# SHECA S/MIME CERTIFICATE POLICY AND CERTIFICATION PRACTICE STATEMENT (CP/CPS)

## Version 1.1 ( Effective Date: May 25, 2026 )

## Version Control

| Version | Released Date | Issuer |
|---|---|---|
| 1.0 (History version) | January 13, 2026 | SHECA Security Certification Committee |
| 1.1 (Current version) | May 25, 2026 | SHECA Security Certification Committee |

## Change Description

| Version | Change Description |
|---|---|
| 1.0 | Combined CP & CPS for S/MIME Certificates |
| 1.1 | 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 SMIME certificates. 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 also complies with the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates published at https://www.cabforum.org. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

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 policy shall be maintained.

### 1.1.3 SHECA CA Hierarchy

Currently, SHECA has the following root CAs for SMIME:

1) **UniTrust Global SMIME RSA Root CA R1**

2) **UniTrust Global SMIME ECC Root CA R2**

All intermediate certification authorities are subordinated to their roots. All the above root CAs and their sub CAs are subject to SHECA S/MIME PKI hierarchy. There is no cross certificates under this 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 S/MIME 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 1.2.156.112570.1.0.9.

The following is a list of OIDs defined for all types of S/MIME certificates by SHECA:

| SHECA OID | CA/Browser Forum OID | Object |
|---|---|---|
| 1.2.156.112570.1.9.1 | 2.23.140.1.5.1.3 | Mailbox-validated strict S/MIME Certificates Policy |
| 1.2.156.112570.1.9.2 | 2.23.140.1.5.2.3 | Organization-validated strict S/MIME Certificates Policy |
| 1.2.156.112570.1.9.3 | 2.23.140.1.5.3.3 | Sponsor-validated strict S/MIME Certificates Policy |
| 1.2.156.112570.1.9.4 | 2.23.140.1.5.4.3 | Individual-validated strict S/MIME 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.

## 1.4 Certificate usage

### 1.4.1 Appropriate certificate uses

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

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

### 1.4.2 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.

# 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

**Affiliate**: A corporation, partnership, joint venture or other entity controlling, controlled by, or under common control with another entity, or an agency, department, political subdivision, or any entity operating under the direct control of a Government Entity.

**Applicant**: The Natural Person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Applicant is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual Certificate Request.

**Applicant Representative**: A Natural Person or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant:

1. who signs and submits, or approves a Certificate Request on behalf of the Applicant;
2. who signs and submits a Subscriber Agreement on behalf of the Applicant; and/or
3. who acknowledges the Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA or is the CA.

**Application Software Supplier**: A supplier of email client software or other relying-party application software such as mail user agents (web-based or application based) and email service providers that process S/MIME Certificates.
**Assumed Name**: Also known as “doing business as”, “DBA”, or “d/b/a” name in the US and “trading as” name in the UK.

**Attestation**: A letter attesting that Subject Information is correct written by an accountant, lawyer, government official, or other reliable third party customarily relied upon for such information.

**Audit Period**: In a period-of-time audit, the period between the first day (start) and the last day of operations (end) covered by the auditors in their engagement. (This is not the same as the period of time when the auditors are on-site at the CA.) The coverage rules and maximum length of audit periods are defined in Section 8.1.

**Audit Report**: A report from a Qualified Auditor stating the Qualified Auditor’s opinion on whether an entity’s processes and controls comply with the mandatory provisions of these Requirements.

**CA Key Pair**: A Key Pair where the Public Key appears as the Subject Public Key Info in one or more Root CA Certificate(s) and/or Subordinate CA Certificate(s).

**Certificate**: An electronic document that uses a digital signature to bind a Public Key and an identity.

**Certification Authority (or CA)**: An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Root CAs and Subordinate CAs.

**Certification Authority Authorization (or CAA)**: From RFC 9495: "The Certification Authority Authorization (CAA) DNS resource record (RR) provides a mechanism for domains to express the allowed set of Certification Authorities that are authorized to issue certificates for the domain."

**Certificate Data**: Certificate requests and data related thereto (whether obtained from the Applicant or otherwise) in the CA's possession or control or to which the CA has access.

**Certificate Management Process**: Processes, practices, and procedures associated with the use of keys, software, and hardware, by which the CA verifies Certificate Data, issues Certificates, maintains a Repository, and revokes Certificates.

**Certificate Policy (or 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.

**Certification Practice Statement (or CPS)**: One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.

**Certificate Problem Report**: Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.

**Certificate Profile**: A set of documents or files that defines requirements for Certificate content and Certificate extensions in accordance with Section 7 e.g., a section in a CA's CPS or a Certificate template file used by CA software.

**Certificate Revocation List**: A regularly updated time-stamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates.

**Certificate Type**: The S/MIME Baseline Requirements define Certificate Profiles differentiated by the type of Subject, (for example Mailbox, Organization, Sponsored, Individual).

**Control**: "Control" (and its correlative meanings, "controlled by" and "under common control with") means possession, directly or indirectly, of the power to: (1) direct the management, personnel, finances, or plans of such entity; (2) control the election of a majority of the directors; or (3) vote that portion of voting shares required for "control" under the law of the entity's Jurisdiction of Incorporation or Registration but in no case less than 10%.

**Conversion**: The process of converting text from one writing system to ASCII characters.

**Country**: Either a member of the United Nations OR a geographic region recognized as a Sovereign State by at least two UN member nations.

**Cross Certificate**: A Certificate that is used to establish a trust relationship between two Root CAs.

**CSPRNG**: A pseudo-random number generator intended for use in a cryptographic system.

**Delegated Third Party**: A Natural Person or Legal Entity that is not the CA but is authorized by the CA, and whose activities are not within the scope of the appropriate CA audits, to assist in the Certificate Management Process by performing or fulfilling one or more of the CA requirements found herein.

**Digital Identity Document**: a government-issued identity document that is issued in a machine-processable form, that is digitally signed by the issuer, and that is in purely digital form.

**Domain Label**: From RFC 8499: "An ordered list of zero or more octets that makes up a portion of a domain name. Using graph theory, a label identifies one node in a portion of the graph of all possible domain names."

**Domain Name**: An ordered list of one or more Domain Labels assigned to a node in the Domain Name System.

**Electronic Identification (eID)**: A credential containing Individual identification data and/or attributes and which is used for authentication for an online service.

**Enterprise RA**: An employee or agent of an organization unaffiliated with the CA who authorizes issuance of Certificates to that organization.

**European Unique Identifier (EUID)**: The EUID uniquely identifies officially-registered organizations, Legal Entities, and branch offices within the European Union or the European Economic Area. The EUID is specified in chapter 9 of the Annex contained in the Implementing Regulation (EU) 2021/1042 which describes rules for the application of Directive (EU) 2017/1132 "relating to certain aspects of company law (codification)".

**Expiry Date**: The "Not After" date in a Certificate that defines the end of a Certificate's validity period.

**Extant S/MIME CA**: A Subordinate CA that:

1. Is a Publicly-Trusted Subordinate CA Certificate whose `notBefore` field is before September 1, 2023 and which is included in a valid trust chain of an end entity S/MIME Certificate;
2. The CA Certificate includes no Extended Key Usage extension, contains `anyExtendedKeyUsage` in the EKU extension, or contains `id-kp-emailProtection` in the EKU extension;
3. The CA Certificate complies with the profile defined in RFC 5280. The following two deviations from the RFC 5280 profile are acceptable:
    1. The CA Certificate contains a `nameConstraints` extension that is not marked critical;
        1. The CA Certificate contains a policy qualifier of type UserNotice which contains `explicitText` that uses an encoding that is not permitted by RFC 5280 (i.e., the `DisplayText` is encoded using BMPString or VisibleString); and
4. The CA Certificate contains the `anyPolicy` identifier (2.5.29.32.0) or specific OIDs in the `certificatePolicies` extension that do not include those defined in Section 7.1.6.1 of these Requirements.

