Raytonne Trust Services

Certification Practice Statement

Document Issue: 2.0

Date of Issue: October 17, 2022

Copyright Notice

Contents

1. INTRODUCTION

Raytonne Trust Services is a Certification Authority (CA) that issues high quality and highly trusted digital Certificates to entities including private and public companies and individuals in accordance with Raytonne Trust Services Certification Practice Statement (CPS). In its role as a CA, Raytonne Trust Services performs functions associated with public key operations that include receiving requests, issuing, revoking and renewing a digital Certificate and the maintenance, issuance and publication of Certificate Revocation Lists (CRLs) for users within the Raytonne Public Key Infrastructure (PKI).

Subscriber agrees to comply with this CPS together with all other applicable terms and conditions.

1.1. Overview

For issuance of Server Certificates, Raytonne Trust Services conforms to the current version of the Baseline Requirements (BR) and EV Guidelines (EVG) issued and managed by the CAB Forum. In the event of any inconsistency between this CPS and the other documents specified in this paragraph, those documents take precedence over this CPS.

This CPS is only one of a set of documents relevant to the provision of Certification Services by Raytonne Trust Services and that the list of documents contained in this clause are other documents that this CPS will from time to time mention, although this is not an exhaustive list. The document name, location of and status, whether public or private, are detailed below.

Document Status Location	Status	Location
Raytonne Trust Services Certification Practice Statement	Public	https://www.raytonne.com/PKI/
Raytonne Trust Services Certificate Policy	Public	https://www.raytonne.com/PKI/
Raytonne Trust Services Subscriber Agreement	Public	https://www.raytonne.com/PKI/
Raytonne Trust Services Relying Party Agreement	Public	https://www.raytonne.com/PKI/
Raytonne Trust Services Dengzhou Certificate Authority Agreement	Public	https://www.raytonne.com/PKI/

This CPS, related agreements and Certificate policies referenced within this document are available online at https://www.raytonne.com/PKI/.

1.2. Document Name and Identification

This document is the Raytonne Trust Services Certification Practice Statement (CPS). It outlines the legal, commercial and technical principles and practices that Raytonne Trust Services employs in providing certification services that include, but are not limited to, approving, issuing, using and managing of Digital Certificates and in maintaining a X.509 Certificate based public key infrastructure (PKI) in accordance with the

Certificate Policies determined by Raytonne Trust Services. It also defines the underlying certification processes for Subscribers and describes Raytonne Trust Services' repository operations. The CPS is also a means of notification of roles and responsibilities for parties involved in Certificate based practices within the Raytonne PKI.

The Raytonne Trust Services CPS is a public statement of the practices of Raytonne Trust Services and the conditions of issuance, revocation and renewal of a Certificate issued under Raytonne Trust Services' own hierarchy.

1.3. PKI Participants

This section identifies and describes some of the entities that participate within the Raytonne PKI. Raytonne Trust Services conforms to this CPS and other obligations it undertakes through adjacent contracts when it provides its services.

1.3.1. Certification Authorities

In its role as a CA, Raytonne Trust Services provides Certificate services within the Raytonne PKI. Raytonne Trust Services will:

- Conform its operations to the CPS (or other CA business practices disclosure), as the same may from time to time be modified by amendments published in the Repository,
- Issue and publish Certificates in a timely manner in accordance with the issuance times set out in this CPS,
- Upon receipt of a valid request to revoke the Certificate from a person authorized to request revocation using the revocation methods detailed in this CPS, revoke a Certificate issued for use within the Raytonne PKI,
- Publish CRLs on a regular basis, in accordance with the applicable Certificate Policy and with provisions described in this CPS,
- Distribute issued Certificates in accordance with the methods detailed in this CPS,
- Update CRLs in a timely manner as detailed in this CPS,
- Notify Subscribers via email of the imminent expiry of their Raytonne Trust Services issued Certificate (for a period disclosed in this CPS).

1.3.2. Internal Registration Authority

Raytonne Trust Services operates its own internal Registration Authority ("RA") that allows retail customers as well as all customers of Reseller Partners to manage their Certificate lifecycle, including application, issuance, renewal and revocation. Raytonne Trust Services' RA adheres to Raytonne Trust Services' CPS.

For the issuance of Server Certificates, this RA is also equipped with automated systems that validate domain control. For that minority of Server Certificates for which the validation of domain control is not possible by completely automated means, the specially trained and vetted staff that Raytonne Trust Services employs in its RA have the ability to cause the issuance of Certificates—but only when they are authenticated to Raytonne Trust Services' issuance systems using two-factor authentication.

1.3.3. Subscribers (End Entities)

Subscribers of Raytonne Trust Services are individuals or companies that use PKI in relation with Raytonne Trust Services supported transactions and communications. Subscribers are parties that are identified in a

Certificate and hold the Private Key corresponding to the Public Key listed in the Certificate. Prior to verification of identity and issuance of a Certificate, a Subscriber is an Applicant for the services of Raytonne Trust Services. issuance systems using two-factor authentication.

1.3.4. Relying Parties

Relying Parties use PKI services in relation with various Raytonne Trust Services Certificates for their intended purposes and may reasonably rely on such Certificates and/or digital signatures verifiable with reference to a Public Key listed in a Subscriber Certificate.

Because not all Raytonne Trust Services Certificate products are intended to be used in an e-commerce transaction or environment, parties who rely on Certificates not intended for e-commerce do not qualify as a Relying Party. Please refer to section 1.4 of this CPS to determine whether a particular product is intended for use in e-commerce transactions.

To verify the validity of a digital Certificate they receive, Relying Parties must refer to the CRL or Online Certificate Status Protocol (OCSP) response prior to relying on information featured in a Certificate to ensure that Raytonne Trust Services has not revoked the Certificate. The CRL location is detailed within the Certificate. OCSP responses are sent through the OCSP responder.

1.3.5. Other Participants

Raytonne Trust Services has several categories of partner, which assist in the provision of certification services.

1.3.5.1. Reseller Partners

Raytonne Trust Services operates a Reseller Partner network that allows authorized partners to integrate Raytonne Trust Services digital Certificates into their own product portfolios. Reseller Partners are responsible for referring digital Certificate customers to Raytonne Trust Services, who maintain full control over the Certificate lifecycle process, including application, issuance, renewal and revocation. Due to the nature of the reseller program, the Reseller Partner must authorize a pending customer order made through its Reseller Partner account prior to Raytonne Trust Services instigating the validation of such Certificate orders. All Reseller Partners are required to provide proof of organizational status (refer to section 3.2.2 of this CPS for examples of documentation required) and must enter into a Raytonne Trust Services Reseller Partner agreement prior to being provided with Reseller Partner facilities.

1.4. Certificate Usage

A digital Certificate is a formatted data that cryptographically binds an identified Subscriber with a Public Key. A digital Certificate allows an entity taking part in an electronic transaction to prove its identity to other participants in such transaction. Digital Certificates are used in commercial environments as a digital equivalent of an identification card.

Raytonne Trust Services currently offers a portfolio of digital Certificates and related products that can be used to address the needs of users for secure personal and business communications.

Raytonne Trust Services may update or extend its list of products, including the types of Certificates it issues, as it sees fit. The publication or updating of the list of Raytonne Trust Services products creates no claims by any third party.

1.4.1. Appropriate Certificate Uses

As detailed in this CPS, Raytonne Trust Services offers a range of distinct Certificate types. The different Certificate types have differing intended usages and differing policies. Pricing and Subscriber fees for the Certificates are made available on the relevant official Raytonne Trust Services websites. The maximum warranty associated with each Certificate is set forth in detail in section 9.2.3 of this CPS.

As the suggested usage for a digital Certificate differs on a per application basis, Subscribers are urged to appropriately study their requirements for their specific application before applying for a specific Certificate. Revoked Certificates are appropriately referenced in CRLs and published in Raytonne Trust Services directories.

1.4.1.1. Server Certificates

Server Certificates, also known as SSL or TLS certificates, facilitate the exchange of encryption keys in order to enable the encrypted communication of information over the Internet between the user of an Internet browser and a website. There are typically three levels of validation for Server Certificates.

Domain Validated (DV) Certificates: The appropriate use of DV Certificates is to keep information encrypted when sent between a client and a server where there are low risks and consequences of data compromise and where the identity of the server operator is of little consequence. DV Certificates are appropriate for entities needing low cost Certificates issued at a fast pace. DVs do not provide authentication or validation, and are the lowest cost means of securing a website.

Organization Validated (OV) Certificates: OV Certificates are used to keep information encrypted that is sent between a client and a server where there are moderate risks and consequences of data compromise, and therefore the end user desires to have reasonable assurance of the identity of the server operator. OV Certificates include business and company validation. Additionally, OV Certificates provide higher levels of trust and security than DV certificates, but provide lower levels of trust and security than EV Certificates.

Extended Validated (EV) Certificates: Clearly identify the legal entity that controls a website. EV certificates provide a greater level of assurance to the user of an Internet browser that the website the user is accessing is controlled by a specific legal entity identified in the Certificate Subject by name, address of place of business, jurisdiction of incorporation or registration, and the entities registration number or other disambiguating information.

Multidomain Certificates (MDC) are Certificates that may contain multiple FQDNs or IP addresses in the subjectAlternativeName field.

Wildcard Certificates are Certificates that cover sub-domains of any single domain. Wildcard Domain Names MUST NOT be issued in EV Certificates.

1.4.2. Prohibited Certificate Uses

Certificates are prohibited from being used to the extent that the use is inconsistent with applicable law. Certificates are prohibited from being used as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control systems, or weapons control systems, where failure could lead directly to death, personal injury, or severe damage to persons or property.

DV Certificates are not for use as a means of providing identity assurance.

1.5. Policy Administration

Information located in this section includes the contact information of the organization responsible for drafting, registering, maintaining, updating, and approving the Raytonne Trust Services CPS.

1.5.1. Organization Administering the Document

The Raytonne Trust Services Certificate Policy Authority maintains this CPS, related agreements and Certificate policies referenced within this document.

1.5.2. Contact Person

The Raytonne Trust Services Certificate Policy Authority may be contacted at the following address:

Henan Raytonne Trading Company
386 Changjiang Road
Nanyang, Henan 473000
China

To report abuse, fraudulent, or malicious use of Certificates issued by Raytonne Trust Services, please send email to:

- contact@raytonne.com.

1.5.3. Person Determining CPS Suitability for the Policy

The Raytonne Trust Services Certificate Policy Authority is responsible for determining the suitability of Certificate policies illustrated within this CPS. The Raytonne Trust Services Certificate Policy Authority is also responsible for determining the suitability of proposed changes to the CPS prior to the publication of an amended edition.

1.5.4. CPS approval procedures

This CPS and any subsequent changes, amendments, or addenda, shall be approved by the Henan Raytonne Trading Company Director of Technology.

1.6. Definitions and Acronyms

The list of definitions and acronyms located in this section are for use within the Raytonne Trust Services CPS.

1.6.1. Definitions

Term	Definition

Applicant	Means the natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Applicant is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual Certificate request.
Applicant Representative	Means a natural person or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant: (i) who signs and submits, or approves a Certificate request on behalf of the Applicant, and/or (ii) who signs and submits a Subscriber Agreement on behalf of the Applicant, and/or (iii) who acknowledges and agrees to the Certificate Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA.
Audit Report	Means a report from a Qualified Auditor stating the Qualified Auditor's opinion on whether an entity's processes and controls comply with the mandatory provisions of these Requirements.
Authorization Domain Name	Means the Domain Name used to obtain authorization for Certificate issuance for a given FQDN.
Basic Constraints	Means an extension that specifies whether the subject of the Certificate may act as a CA or only as an end-entity.
Baseline Requirements (BR)	Means the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, published at https://www.cabforum.org/.
Certificate	Means an electronic document that uses a digital signature to bind a Public Key and an entity.
Certificate Management System	Means a system used to process, approve issuance of, or store Certificates or Certificate status information, including the database, database server, and storage.
Certificate Management	Means the functions that include but are not limited to the following: verification of the identity of an Applicant of a Certificate; authorizing the issuance of Certificates; issuance of Certificates; revocation of Certificates; listing of Certificates; distributing Certificates; publishing Certificates; storing Certificates; storing Private Keys; escrowing Private Keys; generating, issuing, decommissioning, and destruction of key pairs; retrieving Certificates in accordance with their particular intended use; and verification of the domain of an Applicant of a Certificate.
Certificate Policy	Means a statement of the issuer that corresponds to the prescribed usage of a digital Certificate within an issuance context.

Certificate Systems	Means the system used by Raytonne Trust Services or a delegated third party in providing identity verification, registration and enrollment, Certificate approval, issuance, validity status, support, and other PKI related services.
Certificate Transparency	Means the protocol described in RFC 6962 for publicly logging the existence of Transport Layer Security (TLS) certificates as they are issued or observed.
Certification Authority Authorization	Means a DNS domain holder specify one or more CAs authorized to issue certificates for that domain name. This is described in RFC 8659.
Domain Contact	Means the Domain Name Registrant, technical contact, or administrative contract (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA record.
Domain Name	Means the label assigned to a node in the Domain Name System.
Domain Name Registrant	Means the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the "Registrant" by WHOIS or the Domain Name Registrar, and sometimes referred to as the "owner" of a Domain Name.
Domain Name Registrar	Means a person or entity that registers Domain Names under the auspices of or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN), (ii) a national Domain Name authority/registry, or (iii) a Network Information Center (including their affiliates, contractors, delegates, successors, or assigns).
EV Guidelines (EVG)	CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates published at https://www.cabforum.org/.
Grace Period	Means the period during which the Subscriber must make a revocation request.
IP Address Registration Authority	The Internet Assigned Numbers Authority (IANA) or a Regional Internet Registry (RIPE, APNIC, ARIN, AfriNIC, LACNIC).
Issuing System	Means a system used to sign Certificates or validity status information.
Legal Entity	Means an association, corporation, partnership, proprietorship, trust, government entity, or other entity with legal standing in a country's legal system.
Precertificate	Means a certificate that is constructed from the certificate to be issued by adding a special critical poison extension for the purpose of submission to a CT log in accordance with RFC 6962.
Private Key	Means the key of a key pair that is kept secret by the holder of the key pair, and that is used to create digital signatures and/or to decrypt

	electronic records or files that were encrypted with the corresponding Public Key.
Public Key	Means the key of a key pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify digital signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.
Random Value	Means a value specified by Raytonne Trust Services to the Applicant that exhibits at least 112 bits of entropy.
Reliable Method of Communication	Means a method of communication, such as a postal/courier delivery address, telephone number, or email address, that was verified using a source other than the Applicant Representative.
Relying Party	Means an entity that relies upon the information contained within the Certificate.
Relying Party Agreement	Means an agreement between Raytonne Trust Services and a Relying Party that must be read and accepted by a Relying Party prior to validating, relying on or using a Certificate and is available for reference in the Repository.
Repository	Means Raytonne Trust Services' repository, available at https://www.raytonne.com/PKI/.
Request Token	Means a value derived in a method specified by Raytonne Trust Services which binds a demonstration of control to the certificate request.
Root CA System	Means a system used to create a Root Certificate or to generate, store, or sign with the Private Key associated with a Root Certificate.
Policy Authority	Means the entity charged with the maintenance and publication of this CPS.
Security Support System	Means a system used to provide security support functions, such as authentication, network boundary control, audit logging, audit log reduction and analysis, vulnerability scanning, and anti-virus.
Subscriber	Means is an entity that has been issued a Certificate.
Subscriber Agreement	Means an agreement that must be read and accepted by an Applicant before applying for a Certificate. The Subscriber Agreement is specific to the digital Certificate product type as presented during the product online order process and is available for reference in the Repository.
Verified Method of Communication	Method of communication as defined and verified in conformance with Section 11.5 of the EVG.

WebTrust for Certification Authorities	Means the current program for CAs located at CPA Canada WebTrust Principles and Criteria.
Wildcard Certificate	A Certificate containing an asterisk (*) in the left-most position of any of the FQDNs contained in the Certificate Subject.
Wildcard Domain Name	A Domain Name consisting of a single asterisk character followed by a single full stop character (*.) followed by a FQDN.
X.509	Means the ITU-T standard for Certificates and their corresponding authentication framework.

1.6.2. Acronyms

Acronyms and abbreviations used throughout this CPS shall stand for the phrases or words set forth below:

Acronym	Full Name
ADN	Authorization Domain Name
BR	Baseline Requirements (see Definitions)
CA	Certificate Authority
CAA	Certification Authority Authorization
CA/B (or CAB)	Certificate Authority/Browser (Forum)
CMS	Certificate Management System
CPS	Certification Practice Statement
CRL(s)	Certificate Revocation List(s)
CSR	Certificate Signing Request
CT	Certificate Transparency
DN	Distinguished Name
DSA	Digital Signature Algorithm
EPKI	Enterprise Public Key Infrastructure Manager
ECDSA	Elliptic Curve Digital Signature Algorithm
EVG	EV Guidelines (see Definitions)
FIPS PUB	Federal Information Processing Standards Publication

FQDN	fully qualified domain name
FTP	File Transfer Protocol
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
ICANN	Internet Corporation for Assigned Names and Numbers
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
JoI	Jurisdiction of Incorporation
MDC	Multiple Domain Certificate
NIST	National Institute for Standards and Technology
OCSP	Online Certificate Status Protocol
PA	Policy Authority
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure (based on X.509 Digital Certificates)
PKCS	Public Key Cryptography Standard
RA(s)	Registration Authority(ies)
RFC	Request for Comments
RSA	Rivest Shamir Adleman
SAN	Subject Alternate Name
SHA	Secure Hash Algorithm
SSL	Secure Sockets Layer
TLS	Transport Layer Security
UTC	Coordinated Universal Time

URL	Uniform Resource Locator

1.6.3. Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”,

“SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in these Requirements shall be interpreted in accordance with RFC 2119.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

Raytonne Trust Services publishes this CPS, Certificate terms and conditions, the Relying Party Agreement and copies of all Subscriber Agreements and a list of EV Jurisdiction of Incorporation/Registration data sources in the Repository. The Raytonne Trust Services Certificate Policy Authority maintains the Raytonne Trust Services Repository. All updates, amendments and legal promotions are logged in accordance with the logging procedures referenced in section 5.4 of this CPS.

Published critical information may be updated from time to time as prescribed in this CPS. Such updates shall be indicated through appropriate version numbering and publication date on any new version.

2.1. Repositories

Raytonne Trust Services publishes a repository of legal notices regarding its PKI services, including this CPS, agreements and notices, references within this CPS, as well as any other information it considers essential to its services. The Repository may be accessed at https://www.raytonne.com/PKI/.

2.2. Publication of Certification Information

The Raytonne Trust Services Certificate services and the Repository are accessible through several means of communication:

- On the web: https://www.raytonne.com/PKI/
- By email: contact@raytonne.com

2.3. Time or Frequency of Publication

Issuance and revocation information regarding Certificates will be published as soon as possible. Updated or modified versions of Subscriber Agreements and Relying Party Agreements are usually published within seven days after approval. The Raytonne Trust Services CPS is reviewed and updated or modified versions are published at least once per year and in accordance with section 9.12 of this CPS. For CRL issuance frequency, see section 4.9.7 of this CPS.

2.4. Access Controls on Repositories

Documents published in the Repository are for public information and access is freely available. Raytonne Trust Services has logical access control and version control measures in place to prevent unauthorized modification of the Repository.

2.5. Accuracy of Information

Raytonne Trust Services, recognizing its trusted position, makes all reasonable efforts to ensure that parties accessing the Repository receive accurate, updated and correct information. Raytonne Trust Services, however, cannot accept any liability beyond the limits set in this CPS and the Raytonne Trust Services insurance policy.

3. IDENTIFICATION AND AUTHENTICATION

Raytonne Trust Services offers Server Certificates for secure online transactions. Prior to the issuance of a Certificate, Raytonne Trust Services will validate an application in accordance with this CPS that may involve the request by Raytonne Trust Services to the Applicant for relevant official documentation supporting the application.

