UniTrust Network Trust Service Hierarchy

Extended Validation Certification Practice Statement

Version 1.5.9

Valid from: July 25, 2025

Shanghai Electronic Certification Authority Co.Ltd

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

UniTrust Network Trust Service Hierarchy Extended Validation Certification Practice Statement

This document is redacted and issued by Shanghai Electronic Certification Authority Co.Ltd. (SHECA). The total copyright belongs to SHECA.

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

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

Postal Code: 200080

Tel: 86-21-36393197

E-mail: cps@sheca.com

Brand Explanation

"UniTrust" and "协卡" are registered trademark of Shanghai Electronic Certification Authority Co.Ltd., which are also the service identification of SHECA.

Changing History Record of this document

Version	Valid date	Author	Issuer	Notes
V1.5.9	2025-07-25	Alice Shao	SHECA Security Authentication Committee	Current Version
V1.5.8	2025-04-30	Alice Shao	SHECA Security Authentication Committee	Previous Version
V1.5.7	2024-11-18	Alice Shao	SHECA Security Authentication Committee	Previous Version
V1.5.6	2024-07-01	Alice Shao	SHECA Security Authentication Committee	Previous Version
V1.5.5	2023-07-21	Celia Yu	SHECA Security Authentication Committee	Previous Version
V1.5.4	2023-06-12	Celia Yu	SHECA Security Authentication Committee	Previous Version
V1.5.3	2023-04-18	Celia Yu	SHECA Security Authentication Committee	Previous Version
V1.5.2	2022-04-18	Toria Chen	SHECA Security Authentication Committee	Previous Version
V1.5.1	2021-11-15	Toria Chen	SHECA Security Authentication Committee	Previous Version
V1.5	2021-6-18	Toria Chen	SHECA Security Authentication Committee	Previous Version
V1.4.9	2021-4-29	Toria Chen	SHECA Security Authentication Committee	Previous Version
V1.4.8	2020-8-11	Toria Chen	SHECA Security Authentication Committee	Previous Version
V1.4.7	2020-6-5	Toria Chen	SHECA Security Authentication Committee	Previous Version
V1.4.6	2020-4-30	Toria Chen	SHECA Security Authentication Committee	Previous Version
V1.4.5	2020-3-27	Toria Chen	SHECA Security Authentication Committee	Previous Version
V1.4.4	2019-5-29	Toria Chen	SHECA Security Authentication Committee	Previous Version
V1.4.3	2018-9-10	Toria Chen	SHECA Security Authentication Committee	Previous Version

V1.4.2	2018-8-31	Toria Chen	SHECA Security Authentication Committee	Previous Version
V1.4.1	2018-7-12	Toria Chen	SHECA Security Authentication Committee	Previous version
V1.4	2018-6-1	Toria Chen	SHECA Security Authentication Committee	Previous version
V1.3	2017-5-24	Ruby Xiong	SHECA Security Authentication Committee	Previous version
V1.2	2016-5-25	John Cui	SHECA Security Authentication Committee	Previous version
V1.1	2014-4-25	John Cui	SHECA Security Authentication Committee	Previous version
V1.0	2013-4-28	John Cui	SHECA Security Authentication Committee	Previous version

Changes Description

Version	Description
V1.5.9	Disclose tset web pages for EV certificates; Update initial identity validation requirements and methods; Update signature algorithm identifier; Update frequency and circumstances of assessment; Align paragraph structure with outline in RFC3647 section 6； Adjustment of wording;
V1.5.8	Update UniTrust EV PKI Hierarchy; Adjustment of wording
V1.5.7	Disclosure of newly issued Sub-CAs
V1.5.6	Update Sub-CAs status
V1.5.5	Disclosure of newly issued Sub-CAs Xinnet DV SSL /Xinnet OV SSL
V1.5.4	Information of reissued corss-signed UCA Global Root G2
V1.5.3	Disclosure of newly issued Sub-CAs SHECA OV Server CA G7; Update Sub-CAs status; Update CRL/ARL renewal cycle
V1.5.2	Disclosure of newly issued Subordinate Root CECloud Secure Server CA V1
V1.5.1	Information about disable partial Subordinate Roots Disclose special domain validation rules of China e-government extranet
V1.5	Update ARL renewal cycle Revise key length requirement of Code Signing and Timestamp certificate
V1.4.9	Disclosure of newly issued Sub-CAs

	Delete outdated domain validation method listed in section 3.2.4.1 2(8),(9) of last version
V1.4.8	Disclosure of LDAP address Power supply of server room
V1.4.7	Information of new Root UniTrust Global Root CA R1，UniTrust Global Root CA R2； Information of Root newly used for issuing EV certificates, UCA Global G2 Root Revise revocation mechanism
V1.4.6	Delete outdated domain validation method listed in section 3.2.5 2(3) of last version Revise revocation mechanism Add an initial investigation reporting mechanism
V1.4.5	Information of new cross-signed UCA Global G2 Root Certificate validity changed Certificate domain validation method changed
V1.4.4	Information of new root certificate UniTrust PTC Root CA R1, UniTrust PTC Root CA R2 Added Reason for Revoking Code Signing Certificate
V1.4.3	Added Changes Description
V1.4.2	Revise EV Certificate hierarchical structure Chart; Fix some translation errors
V1.4.1	Revised Data Source Accuracy, stated the 825 validity; IP Address Recognition and Identification; CAA Record Checking Requirement
V1.4	Modified UniTrust Network Trust Service Hierarchy; Added Object Identifier (OID); Modified Validation of Domain Name
V1.3	Revised Revocation Request Process and Who Can Request Revocation
V1.2	Revised Key Pair and Certificate Usage
V1.1	Added the Situation of Certificate Revocation Modified Revocation Process

	Adde endix at
V1.0	N.A.

@Shanghai Electronic Certification Authority Co. Ltd. all rights reserved.

The total copyright belongs to Shanghai Electronic Certification Authority Co. Ltd. =uÅuÅc c uĎıC.

