SHECA TLS CERTIFICATE POLICY AND CERTIFICATION PRACTICE STATEMENT (CP/CPS)

Version 1.4 (Effective Date: May 25, 2026)

Version Control

Version	Released Date	Issuer
1.0 (History version)	September 12, 2025	SHECA Security Certification Committee
1.1 (History version)	November 20, 2025	SHECA Security Certification Committee
1.2 (History version)	December 11, 2025	SHECA Security Certification Committee
1.3 (History version)	March 11, 2026	SHECA Security Certification Committee
1.4 (Current version)	May 25, 2026	SHECA Security Certification Committee

Change Description

Version	Change Description
1.0	Combined CP & CPS for TLS Certificates
1.1	Add Notice of Prohibited Certificate Uses in Section 1.4.2; Add Notice of Revocation Time Limit in Section 4.9.5; Adjust Description of Mass Revocation Plan in Section 5.7.1
1.2	Convert the Document to Markdown Format; Adjust Document Introduction in Section 1.1.2
1.3	Update Validation Methods of Domain Authorization or Control in Section 3.2.2.4; Update the Data Reuse Period in Section 4.2.1; Update the Certificate Validity Period in Section 6.3.2
1.4	Update Validation Methods of Domain Authorization or Control in Section 3.2.2.4; Update Certificate Extensions in Section 7.1.2; Update Description of Self-Audits in Section 8.7; Adjustments of wordings

Copyright Notices

Address: 18F, No.1717 North Sichuan Road, Shanghai, PRC(200080) Tel: +86-21-36393197 Fax: +86-21-36393200 E-mail: report@sheca.com.

For the latest version of the CP/CPS, please visit our website https://www.sheca.com/repository. Without further notice to specific individuals, businesses, governments or other social organizations, SHECA Security Certification Committee is responsible for the interpretation of this CP/CPS.

Note:

SHECA's electronic certification services are provided in full compliance with the laws and regulations of the People's Republic of China (PRC). For any individual, institution, or other organization that violates relevant laws and regulations, thereby affecting the operation of SHECA's electronic certification services, SHECA reserves the right to exercise all legal remedies to safeguard its legitimate rights and interests.

1.Introduction

1.1 Overview

1.1.1 SHECA Introduction

Shanghai Electronic Certification Authority Co.,Ltd. (hereinafter referred to as "SHECA") is an electronic certification service agency established in 1998, with professional management, operation and technical supporting capabilities providing users with various types of digital certificate services and takes efforts to construct a harmonious, trusted network environment. As one of the earliest professional electronic certification authorities in China, SHECA has obtained the "Electronic Authentication Service License" issued by the Ministry of Industry and Information Technology and the "License for Using Cryptography in Electronic Certification Services" issued by the State Cryptography Administration. SHECA has passed the international WebTrust certification since 2010, and has successively passed certifications such as CMMI3, ISO9001, and ISO27001.

1.1.2 Document Introduction

The "Certificate Policy and Certification Practice Statement" (CP/CPS for short) described in this document is the highest policy and practice rules for SHECA's TLS certificates. It applies to all the PKI participating entities of SHECA TLS Hierarchy. This CP/CPS clarifies how SHECA conducts electronic certification services, including service modes and processes of approving, issuing, managing, revoking and renewal certificates, as well as the corresponding service, legal and technical measures and safeguards for the participants of electronic certification activities to understand and follow.

This CP/CPS follows the framework requirements of RFC 3647, and its general provision structure conforms to the Standards for Electronic Certification Practice Statement (Trial) issued by the Ministry of Industry and Information Technology and during the formulation process, follow the requirements of laws and regulations of Electronic Signature Law of the People's Republic of China, Measures for the Administration of Electronic Certification Services, Measures for the Administration of Cipher Codes for Electronic Certification Services, etc.

This CP/CPS also complies with the latest version of Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates ("Baseline Requirements" for short) and Guidelines for the Issuance and Management of Extended Validation Certificates ("EV Guidelines" for short), Network and Certificate System Security Requirements ("NCSSR" for short) issued by CA/Browser Forum, to issue and manage public trusted TLS certificates.

SHECA will notify the CA/B Forum if a court or government body in China with jurisdiction over the activities covered by the EV Guidelines determines that the performance of any mandatory requirement is illegal. SHECA regularly checks standards updated from CA/Browser Forum and continuously revises the CP/CPS according to the published version. If this CP/CPS and the terms in the relevant standards and specifications issued by CA/Browser Forum are inconsistent, the specifications issued by CA/Browser Forum will prevail.

For root certificates already included in the browser root store, compliance with the current root program and CCADB policy shall be maintained.

1.1.3 SHECA CA Hierarchy

Currently, SHECA has the following root CAs for TLS:

1) **UCA Global G2 Root**

2) **UCA Extended Validation Root**

3) **UniTrust Global Root CA R1 (ceased)**

4) **UniTrust Global Root CA R2 (ceased)**

5) **UniTrust Global TLS RSA Root CA R1**

6) **UniTrust Global TLS ECC Root CA R2**

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

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

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

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

1.2 Document name and identification

This document is called SHECA TLS Certificate Policy and Certification Practice Statement (SHECA's CP/CPS, or this CP/CPS for short), CP is short for Certificate Policy and CPS is short for Certification Practice Statement. In this document, CP/CPS is equivalent to the name and the applicable name of the document defined in this section.

The object identifier (OID) defined by SHECA for this document is 1.2.156.112570.1.0.8.

The following is a list of OIDs defined for all types of SSL certificates by SHECA:

OID	Object
1.2.156.112570.1.1.1,2.23.140.1.2.1	Domain Validation SSL Certificates Policy
1.2.156.112570.1.1.2,2.23.140.1.2.2	Organization Validation SSL Certificates Policy
1.2.156.112570.1.1.3,2.23.140.1.1	Extended Validation SSL Certificates Policy

1.3 PKI participants

1.3.1 Certification authorities

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

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

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

Based on business requirements, SHECA builds interconnection with other CAs which is not involved in the SHECA certification system. Interconnection refers to two certification authorities that are of complete independence, and use their CPSs respectively to establish mutual trust so that mutual customers can achieve mutual authentication. When SHECA needs to build interconnection with a CA, it means that the certificate a CA issued has been trusted, SHECA will review CPS, related certificate business documents, commitment and operational procedures. If all institutions, which are trusting SHECA, are willing to accept the certificates issued by CA who has interconnection with SHECA, they must examine their own practical specification and other related certificate business documents. Interconnection does not mean that SHECA approved or offer other rights for non-SHECA agencies of independence.

1.3.2 Registration authorities

A registration authority (RA) represents a CA to establish certificate registration process, confirm the identity of certificate applicants (subscribers), approve or reject certificate applications, approve subscribers' requests for certificate revocation or directly revoke certificates and approve subscribers' certificate renewal requests.

Besides acting as a CA, SHECA also act as an RA, and no external RA will be established separately.

1.3.3 Subscribers

Subscribers refer to who have applied and attained certificates from SHECA. A subscriber usually has to sign an agreement with SHECA or RA to obtain a certificate and fulfills responsibilities as a certificate subscriber.

In digital signature applications, digital signers and certificate holders are equivalent to subscribers. The subscriber represents the unique entity bound to the public key in the SSL certificate and has ultimate control over the private key that uniquely corresponds to its certificate. The subscriber SHALL use the certificate within the scope of this CP/CPS and bears the agreed obligations of this CP/CPS.

1.3.4 Relying parties

A relying party of SHECA refers to an entity that uses and trusts the certificate issued by SHECA or its RA. A relying party may or may not be a certificate subscriber of SHECA.

Before the trust or use of a certificate, a relying party MUST verify the certificate's revocation information by querying the Certificate Revocation List (CRL) or using OCSP to query the certificate status. A relying party MUST perform reasonable check before trusting a certificate.

1.3.5 Other participants

Other participants refer to entities that provide supporting services for SHECA's digital certification. This includes, for example, agents or third-party CAs that offer cross-services to SHECA, as well as other CAs to whom SHECA provides cross-services.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

SSL certificates issued by SHECA are mainly used for identifying the identity of Website or Web server, proving the identity of Website and providing SSL encryption tunnels.

SSL certificates issued by SHECA are classified as DV SSL (Domain Validation SSL) certificates, OV SSL (Organization Validation SSL) certificates and EV SSL (Extended Validation SSL) certificates. Subscribers may decide to apply appropriate certificate types according to actual needs.

1.EV SSL Certificate

EV SSL certificate is short for Extended Validation SSL Certificate. EV SSL certificate can be used to verify control of the domain listed in the certificate and the identity of corporation who is using this certificate. All EV certificates issued by SHECA are confirmed after verification that the information contained in the certificate is true and effective and has passed appropriate and reliable identity and domain authentication procedures. EV SSL certificate can be used for encrypt network traffic between server and client, and verify the identity of the websites.

2.OV SSL Certificate

OV SSL Certificate (Organization Validation Certificate) is a standard SSL certificate that needs to verify the true identity of the website's affiliate. OV SSL certificate can be used for encrypt network traffic between server and client, and verify the identity of the websites.

3.DV SSL Certificate

DV SSL Certificate (Domain Validation SSL Certificate) is a simple SSL certificate that only verifies the control over website's domain name. DV SSL certificate only provides the encryption function of website connections.

1.4.2 Prohibited certificate uses

Certificates issued by SHECA is prohibited to be used under any circumstance in which the national laws and regulations be violated or national security be undermined, and is prohibited to be used for man-in-the-middle (MITM) or traffic management，otherwise the subscriber shall bear all the legal liability arising therefrom; meanwhile, all certificates are not designed to, intended to or authorized to be used in control equipment in

dangerous environment or for the occasion where the failure is required to avoid, such as operations of nuclear equipment, navigation or telecommunication systems of space shuttles, air transportation control systems or weapon control systems, as any failure may lead to death, personal injury or severe environmental damage.

Notice:

Publicly Trusted TLS Certificates must strictly comply with the revocation timeframe requirements specified in the TLS Baseline Requirements. Therefore, for systems involving services of **Critical Infrastructure**, if subscribers are unable to meet the revocation timeframe outlined in **Section 4.9.1.1**, the use of Publicly Trusted TLS Certificates is **NOT** recommended. It is advisable to adopt private PKI solutions.

1.5 Policy administration

1.5.1 Organization administering the document

SHECA Security Certification Committee is the administration body for all the policies under the SHECA certification system. It consists of members from management layer, directors of relevant departments (service, operational and technical departments, etc.) . It is responsible for approving CP/CPS, and implementing inspection and supervision over CP/CPS as the highest decision-making body.

SHECA Strategy Department is responsible for drafting the CP/CPS，and takes charge of internal or external consultation services in this regard.

When more than half of the approval votes are cast by the Committee members, and only when the chairman of the Committee approves the approval, the CP/CPS version may be deemed to be approved.

1.5.2 Contact person

SHECA implements strict version control over this CP/CPS and assigns specific department responsible for related issues. For any problem, suggestion or question, please contact us as follows:

Contact Person: SHECA Strategy Development Department

Tel: 86-21-36393197

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

Postal Code: 200080

Email: report@sheca.com

1.5.3 Person determining CP/CPS suitability for the policy

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

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

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

1.5.4 CP/CPS approval procedures

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

1.6 Definitions and acronyms

1.6.1 Definitions

Term	Definition
Security Policy Administration Committee	It refers to the supreme policy administration and supervision organization in the certification service system and the decisive organization for CP/CPS consistency.
Certification Authority	It refers to a certificate authentication organization, and it is also an entity that issues certificates.
Registration Authority（RA）	It refers to an entity that is responsible for handling service requests from certificate applicants and certificate subscribers, submitting requests to certification authority, and creating the registration process for end certificate applicants. It is responsible for identifying and authenticating the identity of certificate applicants,initiating or delivering certificate revocation requests as well as approving the applications for updating certificates or keys on behalf of certification authority.
Certificate Policy（CP）	A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements. For example, a specific CP can specify that a type of certificate applies to the identification of products and services within the given price range for participants involved in business-to-business transactions.
Certification Practice	One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.
Certification Path	It refers to a sequential certificate sequence (including the public key of the start object in the path), and the public key of the end object can be obtained by processing this sequence.
Policy qualifier	It refers to information that depends on the policy and may exist in X.509 certificate together with CP identifier.
Digital Certificate	It refers to a digital certificate which used as a digital signature to identify the identity of the signer and the signer recognized the signature.
E-Signature	It refers to a technical means which has functions of identifying the identity of the signer and signifying that the signer accepts the signature data.
Digital Signature	It refers to a type of e-signature which uses an asymmetric cryptographic system to encrypt or decrypt the electronic -record.
Electronic Signer	It refers to the one who holds the e-signature creation data and implements the e-signature in person or in the name of assigned representatives.
E-signature Relying Party	It refers to the one who trust e-signature certification certificates or e-signature and undertake related activities.
Private Key (E-signature creation data)	It refers to the data that is used in the process of electronic signing and reliably relates e-signature with electronic signer, such as characters, codes, etc.
Public Key (E-signature verifying data)	It refers to the data used by Subscriber to verify e-signature.
Subscriber	It refers to an entity that receives certificates from certification authority, namely certificate holder. In e-signature applications, Subscriber is the electronic signer.

Term	Definition
Relying Party	It refers to an entity which relies on the authenticity of a certificate. In e-signature applications, it also refers to an e-signature relying party. A relying party may or may not be a subscriber.

1.6.2 Acronyms

Acronym	Meaning
AICPA	American Institute of Certified Public Accountants
ADN	Authorization Domain Name
CA	Certification Authority
CAA	Certification Authority Authorization
ccTLD	Country Code Top-Level Domain
CICA	Canadian Institute of Chartered Accountants
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DBA	Doing Business As
DNS	Domain Name System
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully-Qualified Domain Name
IM	Instant Messaging
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ISO	International Organization for Standardization
NIST	(US Government) National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
RA	Registration Authority
S/MIME	Secure MIME (Multipurpose Internet Mail Extensions)
SSL	Secure Sockets Layer
TLS	Transport Layer Security
VoIP	Voice Over Internet Protocol

1.6.3 References

ETSI EN 319 403, Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers

ETSI EN 319 411-1, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements

FIPS 140-2, Federal Information Processing Standards Publication - Security Requirements For Cryptographic Modules, Information Technology Laboratory, National Institute of Standards and Technology, May 25, 2001.

FIPS 140-3, Federal Information Processing Standards Publication - Security Requirements For Cryptographic Modules, Information Technology Laboratory, National Institute of Standards and Technology, March 22, 2019.

FIPS 186-5, Federal Information Processing Standards Publication - Digital Signature Standard (DSS), Information Technology Laboratory, National Institute of Standards and Technology, February 2023.

ISO 21188:2018, Public key infrastructure for financial services – Practices and policy framework.

Network and Certificate System Security Requirements, Version 1.7, available at https://cabforum.org/network-security-requirements/

NIST SP 800-89, Recommendation for Obtaining Assurances for Digital Signature Applications, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-89.pdf.

RFC2119, Request for Comments: 2119, Key words for use in RFCs to Indicate Requirement Levels. S. Bradner. March 1997.

RFC3492, Request for Comments: 3492, Punycode: A Bootstring encoding of Unicode for Internationalized Domain Names in Applications (IDNA). A. Costello. March 2003.

RFC3647, Request for Comments: 3647, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework. S. Chokhani, et al. November 2003.

RFC3912, Request for Comments: 3912, WHOIS Protocol Specification. L. Daigle. September 2004.

RFC3986, Request for Comments: 3986, Uniform Resource Identifier (URI): Generic Syntax. T. Berners-Lee, et al. January 2005.

RFC4035, Request for Comments: 4035, Protocol Modifications for the DNS Security Extensions. R. Arends, et al. March 2005.

RFC4509, Request for Comments: 4509, Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs). W. Hardaker. May 2006.

RFC5019, Request for Comments: 5019, The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments. A. Deacon, et al. September 2007.

RFC5155, Request for Comments: 5155, DNS Security (DNSSEC) Hashed Authenticated Denial of Existence. B. Laurie, et al. March 2008.

RFC5280, Request for Comments: 5280, Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile. D. Cooper, et al. May 2008.

RFC5702, Request for Comments: 5702, Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC. J. Jansen. October 2009.

RFC5890, Request for Comments: 5890, Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework. J. Klensin. August 2010.

RFC5952, Request for Comments: 5952, A Recommendation for IPv6 Address Text Representation. S. Kawamura, et al. August 2010.

RFC6840, Request for Comments: 6840, Clarifications and Implementation Notes for DNS Security (DNSSEC). S. Weiler, et al. February 2013.

RFC6960, Request for Comments: 6960, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. S. Santesson, et al. June 2013.

RFC6962, Request for Comments: 6962, Certificate Transparency. B. Laurie, et al. June 2013.

RFC7231, Request For Comments: 7231, Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content. R. Fielding, et al. June 2014.

RFC7482, Request for Comments: 7482, Registration Data Access Protocol (RDAP) Query Format. A. Newton, et al. March 2015.

RFC7538, Request For Comments: 7538, The Hypertext Transfer Protocol Status Code 308 (Permanent Redirect). J. Reschke. April 2015.

RFC8499, Request for Comments: 8499, DNS Terminology. P. Hoffman, et al. January 2019.

RFC8659, Request for Comments: 8659, DNS Certification Authority Authorization (CAA) Resource Record. P. Hallam-Baker, et al. November 2019.

RFC8738, Request for Comments: 8738, Automated Certificate Management Environment (ACME) IP Identifier Validation Extension. R.B.Shoemaker, Ed. February 2020.

RFC8954, Request for Comments: 8954, Online Certificate Status Protocol (OCSP) Nonce Extension. M. Sahni, Ed. November 2020.

WebTrust for Certification Authorities, SSL Baseline with Network Security, available at https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/overview-of-webtrust-services/principles-and-criteria

WebTrust Principles and Criteria for Certification Authorities – SSL Baseline

X.509, Recommendation ITU-T X.509 (08/2005) | ISO/IEC 9594-8:2005, Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.

1.6.4 Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in these Requirements shall be interpreted in accordance with RFC 2119.

By convention, this document omits time and timezones when listing effective requirements such as dates. Except when explicitly specified, the associated time with a date shall be 00:00:00 UTC.

2. PUBLICATION AND REPOSITORY

2.1 Repositories

SHECA repository includes following contents: CP/CPS, Subscriber agreement, relying party agreement, Root CA certificate and all intermediate CA certificates.

2.2 Publication of certification information

SHECA's certificate services, Certification Practice Statement (CPS), Certification Policy (CP), and associated repository are accessible through multiple channels:

Website: https://www.sheca.com/repository

(Also accessible via URIs embedded within the certificates themselves)

Email: getcps@sheca.com

Mailing Address:

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

Telephone: +86-21-36393197

Fax: +86-21-36393200

As specified in Section 1.1, this CPS and the corresponding CP are structured in accordance with RFC 3647, and include all content mandated by the framework.

SHECA hosts test web pages that enable Application Software Suppliers to validate the interoperability of their software with Subscriber certificates.

2.3 Time or frequency of publication

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

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

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

SHECA MUST host test Web pages that allow Application Software Suppliers to test their software with EV Certificates that chain up to each EV Root Certificate. At a minimum, SHECA MUST host separate Web pages using certificates that are Valid, Revoked, and Expired.

ROOT	Test Web Page
UniTrust Global TLS RSA Root CA R1	hhttps://rsaev1a.good.sheca.com; https://rsaev1a.revoked.sheca.com; https://rsaev1a.expired.sheca.com
UniTrust Global TLS ECC Root CA R2	https://eccev2a.good.sheca.com; https://eccev2a.revoked.sheca.com; https://eccev2a.expired.sheca.com
UCA Global G2 Root	https://rsaovg5.good.sheca.com; https://rsaovg5.revoked.sheca.com; https://rsaovg5.expired.sheca.com
UCA Extended Validation Root	https://rsaevg3.good.sheca.com; https://rsaevg3.revoked.sheca.com; https://rsaevg3.expired.sheca.com

2.4 Access controls on repositories

The information in the SHECA repository (https://www.sheca.com/repository) is open to the public in read-only mode.

SHECA uses network security protection, system security design, and process management controls to ensure that only authorized personnel can add, delete, modify, and publish information to the repository.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

In order to distinguish from other applicants, Certification authority issues certificate in accordance with specific procedures to save the particular record of the certificate registration process, identify specific object identification. This name appeared with naming process, including the distinguished name and the unique identifiers included in certificate extension item, is able to identify a group of real-world entity.

The Subject Name of certificate generated and identified by SHECA uses the way of X.501 Distinguished Name (DN).

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

As a third party certification authority trusted who is responsible for identifying the link between the public key and the named entities. This relationship will be confirmed unequivocally through a certificate.

3.1.2 Need for names to be meaningful

SHECA ensures that both the subjectDN and issuerDN extensions of certificates include clear and meaningful identifiers. These identifiers are used to distinguish the subject and issuer. Certificates for end entities must use names that are easily understood and provide a clear indication of the subject’s identity. CA certificates adhering to this policy should clearly state the subject as a CA and specify the namespace under its authority, for example: c=country, o=Issuer Organization Name, cn=OrganizationX CA-3. Furthermore, in line with RFC 5280, the subject name of a CA certificate must correspond with the issuer name of certificates it issues.

3.1.3 Anonymity or pseudonymity of subscriber

No stipulations.

3.1.4 Rules for interpreting various name forms

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

3.1.5 Uniqueness of names

For SSL/TLS server certificates, the domain name’s uniqueness is controlled by ICANN. For internationalized domain names (IDNs), SHECA may include the Punycode version of the IDN as the subject name. The uniqueness of the subject name is enforced within the subordinate CA and the customer’s subdomain for specific certificate types. Multiple certificates can be issued to the same entity without violating the uniqueness of the name.

3.1.6 Recognition, authentication, and role of trademarks

No stipulations.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

Certificate applicants must prove possession of the private key corresponding to the public key to be registered by submitting a digitally signed PKCS#10 Certificate Signing Request (CSR) or other equivalent key identification methods approved by SHECA, with the digital signature verification ensuring that the private key created the signature and that the signed data has not been altered since its creation.

3.2.2 Authentication of Organization and Domain Identity

3.2.2.1 Organizational Identity Verification

SHECA will verify the applicant's identity and address in accordance with the latest version of the CA/Browser Forum's "TLS Baseline Requirements for Issuing and Managing Publicly Trusted Certificates" (commonly referred to as the TLS Baseline Requirements) for secure server/TLS certificates, using documents provided by or obtained through communication with at least one of the following:

1. A government agency within the applicant's legal jurisdiction, presence, or recognition;

2. A reliable and regularly updated third-party database;

3. A letter of attestation.

When using a third-party letter of attestation to verify an organization's identity, SHECA ensures the following controls:

1. The letter is issued by a trusted third party;

2. The letter includes supporting documentation for the facts being attested;

3. The authenticity of the letter is confirmed through a trusted communication method.

SHECA may use the same documents or communication methods listed above to verify the applicant's identity and address.

3.2.2.2 DBA/Tradename

SHECA does not accept DBA information as the organization information when applying for SSL certificates.

3.2.2.3 Verification of Country

For publicly-trusted TLS certificates, if the applicant requests a certificate that includes only the countryName field in the Subject Identity Information, SHECA verifies the country associated with the subject using a verification process that complies with section 3.2.2.3 of the CAB Forum Baseline Requirements.

If the applicant requests a certificate containing the countryName field along with other subject identity information, SHECA verifies the applicant's identity and the authenticity of the applicant's certificate request through a process that meets the requirements of section 3.2.2.1 of the CAB Forum Baseline Requirements. SHECA also thoroughly inspects any documents used to verify the information to detect any alterations or falsifications.

When the countryName field is present, SHECA verifies the country associated with the subject using one of the following methods:

1. IP address range assignment by country, either for:

a. The website's IP address, as indicated by the DNS record for the website, or

b. The applicant's IP address;

2. The country code top-level domain (ccTLD) of the requested domain name;

3. Information provided by the domain name registrar.

SHECA may also implement a process to screen proxy servers to ensure that the IP address is assigned to the country where the applicant is actually located, preventing reliance on IP addresses from other countries.

3.2.2.4 Validation of Domain Authorization or Control

This section defines the permitted processes and procedures for validating the Applicant’s ownership or control of the domain.

Prior to issuance, SHECA validates each Fully-Qualified Domain Name (FQDN) listed in the Certificate.

SHECA should confirm the requested domain name is not in the form of “.onion”, “in-addr.arpa” or “ip6.arpa”. Certificate issuance for a domain name in these forms is not allowed by SHECA.

