6+ (&$ 7/ 6 &(57,) ,&$7(32/ ,&< $1'
&(57,) ,&$7,21 35$&7,&(
67$7(0 (17

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

6+ (&$ &$ + LHUDUFK\

Currently, SHECA has the following root CAs for TLS:

8 &$ * OREDO* 5 RRW

8 &$ ([VMQGHG 9 DOLGDWRQ 5 RRW

8 QL7 UXVW* OREDO 5 RRW &$ 5 FHDVHG

8 QL7 UXVW* OREDO 5 RRW &$ 5 FHDVHG

8 QL7 UXVW* OREDO 7 / 6 5 6$ 5 RRW &$ 5

8 QL7 UXVW* OREDO 7 / 6 (&& 5 RRW &$ 5

8 &$ * OREDO* 5 RRW is cross signed by &HUWXP 7 UXVWHG 1 HWZ RUN &$.

8 QL7 UXVW* OREDO 7 / 6 5 6$ 5 RRW &$ 5 is cross signed by 8 &$ * OREDO* 5 RRW

8 QL7 UXVW* OREDO 7 / 6 (&& 5 RRW &$ 5 is cross signed by 8 &$ * OREDO* 5 RRW

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

1.2 Document name and identification

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

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

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

2 ,'	2 EMFW
1.2.156.112570.1.1.1 2.23.140.1.2.1	Domain Validation SSL Certificates Policy
1.2.156.112570.1.1.2 2.23.140.1.2.2	Organization Validation SSL Certificates Policy
1.2.156.112570.1.1.3 2.23.140.1.1	Extended Validation SSL Certificates Policy

1.3 PKI participants

1.3.1 Certification authorities

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

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

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

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

1.3.2 Registration authorities

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

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

1.3.3 Subscribers

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

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

1.3.4 Relying parties

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

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

1.3.5 Other participants

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

1.4 Certificate usage

1.4.1 Appropriate certificate uses

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

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

1.EV SSL Certificate

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

2.OV SSL Certificate

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

3.DV SSL Certificate

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

1.4.2 Prohibited certificate uses

Certificates issued by SHECA is prohibited to be used under any circumstance in which the

national laws and regulations be violated or national security be undermined, and is prohibited to be used for man-in-the-middle (MITM) or traffic management，otherwise the subscriber shall bear all the legal liability arising therefrom; meanwhile, all certificates are not designed to, intended to or authorized to be used in control equipment in dangerous environment or for the occasion where the failure is required to avoid, such as operations of nuclear equipment, navigation or telecommunication systems of space shuttles, air transportation control systems or weapon control systems, as any failure may lead to death, personal injury or severe environmental damage.

Notice:

Publicly Trusted TLS Certificates must strictly comply with the revocation timeframe requirements specified in the TLS Baseline Requirements. Therefore, for systems involving services of &ULWLFDO,QIUDVWUXFWXUH, if subscribers are unable to meet the revocation timeframe outlined in 6HFWLRQ , the use of Publicly Trusted TLS certificates is 127 recommended. It is advisable to adopt private PKI solutions.

1.5 Policy administration

1.5.1 Organization administering the document

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

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

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

1.5.2 Contact person

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

Contact Person: SHECA Strategy Development Department

Tel: 86-21-36393197

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

Postal Code: 200080

Email: report@sheca.com

1.5.3 Person determining CP/CPS suitability for the policy

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

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

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

1.5.4 CP/CPS approval procedures

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

1.6 Definitions and acronyms

1.6.1 Definitions

7HUP	' HILQLWLRQ

Security Policy Administration Committee	It refers to the supreme policy administration and supervision organization in the certification service system and the decisive organization for CP/CPS consistency.
Certification Authority	It refers to a certificate authentication organization, and it is also an entity that issues certificates.
Registration Authority （RA）	It refers to an entity that is responsible for handling service requests from certificate applicants and certificate subscribers, submitting requests to certification authority, and creating the registration process for end certificate applicants. It is responsible for identifying and authenticating the identity of certificate applicants,initiating or delivering certificate revocation requests as well as approving the applications for updating certificates or keys on behalf of certification authority.
Certificate Policy（CP）	A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements. For example, a specific CP can specify that a type of certificate applies to the identification of products and services within the given price range for participants involved in business-to-business transactions.
Certification Practice Statement（CPS）	One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.
Certification Path	It refers to a sequential certificate sequence (including the public key of the start object in the path), and the public key of the end object can be obtained by processing this sequence.