Raytonne Trust Services conducts the overall certification management within the Raytonne PKI.

3.1. Naming

3.1.1. Types of Names

Raytonne Trust Services issues Certificates with non-null subject DNs. The constituent elements of the subject DN conform with ITU X.500.

Raytonne Trust Services does not issue pseudonymous Certificates.

Server authentication Certificates in general include entries in the subjectAlternateName (SAN) extension which are intended to be relied upon by relying parties.

3.1.2. Need for Names to be Meaningful

Raytonne Trust Services puts meaningful names in both the subjectDN and the issuerDN extensions of Certificates. The names in the Certificates identify the subject and issuer respectively.

3.1.3. Anonymity or Pseudonymity of Subscribers

Raytonne Trust Services does not issue pseudonymous Certificates for server authentication.

3.1.4. Rules for Interpreting Various Name Forms

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

3.1.5. Uniqueness of Names

Raytonne Trust Services does not in general enforce uniqueness of subject names. However, Raytonne Trust Services assigns Certificate serial numbers that appear in Raytonne Trust Services Certificates. Assigned serial numbers are unique. Raytonne Trust Services generates at least 64-bit serial numbers. These numbers are the output of a CSPRNG. We have a separate uniqueness check that verifies that serial numbers are never re-used.

For Server Certificates, domain name uniqueness is controlled by ICANN.

3.1.6. Recognition, Authentication, and Role of Trademarks

Subscribers and Applicants may not request Certificates with content that infringes the intellectual property rights of another entity. Unless otherwise specifically stated in this CPS, Raytonne Trust Services does not verify an Applicant’s or Subscriber’s right to use a trademark. Raytonne Trust Services does not resolve

trademark disputes. Raytonne Trust Services may reject any application or revoke any Certificate that is part of a trademark dispute.

Raytonne Trust Services does check subject names against a limited number of trademarks and brand names which are perceived to be of high value. A match between a part of the subject name and one of these high value names triggers a more careful examination of the subject name and Applicant.

3.2. Initial Identity Validation

This section contains information about Raytonne Trust Services' identification and authentication procedures for registration of subjects such as Applicants, RAs, CAs, and other participants. Raytonne Trust Services may use any legal means of communication or investigation to validate the identity of these subjects.

From time to time, Raytonne Trust Services may modify the requirements related to application information to respond to Raytonne Trust Services' requirements, the business context of the usage of a digital Certificate, other industry requirements, or as prescribed by law.

3.2.1. Method to Prove Possession of Private Key

Verification of a digital signature is used to determine that:

- the Private Key corresponding to the Public Key listed in the signer's Certificate created the digital signature, and
- the signed data associated with this digital signature has not been altered since the digital signature was created.

The usual means by which Raytonne Trust Services accepts signed data from an Applicant to prove possession of a Private Key is in the receipt of a PKCS#10 Certificate Signing Request (CSR).

3.2.2. Authentication of Organization and Domain Identity

Authentication of an organization identity is performed through the validation processes specified below and depends on the type of Certificate. Applications for Raytonne Trust Services Certificates are supported by appropriate documentation to establish the identity of an Applicant.

The following elements are critical information elements for a Raytonne Trust Services Certificate issued to an Organization. Those elements marked with PUBLIC are present within an issued Certificate and are therefore within the public domain. Those elements not marked with PUBLIC remain confidential in line with the privacy and protection of data provisions outlined in this CPS.

- Legal Name of the Organization (PUBLIC)
- Organizational unit (PUBLIC) (if applicable)
- Street, city, postal/zip code, country (PUBLIC) (if applicable)
- VAT-number (if applicable)
- Company/DUNS number (if available)
- Server Software Identification
- Payment Information
- Administrator contact full name, email address, and telephone

- Billing contact persons and organizational representative
- Fully Qualified Domain Name / Network Server Name / Public or Private IP (PUBLIC)
- Public Key (PUBLIC)
- Proof of right to use name
- Proof of existence and organizational status of the Organization
- Subscriber Agreement, signed (if applying out of bands)

3.2.2.1. Domain and IP Address Verification

3.2.2.1.1. Domain Verification

For each domain name to be included in the Server Certificate Subject, Raytonne Trust Services verifies the Applicant's control of the domain name in accordance with the Baseline Requirements, section 3.2.2.4, and maintains a record of the method used, using one of the following methods for each FQDN;

1. Email, Fax, SMS, or Postal Mail to Domain Contact as defined in section 3.2.2.4.2 of the Baseline Requirements.

   Communicating directly with the Domain Name Registrant using a postal address, email address, or telephone number provided by the Domain Name Registrar;

   Confirming the Applicant's control over the FQDN by sending a Random Value via email, fax, SMS, or postal mail to a recipient identified as a Domain Contact and then receiving a confirming response utilizing the Random Value.

   The Random Value, which is unique, is generated by Raytonne Trust Services and remains valid for use in a confirming response for no more than 30 days from its generation.

2. Constructed email to domain contact as defined in section 3.2.2.4.4 of the Baseline Requirements.

   Communicating directly with the Domain Contact confirming the Applicant's control over the requested FQDN using a constructed email address by:

   a. sending an email to one or more addresses created by using 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the at-sign ("@"), followed by an Authorization Domain Name,

   b. including a Random Value in the email, and

   c. having the Applicant submit (by clicking or otherwise) the Random Value to Raytonne Trust Services' servers to confirm receipt and authorization.

   The Random Value, which is unique, is generated by Raytonne Trust Services and remains valid for use in a confirming response for no more than 30 days from its generation.

3. DNS Change as defined in section 3.2.2.4.7 of the Baseline Requirements.

Confirming the Applicant's control over the requested FQDN by confirming the presence of a Random Value or Request Token in a DNS CNAME or TXT record for an Authorization Domain Name or an Authorization Domain Name that is prefixed with a label that begins with an underscore character. The Random Value, which is unique, is generated by Raytonne Trust Services and remains valid for no more than 30 days from its generation.

4. IP Address as defined in section 3.2.2.4.8 of the Baseline Requirements.

   Confirming the Applicant's control over the requested FQDN by confirming that the Applicant controls an IP address returned from a DNS lookup for A or AAAA records for the FQDN.

   This method is not used for validating wildcard domain names.

5. Email to DNS CAA contact as defined in section 3.2.2.4.13 of the Baseline Requirements.

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

   The Random Value, which is unique, is generated by Raytonne Trust Services and remains valid for no more than 30 days from its generation.

6. Email to DNS TXT contact as defined in Section 3.2.2.4.14 of the Baseline Requirements.

   Confirming the Applicant's control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value. The Random Value MUST be sent to an email address identified as a DNS TXT record email contact for the Authorization Domain Name selected to validate the FQDN.

   The Random Value, which is unique, is generated by Raytonne Trust Services and remains valid for no more than 30 days from its generation.

7. Phone contact with domain contact as defined in Section 3.2.2.4.15 of the Baseline Requirements.

   Confirming the Applicant's control over the FQDN by calling the domain contact's phone number and obtain a confirming response to validate the ADN.

   In the event of reaching voicemail, Raytonne Trust Services will leave a Random Value and the ADNs being validated and then receiving a confirming response utilizing the Random Value.

   The Random Value, which is unique, is generated by Raytonne Trust Services and remains valid for no more than 30 days from its generation.

8. Phone contact with DNS TXT record phone contact as defined in Section 3.2.2.4.16 of the Baseline Requirements.

Confirming the Applicant's control over the FQDN by calling the DNS TXT record phone contact's phone number and obtain a confirming response to validate the ADN.

In the event of reaching voicemail, Raytonne Trust Services will leave a Random Value and the ADNs being validated and then receiving a confirming response utilizing the Random Value.

The Random Value, which is unique, is generated by Raytonne Trust Services and remains valid for no more than 30 days from its generation.

9. Phone contact with DNS CAA phone contact as defined in Section 3.2.2.4.17 of the Baseline Requirements.

   Confirming the Applicant's control over the FQDN by calling the DNS CAA phone contact's phone number and obtain a confirming response to validate the ADN. The relevant CAA Resource Record Set MUST be found using the search algorithm defined in RFC 8659 Section 3.

   In the event of reaching voicemail, Raytonne Trust Services will leave a Random Value and the ADNs being validated and then receiving a confirming response utilizing the Random Value.

   The Random Value, which is unique, is generated by Raytonne Trust Services and remains valid for no more than 30 days from its generation.

10. Agreed-upon change to website v2 as defined in section 3.2.2.4.18 of the Baseline Requirements

    Confirming the Applicant's control over the requested FQDN by verifying that the Request Token or Random Value is contained in the contents of a file.

    Confirming that the Request Token or Random Value is located on the Authorization Domain Name, under the HTTP[S]://<Authorization Domain>/.well-known/pki-validation/ over port 80 (HTTP) or 443 (HTTPS).

    Raytonne Trust Services follows the requirements set in the BR section 3.2.2.4.18 regarding redirects when applicable.

    The Random Value, which is unique, is generated by Raytonne Trust Services and remains valid for use for no more than 30 days from its generation.

11. Agreed-upon change to website—ACME as defined in section 3.2.2.4.19 of the Baseline Requirements.

    Confirming the Applicant's control over the FQDN by validating domain control of the FQDN using the ACME HTTP Challenge method as defined in section 8.3 of RFC 8555.

    The token (as defined in section 8.3 of the RFC 8555) is generated by Raytonne Trust Services and remains valid for use for no more than 30 days from its generation.

    Raytonne Trust Services follows the requirements set in the BR section 3.2.2.4.18 regarding redirects when applicable.

12. TLS using ALPN as defined in section 3.2.2.4.20 of the Baseline Requirements.

Confirming the Applicant's control over a FQDN by validating domain control of the FQDN by negotiating a new application layer protocol using the TLS Application-Layer Protocol Negotiation (ALPN) Extension [RFC7301] as defined in RFC 8737. The token (as defined in RFC 8737, section 3) SHALL NOT be used for more than 30 days from its creation.

This method is not used for validating wildcard domain names.

3.2.2.1.2. IP Address Verification

For each IP Address to be included in the Server Certificate Subject, Raytonne Trust Services verifies the Applicant's control of the IP in accordance with the Baseline Requirements, section 3.2.2.5, using one of the following methods for each IP:

1. Agreed-upon change to website as defined in section 3.2.2.5.1 of the Baseline requirements.

   Confirming the Applicant's control over the requested IP Address by confirming the presence of a Request Token or Random Value contained in the content of a file or webpage in the form of a meta tag under the "/.well-known/pki-validation" directory, or another path registered with IANA for the purpose of validating control of IP Addresses, on the IP Address that is accessible by the CA via HTTP/HTTPS over an Authorized Port. The Request Token or Random Value SHALL NOT appear in the request.

   When a Random Value, which is unique, is used it remains valid for use for no more than 30 days from its generation.

2. Email, Fax, SMS, or Postal Mail to IP Address Contact as defined in section 3.2.2.5.2 of the Baseline Requirements.

   Confirming the Applicant's control over the IP Address by sending a Random Value via email, fax, SMS, or postal mail and then receiving a confirming response utilizing the Random Value. The Random Value MUST be sent to an email address, fax/SMS number, or postal mail address identified as an IP Address Contact. The Random Value SHALL be unique in each email, fax, SMS, or postal mail. The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation.

3. Reverse address lookup as defined in section 3.2.2.5.3 of the Baseline Requirements.

   Confirming the Applicant's control over the IP Address by obtaining a Domain Name associated with the IP Address through a reverse-IP lookup on the IP Address and then verifying control over the FQDN using a method permitted under Section 3.2.2.1.1 above.

4. Phone contact with IP Address contact as defined in section 3.2.2.5.5 of the Baseline Requirements.

   Confirming the Applicant's control over the IP Address by calling the IP Address contact's phone number and obtain a confirming response to validate the IP Address. Raytonne Trust Services makes the call to a phone number identified by the IP Address Registration Authority as the IP Address contact.

   In the event of reaching voicemail, Raytonne Trust Services will leave a Random Value and the IP Address being validated and then receiving a confirming response utilizing the Random Value.

The Random Value, which is unique, is generated by Raytonne Trust Services and remains valid for no more than 30 days from its generation.

5. ACME "http-01" method for IP Addresses as defined in section 3.2.2.5.6 of the Baseline Requirements.

   Confirming the Applicant's control over the IP Address by performing the procedure documented for a "http-01" challenge in draft 04 of "ACME IP Identifier Validation Extension", available at https://tools.ietf.org/html/draft-ietf-acme-ip-04#section-4.

6. ACME "tls-alpn-01" method for IP Addresses as defined in section 3.2.2.5.7 of the Baseline Requirements.

   Confirming the Applicant's control over the IP Address by performing the procedure documented for a "tls-alpn-01" challenge in draft 04 of "ACME IP Identifier Validation Extension", available at https://tools.ietf.org/html/draft-ietf-acme-ip-04#section-4.

3.2.2.2. Authentication of Organization Identity for OV TLS Server Certificates

In addition to the verification of domain control using the procedures listed above in section 3.2.2.1, Raytonne Trust Services verifies the identity and address of the Applicant in accordance with the *CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates* (commonly referred to as the Baseline Requirements), using documentation that is provided by, or through communication with at least one of the following:

- A government agency in the jurisdiction of the Applicant's legal creation, existence or recognition;
- A third-party database that is periodically updated and considered a Reliable Data Source;
- A site visit by the CA or a third party who is acting as an agent for the CA; or,
- An attestation letter;

Raytonne Trust Services MAY use the same documentation or communication described in 1 through 4 above to verify both the Applicant's identity and address. Alternatively, Raytonne Trust Services MAY verify the address of the Applicant (but not the identity of the Applicant) using a utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that Raytonne Trust Services determines to be reliable.

If the Subject Identity Information in the certificate is to include a DBA or Trade Name, Raytonne Trust Services shall verify the Applicant's right to use such DBA/Trade Name using number 1, 2, or 4 above, or:

1. Communication directly with a government agency responsible for the management of such DBAs or trade names, or;
2. A utility bill, bank statement, credit card statement, government issued tax document, or other form of identification that Raytonne Trust Services determines to be reliable.

3.2.2.3. Authentication of Organization Identity for EV TLS Server Certificates

Before issuing an EV Certificate, Raytonne Trust Services ensures that all Subject organization information to be included in the EV Server Certificate conforms to the requirements of, and is verified in accordance with the *CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates* (commonly referred to as the EV Guidelines).

Raytonne Trust Services will verify:

- Applicant's Legal Existence and Identity
- Applicant's Assumed Name (if applicable)
- Applicant's Physical Existence and Business Presence
- Verified Method of Communication with the Applicant
- Applicant's Operational Existence
- The Name, Title, and Authority of Contract Signer and Certificate Approver
- Signature on Subscriber Agreement and EV Certificate Requests
- Approval of EV Certificate Request

For purposes of verifying the Applicant's Legal Existence/Jurisdiction of Incorporation or Registration information Raytonne Trust Services uses the data published at government websites.

3.2.3. Authentication of Individual Identity

Authentication of an individual identity is performed through the validation processes specified below, and depends on the type of Certificate. Applications for Raytonne Trust Services Certificates are supported by appropriate documentation to establish the identity of an Applicant.

The following elements are critical information elements for a Raytonne Trust Services Certificate issued to an individual:

- Legal Name of the Individual (PUBLIC)
- Organizational unit (PUBLIC) (if applicable)
- Street, city, postal/zip code, country (PUBLIC) (if applicable)
- VAT-number (if applicable)
- Server Software Identification
- Payment Information
- Administrator contact full name, email address and telephone
- Billing contact persons and organizational representative
- Fully Qualified Domain Name / Network Server Name / Public or Private IP (PUBLIC)
- Public Key (PUBLIC)
- Proof of right to use name
- Proof of existence and organizational status of the Organization
- Subscriber Agreement, signed (if applying out of bands)

3.2.3.1. Domain and IP Address Verification

Same as section 3.2.2.1 for Organizational Applicants.

3.2.3.2. Individual Identity Verification for OV TLS Server Certificates

In addition to the verification of domain control using the procedures listed above in section 3.2.2.1 of this CPS, if the Applicant is a natural person, Raytonne Trust Services verifies the identity and address of the Applicant in accordance with the Baseline Requirements, using:

1. Verify the Applicant's name using a legible copy, which discernibly shows the Applicant's face, of at least one currently valid government issued photo ID (passport, driver's license, military ID, national ID or equivalent document type)
2. Verify the Applicant's address using a form of identification that Raytonne Trust Services determines to be reliable such as a government ID, utility bill, or bank or credit card statement. Raytonne Trust Services MAY rely on the same government issued ID that was used to verify the Applicant's name.

Raytonne Trust Services may accept or require, at its discretion, other official documentation supporting an application, possibly including, but not limited to, requiring face to face verification of the Applicant's identity before an authorized agent of Raytonne Trust Services, an attorney, a CPA, a Latin notary, a notary public or equivalent.

Raytonne Trust Services verifies the certificate request with the Applicant using a Reliable Method of Communication.

3.2.3.3. Individual Identity Verification for EV TLS Server Certificate

Raytonne Trust Services does not issue EV TLS Server Certificates to Individual Applicants.

3.2.4. Non-Verified Subscriber Information

Notwithstanding the limited warranties provided under this CPS, Raytonne Trust Services shall not be responsible for non-verified Subscriber information submitted to Raytonne Trust Services, or the Raytonne Trust Services directory or otherwise submitted with the intention to be included in a Certificate.

For server authentication Certificates, Raytonne Trust Services verifies the subject elements as defined in section 9.2 of the Baseline Requirements.

3.2.5. Validation of Authority

Validation of authority involves a determination of whether a person has specific rights, entitlements, or permissions, including the permission to act on behalf of an organization to obtain a Certificate. Validation of authority is dependent on the type of Certificate requested and is performed in accordance with section 3.2.7 of this CPS.

3.2.5.1. Domain Registrant Authorization of TLS Server Certificates

Authorization by the Domain Name Registrant is verified as documented in section 3.2.2.1 of this CPS.

3.2.5.2. OV TLS Server Certificates

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

Raytonne Trust Services MAY use the sources listed in section 3.2.2.2 to verify the Reliable Method of Communication. Provided that a Reliable Method of Communication is used, Raytonne Trust Services MAY establish the authenticity of the certificate request directly with the Applicant Representative or with an authoritative source within the Applicant's organization, such as the Applicant's main business offices,

corporate offices, human resource offices, information technology offices, or other department that Raytonne Trust Services deems appropriate.

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

3.2.5.3. EV TLS Server Certificates

The request is verified in accordance with the CA/B Forum Guidelines for the Issuance and Management of Extended Validation Certificates section 11.5.

3.2.6. Criteria for Interoperation

Raytonne Trust Services may provide services allowing for another CA to operate within, or interoperate with, its PKI. Such interoperation may include cross-certification, unilateral certification, or other forms of operation. Raytonne Trust Services reserves the right to provide interoperation services and to interoperate transparently with other CAs; the terms and criteria of which are to be set forth in the applicable agreement.

3.2.7. Application Validation

Prior to issuing a Certificate Raytonne Trust Services employs controls to validate the identity of the Subscriber information featured in the Certificate application.

3.3. Identification and Authentication for Re-Key Requests

Raytonne Trust Services supports rekeys on:

- Replacement, which is when a Subscriber wishes to change some (or none) of the subject details in an already issued Certificate and may (or may not) also wish to change the key associated with the new Certificate; and
- Renewal, which is when a Subscriber wishes to extend the lifetime of a Certificate which has been issued and may at the same time vary some (or none) of the subject details and may also change the key associated with the Certificate.

In both cases, Raytonne Trust Services requires the Subscriber to use the same authentication details (typically username and password) which they used in the original purchase of the Certificate. In either case, if any of the subject details are changed during the replacement or renewal process then the subject must be reverified.

3.3.1. Identification and Authentication for Routine Re-Key

As stated above—in both cases, Raytonne Trust Services requires the Subscriber to use the same authentication details (typically username and password) which they used in the original purchase of the Certificate.