**Fully-Qualified Domain Name**: A Domain Name that includes the Domain Labels of all superior nodes in the Internet Domain Name System.
**Generation**: The S/MIME Baseline Requirements define several Generations of Certificate Profile for each Certificate Type.

**Government Entity**: A government-operated legal entity, agency, department, ministry, branch, or similar element of the government of a country, or political subdivision within such country (such as a state, province, city, county, etc.).

**Individual**: A Natural Person.

**Individual-Validated**: Refers to a Certificate Subject that includes only Individual (Natural Person) attributes, rather than attributes linked to an Organization.

**Issuing CA**: In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA.

**Jurisdiction of Incorporation**: The country and (where applicable) the state or province or locality where the organization's legal existence was established by a filing with (or an act of) an appropriate government agency or entity (e.g., where it was incorporated). In the context of a Government Entity, the country and (where applicable) the state or province where the Entity's legal existence was created by law.

**Key Compromise**: A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, or an unauthorized person has had access to it.

**Key Generation Script**: A documented plan of procedures for the generation of a CA Key Pair.

**Key Pair**: The Private Key and its associated Public Key.

**Legal Entity**: An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country's legal system.

**Linting**: A process in which the content of digitally signed data such as a Precertificate [RFC 6962], Certificate, CRL, or OCSP response, or data-to-be-signed object such as a `tbsCertificate` (as described in RFC 5280, Section 4.1.1.1) is checked for conformance with the profiles and requirements defined in these Requirements.

**Mailbox-Validated (MV)**: Refers to a Certificate Subject that is limited to (optional) `subject:emailAddress` and/or `subject:serialNumber` attributes.

**Mailbox Address**: Also Email Address. The format of a Mailbox Address is defined as a "Mailbox" as specified in Section 4.1.2 of RFC 5321 and amended by Section 3.2 of RFC 6532, with no additional padding or structure.

**Mailbox Field**: In Subscriber Certificates contains a Mailbox Address of the Subject via `rfc822Name` or `otherName` value of type `id-on-SmtpUTF8Mailbox` in the `subjectAltName` extension, or in Subordinate CA Certificates via `rfc822Name` in permittedSubtrees within the `nameConstraints` extension.

**Multi-Perspective Issuance Corroboration**: A process by which the determinations made during domain validation and CAA checking by the Primary Network Perspective are corroborated by other Network Perspectives before Certificate issuance.

**Multipurpose Profile**: The S/MIME Multipurpose Generation profiles are aligned with the more defined Strict Profiles, but with additional options for `extKeyUsage` and other extensions. This is intended to allow flexibility for crossover use cases between document signing and secure email.

**Natural Person**: An Individual; a human being as distinguished from a Legal Entity.

**Network Perspective**: Related to Multi-Perspective Issuance Corroboration. A system (e.g., a cloud-hosted server instance) or collection of network components (e.g., a VPN and corresponding infrastructure) for sending outbound Internet traffic associated with a domain control validation method and/or CAA check. The location of a Network Perspective is determined by the point where unencapsulated outbound Internet traffic is typically first handed off to the network infrastructure providing Internet connectivity to that perspective.

**Object Identifier**: A unique alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object class.

**OCSP Responder**: An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol.

**Online Certificate Status Protocol**: An online Certificate-checking protocol that enables relying-party application software to determine the status of an identified Certificate. See also OCSP Responder.

**Organization-Validated**: Refers to a Certificate Subject that includes only Organizational (Legal Entity) attributes, rather than attributes linked to an Individual.

**Parent Company**: A company that Controls a Subsidiary Company.

**Personal Name**: Personal Name is a name of an Individual Subject typically presented as `subject:givenName` and/or `subject:surname`. However, the Personal Name may be in a format preferred by the Subject, the CA, or Enterprise RA as long as it remains a meaningful representation of the Subject's verified name.

**Physical Identity Document**: a government-issued identity document issued in physical and human-readable form (such as a passport or national identity card).

**Primary Network Perspective**: The Network Perspective used by the CA to make the determination of 1) the CA's authority to issue a Certificate for the requested domain(s) or IP address(es) and 2) the Applicant's authority and/or domain authorization or control of the requested domain(s) or IP address(es).

**Private Key**: The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

**Pseudonym**: A fictitious identity that a person assumes for a particular purpose. Unlike an anonymous identity, a pseudonym can be linked to the person's real identity.

**Public Key**: The key of a Key Pair that can be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

**Public Key Infrastructure**: A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key Cryptography.

**Publicly-Trusted Certificate**: A Certificate that is trusted by virtue of the fact that its corresponding Root CA Certificate is distributed as a trust anchor in widely-available application software.

**Qualified Auditor**: A Natural Person or Legal Entity that meets the requirements of Section 8.2.

**Random Value**: A value specified by a CA to the Applicant that exhibits at least 112 bits of entropy.

**Registered Domain Name**: A Domain Name that has been registered with a Domain Name Registrar.

**Registration Authority (RA)**: Any Legal Entity that is responsible for identification and authentication of subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA MAY assist in the certificate application process or revocation process or both. When "RA" is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.

**Registration Reference**: An identifier assigned to a Legal Entity.

**Registration Scheme**: A scheme for assigning a Registration Reference meeting the requirements identified in Appendix A.

**Reliable Data Source**: An identification document or source of data used to verify Subject Identity Information that is generally recognized among commercial enterprises and governments as reliable, and which was created by a third party for a purpose other than the Applicant obtaining a Certificate.

**Reliable Method of Communication**: A method of communication, such as a postal/courier delivery address, telephone number, or email address, that was verified using a source other than the Applicant Representative.

**Relying Party**: Any Natural Person or Legal Entity that relies on a Valid Certificate. An Application Software Supplier is not considered a Relying Party when software distributed by such Supplier merely displays information relating to a Certificate.

**Repository**: An online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response.

**Requirements**: The S/MIME Baseline Requirements found in this document.

**Root CA**: The top level Certification Authority whose Root CA Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.

**Root CA Certificate**: The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.

**Sovereign State**: A state or country that administers its own government, and is not dependent upon, or subject to, another power.

**Sponsor-validated**: Refers to a Certificate Subject which combines Individual (Natural Person) attributes in conjunction with an `subject:organizationName` (an associated Legal Entity) attribute. Registration for Sponsor-validated Certificates MAY be performed by an Enterprise RA where the `subject:organizationName` is either that of the delegated enterprise, or an Affiliate of the delegated enterprise, or that the delegated enterprise is an agent of the named Subject Organization.

**Strict Profile**: The S/MIME Strict Generation profiles are the long term target profile for S/MIME Certificates with `extKeyUsage` limited to `id-kp-emailProtection`, and stricter use of Subject DN attributes and other extensions.

**Subject**: The Natural Person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a mailbox under the control and operation of the Subscriber.

**Subject Identity Information**: Information that identifies the Certificate Subject. Subject Identity Information does not include a Mailbox Address listed in the `subject:commonName` or `subject:emailAddress` fields, or in the `subjectAltName` extension.

**Subordinate CA**: A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.

**Subscriber**: A Natural Person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement or Terms of Use.

**Subscriber Agreement**: An agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties.

**Subsidiary Company**: A company that is controlled by a Parent Company.

**Supplementary Evidence**: Used in addition to authoritative evidence to strengthen the reliability of the identity verification and/or as evidence for attributes that are not evidenced by the authoritative evidence.

**Technically Constrained Subordinate CA Certificate**: A Subordinate CA Certificate which uses a combination of Extended Key Usage settings and Name Constraint settings to limit the scope within which the Subordinate CA Certificate MAY issue Certificates to Subscriber or additional Subordinate CAs.

**Terms of Use**: Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with these Requirements when the Applicant/Subscriber is an Affiliate of the CA or is the CA.