Completed validations of Applicant authority may be valid for the issuance of multiple Certificates over time. In all cases, the validation must have been initiated within the time period specified in the relevant requirement (such as Section 4.2.1 of this document) prior to Certificate issuance. For purposes of domain validation, the term Applicant includes the Applicant’s Parent Company, Subsidiary Company, or Affiliate.

From March 15th, 2026, SHECA performs DNSSEC validation back to the IANA DNSSEC root trust anchor on all DNS queries associated with the validation of domain authorization or control by the Primary Network Perspective.

SHECA maintains a record of which domain validation method, including relevant BR version number, they used to validate every domain.

SHECA performs Authentication of domain name control by one of the following methods:

1. Constructed Email to Domain Contact, in accordance with BR Section 3.2.2.4.4
2. DNS Change, in accordance with BR Section 3.2.2.4.7
3. Email to DNS TXT Contact, in accordance with BR Section 3.2.2.4.14
4. Agreed - Upon Change to Website v2, in accordance with BR Section 3.2.2.4.18
5. Agreed-Upon Change to Website - ACME, in accordance with BR Section 3.2.2.4.19
6. DNS TXT Record with Persistent Value, in accordance with BR Section 3.2.2.4.22

Method 1: Constructed Email to Domain Contact
Confirming the Applicant's control over the FQDN by sending an e-mail including a Random Value created by using 'admin', 'administrator', 'webmaster', 'hostmaster' or 'postmaster' as the local part followed by the ("@") sign, followed by an Authorization Domain name, and receiving a confirming response using the Random Value, performed in accordance with BR Section 3.2.2.4.4.

The Random Value is unique to the certificate request. The Random Value remains valid for use in a confirming response for 30 days from its creation.

Method 2: DNS Change

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

The Random Value is unique to the certificate request. The Random Value remains valid for use in a confirming response for 30 days from its creation.

Under this method, SHECA MUST implement Multi-Perspective Issuance Corroboration. To count as corroborating, a Network Perspective MUST observe the same token as the Primary Network Perspective.

Wildcard should not be issued under this method.

Method 3: Email to DNS TXT Contact

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

The Random Value is unique to the certificate request. The Random Value remains valid for use in a confirming response for 30 days from its creation.

Effective March 15, 2026, this method SHOULD NOT be used to issue Subscriber Certificates.

Effective March 15, 2028: - The CA MUST NOT rely on this method. - Prior validations using this method and validation data gathered according to this method MUST NOT be used to issue Subscriber Certificates.

Method 4: Agreed - Upon Change to Website v2

Confirming the Applicant's control over the FQDN by verifying that the Request Token or Random Value is contained in the contents of a file, performed in accordance with BR Section 3.2.2.4.18;

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

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

2) SHECA MUST receive a successful HTTP response from the request .

The file containing the Request Token or Random Number:

1) is located on the Authorization Domain Name;

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

3) is retrieved via either the "http" or "https" scheme, and

4) is accessed over an Authorized Port.

The HTTP response code for redirects must be 301, 302, 307, and redirect to a resource URL with "http" or "https". The number of redirects cannot exceed five times.

The Random Value is unique to the certificate request. The Random Value remains valid for use in a confirming response for 30 days from its creation.

When performing validations using this method, SHECA MUST implement Multi-Perspective Issuance Corroboration. To count as corroborating, a Network Perspective MUST observe the same token as the Primary Network Perspective.

Wildcard should not be issued under this method.

Method 5: Agreed-Upon Change to Website - ACME

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

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

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

2) SHECA MUST receive a successful HTTP response from the request .

The file containing the Request Token or Random Number:

1) is located on the Authorization Domain Name;

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

3) is retrieved via either the "http" or "https" scheme, and

4) MUST be accessed over an Authorized Port.

The HTTP response code for redirects must be 301, 302, 307, and redirect to a resource URL with "http" or "https". The number of redirects cannot exceed five times.

The Random Value is unique to the certificate request. The Random Value remains valid for use in a confirming response for 30 days from its creation.

When performing validations using this method, SHECA MUST implement Multi-Perspective Issuance Corroboration. To count as corroborating, a Network Perspective MUST observe the same token as the Primary Network Perspective.

Wildcard should not be issued under this method.

Method 6: DNS TXT Record with Persistent Value

Confirming the Applicant's control over a FQDN by verifying the presence of a Persistent DCV TXT Record identifying the Applicant, performed in accordance with BR Section 3.2.2.4.22;

When performing validations using this method, SHECA MUST implement Multi-Perspective Issuance Corroboration. To count as corroborating, a Network Perspective MUST observe the same record as the Primary Network Perspective.

Once the FQDN has been validated using this method, SHECA MAY also issue Certificates for other FQDNs that end with all the Domain Labels of the validated FQDN.

This method is suitable for validating Wildcard Domain Names.

3.2.2.5 Validation of IP Authorization or Control

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

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

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

SHECA confirms Applicant has control over the IP address by one of the following methods:

1. Agreed-Upon Change to Website, in accordance with BR Section 3.2.2.5.1
2. Email, Fax, SMS, or Postal Mail to IP Address Contact, in accordance with BR Section 3.2.2.5.2
3. Reverse Address Lookup, in accordance with BR Section 3.2.2.5.3
4. ACME “http-01” method for IP Addresses, in accordance with BR Section 3.2.2.5.6

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

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

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

b. The CA MUST receive a successful HTTP response from the request .

The file containing the Request Token or Random Number:

a. is located on the Authorization Domain Name;

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

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

d. MUST be accessed over an Authorized Port.

e. the HTTP response code for redirects must be 301, 302, 307, and redirect to a resource URL with "http" or "https". The number of redirects cannot exceed five times.

The Random Value is unique to the certificate request. The Random Value remains valid for use in a confirming response for 30 days from its creation.

When performing validations using this method, SHECA implements Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9. To count as corroborating, a Network Perspective MUST observe the same challenge information (i.e. Random Value or Request Token) as the Primary Network Perspective.

Method 2: Email, Fax, SMS, or Postal Mail to IP Address Contact

Confirming the Applicant's control over the IP Address by sending a Random Value via email, fax, SMS, or postal mail and then receiving a confirming response utilizing the Random Value, performed in accordance with Baseline Requirements Section 3.2.2.5.2.

Each email, fax, SMS, or postal mail MAY confirm control of multiple IP Addresses.

SHECA MAY send the email, fax, SMS, or postal mail identified under this section to more than one recipient provided that every recipient is identified by the IP Address Registration Authority as representing the IP Address Contact for every IP Address being verified using the email, fax, SMS, or postal mail.

The Random Value is unique in each email, fax, SMS, or postal mail. SHECA MAY resend the email, fax, SMS, or postal mail in its entirety, including re-use of the Random Value, provided that the communication's entire contents and recipient(s) remain unchanged. The Random Value remains valid for use in a confirming response for 30 days from its creation.

Effective March 15, 2026, this method SHOULD NOT be used to issue Subscriber Certificates.

Effective March 15, 2027: - The CA MUST NOT rely on this method. - Prior validations using this method and validation data gathered according to this method MUST NOT be used to issue Subscriber Certificates.

Method 3: Reverse Address Lookup

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

When performing validations using this method, SHECA implements Multi-Perspective Issuance Corroboration. To count as corroborating, a Network Perspective MUST observe the same token as the Primary Network Perspective.

Effective March 15, 2027: - The CA MUST NOT rely on this method. - Prior validations using this method and validation data gathered according to this method MUST NOT be used to issue Subscriber Certificates.

Method 4: ACME "http-01" method for IP Addresses

Confirming the Applicant's control over the IP Address by performing the procedure documented for an "http-01" challenge in RFC 8738, performed in accordance with Baseline Requirements Section 3.2.2.5.6.

When performing validations using this method, SHECA implements Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9. To count as corroborating, a Network Perspective MUST observe the same challenge information (i.e. token) as the Primary Network Perspective.

Note: SHECA does not issue EV certificates for IP addresses.

3.2.2.6 Wildcard Domain Validation

SHECA generally considers a domain name that starts with "*", such as *.sheca.com or *.api.sheca.com, as a wildcard domain name. For wildcard domain names, SHECA verifies the ownership of their root domain. For example, both *.sheca.com and *.api.sheca.com require verification of the ownership of sheca.com. The specific verification methods are detailed in Section 3.2.2.4.1.

SHECA refuses to issue wildcard certificates for domain names in the Public Suffix List (PSL). The PSL is maintained by Mozilla, includes parts of the new generic top-level domains (gTLDs) authorized by ICANN, and is updated regularly.

SHECA does not issue EV certificates for wildcard domain names.

3.2.2.7 Data Source Accuracy

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

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

SHECA shall obtain data from authoritative third-party data providers and carry out the authentication work as described in Section 3.2.
SHECA publicly discloses the source of the authentication data on the official website. SHECA will update and disclose in this document before using any new authentication data source. Document link:

https://assets-cdn.sheca.com/documents/SHECA%20verification%20data%20source%20v4.0.docx

3.2.2.8 CAA Records

Prior to issuing a publicly trusted SSL certificate, SHECA shall check CAA records for each dNSName in the extension of the Subject Alternative Name of the certificate. SHECA will issue the certificate to subscriber within 8 hours after checking the CAA record. SHECA shall check the CAA record again if it exceeds 8 hours.

SHECA handles the property tags of "issue", "issuewild" and "iodef" in accordance with the regulations of RFC8659. If "sheca.com" are not contained in "issue" and "issuewild" tags, SHECA will not issue the corresponding certificate; When the certificate requests or issuance violate the security policy of SHECA or the FQDN holder, the tag "iodef" exists in CAA records, SHECA will not dispatch reports of such issuance requests to the contact(s) stipulated in the CAA iodef record(s).

Note: Some methods used to verify the Applicant's ownership or control of the Subject Domain Name(s) listed in the Certificate (see Section 3.2.2.4) or IP Address(es) (see Section 3.2.2.5) require retrieving and processing CAA records from additional Remote Network Perspectives (see Section 3.2.2.9) before certificate issuance. To corroborate the Primary Network Perspective, the CAA check responses from Remote Network Perspectives must be interpreted as allowing issuance, regardless of whether the responses from the two Perspectives are byte-for-byte identical. Additionally, if one or both Perspectives experience an acceptable CAA record lookup failure as defined in this Section, SHECA may treat the Remote Network Perspective's response as corroboration.

3.2.2.8.1 DNSSEC Validation of CAA Records

From 2026-03-15, SHECA performs DNSSEC validation back to the IANA DNSSEC root trust anchor on all DNS queries associated with CAA record lookups performed by the Primary Network Perspective. The DNS resolver SHECA used for all DNS queries associated with CAA record lookups performed by the Primary Network Perspective complies with BR 3.2.2.8.1.

3.2.2.9 Multi-Perspective Issuance Corroboration

SHECA uses the verification methods described in Sections 3.2.2.4 and 3.2.2.5 to perform domain authorization and control checks, as well as CAA record checks. It leverages multiple network perspectives to determine domain verification status (pass/fail) and CAA authorization status (permitted/denied), enhancing protection against BGP attacks or hijacking targeting specific prefixes.

As of November 2024, SHECA has two network verification nodes on Alibaba Cloud, located in East China (Shanghai) and North China (Hohhot). This complies with BR regulations, allowing for an exception return for one of the nodes.

SHECA has expanded its network verification nodes to six by March 2025, located in Alibaba Cloud's East China (Shanghai), Southwest China (Chengdu), North China (Hohhot), Hong Kong, the United States (Silicon Valley), and Singapore. These nodes will comply with BR regulations. East China (Shanghai) serves as the "main network perspective," while Southwest China (Chengdu), North China (Hohhot), Hong Kong, the United States (Silicon Valley), and Singapore serve as the five "remote network perspectives." These five remote perspectives are located in two different Regional Internet Registries (RIRs), ARIN and RIPE NCC.

SHECA conducts or performs vulnerability scans on its DCV verification system every three months and penetration tests one to two times a year. Within six months of a security patch release, SHECA will decide whether to install the patch at its discretion based on its impact on the system and the vulnerability threat level.

SHECA configures rules on each network boundary control (such as firewalls, switches, routers, and gateways) to allow only the services, protocols, ports, and communications required for operation. SHECA relies on the following network security measures:

1) Use mechanisms based on Secure Inter-Domain Routing (RFC 6480), such as BGP Prefix Origin Verification (RFC 6811).

2) Use other non-RPKI route leak prevention mechanisms, such as RFC 9234.

3) Adopt current best practices as described in BCP 194. While multi-perspective authentication through RPKI filtering of invalid BGP routes is recommended under normal operating conditions, this measure is not mandatory.

3.2.3 Authentication of individual identity

SHECA does not issue IV SSL certificates and does not involve personal identity verification.

3.2.4 Non-verified subscriber information

This CP/CPS only describes the verification of TLS Server Certificates. SHECA verifies all certificates according to the latest versions of "Baseline Requirements for TLS Server Certificates" and "EV Guidelines for TLS Server Certificates."

3.2.5 Validation of authority

If the Applicant for a Certificate containing Subject Identity Information is an organization, the CA SHALL use a Reliable Method of Communication to verify the authenticity of the Applicant Representative's certificate request.

The CA MAY use the sources listed in Section 3.2.2.1 to verify the Reliable Method of Communication. Provided that the CA uses a Reliable Method of Communication, the CA MAY establish the authenticity of the certificate request directly with the Applicant Representative or with an authoritative source within the Applicant's organization, such as the Applicant's main business offices, corporate offices, human resource offices, information technology offices, or other department that the CA deems appropriate.

In addition, the CA SHALL establish a process that allows an Applicant to specify the individuals who may request Certificates. If an Applicant specifies, in writing, the individuals who may request a Certificate, then the CA SHALL NOT accept any certificate requests that are outside this specification. The CA SHALL provide an Applicant with a list of its authorized certificate requesters upon the Applicant's verified written request.

3.2.6 Criteria for interoperation

SHECA can interoperate with other certification authorities and require that their CPSs shall conform to the requirements of SHECA's CP/CPS and these authorities shall sign relevant agreements with SHECA.

If national laws and regulations have requirements over the matter, SHECA will strictly abide by them.

All the cross-certification certificates are disclosed on SHECA's website.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

SHECA supports the following types of key updates:

• **Replacement**: A subscriber wishes to change some or all of the subject information in an already issued certificate and may or may not wish to replace the key associated with the new certificate.

• **Renewal**: A subscriber wishes to extend the validity period of a certificate and optionally change some or all of the subject information, potentially also replacing the associated key.

In both cases, SHECA requires the subscriber to provide the same authentication information (typically username and password) as when initially purchasing the certificate. If any subject information is changed during the replacement or renewal process, the subject must be re-authenticated.

3.3.2 Identification and authentication for re-key after revocation

SHECA will not re-key certificates when they are revoked.

3.4 Identification and authentication for revocation request

SHECA provides the following two methods to assist users in revoking certificates:

1. The subscriber submits a written request, which must include the applicant's handwritten signature and application date. SHECA will provide the subscriber with a standard template.

2. SHECA will regenerate the domain validation value and require the subscriber to configure the new validation value. Once the system detects this validation value, the revocation process will be triggered.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

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

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

1. lApplicants fill in and sign (or seal) a written application form

2. lApplicants' (individual or organization) original identification material and photocopy or digital scan (the specific requirements mentioned as individual and organization certificates requirements above).

3. lApplicants must submit a written commitment documents about the domain name (or IP address of the Internet), including the usage of domain ownership information and assurance to indicate that the domain name (or IP address) belonging to all applicants, and the certificate is legitimate used. SHECA will take appropriate way to assess applicants for the domain ownership, please refer to Section 3.2.2.4.

4. lIf it is entrusted to handle, which is required to submit an original and copy or digital scan of identification documents of an application and the trustee and a letter of attorney signed by the applicant.

4.1.1 Who can submit a certificate application

Certificate applications may be submitted by the applicant in person or through an authorized representative. Applicants are responsible for all data provided to SHECA by them or their agents. EV certificate applications must be submitted by authorized applicants, approved by the certificate approver, and accompanied by a signed (written or electronic) subscriber agreement.

SHECA maintains an internal database that records all revoked certificates and certificate applications rejected due to suspected fraud or other issues. This database contains information such as public keys, organizations, and domain names. If a user's application information matches a record in the database, SHECA's compliance department will manually verify the application. The final decision on whether to issue the certificate rests with the compliance department.

4.1.2 Enrollment process and responsibilities

The certificate registration operation complies with the guidelines issued by CA/Browser Forum through www.cabforum.org.

1. The applicant shall learn matters stipulated in subscriber agreements, the SHECA's CP/CPS, etc beforehand, especially contents related to range of application, rights, obligations and warranties of certificates.

2. The applicant shall submit relevant supporting documents to SHECA, which means that the applicant has already understood and accepted the above contents.

3. Subscribers shall generate key pairs by themselves, generate PKCS#10 certificate request file, submit to SHECA and pay any applicable fee.

4. Subscriber is responsible for providing true, complete and accurate certificate application information and materials to SHECA.

SHECA is responsible for checking the consistency between the certificate application information and identity proof documents provided by subscribers, and meanwhile, SHECA is responsible for the corresponding authentication.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

The certificate request MAY include all factual information about the Applicant to be included in the Certificate, and such additional information as is necessary for SHECA to obtain from the Applicant in order to comply with these Requirements and the CA's Certificate Policy and/or Certification Practice Statement. In cases where the certificate request does not contain all the necessary information about the Applicant, SHECA SHALL obtain the remaining information from the Applicant or, having obtained it from a reliable, independent, third-party data source, confirm it with the Applicant. SHECA SHALL establish and follow a documented procedure for verifying all data requested for inclusion in the Certificate by the Applicant.

Applicant information MUST include, but not be limited to, at least one Fully-Qualified Domain Name or IP address to be included in the Certificate's `subjectAltName` extension.

Section 6.3.2 limits the validity period of Subscriber Certificates.

SHECA MAY use the documents and data provided in Section 3.2 to verify certificate information, or may reuse previous validations themselves, provided that SHECA obtained the data or document from a source specified under Section 3.2 or completed the validation itself within the maximum number of days prior to issuing the Certificate, as defined in the following table:

Subject Identity Information validation data reuse periods		
Certificate issued on or after	**Certificate issued before**	**Maximum data reuse period**
	March 15, 2026	825 days
March 15, 2026		398 days

For validation of Domain Names and IP Addresses according to Section 3.2.2.4 and Section 3.2.2.5, any data, document, or completed validation used MUST be obtained within the maximum number of days prior to issuing the Certificate, as defined in the following table:

Domain Name and IP Address validation data reuse periods		
Certificate issued on or after	**Certificate issued before**	**Maximum data reuse period**
	March 15, 2026	398 days
March 15, 2026	March 15, 2027	200 days
March 15, 2027	March 15, 2029	100 days
March 15, 2029		10 days

In no case may a prior validation be reused if any data or document used in the prior validation was obtained more than the maximum time permitted for reuse of the data or document prior to issuing the Certificate.
After the change to any validation method specified in the Baseline Requirements or EV Guidelines, SHECA may continue to reuse validation data or documents collected prior to the change, or the validation itself, for the period stated in Section 4.2.1 unless otherwise specifically provided in a ballot.

SHECA SHALL develop, maintain, and implement documented procedures that identify and require additional verification activity for High Risk Certificate Requests prior to the Certificate's approval, as reasonably necessary to ensure that such requests are properly verified under these Requirements.

SHECA performs CAA check according to BR 3.2.2.8.

4.2.2 Approval or rejection of certificate applications

After completing the identification and authentication in Section 4.2.1 of this CP/CPS, SHECA can approve or reject the application according to the result of authentication. If an application is rejected, SHECA shall notify the certificate applicant in a proper manner within a reasonable time.

If SHECA believes that the issuance of a certificate may cause disputes, legal disputes or losses to SHECA, SHECA may also refuse the application of the certificate.

SHECA has the right to refuse to issue a certificate for an agency that is explicitly prohibited by laws and regulations, state government departments, industry regulators, or local governments from commercial activities or other public activities. In addition, if the personnel related to the certificate application are restricted by the laws and regulations, the state or local government, SHECA may not accept the certificate application that the personnel are involved.

SHECA SHALL NOT issue Certificates containing Internal Names or Reserved IP Addresses, as such names cannot be validated according to Section 3.2.2.4 or Section 3.2.2.5.

Effective 2026-03-15, SHECA SHALL NOT issue Certificates containing Domain Names that end in an IP Reverse Zone Suffix.

4.2.2.1 Approval of Certificate Applications

SHECA may approve a certificate application if:

1. according to regulations in Section 3.2 of this CP/CPS, all necessary subscriber information has been successfully identified and authenticated;

2. the subscriber accepts or does not oppose the contents or requirements of subscriber agreements;

3. the subscriber has paid the corresponding fees according to regulations.

4.2.2.2 Rejection of Certificate Applications

SHECA has the right to reject a certificate application if:

1. according to Section 3.2 of this CP/CPS, it cannot fulfil the identification and authentication of all necessary subscriber information.

2. the subscriber cannot provide necessary identity proof materials;

3. the subscriber opposes or cannot accept the relevant contents or requirements of subscriber agreements;

4. the subscriber fails to or cannot pay corresponding fees according to regulations;

5. SHECA or the RA believes that the approval of this application will bring disputes, legal disputes or losses to SHECA.

6. The information submitted by the subscriber hits the high-risk database maintained by SHECA.

Regarding rejected certificate applications, SHECA will inform the applicant of the failure of the application.

4.2.3 Time to process certificate applications

SHECA starts processing the certificate application within a reasonable time of receipt of the certificate request. In the case that the application materials submitted by the client are complete, SHECA will complete the certificate application within 7 working days.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

SHECA's root CA requires at least two trusted internal parties authorized by SHECA to issue certificates directly after a rigorous approval process.

Before issuing subscriber certificates, SHECA ensures that the authenticity of received certificate applications has been verified by the RA.

For CA certificate issuance by SHECA, the CA system operator (authorized personnel of the CA) shall manually perform certificate issuance strictly in accordance with the certificate issuance procedures, accompanied by compliance staff.

When using a CA to issue a certificate, the RA packages the certificate application information into a data package, signs and encrypts the data package, and sends it to the CA. The CA verifies the integrity of the data package by verifying the signature on the data package and identifies the sender's identity and authority based on the signer's information. Once verified, the CA signs the certificate application with its private key and generates the subscriber certificate.

SHECA does not issue end-entity certificates directly from its root certificate. Before requesting the SCT (Signed Certificate Timestamp), SHECA uses a linting tool to perform error detection on pre-certificates to prevent the issuance of certificates that violate the CA/Browser Forum baseline requirements. SHECA records SSL/TLS server certificates that are expected to be trusted in Chrome in two or more Certificate Transparency databases.

4.3.2 Notification to subscriber by the CA of issuance of certificate

After the certificate issuance system of SHECA has issued a certificate, SHECA shall notify the subscriber of the certificate issuance and provide subscribers with methods to obtain the certificate.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

An issued Certificate is delivered via email. A Subscriber is deemed to have accepted a

Certificate when:

• the Subscriber uses the Certificate, or

• 30 days pass from the date of the issuance of a Certificate

4.4.2 Publication of the certificate by the CA

SHECA publishes root certificates, subordinate certificates, and cross certificates in a repository .

SHECA issues end-entity certificates by delivering them to subscribers.

4.4.3 Notification of certificate issuance by the CA to other entities

SHECA and its RA do not notify other entities of issued certificates.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

The actions of submitting a certificate application and accepting the certificate issued by SHECA shall be deemed the subscriber has agreed to abide by the terms and conditions of rights and obligations related to SHECA and the relying parties. Key pairs and certificates shall not be used for purposes other than the prescribed and approved purposes.

Subscribers shall protect their private keys from unauthorized use and shall not use expired or revoked certificates. Parties other than subscribers are not allowed to archive the private key of subscribers.

4.5.2 Relying party public key and certificate usage

Relying parties should consider the overall circumstance and the loss risk before trusting a certificate.

After a relying party receives information loaded with a digital signature, it is obligated to perform the following verification operations:

1) obtaining the certificate and trust chain corresponding to the digital signature;

2) confirming that the certificate corresponding to the signature is a certificate trusted by the relying party;

3) confirming whether the certificate corresponding to this signature has been revoked by querying CRL or OCSP;

4) confirming the purpose of the certificate is applicable to the corresponding signature;

5) verifying the signature with the public key in the certificate.

6) considering other information in this CP/CPS or elsewhere.

If the above conditions are not satisfied, the relying party is liable to reject the signature information.

4.6 Certificate renewal

4.6.1 Circumstance for certificate renewal

SHECA can provide certificate renewal services for the same user, provided their application information remains unchanged and their private key is not leaked.

