TrustAsia Certificate Policy and Certification Practice Statement for Mark Certificate Service (CP&CPS) V1.0.0

TrustAsia Technologies, Inc.

2026-05-09

Table of Contents

1. INTRODUCTION

1.1 Overview

This document is the Certificate Policy and Certification Practice Statement (CP&CPS) formulated by TrustAsia Technologies, Inc. (Chinese abbreviation: "亚洲诚信", English abbreviation: "TrustAsia") for its Mark Certificate Service. This document adopts the RFC 3647 format and outlines the principles and practices related to X.509 digital certificates certified by TrustAsia CA.

All practices of TrustAsia CA regarding the issuance and management of Mark Certificates (MCs) are carried out in accordance with the latest version of the Minimum Security Requirements for Issuance of Mark Certificates (hereinafter referred to as "MCR"). These requirements are available at https://bimigroup.org/supporting-documents/. All Subscribers, Mark Asserting Entities (MAEs), Consuming Entities, and Relying Parties are bound by the "MC Terms" in Appendix D of the MCR.

1.1.1 Company Introduction

TrustAsia Technologies, Inc. (Chinese abbreviation: "亚洲诚信", English abbreviation: "TrustAsia") was established in April 2013. In December 2020, TrustAsia CA passed the qualification review organized by the State Cryptography Administration (SCA) and was granted the "Electronic Authentication Service Cryptography License" issued by SCA (License number: 0060). In November 2021, TrustAsia CA obtained the "Electronic Certification Service License" issued by the Ministry of Industry and Information Technology of China (License number: ECP31010421056).

TrustAsia CA was granted "ISO9001 Quality Management System Certification", "ISO 27001 Information Security Management System Certification", and "ISO22301 Business Continuity Management System Certification" by China Quality Certification Centre (CQC), all of which were accredited by China National Accreditation Service for Conformity Assessment (CNAS) and the International Accreditation Forum (IAF).

TrustAsia CA is an outstanding domestic cybersecurity digital certificate and security monitoring solution provider. Its brand, TrustAsia, specializes in providing internationally renowned digital certificates and cybersecurity management solutions, and is recognized and trusted in the field of cybersecurity.

With internationally standardized operational management and service capabilities, TrustAsia CA provides globalized electronic authentication services for users with requirements on communication and information security in a variety of industries.

1.1.2 Service System/Hierarchy

This document describes the integrated technology, protocols, and identity and trademark verification standards implemented by TrustAsia CA for issuing consumer-trusted Mark Certificates. This CP&CPS covers the following four types of Mark Certificates:

Common Mark Certificates (CMC):

a. Prior Use Mark Certificates

b. Modified Registered Mark Certificates

Verified Mark Certificates (VMC):

a. Registered Mark Certificates

b. Government Mark Certificates

TrustAsia CA issues certificates based on different use cases and algorithms. Please refer to the repository at https://repository.trustasia.com for details.

1.1.3 Certificate Policy (CP) and Certification Practice Statement (CPS)

This CP&CPS is compiled in accordance with the "Measures for the Administration of Electronic Certification Services" and the "Rules for Electronic Authentication Business (for Trial Implementation)" issued by the Ministry of Industry and Information Technology of the People's Republic of China.

This CP&CPS describes how TrustAsia CA carries out electronic certification business, including the business methods and processes of applying for, approving, issuing, managing, revoking and updating certificates, as well as the corresponding service, legal and technical measures and safeguards, for electronic certification participants to understand and follow.

The contents described in this CP&CPS follow the following policies, guidelines and requirements:

1. The RFC 3647 standard issued by the Internet Engineering Task Force (IETF)
2. The latest version of the Mark Certificate Guidelines published by the BIMI Group (prior to the release of this CP&CPS)

TrustAsia CA will periodically review its updates and will continue to revise the CP&CPS. If there is any inconsistency between this CP&CPS and the above relevant standards, the above officially published specifications shall prevail.

1.2 Document Name and Identification

This document is the TrustAsia Certificate Policy and Certification Practice Statement for Mark Certificate Service.

1.2.1 Object Identifiers

TrustAsia CA issues Mark Certificates in accordance with MCR requirements, and includes the MC policy OID in the Certificate Policies Extension. For details, see Section 7.1.6 of this CP&CPS.

The following are some of the object identifiers used in this CP&CPS:

Object Identifier (OID)	Object Represented	Type
1.3.6.1.4.1.44494.2.7	TrustAsia CA Mark Certificate Policy Identifier	Certificate Policy

Object Identifier (OID)	Object Represented	Type
1.3.6.1.4.1.53087.1.1	Reserved Mark Certificate Policy Identifier	Certificate Policy
1.3.6.1.5.5.7.3.31	BIMI Extended Key Usage	Extended Key Usage
1.3.6.1.5.5.7.3.9	OCSP Response Signing	Extended Key Usage
1.3.6.1.4.1.53087.1.13	Mark Type	Subject Field
1.3.6.1.4.1.53087.1.3	Trademark Registration Country	Subject Field
1.3.6.1.4.1.53087.1.2	Trademark Office Name	Subject Field
1.3.6.1.4.1.53087.1.4	Trademark Identifier	Subject Field
1.3.6.1.4.1.53087.1.5	Legal Entity Identifier (LEI)	Subject Field
1.3.6.1.4.1.53087.1.6	Word Mark	Subject Field
1.3.6.1.4.1.53087.3.2	Statute Country Code	Subject Field
1.3.6.1.4.1.53087.3.3	Statute State/Province	Subject Field
1.3.6.1.4.1.53087.3.4	Statute Locality	Subject Field
1.3.6.1.4.1.53087.3.5	Statute Reference	Subject Field
1.3.6.1.4.1.53087.3.6	Statute URL	Subject Field
1.3.6.1.4.1.53087.5.1	Prior Use Mark Source URL	Subject Field
1.3.6.1.4.1.311.60.2.1.1	Jurisdiction Locality	Subject Field
1.3.6.1.4.1.311.60.2.1.2	Jurisdiction State/Province	Subject Field
1.3.6.1.4.1.311.60.2.1.3	Jurisdiction Country	Subject Field
1.3.6.1.5.5.7.1.12	Logotype Extension	Certificate Extension
1.3.6.1.4.1.11129.2.4.2	SCT Record	Certificate Extension

1.2.2 Revision History

Release Date	Update Content	Version
2026-05-09	Issue initial version	V1.0.0

1.3 PKI Participants

1.3.1 Certification Authorities

TrustAsia CA operates simultaneously as a Certification Authority (CA) and a Mark Verifying Authority (MVA).

TrustAsia CA is a legally established electronic certification service organization. It participates in electronic certification activities by issuing digital certificates to parties engaged in electronic transactions and providing digital certificate verification services.

As an operator of multiple CAs, TrustAsia CA executes functions related to public key operations, including receiving certificate requests, issuing, revoking and updating digital certificates, and maintaining, issuing and publishing CRLs and OCSP responses. For information about TrustAsia CA's products and services, please visit www.trustasia.com.

1.3.2 Registration Authorities

On behalf of the CA, the Registration Authority (RA) establishes the certificate registration process, confirms the identity of the certificate applicant (Subscriber), approves or rejects certificate applications, approves Subscriber certificate revocation requests or directly revokes certificates, and approves Subscriber certificate renewal requests.

In addition to assuming the role of CA, TrustAsia CA will act as its own RA and will not establish a separate RA.

1.3.3 Subscribers

Subscribers are all end-users who obtain certificates from TrustAsia CA, also referred to as Mark Asserting Entities.

1.3.4 Relying Parties

Relying Parties are any natural or legal persons who rely on the Mark Certificates issued by TrustAsia CA, or who rely on the information or marks contained in the Mark Certificates, or who rely on the information or marks presented to them by a Consuming Entity.

1.3.5 Other Participants

Other participants refer to other entities that provide related services for TrustAsia CA's electronic certification activities, including the CPA Canada WebTrust Working Group.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

Certificates issued pursuant to this CP&CPS are intended to enable efficient and secure electronic communication, while addressing user concerns about certificate trustworthiness, and helping users make informed decisions when relying on certificates.

1.4.2 Prohibited Certificate Uses

Digital certificates issued by TrustAsia CA are functionally limited and may only be used for purposes appropriate to the identity represented by the certificate. Uses of certificates that exceed the scope defined in this CP&CPS will not be protected by this CP&CPS.

Certificates issued by TrustAsia CA are prohibited from use in any circumstances that violate national laws, regulations or undermine national security, from use in man-in-the-middle (MITM) attacks, and from use in any criminal activity or related business prohibited by law. Otherwise, the

Subscriber shall bear all legal consequences arising therefrom.

1.5 Policy Administration

1.5.1 Organization Administering the Document

The governing body of this CP&CPS is the TrustAsia CA Security Policy Committee, which is responsible for formulating, approving, issuing, implementing, updating and revoking this CP&CPS. The Security Policy Committee is composed of appropriate representatives from the company's management responsible for operational security, technical security, customer service and human resources security.

The daily work of external consulting services for this policy document is handled by the Policy Department.

1.5.2 Contact Person

1.5.2.1 CP&CPS Contact Person

TrustAsia CA will implement strict version control over the CP&CPS, and a designated department is responsible for related matters. Any questions, suggestions or inquiries regarding the CPS can be submitted through the following channels:

Contact Department: Policy Department

Contact Email: cps@trustasia.com

Address: 32/F, Building B, No. 391, Guiping Road, Xuhui District, Shanghai, China (200233)

Tel.: 0086-021-58895880

Fax No.: 0086-021-51861130

Official Website: https://www.trustasia.com

1.5.2.2 Certificate Revocation Contact Person

Certificate problem reports and certificate revocation requests must be submitted through one of the following methods, and certificate revocation requests must be submitted in written form:

- Email: revoke@trustasia.com
- Tel.: 400-880-8600 (Domestic) or 86-21-58895880 (International)

1.5.3 Person Determining CPS Suitability for the Policy

The TrustAsia CA Security Policy Committee is the primary body for policy formulation and the highest authority for reviewing and approving this CP&CPS.

1.5.4 CPS Approval Procedures

This CP&CPS is compiled by a CP&CPS drafting team organized by the TrustAsia CA Security Policy Committee. Upon completion, it is submitted to the Security Policy Committee for review and, upon approval, is officially published on the TrustAsia CA official website.

This CP&CPS is revised in accordance with national policies and regulations, technical requirements, business developments, and the MCR requirements published by the BIMI Group. The CP&CPS drafting team prepares the revision content and submits it to the Security Policy Committee for review. Upon approval, the version number is incremented, the release/effective date and revision history are updated, and the CP&CPS is officially published on the TrustAsia CA website.

1.6 Definitions and Acronyms

1.6.1 Definitions

Term	Definition
Accountant	A person who holds a Certified Public Accountant, Chartered Accountant, or equivalent license in the jurisdiction where the Applicant is incorporated or registered, or in any jurisdiction where the Applicant has offices or physical facilities; provided that the accounting standards body of the jurisdiction maintains full membership in the International Federation of Accountants (IFAC).
Affiliate	A company, partnership, joint venture, or other entity that controls, is controlled by, or is under common control with another entity; or an agency, department, political subdivision, or any entity operating under the direct control of a government entity.
Security Policy Committee	The highest policy management and oversight body within the certification service system and the decision-making body for CP&CPS compliance.
Certification Authority (CA)	Also referred to as Mark Verifying Authority (MVA), is the entity that issues certificates and is responsible for establishing, issuing, revoking and managing certificates. This term applies to both Root CAs and Subordinate CAs.
CAA	Certification Authority Authorization; allows domain name holders to specify CAs authorized to issue certificates for their domain.
Registration Authority (RA)	An entity responsible for processing service requests from certificate applicants and Subscribers, submitting them to the CA, establishing the registration process for end certificate applicants, performing identity identification and authentication of certificate applicants, initiating or relaying certificate revocation requests, and approving certificate renewal or re-key requests on behalf of the CA.

Term	Definition
Certificate Policy (CP)	A named set of rules indicating the applicability of a certificate to a particular community or class of applications with common security requirements.
Certification Practice Statement (CPS)	A statement of the practices that a CA employs in issuing, managing, revoking, and renewing or re-keying certificates.
Certification Path	An ordered sequence of certificates (containing the public key of the starting object in the path) through which the public key of the end object can be obtained.
Policy Qualifier	Policy-dependent information that may appear with a CP identifier in an X.509 certificate. This information may include the URL of an available CP&CPS or relying party agreement, or the text of certificate usage terms.
Digital Certificate	An electronic document that uses a digital signature to bind a public key and an identity. In this document, this refers primarily to Mark Certificates.
Cross Certificate	A certificate used to establish a trust relationship between two Root CAs.
CSPRNG	A random number generator used for cryptographic systems.
Certificate Problem Report	A complaint about a mis-issued certificate, certificate abuse, or other fraud, compromise, or improper conduct.
Certificate Profile	A document or set of documents defining the content and extension requirements for a certificate.
Certificate Revocation List (CRL)	A periodically updated, timestamped, digitally signed list of revoked certificates published by the issuing CA.
Certificate Approver	A natural person employed by or holding explicit authorization to represent the Applicant, who is responsible for exercising the Certificate Requester function and approving requests submitted by other requesters.
Certificate Data	Certificate requests and related data owned, controlled, or accessible by the CA.
Certificate Management Process	Processes, practices, and procedures related to the use of keys, software, and hardware, through which the CA validates data, issues certificates, maintains the repository, and revokes certificates.
Electronic Signature	A technical means of identifying the signatory's identity and indicating the signatory's approval of the signed data.
Digital Signature	An electronic signature implemented by encrypting and decrypting an electronic record using an asymmetric cryptographic system.
Electronic Signatory	A person who holds electronic signature creation data and executes an electronic signature in their own name or on behalf of a represented party.
Electronic Signature Relying Party	A person who engages in relevant activities based on trust in an electronic signature certificate or electronic signature.

Term	Definition
Public Key Infrastructure (PKI)	A set of hardware, software, people, processes, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of certificates and keys based on public key cryptography.
Key Pair	A private key and its associated public key.
Private Key	The private key of a key pair, kept confidential by the key pair holder, used in an electronic signature to create digital signatures and/or decrypt electronic records encrypted with the corresponding public key.
Public Key	The public key of a key pair, which may be publicly disclosed by the holder of the corresponding private key, used by Relying Parties to verify digital signatures created with the holder's private key and/or encrypt messages.
Applicant	An individual, entity, or organization that has applied for but has not yet been granted a Mark Certificate; or an individual, entity, or organization that currently holds one or more Mark Certificates and is applying to renew or obtain additional Mark Certificates.
Applicant Representative	A natural person who is either the Applicant themselves, or is employed by or holds explicit authorization to represent the Applicant: (i) to sign and submit or approve a Certificate Request on behalf of the Applicant, and/or (ii) to sign and submit a Subscriber Agreement on behalf of the Applicant, and/or (iii) to acknowledge the Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA or the CA itself.
Confirming Person	A position within the Applicant's organization responsible for confirming specific facts.
Mark Asserting Entity ("MAE")	The applicant/subscriber for a Mark Certificate. May be the same entity as the Applicant and/or Subscriber.
Conflicting Trademark Owner	A registered trademark owner or licensee who asserts that the mark representation in a Mark Certificate infringes their registered trademark rights.
Court Order of Infringement	A final order from a court or Trademark Office tribunal of competent jurisdiction declaring that the mark representation in a Mark Certificate improperly infringes the registered trademark of a Conflicting Trademark Owner.
Subscriber	An entity that receives a certificate from a CA, also referred to as the certificate holder. In electronic signature applications, the Subscriber is the electronic signatory.
Consuming Entity	An entity that integrates and uses the mark representation and associated data from MC Terms in its products and services, including email service providers.