Policy qualifier	It refers to information that depends on the policy and may exist in X.509 certificate together with CP identifier.
Digital Certificate	It refers to a digital certificate which used as a digital signature to identify the identity of the signer and the signer recognized the signature.
E-Signature	It refers to a technical means which has functions of identifying the identity of the signer and signifying that the signer accepts the signature data.
Digital Signature	It refers to a type of e-signature which uses an asymmetric cryptographic system to encrypt or decrypt the electronic -record.
Electronic Signer	It refers to the one who holds the e-signature creation data and implements the e-signature in person or in the name of assigned representatives.
E-signature Relying Party	It refers to the one who trust e-signature certification certificates or e-signature and undertake related activities.
Private Key (E-signature creation data)	It refers to the data that is used in the process of electronic signing and reliably relates e-signature with electronic signer, such as characters, codes, etc.

Public Key (E-signature verifying data)	It refers to the data used by Subscriber to verify e-signature.
Subscriber	It refers to an entity that receives certificates from certification authority, namely certificate holder. In e-signature applications, Subscriber is the electronic signer.
Relying Party	It refers to an entity which relies on the authenticity of a certificate. In e-signature applications, it also refers to an e-signature relying party. A relying party may or may not be a subscriber.

1.6.2 Acronyms

$FURQ\P	) XOO1DPH	&KLQHVH7UDQVODWLRQ
CA	Certification Authority	电子认证服务机构，证书颁发机构
CP	Certificate Policy	证书策略
CPS	Certification Practice Statement	电子认证业务规则
SSL	Secure Sockets Layer	加密套接层协议
CRL	Certificate Revocation List	证书撤消列表

LDAP	Lightweight Directory Access Protocol	轻型目录访问协议
OCSP	Online Certificate Status Protocol	在线证书状态协议
PIN	Personal Identification Number	个人身份识别码
PKCS	Public Key Cryptography Standards	公共密钥密码标准
PKI	Public Key Infrastructure	公共密钥基础设施
RA	Registration Authority	注册审核服务机构
RFC	Request For Comments	请求评注标准（一种互联网建议标准）

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: cps@sheca.com

Mailing Address:

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

Telephone: +86-21-36393197

Fax: +86-21-36393200

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

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

2.3 Time or frequency of publication

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

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

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

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

ROOT	Test Web Page
UCA Extended Validation Root	https://rsaevg3.good.sheca.com https://rsaevg3.revoked.sheca.com https://rsaevg3.expired.sheca.com
UniTrust Global TLS ECC Root CA R2	https://eccev2a.good.sheca.com https://eccev2a.revoked.sheca.com https://eccev2a.expired.sheca.com

UniTrust Global TLS RSA Root CA R1	https://rsaev1a.good.sheca.com https://rsaev1a.revoked.sheca.com https://rsaev1a.expired.sheca.com

2.4 Access controls on repositories

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

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

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

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

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

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

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

3.1.2 Need for names to be meaningful

SHECA ensures that both the subjectDN and issuerDN extensions of certificates include clear and meaningful identifiers. These identifiers are used to distinguish the subject and issuer. Certificates

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

3.1.3 Anonymity or pseudonymity of subscriber

No stipulations.

3.1.4 Rules for interpreting various name forms

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

3.1.5 Uniqueness of names

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

3.1.6 Recognition, authentication, and role of trademarks

No stipulations.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

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

3.2.2 Authentication of Organization and Domain Identity

3.2.2.1 Organizational Identity Verification

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

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

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

3. A letter of attestation.

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

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

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

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

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

3.2.2.2 DBA/Tradename

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

3.2.2.3 Verification of Country

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

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

information to detect any alterations or falsifications.

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

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

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

b. The applicant's IP address;

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

3. Information provided by the domain name registrar.

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

3.2.2.4 Validation of Domain/IP Authorization or Control

3.2.2.4.1 Validation of Domain Authorization or Control

If the certificate name is a domain name, SHECA requires the applicant to provide additional evidence material of domain name in addition to the written materials submitted by the applicant to audit. SHECA must proceed the following procedure while performing verification.