**Valid Certificate**: A Certificate that passes the validation procedure specified in RFC 5280.

**Validation Specialist**: Someone who performs the information verification duties specified by these Requirements.

**Validity Period**: From RFC 5280: “The period of time from notBefore through notAfter, inclusive.”

### 1.6.2 Acronyms

| Acronym | Meaning |
|---|---|
| CA | Certification Authority |
| CAA | Certification Authority Authorization |
| CP | Certificate Policy |
| CPS | Certification Practice Statement |
| CRL | Certificate Revocation List |
| DBA | Doing Business As |
| DNS | Domain Name System |
| ETSI | European Telecommunications Standards Institute |
| FIPS | (US Government) Federal Information Processing Standard |
| ICAO | International Civil Aviation Organization |
| ISO | International Organization for Standardization |
| MPIC | Multi-perspective issuance corroboration |
| MV | Mailbox-validated |
| 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) |
| TLS | Transport Layer Security |

### 1.6.3 References

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

ETSI EN 319 403-1, Electronic Signatures and Trust Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1 - Requirements for conformity assessment bodies assessing Trust Service Providers.

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

ETSI EN 319 411-2, Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.

ETSI EN 119 411-6, Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 6: Requirements for Trust Service Providers issuing publicly trusted S/MIME certificates.

ETSI EN 319 412-1, Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures.

ETSI EN 319 412-5, Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements.

ETSI TS 119 172-4, Electronic Signatures and Trust Infrastructures (ESI); Signature Policies;. Part 4: Signature applicability rules.

ETSI TS 119 495, Electronic Signatures and Trust Infrastructures (ESI); Sector Specific Requirements; Certificate Profiles and TSP Policy Requirements for Open Banking.

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.

ICAO DOC 9303, Machine Readable Travel Documents, Part 10, Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC), International Civil Aviation Organization, Eighth Edition, 2021.

ICAO DOC 9303, Machine Readable Travel Documents, Part 11, Security Mechanisms for MRTDs, International Civil Aviation Organization, Eighth Edition, 2021.

ISO 17065:2012, Conformity assessment — Requirements for bodies certifying products, processes and services.

ISO 17442-1:2020, Financial services — Legal entity identifier (LEI) - Part 1: Assignment.

ISO 17442-2:2020, Financial services — Legal entity identifier (LEI) - Part 2: Application in digital certificates.

Network and Certificate System Security Requirements, Version 2.0 or later. See https://cabforum.org/network-security-requirements/.

NIST SP 800-89, Recommendation for Obtaining Assurances for Digital Signature Applications.

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

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

RFC 3739, Request for Comments: 3739, Internet X.509 Public Key Infrastructure: Qualified Certificates Profile, S. Santesson, et al. March 2004.

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

RFC 4262, Request for Comments: 4262, X.509 Certificate Extension for Secure/Multipurpose Internet Mail Extensions (S/MIME) Capabilities, S. Santesson. December 2005.

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

RFC 5019, 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.

RFC 5280, 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.

RFC 6818, Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, P. Yee. January 2013.

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

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

RFC 8823, Request for Comments: 8823, Extensions to Automatic Certificate Management Environment for End-User S/MIME Certificates, A. Melnikov. April 2021.

RFC 8555, Request for Comments: 8555, Automatic Certificate Management Environment (ACME), R. Barnes et al. March 2019.

RFC 9598, Request for Comments: 9598, Internationalized Email Addresses in X.509 Certificates, A. Melnikov, et al. May 2024.

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

RFC 9495, Request for Comments: 9495, Certification Authority Authorization (CAA) Processing for Email Addresses, C. Bonnell. October 2023.

RFC 9598, Request for Comments: 9598, Internationalized Email Addresses in X.509 Certificates, A. Melnikov, et al. May 2024.

“TLS Baseline Requirements” means the current version of the CA/Browser Forum’s “Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates”. See https://cabforum.org/baseline-requirements-documents/

WebTrust for Certification Authorities, CPA Canada.

X.509, Recommendation ITU-T X.509 (10/2012) | ISO/IEC 9594-8:2014 (E), 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.

# 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 CP/CPS SHALL be structured in accordance with RFC 3647 and SHALL include all material required by RFC 3647.

*SHECA conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates published at https://www.cabforum.org. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.*

## 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.

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.

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.

## 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

SHECA issues Certificates with null and non-null subjectDNs. The constituent elements of the subjectDN conform with ITU X.500.

SHECA does not issue pseudonymous Certificates.

### 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

SHECA does not issue pseudonymous Certificates for email use.

### 3.1.4 Rules for interpreting various name forms

The name forms used in Certificate subjectDNs and issuerDNs conform to a subset of those defined and documented in RFC 2253 and ITU-TX.520.

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

| **Distinguished Name（DN）** | **Explanation** | **Content(demonstration)** |
|---|---|---|
| 1、Country(C) | The company's country name | C=CN |
| 2、Organization(O) | Company Name | O=SHECA |
| 3、Organization Unit（OU） | Unit or Department name | OU=Technical Support Center |
| 4、Common Name（CN） | Subscriber's name or email address | CN=Zhang Shan orCN=zhangshan@sheca.com |

SHECA MAY use geographic endonyms and exonyms in the subject\:localityName and subject\:stateOrProvinceName attributes. SHECA SHOULD avoid the use of archaic geographic name.

### 3.1.5 Uniqueness of names

No stipulation.

### 3.1.6 Recognition, authentication, and role of trademarks

No stipulation.

# 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 Validation of mailbox authorization or control

This section defines the permitted processes and procedures for confirming the Applicant's control of Mailbox Addresses to be included in issued Certificates.

SHECA SHALL verify that Applicant controls the email accounts associated with all Mailbox Fields referenced in the Certificate or has been authorized by the email account holder to act on the account holder's behalf.

SHECA SHALL NOT delegate the verification of mailbox authorization or control.

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

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

### 3.2.2.1 Validating authority over mailbox via domain

SHECA does not support this validation method.

### 3.2.2.2 Validating control over mailbox via email

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

The verification process is as below,

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

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

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

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

The Random Value is unique in each email. The Random Value remains valid for use in a confirming response for no more than 24 hours from its creation.

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

#### 3.2.2.3 Validating applicant as operator of associated mail server(s)

SHECA does not support this validation method.

#### 3.2.2.4 Validating control over mailbox using ACME extensions

SHECA does not support this validation method.

### 3.2.3 Authentication of organization identity

The following requirements SHALL be fulfilled to authenticate Organization identity included in the `Organization-validated` and `Sponsor-validated` profiles.

#### 3.2.3.1 Attribute collection of organization identity

SHECA SHALL collect and retain evidence supporting the following identity attributes for the Organization:

1. Formal name of the Legal Entity;
2. A registered Assumed Name for the Legal Entity (if included in the Subject);
3. An Affiliate of the Legal Entity as described in Section 7.1.4.2.2 (if included in the Subject as an `subject:organizationalUnitName`);
4. An address of the Legal Entity (if included in the Subject);
5. Jurisdiction of Incorporation or Registration of the Legal Entity; and
6. Identifier and type of identifier for the Legal Entity.

The identifier SHALL be included in the Certificate `subject:organizationIdentifier` as specified in Section 7.1.4.2.2 .

#### 3.2.3.2 Validation of organization identity

If an Attestation is used as evidence for the validation of the attributes described in this section, then the Attestation SHALL be verified for authenticity as described in Section 3.2.8.

#### 3.2.3.2.1 Verification of name, address, and identifier

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

1. A government agency in the jurisdiction of the Legal Entity's creation, existence, or recognition;
2. A Legal Entity Identifier (LEI) data reference;
3. A site visit by the CA or a third party who is acting as an agent for the CA; or
4. An Attestation which includes a copy of supporting documentation used to establish the Applicant's legal existence (such as a certificate of registration, articles of incorporation, operating agreement, statute, or regulatory act) and its current status.