Term	Definition
Delegated Third Party	A natural person or legal entity authorized by the CA to assist with the Certificate Management Process by fulfilling one or more CA requirements.
Subscriber Agreement	An agreement that an Applicant must read and accept before receiving a certificate, governing the issuance and use of the certificate.
Relying Party	An entity that relies on the authenticity of a certificate. In electronic signature applications, this is the electronic signature relying party. A Relying Party may or may not be a Subscriber.
Relying Party Agreement	An agreement that must be read and accepted by a Relying Party before verifying, relying on, or using a certificate, or before accessing or using the TrustAsia CA repository.
Mark Representation	A digital representation (such as a digital or computer file) of a combination mark, figurative mark, or word mark, containing structured binary or text data that can be parsed to reconstruct (render) the visual representation of the mark so as to make it visible. This mark representation will be used as the logotype extension under Section 7.1.2.3.
Application Software Supplier	A supplier of Relying Party application software capable of displaying or using Mark Certificates and that has integrated the Root Certificate.
Archive Webpage Source	A reliable, publicly available online source that can display screenshots of web pages along with the date on which the screenshots were taken.
Professional Opinion Letter	A letter written by an accountant, attorney, government official, or other reliable third party customarily relied upon, attesting to the accuracy of subject information.
Audit Period	In a period-of-time audit, the period from the first day (start) to the last day (end) covered by the auditor's engagement.
Audit Report	A report issued by a Qualified Auditor stating whether an entity's processes and controls comply with the mandatory provisions of these requirements.
Qualified Auditor	A natural person or legal entity that meets the requirements of Section 8.2 of this CPS.
Qualified Government Information Source (QGIS)	A publicly available database maintained by a government entity, where reporting data is required by law and false reporting is subject to legal penalties.
Qualified Independent Information Source (QIIS)	A regularly updated, publicly available general-purpose database designed to provide accurate information and recognized as a reliable source.
Authorization Domain Name	The domain name used to obtain authorization for issuing a certificate for a given FQDN.
Authorized Port	One of the following ports: 80 (http), 443 (https), 25 (smtp), 22 (ssh).

Term	Definition
Base Domain Name	The first domain name node to the left of the registrar-controlled suffix or public suffix in the requested FQDN, plus that suffix (e.g., "example.com").
Business Entity	Any entity other than a Private Organization, Government Entity, or Non-Commercial Entity; for example, general partnerships, unincorporated associations, sole proprietorships, etc.
Common Mark	A mark or logo that the Applicant or Subscriber claims rights to use under common law (or an equivalent system in civil law jurisdictions). A Common Mark may or may not be a registered trademark.
Figurative Mark	A mark consisting of graphic design, stylized logos, or images, without text and/or letters. For clarity, a "Figurative Mark" includes marks consisting solely of design elements.
Word Mark	A mark consisting solely of text, expressed without regard to font, style, size, or color.
Design Mark	A mark consisting of graphic design, artistic logos, or images, without text and/or letters.
Combination Mark	A mark consisting of graphic design, stylized logos, or images together with text and/or letters in a particular stylized appearance. For clarity, a "Combination Mark" includes marks consisting of both text elements and design elements.
Common Mark Certificate (CMC)	A certificate containing the subject information and extensions specified in the MCR, verified and issued by a Mark Verifying Authority in accordance with the MCR. Additionally, the certificate contains a mark representation that has not been verified as a "Registered Mark" or "Government Mark".
Verified Mark Certificate (VMC)	A certificate containing the subject information and extensions specified in the MCR, verified and issued in accordance with the MCR. Additionally, the certificate contains a mark representation that has been verified as a "Registered Mark" or "Government Mark".
Government Mark	A mark or equivalent identifier granted to or claimed by a government organization (or granted to a private organization or other organization) through a formal statute, regulation, treaty, or government act, whose appearance or description is as shown in such statute, regulation, treaty, or government act, and confirmed by a Mark Verifying Authority in accordance with the procedures set forth in Section 3.2.17.2. A mark registered as a trademark with a Trademark Office by a government entity is not considered a "Government Mark".
Mark Verifying Authority (MVA)	The organization that issues Mark Certificates, also referred to as the CA.
Mark Certificate (MC)	A certificate containing the attributes and extensions specified in these requirements, verified and issued by a Mark Verifying Authority.

Term	Definition
MC Authorization Source	A source other than the Certificate Approver used to confirm that the Certificate Approver has received explicit authorization from the Applicant.
MC Certificate Request	A request for certificate issuance made by the Applicant to the CA, signed by the Certificate Approver.
MCR	These Mark Certificate Requirements.
MC Terms	The terms and conditions applicable to the display and use of Mark Certificates and the data contained therein. See Chapter 12 of this CPS.
WebTrust	The current version of the WebTrust Program for Certification Authorities issued by CPA Canada.
Domain Authorization Document	A document provided by a Domain Name Registrar or registrant proving that the Applicant has the right to request certificates for a specific domain namespace.
Domain Contact	The domain registrant, technical contact, or administrative contact obtained from WHOIS records, DNS SOA records, or directly from the domain registrar.
Internal Name	A string of characters in the Common Name or Subject Alternative Name field of a certificate (that is not an IP address) that cannot be verified as globally unique in public DNS at the time of issuance because it does not end with a top-level domain registered in the IANA Root Zone Database.
Top-Level Domain (TLD)	According to RFC 8499, a top-level domain is a zone one level below the root, such as "com" or "cn".
SVG Guidelines	A document published by the AuthIndicators Working Group regarding SVG Tiny PS specifications and validation tools.
Trademark Office	An intellectual property office recognized by the World Intellectual Property Organization (WIPO) responsible for trademark registration.

1.6.2 Acronyms

BR	Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates	Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates
CA	Certification/Certificate Authority	Certification Authority
CAA	Certification Authority Authorization	Certification Authority Authorization
ccTLD	Country Code Top-Level Domain	Country Code Top-Level Domain
CP	Certificate Policy	Certificate Policy

BR	Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates	Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates
CPS	Certification Practice Statement	Certification Practice Statement
CRL	Certificate Revocation List	Certificate Revocation List
CSR	Certificate Signing Request	Certificate Signing Request
DBA	Doing Business As	Doing Business As
DN	Distinguished Name	Distinguished Name
DNS	Domain Name System	Domain Name System
EV	Extended Validation	Extended Validation
EVG	Guidelines for the Issuance and Management of Extended Validation Certificates	Guidelines for the Issuance and Management of Extended Validation Certificates
FIPS	(US Government) Federal Information Processing Standard	(US Government) Federal Information Processing Standard
FQDN	Fully Qualified Domain Name	Fully Qualified Domain Name
gTLD	Generic Top-Level Domain	Generic Top-Level Domain
IANA	Internet Assigned Numbers Authority	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers	Internet Corporation for Assigned Names and Numbers
KM	Key Management	Key Management
LDAP	Lightweight Directory Access Protocol	Lightweight Directory Access Protocol
LRA	Local Registration Authority	Local Registration Authority
MAE	Mark Asserting Entity	Mark Asserting Entity
MVA	Mark Verifying Authority	Mark Verifying Authority
OCSP	Online Certificate Status Protocol	Online Certificate Status Protocol
OID	Object Identifier	Object Identifier
OSCCA	State Cryptography Administration Office of Security Commercial Code Administration of China	State Cryptography Administration of China

BR	Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates	Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates
PKCS	Public Key Cryptography Standards	Public Key Cryptography Standards
PKI	Public Key Infrastructure	Public Key Infrastructure
RA	Registration Authority	Registration Authority
RFC	Request for Comments	Request for Comments
SSL	Secure Sockets Layer	Secure Sockets Layer
S/MIME	Secure/Multipurpose Internet Mail Extensions	Secure/Multipurpose Internet Mail Extensions
TLS	Transport Layer Security	Transport Layer Security
TTL	Time to Live	Time to Live
X.509	The ITU-T standard for Certificates and their corresponding authentication	ITU-T Certificate Standard and Corresponding Authentication

1.6.3 References

- RFC 3647 standard issued by the Internet Engineering Task Force (IETF)
- Latest version of the Mark Certificate Guidelines published by the BIMI Group (prior to the release of this CP&CPS)
- Apple Root Certificate Program

1.6.4 Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

Dates mentioned in this document, where time is omitted, default to 00:00:00 Beijing Time (UTC+8).

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

TrustAsia CA's repository is a publicly accessible repository that provides information services to Subscribers and Relying Parties. The repository includes, but is not limited to, the following content: CP&CPS, Subscriber Agreements, Relying Party Agreements, Root Certificates, Subordinate CA Certificates, and other information published by TrustAsia CA as necessary.

2.2 Publication of Certification Information

2.2.1 Publication of Repository

TrustAsia CA's repository information will be published in a timely manner on the official website (https://www.trustasia.com/cps), or through other possible forms of information publication as needed. The published content includes CA Certificates, CP&CPS revisions, and other materials. These contents must remain consistent with the CP&CPS and relevant laws and regulations.

2.2.2 Publication of CRL

TrustAsia CA publishes the Certificate Revocation List (CRL) via HTTP. Subscribers or Relying Parties can obtain the CRL through the CRL Distribution Point address in the certificates issued by TrustAsia CA. Each CRL published by TrustAsia CA contains an incrementing serial number.

2.2.3 Publication of OCSP

TrustAsia CA provides an Online Certificate Status Protocol (OCSP) service, allowing Subscribers or Relying Parties to query the status information of certificates in real time.

2.3 Time or Frequency of Publication

2.3.1 CPS Publication Time and Frequency

TrustAsia CA's CP&CPS is available 24/7 through the repository. The CP&CPS is published at least once a year.

TrustAsia CA will regularly track changes to the BIMI Group MCR and adjust the CP&CPS in a timely manner to comply with the standards.

2.3.2 CRL Publication Time and Frequency

TrustAsia CA publishes the CRL for Subscriber Certificates at least every 7 days. For Subordinate CA Certificates, the CRL is published at least every 12 months. If a Subordinate CA Certificate is revoked, the CA Certificate's CRL is updated and published within 24 hours.

2.4 Access Controls on Repositories

The information in TrustAsia CA's repository is provided to the public in a read-only manner for inquiry and retrieval.

TrustAsia CA ensures through network security protection, system security design, and security management policies that only authorized personnel can add, delete, modify, or publish information in the repository.

All versions of the CP&CPS, including historical versions, will be made public in the repository.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

Digital certificates issued by TrustAsia CA conform to the X.509 standard and assign a unique Distinguished Name (DN) to the certificate holder, using the X.500 standard naming format. The naming practices comply with RFC 5280 and the MCR. TrustAsia CA certificates contain the Subject DN of the issuing authority and the certificate subscriber, authenticating the identity and other attributes of the certificate applicant and recording their information with different identifiers. The certificate holder’s identity name is included in the certificate subject in the form of a DN, which is the unique DN of the certificate holder.

MC Certificate Subject attributes will not contain only metadata, such as ".", "-", and " " (i.e., space) characters, and any other indications that a value is missing, incomplete, or not applicable. The Subject Alternative Name extension must contain at least one entry, and each entry must contain a Fully Qualified Domain Name. Internal Names must not be used. Entries of dNSName conform to the preferred name syntax defined in RFC 5280 and do not contain underscore characters.

3.1.2 Need for Names to be Meaningful

TrustAsia CA uses the DN (Distinguished Name) to identify the entities of the certificate subject and the certificate issuer. The name in the DN has certain representative significance and can be related to the identity or specific attributes of the end entity using the certificate. The Certificate Subject Name identifies the specific name of the end entity referred to by the certificate, describing the entity information bound to the public key in the subject’s public key.

3.1.3 Anonymity or Pseudonymity of Subscribers

TrustAsia CA does not issue anonymous or pseudonymous certificates for MC Certificates.

3.1.4 Rules for Interpreting Various Name Forms

The digital certificates issued by TrustAsia CA comply with the X.509 V3 standard, and the Distinguished Name format complies with the X.500 standard. The naming rules for Distinguished Names are defined by TrustAsia CA.

3.1.5 Uniqueness of Names

Within the TrustAsia CA trust domain, the Subject DNs of different Subscribers' certificates cannot be the same and must be unique. However, for the same Subscriber, TrustAsia CA may issue multiple certificates using its unique Subject DN. When the same name appears among different Subscribers applying for certificates, the principle of "first applicant has priority" is followed, and the subsequent applicant must add additional identifying information to distinguish them.

3.1.6 Recognition, Authentication, and Role of Trademarks

Certificate applicants must not use names in their certificate applications that may infringe upon the intellectual property rights of others. TrustAsia CA does not verify the Subscriber's right to use a trademark when issuing a certificate, nor is it responsible for resolving trademark-related disputes. TrustAsia CA may reject or revoke relevant certificates involved in trademark disputes.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

Because the public key contained in a Mark Certificate will not be used, TrustAsia CA does not require the Applicant to prove possession of the associated private key. Subscribers can generate the private key themselves. The proof method can be submitting a digitally signed Certificate Signing Request (CSR) in PKCS#10 format.

3.2.2 Authentication of Organization and Domain Identity

3.2.2.1 Authentication of Organization Identity

TrustAsia CA only issues Mark Certificates to Applicants that qualify as Private Organizations, Government Entities, Business Entities, or Non-Commercial Entities as specified below.

Before issuing a Mark Certificate, TrustAsia CA will ensure that all Subject Organization information included in the certificate complies with relevant requirements. It will choose one or more of the following to verify the organization's identity and address information, and use reliable communication methods to confirm the Applicant Organization's intent to apply:

1. Confirm that the organization is a real, legally existing entity through valid documents issued by government agencies (including but not limited to business licenses, public institution legal person certificates, unified social credit code certificates, etc.) or through authoritative third-party databases that issue valid documents.
2. Obtain the organization's address and contact information through a trusted QGIS or QIIS, and contact the organization by phone, email, or postal mail to confirm the authenticity of the information provided by the Applicant Organization and the Applicant's authorization.
3. Verify information through a Professional Opinion Letter issued by a licensed attorney, accountant, etc.

