Sinorail Certification Authority
Certification Practice Statement
(Version 2.0.3)

Copyright Notice

For the latest version of these rules, please refer to the company's website at www.sinorailca.com, or contact Sinorail Certification Authority. If there is any change to this CPS, unless otherwise required by laws and regulations, no further notice will be given to specific recipients.

Address: 2nd Floor, Building 1, Yard 2, Maliandao South Street, Xicheng District, Beijing
Tel: 010-51892503
Email: srca@sinorail.com

Notes

The "Sinorail CA Certification Practice Statement" is subject to the laws and regulations of the People's Republic of China, including but not limited to:

The Criminal Law, the Civil Code, the Copyright Law, the Law on Guarding State Secrets, the Trademark Law, the Civil Procedure Law, the Decision of the Standing Committee of the National People's Congress on Safeguarding Internet Security, the Regulations on the Security Protection of Computer Information Systems, the Regulation on the Administration of Commercial Cipher Codes, the Measures for the Administration of Ciphers for Electronic Certification Services, the Electronic Signature Law, and the Measures for the Administration of Electronic Certification Services.

Sinorail CA will reserve the right to prosecute any organisation, entity or individual that has been or is about to allegedly violate laws or regulations and thus affecting Sinorail CA certificate services according to law.

Revision History

Version	Release date	Remarks
1.0	18 April 2009	Revised according to the “Certification Practice Statement Standard (Trial)” issued by the Electronic Certification Service Management Office, Ministry of Industry and Information Technology
2.0	26 June 2019	Revised according to the “Certification Practice Statement Standard (Trial)” issued by the Electronic Certification Service Management Office, Ministry of Industry and Information Technology
2.0.1	9 December 2020	Modified 4.4.1 Acts that constitute acceptance of a certificate. Added 4.6.1 how to secure certificate renewal
2.0.2	13 December 2024	Modified 1.1.2 Overview of Sinorail Certification Authority, which summarily describes the conduct of cross-border electronic certification services. Modified 1.1.3 certificate categories, 14.2 registration authority, 1.5.2 certificate application list or types prohibited by certificates issued, 1.6.1 policy document management organization, 1.7. definitions and abbreviations, 2.1 release of certification information, 2.2 timing or frequency of release, 3.1.4 rules for different name forms, 3.3 identification and authentication of key renewal requests, 4.3.2 notification from electronic certification service organization and registration authority to subscribers, 4,4.1 acts that constitute acceptance of certificates, 4.5.1 use of private key and certificate by subscribers, 4.9 certificate revocation and suspension, 4.12.1 policies and acts of key generation, backup and recovery, 5.1.2 physical access, 5.1.8 offsite backup, 5.5.1. types of archived records, 5.6 electronic certification service organization key replacement, 6.1.5 key length, 6.2.2 multiperson control of keys, 7.1.2 algorithm object identifier, 7.2.2 CRL and cRL entry extensions, 9.3.1 confidential business information, 9.9.1 liability of SRCA for indemnification, 9.12 amendment, 9.13 dispute resolution, among other relevant descriptive contents.
2.0.3	18 September	Modified 4.9.9 query billing method for online status, 5.3.1 probation

	2025	period for new employees, 5.4.2 Log processing cycle,5.4.3 retention period for audit logs,5.4.6 audit collection system,5.7 damage caused and disaster recovery progress , 8.2 Revising the Selection Scope for Internal Audit Assessors, 8.4 Audit Assessment Specifications, Correcting Errors in Document Content

Contents

1. Summary Description

This document is the Certification Practice Statement (CPS) of Sinorail Certification Authority (SRCA).

The structure of this CPS conforms to the “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”, i.e,. RFC3647 standard formulated by an internet organization called Internet Engineering Task Force. The RFC3647 framework has become a standard in the PKI industry. Sinorail CA does its best to make the CPS compliant with RFC3647 standard, but it reserves the right to adopt a different structure from the RFC3647 when necessary, for example, in order to improve the quality of the CPS or its suitability to participants in the Sinorail CA trust domain. And the structure of the SRCACPS will not necessarily be consistent with later versions of the RFC3647.

1.1 Overview

1.1.1 Certification Practice Statement

Sinorail CA Certification Practice Statement (CPS) is a detailed description and statement of the specifications followed by Sinorail CA for the business practices (such as issuance, management, revocation, and renewal of certificates or keys) in the lifecycle of all certificate services provided by Sinorail CA, including the scope of responsibility, operation specifications and information security assurance measures, etc., and is a collection of policy rules such as certificate management, certificate services, certificate application, certificate classification, certificate authorisation, and certificate responsibility. The basis of preparation by Sinorail CA CPS, i.e, the "Certification Practice Statement Standard (Trial)", complies with the "Electronic Signature Law of the People's Republic of China", the " Measures for the Administration of Electronic Certification Services" issued by the Ministry of Industry and Information Technology and the RFC3647 "Public Key Infrastructure Certificate Policy and Certification Practices Framework" , mainly composed of the following parts:

(I) Summary description

(II) Information release and information management

(III) Identity and identification

(IV) Operating requirements for certificate lifecycle

(V) Certification body facilities, management and operation control

(VI) Technical security control of the certification system

(VII) Certificates, certificate revocation lists, and online certificate status protocol

(VIII) Certification body audit and other assessments

(IX) Legal liability and other terms of business

The entities within the Sinorail CA certification system and the holders of Sinorail CA digital certificates must fully understand and implement the terms stipulated in the Sinorail CA Certification Practice Statement, and assume the corresponding responsibilities and obligations.

1.1.2 Sinorail Certification Authority

Sinorail Certification Authority, or SRCA, is abbreviated as Sinorail CA. Sinorail CA was established in 2008 and is operated and managed by Sinorail Hongyuan (Beijing) Software Technology Co., Ltd.

SRCA is a third-party electronic certification service organization proposed, designed, constructed and operated by Sinorail Hongyuan (Beijing) Software Technology Co., Ltd., which provides identity authentication and trust services to the public (including but not limited to government agencies, companies, public institutions, and individuals) in accordance with the "Electronic Signature Law of the People's Republic of China", "Measures for the Administration of Ciphers for Electronic Certification Services " and other laws and regulations. In April 2009, Sinorail CA passed the expert demonstration of the construction implementation plan organized by the Office of the State Secret Code Regulatory Commission, passed the security review organized by the Office of State Secret Code Regulatory Commission, and passed the system security review organized by the State Cryptography Administration. SRCA is engaged in operation services in strict accordance with the requirements of the Ministry of Industry and Information Technology, the State Cryptography Administration and other competent authorities, and has obtained the password license for electronic certification services issued by the State Cryptography Administration, whereby the keys used are provided by Sinorail KMC.

Sinorail Certification Authority is a nationwide information security certification body built in accordance with the requirements of national standards, which undertakes the application, review, issuance, revocation, renewal and query of digital certificates.

Sinorail Certification Authority (Sinorail CA) relies on the broad IT-enabled transportation application of the railway, and provides electronic certification services with autonomous characteristics for the national market. According to different application requirements, we provide a full range of specialized services of different categories and levels based on digital certification, electronic signature and other services.

Sinorail CA will provide different categories and different levels of specialized services according to different applications and needs. According to the different nature of customer applications, it can be divided into different service categories such as individual, enterprise, and system, and provide targeted and professional customized services; According to different application requirements, it can be divided into different services such as digital certificate authentication service, electronic signature service, and overall system security assurance solutions.

For the railway market, it can be divided into different categories of services such as transportation application services, operation management applications, construction and operation applications, e-commerce applications, etc., and provide customized services in combination with the application system to ensure the legitimacy and effectiveness of security services such as data exchange, information exchange, identity authentication, and electronic signature.

When carrying out cross-border electronic certification services, Sinorail Certification Authority shall comply with China's cipher-related laws and regulations, technical standards and administrative requirements, and agree on the cryptographic algorithm and certificate format, identification and authentication, certificate lifecycle operation requirements, technical security control and legal liability and other terms of business of the certification system in such a manner as set forth in the electronic certification cross-border cooperation agreement or contract, and based on the realities of cross-border electronic certification business.

1.1.3Certificate category

The CA certificate policy is divided into four types of certificates according to the different entities involved in social activities, which are subdivided according to the level of security and the scope of application of the certificate, for protecting the rights and obligations of each participant.

The first type of certificates is personal certificate, which provides the basic level of security and is mainly issued to individual users, divided into personal security email certificates, personal identity certificates, and personal code signature certificates. The first type of certificate represents the online identity of a legal citizen engaged in social activities within the territory of the People's Republic of China, and only bears the responsibility caused by the individual's behavior. The first type of certificates can be applied to digital signature, encryption and access control, as well as proof of identity in medium-sized transactions.

In accordance with the provisions of the Sinorail CA Certificate Policy, the electronic signatures generated by the Class I certificates attested by Sinorail CA or relevant registration authorities meet the requirements of the Electronic Signature Law of the People's Republic of China under the condition that they meet other provisions of the Electronic Signature Law of the People's Republic of China.

The second type of certificate is entity certificate, which provides a high level of security and is mainly issued to organizations, divided into corporate or institutional secure email certificate, corporate or institutional identity certificate, legal representative certificate, and enterprise code signature certificate. The second-type certificates are used to provide identification of an enterprise or institution, representing the identity of the organization in the territory of the People's Republic of China or on transnational (territory) network, and directly or indirectly (through the certificate of authorized person) bear the responsibility of the enterprise's online behavior.

In accordance with the provisions of the Sinorail CA Certificate Policy, the electronic signatures generated by the Class II certificates attested by Sinorail CA or relevant registration authorities meet the requirements of the Electronic Signature Law of the People's Republic of China under the condition that they meet other provisions of the Electronic Signature Law of the People's Republic of China.

The third type of certificates are device certificates, which provide advanced security levels, mainly divided into server certificates, gateway certificates, SSL certificates, application system certificates, terminal device certificates (mobile terminals, PC terminals, etc.), Internet of Things device certificates, etc., functioning to protect the identity of various devices.

They support individual, entity and device certificates to conduct authentication and electronic signature in mobile internet business scenarios. Private keys of subscribers are generated from collaborative operation by subscriber terminal and collaborative signature server, with certificate request information containing electronic signature made using private keys, while Sinorail CA uses public keys of subscribers to verify the validity of private key signatures and integrity of application data.

The fourth type of certificates are event-based certificates, which provide the basic level of security and provide temporary identities for events or activities, and are mainly used for one-time event-based electronic signatures, with private keys destroyed after signing. By signing the data in the business scenario of the signing behavior, it proves that the data has not been tampered with since the signing, ensuring the integrity of the data and the non-repudiation of the signing behavior in the specific business scenario.

In accordance with the provisions of the Sinorail CA Certificate Policy, the electronic signatures generated by the fourth type of certificates attested by Sinorail CA or relevant registration authorities meet the requirements of the Electronic Signature Law of the People's Republic of China under the condition that they meet other provisions of the Electronic Signature Law of the People's Republic of China.

1.2 SRCA Logo

SRCA is the abbreviation of Sinorail Certification Authority. At the same time, Sinorail CA is also valid abbreviations of Sinorail Certification Authority. "SRCA", "Sinorail CA", and their related words, logos, icons, etc. all represent the image of their owner, Sinorail Certification Authority, as well as the stakeholders represented in different places.

The standard icon of Sinorail Certification Authority, "SRCA" and "Sinorail CA" is as follows:

1.3 Document Description

1.3.1 Name

The name of this document is SRCA Certification Practice Statement, which is a comprehensive description by Sinorail Certification Authorityof the third-party certification services and related services provided by it. "Sinorail CA Certification Practice Statement", "SRCA Certification Practice Statement", "Sinorail CA CPS", "SRCACPS", "SRCA Certification Business Statement", "Sinorail CA Certification Business Statement" and similar expressions, regardless of the place of their appearance, shall all be regarded as referring to or reference to this document.

1.3.2 Version

The version number of this Certification Practice Statement (CPS) is 2.0.2. This CPS will be updated in line with the development of SRCA's third-party certification business. The version information ("version 2.0.2 " or "CPS 2.0.2") shall be indicated after the Certification Practice Statement (CPS).

1.3.3 Release

This document will be publicly released to the general public through Sinorail CA’s website at www.sinorailca.com. If there is an update, the update description and the latest version will be provided on Sinorail CA’s website.

1.4 Participants in e-certification activities

1.4.1 Electronic certification service organization

Sinorail Certification Authority is the entity that issues certificates and also provides electronic signature authentication services for certificate users. Sinorail CA and its subordinate bodies are collectively referred to as SRCA.

Sinorail CA is the root of all SRCA organizations and entities. Under the control of a very strict confidentiality and security mechanism, SRCA generates its own key pair and issues the root certificate according to the policy on the validity period of the root certificate. SRCA issues the next-level certificates pursuant to the authority and agreement. The certificate issued by SRCA is bundled with the public key of each certificate-claiming entity. For a certificate that has been issued by SRCA and is within its validity period, the information and status of the certificate that can be publicized will be published using the Certificate Directory Server and the Certificate Revocation List (CRL) service.

SRCA will establish cross-certification relationship with other CAs that are not involved in the SRCA service framework system according to its business needs to achieve interconnectivity. Cross-certification refers to the establishment of a relationship of mutual trust between two completely independent certification authorities that adopt their respective CPS, so that the certificate users of both parties can authenticate to each other.

1.4.2 Registration Authority

The registration authority RA, as a subordinate organization authorized by SRCA, is responsible for reviewing, collating and aggregating certificate user information, statistical analysis, data exchange with the superior CA, and managing and serving subordinate business terminals(BTs), etc. Each RA can be divided into BTs as per industry, administrative territory or other factors to provide services to end users. The RA is the entity that establishes the registration process for the final certificate applicant, identifies and authenticates the certificate applicant, initiates or transmits the certificate revocation request, and approves the application for renewal of certificate or updating of the key on behalf of the electronic certification service authority. The RA requires certificate applicants or their agents to provide personal information when accepting applications for certificate and relevant electronic signature business according to relevant laws and regulations, including such personal privacy information as name, contact details, ID card number, address and ID card (original and/or copy of any form). The RA properly keeps the data of certificate users in accordance with the relevant laws and regulations and this CPS, and is not allowed to disclose the data of certificate users to any entity or individual unrelated to the certificate business, or use the same for commercial purposes. RAs must be authorized by SRCA to engage in various certificate services according to their authorization, and to expand the corresponding lower-level service organizations according to their authorization.

1.4.3 Business Terminal

After the review of SRCA and a registration authority authorized by it, SRCA and the authorized registration authority may authorize a specific unit or entity to become a business terminal responsible for handling certificate services such as application for, and revocation and query of digital certificates. The application procedures, handling procedures and acceptance requirements for certificate-related services must be consistent with the CP, CPS carried out by SRCA and the BT license agreement signed by SRCA with it. The BT is responsible for providing the SRCA or RA with information about the applicant entity for certificate services, including the name of the applicant entity, the legal identifying logo, and any legal supporting documents and contact information (mailing address, e-mail address, telephone number) required by SRCA. Based on this information, the BT provides the applicant entity with authorized services such as certificate application, certificate production, signing key generation, certificate query, certificate revocation, certificate renewal, etc., or provides the applicant entity with any other services and technical support that comply with this CPS and are published by SRCA according to the requirements of the applicant entity. The BT is legally responsible for the process of accepting requests for the certificate services it provides, including but not limited to the relevant provisions of this CPS and the License agreement. Depending on whether or not to bear the cost of the certificate applicant, BTs can be divided into sponsoring BT and non-sponsoring BT. Unless otherwise specified, BT generally refers to a non-sponsoring BT.

If a BT meets and fulfills the requirements of SRCA for the implementation of the certificate sponsoring service, and is authorized by SRCA and its authorized body, the BT is called the sponsoring BT.

If a BT does not bear the cost of the certificate applicant (which is different from the sponsoring certificate BT), the BT is said to be a non-sponsoring BT.

1.4.4 Sponsor

Sponsor is a group or organization that can bear all costs of certificate services for the subscribers or potential subscribers belonging to or served by it. In accordance with the provisions of this CPS, other regulations published by SRCA, and as required by laws and policies, a sponsor has the right to cancel all or part of the certificate services to certificate holders that are paid for by it, including but not limited to the cancellation of the holder's digital certificate. A sponsor must pre-book the number of certificates and pay all certificate fees in advance according to the agreement signed with SRCA, and can enjoy certain preferential policies according to SRCA's regulations. A sponsor must be responsible for the authenticity of the identity of all certificate holders for whom it pays fees.

1.4.5 Subscriber

Subscriber, i.e., Certificate Holder, Certificate User or Certificate Client, is an entity that received certificates from SRCA. It includes individuals, enterprises, organizations, institutions, server equipment, websites and other entities that have applied for and have digital certificates issued by SRCA, as well as any other subjects that have certain identifiers and hold various certificates issued by SRCA, including any entity or non-entity person, object and organization.

Subscribers fall into two categories:

(1) Certificate holder who has been sponsored, and whose certificate fee is borne by the sponsor;

(2) Certificate holder who bears the certificate fee.