3.3.2. Identification and Authentication for Re-Key after Revocation

Raytonne Trust Services does not routinely permit rekeying (or any form of reissuance or renewal) after revocation. Revocation is a terminal event in the Certificate lifecycle.

Where a request for replacement or renewal of a Certificate after revocation is considered, Raytonne Trust Services requires the Subscriber to authenticate itself using the original authentication details (typically username and password) used in the initial purchase of the Certificate. However, this may be varied, or rekeying may be refused after revocation, where the exact circumstances and reasons for which the Certificate was revoked are not adequately explained. Reissuance or replacement after revocation is solely at Raytonne Trust Services' discretion.

3.4. Identification and Authentication for Revocation Request

Revocation at the Subscriber's request:

The Subscriber must either be in possession of the authentication details (typically username and password) which were used to purchase the Certificate originally OR the Subscriber must be able to send an S/MIME email signed with the Private Key associated with the Certificate.

Revocation at the RA's request:

The RA must be in possession of the authentication details used to affect the original Certificate request to the CA.

Revocation at the CA's request:

Raytonne Trust Services does not revoke Certificates at the request of other CAs. Raytonne Trust Services can and does revoke Subscriber Certificates for cause as set out in section 4.9 of this CPS, but identification and authentication are not required in these cases.

Raytonne Trust Services employs the following procedure for authenticating a revocation request:

- The revocation request must be sent by the administrator contact associated with the Certificate application. Raytonne Trust Services may, if necessary, also request that the revocation request be made by either/or the organizational contact and billing contact.
- Upon receipt of the revocation request Raytonne Trust Services will request confirmation from the known administrator out of bands contact details, either by telephone or by fax.
- Raytonne Trust Services validation personnel will then command the revocation of the Certificate and logging of the identity of validation personnel and reason for revocation will be maintained in accordance with the logging procedures covered in this CPS.

4. CERTIFICATE LIFECYCLE OPERATIONAL REQUIREMENTS

This section describes the Certificate application process, including the information required to make and support a successful application. Additionally, this section describes some of the requirements imposed upon RAs, Subscribers, and other participants with respect to the lifecycle of a Certificate.

The validity period of Raytonne Trust Services Certificates varies dependent on the Certificate type, but typically, a Certificate will be valid for 1 year.

The following steps describe the milestones to issue a Server Certificate:

1. The Applicant fills out the online request on Raytonne Trust Services' website and the Applicant submits the required information: Certificate Signing Request (CSR), e-mail address, common name, organizational information, country code, verification method and billing information.
2. The Applicant accepts the online Subscriber Agreement.
3. The Applicant submits the required information to Raytonne Trust Services.
4. The Applicant pays the Certificate fees.
5. Raytonne Trust Services verifies the submitted information using third party databases and Government records.
6. Upon successful validation of the application information, Raytonne Trust Services may issue the Certificate to the Applicant or should the application be rejected, Raytonne Trust Services will alert the Applicant that the application has been unsuccessful.
7. Renewal is conducted as per the procedures outlined in this CPS and the official Raytonne Trust Services websites.
8. Revocation is conducted as per the procedures outlined in this CPS.

4.1. Certificate Application

A Certificate request can be done according to the following means:

On-line: Via the Web (https). The Certificate Applicant submits an application via a secure online link according to a procedure provided by Raytonne Trust Services. Additional documentation in support of the application may be required so that Raytonne Trust Services verifies the identity of the Applicant. The Applicant submits to Raytonne Trust Services such additional documentation. Upon verification of identity, Raytonne Trust Services issues the Certificate and sends a notice to the Applicant. The Applicant downloads and installs the Certificate to its device. The Applicant must notify Raytonne Trust Services of any inaccuracy or defect in a Certificate promptly after receipt of the Certificate or earlier notice of informational content to be included in the Certificate.

Raytonne Trust Services may at its discretion, accept applications via email.

4.1.1. Who Can Submit a Certificate Application

Generally, Applicants will complete the online forms made available by Raytonne Trust Services. Under special circumstances, the Applicant may submit an application via email; however, this process is available at the discretion of Raytonne Trust Services.

4.1.2. Enrollment Process and Responsibilities

All Certificate Applicants must complete the enrolment process, which may include:

- Generate an RSA or ECC key pair and demonstrate to Raytonne Trust Services ownership of the Private Key associated with the Public Key to be included in the Certificate through the submission of a valid PKCS#10 Certificate Signing Request (CSR) (or SPKAC request for certain client authentication or email Certificates).
- Make all reasonable efforts to protect the integrity and confidentiality of the Private Key.
- Submit to Raytonne Trust Services a Certificate application, including application information as detailed in this CPS, a Public Key corresponding to the Private Key of which they are in possession, and agree to the terms of the relevant Subscriber Agreement.
- Provide proof of identity through the submission of official documentation as requested by Raytonne Trust Services during the enrolment process.

4.2. Certificate Application Processing

The following table details the entity(s) involved in the processing of Certificate applications.

Certificate Type	Enrolment Entity	Processing Entity	Issuing Authority
Server Certificate—all types as per section 2.4.1 of this CPS	End Entity Subscriber	Raytonne Trust Services	Raytonne Trust Services
Server Certificate—all types as per section 2.4.1 of this CPS	Reseller on behalf of End Entity Subscriber	Raytonne Trust Services	Raytonne Trust Services

4.2.1. Performing Identification and Authentication Functions

Upon receipt of an application for a digital Certificate and based on the submitted information, Raytonne Trust Services confirms the following information:

- The Certificate Applicant is the same person as the person identified in the Certificate request.
- The Certificate Applicant holds the Private Key corresponding to the Public Key to be included in the Certificate.
- The information to be published in the Certificate is accurate, except for non-verified Subscriber information.
- Any agents who apply for a Certificate listing the Certificate Applicant’s Public Key are duly authorized to do so.

Raytonne Trust Services may use the services of a third party to confirm information on a business entity that applies for a digital Certificate. Raytonne Trust Services accepts confirmation from third party organizations, other third-party databases, and government entities.

Raytonne Trust Services' controls may also include trade registry transcripts that confirm the registration of the Applicant company and state the members of the board, the management and directors representing the company.

Raytonne Trust Services may use any means of communication at its disposal to ascertain the identity of an organizational or individual Applicant. Raytonne Trust Services reserves right of refusal in its absolute discretion.

Raytonne Trust Services has a system in place which examines subject details, including domain names, for matches or near matches to some known high profile or pre-notified names that may indicate that a certificate is at a higher than normal risk of fraudulent applications being made and in those cases the certificate application is flagged for manual review.

4.2.2. Approval or Rejection of Certificate Applications

Following successful completion of all required validations of a Certificate application Raytonne Trust Services approves an application for a digital Certificate.

If the validation of a Certificate application fails, Raytonne Trust Services rejects the Certificate application. Raytonne Trust Services reserves its right to reject applications to issue a Certificate to Applicants if, on its own assessment, by issuing a Certificate to such parties the good and trusted name of Raytonne Trust Services might get tarnished, diminished or have its value reduced and under such circumstances may do so without incurring any liability or responsibility for any loss or expenses arising as a result of such refusal.

Applicants whose applications have been rejected may subsequently reapply.

In all types of Raytonne Trust Services Certificates, the Subscriber has a continuous obligation to monitor the accuracy of the submitted information and notify Raytonne Trust Services of any changes that would affect the validity of the Certificate. Failure to comply with the obligations as set out in the Subscriber Agreement will result in the revocation of the Subscriber's Certificate without further notice to the Subscriber and the Subscriber shall pay any charges payable but that have not yet been paid under the Subscriber Agreement.

4.2.3. Time to Process Certificate Applications

Raytonne Trust Services makes reasonable efforts to confirm Certificate application information and issue a digital Certificate within a reasonable time frame. The time frame is greatly dependent on the Subscriber providing the necessary details and/or documentation in a timely manner. Upon the receipt of the necessary details and/or documentation, Raytonne Trust Services aims to confirm submitted application data and to complete the validation process and issue/reject a Certificate application within 2 working days.

From time to time, events outside of the control of Raytonne Trust Services may delay the issuance process, however Raytonne Trust Services will make every reasonable effort to meet issuance times and to make Applicants aware of any factors that may affect issuance times in a timely manner.

4.2.4. Certificate Authority Authorization

Where an application is for a Certificate which includes a domain-name and is to be used for server authentication, Raytonne Trust Services examines the Certification Authority Authorization (CAA) DNS

Resource Records as specified in RFC 8659 and, if such CAA Records are present and do not grant Raytonne Trust Services the authority to issue the Certificate, the application is rejected.

Where the 'issue' and 'issuewild' tags are present within a CAA record, Raytonne Trust Services recognizes the following domain names within those tags as granting authorization for issuance by Raytonne Trust Services.

- raytonne.com
- ruiduntrading.com

4.3. Certificate Issuance

Raytonne Trust Services issues a Certificate upon approval of a Certificate application. A digital Certificate is deemed to be valid at the moment a Subscriber accepts it (refer to section 4.4 of this CPS). Issuing a digital Certificate means that Raytonne Trust Services accepts a Certificate application.

Raytonne Trust Services Certificates are issued to organizations or individuals.

Subscribers shall solely be responsible for the legality of the information they present for use in Certificates issued under this CPS, in any jurisdiction in which such content may be used or viewed.

4.3.1. CA Actions during Certificate Issuance

Raytonne Trust Services' automated systems receive and collate:

- evidence gathered during the verification process, and/or
- assertions that the verification has been completed according to the policy and internal documentation that sets out the acceptable means of verifying subject information.

Raytonne Trust Services' automated systems record the details of the business transaction associated with the submission of a Certificate request and the eventual issuance of a Certificate, one example of which is a sales process involving a credit card payment.

Raytonne Trust Services' automated (and manual) systems record the source of, and all details submitted with, evidence of verification, having been performed either by external RAs or by Raytonne Trust Services' internal RA.

The correct authentication of verification evidence provided by external RAs is required before that evidence will be considered for Certificate issuance.

The only certificates Raytonne Trust Services issues from its root CAs are intermediate CA certificates and cross certificates. Our CA has no facility for the automated signature of such certificates, so this activity necessarily involves manual intervention by privileged users to sign such certificates. Certificate issuance by the Root CA requires an individual authorized by the CA (i.e. the CA system operator, system officer, or PKI administrator) to deliberately issue a direct command in order for the Root CA to perform a certificate signing operation.

4.3.2. Notification to Subscriber by the CA of Issuance of Certificate

Raytonne Trust Services notifies Subscriber of the issuance of a Certificate through delivery.

Subscribers are notified of certificate issuance via email using the administrator contact email address provided during the application process. Subscriber downloads the certificate securely from the Raytonne Trust Services online account manager.

4.3.3. Refusal to Issue a Certificate

Raytonne Trust Services reserves its right to refuse to issue a Certificate to any party as it sees fit, without incurring any liability or responsibility for any loss or expenses arising out of such refusal. Raytonne Trust Services reserves the right not to disclose reasons for such a refusal.

4.4. Certificate Acceptance

This section describes some of the actions by Subscriber in accepting a Certificate. Additionally, it describes how Raytonne Trust Services publishes a Certificate and how Raytonne Trust Services notifies other entities of the issuance of a Certificate.

4.4.1. Conduct Constituting Certificate Acceptance

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

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

4.4.2. Publication of the Certificate by the CA

A Certificate is published through various means: (1) by Raytonne Trust Services making the Certificate available in the Repository; and (2) by Subscriber using the Certificate subsequent to Raytonne Trust Services' delivery of the Certificate to Subscriber.

4.4.3. Notification of Certificate Issuance by the CA to Other Entities

Raytonne Trust Services publishes the issuance data of all TLS Server Certificates in the form of a Precertificate, to Certificate Transparency (CT) logs.

4.5. Key Pair and Certificate Usage

This section is used to describe the responsibilities relating to the use of keys and Certificates.

4.5.1. Subscriber Private Key and Certificate Usage

The intended scope of usage for a private key shall be specified through certificate extensions, including the key usage and extended key usage extensions, in the associated certificate.

4.5.2. Relying Party Public Key and Certificate Usage

The final decision concerning whether or not to rely on a verified digital signature is exclusively that of the Relying Party. Reliance on a digital signature should only occur if:

- the digital signature was created during the operational period of a valid Certificate and it can be verified by referencing a validated Certificate;

- the Relying Party has checked the revocation status of the Certificate by referring to the relevant CRLs and the Certificate has not been revoked;
- the Relying Party understands that a digital Certificate is issued to a Subscriber for a specific purpose and that the digital Certificate may only be used in accordance with the usages suggested in the CPS and named as Object Identifiers in the Certificate profile; and
- the Certificate applied for is appropriate for the application it is used in.

Reliance is accepted as reasonable under the provisions made for the Relying Party under this CPS and within the Relying Party agreement. If the circumstances of reliance exceed the assurances delivered by Raytonne Trust Services under the provisions made in this CPS, the Relying Party must obtain additional assurances.

Warranties are only valid if the steps detailed above have been carried out.

4.6. Certificate Renewal

Certificate renewal means the issuance of a new Certificate to the Subscriber without changing the Subscriber's, or other participant's, Public Key or any other information in the Certificate.

Renewal fees are detailed on the official Raytonne Trust Services websites and within communications sent to Subscribers approaching the Certificate expiration date.

4.6.1. Circumstance for Certificate Renewal

Raytonne Trust Services shall make reasonable efforts to notify Subscribers via e-mail of the imminent expiration of a digital Certificate. Notice shall ordinarily be provided within a 60- day period prior to the expiry of the Certificate.

4.6.2. Who May Request Renewal

Those who may request renewal of a Certificate include, but are not limited to, a Subscriber on behalf of itself, and an RA on behalf of a Subscriber. Raytonne Trust Services does not automatically renew Certificates.

4.6.3. Processing Certificate Renewal Requests

In order to process Certificate renewal requests, Raytonne Trust Services gets the Subscriber to reauthenticate itself. Renewal application requirements and procedures are the same as those employed for the application validation and issuance requirements detailed for new customers.

4.6.4. Notification of New Certificate Issuance to Subscriber

Notification to the Subscriber about the issuance of a renewed Certificate is given using the same means as a new Certificate, described in section 4.3.2 of this CPS.

4.6.5. Conduct Constituting Acceptance of a Renewal Certificate

Subscriber's conduct constituting acceptance of a renewal Certificate is the same as listed in section 4.4.1 of this CPS.

4.6.6. Publication of the Renewal Certificate by the CA

Raytonne Trust Services publishes a renewed Certificate by delivering it to the Subscriber. In the limited circumstances where Raytonne Trust Services publishes a renewed Certificate by alternate means, Raytonne Trust Services does so by using the LDAP server—a publicly accessible directory of client Certificates.

4.6.7. Notification of Certificate Issuance by the CA to Other Entities

Generally, Raytonne Trust Services does not notify other entities of a renewed Certificate. In limited circumstances, Raytonne Trust Services will notify other entities through the means described in section 4.6.6 of this CPS. Raytonne Trust Services may also notify an RA, if the RA was involved in the renewal process.

4.7. Certificate Re-Key

The section is used to describe elements/procedures generating a new key pair and applying for the issuance of a new Certificate that certifies the new Public Key. Rekeying (or re-keying) a Certificate may comprise of creating a new Certificate with a new Public Key and serial number, while retaining the Certificate's subject information.

4.7.1. Circumstances for Certificate Re-Key

Certificate rekey will ordinarily take place as part of a Certificate renewal or Certificate replacement, as stated in section 3.2 of this CPS. Certificate rekey may also take place when a key has been compromised.

4.7.2. Who May Request Certificate Re-Key

Those who may request a Certificate rekey include, but are not limited to, the Subscriber, the RA on behalf of the Subscriber, or Raytonne Trust Services at its discretion.

4.7.3. Processing Certificate Re-Key Requests

Depending on the circumstances, the procedure to process a Certificate rekey may be the same as issuing a new Certificate. Under other circumstances, Raytonne Trust Services may process a rekey request by having the Subscriber authenticate its identity.

4.7.4. Notification of Re-Key to Subscriber

Raytonne Trust Services will notify Subscriber of a Certificate rekey by the means delineated in section 4.3.2 of this CPS.

4.7.5. Conduct Constituting Acceptance of a Re-Keyed Certificate

Subscriber's conduct constituting acceptance of a rekeyed Certificate is the same as listed in section 4.4.1 of this CPS.

4.7.6. Publication of the Re-Keyed Certificate by the CA

Publication a rekeyed Certificate is performed by delivering it to the Subscriber.

4.7.7. Notification of Certificate Issuance by the CA to Other Entities

Generally, Raytonne Trust Services does not notify other entities of the issuance of a rekeyed Certificate. Raytonne Trust Services may notify an RA of the issuance of a rekeyed Certificate when an RA was involved in the issuance process.

4.8. Certificate Modification

Raytonne Trust Services does not offer Certificate modification. Instead, Raytonne Trust Services will revoke the old Certificate and issue a new Certificate as a replacement.

4.9. Certificate Revocation and Suspension

Revocation of a Certificate is to permanently end the operational period of the Certificate prior to reaching the end of its stated validity period. In other words, upon revocation of a Certificate, the operational period of that Certificate is immediately considered terminated. The serial number of the revoked Certificate will be placed within the CRL and remains on the CRL until sometime after the end of the Certificate's validity period.

Raytonne Trust Services does not utilize Certificate suspension.

4.9.1. Circumstances for Revocation

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

- The Subscriber requests in writing that the CA revoke the Certificate;
- The Subscriber notifies Raytonne Trust Services that the original Certificate request was not authorized and does not retroactively grant authorization;
- Raytonne Trust Services reasonably believes there has been loss, theft, modification, unauthorized disclosure, or other compromise of the Private Key associated with the Certificate;
- Raytonne Trust Services reasonably believes that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address in the Certificate should not be relied upon;

Raytonne Trust Services SHOULD revoke within 24 hours but MUST revoke within 5 days if one or more of the following occurs:

- The Subscriber or Raytonne Trust Services has breached a material obligation under this CPS or the relevant Subscriber Agreement;
- The Certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6 of the Baseline Requirements;
- Raytonne Trust Services is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);
- Raytonne Trust Services is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
- Either the Subscriber's or Raytonne Trust Services' obligations under this CPS or the relevant Subscriber Agreement are delayed or prevented by a natural disaster, computer or communications failure, or other

cause beyond the person's reasonable control, and as a result another person's information is materially threatened or compromised;
- There has been a modification of the information pertaining to the Subscriber that is contained within the Certificate;
- Raytonne Trust Services is made aware of a material change in the information contained in the Certificate, or the information contained in the Certificate is inaccurate;
- A personal identification number, Private Key or password has, or is likely to become known to someone not authorized to use it, or is being or is likely to be used in an unauthorized way
- The Certificate has not been issued in accordance with the policies set out in this CPS;
- The Subscriber has used the Certificate contrary to law, rule or regulation, or Raytonne Trust Services reasonably believes that the Subscriber is using the Certificate, directly or indirectly, to engage in illegal or fraudulent activity;
- The Certificate was issued to persons or entities identified as publishers of malicious software or that impersonated other persons or entities;
- The Certificate was issued as a result of fraud or negligence;
- Raytonne Trust Services is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise, methods have been developed that can easily calculate it based on the Public Key, or if there is clear evidence that the specific method used to generate the Private Key was flawed;
- Raytonne Trust Services right to issue Certificates under the Baseline Requirements expires or is revoked or terminated, unless Raytonne Trust Services has made arrangements to continue maintaining the CRL/OCSP Repository; or
- The Certificate, if not revoked, will compromise the trust status of Raytonne Trust Services.