In addition, TrustAsia CA may establish other necessary authentication methods and materials if necessary. The Applicant is obligated to ensure the authenticity and validity of the application materials and bear the relevant legal responsibilities.

3.2.2.1.1 Identity Authentication of Private Organizations

An Applicant Organization must meet all the following criteria or have obtained the following specified information to be considered a Private Organization:

1. The legal existence of the Private Organization must be created or recognized by a filing or

corresponding action with a registering or recording agency in its Jurisdiction of Incorporation or Registration (e.g., by issuance of a certificate of incorporation, assignment of a registration number, etc.), or created or recognized by a government agency (e.g., under a charter, treaty, convention, or equivalent recognition document);

2. The specific registration number of the Private Organization is assigned by the registering or recording agency in its Jurisdiction of Incorporation or Registration. If the registering or recording agency has not assigned a registration number, TrustAsia CA will use the date of incorporation or registration of the Private Organization;
3. The Private Organization must designate a registered agent, registered office (as required by the laws of its Jurisdiction of Incorporation or Registration), or equivalent to the company registering or recording agency;
4. The Private Organization must not be marked with labels such as "inactive," "invalid," "not current," or labels with equivalent meaning in the records of the company registering or recording agency;
5. The physical address provided by the Private Organization must be the address where the Applicant Organization or its Parent/Subsidiary Company conducts business operations, and it must be the Applicant Organization's Place of Business. If the Applicant Organization's Place of Business is not in the country of incorporation or registration, the Applicant Organization may also provide a verified Professional Opinion Letter proving the address of the Applicant Organization's Place of Business and confirming that business is conducted at that location;
6. To verify the Applicant Organization's ability to engage in business, TrustAsia CA chooses any one of the following to verify the operational existence of the Applicant Organization or its Affiliate, Parent, or Subsidiary Company:
    1. The date of incorporation of the Applicant Organization, Affiliate, Parent, or Subsidiary Company must be no less than three years prior to the certificate application, or it must be listed in a current Qualified Independent Information Source (QIIS) or Qualified Government Tax Information Source (QTIS); or
    2. By receiving certified proof documents directly from a Regulated Financial Institution, verify that the Applicant Organization, Affiliate, Parent, or Subsidiary Company has an active current Demand Deposit Account with that institution; or
    3. Verify through a verified Professional Opinion Letter that the Applicant Organization has an active current Demand Deposit Account with a Regulated Financial Institution;
7. The Jurisdiction of Incorporation, Registration, Charter, or License of the Private Organization and its Place of Business must not be located in any country/region where the laws of TrustAsia CA's operational jurisdiction prohibit conducting business or issuing certificates, nor may it be included in the government denial or prohibition lists of TrustAsia CA's operational jurisdiction.

3.2.2.1.2 Identity Authentication of Government Entities

An Applicant Organization must meet all the following criteria or have obtained the following specified information to be considered a Government Entity:

1. The legal existence of the Government Entity must be established by the political subdivision in which it operates;
2.

TrustAsia CA will attempt to obtain the date of incorporation, registration, or establishment of the Government Entity, or the identifier of the legislative act that created the Government Entity. For Government Entities without a registration number or where the date of establishment cannot be easily verified, TrustAsia CA will use the term "Government Entity" instead;

3. The Government Entity must not be located in any country/region where the laws of TrustAsia CA's operational jurisdiction prohibit conducting business or issuing certificates, nor may it be included in the government denial or prohibition lists of TrustAsia CA's operational jurisdiction.

3.2.2.1.3 Identity Authentication of Business Entities

Any entity that is not a Private Organization, Government Entity, or Non-Commercial Entity is classified as a Business Entity. This includes but is not limited to: general partnerships, unincorporated associations, sole proprietorships, etc. The Applicant Organization must meet all the following criteria or have obtained the following specified information:

1. The Business Entity must be a legally recognized entity, its establishment must involve submitting forms to a registering agency in its jurisdiction, which issues or approves a charter, certificate, or license, and its existence is verified through that registering agency;
2. The physical address provided by the Business Entity must be the address where the Applicant Organization conducts business operations, and it must be the Applicant Organization's Place of Business;
3. The unique registration number of the Business Entity is assigned by the registering agency in its jurisdiction of registration. If the registering agency has not assigned a registration number, TrustAsia CA uses its date of incorporation or registration;
4. To verify the Applicant Organization's ability to engage in business, TrustAsia CA chooses any one of the following to verify the operational existence of the Applicant Organization or its Affiliate, Parent, or Subsidiary Company:
    1. The date of incorporation of the Business Entity must be no less than three years prior to the certificate application, or it must be listed in a current Qualified Independent Information Source (QIIS) or Qualified Government Tax Information Source (QTIS); or
    2. By receiving certified proof documents directly from a Regulated Financial Institution, verify that the Applicant Organization has an active current Demand Deposit Account with that institution; or
    3. Verify through a verified Professional Opinion Letter that the Applicant Organization has an active current Demand Deposit Account with a Regulated Financial Institution;
5. TrustAsia CA must conduct a "face-to-face validation" with at least one "Principal Individual" associated with the Business Entity. A "Principal Individual" can be an owner, partner, managing member, director, or officer of the entity, or an individual proven to be a "Principal Individual" through an authorization letter issued by the Applicant Organization. TrustAsia CA will arrange a "face-to-face audit" for the "Principal Individual". The methods for face-to-face audit (or equivalent) include but are not limited to video calls, video recordings, in-person audits, etc. During the face-to-face audit, the "Principal Individual" must present a government-issued ID and provide at least two supporting pieces of documentary evidence to prove their identity, one of which must be from a financial institution. The "Principal Individual" must

present the original ID document as required by the auditor and sign the application form regarding personal information statements on the spot to complete the audit. The "Principal Individual" must also attest that the representations made in the Subscriber Agreement are true. TrustAsia CA will review the documents provided by the customer to ensure the information is consistent, matches the information in the application form, and can identify the "Principal Individual";

6. The Business Entity and its associated identified "Principal Individuals" must not be located in any country/region where the laws of TrustAsia CA's operational jurisdiction prohibit conducting business or issuing certificates, and neither the Business Entity nor its associated identified "Principal Individuals" may be included in the government denial or prohibition lists of TrustAsia CA's operational jurisdiction.

3.2.2.1.4 Identity Authentication of Non-Commercial Entities

An Applicant Organization must meet all the following criteria or have obtained the following specified information to be considered a Non-Commercial Entity:

1. The Non-Commercial Entity is an International Organization Entity established pursuant to a charter, treaty, convention, or equivalent instrument signed by multiple national governments (or on behalf of multiple national governments);
2. For a Non-Commercial Entity for which a legislative document identifier cannot be easily created or the date of establishment cannot be easily verified, TrustAsia CA will use the term "International Organization Entity" instead;
3. To verify the Applicant Organization's ability to engage in business, TrustAsia CA chooses any one of the following to verify the operational existence of the Applicant Organization or its Affiliate, Parent, or Subsidiary Company:
    1. The date of incorporation of the Applicant Organization, Affiliate, Parent, or Subsidiary Company must be no less than three years prior to the certificate application, or it must be listed in a current Qualified Independent Information Source (QIIS) or Qualified Government Tax Information Source (QTIS); or
    2. By receiving certified proof documents directly from a Regulated Financial Institution, verify that the Applicant Organization, Affiliate, Parent, or Subsidiary Company has an active current Demand Deposit Account with that institution; or
    3. Verify through a verified Professional Opinion Letter that the Applicant Organization has an active current Demand Deposit Account with a Regulated Financial Institution;
4. The country where the headquarters of the Non-Commercial Entity is located must not be located in any country/region where the laws of TrustAsia CA's operational jurisdiction prohibit conducting business or issuing certificates, nor may it be included in the government denial or prohibition lists of TrustAsia CA's operational jurisdiction.

In addition, subordinate organizations or agencies of an entity that qualifies as a Non-Commercial Entity may also apply for a Non-Commercial Entity Mark Certificate.

3.2.2.2 Face-to-Face Validation Procedures

TrustAsia CA requires that the Contract Signer or Certificate Approver of the Applicant

Organization must undergo a face-to-face validation procedure. TrustAsia CA will arrange a "face-to-face audit" for them with reference to the video conference validation requirements described in the MCR.

TrustAsia CA will initiate a live-recorded video conference with the designated person. During the video conference, the designated person needs to state their basic information, including name, address, organization name, phone number, ID type (passport, resident ID card, driver's license, etc.), and ID number.

The designated person must also present their ID document during the video conference as required. After the video conference ends, TrustAsia CA will approve or reject the identity verification request based on the audit results and securely archive the recording. The retention period for the recording shall be no less than 2 years after the end of the certificate's validity period.

3.2.2.3 Validation of DBA/Assumed Name

The Applicant Organization may request that an assumed name (DBA) be included in the certificate, but the Applicant Organization must have registered its use of the assumed name with the relevant government agency within its jurisdiction of incorporation or registration, and its assumed name registration must remain valid.

TrustAsia CA will verify the authenticity of the assumed name through any one of the following methods:

1. By verifying with the relevant government agency through QGIS, or directly via mail, phone, or website;
2. When a QIIS has already verified the assumed name with the corresponding government agency, TrustAsia CA may verify it by using the QIIS;
3. Through a verified Professional Opinion Letter, which must state the assumed name under which the Applicant Organization conducts business, the government agency where the assumed name is registered, and that the registration remains valid.

3.2.2.4 Validation of Country

If the Certificate Subject includes a Country field, TrustAsia CA will confirm the country of location through the organization proof information provided by the Applicant in Section 3.2.2.1.

3.2.2.5 Validation of Domain Authorization or Control

When a user applies for a Mark Certificate, TrustAsia CA must verify the Applicant's control over the domain name in the requested certificate. This validation process is performed by TrustAsia CA and will not be delegated to a third party.

TrustAsia CA maintains a validation record for each domain name, including which validation method was used and the corresponding MCR version number.

3.2.2.5.1 Validating the Applicant as a Domain Contact

TrustAsia CA does not support this method.

3.2.2.5.2 Email, Fax, SMS, or Postal Mail to Domain Contact

TrustAsia CA does not support this method.

3.2.2.5.3 Phone Contact with Domain Contact

TrustAsia CA does not support this method.

3.2.2.5.4 Constructed Email to Domain Contact

As defined in Section 3.2.14.4 of the MCR, construct an email to a domain contact.

Confirm the Applicant's control over the requested FQDN by communicating directly with the Domain Contact using a constructed email address through the following method:

1. Send an email to one or more email addresses constructed by using "admin", "administrator", "webmaster", "hostmaster", or "postmaster" as the local part, followed by the at-sign ("@"), followed by an Authorization Domain Name,
2. Include a Random Value in the email, and
3. Require the Applicant to submit (by clicking or otherwise) the Random Value to TrustAsia CA's servers to confirm receipt and authorization.

TrustAsia CA may resend the email, including reusing the Random Value, provided the email content and recipient remain unchanged.

The unique Random Value is generated by TrustAsia CA and is valid for no more than 30 days from the date of generation.

3.2.2.5.5 Domain Authorization Document

TrustAsia CA does not support this method.

3.2.2.5.6 Agreed-Upon Change to Website

TrustAsia CA does not support this method.

3.2.2.5.7 DNS Change

As defined in Section 3.2.14.7 of the MCR, the Subscriber resolves a specified TXT or CNAME record with a Random Value or Request Token for the domain to be verified. Domain ownership validation is complete once TrustAsia CA successfully queries the specified record.

The unique Random Value is generated by TrustAsia CA and is valid for no more than 30 days from the date of generation. If a domain name completes control validation via this method, TrustAsia CA may issue certificates for this domain name and any subordinate domain names ending with this domain name.

3.2.2.5.8 IP Address

TrustAsia CA does not support this method.

3.2.2.5.9 Test Certificate

TrustAsia CA does not support this method.

3.2.2.5.10 TLS Using a Random Number

TrustAsia CA does not support this method.

3.2.2.5.11 Any Other Method

TrustAsia CA does not support this method.

3.2.2.5.12 Validating Applicant as a Domain Contact

TrustAsia CA does not support this method.

3.2.2.5.13 Email to DNS CAA Contact

TrustAsia CA does not support this method.

3.2.2.5.14 Email to DNS TXT Contact

As defined in Section 3.2.14.14 of the MCR, TrustAsia CA will send a validation email to the Domain Contact email address obtained via a DNS query of the TXT record for "_validation-contactemail.AuthorizationDomainName". The validation email will contain a unique Random Value. Upon receiving the validation email, the Subscriber accesses the validation link with the Random Value and clicks approve to complete the domain ownership validation.

The unique Random Value is generated by TrustAsia CA and is valid for no more than 30 days from the date of generation. If a domain name completes control validation via this method, TrustAsia CA may issue certificates for this domain name and any subordinate domain names ending with this domain name.

3.2.2.5.15 Phone Contact with Domain Contact

TrustAsia CA does not support this method.

3.2.2.5.16 Phone Contact with DNS TXT Record Phone Contact

TrustAsia CA does not support this method.

3.2.2.5.17 Phone Contact with DNS CAA Phone Contact

TrustAsia CA does not support this method.

3.2.2.5.18 Agreed-Upon Change to Website v2

As defined in Section 3.2.14.18 of the MCR, the Subscriber places a specified validation file containing a Random Value or Request Token under the /.well-known/pki-validation/ directory on

the site of the domain to be verified. Domain ownership validation is complete when TrustAsia CA successfully accesses the specified validation content via the default port for HTTP/HTTPS protocols.

The unique Random Value is generated by TrustAsia CA and is valid for no more than 30 days from the date of generation. If a domain name completes control validation via this method, TrustAsia CA may only issue certificates for this specific domain name. TrustAsia CA supports HTTP redirect requests with status codes 301 and 302; the redirected address must match the verified domain name, may use HTTP or HTTPS, and must be on a default authorized port.

3.2.2.5.19 Agreed-Upon Change to Website - ACME

As defined in Section 3.2.14.19 of the MCR, confirm the Applicant's control over the FQDN by verifying domain control of the FQDN using the ACME HTTP Challenge method defined in Section 8.3 of RFC 8555.

The token (unique Random Value, as defined in Section 8.3 of RFC 8555) is generated by TrustAsia CA and is valid for 30 days from the date of generation.

TrustAsia CA supports HTTP redirect requests with status codes 301 and 302 initiated via HTTP; the redirected address must match the verified domain name, may use HTTP or HTTPS, and must be on a default authorized port. This method is not used to validate wildcard domain names.

3.2.2.5.20 TLS Using ALPN Extension

TrustAsia CA does not support this method.

3.2.2.6 CAA Records for Mark Certificates

See Section 4.2.4 of this CPS.

3.2.2.7 Mark Validation in Common Mark Certificates

Common Mark Certificates are categorized into Prior Use Mark Certificates and Modified Registered Mark Certificates.