1. SHECA should confirm the requested domain name is not in the form of ³RQLRQ´ ³LQDGGUDUSD´ RU³LS DUSD´

Certificate issuance for a domain name in these forms is not allowed by SHECA;

2. Authentication of domain name by one of the following methods:

(1) Email, Fax, SMS, or Postal Mail to Domain Contact

Validating the applicant’s control over the FQDN by sending a Random Value via email, fax, SMS, or postal mail, to the Domain Contact and receiving a confirmation utilizing the Random Value, performed in accordance with BR Section 3.2.2.4.2;

Effective January 15, 2025: - When issuing Subscriber Certificates, the CA MUST NOT rely on Domain Contact information obtained using an HTTPS website, regardless of whether previously obtained information is within the allowed reuse period. Effective July 15, 2025: - The CA MUST NOT rely on this method. - Prior validations using this method and validation data gathered according to this method MUST NOT be used to issue Subscriber Certificates.

(2) Constructed Email to Domain Contact

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

(3) DNS Change

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

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

(4) IP Address

By confirming the Applicant's control over the FQDN through control of an IP address returned from a DNS lookup for A or AAAA records for the FQDN, performed in accordance with BR Section 3.2.2.4.8;

(5) Email to DNS CAA Contact

Confirming the Applicant's control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value. The Random Value MUST be sent to a DNS CAA Email Contact. The relevant CAA Resource Record Set MUST be found using the search algorithm defined in RFC 8659, Section 3. This method should be performed in accordance with BR Section 3.2.2.4.13;

(6) Email to DNS TXT Contact

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

(7) Agreed - Upon Change to Website v2

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

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

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

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

The file containing the Request Token or Random Number:

a. is located on the Authorization Domain Name;

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

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

d. MUST be accessed over an Authorized Port.

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

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

(8) Agreed-Upon Change to Website - ACME

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

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

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

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

The file containing the Request Token or Random Number:

a. is located on the Authorization Domain Name;

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

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

d. MUST be accessed over an Authorized Port.

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

(9) DNS Labeled with Account ID - ACME

Confirming the Applicant's control over the FQDN by performing the procedure documented for a "dns-account-01" challenge in draft 00 of "ACME DNS Labeled With ACME Account ID Challenge" available at the following link, performed in accordance with BR Section 3.2.2.4.21.

https://datatracker.ietf.org/doc/draft-ietf-acme-dns-account-label/

When using this method, the host record will be generated based on the user's ID, no longer limited to _acme-challenge or _dnsauth.

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

Note:

The Random Value used in the methods listed above shall remain valid for no more than 30 days from its creation.

Method (4), (7) and (8) is not suitable for Wildcard Certificate Domain Name validation. Other methods are suitable for Wildcard Certificate Domain Name validation.

3.2.2.4.2 Validation of IP Authorization or Control

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

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

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

2 Confirm Applicant has control over the IP address by either:

(1) Agreed-Upon Change to Website: confirming the Applicant's control over the requested IP

Address by confirming the presence of a Request Token or Random Value contained in the content of a file or webpage in the form of a meta tag under the “/.well-known/pki-validation” directory, performed in accordance with Baseline Requirements Section 3.2.2.5.1.

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

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

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

The file containing the Request Token or Random Number:

a. is located on the Authorization Domain Name;

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

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

d. MUST be accessed over an Authorized Port.

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

(2) Email, Fax, SMS, or Postal Mail to IP Address Contact: Confirming the Applicant’s control over the IP Address by sending a Random Value via email, fax, SMS, or postal mail and then receiving a confirming response utilizing the Random Value, performed in accordance with Baseline Requirements Section 3.2.2.5.2.

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

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

(4) ACME method for IP Addresses: Confirming the Applicant’s control over the IP Address by validating domain control of the FQDN using the ACME HTTP Challenge method.

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

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

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

The file containing the Request Token or Random Number:

a. is located on the Authorization Domain Name;

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

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

d. MUST be accessed over an Authorized Port.

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

Note:

The random value used in the above validation methods remains valid for no more than 30 days from the time of creation.

SHECA does not issue EV certificates for IP addresses.

3.2.2.4.3 Wildcard Domain Validation

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

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

SHECA does not issue EV certificates for wildcard domain names.

3.2.2.4.4 Verification of Country

For publicly-trusted TLS, if the Applicant requests a Certificate that will contain Subject Identity Information comprised only of the countryName field, then SHECA verifies the country associated with the Subject using a verification process meeting the requirements of section 3.2.2.3 in the CAB Forum Baseline Requirements and meets the requirements of this section.