6.3 Other Aspects of Key Pair Management 69
6.3.1 Public Key Archival 69
6.3.2 Certificate Operational Periods and Key Pair Usage Periods 69
6.4 Activation Data 70
6.4.1 Activation Data Generation and Installation 70
6.4.2 Activation Data Protection 70
6.4.3 Other Aspects of Activation Data 70
6.5 Computer Security Controls 70
6.5.1 Specific Computer Security Technical Requirements 70
6.5.2 Computer Security Rating 71
6.6 Life Cycle Technical Controls 71
6.6.1 System Development Controls 71
6.6.2 Security Management Controls 71
6.6.3 Life Cycle Security Controls 71
6.7 Network Security Controls 71
6.8 Time-Stamping 71
7. Certificate, CRL, and OCSP Profiles 72
7.1 Certificate Profile 72
7.1.1 Version Number(s) 72
7.1.2 Certificate Extensions 72
7.1.3 Algorithm Object Identifiers 72
7.1.4 Name Forms 73
7.1.5 Name Constraints 73
7.1.6 Certificate Policy Object Identifier 73
7.1.7 Usage of Policy Constraints Extension 73
7.1.8 Policy Qualifiers Syntax and Semantics 73
7.1.9 Processing Semantics for the Critical Certificate Policies Extension 73
7.2 CRL Profile 73
7.2.1 Version Number(s) 73
7.2.2 CRL and CRL Entry Extensions 73
7.3 OCSP Profile 73
7.3.1 Version Number(s) 73
7.3.2 OCSP Extensions 74
8. Compliance Audit and Other Assessments 74
8.1 Frequency and Circumstances of Assessment 74
8.2 Identity/Qualifications of Assessor 74

8.3 Assessor's Relationship to Assessed Entity 74
8.4 Topics Covered by Assessment 74
8.5 Actions Taken as a Result of Deficiency 75
8.6 Communications of Results 75
9. Other Business and Legal Matters 75
9.1 Fees 75
9.1.1 Certificate Issuance or Renewal Fees 75
9.1.2 Certificate Access Fees 75
9.1.3 Revocation or Status Information Access Fees 75
9.1.4 Fees for Other Services 76
9.1.5 Refund Policy 76
9.2 Financial Responsibility 76
9.2.1 Insurance coverage 76
9.2.2 Other Assets 76
9.2.3 Insurance or Warranty Coverage for End-Entities 76
9.3 Confidentiality of Business Information 77
9.3.1 Scope of Confidential Information 77
9.3.2 Information Not Within the Scope of Confidential Information 77
9.3.3 Responsibility to Protect Confidential Information 77
9.4 Privacy of Personal Information 77
9.4.1 Privacy Plan 77
9.4.2 Information Treated as Private 77
9.4.3 Information Not Deemed Private 77
9.4.4 Responsibility to Protect Private Information 77
9.4.5 Notice and Consent to Use Private Information 77
9.4.6 Disclosure Pursuant to Judicial or Administrative Process 78
9.4.7 Other Information Disclosure Circumstances 78
9.5 Intellectual Property rights 78
9.6 Representations and Warranties 78
9.6.1 CA Representations and Warranties 79
9.6.2 RA Representations and Warranties 79
9.6.3 Subscriber Representations and Warranties 79
9.6.4 Relying Party's Representations and Warranties 80
9.6.5 Representations and Warranties of Other Participants 80
9.7 Disclaimers of Warranties 80
9.8 Limitations of Liability 81

9.9 Indemnities 81
9.10 Term and Termination 81
9.10.1 Term 81
9.10.2 Termination 81
9.10.3 Effect of Termination and Survival 82
9.11 Individual Notices and Communications with Participants 82
9.12 Amendments 82
9.12.1 Procedure for Amendment 82
9.12.2 Notification Mechanism and Period 82
9.12.3 Circumstances Under Which OID Must be changed 82
9.13 Dispute Resolution Provisions 83
9.14 Governing Law 83
9.15 Compliance with Applicable Law 83
9.16 Miscellaneous Provisions 83
9.16.1 Entire Agreement 83
9.16.2 Assignment 83
9.16.3 Severability 83
9.16.4 Enforcement 83
9.16.5 Force Majeure 83
9.17 Other Provisions 84
Appendix A Acronyms and Definition 85
Appendix B Terminology and Abbreviations 87
EV Certificates Required Certificate Extensions 89

1. Introduction

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

UNTSH EV CPS explains the specific requirements SHECA shall obey when providing the certificate services that include, but not limited to, issuing, managing, revoking, and renewal certificate. UNTSH EV CPS is formulated by UniTrust Network Trust Service Hierarchy Extended Validation Certificates Policies (UNTSH EV CP), following the rule of 'Electronic Signature Law of People's Republic of China' and the requirements of UNTSH EV CP. UNTSH CP is the principal statement of policy governing the UNTSH. It establishes the business, legal, and technical requirements for approving, issuing, managing, using, revoking, and renewing, digital Certificates within UNTSH and providing associated trust services. These requirements protect the security and integrity of the UNTSH EV Certificate, apply to all UNTSH EV Participants, and thereby provide assurances of uniform trust throughout the UNTSH EV. More information is available in UNTSH EV CP.

UNTSH operated by SHECA, contains users, subscribers and relying parties subjected to it. While the UNTSH EV CP sets forth requirements that UNTSH EV Participants must meet, this CPS describes the practices how SHECA and participants meet these requirements:

- securely managing the core infrastructure that supports the UNTSH, and
- issuing, managing, revoking, and renewing UNTSH EV Certificates in accordance with the requirements of the CP

This CPS conforms to RFC 3647 for Certificate Policy and Certification Practice Statement construction, also conforms to the current version of the CA/Browser Forum (CA/BROWSER FORUM) requirements published at www.cabforum.org including:

- Guidelines for the Issuance and Management of Extended Validation (EV) Certificates
- Guidelines for the Issuance and Management of Extended Validation (EV) Code-Signing Certificates
- Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates

In the event of any inconsistency between this document and those Requirement, those Requirements take precedence over this document. The EV Certificates SHECA issued under UNTSH EV CP conform to the CA/BROWSER FORUM Requirements. SHECA assert that all Certificates issued containing UNTSH EV CP and CPS identifier(s) are issued and managed in conformance with the CA/Browser Forum Requirements.

1.1 Overview

This CPS sets forth procedures which SHECA should follow to issue certificate, according to Guidelines for Extended Validation Certificates published by CA/Browser Forum which set forth the minimum requirements.

The CPS applies to UNTSH EV Certificate hierarchy (refer to Section 1.1.2) and related user, subscriber and replying party, etc. The CPS, as a single document, covers practices and procedures concerning the issuance and management of all EV Certificates. SHECA may publish Certificate Practices Statements that are supplemental to this CPS in order to conform to the specific policy requirements of Government, or other industry standards and requirements. These supplemental certificate policies shall applicable to subscribers for the certificates issued under the supplemental policies and their relying parties. The CPS is only one of a set of documents relevant to UNTSH. These other documents include:

- Subscriber Agreement
- CA/RA Operation Standard

- Relying Party Agreement
- Assessment and Audit Standard
- Other Related Agreement and Standard

The object of EV certificates which issued in accordance with the CPS, is various organizations applied for EV Certificate and validated the identity by SHECA. All UNTSH EV Certificate subscriber and relying party must decide how to use and trust certificate correspond related provisions of this CPS and CP.