SHECA MAY use the same documentation or communication described in 1 through 4 above to verify both the Applicant's identity and address.
In cases 1 and 4 above, SHECA SHALL verify that the status of the Applicant is not designated by labels such as "ceased," "inactive," "invalid," "not current," or the equivalent.

In case 2 above when LEI data reference is used, SHECA SHALL verify that the RegistrationStatus is ISSUED and the EntityStatus is ACTIVE. SHECA SHALL only allow use of an LEI if the ValidationSources entry is FULLY_CORROBORATED. An LEI SHALL NOT be used if ValidationSources entry is PARTIALLY_CORROBORATED, PENDING, or ENTITY_SUPPLIED_ONLY.

#### 3.2.3.2.2 Verification of assumed name

Applicants MAY request an Assumed Name to be included in the Certificate. SHECA SHALL verify that:

1. The Applicant has registered its use of the Assumed Name with the appropriate government agency for such filings in the jurisdiction of its incorporation or registration; and
2. The Assumed Name filing continues to be valid.

SHECA MAY rely on an Attestation that indicates the Assumed Name under which the Applicant conducts business, the government agency with which the Assumed Name is registered, and that such filing continues to be valid.

### 3.2.3.3 Disclosure of verification sources

SHECA SHALL verify the Registration Reference to be included in the Certificate from a register that is maintained or authorized by the relevant government agency. SHECA discloses the authorized sources it uses to verify the Applicant's creation, existence, or recognition in the repository available on:

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

Nothing in these Requirements prohibits the use of third-party vendors to obtain regularly-updated and current information from the government register provided that the third party obtains the information directly from the government.

In the case of a LEI data reference, the CA or RA SHALL verify the associated data record with the Global Legal Entity Identifier Foundation.

## 3.2.4 Authentication of individual identity

When an email address is present as the certificate subject, SHECA shall reasonably verify that the individual applicant has control over the email address.

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

a. Given name(s) and surname(s), which SHALL be current names;

b. Title (if used);

c. Address (if displayed in Subject); and

d. Further information as needed to uniquely identify the Applicant.

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

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

SHECA verifies the certificate request with the Applicant using a Reliable Method of Communication.

### 3.2.4.1 Attribute collection of individual identity

1. **From a physical identity document**

- SHECA accepts only government-issued passports, identity cards, driver's licenses, military IDs, and other official identity documents of comparable reliability as evidence for individual identity attributes.
- All accepted physical identity documents must contain a face photo and/or other information that can be compared with the Applicant's physical appearance.

### 3.2.4.2 Validation of individual identity

SHECA or its RA SHALL validate all identity attributes of the Individual to be included in the Certificate.

If the identity document has an explicit validity period, SHECA SHALL verify that the identity validation time falls within this period.

SHECA or its RA MAY reuse existing evidence for individual identity validation, provided that such reuse complies with the age restrictions specified in Section 4.2.1.

1. **Validation of a physical identity document (In-Person & Remote Video Modes)**

- **Document Presentation Requirement**: The original physical identity document must be presented. For in-person verification, the Applicant shall provide the original document face-to-face. For remote video verification, the Applicant shall hold the original document in hand and present it in real-time in front of the camera.

- **Genuineness Check**: SHECA shall implement procedures to confirm that the presented identity document is genuine, non-counterfeited, and non-falsified/modified.
- **Visual Comparison**: The SHECA or RA registration agent shall conduct a visual comparison between the Applicant's physical appearance and the face photo and/or other identifying information on the identity document. This applies to both in-person and remote video verification (via real-time camera feed).
- **Authoritative Reference Access**: The SHECA or RA registration agent shall have access to authoritative sources detailing the appearance and validation criteria for all accepted identity document types.
- **Record Retention**: SHECA or its RA SHALL retain sufficient information to evidence the completion of the identity validation process and the verified attributes. Mandatory recorded information includes: document issuer, document validity period, document unique identification number, and all verified identity attributes.
- **Process Combination**: Automated and manual processes MAY be used in combination. For example, SHECA or its RA may deploy automated tools to assist registration agents, or implement an automated process that falls back to a registration agent for uncertain results.

### 3.2.5 Non-Verified Subscriber information

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

### 3.2.6 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.

### 3.2.7 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.

SHECA has no cross-certified S/MIME certificates.

### 3.2.8 Reliability of verification sources

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

1. The age of the information provided,

2. The frequency of updates to the information source,

3. The data provider and purpose of the data collection,

4. The public accessibility of the data availability, and

5. The relative difficulty in falsifying or altering the data.

For S/MIME certificates, SHECA may reuse completed validations and/or supporting evidence performed in accordance within the following limits:

1. Completed validation of mailbox server control shall be obtained no more than 398 days prior to issuing the certificate.

2. Completed validation of mailbox control shall be obtained no more than 30 days prior to issuing the certificate.

3. Completed validation of organization identity or individual identity shall be obtained no more than 825 days prior to issuing the certificate.

## 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

### 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.

### 4.1.2 Enrollment process and responsibilities

Prior to the issuance of a Certificate, SHECA SHALL obtain the following documentation from the Applicant:

1. A Certificate Request; and
2. An executed Subscriber Agreement and/or Terms of Use.

The Certificate Request and Subscriber Agreement or Terms of Use SHALL be in a form prescribed by SHECA and SHALL comply with these Requirements including Section 9.6.3. SHECA SHOULD obtain any additional documentation the CA determines necessary to fulfill these Requirements.
The Certificate Request SHALL contain a request from, or on behalf of, the Applicant for the issuance of a Certificate, and a certification by, or on behalf of, the Applicant that all of the information contained therein is correct.

One Certificate Request MAY suffice for multiple Certificates to be issued to the same Applicant, subject to the validation reuse periods described in Section 4.2.1, provided that each Certificate is supported by a valid, current Certificate Request signed by the appropriate Applicant Representative on behalf of the Applicant.

SHECA may rely on a previously verified Certificate Request to issue a replacement Certificate if:

1. The previous Certificate being referenced was not revoked;
2. The expiration date of the replacement Certificate is the same as the previous Certificate being referenced; and

3. The Subject Information of the Certificate is the same as the previous Certificate being referenced.

## 4.2 Certificate application processing

### 4.2.1 Performing identification and authentication functions

After SHECA and its RA receive a subscriber's certificate application, SHECA shall identify and authenticate the subscriber's identity in accordance with the requirements in Section 3.2 of this CP/CPS.

Based on prior rejected certificate requests or revoked certificates due to suspicion of phishing or other fraud purpose or other concerns, SHECA establishes and maintains a list of certificate high-risk database, which will be queried when SHECA accepts a certificate application. For subscribers that exist in the list, SHECA will perform additional validation.

### 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.

#### 4.2.2.1 Certification authority authorization

SEHCA performs CAA check according to RFC 9495: Certification Authority Authorization (CAA) Processing for Email Addresses.

Accepted issuer domain name: sheca.com

Starting on September 15, 2024 prior to issuing a Certificate that includes a Mailbox Address, the CA SHOULD retrieve and process CAA records in accordance with Section 4 of RFC 9495: Certification Authority Authorization (CAA) Processing for Email Addresses.

Starting on March 15, 2025 prior to issuing a Certificate that includes a Mailbox Address, the CA SHALL retrieve and process CAA records in accordance with Section 4 of RFC 9495: Certification Authority Authorization (CAA) Processing for Email Addresses.

When processing CAA records, CAs SHALL process the `issuemail` property tag as specified in RFC 9495. Additional property tags MAY be supported, but SHALL NOT conflict with or supersede the authorizations to issue S/MIME Certificates as specified in the `issuemail` property tag.

If the CA issues a Certificate following a CAA check, they SHALL do so within the TTL of the CAA record, or 8 hours, whichever is greater. This stipulation does not prevent the CA from checking CAA records at any other time.