When the subject:countryName field is present, then SHECA verifies the country associated with

the Subject using one of the following:

1. The IP Address range assignment by country for either

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

b. The Applicant's IP address;

2. The ccTLD of the requested Domain Name;

3. Information provided by the Domain Name Registrar;

3.2.2.4.5 Multi-Perspective Issuance Corroboration

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

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

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

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

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

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

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

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

3.2.2.4.6 Certification Authority Authorization (CAA)

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

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

SHECA treats a record lookup failure as permission to issue if:

1) the failure is outside the SHECA's infrastructure;

2) the lookup has been retried at least once; and

3) the domain's zone does not have a DNSSEC verification chain to the ICANN root.

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

3.2.3 Authentication of individual identity

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

3.2.4 Non-verified subscriber information

This CP/CPS only describes the verification of TLS Server Certificates. SHECA verifies all

certificates according to the latest versions of "Baseline Requirements for TLS Server Certificates" and "EV Guidelines for TLS Server Certificates."

3.2.5 Validation of authority

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

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

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

3.2.6 Criteria for interoperation

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

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

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

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

SHECA supports the following types of key updates:

- 5 HSODFH PHQW 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.

• 5HQHZDO A subscriber wishes to extend the validity period of a certificate and optionally change some or all of the subject information, potentially also replacing the associated key.

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

3.3.2 Identification and authentication for re-key after revocation

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

3.4 Identification and authentication for revocation request

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

1. The subscriber submits a written request, which must include the applicant's handwritten signature and application date. SHECA will provide the subscriber with a standard template.
2. SHECA will regenerate the domain validation value and require the subscriber to configure the new validation value. Once the system detects this validation value, the revocation process will be triggered.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

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

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

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

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

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

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

4.1.1 Who can submit a certificate application

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

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

4.1.2 Enrollment process and responsibilities

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

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

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

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

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

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

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

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.

SHECA will perform a CAA record check for each dNSName in the SSL certificate extension Subject Alternative Name, and determine whether to approve the certificate application according to the inspection method and result in 3.2.2.8.

After verifying application materials submitted by an applicant, based on the verification result, SHECA will decide whether to accept or reject the application or require the applicant to submit additional relevant materials. In the process of handling a certificate application, SHECA will ensure the consistency between certificate information and correct application information through effective means and issue the certificate to the right applicant.

For OV and EV SSL certificates SHECA can reuse previous validations if SHECA obtained the data or document from a source specified under Section 3.2 of this CP/CPS or completed the validation no more than 398 days prior to issuing the Certificate. For validation of Domain Names and IP Addresses according to Section 3.2.2.4, SHECA can reuse data, document, or completed validation if they are obtained no more than 398 days prior to issuing the Certificate.

For DV SSL certificatess, SHECA does not reuse domain verification data.

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 Approval of Certificate Applications

SHECA may approve a certificate application if:

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

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

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

4.2.2.2 Rejection of Certificate Applications

SHECA has the right to reject a certificate application if:

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

2. the subscriber cannot provide necessary identity proof materials;

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

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

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

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

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

4.2.3 Time to process certificate applications

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

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

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

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

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

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

4.3.2 Notification to subscriber by the CA of issuance of certificate

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

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

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

Certificate when:

- the Subscriber uses the Certificate, or
- 30 days pass from the date of the issuance of a Certificate

4.4.2 Publication of the certificate by the CA

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

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

4.4.3 Notification of certificate issuance by the CA to other entities

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

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

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

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

4.5.2 Relying party public key and certificate usage

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

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

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

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

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

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

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

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

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

4.6 Certificate renewal

4.6.1 Circumstance for certificate renewal

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

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

4.6.2 Who may request renewal

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

4.6.3 Processing certificate renewal requests

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

4.6.4 Notification of new certificate issuance to subscriber

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

4.6.5 Conduct constituting acceptance of a renewal certificate

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

4.6.6 Publication of the renewal certificate by the CA

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

4.6.7 Notification of certificate issuance by the CA to other entities

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

4.7 Certificate re-key

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

4.7.1 Circumstance for certificate re-key

Examples of situations where a certificate needs to be rekeyed include certificate renewal, loss of

the certificate's private key, or compromise of the certificate's private key.

