the Renewal Certificate by the CA

See section 4.4.2

4.6.7. Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3.

4.7. Certificate Re-Key

Certificate re-key is that subscriber requires to generate new certificate under the circumstances where certificate information does not change, CA issue a new certificate for subscriber using its new public key.
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.

4.7.1. Circumstances for Certificate Re-Key

Every certificate has its valid period, prior to the expiration of an existing Subscriber’s Certificate, it is necessary for the Subscriber to re-key the certificate to maintain continuity of Certificate usage.

If the certificate has expired, subscriber could still obtain a new certificate by certificate re-key. Revoked certificate cannot apply for re-key, but only can apply for a new certificate in accordance with the process of initial certificate application.

4.7.2. Who May Request Certification of a New Key

Only the following persons could require certificate re-key

- The individual certificate subscriber, if the subscriber authorizes others to do, the authorization documents is required to provide.
- The authorized representative for an organization certificate.
- Individual for a facility certificate, the authorized representative for a facility certificate.

4.7.3. Processing Certificate Re-Keying Requests

For certificate re-key, its process need to ensure that the person submit certificate re-key request is the subscriber identified by certificate renewal. While issuing new certificates, SHECA could require applicants in demand of certificate renewal to submit information enough to identify subscriber, or share the same process as initial certificate issuance to identify subscriber.

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, 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.

Subscriber could also choose the general process of certificate application to perform certificate re-key, and submit corresponding certificate application and confirmation documents in accordance with requirements. In any case, SHECA could use the way of initial certificate application as a means of identification in the certificate renewal.

4.7.4. Notification of New Certificate Issuance to Subscriber

See Section 4.3.2

4.7.5. Conduct Constituting Acceptance of a Re-keyed Certificate

See Section 4.4.1

4.7.6. Publication of the Re-Keyed Certificate by the CA

See Section 4.4.2

4.7.7. Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3

4.8. Certificate Modification

Certificate modification refers to that subscriber requires to generate new certificate for the information within the certificate changes under the circumstances where certificate public key does not change. 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.

4.8.1. Circumstances for Certificate Modification

Within the valid period, if the information involved in the subscriber certificate is modified, and the modification shall not affect subscriber's rights and obligations, certificate modification could be applied. It includes:

- Subscriber's name, telephone, address and other information has been modified
- Subscriber himself/herself/itself has been modified due to reorganization.
- Other information has been modified

If information contained in the certificate changes that may affect the rights and obligations of subscriber modification. 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. Request Certificate Modification

See Section 4.1.1

4.8.3. Processing Certificate Modification Requests

See Section 3.2

4.8.4. Notification of New Certificate Issuance to Subscriber

See Section 4.3.2

4.8.5. Conduct Constituting Acceptance of Modified Certificate

See Section 4.4.1

4.8.6. Publication of the Modified Certificate by the CA

See Section 4.4.2

4.8.7. Notification of Certificate Issuance by the CA or Other Entities

See Section 4.4.3

4.9. Certificate Revocation and Suspension

Certificate Revocation includes applying for revocation and forcing revocation. After the certificate is revoked,subscriber could re-apply for and re-issue new certificate ,the same as the procedure and requirements in the initial application.

At present,SHECA does not offer certificate suspension.

4.9.1. Circumstances for revocation

If the following circumstances happens, subscriber certificate could be revoked:

- Subscriber asks revocation request;
- CA or RA is made aware of that the original certificate request was not authorized and authorization is not retroactively granted;
- Subscriber, CA, RA or other relevant parties have reason to believe or strongly suspects that there has been a compromise of subscriber's private key, or no longer comply with the requirement of key size and key parameters settings in the CP or relevant CPS;
- CA or RA or other relevant parties have reason to believe that the subscriber has materially breached a material obligation, representation, or warranty under the applicable Subscriber Agreement;
- The Subscriber Agreement with the Subscriber has been terminated;
- CA or RA has reasons to believe that the certificate was issued in a manner not materially in accordance with the provisions in the CP or relevant CPS;

- CA or RA has reason to believe that a material fact in certificate application is false or contrary to the facts of mistake or misleading;
- CA or RA determines that a material prerequisite to certificate issuance was neither satisfied nor waived;
- Subscriber's organization name changes;
- The information within the certificate (includes the non-verified subscriber information within the certificate), such as common name or other identification is incorrect or has changed;
- The certificate is misused;
- The Changes in certificate system will affect subscriber's level of subscriber and warranty;
- Certification Authority, enterprise and institution or other social bodies applied for certificates for its employee, but the employee has left the organization;
- The key of CA used for issuing the certificate changes, or possibly compromises ;
- The relevant provisions of laws and regulations or requirements;
- Other revocation which is required by the UNTSH's CP and/or CPS.

For the certificate used in UNTSH certificate service system, such as the certificate used by CA, RA, RAT or other service subjects (including facility certificate used in the service system) could be revoked in the following circumstance:

- The agreement between CA and RA,CA and PAT has been terminated or otherwise has ended;
- Certificate private key has safety damage or is suspected with safety damage;
- Owing to the requirements for management.

If certificate subscriber finds or suspects compromise of its private key,CA should be notified and revoked the certificate right now.

Besides, for SSL certificates, CA should revoke the certificates if any one or more of the following circumstances happen:

- SHECA aware that the domain name is no longer legal because of some reason, such as the courts determined that the domain name was illegal, contract termination with domain name registrant, licensing or services agreement between the Domain Name Registrant and the Applicant has terminated etc.;
- CA aware that a wildcard certificate was used to authenticate a fraudulently misleading subordinate domain name;
- SHECA ceased operations and did not arrange for another certificate authority to provide revocation support for the certificates;
- SHECA's right to manage certificates under applicable industry standards was terminated (unless arrangements have been made to continue revocation services and maintain the CRL/OCSP Repository);
- The technical content or format of the certificate presents an unacceptable risk to application software vendors, Relying Parties, or others;

Besides, for S/MIME certificates, CA should revoke the certificates if any one or more of the following circumstances happen:

- The S/MIME Certificate no longer complies with the requirements of Section 6.1.5 and Section 6.1.6 Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates;
- SHECA is made aware of any circumstance indicating that use of an email address or Fully‐Qualified Domain Name 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’s right to issue Certificates under these Requirements expires or is revoked or terminated, unless SHECA has made arrangements to continue maintaining the CRL/OCSP Repository;
- 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.

Besides the circumstances above, when one or more of the followings happen to a code signing certificate, revocation is also needed.