Raytonne Trust Services will revoke a Subordinate CA Certificate within seven (7) days if one or more of the following occurs:

- The Subordinate CA requests revocation in writing;
- The Subordinate CA notifies Raytonne Trust Services that the original certificate request was not authorized and does not retroactively grant authorization;
- Raytonne Trust Services obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Sections 6.1.5 and 6.1.6 of the Baseline Requirements;
- Raytonne Trust Services obtains evidence that the Subordinate CA Certificate was misused;
- The Subordinate CA Certificate was not issued by 邓州 ClientServer 2032 and Raytonne Trust Services is made aware that that Subordinate CA Certificate was not issued in accordance with, or that Subordinate CA has not complied with, the Baseline Requirements or this CPS;
- The Subordinate CA Certificate was issued by 邓州 ClientServer 2032 and Raytonne Trust Services is made aware that that Subordinate CA Certificate was not issued in accordance with, or that Subordinate CA has not complied with, the Baseline Requirements or this CPS or the Dengzhou Certificate Authority Agreement;
- Raytonne Trust Services determines that any of the information appearing in the Subordinate CA Certificate is inaccurate or misleading;
- Raytonne Trust Services or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
- Raytonne Trust Services', or Subordinate CA's, right to issue Certificates under the Baseline Requirements expires or is revoked or terminated, unless Raytonne Trust Services has made arrangements to continue maintaining the CRL/OCSP Repository;

- Revocation is required by this CPS;
- The Subordinate CA has used the Certificate contrary to law, rule or regulation, or Raytonne Trust Services reasonably believes that the Subordinate CA is using the Certificate, directly or indirectly, to engage in illegal or fraudulent activity;
- The Subordinate CA Certificate was issued to persons or entities identified as publishers of malicious software or that impersonated other persons or entities;
- The Subordinate CA Certificate was issued as a result of fraud or negligence;
- The Subordinate CA Certificate, if not revoked, will compromise the trust status of Raytonne Trust Services.

4.9.2. Who Can Request Revocation

A Subscriber or another appropriately authorized party can request revocation of a Certificate. An authorized party includes an RA, regardless of whether on behalf of the Subscriber may request revocation through their account. Other parties may report suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates, in the first instance, by email to contact@raytonne.com.

4.9.3. Procedure for Revocation Request

Raytonne Trust Services accepts and responds to revocation requests and problem reports on a 24/7 basis. Prior to the revocation of a Certificate, Raytonne Trust Services will verify that the revocation request has been:

- Made by the organization or individual entity that has made the Certificate application.
- Made by the RA on behalf of the organization or individual entity that used the RA to make the Certificate application, and
- Has been authenticated by the procedures in section 3.4 of this CPS.

4.9.4. Revocation Request Grace Period

The revocation request grace period ("Grace Period") means the period during which the Subscriber must make a revocation request. The Grace Period is defined in the Subscriber Agreement applicable to the individual Subscriber. In the event that a Grace Period is not defined in the Subscriber Agreement, Subscribers are required to request revocation within 24 hours after detecting the loss or compromise of the Private Key.

4.9.5. Time Within Which Raytonne Trust Services Will Process the Revocation Request

Raytonne Trust Services SHALL process revocation requests in accordance with BR sections 4.9.1.1 and 4.9.5. Once a certificate has been revoked the revocation will be reflected in the OCSP responses issued within 1 hour, and in the CRLs within 24 hours.

4.9.6. Revocation Checking Requirement for Relying Parties

Parties relying on a digital Certificate must verify a digital signature at all times by checking the validity of a digital Certificate against the relevant CRL published by Raytonne Trust Services or using the Raytonne Trust Services OCSP responder. Note that CRL MAY lag behind OCSP creating a situation where a revoked certificate MAY show as Revoked on OCSP yet MAY NOT show as revoked in the most recent CRL available. Therefore, it is recommended to obtain revocation information from Raytonne Trust Services' OCSP responder

whenever possible. Relying parties are alerted that an unverified digital signature cannot be assigned as a valid signature of the Subscriber.

Relying on an unverifiable digital signature may result in risks that the Relying Party, and not Raytonne Trust Services, assume in whole.

By means of this CPS, Raytonne Trust Services has adequately informed relying parties on the usage and validation of digital signatures through this CPS and other documentation published in the Repository or by contacting via out of bands means via the contact address as specified in the Document Control section of this CPS.

4.9.7. CRL Issuance Frequency

Raytonne Trust Services publishes CRLs to allow relying parties to verify a digital signature made using a Raytonne Trust Services issued digital Certificate. Each CRL contains entries for all revoked un-expired Certificates issued and is valid for 24 hours. Raytonne Trust Services issues a new CRL every 24 hours and includes a monotonically increasing sequence number for each CRL issued. Under special circumstances, Raytonne Trust Services may publish new CRLs prior to the expiry of the current CRL. All expired CRLs are archived (as described in section 3.4 of this CPS) for a period of 7 years or longer if applicable.

4.9.8. Maximum Latency for CRLs

The maximum latency for CRLs means the maximum time between the generation of CRLs and posting of the CRLs to the repository (i.e., the maximum amount of processing and communication-related delays in posting CRLs to the repository after the CRLs are generated). Raytonne Trust Services does not employ a maximum latency for CRLs. Generally, however, CRLs are published within 1 hour.

4.9.9. On-Line Revocation/Status Checking Availability

In addition, Raytonne Trust Services' systems are configured to generate and serve OCSP responses. This provides real-time information regarding the validity of the Certificate making the revocation information immediately available through the OCSP protocol. CRLs and OSCP are available 24/7 to anyone.

4.9.10. On-Line Revocation Checking Requirements

OCSP responders operated by Raytonne Trust Services SHALL support the HTTP GET method, as described in RFC 6960 and/or RFC 5019.

Raytonne Trust Services' OCSP responses are either:

- Signed by the CA that issued the Certificates whose revocation status is being checked, OR;
- The OCSP response is signed by a separate OCSP Responder Certificate which is signed by the CA that issued the Certificate whose revocation status is being checked. In this case the signing certificate will contain an extension of type id-pkix-ocsp-nocheck, as defined by RFC6960.

All Raytonne Trust Services' OCSP responses are updated at least every 3.5 days and:

1. have a validity interval greater than or equal to eight hours;
2. have a validity interval less than or equal to ten days;

3. with validity intervals less than sixteen hours, Raytonne Trust Services SHALL update the information provided via an Online Certificate Status Protocol prior to one-half of the validity period before the nextUpdate.
4. with validity intervals greater than or equal to sixteen hours, Raytonne Trust Services SHALL update the information provided via an Online Certificate Status Protocol at least eight hours prior to the nextUpdate, and no later than four days after the thisUpdate.

Subordinate CA Certificates' revocation information is not served via OCSP.

Raytonne Trust Services' OCSP responder does not respond with a "good" status when receives a request for the status of a certificate serial number that is "unused".

Raytonne Trust Services monitors the OCSP responder for all requests as part of its security procedures.

Relying parties must perform online revocation/status checks in accordance with section 4.9.6 of this CPS prior to relying on the Certificate.

4.9.11. Other Forms of Revocation Advertisements Available

No stipulation.

4.10. Certificate Status Services

CRL and OCSP are Certificate status checking services available to relying parties.

4.10.1. Operational Characteristics

Lightweight OCSP conforms to RFC 5019. Raytonne Trust Services provides revocation information for Certificates through 1 day after the expiry date of the Certificate.

4.10.2. Service Availability

Certificate status services are available 24/7.

4.10.3. Optional Features

No stipulation.

4.11. End of Subscription

A Subscriber's subscription service ends if

- Raytonne Trust Services ceases operation,
- All of Subscriber's Certificates issued by Raytonne Trust Services are revoked without the renewal or rekey of the Certificates, or
- The Subscriber's Subscriber Agreement terminates or expires without renewal.

4.12. Key Escrow and Recovery

Except where Raytonne Trust Services is also the hosting provider, Raytonne Trust Services does not create or store the Subscriber's private key for publicly trusted TLS Server Certificates. In general, Raytonne Trust Services does not provide key escrow or key backup services. In general, Raytonne Trust Services expects an Applicant to generate key-pairs in its own environment and to pass only the Public Key to Raytonne Trust Services for inclusion in the Certificates issued.

4.12.1. Key Escrow and Recovery Policy and Practices

No Stipulation.

4.12.2. Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

This section of the CPS outlines the security policy, physical access control mechanisms, service levels and personnel policy in use to provide trustworthy and reliable CA operations.

Raytonne Trust Services asserts that it makes every reasonable effort to detect and prevent material breaches, loss, damage or compromise of assets, and interruption to business activities.

5.1. Physical Controls

All sites operate under a security policy designed to provide reasonable assurance of the detection, deterrence and prevention of unauthorized logical or physical access to CA related facilities.

5.1.1. Site Location and Construction

Raytonne Trust Services operates within China and the United States, with separate operations, research & development and server operation sites. Physical barriers are used to segregate secure areas within buildings and are constructed so as to extend from real floor to real ceiling to prevent unauthorized entry. External walls of the site are of solid construction.

5.1.2. Physical Access

Card access systems are in place to control and monitor access to all areas of the facility. Access to the Raytonne Trust Services physical machinery within the secure facility is protected with locked cabinets and logical access controls. Security perimeters are clearly defined for all Raytonne Trust Services locations. All of Raytonne Trust Services' entrances and exits are secured or monitored by security personnel, reception staff, or monitoring/control systems.

5.1.3. Power and Air Conditioning

Raytonne Trust Services secure facilities have a primary and secondary power supply and ensure continuous, uninterrupted access to electric power. Heating/air ventilation systems are used to prevent overheating and to maintain a suitable humidity level.

5.1.4. Water Exposures

Raytonne Trust Services has made reasonable efforts to ensure its secure facilities are protected from flood and water damage. Raytonne Trust Services has personnel located on-site to reduce the extent of damage from a flood and any subsequent water exposure.

5.1.5. Fire Prevention and Protection

Raytonne Trust Services has made reasonable efforts to ensure its secure facilities are protected from fire and smoke damage (fire protection is made in compliance with local fire regulations). IT equipment is located to reduce the risk of damage or loss by fire. The level of protection from fire reflects the importance of the equipment.

5.1.6. Media Storage

Amongst other ways, Raytonne Trust Services protects media by storing it away from known or obvious fire/water hazards. Media is also backed up on-site and off-site.

5.1.7. Waste Disposal

Raytonne Trust Services disposes of waste in accordance with industry best practice. Raytonne Trust Services has procedures in place to dispose of all media types, including, but not limited to, paper documents, hardware, damaged devices, and read only optical devices. These procedures apply to all information classification levels, with the method of disposal dependent on the classification.

5.1.8. Off-Site Backup

Raytonne Trust Services backs up much of its information to a secure, off-site location that is sufficiently distant to escape damage from a disaster at the primary location. The frequency, retention, and extent of the backup is determined by the infrastructure team, taking into account the criticality and security requirements of the information. Backup of critical CA software is performed weekly and is stored offsite. Backup of critical business information is performed daily and is stored offsite. Access to backup servers/media is restricted to authorized personnel only. Backup media is regularly tested through restoration to ensure it can be relied on in the event of a disaster. Backup servers/media is appropriately labeled according to the confidentiality of the information.

5.2. Procedural Controls

5.2.1. Trusted Roles

Trusted roles are assigned by senior members of the management team who decide permissions with signed authorizations being archived.

The list of personnel appointed to trusted roles is maintained and reviewed annually.

The functions and duties performed by persons in trusted roles are distributed so that a lone person cannot subvert the security and trustworthiness of PKI operations. All personnel in trusted roles must be free from conflicts of interest that might prejudice the impartiality of Raytonne PKI operations.

Persons acting in trusted roles are only allowed to access a Certificate Management System (CMS) after they are authenticated using a method approved as being suitable for the control of PIV-I Hardware.

5.2.1.1. CA Administrators

The CA Administrator installs and configures the CA software, including key generation, and key backup (as part of key generation) and subsequent recovery.

CA Administrators do not issue certificates to Subscribers.

5.2.1.2. CA Officers (e.g., CMS, RA, Validation and Vetting Personnel)

The CA Officer role is responsible for issuing and revoking certificates, the verification of identity, and compliance with the required issuance steps including those defined in this CPS and recording the details of approval and issuance steps taken identity vetting tasks are completed.

CA Officers must identify and authenticate themselves to systems before access is granted. Identification is via a username, with authentication requiring a password and digital Certificate.

5.2.1.3. Operator (e.g. System Administrators/ System Engineers)

Operators install and configure system hardware, including servers, routers, firewalls, and networks. The Operator also keeps CA, CMS and RA systems updated with software patches and other maintenance needed for system stability, security, and recoverability.

5.2.1.4. Internal Auditors

Internal Auditors are responsible for reviewing, maintaining, and archiving audit logs and performing or overseeing internal compliance audits to determine if Raytonne Trust Services, an external CA, or RA is operating in accordance with this CPS and, where relevant, an RA's contract.

5.2.2. Number of Persons Required per Task

Raytonne Trust Services requires that at least two CA Administrators take action to activate Raytonne Trust Services' CA Private Keys for signing, to generate new CA key-pairs, or to restore Private Keys.

No single person has the capability to issue a PIV-I credential, or to issue an EV TLS or EV Code signing certificate.

5.2.3. Identification and Authentication for Each Role

All personnel are required to authenticate themselves to CA and RA systems before they may perform the duties of their role involving those systems.

5.2.4. Roles Requiring Separation of Duties

No Trusted Roles can assume any other role, except Operator.

5.3. Personnel Controls

Access to the secure parts of Raytonne Trust Services' facilities is limited using physical and logical access controls and is only accessible to appropriately authorized individuals filling trusted roles for which they are properly qualified and to which they have been appointed by management.

Raytonne Trust Services requires that all personnel filling trusted roles are properly trained and have suitable experience before being permitted to adopt those roles.

5.3.1. Qualifications, Experience, and Clearance Requirements

Consistent with this CPS, Raytonne Trust Services follows personnel and management practices that provide reasonable assurance of the trustworthiness and competence of their employees and of the satisfactory performance of their duties.

The Operator Role is only granted on Raytonne Trust Services IT systems when there is a specific business need. New Operators are not given full administrator rights until they have demonstrated a detailed knowledge of Raytonne Trust Services IT systems & policies and that they have reached a suitable skill level satisfactory to the Server Systems Manager/Administrator or CEO. New administrators are closely monitored by the Server Systems Manager/Administrator for the first three months. Where systems allow, administrator access authentication is via a public/Private Key specifically issued for this purpose. This provides accountability of individual administrators and permits their activities to be monitored. The CA Officer Role is granted certificate issuance privileges only after sufficient training in Raytonne Trust Services' validation and verification policies and procedures. This training period MUST be at least six months before issuance privileges will be granted for EV certificates.

5.3.2. Background Check Procedures

All trusted personnel have background checks before access is granted to Raytonne Trust Services' systems. These checks may include, but are not limited to, verification of the individual's identity using a government issued photo ID, credit history, employment history, education, character references, social security number, criminal background, and a Companies House cross-reference to disqualified directors.

5.3.3. Training Requirements

Raytonne Trust Services provides suitable training to all staff before they take on a Trusted Role should they not already have the complete skill-set required for that role. Training of personnel is undertaken via a mentoring process involving senior members of the team to which they are attached. CA Administrators are trained in the operation and installation of the CA software. Operators are trained in the maintenance, configuration, and use of the specific software, operating systems, and hardware systems used by Raytonne Trust Services.

Internal Auditors are trained to proficiency in the general principles of systems and process audit as well as familiarity with Raytonne Trust Services' policies and procedures. CA Officers are trained in Raytonne Trust Services' validation and verification policies and procedures.

5.3.4. Retraining Frequency and Requirements

Personnel in Trusted Roles have additional training when changes in industry standards or changes in Raytonne Trust Services' operations require it. Raytonne Trust Services provides refresher training and informational updates sufficient to ensure that Trusted Personnel retain the requisite degree of expertise.

5.3.5. Job Rotation Frequency and Sequence

No stipulation.

5.3.6. Sanctions for Unauthorized Actions

Any personnel who, knowingly or negligently, violate Raytonne Trust Services' security policies, exceed the use of their authority, use their authority outside the scope of their employment, or allow personnel under their supervision to do so may be liable to disciplinary action up to and including termination of employment. Should the unauthorized actions of any person reveal a failure or deficiency of training, sufficient training or retraining will be employed to rectify the shortcoming.

5.3.7. Independent Contractor Requirements

Once the independent contractor completes the work for which it was hired, or the independent contractor's employment is terminated, all access rights assigned to that contractor are removed as soon as possible and within 24 hours from the time of termination.

5.3.8. Documentation Supplied to Personnel

The selection of documentation supplied to Raytonne Trust Services personnel is based on the role(s) they are to fill. Such documentation may include a copy of this CPS, the CA/B Forum Baseline Requirements, EV Guidelines, and other technical and operational documentation necessary to maintain Raytonne Trust Services' CA operations.

5.4. Audit Logging Procedures

For audit purposes, Raytonne Trust Services maintains electronic or manual logs of the following events for core functions.

5.4.1. Types of Events Recorded

An audit log is maintained of each movement of the removable media.

CA & Certificate Lifecycle Management Events:

- CA Root signing key functions, including key generation, backup, recovery and destruction
- Subscriber Certificate lifecycle management, including successful and unsuccessful Certificate applications, Certificate issuances, Certificate re-issuances and Certificate renewals
- Subscriber Certificate revocation requests, including revocation reason
- Subscriber changes of affiliation that would invalidate the validity of an existing Certificate
- CRL updates, generations and issuances
- Custody of keys and of devices and media holding keys
- Compromise of a Private Key

Security Related Events:

- System downtime, software crashes and hardware failures
- CA system actions performed by Raytonne Trust Services personnel, including software updates, hardware replacements and upgrades
- Cryptographic hardware security module events, such as usage, de-installation, service or repair and retirement
- Successful and unsuccessful Raytonne PKI access attempts

- Secure CA facility visitor entry and exit

Certificate Application Information:

- The documentation and other related information presented by the Applicant as part of the application validation process
- Storage locations, whether physical or electronic, of presented documents

All logs include the following elements:

- Date and time of entry
- Serial or sequence number of entry
- Method of entry
- Source of entry
- Identity of entity making log entry
- Description of the entry

5.4.2. Frequency of Processing Log

Logs are archived by the system administrator on a weekly basis and event journals reviewed on a weekly basis by CA management.

5.4.3. Retention Period for Audit Log

Audit logs SHALL be retained for a minimum of two (2) years. When the removable media reaches the end of its life it is wiped by a third-party secure data destruction facility and the Certificates of destruction are archived.

5.4.4. Protection of Audit Log

These media are only removed by Raytonne Trust Services staff on a visit to the data center, and when not in the data center are held either in a safe in a locked office within the development site, or off-site in a secure storage facility.

Both current and archived logs are maintained in a form that prevents unauthorized modification, substitution or destruction.

5.4.5. Audit Log Backup Procedures

All logs are backed up on separate local servers/HDDs and transferred off-site over encrypted VPN to remote servers/HDDs.

5.4.6. Audit Collection System (Internal vs. External)

Automatic audit collection processes run from system startup to system shutdown. The failure of an automated audit system which may adversely affect the integrity of the system or the confidentiality of the information protected by the system will lead to Raytonne Trust Services' Operators and/or CA Administrators evaluating whether a suspension of operations is required until the problem is remedied.

5.4.7. Notification to Event-Causing Subject

No stipulation.

5.4.8. Vulnerability Assessments

A vulnerability is a weakness in the organization or in an information system that might be exploited by a threat, with the possibility of causing harm to assets. In order to mitigate the risk or possibility of causing harm to assets, Raytonne Trust Services performs regular vulnerability assessment by taking a two-pronged approach. Raytonne Trust Services assesses vulnerabilities by (1) making an assessment of the threats to, impacts on, and the vulnerabilities of assets and the likelihood of their occurrence, and (2) by developing a process of selecting and implementing security controls in order to reduce the risks identified in the risk assessment to an acceptable level. Raytonne Trust Services routinely performs vulnerability assessments by identifying the vulnerability categories that face an asset. Some of the vulnerability categories that Raytonne Trust Services evaluates are technical, logical, human, physical, environmental, and operational.