Subscribers have been advised to receive appropriate training on the use of electronic certification technology before applying for a certificate. Subscribers can obtain documents and learning materials related to electronic signatures, certificates, PKIs, etc., which will be made available by SRCA through the website, training activities, promotional materials, etc., depending on the situation. SRCA offers different types of certificates, and it is up to subscribers to decide which certificate is suitable for their needs. The Subscriber agrees to notify the Issuing Authority in a timely manner in the event of a situation that compromises the security of the private key.

1.4.6 Relying Party

For the relying party, SRCA undertakes that all information in the certificate is accurate, except for unverified subscriber information. The relying party should reasonably trust the certificate and relevant digital signatures. If additional guarantees are required to trust a digital signature, the relying party must obtain these guarantees before it can reasonably trust the digital signature.

A relying party who is a SRCA Certificate Subscriber has all the corresponding rights prescribed by the SRCCAS, including the certificate assurance that SRCA may provide, as well as the rights and interests involved in this CPS. As to a relying party who is not a SRCA subscriber, SRCA shall have no obligation or liability other than to guarantee the authenticity of the certificates and related signature information that it trusts and is issued by SRCA.

1.4.7 Certificate Application Industry Organization

The Certificate Application Industry Organization is an important participant in SRCA's electronic certification services. The application of SRCA digital certificates in the industry benefits from the permission of the certificate application industry organization. The certificate application industry organization has the right to decide whether the user of the SRCA basic certificate has the right to use in the specific application in the industry. In order to facilitate the expansion of certificates in various industries and maintain the universality of basic certificates, SRCA defines in the certificate the permissions of certificate subscribers in industry applications, and uses the certificate extension domain to define the key information required by certificate users in industry applications.

1.4.8 Other Participants

Other participants in the SRCA e-Certification activities include other types of entities that are not mentioned above and are part of the SRCA certification system and are related to the e-certification services. For example, SRCA-selected PKI application technology service providers, directory service providers, etc.

1.5 Application of Certificates

1.5.1 Application of suitable certificates

Certificates issued by SRCA can functionally meet the following security requirements, and unless otherwise required, SRCA is generally not responsible for the implementation of the following security requirements: identity authentication - to ensure the authenticity of the identity of the certificate holder using the SRCA trust service; Verify information integrity – to ensure that when using SRCA certificates and digital signatures, it can verify whether the information has been tampered with during the transmission process, and whether the information sent and received is complete and consistent; Verify digital signatures - Verify digital signatures, the basis for the non-repudiation of trust-body transactions. It is important to note that the non-repudiation of any electronic communication or transaction shall be adjudicated in accordance with the law and dispute resolution process. The SRCA certificate supports confidentiality. Confidentiality guarantees the secrecy of the sender's and receiver's information, which will not be disclosed to other parties not legally authorized. However, SRCA is not obliged to assume responsibility for confidential events. SRCA shall not be liable for any direct or indirect damages or losses arising from the confidential use. SRCA currently supports two different trust levels of user certificates, official certificates and test certificates. Applicants for the official certificate must pass the prescribed entity identity authentication and identification procedures required by SRCA, which are generally valid for 1 year. The test certificate is generally valid for no more than 3 months. SRCA generally does not accept special requirements from certificate subscribers for the validity period of the certificate unless the sponsor, the certificate application industry organization and the SRCA have negotiated and formed a specific agreement on the validity period of the certificate. Entities and individuals involved in the issuance, application for, acceptance, operation, management, and use of certificates should be familiar with the terms, conditions, requiremetns, suggestions, and rights and interests set forth in this CPS.

SRCA certificate can be applied in many fields such as e-commerce, e-government, corporate IT drive, online information transmission, online public services, etc., providing basic trust services for the construction of internet trust environment. For more information, please refer to Sinorail CA website at www.sinorailca.com. Certificate applicants, subscribers, relying parties, and other entities can independently judge and decide to adopt the corresponding suitable certificate type, understand the type and scope of application of certificate, and choose their own manner of application according to their actual needs.

Except as specifically stated in this CPS, SRCA shall have no obligation to bear additional liability for damages arising from any use of the certificate.

1.5.2 Certificate application lists or types prohibited by certificates issued

The SRCA certificate is forbidden to be used in any circumstance of violation of national laws, regulations or compromising national security, otherwise the resulting legal consequences shall be borne by the subscriber concerned.

Digital certificates issued by SRCA realize associated binding of entity information about individual, organization and equipment mainly in such application scenarios as identity authentication, data integrity, data confidentiality and non-repudiation in the railway industry, so the legal consequences of any use outside the railway industry will be borne by subscribers themselves.

1.6 Policy management

1.6.1 Policy Document Management Organization

In accordance with the requirements of the Electronic Signature Law of the People's Republic of China, the Administrative Measures for Electronic Certification Services and other laws and regulations, Sinorail CA formulates this CPS.

The Security Policy Committee of Sinorail CA is the highest governing body for SRCA certification practice statement, which is composed of management personnel, technical personnel and customer service personnel convened by Security Strategy Committee, responsible for reviewing and approving CPS, and serving as the highest decision-making body for CPS implementation inspection and supervision.

1.6.2 Contact Details

SRCA performs strict version control of the certification practice statement, of which Sinorail CA is responsible for interpretation.

Tel: 010-51892503

Address: 2nd Floor, Building 1, Yard 2, Maliandao South Street, Xicheng District, Beijing

Zip code: 100055

Email: srca@sinorail.com

1.6.3 CPS Approval Procedure

The CPS of SRCA is drafted by a special person or writing team designated by the security policy committee of Sinorail CA, and then submitted to the security policy committee of Sinorail CA for review. If a change is required, a designated person or writing team will submit a change report and make modifications, and the security policy committee of Sinorail CA will study and analyze the change suggestions provided and solicit the relevant opinions of legal counsel to form a final resolution. SRCA will publish the official document of the revised Certification Practice Statement on its website after the resolution is formed.

1.7 Definitions and Abbreviations

Public Key Infrastructure (PKI): Public Key Infrastructure (PKI) is an infrastructure established using public key theory and technology to provide information security services. The public key system is currently the most widely used encryption system, in which the encryption key and the decryption key are different, the information sender uses the receiver's public key to send the encrypted information, and the receiver uses his own private key to decrypt it. This approach not only ensures the confidentiality of the information, but also ensures that the information is non-repudiated. At present, the public key system is widely used in the fields like CA certification, digital signature, and key exchange.

Certification Authority (CA): A trusted third-party organization or company that issues electronic signature authentication certificates for the creation of digital signatures and public/private key pairs. In this CPS, it refers to the Sinorail Digital Certification System or SRCA.

Registration Authority (RA): The registration authority of the certificate, which is responsible for application for the certificate. In this CPS, it refers to the registration authority of Sinorail Digital Certification System.

Key Management Center (KMC): Key Management Center is responsible for the whole process of managing and maintaining keys, including generation, storage, backup and recovery, etc. In this CPS, it refers to Sinorail KMC.

CPS: Certification Practice Statement is a detailed description and statement of the rules followed by the business practices (such as issuance, management, revocation, and renewal of certificates or keys) of the electronic certification service organization throughout the life cycle of the certificate service, and provides other business, legal and technical details. SRCA CPS is the operating rules of SRCA certificate-related services and systems.

Certificate Policy (CP): Certificate Policy is a designated collection of rules formulated with respect to electronic certification service organization, indicating the suitability of a certificate for a particular group and (or) specific application class having general security requirements.

Certificate revocation list (CRL): A list of revoked certificates issued and published by the certification authority. Certificate revocation might occur due to expired certificates, theft of private keys, or other reasons. It is also known as certificate revocation list and certificate blacklist.

CA revocation list (ARL): Certification authority revocation list is a list of public key certificates of CA that are marked as revoked, indicating that these certificates are already invalid.

Online Certificate Status Protocol (OCSP): Online Certificate Status Protocol, part of the X.509 public key infrastructure, is a protocol for judging the status of a certificate without requesting a CRL.

Electronic Signature Certification Certificate (Certificate): A certificate is a data message or other electronic record issued by an authoritative, trustworthy and impartial third-party electronic certification service organization that can prove the connection between electronic signer and electronic signature making data. The certification authority can issue its own certificate, a self-signed certificate which is called the root certificate of the CA and is used to sign subordinate certificates.

Electronic signer: refers to an entity that holds the data for the creation of electronic signatures and executes electronic signatures in its own capacity or in the name of the one it represents.

Electronic signature relying party: refers to an entity that engages in relevant activities based on reliance on electronic signature authentication certificates or electronic signatures.

Private key (electronic signature making data): is one of two keys generated by an asymmetric algorithm, uniquely held by the end subscriber, and used to make electronic signatures.

Public key (electronic signature verification data): It is one of the two keys generated by the asymmetric algorithm, which is bundled into the electronic signature authentication certificate and published on the public network through SRCA to verify the validity of the electronic signature information.

2.Information Release and Information Management

2.1 Release of certification information

SRCA provides information services via its website at www.sinorailca.com, including but not limited to the following: certification practice statement (CPS), certificate policy (CP), certificate and certificate revocation list (CRL) query service, online certificate status query service (OCSP) and information released by SRCA from time to time. SRCA certificate subscribers can query relevant information via SRCA website at www.sinorailca.com.

SRCA publishes relevant information about the status of the certificate through the Directory Service (LDAP), and subscribers can obtain information about the certificate by accessing SRCA's directory server. SRCA stores the public information about the user's identity authentication and certificate related information, and does not contain any transaction data, with data information stored in the form of a database. After the SRCA system successfully issues a certificate, the subscriber certificate and CRL are published to the directory server at the same time for the subscriber to query the certificate online. SRCA certificate subscribers can query, download, and verify subscriber certificates through LDAP.

2.2 Timing or Frequency of Release

When a certificate is issued through a directory server, SRCA will publish it at the same time as the certificate is successfully issued. After suspending or revoking a certificate, the issuing authority must update the certificate revocation list and online certificate status protocol within 24 hours by issuing a suspension and revocation announcement in the SRCA database. The latest CRL can also be released manually as needed.

Unless otherwise specified, SRCA guarantees to publish Revocation Lists (CRLs) for all types of certificates at least once every 24 hours, providing online certificate status protocol (OSCP). In the event of an emergency, SRCA may, at its sole discretion, shorten the time taken to publish the certificate revocation list. The announcement of the website, the release of SRCA CPS, the application of certificates, learning materials and other information are updated from time to time, without fixed release time or frequency.

2.3 Information repository access control

2.3.1 Release and processing of information

SRCA will publish new information (e.g. announcements, learning materials, certificate applications, etc.) on the website in a timely manner. Only authorised SRCA staff have the right to process the information on the SRCA website.

SRCA publishes certificate information and CRL information to the outside, and any SRCA subscriber or non-subscriber can use LDAP to query the certificate and obtain the current certificate status information.

2.3.2 Information access control and security audit

SRCA has information access control and security audit measures in place to ensure that only authorized SRCA staff are allowed to write and modify announcements or released information on the SRCA website. The SRCA website is not physically associated with the SRCA system.

2.3.3 Information rights management

SRCA may, when necessary, choose whether or not to implement access management of information to ensure that only authorized persons or institutions have access to information under SRCA's control and to ensure the actual interests of SRCA-related entities.

3.Identification and authentication

3.1 Naming

3.1.1 Name type

In accordance with specific issuance procedures, the certification body keeps specific records related to the certificate registration process and authenticates the identity of specific objects to distinguish them from other applicants. The main identifying name (SubjectName) of a certificate generated or issued by SRCA is in the form of X.501 Distinguished Name (DN). Each certificate subscriber will correspond to a distinguished name as specified in X.509. The certification authority, which acts as a trusted third party, is responsible for confirming the connection between the public key and the named entity. This confirming relation is unambiguously expressed through a certificate. The naming can be either negotiated between SRCA and the applicant, or done independently by the applicant.

3.1.2 Requirements for the meaning of name

The user identification information used in the SRCA logo name generally has a clear, traceable and positive representative significance, so the subscriber should use the real name, such that the individual subscriber shall use the name indicated on the identity document; corporate subscribers shall use the name indicated on the business license, organization code certificate of enterprises and institutions, etc.; device certificate should use a name that identifies the device. Anonymity or pseudonymization is allowed in special circumstances.

3.1.3 Anonymity or pseudonymization of subscribers

The SRCA allows subscribers to use anonymity or pseudonyms, but only limited to application for certificate for which the party or government departments have special requirements. The Subscriber must clearly state the purpose and scope of use of certificate for which it filed anonymous or pseudonymous application at the time of application, and SRCA will strictly review it and require the subscriber to ensure that the scope of use of the certificate is controlled and sign an agreement, provided that any and all consequences caused by any use beyond the scope shall be borne by the Subscriber. The name will be an abstract common name, such as: zf1401020012, bb140000007602, etc. The SRCA will archive applications filed by user departments with special requirements

3.1.4 Rules for different forms of names

The content format of the distinguished name DN of the certificate issued by SRCA conforms to the way of naming of X.501 Distinguished Name (DN), and the distinguished name of user certificate from Sinorail CA comprises the components listed in the following table:

Distinguished Name (DN)	Description	Contents (exemplary)
Country(C)	The name of the country	C=CN
Organization(O)	Certificate Authority	O= Sinorail Certification Authority
Organization Unit（OU）	The name of the organization or department	This may be left blank. It can be used as a reserved field for application, and the specific definition is done in conjunction with the certificate application. A certificate can contain multiple OU attributes.
Common Name（CN）	The general common name of the certificate holder	CN=Zhang San This field is required.

The common name CN is included in the subject of each certificate, and the way of naming varies from one type of certificate to another, but the common name of all certificate subscribers needs to be scrutinized. The general way of naming is as follows:

1	Personal Certificate	Individual's name (as indicated on the ID card)
2	Organization Certificate	The name of the organization or a department subordinate to the organization (consistent with that indicate on the business license, organization code certificate and other valid ID documents of the organization)
3	Device	A name that identifies the device (such as a domain name or IP address)

	certificates	
4	Event-based certificates	Determine the logo name based on business and scenario requirements.

3.1.5 Uniqueness of name

For all SRCA certificate holders, the distinguished name must be unique. SRCA effectively identifies certificate holders based on this name. When the same name appears, the first applicant will take precedence to use the name, and SRCA has no right or obligation to deal with the relevant disputes arising therefrom, so the relevant users may apply to the relevant competent authorities for resolution.

When the name of a subscriber or applicant is proved to be the property of another subscriber or applicant by a legal document issued by the relevant authority, SRCA will immediately revoke the right of the previous user to use the name, and the user must bear the legal liability arising therefrom.

3.1.6 Identification, authentication and role of trademarks

For the use of a trademark as an identifier, documentary proof of ownership of the trademark registrant shall be provided to SRCA. SRCA respects the rights of registered trademarks to and in the name of any subscriber and prohibits any infringement upon the intellectual property rights of others by any applicant for the certificate. However, SRCA does not verify or endorse whether the identifier provided by the certificate applicant in its certificate application has intellectual property rights, and does not guarantee the uniqueness of such rights. SRCA shall not be liable for arbitration or conciliation of disputes arising from the ownership of trademarks, service marks, etc., which is not within the scope of SRCA's terms of reference.

3.2 Initial Identity Confirmation

3.2.1 Methods to prove possession of a private key

The issuing authority must verify the legitimacy and correctness of the applicant's possession of the private key. Verify the applicant's private key by at least any one of the following methods:

(1) Prove that the certificate applicant holds the private key corresponding to the registered public key through the digital signature contained in the certificate request. In the SRCA electronic certification service system, the private key is generated on the user side, the certificate request information contains a digital signature made with the private key, and SRCA uses its corresponding public key to verify the signature.

(2) SRCA provides the certificate applicant with the initialization information required to complete the certificate application. The certificate applicant must use these initialization information in order to apply for the certificate or in certain operations of the certificate to assure the SRCA that he or she is the rightful owner of the private key.

SRCA requires certificate applicants to keep their private keys properly, so they are considered to be the sole holders of their private keys.

3.2.2 Authentication of identity of an organization

In the process of authenticating the identity of an organization applicant, SRCA will carry out different verifications according to the requirements of each kind of certificate. The certificate application form needs to be signed by the authorized representative (agent) of the organization, and the agent should present the identity document for identity authentication. SRCA or its authorized BTs and other electronic certification service organizations must check the documents submitted by the applicant, and the applicant shall provide SRCA with valid proof of the existence of the organization or server, including but not limited to business license, tax registration certificate, organization code certificate of enterprises and institutions, etc., and the identity certificate of the legal representative shall also be provided when applying for the legal representative certificate; The applicant has the obligation to ensure the authenticity and validity of the application materials and assumes the legal responsibilities related thereto. SRCA is not obliged to screen the legitimacy of the applicant's identity documents (e.g. ID card) after conducting a limited review prescribed by law.

SRCA retains all application materials of the organization for a specified period of time, which is determined by the requirements of laws, policies and competent authorities.

3.2.3 Authentication of Individual Identity

In the process of authenticating the identity of individual applicants, the following valid identity documents may be used: ID card, passport, military officer ID, police officer ID, soldier ID, non-commissioned officer ID, civilian officer ID, etc. The certificate application form bears the signature of the applicant himself or a duly authorized representative of the certificate applicant. SRCA authenticates individual identity primarily through face-to-face identification. SRCA compares the applicant with two copies of identification (original and photocopy). The identification document must be a valid ID. If the identity of the individual applicant has been explicitly confirmed by the SRCA or the BT, the SRCA or BT may rely on the existing attestation.