- The Code Signing Certificate no longer complies with the requirements of Section 6.1.5 and Section 6.1.6 Code Signing Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates;
- SHECA’s right to issue Certificates under these Requirements expires or is revoked or terminated, unless SHECA has made arrangements to continue maintaining the CRL/OCSP Repository;
- 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;

Besides the circumstances above, when one or more of the followings happen to a code signing certificate, revocation is also needed.

- The Code Signing Certificate no longer complies with the requirements of Section 6.1.5 and Section 6.1.6 Code Signing Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates;
- SHECA’s right to issue Certificates under these Requirements expires or is revoked or terminated, unless SHECA has made arrangements to continue maintaining the CRL/OCSP Repository;
- 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;
- If an Application Software Supplier requests the revocation:
  a. Within 2 business days of receiving this request, SHECA either revokes the certificate or informs the Application Software Supplier that it is conducting an

investigation;
b. If SHECA chooses to conduct an investigation, it informs the Application Software Supplier whether or not it will revoke the certificate within 2 business days; and
c. If SHECA determines that revocation will have an unreasonable impact on its customer, it proposes an alternative course of action to the Application Software Supplier, based on its investigation.

4.9.2. Who Can Request certificate 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 start the investigation process and provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate Problem Report.

(4) SHECA shall decide whether revocation or other appropriate action is warranted during two workdays.

(5) 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. Usually, the interval between finding revocation request and submitting revocation request must not exceed 8 hours.

4.9.5. Time within Which CA Must Process the Revocation Request

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

4.9.6. Revocation Checking Requirements for Relying Parities

Relying parties shall check the status of certificates before trusting UNTSH certificate, including checking CRL, checking the status of certificates at www.sheca.com or via online certificate status protocol (OCSP)

4.9.7. CRL Issuance Frequency

For subscriber certificates, SHECA should issue CRLs at least every 5 days, or within 24 hours after the subscriber certificate is revoked. The difference between the next update time (nextUpdate) field and this update time (thisUpdate) field of the subscriber certificate CRL must be less than or equal to 7 days.
For Sub-CA Certificates, a ARL should be published at least once every 7 months or within 24 hours after revoked. The difference between nextUpdate time (nextUpdate) and this update time (thisUpdate) of the root/intermediate root certificate ARL must be less than or equal to 10 months.
If the CA or Sub-CA Certificate is revoked, SHECA will publish the revocation information on the website.
SHECA security certification committee could decide by itself to shorten the time of CRL issuance and renewal according to different circumstances, except provided in laws and regulations.

4.9.8. Maximum Latency for CRLs

After certificate is revoked, the revocation should be released to CRL within a reasonable period, usually depending on the processing speed of system. UNTSH ensure that the revocation should be released to CRL within 24 hours after certificate is revoked.

4.9.9. On-Line Revocation/Status Checking Availability

SHECA provides online certificate status protocol (ocsp) service or certificate status consultancy based on web.

4.9.10. On-Line Revocation Checking Requirements

A relying party must check the status of a certificate before he/she/it wishes to rely on. If a relying party does not consult CRL, the relying party shall check certificate status by consulting OCSP or website.

4.9.11. Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12. Special Requirements Regarding Key Compromise

If UNTSH Participants find or suspect that key is compromised, they should revoke the certificates at once. If CA key (root CA or sub-CA key) is an actual or suspected to be comprised, subscriber and relying party shall be notified by reasonable means timely within reasonable time.

4.9.13. Circumstances for suspension

No stipulation.

4.9.14. Who Can Request Suspension

No stipulation.

4.9.15. Procedure for Suspension Request

No stipulation.

4.9.16. Limits on Suspension Period.

No stipulation.

4.10. Certificate Status Services

4.10.1. Operational Characteristics

Certificate status is available via CRL, LDAP, OCSP, or URL published by CA. Certificate status services in the ways above should have a reasonable response and simultaneous processing capacity with query request.

4.10.2. Service Availability

Certificate Status Services must be available 24×7 without scheduled interruption.

4.10.3. Optional Features

OCSP is an optional service feature that is not available for all products and must be specifically enabled for other products.

4.11. End of Subscription

A subscriber may end a subscription for certificate services in the following situations:

- No certificate renewal after the expiration of valid period
- Certificate is revoked before expiration
- End of subscription is required before expiration

4.12. Key Escrow and Recovery

4.12.1. Key Escrow and Recovery Policy and Practices

In order to ensure the security and uniqueness of subscribers' signature private key, UNTSH does not escrow any subscriber’s private keys, and therefore it does not provide key recovery services.

4.12.2. Session Key Encapsulation and Recovery Policy and Practices

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.

However, the subscriber could apply to recover the private key through SHECA to the National Key Management Authority The subscriber need to pay for the restoration fee.

For more details, please refer to CPS.

5. Facility, Management, and Operational Controls

5.1. Physical Controls

UNTSH has detailed documented about physical control and security policies for CA and RAs to adhere. Compliance with these policies is included in the UNTSH independent audit requirements described in Section 8.These documents contain sensitive security information and are only available upon agreement with SHECA. An overview of the requirements is described in the

following subsections.

5.1.1. Site Location and Construction

All UNTSH CA and RA shall be conducted within a physical protected environment that deters, prevents, and stops unauthorized use, access, or disclosure of sensitive information and systems. For all CA and RAs, they shall comply with the requirements of SHECA's physical environment.

Environment security controls are based on the establishment of physical security tiers. A tier is a barrier such as a locked door or gate that provides mandatory access control for individuals, which could control each individual proceed to each area and is able to provide a positive preventive function, for example, it may remind access to the mode of locking or opening status of the door. The method to control physical security tier is progressive, and each successive tier provides more restricted access and greater physical security against intrusion or unauthorized access from the outside. Moreover, each physical security tier encapsulates the next inner tier, the outermost tier being the outside wall of the building.

CA shall describer physical security tier in more detail in their CPS.

5.1.2. Physical Access

Access to each tier of physical security shall be auditable and controlled so that each tier can be accessed only be authorized personnel.

5.1.3. Power and Air Conditioning

The secure facilities of CA and RAs shall be equipped with primary and backup systems to ensure continuous, uninterrupted access to electric power. Also, these secure facilities shall be equipped with air-conditioning system to control temperature and relative humidity.

5.1.4. Water Exposures

The secure facilities of CA and RA shall be constructed and equipped, and procedures shall be formulated, to prevent floods or other damaging exposure for water.

5.1.5. Fire Prevention and Protection

The secure facilities of CA and RA shall be constructed and equipped, and procedures shall be formulated, to prevent and extinguish fires or other damaging exposure to flame or smoke.

These measures shall meet local applicable safety regulations.