3.2.2.7.1 Validation of Prior Use Mark Certificates

1. This type of Mark Certificate applies to Common Marks that are not registered trademarks.

The Applicant should provide TrustAsia CA with the mark representation in SVG format that it wishes to include in the Mark Certificate. TrustAsia CA will verify the following:

a. The trademark displayed on the current website must match the mark representation provided when applying for the certificate. And the Applicant's control over the website domain name must be verified through at least one method specified in Section 3.2.14 of the MCR;

b. The mark matching this mark representation has been displayed on the same verified domain controlled by the Applicant for at least 12 months prior to the mark validation date. The historical display record must be verified through "Archive Webpage Sources". TrustAsia CA must be able to obtain the URL of the mark representation during the validation process and write it into the corresponding certificate field.

TrustAsia CA will also retain screenshots or other records of the mark representation provided by the Applicant, as well as all mark images found during the above validation process.

2. TrustAsia CA will use one of the following Archive Webpage Sources for Mark Representation validation:
    - https://archive.org

This approved list may be modified from time to time.

3. Color Restrictions: For Mark Certificates based on prior use evidence, the mark representation must comply with the same color rules applicable to common marks in the relevant jurisdiction, and must be consistent with the colors used during its prior use. TrustAsia CA will review the prior use to determine any specific validations claimed by the mark owner.

3.2.2.7.2 Validation of Modified Registered Mark Certificates

TrustAsia CA will verify the registered trademark proposed to be modified by the Applicant according to the following validation requirements. The Applicant must provide the mark representation in SVG format that it wishes to include in the Mark Certificate.

1. Confirmation of Mark Representation

TrustAsia CA accepts the following types of modifications to the mark representation of a registered trademark:

a. Combination Marks: For Combination Marks, the position of any Word Mark element can be rearranged relative to the Design Mark element.

b. Figurative Marks and Combination Marks: For Figurative Marks and Combination Marks, part of the design elements may be removed, provided the removed portion does not exceed 49% of the design elements, and the remaining portion must not be altered. For Combination Marks, the Word Mark elements may be adjusted as described in (a), but relative to the remaining Design Mark elements.

c. Word Marks and Combination Marks: For Word Marks and Combination Marks where the Word Mark element consists of a single word, the word may be divided into multiple parts, which may or may not be stacked.

d. Word Marks and Combination Marks: For Word Marks and Combination Marks where the Word Mark element consists of multiple words, the words may be divided into multiple parts, which may or may not be stacked, or multiple words may be combined into a single word.

e. The modified registered trademark may use any font or color, and may be paired with a colored or patterned background.

TrustAsia CA will verify the modified mark representation to determine whether the modification causes a material alteration to the obvious meaning of the original mark (compared to the registered trademark). If it causes a material alteration, TrustAsia CA will notify the Applicant that the submitted modification cannot be accepted and must be further modified. The Applicant may choose to continue applying and submit a modified Mark Certificate request.

As a condition for accepting modifications to the mark representation of a registered trademark,

TrustAsia CA may require the Applicant to defend, indemnify, and hold TrustAsia CA harmless against any claims by any party that may arise from such modification.

2. Trademark Country or Region Validation

TrustAsia CA must verify the country or region of the Trademark Office for the registered trademark and enter it in the form of a two-letter country and intergovernmental/regional agency code per WIPO ST.3 standard.

3. Trademark Office Name Validation

When the country or region of the trademark has more than one national or regional intellectual property office where a trademark can be registered, TrustAsia CA will specify the exact office to eliminate ambiguity. When the country or region has only one official trademark registration agency, TrustAsia CA may leave it unspecified.

TrustAsia CA will identify the Trademark Office by inserting the name of the Trademark Office listed in the "Office" column of the WIPO Directory of National and Regional Intellectual Property Offices, as well as a reliable data source recognized by TrustAsia CA.

4. Trademark Number Validation

The Applicant must provide the trademark number to TrustAsia CA. TrustAsia CA will verify whether the trademark number assigned by the Trademark Office to identify the registered trademark or registered trademark application is consistent with the one provided by the Applicant. Furthermore, TrustAsia CA will verify whether the trademark corresponding to the trademark number is in "good standing" by accessing the official database of the relevant Trademark Office or the WIPO Global Brand Database.

3.2.2.8 Mark Validation in Verified Mark Certificates

TrustAsia CA issues Verified Mark Certificates for trademarks that have been registered with a Trademark Office and meet the qualifications for a registered trademark. Verified Mark Certificates are categorized into Registered Mark Certificates and Government Mark Certificates. TrustAsia CA will verify the trademark in a Verified Mark Certificate through one of the following methods.

3.2.2.8.1 Validation of Registered Mark Certificates

1. Trademark Validation with Trademark Office

TrustAsia CA will verify the following provided by the Subscriber:

a. The trademark registration number of the registered trademark and the name of the Trademark Office that granted the trademark registration;
b. The mark representation in SVG format that the Applicant wishes to include in the Verified Mark Certificate.

The registered trademark must be valid and must be verified by consulting the official database of the relevant Trademark Office before it is permitted to be included in the VMC certificate.

Alternatively, TrustAsia CA may verify the registered trademark through the WIPO Global Brand

Database (https://www.wipo.int/reference/en/branddb/).

2. Registered Trademark Ownership or License Validation

TrustAsia CA will confirm that the registered trademark owner identified in the official database of the relevant Trademark Office or the WIPO Global Brand Database is the same organization as the Subject Organization verified in Section 3.2.2.1 of this CPS, or a Parent, Subsidiary, or Affiliate of that organization.

If the owner of the registered trademark is not the organization itself, the Subject Organization must have obtained the right to use the registered trademark through a mutually agreed license agreement signed with the registered trademark owner (or the owner's Parent, Subsidiary, or Affiliate).

If the owner of the registered trademark is not the Applicant, TrustAsia CA will not issue a certificate for that registered trademark unless TrustAsia CA obtains a letter of authorization issued by the registered trademark owner.

3. Confirmation of Mark Representation

TrustAsia CA will verify that the trademark submitted by the Applicant is completely identical to the registered trademark. This verification will be recorded by comparing the trademark with the official database of the relevant Trademark Office or the WIPO Global Brand Database.

4. Color Restrictions

Verified Mark Certificates containing Combination Marks and Design Marks may only display the range of colors explicitly permitted for use with the registered trademark by the relevant Trademark Office. TrustAsia CA will review the registered trademark to determine any specific colors claimed by the registered trademark owner.

5. Trademark Country or Region Validation

Refer to Section 3.2.2.7.2(2) of this CPS.

6. Trademark Office Name Validation

Refer to Section 3.2.2.7.2(3) of this CPS.

7. Trademark Number Validation

Refer to Section 3.2.2.7.2(4) of this CPS.

3.2.2.8.2 Validation of Government Mark Certificates

TrustAsia CA issues these for marks granted to or claimed by Government Entities or Non-Commercial Entities (International Organizations), or marks granted by Government Entities or Non-Commercial Entities (International Organizations) to a private organization or other organization via an official statute, regulation, treaty, or government act. The mark shall match its appearance or description in the relevant statute, regulation, treaty, or government act, and must be confirmed by the Mark Verifying Authority.

1. Validation of Statute, Regulation, Treaty, or Act

TrustAsia CA must confirm that the Government Mark is granted to or claimed by a Government Entity or Non-Commercial Entity (International Organization) by verifying public records of the official statute, regulation, treaty, or government act.

A Government Mark may also be granted to a private organization or other types of organizations by a Government Entity or Non-Commercial Entity via an official statute, regulation, treaty, or government act.

TrustAsia CA will retain a copy of the relevant statute, regulation, treaty, or government act, including all official reference information (e.g., statute or regulation number and its jurisdiction), and a copy of the mark contained or referenced in the statute or regulation. TrustAsia CA will also retain screenshots or other records of the mark representation provided by the Applicant, as well as all information obtained from the relevant statute, regulation, treaty, or government act used to support the Government Mark validation. The specific citation to the official statute, regulation, treaty, or government act granting or claiming the Government Mark will be included in the certificate. TrustAsia CA may use abbreviations and will, as much as possible, comply with applicable legal guidelines of the relevant jurisdiction regarding the typical citation formats for such official statutes, regulations, treaties, or government acts (e.g., "The Bluebook: A Uniform System of Citation" or other similar standard citation systems).

2. Government Mark Ownership or License Validation

TrustAsia CA must confirm that the Government Mark owner identified in (1) is the same organization as the Subject Organization verified in Section 3.2.2.1 of this CPS, and has obtained the right to use the Government Mark through the relevant statute, regulation, treaty, or government act, or through a mutually agreed license agreement.

When the owner of the Government Mark is not the Applicant, the Applicant may only use the Government Mark after TrustAsia CA obtains a written letter of authorization from the registered owner of the Government Mark.

In determining whether the Applicant is the owner or licensee of the Government Mark for the corresponding mark representation, TrustAsia CA will base its decision and rationale on the records required to be retained in (1).

3. Confirmation of Mark Representation

TrustAsia CA will confirm that the mark representation submitted by the Applicant matches the Government Mark confirmed under (1) and will retain the relevant decisions and rationale.

4. Color Restrictions

The mark representation of Combination Marks and Design Marks included in the Verified Mark Certificate is limited to the colors permitted for use with that Government Mark by the statute, regulation, treaty, or government act verified by TrustAsia CA.

TrustAsia CA will review the submitted Government Mark to determine what rights the Subject Organization has regarding the colors in the mark representation submitted by the Subscriber.

TrustAsia CA will determine, in accordance with the requirements of (1), whether the colors in the mark representation submitted by the Subscriber comply with the permitted colors in the statute, regulation, treaty, or government act verified by TrustAsia CA.

5. Competent Legal Jurisdiction of the Government Entity Establishing the Government Mark

TrustAsia CA must verify the competent legal jurisdiction of the Government Entity that established the Government Mark; specific verification items are Statute Country, Statute State/Province, and Statute Locality.

Validation criteria: Unless relevant to the level of the Government Entity or Non-Commercial Entity (International Organization) establishing the Government Mark through a statute, regulation, treaty, or government act, the certificate must not include the following fields.

For example, the jurisdiction of a Government Entity or Non-Commercial Entity (International Organization) operating at the national level must include the "Statute Country" field, but must not include the "Statute State/Province" and "Statute Locality" fields.

The jurisdiction of an applicable Government Entity or Non-Commercial Entity (International Organization) at the state or provincial level must include the "Statute Country" and "Statute State/Province" fields, but must not include the "Statute Locality" field.

The jurisdiction of an applicable Government Entity or Non-Commercial Entity (International Organization) at the local level must include the "Statute Country", "Statute State/Province", and "Statute Locality" fields.

TrustAsia CA will use the two-letter ISO country/region code to specify the "Statute Country" field.

The "Statute State/Province" and "Statute Locality" fields will be specified using the full name of the applicable jurisdiction.

3.2.3 Authentication of Individual Identity

The issuance target of TrustAsia CA’s certificates must be an Applicant, which is an organizational entity. However, during the certificate issuance process, TrustAsia CA will verify the personal identity of the Applicant Representative. The Applicant Representative must be a natural person and can be an authorized employee or authorized agent of the Applicant Organization. TrustAsia CA will use the validation methods in Section 3.2.2.1 to verify the Applicant’s intent to apply with the Applicant Representative.

The Applicant Representative may be required to submit a clear copy of a valid government-issued photo ID (such as a resident ID card, passport, driver’s license, military officer ID, or other equivalent document). TrustAsia CA will verify whether the copy of the document matches the requested name and whether other relevant information is correct.

For Business Entity type organizations applying for a Mark Certificate, TrustAsia CA will conduct a "face-to-face validation" of the "Principal Individual" in accordance with the requirements in Section 3.2.2.1.3.

3.2.4 Non-Verified Subscriber Information

Generally, except for the identity information that is explicitly and reliably required to be verified for the specific type of certificate, TrustAsia CA makes no commitment to the authenticity of unverified Subscriber information and assumes no related legal responsibilities. Information in the certificate must be verified, the validation must come from trusted third-party data sources, and unverified information must not be written into the certificate.

3.2.5 Validation of Authority

When an organizational Subscriber authorizes an Applicant Representative to handle certificate business, TrustAsia CA's validation of the Applicant's authorization includes:

1. Validation of personnel in relevant roles of the Applicant Organization:

TrustAsia CA will verify the names, titles, and authorizations of the Certificate Requester, Certificate Approver, and Contract Signer; and review whether these role personnel are listed on a denial list. If they are on the list, TrustAsia CA has the right to refuse to issue the certificate or require the replacement of relevant contacts. TrustAsia CA will contact the Certificate Requester or Certificate Approver using a valid communication method selected through the validation methods in Section 3.2.2.1, and obtain an affirmative response to verify the authenticity of the Applicant Representative applying for the certificate.

Certificate Requester: The submitter of the Mark Certificate application and the contact person for order review. The Certificate Requester is a natural person and can be an employee of the Applicant Organization or an authorized agent explicitly authorized to submit certificate applications on behalf of the Applicant Organization.

Certificate Approver: The approver for the Mark Certificate request. The Certificate Approver is a natural person and can be an employee of the Applicant Organization or an authorized agent explicitly authorized to approve certificate applications on behalf of the Applicant Organization.

Contract Signer: The signer of the Mark Certificate Subscriber Agreement. The Contract Signer is a natural person and can be an employee of the Applicant Organization or an authorized agent explicitly authorized to sign the Subscriber Agreement on behalf of the Applicant Organization.

The Applicant Organization may authorize one person to serve in two or more of these roles, and the Applicant Organization may also authorize more than one person to serve in any of these roles.

2. Signature Validation of the Subscriber Agreement

TrustAsia CA requires that the Contract Signer or a formally authorized individual must sign the Subscriber Agreement and agree to the terms of use. For the signature of the Subscriber Agreement, TrustAsia CA will require the Subscriber to complete it on the order page.

3. Signature Validation of the Certificate Request

TrustAsia CA requires that the Certificate Approver must sign the certificate request. TrustAsia CA will send an online approval link via email, and the Certificate Approver completes the online approval.

3.2.6 Criteria for Interoperation

Other electronic certification service organizations may interoperate with TrustAsia CA, but their CPS must comply with TrustAsia CA CP&CPS requirements and sign corresponding agreements with TrustAsia CA.

If national laws and regulations have provisions regarding this, TrustAsia CA will strictly implement them.

TrustAsia CA will disclose all Cross Certificates it issues.

3.3 Identification and Authentication for Re-key Requests

For keys generated by the Subscriber, TrustAsia CA will rely on previously provided or obtained information to authenticate key update requests.

3.3.1 Identification and Authentication for Routine Re-key

TrustAsia CA supports key update requests for Subscribers with certificates within their validity period. Subscribers may choose to generate a new key pair to replace the currently used or soon-to-expire key pair.

3.3.2 Identification and Authentication for Re-key After Revocation

TrustAsia CA does not provide key updates after a certificate has been revoked.