Vulnerability scans are run by trusted staff on a weekly schedule. Additional scans are run following system updates, changes, or when deemed necessary.

Raytonne Trust Services employs external parties to perform regular annual vulnerability scans & penetration testing on our CA systems/infrastructure.

5.5. Records Archival

Raytonne Trust Services implements a backup standard for all business-critical systems located at its data centers. Raytonne Trust Services retains records in electronic or in paper-based format in conformance with this subsection of this CPS.

5.5.1. Types of Records Archived

Raytonne Trust Services backs up both application and system data. Raytonne Trust Services may archive the following information:

- Audit data, as specified in section 5.4 of this CPS;
- Certificate application information;
- Documentation supporting a Certificate application;
- Certificate lifecycle information.

5.5.2. Retention Period for Archive

The retention period for archived information depends on the type of information, the information’s level of confidentiality, and the type of system the information is stored on.

Raytonne Trust Services retains all documentation relating to certificate requests and the verification thereof, and all Certificates and revocation thereof for a term of not less than 7 years after any Certificate based on that documentation ceases to be valid, or as necessary to comply with applicable laws. The retention term begins on the date of expiration or revocation. Copies of Certificates are held, regardless of their status (such as expired or revoked). Such records may be retained in electronic, in paper-based format or any other format that Raytonne Trust Services may see fit.

5.5.3. Protection of Archive

Records are archived at a secure off-site location and are maintained in a form that prevents unauthorized modification, substitution or destruction. Access to backup servers and/or backup media, whether Windows or Linux, backup utilities, or backup data, is restricted to authorized personnel only and adheres to a strict default deny policy.

5.5.4. Archive Backup Procedures

Administrators at each Raytonne Trust Services location are responsible for carrying out and maintaining backup activities. Raytonne Trust Services employs both scheduled and unscheduled backups. Scheduled backups are automated using approved backup tools. Scheduled backups are monitored using automated tools. Unscheduled backups occur before carrying out major changes to critical systems and are part of any change request that has a possible impact on data integrity or security. All backup media is labeled according to the information classification, which is based on the backup information stored on the media.

5.5.5. Requirements for Time-Stamping of Records

Records that are time-stamped include, but are not limited to, the following:

- Visitor entry,
- Visitor exit,
- Emails within Raytonne Trust Services,
- Emails sent between Raytonne Trust Services and third parties,
- Subscriber Agreements,
- Certificate issuance, and
- Certificate revocation.

5.5.6. Archive Collection System (Internal or External)

Raytonne Trust Services' archive collection system is both internal and external. As part of its internal collection procedures, Raytonne Trust Services may require Subscribers to submit appropriate documentation in support of a Certificate application.

As part of Raytonne Trust Services' external collection procedures, RAs may require documentation from Subscribers to support Certificate applications, in their role as a Raytonne Trust Services RA. In such circumstances, RAs are obliged to retain such records in line with the practices of record retention and protection as used by Raytonne Trust Services and as stated in this CPS.

5.5.7. Procedures to Obtain and Verify Archive Information

Raytonne Trust Services RAs are required to submit appropriate documentation and prior to being validated and successfully accepted as an approved Raytonne Trust Services RA.

5.6. Key Changeover

Towards the end of each root or intermediate CA's lifetime, a new CA signing key pair is commissioned and all subsequently issued Certificates and CRLs are signed with the new private signing key. Both keys may be

concurrently active. The corresponding new CA Certificate is provided to Subscribers and relying parties through the delivery methods detailed below.

Raytonne Trust Services makes all its CA Root Certificates available in the Repository.

Raytonne Trust Services provides the full Certificate chain to the Subscriber upon issuance and delivery of the Subscriber Certificate.

5.7. Compromise and Disaster Recovery

Organizations are regularly faced with events that may disrupt their normal business activities or may lead to loss of information and assets. These events may be the result of natural disasters, accidents, equipment failures, or deliberate actions. This section details the procedures Raytonne Trust Services employs in the event of a compromise or disaster.

5.7.1. Incident and Compromise Handling Procedures

All incidents (including compromises), both suspected and actual, are reported to the appropriate authority for investigation. Depending on the nature and immediacy of the incident, the reporter of an incident is to document the incident details to help with incident assessment, investigation, solution, and future operational changes. Once the incident is reported, the appropriate authority makes an initial assessment. Next, a containment strategy is chosen and implemented. After an incident has been contained, eradication is necessary to eliminate components of the incident. During eradication, importance is given to identifying all affected areas so they can be remedied.

These procedures are in place to ensure that:

- a consistent response to incidents happening to Raytonne Trust Services' assets,
- incidents are detected, reported, and logged, and
- clear roles and responsibilities are defined.

To maintain the integrity of its services Raytonne Trust Services implements, documents, and periodically tests appropriate contingency and disaster recovery plans and procedures. These procedures define and contain a formal incident management reporting process, incident response, and incident escalation procedures to ensure professional incident management and the return to normal operations within a timely manner. The process also enables incidents to be analyzed in a way as to identify possible causes such that any weaknesses in Raytonne Trust Services' processes may be improved in order to prevent reoccurrence. Such plans are revised and updated as may be required at least once a year.

5.7.2. Computing Resources, Software, And/or Data Are Corrupted

If Raytonne Trust Services determines that its computing resources, software, or data operations have been compromised, Raytonne Trust Services will investigate the extent of the compromise and the risk presented to affected parties. Depending on the extent of the compromise, Raytonne Trust Services reserves the right to revoke affected Certificates, to revoke entity keys, to provide new Public Keys to users, and to recertify subjects.

5.7.3. Entity Private Key Compromise Procedures

Due to the nature of the CA Private Keys, these are classified as highly critical to Raytonne Trust Services' business operations and continuity. If any of the CA's private signing keys were compromised or were suspected of having been compromised, Raytonne Trust Services would make an assessment to determine the nature and extent of the compromise. In the most severe circumstances, Raytonne Trust Services would revoke all Certificates ever issued by the use of those keys, notify all owners of Certificates (by email) of that revocation, and offer to reissue the Certificates to the customers with an alternative or new private signing key.

5.7.4. Business Continuity Capabilities after a Disaster

Raytonne Trust Services operates a fully redundant CA system. In the event of a short- or long- term loss of an office location, operations at other offices will be increased. The backup CA is readily available in the event that the primary CA should cease operation. All of Raytonne Trust Services' critical computer equipment is housed in a colocation facility run by a commercial data-center, and all of the critical computer equipment is duplicated within the facility. Incoming power and connectivity feeds are duplicated. The duplicate equipment is ready to take over the role of providing the implementation of the CA, and allows Raytonne Trust Services to specify a maximum system outage time (in case of critical systems failure) of 1 hour. Raytonne Trust Services operations are distributed across several sites worldwide. All sites offer facilities to manage the lifecycle of a Certificate, including but not limited to the application, issuance, revocation and renewal of such Certificates. As well as a fully redundant CA system, Raytonne Trust Services maintains provisions for the activation of a backup CA and a secondary site should the primary site suffer a total loss of systems. This disaster recovery plan states that Raytonne Trust Services will endeavor to minimize interruptions to its CA operations.

5.8. CA or RA Termination

In case of termination of CA operations for any reason whatsoever, Raytonne Trust Services will provide timely notice and transfer of responsibilities to succeeding entities, maintenance of records, and remedies. Before terminating its own CA activities, Raytonne Trust Services will take the following steps, where possible:

- Providing Subscribers of valid Certificates, Relying Parties, and other affected parties with ninety (90) days' notice of its intention to cease acting as a CA.
- Revoking all Certificates that are still un-revoked or un-expired at the end of the ninety (90) day notice period without seeking Subscriber's consent.
- Giving timely notice of revocation to each affected Subscriber.
- Making reasonable arrangements to preserve its records according to this CPS.
- Reserving its right to provide succession arrangements for the re-issuance of Certificates by a successor CA that has all relevant permissions to do so and complies with all necessary rules, while its operation is at least as secure as Raytonne Trust Services'.

The requirements of this article may be varied by contract, to the extent that such modifications affect only the contracting parties.

6. TECHNICAL SECURITY CONTROLS

This section addresses certain technological aspects of the Raytonne Trust Services infrastructure and PKI services.

Raytonne Trust Services is not involved in functions associated with the generation, issuance, decommissioning or destruction of a Subscriber key pair.

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

6.1.1.1. Subscriber Key Pairs

In general, unless otherwise noted in this CPS, Subscriber is solely responsible for the generation of an asymmetric cryptographic key pair (RSA or ECDSA) appropriate to the Certificate type being applied for. During application, the Subscriber will generally be required to submit a Public Key and other personal/corporate details in the form of a Certificate Signing Request (CSR) or SPKAC.

Server Certificate requests are usually generated using the key generation facilities available in the Subscriber's webserver software.

Raytonne Trust Services SHALL reject a certificate request if one or more of the following conditions are met:

1. The Key Pair does not meet the requirements set forth in Section 6.1.5 and/or Section 6.1.6;
2. There is clear evidence that the specific method used to generate the Private Key was flawed;
3. Raytonne Trust Services is aware of a demonstrated or proven method that exposes the Applicant's Private Key to compromise;
4. Raytonne Trust Services has previously been made aware that the Applicant's Private Key has suffered a Key Compromise, such as through the provisions of Section 4.9.1;
5. Raytonne Trust Services is aware of a demonstrated or proven method to easily compute the Applicant's Private Key based on the Public Key (such as a Debian weak key, see https://wiki.debian.org/SSLkeys).

If the Subscriber Certificate will contain an extKeyUsage extension containing either the values id-kpserverAuth [RFC5280] or anyExtendedKeyUsage [RFC5280], Raytonne Trust Services SHALL NOT generate a Key Pair on behalf of a Subscriber.

6.1.1.2. CA and Intermediate CA Key Pairs

For Root CA Key Pairs created under this CPS Raytonne Trust Services:

- prepares and follows a Key Generation Script,
- has a Qualified Auditor witness the Root CA Key Pair generation process or records a video of the entire Root CA Key Pair generation process, and
- has a Qualified Auditor issue a report opining that the CA followed its key ceremony during its Key and Certificate generation process and the controls used to ensure the integrity and confidentiality of the Key Pair.

For other CA Key Pairs created for Raytonne Trust Services or an Affiliate, Raytonne Trust Services:

- prepares and follows a Key Generation Script and
- has a Qualified Auditor witness the Root CA Key Pair generation process or records a video of the entire Root CA Key Pair generation process.

Raytonne Trust Services' CA keys are generated in Hardware Security Modules (HSM)s that SHALL be compliant, as a minimum, to FIPS 140-2 level 3. CA keys are never available outside the HSM or key ceremonies in plain text form. All CA key operations are performed within the security of the HSM, whether this be the initial key generation or their end use in the live production environment. All keys that are exported from the HSM are encrypted with a suitable encryption algorithm with the encryption key generated by the HSM.

Access to CA keys is restricted to authorized, trusted personnel of Raytonne Trust Services. CA key data must be stored securely at all times unless attended by authorised personnel of Raytonne Trust Services.

CA key generation that involves an HSM is performed in a 'CA key ceremony'. All CA key ceremonies are performed in a secure, controlled area. During the ceremony, at least two authorised Raytonne Trust Services personnel are present at all times. It may be required that authorised auditors be present to witness the CA key ceremonies. No other persons are allowed in the secure area during the key ceremonies to protect against information loss through tampering or overseeing. All visible 'Sensitive' information is kept to a minimum at all times during the CA key ceremonies.

All CA key ceremonies are performed on a computer with a verified clean installation of the operating system that is isolated from all computer networks. The Cryptographic operation control software shall be a fresh install and verified to be operating correctly before use.

All media created from a CA key ceremony that contains CA key backup data must be classified and stored in accordance with this classification.

All obsolete media from a CA Key ceremony must be disposed of in a secure manner i.e., destruction, at the end of the CA key ceremony, or within a maximum period of 1 working day. All media that is not fully disposed of immediately, must be partially destroyed and securely stored until full disposal takes place.

6.1.2. Private Key Delivery to Subscriber

Except where Raytonne Trust Services is also the hosting provider, Raytonne Trust Services does not generate keys for SSL/TLS end entity server certificates. Where Raytonne Trust Services is the hosting provider the keys are generated and the private key remains only on the hosting server.

6.1.3. Public Key Delivery to Certificate Issuer

Server Certificate requests are generated using the Subscriber's webserver software and the request is submitted to Raytonne Trust Services in the form of a PKCS #10 Certificate Signing Request (CSR). Submission is made electronically via the Raytonne Trust Services website or through a Raytonne Trust Services approved RA.

Secure Email Certificate requests are generated using the Subscriber's cryptographic service provider software present in the Subscriber's browser and submitted to Raytonne Trust Services in the form of a PKCS#10 Certificate Signing Request (CSR). The Subscriber's browser generally makes submission automatically.

6.1.4. CA Public Key Delivery to Relying Parties

Raytonne Trust Services' Public Keys are provided to Relying Parties in a few ways. One way is through the Repository. Additionally, Public Keys of Raytonne Trust Services' Root CAs are embedded in browsers.

6.1.5. Key Sizes

Root Certificates' key sizes:

Common Name	Key Size
瑞亟—宛（Staging）	ECC 384

Root certificates and any certificates which chain up to them have:

- RSA keys whose modulus size in bits is divisible by 8, and is at least 2048; or
- ECDSA keys on the P-256 or P-384 curves.

6.1.6. Public Key Parameters Generation and Quality Checking

Raytonne Trust Services generates the Public Key parameters. Raytonne Trust Services' CA keys SHOULD be generated within a FIPS 140-2 Level 3 certified HSM.

RSA: Raytonne Trust Services confirms that the value of the public exponent is an odd number equal to 3 or more. Additionally, the public exponent SHOULD be in the range between 2^{16}+1 and 2^{256}-1. The modulus SHOULD also have the following characteristics: an odd number, not the power of a prime, and have no factors smaller than 752. [Source: Section 5.3.3, NIST SP 800-89]

ECC: Raytonne Trust Services confirms the validity of all keys using either the ECC Full Public Key Validation Routine or the ECC Partial Public Key Validation Routine. [Source: Sections5.6.2.3.2 and 5.6.2.3.3, respectively, of NIST SP 800-56A: Revision 2]

6.1.7. Key Usage Purposes (As per X.509v3 Key Usage Field)

Raytonne Trust Services Certificates are general purpose and may be used without restriction on geographical area or industry. In order to use and rely on a Raytonne Trust Services Certificate the Relying Party must use X.509v3 compliant software. Raytonne Trust Services Certificates include key usage extension fields to specify the purposes for which the Certificate may be used and to technically limit the functionality of the Certificate when used with X.509v3 compliant software. Reliance on key usage extension fields is dependent on correct software implementations of the X.509v3 standard and is outside of the control of Raytonne Trust Services.

The possible key purposes identified by the X.509v3 standard are the following:

1. Digital signature, for verifying digital signatures that is, for entity authentication and data origin authentication with integrity
2. Non-repudiation, for verifying digital signatures used in providing a nonrepudiation service which protects against the signing entity falsely denying some action
3. Key encipherment, for enciphering keys or other security information, e.g., for key transport

4. Data encipherment, for enciphering user data, but not keys or other security information
5. Key agreement, for use as a Public Key agreement key
6. Key Certificate signing, for verifying a CA's signature on Certificates, used in CA Certificates only
7. CRL signing, for verifying a CA's signature on CRLs
8. Encipher only, Public Key agreement key for use only in enciphering data when used with key agreement
9. Decipher only, Public Key agreement key for use only in deciphering data when used with key agreement

The appearance of a key usage in this section of the CPS does not indicate that Raytonne Trust Services does or will issue a certificate with that key usage.

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

10. Self-signed Certificates to represent the Root CA itself;
11. Certificates for Subordinate CAs and Cross Certificates;
12. Certificates for infrastructure purposes (administrative role certificates, internal CA operational device certificates); and
13. Certificates for OCSP Response verification.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

The Raytonne Trust Services Infrastructure uses trustworthy systems to provide Certificate services. A trustworthy system is computer hardware, software and procedures that provide an acceptable resilience against security risks, provide a reasonable level of availability, reliability and correct operation, and enforce a security policy.

Raytonne Trust Services strongly urges Subscribers to use a password or equivalent authentication method to prevent unauthorized access and usage of the Subscriber Private Key.

6.2.1. Cryptographic Module Standards and Controls

Raytonne Trust Services securely generates and protects its own Private Key(s), using a trustworthy system and takes necessary precautions to prevent the compromise or unauthorized usage of it. Such system SHOULD be certified to FIPS 140-2 Level 3 or higher.

The Raytonne Trust Services Root keys were generated in accordance with the guidelines detailed in the Root Key Generation Ceremony document. The activities undergone and the personnel involved in the Root Key Generation Ceremony are recorded for audit purposes. Subsequent Root Key Generation Ceremonies are to follow the documented reference guide also.

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

The decryption key is split across **m** removable media and requires **n** of **m** to reconstruct the decryption key. Custodians in the form of two or more authorized Raytonne Trust Services officers are required to physically retrieve the removable media from the distributed physically secure locations.

Except during key pair generation, export, and import, access to the cryptographic operation software on the HSM is controlled through the use of Smart Cards (or cryptographic tokens of other forms) and their associated PINs which must be entered/presented before any key operations may be performed. Access to the Smart Cards & PINs is restricted to authorized Raytonne Trust Services Officers. The HSMs are configured to require N from M cards to be present. A list is maintained of authorized Raytonne Trust Services personnel with access to Smart Cards & PINs.

6.2.3. Private Key Escrow

Raytonne Trust Services does not escrow Subscriber Private Keys.

6.2.4. Private Key Backup

Except in cases where Raytonne Trust Services or its affiliates host the server, the Subscriber is solely responsible for protection of their Private Keys.

6.2.5. Private Key Archival

When any CA Root Signing Key pair expires, they will be archived for at least 7 years. The keys will be archived in a secure cryptographic hardware module, as per their secure storage prior to expiration, as detailed in section 6.3.2 of this CPS.

6.2.6. Private Key Transfer into or from a Cryptographic Module

Where CA Root signing keys are backed up to another cryptographic hardware security module, such keys are transferred between devices in encrypted format only.

6.2.7. Private Key Storage on Cryptographic Module

Private Keys are generated and stored inside Raytonne Trust Services' Hardware Security Modules (HSMs). HSMs SHALL be certified to at least FIPS 140-2 Level 3.

For CA Root key recovery purposes, the Root CA signing keys are encrypted and stored within a secure environment.

6.2.8. Method of Activating Private Key

Depending on the circumstances and the type of Certificate, a Private Key can be activated by Raytonne Trust Services, Subscriber, or other authorized personnel. Raytonne Trust Services' Private Keys are activated in accordance with the specifications of the cryptographic module. Subscriber must make all reasonable efforts to protect the integrity and confidentiality of its Private Key(s). Private Keys remain active until deactivated.

6.2.9. Method of Deactivating Private Key

Depending on the circumstances and the type of Certificate, a Private Key can be deactivated by Raytonne Trust Services, Subscriber, or other authorized personnel.

6.2.10. Method of Destroying Private Key

Destroying a Private Key means the destruction of all active keys, both backed-up and stored. Destroying a Private Key may comprise of removing it from the HSM or removing it from the active backup set. Private Keys are destroyed in accordance with NIST SP 800-88.

6.2.11. Cryptographic Module Rating

See section 6.2.1 of this CPS.

6.3. Other Aspects of Key Pair Management

This section considers other areas of key management. Particular subsections may be applicable to issuing CAs, repositories, subject CAs, RAs, Subscribers, and other participants.

6.3.1. Public Key Archival

When Public Keys are archived, they are archived according to procedures outlined in section 5.5 of this CPS.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

Certificates are valid upon issuance by Raytonne Trust Services and acceptance by the Subscriber. Generally, the Certificate validity period will be from 1 to 10 years, however, Raytonne Trust Services reserves the right to offer validity periods outside of this standard validity period. The maximum duration of a SSL/TLS end entity server certificate is 398 days and Raytonne Trust Services verifies all information that is included in SSL/TLS Certificates (in the subjectDN) at time intervals of 825 days or less (for EV SSL certificates, this validation does not exceed 398 days), except the information of the domain name or IP address validation according to sections 3.2.2.1 which is also set to 398 days or less.