If the Certificate includes more than one Mailbox Address, then the CA SHALL perform the above procedure for each Mailbox Address.

The CA SHALL NOT issue a Certificate unless the CA determines that Certificate Request is consistent with the applicable CAA RRset. The CA SHALL log all actions taken, if any, consistent with its CAA processing practice.

CAs MUST document potential issuances that were prevented by a CAA record in sufficient detail to provide feedback to the CA/Browser Forum on the circumstances, and SHOULD dispatch reports of such issuance requests to the contact(s) stipulated in the CAA iodef record(s), if present. CAs are not expected to support URL schemes in the iodef record other than mailto: or https:.

#### 4.2.2.1.1 DNSSEC validation of CAA records

Effective March 15, 2026 DNSSEC validation back to the IANA DNSSEC root trust anchor MUST be performed on all DNS queries associated with CAA record lookups performed by the Primary Network Perspective. The DNS resolver used for all DNS queries associated with CAA record lookups performed by the Primary Network Perspective MUST:

- perform DNSSEC validation using the algorithm defined in RFC 4035 Section 5; and
- support NSEC3 as defined in RFC 5155; and
- support SHA-2 as defined in RFC 4509 and RFC 5702; and
- properly handle the security concerns enumerated in RFC 6840 Section 4.

Effective March 15, 2026 CAs MUST NOT use local policy to disable DNSSEC validation on any DNS query associated with CAA record lookups.
Effective March 15, 2026 DNSSEC-validation errors observed by the Primary Network Perspective (e.g., SERVFAIL) MUST NOT be treated as permission to issue.

DNSSEC validation back to the IANA DNSSEC root trust anchor MAY be performed on all DNS queries associated with CAA record lookups performed by Remote Network Perspectives as part of Multi-Perspective Issuance Corroboration.

DNSSEC validation back to the IANA DNSSEC root trust anchor is considered outside the scope of self-audits performed to fulfill the requirements in Section 8.7.

### 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.

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.

Effective March 15, 2025 SHECA SHOULD implement a Linting process testing compliance with these Requirements for S/MIME Certificates. Effective September 15, 2025 SHECA SHALL implement a Linting process testing compliance with these Requirements for S/MIME Certificates.

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

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

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

SHECA SHOULD use the Linting tools that have been widely adopted by the industry (see https://cabforum.org/resources/tools/).

### 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 SHALL revoke a Certificate within 24 hours if one or more of the following occurs:

1. The Subscriber requests in writing that the CA revoke the Certificate;
2. The Subscriber notifies the CA that the original Certificate Request was not authorized and does not retroactively grant authorization;
3. The CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise;
4. The CA is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate (such as a Debian weak key, see https://wiki.debian.org/SSLkeys);
5. The CA obtains evidence that the validation of domain authorization or mailbox control for any Mailbox Address in the Certificate should not be relied upon.

SHECA SHOULD revoke a Certificate within 24 hours and SHALL revoke a Certificate within 5 days if one or more of the following occurs:

1. The Certificate no longer complies with the requirements of Section 6.1.5 and Section 6.1.6;
2. The CA obtains evidence that the Certificate was misused;
3. The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use;
4. The CA is made aware of any circumstance indicating that use of an email address or Fully-Qualified Domain Name in the Certificate is no longer legally permitted (e.g., a court or arbitrator has revoked the right to use an email address or Domain Name, a relevant licensing or services agreement between the Subscriber has terminated, or the account holder has failed to maintain the active status of the email address or Domain Name);
5. The CA is made aware of a material change in the information contained in the Certificate;
6. The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's CP and/or CPS;
7. The CA determines or is made aware that any of the information appearing in the Certificate is inaccurate;
8. The CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository;
9. Revocation is required by the CA's CP and/or CPS; or

10. The CA is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed.

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 requests revocation in writing;
2. The Subordinate CA notifies the Issuing CA that the original Certificate Request was not authorized and does not retroactively grant authorization;
3. The Issuing CA 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 of Section 6.1.5 and Section 6.1.6;
4. The Issuing CA obtains evidence that the Certificate was misused;
5. The Issuing CA is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with this document or the applicable CP and/or CPS;
6. The Issuing CA determines that any of the information appearing in the Certificate is inaccurate or misleading;
7. The Issuing CA or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
8. The Issuing CA's or Subordinate CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository; or
9. Revocation is required by the Issuing CA's CP and/or CPS.

### 4.9.2 Who can request revocation

The Subscriber, RA, or Issuing CA can initiate revocation. Additionally, Subscribers, Relying Parties, Application Software Suppliers, and other third parties MAY submit Certificate Problem Reports informing the Issuing CA of reasonable cause to revoke a 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

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.

### 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 S/MIME 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.

The business continuity plan SHALL include:

1. The conditions for activating the plan;
2. Emergency procedures;
3. Fallback procedures;
4. Resumption procedures;
5. A maintenance schedule for the plan;
6. Awareness and education requirements;
7. The responsibilities of the individuals;
8. Recovery time objective (RTO);
9. Regular testing of contingency plans;
10. The CA’s plan to maintain or restore the CA’s business operations in a timely manner following interruption to or failure of critical business processes;
11. A requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location;
12. What constitutes an acceptable system outage and recovery time;

13. How frequently backup copies of essential business information and software are taken;
14. The distance of recovery facilities to the CA's main site; and
15. Procedures for securing its facility to the extent possible during the period of time following a disaster and prior to restoring a secure environment either at the original or a remote site.

### 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  RA Key Pair Generation

No stipulation.

#### 6.1.1.3 Subscriber key pair generation

SHECA SHALL reject a Certificate Request if one or more of the following conditions are met:

1. The Key Pair does not meet the requirements set forth in Section 6.1.5 and/or Section 6.1.6;
2. There is clear evidence that the specific method used to generate the Private Key was flawed;
3. The CA is aware of a demonstrated or proven method that exposes the Applicant's Private Key to compromise;
4. The CA has previously been made aware that the Applicant's Private Key has suffered a Key Compromise, such as through the provisions of Section 4.9.1.1;
5. The CA is aware of a demonstrated or proven method to easily compute the Applicant's Private Key based on the Public Key (such as a Debian weak key, see https://wiki.debian.org/SSLkeys).

### 6.1.2 Private key delivery to subscriber

SHECA does not generate the Private Key on behalf of the Subscriber.

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

### 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

For RSA key pairs the CA SHALL:

- Ensure that the modulus size, when encoded, is at least 2048 bits; and
- Ensure that the modulus size, in bits, is evenly divisible by 8.

For ECDSA key pairs, the CA SHALL:

- Ensure that the key represents a valid point on the NIST P-256, NIST P-384, or NIST P-521 elliptic curve.

### 6.1.6 Public key parameters generation and quality checking

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

For ECDSA key pairs: the CA SHOULD confirm the validity of all keys using either the ECC Full Public Key Validation Routine or the ECC Partial Public Key Validation Routine. (See NIST SP 800-56A: Revision 2, Sections 5.6.2.3.2 and 5.6.2.3.3.)

### 6.1.7 Key usage purposes

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

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

## 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 root and 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

| Generation | Certificate Maximum Validity Period |
|---|---|
| Strict and Multipurpose | 825 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.

### 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 content and extensions; application of RFC 6818

This section specifies the additional requirements for Certificate content and extensions for Certificates.

#### 7.1.2.1 Root CA certificates

1. `basicConstraints` (SHALL be present)

   This extension SHALL be marked critical. The `cA` field SHALL be set true. The `pathLenConstraint` field SHOULD NOT be present.

2. `keyUsage` (SHALL be present)

   This extension SHALL be marked critical. Bit positions for `keyCertSign` and `cRLSign` SHALL be set. If the Root CA Private Key is used for signing OCSP responses, then the `digitalSignature` bit SHALL be set.