4.7.2 Who may request certification of a new public key

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

4.7.3 Processing certificate re-keying requests

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

4.7.4 Notification of new certificate issuance to subscriber

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

4.7.5 Conduct constituting acceptance of a re-keyed certificate

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

4.7.6 Publication of the re-keyed certificate by the CA

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

4.7.7 Notification of certificate issuance by the CA to other entities

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

4.8 Certificate modification

4.8.1 Circumstance for certificate modification

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

4.8.2 Who may request certificate modification

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

4.8.3 Processing certificate modification requests

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

4.8.4 Notification of new certificate issuance to subscriber

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

4.8.5 Conduct constituting acceptance of modified certificate

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

4.8.6 Publication of the modified certificate by the CA

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

4.8.7 Notification of certificate issuance by the CA to other entities

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

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

5HDVRQVIRU5HYRNLQJ D6XEVFULEHU&HUWLILFDWH

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

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

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

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

4. SHECA obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address in the Certificate should not be relied upon.

5. SHECA obtains evidence that the certificate was misused;

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

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

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

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

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

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

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

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

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

9. Revocation is required by the CP/CPS;

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

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

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

Note:

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

5HDVRQVIRU5HYRNLQJ D6XERUGLQDWH&$ &HUWLILFDWH

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

1. the subordinate CA formally requests revocation of the certificate in writing;
2. the subordinate CA has found and notifies Root CA that the original certificate request is not authorized and does not retroactively grant authorization;
3. SHECA obtains evidence that the subordinate CA’s private key corresponding to the public key in the certificate suffered a key compromise or no longer complies with the requirements in sections 6.1.5 and 6.1.6 of Baseline Requirements;
4. SHECA obtains evidence that the certificate was misused;
5. SHECA is made aware that the subordinate certificate was not issued in accordance with Baseline Requirements, or the subordinate certificate fails to comply with the CP/CPS;

application software supplier through email immediately.

5.7.4 Business continuity capabilities after a disaster

1. Business Continuity Management (BCMP)

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

2. Redundant CA System

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

3. Disaster Recovery System

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

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

5.8 CA or RA termination

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

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

2. Arrange the business to undertake.

- Save all of the operational information related to certification service, including certificates, user information, system files, CPS, norms and agreements.

- Stop the related operation services.

- Clear system root key.

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

6. TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

6.1.1.1 CA Key Pair Generation

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

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

6.1.1.2 Subscriber Key Pair Generation

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

6.1.3 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 key through registration authority. When network transmission is needed, Secure Sockets Layer (SSL) and other secure protocols shall be used.

6.1.4 CA public key delivery to relying parties

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

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

6.1.5 Key sizes

SHECA uses the keys with the following specifications：

5RRW&$&HUWLILFDWHV

digest algorithm：SHA256 and SHA384 and SHA512

RSA modulus size：4096

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 subscribers' SSL certificates.

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

7\SH	3ULYDWH. H\ 8VH	&HUWLFDWH9DOLGLW\
Publicly Trusted Root CAs	No stipulation	25 years
Publicly Trusted Sub CAs / Issuer CAs	No stipulation	15 years
CRL and OCSP responder signing	3 years	No Stipulation
DV SSL/TLS Server	No stipulation	398 days
OV SSL/TLS Server	No stipulation	398 days
EV SSL/TLS Server	No stipulation	398 days

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 dati

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.

7KH YHUVLRQ QXPEHU it is used to specify the version information of CRL, and SHECA adopts the CRL V2 version corresponding to the X.509 V3 certificate.

6LJQDWXUH DOJRULWKP: SHECA adopts signature algorithms of SHA256WithRSA or SHA384WithRSA.

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

(IIHFWLYH GDWH specify a date/time value to indicate the time when the CRL is generated.

1H[W8SGDWH specify a date/time value to indicate the time when the next CRL will be generated .

5HYRFDWHG &HUWV t 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.

$XWKRULW\. H\ ,GHQWLILHU this identifier is used to verify the public key signed on the CRL. It can identify different keys used by the same CA.

1H[W&5/ 3XEOLVK specify a date/time value to indicate the time when the next CRL will be published.

5HDVRQ&RGH 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:

NH\&RP SURP LVH

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.

SULYLOHJH LWKGUDZQ

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.

FHVVDWLRQ2I2SHUDWLRQ

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.

DIILODWRQ&KDQJHG

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.

VXSHUVHGHG

The CRLReason superseded is used when:

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

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

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

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

- SHECA revoked the certificate due to domain authorization or compliance issues other than those related to keyCompromise or privilegeWithdrawn.

7.3 OCSP profile

The OCSP response issued by SHECA's certification system conforms to the RFC6960 Standard, which defines a standard request and response information format to confirm the status of the certificate.