In addition, SHECA may also renew certificates to provide customer services or re-encrypt certificates. SHECA will notify subscribers of renewal requirements before the certificate expires, and additional fees may apply. To ensure the continued validity of the certificate, subscribers should renew their certificates promptly before expiration.

4.6.2 Who may request renewal

Only the certificate subject or an authorized representative of the certificate subject may request renewal of the Subscriber's Certificates.

4.6.3 Processing certificate renewal requests

The requirements and procedures for certificate renewal are generally the same as when the certificate was originally issued, but SHECA may base its renewal on previously collected information, provided that such information is still valid under applicable industry standards. If any information exceeds the validity period of the applicable standard, SHECA will update it. If SHECA is unable to verify the information that needs to be re-verified, the renewal application may be rejected.

4.6.4 Notification of new certificate issuance to subscriber

After the certificate issuance system of SHECA has issued a certificate, SHECA shall notify the subscriber of the certificate issuance and provide subscribers with methods to obtain the certificate.

4.6.5 Conduct constituting acceptance of a renewal certificate

Renewed Certificates are considered accepted 30 days after the Certificate's renewal, or earlier upon use of the Certificate when evidence exists that the Subscriber used the Certificate.

4.6.6 Publication of the renewal certificate by the CA

SHECA issues end-entity certificates by delivering them to subscribers.

4.6.7 Notification of certificate issuance by the CA to other entities

RAs may receive notification of a Certificate's renewal if the RA was involved in the issuance process.

4.7 Certificate re-key

Re-keying a Certificate consists of creating a new Certificate with a new Public Key and serial number while keeping the subject information the same.

4.7.1 Circumstance for certificate re-key

Examples of situations where a certificate needs to be rekeyed include certificate renewal, loss of the certificate's private key, or compromise of the certificate's private key.

4.7.2 Who may request certification of a new public key

Only the certificate subject or the authorized representative of the certificate subject can request to update the certificate key. After the certificate key is updated, SHECA will not revoke the original certificate by default. The subscriber can choose whether to revoke the original certificate.

4.7.3 Processing certificate re-keying requests

SHECA only accepts key update requests from certificate subjects, authorized representatives of organization certificates, or PKI initiators.

4.7.4 Notification of new certificate issuance to subscriber

After the certificate issuance system of SHECA has issued a certificate, SHECA shall notify the subscriber of the certificate issuance and provide subscribers with methods to obtain the certificate.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

Issued Certificates are considered accepted 30 days after the Certificate is rekeyed.

4.7.6 Publication of the re-keyed certificate by the CA

SHECA issues end-entity certificates by delivering them to subscribers.

4.7.7 Notification of certificate issuance by the CA to other entities

After the certificate issuance system of SHECA has issued a certificate, SHECA shall notify the subscriber of the certificate issuance and provide subscribers with methods to obtain the certificate.

4.8 Certificate modification

4.8.1 Circumstance for certificate modification

Certificate modification refers to the application for a new certificate due to change of information other than the subject information and the valid period of the existing certificate. When the certificate is modified, SHECA will re-verify certificate information and only the modified information will be authenticated if the certificate application materials are within the valid period and can be directly used.

4.8.2 Who may request certificate modification

Only the certificate subject or the authorized representative of the certificate subject can request to update the certificate key. After the certificate key is updated, SHECA will not revoke the original certificate by default. The subscriber can choose whether to revoke the original certificate.

4.8.3 Processing certificate modification requests

After receiving the modification request, SHECA will re-verify the certificate request and will issue the certificate after all information is verified.

4.8.4 Notification of new certificate issuance to subscriber

After the certificate issuance system of SHECA has issued a certificate, SHECA shall notify the subscriber of the certificate issuance and provide subscribers with methods to obtain the certificate.

4.8.5 Conduct constituting acceptance of modified certificate

Modified Certificates are considered accepted 30 days after the Certificate is modified, or earlier upon use of the Certificate when evidence exists that the Subscriber used the Certificate.

4.8.6 Publication of the modified certificate by the CA

SHECA issues end-entity certificates by delivering them to subscribers.

4.8.7 Notification of certificate issuance by the CA to other entities

After the certificate issuance system of SHECA has issued a certificate, SHECA shall notify the subscriber of the certificate issuance and provide subscribers with methods to obtain the certificate.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

4.9.1.1 Reasons for Revoking a Subscriber Certificate

SHECA will revoke the certificate within 24 hours if one or more of the following occurs:

1. The subscriber requests revocation of the certificate in writing;

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

3. SHECA obtains evidence that the subscriber’s private key corresponding to the public key in the certificate suffered a key compromise or no longer complies with the requirements in sections 6.1.5 and 6.1.6 of Baseline Requirements;

4. 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.

5. SHECA obtains evidence that the certificate was misused;

SHECA will revoke the certificate within 5 days if one or more of the following occurs:

1. SHECA is made aware that the subscriber has violated one or more of its material obligations under the subscriber agreement and CP/CPS;

2. SHECA is made aware of any circumstance indicating that use of a FQDN or IP address is no longer legally permitted .

3. SHECA is made aware that a wildcard certificate has been used to authenticate a fraudulently misleading subdomain name;

4. SHECA is made aware of a material change in the information contained in the certificate;

5. SHECA is made aware that the certificate was not issued in accordance with Baseline Requirements, or the CP/CPS;

6. SHECA believes any information in the certificate is inaccurate, untrue or misleading;

7. SHECA ceases operations for any reason and has not made agreements for another CA to provide revocation support for the certificate;

8. SHECA's right to issue certificates as per Baseline Requirements expires or is revoked or terminated, unless it continues to maintain the CRL/OCSP repository;

9. Revocation is required by the CP/CPS;

10. SHECA is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise, methods have been developed that can easily calculate it based on the Public Key (such as a Debian weak key, see http://wiki.debian.org/SSLkeys), or if there is clear evidence that the specific method used to

generate the Private Key was flawed.

11. The fulfillment of obligations in CP/CPS is delayed or impeded by force majeure; natural disasters; computer or communication failure; changes in laws and regulations; government actions; or other causes that are beyond individual control and pose a threat to information of others;

12. After SHECA has fulfilled its obligation to remind payment, the subscriber still fails to pay the fee for services;

Note:

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

SHECA shall revoke a subordinate CA certificate within 7 days if one or more of the following occurs:

1. the subordinate CA formally requests revocation of the certificate in writing;

2. the subordinate CA has found and notifies Root CA that the original certificate request is not authorized and does not retroactively grant authorization;

3. SHECA obtains evidence that the subordinate CA's private key corresponding to the public key in the certificate suffered a key compromise or no longer complies with the requirements in sections 6.1.5 and 6.1.6 of Baseline Requirements;

4. SHECA obtains evidence that the certificate was misused;

5. SHECA is made aware that the subordinate certificate was not issued in accordance with Baseline Requirements, or the subordinate certificate fails to comply with the CP/CPS;

6. SHECA believes any information in the certificate is inaccurate, untrue or misleading;

7. SHECA ceases operations for any reason and has not made agreements for another CA to provide revocation support for the certificate;

8. SHECA's right to issue certificates as per Baseline Requirements expires or is revoked or is terminated unless it continues to maintain the CRL/OCSP repository;

9. this CP/CPS requires to revoke the subordinate CA certificate.

4.9.2 Who can request revocation

The subscriber, SHECA and its RA, or judicial personnel authorized by judicial authorities can initiate revocation. In addition, relying parties, application software providers, anti-virus agencies or other third parties may submit certificate problem reports to inform SHECA of reasonable cause to revoke the certificate.

4.9.3 Procedure for revocation request

4.9.3.1 A Subscriber Makes an Application for Revocation on One's Own Initiative

the subscriber submits the revocation request to SHECA and explains reasons for revocation;

SHECA verifies the certificate revocation request based on the provisions in Section 3.4 of this CP/CPS, and carries out the revocation if the request passes the verification.

SHECA publishes the result to the certificate revocation list in time after the revocation;

SHECA notifies the subscriber of revocation of the certificate and reasons for the revocation via telephone, email or other proper means; in the case of failing to contact with the subscriber, SHECA will announce the revoked certificate through websites if necessary;

SHECA provides 7*24 hours certificate revocation application service. Subscribers can apply for revocation through the contract published in SHECA website.

4.9.3.2 A Subscriber Is Forced to Revoke a Certificate

1. when SHECA has sufficient reason to believe that circumstances that will cause the enforced revocation of subscriber certificates in Section 4.9.1.1 of this CP/CPS, SHECA will apply for the revocation of the certificate through the internal process;

2. when security risks arise from the private keys corresponding to the Root certificate or the subordinate CA certificate of SHECA, the subscriber certificate revocation can be carried out directly after approval of national digital certification service authorities;

when third parties such as relying parties, judicial organizations, application software providers, anti-virus agencies, etc. submit certificate problem reports, SHECA shall organize an investigation and determine whether to revoke the certificate according to the investigation result, if SHECA confirms that the certificate needs to be revoked through investigation, the period from receipt of the certificate problem report to the revocation of the certificate shall not exceed the period specified in 4.9.1.

3. SHECA or RA will notify the subscriber of revocation of the certificate and reasons for the revocation via telephone, email or other proper means. In case of failing to contact with the subscriber, SHECA will announce the revoked certificate through websites if necessary.

4.9.4 Revocation request grace period

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

4.9.5 Time within which CA must process the revocation request

Within 24 hours upon the receipt of a certificate problem report, SHECA shall investigate contents of the certificate problem report to decide whether to revoke the certificate or take other proper actions.

If SHECA confirms that the certificate needs to be revoked through investigation, the period from receipt of the certificate problem report to the revocation of the certificate shall not exceed the period specified in 4.9.1.

Notice:

Regardless of the scenario in which the certificate is used (including services related to critical infrastructure), SHECA DOES **NOT** accept any request of **Delayed Revocation** from any party. **Mandatory Revocation MUST** be enforced to meet the revocation timeline of Baseline Requirements.

4.9.6 Revocation checking requirement for relying parties

Relying parties shall check whether their trusted certificates are revoked through the OCSP service or CRL query provided by SHECA.

4.9.7 CRL issuance frequency

All CRL will be released by the SHECA directory server.

Within twenty-four (24) hours of issuing its first Certificate, CAs MUST generate and publish the CRL.

CAs issuing Subscriber Certificates:

1. MUST update and publish a new CRL at least every: - seven (7) days, all Certificates include an Authority Information Access extension with an id-ad-ocsp accessMethod ("AIA OCSP pointer");

2. MUST update and publish a new CRL within twenty-four (24) hours after recording a Certificate as revoked.

3. The difference of between nextUpdate and thisUpdate must be less than or equal to (7) days.

CAs issuing CA Certificates:

1. MUST update and publish a new CRL at least every twelve (12) months;

2. MUST update and publish a new CRL within twenty-four (24) hours after recording a Certificate as revoked.

3. The difference between nextUpdate and thisUpdate must be less than or equal to (10) months.

CAs MUST continue issuing CRLs until one of the following is true: - all Subordinate CA Certificates containing the same Subject Public Key are expired or revoked; OR - the corresponding Subordinate CA Private Key is destroyed.

4.9.8 Maximum latency for CRLs

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

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

4.9.9 On-line revocation/status checking availability

The validity interval of an OCSP response is the difference in time between the `thisUpdate` and `nextUpdate` field, inclusive. For purposes of computing differences, a difference of 3,600 seconds shall be equal to one hour, and a difference of 86,400 seconds shall be equal to one day, ignoring leap-seconds.

SHECA shall provide certificate subscribers and relying parties with online certificate status protocol (OCSP) services. OCSP service of SHECA meets the requirements of RFC6960.

OCSP responses MUST either:

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

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

SHECA provides OCSP services at:

http://ocsp.global.sheca.com

4.9.10 On-line revocation checking requirements

SHECA supports OCSP functionality using the GET method for certificates issued in accordance with these requirements.

1. Regarding the status of subscriber certificates:

SHECA updates the information provided via the Online Certificate Status Protocol (OCSP) in real time. The OCSP response for this service has a minimum validity period of 8 hours and a maximum validity period of 7days.

2. Regarding the status of subordinate CA certificates:

SHECA shall update the information provided via the Online Certificate Status Protocol (OCSP) at least 1) every 12 months and 2) within 24 hours of revoking a subordinate CA certificate.

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

4.9.11 Other forms of revocation advertisements available

Apart from CRL or OCSP servers for certificate revocation information query, SHECA does not provide other publication forms of revocation information.

4.9.12 Special requirements re key compromise

Any subscriber or RA who has found the security of a certificate's key is compromised shall immediately request revocation of the certificate from SHECA.

Any subscribers or relying parties could send certificate problem reports to SHECA (vetting@ptc.sheca.com), and provide evidences of key compromise in the email. Upon verification of the key compromise, SHECA will revoke all instances of that compromised key across all subscribers. If it cannot be verified that the key has indeed been compromised, SHECA will only revoke all certificates associated with that subscriber that contain that public key and will block issuance of future certificates with that key.

If the security of a CA key (root CA or subordinate CA key) is compromised or is suspected to be compromised, SHECA will inform the subscriber and relying parties timely in a proper manner within a reasonable time.

4.9.13 Circumstances for suspension

SHECA does not support certificate suspension.

4.9.14 Who can request suspension

Not applicable.

4.9.15 Procedure for suspension request

Not applicable.

4.9.16 Limits on suspension period

Not applicable.

4.10 Certificate status services

4.10.1 Operational characteristics

Regarding a revoked certificate, SHECA does not delete its revocation records from OCSP server; SHECA does not delete its revocation records from CRL until the certificate expires. SHECA's certificate status query is provided in the form of network service:

For CRL, it is provided using HTTP protocol;

For OCSP, it is provided in compliance with RFC6960, and it is provided using HTTP protocol.

4.10.2 Service availability

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

The response time is no more than 10 seconds .

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

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

4.10.3 Optional features

Not applicable.

4.11 End of subscription

End of subscription includes the following circumstances:

1. a certificate is not renewed after expiration;

2. a certificate is revoked before expiration.

Once a user terminates the use of certification service of SHECA within the valid period of the certificate, SHECA will revoke the certificate of the subscriber after approving the subscriber's termination request, and publish it in accordance with CRL publication policy; SHECA records the operation process of certificate revocation in details and regularly archives the certificates of those subscribers who end subscription and the relevant subscriber data.

4.12 Key escrow and recovery

SHECA does not hold any private key in escrow for certificate subscribers, thereby not providing key recovery service.

4.12.1 Key escrow and recovery policy and practices

Not applicable.

4.12.2 Session key encapsulation and recovery policy and practices

Not applicable

5.FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

5.1.1 Site location and construction

SHECA maintains independent operations, R\&D, and server facilities in mainland China. Physical barriers are used to isolate secure areas, and the exterior walls are constructed with solid structures to further enhance security.

All SHECA CA systems are located in a strictly protected environment, capable of preventing and detecting any unauthorized access, use, or disclosure of sensitive information. The facilities housing CA equipment and remote workstations for CA administration are equally rigorously protected as those housing high-value, sensitive information. Multiple physical security measures, including guards, robust locks, and intrusion sensors, ensure that CA equipment and records are protected from unauthorized access.

SHECA's operational and backup CA facilities utilize at least four levels of physical security. All verification operations are conducted at Tier 2 or higher, while SHECA places its required information service systems at Tier 4 or higher to ensure the strongest security.

5.1.1.1 Public Area

The entrance, office area, auxiliary and support area of SHECA's site belong to the public area, and the access control measures are used to control the entry and exit by using identification card.

5.1.1.2 Service Area

The service area is the workspace of RA operators and managers. It requires both identification card and facial identification at the same time for the access. There shall be log record for personnel's entry and exit of service area.

5.1.1.3 Management Area

The management area is the CA operation & management area, and the system monitoring room, the security monitoring room and the distribution room, etc. all belong to this area. This area requires identification card and facial identification for the access.

5.1.1.4 Core Area

The certificate certification system, the cryptographic devices and other related cryptographic facilities are stored in the area, wherein the CA server, the database system, and the cryptographic devices are located in the shielding machine room of the core area.

The core area requires identification card and facial identification for the access; it requires two trusted personnel in the shielding machine room using identification card and facial identification at the same time for the access to ensure that a single person cannot perform sensitive operations in the shielded area.

5.1.2 Physical access

SHECA's access control system in the service area, the management area and the core area can realize the entry and exit control of all areas, with the following functions:

1)The access control of each door is controlled by means of identification card and facial identification;

2)There are log records for the entry and exit of every door;

3)Doors of the service area, the management area and the core area are all equipped with forcible entry alarm and overtime alarm;

4)The whole access control system is connected to UPS, and emergency power supply is provided by UPS at the time of power interruption.

The whole area is also equipped with video surveillance system, which carries out continuous video recording of important passages inside and outside the site for 7*24 hours. All video materials should be kept for at least 12 months for queries.

5.1.3 Power and air conditioning

SHECA has a safe and reliable power supply system and an electric power reserve system to ensure the normal power supply for 7*24 hours and to provide normal services in the case of power supply interruptions in the power supply system. In addition, SHECA also has a heating /ventilation /air conditioning system to control the temperature and humidity in the operation facilities.

SHECA's machine room uses an uninterruptible power supply system UPS, which can provide power supply for at least 8 hours. Anti-static precautions are adopted in the computer room to realize the potential bonding and grounding of cabinets, servers and network equipment, etc.

The air conditioner in the computer room adopts air-cooled condenser set, and the outdoor air-cooled condenser unit is placed on the top floor. The interior design temperature of the machine room is 23 + 2 C.

5.1.4 Water exposures

The water leakage alarm system is deployed in SHECA's machine room. Once flood occurs, the system will immediately give an alarm to notify the relevant personnel to take emergency measures.

5.1.5 Fire prevention and protection

Smoke and temperature fire detectors are used in all areas of SHECA's machine room, and the automatic fire alarm system and the gas automatic fire extinguishing system have been installed. The system has two starting modes, automatic and manual operation.

In the automatic state, when the fire occurs in the protection area, the fire alarm controller sends the linkage signal immediately after receiving the two independent fire alarm signals in the protection area. After 30-second time delay, the fire alarm controls the output signal and starts the fire extinguishing system. At the same time, the alarm controller receives the feedback signal of the pressure signal device, and the door lights inside the protection area turn bright to avoid personnel straying.

When there are often people working in the protection area, the automatic state of the system can be switched to the manual state through the manual /automatic transfer switch outside the door of the protection area. In the case of ringing a fire alarm in the protection area, the alarm controller only sends out the alarm signal and does not

output the action signal. The operator on duty confirms the fire alarm, presses the control panel or breaks the emergency start button outside the protection area, and it can immediately start the system and discharge the gas extinguishing agent.

In addition, according to the relevant national requirements on fire protection, SHECA has set up emergency exits in the management area. There are fire exit doors at emergency exits, while there is no opening device outside these doors, and only from the inside can open these doors. Emergency exits have video surveillance devices for real-time monitoring. When a fire exit door is opened, the surveillance system will ring an alarm to notify personnel on duty.

5.1.6 Media storage

SHECA keeps the media storing software and data, archiving, auditing, or backup information in security facilities. These facilities are protected by appropriate physical and logical access control, allowing only the access of the authorized personnel and preventing these media from accidental compromise .

5.1.7 Waste disposal

SHECA follows industry best practices for waste disposal, ensuring all media types—such as paper documents, hardware, damaged devices, and read-only optical devices—are properly disposed of. The disposal procedures apply to all information classification levels, with the method of disposal determined by the classification.

Sensitive media and paper SHALL be destroyed according to the relevant destruction policies for such materials.

5.1.8 Off-site backup

SHECA makes off-site backups for critical system data and audit log data, and the security level of backup locations shall be no lower than the production environment.

5.2 Procedural controls

5.2.1 Trusted roles

In the process of providing certification service, roles that essentially affect key operations, such as certificate issuance, use, administration, revocation, etc. will be regarded as trusted roles by SHECA. These roles include but are not limited to:

1. Key and cryptographic devices personnel, who is responsible for the management of CA keys, certificates life-cycle and cryptographic devices;

2. Validation and customer service personnel, who is responsible for the validation of subscriber certificates, and customer support services;

3. System maintenance personnel, who is responsible for the maintenance of the hardware and software of CA system;

4. Security management personnel, who is responsible for the area security and daily physical security management;

5. Security audit personnel, who is responsible for the audit of the operations;

Human resource management personnel, who is responsible for conducting the background investigation on trusted roles and the management of personnel security.

5.2.2 Number of persons required per task

SHECA has strict control procedures for service operation process. In accordance with the policy of separation of duties specified in Section 5.2.4 in this CP/CPS, SHECA shall ensure that an individual couldn't play multiple roles, and that sensitive operations be jointly completed by multiple trusted individuals, which include:

1. The access to the electromagnetic shielding area should be dual access;

2. The safe box for saving the activation data of the root key is set to dual access ;

3. The admin privileges of the cryptographic devices shall use 3 of 5 PINs, and each share of the PINs shall be held by different trusted personnel;

4. The super admin password should be split into two segments held by different trusted personnel;

The validation requires the participation of at least 2 trusted personnel.

5.2.3 Identification and authentication for each role

Before granting access to equipment and facilities, SHECA must verify the identity and authorization of all trusted personnel. This includes:

1. Granting access to equipment and necessary facility access;

2. Granting electronic credentials to access CA systems and perform specific functions.

Authentication requires these individuals to appear in person before a trusted personnel responsible for human resources or security and present valid identification. Furthermore, their identity must be further confirmed through the background check process described in Section 5.3.

5.2.4 Roles requiring separation of duties

Roles requiring separation of duties include:

1. Individuals performing authorization functions, such as verifying information in certificate applications and approving certificate applications and revocation requests;

2. Individuals performing backup, record-keeping, and document preservation functions;

3. Individuals performing audit, review, oversight, or coordination functions;

4. Individuals performing duties related to CA/TSA key management or CA/TSA administration.

SHECA's system identifies and authenticates individuals in trusted roles and ensures that individuals do not perform multiple roles simultaneously.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

SHECA has the following qualification requirements for the personnel who play trusted roles:

1. Have good social and work backgrounds;

2. Abide by national laws and regulations with no criminal record;

3. Abide by SHECA's regulations, norms and systems related to security management;

4. Have responsible and conscientious working attitude and favourable working experience;

5. Have good team work spirit.

5.3.2 Background check procedures

In order to ensure the personnel with trusted roles to be qualified for the relevant work, SHECA will firstly conduct background investigation on employees in accordance with trusted employee requirements in SHECA Human Resource Management Policy. Background investigation conforms to the requirements of laws and regulations, verifies the background information through relevant organizations and departments as far as possible and protects individual privacy.

All trusted employees and trusted employees who apply for transfer-in shall provide written consent to the background investigation. Background investigation is divided into: basic investigation and advanced investigation.

Basic investigation includes investigations on work experience and educational background.

Advanced investigation also includes investigations on criminal records, apart from items of basic investigation.

Investigation procedures include:

1. HR department is responsible for confirming the personal materials of the applicants. The following materials shall be provided: CV, graduation certificate of highest education, diploma, qualification certificates, ID, etc.

2. HR department identifies the authenticity of the provided materials by telephone and network, etc.

3. In the background investigation, the qualification to become a trusted person can be directly rejected for those who perform any one of the following behaviours:

a. The act of fabricating facts or materials;

b. With the aid of the proof of unreliable personnel;

c. The use of illegal identity certificates, education, or qualification certificates;

d. There is a serious dishonesty at work.

4. After completing the investigation, HR department will report the results to the leaders in charge of related work for approval.

5. SHECA signs a confidentiality agreement with its employees to restrain employees from divulging all confidential and sensitive information of CA certificate service.

5.3.3 Training requirements

In order to make the relevant personnel competent for their work, SHECA has a special training program for all the personnel of the trusted roles. The training contents include:

1. CP and CPS issued by SHECA;

2. Basic knowledge of PKI;

3. SHECA's operation management system, technical system and security rules;

4. Description of job duties and posts;

5. BR and EV Guidelines compliance training.

SHECA requires all relevant personnel to pass an examination on the information verification requirements outlined in these Requirements.

5.3.4 Retraining frequency and requirements

Those who act as trusted roles or other important roles receive a training organized by SHECA at least once a year. Those who are related to the certification system operation receive relevant skill and knowledge training at least once a year. In addition, SHECA will irregularly require the personnel to continue the training according to the requirements of system upgrades and configuration modifications, etc.

5.3.5 Job rotation frequency and sequence

The job rotation frequency and sequence of SHECA's in-service personnel shall be decided according to the internal work arrangement.