EV SSL Certificates are used on the Internet SSL / TLS authentication, aiming to establish a secure communications pipeline through SSL/TLS protocol. The owner of the certificate may be displayed in a specific way, enabling the users to confirm the website is controlled by a trusted entity.

The primary purpose of EV SSL Certificate is to identify the legal identity that controls a website (EV SSL Certificate contained information such as institution name, business address, registered institution and registered code, etc., could reasonable guarantee that the website visited is owned and controlled by a legal entity), and enable encrypted channel (data encryption and transfer between user browser and website).

Secondly, by confirming an entity's legal and existence in reality, the EV Certificate help the entity get a legality statement to operate a website, while assist in proving solution to phishing and other forms of online fraud (making phishing and online identity fraud used SSL certificate more difficult, and can also assist in law enforcement investigation of phishing and other forms of online fraud).

In addition, EV SSL certificates only concerns the identity of the subject named in the certificate, not the subject's behavior. EV SSL Certificate do not provide any guarantee, statement or warranties on whether the entity is comply with law, regulation requirements, business integrity and the security of the business.

1.1.1 UNTSH Structure

The EV CPS is formulated in accordance with UNTSH EV CP. SHECA doesn't set Affiliate, subcontractor, external RA or Enterprise RA that relate to EV Certificates. Subscriber, relying party and related entities use and trust certificate in accordance with this EV CPS and EV CP while performing obligations.

UNTSH EV Structure contains root CAs and subordinate CAs. EV Certificate services and management within UNTSH EV Structure should completely, accurately and comprehensively perform and implement the requirements of this document and EV CP.

1.1.2 UNTSH EV Certificate hierarchical structure

UNTSH EV Certificate hierarchical structure is as follows:

UCA Global G2 Root

- SHECA EV Server CA G2 (revoked)

UCA Extended Validation Root

- SHECA RSA Extended Validation Code Signing CA (revoked)
- SHECA RSA Extended Validation Server CA (revoked)
- SHECA EV Server CA G3
- SHECA EV Code Signing CA G2
- SHECA Extended Validation SSL CA (revoked)
- SHECA Extended Validation Code Signing CA (revoked)

- SHE

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

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

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

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

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

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

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

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

Authorized CAA Records of SHECA is: sheca.com

4.2.2 Approval or Rejection of Certificate Applications

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

If the application is clearly prohibit the by laws and regulations, or is a SHECA considered high-risk, SHECA should reject the application,

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

For those organizations is prohibited engaging in commercial activities or public activities by laws and regulations, national government departments, industry regulators, SHECA has the right to refuse issuing an EV certificate. In addition, if the certificate applicants restricted by relevant laws and regulations, the State or local government, SHECA can reject their participation in the EV certificate request.

4.2.3 Time to Process Certificate Applications

SHECA should complete processing certificate applications within a reasonable time.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

CA will generate and issue certificates after the certificate application is approved. CA generates and issues a certificate to the applicant based on the information which has been

approved in the certificate application. Operation of issuing certificates is in compliance with requirements of guidance issued by CA / Browser Forum through www.cabforum.org .

(1) Submit the request documents self-generated in PKCS # 10 formats on application date to SHECA in reliable manner

(2) CA verify that the request does come from the applicant

(3) Confirm the integrity of the PKCS # 10 format request file in the way verifying the digital signature.

(4) Check whether the name and other information in request file is consistent with the validated name in the application form.

(5) The subscriber certificate should be issued after verification.

(6) Upon completion of the issuance of the certificate, subscribers will be informed offline or online to download or receive it.

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

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

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

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

The following conduct constitutes certificate acceptance:

- Download or install a Certificate.
- Fail to object to the certificate or its content.

After a certificate is received, the subscriber should do the following procedures:
(1) Confirm the consistency of the certificate content and application information
(2) Confirm the correctness of certificate contents
(3) Verify whether the public key information in certificate is the same with the content in PKCS # 10 certificate request
(4) Verify the validity and legitimacy of the certificate with CA certificate
If exception is found by implementing of the above process, the subscriber should inform SHECA immediately to revoke the certificate and renew the request for issuance.
After receiving the applied certification, subscriber must confirm fully understand and agreement to the rights and obligations of certificate usage, if not, the certificate shall be deemed rejected, SHECA should revoke the certificate.

4.4.2 Publication of the Certificate by the CA

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

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

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

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

4.5.2 Relying Party Public Key and Certificate Usage

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

Relying Party should rely on a certificate under reasonable circumstances. If the circumstances indicate additional assurances are required, the Relying Party must obtain assurances for such reliance to be deemed reasonable.

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

- Certificates should be used properly under specific situation, and could not be used for any forbidden or limited situation identified by CPS. SHECA has no responsibility to assess whether the certificate has been properly used
- The certificate is being used in accordance with the .H8VDJHfield extensions included in the certificate.
- The status of the certificates in the certificate should be verified. If any of the Certificates in the Certificate Chain has been revoked, the Relying Party should judge independently whether the digital signature is signed prior to the revocation.

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

Before relying party trust certificates issued by SHECA, at least the following should be operated to determine whether trust the certificate or not:
(1) Obtain the EV Root Certificates of SHECA
(2) Check whether the certificate and the subscriber's certificate is in validity period
(3) Check whether the certificate is valid digital signature
(4) Check whether the certificate is revoked
(5) Verify the digital signature contained in the subscriber certificate with public key of certificate.
(6) Check whether the subscriber certificate is revoked.
If these operations fail validation, which means that subscribers certificate that relying parties obtained is not issued by SHECA, or the certificate has expired, or if the certificate has been revoked, or the certificate digital signature cannot be authenticated, relying party should not trust the subscriber certificate.

4.6 Certificate Renewal

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

4.6.1 Circumstances for Certificate Renewal

SHECA doesn't provide the certificate renewal service.

4.6.2 Who May Request Renewal

No stipulation.

4.6.3 Processing Certificate Renewal Requests

No stipulation.

4.6.4 Notification of New Certificate Issuance to Subscriber

No stipulation.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

No stipulation.

4.6.6 Publication of the Renewal Certificate by the CA

No stipulation.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.7 Certificate Re-key

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

4.7.1 Circumstances for Certificate Re-key

Certificate re-key refers to requirements in Section 3.3.1.

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

4.7.2 Who May Request Re-key

Subscribers are the subjects of certificate re-key application.