7.3.1 Version number(s)

RFC6960 defines the OCSP V1.

7.3.2 OCSP extensions

OCSP request contains the following data: protocol version, service request, target certificate identifier, and optional extensions, etc.

After receiving a request, the OCSP server conducts the following detections when responding:

- the message is well formatted
- the responder is configured to provide the request service.

The request includes the information needed by the responder server, and if any one of the prerequisites is not satisfied, the OCSP server will generate an error message; otherwise, return a definite reply.

All definite replies are digitally signed by SHECA OCSP signing certificate. The main reply status includes: the certificate is valid, revoked, unknown. The reply information is composed of the following parts：

- Version of the response syntax
- Identifier of the responder server
- Response to the request certificate
- Time when the response was generated
- Optional extensions
- The object identifier of signature algorithm
- The signature of the hashed reply information

If an error occurs, the OCSP responder server will return an error message which does not contain the signature of SHECA OCSP certificate. Error information may include:

- Request with incorrect formatting
- Internal error

- Please try again later
- Require signature
- Unauthorized

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

SHECA should perform the audit and assessment as follows:

1) carry out an operational quality assessment quarterly to ensure the reliability, security and controlability of operation services.

2) carry out an internal audit of authentication quarterly and draw at least 3% of certificate samples.

3) carry out an annual CCADB Self-Assessment according to CA/Browser Forum CCADB policy.

4) carry out an annual self-audit of physical control, key management, operation control, and authentication execution, etc. to determine whether the actual circumstance is consistent with the predetermined standards and requirements and take actions according to the results of the review.

5) carry out an annual operation risk assessment to identify internal and external threats, to assess the possibility and compromise of the threats, and to formulate and implement a disposal plan based on the results of the risk assessment.

6) in addition to internal audit and assessment, SHECA also employs independent auditing firms to conduct external audits and assessments in accordance with WebTrust standards.

8.2 Identity/qualifications of assessor

Internal audit and assessment are carried out by SHECA's internal audit and assessment team.

External audit will be done by the authority with the following qualifications:

1. Must be a licensed and certified assessment authority, honored a good reputation in the industry;

2. Have sufficient knowledge in the computer information security system, communication network security requirements, PKI technology, standards and operation;

3. Possess professional skills and tools to check the system operating performance;

4. Possess the qualification of WebTrust audit.

8.3 Assessor's relationship to assessed entity

The position of internal auditors and the system administrators, business managers and business operators of this organization must not overlap.

The relationship between external assessors and SHECA is independent, and there is no stake between them that may affect the objectivity of the assessment.

8.4 Topics covered by assessment

The internal audit shall involve the following schemes:

1. whether the operation process and system are strictly observed.

2. whether the certification service is done strictly according to CP/CPS, service specifications and security requirements.

3. whether all kinds of logs and records are integrated and whether there are any problems;

4. whether there is any other potential security risk.

In accordance with the requirements of WebTrust standards, the third-party auditors audit SHECA independently.

8.5 Actions taken as a result of deficiency

Regarding problems in the internal audit results, the audit assessment team is responsible for overseeing the improvement of the responsible departments.

After the completion of the third-party Auditor's assessment, SHECA will rectify and reform in accordance with the work report and accept re-audit and assessment.

8.6 Communication of results

There will be formal notification of internal audit results to the responsible departments, and

SHECA will inform the subscribers in time of the potential security risks.

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.

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.

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

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. Du[illegible]asons[illegible]rivat[illegible]key of the certificate is deciphered, stolen and [illegible]d.[illegible]g[illegible]upt or t[illegible]ying par[illegible]suffer lo[illegible]

5. SHEC[illegible]fai[illegible]o revo[illegible]th[illegible]rtificate in[illegible]ime, causing the[illegible]ying[illegible]ty to suff[illegible]sses.

In addition, the i[illegible]mnity limit[illegible]SHECA is specified as f[illegible]

1. Al[illegible]demnifi[illegible]ion obliga[illegible]s of SHECA s[illegible]exceed the up[illegible] limit of t[illegible]ndemn[illegible], [illegible] upper limit [illegible]in[illegible] can be r[illegible]ulated by SHEC[illegible]according to the specific circumstance, and SHEC[illegible]will imm[illegible]ately notify [illegible]e parties concerned of the circumstance after the refo[illegible]lation.

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[illegible]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.

,QGHPQLILFDWLRQE\ 6XEVFULEHUV

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 the 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's subscriber or other entities that have the