The expiration of Raytonne Trust Services' Root CA keys is set out in the table below. Subordinate CA key lifetimes are either the same or shorter than those of the CA by which they are signed.

Common Name	Valid To
瑞亟—宛（Staging）	2036-01-01T00:00:00Z

Raytonne Trust Services protects its CA Root key pairs in accordance with its WebTrust program compliant infrastructure and CPS.

6.4. Activation Data

Activation data refers to data values other than whole Private Keys that are required to operate Private Keys or cryptographic modules containing Private Keys. Examples of activation data include, but are not limited to, PINs, passphrases, and portions of Private Keys used in a key-splitting regime.

6.4.1. Activation Data Generation and Installation

Activation data is generated in accordance with the specifications of the HSM. This hardware SHALL be certified to FIPS 140-2.

6.4.2. Activation Data Protection

The procedures used to protect activation data is dependent on whether the data is for smartcards or passwords. Smartcards are held by highly trusted personnel. Passwords and smartcards are subject to Raytonne Trust Services' Cryptographic Policy.

6.4.3. Other Aspects of Activation Data

No stipulation.

6.5. Computer Security Controls

6.5.1. Specific Computer Security Technical Requirements

Raytonne Trust Services ensures the integrity of its computer systems by implementing controls, such as

- Applying the same security controls to all systems co-located in the same zone with a Certificate System;
- Maintaining Root CA Systems in a high security zone and in an offline state or air-gapped from other networks;
- Maintaining and protecting Issuing Systems, Certificate Management Systems, and Security Support systems;
- Configuring Issuing Systems, Certificate Management Systems, Security Support Systems, and Front End/Internal Support Systems by removing or disabling all accounts, applications, services, protocols, and ports that are not used in Raytonne Trust Services' operations and allowing only those that are approved by Raytonne Trust Services;
- Reviewing configurations of Issuing Systems, Certificate Management Systems, Security Support Systems, and Front-End/Internal-Support Systems on a weekly basis;
- Undergoing penetration tests on a periodic basis and after significant infrastructure or application upgrades;
- Granting administration access to Certificate Systems only to persons acting in trusted roles and requiring their accountability for the Certificate System's security; and
- Changing authentication keys and passwords for any privileged account or service account on a Certificate System whenever a person's authorization to administratively access that account on the Certificate System is changed or revoked.

6.5.2. Computer Security Rating

No stipulation.

6.6. Lifecycle Technical Controls

6.6.1. System Development Controls

Raytonne Trust Services has formal policies in place to control, document and monitor the development of its CA systems. Development requests may only be raised by a restricted set of personnel. Development tasks are prioritized by the 'task requesters' within their area and then further prioritized by the development manager whilst considering the development task list in its entirety. The majority of changes are developed in-house by Raytonne Trust Services. In the event that Raytonne Trust Services 'buys-in' services (hardware and/or software), vendors are selected based on reputation and ability to supply products 'fit for purpose'.

On receipt of each development request a unique task ID and title are assigned that stay with the task throughout the development lifecycle.

Each development task has an associated risk assessment carried out as a part of the development lifecycle. All tasks are viewed as carrying some form of risk, from issues relating to task scope and complexity to a lack of availability of resources. The management of risk is addressed through a formal risk management process with the request not being applied to the production environment until an acceptable level of risk is achieved.

The work-product of all development requests undergo peer review prior to release to the production environment to prevent malicious or erroneous software being loaded into the production environment.

Each task must be tested and signed off by the QA team before being deployed to the production environment. Developers are not permitted to be involved in the testing of their own work. When issues are found by QA the QA team provide feedback to the developer to resolve the issues before development may proceed to release.

Development and QA team members do not have any access to the production environment. Access to these areas is strictly controlled.

Once the change has gone live to the production environment the task requester along with the testing team are advised and the change re-tested.

6.6.2. Security Management Controls

Raytonne Trust Services has tools and procedures to ensure that Raytonne Trust Services' operational systems and applications retain their integrity and remain configured securely. These tools and procedures include checking the integrity of the application and security software.

6.6.3. Lifecycle Security Controls

No stipulation.

6.7. Network Security Controls

Raytonne Trust Services develops, implements, and maintains a comprehensive security program designed to protect its networks. In this security program, general protections for the network include:

- Segmenting Certificate Systems into networks or zones based on their functional, logical, and physical relationship;
- Applying the same security controls to all systems co-located in the same zone with a Certificate System;
- Maintaining Root CA Systems in a high security zone and in an offline state or air-gapped from other networks;
- Implementing and configuring Security Support Systems that protect systems and communications between systems inside secure zones and communications with non-Certificate Systems outside those zones;
- Configuring network boundary controls (firewalls, switches, routers, and gateways) with rules that support only the services, protocols, ports, and communications that Raytonne Trust Services has identified as necessary to its operations;
- For Certificate Systems, implementing detection and prevention controls to guard against viruses and malicious software; and

- Changing authentication keys and passwords for any privileged account or service account on a Certificate System whenever a person's authorization to administratively access that account on the Certificate System is changed or revoked.

6.8. Time-Stamping

No stipulation.

7. CERTIFICATE, CRL, AND OCSP PROFILES

Raytonne Trust Services uses version 3 of the X.509 standard to construct digital Certificates for use within the Raytonne PKI. X.509v3 allows a CA to add certain Certificate extensions to the basic Certificate structure. Raytonne Trust Services uses a number of Certificate extensions for the purposes intended by X.509v3 as per Amendment 1 to ISO/IEC 9594-8, 1995. X.509v3 is a standard of the International Telecommunications Union for digital Certificates.

7.1. Certificate Profile

Raytonne Trust Services incorporates by reference the following information in every digital Certificate it issues:

- Terms and conditions of the digital Certificate.
- Any other applicable Certificate policy as may be stated on an issued Raytonne Trust Services Certificate, including the location of this CPS.
- The mandatory elements of the standard X.509v3.
- Any non-mandatory but customized elements of the standard X.509v3.
- Content of extensions and enhanced naming that are not fully expressed within a Certificate.
- Any other information that is indicated to be so in a field of a Certificate.
- A Certificate profile contains fields as specified below:
  - key usage extension field (CPS section 6.1.7)
  - extension criticality field (CPS section 7.1.9)
  - basic constraints extension (CPS section 7.1.7)

Typical content of information published on a Raytonne Trust Services Certificate may include but is not limited to the following elements of information:

- Applicant’s name or organizational name.
- Code of Applicant’s country.
- Organizational unit name, street address, city, state.
- Issuing certification authority (Raytonne Trust Services).
- Applicant’s Public Key.
- Raytonne Trust Services digital signature.
- Signing algorithm.
- Validity period of the digital Certificate.
- Serial number of the digital Certificate.
- Applicant’s fully qualified domain name(s).

7.1.1. Version Number(s)

Certificate versions are all X.509 version 3

7.1.2. Certificate Extensions

Certificate extensions are in conformance to RFC 5280 and the Baseline Requirements.

Enhanced naming is the usage of an extended organization field in an X.509v3 Certificate. Information contained in the organizational unit field is also included in the Certificate Policy extension that Raytonne Trust Services may use.

7.1.2.1. Root CAs

Raytonne Trust Services Root CA certificates contain a basicConstraints extension marked critical. The cA field is set true. The pathLenConstraint is not present.

Raytonne Trust Services Root CA certificates contain a keyUsage extension marked critical. Bit positions for keyCertSign and cRLSign are set. The digitalSignature bit may also be set if this CA also signs OCSP responses.

Raytonne Trust Services Root CA certificates may contain a non-critical cRLDistributionPoints extension containing the HTTP URL of the CA's CRL service.

Raytonne Trust Services Root CA certificates do not contain a certificatePolicies extension.

7.1.2.2. Subordinate CAs

Raytonne Trust Services Subordinate CA certificates contain a certificatePolicies extension that includes one or more policyIdentifiers and usually contains a policyQualifier referring to the CPS URI but not including a userNotice.

Raytonne Trust Services Subordinate CA certificates contain a non-critical cRLDistributionPoints extension containing the HTTP URL of the Issuing CA's CRL service.

Raytonne Trust Services Subordinate CA certificates contain a non-critical authorityInformationAccess extension containing the HTTP URL of the Issuing CA's OCSP responder and also containing the HTTP URL of the Issuing CA's certificate.

Raytonne Trust Services Subordinate CA certificates contain a basicConstraints extension marked critical. The cA field is set true. The pathLenConstraint is often present and the pathLenConstraint is usually set to 0.

Raytonne Trust Services Subordinate CA certificates contain a keyUsage extension marked critical. Bit positions for keyCertSign and cRLSign are set. The digitalSignature bit is also set if this CA also signs OCSP responses.

7.1.2.3. Subscriber Certificates

Raytonne Trust Services Subscriber Certificates contain a certificatePolicies extension that includes one or more policyIdentifiers and usually contains a policyQualifier referring to the CPS URI but not including a userNotice.

Raytonne Trust Services Subscriber Certificates may contain a non-critical cRLDistributionPoints extension containing the HTTP URL of the Issuing CA's CRL service.

Raytonne Trust Services Subscriber Certificates contain a non-critical authorityInformationAccess extension containing the HTTP URL of the Issuing CA's OCSP responder and also containing the HTTP URL of the

Issuing CA's certificate. This extension MUST be present. It MUST NOT be marked critical, and it MUST contain the HTTP URL of the Issuing CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1). It SHOULD also contain the HTTP URL of the Issuing CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2).

Raytonne Trust Services Subscriber certificates contain a basicConstraints extension marked critical. The cA field is not set.

Raytonne Trust Services Subscriber certificates contain a keyUsage extension marked critical. Bit positions for keyCertSign and cRLSign are NOT set.

Raytonne Trust Services Subscriber certificates contain a non-critical extKeyUsage extension.

Server authentication certificates contain id-kp-serverAuth and id-kp-clientAuth. Other values are not typically present in server authentication certificates.

7.1.2.4. All Certificates

All other fields and extensions are in accordance with RFC5280.

Raytonne Trust Services does not issue certificates containing keyUsage or extendedKeyUsage values, or Certificate extensions, or other data not specified in sections 7.1.2.1, 7.1.2.2, or 7.1.2.3 above unless Raytonne Trust Services is aware of a reason for including the data in the Certificate.

Raytonne Trust Services does not issue certificates containing Extensions that do not apply in the context of the public Internet unless:

- such value falls within an OID arc for which the Applicant demonstrates ownership, or
- the Applicant can otherwise demonstrate the right to assert the data in a public context;

Raytonne Trust Services does not issue certificates containing semantics that, if included, will mislead a Relying Party about the certificate information verified by Raytonne Trust Services.

7.1.2.5. Application of RFC 5280

For purposes of clarification, a Precertificate, as described in RFC 6962—Certificate Transparency, shall not be considered to be a "certificate" subject to the requirements of RFC 5280—Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile under this CPS.

7.1.3. Algorithm Object Identifiers

Raytonne Trust Services Certificates are signed using algorithms with these identifiers:

From RFC3279:

(not used for SSL/TLS Server Certificates or OCSP Certificates)

```
sha-1WithRSAEncryption OBJECT IDENTIFIER  ::=  {
    iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)
    pkcs-1(1) 5  }
```

From RFC5754:

```
sha256WithRSAEncryption  OBJECT IDENTIFIER  ::=  { iso(1)
  member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 }

sha384WithRSAEncryption  OBJECT IDENTIFIER  ::=  { iso(1)
  member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12 }
```

From RFC5758:

```
ecdsa-with-SHA256 OBJECT IDENTIFIER ::= { iso(1) member-body(2)
     us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 2 }

ecdsa-with-SHA384 OBJECT IDENTIFIER ::= { iso(1) member-body(2)
     us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3 }
```

Raytonne Trust Services does not sign Certificates using RSA with PSS padding.

For ECDSA, Raytonne Trust Services uses and accepts only the NIST Suite B curves.

7.1.4. Name Forms

Name forms are as stipulated in 3.1.1 of this CPS.

7.1.4.1. Issuer Information

For every valid Certification Path (as defined by RFC 5280, Section 6):

- For each Certificate in the Certification Path, the encoded content of the Issuer Distinguished Name field of a Certificate SHALL be byte-for-byte identical with the encoded form of the Subject Distinguished Name field of the Issuing CA certificate.
- For each CA Certificate in the Certification Path, the encoded content of the Subject Distinguished Name field of a Certificate SHALL be byte-for-byte identical among all Certificates whose Subject Distinguished Names can be compared as equal according to RFC 5280, Section 7.1, and including expired and revoked Certificates.

7.1.4.2. Subject Information – Subscriber Certificates

Raytonne Trust Services represents that it followed the procedure set forth in its Certification Practice Statement to verify that, as of the Certificate's issuance date, all of the Subject Information was accurate.

Raytonne Trust Services does not include Domain Names or IP Addresses in a Subject attribute except as specified in Section 3.2.2 of this CPS.

7.1.4.2.1. Subject Alternative Name Extension

For serverAuthentication certificates, this extension will be present and will contain at least one entry. Each entry is either a dNSName containing the Fully-Qualified Domain Name or an iPAddress containing the IP address of a server. Raytonne Trust Services confirms that the Applicant controls the Fully-Qualified Domain

Name or IP address or has been granted the right to use it by the Domain Name Registrant or IP address assignee, as appropriate. Wildcard FQDNs are permitted.

7.1.4.2.2. Subject Distinguished Name Fields commonName

If present, this field contains a single IP address or Fully-Qualified Domain Name that is one of the values contained in the Certificate's subjectAltName extension (see above).

organizationName

If present, this field contains the Subject's name and/or DBA as verified under Section 3.2.2.2 or 3.2.2.3.

Raytonne Trust Services may include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that any abbreviations used are locally accepted abbreviations; e.g., if the official record shows "Company Name Incorporated", we may use "Company Name Inc." or "Company Name".

Because Subject name attributes for individuals (e.g. givenName (2.5.4.42) and surname (2.5.4.4)) are not broadly supported by application software, we may use the subject:organizationName field to convey a natural person Subject's name or DBA.

streetAddress

If present, this field contains the Subject's street address information as verified under Section 3.2.2.2 or 3.2.2.3.

localityName

If present, this field contains the Subject's locality information as verified under Section 3.2.2.2 or 3.2.2.3.

Where the subject:countryName field specifies the ISO 3166-1 user-assigned code of XX in accordance with Section 7.1.4.2.2(7), the localityName field may contain the Subject's locality and/or state or province information as verified under Section 3.2.2.2 or 3.2.2.3.

stateOrProvinceName

If present, this field contains the Subject's state or province information as verified under Section 3.2.2.2 or 3.2.2.3.

If the subject:countryName field specifies the ISO 3166-1 user-assigned code of XX in accordance with Section 7.1.4.2.2(7), the subject:stateOrProvinceName field may contain the full name of the Subject's country information as verified under Section 3.2.2.2 or 3.2.2.3.

postalCode

If present, this field contains the Subject's zip or postal code information as verified under Section 3.2.2.2 or 3.2.2.3.

countryName

This field contains the Subject's two-letter ISO 3166-1 country code information as verified under Section 3.2.2.2 or 3.2.2.3.

If a Country is not represented by an official ISO 3166-1 country code, Raytonne Trust Services will specify the ISO 3166-1 user-assigned code of XX indicating that an official ISO 3166-1 alpha-2 code has not been assigned.

organizationalUnitName

Raytonne Trust Services implements processes that prevent an organizationalUnitName attribute from including a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless the we have verified this information in accordance with Section 3.2.2.2 or 3.2.2.3 and the Certificate also contains subject:organizationName, subject:givenName, subject:surname, subject:localityName, and subject:countryName attributes, also verified in under Section 3.2.2.2 or 3.2.2.3.

EV Certificates SHALL also include the following fields as per Section 9.2 of the EVG:

1. Subject Business Category
   a. subject:businessCategory (OID: 2.5.4.15)
2. Subject Jurisdiction of Incorporation or Registration
   a. subject:jurisdictionLocalityName (OID: 1.3.6.1.4.1.311.60.2.1.1) (if required)
   b. subject:jurisdictionStateOrProvinceName (OID: 1.3.6.1.4.1.311.60.2.1.2) (if required)
   c. subject:jurisdictionCountryName (OID: 1.3.6.1.4.1.311.60.2.1.3)
3. Subject Registration Number
   a. Subject:serialNumber (OID: 2.5.4.5)

EV Certificates SHALL NOT contain other subject attributes. If present in other types of certificates, all other optional attributes, will contain information that has been verified by Raytonne Trust Services. Optional attributes will not contain metadata such as '.', '-', and ' ' (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable.

7.1.4.3. Subject Information – Root Certificates and Subordinate CA Certificates

Raytonne Trust Services represents that it followed the procedure set forth in its Certification Practice Statement to verify that, as of the Certificate's issuance date, all of the Subject Information was accurate.

7.1.4.3.1. Subject Distinguished Name Fields commonName

This field will be present and may be used as an identifier for the CA certificate. Across all CA certificates issued by Raytonne Trust Services, each unique subject:commonName will be paired with only one CA keypair.

organizationName

This field will be present and contains the Subject CA's name or DBA as verified under Section 3.2.2.2.

Raytonne Trust Services may include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that any abbreviations used are locally accepted abbreviations;

e.g., if the official record shows “Company Name Incorporated”, we may use “Company Name Inc.” or “Company Name”.

countryName

This field will be present and contains the Subject’s two-letter ISO 3166-1 country code information as verified under Section 3.2.2.2 or 3.2.2.3.

7.1.5. Name Constraints

Raytonne Trust Services includes Name Constraints in Subordinate CA Certificates when relevant. Raytonne Trust Services places Name Constraints in a non-critical nameConstraints extension within the CA certificate.

Raytonne Trust Services does not include the anyExtendedKeyUsage EKU in Name Constrained CA certificates.

7.1.5.1. TLS Web Server Authentication

For Name Constrained CA certificates that include the id-kp-serverAuth extended key usage, the CA certificate

includes the Name Constraints X.509v3 extension with constraints on dNSName, iPAddress and DirectoryName as follows:

1. For each dNSName in permittedSubtrees, Raytonne Trust Services confirms that the Applicant has registered the dNSName or has been authorized by the domain registrant to act on the registrant’s behalf in line with the verification practices of section 3.2.2.1 of this CPS.
2. For each iPAddress range in permittedSubtrees, Raytonne Trust Services confirms that the Applicant has been assigned the iPAddress range or has been authorized by the assigner to act on the assignee’s behalf.
3. For each DirectoryName in permittedSubtrees Raytonne Trust Services confirms the Applicant’s and/or Subsidiary’s Organizational name and location.

If the Subordinate CA Certificate is not allowed to issue certificates with an iPAddress, then the Subordinate CA Certificate will specify the entire IPv4 and IPv6 address ranges in excludedSubtrees. The Subordinate CA Certificate will include within excludedSubtrees an iPAddress GeneralName of 8 zero octets (covering the IPv4 address range of 0.0.0.0/0). The Subordinate CA Certificate will also include within excludedSubtrees an iPAddress GeneralName of 32 zero octets (covering the IPv6 address range of ::0/0).

Otherwise, the Subordinate CA Certificate will include at least one iPAddress in permittedSubtrees.

7.1.6. Certificate Policy Object Identifier

Henan Raytonne Trading Company uses policy OIDs under the arcs: iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) 54983 certificates(1).