4.7.3 Processing Certificate Renewal Requests

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

Certificate issuance is in accordance with Section 4.3.

4.7.4 Notification of New Certificate Issuance to Subscriber

Refer to Section 4.3.2

4.7.5 Conduct Constituting Acceptance of a Renewal Certificate

Refer to Section 4.4

4.7.6 Publication of the Re-key Certificate by the CA

Refer to Section 4.4.2.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

Refer to Section 4.4.3.

4.8 Certificate Modification

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

4.8.1 Circumstances for Certificate Modification

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

4.8.2 Who May Request Certificate Modification

No stipulation.

4.8.3 Processing Certificate Modification Requests

No stipulation.

4.8.4 Notification of New Certificate Issuance to Subscriber

No stipulation.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

No stipulation.

4.8.6 Publication of the Modified Certificate by the CA

No stipulation.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.9 Certificate Revocation and Suspension

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

4.9.1 Circumstances for Revocation

4.9.1.1 Reasons for Revoking a Subscriber Certificate

In any of the following circumstances, the subscriber certificate should be revoked in 24 hours:

- Subscriber (or authorized proxy) request to revoke certificate, and CA make sure the request is from the subscriber;
- Because the certificate is improper used in violation of the main and important obligations of national laws and regulations;
- SHECA is made aware that the original certificate request was not authorized and does not retroactively grant authorization;
- Certificate's private key is lost, stolen, tampered, unauthorized disclosure or damaged, or no longer comply with the requirements of key size and key parameters setting and quality check in section 6.1.5 and section 6.1.6;
- SHECA is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate;
- SHECA obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address in the Certificate should not be relied upon.
- SHECA obtains evidence that the Certificate was misused;
- SHECA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully- Qualified Domain Name;
- SHECA is made aware that the Certificate was not issued in accordance with these Requirements or SHECA's Certificate Policy or Certification Practice Statement;
- 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;
- Revocation is required by SHECA's Certificate Policy and/or Certification Practice Statement;

- Within the validity period, the information contained in the subscriber certificate changes, exists errors or mistakes, is inconsistent with the actual information of subscriber;
- Subscriber information in the certificate is substantially changed;
- After certificate installation, if false information is found by SHECA in the application materials provided by EV certificate subscriber
- The application for certificate is not authorized or can't be traced to the authorization
- Subscriber doesn't use EV certificate according to CP/CPS or the agreement, or changes the usage of EV certificate, or use this certificate to fishing, cheating or other crimes.
- Private key of subscriber is confirmed or suspected to be cracked, damaged, lost, or tampered
- Subscribers violates the obligations of CP and CPS, Subscriber Agreement and other provisions, representations or warranties, or subscribers cannot fulfill the obligations specified in the relevant agreement
- Subscribers failed to fulfill the obligation to pay
- Continuity of using the certificate will cause harm to SHECA business credit and trust mode
- The change, revocation or dismiss of subscriber legal identification
- Private key of SHECA EV Root or EV sub CA certificate exists security risk or being cracked or blabbed
- SHECA found that the issuance of EV subscriber certificates does not comply with the guide or SHECA EV certificate policy; Or believe that the information displayed in the EV certificate is not correctly
- SHECA terminates operation and has not arranged other EV certificate issuing authorities to offer revoke services; or SHECA no longer have the rights or qualifications to issue EV certificates
- Evolution of technologies or standards may lead to unacceptable risk for the relying party or software providers.
- Judgments of the judiciary, such as the domain name in the certificate, the certificate subject information does not remain effective or continue to be trusted
- When SHECA obtains evidence or is made aware that the subscriber has suspect Code in their signed software object, the Code Singning Certificate should be revoked;
- The relevant provisions of laws and regulations or requirements

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

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

In any of the following circumstances, the Subordinate CA Certificate should be revoked in 7 days:

1. The Subordinate CA requests revocation in writing;
2. The Subordinate CA notifies the SHECA that the original

SHECA establishes process management rules which bind employees not to reveal sensitive information of SHECA Certificate Services system. All employees should sign confidentiality agreement with SHECA, and are not allowed engaging in similar work as SHECA two years after the contract expires.

If necessary, SHECA can cooperates with the relevant government departments and investigative agencies to complete background checks on employees.

5.3.3 Training Requirements

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

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

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

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

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

It would be recorded after training.

5.3.4 Retraining Frequency and Requirements

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

The training of corporate security management strategy should be conducted at least once a year.

Operators of UniTrust Network Trust Service should take relevant skills and knowledge training at least once a year.

Appropriate training needed to be arranged for upgrades authentication system, using the new system, PKI / CA and password technological advances, etc.

5.3.5 Job Rotation Frequency and Sequence

No stipulation

5.3.6 Sanctions for Unauthorized Actions

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

Typically, when an employee is suspected or has been carried out unauthorized operations, such as abuse of rights without authorization, exceeding authority or unauthorized using SHECA system operation, SHECA forbids that employee entering workplace once receiving information. According to the severity of the circumstances, take actions of education, expulsion, submitting Judiciary treatment, etc.

Once detecting unauthorized behavior, security token should be revoked or terminated.

5.3.7 Independent Contractor Requirements

In limited circumstances of human resource or special requirements, CA and RA can use independent contractors or consultants to fill Trusted Persons as long as it meets the following conditions:

- No suitable Trusted Person and independent contractors or consultants can take this role.
- Independent contractor or consultant can be trusted as a trusted employee

Otherwise, independent contractors and consultants are permitted access to secure facilities only to the extent they are escorted and directly supervised by Trusted Persons at all times.

In addition to signing confidentiality agreement, independent contractors or consultants should take training of necessary knowledge and safety regulations to comply with SHECA specifications strictly.

5.3.8 Documentation Supplied to Personnel

SHECA provides its employees the requisite training and other documentation needed to perform their job responsibilities competently and satisfactorily, including at least:

- CA system operation documentation
- Key equipment operating documentation
- Certificate Services Guide and related specifications
- CP, CPS, and related specifications
- Internal operating documents, including backup manual, disaster recovery programs
- Job descriptions
- Company related training materials
- Safety regulations

For sensitive and confidential documents, SHECA strictly limits range of personnel and specify confidentiality requirements and take appropriate measures.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

CA and RA manually or automatically log the following events:

- The type of event,
- The result of event,
- The date and time the event occurred,
- The entity or person caused the event.