3. `certificatePolicies` (SHOULD NOT be present)

   This extension SHOULD NOT be present.

4. `extKeyUsage` (SHALL NOT be present)

   This extension SHALL NOT be present.

5. `subjectKeyIdentifier` (SHALL be present)

   This extension SHALL NOT be marked critical. It SHALL contain a value that is included in the `keyIdentifier` field of the `authorityKeyIdentifier` extension in Certificates issued by the Root CA.

#### 7.1.2.2 Subordinate CA certificates

1. The issuance of end entity S/MIME Certificates by Extant S/MIME CAs is described in Appendix B.
    1. `certificatePolicies` (SHALL be present)

       This extension SHOULD NOT be marked critical.

       All `policyIdentifier`s included in this extension SHALL be included in accordance with Section 7.1.6.3.

       If the value of this extension includes a `PolicyInformation` which contains a qualifier of type `id-qt-cps` (OID: 1.3.6.1.5.5.7.2.1), then the value of the qualifier SHALL be a HTTP or HTTPS URL for the Issuing CA's CP and/or CPS, Relying Party Agreement, or other pointer to online policy information provided by the Issuing CA. If a qualifier of type `id-qt-unotice` (OID: 1.3.6.1.5.5.7.2.2) is included, then it SHALL contain `explicitText` and SHALL NOT contain `noticeRef`.

        1. `cRLDistributionPoints` (SHALL be present)

           This extension SHALL NOT be marked critical. It SHALL contain the HTTP URL of the CA's CRL service.

        2. `authorityInformationAccess` (SHOULD be present)

           This extension SHALL NOT be marked critical.

           It SHOULD contain the HTTP URL of the Issuing CA Certificate (`accessMethod` = 1.3.6.1.5.5.7.48.2). It MAY contain the HTTP URL of the Issuing CA OCSP responder (`accessMethod` = 1.3.6.1.5.5.7.48.1).

3. `basicConstraints` (SHALL be present)

   This extension SHALL be marked critical. The `cA` field SHALL be set true. The `pathLenConstraint` field MAY be present.

4. `keyUsage` (SHALL be present)

   This extension SHALL be marked critical. Bit positions for `keyCertSign` and `cRLSign` SHALL be set. If the Subordinate CA Private Key is used for signing OCSP responses, then the `digitalSignature` bit SHALL be set.

5. `nameConstraints` (MAY be present)

   This extension SHOULD be marked critical[1].

6. `extKeyUsage` (MAY be present for Cross Certificates; SHALL be present otherwise)

   For Cross Certificates that share a Subject Distinguished Name and Subject Public Key with a Root CA Certificate operated in accordance with these Requirements, this extension MAY be present. If present, this extension SHOULD NOT be marked critical. This extension SHALL only contain usages for which the Issuing CA has verified the Cross Certificate is authorized to assert. This extension SHALL NOT contain the `anyExtendedKeyUsage` usage.

   For all other Subordinate CA Certificates, including Technically Constrained Subordinate CA Certificates, this extension SHALL be present and SHOULD NOT be marked critical[2].

   For Subordinate CA Certificates that will be used to issue S/MIME Certificates, the value `id-kp-emailProtection` SHALL be present. The values `id-kp-serverAuth`, `id-kp-codeSigning`, `id-kp-timeStamping`, and `anyExtendedKeyUsage` SHALL NOT be present. Other values MAY be present.

7. `authorityKeyIdentifier` (SHALL be present)

   This extension SHALL NOT be marked critical. It SHALL contain a `keyIdentifier` field and it SHALL NOT contain a `authorityCertIssuer` or `authorityCertSerialNumber` field.

8. `subjectKeyIdentifier` (SHALL be present)

   This extension SHALL NOT be marked critical. It SHALL contain a value that is included in the `keyIdentifier` field of the `authorityKeyIdentifier` extension in Certificates issued by the Subordinate CA.

#### 7.1.2.3 Subscriber certificates

1. `certificatePolicies` (SHALL be present)

   This extension SHOULD NOT be marked critical. It SHALL include exactly one of the reserved `policyIdentifiers` listed in Section 7.1.6.1, and MAY contain one or more identifiers documented by the CA in its CP and/or CPS.

   If the value of this extension includes a `PolicyInformation` which contains a qualifier of type `id-qt-cps` (OID: 1.3.6.1.5.5.7.2.1), then the value of the qualifier SHALL be a HTTP or HTTPS URL for the Issuing CA's CP and/or CPS, Relying Party Agreement, or other pointer to online policy information provided by the Issuing CA. If a qualifier of type `id-qt-unotice` (OID: 1.3.6.1.5.5.7.2.2) is included, then it SHALL contain `explicitText` and SHALL NOT contain `noticeRef`.

2. `cRLDistributionPoints` (SHALL be present)

This extension SHOULD NOT be marked critical. It SHALL contain at least one `distributionPoint` whose `fullName` value includes a GeneralName of type `uniformResourceIdentifier` that includes a URI where the Issuing CA's CRL can be retrieved.

| Generation | Allowed URI scheme | | :--------- | :---------- | | Strict | Every `uniformResourceIdentifier` SHALL have the URI scheme HTTP. Other schemes SHALL NOT be present. |

3. `authorityInformationAccess` (SHOULD be present)

   This extension SHALL NOT be marked critical.

   1. `id-ad-ocsp`

      The `authorityInformationAccess` extension MAY contain one or more `accessMethod` values of type `id-ad-ocsp` that specifies the URI of the Issuing CA's OCSP responder.

      | Generation | Allowed URI scheme |

      ```
      | :--------- | :----------------------------------------------------------------
        ------------------------------------ |
        | Strict     | When provided, every accessMethod SHALL have the URI scheme HTTP.
      Other schemes SHALL NOT be present. |
      ```

      1. `id-ad-caIssuers`

         The `authorityInformationAccess` extension SHOULD contain at least one `accessMethod` value of type `id-ad-caIssuers` that specifies the URI of the Issuing CA's Certificate.

         | Generation | Allowed URI scheme | | :--------- | :---------- | | Strict | When provided, every `accessMethod` SHALL have the URI scheme HTTP. Other schemes SHALL NOT be present. |

4. `basicConstraints` (optional)

   This extension MAY be present. The `cA` field SHALL NOT be true. `pathLenConstraint` field SHALL NOT be present.

5. `keyUsage` (SHALL be present)

   This extension SHOULD be marked critical.

   | Generation | `rsaEncryption` | `id-ecPublicKey` | `id-Ed25519` and `id-Ed448` | | :--------- | :---------- | | Strict | For signing only, bit positions SHALL be set for `digitalSignature` and MAY be set for `nonRepudiation`. For key management only, bit positions SHALL be set for `keyEncipherment`. For dual use, bit positions SHALL be set for `digitalSignature` and `keyEncipherment` and MAY be set for `nonRepudiation`. | For signing only, bit positions SHALL be set for `digitalSignature` and MAY be set for `nonRepudiation`. For key management only, bit positions SHALL be set for `keyAgreement` and

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

Other bit positions SHALL NOT be set.

| **Generation** | **`id-ml-dsa`** | **`id-ml-kem`** |
|---|---|---|
| Strict | Bit positions SHALL be set for `digitalSignature` and MAY be set for `nonRepudiation`. Other bit positions SHALL NOT be set. | `keyEncipherment` SHALL be the only key usage set. |

1. `extKeyUsage` (SHALL be present)

   | Generation | `KeyPurposeId` | | :--------- | :---------- | | Strict | `id-kp-emailProtection` SHALL be present. Other values SHALL NOT be present. |

   The values `id-kp-serverAuth`, `id-kp-codeSigning`, `id-kp-timeStamping`, and `anyExtendedKeyUsage` SHALL NOT be present.