5.1.6. Media Storage

CA and RA shall protect the magnetic media holding back ups of critical system data or any other sensitive information from water, fire, electromagnetism or other environment hazards, and shall use protective measures to deter, detect, and prevent the unauthorized use, access, or disclosure of such media.

5.1.7. Waste Disposal

CA and RA shall set up procedures for the disposal of waste, especially paper involved in private or sensitive information, electronic media or other waste, to prevent the unauthorized use, access, or disclosure of waste containing private or sensitive information.

5.1.8. Off-Site Backup

CA and RA shall maintain back up measures of critical system data or any other sensitive information including audit data, to make sure data is in the safety facilities.

5.2. Procedural Controls

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. To be Trusted Persons shall meet the requirements of personnel background in this CP.

Trusted Persons including employees, third-party services, consultant that have access to or control authentication or cryptographic operations, and they may materially affect:

- The verification and validation of information in certificate applications
- acceptance, rejection, or other processing of the applications, cancellation, of certificate
- The issuance and revocation of certificates
- Access to the repository that has restrict access-control

- Handling subscriber information or requests

Trusted Persons includes, but are not limited to:

- Customer service personnel
- System administration and operation personnel
- System design research personnel
- Security management personnel
- Facility management personnel
- Room management personnel
- Human resources management personnel

5.2.2. Number of Persons Request 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 and 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.

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.

5.2.3. Identification and Authentication for 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 CP.

5.2.4. Roles Requiring Separation of Duties

Roles required 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

5.3. Personnel Controls

5.3.1. Qualifications, Experience, and Clearance Requirements

CAs and RAs shall require that personnel seeking to become Trusted Persons present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities competently and satisfactorily, as well as proof of any government clearances, if any, necessary to perform certification services under government contracts.

5.3.2. Background Check Procedures

A rigorous background investigation process need to be done to the personnel as trusted role, generally re-investigate 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 The human resources department and security personnel.

The information and procedures, which is required to be verified by background investigation , include but are not limited 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

5.3.3. Training Requirements

CAs and RAs shall provide their personnel with the requisite training and pre-job training needed for their personnel to perform their job responsibilities relating to CA or RA operations competently and satisfactorily. Training should include but are not limited to the following:

- UNTSH certificate policy and electronic certification practice statement
- PKI basics
- Electronic Signature Law and relevant laws and regulation
- Job responsibilities and position descriptions
- Security management strategies and requirements
- Appropriate knowledge

5.3.4. Retraining Frequency and Requirements

CA and RA should arrange for regular training for staff in important positions regularly, which are more in line with job requirements. The company Safety management strategy should be training at least once a year. The personnel in the important position shall accept business skills training once a year.

5.3.5. Job Rotation Frequency and Sequence

No stipulation

5.3.6. Sanction for Unauthorized Actions

CA shall establish, maintain, and enforce employment policies for discipline of personnel unauthorized actions or other actions damaging CA, including termination of labor contracts, position removing, fines, criticism and education etc. Disciplinary actions should comply with laws and regulations.

5.3.7. Independent Contractor Requirements

For independent contractors of providing the third-party services, including consultants, personnel of maintaining system and facility, personnel of supporting external technology, if their positions are trusted, their security requirements is the same as the CA employees. In addition to signing a confidentiality agreement on the content of the work, and the service personnel shall do related work with supervising and accompanying by specially-assigned person in SHECA. It is also necessary to conduct the imperative training of knowledge and safety standards to enable them to abide strictly specifications.

5.3.8. Documentation Supplied Personnel

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

- Position Description
- Relevant business operation description
- Relevant security management standards
- Relevant training materials

5.4. Audit Logging Procedures

5.4.1. Types of Events Record

SHECA must record the events of operating system-related with the CA and RA. These records whether handwritten, written or electronic format must include:

- The date of the event
- The context of event
- The entity of recording time
- The type of recording etc

The recorded contexts include but are not limited to:

- CA Key lifecycle events, including the generation, backup, storage, recovery, filing, destruction of keys.
- Cryptographic device lifecycle events, such as receiving, using, uninstalling and disusing.
- Certificate Lifecycle events include the application, approvement, renewal, revocation of certificate etc.
- 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.
- Security events recorded by firewalls and routers
- System operation events, including system startup and shutdown, the creation, deletion, setting or passwords modification of system privilege.
- Access to certification authority facility, including authorized personnel entering and exiting certification authority facility, unauthorized personnel entering and exiting certification authority facility, attendant and access to security storage facility.
- 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.

5.4.2. Frequency of Processing Log

Certification authority shall review audit logs in response to determine the important secure and operational events, take appropriate measures for security events, record and backup for audit actions.

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 with an strictly physical and logical control that includes mechanisms to protect the log files from unauthorized viewing, modification, deletion, or other tampering.

5.4.5. Audit Log Backup Procedures

SHECA should set up and carry out the reliable system for backups of audit logs, and full backups are performed periodically.

5.4.6. Audit Collection System (Internal & External)

No stipulation

5.4.7. Notification to Event-Causing Subject

When an event is logged by the audit collection system, no notice is required to be given to the individual, organization, device, or application that causes the event. But SHECA shall decide whether to notify relevant entity (for example the severity of the time) in accordance with audit results.

5.4.8. Vulnerability Assessments

Based on events in the audit process, SHECA has safety and vulnerabilities assessments, and appropriate remedial measures shall be taken on the basis of the assessment report. This assessment should be taken every day, every week or every year based on the events record. SHECA conducts the system safety assessment at least once a year, which is a part of annual assessment of the entire certificate operation services.

5.5. Records Archived

5.5.1. Types of Records Archived

Records to be filed, besides in terms of Section 5.4.1, the following records shall be archived, including:

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

- The documents of construction and the upgrade of certificate system .

- Certificates and CRL etc.,
- Documentation of supporting certificate applications, the information of accepted and rejected by certificate services, the agreement with subscriber
- Audit records
- Certificate policies
- Employee information, including background checks, employment, training etc.
- Various types of external and internal assessment documents.

5.5.2. Retention Period for Archive

The retention period shall vary with the different archive records. The retention period of different archive records as follows on base of laws and regulations, business requirements and actual operational services:

- Subscriber certificate and its relevant application information shall be retained for no less than 7 years since certificate expires or is revoked.
- CA, sub-CA and key, as well as relevant records generated shall be retained for no less than 10 years since certificate expires or is revoked.
- Physical access records shall be retained for no less than 2 years
- System operations and management records shall be retain for no less than 2 years
- External assessment records and internal annual assessment and audit record shall be retained for no less than 7 years
- Business management records shall be retained for no less than 7 years.

5.5.3. Protection Period for Archive

All archive records shall take appropriate measures to control physical and logical access so that only Trusted Persons who have been authorized access to records.