5.3.6 Sanctions for unauthorized actions

SHECA has established and maintained a set of management measures to punish unauthorized actions, including rescinding or terminating labour contracts, removing from posts of duty, fines, and criticizing and educating, etc. These sanctions should comply with the requirements of laws and regulations.

5.3.7 Independent contractor requirements

SHECA doesn't hire external personnel engaged in the work related to TLS certificate life cycle or management.

5.3.8 Documentation supplied to personnel

Documentation supplied to personnel generally includes CP/CPS, employee guidelines, job description, work process and procedure specification, etc.

5.4 Audit logging procedures

5.4.1 Types of events recorded

SHECA shall record the following types of events:

CA certificate and key lifecycle events, including:

- Key generation, backup, storage, recovery, archival, and destruction; - Certificate requests, renewal, and re-key requests, and revocation; - Approval and rejection of certificate requests; - Cryptographic device life cycle management events; - Generation of Certificate Revocation Lists; - Signing of OCSP Responses (as described in Section 4.9 and Section 4.10); and - Introduction of new Certificate Profiles and retirement of existing Certificate Profiles.

Subscriber Certificate life cycle management events, including:

- Certificate requests, renewal, and re-key requests, and revocation; - All verification activities stipulated in these Requirements and the CP/CPS; - Approval and rejection of certificate requests; - Issuance of Certificates; - Generation of Certificate Revocation Lists; and - Signing of OCSP Responses (as described in Section 4.9 and Section 4.10).

Security events, including:

- Successful and unsuccessful PKI system access attempts; - PKI and security system actions performed; - Security profile changes; - Installation, update and removal of software on a Certificate System; - System crashes, hardware failures, and other anomalies; - Firewall and router activities; and - Entries to and exits from the CA facility.
These records consist of auto logs of the system and manual records of operators.

Log entries must include the following elements:

Date and time of entry;

The registered serial number or ordinal number for auto entry record;

Identity of the person making the journal entry; and

Description of the entry.

5.4.2 Frequency of processing log

SHECA checks and summarizes the system's automatic log and operators' manual records once a month.

SHECA tracks and handles the system security log once a month to check violations of policies and other major events.

5.4.3 Retention period for audit log

SHECA keeps the audit log of the CA service properly, and the audit log related to certificate requests and certificate authentication, verification, issuance and revocation shall be retained for at least 5 years after the certificate expires; other audit logs shall be kept for at least 2 years.

5.4.4 Protection of audit log

SHECA's system log is backed up in the log server, manual electronic records are backed up in SVN, and manual paper records are archived and stored in the management area.

SHECA has taken physical and logical access control methods to ensure that only the authorized personnel can approach these review records and strictly prohibit unauthorized access, reading, alteration and deletion.

5.4.5 Audit log backup procedures

SHECA's system log is backed up to the log server in real time, and to the different places daily.

5.4.6 Audit collection system

The automated audit collection process runs from system startup to system shutdown, under the control of trusted roles. If a failure or alarm in the audit collection system occurs that could adversely affect the integrity of the system or the confidentiality of the information protected by the system, SHECA's CA administrator will assess whether operations need to be suspended until the issue is resolved.

5.4.7 Notification to event-causing subject

When SHECA detects the attack, it will record the attacker's behaviors, trace the attacker to the extent permitted by the law, and retain the right to take the corresponding countermeasures. SHECA has the right to decide whether to notify subjects related to the event.

5.4.8 Vulnerability assessments

According to the requirements of CA/B Forum NCSSR, SHECA conducts vulnerability scanning work every 3 months and conducts a penetration test every year, and when there is a significant modification in the system or when receiving a request from CA/B, a vulnerability scanning or penetration test will also be conduct . According to security events found by the audit, SHECA will conduct the annual security vulnerability assessment of the system, physical sites, operation management, etc., and take measure to reduce the operational risk based on the assessment report.

5.5 Records archival

5.5.1 Types of records archived

SHECA archives the following types of records:

1. Documentation related to the security of their Certificate Systems;

2. Documentation related to their verification, issuance, and revocation of certificate requests and Certificates;

3. CP, CPS and CP/CPS;

4. Employee materials, including but not limited to materials of background investigation, employment, training, etc.; and

5. Various external and internal evaluation documents.

5.5.2 Retention period for archive

Archived audit logs (as set forth in Section 5.5.1) SHALL be retained for a period of at least two (2) years from their record creation timestamp, or as long as they are required to be retained per Section 5.4.3, whichever is longer.

5.5.3 Protection of archive

SHECA has secure physical and logical protection measures and strict management procedures for various electronic and paper filing documents, ensuring that the archived documents will not be compromised and preventing unauthorized access, alteration, deletion or other tampering behaviors.

5.5.4 Archive backup procedures

Backups of electronic archiving records generated by the system shall be made regularly and backup files shall be stored in different places; the manual electronic records shall be archived in SVN.

For written archive materials, backup is not required, yet strict measures are required to protect their security and prevent deletion, alteration, etc. of archives and their backups.

5.5.5 Requirements for time-stamping of records

SHECA automatically adds a non-encrypted system timestamp to archived records upon creation. The system time is synchronized at least every eight hours with the real-time value published by an accredited national metrology institute.

5.5.6 Archive collection system

Archive information is collected internally by SHECA.

5.5.7 Procedures to obtain and verify archive information

SHECA takes physical and logical access control methods to ensure that only the authorized personnel can approach the archive information and strictly prohibit unauthorized operations such as access, reading, alteration and deletion, etc.

5.6 Key changeover

The end time of any certificate issued by SHECA's root certificate, including CA certificate and subscriber certificate, does not exceed the end time of the root certificate, and the end time of any subscriber certificate issued by CA certificate does not exceed the end time of CA certificate.

When the lifetime of the key pair that corresponds to the CA certificate exceeds the maximum life cycle specified in this CP/CPS, SHECA will start the key renewal process and replace the already expired CA key pair. For CA key changeover, SHECA will notify subscribers and other relevant parties in advance to avoid possible disruption of the CA services.

The key changeover of SHECA is carried out in the following ways:

1. the higher CA will stop issuing a new subordinate CA certificate ("the date of stopping issuance") before the expiration time of its private key is less than the lifetime of the subordinate CA key.

2. generate a new key pair and issue a new higher CA certificate.

3. after "the date of stopping certificate issuance", a new CA key will be adopted for issuing certificates for the approved subordinate CA or subscriber certificate request.

4. the higher CA continues to use the original CA private key to issue CRL until the last certificate issued by the original private key expires

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

SHECA has developed incident response and disaster recovery plans, and documented business continuity and disaster recovery procedures designed to notify application software vendors, subscribers, and relying parties and provide reasonable protection in the event of a disaster, security breach, or business failure. SHECA can provide its business continuity and security plans upon request to external auditors. SHECA tests, reviews, and updates these procedures annually to ensure their effectiveness and adaptability.

Mass Revocation Plan

To comply with BR requirements, SHECA has also developed a comprehensive and actionable mass revocation plan specifically designed to address events that could result in mass certificate revocation. SHECA shall test its mass revocation plan at least once a year and continuously update and optimize the plan based on the test results. All lessons learned shall be incorporated into plan adjustments to enhance the ability to respond to future mass revocation events. The plan shall be regularly updated, and relevant documentation and reports be provided to external auditors as needed to ensure transparency and compliance.

This mass revocation plan includes:

Activation criteria – specific, objective, and measurable thresholds at which the mass revocation plan is triggered based on the CA's risk profile, issuance volumes, and operational capabilities;

Customer contact information – how subscriber and customer contact details are stored, maintained, and kept up to date;

Automation points – processes that are automated or could be automated, and those processes that require manual intervention;

Targets and timelines – for incident triage, revocation initiation, certificate replacement, and post-event review;

Subscriber notification methods – mechanisms for notifying impacted Subscribers;

Role assignments – roles and responsibilities of personnel responsible for initiating, coordinating, and executing the plan;

Training and education – training, awareness, and readiness activities for personnel responsible for, or supporting, the plan;

Plan testing – annual operational testing to assess readiness and demonstrate implementation feasibility, using one or more of tabletop exercises, simulations, parallel testing, or controlled test environments that DO NOT involve the revocation of active Subscriber Certificates; and

Post-test analysis and update schedule – how lessons learned from testing or live incidents are incorporated into the plan, and how often it is reviewed and updated.

SHECA's Mass Revocation Incident Preparation and Testing Plan (MRIP\&TP) can be obtained at https://www.sheca.com/repository

5.7.2 Computing resources, software, and/or data are corrupted

SHECA has backed up the resources, software and/or data of the service system and other important systems, and has developed the corresponding emergency handling process. In case of network failure, system and software compromise, database failure, etc., or a disaster caused by force majeure, SHECA will implement the recovery in accordance with the disaster recovery plan.

5.7.3 Entity private key compromise procedures

SHECA will handle the compromise of entity certificate private key in line with the following procedures:

1) When the certificate subscriber finds that the entity certificate private key is compromised, the subscriber must immediately stop using the private key and immediately visit certificate service sites of SHECA or its RA to revoke the certificate, or immediately notify SHECA or its RA to revoke the certificate by telephone, etc., and reapply for a new certificate according to the relevant process. SHECA will issue certificate revocation information according to Section 4.9 of this CP/CPS.

2) When SHECA or RA finds that the entity certificate private key of the subscriber certificate is compromised, SHECA or RA will immediately revoke the certificate and notify the certificate subscriber; the subscriber must immediately stop using the private key and reapply for a new certificate according to the relevant process. SHECA will issue certificate revocation information according to Section 4.9 of this CP/CPS.

3) When the private key of SHECA root CA or subordinate CA is compromised, SHECA will handle the emergency according to key emergency plan, and notify the relying party and application software supplier through email immediately.

5.7.4 Business continuity capabilities after a disaster

1. Business Continuity Management (BCMP)

To ensure service integrity, SHECA includes data backup and recovery as part of its Business Continuity Management Plan (BCMP). The goal of the BCMP is to minimize the impact on certificate status services and maintain or restore other services as quickly as possible in the event of a disaster at the primary facility. SHECA reviews, tests, and updates the BCMP and its supporting procedures at least annually.

2. Redundant CA System

SHECA has multiple sites, each providing certificate lifecycle management services, including application, issuance, revocation, and renewal. In addition to a fully redundant CA system, SHECA has established a mechanism for activating backup CAs and secondary sites in the event of a complete failure of the primary site. Its disaster recovery plan aims to minimize disruption to CA operations and ensure continuous service availability.

3. Disaster Recovery System

To further strengthen business continuity, SHECA has established a comprehensive disaster recovery system. This system includes primary and backup data centers, real-time data synchronization, redundant networks and power supplies, and a cross-regional backup operating environment. If the primary site encounters an unexpected disaster or system failure, the disaster recovery center can quickly take over critical operations, ensuring that core services are restored in the shortest possible time.

SHECA has also established regular drills and emergency response mechanisms. Through continuous testing and optimization, we ensure the effectiveness and feasibility of our disaster recovery plan, minimizing the risk of service interruption and ensuring business continuity and security for our customers.

5.8 CA or RA termination

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

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

2. Arrange the business to undertake.

- Save all of the operational information related to certification service, including certificates, user information, system files, CPS, norms and agreements.
- Stop the related operation services.
- Clear system root key.

When certification service agencies authorized by SHECA discontinues service for any reason, SHECA deals with related business matters and other matters in accordance with the signing agreement. Termination of service for any reason, SHECA will operate in accordance with the RA operation agreement to undertake the business matters and other matters.

6. TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

6.1.1.1 CA Key Pair Generation

SHECA uses the HSMs complying with FIPS140-2 Level 3 specifications for CA key generation, management, storage, backup and recovery.

The process of CA key pair generation is witnessed by special key managers and several reliable employees of SHECA and auditors of an independent third party, and is completed in shielding computer rooms of SHECA in accordance with SHECA Key Ceremony. SHECA Key Ceremony stipulates the process control of CA key generation and participants.

6.1.1.2 Subscriber Key Pair Generation

For publicly trusted TLS certificates, if the public key submitted in the application does not comply with the relevant specifications of Sections 6.1.5 and 6.1.6 of the applicable Baseline Requirements, SHECA will not issue the certificate. If SHECA confirms that the applicant's private key has been leaked (for example, in accordance with Section 4.9.1.1 of the applicable Baseline Requirements), or discovers that the applicant has used a known weak private key (such as Debian weak key, refer to http://wiki.debian.org/SSLkeys), or there is clear evidence that the private key generation method has a security flaw, SHECA will refuse to process the certificate application. SHECA does not generate key pairs for Subscribers.

6.1.2 Private key delivery to subscriber

SHECA does not generate keys for TLS end entity certificates.

6.1.3 Public key delivery to certificate issuer

Subscriber shall electronically submit the public key to SHECA for certificate issuing, using the file package of certificate signing request information in PKCS#10 format or other digital signature on Subscriber's own or through registration authority. When network transmission is needed, Secure Sockets Layer (SSL) and other secure protocols shall be used.

6.1.4 CA public key delivery to relying parties

The public key of SHECA is included in the root CA certificate and the subordinate CA certificate issued by SHECA. The subscriber and relying parties can download the certificates from SHECA's certificate service site.

(https://www.sheca.com/repository#certificates).

6.1.5 Key sizes

SHECA uses the keys with the following specifications：

Root CA Certificates：

digest algorithm：SHA256 and SHA384 and SHA512

RSA modulus size：4096

ECC modulus size：384

Subordinate CA Certificates：

digest algorithm：SHA256 and SHA384 and SHA512

RSA modulus size：2048 and 3072 and 4096

ECC modulus size：256 and 384 and 521

Subscriber Certificates：

digest algorithm：SHA256 and SHA384 and SHA512

RSA modulus size：2048 and 3072 and 4096

ECC modulus size：256and 384 and 521.

SHECA will adjust the algorithm type and key size according to the latest requirements of BR and the latest browser rooting rules.

6.1.6 Public key parameters generation and quality checking

Public key parameters shall be generated by using the cryptographic hardware and media complying with FIPS140-2 specifications.

Regarding the parameter quality check, since keys are generated and stored using the cryptographic hardware and media complying with FIPS140-2 specifications, the parameters have already met the requirements on high security level.

6.1.7 Key usage purposes

X.509v3 certificate issued by SHECA includes key usage extensions, and their usage conforms to RFC5280 Standard. Regarding the purposes specified by SHECA in key usage extensions of the issued certificate, the certificate Subscriber shall use the key according to specified purposes.

The root CA key is generally used to issue the following certificates and CRL:

- self-signed certificate representing the root CA;
- subordinate CA certificate and cross certificate;
- the CRL (ARL) of the root CA and the subordinate CA;
- PKI system function certificates for specific purposes (such as OCSP certificates).

The subordinate CA key is generally used to issue the following certificates and CRL:

- subscriber certificate;
- time stamping certificate;
- PKI system function certificate with specific purposes (e.g. OCSP certificate);
- subscriber CRL.

The subscriber's key can be used to provide security services, such as information encryption and signature, etc. SHECA's CA Certificates have at least two key usage bits set: keyCertSign and cRLSign, and for signing OCSP responses, the digitalSignature bit is also set.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

SHECA keys are generated using the HSMs complying with FIPS140-2 Level 3 specifications.

The process of CA key pair generation is completed by special key managers and several trusted employees of SHECA in SHECA's shielding computer room in accordance with SHECA Key Generation Regulation. SHECA Key Generation Regulation stipulates the process control of CA key generation and relevant participants.

The cryptographic modules using to generate and store subscriber key pairs comply with FIPS140-2 Level 2 or higher specifications. The subscriber should protect and keep the cryptographic module to prevent the theft, loss, compromise and unauthorized use.

6.2.2 Private key (n out of m) multi-person control

The generation, backup and recovery, etc. of all kinds of CA private keys of SHECA adopts a multi-person control mechanism. This mechanism is realized by splitting management jurisdiction of the cryptographic device through selecting three out of five, i.e. the management jurisdiction of the private key is dispersed in five different media (called secret split share, or secret split) to five trusted roles (called secret shareholders), and they save in internal safe boxes of SHECA. Only under the circumstance that at least three of them are present and permit, insert the administrator media and enter the PIN code can perform the operations of backup or recovery on the private key. The splits called secret shares is stored in the safe box in the shielding machine room when it is not used.

The activation of CA private keys of SHECA needs user jurisdiction media which have operator authority and are held by the key manager. The media are kept in the safe box in the shielding machine room until it’s used to activated CA private keys.

6.2.3 Private key escrow

SHECA neither allows escrow for the root private key or CA private key, nor provides escrow service of private key for subscribers.

6.2.4 Private key backup

SHECA backs up CA private keys in two ways: One is to generate a backup ciphertext file and backup permission recovery media according to the operating specifications provided by the cryptographic device manufacturer, and store them in a safe in a shielded computer room (or a bank safe deposit box, etc., with a security level no less than that of local backups); the other is to generate a clone device and administrator media according to the operating specifications provided by the cryptographic device manufacturer.

SHECA does not provide private key backup services for subscriber certificates. SHECA suggests subscribers to backup private keys according to their needs, and the security level of the cryptographic modules used for backup and recovery should be the same as the initial one.

6.2.5 Private key archival

When CA key pairs of SHECA go beyond the service life, these CA key pairs shall be archived and retained for at least 7 years. The archived CA key pairs are retained on the hardware cryptographic module mentioned in Section 6.2.1 of this CP/CPS.

SHECA or registration authority does not archive private keys of subscriber certificates; if subscriber's cryptographic module that retains certificate private keys allows backup of private keys, SHECA suggests subscribers to archive private keys and protect the archived private keys by adopting passwords or other access control mechanisms so as to prevent from unauthorized disclosure.

6.2.6 Private key transfer into or from a cryptographic module

All keys must be generated and stored in a certified encryption module. Private keys may only be exported to backup media under specific circumstances for HSM migration, offline storage, and redundant backup. Private keys will be encrypted when leaving the encryption module and must not be exposed in plain text. When transmitting between different encryption modules, SHECA will encrypt the private key and take measures to prevent the key used for encryption from being leaked. The encrypted private key used for backup must be stored securely and must be accessed by at least two authorized personnel. If SHECA confirms that the private key of a subordinate CA has been leaked to an unauthorized individual or unrelated entity, SHECA will immediately revoke all certificates containing the relevant public key.

6.2.7 Private key storage on cryptographic module

SHECA's private keys are stored in a FIPS 140-2 Level 3-compliant hardware cryptographic module (HSM), and all private key operations are performed within this module.

SHECA does not directly store the private keys of subscribers' SSL certificates, but recommends that users take necessary security measures to prevent unauthorized access, acquisition, or use of their private keys. Recommended measures include:

- Setting password protection for private key usage;
- Ensuring that the server and cryptographic module are located in a secure and controlled physical environment.

6.2.8 Method of activating private key

SHECA's private keys are stored on the hardware cryptographic module, and the activation is conducted by operation authority according to Section 6.2.2 of this CP/CPS. When the CA private key (in the online or offline cryptographic module) is needed for activating, the key manager in the company of Security management personnel obtains the user jurisdiction media, and then by the witness of System maintenance personnel accomplishes the activation.

Private keys of subscriber certificate that are saved on the cryptographic module can be activated and used only after the user inputs key protection information (activation data), such as password (or PIN code) or fingerprint, etc.

6.2.9 Method of deactivating private key

Regarding private keys of SHECA, when CA system sends logout instruction to the cryptographic module or when the cryptography management software sends close instruction to the cryptographic module, or when the hardware cryptographic module that stores private keys is power off, private keys enter the inactivated state.

Subscriber deactivates the activated state of private key at the Subscriber's sole discretion, and when the service program is closed, or when the system is logged off, or when the system is power off, private keys then enter the inactivated state.

6.2.10 Method of destroying private key

After the life cycle of SHECA's private key ends, SHECA will continue to keep the CA private key in a backup hardware cryptographic module and archive it, and the other CA private key backups are safely destroyed. Meanwhile, all PIN codes and media, etc. for activating the private key must be destroyed. The archived CA private key must be destroyed safely under the circumstance of several trusted persons participating after its archive period ends. The destruction of the CA private key will ensure that the CA private key is completely deleted from the hardware cryptographic module without leaving any residual information.

Regarding private keys of subscriber certificate that are out of use, private keys shall be destroyed so as to avoid loss, theft, disclosure or unauthorized use. In case of using private keys for information decryption after the expiry of these private keys or the revocation of the corresponding certificates, the end user shall properly keep private keys for a certain period of time for the convenience of decrypting the encrypted information. If there is no need to save private keys, private keys will be destroyed through deleting private keys or initializing the system or the cryptographic module.

6.2.11 Cryptographic Module Rating

See Section 6.2.1 of this CP/CPS for details.

6.3 Other aspects of key pair management

6.3.1 Public key archival

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

6.3.2 Certificate operational periods and key pair usage periods

Subscriber Certificates issued before 15 March 2026 SHOULD NOT have a Validity Period greater than 397 days and MUST NOT have a Validity Period greater than 398 days.

Subscriber Certificates issued on or after 15 March 2026 and before 15 March 2027 SHOULD NOT have a Validity Period greater than 199 days and MUST NOT have a Validity Period greater than 200 days.

Subscriber Certificates issued on or after 15 March 2027 and before 15 March 2029 SHOULD NOT have a Validity Period greater than 99 days and MUST NOT have a Validity Period greater than 100 days.

Subscriber Certificates issued on or after 15 March 2029 SHOULD NOT have a Validity Period greater than 46 days and MUST NOT have a Validity Period greater than 47 days.

Reference for maximum Validity Periods of Subscriber Certificates		
Certificate issued on or after	**Certificate issued before**	**Maximum Validity Period**
	March 15, 2026	398 days
March 15, 2026	March 15, 2027	200 days
March 15, 2027	March 15, 2029	100 days
March 15, 2029		47 days

For the purpose of calculations, a day is measured as 86,400 seconds. Any amount of time greater than this, including fractional seconds and/or leap seconds, shall represent an additional day. For this reason, Subscriber Certificates SHOULD NOT be issued for the maximum permissible time by default, in order to account for such adjustments.

6.4 Activation data

6.4.1 Activation data generation and installation

SHECA activates the encryption module that carries the CA private key according to the hardware manufacturer's specifications. This process has been evaluated for root CAs and publicly trusted issuing CAs and is compliant with the FIPS 140-2 Level 3 security standard. The use of encryption devices must be conducted by at least three authorized personnel. Furthermore, all SHECA employees and subscribers are required to use strong passwords and properly protect them in accordance with CAB Forum cybersecurity specifications and related requirements to meet best security practices.

6.4.2 Activation data protection

SHECA uses a combination of encryption and physical access control to ensure the security of the data required to unlock the private key. This security measure includes role-based physical control to ensure the security of the activation process. In addition, SHECA requires all employees to remember their passwords and strictly prohibits writing them down or sharing them with others. If an incorrect password is entered five times in a row, SHECA will automatically lock the account to prevent unauthorized access to the CA process.

6.4.3 Other aspects of activation data

Not applicable.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

The information security management of CA system formulates comprehensive security management policies and systems to be implemented, reviewed and recorded in operation according to the national standard Specifications of Cryptography and Related Security Technology for Certificate Authority System, Measures for the Administration of Electronic Certification Services published by the Ministry of Industry and Information Technology, referring to the requirements of the ISO27001 information security management system and other relevant information security standards. The main security technologies and control measures include: identity authentication and verification, logical access control, network access control, etc.

A strict dual-factor verification mechanism is implemented for every trusted person with system (including CA system, RA system) service operating authority, i.e. to use the login mode of double factors, user name, password and digital certificate at the same time.

System operation and maintenance personnel perform operations through the bastion host login system to ensure that CA software and data files are safe and reliable and will not undergo unauthorized access.

The core system must be physically separated from other systems, and the production system is logically isolated from other systems. This separation can prevent access to the network other than the specified applications. Firewall is used to prevent the invasion of the production system network from the intranet and the extranet, and restrict access to the activities of the production system. Only the trusted personnel in the CA system operation and management group who need to work and access the system can access the CA database through passwords.

6.5.2 Computer security rating

SHECA's CA system and its operating environment have been approved by the State Cryptography Administration and Ministry of Industry and Information Technology of the People's Republic of China and obtained the corresponding qualifications.

6.6 Life cycle technical controls

6.6.1 System Development Controls

The CA software of SHECA is purchased from qualified commercial CA software provider in China. SHECA controls the work of bring the certification system online by changing the internal control process, and requires the operation and maintenance personnel to strictly follow the approval and on line process execution, in order to assure the security and availability of the system:

1. The developed system must be strictly and successfully tested in the test environment before applying for the deployment in the production environment;

2. When applying for the deployment, changelog, test reports and deployment instructions, etc. should be provided;

3. The process of approval shall be execution according to the specification before deploying and going online;

4. Effective online backup shall be conducted before changing the deployment;

5. After changing the deployment, it should be tested immediately, and can provide external service only after passing the test.