2. `authorityKeyIdentifier` (SHALL be present)

   This extension SHALL NOT be marked critical. The `keyIdentifier` field SHALL be present. `authorityCertIssuer` and `authorityCertSerialNumber` fields SHALL NOT be present.

3. `subjectAlternativeName` (SHALL be present)

   This extension SHOULD NOT be marked critical unless the `subject` field is an empty sequence.

   The value of this extension SHALL be encoded as specified in Section 7.1.4.2.1.

4. `smimeCapabilities` (optional)

   This extension MAY be present and SHALL NOT be marked critical. May indicate cryptographic capabilities of the sender of a signed S/MIME message, defined in RFC 4262.

5. `subjectDirectoryAttributes` (optional)

   | Generation | `subjectDirectoryAttributes` | | :--------- | :------------------------- | | Strict | Prohibited |

   This extension MAY be present. This extension is used to contain verified attributes which are not part of the Subject's Distinguished Name such as dateOfBirth, placeOfBirth, gender, countryOfCitizenship, or countryOfResidence in accordance with RFC 3739 Section 3.2.2.

6. qcStatements (optional)

   This extension MAY be present and SHALL NOT be marked critical. Indicates a Certificate that is issued as Qualified within a defined legal framework from an identified country or set of countries in accordance with RFC 3739 Section 3.2.6 and/or ETSI EN 319 412-5, Section 4.

7. Legal Entity Identifier (optional)

   | Generation | LEI | | :---------------------- | :---------- | | `Mailbox-validated` | Prohibited | | `Organization-validated` | LEI (1.3.6.1.4.1.52266.1) MAY be present and SHALL NOT be marked critical. Role

(1.3.6.1.4.1.52266.2) SHALL NOT be present. | | `Sponsor-validated` | LEI (1.3.6.1.4.1.52266.1) or for role (1.3.6.1.4.1.52266.2) MAY be present and SHALL NOT be marked critical. | | `Individual-validated` | Prohibited |

The Legal Entity Identifier (LEI) is a 20-character, alpha-numeric code used in accordance with ISO 17442-1:2020, Clause 6 and ISO 17442-2:2020, Clause 4.

The CA SHALL verify that the RegistrationStatus for the LEI record is ISSUED and the EntityStatus is ACTIVE. The CA SHALL only allow use of an LEI if the ValidationSources entry is FULLY_CORROBORATED. An LEI SHALL NOT be used if ValidationSources entry is PARTIALLY_CORROBORATED, PENDING, or ENTITY_SUPPLIED_ONLY.

In cases where the "role" LEI is used, the CA SHALL verify that the LEI data reference is assigned to the Individual Subject whose identity has been verified in accordance with Section 3.2.4.

8. Adobe Extensions (optional)

   | Generation | Adobe Extensions | | :--------- | :---------- | | Strict | Prohibited |

9. `subjectKeyIdentifier` (SHOULD be present)

   This extension SHALL NOT be marked critical. It SHOULD contain a value that is derived from the Public Key included in the Subscriber Certificate.

#### 7.1.2.4 All certificates

All fields and extensions SHALL be set in accordance with RFC 5280. The CA SHALL NOT issue a Certificate that contains a `keyUsage` flag, `extKeyUsage` value, Certificate extension, or other data not specified in Section 7.1.2.1, Section 7.1.2.2, or Section 7.1.2.3 unless the CA is aware of a reason for including the data in the Certificate. If the CA includes fields or extensions in a Certificate that are not specified but are otherwise permitted by these Requirements, then the CA SHALL document the processes and procedures that the CA employs for the validation of information contained in such fields and extensions in its CP and/or CPS.

CAs SHALL NOT issue a Certificate with:

1. Extensions that do not apply in the context of the public Internet (such as an `extKeyUsage` value for a service that is only valid in the context of a privately managed network), unless:
   1. such value 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; or
      2. the extension is defined within an open standards specification and intended for use by other organizations. A Certificate that includes such an extension MUST conform to the specifications of the open standard and of these Requirements.
2. Field or extension values which have not been validated according to the processes and procedures described in these Requirements or the CA's CP and/or CPS.

### 7.1.3 Algorithm object identifiers

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

#### 7.1.3.1 SubjectPublicKeyInfo

##### 7.1.3.1.1 RSA

The CA SHALL indicate an RSA key using the rsaEncryption (OID: 1.2.840.113549.1.1.1) algorithm identifier. The parameters SHALL be present, and SHALL be an explicit NULL.

The CA SHALL NOT use a different algorithm, such as the id-RSASSA-PSS (OID: 1.2.840.113549.1.1.10) algorithm identifier, to indicate an RSA key.

When encoded, the `AlgorithmIdentifier` for RSA keys SHALL be byte-for-byte identical with the following hex-encoded bytes: `300d06092a864886f70d0101010500`

##### 7.1.3.1.2 ECDSA

The CA SHALL indicate an ECDSA key using the id-ecPublicKey (OID: 1.2.840.10045.2.1) algorithm identifier. The parameters SHALL use the `namedCurve` encoding.

- For P-256 keys, the `namedCurve` SHALL be secp256r1 (OID: 1.2.840.10045.3.1.7).
- For P-384 keys, the `namedCurve` SHALL be secp384r1 (OID: 1.3.132.0.34).
- For P-521 keys, the `namedCurve` SHALL be secp521r1 (OID: 1.3.132.0.35).

When encoded, the `AlgorithmIdentifier` for ECDSA keys SHALL be byte-for-byte identical with the following hex-encoded bytes:

- For P-256 keys, `301306072a8648ce3d020106082a8648ce3d030107`.
- For P-384 keys, `301006072a8648ce3d020106052b81040022`.
- For P-521 keys, `301006072a8648ce3d020106052b81040023`.

#### 7.1.3.2 Signature AlgorithmIdentifier

All objects signed by a CA Private Key SHALL 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.
- The `signature` field of a TBSCertificate (for example, as used by a Certificate).
- The `signatureAlgorithm` field of a CertificateList
- The `signature` field of a TBSCertList
- The `signatureAlgorithm` field of a BasicOCSPResponse.

No other encodings are permitted for these fields.

##### 7.1.3.2.1 RSA

The CA SHALL use one of the following signature algorithms and encodings. When encoded, the `AlgorithmIdentifier` SHALL be byte-for-byte identical with the specified hex-encoded bytes.

- RSASSA-PKCS1-v1_5 with SHA-256:

Encoding: `300d06092a864886f70d01010b0500`.

- RSASSA-PKCS1-v1_5 with SHA-384:

  Encoding: `300d06092a864886f70d01010c0500`.

- RSASSA-PKCS1-v1_5 with SHA-512:

  Encoding: `300d06092a864886f70d01010d0500`.

- RSASSA-PSS with SHA-256, MGF-1 with SHA-256, and a salt length of 32 bytes:

  Encoding:

```
304106092a864886f70d01010a3034a00f300d060960864801650304020 1
  0500a11c301a06092a864886f70d010108300d060960864801650304020 1
  0500a203020120
```

- RSASSA-PSS with SHA-384, MGF-1 with SHA-384, and a salt length of 48 bytes:

  Encoding:

```
304106092a864886f70d01010a3034a00f300d060960864801650304020 2
  0500a11c301a06092a864886f70d010108300d060960864801650304020 2
  0500a203020130
```

- RSASSA-PSS with SHA-512, MGF-1 with SHA-512, and a salt length of 64 bytes:

  Encoding:

```
304106092a864886f70d01010a3034a00f300d060960864801650304020 3
  0500a11c301a06092a864886f70d010108300d060960864801650304020 3
  0500a203020140
```

#### 7.1.3.2.2 ECDSA

The CA SHALL use the appropriate signature algorithm and encoding based upon the signing key used.

If the signing key is P-256, the signature SHALL use ECDSA with SHA-256. When encoded, the `AlgorithmIdentifier` SHALL be byte-for-byte identical with the following hex-encoded bytes: `300a06082a8648ce3d040302`.