Archive records shall be protected from the unauthorized browsing, modifying, deleting and other illegal operations, and should be saved in reliable systems or sites.

Archive records should be accessed effectively in the period retained under this CP.

5.5.4. Archive Backup Procedures

Electronic archive record generated by system should be backed up periodically, and the file backed up should be saved off-site.

The archive records in writing don't need to be backed up, but its security should be ensured by taking strict measures.

5.5.5. Requirements for Time-stamping of Records

Archive records shall contain time and date information. Such time information need not be cryptographic-based.

5.5.6. Archive Collection System (Internal or External)

CA, RA and other entities within UNTSH are archived by internal archive collection systems.

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

When the certificate of CA expires, SHECA will renew the certificate of CA.As long as CA key pair does not exceed the maximum lifetime specified in Section 6.3.2, the certificate of CA could renew using original key. Or new key pair shall be generated to replace the expired certificate of CA. That is to say, in the key pair life cycle, SHECA could also generate new certificate of CA by using new key pair. Before the certificate of former level CA expires, key changeover shall be performed to ensure that the entities in the superior CA system shall switch from original key pair to new key pair gradually.

New CA key pair is generated, which must comply with the terms of key management of SHECA strictly. While generating new key pair,SHECA shall issue and publish new the CA certificate timely,and it shall be available for subscriber and relying party to obtain new CA certificate .

Make sure that the entire certificate chain transits smoothly in CA key changeover.

5.7. Compromise and Disaster Recovery

CA should formulate and maintain the reliable plan of compromise and disaster recovery by physical, logical, procedural control and other effective comprehensive solutions to reduce the risk and potential effects resulted by key compromise and other disasters to the minimum, and the business operation shall be recovered within the reasonable period. SHECA assigns a reliable damage and disaster recovery plan in response to system issues caused by accidents ,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

CA should establish the procedures of handling incident and investigate, respond and handle the incident. In accordance with the plan of disaster recovery, the backups shall be stored appropriately. Once compromise and disaster occur, these procedures shall be effectively utilized to recover business as soon as possible.

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

Following corruption of computing resources, software, and/or data, a report of the incident and a response to the event, shall be promptly made to security management department and utilize the incident and compromise handling procedures, if necessary, the disaster recovery procedures could be used.

5.7.3. Entity Private Key Compromise Procedures

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

- 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.
- 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.
-

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

- After the new root certificate issued by SHECA, it will be immediately published by SHECA repository, directory server, HTTP, etc..
- Take reasonable efforts to promptly inform users and relying parties which include Asseco Data Systems S.A..

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

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

- subscriber certificate is re-issued in accordance with the CP about provision of a certificate issued after the new sub-CA certificate is issued.

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

When the private key of certificate subscriber is lost,disclosed,decrypted,or stolen and by a third-party,according to the terms of the CP,subscriber shall revoke the certificate and notify the relying party as far as possible. Certification authority shall revoke subscriber certificate promptly and publish the revocation. Certificate subscriber shall re-apply certificate to maintain the continuity to use.

5.7.4. Business Continuity Capabilities 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 When the abnormal disaster ,system could be recovered and services shall be provided as soon as possible in order that the risk shall be reduced to the minimum. And CA shall ensure that:

- The business system should be recovered in the shortest period of time, no more than 24 hours.

- The information of customers should be recovered.

- The operation site should meet the security requirements after recovered.
- The services should be recovered for old users and new users.
- There are adequate personnel to operate business and the duty-spilt requirement shall not be violated.

5.8. CA or RA Termination

As CA or RA needs to terminate operation, the relevant party shall notify subscriber, relying party and other affected entities within the reasonable time as soon as possible before operation is stopped.

If certification authority shall terminate operation,it shall formulate business take-over plan to reduce the losses of subscriber and relying party to the minimum. The termination plan shall include the appropriate terms as follows:

- Notify government agencies
- Notify the parties affected by the termination of CA, such as subscriber and relying party.
- Notify fees
- Revoke the CA certificate issued by certification authority
- Save the archived documents and records of CA up to the specified period.
- Continue of certification revocation, such as issuing CRL or maintaining online certificate status check. If necessary, the unexpired and non-revoked certificate of end-use and sub-CA shall be revoked
- If necessary, for unexpired certificate, and unrevoked certificate, in accordance with indemnification specified or successive CA issue and renew the certificate to subscriber
- Handle the private key of CA and hardware module of the private key.
- The termination of CA services shall be sent to the terms of successive CA.

When RA discontinues service for any reason, SHECA deals with related business matters and other matters in accordance with the signing agreement.

6. Technical Security Controls

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

1. Key of CA Generation

Key pair of CA is generated by the equipment approved and licensed by the state cryptography administration department. The generation, management, storage, backup and recovery of key shall comply with relevant terms of FIPS140-2..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.

To assure the absolute security of key pair of CA, the rigid procedures of key management shall be established to control the security of key pair. At least it includes electromagnetic shielding environment, supervision, key spilt, video surveillance and other conditions.

2. Generation of subscribers signing key pair

The generation of subscribers signing key pair should be performed by subscriber.

Signature certificate subscriber shall use key pair generated by the equipment approved and licensed by the state cryptography administration department, such as encryption machine, encryption card, USB Key, IC card. Subscriber should make sure the security and compliance of the generation process. Before the choice of these devices , users may consult in advance system compatibility and acceptance related towards SHECA. The subscribers may be provided the USB Key by SHECA in accordance with the relevant provisions of the state encryption management as generation and storage devices, and offering relevant guidance.

The key pair of certificate Subscriber used in signing shall be generated in accordance with the terms of national laws and policies.CA shall support multiple means of generating the key pair used in signing of multiple modes. Besides the key pair generated by hardware cryptographic module, server certificate subscriber could take use of the software of web server to generate key pair, e-mail certificate could apply the key modules of the browser, and certificate applicants could select as required. In any way, the security of key during the generation shall be assured. SHECA has already implemented the secure and confidential measures in terms of technology, business procedures and management.

3. Generation for encryption key pair of the subscriber

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

4. Certificate subscribers have the responsibilities and obligations to protect the private key security, and assume the legal liability as this.
5. For certificates issued by UCA Global G2 Root and UCA Extended Validation Root, SHECA must not generate key pair for subscribers.

6.1.2. Private Key Delivery to Subscriber

Under the circumstances where subscriber generates his/her/its key pair, private key is not sent to subscriber as required. If CA generates Key pair for subscriber, CA shall send the private key to end-user subscriber through off-line security channel or adopting anti-tamper packaging. Data applied to activate private key shall be transmitted to subscriber through other channel.CA should record the distribution of the facility.