3.4 Identification and Authentication for Revocation Request

In TrustAsia CA's certificate business, certificate revocation requests can come from the Subscriber, TrustAsia CA, or judicial personnel authorized by judicial agencies. In addition, Relying Parties, Application Software Suppliers, Conflicting Trademark Owners, or other third parties may submit Certificate Problem Reports informing TrustAsia CA of reasonable grounds to revoke a certificate. Furthermore, when TrustAsia CA has grounds described in Section 4.9.1.1 of this CP&CPS to revoke a Subscriber's certificate, it has the right to initiate the revocation of the Subscriber certificate.

The Subscriber submits a request to TrustAsia CA through certain methods, such as email, fax, phone, etc. TrustAsia CA confirms that the person or organization requesting the revocation is indeed the Subscriber or their authorized representative using methods commensurate with the certificate's level of assurance. Depending on the situation, the confirmation method can be one or more of the following: domain control validation, phone, fax, email, mail, or courier service.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

An Applicant or an individual authorized to apply for a certificate on behalf of the Applicant may submit a certificate application. The Applicant is responsible for any data provided to TrustAsia CA by itself or its authorized representative. TrustAsia CA maintains an internal database containing all previously revoked certificates and rejected certificate requests suspected of phishing or other fraudulent use, and uses this database to identify subsequent suspicious requests.

A VMC certificate application must be submitted by an authorized Certificate Requester and approved by a Certificate Approver. The certificate application must be accompanied by a Subscriber Agreement signed (in writing or electronically) by the Contract Signer.

4.1.2 Enrollment Process and Responsibilities

1. The enrollment process includes:
    - Submitting a certificate application;
    - Generating a key pair;
    - Providing the public key of the key pair (a signed CSR) to TrustAsia CA;
    - Agreeing to the applicable Subscriber Agreement;
    - Paying any applicable fees.
2. Responsibilities:
    - The Applicant should understand in advance the matters stipulated in documents such as the Subscriber Agreement and this CP&CPS, especially the contents regarding the certificate’s scope of application, rights, obligations, and warranties.
    - The Subscriber is responsible for providing TrustAsia CA with authentic, complete, and accurate certificate application information and materials.
    - The Registration Authority is responsible for checking and reviewing the certificate application information and identity proof materials provided by the Subscriber.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication

After TrustAsia CA receives a Subscriber’s certificate application, the TrustAsia CA validation team will perform identification and authentication of the Subscriber’s identity in accordance with the requirements of Chapter 3.2 of this CP&CPS. TrustAsia CA will maintain systems and processes to sufficiently verify the Applicant’s identity according to the CP&CPS. The content of communications

via phone, fax, or email will be securely stored along with all information directly provided by the Applicant through the TrustAsia CA WEB interface or API.

The Applicant information must contain at least one Fully Qualified Domain Name, which will be included in the Subject Alternative Name extension of the certificate.

For information in a Common Mark Certificate, if the data or proof document obtained by TrustAsia CA from the sources specified in Chapter 3.2 of this CP&CPS is not more than 398 days old and the information has not changed, TrustAsia CA may use that data or proof document; for a Verified Mark Certificate, if the data or proof document obtained by TrustAsia CA from the sources specified in Chapter 3.2 of this CP&CPS is not more than 1858 days old and the information has not changed, TrustAsia CA may use that data or proof document.

There is an exception to the above 398-day validation data reuse: TrustAsia CA maintains an up-to-date authorized representative system authorized by Subscribers. As long as the authorized representatives in this system maintain direct contact with TrustAsia CA during the certificate's validity period, there is no need to re-verify the Subscriber.

4.2.2 Approval or Rejection of Certificate Applications

TrustAsia CA does not issue certificates containing Internal Names or reserved IP addresses.

4.2.2.1 Approval of Certificate Applications

After TrustAsia CA successfully completes the necessary confirmation steps for a certificate application, it approves the certificate application by issuing the official certificate.

TrustAsia CA may approve a certificate application if the following conditions are met:

1. The application fully meets the provisions of Chapter 3.2 of the CP&CPS regarding Subscriber identification and authentication;
2. The Subscriber accepts or does not object to the contents and requirements of the Subscriber Agreement;
3. The Subscriber has paid the corresponding fees as required.

4.2.2.2 Rejection of Certificate Applications

TrustAsia CA has the right to reject a certificate application under the following circumstances:

1. The application does not meet the provisions of Chapter 3.2 of this CP&CPS regarding Subscriber identification and authentication;
2. The Subscriber cannot provide the required identity proof materials as requested;
3. The Subscriber objects to or cannot accept the relevant contents and requirements of the Subscriber Agreement;
4. The Subscriber has not paid or cannot pay the corresponding fees as required;
5. The applied certificate contains a new gTLD (generic top-level domain) under consideration by ICANN (The Internet Corporation for Assigned Names and Numbers);

6. The usage of the Subscriber's certificate does not comply with local laws and regulations;
7. TrustAsia CA believes that approving the application will bring disputes, legal issues, or losses to TrustAsia CA;
8. The public key length, algorithm, or other factors in the submitted application present security risks.

For rejected certificate applications, TrustAsia CA will notify the Subscriber via email that the certificate application failed.

4.2.3 Time to Process Certificate Applications

Under normal circumstances, TrustAsia CA will verify the Subscriber's information and issue the certificate within a reasonable time frame. Unless otherwise agreed with the relevant Subscriber or stated in other agreements, no specific processing time is stipulated for completing a certificate application.

The certificate processing time largely depends on when the Subscriber provides the detailed information and documents required to complete the verification and whether they respond to TrustAsia CA's management requirements in a timely manner. The certificate application request remains valid until it is rejected.

4.2.4 CAA Records

For Mark Certificates, prior to certificate issuance, a DNS CAA record check is performed for all domain names in the alternative names of the certificate application.

TrustAsia CA processes the "issuevmc" and "iodef" property tags in CAA records in accordance with the provisions of the MCR.

When processing property tags in CAA records, TrustAsia CA will not act upon the contents of the "iodef" property tag. TrustAsia CA recognizes critical tags, but if it encounters an unrecognized property set in a critical tag, it will refuse to issue the certificate.

If an "issuevmc" tag is present in the CAA record and its value does not contain "trustasia.com", TrustAsia CA will refuse to issue the corresponding certificate.

TrustAsia CA may still issue a certificate if the CAA query fails under the following circumstances:

1. The CAA query failure is not caused by TrustAsia CA's infrastructure, and
2. TrustAsia CA has retried the query at least once, and
3. There is no DNSSEC validation chain pointing to the ICANN root zone for the domain in question.

TrustAsia CA will issue the certificate to the Subscriber within the validity period of the queried CAA record (the validity period is the TTL of the CAA record or 8 hours, whichever is greater); it will also log in detail any potential issuances blocked by CAA records.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

For Subscriber certificates, TrustAsia CA confirms the source of the certificate request before issuance. Before issuing a Mark Certificate, a precertificate of that certificate will be logged into one or more approved Certificate Transparency logs.

During the issuance process, the RA administrator is responsible for approving the certificate application and sending the certificate issuance request to the CA's certificate issuance system by operating the RA system. The certificate issuance request information sent by the RA to the CA must have RA identity authentication and information confidentiality measures to ensure that the request is sent to the correct CA certificate issuance system. After receiving the certificate issuance request, the CA certificate issuance system authenticates and decrypts the information from the RA.

The Root CA's certificate issuance process involves a manual, explicit command issued by an individual authorized by TrustAsia CA (CA system operator, system administrator, or PKI administrator) so that the Root CA performs the certificate signing operation.

TrustAsia CA does not directly issue end-entity certificates from its Root Certificates.

Database storage and CA processes occurring during certificate issuance are protected against unauthorized modification.

For a valid certificate issuance request, the CA certificate issuance system sends it to the Subscriber.

TrustAsia CA deploys multi-factor authentication for all accounts capable of directly issuing certificates.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

TrustAsia CA provides the certificate in any secure manner within a reasonable time after issuance. Usually, TrustAsia CA will email the certificate to the email address specified by the Subscriber during the application process.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

The Subscriber is solely responsible for installing the issued certificate on the Subscriber's computer or hardware security module.

Actions by which a Subscriber is deemed to have accepted the issued certificate include, but are not limited to:

1. The Subscriber independently accessing the dedicated TrustAsia CA certificate service website, downloading the certificate to a digital certificate carrier, and completing the download.
2. With the Subscriber's permission, TrustAsia CA downloading the certificate on behalf of the

Subscriber and sending it to the Subscriber via a secure carrier.

3. After a certificate acquisition notification is sent to the Subscriber, the Subscriber downloads the certificate via that notification.
4. The Subscriber accepts the method of obtaining the certificate and does not raise objections to the certificate or its contents.

4.4.2 Publication of the Certificate by the CA

TrustAsia CA considers the delivery of the certificate to the Subscriber as the publication of the certificate. Depending on the usage scenario of the Subscriber's certificate and according to the requirements of the BIMI Group MCR, TrustAsia CA will also choose to publish the certificate in one or more recognized CT log servers.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

TrustAsia CA will not notify other entities.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

The Mark Certificate Subscriber's private key requires no protection and may be discarded after use, as the public key is solely used to identify the mark representation and is not used to encrypt communications.

4.5.2 Relying Party Public Key and Certificate Usage

Relying Parties should consider the overall situation and the risk of loss before relying on a certificate.

When a Relying Party receives information loaded with a digital signature, it is obligated to perform the following confirmation operations:

1. Obtain the certificate and trust chain corresponding to the digital signature;
2. Verify the validity period of the certificate to ensure the certificate is used within its validity period;
3. Confirm that the certificate corresponding to the signature is a certificate trusted by the Relying Party;
4. Confirm whether the certificate corresponding to the signature has been revoked by checking the CRL or OCSP;
5. Ensure the certificate's usage is appropriate for the corresponding signature;
6. Use the public key on the certificate to verify the signature;
7. Consider other information stipulated in this CP&CPS or elsewhere.

If the above conditions are not met, the Relying Party is responsible for rejecting the signed

information.

4.6 Certificate Renewal

4.6.1 Circumstance for Certificate Renewal

For Subscriber certificates issued by TrustAsia CA, certificate renewal can be performed before the certificate expires. The Subscriber may choose to retain the original key pair for certificate re-issuance. Before the certificate expires, TrustAsia CA will notify the Subscriber via email to renew the certificate.

If the Subscriber does not change the Certificate Subject DN and relevant identity information when submitting a certificate renewal request, and the original certificate's validation time limit has not exceeded the period specified in Section 4.2.1 of this CP&CPS, TrustAsia CA may refer to the data and proof documents verified for the original certificate to validate the information for the renewed certificate.

If the Subscriber needs to change some certificate information when submitting a certificate renewal request, or if the original certificate's validation time limit has exceeded the period specified in Section 4.2.1 of this CP&CPS, TrustAsia CA will perform validation according to the procedures and requirements for an initial certificate application.

If the Subscriber's original certificate has already expired, applying for a certificate again will be validated according to the procedures and requirements for an initial certificate application.

4.6.2 Who May Request Renewal

The entity requesting certificate renewal is a Subscriber who has already applied for a TrustAsia CA certificate or their authorized representative.

4.6.3 Processing Certificate Renewal Requests

For certificate renewal, the processing includes application identification and authentication, certificate information validation, and certificate issuance.

1. The identification and authentication of the application must be based on the following aspects:

a. The Subscriber's original certificate exists and was issued by TrustAsia CA;

b. The certificate renewal request is within the permitted time limit;

c. The Subscriber can submit sufficient information to identify the original certificate, such as the Subscriber DN, certificate serial number, etc.

2. For the certificate information validation process, TrustAsia CA will process it in accordance with the provisions of Section 3.3.1 of this CP&CPS; TrustAsia CA may also choose to validate it according to the general initial certificate application process based on the specific circumstances of the Subscriber's certificate renewal application.
3. Only after all the above identification and authentication have passed can TrustAsia CA approve the issuance of the certificate.

4.6.4 Notification of New Certificate Issuance to Subscriber

Same as Section 4.3.2 of the CP&CPS.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Same as Section 4.4.1 of the CP&CPS.

4.6.6 Publication of the Renewal Certificate by the CA

Same as Section 4.4.2 of the CP&CPS.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

Same as Section 4.4.3 of the CP&CPS.

4.7 Certificate Re-key

4.7.1 Circumstance for Certificate Re-key

When the Subscriber's certificate encounters the following circumstances, the Subscriber may choose the certificate key update service:

1. The Subscriber's certificate (file) is lost or compromised, or the Subscriber believes the original certificate and key are insecure;
2. The Subscriber's certificate needs to use a different key pair;
3. The Subscriber needs to obtain certificates of multiple algorithms (RSA, ECC);
4. The Subscriber's certificate is about to expire and they believe the key needs to be updated when renewing the certificate;
5. Other circumstances that may lead to a key update.

4.7.2 Who May Request Certification of a New Public Key

The entity requesting a certificate key update is a Subscriber who has already applied for a TrustAsia CA certificate and whose certificate has not expired, or their authorized representative.

4.7.3 Processing Certificate Re-keying Requests

TrustAsia CA processes certificate key update requests through the certificate renewal request processing workflow, as described in Section 4.6.3 of this CP&CPS.

4.7.4 Notification of New Certificate Issuance to Subscriber

Same as Section 4.3.2 of the CP&CPS.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

Same as Section 4.4.1 of the CP&CPS.

4.7.6 Publication of the Re-keyed Certificate by the CA

Same as Section 4.4.2 of the CP&CPS.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

Same as Section 4.4.3 of the CP&CPS.

4.8 Certificate Modification

4.8.1 Circumstance for Certificate Modification

Certificate modification may be initiated when non-subject information of the certificate changes.

4.8.2 Who May Request Certificate Modification

The entity requesting a certificate modification is a Subscriber who has already applied for a TrustAsia CA certificate and whose certificate has not expired, or their authorized representative.

4.8.3 Processing Certificate Modification Requests

If the following conditions are met, a replacement certificate is issued based on a previously validated certificate request, provided the referenced certificate was not revoked due to fraud or other illegal acts:

1. The validity period of the replacement certificate is the same as the validity period of the replaced MC, and
2. The subject information of the certificate is the same as the subject information in the replaced MC.

4.8.4 Notification of New Certificate Issuance to Subscriber

Same as Section 4.3.2 of the CP&CPS.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Same as Section 4.4.1 of the CP&CPS.

4.8.6 Publication of the Modified Certificate by the CA

Same as Section 4.4.2 of the CP&CPS.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Same as Section 4.4.3 of the CP&CPS.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

4.9.1.1 Reasons for Revoking a Subscriber Certificate

TrustAsia CA lists the above revocation reasons in the Subscriber Agreement and provides an explanation of when to choose each option. The revocation tool TrustAsia CA provides to Subscribers allows them to specify a reason themselves. When the Subscriber does not select one, the default value is "unspecified (0)", and in this case, no "reasonCode" extension is provided in the CRL.