The applicant must bear the responsibility for the authenticity of the materials, and SRCA is not obliged to screen the legitimacy of the applicant's identity documents (such as ID cards) after conducting a limited review prescribed by law. SRCA and its authorized registration authority and BT shall retain all application materials of the applicant for a specified period of time, which shall be determined by the requirements of laws, policies and competent authorities.

3.2.4 Confirmation and authentication of domain names (or IP addresses).

If the name of the certificate is a domain name (or IP address), in addition to the review of the written materials submitted by the applicant, SRCA requires the applicant to provide additional proof of the right to use the domain name (or IP address), and the applicant must bear the responsibility for the authenticity of the materials, provided that SRCA is not obliged to screen the legitimacy of the certification materials after conducting a limited review prescribed by law.

3.2.5 Non-verified subscriber information

Information other than the information contained in the subscriber certificate is the subscriber information that has not been verified.

3.2.6 Authorization Confirmation

To ensure that the agent has specific permissions to obtain digital certificates on behalf of the organization, the organization is required to authorize them. When an organization affixes the organization's official seal to SRCA's digital certificate application form, it proves that the organization confirms the authorization of the agent.

3.2.7 Interoperability Criteria

For other electronic certification service organizations, if there is an agreement between the two parties, SRCA will accept the information authenticated by the organization and issue the corresponding certificate according to the contents of the agreement. If there is no agreement between the parties, SRCA will decide whether to accept the information that has been authenticated and reviewed by other agencies for handling according to its business requirements.

If there are provisions in national laws and regulations in this regard, SRCA will strictly enforce them.

3.3 Identification and authentication of key renewal requests

3.3.1 Identification and authentication of routine key renewal

Before a subscriber certificate expires, the subscriber needs to obtain a new certificate to maintain the continuity of certificate usage. SRCA generally requires the subscriber to generate a new key pair in place of the expired key pair, known as a "key renewal".

When a subscriber uses the current private key to sign the key renewal request, the authentication of the subscriber is either identified by using the public key held by the subscriber to verify and confirm the signature or identified and authenticated using the same process as initial authentication.

For SRCA certificate authentication services, certificates with the same issuer, subject name, and certificate purpose can only be issued through key renewal or certificate renewal before the certificate validity period expires. Unless the certificate is revoked first, one cannot obtain a certificate with the same issuer, subject name, identification and certificate purpose by applying for a new certificate before the certificate’s valid period expires.

The event-based certificates don’t involve key renewal.

3.3.2 Identification and authentication of key renewal after revocation

SRCA does not provide key renewal for any certificate that has been revoked, so subscribers for revoked certificates must undergo identity authentication and registration again and apply to SRCA for reissuance of the certificate. It is the responsibility of subscribers to provide accurate and valid information in the certificate application and to provide relevant supporting documents when applying for the reissuance of the certificate.

3.4 Identification and authentication of revocation requests

The identification and authentication of subscriber revoked certificates is carried out by one of the following methods:

(1) Submit a revocation application to SRCA or its authorized certificate service organization and undergo identity authentication.

(2) If the on-site audit cannot be conducted due to the constraints of the conditions, SRCA will first suspend the certificate to temporarily invalidate the certificate until the identity authentication is completed, and then revoke the certificate. The identification and authentication of the subscriber when revoking by himself or herself are subject to the same process as the original identity verification, as detailed in 3.2.2 authentication of identity of an organization and 3.2.3 authentication of individual identity.

If the identity of the applicant has been expressly confirmed by SRCA or its authorized certificate service organization, then SRCA or its authorized certificate service organization may rely on the existing attestation.

If a BT applies for revocation of the certificate of a subscriber because the subscriber has not fulfilled its obligations under this CPS, it is not necessary to identify or authenticate the subscriber.

SRCA warrants that the authentication of revocation requests is carried out reasonably.

4.Operating Requirements for Certificate Lifecycle

The certificates described in this section include CA certificates, administrator certificates, and ordinary subscriber certificates. This section describes the certification practice statement mainly using ordinary subscriber certificate as an example.

4.1 Application for Certificate

4.1.1 Applicant entity

In the process of applying for a certificate, the entities involved in the entire application process mainly include:

(1) Certificate applicant, including individuals, government agencies, enterprises, public institutions, social organizations and other organizations. Any lawful organization and individual, as well as other internet entities with clear identity attribution, can apply for a certificate to ensure the security and reliability of internet operations;

(2) Registration service handling organization, including RAs, BTs, sponsors, and corresponding systems, administrators, and operators, etc.;

(3) Electronic certification service organization, referred to as SRCA in this CPS;

(4) Subscriber, the entity that receives the certificate from SRCA, as detailed in 1.4.5.

(5) Competent authorities, including various competent authorities prescribed by the "Electronic Signature Law of the People's Republic of China", "Measures for the Administration of Electronic Certification Services", "Measures for the Administration of Ciphers for Electronic Certification Services ", etc.

4.1.2 Certificate Application Process and Responsibilities

I. Certificate application process

1. The certificate applicant obtains the digital certificate application form (in triplicate) through Sinorail CA website www.sinorailca.com or at the SRCA authorized business terminal, fill in the application form seriously, truthfully and completely according to the precautions on the application form, and sign (individual) or seal (entity) the application form.

2. The certificate applicant brings the application form and identification materials to the SRCA authorized BT for identity verification.

3. The BT checks the certificate applicant and relevant identity information. If the authentication fails, the BT will refuse to issue the certificate to the user and archive the failed information.

4. If the identity authentication is passed, the BT enters the information, reviews the certificate application information, and submits it to the CA for processing. The BT may enter the information on the certificate applicant in advance.

5. The CA issues the certificate according to the certificate request.

6. After downloading the certificate, the BT submits it to the applicant.

II. Responsibilities of the participants

1. Responsibilities of electronic certification service organization

Ensure that the signature private key of the electronic certification service organization itself is securely stored and protected within SRCA, and that the security mechanism established and implemented by SRCA is in line with the provisions of relevant national policies.

The electronic certification service organization audits and manages its authorized registration authority and business terminals to ensure the security and reliability of the entire application process.

The electronic certification service organization ensures the safe and reliable operation of the entire CA system. SRCA will not be liable for any failure or delay in operation due to objective accidents or other force majeure events. These events include but not limited to strike or other labor disputes, violence, civil commotion, intentional or unintentional acts of suppliers, acts of God, war, fire, explosion, earthquake, flood or other disasters.

Due to the advancement and development of technology, electronic certification service organizations will require certificate subscribers to renew their certificates in a timely manner to ensure the reliability of certificates.

2. Responsibilities of the RA

The electronic certification service organization manages the RA in accordance with this CPS and the license agreement. The RA obtains the authorization of the SRCA in accordance with the procedures, follows this CPS, the licensed operation agreement of SRCA and other standards and procedures published by SRCA, accepts and processes the certificate service requests of the certificate service applicant, and sets up and manages the subordinate BT in accordance with the authorization. The RA must follow the service acceptance specifications, system operation specifications and management specifications formulated by SRCA, and determine the way of management of subordinate BTs. Ensure that its operation systems are in a secure physical environment with corresponding security management measures in place in accordance with the provisions of this CPS. SRCA will continuously improve and publish relevant norms and standards in a timely manner.

3. Responsibility of the business terminal (BT).

BT is authorized by SRCA and its superior RA in accordance with the procedures to accept and process certificate service requests from applicants for certificate services in accordance with this CPS and the relevant licensed operation agreement and other standards and procedures published by SRCA. The BT must follow the service acceptance specifications, system operation specifications and management specifications formulated by SRCA and its superior RA, while SRCA and its superior RA will continuously improve and publish the relevant norms and standards in a timely manner. In accordance with the specifications published by this CPS, SRCA and its superior RAs, the BT has the right to decide whether to provide the corresponding certificate services to the applicant. In accordance with the provisions of this CPS, the BT shall ensure that its operation systems are in a secure physical environment and that corresponding security management measures are in place. SRCA and its superior RA manage BTs in accordance with this CPS and the license agreement, including conducting service qualification audits and compliance checks. SRCA has the final authority to process all service requests from certificate services applicants. SRCA reserves the right to review the applicant's submittals.

BT is responsible for the verification of information on the identity data of all certificate service applicants, regardless of whether such applications are accepted or not. All losses caused by a BT's lax examination of applicants' qualifications shall be borne by the BT

4. Responsibilities of sponsor

The sponsor must bear all the fees for the certificate advanced by it and pay in full in the manner prescribed by the SRCA. The advance made by a sponsor indicates that it is willing and able to assume the responsibility for guaranteeing the authenticity of the identity of the certificate service applicant as stipulated in this CPS and relevant agreements of SRCA.

5. Responsibilities of certificate applicant

Certificate applicants must strictly adhere to the specifications related to certificate applications and the ownership and secure storage of private keys. The certificate applicant undertakes that all statements and information filled out on the certificate application form must be complete, accurate, true and correct and available for inspection and verification by the issuing authority; The certificate applicant shall be liable for any legal consequences arising from the provision of false or forged information. If the issuing authority is unable to correctly issue the certificate due to the applicant's own reasons, the applicant shall bear the relevant losses and responsibilities.

The certificate applicant must carefully read and understand the content of this CPS or the security measures recommended or used by SRCA in order to fully understand the importance of private key retention and ensure the security of private keys. Before applying for and accepting the certificate and its related services, the certificate applicant needs to be familiar with the regulations of this CPS and the policies and regulations related to the certificate, and SRCA will consider that the holder has understood the content of this CPS and undertakes to comply with the relevant restrictions on the use of the certificate by the certificate holder before receiving any application for services from the certificate applicant.

Once the SRCA approves the application of a certificate applicant and issues a certificate to him/her, the certificate applicant becomes a certificate subscriber, regardless of whether the certificate has been obtained or not.

Subscribers must ensure the security of their private keys. The SRCA only informs, but does not require the certificate applicant, to comply with the security measures set forth by the SRCA; Subscribers may choose any measure they deem able to keep private keys confidential; At the same time, SRCA declares that SRCA does not assume all liability arising from problems with the Subscriber's private key storage, unless the Subscriber can legitimately prove that SRCA is primarily responsible for such problems.

7. The responsibility of the certificate application industry organization

(1) The certificate application industry organization is tasked with examination and approval of whether the certificate subscriber has the application authority in the industry in which it operates, and bears the corresponding responsibility;

(2) According to the specific application, the certificate application industry organization may review the authenticity of the identity of the industry subscribers according to the agreement and assume the corresponding responsibility;

(3) The certificate application industry organization is not responsible for requiring industry users to accept the SRCA certificate and become SRCA certificate subscribers.

8. Responsibilities of the Relying Party

When relying on any certificate issued by SRCA, the relying party must ensure compliance with and implement the following terms:

(1) The relying party is familiar with the terms of this CPS and the policies and laws related to the certificate, and understands the purpose and restrictions on the use of the certificate;

(2) Before relying on a certificate issued by SRCA, the relying party must conduct a reasonable review of the certificate, including but not limited to: checking whether the certificate is within the validity period; Check the valid CRL published by SRCA to get the status of the certificate. SRCA is of the opinion that the relying party has complied with this clause at all times. Once the relying party violates this clause due to negligence or other reasons, the loss caused by it shall be borne by itself. SRCA reserves the right to take legal action in the event of any loss caused to SRCA;

(3) All relying parties must acknowledge that their reliance on certificates indicates that they acknowledge and understand the relevant provisions of this CPS, including the terms of exemption, rejection and limitation of obligations.

4.2 Certificate application review

4.2.1 Performing identification and authentication functions

SRCA will strictly implement user identification and authentication when handling certificate application and registration formalities. For details of the authentication process, please refer to 3.2.2 Authentication of organizational identity and 3.2.3 Authentication of individual identity. SRCA will strictly check all kinds of credentials provided by the user, process the business after confirming that they are correct, and will properly keep all kinds of supporting materials and user certificate application forms provided by the user.

After a certificate has been issued, SRCA shall not be responsible for monitoring and investigating the accuracy of the information contained in the certificate unless notified of the security breach described in this CPS with respect to the certificate.

4.2.2 Certificate application review process

After receiving the applicant's application, SRCA will review the application information and identity information and approve the application after confirming that it is accurate. If the applicant fails to pass the authentication, SRCA will reject the certificate application and notify the applicant of the failure of authentication. SRCA has the right to refuse to explain the reasons for the failure of authentication without notice to the applicant, unless expressly required by laws and regulations. In the event of a failure of authentication due to third-party information, SRCA will provide the third party's contact information to the applicant for easy query. SRCA uses reasonable means to notify the certificate applicant that its certificate application has failed.

SRCA may, in its sole discretion, refuse to issue a certificate to a particular applicant without explanation or being liable for any loss or expense incurred as a result. Unless fraudulent or falsified information is submitted by the certificate applicant, SRCA will refund the certificate purchase fee paid by the certificate applicant after refusing to issue the certificate, except for the previously incurred costs such as postage and material costs paid by the certificate applicant. Rejected certificate applicants may apply again subsequently.

4.2.3 Time required to process certificate application

SRCA will authenticate and review the information submitted by the certificate applicant within the five days of acceptance of user application, and make a decision to approve or reject it.

The ability of the BT to process the certificate application more quickly within the above time frame depends on whether the certificate applicant has submitted the relevant information truthfully, completely and accurately, and whether it has responded to the SRCA management requirements in a timely manner.

4.3 Certificate issuance

4.3.1 The acts of the registration authority and the electronic certification service organization in the issuance of certificates

Once the applicant has submitted the application, the subscriber is deemed to have consented to the issuance of the certificate by SRCA, despite the fact that the certificate has not yet been obtained.

After the identity of the certificate applicant is verified by BT subordinate to the registration authority, the user certificate DN information and public key are sent to the SRCA certificate issuance system in a secure manner.

The certificate issuance system organizes the user DN information and public key submitted by the RA according to the X.509 certificate format standard, issues a digital certificate, and then sends it to the RA. The issued certificate is released through LDAP. The release of the certificate means that the SRCA has finally and officially approved the certificate application. The RA issues the successfully issued digital certificate to the user within the specified time.

4.3.2 Notification to subscribers from e-certification service organization and registration authority

The SRCA digital certificate is uniformly applied for and issued by the Sinorail CA, and stored in the certificate carrier UKEY or stored in other storage media according to the certificate applicant's requirements, in which case the certificate applicant fills in or supervises the SRCA staff to fill in the application information, and the public key certificate is stored into the certificate carrier UKEY or other secure storage media after the certificate is successfully issued, as well as delivered in such manner as agreed with the certificate applicant.

SRCA does not provide the service of door-to-door certificate installation for subscribers. If a certificate applicant needs it, SRCA may come to the site for installation, but there is a corresponding service fee payable by the applicant. SRCA and its authorized certificate service organizations provide hotline support services. The contact details are published by the websites of SRCA and its authorized certificate service organizations.

4.4 Certificate Acceptance

4.4.1 Acts that constitute acceptance of certificates

The certificate applicant is deemed to have agreed to accept the certificate from the moment the certificate is issued upon successful submission of the certificate application to the SRCA.

Where a certificate is stored in the certificate carrier UKEY, it will be delivered via personal delivery or real-name mailing by SF Express or EMS.

Where a certificate is stored in other secure storage media, such as mobile terminal and PC terminal, it will be delivered in such a manner as agreed with the certificate applicant.

After obtaining the certificate, SRCA certificate subscribers should check the certificate subject information and other identification contents in detail, bundle it with the corresponding railway industry information system, and contact SRCA within 5 working days to solve any problems. After the subscriber accepts the digital certificate, he or she should properly keep the private key corresponding to the certificate.

4.4.2 Release of of certificates by electronic certification service organization

SRCA will publish a copy of the certificate in its information repository and directory service. SRCA may decide to publish a copy of the certificate in other information repositories. Subscribers can also publish their certificates at other venues. Subscribers and relying parties can download their own or others' certificates through the Certificate Directory service.

4.4.3 Notification from the e-certification service organization to other entities

Once the Subscriber has accepted the Certificate, SRCA will not specifically notify entities such as Registration Authorities, BTs and competent authorities, etc., which may obtain the Subscriber's Certificate and related information through directory service or by querying the SRCA information repository.

4.5 Use of key pairs and certificates

4.5.1 Use of private keys and certificates by subscriber

When using a certificate, the subscriber must properly keep and store the private key associated with the certificate to prevent loss, leakage, tampering, or theft. Anyone who uses a certificate must verify the validity of the certificate, including whether the certificate has been revoked, whether it is still valid, whether it was issued by SRCA, etc.

The Participants (SRCA, Certificate Subscribers, Relying Parties, etc.) have the rights and obligations pursuant to this CPS when using the signatures and signed information relating to the certificates issued by SRCA.

Each participant is deemed to have been notified and agrees to abide by the terms of this CPS and the agreements and specifications signed between SRCA and the parties, as well as refuse to use any certificates and private keys beyond the provisions of this CPS.

The various types of certificates issued by SRCA are only used for the use of private keys and certificates within the scope of application specified in the SRCA certificate policy, otherwise, their application is not protected by relevant laws and SRCA certificate policies.