6.1.3. Public Key Delivery to Certificate Issuer

Certificate subscribers apply for a certificate by the public key to SHECA,(For example, PKCS # 10 format) 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

The public key of CA shall be published to relying parties by downloading on the website .While issuing subscriber certificate, CA could transmit the certificate chain containing the public key of CA to the final subscribers in the PKCS#7 format. Also CA shall publish its public key through LDAP.

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

6.1.5. Key Sizes

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 generated by the encryption equipment approved and permitted by the national password authorities, such as encryption machine, encryption card, USB Key, IC card, and follow generation norms and standards of these devices.
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.

6.1.7. Key Usage Purposes

Certificate issued by SHECA is X.509 version3, 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 key usage must conform to the terms of the CP and related CPS.

See section 7.1.2

6.2. Private Key Protection and Cryptographic Module Engineering Controls

6.2.1. Cryptographic Module Standards and Controls

Key pair of CA is generated by the equipment that is approved and licensed by state cryptography administration department of China. The generation, management, storage, backup and recovery of key shall comply with relevant terms of FIPS140-2..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.

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

The private key of CA is operated by multi-person control (means n out of m policy, m>n, n>=3), and adopt "Secret Sharing" technology to spilt the activated data required in operating the private key of CA into the several parts which are held by the members of SHECA Security Certification Committee. At least 3 or more than 3 Trusted Persons are required to accomplish the procedures of generation and split while operating the private key.

6.2.3. Private Key Escrow

No stipulation.

6.2.4. Private Key Backup

In order to ensure ongoing operations, electronic certification service agencies must create backup of the CA private key for disaster recovery. Such keys are stored in encrypted form within hardware cryptographic modules and associated key storage devices Backup of the private key in encrypted form is stored in the hardware cryptographic module ,and cryptographic modules used for CA private key storage meet the requirements of 6.2.1. CA private key is copied to backup for hardware cryptographic module to meet the requirements of 6.2.6.

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

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

6.2.5. Private Key Archival

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

6.2.6. Private Key Transfer Into or From a Cryptographic Module

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

SHECA does not provide subscriber for the way that private key derived from the hardware cryptographic module and does not allow this operation. As for the private key stored in the software code module , and if subscribers are willing to bear the relevant risks , the subscriber can choose the way of import and export, the operation using password protection and other control measures authorized access .

6.2.7. Private Key Storage on Crytographic Module

SHECA store the private key using the encryption equipment and modules approved and permitted by the national encryption department, and all the private keys stored in the cryptographic modules is 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 is stored in the form of cipher text. For the private key generated by software cryptographic modules, it is better for them to be used and stored in hardware cryptographic modules (such as USB Key, Smart Card)as well as other specific software code modules with security measures.

For code signing certificates and EV code signing certificates, SHECA ensure that the Subscriber’s Private Key is generated, stored, and used in a suitable Hardware Crypto Module that meets the requirements specified in Section 6.2.7.4 of the current Code Signing Baseline Requirement.

6.2.8. Method of Activating Private Key

All private keys shall be advised to be activated through entering password, unless subscriber himself/herself/itself prefers to modify and is willing to assume the appropriate responsibilities.

The private key of CA shall be saved in hardware cryptographic module, and its activation data shall be spilt in accordance with Section 6.2.2, and be saved in the hardware media such as IC card. The private key must be activated through entering the data with the way of n out of m.

For the private key stored in the subscriber's computer software code module, the subscriber should take reasonable measures to protect physically the computers in order to prevent users without the authorization using subscribers' computers and the relevant private key from the others. If the private key is stored in software password module without the 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 also input the protection password to activate the private key.

For the private key saved in such as 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. After the subscribers computer is installed the appropriate driver, the USB Key, smart cards are plugged into the appropriate device to enter the protection password or fingerprint, and then the private key is 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.
The method of deactivating private key includes logout, power cut, removal of hardware cryptographic module, cancellation of user or system etc.

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.

For the private key of CA, as the encryption equipment powers off where the private key saves, the private key will enter into inactivated status.

6.2.10. Method of Destroying Private Key

If the private key of CA shall not be used any longer, or the public key corresponding with the private key expires or has been revoked, the private shall be archived as required, and the non-archiving private key shall be deleted from encryption devices thorough, and the encryption equipment shall be initialized and be destroyed physically. The archived private key of CA shall be destroyed by multiple Trusted Persons during its archiving period, and be deleted thorough from encryption equipment, the encryption equipment shall be initialized and be destroyed by encryption equipment physically. All things used in activating such as PIN code, IC card, dynamic token etc shall also be destroyed or recycled with the private key.

If the private key of CA shall not be used any longer, or the public key corresponding with the

private key expires or has been revoked, subscriber shall determine the method of destroying the private key, including deletion of private key, initialization of system or cryptographic module, destruction of the module where the private key saves physically and other methods. The subscriber must ensure log off effectively the private key, and bear the relevant responsibility.

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, supplier qualifications and other aspects.

6.3. Other Aspects of Key Pair Management

6.3.1. Public Key Archival

CAs shall archive their own public keys, as well as the public keys of all CAs within their Sub-domains, in accordance Section 5.5.

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. For subscriber certificate, the validity period for a maximum does not exceed four years. For SSL certificates issued after September 1th, 2020, the maximum validity must not exceed 398 days. For S/MIME certificates (strict or multipurpose generation), the maximum validity must not exceed 825 days. For S/MIME certificates (legacy generation), the maximum validity must not exceed 1185 days. For CA certificates, the longest period does not exceed 30 years. Refer to CPS 6.3.3 for details.

6.4. Activation Data

6.4.1. Activation Data Generation and Installation

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 unauthorized.

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 .
All protection password shall be not easy to guess, and shall comply with the following principles:

- 8 characters at least
- Containing one character and a number at least
- Containing one lower-case letter at least
- Without containing many same characters
- No name is the same as the operator
- Without using birthday, telephone and other numbers.
- Longer Sub-characters in the information of user name

6.4.2. Activation Data Protection

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.

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.

6.5. Computer Security Controls

6.5.1. Specific Computer Security Technical Requirements

Information security management of UNTSH 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 standards, has implementation, review and record within operations.
Main security technology and control measures includes:identification and validation,logical access control, physically access control,personnel duty decentralized management,network access control,etc.

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

UNTSH system passes 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 third-party agencies.

6.6. Life Cycle Technical Controls

6.6.1. System Development Controls

Development controls of UNTSH system includes Trusted Person management, development environment security management, product designing and development assessment, the usage of reliable development tools etc, and product system designed to meet the requirements of redundancy, fault tolerance, modularity.