If the signing key is P-384, the signature SHALL use ECDSA with SHA-384. When encoded, the `AlgorithmIdentifier` SHALL be byte-for-byte identical with the following hex-encoded bytes: `300a06082a8648ce3d040303`.

If the signing key is P-521, the signature SHALL use ECDSA with SHA-512. When encoded, the `AlgorithmIdentifier` SHALL be byte-for-byte identical with the following hex-encoded bytes: `300a06082a8648ce3d040304`.

### 7.1.4 Name forms

Attribute values SHALL be encoded according to RFC 5280.

### 7.1.5 Name constraints

For a Subordinate CA Certificate to be considered Technically Constrained, the Certificate SHALL include an Extended Key Usage (EKU) extension specifying all extended key usages for which the Subordinate CA Certificate is authorized to issue Certificates. The `anyExtendedKeyUsage` KeyPurposeId SHALL NOT appear within this extension.

If the Subordinate CA Certificate includes the `id-kp-emailProtection` extended key usage, then for the Subordinate CA Certificate to be considered Technically Constrained it SHALL include the `nameConstraints` X.509v3 extension with constraints on `rfc822Name` and `directoryName` as follows:

1. For each `rfc822Name` in `permittedSubtrees`, each `rfc822Name` SHALL contain either a FQDN or a U+002E FULL STOP (“.”) character followed by a FQDN. The `rfc822Name` SHALL NOT contain an email address. The CA SHALL confirm that the Applicant has registered the FQDN contained in the `rfc822Name` or has been authorized by the domain registrant to act on the registrant’s behalf in line with the verification practices of Section 3.2.2.3.
2. For each `directoryName` in `permittedSubtrees`, the CA SHALL confirm the Applicant’s and/or Subsidiary’s Organizational name and location such that end entity Certificates issued from the Subordinate CA Certificate will be in compliance with Section 7.1.2.4.

### 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

SHECA SHALL undergo an audit in accordance with one of the following schemes:

1. For Audit Periods starting before the Effective Date defined in Section 1.2.1 of the first version of these Requirements, “WebTrust for CAs v2.2.2 or newer”; or
2. For Audit Periods starting after the Effective Date defined in Section 1.2.1 of the first version of these Requirements, “WebTrust for CAs v2.2.2 or newer” AND “WebTrust for S/MIME Baseline Requirements v1.0.0 or newer”; or
3. For Audit Periods starting after April 1, 2025, “WebTrust for CAs v2.2.2 or newer” AND “WebTrust for S/MIME Baseline Requirements v1.0.0 or newer” AND “WebTrust for Network Security v2.0 or newer”; or
4. ETSI TS 119 411-6 v1.1.1 or newer, which includes normative references to ETSI EN 319 401, ETSI EN 319 411-1 and ETSI EN 319 411-2 (the latest version of the referenced ETSI documents should be applied); or
5. If a Government CA is required by its Certificate Policy to use a different internal audit scheme, it MAY use such scheme provided that the audit either
    1. encompasses all requirements of one of the above schemes; or
        1. consists of comparable criteria that are available for public review. Whichever scheme is chosen, it SHALL incorporate periodic monitoring and/or accountability procedures to ensure that its audits continue to be conducted in accordance with the requirements of the scheme.

The audit SHALL be conducted by a Qualified Auditor, as specified in Section 8.2.

## 8.5 Actions taken as a result of deficiency

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.

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

During the period in which SHECA issues Certificates, SHECA SHALL monitor adherence to its CP/CPS and these Requirements and control its service quality by performing self audits on at least a quarterly basis against a randomly selected sample including a minimum of the greater of thirty (30) Certificates or three percent (3%) of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken.

Effective March 15, 2025 SHECA SHOULD use a Linting process to verify the technical accuracy of Certificates within the selected sample set independently of previous linting performed on the same Certificates.

## 8.8 Review of delegated parties

SHECA does not have delegated parties.

# 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.

### 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

By issuing a Certificate, SHECA makes the warranties listed herein to the following Certificate Beneficiaries:

1. The Subscriber that is a party to the Subscriber Agreement or Terms of Use for the Certificate;
2. All Application Software Suppliers with whom the Root CA has entered into a contract for inclusion of its Root CA Certificate in software distributed by such Application Software Supplier; and
3. All Relying Parties who reasonably rely on a Valid Certificate.

The Certificate Warranties specifically include, but are not limited to, the following:

1. **Right to Use Mailbox Address**: That, at the time of issuance, the CA:
    1. implemented a procedure for verifying that the Applicant either had the right to use, or had control of, the Mailbox Addresses listed in the Certificate's `subject` field and `subjectAltNam e` extension (or was delegated such right or control by someone who had such right to use or control);
        1. followed the procedure when issuing the Certificate; and
        2. accurately described the procedure in the CA's CP and/or CPS;
2. **Authorization for Certificate**: That, at the time of issuance, the CA:
    1. implemented a procedure for verifying that the Subject authorized the issuance of the Certificate and that the Applicant Representative is authorized to request the Certificate on behalf of the Subject;
        1. followed the procedure when issuing the Certificate; and
        2. accurately described the procedure in the CA's CP and/or CPS;
3. **Accuracy of Information**: That, at the time of issuance, the CA:
    1. implemented a procedure for verifying the accuracy of all of the information contained in the Certificate (with the exception of the subject\:serialNumber attribute);
        1. followed the procedure when issuing the Certificate; and
        2. accurately described the procedure in the CA's CP and/or CPS;
4. **Identity of Applicant**: That, if the Certificate contains Subject Identity Information, the CA:

1. implemented a procedure to verify the identity of the Applicant in accordance with Section 3.2 and Section 7.1.4.2.2;
    1. followed the procedure when issuing the Certificate; and
    2. accurately described the procedure in the CA's CP and/or CPS;
5. **Subscriber Agreement**: That, if the CA and Subscriber are not Affiliated, the Subscriber and CA are parties to a legally valid and enforceable Subscriber Agreement that satisfies these Requirements, or, if the CA and Subscriber are the same entity or are Affiliated, the Applicant Representative acknowledged the Terms of Use;
6. **Status**: That the CA maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (Valid or Revoked) of all unexpired Certificates; and
7. **Revocation**: That the CA will revoke the Certificate for any of the reasons specified in these Requirements.

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

The Subscriber Agreement or Terms of Use SHALL contain provisions imposing on the Applicant itself (or made by the Applicant on behalf of its principal or agent under a subcontractor or hosting service relationship) the following obligations and warranties:

1. **Accuracy of Information**: An obligation and warranty to provide accurate and complete information at all times to the CA, both in the Certificate Request and as otherwise requested by the CA in connection with the issuance of the Certificate(s) to be supplied by the CA;
2. **Protection of Private Key**: An obligation and warranty by the Applicant to take all reasonable measures to assure control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device such as a password or token);
3. **Acceptance of Certificate**: An obligation and warranty that the Subscriber will review and verify the Certificate contents for accuracy;
4. **Use of Certificate**: An obligation and warranty to use the Certificate only on MailBox Addresses listed in the Certificate, and to use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement or Terms of Use;
5. **Reporting and Revocation**: An obligation and warranty to:
    1. promptly request revocation of the Certificate, and cease using it and its associated Private Key, if there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate, and
        1. promptly request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate;
6. **Termination of Use of Certificate**: An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise.
7. **Responsiveness**: An obligation to respond to the CA's instructions concerning Key Compromise or Certificate misuse within a specified time period.
8. **Acknowledgment and Acceptance**: An acknowledgment and acceptance that the CA is entitled to revoke the Certificate immediately if the Applicant were to violate the terms of the Subscriber Agreement or Terms of Use, or if revocation is required by the CA's CP and/or CPS, or by these Requirements.

### 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.