The scope and purpose of a certificate can be specified in the certificate issued by SRCA, such as the Certificate Policy Object Identifier (OID), which determines whether a particular certificate can be trusted in a particular application, in which case the certificate will only be allowed to be used within this scope.

Scope of application of certificates:

Certificate type	Type of application scope	Purpose of the subscriber's private key and certificate
Personal Certificate	Personal Secure Email Certificate	The Personal Secure Email Security Certificate contains the subscriber's email address, public key, and SRCA signature. Subscribers using secure email certificate can send and receive encrypted and digitally signed messages.
	Personal identity certificate	The personal identity security certificate contains the personal identity information of the certificate holder, the public key and the signature of the SRCA, which identifies the personal identity of the certificate holder in network communication, and can be used to indicate the identity of individuals in various online activities such as contract signing, ordering, and payment.
	Personal code signing certificate	Personal code signing certificate is a digital certificate issued by CA to independent software writers, containing ID information, public key and SRCA signature of the software provider.
Organization Certificate	Enterprise or institution secure email certificate	The entity email security certificate contains the subscriber's email address, public key, and SRCA signature. Subscribers using secure email certificate can send and receive encrypted and digitally signed emails.
	Enterprise or Institution Identity Certificate	The organization identity security certificate contains the organization information, public key, and SRCA signature, which identifies the identity of the certificate holder in network communication.
	Certificate of legal representative	The legal representative certificate is used to indicate that the certificate holder is the legal representative of the organization, and identifies the identity of the legal representative of the organization in the network communication, containing the identity information of the certificate holder, the public key and the signature of the SRCA.

	Enterprise or institution code signing certificate	Enterprise code signing certificate is a digital certificate issued by CA to software providers, containing ID information, public key and SRCA signature of the software provider.
Device certificates	Server certificate	The server certificate contains the server information, public key, and SRCA signature, which identifies and verifies the server's identity in network communication. In a network application system, the server software uses a certificate mechanism to ensure the security of communication with other servers or clients.
	Gateway certificate	The payment gateway or VPN gateway certificate contains the gateway information, public key, and SRCA signature, which identifies the identity of the gateway server in network communication.
	SSL certificate	SSL certificate contains domain name, IP information public key and SRCA signature.
	Application system certificate	Application system certificate contains name and other identifying information, public key and SRCA signature of an application system.
	Terminal device certificate (mobile terminal, PC terminal, etc)	Terminal device certificate contains the subject identifying information, public key and SRCA signature of the terminal.
	IoT device certificate	IoT device certificate contains the subject identifying information, public key and SRCA signature of the device.
Event-based certificate	Event-based certificate	Event-based certificate contains relevant data information, public key and SRCA signature of business scenario.

4.5.2 Signature and Verification

Signatures can only be created if the following conditions are met:

(1) It is created during the validity period of the certificate;

(2) The signature can be correctly verified by confirming the certificate chain;

(3) The relying party has not discovered or noticed the signatory's breach of the requirements of this CPS;

(4) The signatory and relying parties comply with all provisions of this CPS;

The use of the certificate does not imply that the subscriber has the right to act in the interest of any individual or to take any special action.

Verification of signature is done to confirm that the signature was created with the private key corresponding to the public key listed in the signer's certificate, and that the information that was signed after the signature was created has not been altered. Validating the validity of a certificate includes three aspects:

(1) Verify the signature in the certificate with the SRCA certificate to confirm that the certificate was issued by SRCA and that the contents of the certificate have not been tampered with.

(2) Check the validity period of the certificate and confirm that the certificate is within the validity period.

(3) Query the certificate status and confirm that the certificate is not included in the CRL (certificate blacklist).

When verifying an electronic signature, the relying party should know exactly what data has been signed, and in the public key cryptography standard, the standard signature information format can accurately represent the signed data.

4.5.3 Use of public keys and certificates by relying party

Before trusting a certificate and signature, the relying party should make due efforts and reasonable judgment independently. Except as otherwise set forth in this CPS, a certificate is not a commitment as to any rights or privileges from the issuing authority. The Relying Party relies on the Certificate and the Keys contained in the Certificate to the extent specified in this CPS, and makes a decision thereon.

The scope and purpose of a certificate can be specified in certain fields in the certificate issued by SRCA, and if these applications are specified in the certificate policy of SRCA, then the certificate will only be allowed to be used within this scope. When the relying party receives the digitally signed message, it should,

① Obtain the certificate and chain of trust corresponding to the digital signature.

② Confirm that the certificate corresponding to the signature is a certificate trusted by the relying party, and verify the validity of its certificate.

③ The purpose of the certificate applies to the corresponding signature.

④ Verify the signature with the public key on the certificate.

If any of the above steps fails, the relying party should refuse to accept the signature information. When the relying party needs to send encrypted information to the recipient, it must first obtain the receiver's encryption certificate through appropriate channels, and then use the public key on the certificate to encrypt the information. The relying party shall send the encryption certificate to the recipient along with the encryption information.

4.6 Certificate renewal

Certificate renewal means that SRCA issues a new certificate to a certificate subscriber without changing the subscriber's public key or any other information in the certificate. Subject to compliance with relevant national laws, regulations and rules, certificate renewal for subscribers shall be completed in principle in such a manner as key renewal is handled.

4.6.1How to renew a certificate

SRCA provides two ways to renew certificates: on-site and online:

4.6.1.1On-site renewal

Before the expiration of the validity period of the certificate, submit the paper renewal application materials and apply for the renewal of the certificate at the SRCA BT.

4.6.1.2 Online renewal

Submit the certificate renewal application on the SRCA digital certificate online certificate acceptance website and mail the paper renewal application materials to the SRCA BT for offline review, whereupon the user can download the renewed digital certificate online after passing the review (see Sinorail CA website www.sinorailca.com, " Online Renewal Self-Service" for the website address).

4.6.2 Circumstances of certificate renewal

Before the expiration of the certificate of a certificate holder, SRCA will make reasonable efforts to send a certificate renewal reminder to the certificate subscriber or sponsor before the certificate expires. Reasonable efforts include, but not limited to, website prompts, system prompts, written prompts, email notices or other means, and SRCA's use of any of the foregoing prompts or notices may be deemed that reasonable efforts have been made. In general, the certificate subscriber should submit a renewal application within one month before the certificate expires. Under special circumstances, an expired certificate can be renewed only if the application is made within one month after the expiration of the certificate and the service fee of the current month is paid retroactively.

4.6.3 Entities requesting certificate renewal

Any subscriber who legally holds a SRCA certificate that has not yet expired may apply to SRCA for renewal of the certificate it holds.

4.6.4 Processing of certificate renewal requests

When the subscriber applies for certificate renewal, the BT of SRCA will issue the corresponding "Digital Certificate Application (Renewal) Form" according to the type of certificate requested to be renewed, and the subscriber shall pay the corresponding fee according to the application form after filling it out. The BT shall renew the certificate according to the application form; the subscriber will collect the renewed certificate by virtue of the "User Copy" of the application form and the payment voucher.

It is the responsibility of the subscriber to provide accurate and valid information in the certificate application, provide relevant supporting documents, and pay the corresponding fees on time when applying for certificate renewal.

4.6.5 Precautions on certificate renewal

Subscribers are requested to decrypt encrypted files such as encrypted emails and back them up (e.g., copy the contents of the email and store it in clear text or save the email attachments) before renewing the certificate. After the preceding operations are completed, the certificate can be renewed. SRCA is not responsible for any loss that may arise from the subscriber's certificate renewal without decrypting the files.

4.6.6 Notification to subscribers when a new certificate is issued

SRCA will inform subscribers of the time and location to collect their new certificates when they submit certificate renewal application. It will automatically notify subscribers when they receive a renewed certificate or inform them face-to-face that a new certificate has been issued.

4.6.7 Acts that constitute acceptance of a renewed certificate

After a subscriber who needs to renew their certificates successfully submits a certificate renewal application to SRCA, the issuance of a new certificate means that the subscriber has accepted the certificate. Subscribers will collect the digital certificate by virtue of certificate renewal application form and payment vouchers, after which subscribers are requested to check the certificate and its content in detail, and can contact SRCA for resolution within 5 working days in case of any problem.

4.6.8 The issuance of the renewed certificate by the electronic certification service organization

Once a subscriber accepts the renewed certificate, SRCA will publish a copy of the certificate in its information repository and directory service. SRCA may decide to publish a copy of the certificate in other information repositories. Subscribers may also publicize their renewed certificates elsewhere.

4.6.9 Notification from the e-Certification Service Organization to other entities

Once a Subscriber has accepted the renewed certificate, SRCA will not specifically notify entities such as registration authorities, BTs and competent authorities etc., which may obtain the Subscriber's renewed certificate and related information through directory services or by consulting the SRCA Repository.

4.7 Certificate key renewal

Certificate key renewal means a subscriber or other participant generates a new pair of keys and applies for issuance of a new certificate for the new public key. Due to the constant updating of technology, SRCA can require subscribers to renew the key of the certificate for the security of encryption.

The validity period of the private key of the final subscriber is generally the same as the validity period of the certificate. However, for the CA's signing key, the validity period of the private key should be shorter than the validity period of the certificate. The reason for this is to prevent the certificate issued by the electronic certification service organization from becoming invalid shortly after issuance.

4.7.1 Circumstances of certificate key renewal

Subscribers must renew their certificate keys if:

(1) The certificate expires and the key pair's usage period also expires;

(2) The security of the certificate key pair cannot be guaranteed because it has been or is suspected to have been leaked, stolen, tampered with or otherwise;

(3) The certificate needs to be re-acquired after the certificate is revoked;

(4) Any and all certificates used within SRCA, including certificates of RAs and service operators, etc., must undergo certificate key renewal when the certificate expires.

4.7.2 Subscriber entity requesting the certificate key renewal

Any subscriber who legally holds a SRCA certificate that has not yet expired may apply to SRCA for renewal the certificate key it holds.

4.7.3 Processing of certificate key renewal requests

When a subscriber applies for certificate key renewal, the BT of the SRCA will issue the corresponding "Digital Certificate Application (Renewal) Form" according to the type of certificate with respect to which the key is requested to be renewed, and the subscriber shall fill in the application form and pay the corresponding fee according to the completed application form. The BT shall renew the certificate key according to the application form; The subscriber collects the certificate with the renewed key by virtue of the "User Copy" of the application form and the payment vouchers. When applying for a certificate key renewal, the subscriber is responsible for providing accurate and valid information in the certificate application, providing relevant supporting documents, and paying the corresponding fees on time.

4.7.4 Precautions on key renewal

Subscribers are requested to decrypt encrypted files such as encrypted e-mails and back them up (e.g., copy e-mail contents and store them in clear text or save e-mail attachments) before renewing the key. After the preceding operations are completed, the key can be renewed. SRCA is not responsible for any loss that may arise from the subscriber's certificate renewal without decrypting the files.

4.7.5 Notification to subscribers when a new certificate is issued

SRCA's notice to subscribers when issuing new certificates is the same as in 4.6.6.

4.7.6 Acts that constitute acceptance of key renewal certificate

The act of formally accepting a key renewal certificate is the same as in 4.6.7.

4.7.7 Issuance of the key renewal certificate by the electronic certification service organization

SRCA's issuance of the Key Renewal Certificate is the same as that of 4.6.8.

4.7.8 Notification from the e-Certification Service Organization to other entities

SRCA's notice to other entities is the same as in 4.6.9.

4.8 Certificate Change

Within the validity period of a certificate, when the subscriber information changes, the subscriber shall change the certificate and apply for issuance of a new certificate. SRCA will reissue the certificate after verifying and confirming the information submitted by the applicant.

4.8.1 Circumstances in which the certificate is changed

Certificate change refers to a circumstance in which a new certificate is issued due to changing the subscriber information in the certificate. When the subscriber's entity identity information changes, affecting the content of the certificate particulars, the certificate subscriber is obliged to report to SRCA and apply for the certificate change, and have the certificate reissued after revoking the certificate.

4.8.2 Subscriber entities requesting the certificate change

The subscriber entities requesting the certificate change are the same as in 4.6.3.

4.8.3 Processing of certificate change requests

When a subscriber applies for certificate change, the BT of SRCA will issue the corresponding "Digital Certificate Application (Renewal) Form" according to the type of certificate requested to be renewed, and the subscriber will pay the corresponding fee according to the application form after filling it out. The BT shall conduct certificate change according to the application form; the subscriber will collect the changed certificate by virtue of the "User Copy" of the application form and the payment vouchers.

It is the responsibility of the subscriber to provide accurate and valid information in the certificate application, provide relevant supporting documents, and pay the corresponding fees on time when applying for a certificate change.

4.8.4 Precautions on certificate change

After a certificate is changed, the validity period of the certificate remains the same as the original certificate. Other precautions are the same as in 4.6.4.

4.8.5 Notification to subscribers when a certificate is changed

SRCA's notice to subscribers when issuing new certificates is the same as in 4.6.6.

4.8.6 Act that constitute acceptance of changed certificate

The acts of formal acceptance of a changed certificate are the same as in 4.6.7.

4.8.7 Issuance of changed certificate by the electronic certification service organization

The issuance of changed certificate by SRCA is the same as in 4.6.8,

4.8.8 Notification from the e-Certification Service Organization to other entities

SRCA's notice to other entities is the same as in 4.6.9.

4.9 Certificate revocation and suspension

Subscribers, electronic certification service organizations, national legal authorities or government public authorities may require that a certificate be revoked or suspended.

4.9.1 Circumstances of certificate revocation

Certificate revocation is divided into active revocation and passive revocation, of which active revocation means that the subscriber actively applies for the revocation of its digital certificate, and the BT revokes the certificate after reviewing the application. Passive revocation means that the electronic certification service organization confirms that the user has applied for or used any certificate in violation of the CPS rules or any risky circumstance has occurred such as extinction of the certificate holder, leakage of private key or loss of UKEY, in which case the digital certificate is revoked.

I. During the validity period of the certificate, if any of the following circumstances occurs (including but not limited to the following circumstances), SRCA may directly revoke the certificate:

1. Due to the unsuitability of the certificate management system or the need for integration of the certificate system;

2. These entities entitled to claim revocation require revocation due to the fact that the certificate subscriber has failed to fulfill the agreement with the participants (e.g., failure to pay fees, etc.);

3. Violation of national laws and regulations and the main and material obligations stipulated in this CPS due to improper use of the certificate;

4. The public authorities of the government or the legal authorities of the state submit an application in accordance with formal and legal procedures;

5. When a subscriber applies for the certificate service, he or she provides untrue or deceptive materials;

6. It is found and confirmed that the certificate has not been issued in accordance with the procedures required by this CPS;

7. The electronic certification service organization loses the confidentiality of important data within the CA or the CA root key due to operational problems;

8. The private key of the certificate is lost, stolen, tampered with, leaked without authorization or damaged;

9. The execution of the subscriber's responsibilities is delayed or prevented due to force majeure, natural disasters, computer or communication failures, modifications of laws and regulations, government actions (including but not limited to the restrictive acts of the export control authorities) or other reasons beyond the reasonable human control.

II During the validity period of the certificate, a subscriber must submit a request for revocation if:

1. The private key corresponding to the public key in the certificate is leaked, stolen, tampered with or otherwise, causing security concerns about the private key;

2. The subscriber-related information in the certificate is changed and an application is therefore filed for certificate change;

3. The certificate is no longer required to be used for its original purpose and is therefore required to be terminated;

4. The relevant content in the certificate is inconsistent with the application materials submitted at the time of application;

5. The certificate holder has been unable to perform or violated the responsibilities and obligations stipulated in this CPS or other agreements, regulations and laws.

III. Other reasons for which SRCA deems it fit to revoke a certificate.

IV. SRCA is not obliged to disclose the reasons for the revocation of a particular certificate.

4.9.2 Entities requesting certificate revocation

Entities that can request the revocation of a certificate include:

1. Certificate subscribers who pay the certificate fee by themselves;

2. Sponsors or sponsor-type certificate service organization;

3. Duly authorized representative of the certificate holder;

4. Various organizations inside the electronic certification service system;

5. National legal authorities, government authorities and other public authorities.

4.9.3 The process for revocation request

If SRCA proactively discovers that a subscriber certificate meets the conditions for compulsory revocation, it will submit an application and written supporting materials, file it, and revoke the subscriber certificate within 24 hours after signing the mandatory revocation order. It is not necessary for SRCA to notify the Subscriber before the mandatory revocation of the Subscriber's certificate, but after the mandatory revocation, the Subscriber shall be notified by telephone, fax, website announcement or e-mail within 5 working days.

The public authorities of the government may also submit a request for certificate revocation, and must issue written supporting materials in accordance with the regulations, fill in the revocation application form, and sign and seal it. SRCA will revoke the certificate within 24 hours after review and approval of the submittals, and notify the subscriber within 5 working days via telephone, fax, website announcement or email.

The process of voluntary revocation is as follows:

1. The certificate subscriber (or its authorized agent) fills in the application form in writing, signs and seals the same, applies to SRCA for revocation, and submits legal supporting materials.

2. After receiving the revocation application, SRCA shall verify the legitimacy of the applicant's identity, authority and reasons for revocation, and file the review materials in writing, and make a revocation decision and deal with it in a timely manner after verifying that they are correct.