SHECA has developed validation system for RA API; the software and hardware used in the development of validation system should be deployed in secure controlled environment, and the process of developing and testing should comply with the specification defined and documented by SHECA. The going online of this kind of system should also follow the internal change control process mentioned above, and then the operation and maintenance personnel shall execute the process.

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

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

6.6.2 Security Management Controls

SHECA has formulated various security policies, management regulations and processes for the safety management of the certification system.

The information security management of the certification system strictly follows the relevant operation and management regulations of the State Cryptography Administration.

The use of the certification system should have strict control measures. All systems have been strictly tested and verified for secure use, and any modification and upgrading will be recorded.

SHECA regularly performs security check on the system to identify whether the devices are being invaded, whether there are security vulnerabilities, etc.

6.6.3 Life Cycle Security Controls

SHECA controls the certification system's research and development as well as launching through the internal change control process to ensure the security and reliability of the system.

6.6.1 System development controls

The CA software of SHECA is purchased from qualified commercial CA software provider in China. SHECA controls the work of bring the certification system online by changing the internal control process, and requires the operation and maintenance personnel to strictly follow the approval and on line process execution, in order to assure the security and availability of the system:

l The developed system must be strictly and successfully tested in the test environment before applying for the deployment in the production environment;

l When applying for the deployment, changelog, test reports and deployment instructions, etc. should be provided;

l The process of approval shall be execution according to the specification before deploying and going online;

l Effective online backup shall be conducted before changing the deployment;

l After changing the deployment, it should be tested immediately, and can provide external service only after passing the test.

SHECA has developed validation system for RA API; the software and hardware used in the development of validation system should be deployed in secure controlled environment, and the process of developing and testing should comply with the specification defined and documented by SHECA. The going online of this kind of system should also follow the internal change control process mentioned above, and then the operation and maintenance personnel shall execute the process.

6.6.2 Security management controls

SHECA has formulated various security policies, management regulations and processes for the safety management of the certification system.

The information security management of the certification system strictly follows the relevant operation and management regulations of the State Cryptography Administration.

The use of the certification system should have strict control measures. All systems have been strictly tested and verified for secure use, and any modification and upgrading will be recorded.

SHECA regularly performs security check on the system to identify whether the devices are being invaded, whether there are security vulnerabilities, etc.

6.6.3 Life cycle security controls

SHECA controls the certification system's research and development as well as launching through the internal change control process to ensure the security and reliability of the system.

6.7 Network security controls

All CA and RA systems of SHECA must be protected in accordance with CA/B Forum NCSSR.

Specific security control measures include, but are not limited to:

Deploy hardware firewalls for network boundary protection;

1) Continuously monitor system operation status and security incidents;

2) Quarterly vulnerability scans, annually penetration tests, and promptly apply security patches;

3) Manage logical access rights through formal processes;

4) Implement multi-factor authentication mechanisms;

5) Review and monitor access right configurations;

6) Conduct regular security training for personnel in trusted roles.

Vulnerability Handling Timeframes

1) SHECA's vulnerability handling framework is based on risk assessments, which are grounded in documented security analyses considering principles including but not limited to:

2) Asset criticality;

3) Maintenance of asset confidentiality, integrity, and availability;

4) Regulatory requirements;

5) Likelihood and impact of vulnerability exploitation;

6) Dependencies and interdependencies;

7) Resource requirements for remediation;

8) Historical data;

9) Current threat landscape.

Vulnerability Remediation Timelines

1) Internet-facing vulnerabilities: High-risk: Remediated within 24 hours, Medium-risk: Remediated within 3 days;

2) Non-internet-facing vulnerabilities: High-risk: Remediated within 7 days, Medium-risk: Remediated within 14 days; Low-risk: Remediated timely as possible;

3) For vulnerabilities temporarily unrepairable, formulate remediation plans and security monitoring plans, and organize or urge vendors to rectify within a specified period.

4) For vulnerabilities that cannot be fixed under special circumstances, implement measures such as access control to mitigate risks.

6.8 Time-stamping

The digital certificate and CRL issued by SHECA's certification system contain time and date information, and these time and date information are digitally signed.

All system logs and operation logs should have corresponding time records. These time records do not require the use of digital timestamp technology based on cryptography. The time source of certification system is the national trusted standard time.

SHECA provides a time stamping service compliant with RFC 3161, issuing trusted time stamping tokens for the signatures on PDF documents. Our time stamping service uses a trustworthy source of time. The private key for time stamping certificate is generated and stored in HSMs complying with FIPS140-2 Level 3 specifications.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

SHECA uses the ITU X.509 version 3 standard to build its PKI digital certificates and, in accordance with ISO/IEC 9594-8:1995 Revision 1, adds specific extensions to the basic certificate structure to ensure compliance with the intended application of X.509v3. The certificate serial numbers generated by SHECA are discontinuous and are positive integers greater than zero, containing at least 64 bits of random numbers generated by a CSPRNG.

SHECA does not use SHA-1 signatures in Certificates or CRLs.

7.1.1 Version number(s)

Certificates must be of type X.509 V3, and the version information is stored in the certificate version format column.

7.1.2 Certificate extensions

SHECA asserts compliance with these Baseline Requirements, all certificates that it issues MUST comply with one of the following Certificate Profiles, which incorporate, and are derived from RFC 5280.

- CA Certificates
    - BR Section 7.1.2.1 - Root CA Certificate Profile
        - Subordinate CA Certificates
            - BR Section 7.1.2.2 - Cross-Certified Subordinate CA Certificate Profile
                - BR Section 7.1.2.6 - TLS Subordinate CA Certificate Profile
- BR Section 7.1.2.7 - Subscriber (End-Entity) Certificate Profile
- BR Section 7.1.2.8 - OCSP Responder Certificate Profile
- BR Section 7.1.2.9 - Precertificate Profile

7.1.2.1 Root CA Certificate Profile

Field	Description
`tbsCertificate`	
`version`	MUST be v3(2)
`serialNumber`	MUST be a non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG.
`signature`	See Section 7.1.3.2
`issuer`	Encoded value MUST be byte-for-byte identical to the encoded `subject`
`validity`	See Section 7.1.2.1.1
`subject`	See Section 7.1.2.10.2
`subjectPublicKeyInfo`	See Section 7.1.3.1
`issuerUniqueID`	MUST NOT be present
`subjectUniqueID`	MUST NOT be present
`extensions`	See Section 7.1.2.1.2
`signatureAlgorithm`	Encoded value MUST be byte-for-byte identical to the `tbsCertificate.signature`
`signature`	

7.1.2.1.1 Root CA Validity

Field	Minimum	Maximum
`notBefore`	One day prior to the time of signing	The time of signing
`notAfter`	2922 days (approx. 8 years)	9132 days (approx. 25 years)

Note: This restriction applies even in the event of generating a new Root CA Certificate for an existing `subject` and `subjectPublicKeyInfo` (e.g. reissuance). The new CA Certificate MUST conform to these rules.

7.1.2.1.2 Root CA Extensions

Extension	Presence	Critical	Description
`authorityKeyIdentifier`	RECOMMENDED	N	See Section 7.1.2.1.3
`basicConstraints`	MUST	Y	See Section 7.1.2.1.4
`keyUsage`	MUST	Y	See Section 7.1.2.10.7
`subjectKeyIdentifier`	MUST	N	See Section 7.1.2.11.4
`extKeyUsage`	MUST NOT	-	-
`certificatePolicies`	NOT RECOMMENDED	N	See Section 7.1.2.10.5
Signed Certificate Timestamp List	MAY	N	See Section 7.1.2.11.3
Any other extension	NOT RECOMMENDED	-	See Section 7.1.2.11.5

7.1.2.1.3 Root CA Authority Key Identifier

Field	Description
`keyIdentifier`	MUST be present. MUST be identical to the `subjectKeyIdentifier` field.
`authorityCertIssuer`	MUST NOT be present
`authorityCertSerialNumber`	MUST NOT be present

7.1.2.1.4 Root CA Basic Constraints

Field	Description
`cA`	MUST be set TRUE
`pathLenConstraint`	NOT RECOMMENDED

7.1.2.2 Cross-Certified Subordinate CA Certificate Profile

This Certificate Profile MAY be used when issuing a CA Certificate using the same Subject Name and Subject Public Key Information as one or more existing CA Certificate(s), whether a Root CA Certificate or Subordinate CA Certificate.

Before issuing a Cross-Certified Subordinate CA, the Issuing CA MUST confirm that the existing CA Certificate(s) are subject to these Baseline Requirements and were issued in compliance with the then-current version of the Baseline Requirements at time of issuance.

Field	Description
`tbsCertificate`	
`version`	MUST be v3(2)
`serialNumber`	MUST be a non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG.
`signature`	See Section 7.1.3.2
`issuer`	MUST be byte-for-byte identical to the `subject` field of the Issuing CA. See Section 7.1.4.1
`validity`	See Section 7.1.2.2.1
`subject`	See Section 7.1.2.2.2
`subjectPublicKeyInfo`	See Section 7.1.3.1
`issuerUniqueID`	MUST NOT be present
`subjectUniqueID`	MUST NOT be present
`extensions`	See Section 7.1.2.2.3
`signatureAlgorithm`	Encoded value MUST be byte-for-byte identical to the `tbsCertificate.signature`.
`signature`	

7.1.2.2.1 Cross-Certified Subordinate CA Validity

Field	Minimum	Maximum
`notBefore`	The earlier of one day prior to the time of signing or the earliest `notBefore` date of the existing CA Certificate(s)	The time of signing
`notAfter`	The time of signing	Unspecified

7.1.2.2.2 Cross-Certified Subordinate CA Naming

The `subject` MUST comply with the requirements of Section 7.1.4, or, if the existing CA Certificate was issued in compliance with the then-current version of the Baseline Requirements, the encoded `subject` name MUST be byte-for-byte identical to the encoded `subject` name of the existing CA Certificate.

Note: The above exception allows the CAs to issue Cross-Certified Subordinate CA Certificates, provided that the existing CA Certificate complied with the Baseline Requirements in force at time of issuance. This allows the requirements of Section 7.1.4 to be improved over time, while still permitting Cross-Certification. If the existing CA Certificate did not comply, issuing a Cross-Certificate is not permitted.

7.1.2.2.3 Cross-Certified Subordinate CA Extensions

Extension	Presence	Critical	Description
`authorityKeyIdentifier`	MUST	N	See Section 7.1.2.11.1
`basicConstraints`	MUST	Y	See Section 7.1.2.10.4
`certificatePolicies`	MUST	N	See Section 7.1.2.2.6
`crlDistributionPoints`	MUST	N	See Section 7.1.2.11.2
`keyUsage`	MUST	Y	See Section 7.1.2.10.7
`subjectKeyIdentifier`	MUST	N	See Section 7.1.2.11.4
`authorityInformationAccess`	SHOULD	N	See Section 7.1.2.10.3
`nameConstraints`	MAY	*[1]	See Section 7.1.2.10.8
Signed Certificate Timestamp List	MAY	N	See Section 7.1.2.11.3
Any other extension	NOT RECOMMENDED	-	See Section 7.1.2.11.5

In addition to the above, `extKeyUsage` extension requirements vary based on the relationship between the Issuer and Subject organizations represented in the Cross-Certificate.
The `extKeyUsage` extension MAY be “unrestricted” as described in the following table if:

- the `organizationName` represented in the Issuer and Subject names of the corresponding certificate are either:
  - the same, or
    - the `organizationName` represented in the Subject name is an affiliate of the `organizationName` represented in the Issuer name
- the corresponding CA represented by the Subject of the Cross-Certificate is operated by the same organization as the Issuing CA or an Affiliate of the Issuing CA organization.

Cross-Certified Subordinate CA with Unrestricted EKU			
Extension	**Presence**	**Critical**	**Description**
`extKeyUsage`	SHOULD[2]	N	See Section 7.1.2.2.4

In all other cases, the `extKeyUsage` extension MUST be "restricted" as described in the following table:

Cross-Certified Subordinate CA with Restricted EKU			
Extension	**Presence**	**Critical**	**Description**
`extKeyUsage`	MUST[3]	N	See Section 7.1.2.2.5

7.1.2.2.4 Cross-Certified Subordinate CA Extended Key Usage - Unrestricted

Unrestricted Extended Key Usage Purposes (Affiliated Cross-Certified CA)	
Key Purpose	**Description**
`anyExtendedKeyUsage`	The special extended key usage to indicate there are no restrictions applied. If present, this MUST be the only key usage present.
Any other value	CAs MUST NOT include any other key usage with the `anyExtendedKeyUsage` key usage present.

Alternatively, if the Issuing CA does not use this form, then the Extended Key Usage extension, if present, MUST be encoded as specified in Section 7.1.2.2.5.

7.1.2.2.5 Cross-Certified Subordinate CA Extended Key Usage - Restricted

Restricted TLS Cross-Certified Subordinate CA Extended Key Usage Purposes (i.e., for restricted Cross-Certified Subordinate CAs issuing TLS certificates directly or transitively).

TLS Cross-Certified Subordinate CA EKU	
Key Purpose	**Description**
`id-kp-serverAuth`	MUST be present.
`id-kp-clientAuth`	MAY be present.
`id-kp-emailProtection`	MUST NOT be present.
`id-kp-codeSigning`	MUST NOT be present.
`id-kp-timeStamping`	MUST NOT be present.
`anyExtendedKeyUsage`	MUST NOT be present.
Any other value	NOT RECOMMENDED.

Restricted Non-TLS Cross-Certified Subordinate CA Extended Key Usage Purposes (i.e., for restricted Cross-Certified Subordinate CAs not issuing TLS certificates directly or transitively).

Non-TLS Cross-Certified Subordinate CA EKU	
Key Purpose	**Description**
`id-kp-serverAuth`	MUST NOT be present.
`anyExtendedKeyUsage`	MUST NOT be present.
Any other value	MAY be present.

Each included Extended Key Usage key usage purpose:

1. MUST apply in the context of the public Internet (e.g. MUST NOT be for a service that is only valid in a privately managed network), unless:
    1. the key usage purpose falls within an OID arc for which the Applicant demonstrates ownership; or,
        1. the Applicant can otherwise demonstrate the right to assert the key usage purpose in a public context.
2. MUST NOT include semantics that will mislead the Relying Party about the certificate information verified by the CA, such as including a key usage purpose asserting storage on a smart card, where the CA is not able to verify that the corresponding Private Key is confined to such hardware due to remote issuance.
3. MUST be verified by the Issuing CA (i.e. the Issuing CA MUST verify the Cross-Certified Subordinate CA is authorized to assert the key usage purpose).

CAs MUST NOT include additional key usage purposes unless the CA is aware of a reason for including the key usage purpose in the Certificate.

7.1.2.2.6 Cross-Certified Subordinate CA Certificate Certificate Policies

The Certificate Policies extension MUST contain at least one `PolicyInformation`. Each `PolicyInformation` MUST match the following profile:

No Policy Restrictions (Affiliated CA)		
Field	**Presence**	**Contents**
`policyIdentifier`	MUST	When the Issuing CA wishes to express that there are no policy restrictions, and if the Subordinate CA is an Affiliate of the Issuing CA, then the Issuing CA MAY use the `anyPolicy` Policy Identifier, which MUST be the only `PolicyInformation` value.
`anyPolicy`	MUST	
`policyQualifiers`	NOT RECOMMENDED	If present, MUST contain only permitted `policyQualifiers` from the table below.

Policy Restricted		
Field	**Presence**	**Contents**
`policyIdentifier`	MUST	One of the following policy identifiers:
A Reserved Certificate Policy Identifier	MUST	The CA MUST include at least one Reserved Certificate Policy Identifier (see Section 7.1.6.1) associated with the given Subscriber Certificate type (see Section 7.1.2.7.1) transitively issued by this Certificate.
`anyPolicy`	MUST NOT	The `anyPolicy` Policy Identifier MUST NOT be present.
Any other identifier	MAY	If present, MUST be defined by the CA and documented by the CA in its Certificate Policy and/or Certification Practice Statement.
`policyQualifiers`	NOT RECOMMENDED	If present, MUST contain only permitted `policyQualifiers` from the table below.

This Profile RECOMMENDS that the first `PolicyInformation` value within the Certificate Policies extension contains the Reserved Certificate Policy Identifier (see 7.1.6.1)[4]. Regardless of the order of `PolicyInformation` values, the Certificate Policies extension MUST include at least one Reserved Certificate Policy Identifier. If any Subscriber Certificates will chain up directly to the Certificate issued under this Certificate Profile, this Cross-Certified Subordinate CA Certificate MUST contain exactly one Reserved Certificate Policy Identifier.
Note: `policyQualifiers` is NOT RECOMMENDED to be present in any Certificate issued under this Certificate Profile because this information increases the size of the Certificate without providing any value to a typical Relying Party, and the information may be obtained by other means when necessary.

If the `policyQualifiers` is permitted and present within a `PolicyInformation` field, it MUST be formatted as follows:

Permitted `policyQualifiers`

7.1.2.3 Technically Constrained Non-TLS Subordinate CA Certificate Profile

SHECA does not have Technically Constrained Non-TLS Subordinate CA.

7.1.2.4 Technically Constrained Precertificate Signing CA Certificate Profile

SHECA does not have Technically Constrained Precertificate Signing CA.

7.1.2.5 Technically Constrained TLS Subordinate CA Certificate Profile

SHECA does not have Technically Constrained TLS Subordinate CA.

7.1.2.6 TLS Subordinate CA Certificate Profile

Field	Description
`tbsCertificate`	
`version`	MUST be v3(2)
`serialNumber`	MUST be a non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG.
`signature`	See Section 7.1.3.2
`issuer`	MUST be byte-for-byte identical to the `subject` field of the Issuing CA. See Section 7.1.4.1
`validity`	See Section 7.1.2.10.1
`subject`	See Section 7.1.2.10.2
`subjectPublicKeyInfo`	See Section 7.1.3.1
`issuerUniqueID`	MUST NOT be present
`subjectUniqueID`	MUST NOT be present
`extensions`	See Section 7.1.2.6.1
`signatureAlgorithm`	Encoded value MUST be byte-for-byte identical to the `tbsCertificate.signature`.
`signature`	

7.1.2.6.1 TLS Subordinate CA Extensions

Extension	Presence	Critical	Description
`authorityKeyIdentifier`	MUST	N	See Section 7.1.2.11.1
`basicConstraints`	MUST	Y	See Section 7.1.2.10.4
`certificatePolicies`	MUST	N	See Section 7.1.2.10.5
`crlDistributionPoints`	MUST	N	See Section 7.1.2.11.2
`keyUsage`	MUST	Y	See Section 7.1.2.10.7
`subjectKeyIdentifier`	MUST	N	See Section 7.1.2.11.4
`extKeyUsage`	MUST[11]	N	See Section 7.1.2.10.6
`authorityInformationAccess`	SHOULD	N	See Section 7.1.2.10.3
`nameConstraints`	MAY	*[12]	See Section 7.1.2.10.8
Signed Certificate Timestamp List	MAY	N	See Section 7.1.2.11.3
Any other extension	NOT RECOMMENDED	-	See Section 7.1.2.11.5

7.1.2.7 Subscriber (Server) Certificate Profile

Field	Description
`tbsCertificate`	
`version`	MUST be v3(2)
`serialNumber`	MUST be a non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG.
`signature`	See Section 7.1.3.2
`issuer`	MUST be byte-for-byte identical to the `subject` field of the Issuing CA. See Section 7.1.4.1
`validity`	
`notBefore`	A value within 48 hours of the certificate signing operation.
`notAfter`	See Section 6.3.2
`subject`	See Section 7.1.2.7.1
`subjectPublicKeyInfo`	See Section 7.1.3.1
`issuerUniqueID`	MUST NOT be present
`subjectUniqueID`	MUST NOT be present
`extensions`	See Section 7.1.2.7.6
`signatureAlgorithm`	Encoded value MUST be byte-for-byte identical to the `tbsCertificate.signature`.
`signature`	

7.1.2.7.1 Subscriber Certificate Types

There are four types of Subscriber Certificates that may be issued, which vary based on the amount of Subject Information that is included. Each of these certificate types shares a common profile, with three exceptions: the `subject` name fields that may occur, how those fields are validated, and the contents of the `certificatePolicies` extension.

Type	Description
Domain Validated (DV)	See Section 7.1.2.7.2
Individual Validated (IV)	See Section 7.1.2.7.3
Organization Validated (OV)	See Section 7.1.2.7.4
Extended Validation (EV)	See Section 7.1.2.7.5

Note: Although each Subscriber Certificate type varies in Subject Information, all Certificates provide the same level of assurance of the device identity (domain name and/or IP address).

7.1.2.7.2 Domain Validated

For a Subscriber Certificate to be Domain Validated, it MUST meet the following profile:

Field	Requirements
`subject`	See following table.
`certificatePolicies`	MUST be present. MUST assert the Reserved Certificate Policy Identifier of `2.23.140.1.2.1` as a `policyIdentifier`. See Section 7.1.2.7.9.
All other extensions	See Section 7.1.2.7.6

All `subject` names MUST be encoded as specified in Section 7.1.4.
The following table details the acceptable `AttributeType`s that may appear within the `type` field of an `AttributeTypeAndValue`, as well as the contents permitted within the `value` field.

Domain Validated `subject` Attributes			
Attribute Name	**Presence**	**Value**	**Verification**
`countryName`	MAY	The two-letter ISO 3166-1 country code for the country associated with the Subject.	Section 3.2.2.3
`commonName`	NOT RECOMMENDED	If present, MUST contain a value derived from the `subjectAltName` extension according to Section 7.1.4.3.	
Any other attribute	MUST NOT	-	-

7.1.2.7.3 Individual Validated

For a Subscriber Certificate to be Individual Validated, it MUST meet the following profile:

Field	Requirements
`subject`	See following table.
`certificatePolicies`	MUST be present. MUST assert the Reserved Certificate Policy Identifier of `2.23.140.1.2.3` as a `policyIdentifier`. See Section 7.1.2.7.9.
All other extensions	See Section 7.1.2.7.6

All `subject` names MUST be encoded as specified in Section 7.1.4.
The following table details the acceptable `AttributeType`s that may appear within the `type` field of an `AttributeTypeAndValue`, as well as the contents permitted within the `value` field.

Individual Validated `subject` Attributes			
Attribute Name	**Presence**	**Value**	**Verification**
`countryName`	MUST	The two-letter ISO 3166-1 country code for the country associated with the Subject. If a Country is not represented by an official ISO 3166-1 country code, the CA MUST specify the ISO 3166-1 user-assigned code of `XX`, indicating that an official ISO 3166-1 alpha-2 code has not been assigned.	Section 3.2.3
`stateOrProvinceName`	MUST / MAY	MUST be present if `localityName` is absent, MAY be present otherwise. If present, MUST contain the Subject's state or province information.	Section 3.2.3
`localityName`	MUST / MAY	MUST be present if `stateOrProvinceName` is absent, MAY be present otherwise. If present, MUST contain the Subject's locality information.	Section 3.2.3
`postalCode`	NOT RECOMMENDED	If present, MUST contain the Subject's zip or postal information.	Section 3.2.3
`streetAddress`	NOT RECOMMENDED	If present, MUST contain the Subject's street address information. Multiple instances MAY be present.	Section 3.2.3
`organizationName`	NOT RECOMMENDED	If present, MUST contain the Subject's name and/or DBA/tradename. The CA MAY include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that the CA documents the difference and any abbreviations used are locally accepted abbreviations. If both are included, the DBA/tradename SHALL appear first, followed by the Subject's name in parentheses.	Section 3.2.3
`surname`	MUST	The Subject's surname.	Section 3.2.3
`givenName`	MUST	The Subject's given name.	Section 3.2.3
`organizationalUnitName`	MUST NOT	-	-
`commonName`	NOT RECOMMENDED	If present, MUST contain a value derived from the `subjectAltName` extension according to Section 7.1.4.3.	
Any other attribute	NOT RECOMMENDED	-	See Section 7.1.4.4

In addition, `subject` Attributes MUST NOT contain only metadata such as '.', '-', and ' ' (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable.

7.1.2.7.4 Organization Validated

For a Subscriber Certificate to be Organization Validated, it MUST meet the following profile:

Field	Requirements
`subject`	See following table.
`certificatePolicies`	MUST be present. MUST assert the Reserved Certificate Policy Identifier of `2.23.140.1.2.2` as a `policyIdentifier`. See Section 7.1.2.7.9.
All other extensions	See Section 7.1.2.7.6

All `subject` names MUST be encoded as specified in Section 7.1.4.
The following table details the acceptable `AttributeType`s that may appear within the `type` field of an `AttributeTypeAndValue`, as well as the contents permitted within the `value` field.