1. If one or more of the following circumstances occur, TrustAsia CA will revoke the certificate within 24 hours and use the corresponding CRLReason:

a. The Subscriber requests in writing that the CA revoke the certificate;

b. The Subscriber notifies TrustAsia CA that the original certificate request was not authorized and is not retroactively granted;

c. TrustAsia CA obtains evidence that validation of domain authorization or control for any Fully-Qualified Domain Name or IP address in the certificate should not be relied upon.

2. If one or more of the following circumstances occur, TrustAsia CA should revoke the certificate within 24 hours and MUST revoke the certificate within 5 days, and use the corresponding CRLReason:

a. TrustAsia CA is made aware that the certificate no longer complies with the relevant requirements of Sections 6.1.5 and 6.1.6 of the BR;

b. TrustAsia CA obtains evidence that the certificate was misused;

c. TrustAsia CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or CP&CPS;

d. TrustAsia CA is made aware of any circumstance indicating that use of a FQDN or email 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, or the official email address in the certificate is no longer legally used by the Subscriber);

e. TrustAsia CA is made aware of a material change in the information contained in the certificate;

f. TrustAsia CA is made aware that the certificate was not issued in accordance with TrustAsia CA’s CP&CPS;

g. TrustAsia CA determines that any of the information appearing in the certificate is inaccurate, false, or misleading;

h. TrustAsia CA's right to issue certificates under the BIMI Group MCR expires or is revoked or terminated, unless TrustAsia CA has made arrangements to continue maintaining the CRL/OCSP repository;

i. In addition to the circumstances described in this Section 4.9.1.1, the Subscriber's certificate is revoked in accordance with TrustAsia CA's CP&CPS requirements;

j. TrustAsia CA receives an infringement court order, confirms the authenticity of the court order, and provides the Subscriber with 3 business days' notice;

k. The fulfillment of duties under the CP&CPS is delayed or hindered by force majeure; natural disasters; computer or communication failures; changes in laws, regulations, or other legal provisions; government acts; or other reasons beyond personal control that pose a threat to the information of others;

l. The Subscriber has not paid the service fee after TrustAsia CA has fulfilled its obligation to demand payment.

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

If one or more of the following circumstances occur, TrustAsia CA shall revoke the Subordinate CA certificate within 7 days:

1. The Subordinate CA certificate issuing agency formally requests revocation in writing;
2. The Subordinate CA certificate issuing agency discovers and notifies TrustAsia CA that the initial certificate request was unauthorized and not retroactively granted;
3. TrustAsia CA obtains evidence proving that the Subordinate CA private key corresponding to the public key in the certificate has been compromised, or no longer complies with the relevant requirements of Sections 6.1.5 and 6.1.6 of the BR;
4. TrustAsia CA obtains evidence that the certificate was misused;
5. TrustAsia CA is made aware that the Subordinate CA certificate was not issued in accordance with BR requirements, or that the Subordinate CA has not complied with the CP&CPS;
6. TrustAsia CA determines that any of the information appearing in the Subordinate CA certificate is inaccurate, false, or misleading;
7. TrustAsia CA ceases operations for any reason and has not made an agreement with another CA to provide certificate revocation services;
8. TrustAsia CA's right to issue certificates under the BR expires or is revoked or terminated, unless TrustAsia CA has made arrangements to continue maintaining the CRL/OCSP repository;
9. This CP&CPS requires the revocation of the Subordinate CA certificate.

4.9.2 Who Can Request Revocation

The entities that can request certificate revocation are the Subscriber, TrustAsia CA, or judicial personnel authorized by judicial agencies. In addition, Relying Parties, Application Software Suppliers, Conflicting Trademark Owners, or other third parties may submit Certificate Problem Reports informing TrustAsia CA of reasonable grounds to revoke a certificate.

4.9.3 Procedure for Revocation Request

4.9.3.1 Subscriber Proactively Requests Revocation

1. The Subscriber submits a certificate revocation application and relevant identity proof materials to TrustAsia CA; the application materials must state the reason for revocation;
2. TrustAsia CA authenticates the certificate revocation request in accordance with the provisions of Section 3.4 of this CP&CPS;
3. After completing the revocation work, TrustAsia CA should promptly publish it to the Certificate Revocation List;
4. After the certificate is revoked, TrustAsia CA will notify the Subscriber by email or other appropriate means. If the Subscriber cannot be contacted, TrustAsia CA may, if necessary, announce the revoked certificate on its website;
5. TrustAsia CA provides a 24/7 certificate revocation application service. Subscribers can apply for certificate revocation through the contact information provided in Section 1.5.2 of this CP&CPS.

4.9.3.2 Mandatory Certificate Revocation

1. When TrustAsia CA has sufficient reason to believe that a circumstance leading to mandatory revocation of a Subscriber certificate as described in Section 4.9.1.1 of this CP&CPS has occurred, TrustAsia CA will apply for certificate revocation through an internal process;
2. When a security risk occurs with the private key corresponding to TrustAsia CA's Root Certificate or Subordinate CA Certificate, TrustAsia CA may directly revoke Subscriber certificates after approval from the national electronic certification service authority;
3. When a Relying Party, judicial agency, Application Software Supplier, Conflicting Trademark Owner, or third party submits a Certificate Problem Report, TrustAsia CA should organize an investigation and decide whether to revoke the certificate based on the investigation results;
4. After the certificate is revoked, TrustAsia CA will notify the end Subscriber that the certificate has been revoked and the reason for revocation through appropriate means, including email, phone, etc.; if the Subscriber cannot be contacted, TrustAsia CA may, if necessary, announce the revoked certificate on its website;
5. TrustAsia CA provides a 24/7 Certificate Problem Report and handling service. Relevant parties can report problems through the contact information provided in Section 1.5.2 of this CP&CPS.

4.9.4 Revocation Request Grace Period

TrustAsia CA does not support a revocation request grace period.

4.9.5 Time Within Which CA Must Process the Revocation Request

Within 24 hours after receiving a revocation request, TrustAsia CA will investigate the facts and circumstances related to the revocation request and provide a preliminary investigation report to the Subscriber and the entity that submitted the revocation request. For infringement court orders, TrustAsia CA will verify the facts and take action within a commercially reasonable timeframe.

After reviewing the facts and circumstances, the CA will work with the Subscriber and the entity that escalated the preliminary report on the certificate or other revocation-related entities to determine whether to revoke the certificate or take other reasonable handling actions. If it is determined to revoke, the time from when the CA receives the revocation request or revocation-related notification to the publication of the revocation will not exceed the time frames specified in Section 4.9.1.1.

For the time of revocation, the CA will consider the following criteria:

1. The nature of the problem (scope, background, severity, magnitude, risk of harm);
2. The consequences of revocation (direct and collateral impact on Subscribers and Relying Parties);
3. The number of revocation requests received concerning a particular certificate or Subscriber;
4. The entity making the complaint (for example, a complaint from a law enforcement official that a website is engaged in illegal activities takes precedence over a consumer complaining that they did not receive the goods they ordered); and
5. Relevant legislation.

4.9.6 Revocation Checking Requirement for Relying Parties

As public information, the Certificate Revocation List (CRL) does not have security settings for read access. Relying Parties are free to query as needed, including querying the Certificate Revocation List, querying the certificate status through TrustAsia CA's designated website, and querying via the Online Certificate Status Protocol (OCSP).

Before trusting this certificate, Relying Parties should proactively check the status of the certificate according to the latest CRL published by TrustAsia CA, and must also verify the reliability and integrity of the CRL to confirm the validity of the certificate.

4.9.7 CRL Issuance Frequency

The CRL can be accessed via a public HTTP URL. Within 24 hours of issuing the first certificate, the CA will produce and publish:

- A complete CRL, or
- CRL partitions which, when aggregated, can recover the complete CRL.

For CAs that issue Subscriber certificates:

1. Update and publish a new CRL at least every 7 days, with the maximum validity period of the CRL not exceeding 10 days;
2. Update and publish a new CRL within 24 hours after a certificate is revoked.

For CAs that issue CA certificates:

1. Update and publish a new CRL at least every 12 months;
2. Update and publish a new CRL within 24 hours after a certificate is revoked.

The CA will continue to publish the CRL until the following occurs:

- All CA certificates containing the same subject public key have expired or been revoked; or
- The corresponding CA private key is destroyed.

4.9.8 Maximum Latency for CRLs

After generation, the TrustAsia CA CRL is automatically published to the public network. Generally, it takes effect within 1 hour, and at most within 24 hours.

4.9.9 On-line Revocation/Status Checking Availability

The valid time interval of an OCSP response is the time difference between the thisUpdate and nextUpdate fields, inclusive. When calculating the time difference, 3,600 seconds equals one hour, and 86,400 seconds equals one day, ignoring leap seconds.

For the following certificate serial number situations, the certificate is marked as "assigned":

1. A certificate or precertificate with that serial number has been issued by the Issuing CA, or
2. A certificate or precertificate with that serial number has been issued by a precertificate signing certificate associated with the Issuing CA.

For certificates whose serial number is not marked as "assigned", they are marked as "unassigned".

The following applies to certificates and precertificates containing an Authority Information Access extension with the id-ad-ocsp access method.

The OCSP request service provided by TrustAsia CA supports both GET and POST methods. TrustAsia CA processes the Nonce extension (1.3.6.1.5.5.7.48.1.2) in accordance with the provisions of RFC 8954.

For the status of Subscriber or Pre-signed certificates:

- Provide a correct OCSP response no later than 15 minutes after the certificate or precertificate is first published or otherwise made available;
- If the valid time interval of the OCSP response is less than sixteen hours, TrustAsia CA updates the information provided via the Online Certificate Status Protocol before half of the validity period prior to nextUpdate has passed;

If the valid time interval of the OCSP response is greater than or equal to sixteen hours, TrustAsia CA updates the information provided via the Online Certificate Status Protocol at least eight hours before nextUpdate and no later than four days after thisUpdate. The valid time interval for Subscriber certificate OCSP responses is greater than or equal to eight hours and less than or equal to ten days.

For the status of Subordinate CA certificates:

TrustAsia CA updates the information provided via the Online Certificate Status Protocol at least every twelve months; and updates the information within 24 hours after revoking a Subordinate

CA certificate.

The following applies to the certificate status to which the OCSP responder is required to respond.

The OCSP responses provided by TrustAsia CA comply with RFC 6960 and/or RFC 5019. The OCSP response meets either of the following conditions:

1. Signed by the CA that issued the certificate whose revocation status is being checked, or
2. Signed by an OCSP Responder whose certificate is signed by the CA that issued the certificate whose revocation status is being checked.

If the OCSP responder receives a certificate status request for an "unassigned" serial number, the responder does not respond with a "good" status.

4.9.10 On-line Revocation Checking Requirements

Consistent with RFC 6960.

4.9.11 Other Forms of Revocation Advertisements Available

Not applicable.

4.9.12 Special Requirements Regarding Key Compromise

If a Subscriber or TrustAsia CA discovers or suspects that a private key has been compromised, immediate measures should be taken to revoke the certificate with the compromised key and reissue the certificate according to the CP&CPS requirements.

Any Relying Party who discovers a private key compromise may report it to TrustAsia CA via email (revoke@trustasia.com). The email must provide evidence of the private key compromise:

1. The private key itself;
2. A CSR signed with the compromised private key, with the Common Name of the CSR being "Proof of Private Key Compromise for TrustAsia";
3. Proof of private key compromise through the certificate revocation method of the ACME protocol defined in Section 7.6 of RFC 8555.

4.9.13 Circumstances for Suspension

TrustAsia CA does not support certificate suspension.

4.9.14 Who Can Request Suspension

Not applicable.

4.9.15 Procedure for Suspension Request

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

Certificate status information is available via CRL and OCSP responses.

For revoked certificates, TrustAsia CA does not remove their revocation records from the CRL and OCSP before the certificate expires.

4.10.2 Service Availability

The certificate status service is provided 24/7. TrustAsia CA operates and maintains its CRL and OCSP capabilities with sufficient resources to provide a response time of 10 seconds or less under normal operating conditions.

TrustAsia CA responds 24/7 to high-priority certificate problem reports. Where appropriate, TrustAsia CA will forward such issues to law enforcement agencies and revoke the subject certificates associated with such issues.

4.10.3 Optional Features

The OCSP responder may not be applicable to all certificate types.

4.11 End of Subscription

TrustAsia CA develops, implements, and maintains a comprehensive security program designed to:

1. Protect the confidentiality, integrity, and availability of certificate data and the certificate management process;
2. Prevent anticipated threats or hazards to the confidentiality, integrity, and availability of certificate data and the certificate management process;
3. Prevent unauthorized or illegal access, use, disclosure, alteration, or destruction of any certificate data or the certificate management process;
4. Prevent accidental loss, destruction, or damage of any certificate data or the certificate management process; and
5. Comply with all other security requirements applicable to the CA under the law.

TrustAsia CA's certificate management process includes:

1. Physical security and environmental controls;
2. System integrity controls, including configuration management, maintenance of trusted code integrity, and malware detection/prevention;

3. Network security and firewall management, including port restrictions and IP address filtering;
4. User management, separation of trusted roles, education, awareness, and training; and
5. Logical access controls, activity logging, and inactivity timeouts to provide individual accountability.

TrustAsia CA's security program includes an annual risk assessment, which:

1. Identifies foreseeable internal and external threats that could lead to unauthorized access, disclosure, misuse, alteration, or destruction of any certificate data or the certificate management process;
2. Evaluates the likelihood and potential damage of these threats, taking into consideration the sensitivity of the certificate data and the certificate management process; and
3. Assesses the adequacy of the policies, procedures, information systems, technologies, and other arrangements established by the CA to counter such threats.

Based on the risk assessment, TrustAsia CA develops, implements, and maintains a security program consisting of security procedures, measures, and products designed to achieve the above objectives and manage and control the risks identified during the risk assessment, commensurate with the sensitivity of the certificate data and the certificate management process. The security program includes administrative, organizational, technical, and physical safeguards appropriate for the sensitivity of the certificate data and the certificate management process. The security program also takes into account the technology available at the time and the cost of implementing specific measures, and should implement a reasonable level of security appropriate for the harm that could result from security vulnerabilities and the nature of the protected data.

5.1 Physical Controls

5.1.1 Site Location and Construction

The construction of TrustAsia CA's computer rooms and systems is implemented in accordance with the following standards:

1. "Technical Requirements for Computer Sites" (GB 2887-89)
2. "Code for Design of Electronic Information System Rooms" (GB 50174-2008)
3. "Code for Fire Protection Design of Interior Decoration of Buildings" (GB50222-95)
4. "Code for Design of Low Voltage Electrical Installations" (GBJ50054-95)
5. "Technical Requirements and Testing Methods for Electromagnetic Shielding Enclosures for Processing Classified Information" Class C (BMB3-1999)
6. "General Specification for Electronic Computer Sites" (GB/T 2887-2011)
7. "Design Code for Protection of Structures against Lightning" (GB/50057-2010)

5.1.1.1 Public Area

The entrance and power distribution of TrustAsia CA's site are located in this area. Access control measures are adopted, requiring the use of an access card or fingerprint authentication to enter.