SHECA records logs and events types, including but not limited to the following:

- Running event, including but not limited to Key generation of CA and Sub CA; System go live and off-line; System and application startup and shutdown; CA Key and information change, Password equipment life-cycle-related events; CA private key activation data manipulation and physical access logs; Changes and maintenance of system configuration including key, activation data or Media Destruction of Personal Information
- Certificate life cycle event, including but not limited to issuing, renewal, re-key, revocation, suspended;
- Certificate applicant identity documents and Identity verification audit records (including verification content, time, methods and etc.)
- Certificate format adjustments or changes
- CP, CPS modification
- Trusted Person events, including but not limited to logon and logoff attempts, password creation, Delete and Set, User system rights chance, and related personnel changes
- Abnormal and accident reports
- Read and write operations of certificate and information repository
- Certificate generation policy changes, such as changing validity
- Physical and Environmental Management
- Security events
- Audit events

5.4.2 Frequency of Processing Log

SHECA reviews audit logs monthly or quarterly to verify real time alerts of significant security and operational events according to the operational requirements. Actions taken based on audit log reviews are also documented.

Review is carried out not less than twice a year.

5.4.3 Retention Period for Audit Log

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

5.4.4 Protection of Audit Log

Audit logs are protected avoid unauthorized viewing, modification, reading, deletion, or other tampering in order to make sure:

- Only authorized person can read audit logs
- Only authorized person can backup audit logs
- Using logical access control to save currently exist and archived electronic audit records, and store in non-rewritable discs or other media which cannot be modified
- Audit records in paper and other media are stored in a safe place

5.4.5 Audit Log Backup Procedures

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

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

5.4.6 Audit Collection System

No stipulation.

5.4.7 Notification to Event-Causing Subject

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

5.4.8 Vulnerability Assessments

Events recorded in the audit section is used to monitor system vulnerabilities, logical security vulnerability assessment data can be recorded in real time, daily, monthly, and annual basis.

SHECA performs regular vulnerability assessments at least annually, which focus on internal and external threats facing. Based on the assessment results and the implementation of regular audit of system log, the safety control measures related to system operation should be timely adjusted in order to minimize the risk of system operation. Including:

- Vulnerability Assessment of operating system
- Vulnerability Assessment of physical facilities
- Vulnerability Assessment of Certificate System
- Vulnerability Assessment of network

5.5 Records Archival

5.5.1 Types of Records Archived

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

- Audit data collected in Section 5.4;
- Documentation of certificate system construction and upgrade;
- CP, CPS and related specifications
- Certificate
- Background survey
- Audit assessment data
- Certificate application information
- Certificate application documentation
- Certificate lifecycle information

5.5.2 Retention Period for Archive

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

5.5.3 Protection of Archive

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

Archived content is protected by both physical security measures and cryptographic techniques to ensure long term valid storage. Only authorized staff could access in a specific security way. No one get free access to obtain it without legal requirements and certification practices.

SHECA protects related information files from threats of harsh environments, such as the destruction of temperature, humidity and strong magnetic force, etc., in order to ensure that the archives in the specified period meet any legitimate using requirement. For critical data, SHECA will use off-site backup to save.

The identity information of applicants, subscribers and authentication data which SHECA preserves can't be accessed to any unrelated third parties without lawful means from governmental authority or the judiciary.

5.5.4 Archive Backup Procedures

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

Paper materials need to be preserved in the secure facility.

5.5.5 Requirements for Time-Stamping of Records

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

Archive of electronic records (such as certificates, certificate revocation lists, etc.) shall contain date and time information using the date and time of computer operating system. All computer systems are regularly checked to ensure the accuracy and reliability of date and time information in electronic records.

Archived hard copy records date and time information if necessary. Written records of the date and time cannot be changed freely, and any changes must be confirmed with the auditor's signature.

5.5.6 Archive Collection System

All filing related to certification services are performed by internal staff in accordance with privileges and responsibilities. Audit logs are generated by the internal system and the relevant documentation of certificate system operation is collected and managed by relevant persons with permission.

5.5.7 Procedures to Obtain and Verify Archive Information

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

Archived data can be obtained only after formal authority with written application. Auditors are responsible for archiving data verification. The authenticity of the document and the date of the issuer of written document must be verified. The digital signature of electronic documents should be verified or in cryptography way.

5.6 Key Changeover

To reduce the risk of CA private key cracked, SHECA regularly updates CA certificate private key.

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

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

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

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

SHECA develops recovery process for broken systems and data, and does the corresponding drill annually.

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

If the CA's computer equipment is destroyed or run out, but the CA private key is not damaged, then databases and knowledge repository recovery and backup systems should be resumed in priority to quickly re-implement functions of issuance, revocation and management of certificates.

5.7.3 Entity Private Key Compromise Procedures

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

5.7.4 Business Continuity Capabilities after a Disaster

CA and RA should develop, build, test, maintain and execute a disaster recovery plan when necessary to mitigate the effects of any manual or natural catastrophes. Disaster recovery plan should clarify conditions of activation plan, acceptable system outage and system recovery time. Business continuity is compliance with requirements of guide that CA / Browser Forum (CA / Browser Forum) published by www.cabforum.org.

In the event of a natural disaster or other catastrophe, if certificate status services couldn’t be recovered in a 24-hour, CA will open offsite backup lab facilities to provide the certificate status service within 24 hours after the opening.

5.8 CA or RA Termination

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

When termination is required, SHECA will take actions to minimize disruption to system operation by reasonable arrangements to transfer business to other legitimate certificate authority to continue.

Arising from the business end, contract termination, company consolidation, company integration which leads that certificate services could not be maintained, SHECA will process according to the following:

(1) Before the deadline of laws and regulations, notify the responsibility authorities, certificate holders and all other related parties.

(2) Three months prior to the termination of service, the termination of service and the fact that other related certificate authority would undertake the business will be notified to subscribers and published in the knowledge repository.

(3) Arrange business undertaking and transfer certificates, keys, etc. to the relevant undertaking agency.

(4) Transfer relevant data such as CP, CPS, operations manuals, subscriber agreement, knowledge repository, user application documents, audit records and other documents to undertaking agency.

(5) Clear CA key.

(6) Formally declare the notice to subscribers that certificate business was transferred to undertaking agency.

When business is terminated, rights and obligations will be handled in accordance with the subscriber agreement.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

CA key pair is generated by device with approval and permission of the national competent authority. Due to strict requirements for cryptographic products and systems, SHECA should comply with relevant state regulations during key generation, management, storage, backup and recovery. Besides, SHECA should follow CNS 15135, ISO 19790, or Hardware CA key generation and management regulations FIPS140-2 standard, and use standard hardware devices to generate and manage CA keys.

CA key generation process needs to be carried out under independent third party impartial witness and they should issue witness report.