3. SRCA publishes the certificate revocation information to the information repository and directory service within 24 hours for query.

4.9.4 Grace period of revocation request

Once it is found that a certificate needs to be revoked, the subscriber should submit a revocation request in real time, or within 8 hours if the delay is caused indeed due to objective reasons.

SRCA mandatorily revokes the subscriber's certificate in cases where it should be revoked, and the mandatory revocation is effective immediately and the subscriber cannot request any grace period.

4.9.5 Time limit for the electronic certification service authority to process revocation requests

SRCA shall complete the whole process of processing of revocation request within 24 hours from receiving the complete revocation request materials, the completion of the review, making the revocation decision to the publication of the revoked certificate to the directory server.

4.9.6 The requirements for relying party to check certificate revocation

The certificate revocation list (CRL), as public information, has no security settings regarding read/write permissions, so the relying party can freely query it as needed. Before relying on a certificate, the relying party should actively check the status of the certificate according to the latest CRL published by SRCA. At the same time, it is also necessary to verify the reliability and integrity of the CRL to ensure that it is issued through SRCA and contains digital signature of SRCA.

4.9.7 CRL issuance frequency

CRL is one of the certificate issuance services provided by SRCA, and subscribers can access CRL to verify the current status of the certificate. In order to ensure that the CRL is issued at least once every 24 hours, the SRCA CRL adopts a policy of updating every 8 hours. Depending on the circumstances, the SRCA may, at its sole discretion, shorten the time it takes to generate and update CRLs.

4.9.8 The maximum lag time for CRL issuance

CRLs generally take effect within 24 hours of approving a revocation request. It can take effect immediately in special emergencies (regardless of the effects of network transmission conditions, because differences in the timeliness caused by network factors are allowed). Entry into force means that SRCA will publish the revoked certificate in the CRL.

SRCA undertakes to publish a certificate revocation list within 24 hours of the revocation at the latest after certificate revocation.

4.9.9 Availability of online status queries

SRCA provides a 7x24 LDAP directory query service. Additionally, OCSP is offered as an optional, complimentary method for online status verification.

4.9.10 Online Status Query Requirements

Online status query allows querying the real-time status of a certificate through information such as the serial number and subject of the certificate.

4.9.11 Other forms of publication of revocation information

OCSP is available as an optional and free method for distributing revocation information.

4.9.12 Special requirements for key compromise

When the root key of SRCA is compromised, SRCA will proactively revoke the certificate immediately and publish the certificate to the CRL in real time. SRCA bears the losses incurred to the subscriber due to the damage to the key and issues a new certificate for it in a timely manner.

4.9.13 Circumstances where a certificate is suspended

When a certificate is still valid, in order to retain the subscriber's right to use the certificate without applying for revocation of the certificate, the certificate can be suspended in any of the following circumstances:

1. The subscriber of the certificate requests to suspend the use of the certificate for a period of time;

2. The Subscriber fails to fulfill its obligations under the agreement with SRCA, but after applying to SRCA and obtaining its approval;

3. Entities other than certificate subscribers (or their authorized agents), such as electronic certification service organizations and their authorized service agencies, national legal authorities, government authorities and other public authorities. A request for certificate suspension is filed to SRCA and approval obtained from it.

4.9.14 Subscriber entities entitled to request certificate suspension

Only the certificate subscriber entity or its authorized agent, as well as the electronic certification service organization and its authorized service organization, national legal authorities, government authorities and other public authorities, etc., have the right to make a request for certificate suspension.

4.9.15 The process for suspending and unsuspending a certificates

When a subscriber applies for suspension and unsuspension of a certificate, the registration authority and BT of SRCA will issue the corresponding application form according to the type of certificate requested to be changed, and the subscriber shall pay the corresponding fee according to the completed application form after filling in the application. According to the application form, the registration authority shall make the certificate suspended or unsuspended When applying for certificate suspension or unsuspension, the subscriber is responsible for providing accurate and valid information in the certificate application, providing relevant supporting documents, and paying the corresponding fees on time. Entities other than certificate subscribers, such as SRCA authorized agencies, national legal authorities, government public authorities, etc., are also required to fill out an application form and submit supporting materials as required to submit a certificate suspension request.

After the SRCA reviews and approves the suspension request, the suspension operation shall be completed within 24 hours. Subscriber certificates that are mandatorily suspended must be notified to subscribers within 5 working days by email, telephone, fax or website announcement. If the subscriber needs to unsuspend it, he or she needs to submit supporting materials in accordance with relevant laws and regulations to prove the legitimacy and other original status of the certificate, so that SRCA can go through the unsuspension procedures in accordance with the prescribed procedures.

4.9.16 Time limit of suspension

After a certificate is suspended, if the subscriber does not apply for unsuspending, revoking or restoring other certificate-related services within the specified time, SRCA will unsuspend the certificate, and the subscriber is requested to revoke, restore or unsuspend the certificate in a timely manner.

SRCA shall not be liable for any loss caused by the Subscriber's failure to deal with it in a timely manner. The maximum period of suspension of a certificate is 6 months, and if no legal revocation notice is received, the certificate will be unsuspended. If the certificate expires within the suspension time, SRCA will rescind the certificate.

4.10 Certificate Status Service

4.10.1 Operational characteristics

SRCA certificates and CRLs are published in directory servers that support the LDAP protocol standard to provide certificate status services to subscribers. The query of certificates and CRLs is implemented through the LDAP protocol. The certificate is issued by the issuing server to the main directory server of the system, where the certificate is mapped to the slave directory server through the automatic mapping function of the directory server for users to query and download. The user needs to load the CRL locally for verification, including verifying the legitimacy of the CRL and checking whether the CRL contains the serial number of the certificate to be inspected.

4.10.2 Service Availability

SRCA provides 24/7 certificate status query service.

If the query cannot be made through the directory service due to unpredictable reasons, SRCA will publish the certificate status information in the CA database to the SRCA website through query within 48 hours.

4.10.3 Optional features

At the request of the subscriber, the SRCA may query the status of the certificate subscriber in the CA database and notify the subscriber of it after the requester pays relevant fees. It can also provide a paid notification service for requestors when a specified certificate is revoked.

4.11 End of subscription

If the certificate has expired, the user shall be deemed to have terminated the subscription if the user does not declare that he will continue to use the certification services, and the user certificate may be revoked by SRCA or the authorized BT.

If a certificate does not expire and the user declares that he will not continue to use the SRCA certification service, the SRCA-authorized BT will revoke or suspend the user's digital certificate upon the user's request. When a user applies for the revocation or suspension of the certificate, the user will fill in the application form (in triplicate), and the SRCA-authorized BT will approve or reject it according to the revocation process in 4.9.3 or the suspension process in 4.9.15, such that the subscription ends when certificate is revoked within the validity period,

If the certificate has not expired, the government public authorities will request the revocation of the certificate, issue written supporting materials in accordance with the regulations, fill in the revocation application form, and sign and seal it. SRCA will revoke the certificate within 24 hours after the approval of the submittals, and after the certificate is revoked within the validity period, that is, the subscription ends , SRCA will notify the subscriber by telephone, fax, website announcement or e-mail within 5 working days.

4.12 Key generation, backup, and recovery

Since the key pair is the key to the security mechanism, corresponding provisions have been formulated in the CPS to ensure the confidentiality, integrity and non-repudiation of the key pair generation, transmission and installation. The encryption key pair of certificate users is generated by the Sinorail KMC, which determines the generation, backup and recovery policies at its own discretion.

The signing key pair is generated by the client, and the certificate applicant uses the media supported by the SRCA digital certificate issuance system recognized by the State Cryptography Administration to generate the signing key pair. The signing key is stored in the media and cannot be exported, ensuring that the signing key pair cannot be copied.

4.12.1 Policies and acts of key generation, backup, and recovery

The signing key pair of subscribers is generated from certificate carrier held or designated by users, including but not limited to intelligent key UKEY, cryptographic device and cryptographic module. Subscriber-encrypted certificate keys are generated and saved securely from Sinorail Key Management Center (“Sinorail KMC”) in a centralized manner.

Signing keys of event-based certificates are destroyed immediately after the signing device generates the key and executes signature.

Key recovery refers to recovery of subscriber encryption key pair. The KMC is not responsible for recovery of signing keys. Key recovery is a strictly controlled process, such that key recovery is only allowed under the following circumstances:

1) The certificate holder submits an application;

2) The registration authority makes the application for good reasons;

3) The national law enforcement and judicial authorities need it for law enforcement and justice purposes;

4) Administrative needs of other national authorities.

Key recovery is carried out only when necessary, and the application must be made with sufficient reasons and supported by relevant documents and materials.

Key recovery is divided into user key recovery and judicial key recovery.

User key recovery: when a subscriber's key is damaged or lost, certain encrypted data cannot be restored, at which time the subscriber may apply for key recovery. After the subscriber applies to the registration authority and submits relevant documents and materials and have them reviewed and approved, CA files a request to the KMC; the key recovery module accepts subscriber's recovery request, recovers the subscriber's key and store it in the medium of subscriber certificate.

Judicial key recovery: after the judicial forensic personnel files an application at KMC, submits relevant materials and documents and have them reviewed and approved, the key recovery module will recover required keys and record them into the designated medium.

4.12.2 Policies and acts of encapsulation and recovery of session keys

The session key refers to the encryption key temporarily generated by the user when the user establishes an encryption channel with the certificate, which is determined by the application environment and not saved or recovered by Sinorail CA.

5.Certification Body Facilities, Management and Operational Control

5.1 Physical control

5.1.1 Site location and architecture

The construction of SRCA's buildings and computer rooms is carried out in accordance with the following standards:

（1）GB 50174—93 "Code for Design of Computer Room"

（2）GB 2887—89 "Technical Conditions for Computing Stations"

(3) GB 9361-88 "Safety Requirements for Computing Station Sites"

（4）GB 6650—1986 "Technical Conditions for Raised Flooring in Computer Room"

（5）GB 50034—1992 "Lighting Design Standards for Industrial Enterprises"

(6) GB 5054-95 "Code for Design of Low-Matching Electrical Devices and Circuits "

(7) GBJ 19-87 "Design Code for Heating, Ventilation and Air Conditioning"

(8) GB 157 "Code for lightning protection design of buildings"

(9) GBJ 79-85 "Code for Design of Communication Grounding in Industrial Enterprises"

The SRCA computer room is located on the 2nd floor of Building 1, Yard 2, Maliandao South Street, Xicheng District, Beijing.It implements zonal access control for security management, and the functional areas of SRCA are divided into certification room, office area and computer room area.

5.1.2 Physical access

The access control system assigns corresponding permissions to personnel, determining whether their entry is authorized. Operations staff must register before entering the computer room and gain access by swiping their access cards. Personnel entering the core area must pass through both access control and biometric authentication, following a two-person, two-factor verification process. Non-operations personnel must complete registration procedures and be accompanied by facility management staff when entering the computer room. All areas of the computer room are equipped with 7x24 video surveillance.

5.1.3 Electricity and Air Conditioning

According to the load requirements, the power cable of the corresponding wire diameter and the power filter of different capacities are selected for the power supply to the computer room. Power filters with low leakage current are used in many places to achieve the effect that the insertion attenuation capacity is consistent with the comprehensive effectiveness of the shielded room.

Three-phase power supply is adopted. The computer room uses an online UPS connected with backup battery pack such that when the mains power is cut off, the battery pack will supply power to the UPS, and the mains power supply and the battery pack power supply will be switched in zero seconds to ensure that the computers do not lose data during the power switching process.

The air conditioning in the computer room adopts a high-performance and high-sensitivity air-conditioning system, supported by ventilation, humidification and other measures to control the temperature and humidity in the operating facilities to ensure the normal operation of the system.

5.1.4 Flood control

Corresponding measures have been taken during the construction of the computer room to prevent the occurrence of water leakage and to minimize the impact of water leakage on the certification system in the event of water leakage.

5.1.5 Fire protection

The design of SRCA fire alarm system is based on GBJ116-88 "Design of Automatic Fire Alarm System". The system collects fire safety data through the temperature and smoke detectors set up in the computer room and provides alarm data of the automatic fire alarm terminal and the system operation status data for real-time handling of fires. There are two modes of system management: manual mode and automatic mode.

5.1.6 Media storage

SRCA media storage is in compliance with the regulations and requirements of the relevant national authorities, and the cryptographic equipment containing the keys is placed in the premises with a high degree of physical security protection and access security control. Personnel who have access to the key system must undergo rigorous background checks to ensure that they are trustworthy.

5.1.7 Waste treatment

When the hardware equipment, storage equipment, and cryptographic equipment used in the SRCA electronic certification service system are discarded, they will be scrapped in accordance with the relevant national regulations, such that the sensitive and confidential information involved will be securely and completely eliminated to ensure that the information cannot be recovered and read.

SRCA will uniformly destroy retained data once it is no longer needed or its retention period expires, under the direction of the superior department.

All treatment acts will be carried out by at least 2 individuals at the same time, supervising each other, and will then be recorded and signed off for future review

5.1.8 Offsite backup

SRCA is backed up to the main data center of China Railway Corporation by means of offsite backup.

5.2 Operational process control

5.2.1 Trusted roles

SRCA Trusted Roles are defined as "those who have undergone and passed an extensive background check and have demonstrated their ability to maintain key operations of the CA system in their respective functional posts, including, but not limited to, personnel rated to customer service, operation and maintenance and security management jobs" Trusted role policies are the foundation of personnel security system. In view of the special nature of the construction of the electronic certification service system, it is necessary to appoint trusted employees to perform the security operations related to the electronic certification service system, that is, all staff members who have access to sensitive operations must be trustworthy personnel.

In general, trusted employees include, but are not limited to, the following:

(1) Have access to the electronic certification service system;

(2) Have access to a combination of safes and/or keys of safes;

(3) Have access to security-sensitive materials;

(4) Identification and approval of certificate requests and issuance of certificates;

（5）Grant physical and/or logical access rights.

In addition, relevant individuals who are assigned to senior executive levels should also be trusted employees. In accordance with this CPS and the license agreement, SRCA formulates the management specifications of its authorized certificate service organizations (RA, BT, etc.) to standardize the operation of management personnel and operators. In the software design related to this, full consideration is given to security constraints and restrictions. SRCA provides a reasonable division of responsibilities for its authorized certificate service organizations and guarantees the responsibility and obligations for system and technology implementation and management.

5.2.2 Number of people required for each task

SRCA ensures that a single person cannot access, export, restore, update or revoke the private key corresponding to the root certificate stored by SRCA. At least three people use a key splitting and synthesis technique that is confidential to the participating operators to perform any CA key generation and recovery operations.

SRCA has a clear division of labor for functions related to operation and manipulation, and implements a security mechanism that checks and supervises each other.

5.2.3 Identification and authentication of each role

All SRCA in-service personnel must pass the certification to be issued the required security tokens such as system operation cards, access control cards, login passwords, operation certificates, and work accounts according to the nature of respective work and the position-specific authority. For employees who use security tokens, the SRCA system will independently and completely record all of their actions, and all SRCA key personnel must ensure that:

(1) The security tokens issued belong only directly to individuals or organizations;

(2) The issued security tokens are not allowed to be shared;

(3) SRCA's systems and procedures control the authority of the operator by identifying different tokens.

5.2.4 Roles that require segregation of duties

The acceptance of the certificate service requests must be completed through the two roles of entry clerk and auditor at the same time. For root key operations, three root key administrators must be present at the same time in order to perform the relevant operations. When the SRCA found its system in emergency and needs joint emergency repair, it must report to the security policy committee, and after approval, at least one individual designated by the security policy committee shall be present, and the emergency repair personnel shall perform the permitted operations under the supervision of the individual, with all operations and modifications documented.

If a non-SRCA employee needs to enter the SRCA data center for repairs due to physical repairs, fire protection, high-voltage failures, etc., they must report to the security policy committee, and after approval, the identity of the repairer will be authenticated first, and then a person designated by the security policy committee will accompany and supervise at all times to complete the repair of agreed parts.

5.3 Personnel control

5.3.1 Qualifications, Experience, and No-Fault Requirements

The recruitment of SRCA staff is rigorously vetted, and the number of trusted employees is increased according to job requirements.

Upon completion of the probation period, new staff shall be assigned to appropriate positions based on the assessment outcome. SRCA trains its employees on responsibilities, jobs, technology, policies, laws, and safety as needed. SRCA conducts rigorous background checks on its employees in key positions. Operators of the registration authority and BT can be vetted by reference to the SRCA's approach to the examination of trustworthy employees. On this basis, the registration authority and BT may add probation and training clauses, but not inconsistent with the SRCA certificate acceptance procedure and SRCA CPS.

5.3.2 Background check procedure

A dedicated team is required to be formed to investigate all those who need to be in credible roles, including verification of previous employment; verification of the highest degree obtained; criminal record checks (local, provincial, and national).

All employees sign a confidentiality agreement with SRCA and are bound by the contract and articles of association to not disclose any sensitive information about the SRCA certificate service system.

SRCA may, as required, work with relevant government departments and investigative agencies to complete background checks on SRCA's trusted employees.