5.1.1.2 Management Service Area

The service area is the workspace for TrustAsia CA operators and management personnel. Entry requires two trusted persons using access cards and fingerprint authentication simultaneously. Entry and exit of personnel in the service area are logged.

5.1.1.3 Core Area

The core area is the CA operational management area. This area can only be entered using an access card and fingerprint authentication.

At the same time, the certificate authentication system, cryptographic equipment, and other related cryptographic items are also stored in this area. The CA server, database system, cryptographic equipment, and other related cryptographic items are located within a shielded room inside the core area. The shielded room requires two trusted persons to use access cards and fingerprint authentication simultaneously to enter, ensuring that no single person can complete sensitive operations within the shielded area.

There is a separate buffer zone inside the shielded area to prevent electromagnetic waves from leaking when the shielded door is opened.

5.1.2 Physical Access

The TrustAsia CA data center has installed an access control system with the following functions:

1. Uses access cards and fingerprint authentication to control entry through each door;
2. Logs entry and exit through every door;
3. Both the management service area and core area doors are equipped with forced entry and timeout alarms;
4. The entire access control system is connected to a UPS, which provides emergency power when utility power is interrupted.

The entire area also has a video surveillance system with no blind spots, providing 24/7 continuous recording of important passages inside and outside the site. All video data is kept for at least 3 months, and videos of major incidents are archived separately for future inquiry. Intrusion detection alarms, environmental control detection alarms, and audible/visual alarms are installed, while simultaneously notifying operations and maintenance personnel.

5.1.3 Power and Air Conditioning

TrustAsia CA has a secure and reliable power supply system and a dual-feed backup power system to ensure 24/7 normal power supply for the system and provide normal service in the event of a power interruption. In addition, dedicated diesel generators are used, which can provide more than 12 hours of endurance for all racks in the new computer room at full load.

The computer room has an air conditioning system to control the temperature and humidity in the operating facility. The power is configured according to the number of racks in each room and equipment at full load.

5.1.4 Water Exposures

TrustAsia CA's computer room is elevated 1.45 meters above the ground and is equipped with a water leak alarm system. In the event of a flood, the system will immediately issue an alarm and notify relevant personnel to take emergency measures.

5.1.5 Fire Prevention and Protection

The fire alarm system of TrustAsia CA's computer room uses a cabinet-type Heptafluoropropane automatic fire extinguishing device. The system collects fire data through temperature and smoke sensors installed in the computer room, while also supplying the system to process alarm data from user automatic fire alarm terminals and system operational status data in real-time.

System management is divided into manual mode and automatic mode, enabling real-time detection and monitoring of the network system, setting manual and automatic control modes, and completing various associated linkage actions designed for the system.

5.1.6 Media Storage

TrustAsia CA stores media containing audit, archive, and backup information in secure facilities protected by physical access controls. Only authorized personnel are allowed access, and at least two trusted persons must be present. A media usage registry is used to record the status of the media, and measures are taken to prevent accidental damage to the media.

5.1.7 Waste Disposal

TrustAsia CA shreds unused paper documents and data CDs, rendering the information unrecoverable. Before cryptographic equipment is disposed of, it is initialized and physically destroyed according to the method provided by the equipment manufacturer.

When processing obsolete content, at least two trusted persons must be present.

5.1.8 Off-Site Backup

TrustAsia CA uses offline media to back up critical data and audit log data and transports it to an off-site location for storage. The storage facility meets the description for media storage in Section 5.1.6.

5.2 Procedural Controls

5.2.1 Trusted Roles

During the process of providing electronic certification services, TrustAsia CA considers positions involving key operations that can substantially affect the issuance, use, management, and revocation of certificates as trusted roles. These roles include, but are not limited to:

1. Authentication and Customer Service Personnel: Responsible for entering Subscriber information, verifying digital certificate application information, completing authentication, approval, and revocation operations, and providing related support services;

2. Key and Cryptographic Equipment Management Personnel: Responsible for maintaining CA keys and the certificate lifecycle, and managing cryptographic equipment;
3. System Maintenance Personnel: Responsible for performing routine maintenance on the hardware and software of the CA system, and monitoring and troubleshooting faults;
4. Security Management Personnel: Responsible for site security and daily security management work;
5. Security Audit Personnel: Responsible for auditing business operations;
6. Human Resources Management Personnel: Responsible for conducting trustworthiness background checks, security management, and other work for personnel in critical positions.

Trusted roles are appointed by management. The list of personnel appointed to trusted roles is maintained and reviewed annually.

5.2.2 Number of Persons Required per Task

TrustAsia CA strictly controls critical tasks within its specific operational specifications. The following sensitive operations require multiple trusted roles to be completed collaboratively, for example:

1. Access to the Shielded Area: Set to a two-trusted-person access mode;
2. Authentication, Review, and Issuance of Certificates: Requires two trusted persons to complete collaboratively;
3. Safes Storing Root Key Activation Data: Set to a two-trusted-person opening mode;
4. Operation and Storage of CA Keys and Cryptographic Equipment: Requires 3 out of 5 trusted persons to complete collaboratively;
5. CA System Backend Operations: Requires two trusted persons to complete collaboratively;
6. Operation and Maintenance of Important System Data: Requires at least 1 person to operate and 1 person to supervise and record.

5.2.3 Identification and Authentication for Each Role

Before TrustAsia CA allows any personnel to access and execute the systems necessary for their trusted roles, they are required to authenticate to the CA and RA systems. For example:

1. For physical access by trusted personnel, authentication is performed via access cards and fingerprint recognition, and corresponding permissions are determined.
2. For trusted personnel managing the Subscriber certificate lifecycle, certificate management tasks are performed by accessing the system using the corresponding digital certificates.
3. For system maintenance personnel, they use their respective accounts and passwords to log into the system via a bastion host for maintenance work.

5.2.4 Roles Requiring Separation of Duties

To ensure system security, TrustAsia CA adheres to the principle of separation of trusted roles,

meaning TrustAsia CA's trusted roles are held by different individuals. For MC Certificates, TrustAsia CA ensures that no single person can independently verify and authorize the issuance of such certificates, and such controls are auditable.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

The qualification requirements for TrustAsia CA staff holding trusted roles are as follows:

1. Possess a good social and professional background.
2. Abide by national laws and regulations, and have no criminal record.
3. Comply with TrustAsia CA's specifications, regulations, and systems regarding security management.
4. Possess a conscientious and responsible work attitude and good professional experience.
5. Possess good teamwork spirit.
6. Staff in critical and core positions must have relevant work experience or pass TrustAsia CA's related training and assessments before taking up the post.

5.3.2 Background Check Procedures

TrustAsia CA, or in cooperation with relevant government departments and investigation agencies, completes background checks on trusted employees. All trusted employees and trusted employees transferring in must provide written consent to undergo a background check. The background check must comply with the requirements of laws and regulations; the content, methods, and personnel conducting the investigation must not violate laws and regulations. The background check should use legal means to verify the individual's background information as much as possible through relevant organizations and departments.

Background checks are divided into: basic investigations and comprehensive investigations. Basic investigations include checks on work experience, professional references, education, and social relations. Comprehensive investigations include basic investigation items as well as checks on criminal records, social relations, and social security. Personnel in critical positions for public trust certificate businesses must undergo comprehensive investigations.

The Human Resources Department investigation procedures include:

1. Confirming the personal information of the candidate. The following materials are provided: resume, highest education diploma, degree certificate, qualification certificate, ID card, and other relevant valid proofs.
2. Authenticating the truthfulness of the materials provided via phone, internet, etc.
3. During the background check, if an individual is found to have any of the following circumstances, their qualification to become a trusted person may be directly rejected:
    - Falsifying facts or materials;
    - Using testimonies from unreliable persons;

- Using illegal identity proofs, or educational/professional qualification proofs;
- Exhibiting severely dishonest behavior at work.

4. After completing the investigation, the results are reported to the relevant leadership in charge for approval.
5. TrustAsia CA signs confidentiality agreements with employees to restrict them from disclosing any confidential and sensitive information regarding CA certificate services. Meanwhile, positional evaluations are conducted for all active personnel holding trusted roles to continuously verify their trustworthiness and work capability.

5.3.3 Training Requirements

TrustAsia CA provides appropriate pre-job training according to the position requirements of trusted roles and keeps records of employees' training participation in files. These trainings include:

1. Basic Public Key Infrastructure (PKI) knowledge;
2. CP&CPS and relevant standards and procedures;
3. Identity authentication and validation policies and procedures;
4. Security management policies and mechanisms;
5. Disaster recovery and business continuity procedures;
6. Unified requirements for job responsibilities;
7. CA/Browser Forum BR, EVG, and other guidelines;
8. National laws, regulations, standards, and procedures regarding electronic certification services;
9. Other necessary training, etc.

Validation personnel performing information validation duties must receive all the above training before taking up their posts to ensure they can satisfactorily perform their duties. Validation personnel must pass related knowledge assessments periodically arranged by TrustAsia CA to ensure they possess the necessary skills to fulfill their duties.

5.3.4 Retraining Frequency and Requirements

Personnel acting in trusted roles or other important roles shall irregularly undergo training organized by TrustAsia CA. For personnel related to certification system operations, relevant skills and knowledge training should reach a level consistent with the job requirements. Furthermore, TrustAsia CA will irregularly require personnel to undergo continuous training based on requirements such as organizational system upgrades and policy adjustments.

5.3.5 Job Rotation Frequency and Sequence

The job rotation cycle and sequence for active personnel at TrustAsia CA will be determined based on the organization’s security management policies.

5.3.6 Sanctions for Unauthorized Actions

When active personnel use TrustAsia CA systems to perform certification business operations without authorization or beyond their authorization, once confirmed, TrustAsia CA will immediately revoke the person's login certificate and terminate their system access permissions. Depending on the severity of the person's unauthorized actions, measures will be implemented, including adjusting the person's job position, circulating a notice of criticism, imposing fines, dismissal, and submitting the matter to judicial agencies for handling.

5.3.7 Independent Contractor Requirements

TrustAsia CA does not currently employ external independent contractors to engage in certification-related work.

5.3.8 Documentation Supplied to Personnel

The documentation TrustAsia CA typically provides to personnel includes, but is not limited to, the following categories:

1. CP&CPS and related standards and specifications;
2. Employee handbook;
3. Job descriptions, workflows, and specifications;
4. Internal operational documents, including business continuity management and disaster recovery plans;
5. Security management systems, etc.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

TrustAsia CA will record the details of actions taken to process certificate applications and issue certificates, including all information generated and documents received related to the certificate application, time and date, and the personnel involved.

If TrustAsia CA's applications cannot automatically log events, manual procedures will be implemented to meet the requirements.

These events include, but are not limited to:

1. CA Certificate and Key Lifecycle Management Events, including:

a. Key generation, backup, storage, recovery, archiving, and destruction;
b. Certificate requests, renewals, key update requests, and revocations;
c. Approval and rejection of certificate applications, including successful or failed certificate operations;
d. Cryptographic equipment lifecycle management events, including: equipment receipt,

installation, uninstallation, activation, usage, maintenance, etc.;

e. Generation of CRL entries;

f. Signing of OCSP responses;

g. Records of introducing new certificate profiles and retiring existing certificate profiles.

2. Subscriber Lifecycle Management Events:

a. Certificate requests, renewals, key update requests, and revocations;

b. All validation activities required by the BIMI Group and stipulated in this CP&CPS;

c. Acceptance and rejection of certificate requests, including acceptance of Subscriber Agreements, verification of application materials, and retention of application and verification materials;

d. Issuance of certificates;

e. Generation of CRL entries;

f. Signing of OCSP responses;

3. Security Events:

a. Successful and unsuccessful PKI system access attempts;

b. Executed PKI and security system actions;

c. Changes to security profiles;

d. Installation, update, and removal of software on the certificate system;

e. System crashes, hardware failures, and other anomalies;

f. Firewall and router activity; and

g. Entry to and exit from CA facilities, including access by authorized and unauthorized personnel to secure storage facilities.

4. System Operation Events, including:

a. System startup and shutdown;

b. Creation and deletion of system privileges, and setting or modification of passwords;

c. Unauthorized access and access attempts to the CA system network;

d. Unauthorized access and access attempts to system files;

e. Reading, writing, or deleting of secure or sensitive files or records;

5. Trusted Personnel Management Records, including:

a. Account application records for network permissions;

b. Application, modification, and creation application records for system permissions;

c. Changes in personnel status.

Logging records generally must include:

1. Date and time of the record;
2. Serial number of the record;
3. Identity of the entity making the log entry;
4. Description of the recorded content.

5.4.1.1 Router and Firewall Activity Logs

TrustAsia CA router and firewall logs include at least:

1. Successful and unsuccessful login attempts to routers and firewalls;
2. Logging of all management operations executed on routers and firewalls, including configuration changes, firmware updates, and access control modifications;
3. Logging of all changes made to firewall rules, including additions, modifications, and deletions;
4. Logging of all system events and errors, including hardware failures, software crashes, and system reboots.

5.4.2 Frequency of Processing Log

Irregularly process the system’s automatic logs and the operators' manual records.

Irregularly process system security logs, track processing, and inspect major events that violate policies and specifications.

5.4.3 Retention Period for Audit Log

TrustAsia CA retains the following logs for at least two years:

1. CA certificate and key lifecycle management event records after the occurrence of the following:

a. CA private key destruction; or
b. The CA field in the X.509v3 Basic Constraints extension of the certificate is set to "TRUE", and the final CA certificate sharing the public key with that CA private key is revoked or expires.

2. Subscriber certificate lifecycle management event records after the revocation or expiration of the Subscriber certificate.
3.
4. Any security event records after an incident occurs.

5.4.4 Protection of Audit Log

TrustAsia CA’s audit logs are stored in a database and backed up; this includes the audit information and event records in the related documents.

TrustAsia CA implements strict physical and logical access control measures to ensure that only authorized personnel can access these audit records, and unauthorized access, reading,

modification, and deletion operations are strictly prohibited.

5.4.5 Audit Log Backup Procedures

TrustAsia CA's system logs are synchronized in real-time to the log server and irregularly backed up to an off-site location; manual paper records are periodically archived and stored in dedicated filing cabinets.

5.4.6 Audit Collection System

Regarding electronic audit information, TrustAsia CA's audit log collection system involves:

1. Certificate Management System;
2. Certificate Issuance System;
3. Certificate Directory System;
4. Telecommunication System;
5. Certificate Acceptance System;
6. Access Control System;
7. Website and Database Security Management Systems;
8. Other systems requiring auditing.

For paper audit information, dedicated filing cabinets are used to achieve collection and archiving.