Organization Validated `subject` Attributes			
Attribute Name	**Presence**	**Value**	**Verification**
`domainComponent`	MAY	If present, this field MUST contain a Domain Label from a Domain Name. The `domainComponent` fields for the Domain Name MUST be in a single ordered sequence containing all Domain Labels from the Domain Name. The Domain Labels MUST be encoded in the reverse order to the on-wire representation of domain names in the DNS protocol, so that the Domain Label closest to the root is encoded first. Multiple instances MAY be present.	Section 3.2
`countryName`	MUST	The two-letter ISO 3166-1 country code for the country associated with the Subject. If a Country is not represented by an official ISO 3166-1 country code, the CA MUST specify the ISO 3166-1 user-assigned code of `XX`, indicating that an official ISO 3166-1 alpha-2 code has not been assigned.	Section 3.2.2.1
`stateOrProvinceName`	MUST / MAY	MUST be present if `localityName` is absent, MAY be present otherwise. If present, MUST contain the Subject's state or province information.	Section 3.2.2.1
`localityName`	MUST / MAY	MUST be present if `stateOrProvinceName` is absent, MAY be present otherwise. If present, MUST contain the Subject's locality information.	Section 3.2.2.1
`postalCode`	NOT RECOMMENDED	If present, MUST contain the Subject's zip or postal information.	Section 3.2.2.1
`streetAddress`	NOT RECOMMENDED	If present, MUST contain the Subject's street address information. Multiple instances MAY be present.	Section 3.2.2.1
`organizationName`	MUST	The Subject's name and/or DBA/tradename. The CA MAY include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that the CA documents the difference and any abbreviations used are locally accepted abbreviations; e.g. if the official record shows "Company Name Incorporated", the CA MAY use "Company Name Inc." or "Company Name". If both are included, the DBA/tradename SHALL appear first, followed by the Subject's name in parentheses.	Section 3.2.2.2
`surname`	MUST NOT	-	-
`givenName`	MUST NOT	-	-
`organizationalUnitName`	MUST NOT	-	-
`commonName`	NOT RECOMMENDED	If present, MUST contain a value derived from the `subjectAltName` extension according to Section 7.1.4.3.	
Any other attribute	NOT RECOMMENDED	-	See Section 7.1.4.4

In addition, `subject` Attributes MUST NOT contain only metadata such as '.', '-', and ' ' (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable.

7.1.2.7.5 Extended Validation

For a Subscriber Certificate to be Extended Validation, it MUST comply with the Certificate Profile specified in the then-current version of the Guidelines for the Issuance and Management of Extended Validation Certificates.

In addition, it MUST meet the following profile:

Field	Requirements
`subject`	See Guidelines for the Issuance and Management of Extended Validation Certificates, Section 7.1.4.2.
`certificatePolicies`	MUST be present. MUST assert the Reserved Certificate Policy Identifier of `2.23.140.1.1` as a `policyIdentifier`. See Section 7.1.2.7.9.
All other extensions	See Section 7.1.2.7.6 and the Guidelines for the Issuance and Management of Extended Validation Certificates.

In addition, `subject` Attributes MUST NOT contain only metadata such as '.', '-', and ' ' (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable.

7.1.2.7.6 Subscriber Certificate Extensions

Extension	Presence	Critical	Description
`authorityInformationAccess`	MUST	N	See Section 7.1.2.7.7
`authorityKeyIdentifier`	MUST	N	See Section 7.1.2.11.1
`certificatePolicies`	MUST	N	See Section 7.1.2.7.9
`extKeyUsage`	MUST	N	See Section 7.1.2.7.10
`subjectAltName`	MUST	*	See Section 7.1.2.7.12
`nameConstraints`	MUST NOT	-	-
`keyUsage`	SHOULD	Y	See Section 7.1.2.7.11
`basicConstraints`	MAY	Y	See Section 7.1.2.7.8
`crlDistributionPoints`	*	N	See Section 7.1.2.11.2
Signed Certificate Timestamp List	MAY	N	See Section 7.1.2.11.3
`subjectKeyIdentifier`	NOT RECOMMENDED	N	See Section 7.1.2.11.4
Any other extension	NOT RECOMMENDED	-	See Section 7.1.2.11.5

Notes:

- whether or not the `subjectAltName` extension should be marked Critical depends on the contents of the Certificate's `subject` field, as detailed in Section 7.1.2.7.12.
- whether or not the CRL Distribution Points extension must be present depends on 1) whether the Certificate includes an Authority Information Access extension with an `id-ad-ocsp` accessMethod and 2) the Certificate's validity period, as detailed in Section 7.1.2.11.2.

7.1.2.7.7 Subscriber Certificate Authority Information Access

The `AuthorityInfoAccessSyntax` MUST contain one or more `AccessDescription`s. Each `AccessDescription` MUST only contain a permitted `accessMethod`, as detailed below, and each `accessLocation` MUST be encoded as the specified `GeneralName` type.

The `AuthorityInfoAccessSyntax` MAY contain multiple `AccessDescription`s with the same `accessMethod`, if permitted for that `accessMethod`. When multiple `AccessDescription`s are present with the same `accessMethod`, each `accessLocation` MUST be unique, and each `AccessDescription` MUST be ordered in priority for that `accessMethod`, with the most-preferred `accessLocation` being the first `AccessDescription`. No ordering requirements are given for `AccessDescription`s that contain different `accessMethod`s, provided that previous requirement is satisfied.

Access Method	Access Location	Presence	Maximum	Description
`id-ad-ocsp` (OID: 1.3.6.1.5.5.7.48.1)	`uniformResourceIdentifier`	MAY	*	A HTTP URL of the Issuing CA's OCSP responder.
`id-ad-caIssuers` (OID: 1.3.6.1.5.5.7.48.2)	`uniformResourceIdentifier`	SHOULD	*	A HTTP URL of the Issuing CA's certificate.
Any other value	-	MUST NOT	-	No other `accessMethod`s may be used.

7.1.2.7.8 Subscriber Certificate Basic Constraints

Field	Description
`cA`	MUST be FALSE
`pathLenConstraint`	MUST NOT be present

7.1.2.7.9 Subscriber Certificate Certificate Policies

If present, the Certificate Policies extension MUST contain at least one `PolicyInformation`. Each `PolicyInformation` MUST match the following profile:

Field	Presence	Contents
`policyIdentifier`	MUST	One of the following policy identifiers:
A Reserved Certificate Policy Identifier	MUST	The Reserved Certificate Policy Identifier (see Section 7.1.6.1) associated with the given Subscriber Certificate type (see Section 7.1.2.7.1).
`anyPolicy`	MUST NOT	The `anyPolicy` Policy Identifier MUST NOT be present.
Any other identifier	MAY	If present, MUST be defined and documented in the CA's Certificate Policy and/or Certification Practice Statement.
`policyQualifiers`	NOT RECOMMENDED	If present, MUST contain only permitted `policyQualifiers` from the table below.

This Profile RECOMMENDS that the first `PolicyInformation` value within the Certificate Policies extension contains the Reserved Certificate Policy Identifier (see 7.1.6.1)[13]. Regardless of the order of `PolicyInformation` values, the Certificate Policies extension MUST contain exactly one Reserved Certificate Policy Identifier.

Permitted `policyQualifiers`			
Qualifier ID	**Presence**	**Field Type**	**Contents**
`id-qt-cps` (OID: 1.3.6.1.5.5.7.2.1)	MAY	`IA5String`	The HTTP or HTTPS URL for the Issuing CA's Certificate Policies, Certification Practice Statement, Relying Party Agreement, or other pointer to online policy information provided by the Issuing CA.
Any other qualifier	MUST NOT	-	-

7.1.2.7.10 Subscriber Certificate Extended Key Usage

Key Purpose	OID	Presence
`id-kp-serverAuth`	1.3.6.1.5.5.7.3.1	MUST
`id-kp-clientAuth`	1.3.6.1.5.5.7.3.2	MAY
`id-kp-codeSigning`	1.3.6.1.5.5.7.3.3	MUST NOT
`id-kp-emailProtection`	1.3.6.1.5.5.7.3.4	MUST NOT
`id-kp-timeStamping`	1.3.6.1.5.5.7.3.8	MUST NOT
`id-kp-OCSPSigning`	1.3.6.1.5.5.7.3.9	MUST NOT
`anyExtendedKeyUsage`	2.5.29.37.0	MUST NOT
Precertificate Signing Certificate	1.3.6.1.4.1.11129.2.4.4	MUST NOT
Any other value	-	NOT RECOMMENDED

7.1.2.7.11 Subscriber Certificate Key Usage

The acceptable Key Usage values vary based on whether the Certificate's `subjectPublicKeyInfo` identifies an RSA public key or an ECC public key. CAs MUST ensure the Key Usage is appropriate for the Certificate Public Key.

Key Usage for RSA Public Keys		
Key Usage	**Permitted**	**Required**
`digitalSignature`	Y	SHOULD
`nonRepudiation`	N	–
`keyEncipherment`	Y	MAY
`dataEncipherment`	Y	NOT RECOMMENDED
`keyAgreement`	N	–
`keyCertSign`	N	–
`cRLSign`	N	–
`encipherOnly`	N	–
`decipherOnly`	N	–

Note: At least one Key Usage MUST be set for RSA Public Keys. The `digitalSignature` bit is REQUIRED for use with modern protocols, such as TLS 1.3, and secure ciphersuites, while the `keyEncipherment` bit MAY be asserted

to support older protocols, such as TLS 1.2, when using insecure ciphersuites. Subscribers MAY wish to ensure key separation to limit the risk from such legacy protocols, and thus a CA MAY issue a Subscriber certificate that only asserts the `keyEncipherment` bit. For most Subscribers, the `digitalSignature` bit is sufficient, while Subscribers that want to mix insecure and secure ciphersuites with the same algorithm may choose to assert both `digitalSignature` and `keyEncipherment` within the same certificate, although this is NOT RECOMMENDED. The `dataEncipherment` bit is currently permitted, although setting it is NOT RECOMMENDED, as it is a Pending Prohibition (https://github.com/cabforum/servercert/issues/384).

Key Usage for ECC Public Keys		
Key Usage	**Permitted**	**Required**
`digitalSignature`	Y	MUST
`nonRepudiation`	N	–
`keyEncipherment`	N	–
`dataEncipherment`	N	–
`keyAgreement`	Y	NOT RECOMMENDED
`keyCertSign`	N	–
`cRLSign`	N	–
`encipherOnly`	N	–
`decipherOnly`	N	–

Note: The `keyAgreement` bit is currently permitted, although setting it is NOT RECOMMENDED, as it is a Pending Prohibition (https://github.com/cabforum/servercert/issues/384).

7.1.2.7.12 Subscriber Certificate Subject Alternative Name

For Subscriber Certificates, the Subject Alternative Name MUST be present and MUST contain at least one `dNSName` or `iPAddress` `GeneralName`. See below for further requirements about the permitted fields and their validation requirements.

If the `subject` field of the certificate is an empty SEQUENCE, this extension MUST be marked critical, as specified in RFC 5280, Section 4.2.1.6. Otherwise, this extension MUST NOT be marked critical.

`GeneralName` within a `subjectAltName` extension		
Name Type	**Permitted**	**Validation**
`otherName`	N	-
`rfc822Name`	N	-
`dNSName`	Y	The entry MUST contain either a Fully-Qualified Domain Name or Wildcard Domain Name that the CA has validated in accordance with Section 3.2.2.4. Wildcard Domain Names MUST be validated for consistency with Section 3.2.2.6. The entry MUST NOT contain an Internal Name. Effective 2026-03-15, the entry MUST NOT contain a Domain Name that ends in an IP Address Reverse Zone Suffix. The Fully-Qualified Domain Name or the FQDN portion of the Wildcard Domain Name contained in the entry MUST be composed entirely of P-Labels or Non-Reserved LDH Labels joined together by a U+002E FULL STOP (“.”) character. The zero-length Domain Label representing the root zone of the Internet Domain Name System MUST NOT be included (e.g. “example.com” MUST be encoded as “example.com” and MUST NOT be encoded as “example.com.”).
`x400Address`	N	-
`directoryName`	N	-
`ediPartyName`	N	-
`uniformResourceIdentifier`	N	-
`iPAddress`	Y	The entry MUST contain the IPv4 or IPv6 address that the CA has confirmed the Applicant controls or has been granted the right to use through a method specified in Section 3.2.2.5. The entry MUST NOT contain a Reserved IP Address.
`registeredID`	N	-

Note: As an explicit exception from RFC 5280, P-Labels are permitted to not conform to IDNA 2003. These Requirements allow for the inclusion of P-Labels that do not conform with IDNA 2003 to support newer versions of the Unicode character repertoire, among other improvements to the various IDNA standards.

7.1.2.8 OCSP Responder Certificate Profile

If the Issuing CA does not directly sign OCSP responses, it MAY make use of an OCSP Authorized Responder, as defined by RFC 6960, Section 4.2.2.2. The Issuing CA of the Responder MUST be the same as the Issuing CA for the Certificates it provides responses for.

Field	Description
`tbsCertificate`	
`version`	MUST be v3(2)
`serialNumber`	MUST be a non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG.
`signature`	See Section 7.1.3.2
`issuer`	MUST be byte-for-byte identical to the `subject` field of the Issuing CA. See Section 7.1.4.1
`validity`	See Section 7.1.2.8.1
`subject`	See Section 7.1.2.10.2
`subjectPublicKeyInfo`	See Section 7.1.3.1
`issuerUniqueID`	MUST NOT be present
`subjectUniqueID`	MUST NOT be present
`extensions`	See Section 7.1.2.8.2
`signatureAlgorithm`	Encoded value MUST be byte-for-byte identical to the `tbsCertificate.signature`.
`signature`	

7.1.2.8.1 OCSP Responder Validity

Field	Minimum	Maximum
`notBefore`	One day prior to the time of signing	The time of signing
`notAfter`	The time of signing	Unspecified

7.1.2.8.2 OCSP Responder Extensions

Extension	Presence	Critical	Description
`authorityKeyIdentifier`	MUST	N	See Section 7.1.2.11.1
`extKeyUsage`	MUST	-	See Section 7.1.2.8.5
`id-pkix-ocsp-nocheck`	MUST	N	See Section 7.1.2.8.6
`keyUsage`	MUST	Y	See Section 7.1.2.8.7
`basicConstraints`	MAY	Y	See Section 7.1.2.8.4
`nameConstraints`	MUST NOT	-	-
`subjectAltName`	MUST NOT	-	-
`subjectKeyIdentifier`	SHOULD	N	See Section 7.1.2.11.4
`authorityInformationAccess`	NOT RECOMMENDED	N	See Section 7.1.2.8.3
`certificatePolicies`	SHOULD NOT	N	See Section 7.1.2.8.8
`crlDistributionPoints`	MUST NOT	N	See Section 7.1.2.11.2
Signed Certificate Timestamp List	MAY	N	See Section 7.1.2.11.3
Any other extension	NOT RECOMMENDED	-	See Section 7.1.2.11.5

7.1.2.8.3 OCSP Responder Authority Information Access

For OCSP Responder certificates, this extension is NOT RECOMMENDED, as the Relying Party should already possess the necessary information. In order to validate the given Responder certificate, the Relying Party must have access to the Issuing CA's certificate, eliminating the need to provide `id-ad-caIssuers`. Similarly, because of the requirement for an OCSP Responder certificate to include the `id-pkix-ocsp-nocheck` extension, it is not necessary to provide `id-ad-ocsp`, as such responses will not be checked by Relying Parties.

If present, the `AuthorityInfoAccessSyntax` MUST contain one or more `AccessDescription`s. Each `AccessDescription` MUST only contain a permitted `accessMethod`, as detailed below, and each `AuthorityInfoAccessSyntax` MUST contain all required `AccessDescription`s.

Access Method	Access Location	Presence	Maximum	Description
`id-ad-ocsp` (OID: 1.3.6.1.5.5.7.48.1)	`uniformResourceIdentifier`	NOT RECOMMENDED	*	A HTTP URL of the Issuing CA's OCSP responder.
Any other value	-	MUST NOT	-	No other `accessMethod`s may be used.

7.1.2.8.4 OCSP Responder Basic Constraints

OCSP Responder certificates MUST NOT be CA certificates. The issuing CA may indicate this one of two ways: by omission of the `basicConstraints` extension, or through the inclusion of a `basicConstraints` extension that sets the `cA` boolean to FALSE.

Field	Description
`cA`	MUST be FALSE
`pathLenConstraint`	MUST NOT be present

Note: Due to DER encoding rules regarding the encoding of DEFAULT values within OPTIONAL fields, a `basicConstraints` extension that sets the `cA` boolean to FALSE MUST have an `extnValue` `OCTET STRING` which is exactly the hex-encoded bytes `3000`, the encoded representation of an empty ASN.1 `SEQUENCE` value.

7.1.2.8.5 OCSP Responder Extended Key Usage

Key Purpose	OID	Presence
`id-kp-OCSPSigning`	1.3.6.1.5.5.7.3.9	MUST
Any other value	-	MUST NOT

7.1.2.8.6 OCSP Responder id-pkix-ocsp-nocheck

The CA MUST include the `id-pkix-ocsp-nocheck` extension (OID: 1.3.6.1.5.5.7.48.1.5).

This extension MUST have an `extnValue` `OCTET STRING` which is exactly the hex-encoded bytes `0500`, the encoded representation of the ASN.1 NULL value, as specified in RFC 6960, Section 4.2.2.2.1.

7.1.2.8.7 OCSP Responder Key Usage

Key Usage	Permitted	Required
`digitalSignature`	Y	Y
`nonRepudiation`	N	–
`keyEncipherment`	N	–
`dataEncipherment`	N	–
`keyAgreement`	N	–
`keyCertSign`	N	–
`cRLSign`	N	–
`encipherOnly`	N	–
`decipherOnly`	N	–

7.1.2.8.8 OCSP Responder Certificate Policies

If present, the Certificate Policies extension MUST contain at least one `PolicyInformation`. Each `PolicyInformation` MUST match the following profile:

Permitted `policyQualifiers`		
Field	**Presence**	**Contents**
`policyIdentifier`	MUST	One of the following policy identifiers:
A Reserved Certificate Policy Identifier	NOT RECOMMENDED	
`anyPolicy`	NOT RECOMMENDED	
Any other identifier	NOT RECOMMENDED	If present, MUST be defined by the CA and documented by the CA in its Certificate Policy and/or Certification Practice Statement.
`policyQualifiers`	NOT RECOMMENDED	If present, MUST contain only permitted `policyQualifiers` from the table below.

Qualifier ID	Presence	Field Type	Contents
`id-qt-cps` (OID: 1.3.6.1.5.5.7.2.1)	MAY	`IA5String`	The HTTP or HTTPS URL for the Issuing CA's Certificate Policies, Certification Practice Statement, Relying Party Agreement, or other pointer to online policy information provided by the Issuing CA.
Any other qualifier	MUST NOT	-	-

Note: Because the Certificate Policies extension may be used to restrict the applicable usages for a Certificate, incorrect policies may result in OCSP Responder Certificates that fail to successfully validate, resulting in invalid OCSP Responses. Including the `anyPolicy` policy can reduce this risk, but add to client processing complexity and interoperability issues.

7.1.2.9 Precertificate Profile

A Precertificate is a signed data structure that can be submitted to a Certificate Transparency log, as defined by RFC 6962. A Precertificate appears structurally identical to a Certificate, with the exception of a special critical poison extension in the `extensions` field, with the OID of 1.3.6.1.4.1.11129.2.4.3. This extension ensures that the Precertificate will not be accepted as a Certificate by clients conforming to RFC 5280. The existence of a signed Precertificate can be treated as evidence of a corresponding Certificate also existing, as the signature represents a binding commitment by the CA that it may issue such a Certificate.

A Precertificate is created after a CA has decided to issue a Certificate, but prior to the actual signing of the Certificate. The CA MAY construct and sign a Precertificate corresponding to the Certificate, for purposes of submitting to Certificate Transparency Logs. The CA MAY use the returned Signed Certificate Timestamps to then alter the Certificate's `extensions` field, adding a Signed Certificate Timestamp List, as defined in Section 7.1.2.11.3 and as permitted by the relevant profile, prior to signing the Certificate.

Once a Precertificate is signed, relying parties are permitted to treat this as a binding commitment from the CA of the intent to issue a corresponding Certificate, or more commonly, that a corresponding Certificate exists. A Certificate is said to be corresponding to a Precertificate based upon the value of the `tbsCertificate` contents, as transformed by the process defined in RFC 6962, Section 3.2.

This profile describes the transformations that are permitted to a Certificate to construct a Precertificate. CAs MUST NOT issue a Precertificate unless they are willing to issue a corresponding Certificate, regardless of whether they have done so. Similarly, a CA MUST NOT issue a Precertificate unless the corresponding Certificate conforms

to these Baseline Requirements, regardless of whether the CA signs the corresponding Certificate.

A Precertificate may be issued either directly by the Issuing CA or, when issued prior to 2026-03-15, by a Technically Constrained Precertificate Signing CA, as defined in Section 7.1.2.4. If issued by a Precertificate Signing CA, then in addition to the precertificate poison and signed certificate timestamp list extensions, the Precertificate issuer field and, if present, `authorityKeyIdentifier` extension, may differ from the Certificate, as described below.

When the Precertificate is issued directly by the Issuing CA	
Field	**Description**
`tbsCertificate`	
`version`	Encoded value MUST be byte-for-byte identical to the `version` field of the Certificate
`serialNumber`	Encoded value MUST be byte-for-byte identical to the `serialNumber` field of the Certificate
`signature`	Encoded value MUST be byte-for-byte identical to the `signature` field of the Certificate
`issuer`	Encoded value MUST be byte-for-byte identical to the `issuer` field of the Certificate
`validity`	Encoded value MUST be byte-for-byte identical to the `validity` field of the Certificate
`subject`	Encoded value MUST be byte-for-byte identical to the `subject` field of the Certificate
`subjectPublicKeyInfo`	Encoded value MUST be byte-for-byte identical to the `subjectPublicKeyInfo` field of the Certificate
`issuerUniqueID`	Encoded value MUST be byte-for-byte identical to the `issuerUniqueID` field of the Certificate, or omitted if omitted in the Certificate
`subjectUniqueID`	Encoded value MUST be byte-for-byte identical to the `subjectUniqueID` field of the Certificate, or omitted if omitted in the Certificate
`extensions`	See Section 7.1.2.9.1
`signatureAlgorithm`	Encoded value MUST be byte-for-byte identical to the `tbsCertificate.signature`.
`signature`	

When the Precertificate is issued by a Precertificate Signing CA on behalf of an Issuing CA	
Field	**Description**
`tbsCertificate`	
`version`	Encoded value MUST be byte-for-byte identical to the `version` field of the Certificate
`serialNumber`	Encoded value MUST be byte-for-byte identical to the `serialNumber` field of the Certificate
`signature`	Encoded value MUST be byte-for-byte identical to the `signature` field of the Certificate
`issuer`	Encoded value MUST be byte-for-byte identical to the `subject` field of the Precertificate Signing CA Certificate
`validity`	Encoded value MUST be byte-for-byte identical to the `validity` field of the Certificate
`subject`	Encoded value MUST be byte-for-byte identical to the `subject` field of the Certificate
`subjectPublicKeyInfo`	Encoded value MUST be byte-for-byte identical to the `subjectPublicKeyInfo` field of the Certificate
`issuerUniqueID`	Encoded value MUST be byte-for-byte identical to the `issuerUniqueID` field of the Certificate, or omitted if omitted in the Certificate
`subjectUniqueID`	Encoded value MUST be byte-for-byte identical to the `subjectUniqueID` field of the Certificate, or omitted if omitted in the Certificate
`extensions`	See Section 7.1.2.9.2
`signatureAlgorithm`	Encoded value MUST be byte-for-byte identical to the `tbsCertificate.signature`.
`signature`	

Note: This profile requires that the `serialNumber` field of the Precertificate be identical to that of the corresponding Certificate. RFC 5280, Section 4.1.2.2 requires that the `serialNumber` of certificates be unique. For the purposes of this document, a Precertificate shall not be considered a “certificate” subject to that requirement, and thus may have the same `serialNumber` of the corresponding Certificate. However, this does not permit two Precertificates to share the same `serialNumber`, unless they correspond to the same Certificate, as this would otherwise indicate there are two corresponding Certificates that share the same `serialNumber`.