5.3.3 Training requirements

SRCA conducts comprehensive training of employees on:

(1) SRCA security policy;

(2) Introduction to the software used by SRCA;

(3) The systems and networks operated by SRCA;

(4) SRCA job responsibilities;

(5) SRCA policies, standards and procedures;

(6) Relevant laws, arbitration rules, administrative measures, etc.

5.3.4 Retraining cycle and requirements

According to SRCA's policy adjustments, system updates, etc., SRCA will continue to train its employees to adapt to new changes. Relevant skills and knowledge training is conducted at least once a year.

5.3.5 Job rotation cycle and sequence

The employees responsible for the operation of the system and design, development and maintenance of the CA system at SRCA have different responsibilities, and the jobs of both sides are separated from each other.

In order to meet the operational needs of the certification system and the needs of job adaptability, SRCA might select suitable candidates to rotate in different jobs. This rotation must not contradict the preceding principle of post separation.

5.3.6 Penalties for Unauthorized Conduct

When an SRCA employee performs unauthorized or ultra vires operations, SRCA will immediately suspend the employee's access to the electronic certification service system after confirmation. Depending on the severity of the circumstances, measures are to be implemented, including referral to the judicial organs for handling. Upon becoming aware of any of the above, SRCA immediately invalidates or terminates the individual's security token and corresponding permissions.

5.3.7 Requirements for Independent Contractors

Due to insufficient human resources or special needs, SRCA hires professional outsourced personnel to participate in the operation of the system, and the rights and responsibilities of the independent contractors are the same as those of trusted employees, except that they must sign a confidentiality agreement regarding the work content. At the same time, it is also necessary to train them in job skills and knowledge and norms, so that they can strictly comply with the requirements of the SRCA normative system.

5.3.8 Documents provided to employees

SRCA employees can view technical manuals for the relevant hardware, software, and applications of the CA system, as well as SRCA business process descriptions and certificate policies.

5.4 Audit log procedure

The security audit service is an important part of the SRCA system services, which provides a reliable service platform for timely discovery of potential security hazards and illegal operations of the certification service system, post-event loophole filling, system reinforcement, system operation status review, accident investigation and evidence collection, etc.

5.4.1 Type of event recorded

The Certificate Service Organization within the SRCA architecture must log events related to the CA and RA, as well as the BT operating systems. These records shall contain the content of event, the time of event, and event-related entities..

(1) Information data and materials generated in the process of certificate subscriber service, such as application forms, agreements, identity information, etc.;

(2) Log records generated by the daily operation of the certification system;

(3) Work records involving access to sensitive areas;

(4) Agreements, specifications and related work records between certification bodies, registration authorities and BTs;

(5) Other contents that need to be recorded according to regulations.

5.4.2 Period of log processing

SRCA employs a log audit system to collect in real-time and archive periodically the logs generated from the daily operation of the certification system. Results from continuous tracking are compiled and analyzed, with any anomalies leading to a report that is documented and addressed by the relevant technical department.

As mandated by internal policies, internal auditors conduct regular reviews of other records. A thorough investigation is conducted into any anomalies or warnings discovered, and the entire process and its outcomes are fully documented.

5.4.3 Retention period of audit logs

SRCA's audit logs are compiled into new archive files annually, which are then transferred to the relevant department for preservation. Meanwhile, the logs generated from the daily operation of the certification system must be retained for at least five years after the associated certificate information becomes invalid.

5.4.4 Protection of audit logs

SRCA implements strict management to ensure that only SRCA authorized personnel have access to these audit records. These records are strictly protected and are strictly prohibited from being accessed, read, modified, and deleted.

5.4.5 Audit log backup procedure

SRCA warrants that all audit records and audit checks are backed up in accordance with SRCA backup standards and procedures. Depending on the nature and requirements of the records, there are various forms of backup, such as real-time, daily, weekly, monthly, and yearly, using a variety of backup tools, both online and offline.

5.4.6 Audit collection system

All management operations in the SRCA system are stored in the log database of each subservice. Since the maintenance of the log database of each subservice is active and independent, and does not have any contact with any other module or subsystem, the authority and independence of the log database can be guaranteed.

The SRCA audit collection system is performed automatically by the log audit system, involving the following areas:

(1) Certificate registration management system;

(2) Certificate issuance management system;

(3) Certificate directory service system;

(4) Certificate key management system;

(5) Other systems that SRCA deems necessary to review.

5.4.7 Notification to the entity that caused the event

In the event of an incident affecting security controls occurring in the operation of the certification system, the security policy committee must be notified and relevant response measures taken.

According to the severity of the circumstances, the security policy ccommitee decides to take measures such as separate notification, meeting notification, warning, punishment, and dismissal against the entity that caused the event, when SRCA found any violation of service acceptance specifications, system operation specifications or operational events in the audit.

SRCA will keep a detailed record of the attacks found in the audit, trace the attacker to the extent permitted by law, and reserve the right to take appropriate countermeasures. Depending on the attacker's behavior, it takes measures such as cutting off the service already open to attackers, and referral to the judicial department for resolution. SRCA has the right to decide whether to notify the attacker or perpetrator identified in the review.

5.4.8 Risk assessment

SRCA records some of the events found during the audit as weaknesses in the system, and will perform a security risk assessment after checking such events. Risk assessment is based on real-time, automatic record data and an annual assessment of the system is conducted based on security and audit requirements. Based on the results of the assessment, the security controls that are closely related to the operation of the system are adjusted at any time to minimize the risk of system operation.

5.5 Records archiving

5.5.1 The type of archived record

SRCA will regularly archive and maintain the relevant materials of the electronic certification service, including:

(1) Certificate application information, certificate service approval and rejection information, agreements with certificate subscribers, certificates, etc.;

(2) Audit data on system operation and certification services;

(3) Other information deemed necessary to archive and keep.

5.5.2 Retention period of archived records

In addition to the retention period proposed by laws and regulations and the certification authority, the archival retention period of third-party electronic certification service operation information formulated by SRCA shall be at least as follows:

(1) CPS, user application information forms and related agreements, certificates applied for, renewed, revoked and suspended by subscribers and expired certificates, which shall be kept for at least 5 years after the end of the validity period of the certificate;

(2) The service records of certificate users applying for, querying, and revoking certificates shall be kept for at least 5 years after the end of the validity period of the certificate;

(3) The information on relevant changes to the subscriber's certificate and key, which shall be kept for at least 5 years after expiration of electronically signed certification;

(4) If it is inconsistent with the provisions of laws and policies, the longer of the two shall be chosen for retention

In addition, SRCA may determine the duration of the archiving of information at its own discretion without the need to explain it, provided that it does not violate the laws, regulations and regulations of the competent authorities.

5.5.3 Protection of archived files

Archived content is guaranteed by both physical security measures and cryptographic technology. Access to it is restricted to authorized staff in a specific secure manner. SRCA protects the relevant archives from harsh environmental threats, such as temperature, humidity and magnetic damage. For the data deemed necessary, SRCA will keep it by means of off-site backup.

The basic information and identification data about applicants and subscribers kept by SRCA cannot be obtained by any unrelated third party unless they have been applied for through legal means by the national legal authorities, the competent government authorities or other public authorities.

5.5.4 A backup program for archived files

Archived databases are generally physically or logically isolated from information interaction with the outside world. Only authorized staff members are allowed to read the files under supervision. In terms of security mechanism, SRCA warrants that it prohibits the deletion, modification and other manipulations of files and their backups. If the certification system fails to operate normally due to abnormal conditions, the data stored in these archives is used to restore the system according to the SRCA recovery policy.

5.5.5 Record timestamp requirements

All archived content described in this CPS5.5.1 is timestamped, such as the time automatically recorded by the system, or manually marked by the operator.

If necessary, SRCA will add timestamp services to the relevant records.

5.5.6 Archive collection system

All operational information of the electronic certification service system is generated and collected by SRCA's internal staff or internal systems with security controls, both manually and automatically. It is managed by someone with the relevant authority.

5.5.7 Procedures for obtaining and verifying archived information

On an annual basis, SRCA verifies the integrity of the archived information in accordance with provisions. Two backups of archived information are kept both online and offline in order to ensure accuracy of archived information.

5.6 Key replacement of electronic certification service organization

The SRCA root certificate is valid for no more than 20 years. Before the SRCA certificate expires, SRCA will replace the root private key. The key conversion program plays a transitional role in the conversion process from the old key pair to the new key pair, and when the old SRCA certificate expires, the SRCA will issue the certificate with the new CA key pair. The manner of SRCA key replacement is as follows:

1）New subscriber certificate ceases to be issued before the expiration time of SRCA root certificate is less than the validity period of subscriber;

2) A new key pair is generated and new root certificate is issued

3) After the old root certificate ceases to be issued, subscriber certificate will be issued using the new root key.

SRCA will continue using CRL issued using the old root private key until the certificate issued by the old CA root private key expires.

5.7 Damage and disaster recovery

In order to be able to resume the operation of the certification system in the shortest possible time in the event of an abnormal or catastrophic situation, SRCA has developed a reliable damage and disaster recovery plan to deal with system problems caused by unexpected incidents.

Possible damage and disaster recovery scenarios are as follows:

(1) Scenarios where SRCA is subjected to attacks, resulting in the destruction of communication network resources, failure of computer equipment systems to provide normal services, software damage, database tampering, or disasters caused by force majeure;

(2) The revocation of the SRCA root certificate;

(3) A disaster involving the compromise of the root private key;

(4) Natural disasters or other catastrophes.

In the event of any of the aforementioned damages or disasters, SRCA will execute recovery in accordance with its Business Continuity Plan.

5.7.1 Accident and Damage Handling Procedures

SRCA will develop a disaster contingency plan for possible accidents, and will deal with an accident according to the plan after the accident occurs. The Disaster Contingency Plan is modified and refined by SRCA each year after conducting a risk assessment.

5.7.2 Corruption of computing resources, software, and/or data

When the software, data or other information used in the operation of the authentication system is abnormally damaged, the system recovery operation can be carried out in accordance with the SRCA system backup and recovery operation manual, based on the internal backup data of the system or the data backed up offsite, so that the certification system can operate normally again.

When the hardware device used by the certification system is damaged, the backup hardware device and the related backup operating system and certification system can be started in accordance with the SRCA System Backup and Recovery Operation Manual to restore the system operation.

5.7.3 SRCA certificate invalid

When an SRCA certificate is revoked, SRCA shall notify the certificate holder in accordance with the relevant provisions of this CPS, and the certificate will be invalidated.

5.7.4 Entity private key compromise handling procedure

In the event that the root private key of the SRCA is damaged, lost, leaked, cracked, tampered with, or is suspected of being stolen by a third party, the SRCA should:

(1) Immediately report to the Ministry of Industry and Information Technology and other government authorities, and immediately revoke all certificates that have been issued, and update the CRL information for certificate subscribers and relying parties to query. At the same time, SRCA immediately generates a new key pair and issues a new root certificate by itself.

(2) After the issuance of the new root certificate, the subordinate certificate shall be re-issued in accordance with the provisions of this CPS on certificate issuance;

(3) After the new SRCA root certificate is issued, it will be released immediately through the directory server, website, etc.

5.7.5 Business continuity capabilities after a disaster

Unless there is a devastating and irreversible disaster at the physical site, SRCA has the ability to resume the following operations within 48 hours after the disaster occurs: certificate issuance, certificate revocation, relesae of certificate revocation information, and provision of key recovery information.

SRCA plans to establish a disaster recovery site off-site, which will further enhance SRCA's post-disaster business viability.

5.8 Termination of the electronic certification service organization or registration authority

5.8.1 Termination of the electronic certification service organization

If SRCA plans to terminate its operations for any reason, SRCA will report to the Ministry of Industry and Information Technology in accordance with the relevant legal requirements and follow the statutory procedures, including:

(1) Notifying the Ministry of Industry and Information Technology, the certificate holder and all other relevant entities before the deadline prescribed by laws and regulations;

(2) Arranging business succession;

(3) Keeping all the operation materials related to the certification service, including certificates, user information, system files, CPS, specifications and protocols, etc.;

(4) Stopping the relevant operation service;

(5) Clearing the system root key.

5.8.2 Basis for termination of RA

The business of the RA (including BTs under it) shall be terminated in accordance with the agreement between SRCA and the RA when the SRCA authorised registration authority terminates the service for cause.

6. Certification system technical security control

6.1 Generation and installation of key pairs

6.1.1 Generation of key pairs

Encryption key pair: Generated by a cryptographic device licensed by the State Cryptography Administration of the People's Republic of China (”SCA”) and supported by the SRCA certificate issuance system. Sinorail KMC controls and manages key generation.

Signing key pair: The certificate applicant should use the media recognized by the SCA and supported by the SRCA certificate issuance system to generate the signing key pair. The signing private key is stored in media and cannot be exported, so it cannot be copied. SRCA does not undertake to accept all types of cipher generating devices.

The key pair of the server certificate: generated by the subscriber himself/herself, and the subscriber should keep it properly.

SRCA guarantees the technical, process, and administrative security of key pair generation.

6.1.2 Transmission of the private key

The encrypted private key of the certificate subscriber is generated at Sinorail KMC, and the private key is only stored in Sinorail KMC and the subscriber medium. In the process of transmitting the encrypted private key from Sinorail KMC to the subscriber, the algorithm approved by the SCA is used to encrypt the key, ensuring the key security of the certificate subscriber.

6.1.3 Transmission of public key to the certificate issuing organization

SRCA obtains the subscriber's public key from Sinorail KMC and then issues a certificate for it, during which process it also uses the algorithm approved by the SCA for encryption to ensure the security of the data in transit.

6.1.4 Transmission of public key of the electronic certification service organization to the relying party

The root public key of the SRCA is contained in the root certificate signed by SRCA itself. Certificate subscribers can download the SRCA root certificate from the SRCA website at www.sinorailca.com..

6.1.5 Key Length

The algorithm and length of key comply with regulations of the national cryptography authorities.

6.1.6 Generation and quality check of public key parameters

The generation of public key parameters and the quality of the parameters are carried out by the hardware authenticated and licensed by the SCA and supported by the SRCA certificate issuance system, the protocols and algorithms built in which all conform to requirements of the national cryptography authorities..

6.1.7 Purpose of key use

The purpose of the key in the SRCA electronic certification service system is closely related to the type of certificate.

The signing private key of SRCA is used to issue its own certificates, subordinate certificates, and certificate revocation list (CRL) of all issued certificates, while the public key of SRCA is used to verify the signature of the SRCA private key.

The subscriber's signing key is used to provide network security services, such as the information being not tampered with during transmission, the receiver being able to confirm the identity of the sender through the certificate, and the sender being unable to deny the information it sends. The encryption key is used to encrypt the information that needs to be transmitted on the network to ensure that the information is not stolen or tampered with by others except the sender and receiver. Signing keys and encryption keys can be used together to implement security mechanisms such as identity authentication, authorization management, and responsibility determination.

If SRCA specifies the purpose of the certificate in the standard extension of the certificate it issues, the certificate subscriber must use the key for that specified purpose.

6.2 Private key protection and cryptographic module engineering control

6.2.1 Standards and control of cryptographic module

SRCA uses products licensed by the SCA. The standards, operation, and control of the cryptographic modules are in full compliance with national regulations.

6.2.2 Multiperson control of private key

The generation, renewal, revocation, backup and recovery of SRCA private key adopts multiperson control mechanism, i.e., three-out-of-five process, in which the management permissions of private key are dispersed into five administrator cards, and the aforesaid operations of the private key can be performed only when three or more of these administrators are present and approve.

6.2.3 Private key hosting

SRCA does not entrust the root private key to the care of any third party organization.

The private key corresponding to the SRCA subscriber's signing certificate is kept by the subscriber itself, but not hosted by Sinorail KMC and SRCA in trust, so as to ensure its non-repudiation. Sinorail KMC strictly guarantees the security of user key pairs, by keeping the keys in ciphertext, and using the keystore that has the highest security level, prohibiting illegal access from the outside world.

6.2.4 Private key backup

The certificate subscriber's signature private key is not backed up by either Sinorail KMC or SRCA. Sinorail KMC backs up the encrypted private key, and the backup data is saved in ciphertext.

6.2.5 Private key archiving

Sinorail KMC provides archiving services for expired encrypted private keys.

6.2.6 Importing and exporting of private keys into and out of cryptographic module

In the SRCA electronic certification service system, the SRCA software can be used to import the private key of a subscriber's encryption certificate into the cryptographic module. Private keys cannot be exported from hardware and software cryptographic modules. Password verification is required to be passed before encryption and decryption operations can be performed using the private key stored in the cryptographic module.

6.2.7 Storage of private key in cryptographic module

The holder of a certificate can save the private key in either the hardware cryptographic module or the software cryptographic module. The signing private key of the SRCA must be kept in the hardware cryptographic module.

6.2.8 Method to activate private keys

SRCA defaults to the fact that the subscriber can only activate his private key after the password has been authenticated, unless the subscriber makes the change himself and is willing to assume the responsibility for the change.

6.2.9 Method to deactivate private keys

Once a private key is activated, the private key is always active unless this state is lifted. In use of some private keys, the private key can only be manipulated once every time it is activated, and if it is to be manipulated the second time, it needs to be activated again.

The Subscriber deactivates the private key in such a manner as at his/her discretion, such as exiting, cutting off the power, removing the token/key, auto-freezing, etc. The Subscriber must do so at its own risk and responsibility for the Private Key Activation.