6.6.2. Security Management Controls

Information security management of UNTSH 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 the whole system has a strict control measures, 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.

Operation system shall use a strict management system to control and monitor the configuration of system 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 are upgraded, SHECA must confirm whether the information for affecting authenticate business security is in waste equipment during the process.

6.6.3. Life Cycle Security Controls

No stipulation.

6.7. Network Security Controls

UNTSH system shall use and upgrade timely multi-level firewalls, intrusion detection, security auditing and virus protection system, and shall audit and assess the policy periodically to reduce

the risks from network as far as possible.

6.8. Time-stamping

All kinds of system log and operations log of authentication system shall contain time and date information. Such time information need not be cryptographic-based.

7. Certificate, CRL and OCSP Profiles

7.1. Certificate Profile

UNTSH certificates generally conform to ITU-T X.509 V3(1997):Information Technology – Open Systems Interconnection – The Directory: Authentication Framework(June 1997) and RFC 5280: Internet X.509 Public Key infrastructure Certificate and CRL Profile(May 2008).

7.1.1. Version Number(s)

UNTSH certificates are 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 privates extensions provided by SHECA itself.

1. Certificate extensions

- Key Usage

Electronic signatures, non-repudiation, key encryption, data encryption, key agreement, verification of certificate signatures, verification of CRL signatures, only encryption and only decryption.

	SSL Certificate	Code Signing Certificate	Timestamp Certificate	CA Certificate
0 digitaSignature	√	√	√	×
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 dual use, bit positions SHALL be set for digitalSignature and keyEncipherment and MAY be set for nonRepudiation and 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. 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	Bit positions SHALL be set for digitalSignature and MAY be set for nonRepudiation.

		keyAgreement is set).	

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

- The Type of Netscape Certificate

The extension is used to declare the approbatory type of certificate approved for a relying party who uses net scape. 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 Constraints

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

- 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.

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.

2. Client-defined Extensions

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

7.1.3. Algorithm Object Identifiers

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

UNTSH certificate, the format and context of its name forms shall conform to the distinguished name format of X.501.

7.1.5. Name Constraints

Subscriber's name must be meaningful, and shall contain the semantics which could be understood, could demonstrate the identity of individual, organization or facility in the certificate subject, subscriber certificate shall not be allowed to use anonyms or pseudonyms. 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.

7.1.6. Certificate Policy Object Identifier

The certificates is issued by SHECA in accordance with the X.509 standard, whose policy object identifier is stored in the relevant topic of certificate policy . Please refer to certificate format specification in the appendix.

7.1.7. Usage of Policy Constraints Extension

No stipulation.

7.1.8. Policy Qualifier Syntax and Semantics

No stipulation.

7.1.9. Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2. CRL Profile

CRL issued by UNTSH shall conform to RC5280.

7.2.1. Version Number(s)

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

No stipulation.

7.2.3. CRL Downloading

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

7.3. OCSP Profile

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

7.3.1. Version Number(s)

RFC2560 defines the OCSP V1.

7.3.2. OCSP Extensions

No stipulation.

8. Compliance Audit and Other Assessments

As a operating subject of UNTSH, SHECA carries out quarterly internal audit and operational assessment to ensure the reliability , security and controllability of certification services, and at least 3% ssl certificates are randomly selected from all the ssl certificates to evaluate each time. In addition to internal audit and assessment, SHECA also hires an independent auditing firm in accordance with WebTrust audit to external assessment for the CA rules .

8.1. Frequency and Circumstances of Assessment

1. SHECA accepts the assessment and inspection authorities annually under the "Electronic Signature Law", "Electronic Authentication Services" and other requirements.
2. SHECA will perform internal assessment and review periodically at least annually, containing assessment and review of other entities (RA, service points etc) according to the requirement of national agencies, the relevant national standards and the operations and services formulated in the CP, as well as the provisions of internal assessment and audit.
3. SHECA will hire independent auditing firm, according to the audit rules formulated by WebTrust for CA, to perform external audit and assesses annually.
4. SHECA will implement risk assessment annual to distinguish the threat internal and external, and evaluate the likelihood of the threat and damage caused by the incident, and make sure whether the current corresponding strategies, technologies, systems, and related measures are adequate to the risk level.

8.2. Qualifications of Assessor

1. SHECA unconditionally receives the assessment from Ministry of Industry and Information Technology. SHECA is implemented evaluation by those who have the qualifications and experiences 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 CP and 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. External auditing firm hired shall have the following qualifications:

    - Must be permitted and qualified assessment agency and have good reputation in the industry.

    - Shall have knowledge of computer information security system, telecommunications

and network security requirements, PKI technology, standards and operations.

- Shall have the expertise and tools to check the system performance.

- Shall have the spirit of independent audit.

8.3. Assessor's Relationship to Assessed Entity

1. The external evaluators (the Ministry of Industry and Information Technology, independent auditing firms and other 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.

8.4. Topics Covered by Assessment

1. SHECA accepts the assessment of any content in accordance with requirements and specifications raised by Ministry of Industry and Information Technology.

2. SHECA internal assessment and audit includes:

- 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 Ministry of Industry and Information Technology 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 evaluators need to list the detailed list of all the problem projects. The evaluators 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 of Results

1. After the assessment, the Ministry of Industry and Information Technology will deal with assessment results in accordance with laws and regulations. The audit results will be published by

the website http://www.sheca.com.

2. 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 evaluator as well as SHECA Safety Certification Committee can understand. Non-certified by the SHECA security committee approval or authorized by object evaluated, the evaluators can not disclose to any other unrelated third parties.

In the 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 http://www.sheca.com.

Any third-party notices the assessment results or similar information to evaluation entity , which must be clear in advance that the purpose and manner of notice will be shown to SHECA and obtain SHECA consent, except otherwise provided by law. SHECA retains the legal authority in this area.

9. Other Business and Legal Matters

The CP as a part of Subscriber Agreement, is a constraint for UNTSH participants. Especially, fees, laws, finance, warranty and other rights and obligations shall be understood and followed sufficiently and adequately by subscriber, relaying parts, CA and RA.

9.1. Fees

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

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

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

9.1.1. Certificate Issuance or Renewal Fees

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

The announcement price is approved by the Shanghai Price Bureau.

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

price prevail.

9.1.2. Certificate Access Fees

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

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

9.1.3. Revocation or Status Information Access Fees

SHECA currently does not charge any fees for certificate revocation and status inquiry. If inquiry charging policy has any change, SHECA will promptly post on the website http://www.sheca.com.

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

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. SHECA shall offer certificate storage media and its related services to subscriber, and the price shall be specified in the agreement between SHECA and subscriber or SHECA and other entities.
3. Other services cost that SHECA will or may provide will be released in time for user to query.