Object Identifier (OID)	Digitally Signed Object
1.3.6.1.4.1.54983.1.0.1	OCSP Responder
1.3.6.1.4.1.54983.1.0.2	Time-Stamping Certificates
1.3.6.1.4.1.54983.1.0.102	Special Purposes Certificates
1.3.6.1.4.1.54983.1.1.1	DV Server Certificates
1.3.6.1.4.1.54983.1.1.2	OV Server Certificates
1.3.6.1.4.1.54983.1.1.3	IV Server Certificates
1.3.6.1.4.1.54983.1.1.4	EV Server Certificates
1.3.6.1.4.1.54983.1.2.1	Code Signing Certificates
1.3.6.1.4.1.54983.1.2.2	EV Code Signing Certificates
1.3.6.1.4.1.54983.1.3.1	Personal S/MIME Certificates
1.3.6.1.4.1.54983.1.3.2	Corporate S/MIME Certificates

TLS Certificates issued to a Subscriber SHALL contain, within the Certificate's certificatePolicies extension, one or more policy identifier(s) that are specified beneath the CA/Browser Forum's reserved policy OID arc of {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1)} (2.23.140.1). The Certificate MAY also contain additional policy identifier(s) defined by Raytonne Trust Services.

7.1.7. Usage of Policy Constraints Extension

No stipulation.

7.1.8. Policy Qualifiers Syntax and Semantics

Raytonne Trust Services includes in End Entity Certificates a non-critical Certificate Policies extension as defined in RFC5280. We include a single PolicyInformation extension that includes the Certificate Policy Identifier and a single Policy Qualifier referring to the CPS URI but not including a userNotice.

7.1.9. Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2. CRL Profile

Raytonne Trust Services manages and makes publicly available directories of revoked Certificates using CRLs. All CRLs issued by Raytonne Trust Services are X.509v2 CRLs, in particular as profiled in RFC5280. Users and relying parties are strongly urged to consult the directories of revoked Certificates at all times prior to relying on information featured in a Certificate. Raytonne Trust Services updates and publishes a new CRL at least every 7 days. The CRL for any certificate issued by Raytonne Trust Services (whether Subscriber certificate or CA certificate) may be found at the URL encoded within the CRLDP field of the certificate itself.

The profile of the Raytonne Trust Services CRL is as per the table below):

Field	Value
Issuer Distinguished Name	Full subject DN of the issuing CA
Issuer Signature Algorithm	sha256WithRSAEncryption; OR sha384WithRSAEncryption; OR ecdsa-with-SHA256; OR ecdsa-with-SHA384
thisUpdate	CRL issue date in UTC format
nextUpdate	Date when the next CRL will issue in UTC format
Issuer's Signature	[Signature]
Revoked Certificates List	List of revoked Certificates, including the serial number and revocation date

7.2.1. Version Number(s)

Raytonne Trust Services issues version 2 CRLs.

7.2.2. CRL and CRL Entry Extensions)

Extension	Value
CRL Number	Never repeated monotonically increasing integer
Authority Key Identifier	Subject Key Identifier of the CRL issuer certificate
Issuing Distribution Point	Configured per RFC 5280 requirements, if included
Invalidity Date	Optional date in UTC format

Reason Code	Optional reason for revocation

reasonCode (OID 2.5.29.21)

If present, this extension MUST NOT be marked critical.

If a CRL entry is for a Root CA or Subordinate CA Certificate, including Cross Certificates, this CRL entry extension MUST be present. If a CRL entry is for a Certificate not technically capable of causing issuance, this CRL entry extension SHOULD be present, but MAY be omitted.

The CRLReason indicated MUST NOT be unspecified (0).

If a reasonCode CRL entry extension is present, the CRLReason MUST indicate the most appropriate reason for revocation of the certificate, as defined below:

- "cessationOfOperation" for cert is no longer needed for the purpose for which it was issued but there is no cause to suspect that the private key has been compromised, and;
- "keyCompromise" for revoked leaf cert (where we've received proof or reasonable suspicion of key compromise), and;
- "caCompromise" for revoked CA cert (where we've received proof or reasonable suspicion of key compromise), and;
- "superseded" for cert has been superseded but there is no cause to suspect that the private key has been compromised.

7.3. OCSP Profile

Raytonne Trust Services also publishes Certificate status information using Online Certificate Status Protocol (OCSP). Raytonne Trust Services' OCSP responders are capable of providing a 'good' or 'revoked' status for all Certificates issued under the terms of this CPS. If queried for a certificate which was not issued by Raytonne Trust Services the responder will provide 'unauthorized'. The OCSP responders will give an 'unknown' response for expired Certificates.

The profile of Raytonne Trust Services OCSP responses is as per this table:

Extension	**Value**
OCSP Response Status	successful (0x0)
Response Type	Basic OCSP Response
Version	1 (0x0)
Responder ID	Same as the subject key identifier listed in the signing certificate
Produced At	The time at which this response was signed

Certificate	Hash Algorithm	sha1
	Issuer Name Hash	Hash of issuer's DN
	Issuer Key Hash	Hash of issuer's public key
	Serial Number	CertificateSerialNumber
Cert Status		Good/Revoked/Unknown
Revocation Time (if Revoked)		The time at which the certificate was revoked or placed on hold
Reason code		If present SHALL contain a value permitted for CRLs, as specified in Section 7.2.2.
This Update		The most recent time at which the indicated certificate status is known by the responder to have been correct
Next Update		The time at or before which newer information will be available about the status of the certificate
Signature Algorithm		sha256WithRSAEncryption; OR ecdsa-with-SHA256

Raytonne Trust Services operates an OCSP service at http://pki.cdn.neminis.net/ocsp/. Revocation information is made immediately available through the OCSP services. The OCSP responder and responses are available 24/7.

For end entity Certificates Raytonne Trust Services publishes a signed OCSP response for every Certificate at least every four days, and the signed OCSP responses are never valid for more than ten days.

If an OCSP response is for a Root CA or Subordinate CA Certificate, including Cross Certificates, and that certificate has been revoked, then the revocationReason field within the RevokedInfo of the CertStatus MUST be present and MUST contain a value permitted for CRLs, as specified in Section 7.2.2.

7.3.1. Version Number(s)

Raytonne Trust Services' OCSP responder conforms to RFC 6960 and 5019.

7.3.2. OCSP Extensions

The singleExtensions of an OCSP response MUST NOT contain the reasonCode (OID 2.5.29.21) CRL entry extension.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The practices specified in this CPS have been designed to meet or exceed the requirements of generally accepted and developing industry standards including the WebTrust for Certification Authorities ("WebTrust for CAs"), and other industry standards related to the operation of CAs.

A regular audit is performed by an independent external auditor to assess Raytonne Trust Services' compliancy with the WebTrust for CAs.

8.1. Frequency or Circumstances of Assessment

The audit mandates that the period during which a CA issues Certificates be divided into an unbroken sequence of audit periods. An audit period must not exceed one year in duration.

8.2. Identity/Qualifications of Assessor

Raytonne Trust Services' audit SHALL be performed by a Qualified Auditor. A Qualified Auditor means a natural person, Legal Entity, or group of natural persons or Legal Entities that collectively possess the following qualifications and skills:

1. Independence from the subject of the audit;
2. The ability to conduct an audit that addresses the criteria specified in an Eligible Audit Scheme (see Section 8.1);
3. Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function;
4. (For audits conducted in accordance with the WebTrust standard) licensed by WebTrust;
5. Bound by law, government regulation, or professional code of ethics; and
6. Except in the case of an Internal Government Auditing Agency, maintains Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage

8.3. Assessor's Relationship to Assessed Entity

The auditor is independent of Raytonne Trust Services, and does not have a financial interest, business relationship, or course of dealing that would create a conflict of interest or create a significant bias (for or against) Raytonne Trust Services.

8.4. Topics Covered by Assessment

As per current version of WebTrust for Certification Authorities, WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security, and WebTrust for Certification Authorities – Extended Validation SSL, which can be found at http://www.webtrust.org.

8.5. Actions Taken as a Result of Deficiency

Either remediate or the auditor posts "qualified report." Auditor would report or document the deficiency, and notify Raytonne Trust Services of the findings. Depending on the nature and extent of the deficiency, Raytonne Trust Services would develop a plan to correct the deficiency, which could involve changing its policies or practices, or both. Raytonne Trust Services would then put its amended policies or practices into operation and

require the auditors to verify that the deficiency is no longer present. Raytonne Trust Services would then decide whether to take any remedial action with regard to Certificates already issued.

8.6. Communication of Results

The audit requires that Raytonne Trust Services makes the Audit Report available to the public no later than 3 months after of the audit period. Raytonne Trust Services is not required to make publicly available any general audit finding that does not impact the overall audit opinion.

The Audit Report MUST contain at least the following clearly-labelled information:

1. name of the organization being audited;
2. name and address of the organization performing the audit;
3. the SHA-256 fingerprint of all Roots and Subordinate CA Certificates, including Cross Certificates, that were in-scope of the audit;
4. audit criteria, with version number(s), that were used to audit each of the certificates (and associated keys);
5. a list of the CA policy documents, with version numbers, referenced during the audit;
6. whether the audit assessed a period of time or a point in time;
7. the start date and end date of the Audit Period, for those that cover a period of time;
8. the point in time date, for those that are for a point in time;
9. the date the report was issued, which will necessarily be after the end date or point in time date

The Audit Report MUST be available as a PDF, and SHALL be text searchable for all information required. Each SHA-256 fingerprint within the Audit Report MUST be uppercase letters and MUST NOT contain colons, spaces, or line feeds.

8.7. Self-Audits

Raytonne Trust Services performs regular self-audits and audits of Registration Authorities in accordance with Section 8.7 of the Baseline Requirements.

9. OTHER BUSINESS AND LEGAL MATTERS

This part describes the legal representations, warranties and limitations associated with Raytonne Trust Services digital Certificates.

9.1. Fees

Raytonne Trust Services charges Subscriber fees for some of the Certificate services it offers, including issuance, renewal and reissues (in accordance with the Raytonne Trust Services Reissue Policy stated in 9.1.6 of this CPS).

Raytonne Trust Services retains its right to affect changes to such fees. Raytonne Trust Services partners, including Reseller Partners, PKI Manager Account Holders, and SSL Partners, will be suitably advised of price amendments as detailed in the relevant partner agreements.

9.1.1. Certificate Issuance or Renewal Fees

Raytonne Trust Services is entitled to charge Subscribers for the issuance, management, and renewal of Certificates. In most circumstances, applicable Certificate fees will be delineated in the Subscriber Agreement between Raytonne Trust Services and Subscriber.

9.1.2. Certificate Access Fees

Raytonne Trust Services may charge a reasonable fee for access to its Certificate databases.

9.1.3. Revocation or Status Information Access Fees

Raytonne Trust Services does not charge fees for the revocation of a Certificate or for a Relying Party to check the validity status of a Raytonne Trust Services issued Certificate using CRLs.

9.1.4. Fees for Other Services

No stipulation.

9.1.5. Refund Policy

Raytonne Trust Services offers a 30-day refund policy. During a 30-day period (beginning when a Certificate is first issued) the Subscriber may request a full refund for their Certificate.

Under such circumstances, the original Certificate may be revoked and a refund provided to the Applicant. Raytonne Trust Services is not obliged to refund a Certificate after the 30-day refund policy period has expired.

9.1.6. Reissue Policy

Raytonne Trust Services offers a 30-day reissue policy. During a 30-day period (beginning when a Certificate is first issued) the Subscriber may request a reissue of their Certificate and incur no further fees for the reissue. If details other than just the Public Key require amendment, Raytonne Trust Services reserves the right to revalidate the application in accordance with the validation processes detailed within this CPS. If the reissue request does not pass the validation process, Raytonne Trust Services reserves the right to refuse the reissue

application. Under such circumstances, the original Certificate may be revoked and a refund provided to the Applicant.

Raytonne Trust Services is not obliged to reissue a Certificate after the 30-day reissue policy period has expired.

9.2. Financial Responsibility

9.2.1. Insurance Coverage

Raytonne Trust Services maintains professional Errors and Omissions Insurance.

9.2.2. Other Assets

No stipulation.

9.2.3. Insurance or Warranty Coverage for End-Entities

If Raytonne Trust Services was negligent in issuing a Certificate that resulted in a Covered Loss to a Relying Party, the Relying Party may be eligible under Raytonne Trust Services' Relying Party Agreement to receive up to the Maximum Certificate Coverage per Incident, subject to the Total Payment Limit**,** for all claims related to that Certificate. For complete terms and conditions, see the Relying Party Agreement located in the Repository.

9.3. Confidentiality of Business Information

Raytonne Trust Services observes applicable rules on the protection of personal data deemed by law or the Raytonne Trust Services privacy policy (see section 9.4.1 of this CPS) to be confidential.

9.3.1. Scope of Confidential Information

Raytonne Trust Services keeps the following types of information confidential and maintains reasonable controls to prevent the exposure of such records to non-trusted personnel.

- Subscriber Agreements.
- Certificate application records and documentation submitted in support of Certificate applications whether successful or rejected.
- Transaction records and financial audit records.
- External or internal audit trail records and reports, except for WebTrust audit reports that may be published at the discretion of Raytonne Trust Services.
- Contingency plans and disaster recovery plans.
- Internal tracks and records on the operations of Raytonne Trust Services infrastructure, Certificate management and enrolment services and data.

9.3.2. Information Not Within the Scope of Confidential Information

Subscribers acknowledge that revocation data of all Certificates issued by the Raytonne Trust Services is public information and is published every 24 hours. Subscriber application data marked as "Public" in the relevant Subscriber Agreement or Certificate request form that is submitted as part of a Certificate application is published within an issued Certificate. Such information is not within the scope of confidential information.

9.3.3. Responsibility to Protect Confidential Information

All Raytonne Trust Services personnel in trusted positions handle all confidential information in strict confidence and are required to sign confidentiality agreements before being employed in a trusted position. Personnel of RA/LRAs especially must comply with the requirements of the Chinese law on the protection of confidential information.

9.3.4. Publication of Certificate Revocation Data

Raytonne Trust Services reserves its right to publish a CRL as may be indicated.

9.4. Privacy of Personal Information

9.4.1. Privacy Plan

Raytonne Trust Services has implemented a privacy policy, which complies with this CPS. The Raytonne Trust Services privacy policy is published at https://www.raytonne.com/privacy-policy/.

9.4.2. Information Treated as Private

See Henan Raytonne Trading Company Privacy Policy. Additionally, personal information obtained from an Applicant during the application or identity verification process is considered private information if the information is not included in the Certificate and if the information is not public information.

9.4.3. Information not Deemed Private

In addition to the information not deemed private in the Henan Raytonne Trading Company Privacy Policy, information made public in a Certificate, CRL, or OCSP is not deemed private.

9.4.4. Responsibility to Protect Private Information

Raytonne Trust Services participants are expected to handle private information with care, and in compliance with local privacy laws in the relevant jurisdiction as well as in accordance with the Raytonne Trust Services privacy policy found at https://www.raytonne.com/privacy-policy/.

9.4.5. Notice and Consent to Use Private Information

Raytonne Trust Services will only use private information after obtaining consent or as required by applicable laws or regulations.

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

Raytonne Trust Services reserves the right to disclose personal information if Raytonne Trust Services reasonably believes that

- disclosure is required by law or regulation, or
- disclosure is necessary in response to judicial, administrative, or other legal process.

9.4.7. Other Information Disclosure Circumstances

See Privacy Policy. Further, Raytonne Trust Services is not required to release any personal information, unless as otherwise required by law, without an authenticated, reasonably specific request by an authorized party specifying:

- The party to whom Raytonne Trust Services owes a duty to keep information confidential.
- The party requesting such information.
- A court order, if any.

9.5. Intellectual Property Rights

Raytonne Trust Services or its partners or associates own all intellectual property rights associated with its databases, websites, Raytonne Trust Services digital Certificates and any other publication originating from Raytonne Trust Services including this CPS.

9.6. Representations and Warranties

9.6.1. CA Representations and Warranties

Raytonne Trust Services makes to all Subscribers and relying parties certain representations regarding its public service, as described below. Raytonne Trust Services reserves its right to modify such representations as it sees fit or required by law.

Except as expressly stated in this CPS or in a separate agreement with Subscriber, to the extent specified in the relevant sections of the CPS, Raytonne Trust Services represents, in all material aspects, to:

- Comply with this CPS and its internal or published policies and procedures.
- Comply with applicable laws and regulations.
- Provide infrastructure and certification services, including but not limited to the establishment and operation of the Raytonne Trust Services Repository and website for the operation of PKI services.
- Provide trust mechanisms, including a key generation mechanism, key protection, and secret sharing procedures regarding its own infrastructure.
- Provide prompt notice in case of compromise of its Private Key(s).
- Provide and validate application procedures for the various types of Certificates that it may make publicly available. For EV certificates, verify and confirm the legal existence of the organization or entity in the correspondent Jurisdiction of Incorporation (JoI) or Registration.
- Issue digital Certificates in accordance with this CPS and fulfill its obligations presented herein.
- Upon receipt of a request from an RA operating within the Raytonne Trust Services network; act promptly to issue a Raytonne Trust Services Certificate in accordance with this CPS.
- Upon receipt of a request for revocation from an RA operating within the Raytonne Trust Services network; act promptly to revoke a Raytonne Trust Services Certificate in accordance with this Raytonne Trust Services CPS.
- Publish accepted Certificates in accordance with this CPS.
- Provide support to Subscribers and relying parties as described in this CPS.
- Revoke Certificates according to this CPS.
- Provide for the expiration and renewal of Certificates according to this CPS.
- Make available a copy of this CPS and applicable policies to requesting parties.

As the Raytonne Trust Services network includes RAs that operate under Raytonne Trust Services practices and procedures Raytonne Trust Services warrants the integrity of any Certificate issued under its own root within the limits of the Raytonne Trust Services insurance policy and in accordance with this CPS.

The Subscriber also acknowledges that Raytonne Trust Services has no further obligations under this CPS.

9.6.2. RA Representations and Warranties

A Raytonne Trust Services RA operates under the policies and practices detailed in this CPS and also the associated agreements. The RA is bound under contract to:

- Receive applications for Raytonne Trust Services Certificates in accordance with this CPS.
- Perform all verification actions prescribed by the Raytonne Trust Services validation procedures and this CPS.
- Receive, verify and relay to Raytonne Trust Services all requests for revocation of a Raytonne Trust Services Certificate in accordance with the Raytonne Trust Services revocation procedures and the CPS.
- Act according to relevant laws and regulations.

9.6.3. Subscriber Representations and Warranties

Subscribers represent and warrant that when submitting to Raytonne Trust Services and using a domain and distinguished name (and all other Certificate application information) they do not interfere with or infringe any rights of any third parties in any jurisdiction with respect to their trademarks, service marks, trade names, company names, or any other intellectual property right, and that they are not seeking to use the domain and distinguished names for any unlawful purpose, including, without limitation, tortious interference with contract or prospective business advantage, unfair competition, injuring the reputation of another, and confusing or misleading a person, whether natural or incorporated.

Upon accepting a Certificate, the Subscriber represents to Raytonne Trust Services and to relying parties that at the time of acceptance and until further notice:

- Digital signatures created using the Private Key corresponding to the Public Key included in the Certificate is the digital signature of the Subscriber and the Certificate has been accepted and is properly operational at the time the digital signature is created.
- No unauthorized person has ever had access to the Subscriber's Private Key.
- All representations made by the Subscriber to Raytonne Trust Services regarding the information contained in the Certificate are accurate and true.
- All information contained in the Certificate is accurate and true to the best of the Subscriber's knowledge or to the extent that the Subscriber had notice of such information whilst the Subscriber shall act promptly to notify Raytonne Trust Services of any material inaccuracies in such information.
- The Certificate is used exclusively for authorized and legal purposes, consistent with this CPS.
- It will use a Raytonne Trust Services Certificate only in conjunction with the entity named in the organization field of a digital Certificate (if applicable).
- The Subscriber retains control of her Private Key, uses a trustworthy system, and takes reasonable precautions to prevent its loss, disclosure, modification, or unauthorized use.
- The Subscriber is an end-user Subscriber and not a CA, and will not use the Private Key corresponding to any Public Key listed in the Certificate for purposes of signing any Certificate (or any other format of

certified Public Key) or CRL, as a CA or otherwise, unless expressly agreed in writing between Subscriber and Raytonne Trust Services.
- The Subscriber agrees with the terms and conditions of this CPS and other agreements and policy statements of Raytonne Trust Services.
- The Subscriber abides by the laws applicable in his/her country or territory including those related to intellectual property protection, viruses, accessing computer systems etc.
- The Subscriber complies with all export laws and regulations for dual usage goods as may be applicable.