6.2.10 Method for destroying private keys

The private key of a user signature certificate shall be managed and destroyed by the user as needed. The key pair for a user encryption certificate is generated by the KMC of the

Electronic Certification Service Authority. After the user's key pair and certificate become invalid, the Authority shall archive them in an encrypted format. All archived key pairs must be retained for at least five years after certificate expiration before they can be destroyed. The destruction method must ensure the complete and irreversible obliteration of the key information.

6.2.11 Assessment of cryptographic modules

The cryptographic modules used for SRCA key storage are all approved by the SCA, and SRCA will regularly conduct security assessment on the working status and related security parameters of the cryptographic modules in accordance with the security assessment standards.

6.3 Other aspects of key pair management

6.3.1 Public key archiving

The public key in the subscriber certificate is archived periodically by Sinorail KMC and SRCA.

6.3.2 Certificate operation period and key pair usage period

The validity period of all subscriber certificates is the same as that of their corresponding key pairs.

6.4 Activation data

6.4.1 Generation and installation of activation data

The activation data generated by SRCA, the password used to download the certificate, is randomly generated by the hardware device in a secure and reliable environment.

These activation data are delivered to the subscriber in a secure and reliable manner, such as offline face-to-face delivery, postal delivery, etc.

For non-disposable activation data, SRCA recommends that users make their own modifications.

6.4.2 Protection of activation data

The subscriber's activation data must be kept properly or destroyed after being remembered so that it cannot be made known to others. If there is a need for written retention, it must be kept securely and reliably. At the same time, in order to support the security needs of the business system, the activation data should be modified frequently.

6.4.3 Other aspects of activation data

For security reasons, the lifecycle of subscriber activation data is provided for as follows:

(1) The password used by the subscriber to apply for and download the certificate will become invalid after the download is successful.

(2) The password used to protect the private key, IC card, and USB key is recommended to be changed at any time according to the needs of the business application, and must be modified after the use period exceeds 3 months.

6.5 Computer Security Control

6.5.1 Special computer security requirements

The data files and equipment of the SRCA certificate issuance system are maintained by the administrator, and no other personnel can operate or control the system without the authorization of the administrator; other ordinary subscribers do not have a system account or password. The SRCA system is deployed within multiple levels of firewalls from different vendors to ensure system network security. SRCA system passwords have a minimum password length requirement and must meet complexity requirements, and SRCA system administrators change system passwords regularly.

6.5.2 Computer Security Assessment

SRCA's certification business system has passed the relevant evaluation and review of the State Cryptography Administration and other departments.

6.6 Lifecycle Technical Control

6.6.1 System development control

The development of the SRCA system is completed by a reliable software developer who meets the relevant national security and cryptographic standards, while a security and confidentiality agreement has been established with the developer to ensure the authority and reliability of the system.

6.6.2 Security management control

SRCA's system configuration, as well as any modifications and upgrades, are documented and controlled, and SRCA employs effective security management control mechanism to control and monitor the configuration of the system to prevent unauthorized modifications.

6.6.3 Lifecycle security control

SRCA cooperates with relevant product developers and standards bodies to actively adopt advanced technology and equipment at home and abroad and update technology in a timely manner according to international security standards and development dynamics, without affecting the normal provision of services. Any modifications and upgrades to the system by SRCA are documented and controlled.

6.7 Network security control

SRCA is protected by multi-level firewalls and other access control mechanisms, and is configured to allow access only to authorized machines. Only authorized SRCA employees have access to equipment or systems such as the Issuance Management System, Registration Management System, Directory Server and Key Management System, etc. SRCA only opens up the operating functions related to applying for certificates, querying certificates, etc., for users to operate through the network.

6.8 Timestamp

Currently, SRCA provides timestamp services in accordance with the requirements of the relevant information systems.

Depending on the need for security management and control of the system, SRCA decides whether to use timestamps or not. According to the requirements of different data for time sensitivity, rigor and logical relationship, SRCA will determine the relevant specifications and policies for timestamp services.

7. Certificate, certificate revocation list, and online certificate status protocol

7.1 Certificate

The certificates issued by SRCA are in conformity with the X.509 V3 certificate format. and follow RFC5280 standards.

7.1.1 Version number

The version information of a certificate issued by SRCA is stored in the certificate version property bar.

7.1.2 Certificate extensions

The extensions of X.509 V3 certificate include:

（1）Authority Key Identifier:

（2）Subject Key Identifier:

（3）Key Usage:

（4）Subject Alternative Name：

（5）CRL Distribution Points:

For special users, the certificate issued by SRCA may contain a private extension, which can be ignored by applications and relying parties that cannot recognize the private extension.

①Key Usage

②Certificate Policies

③Subject Alt Name

④Basic Constraints

⑤CRL Distribution Points

⑥Issuing CA key identifier

⑦Subject key identifier

⑧Name Restrictions

7.1.3 Algorithm object identifier

Conforms to the algorithm object identifier approved by the national cryptography authorities.

7.1.4 Name form

The distinguished name of the certificate issued by SRCA complies with the X500 provisions regarding distinguished names. For the distinguished name of the certificate subject, O represents the organization to which the certificate holder belongs, and OU represents the department of the certificate holder, and the distinguished name can contain more than one OU for storing other information.

For the distinguished name of Certificate Issuer, O stands for Certificate Issuing Authority and OU stands for Department of Certificate Issuing Authority.

7.1.5 Name Restrictions

The common name in the certificate issued by SRCA cannot be pseudonym or fictitious name.

7.1.6 Certificate Policy Object Identifier

Each type of SRCA certificate (Class I, Class II, Class III and Class IV) corresponds to a Certificate Policy Object Identifier (OID). When using a certificate policy extension, the certificate issued by SRCA contains a certificate policy object identifier that corresponds to the corresponding certificate category.

7.1.7 Usage of policy restriction extension

None.

7.1.8 Syntax and semantics of policy qualifier

None.

7.1.9 Processing rules for key certificate policy extensions

Consistent with ITU X.509 and RFC5280 regulations.

7.2 Certificate revocation list

7.2.1 Version number

SRCA regularly issues CRLs (Certificate Revocation Lists) that comply with the RFC 5280 standard. They are issued in X.509 V2 format.

7.2.2 CRLs and CRL Entry Extensions

（1）Issuer

CN=SRCA
O=Sinorail Certification Authority
C=CN

（2）CRL Release

SRCA automatically publishes the latest CRL at least every 24 hours.

(3) Signature algorithm

SRCA uses the sha256/RSA2048 and SM3/SM2 signature algorithms.

7.3 Online Certificate Status Protocol

SRCA provides OCSP (Online Certificate Status Query Service) for certificate subscribers, and OCSP is an effective supplement to CRL, which allows certificate subscribers to easily query certificate status information in a timely manner. The SRCA OCSP service follows the RFC256 standard.

7.3.1 Version number

SRCA uses OCSP version 1.

7.3.2 OCSP extension

OCSP extension is not used.

8. Certification body audit and other assessments

8.1 Frequency or circumstances of audit assessment

8.1.1 SRCA audit

The auditor shall be appointed by Sinorail CA or the competent legal authority. Sinorail CA is required to audit all processes and operations of SRCA's affiliates (including SRCA-authorized registration authorities, BTs and other certificate system members) to verify whether they comply with the provisions of this CPS and the corresponding certificate policy, the frequency of which may be determined by SRCA or by the regulatory authority established by law. Audits are categorized as internal and external.

Internal audits are conducted by qualified personnel from within the CA organization. The results of internal audits are used by the CA to improve and refine its operations; these results do not need to be made public.

External audits are performed by a third-party auditing agency commissioned by the CA. The basis for external audits includes all business-related security policies, the "Certification Practice Statement", business specifications, management guidelines, as well as applicable national or industry standards.

8.1.2 SRCA audit of affiliates

SRCA conducts regular audits (usually 1 year) of its affiliates, through auditors appointed by SRCA. Auditors must be familiar with the rules of SRCA and the relevant knowledge of trust services, understand the basic knowledge of ensuring security, and independently and impartially make conclusions on conformity or nonconformity of affiliates in accordance with SRCA's specifications, agreements, and performance of responsibilities.

SRCA may conduct security audits of its subordinate affiliates and entities in accordance with the agreement, and has the right to deauthorize or re-authorize its subordinate entities based on the audit results of its superiors and its own audit results.

The number of audits for SRCA's affiliates is generally 1 time a year, no more than 2 times in special circumstances. Higher-level organizations and entities may not audit or charge subordinate entities and organizations fees repeatedly. Decisions as to whether or not to publicize results of the audit shall be made in accordance with the relevant regulations.

SRCA will charge an audit fee for the audit of affiliates. The audit fee is reflected in the agreement between SRCA and the affiliate in question.

8.2 Qualifications of the audit assessor

The internal audit and assessment is conducted by Sinorail CA's Internal Audit and Assessment Team. Personnel selection typically includes:

the CA's Security Officer and security management staff;

the CA Business Officer;

the heads of the certification system and information systems;

internal auditors and audit administrators;

the HR Officer;

other personnel as needed.

The qualifications for external auditors are determined by a third party.

8.3 Relationship between the assessor and the assessee

8.3.1 Audit assessor's relationship with SRCA

The auditor conducting the audit of the SRCA must be an entity independent from the SRCA. The relationship between the SRCA internal assessor and the assessee should also be relatively independent, which does not affect the objectivity of the assessment.

SRCA may select a specialized, impartial and objective audit and assessment organization to assist with internal assessment as needed.

8.3.2 Relationship between audit report and the SRCA

Audits of SRCA will generate audit reports, of which SRCA is not the author and therefore is not responsible for their contents, nor does SRCA express any opinion on these audit reports and is not responsible for any loss arising from reliance on the contents of the audit report related to SRCA.

8.4 Contents of audit assessment

The normative audit and assessment of the SRCA shall include:

1) whether operational workflows and policies are strictly adhered to;

2) whether certification services are conducted strictly in accordance with the CPS, business specifications, and security requirements;

3) the completeness of various logs and records, and whether any issues exist;

4) whether any other potential security risks are present.

8.5 Measures taken to address problems and deficiencies

If deficiencies are found in the implementation standard during the audit and assessment process, SRCA will formulate corrective and preventive measures based on the content of the audit report, and clarify the corresponding actions to be taken. SRCA will resolve issues expeditiously in accordance with generally accepted international practice or regulatory law.

8.6 Communication and publication of audit assessment results

Unless expressly required by law, SRCA generally does not disclose audit results. Where necessary, the specific provisions for notifying SRCA affiliates (e.g., sponsors, registration authorities, BTs) of the results of the audit will be set out in the agreement between SRCA and the affiliates.

9. Legal Liability and Other Terms of Business

9.1 Expenses

9.1.1 Payment of Fees

SRCA charges a fee for the services provided to certificate subscribers and all affiliates (e.g. sponsors, registration authorities, BTs). Certificate subscribers and SRCA affiliates are obligated to pay SRCA fees in accordance with SRCA's price list.

9.1.2 Certificate fees

The relevant fees of certificate are set according to the approval of the price control authorities and published on the website of Sinorail CA. The price list shall take effect as at the time specified by the SRCA or, if no effective time is specified, seven days after the date of publication of the price list. SRCA may also notify Certificate Subscribers or other parties of fee changes through other means. According to the needs for actual application of the certificate, SRCA may make appropriate adjustments to the certificate prices on the premise that the adjusted prices are not higher than the price recognized by the price control authorities.

Serial number	Product name	Unit	Price (RMB Yuan)	Remarks
1	Organization digital certificates	sheet/year	¥500	The same fee also applies to renewal
2	Personal digital certificates	sheet/year	¥100	The same fee also applies to renewal
3	Device digital certificate	sheet/year	¥2,600	The same fee also applies to renewal
4	Mobile terminal digital certificate	sheet/year	¥300	The same fee also applies to renewal
5	Event-based digital certificate			
5	Smart UKey	pcs	¥120	The warranty period is 1 year

9.1.3 Certificate query fee

During the validity period of the certificate, SRCA does not charge a query fee for querying the certificate information. SRCA reserves the right to charge fees for resource-intensive certificate query operations.

9.1.4 Fees for querying certificate revocation or status information

SRCA does not charge information access fees for certificate revocation list queries. The fee for the real-time online certificate sttaus query (OCSP) service shall be separately agreed between SRCA and the client in the agreement. SRCA reserves the right to charge fees for resource-intensive certificate revocation and status information query operations.

9.1.5 Other service fees

SRCA may tailor a variety of notification services at the request of the requester, the specific service fees for which are specified in the agreement with the client.

9.1.6 Refund Policy

Refund Policy - Once the SRCA digital certificate is accepted by the subscriber, SRCA will not deal with formalities for return or refund.

If the subscriber withdraws from the digital certificate service system during the certificate service period, SRCA will not refund the unused portion of service fee for the remaining period.

9.2 Financial responsibility

SRCA-authorized issuing bodies (e.g., registration authorities, BTs, etc.) should have the financial strength sufficient to maintain their operations and fulfil their responsibilities, and should be able to bear the liability risks caused to subscribers, sponsors and other entities that trust the certificates issued by them.

9.3 Confidentiality of Business Information

9.3.1 Confidential Business Information

Agreements, confidential information, correspondence and commercial agreements between SRCA and SRCA-authorized certifying authority, between SRCA and certificate subscribers, and between SRCA-authorized certifying authority and certificate subscribers, etc., may not be disclosed, made available or released to any third party without prior authorization, unless otherwise expressly provided for by law.

Audit reports, audit results, and other information relating to SRCA or SRCA's authorized issuing bodies are confidential and may not be disclosed to any entity other than those authorized and trusted by SRCA. These information may not be used for any purpose other than for the purpose of examination or for purposes required by law. Information about the operation of the SRCA e-Certification Service can only be passed on to SRCA authorised recipients under strictly specified circumstances. SRCA is under no obligation to publish or disclose the security measures that control the hardware and software operations of the issuing authority and the security measures that govern the certification services and registration services. Except as expressly provided for by law, SRCA is under no obligation to publish or disclose information other than the Subscriber Certificate.

9.3.2 Non-Confidential Business Information

The information published in documents related to the certificate such as the application process, the procedures required for the application, and the application operation guide can be disclosed. In addition, SRCA may use such information in the processing of applications, including disseminating such information to third parties. SRCA publishes certificate revocation and suspension information in the directory server for online query. SRCA will release relevant confidential information in this CPS to law enforcement authorities when required to do so by applicable laws, rules or regulations, or as requested by national legal authorities. Such acts shall not be considered a breach of confidentiality requirements or obligations.

9.4 Confidentiality of Personal Information

9.4.1 Confidential Personal Information

The private key paired with the certificate subscriber's certificate public key is confidential and should be kept carefully by the certificate subscriber and may not be disclosed to others. If the certificate subscriber discloses the private key without authorization, the certificate subscriber shall be solely responsible for the consequences arising therefrom.

The SRCA is obliged to keep confidential the private information provided by the certificate applicant that is not used in the certificate, regardless of whether the application is approved or not.

9.4.2 Non-Confidential Personal Information

The basic information in the certificate can be made public and published through the SRCA directory service or otherwise. If, for any reason, the owner of the Confidential Information requests SRCA to make public or disclose the Confidential Information in his possession, the SRCA generally will meet the requests. However, if such act involves or is likely to give rise to an obligation to indemnify any other party, SRCA shall be entitled to reject its request without being liable for any loss or damage related thereto or arising out of the disclosure of confidential information. The owner of the Confidential Information shall be liable for all losses and damages incurred by SRCA in connection therewith or as a result of the disclosure of the Confidential Information.

9.4.3 Retention of customer data

In order to protect customer information from unauthorized infringement, the following rules have been formulated in place:

1. Customer information is kept in a dedicated data room, accessible only to data review personnel and file management personnel in a restricted manner, and other non-relevant personnel are not allowed to read or view customer information.

2. Customer information needs to be archived and kept by the designated personnel, and may not be placed at will to avoid leakage, nor shall customer information be divulged to others for any reason;

3. The relevant personnel who caused the leakage of customer information due to various reasons shall be held accountable, and given appropriate sanctions if the circumstances are serious.

4. Separating employees need to keep the user information accessed by them confidential in accordance with the severance agreement, otherwise they may be held legally responsible.

9.5 intellectual Property

SRCA owns and reserves all unique intellectual property rights to and in the Certificates and all works (including software and logo, etc.) provided by SRCA, including the right to guarantee the integrity of the Certificates and works, the right to name and the right to share benefits. Therefore, SRCA has the right to decide what software system to use for certificate subscribers, relying parties, authorized issuing authorities, etc., and to choose the form, method, time, process and model to be adopted in order to ensure the compatibility and interoperability of the system. Any and all copyrights, trademarks and other intellectual property rights relating to the certificates issued by SRCA and the works provided by SRCA shall be the property of SRCA, including all related documents and user manuals, in accordance with the provisions of this CPS. Authorised issuing bodies may use the relevant documents and manuals with the prior consent of SRCA.