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.

9.2. 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 subscribers'certificates issued by SHECA according to this CP.

At present, UNTSH operated by SHECA can't provide third-party insurance.

9.2.2. Other Assets

No stipulation.

9.2.3. Insurance or Warranty Coverage for Terminal Entities

UNTSH operated by SHECA shall not provide third-party insurance.

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 born by subscriber.

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

4. Under the circumstances 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. UNTSH system structure, configuration, includes system, network, data base etc., the various type of service system security configuration and program; system operation, maintenance records; various type of system operation password.
6. UNTSH documents and records about operation management, including physical security policy and its implementation plans, logical security policy and its implementation plans; key management policy and operational records; a list of Trusted Personnel; internal security management policy and system; the application records approved or rejected by CA or RA etc.

7. All UNTSH certificate holders'identity information, subscriber or his/her/its application systems shall get access to CRL, OCSP (time, frequency) and so on.

8. 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 information, and SHECA shall publish the information in directory server.

5. Certificate Policy (CP), Certification Practice Statement (CPS), Subscriber Agreement and so on.

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 CP, and must protect it through effective technical means and management process.
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 CP, and could publish the relevant confidential information to law-enforcing department according to requirements of laws, regulations, legal doctrines or court judgements. SHECA shall not assume any responsibility. The reveal shall not be regarded as a breach of confidential requirement and obligations.

As 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 of confidential information.

9.4. Privacy of Personal Information

9.4.1. Privacy Plan

SHECA values all users and their privacy, and formulates corresponding management measures to protect the privacy information.

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, and must not disclose the privacy information to a third party at will.

9.4.5. Notice and Consent to Use Private Information

Any subscriber information SHECA obtaining within the scope of certification business, 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.

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.

9.5. Intellectual Property Rights

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

SHECA holds and reserves all of softwares 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.

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 SHECA's responsibility .

9.6. Representative and Warranties

9.6.1. CA Representations and Warranties

1. CA warrants that

- Infrastructure and certification services are offered within the terms of this CP and relevant CPS.
- SHECA ensures that its private key shall be stored and protected securely. SHECA shall establish and implement security mechanism pursuant to the terms of national relevant policies.
- All activities related with certification business shall abide by the provisions of laws and regulations, and agencies in charge of it.
- The relationship between SHECA and certificate subscriber and the relationship between SHECA and relying party shall not be same as the relationship between agent and client. Certificate subscriber and relying party have not rights to let SHECA assume fiduciary duty in the form of contract or in other methods.
- SHECA could not make statement it opposite with the above stipulations in indication with indication, suggestion or in other ways.

2. CA warrants to subscribers

Unless otherwise provided in this CP or the agreement between Issuing Certificate Authority and subscriber, SHECA shall keep commitment to subscriber named in the certificate:

- Without misrepresentation that issuing authority know for 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.

- The certificate issued by Issuing Certificate Authority to subscriber shall comply with all the substantive requirements of this CP.
- Issuing Certificate Authority shall revoke certificate in accordance with this CP
- Issuing Certificate Authority shall notify subscriber any known events which could affect the effectiveness and reliability of certificate fundamentally.

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

3. CA warrants to Relying Parties

Issuing Certificate Authority shall warrants to persons who rely on all signatures reasonably in accordance with this CP and relevant CPS (the signature could be verified by the public key contained in the certificate)

- In addition to unauthenticated subscriber information, all the information in certificate or certificate merger reference to is accurate.
- Issuing Certificate Authority is in full compliance with the provisions of the CP and relevant CPS to issue certificate.

4. CA 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 CP .

9.6.2. RA Representations and Warranties

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

- Follow the agreements between this CP and SHECA, relevant CPS and SHECA, as well as other specifications and procedures published by SHECA , receive and process the applicant's certificate service requests, and set 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.

- According to the provisions of the CP to ensure operating system in the security physical environment, and have the appropriate safety management and quarantine measures.

- Accept the management from SHECA, including the qualification standards and service performance review.

- Admit 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.

2. RAT Warrants:

- Provide certification services and its own management, RAT must complies with the relevant provisions of this CP and related 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.

- 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 to enable subscribers to successfully apply for and use certificates.

9.6.3. Subscriber Representations and Warranties

Once subscriber accepts a certificate issued by Issuing Certificate Authority, from the time of acceptance until the certificate valid throughout the period, if the subscriber does not notice, then the subscriber is considered reasonably trusted with all information contained in the SHECA certificate and makes the following guarantees:

- All statements and information filled in the certificate application form must be complete, accurate, true and correct, and willing to take legal responsibility for any false, forged information.

- If there is an agent, then both subscriber and agent take jointly responsibility .Subscriber is responsible for the agent who makes any false statements and omissions, or notify SHECA and its authorized certification services agencies.

- 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).

- Only use certificate for the authorized or other lawful purpose.

- 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 CP, 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.

- Shall not reject any statement, change, update, upgrade from SHECA, including but not limited to strategy, standards and modification and deletion of certification services.

9.6.4. Relying Party Representations and Warranties

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

- Familiar with the terms of this CPS, understanding the purpose of the certificates usage. Relying party is familiar with the terms of this CP and related 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 CP, 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 .

9.6.5. Representations and Warranties of Other Participants

Advance vendor warrants:

- Advance vendor is required to bear all the cost of the certificate and pays all according to the provisions provided by SHECA .
- Advance business's behavior of advance vendor means advance vendor is willing and able to assume responsibility of guaranteeing applicant authenticity based on this CPS.

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

9.7. Disclaimers of Warranties

Within the scope permitted by laws, Certificate Practice Statement, Subscriber Agreement, Relying Party Agreement and other subscriber agreement of certification authority shall contain clauses exempting from certification authority, it includes any warranty of availability and applicability for certain purpose.

9.8. Limitations of Liability

Within the scope permitted by laws, while assuming any responsibility and obligation, CA only assumes limited responsibility within the law.

9.9. Indemnities

For the subscriber losses caused by CA, CA shall indemnify subscriber, or under the circumstance where relying party performs Relying Party Agreement, the losses of certification authority

resulted by certification authority, shall indemnify relying party.
Subscriber shall indemnify certification authority, because of the losses of relying party and certification authority caused by subscriber himself/herself/itself.

The relying party shall indemnify the losses of certification authority caused by relying party himself/herself/itself.

The scope, limitation, deductibles etc of indemnification, shall be specified in the CPS formulated according to CP, Subscriber Agreement and other documents.