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

For subscriber certificates under UNTSH EV Certificate hierarchical structure (refer to section 1.1.2), SHECA must not generate key pair for subscribers.

6.1.2 Private Key Delivery to Subscriber

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

6.1.3 Public Key Delivery to Certificate

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

6.1.4 CA Public Key Delivery to Relying Parties

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

6.1.5 Key Sizes

RSA Key length (for both CA root key and subscriber key) is 2048 bit. Since June 1st,2021,the key length of codesigning and timestamp certificates should be at least 3072 bits.

These requirements are in accordance with the requirements issued by CA/Browser Forum via www.cabforum.org.

6.1.6 Public Key Parameters Generation and Quality Checking

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

6.1.7 Key Usage Purposes

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

1.Self-signed Certificates to represent the Root CA itself;

2.Certificates for Subordinate CAs and Cross-Certified Subordinate CA Certificates;

3.Certificates for infrastructure purposes (administrative role certificates, internal CA operational device certificates); and

4.Certificates for OCSP Response verification.Subscriber Certificate version issued by SHECA is X509 v3. It contains KeyUsage extension. If SHECA specify the use of issued certificate in KeyUsage extension, subscribers should use the certificate in accordance with the specified purpose.

Subscriber Certificate KeyUsage extension contains digitalSignature, keyEncipherment, dataEncipherment and keyAgreement.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

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

Please find details from hardware product information provided by the device manufacturer with production qualification required by national code authorities.

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

1. SHECA adopts multi-person control strategy to generate, use and deactivate the private key (m out of n)

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

Protection of smart cards or smart-password key related to private key information, as well as passwords protection should be controlled by independent management, and stored in a safely controlled environment.

2. The private key of the subscriber certificate should be controlled by the subscriber

The private key of the subscriber certificate should be controlled by the subscriber and responsible for its safety. If a specify individual is required to manage the private key, the specify person must be effectively authorized in order to prevent the private key from being leaked, damaged, lost, or used unauthorized. When the private key occurs the security problems above, the subscriber has an obligation to immediately inform SHECA.

6.2.3 Private Key Escrow

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

6.2.4 Private Key Backup

SHECA CA private key backup performed in the following way:

(1) Keys are stored in hardware cryptographic modules, in accordance with specified in section 6.2.2, backup in a multiple controlled manner after private key encryption, and encryption key protection information is stored separately in multiple smart cards using secret-division technique. Smart card is hold by different personnel.

(2) Smart card storing cryptographic key information is placed in a security environment with the dual control and sealed for safekeeping by security personnel.

(3) Hardware cryptographic module storing backup private keys is placed inside a controlled environment with strict security. At least two persons hold safe correlation token separately.

6.2.5 Private Key Archival

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

6.2.6 Private Key Transfer into or from a Cryptographic Module

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

6.2.7 Private Key Storage on Cryptographic Module

CA private keys shall be stored in encrypted form within hardware cryptographic devices.

6.2.8 Method of Activating Private Key

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

Provisions related to processes should be in accordance with Section 5.2.

6.2.9 Method of Deactivating Private Key

The activated private keys are deactivated upon logging off their system after Identification or automatically deactivate after predetermined time in order to avoid the private key being used illegally.

6.2.10 Method of Destroying Private Key

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

6.2.11 Cryptographic Module Rating

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

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

After the CA certificate (including the root CA certificate and sub-CA certificate) expires, the certificate should be archived, including the public key contained in the certificate.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

Certificate validity period should be clearly recorded in the CPS, which is in accordance with the requirements of reference issued via www.cabforum.org by CA/Browser Forum.

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

The key pair usage period and certificate validation period are set as following:

Type	Key Pair Usage Period	Certificate Validation Period
Root certificate	30 years	30 years
Subordinate CA certificate	25 years	25 years

EV SSL certificate	No stipulation	398 days
EV CodeSigning certificate	No stipulation	39 months

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

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

The activation data on smart card is read and written by card reader, and protective password with a smart card (Pin code) is used for activated data access authentication.

6.4.2 Activation Data Protection

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

Smart card Pin code cannot be recorded on any paper or other media. If entered incorrectly 3 times, the card will lock automatically. When the transfer of smart card occurs, the new holder must reset the Pin code.

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

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

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

System security meets requirements published by CA / Browser Forum through www.cabforum.org.

Typically, SHECA takes the following controls of Certificate management system through the relevant operating systems, related hardware and software equipment and management measures:

(1) Using identification to login

(2) Providing customized access control

(3) Having security audit capability

(4) Limitations to certificate services and role-based access control

(5) Identification of reliable role and identity

(6) Ensuing communication and database security.

(7) Safe and reliable pipeline associated with roles and identity

(8) Program integrity and security control.

6.5.2 Computer Security Rating

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

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

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

System development follows the ISO27001 specification.

All of core development devices have strict security precautions and means of killing malicious code, and irrelevant hardware and software are not allowed to be installed or developed.

6.6.2 Security Management Controls

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

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

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

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 Network Security Controls

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

Certificate system must be managed and operated by authorized operators after rigorous authentication.

To protect against network intrusions and damages, installation and configuration of firewall, intrusion detection, anti-virus systems and etc. are used to enhance network security.

Certificate system and the internal database server is only connected to the internal network and isolated by firewall. Only internal devices are allowed connection and only authorized personnel or the system gets access to visit after identification.

6.8 Time-Stamping

No stipulation.

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

7.1.1 Version Number(s)

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

7.1.2 Certificate Extensions

The extension of EV certificate is in compliance with RFC 5280 and requirement of CA / Browser Forum 'Guidelines for the Issuance and Management of Extended Validation Certificates ¶

7.1.3 Algorithm Object Identifiers

Keys and hash algorithms for SHECA's EV certificates meet the requirement specified in the CA/B Forum Baseline Requirements and the Applicable EV Guidelines.

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).

7.1.3.2 Signature Algorithm Identifier

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 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

SHA-512 with RSA, (OID) 1.2.840.113549.1.1.13

7.1.3.2.2 ECDSA

SHECA uses the following ECDSA signature algorithms and encodings:

SHA-256 with ECDSA, (OID) 1.2.840.10045.4.3.2

SHA-384 with ECDSA, (OID) 1.2.840.10045.4.3.3

SHA-512 with ECDSA, (OID) 1.2.840.10045.4.3.4

7.1.4 Name Forms

SHECA issues EV certificates with Name Forms and Content comply with X.501（Distinguished Name；DN）and RFC 5280 regulation, and the requirements in Section 7.1.4 of CA/B Forum Baseline Requirements

7.1.5 Name Constraints

SHECA uses the nameConstraints extension as needed.