9.6 Representations and Warranties

Unless otherwise agreed specifically by SRCA, the Subscriber must be bound by this CPS if the provisions of this CPS are in conflict with the other relevant regulations and guidelines established by SRCA. In the agreements signed between SRCA and other parties, including subscribers, which only bind the contracting parties, the parties shall be deemed to have agreed to comply with the provisions of this CPS for anything not agreed in the agreement; The provisions in the agreement that are different from the contents of this CPS shall be implemented in accordance with the contents agreed in the agreement between the parties.

9.6.1 Representations and warranties of electronic certification service organization

SRCA's undertakings in the course of providing e-certification services are as follows:

(1) SRCA shall comply with the provisions of the Electronic Signature Law of the People's Republic of China and related laws, accept the business supervision and guidance of the competent authorities, and assume corresponding responsibilities and obligations for the digital certificates issued by SRCA;

(2) SRCA warrants that the systems and passwords used by it comply with national policies and standards, that SRCA's own signature private key is securely stored and protected internally, and that the security mechanism established and implemented conforms to the provisions of national policies;

(3) The certificates issued by SRCA to Subscribers comply with all the substantive requirements set forth in the SRCA CPS;

(4) SRCA guarantees the validity and reliability of the certificate during its validity period and will notify the certificate subscriber of any known events that may essentially affect the validity and reliability of the certificate;

(5) SRCA will revoke the certificate in time and post it on the CRL for subscribers to query;

(6) After the certificate is publicly released, SRCA warrants to the certificate relying party that all subscriber information in the certificate is accurate, except for unauthenticated subscriber information.

9.6.2 Representations and warranties of the registration authority and BT

SRCA's registration authority and BT undertake while participating in the electronic certification service as follows:

(1) Strictly implement the certificate management and issuance policies formulated by SRCA, and obey the overall management and specification requirements of SRCA; the registration process provided to the certificate subscribers fully complies with all the substantive requirements of the SRCA CPS;

(2) When SRCA generates a certificate, the information in the certificate will not be inconsistent with the information of the certificate applicant due to mistakes of the registration authority and the BT;

(3) Respond to and submit to SRCA requests for services such as subscriber certificate application, revocation, and renewal in a timely manner.

9.6.3 Subscriber's Representations and Warranties

By accepting the certificate issued by SRCA, the Subscriber is deemed to have made the following undertakings to SRCA, the Registration Authority and the relevant parties who rely on the certificate:

(1) The Subscriber has read and understood any and all the terms of this CPS and the certificate use policy related to its certificate, and agrees to assume the relevant responsibilities and obligations of the certificate holder in relation to the certificate;

(2) Any and all statements and information filled out by the Subscriber on the Certificate Application Form must be complete, true and correct and available for inspection and verification by SRCA or the Registration Authority;

(3) The subscriber shall properly keep the private key and take safe and reasonable measures to prevent the loss, leakage and tampering of the private key of the certificate;

(4) The subscriber is responsible for the use of the private key;

(5) In the event of any situation that may lead to a security crisis, such as loss of private key, forgetfulness, leakage of secrets, and other circumstances, the subscriber shall immediately notify SRCA and the registration authority, and apply for certificate revocation and other business processing in a timely manner;

(6) If the subscriber knows that his certificate has been fraudulently used, cracked or illegally used by others, he or she shall apply for revocation of his or her certificate in a timely manner in accordance with the relevant provisions of SRCA CPS.

9.6.4 Representations and Warranties of the Relying Party

The relying party must be familiar with the terms of this CPS and the certificate policies related to the subscriber's digital certificate, and ensure that its certificate is only used for the purpose intended at the time of application.

The Relying Party must take reasonable steps to verify the validity of the Subscriber's Digital Certificate and Digital Signature before relying on another subscriber's Digital Certificate.

The reliance of the relying party on the certificate indicates that they have read and understood any and all the terms of this CPS, and agree to assume the relevant responsibilities and obligations of the relying party in relation to certificate use.

9.6.5 Representations and Warranties of Other Participants

The representations and warranties of the other participants are the same as those provided in 9.6.4.

9.7 Force Majeure

SRCA shall not be liable for any loss, damage or delay in operation due to physical accidents or other force majeure events. These events include but not limited to labor disputes, intentional or unintentional acts of one of the parties to the transaction, strike, riot, unrest, war, fire, explosion, earthquake, flood, or other catastrophes.

In the "SRCA Digital Certificate Application (Renewal) and Use Liability Statement" provided by SRCA to the certificate subscribers, there is disclaimer clause that informs the certificate subscriber in advance: all types of certificates issued by SRCA can only be used to identify the user's identity, ensure the security of data transmission and make electronic signatures on the network, not for any other purposes, and SRCA does not assume any responsibility arising if the user's digital certificate is used for any other purposes. If the issuance of a digital certificate is incorrect, delayed, interrupted, or impossible due to equipment or network failure of CA, CA will re-issue the certificate without any liability for damages.

Prior to the issuance of the SRCA certificate, the certificate applicant has agreed to comply with the provisions of the "SRCA Digital Certificate Application (Renewal) and Use Liability Statement". The liability statement expressly states that SRCA shall not be liable for any form of warranty or obligation. If the certificate applicant intentionally or unintentionally provides false information or fails to update user information in a timely manner, resulting in the wrong certificate issued by the CA, and causing losses to the user and others, the user shall bear all responsibilities.

9.8 Scope of Responsibility

9.8.1 CA's Responsibilities

In accordance with the Company Law of the People's Republic of China, the Electronic Signature Law of the People's Republic of China and other laws and regulations, as a legally established limited liability company, SRCA only assumes limited liability within the limits of the law when assuming any responsibilities and obligations.

SRCA's responsibilities and obligations are:

(1) To ensure that the public key algorithm used and issued by the electronic certification service organization itself will not be breached under the existing normal technical conditions;

(2) To ensure that the signature private key of SRCA is securely stored and protected within SRCA;

(3) The security mechanism established and implemented by SRCA is in accordance with the provisions of national policy.

The above content is additionally explained as follows:

(1) Except for the aforesaid responsibility clause, SRCA, SRCA's service providers, SRCA's authorized issuing bodies, or SRCA's employees shall have no other obligations. It must be noted that nothing in this CPS can imply or be interpreted to the effect that SRCA must assume other obligations or make other undertakings with respect to its acts.

(2) In any of the circumstances of force majeure listed above, SRCA may be relieved of its responsibilities under this section and responsibilities and obligations under the corresponding certificate policy as a result of being affected.

(3) Due to the progress and development of technology, in order to ensure the security of certificates, SRCA will require certificate subscribers to replace their certificates in a timely manner to ensure that SRCA can better fulfill its responsibilities described in this section.

9.8.2 Responsibilities of the registration authority

Registration authorities must comply with all registration procedures and security safeguards. These procedures and safeguards are determined by SRCA and set out in this CPS or the applicable Registration Authority Agreement, as modified by SRCA as appropriate in the circumstances, and published in a timely manner.

Registration authorities must observe and comply with the terms of this CPS.

9.8.3 Responsibilities of the BT

Same as the responsibilities of the Registration Authorities.

9.8.4 Responsibilities of certificate subscribers

All certificate subscribers must strictly follow the procedures regarding the application for certificates and the ownership and secure storage of private keys:

(1) All statements and information provided by the Certificate Subscriber on the Certificate Application Form must be complete, accurate, true and correct and available for inspection and verification by SRCA; certificate subscribers must strictly comply with and follow the security measures set forth in this CPS or recommended by SRCA;

(2) Certificate subscribers shall be familiar with the terms of this CPS and the certificate policy related to their certificates, and shall also comply with the relevant restrictions on the use of certificate by certificate holders;

(3) In the event of any situation that may lead to a security crisis, such as loss of the private key, forgetting or leaking of secrets, and other circumstances, the certificate subscriber shall immediately notify SRCA or the SRCA-authorized issuing body and apply for revocation, suspension and other handling measures.

9.9 Indemnification

Indemnity incurred by SRCA in the course of certification activities shall be dealt with in accordance with the provisions of this CPS, unless otherwise required by laws and regulations.

SRCA will be liable for the loss of certificate subscribers and relying parties due to SRCA's own reasons, such as the wrong issuance or counterfeiting of certificates due to failure to strictly follow the business process for certificate approval, or the leakage or fraudulent use of CA private keys due to management negligence, but such liability is limited. In any event, in the SRCA Chain of Trust, the maximum indemnity limit per certificate for all parties (including, but not limited to, the certificate user, certificate applicant, recipient, or relying party) from CA, registration authority and BT in aggregate shall not exceed five times the price of each certificate. SRCA shall only be liable for direct losses caused by its own fault to users and shall not be liable for any indirect losses or damages.

9.9.1 SRCA’s Liability for Indemnification

In the event of a breach bby SRCA of its duties under Regulation 9.8 above, SRCA's liability for indemnification (other than statutory or contractual exemptions) shall be limited as follows:

(1) All of SRCA's liability shall not exceed five times the price of each certificate applicable to such certificate, which may be re-established by SRCA as the case may be, provided that SRCA will promptly notify the relevant party of the re-established rates.

（2）SRCA is liable for damages only within the period of validity prescribed by law.

9.9.2 Registration Authority’s Liability for Indemnification

The liability of a Registration Authority for indemnification is as set forth in the agreement entered into between the Registration Authority and the SRCA.

9.9.3 BT’s Liability for Indemnification

The liability of a BT for indemnification is as set forth in the agreement concluded between the BT and the SRCA.

9.9.4 Subscriber's Liability for Indemnification

(1) If a subscriber provides untrue materials when applying for a certificate, resulting in losses to SRCA or a third party, the subscriber shall be liable for any and all resulting losses;

(2) If a subscriber causes the leakage or loss of the private key due to its own fault, and fails to notify SRCA to revoke or suspend the private key in time, the subscriber shall bear all the liabilities for indemnification if SRCA or a third party suffers losses as a resut thereof;

(3) If a Subscriber's use of or the relying party's trust in certificate violates this CPS and related operating specifications, the subscriber or the relying party shall be liable for any and all resulting damages;

(4) If there are other indemnification provisions in the agreement signed between SRCA and the subscriber, reference shall be made to such provisions.

9.9.5 Amount of Indemnification

The total amount of indemnification for all parties (including but not limited to subscribers, applicants, recipients or relying parties) from SRCA and its authorized issuing body shall be set in accordance with the approval of the price control authorities and published on the website of Sinorail CA.

For the purposes of this clause, the term "total amount of indemnification" shall apply to any and all forms of damages caused to any and all parties due to their reliance on a certificate issued by SRCA, measured in the unit of each certificate, irrespective of the number of damage events caused by the certificate. The specific amount of the liability of SRCA and subscribers or other parties for indemnity shall be as stipulated by the relevant national laws and regulations, or as determined by the parties through negotiation. If the negotiation fails, it may be submitted to the judicial authority where the SRCA is located for resolution.

9.10 Term and Termination

9.10.1 Term

This CPS shall become effective from the date of issuance, indicating the version number and date of issuance in detail. Unless the SRCA specifically announces that the CPS is terminated, this CPS will remain in effect until a new version of the CPS is issued by SRCA.

9.10.2 Termination

When the new version of CPS is officially released and takes effect, the old version of CPS shall be automatically terminated. The SRCA CPS shall be terminated when the SRCA discontinues its business operations. SRCA shall report to the competent authorities in charge of the information industry 60 days before the termination of its service, and make appropriate arrangements.

9.10.3 Termination and Survival of Effect

Certain provisions of the CPS shall survive the termination, such as intellectual property recognition and confidentiality provisions. In addition, each participant is required to return or secure the destruction of confidential information obtained from other parties.

9.11 Relationship of responsibility between trust bodies

9.11.1 Liability of Trust Bodies and Certificate Subscribers for Damages

(1) If any act or omission of the Trust Body and the Certificate Subscriber causes losses to SRCA and the SRCA authorized issuing body when using or relying on the Certificate, the Trust Body and the Certificate Subscriber shall be jointly and severally liable for damages, corresponding losses, litigation and arbitration costs, and SRCA and the SRCA authorized Issuing Authority shall have the right to claim indemification;

(2) The liability of the Certificate Subscriber is not limited to the provisions of this CPS, and a Certificate Subscriber shall be responsible for the consequences of the Certificate Subscriber's misrepresentation in transmitting information to a third party that the third party would reasonably believe after verifying one or more electronic signatures with the Certificate;

(3) By accepting the Certificate, the Certificate Subscriber agrees to be liable for damages if the Certificate Subscriber (or a person authorized by the Certificate Subscriber to act on the instructions of the Certificate Subscriber) misrepresents or misinterprets the facts, the Certificate Subscriber fails to disclose any substantive fact, and the reason for such error or omission is due to his negligence or his intention to deceive SRCA or other authorities authorized by it, and the Certificate Subscriber fails to take the necessary precautions to prevent the loss or disclosure, modification or use of the private key by any unauthorized person.

(4) When a certificate is issued at the request of the agent of a certificate subscriber, both the agent and the certificate subscriber shall be jointly and severally liable. In the case of the circumstances described in article III, they shall be jointly liable for damages. It is the responsibility of the Certificate Subscriber to notify SRCA or SRCA-authorized bodies of any misrepresentations or omissions made by the Agent.

(5)Other circumstances in which the trust body and certificate subscriber shall be liable for damages according to laws and regulations or pursuant to agreements.

9.11.2 Fiduciary relationship

There is no agency or fiduciary relationship between the electronic certification service organization and the certificate subscriber and the trust body.

Neither the Certificate Subscriber nor the Trust Body has the right to hold SRCA liable as a fiduciary by contract or otherwise.

9.12 Amendment

SRCA has the right to amend, modify and vary any terms, conditions and provisions in this CPS at an appropriate time and without prior notice to any party.

SRCA has the right to set up and publish the results of modification in SRCA's own database or otherwise (e.g. in the form of a modified version of the CPS or on the website).

All amendments, modifications and changes shall be effective immediately upon publication. If a certificate subscriber fails to apply for invalidation (revocation) of the certificate within the time limit published after the result of the amendment, the subscriber shall be deemed to have agreed to such amendment, modification and change. Any and all content provided to certificate subscribers shall be subject to the latest version published on the website of Sinorail CA at www.sinorailca.com.

9.13 Dispute Resolution

Any issues and disputes that arise between the parties who are railway enterprises shall be resolved by both parties through friendly consultations, failing which they shall be resolved through mediation according to relevant regulations of China State Railway Group Co., Ltd. If consultations fail in case of parties outside the railway industry, lawsuit shall be filed to the people’s court where Sinorail CA is located for adjudication.

9.14 Regulatory Laws

This CPS shall be governed by and construed according to the laws of the People's Republic of China in all respects.

9.15 Applicable Law

Regardless of the choice of contract or other legal terms and whether a business relationship is established in China, the implementation, interpretation, translation and validity of the SRCA Certification Practice Statement shall be governed by the laws of the People's Republic of China. The choice of law is to ensure that there are uniform procedures and interpretations for all subscribers, regardless of where they live and where they use their certificates.

9.16 Miscellaneous

9.16.1 Conflict among various norms

In the event of any conflict between the provisions of this CPS and other regulations and guidelines, the Subscriber must be bound by this CPS, unless the provisions of this CPS are prohibited by law, or the relevant provisions or guidelines are clearly stated to take precedence over this CPS.

9.16.2 Property interests in security data

The following security-related information is deemed to be owned by the following named parties:

(1) Certificates: The exercise of the rights to and in the certificate is subject to the management of SRCA, and this rule aims to protect the privacy of subscribers and prevent unauthorized persons from publishing their certificates;

(2) Certification Practice Statement: The property rights to and in this CPS are owned by SRCA;

(3) Distinguished name: The distinguished name is owned by the naming entity (or their employer and person in charge);

(4) Private Key: A private key is the property of the subscriber (or his employer or principal) who lawfully uses or has the right to use the key, regardless of the physical medium in which the key is stored or protected;

(5) Public key: The public key is owned by the subscriber (or its employer or principal), regardless of the medium in which the key is stored or secured;

(6) SRCA's public key: SRCA, as the public key of its own root node, is the property of SRCA, and this public key is distributed under the authority of SRCA and placed on trustworthy hardware or software.

9.17General Terms

9.17.1 Entire Agreement

This Certification Practice Statement shall supersede prior written or oral interpretations relating to the subject matter, and this CPS, together with the Subscriber Agreement, the Relying Party Agreement, and other supplemental agreements, constitutes the entire agreement in the CA Trust Domain.

9.17.2Severability

When a court or other arbitral authority decides that a particular provision of the agreement is invalid or unenforceable for a particular reason, the invalidity of a particular provision will not render the entire agreement invalid.

9.17.3 Enforcement

The discharge of a party from liability for a breach of one part of the agreement shall not mean continued or future release of that party from liability for a breach of other provisions of the agreement.

9.17.4Force Majeure

Force majeure refers to objective circumstances that cannot be foreseen, avoided and overcome. Force majeure may be natural phenomena or natural disasters, such as earthquakes, volcanic eruptions, landslides, mudslides, avalanches, floods, tsunamis, typhoons and other natural phenomena; It may also be a social phenomenon, a social abnormal event, or a government action, such as the government issuing new policies, laws, and administrative regulations after the contract is concluded, making it impossible to perform the contract, or a social abnormal event such as war, strike, or riot.

9.17.5Miscellaneous

The right to interpret this "Certification Practice Statement" shall remain with Sinorail Certification Authority.