9.10. Term and Termination

9.10.1. Term

This CP shall take effect since it is published, and be always valid before certification authority terminate business, version number and release date shall be specified by the document, as new version is published, and it takes effect, the original version shall lose effectiveness automatically.

9.10.2. Termination

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

9.10.3. Effect of Termination and Survival

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

9.11. Individual Notices an Communications with Participants

Unless otherwise specified by agreement between the parties, CA, RA and other entities with UNTSH shall communicate with each other with the reasonable way, and shall not take individual way.

9.12. Amendments

SHECA has the right to revise this CP.SHECA has the right to publish revision results with the form of revised edition on 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 CP once a year at least, to ensure that CP meets the requirements of national laws and regulations and the latest version of CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly – Trusted Certificates, and satisfy the actual requirements of certification business operation.

This CP 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.The revised CP shall be published formally through the approval of SHECA Security Certification Committee.

9.12.2. Notification Mechanism and Period

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

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

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, all revision and modification shall take effect. Even so, if SHECA publishes revision, and the revision could not come into effect timely so that SHECA certification service system shall be damaged, then the amendment should be immediate taken into effect from the date of release.

9.12.3. Circumstance under Which CP Must be Modified

If the following situation occurs, this CP must be modified:

- The encryption technology develops significantly enough to affect the effectiveness of existing CP.
- The standards of relevant certification business shall be renewed.
- Certification system and relevant management regulations take significant upgrade or changes.
- The requirements of laws and regulations and competent department requirement.

- There is some important deficiency in the existing CP.
- OID of certificate policy shall be modified.

9.13. Dispute Resolution Provisions

In case of dispute, relevant parties shall resolve it through negotiations in accordance with agreements, if negotiation fails, it could be resolved by laws.

9.14. Governing Law

UNTSH operated by SHECA, and all of its certificate service activities accept "People's Republic of China Electronic Signatures Laws", "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 choose or whether commercial relationship is established in People's Republic of China, the implementation, explanation, interpretation, effectiveness of this CP shall apply to the laws of People's Republic of China.

9.15. Compliance with Applicable Law

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

9.16. Miscellaneous Provisions

9.16.1. Entire Agreement

The integrated agreement is composed of CP, CPS, Subscriber Agreement and Relying Party Agreement as well as its supplemental agreement. This CP shall affect the clauses and provisions of rights and obligations directly, unless the affected party sends identified information or documents, or as otherwise provided in this, or else oral revision, surrender, supplement, modification or termination. When this CP comes into conflict with other rules, regulations or agreements, all participants involved in certification activities shall be bound by this CP, but the following agreement is excluded:

- Signing agreement prior to the validity date of this CP

- The contract has clearly stated that it handles affairs of related parties in place of this CP, or the provisions of this CP shall be prohibited.

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 CP is invalid or unenforceable in any reason or in any scope, the remainder of the CP shall remain valid.

9.16.4. Enforcement

No stipulation.

9.16.5. Force Majeure

In the extent permitted by applicable law, subscriber agreement and CPS formulated in accordance with the CP shall include force majeure clause to protect each party.

9.17. Other Provisions

No stipulation.

Appendix A Definition and Acronyms

Activation Data

It is data value that is necessary for operating cryptographic module and needs to be protected. (For example, PIN, password, or manual controlling key sharing part), rather than key.

Authentication

The course of confirmation individual, organization or things is the same as claimed

The process of making sure the individual, organization or things is the same as claimed. In the context of PKI, authentication is defined this process that make sure some special name applies or tries to visit some things is the right individual or organization.

Certification Authority

The authority trusted by users is responsible for creating and distributing public key and certificate. Some time, certification authority could also create key for users.

CA-certificate

The certificate is issued by another CA for a public key of CA.

Certificate Policy

A set of naming rules, are used for indicating the applicability of a specific body and (or) application type with the same requirements of security. For instance, a specific CP could indicate that certain type of certificate is applied to verify the parties participating in B-to-B transaction activities, for a given price range of the product and service.

Certification Path

An ordered sequence of certificates (including the public key of initial object in path), could obtain the public key of end-user object by handling the sequence.

Certification Practice Statement

The statement with respect to practices adopted during the course of certificate issuance, management, revocation or renewal (or re-key).

Identification

The course of establishing the identity of individual or organization, for example, shall indicate that someone or some organization is specific individual or organization. In the context of PKI, identification refers to two courses:

A confirm that someone or some organization the given name is associated with the actual identity

of the individual or organization in the real world.

A confirm that the named individual or organization is the individual or organization who applies for or tries to access something. The person who seeks to identifier may be certificate applicant, or the applicant in PKI trusted position, or the individual who tries to access network or applies software.(such as CA administrator tries to access CA system).

Issuing Certification Authority

In the specific context of CA certificate, Issuing certificate authority is CA that issues certificate. (See subject CA)

Participant

The individual or organization plays a role in given PKI, such as subscriber, relying party, CA, RA, certificate-generation authority, repository-service provider, or similar entity.

Policy qualifier

The information of relying on policy, may be saved together with the CP identifier in the certificate conforming to X.509 format. The information may contain the URL of CPS or Relying Party Agreement, the words of certificates usage clause (or number of causing words to appear)

Registration Authority

Entities with one or more functions as follows: identifying and verifying certificate applicant, receiving or rejecting certificate applicant, initial certificate revocation or suspension under certain circumstances, handling request of certificate revocation or suspension, receiving or rejecting the request of certificate renewal or re-key. However, RA does not issue certificate (in other words,RA assumes some tasks in place of CA). [Memo:Local registration authority (LRA) used in other documents is the same conception]

Relying party

Certificate recipient relies on the certificate and (or) the digital signatures verified by the certificate. In this standard, the term "user" and "relying party" could be used interchangeably.

Relying party agreement

The agreement between certification authority and relying party, usually provides the rights and obligations of two sides during the course of verifying digital signatures or in other ways.

Subject Certification Authority

In the specific context of CA certificate, subject CA is CA whose public key is verified in the certificate.(See issuing certificate authority)

Subscriber

Certificate subject is issued a certificate.

Subscriber Agreement

The agreement between CA and subscriber, provides the rights and obligations of two sides during the course of issuing and managing certificate.

UniTrust Network Trust Service Hierarchy

It is an open key infrastructure established and operated by Shanghai Electronic Certification Authority Co.,ltd,(acronymed SHECA), called UNTSH, offering electronic certification services based upon digital certificate. SHECA is established as third-party electronic certification authority, devoted to create harmonious network trust environment, and provides secure, reliable, trusted digital certificate services for internet users.

Validation

It is the course of identifying certificate applicants. Validation is subset of identifier, and refers to identifier during the course of establishing the identity of certificate applicant.