In all cases and for all types of Raytonne Trust Services Certificates the Subscriber has a continuous obligation to monitor the accuracy of the submitted information and notify Raytonne Trust Services of any such changes.

9.6.4. Relying Party Representations and Warranties

A party relying on a Raytonne Trust Services Certificate accepts that in order to reasonably rely on a Raytonne Trust Services Certificate they must:

- Minimize the risk of relying on a digital signature created by an invalid, revoked, expired or rejected Certificate; the Relying Party must have reasonably made the effort to acquire sufficient knowledge on using digital Certificates and PKI.
- Study the limitations to the usage of digital Certificates and be aware through the Relying Party agreement the maximum value of the transactions that can be made using a Raytonne Trust Services digital Certificate.
- Read and agree with the terms of the Raytonne Trust Services CPS and Relying Party agreement.
- Verify a Raytonne Trust Services Certificate by referring to the relevant CRL and the CRLs of intermediate CA and root CA or by checking the OCSP response using the Raytonne Trust Services OCSP responder.
- Trust a Raytonne Trust Services Certificate only if it is valid and has not been revoked or has expired.
- Rely on a Raytonne Trust Services Certificate, only as may be reasonable under the circumstances listed in this section and other relevant sections of this CPS.

9.6.5. Representations and Warranties of other Participants

No stipulation.

9.7. Disclaimers of Warranties

9.7.1. Fitness for a Particular Purpose

Raytonne Trust Services disclaims all warranties and obligations of any type, including any warranty of fitness for a particular purpose, and any warranty of the accuracy of unverified information provided, save as contained herein and as cannot be excluded at law.

9.7.2. Other Warranties

Except as required by applicable law, Raytonne Trust Services does not warrant:

- The accuracy, authenticity, completeness or fitness of any unverified information contained in Certificates or otherwise compiled, published, or disseminated by or on behalf of Raytonne Trust Services except as it may be stated in the relevant product description below in this CPS and in the Raytonne Trust Services insurance policy.

- The accuracy, authenticity, completeness or fitness of any information contained in Raytonne Trust Services Personal Certificates class 1, free, trial or demo Certificates.
- In addition, shall not incur liability for representations of information contained in a Certificate except as it may be stated in the relevant product description in this CPS.
- The quality, functions or performance of any software or hardware device.
- Although Raytonne Trust Services is responsible for the revocation of a Certificate, it cannot be held liable if it cannot execute it for reasons outside its own control.
- The validity, completeness or availability of directories of Certificates issued by a third party (including an agent) unless specifically stated by Raytonne Trust Services.

Raytonne Trust Services assumes that user software that is claimed to be compliant with X.509v3 and other applicable standards enforces the requirements set out in this CPS. Raytonne Trust Services cannot warrant that such user software will support and enforce controls required by Raytonne Trust Services, whilst the user should seek appropriate advice.

9.8. Limitations of Liability

Raytonne Trust Services Certificates may include a brief statement describing limitations of liability, limitations in the value of transactions to be accomplished, validation period, and intended purpose of the Certificate and disclaimers of warranty that may apply.

Subscribers must agree to Raytonne Trust Services Terms & Service at https://www.raytonne.com/terms-of-service/ before signing-up for a Certificate. To communicate information Raytonne Trust Services may use:

- An organizational unit attribute.
- A Raytonne Trust Services standard resource qualifier to a Certificate policy.
- Proprietary or other vendors' registered extensions.

9.8.1. Damage and Loss Limitations

In no event (except for fraud or willful misconduct) will the aggregate liability of Raytonne Trust Services to all parties including without any limitation a Subscriber, an Applicant, a recipient, or a Relying Party for all digital signatures and transactions related to such Certificate exceed the cumulative maximum liability for such Certificate as stated in the Raytonne Trust Services insurance plan detailed section 9.2.3 of this CPS.

9.8.2. Exclusion of Certain Elements of Damages

In no event (except for fraud or willful misconduct) shall Raytonne Trust Services be liable for:

- Any indirect, incidental or consequential damages.
- Any loss of profits.
- Any loss of data.
- Any other indirect, consequential or punitive damages arising from or in connection with the use, delivery, license, performance or non-performance of Certificates or digital signatures.
- Any other transactions or services offered within the framework of this CPS.
- Any other damages except for those due to reliance, on the information featured on a Certificate, on the verified information in a Certificate.

- Any liability incurred in this case or any other case if the fault in this verified information is due to fraud or willful misconduct of the Applicant. Any liability that arises from the usage of a Certificate that has not been issued or used in conformance with this CPS.
- Any liability that arises from the usage of a Certificate that is not valid.
- Any liability that arises from usage of a Certificate that exceeds the limitations in usage and value and transactions stated upon it or on the CPS.
- Any liability that arises from security, usability, integrity of products, including hardware and software a Subscriber uses.
- Any liability that arises from compromise of a Subscriber's Private Key.

9.9. Indemnities

9.9.1. Indemnification by Subscriber

By accepting a Certificate, the Subscriber agrees to indemnify and hold Raytonne Trust Services, as well as its agent(s) and contractors harmless from any acts or omissions resulting in liability, any loss or damage, and any suits and expenses of any kind, including reasonable attorneys' fees, that Raytonne Trust Services, and the above mentioned parties may incur, that are caused by the use or publication of a Certificate, and that arises from:

- Any false or misrepresented data supplied by the Subscriber or agent(s).
- Any failure of the Subscriber to disclose a material fact, if the misrepresentation or omission was made negligently or with intent to deceive the CA, Raytonne Trust Services, or any person receiving or relying on the Certificate.
- Failure to protect the Subscriber's confidential data including their Private Key, or failure to take reasonable precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the Subscriber's confidential data.
- Breaking any laws applicable in his/her country or territory including those related to intellectual property protection, viruses, accessing computer systems etc.

For Certificates issued at the request of a Subscriber's agent, both the agent and the Subscriber shall jointly and severally indemnify Raytonne Trust Services, and its agents and contractors.

Although Raytonne Trust Services will provide all reasonable assistance, Certificate Subscribers shall defend, indemnify, and hold Raytonne Trust Services harmless for any loss or damage resulting from any such interference or infringement and shall be responsible for defending all actions on behalf of Raytonne Trust Services.

9.10. Term and Termination

9.10.1. Term

The term of this CPS, including amendments and addenda, begins upon publication to the Repository and remains in effect until replaced with a new CPS passed by the Raytonne Trust Services Certificate Policy Authority.

9.10.2. Termination

This CPS, including all amendments and addenda, remain in force until replaced by a newer version.

9.10.3. Effect of Termination and Survival

The following rights, responsibilities, and obligations survive the termination of this CPS for Certificates issued under this CPS:

- All unpaid fees incurred under section 9.1 of this CPS;
- All responsibilities and obligations related to confidential information, including those stated in section 9.3 of this CPS;
- All responsibilities and obligations to protect private information, including those stated in section 9.4.4 of this CPS;
- All representations and warranties, including those stated in section 9.6 of this CPS;
- All warranties disclaimed in section 9.7 of this CPS for Certificates issued during the term of this CPS;
- All limitations of liability provided for in section 9.8 of this CPS; and
- All indemnities provided for in section 9.9 of this CPS.

Upon termination of this CPS, all PKI participants are bound by the terms of this CPS for Certificates issued during the term of this CPS and for the remainder of the validity periods of such Certificates.

9.11. Individual Notices and Communications with Participants

Raytonne Trust Services accepts notices related to this CPS by means of digitally signed messages or in paper form. Upon receipt of a valid, digitally signed acknowledgment of receipt from Raytonne Trust Services, the sender of the notice shall deem their communication effective. The sender must receive such acknowledgment within five (5) days, or else written notice must then be sent in paper form through a courier service that confirms delivery or via certified or registered mail, postage prepaid, return receipt requested, addressed as follows:

Henan Raytonne Trading Company
386 Changjiang Road
Nanyang, Henan 473000
China

This CPS, related agreements and Certificate policies referenced within this document are available online in the Repository.

9.12. Amendments

Upon the Raytonne Trust Services Certificate Policy Authority accepting such changes it deems to have significant impact on the users of this CPS, an updated edition of the CPS will be published at the Raytonne Trust Services repository available at https://www.raytonne.com/PKI/ with seven (7) days' notice given of upcoming changes and suitable incremental version numbering used to identify new editions. This CPS SHALL be updated at least once per year.

Revisions not denoted "significant" are those deemed by the Raytonne Trust Services Certificate Policy Authority to have minimal or no impact on Subscribers and Relying Parties using Certificates and CRLs issued by Raytonne Trust Services. Such revisions may be made without notice to users of the CPS and without changing the version number of this CPS.

Controls are in place to reasonably ensure that the Raytonne Trust Services CPS is not amended and published without the prior authorization of the Raytonne Trust Services Certificate Policy Authority.

9.12.1. Procedure for Amendment

An amendment to this CPS is made by the Raytonne Trust Services Certificate Policy Authority. The Raytonne Trust Services Certificate Policy Authority will approve amendments to this CPS, and Raytonne Trust Services will publish amendments in the Repository. Amendments can be an update, revision, or modification to this CPS document, and can be detailed in this CPS or in a separate document. Additionally, amendments supersede any designated or conflicting provisions of the amended version of the CPS.

9.12.2. Notification Mechanism and Period

Raytonne Trust Services provides notice of an amendment to the CPS by posting it to the Repository. Amendments become effective on the date provided in the document, when an amendment is written in a separate document, or on the date provided in this CPS, when written in this document.

Raytonne Trust Services does not guarantee or establish a notice and comment period.

9.12.3. Circumstances Under Which OID Must be Changed

The Raytonne Trust Services Certificate Policy Authority has the sole authority to determine whether an amendment to the CPS requires an OID change.

9.13. Dispute Resolution Provisions

Before resorting to any dispute resolution mechanism including adjudication or any type of Alternative

Dispute Resolution (including without exception mini-trial, arbitration, binding expert's advice, co-operation monitoring and normal expert's advice) all parties agree to notify Raytonne Trust Services of the dispute with a view to seek dispute resolution.

9.14. Governing Law, Interpretation, and Jurisdiction

9.14.1. Governing Law

This CPS is governed by Chinese law. This choice of law is made to ensure uniform interpretation of this CPS, regardless of the place of residence or place of use of Raytonne Trust Services digital Certificates or other products and services. Chinese law applies in all Raytonne Trust Services commercial or contractual relationships in which this CPS may apply or quoted implicitly or explicitly in relation to Raytonne Trust Services products and services where Raytonne Trust Services acts as a provider, supplier, beneficiary receiver or otherwise.

9.14.2. Interpretation

This CPS shall be interpreted consistently within the boundaries of business customs, commercial reasonableness under the circumstances and intended usage of a product or service. In interpreting this CPS, parties shall also take into account the international scope and application of the services and products of Raytonne Trust Services and its international network of RAs as well as the principle of good faith as it is applied in commercial transactions.

The headings, subheadings, and other captions in this CPS are intended for convenience and reference only and shall not be used in interpreting, construing, or enforcing any of the provisions of this CPS.

Appendices and definitions to this CPS are for all purposes an integral and binding part of the CPS.

9.14.3. Jurisdiction

Each party, including Raytonne Trust Services partners, Subscribers, and Relying Parties, irrevocably agrees that the courts of Nanyang have exclusive jurisdiction to hear and decide any suit, action or proceedings, and to settle any disputes, which may arise out of or in connection with this CPS or the provision of Raytonne PKI services.

9.15. Compliance with Applicable Law

This CPS is subject to applicable national, state, local and foreign laws, rules, regulations, ordinances, decrees, and orders, including, but not limited to, restrictions on exporting or importing software, hardware, or technical information. Raytonne Trust Services complies with all applicable laws, rules, regulations, ordinances, decrees, and orders when providing services pursuant to this CPS.

9.16. Miscellaneous Provisions

9.16.1. Entire Agreement

This CPS and all documents referred to herein constitute the entire agreement between the parties, superseding all other agreements that may exist with respect to the subject matter. Section headings are for reference and convenience only and are not part of the interpretation of this agreement.

9.16.2. Assignment

This CPS shall be binding upon the successors, executors, heirs, representatives, administrators, and assigns, whether express, implied, or apparent, of the parties. The rights and obligations detailed in this CPS are assignable by the parties, by operation of law (including as a result of merger or a transfer of a controlling interest in voting securities) or otherwise, provided such assignment is undertaken consistent with this CPS articles on termination or cessation of operations, and provided that such assignment does not effect a novation of any other debts or obligations the assigning party owes to other parties at the time of such assignment.

9.16.3. Severability

If any term, provision, covenant, or restriction contained in this CPS, or the application thereof, is for any reason and to any extent held to be invalid, void, or unenforceable, (i) such provision shall be reformed to the minimum extent necessary to make it valid and enforceable as to affect the original intention of the parties, and (ii) the remainder of the terms, provisions, covenants, and restrictions of this CPS shall remain in full force and effect and shall in no way be affected, impaired or invalidated.

9.16.4. Enforcement (Attorneys' Fees and Waiver of Rights)

This CPS shall be enforced as a whole, whilst failure by any person to enforce any provision of this CPS shall not be deemed a waiver of future enforcement of that or any other provision.

9.16.5. Force Majeure

Neither Raytonne Trust Services nor any independent third-party RA operating under a Raytonne Trust Services Certification Authority, nor any Resellers, Co-marketers, nor any subcontractors, distributors, agents, suppliers, employees, or directors of any of the forgoing shall be in default hereunder or liable for any losses, costs, expenses, liabilities, damages, claims, or settlement amounts arising out of or related to delays in performance or from failure to perform or comply with the terms of the Raytonne Trust Services CPS, any Subscription Agreement, or any Relying Party Agreement due to any causes beyond its reasonable control, which causes include acts of God or the public enemy, riots and insurrections, war, accidents, fire, strikes and other labor difficulties (whether or not Raytonne Trust Services is in a position to concede to such demands), embargoes, judicial action, failure or default of any superior certification authority, lack of or inability to obtain export permits or approvals, necessary labor materials, energy, utilities, components or machinery, acts of civil or military authorities.

9.16.6. Conflict of Rules

When this CPS conflicts with other rules, guidelines, or contracts, this CPS shall prevail and bind the Subscriber and other parties except as to other contracts either:

- Predating the first public release of the present version of this CPS.
- Expressly superseding this CPS for which such contract shall govern as to the parties thereto, and to the extent permitted by law.

9.17. Other Provisions

9.17.1. Subscriber Liability to Relying Parties

Without limiting other Subscriber obligations stated in this CPS, Subscribers are liable for any negligence, willful misconduct acts, omissions or misrepresentations they make in Certificates to third parties that reasonably rely on the representations contained therein and have verified one or more digital signatures with the Certificate.

9.17.2. Duty to Monitor Agents

The Subscriber shall control and be responsible for the data that an agent supplies to Raytonne Trust Services. The Subscriber must promptly notify the issuer of any misrepresentations and omissions made by an agent. The duty of this article is continuous.

9.17.3. Financial Limitations on Certificate Usage

Raytonne Trust Services Certificates may only be used in connection with data transfer and transactions completed using a credit card and having a Chinese Yuan (CNY) or US dollar (USD) value no greater than the max transaction value associated with the Certificate detailed in section 9.2.3 of this CPS.

9.17.4. Ownership

Certificates are the property of Raytonne Trust Services. Raytonne Trust Services gives permission to reproduce and distribute Certificates on a nonexclusive, royalty-free basis, provided that they are reproduced and distributed in full. Raytonne Trust Services reserves the right to revoke the Certificate at any time. Private and

Public Keys are property of the Subscribers who rightfully issue and hold them. All secret shares (distributed elements) of the Raytonne Trust Services Private Key remain the property of Raytonne Trust Services.

9.17.5. Interference with Raytonne Trust Services Implementation

Subscribers, Relying Parties, and any other parties shall not interfere with, or reverse engineer the technical implementation of Raytonne PKI services including the key generation process, the public website and the Raytonne Trust Services repositories except as explicitly permitted by this CPS or upon prior written approval of Raytonne Trust Services.

Failure to comply with this as a Subscriber will result in the revocation of the Subscriber's Certificate without further notice to the Subscriber and the Subscriber shall pay any charges payable but that have not yet been paid under the agreement. Failure to comply with this as a Relying Party will result in the termination of the agreement with the Relying Party, the removal of permission to use or access the Raytonne Trust Services repository and any Certificate or Service provided by Raytonne Trust Services.

9.17.6. Choice of Cryptographic Method

Parties are solely responsible for having exercised independent judgment and employed adequate training in choosing security software, hardware, and encryption/digital signature algorithms, including their respective parameters, procedures, and techniques as well as PKI as a solution to their security requirements.

9.17.7. Raytonne Trust Services Partnerships Limitations

Partners of the Raytonne Trust Services network shall not undertake any actions that might imperil, put in doubt or reduce the trust associated with the Raytonne Trust Services products and services. Raytonne Trust Services partners shall specifically refrain from seeking partnerships with other root authorities or apply procedures originating from such authorities. Failure to comply with this will result in the termination of the agreement with the Relying Party, the removal of permission to use or access the Raytonne Trust Services repository and any Digital Certificate or Service provided by Raytonne Trust Services.

9.17.8. Subscriber Obligations

Unless otherwise stated in this CPS, Subscribers shall exclusively be responsible:

- To minimize internal risk of Private Key compromise by ensuring adequate knowledge and training on PKI is provided internally.
- To generate their own Private/Public Key pair to be used in association with the Certificate request submitted to Raytonne Trust Services or a Raytonne Trust Services RA.
- Ensure that the Public Key submitted to Raytonne Trust Services or a Raytonne Trust Services RA corresponds with the Private Key used.
- Ensure that the Public Key submitted to Raytonne Trust Services or a Raytonne Trust Services RA is the correct one.
- Provide correct and accurate information in its communications with Raytonne Trust Services or a Raytonne Trust Services RA.
- Alert Raytonne Trust Services or a Raytonne Trust Services RA if at any stage whilst the Certificate is valid, any information originally submitted has changed since it had been submitted to Raytonne Trust Services.

- Generate a new, secure key pair to be used in association with a Certificate that it requests from Raytonne Trust Services or a Raytonne Trust Services RA.
- Read, understand and agree with all terms and conditions in this Raytonne Trust Services CPS and associated policies published in the Raytonne Trust Services Repository at https://www.raytonne.com/PKI/.
- Refrain from tampering with a Raytonne Trust Services Certificate.
- Use Raytonne Trust Services Certificates for legal and authorized purposes in accordance with the suggested usages and practices in this CPS.
- Cease using a Raytonne Trust Services Certificate if any information in it becomes misleading obsolete or invalid.
- Cease using a Raytonne Trust Services Certificate if such Certificate is expired and remove it from any applications and/or devices it has been installed on.
- Refrain from using the Subscriber's Private Key corresponding to the Public Key in a Raytonne Trust Services issued Certificate to issue end-entity digital Certificates or subordinate CAs.
- Refrain from using the Subscriber's Private Key corresponding to the Public Key in a Raytonne Trust Services issued Certificate to issue end-entity digital Certificates or subordinate CAs.
- Make reasonable efforts to prevent the compromise, loss, disclosure, modification, or otherwise unauthorized use of the Private Key corresponding to the Public Key published in a Raytonne Trust Services Certificate.
- Request the revocation of a Certificate in case of an occurrence that materially affects the integrity of a Raytonne Trust Services Certificate.
- For acts and omissions of partners and agents, they use to generate, retain, escrow, or destroy their Private Keys.

Appendix A: Change Log

Version	Change Description	Date
1.0	Initial publication	February 21, 2022
2.0	Dengzhou Certificate Authority Update	October 17, 2022