7.1.6 Certificate Policy Object Identifier

SHECA EV Certificates contain the Certificate Policies extension object identifier for the Certificate Policy（Certificate Policies）

The object identifier meets the requirements of CA / Browser Forum EV Guidelines through www.cabforum.org.

7.1.7 Usage of Policy Constraints Extension

SHECA uses the policyConstraints extension as needed.

7.1.8 Policy Qualifiers Syntax and Semantics

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

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2 CRL Profile

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

SHECA issues regularly CRL for the user to query.

7.2.1 Version Number(s)

SHECA issues X 509 V2 version of CRLs.

7.2.2 CRL and CRL Entry Extensions

If a CRL entry reasonCode extension is present, the reason must indicate the most appropriate reason for revocation of the certificate. Refer to the UniTrust CPS Section 7.2.2 for the usage of CRL entry extensions.

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), and the OCSP response issued complies with the RFC6960 standard.OCSP, as an effective supplement to CRL, facilitates certificate users to query certificate status information in time.

7.3.1 Version Number(s)

RFC6960 defines the OCSP V1.

C[illegible] Exte[illegible]n[illegible]

[illegible]sions are [illegible] with RFC6960.

[illegible]gleExtensions of an OCSP res[illegible]e shall not cont[illegible]e reasonCode (OID [illegible]29.21) [illegible]try extension.

[illegible]ompliance Audit and Other Assessments

As an operating subject of UNTSH, SHE[illegible] p[illegible]rms consistency audits and operation assessments quarterly to ensure the relia[illegible]ity, secu[illegible] and controllability of certification services. In addition to internal audit and assessment, SHECA also hires an independent auditing firm in accordance with WebTrust audit for external assessment.

8.1 Frequency and Circumstances of Assessment

SHECA has a currently valid WebTrust Seal of Assurance for CAs. Before issuing EV Certificates, SHECA and its Root CA MUST successfully complete a point-in-time readiness assessment audit against the WebTrust EV Program.

SHECA MUST complete any required point-in-time readiness assessment no earlier than twelve (12) months prior to issuing an EV Certificate.

SHECA MUST undergo a complete audit under such scheme within ninety (90) days of issuing the first EV Certificate.

SHECA conducts an external audits and evaluations at least once a year and executes internal audits and evaluations on a yearly basis.

During the period in which SHECA issues EV Certificates, SHECA MUST strictly control its service quality by performing ongoing self audits against a randomly selected sample of at least three percent of the EV Certificates it has issued in the period beginning immediately after the last sample was taken.

Audit operations should be clearly documented in CPS, and the requirements should be compliant with requirements of guidance published by CA / Browser Forum through www.cabforum.org.

8.2 Identity/Qualifications of Assessor

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The following records shall be kept confidential and private:

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

9.3.2 Information Not Within the Scope of Confidential Information

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

9.3.3 Responsibility to Protect Confidential Information

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

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

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

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

9.4.2 Information Treated as Private

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

9.4.3 Information Not Deemed Private

All information made public in a certificate is deemed not private

9.4.4 Responsibility to Protect Private Information

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

9.4.5 Notice and Consent to Use Private Information

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

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

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

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

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property rights

1. SHECA retain all intellectual property rights in and to SHECA private key, certificate issued, CRL, CP/CPS and other relevant documents.
2. Subscribers retain all intellectual property rights in and to subscriber private key pairs. SHECA will own intellectual right on Certificate once the public key is signed by SHECA to issue the certificate. Subscriber and relying party only have the certificate-use right.
3. SHECA does not guarantee intellectual property rights set forth in the certificate name.

9.6 Representations and Warranties

Within the period of subscriber's EV certificate validity, SHECA warrants specifically include, but are not limited to:

1. Legal existence. From the date of issuance of Subscriber's EV Certificate, SHECA has confirmed that the subject specified in EV Certificate is a valid organization registered in government authority.
2. Identity. From the date of issuance of Subscriber's EV Certificate, SHECA has confirmed that the legal name of the subject specified in EV Certificate consistent with the name recorded by government authority.
3. The right to uses the domain name. From the date of issuance of Subscriber's EV Certificate, SHECA has confirmed the subject specified in EV Certificate has the ownership or exclusive use rights by taking all the necessary and reasonable measure following the relevant clause in Guidelines for the issuance and management of extended validation certificates.
4. EV Certificate Authorization. SHECA has confirmed the subject specified in EV Certificate authorized the issuance of the EV Certificate by taking all the necessary and reasonable measure following the relevant clause in Guidelines for the issuance and management of extended validation certificates.
5. The accuracy of the information. From the date of issuance of Subscriber's EV Certificate, SHECA has taken all necessary and reasonable measures to verify that all information contained in the EV Certificate is accurate.
6. Subscriber Agreement. The application representative of the subject specified in EV certificate has signed a subscriber agreement or accepts the term of use.
7. The certificate status. SHECA maintain an online 24x7 Repository which can be used to check the latest status of all certificate issued by SHECA following the requirement of Guidelines for the issuance and management of extended validation certificates.

8. Revocation. According to the Guidelines for the issuance and management of extended validation certificates, SHECA shall revoke the certificate when a circumstance under which a certificate may or must be revoked happens.

9.6.1 CA Representations and Warranties

SHECA as CA and RA warrants that:

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

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

9.6.2 RA Representations and Warranties

See section 9.6.1 requirements.

9.6.3 Subscriber Representations and Warranties

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

1. Applicant must understand and agree the requirements of CP/CPS and relevant agreement when apply for a EV Certificate,
2. All information and documents in the Certificate Application the Subscriber submitted are true and authentic,
3. Their private key is protected, using the certificate in accordance with restriction requirement in CP/CPS and laws.
4. Applicant should ensure the accurate of information contained in EV Certificate while accept it, also should validate the correspondence of public key and private key in EV Certificate.
5. Subscriber should notify SHECA when the relevant information in the certificate changes occurred.
6. Subscriber should inform SHECA in due time when the private key is lost, leakage or others, and apply for certificate revocation as required. Meanwhile the subscriber should bear the risk and liability arising from using of the certificate before the certificate's revocation status published.

7. Timely renewal certificate in accordance with SHECA provisions,
8. Accept all statements, changes, renewal and upgrades disclosed by SHECA bases on regulation and technology development,
9. For the interest of SHECA and EV certificates' relying party, subscriber should commit and guarantee statements required by Subscriber Agreement.