7.1.2.9.1 Precertificate Profile Extensions - Directly Issued

These extensions apply in the context of a Precertificate directly issued from a CA, and not from a Precertificate Signing CA Certificate, as defined in Section 7.1.2.4.

Extension	Presence	Critical	Description
Precertificate Poison (OID: 1.3.6.1.4.1.11129.2.4.3)	MUST	Y	See Section 7.1.2.9.3
Signed Certificate Timestamp List	MUST NOT	-	
Any other extension	*	*	The order, criticality, and encoded values of all other extensions MUST be byte-for-byte identical to the `extensions` field of the Certificate

Note: This requirement is expressing that if the Precertificate Poison extension is removed from the Precertificate, and the Signed Certificate Timestamp List is removed from the certificate, the contents of the `extensions` field MUST be byte-for-byte identical to the Certificate.

7.1.2.9.2 Precertificate Profile Extensions - Precertificate CA Issued

These extensions apply in the context of a Precertificate from a Precertificate Signing CA Certificate, as defined in Section 7.1.2.4. For such Precertificates, the `authorityKeyIdentifier`, if present in the Certificate, is modified in the Precertificate, as described in RFC 6962, Section 3.2.

Extension	Presence	Critical	Description
Precertificate Poison (OID: 1.3.6.1.4.1.11129.2.4.3)	MUST	Y	See Section 7.1.2.9.3
`authorityKeyIdentifier`	*	*	See Section 7.1.2.9.4
Signed Certificate Timestamp List	MUST NOT	-	
Any other extension	*	*	The order, criticality, and encoded values of all other extensions MUST be byte-for-byte identical to the `extensions` field of the Certificate

7.1.2.9.3 Precertificate Poison

The Precertificate MUST contain the Precertificate Poison extension (OID: 1.3.6.1.4.1.11129.2.4.3).

This extension MUST have an `extnValue` `OCTET STRING` which is exactly the hex-encoded bytes `0500`, the encoded representation of the ASN.1 NULL value, as specified in RFC 6962, Section 3.1.

7.1.2.9.4 Precertificate Authority Key Identifier

For Precertificates issued by a Precertificate Signing CA, the contents of the `authorityKeyIdentifier` extension MUST be one of the following:

1. SHOULD be as defined in the profile below, or;
2. MAY be byte-for-byte identical with the contents of the `authorityKeyIdentifier` extension of the corresponding Certificate.

Field	Description
`keyIdentifier`	MUST be present. MUST be identical to the `subjectKeyIdentifier` field of the Precertificate Signing CA Certificate
`authorityCertIssuer`	MUST NOT be present
`authorityCertSerialNumber`	MUST NOT be present

Note: RFC 6962 describes how the `authorityKeyIdentifier` present on a Precertificate is transformed to contain the value of the Precertificate Signing CA's `authorityKeyIdentifier` extension (i.e. reflecting the actual issuer certificate's `keyIdentifier`), thus matching the corresponding Certificate when verified by clients. These Baseline Requirements RECOMMEND the use of the Precertificate Signing CA's `keyIdentifier` in Precertificates issued by it in order to ensure consistency between the `subjectKeyIdentifier` and `authorityKeyIdentifier` of all certificates in the chain. Although RFC 5280 does not strictly require such consistency, a number of client implementations enforce such consistency for Certificates, and this avoids any risks from Certificate Transparency Logs incorrectly implementing such checks.

7.1.2.10 Common CA Fields

This section contains several fields that are common among multiple CA Certificate profiles. However, these fields may not be common among all CA Certificate profiles. Before issuing a certificate, the CA MUST ensure the certificate contents, including the contents of each field, complies in whole with all of the requirements of at least one Certificate Profile documented in Section 7.1.2.

7.1.2.10.1 CA Certificate Validity

Field	Minimum	Maximum
`notBefore`	One day prior to the time of signing	The time of signing
`notAfter`	The time of signing	Unspecified

7.1.2.10.2 CA Certificate Naming

All `subject` names MUST be encoded as specified in Section 7.1.4.

The following table details the acceptable `AttributeType`s that may appear within the `type` field of an `AttributeTypeAndValue`, as well as the contents permitted within the `value` field.

Attribute Name	Presence	Value	Verification
`countryName`	MUST	The two-letter ISO 3166-1 country code for the country in which the CA's place of business is located.	Section 3.2.2.3
`stateOrProvinceName`	MAY	If present, the CA's state or province information.	Section 3.2.2.1
`localityName`	MAY	If present, the CA's locality.	Section 3.2.2.1
`postalCode`	MAY	If present, the CA's zip or postal information.	Section 3.2.2.1
`streetAddress`	MAY	If present, the CA's street address. Multiple instances MAY be present.	Section 3.2.2.1
`organizationName`	MUST	The CA's name or DBA. The CA MAY include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that the CA documents the difference and any abbreviations used are locally accepted abbreviations; e.g. if the official record shows "Company Name Incorporated", the CA MAY use "Company Name Inc." or "Company Name".	Section 3.2.2.2
`organizationalUnitName`	This attribute MUST NOT be included in Root CA Certificates defined in Section 7.1.2.1 or TLS Subordinate CA Certificates defined in Section 7.1.2.5 or Technically-Constrained TLS Subordinate CA Certificates defined in Section 7.1.2.6. This attribute SHOULD NOT be included in other types of CA Certificates.	-	-
`commonName`	MUST	The contents SHOULD be an identifier for the certificate such that the certificate's Name is unique across all certificates issued by the issuing certificate.	
Any other attribute	NOT RECOMMENDED	-	See Section 7.1.4.4

7.1.2.10.3 CA Certificate Authority Information Access

If present, the `AuthorityInfoAccessSyntax` MUST contain one or more `AccessDescription`s. Each `AccessDescription` MUST only contain a permitted `accessMethod`, as detailed below, and each `accessLocation` MUST be encoded as the specified `GeneralName` type.

The `AuthorityInfoAccessSyntax` MAY contain multiple `AccessDescription`s with the same `accessMethod`, if permitted for that `accessMethod`. When multiple `AccessDescription`s are present with the same `accessMethod`, each `accessLocation` MUST be unique, and each `AccessDescription` MUST be ordered in priority for

that `accessMethod`, with the most-preferred `accessLocation` being the first `AccessDescription`. No ordering requirements are given for `AccessDescription`s that contain different `accessMethod`s, provided that previous requirement is satisfied.

Access Method	Access Location	Presence	Maximum	Description
`id-ad-ocsp` (OID: 1.3.6.1.5.5.7.48.1)	`uniformResourceIdentifier`	MAY	*	A HTTP URL of the Issuing CA's OCSP responder.
`id-ad-caIssuers` (OID: 1.3.6.1.5.5.7.48.2)	`uniformResourceIdentifier`	MAY	*	A HTTP URL of the Issuing CA's certificate.
Any other value	-	MUST NOT	-	No other `accessMethod`s may be used.

7.1.2.10.4 CA Certificate Basic Constraints

Field	Description
`cA`	MUST be set TRUE
`pathLenConstraint`	MAY be present

7.1.2.10.5 CA Certificate Certificate Policies

If present, the Certificate Policies extension MUST contain at least one `PolicyInformation`. Each `PolicyInformation` MUST match the following profile:

No Policy Restrictions (Affiliated CA)		
Field	**Presence**	**Contents**
`policyIdentifier`	MUST	When the Issuing CA wishes to express that there are no policy restrictions, and if the Subordinate CA is an Affiliate of the Issuing CA, then the Issuing CA MAY use the `anyPolicy` Policy Identifier, which MUST be the only `PolicyInformation` value.
`anyPolicy`	MUST	
`policyQualifiers`	NOT RECOMMENDED	If present, MUST contain only permitted `policyQualifiers` from the table below.

Policy Restricted		
Field	**Presence**	**Contents**
`policyIdentifier`	MUST	One of the following policy identifiers:
A Reserved Certificate Policy Identifier	MUST	The CA MUST include exactly one Reserved Certificate Policy Identifier (see Section 7.1.6.1) associated with the given Subscriber Certificate type (see Section 7.1.2.7.1) directly or transitively issued by this Certificate.
`anyPolicy`	MUST NOT	The `anyPolicy` Policy Identifier MUST NOT be present.
Any other identifier	MAY	If present, MUST be defined by the CA and documented by the CA in its Certificate Policy and/or Certification Practice Statement.
`policyQualifiers`	NOT RECOMMENDED	If present, MUST contain only permitted `policyQualifiers` from the table below.

The Policy Restricted profile RECOMMENDS that the first `PolicyInformation` value within the Certificate Policies extension contains the Reserved Certificate Policy Identifier (see 7.1.6.1)[14]. Regardless of the order of `PolicyInformation` values, the Certificate Policies extension MUST contain exactly one Reserved Certificate Policy Identifier.

Note: `policyQualifiers` is NOT RECOMMENDED to be present in any Certificate issued under this Certificate Profile because this information increases the size of the Certificate without providing any value to a typical Relying Party, and the information may be obtained by other means when necessary.

If the `policyQualifiers` is permitted and present within a `PolicyInformation` field, it MUST be formatted as follows:

Permitted `policyQualifiers`			
Qualifier ID	**Presence**	**Field Type**	**Contents**
`id-qt-cps` (OID: 1.3.6.1.5.5.7.2.1)	MAY	`IA5String`	The HTTP or HTTPS URL for the Issuing CA's Certificate Policies, Certification Practice Statement, Relying Party Agreement, or other pointer to online policy information provided by the Issuing CA.
Any other qualifier	MUST NOT	-	-

7.1.2.10.6 CA Certificate Extended Key Usage

Key Purpose	OID	Presence
`id-kp-serverAuth`	1.3.6.1.5.5.7.3.1	MUST
`id-kp-clientAuth`	1.3.6.1.5.5.7.3.2	MAY
`id-kp-codeSigning`	1.3.6.1.5.5.7.3.3	MUST NOT
`id-kp-emailProtection`	1.3.6.1.5.5.7.3.4	MUST NOT
`id-kp-timeStamping`	1.3.6.1.5.5.7.3.8	MUST NOT
`id-kp-OCSPSigning`	1.3.6.1.5.5.7.3.9	MUST NOT
`anyExtendedKeyUsage`	2.5.29.37.0	MUST NOT
Precertificate Signing Certificate	1.3.6.1.4.1.11129.2.4.4	MUST NOT
Any other value	-	NOT RECOMMENDED

7.1.2.10.7 CA Certificate Key Usage

Key Usage	Permitted	Required
`digitalSignature`	Y	N[15]
`nonRepudiation`	N	–
`keyEncipherment`	N	–
`dataEncipherment`	N	–
`keyAgreement`	N	–
`keyCertSign`	Y	Y
`cRLSign`	Y	Y
`encipherOnly`	N	–
`decipherOnly`	N	–

7.1.2.10.8 CA Certificate Name Constraints

If present, the Name Constraints extension MUST be encoded as follows. As an explicit exception from RFC 5280, this extension SHOULD be marked critical, but MAY be marked non-critical if compatibility with certain legacy applications that do not support Name Constraints is necessary.

`nameConstraints` requirements	
Field	**Description**
`permittedSubtrees`	
`GeneralSubtree`	The requirements for a `GeneralSubtree` that appears within a `permittedSubtrees`.
`base`	See following table.
`minimum`	MUST NOT be present.
`maximum`	MUST NOT be present.
`excludedSubtrees`	
`GeneralSubtree`	The requirements for a `GeneralSubtree` that appears within a `permittedSubtrees`.
`base`	See following table.
`minimum`	MUST NOT be present.
`maximum`	MUST NOT be present.

The following table contains the requirements for the `GeneralName` that appears within the `base` of a `GeneralSubtree` in either the `permittedSubtrees` or `excludedSubtrees`.

`GeneralName` requirements for the `base` field			
Name Type	**Presence**	**Permitted Subtrees**	**Excluded Subtrees**
`dNSName`	MAY	The CA MUST confirm that the Applicant has registered the `dNSName` or has been authorized by the domain registrant to act on the registrant's behalf. See Section 3.2.2.4.	If at least one `dNSName` instance is present in the `permittedSubtrees`, the CA MAY indicate one or more subordinate domains to be excluded.
`iPAddress`	MAY	The CA MUST confirm that the Applicant has been assigned the `iPAddress` range or has been authorized by the assigner to act on the assignee's behalf. See Section 3.2.2.5.	If at least one `iPAddress` instance is present in the `permittedSubtrees`, the CA MAY indicate one or more subdivisions of those ranges to be excluded.
`directoryName`	MAY	The CA MUST confirm the Applicant's and/or Subsidiary's name attributes such that all certificates issued will comply with the relevant Certificate Profile (see Section 7.1.2), including Name Forms (See Section 7.1.4).	It is NOT RECOMMENDED to include values within `excludedSubtrees`.
`rfc822Name`	NOT RECOMMENDED	The CA MAY constrain to a mailbox, a particular host, or any address within a domain, as specified within RFC 5280, Section 4.2.1.10. For each host, domain, or Domain portion of a Mailbox (as specified within RFC 5280, Section 4.2.1.6), the CA MUST confirm that the Applicant has registered the domain or has been authorized by the domain registrant to act on the registrant's behalf. See Section 3.2.2.4.	If at least one `rfc822Name` instance is present in the `permittedSubtrees`, the CA MAY indicate one or more mailboxes, hosts, or domains to be excluded.
`otherName`	NOT RECOMMENDED	See below	See below
Any other value	NOT RECOMMENDED	-	-

Any `otherName`, if present:

1. MUST apply in the context of the public Internet, unless:
    1. the `type-id` falls within an OID arc for which the Applicant demonstrates ownership, or,
        1. the Applicant can otherwise demonstrate the right to assert the data in a public context.
2. MUST NOT include semantics that will mislead the Relying Party about certificate information verified by the CA.
3. MUST be DER encoded according to the relevant ASN.1 module defining the `otherName` `type-id` and `value`.

CAs SHALL NOT include additional names unless the CA is aware of a reason for including the data in the Certificate.

7.1.2.11 Common Certificate Fields

This section contains several fields that are common among multiple certificate profiles. However, these fields may not be common among all certificate profiles. Before issuing a certificate, the CA MUST ensure the certificate contents, including the contents of each field, complies in whole with all of the requirements of at least one Certificate Profile documented in Section 7.1.2.

7.1.2.11.1 Authority Key Identifier

Field	Description
`keyIdentifier`	MUST be present. MUST be identical to the `subjectKeyIdentifier` field of the Issuing CA.
`authorityCertIssuer`	MUST NOT be present
`authorityCertSerialNumber`	MUST NOT be present

7.1.2.11.2 CRL Distribution Points

The CRL Distribution Points extension MUST be present in:

- Subordinate CA Certificates; and
- Subscriber Certificates that 1) do not qualify as "Short-lived Subscriber Certificates" and 2) do not include an Authority Information Access extension with an `id-ad-ocsp` accessMethod.

The CRL Distribution Points extension SHOULD NOT be present in:

- Root CA Certificates.

The CRL Distribution Points extension is OPTIONAL in:

- Short-lived Subscriber Certificates.

The CRL Distribution Points extension MUST NOT be present in:

- OCSP Responder Certificates.

When present, the CRL Distribution Points extension MUST contain at least one `DistributionPoint`; containing more than one is NOT RECOMMENDED. All `DistributionPoint` items must be formatted as follows:

`DistributionPoint` profile		
Field	**Presence**	**Description**
`distributionPoint`	MUST	The `DistributionPointName` MUST be a `fullName` formatted as described below.
`reasons`	MUST NOT	
`cRLIssuer`	MUST NOT	

A `fullName` MUST contain at least one `GeneralName`; it MAY contain more than one. All `GeneralName`s MUST be of type `uniformResourceIdentifier`, and the scheme of each MUST be "http". The first `GeneralName` must contain the HTTP URL of the Issuing CA's CRL service for this certificate.

7.1.2.11.3 Signed Certificate Timestamp List

If present, the Signed Certificate Timestamp List extension contents MUST be an `OCTET STRING` containing the encoded `SignedCertificateTimestampList`, as specified in RFC 6962, Section 3.3.

Each `SignedCertificateTimestamp` included within the `SignedCertificateTimestampList` MUST be for a `PreCert` `LogEntryType` that corresponds to the current certificate.

7.1.2.11.4 Subject Key Identifier

If present, the `subjectKeyIdentifier` MUST be set as defined within RFC 5280, Section 4.2.1.2. The CA MUST generate a `subjectKeyIdentifier` that is unique within the scope of all Certificates it has issued for each unique public key (the `subjectPublicKeyInfo` field of the `tbsCertificate`). For example, CAs may generate the subject key identifier using an algorithm derived from the public key, or may generate a sufficiently-large unique number, such as by using a CSPRNG.

7.1.2.11.5 Other Extensions

SHECA does not use other extensions.

7.1.3 Algorithm object identifiers

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

7.1.3.1 SubjectPublicKeyInfo

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

7.1.3.1.1 RSA

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

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

7.1.3.1.2 ECDSA

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

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

7.1.3.2 Signature AlgorithmIdentifier

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

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

The signatureAlgorithm field of a Certificate or Precertificate.

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

- The signature Algorithm field of a CertificateList
- The signature field of a TBSCertList

- The signature Algorithm field of a BasicOCSPResponse
- No other encodings are permitted for these fields

7.1.3.2.1 RSA

SHECA uses the following 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

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

7.1.5 Name constraints

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

7.1.6 Certificate policy object identifier

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

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

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

7.1.7 Usage of Policy Constraints extension

No stipulation.

7.1.8 Policy qualifiers syntax and semantics

SHECA may include information in the Certificate Policy extension.

7.1.9 Processing semantics for the critical Certificate Policies extension

No stipulation.

7.2 CRL profile

SHECA issues CRL regularly for subscribers and relying parties to query and use.

7.2.1 Version number(s)

CRL is formatted in accordance with X.509 V2.

7.2.2 CRL and CRL entry extensions

They are consistent with ITU X.509 and RFC5280 regulations.

The version number: it is used to specify the version information of CRL, and SHECA adopts the CRL V2 version corresponding to the X.509 V3 certificate.

Signature algorithm: SHECA adopts signature algorithms of SHA256WithRSA or SHA384WithRSA.

Issuer: the DN name of the issuer is composed of the state, province, city, organization, department and common name, etc.

Effective date: specify a date/time value to indicate the time when the CRL is generated.

Next Update: specify a date/time value to indicate the time when the next CRL will be generated .

Revocation list: it specifies the list of certificates that have been revoked. This list contains the serial number of the certificate and the date and time when the certificate is revoked.

Authority Key Identifier: this identifier is used to verify the public key signed on the CRL. It can identify different keys used by the same CA.

Next CRL Publish: specify a date/time value to indicate the time when the next CRL will be published.

Reason Code: Used for CRL to indicate the reason for revocation.

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

- keyCompromise (1)
- privilegeWithdrawn (9)
- cessationOfOperation (5)
- affiliationChanged (3)
- superseded (4)
- unspecified (0) , in which case the reasonCode entry extension is omitted.

When the CRL reasonCode is not one of the above, the reasonCode extension will not be provided.
The following is a description of each of these reason codes and circumstances where SHECA or a subscriber will be obligated to use it for their revocation circumstances:

keyCompromise

The CRLReason keyCompromise is used if:

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

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

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

• SHECA is made aware of a demonstrated or proven method that can easily compute the certificate subscriber's private key based on the public key in the certificate ; or

• The certificate subscriber requests that SHECA revoke the certificate for this reason, with the scope of revocation being described below.

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

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

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

privilegeWithdrawn

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

CRLReason privilegeWithdrawn is used when:

• SHECA obtains evidence that the certificate was misused; or

• SHECA is made aware that the certificate subscriber has violated one or more of its material obligations under the subscriber agreement or terms of use; or

• SHECA is made aware that a wildcard certificate has been used to authenticate a fraudulently misleading subordinate fully-qualified domain name; or

• SHECA is made aware of a material change in the information contained in the certificate; or

• SHECA determines or is made aware that any of the information appearing in the certificate is inaccurate; or

• SHECA is made aware that the original certificate request was not authorized and that the Subscriber does not retroactively grant authorization.

cessationOfOperation

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

CRL cessationOfOperations is used when:

• The certificate subscriber will no longer be using the certificate because they are discontinuing their website; or

• SHECA is made aware of any circumstance indicating that use of a fully-qualified domain name or IP address in the certificate is no longer legally permitted.

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

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

affiliationChanged

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

CRLReason affiliationChanged is used when:

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

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

superseded

The CRLReason superseded is used when:

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

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

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

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

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

7.3 OCSP profile

The OCSP response issued by SHECA's certification system conforms to the RFC6960 Standard, which defines a standard request and response information format to confirm the status of the certificate.

7.3.1 Version number(s)

RFC6960 defines the OCSP V1.

7.3.2 OCSP extensions

OCSP request contains the following data: protocol version, service request, target certificate identifier, and optional extensions, etc.

After receiving a request, the OCSP server conducts the following detections when responding:

- the message is well formatted;
- the responder is configured to provide the request service.

The request includes the information needed by the responder server, and if any one of the prerequisites is not satisfied, the OCSP server will generate an error message; otherwise, return a definite reply.
All definite replies are digitally signed by SHECA OCSP signing certificate. The main reply status includes: the certificate is valid, revoked, unknown. The reply information is composed of the following parts：

- Version of the response syntax
- Identifier of the responder server
- Response to the request certificate
- Time when the response was generated
- Optional extensions
- The object identifier of signature algorithm
- The signature of the hashed reply information

If an error occurs, the OCSP responder server will return an error message which does not contain the signature of SHECA OCSP certificate. Error information may include:

- Request with incorrect formatting
- Internal error
- Please try again later
- Require signature
- Unauthorized

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

SHECA should perform the audit and assessment as follows:

1) carry out an operational quality assessment quarterly to ensure the reliability, security and controlability of operation services.

2) carry out an internal audit of authentication quarterly and draw at least 3% of certificate samples.

3) carry out an annual CCADB Self-Assessment according to CA/Browser Forum CCADB policy.

4) carry out an annual self-audit of physical control, key management, operation control, and authentication execution, etc. to determine whether the actual circumstance is consistent with the predetermined standards and requirements and take actions according to the results of the review.

5) carry out an annual operation risk assessment to identify internal and external threats, to assess the possibility and compromise of the threats, and to formulate and implement a disposal plan based on the results of the risk assessment.

6) in addition to internal audit and assessment, SHECA also employs independent auditing firms to conduct external audits and assessments in accordance with WebTrust standards.

8.2 Identity/qualifications of assessor

Internal audit and assessment are carried out by SHECA's internal audit and assessment team.

External audit will be done by the authority with the following qualifications:

1. Must be a licensed and certified assessment authority, honored a good reputation in the industry;

2. Have sufficient knowledge in the computer information security system, communication network security requirements, PKI technology, standards and operation;

3. Possess professional skills and tools to check the system operating performance;

4. Possess the qualification of WebTrust audit.

8.3 Assessor's relationship to assessed entity

The position of internal auditors and the system administrators, business managers and business operators of this organization must not overlap.

The relationship between external assessors and SHECA is independent, and there is no stake between them that may affect the objectivity of the assessment.

8.4 Topics covered by assessment

The internal audit shall involve the following schemes:

1. whether the operation process and system are strictly observed.

2. whether the certification service is done strictly according to CP/CPS, service specifications and security requirements.

3. whether all kinds of logs and records are integrated and whether there are any problems;

4. whether there is any other potential security risk.

In accordance with the requirements of WebTrust standards, the third-party auditors audit SHECA independently.

8.5 Actions taken as a result of deficiency

Regarding problems in the internal audit results, the audit assessment team is responsible for overseeing the improvement of the responsible departments.

After the completion of the third-party Auditor's assessment, SHECA will rectify and reform in accordance with the work report and accept re-audit and assessment.

8.6 Communication of results

There will be formal notification of internal audit results to the responsible departments, and SHECA will inform the subscribers in time of the potential security risks.

The Audit Report SHALL state explicitly that it covers the relevant systems and processes used in the issuance of all Certificates that assert one or more of the policy identifiers listed in Section 7.1.6.1.

After the completion of the assessment done by the third-party auditing firm, the audit report will be provided to SHECA. After SHECA's rectification and the reassessment are completed, SHECA will publish the final audit results on the official website.

8.7 Self-Audits

SHECA monitors adherence to its CP-CPS and these Requirements and strictly control its service quality by performing self audits. The self audits are performed contineously at a quarterly basis, against a randomly selected sample of three percent of the certificates issued by SHECA.