9.6.4 Relying Party's Representations and Warranties

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

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

9.6.5 Representations and Warranties of Other Participants

Advance vendor warrants:

Advance vendor is required to bear all the cost of the certificate and pays all according to the provisions provided by SHECA.

Advance business's behavior of advance vendor means advance vendor is willing and able to assume responsibility of guaranteeing applicant authenticity based on this CPS.

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

9.7 Disclaimers of Warranties

SHECA can't bear liability in the following circumstances:

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

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

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

4. If the applicant provide intentionally or unintentionally incomplete, unreliable or outdated, including but not limited to forgery, tampering, false information, but applicant also provides the necessary review documents based on the normal process and gets digital certificates issued by SHECA. The legal problems, the applicant result from above should be assumed full responsibility for the economic disputes, and SHECA doesn't assume the legal and economic responsibility associated with the content of the certificate, but can provide investigation and evidence based on victim's Investigation and proof help.

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

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

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

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

9.8 Limitations of Liability

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

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

SHECA MUST NOT limit its liability to Subscribers or Relying Parties for legally recognized and provable claims to a monetary amount less than two thousand US dollars per Subscriber or Relying Party per EV server Certificate.

9.9 Indemnities

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

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

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

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

9.10 Term and Termination

9.10.1 Term

This CPS is effective since it is published, version number and release date shall be specified by the document, as new version is published, and takes effect, the original version shall lose effectiveness automatically.

9.10.2 Termination

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

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

9.10.3 Effect of Termination and Survival

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

9.11 Individual Notices and Communications with Participants

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

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

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

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

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

Sent to others from SHECA via the following address:

The latest address in SHECA's postal record

9.12 Amendments

9.12.1 Procedure for Amendment

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

This CPS must be revised through the approval and verification of SHECA Security Certification Committee ——the highest policy management agency of SHECA after Strategy Development Department puts forward the revision report.

9.12.2 Notification Mechanism and Period

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

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

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

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

9.12.3 Circumstances Under Which OID Must be changed

No stipulation.

9.13 Dispute Resolution Provisions

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

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

9.14 Governing Law

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

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

9.15 Compliance with Applicable Law

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

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

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

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

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

9.16.2 Assignment

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

9.16.3 Severability

In the event that a clause or provision of this CPS is held to be unenforceable by amendment or other reasons, the remainder of the CPS 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. SHECA isn't responsible for the following force majeure events, the violation, delay or inability to perform that CPS regulated beyond its ability to control.

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

9.17 Other Provisions

No stipulation.

Appendix A Acronyms and Definition

SHECA

Abbreviation for Shanghai Electronic Certification Authority Co.,Ltd.

UniTrust Network Trust Service Hierarchy

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

SHECA Security Authentication Committee

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

Certificate Authority

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

Registration Authority

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

Registration Authority Terminal

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

Electronic Certificate

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

Electronic Signature

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

Digital Signature

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

Electronic Signatory

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

Electronic Signature Relying Party

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

Private Key (Electronic Signature Creation Data)

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

signatory in the electronic signature application.

Key (Electronic Signature Verification Data)

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

Subscriber

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

Relying Party

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

Appendix B Terminology and Abbreviations

AICPA	American Institute of Certified Public Accountants, Inc.
ANS	American National Standard
CA	Certification Authority
CC	Common Criteria
CCITSE	Common Criteria for Information Technology Security Evaluation
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
FIPS	Federal Information Processing Standard
ISO/IEC	the International Organization for Standardisation, The International Electrotechnical Commission
ITSEC	Information Technology Security Evaluation Criteria
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificates Status Protocol
OID	Object Identifier
OECD	Organization for Economic Co-operation and Development
PMA	Policy Management Authority
PIN	Personal Identification number
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
RA	Registration Authority
RCA	Root Certification Authority
RSA	Rivest,Shamir,Adleman(encryption algorithm)
TCSEC	Trusted Computer System Evaluation Criteria
URL	Universal Resources Location

SSL	Secure Socket Layer
EV	Extended Validation

EV Certificates Required Certificate Extensions

1. Root CA Certificate

Root Certificates MUST be of type X.509 v3

（a）*basicConstraints*

This extension MUST appear as a critical extension. The cA field MUST be set true. The pathLenConstraint field SHOULD NOT be present.

（b）*keyUsage*

This extension MUST be present and MUST be marked critical. Bit positions for keyCertSign and cRLSign MUST be set. The others bit positions should not be set.

（c）certificatePolicies

This extension SHOULD NOT be present.

（d）extendedKeyUsage

This extension MUST NOT be present.

All other fields and extensions MUST be set in accordance with RFC 5280.

2. Subordinate CA Certificate

（a）*certificatePolicies*

This extension MUST be present and SHOULD NOT be marked critical. The policy OID MUST contain OID of UNTSH EV Policy.

（b）*cRLDistributionPoint*

This extension MUST be present and MUST NOT be marked critical. It MUST contain the HTTP URL ofthe CA's CRL service.

（c）*authorityInformationAccess*

It MUST NOT be marked critical, and it MUST contain the HTTP URL of the Issuing SHECA's OCSP responder

（d）*basicConstraints*

This extension MUST be present and MUST be marked critical. The cA field MUST be set true. The pathLenConstraint field MAY be present.

（e）*keyUsage*

This extension MUST be present and MUST be marked critical. Bit positions for keyCertSign and cRLSign MUST be set. The others bit positions should not be set.

All other fields and extensions MUST be set in accordance with RFC 5280.

3. Subscriber Certificate

（a）*certificatePolicies*

This extension MUST be present and SHOULD NOT be marked critical. The policy OID MUST contain OID of UNTSH EV Policy.

certificatePolicies:policyIdentifier (Required)

EV policy OID

certificatePolicies:policyQualifiers:policyQualifierId (Required)

id-qt 2 [RFC 5280]

certificatePolicies:policyQualifiers:qualifier (Required)

URI to the Certificate Practice Statement

（b）*cRLDistributionPoint*

This extension SHOULD NOT be marked critical. It MUST contain the HTTP URL of the SHECA's CRL service.

（c）*authorityInformationAccess*

It MUST NOT be marked critical, and it MUST contain the HTTP URL of the Issuing SHECA's OCSP responder

（d）*basicConstraints* (optional)

If present, the CA field MUST be set false.

（e）*keyUsage* (optional)

If present, bit positions for keyCertSign and cRLSign MUST NOT be set.

（f）*extKeyUsage*

Either the value id-kp-serverAuth [RFC5280] or id-kp-clientAuth [RFC5280] or both values MUST be present. Other values SHOULD NOT be present.

（g）*SubjectAltNam* □ ***pM***