SHECA uses a Linting process to verify the technical accuracy of Certificates within the selected sample set independently of previous linting performed on the same Certificates.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate issuance or renewal fees

SHECA charges subscribers fees for some of its certificate services (including issuance, renewal, and reissue). For detailed information on fees, please visit the SHECA official website (www.sheca.com). SHECA reserves the right to adjust fees at any time. SHECA partners (including resellers and EPKI administrator account holders) will promptly notify you of price changes in accordance with the cooperation agreement.

9.1.2 Certificate access fees

During the validity period of the certificate, SHECA does not charge special fees for certificate access. If the user asks for special needs, extra fees may be needed to pay, which will be charged based on the negotiation of SHECA Marketing department with the user.

9.1.3 Revocation or status information access fees

SHECA does not charge any fee for the acquisition of CRL.

SHECA does not charge any fee for OCSP services.

9.1.4 Fees for other services

If SHECA provides the subscriber with certificate storage media and related services, SHECA will specify the price in the agreement signed with the subscriber or other entities.

9.1.5 Refund policy

SHECA offers a 30-day refund policy. Within 30 days (from the date the certificate was first issued), subscribers can apply for a full refund. In this case, all certificates associated with the original order may be revoked and a refund will be issued to the applicant.

If the subscriber contract cannot be fulfilled or the subscriber certificate cannot be used due to SHECA, SHECA will return the related fee to the subscriber.

9.2 Financial responsibility

9.2.1 Insurance coverage

SHECA shall determine the insurance policy according to business development.

Currently, SHECA self-insures for liabilities arising from its performance and obligations under this CP/CPS.

Based on forecasts of user demand and marketing plans, SHECA expects to issue no more than 100 EV certificates annually, including EV SSL certificates and EV Code Signing certificates. According to the financial statements in the past twelve months, SHECA has the financial capacity to fulfill compensation obligations to EV certificate users, considering its financial position and the expected volume of EV certificate applications.

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

If SHECA is judicially determined to bear compensation and/or indemnification liabilities, it will assume the corresponding compensation liabilities in accordance with the ruling of the relevant arbitration institution or the judgment of the court.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

In the electronic certification services provided by SHECA, the following information is considered confidential, and reasonable measures are taken to ensure its security:

1. Personal and company information maintained by SHECA and registration authorities shall also be kept confidential and shall not be disclosed except as required by law.

2. Private keys and activation data used to access private keys or gain access to CA systems.

3. Business continuity, incident response, emergency, and disaster recovery plans.

4. Other security measures used to protect the confidentiality, integrity, or availability of information.

5. Private information held by SHECA pursuant to Section 9.4.

6. Audit logs, archived records, transaction records, financial audit records, external or internal audit trail records, and any audit reports .

The above information is considered confidential, and SHECA will implement appropriate confidentiality measures to prevent its disclosure.

9.3.2 Information not within the scope of confidential information

SHECA treated the following information as not confidential information:

1. Certificates issued by SHECA and information in CRL.

2. Information in the certificate policy supported by SHECA and identified by CP/CPS.

3. Information published on SHECA's website to the public, and approved available for subscribers usage only.

4. The confidentiality of SHECA's other information depends on special data items and applications.

9.3.3 Responsibility to protect confidential information

SHECA has the responsibility and obligation to properly keep and protect the confidential information specified in Section 9.3.1 of this CP/CPS.

CA, its RAs, subscribers and participants related to the certification service are all obliged to undertake the corresponding responsibility for protecting confidential information according to the regulations of this CP/CPS, and shall protect confidential information by effective technical means and management procedures.

When the owner of the confidential information, for some reason, requires SHECA to make public or disclose the confidential information that he or she owns, SHECA should meet the owner's requirements; meanwhile, SHECA will require the owner of the confidential information to authorize the application in writing to express the owner's willingness of publicity or disclosure. If this behavior of disclosing confidential information involves any other party's liability for indemnification, SHECA shall not bear any loss related to or arising from the disclosure of confidential information. The owner of confidential information shall bear all liabilities for indemnification arising from or related to the disclosure of confidential information.

When SHECA is required to provide confidential information stipulated in this CP/CPS through legal procedures by any law, rule, court, or other public authorities, SHECA should publish the relevant confidential information to the law enforcing agencies in accordance with requirements of laws, regulations and court judgments. SHECA assumes no responsibility. Such provision is not regarded as a breach of requirements or obligations on confidentiality.

9.4 Privacy of personal information

SHECA respects the privacy of materials of certificate subscribers and ensures the compliance with the relevant national regulations and laws on privacy protection. Meanwhile, SHECA will ensure that all staff strictly comply with the internal working system and regulations.

9.4.1 Privacy plan

SHECA respects for all users and their privacy, if there is an announcement associated with this explicit privacy protection laws (such as the Personal Information Protection Law) , it will automatically be referenced in this CP/CPS and its privacy protection will become a fundamental basis to perform.

Anyone who choose to use any services of SHECA, has agreed to accept SHECA about the privacy statement.

Information treated as privacy includes:

1. the valid documents number of the subscriber, such as the ID card number, the organization code.

2. the subscriber's phone number.

3. the subscriber's mailing address and home address.

4. the bank account number of the subscriber.

5. the agreement signed between subscriber with SHECA and SHECA's RA.

Please find SHECA's privacy policy at https://www.sheca.com/assets/wwx/laws.html.

9.4.2 Information treated as private

As SHECA manages and uses relevant information offered by subscriber, in addition to the information in the certificate, the basic information and identification information shall be considered as privacy, and the information shall not be published without subscriber’s agreement or the legal requirements of laws and regulations and other agencies.

9.4.3 Information not deemed private

Information that is not deemed private information of the certificate subscriber includes, but is not limited to, the following information:

1. certificate and certificate status information.

2. subscriber's name, organization name, etc.

3. subscriber's gender, organization type, etc.

4. postcode of subscriber's mailing address.

5. subscriber's email.

6. information that subscriber requires to be in the certificate.

9.4.4 Responsibility to protect private information

SHECA, any subscriber, relevant entities and the participants involved in certification business, shall have the obligations to assume corresponding responsibilities of protecting privacy information according to the provisions of this CPS.

At the request of laws and regulations or in any court and the public power sector through legal procedures or the owner or the information written authorization, SHECA can release to specific objects about the relevant privacy information. SHECA do not assume any responsibility, and such disclosure can not be considered as a violation of privacy obligations. If this privacy disclosure leads to any loss, SHECA should not bear any responsibility.

9.4.5 Notice and consent to use private information

Any subscriber information SHECA obtaining within the scope of certification business can only be used for identifying, managing and serving subscribers. As using the information, no matter the privacy is involved or not, SHECA has no obligations to notify subscribers, and doesn't get subscriber consent.

Under any requirements of laws and regulations, and demands for undergoing the legal process of other agencies, or under the circumstance where private information holder submits the written authorization to certain object for publishing the information, SHECA has no obligations to notify subscriber, and to obtain the consent from the subscriber.

If certification authority and registration authority shall apply user’s private information to other purposes beyond the functions agreed between two sides, CA and RA shall notify subscriber to obtain his/her/its agreement and authorization, and the agreement and authorization shall be archived with the form.

9.4.6 Disclosure pursuant to judicial or administrative process

SHECA and its registration agencies will not require any other agencies to provide relevant information with or without the knowledge of subscribers..

9.4.7 Other information disclosure circumstances

Disclosure of other information is subject to laws and subscriber agreements.

9.5 Intellectual property rights

SHECA enjoys and retains intellectual property rights like copyrights and patent rights of all the software, materials, data and information published to the public and provided by SHECA, as well as certificate issued by SHECA through various channels, such as websites.

SHECA enjoys the ownership, right of name, and benefit sharing right of the digital certificate system software, and has intellectual property rights for the issued certificates, certificate revocation lists and the information therein.

SHECA has intellectual property rights for this CP/CPS and related operation management work documents. According to the Mozilla Root Policy, Mozilla can use this CP/CPS on the premise of complying with the CC BY 4.0 agreement .

The certificate subscriber has intellectual property rights for the certificate registration information and the trademarks, service marks, trade names and distinguished names contained in subscriber's certificate.

The key pair of the certificate is the intellectual property of the entity corresponding to the subject or entity owner in the certificate.

9.6 Representations and warranties

9.6.1 CA representations and warranties

SHECA makes following commitment during the process of providing electronic certification services:

1. The certificate issued to the subscriber meets all the substantive requirements of this CP/CPS.

2. Notify the certificate subscriber of any known event that will affect the validity and reliability of the certificate of the subscriber in nature.

3. The certificate will be revoked in time in accordance with the requirements of this CP/CPS.

4. If SHECA is not affiliated with a subscriber, SHECA and the subscriber are two parties of a legally effective and executable subscriber agreement, and the subscriber agreement meets the requirements of the Baseline Requirements issued by the CA/Browser Forum; if SHECA is the same entity or is associated with the subscriber, the applicant has approved the terms of use;

5. Establish and maintain a database that is open 24*7 for all current status information (effective or revoked) of all unexpired certificates.

6. After publicly issuance of the certificate, SHECA ensures that subscriber information in the certificate is verified.

SHECA is not responsible for assessing whether the certificate is used within the appropriate range, and the subscriber and the relying parties ensure that the certificate is used for the appropriate purposes of use in accordance with the subscriber agreement and the relying party's agreement.

9.6.2 RA representations and warranties

The commitment of SHECA's RA in the process of participating in the electronic certification service is as follows:

1. The registration process provided to the certificate subscriber fully complies with all the substantive requirements of this CP/CPS;

2. If a certificate is refused to issue, all fees paid will be refund to the certificate applicant immediately;

3. Verify that the applicant has the right to use or control the domain name and IP address which is listed in the certificate subject field and Subject Alternative Name field;

4. Verify that the applicant or the applicant's representative has been authorized to apply for a certificate on behalf of the applicant;

5. Verify the accuracy of all the information contained in the certificate;

6. Verify the identity of the applicant in accordance with the requirements of Section 3.2 of this CP/CPS;

RA will submit service applications for revocation and renewal, etc. to SHECA in time according to the regulations of CP/CPS.

9.6.3 Subscriber representations and warranties

Once a subscriber accepts the certificate issued by SHECA, it is deemed to make the following commitment to SHECA, its RAs and the relevant parties trusting the certificate:

1. The subscriber has read, known and accepted the responsibility clauses in the subscriber agreement of SHECA's and all the terms and conditions in this CP/CPS when applying for a certificate.

2. The subscriber should use the certificate private key for digital signature within the validity period of the certificate.

3. The information, materials provided and statements made by the subscribers for applying for certificate are true, complete and accurate. In case of any changes in the foregoing information, materials or statements, the subscriber shall notify RA in time in written form. The subscriber shall bear all the legal responsibilities on subscriber's own, if the subscriber intentionally or negligently provides false or falsified information, materials or statements, or the subscriber does not notify RA in time in written form after the provided information, materials and statements are changed.

4. If there is an agent, both the subscriber and the agent are jointly and severally liable. The subscriber is responsible for informing SHECA or its authorized RAs on any false statement or omission made by the agent.

5. Each signature made by the private key corresponding to the public key contained in the subscriber's certificate is the subscriber's own signature, and the certificate is a valid certificate (the certificate is not expired or revoked) when the signature is signed, and the private key of the certificate is accessed and used by the subscriber itself.

6. Once the certificate is accepted, it means that the subscriber knows and accepts all the terms and conditions in this CP/CPS, and knows and accepts the corresponding digital certificate subscribe agreement.

7. Once the certificate is accepted, the subscriber shall assume the following responsibilities: always maintain control of its private key; use trusted system; take safe and reasonable steps to prevent the loss, compromise, tampering, or unauthorized use of the private key, and if the subscriber knows or should know that the private key or password of the certificate has already or may have already been lost, compromised, tampered or used without authorization, the subscriber shall notify the parties concerned in time in written form and terminate using the certificate immediately.

8. Prohibited for rejecting any statements, changes, updates, upgrades published by SHECA, including but not limited to modifications of policies and specifications as well as additions and deletions of certificate services.

9. The subscriber shall use certificate within the range specified in this CP/CPS and is used only for authorized or other legitimate use purposes and shall not be used in scenarios other than the purposes of use.

10. Regarding EV SSL certificates, subscribers have the responsibility and obligation to ensure that certificates are deployed only in the servers corresponding to the subject alternative name listed in the certificate.

9.6.4 Relying party representations and warranties

The relying party claims and commits: it evaluates the suitability of trusting certificates in specific applications and does not trust certificates in applications other than the appropriate purposes of certificates. The commitment of the relying party in the process of participating in the electronic certification service is as follows:

1. Have read CP/CPS and the relying party agreement, agree to comply with all the provisions and constraints of this CP/CPS and the relying party agreement, and agree to the provisions of this CP/CPS on the limitation of SHECA's liability prior to any trust act.

2. Before trusting the certificate, evaluate the appropriateness of trust certificate in a specific application, understand the purpose of the use of the certificate, and confirm whether the use of the certificate is in accordance with the provisions of this CP/CPS within the specified range and period.

3. Verify the trust anchor of the certificate before trusting a certificate.

4. Confirm whether the certificate is revoked by querying CRL and/or OCSP before trusting a certificate.

5. In the event of negligence or other reasons that violate the terms of reasonable check, the relying party is willing to compensate for the loss caused to SHECA and to bear the loss of its own or others.

6. Prohibited for rejecting any statements, changes, updates, upgrades published by SHECA, including but not limited to modifications of policies and specifications as well as additions and deletions of certificate services.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of warranties

One of the following cases shall exempt SHECA from the liability to warranties, and SHECA does not bear any legal liability to any party, including but not limited to liability of compensation and liability of indemnity.

1) When applying for and using SHECA's digital certificate, subscribers have violated one of the following obligations:

- The subscriber is obliged to provide true, complete and accurate materials and information, and shall not provide false or invalid materials or information;

- The subscriber shall keep the digital certificate carrier issued by SHECA properly and protect the PIN code, and shall not leak the PIN code or deliver the digital certificate carrier to others at will;
- When a subscriber applies its own key or uses a digital certificate, the subscriber should use a reliable and secure system;
- When the subscriber knows that the confidentiality of the electronic signature has been compromised or may have been compromised, the subscriber should timely inform SHECA and the relevant parties and terminate the use of the electronic signature;
- When subscribers are using digital certificates, they must abide by the laws, regulations and administrative rules of the country. Digital certificates shall not be used for any other purpose beyond the range of use regulated by SHECA;
- The subscriber shall use the certificate within the valid period of the certificate; shall not use the digital certificate of which the confidentiality has been compromised or may have been compromised, that has been expired, frozen or revoked.

The subscriber is obliged to pay the service fees to SHECA on time as stipulated.
2) Digital certificate issuance delay, interruption, inability to issue, or suspension or termination of all or part of the certificate services caused due to force majeure; "force majeure" stipulated in this provision refers to an unforeseeable, unavoidable and insurmountable objective circumstance, including but not limited to:

- Natural phenomena or natural disasters, including earthquakes, volcanic eruptions, landslides, debris flows, avalanches, floods, tsunamis, typhoons and other natural phenomena;
- Social phenomena, social anomalies, or government acts, including new policies, laws and administrative regulations issued by government, or social anomalies such as war, strike, and riot.

3) Digital certificate issuance delay, interruption, inability to issue, or suspension or termination of all or part of the certificate services caused by SHECA's technical failures such as equipment or network failure; reasons for "technical failures" stipulated in this provision include but are not limited to:

- Force majeure;
- Caused by associated units such as electricity, telecommunication and communication units;
- Hacker attack;
- SHECA's equipment or network failure.

4) SHECA has carefully followed digital certificate certification rules stipulated by national laws and regulations, yet there are still losses arising.

9.8 Limitations of liability

Certificate subscribers and relying parties suffer losses in civil activities due to electronic certification services provided by SHECA, and SHECA will bear the limited liability of indemnification stipulated in Section 9.9 of this CP/CPS.

9.9 Indemnities

9.9.1 Indemnification by CAs

SHECA only bears the liability for the direct loss of the certificate subscriber and the relying party due to its own reasons, and bears no liability for the indirect loss.

The liability of indemnification that SHECA bears for direct loss is limited to: The compensation for each server certificate shall not exceed 5 times the purchase price of the certificate, and the compensation for each subscriber or each relying party for each EV server certificate shall not be less than 2 thousands US Dollars.

If SHECA violates the statement in Section 9.6.1 of this CP/CPS, the end entities, such as the certificate subscriber and the relying party, may apply for indemnity (except for statutory or agreed liability exemptions). In case of the following cases, SHECA bears limited liability of indemnification:

1. SHECA has issued the certificate to the third party other than the subscriber by mistake, causing the subscriber or the relying party to suffer losses;

2. Under the circumstance that the subscriber submits true, complete and accurate information or materials, the certificate issued by SHECA has wrong information, causing the subscriber or the relying party to suffer losses;

3. Under the circumstance that SHECA knows that the subscriber has submitted false information or materials and still issued a certificate to the subscriber, causing the relying party to suffer losses;

4. Due to SHECA's reasons, the private key of the certificate is deciphered, stolen and compromised, causing the subscriber or the relying party to suffer losses;

5. SHECA failed to revoke the certificate in time, causing the relying party to suffer losses.

In addition, the indemnity limit of SHECA is specified as follows:

1. All indemnification obligations of SHECA shall not exceed the upper limit of the indemnity, the upper limit of indemnity can be reformulated by SHECA according to the specific circumstance, and SHECA will immediately notify the parties concerned of the circumstance after the reformulation.

2. Regarding the losses caused by subscribers or relying parties, SHECA does not bear any liability of indemnification, which shall be undertaken by subscribers or relying parties on their own.

3. Regarding the loss incurred during the valid period of the certificate, the subscriber or the relying party shall lodge a claim in written with SHECA within three years from the date of knowing or should know the occurrence of the loss; the claim becomes invalid after the period of three years.

9.9.2 Indemnification by Subscribers

A subscriber shall bear the liability of indemnification if any of the following circumstances causes losses to SHECA and relying parties:

1. SHECA and its RA or the third party with its authorization suffer damages due to the subscriber's intention, negligence or malice of providing untrue, incomplete and inaccurate information while applying certificate;

2. The certificate private key has been compromised intentionally or negligently, subscriber knows that the private key has been compromised and lost without timely notification of SHECA and its RA, resulting in the damage for SHECA and its RA and the third party;

3. The subscriber's usage of certificate violates this CP/CPS and related operation rules, or the subscriber applies the certificate to the business range not specified in this CP/CPS;

4. During the period from the certificate subscriber or other entities that have the right to applying revoke the certificate make a revoke request to SHECA publishes the revocation information of the certificate, if the certificate is used for an illegal transaction, or if a dispute occurs during the transaction, and if SHECA has performed the relevant operations in accordance with the specifications of this CP/CPS, the certificate subscriber shall bear all liabilities for compromise before the publication of the revocation information;

5. The information in the certificate has changed but the subscriber fails to stop using the certificate and fails to timely notify SHECA and its RA;

6. No effective protection measures are taken for the private key, resulting in the loss or being damaged, stolen, compromised of the private key;

7. When knowing the private key is lost or at risk of being compromised, the subscriber fails to stop using the certificate and fails to timely notify SHECA and its RA;

8. The subscriber uses the certificate beyond the valid period of the certificate;

9. The subscriber's certificate information infringes the intellectual property rights of a third party;

10. The subscriber uses the certificate beyond the prescribed range and purposes, such as engaging in criminal activities.

9.9.3 Indemnification by Relying Parties

In the following circumstances leads to the loss of SHECA the relying party bears the liability :

1. The relying party fails to enforce the obligations of SHECA and the relying party or the obligations stipulated in this CP/CPS, resulting in damage to SHECA and its RA or third parties;

2. The relying party fails to make reasonable audits of certificates in accordance with the provisions of this CP/CPS, resulting in damage to SHECA and its RAs or third parties;

3. The relying party fails to verify the trust anchor of the certificate, resulting in damage to SHECA and its RAs or third parties;

4. The relying party fails to confirm whether the certificate is revoked by querying CRL or OCSP, resulting in damage to SHECA and its RA or third parties;

5. The relying party trusts certificates in unreasonable circumstances, such as the circumstance that the relying party trust a certificate when it knows that the certificate is used beyond the prescribed range or period, or the certificate has been or may be compromised.

9.10 Term and termination

9.10.1 Term

The CP/CPS comes into effect at 0:00 on the effective date. This CP/CPS becomes invalid on the day when the next version of CP/CPS becomes effective or when SHECA terminates the electronic certification service.

9.10.2 Termination

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 the termination of this CP/CPS, its effect will be terminated at the same time, but the legal facts that occur before the date of termination, the provisions of the responsibility of the parties and the exemption of liability in this CP/CPS are still applicable, including, but not limited to, the contents of audit, confidential information, privacy protection, intellectual property, etc. in CP/CPS, as well as limited liability clauses relating to indemnification, and are still valid after this CP/CPS is terminated.

When some provisions in CP/CPS, subscriber agreements, relying party agreements and other agreements become invalid due to some reason, such as content modifications or conflict with applicable laws, they do not affect the force of law of other provisions in the corresponding document.

9.11 Individual notices and communications with participants

SHECA and its RA, in the case of the necessary circumstances, such as the active revocation of subscriber certificates, the discovery that the subscriber uses the certificate for purposes other than those regulated purposes and has other behaviors violating the subscriber agreement, should individually notify the subscriber and the relying party by appropriate means, such as telephone, e-mail, letter, and fax, etc.

After the termination of this CP/CPS, SHECA should notify the parties concerned about the invalidation of the document.

9.12 Amendments

9.12.1 Procedure for amendment

Authorized by SHECA's Security Policy Administration Committee, the CP/CPS compiling team reviews this CP/CPS at least once a year to ensure that it complies with national laws and regulations and meets the requirements of administration department, meets relevant international standards, and meets the actual needs of the certification business development.

Regarding the amendment and update of this CP/CPS, the CP/CPS compiling team proposes an amendment report, and organizes the amendment after being approved by SHECA's Security Certification Committee, and the revised CP/CPS will be officially published to the public after being approved by the Committee.

9.12.2 Notification mechanism and period

The revised CP/CPS will be published immediately on SHECA's official website upon approval. SHECA will notify the parties concerned in a reasonable period of time for amendments that need to be notified through e-mail, letter, media and other means. The reasonable time should ensure the least impact on the parties concerned.

9.12.3 Circumstances under which OID must be changed

Circumstances under which SHECA must change this CP/CPS include: the inconsistency between the relevant contents of the CP/CPS and the governing laws, and the specific changes or adjustments is required by national regulatory authorities on the certification service of SHECA.

9.13 Dispute resolution provisions

When there is a dispute among entities such as SHECA, the subscriber and the relying party, it should be resolved firstly through friendly negotiation in accordance with the agreement; if negotiation fails, it can be resolved through legal means.

Regarding any lawsuit against SHECA or its RA on any dispute involved in this CP/CPS, all parties concerned agree to submit it to the jurisdiction of People's Court in the local place of SHECA's industrial and commercial registration.

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 CP/CPS shall apply to the laws of People’s Republic of China. Choice of law is to ensure that all subscribers have uniform procedures and interpretation, regardless of where they live and where to use the certificate.

9.15 Compliance with applicable law

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

9.16 Miscellaneous provisions

9.16.1 Entire agreement

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

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

9.16.2 Assignment

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

9.16.3 Severability

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

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

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

9.16.4 Enforcement

In the case of disputes and lawsuits between SHECA, RA, the subscriber and the relying party, the winning party may ask the other party to pay the relevant legal costs as part of the indemnity. The exemption from a party's indemnity for one contract breach does not mean the exemption from indemnification for other contract breaches.

SHECA states that, if certificate subscriber, relying party or other entities fails to implement a provision in this CP/CPS, it is not considered that the entity will not implement this provision or other provisions in the future.

9.16.5 Force Majeure

When SHECA or its RA do not have ability to provide normal services due to force majeure, such as natural disasters like earthquake, flood, lightning, and wars, etc., SHECA and its RA do not bear losses caused to users.

9.17 Other provisions

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

Certificate: Certificate is SHECA's property. Unless those certificates that isn't in any directory or repository without SHECA expressed written permission, the certificate can be a complete non-exclusive, royalty-free reproduction and distribution. On copyright notice, you can consult to SHECA.

CP/CPS: The CP/CPS is SHECA private property.

Distinguished name: distinguished name is owned by all the named entities.

Private key: Private key is owned by private subscribers (or their representative organizations, agencies or any other entities), regardless of the medium of storage and protection being used.

Public key: Public key is owned by subscribers (or their representative organizations, agencies or any other entities), regardless of the medium of storage and protection being used.

SHECA public key: The public key owned by SHECA is SHECA 's property, and SHECA is allowed to use these public key.

SHECA private key: Private key is SHECA's private property, whether partial or whole.