5.4.7 Notification to Event-Causing Subject

When TrustAsia CA discovers that it is under attack, it will log the attacker's actions, trace the attacker within the scope permitted by law, and reserve the right to take corresponding countermeasures. TrustAsia CA reserves the right to decide whether to notify the entities related to the event.

5.4.8 Vulnerability Assessments

TrustAsia CA performs a risk assessment annually:

1. Identify foreseeable internal and external threats that may cause unauthorized access, disclosure, misuse, alteration, or destruction of any certificate data or certificate management processes;
2. Evaluate the likelihood and potential damage of these threats, considering the sensitivity of the certificate data and certificate management process; and
3. Assess the adequacy of the policies, procedures, information systems, technology, and other arrangements established by TrustAsia CA to address such threats. Based on the risk assessment, develop, implement, and maintain a security program consisting of security procedures, measures, and products designed to achieve the above objectives and manage the risks identified in the risk assessment. The security program includes administrative, organizational, technical, and physical safeguards appropriate for the sensitivity of the

certificate data and certificate management processes. The security plan also considers currently available technology and the cost of implementing specific measures, and implements a reasonable security level appropriate for the damage that a security vulnerability could cause and the nature of the data to be protected.

5.5 Records Archival

5.5.1 Types of Records Archived

In addition to archiving the relevant content in Section 5.4.1, TrustAsia CA also archives and logs the following types of events, including but not limited to:

1. Documents related to the security of its certificate system, certificate management system, Root CA system, and authorized third-party systems; and
2. Documents related to certificate applications and the validation, issuance, and revocation of certificates.

5.5.2 Retention Period for Archive

Archived audit logs (as described in Section 5.5.1) will be retained for at least 2 years from the time their record was created, or the time required by Section 5.4.3, whichever is longer.

Records retained by TrustAsia CA for at least 2 years include:

1. All archived documents specified in Section 5.5.1 related to the security of the certificate system, certificate management system, and Root CA system; and
2. All archived documents related to certificate applications and the validation, issuance, and revocation of certificates (as specified in Section 5.5.1) after the following occurs:

a. Such records and documents are last relied upon for the validation, issuance, or revocation of a certificate request and certificate; or
b. The expiration of the Subscriber certificate relying on such records and documents.

5.5.3 Protection of Archive

TrustAsia CA has secure physical and logical protections for archived documents in both electronic and paper forms. Furthermore, there are strict management procedures to ensure that archived documents are not damaged, preventing unauthorized access, modification, deletion, and other actions.

5.5.4 Archive Backup Procedures

System-generated electronic records are periodically backed up, and the backups are stored off-site in the form of offline media; manual electronic records are collected and backed up on internal storage servers.

Paper documents do not require backup, but strict security measures are taken to ensure their safety and prevent unauthorized access, modification, deletion, and other actions.

5.5.5 Requirements for Time-Stamping of Records

When creating archived records, TrustAsia CA will automatically timestamp them using system time (non-cryptographic method). TrustAsia CA's time source server time is synchronized with a Universal Coordinated Time (UTC) time source recognized by the national measurement institute.

5.5.6 Archive Collection System

System-generated electronic records are synchronized in real-time to the log server and irregularly backed up off-site.

For manual electronic records, the collection and backup work is completed by internal storage servers.

Written archival materials are collected and archived in filing cabinets.

5.5.7 Procedures to Obtain and Verify Archive Information

TrustAsia CA has adopted physical and logical access control methods to ensure that only authorized personnel can access these archived information; unauthorized access, reading, modification, and deletion operations are strictly prohibited.

5.6 Key Changeover

The maximum validity period of TrustAsia CA's Root Certificate does not exceed 25 years. Any certificate issued by it, including CA certificates and Subscriber certificates, will not expire later than the expiration time of the Root Certificate. Any Subscriber certificate issued by a CA certificate will not expire later than the expiration time of the CA certificate.

When the use validity period of the key pair corresponding to the CA certificate exceeds the maximum lifecycle specified in this CP&CPS, TrustAsia CA will initiate the key update process to replace the expired CA key pair. The key changeover proceeds as follows:

1. Before the Parent CA's private key expires prior to the lifecycle of the Subordinate CA's key, the issuance of new Subordinate CA certificates stops ("issuance stop date").
2. After the "issuance stop date", certificates for approved Subordinate CA or Subscriber certificate requests will be issued using the new CA key.
3. Generate a new key pair and issue a new Parent CA certificate.
4. The Parent CA continues to use the original CA private key to issue CRLs until the last certificate issued with the original private key expires.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

TrustAsia CA formulates and records a business continuity plan and disaster recovery plan to notify software suppliers, Subscribers, and Relying Parties in the event of a disaster, security

incident, or business impairment. TrustAsia CA does not publicly disclose the business continuity plan, but it is subject to audit by auditors; these procedures are tested, reviewed, and updated annually. The business continuity plan includes:

1. Conditions for activating the plan.
2. Emergency procedures.
3. Fallback procedures.
4. Recovery procedures.
5. Maintenance schedule for the plan.
6. Awareness and educational requirements.
7. Individual responsibilities.
8. Recovery Time Objective (RTO).
9. Periodic testing of the contingency plan.
10. The CA's plan to maintain or restore CA business operations in a timely manner following an interruption or failure of a critical business process.
11. Requirement to store critical cryptographic materials (i.e., secure cryptographic devices and activation materials) at another location.
12. What constitutes acceptable system interruption and recovery time.
13. How frequently backup copies of critical business information and software are made.
14. The distance of the recovery facility from the primary CA site; and
15. Procedures to secure its facility as much as possible after a disaster and for a period of time before a secure environment is restored at the original or remote site.

5.7.2 Computing Resources, Software, and/or Data Are Corrupted

TrustAsia CA has backed up the resources, software, and data of its business systems and other important systems, and has established corresponding emergency handling processes. When disasters occur such as destruction of network communication resources, inability of computer equipment to provide normal services, software corruption, database tampering, or due to force majeure, TrustAsia CA will implement recovery according to the disaster recovery plan.

5.7.3 Entity Private Key Compromise Procedures

When the private key of TrustAsia CA's Root CA or Subordinate CA is compromised, TrustAsia CA will carry out emergency handling according to the key contingency plan and revoke all certificates issued by that CA.

5.7.4 Business Continuity Capabilities After a Disaster

In the event of a major disaster at the physical site, TrustAsia CA will restore partial services within 48 hours according to the business continuity plan.

5.8 CA or RA Termination

When TrustAsia CA needs to terminate its business, it will strictly follow the provisions of the "Electronic Signature Law of the People’s Republic of China" and related regulations regarding the suspension of business by certification authorities.

Before TrustAsia CA terminates, it must:

1. Designate an organization to take over the business;
2. Draft a TrustAsia CA termination statement;
3. Notify the relevant entities involved in the cessation of operations of TrustAsia CA at least 90 days in advance;
4. Handle archived document records;
5. Stop the services of the Certification Authority;
6. Archive relevant system logs;
7. Process and store sensitive documents.

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

CA key pairs must be generated within a secure physical environment, using cryptographic equipment that complies with FIPS 140-2 Level 3. The generation, management, storage, backup, and recovery of keys comply with the relevant provisions of the FIPS 140-2 standard.

The generation process of CA key pairs is completed in the TrustAsia CA shielded room according to the key generation script prepared by TrustAsia CA in advance, witnessed by multiple key administrators and trusted personnel of TrustAsia CA, as well as qualified independent third-party auditors. The CA key pair generation process and operations must be continuously recorded on video. A qualified independent third-party auditor will issue a report indicating that the processes and controls of TrustAsia CA during the CA key pair generation process can ensure the integrity and confidentiality of the CA key pair.

6.1.1.2 RA Key Pair Generation

Not applicable.

6.1.1.3 Subscriber Key Pair Generation

Not applicable.

6.1.2 Private Key Delivery to Subscriber

Not applicable.

6.1.3 Public Key Delivery to Certificate Issuer

As part of the certificate application process, the Subscriber generates a key pair and submits the public key to TrustAsia CA within a CSR.

6.1.4 CA Public Key Delivery to Relying Parties

TrustAsia CA’s public keys are included in the self-signed Root CA certificates and Subordinate CA certificates issued by TrustAsia CA. Subscribers and Relying Parties can download Root CA certificates and Subordinate CA certificates from TrustAsia CA’s official website.

6.1.5 Key Sizes

To ensure the security strength of the keys, TrustAsia CA uses lint tools for key length detection before issuing certificates to ensure that the keys of different types of TrustAsia CA certificates comply with the following standards:

Certificate Type	Root Certificate	Subordinate Certificate	Subscriber Certificate
Digest Algorithm	SHA384	SHA384	SHA256 or SHA384
RSA Key Length	4096	4096	2048, 3072, or 4096
ECC Curve	P-384	P-384	P-256 or P-384

6.1.6 Public Key Parameters Generation and Quality Checking

Both TrustAsia CA and the Subscriber must generate public keys in accordance with the provisions in Section 6.1.1 of this CP&CPS. The public key parameters are generated by compliant equipment/platforms to ensure the quality of the public key parameters. The public key must meet the requirements in Section 6.1.5 of this CP&CPS.

Before issuing a certificate, TrustAsia CA performs public key parameter detection to ensure the public key parameters satisfy the following:

- For RSA public keys:

1. The public exponent is an odd number greater than or equal to 3.
2. The public exponent range should be between 2^16+1 and 2^256-1.
3. The modulus is an odd number.
4. The modulus length is at least 2048 bits and is an integer multiple of 8.
5. The modulus is not a power of a prime number.
6. The modulus has no factors smaller than 752.
    - For ECDSA public keys:

The validity of all keys is confirmed through a full ECC public key validation routine or a partial ECC public key validation routine.

6.1.7 Key Usage Purposes

The X.509 v3 certificates issued by TrustAsia CA include the key usage extension, which complies with the RFC 5280 standard. For the usages specified by TrustAsia CA in the key usage extension of its issued certificates, the Certificate Subscriber must use the keys according to these specified usages.

Root CA keys are generally used to issue the following certificates and CRLs:

1. Self-signed certificates representing the Root CA;
2. Subordinate CA certificates and cross-certificates, and the sole EKU of these certificates is id-kp-BIMIInternet;
3. OCSP response signing certificates.

Subordinate CA keys are generally used to issue the following certificates and CRLs:

1. Subscriber certificates, and the sole EKU is id-kp-BIMIInternet;
2. OCSP response signing certificates.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

TrustAsia CA implements physical and logical protective measures to prevent unauthorized certificate issuance. For private key backups outside the specified validated systems or equipment mentioned above, TrustAsia CA encrypts and stores the key fragments in physical devices held by different entities to prevent private key compromise. The algorithm and key length used to encrypt the private key fragments are based on current technology, ensuring that the algorithm and key length can withstand cryptanalytic attacks throughout the remaining lifecycle of the encrypted key or key parts.

6.2.1 Cryptographic Module Standards and Controls

The cryptographic modules used by TrustAsia CA for CA key pairs and timestamp key pairs comply with the FIPS 140-2 Level 3 standard.

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

Operations such as generating, updating, revoking, backing up, and restoring TrustAsia CA private keys utilize a multi-person control mechanism. Management authority over the private keys is distributed among 5 key administrators. At least 3 or more key administrators must be present and grant permission by inserting their administrator IC cards or USB Keys and entering their PINs to perform operations on the private keys.

6.2.3 Private Key Escrow

TrustAsia CA will not escrow private keys.

6.2.4 Private Key Backup

See Section 5.2.2 of this CPS. In addition, TrustAsia CA backs up the Root private key and CA private keys. According to the operational specifications provided by the cryptographic equipment manufacturer, backup cipher-text files and backup recovery permission IC cards or USB Keys are generated and stored in the company’s safes (or safe deposit boxes at a bank with a security level no lower than the local backup site).

6.2.5 Private Key Archival

TrustAsia CA does not archive private keys for Subscriber certificates, nor are any CA certificate private keys archived by a third party.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

TrustAsia CA key pairs are generated, stored, and used on hardware cryptographic modules. For

recovery purposes, TrustAsia CA backs up the CA keys under multi-person control according to the operational specifications provided by the cryptographic equipment manufacturer.

Additionally, TrustAsia CA has strict key management processes to control the duplication of CA key pairs. All these effectively prevent the loss, theft, modification, unauthorized disclosure, or unauthorized use of CA private keys.

6.2.7 Private Key Storage on Cryptographic Module

TrustAsia CA private keys are stored in encrypted form in hardware cryptographic modules complying with the FIPS 140-2 Level 3 standard, and the use of the private keys also occurs within the hardware cryptographic modules.

6.2.8 Method of Activating Private Key

TrustAsia CA private keys are stored in hardware cryptographic modules. Activation requires following Section 6.2.2 of this CP&CPS, where under the presence and permission of at least half of the key administrators, the operator permissions of the cryptographic equipment are used to achieve this. When CA private keys need to be used (online or offline), the key administrators must provide operator IC cards or USB Keys and enter the PIN to complete the operation.

6.2.9 Method of Deactivating Private Key

For TrustAsia CA private keys, when the CA system issues a logout command to the cryptographic module, or the cryptographic management software issues a shutdown command to the cryptographic module, or the hardware cryptographic module storing the private key loses power, the private key enters a deactivated state.

The operation to deactivate the private key is performed by a key administrator using their own administrator card to log into the server cryptographic machine and entering the PIN, with the presence and permission of at least half of the key administrators.

6.2.10 Method of Destroying Private Key

After the lifecycle of the TrustAsia CA private key ends, TrustAsia CA will retain the CA private key in a backup hardware cryptographic module, while other CA private key backups are securely destroyed. Meanwhile, all PIN codes, IC cards, or USB Keys used to activate the private key must also be destroyed.

The CA must not destroy its private keys before their commercial purpose or application has lost value, or legal obligations expire.

Archived CA private keys, after their archival period ends, or when CA private key backups or copies are no longer used for valid commercial purposes, must be securely destroyed with the participation of multiple trusted persons. The destruction of CA private keys will ensure that the CA private keys are completely deleted from the hardware cryptographic module, leaving no residual information.

6.2.11 Cryptographic Module Rating

Refer to Section 6.2.1 of this CP&CPS.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

For TrustAsia CA public key archival, refer to Section 5.5.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The maximum validity period for the end Subscriber certificate of a Mark Certificate does not exceed 398 days. If it is a licensee of a registered trademark or word mark rather than the trademark registrant, the certificate's expiration date will not be later than the final expiration date of the Subscriber's possession of the registered trademark or word mark.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The activation data for TrustAsia CA private keys is generated by cryptographic equipment in the presence and with the permission of at least half of the key administrators, according to the operational specifications provided by the cryptographic equipment manufacturer.

The activation data for Subscriber private keys, including passwords used to download certificates (provided in the form of secure envelopes), USB Keys, login passwords for IC cards, etc., must be generated in a secure and reliable environment. This activation data is delivered to the Subscriber through secure and reliable methods, such as in-person delivery offline, special express mail, etc. For non-single-use activation data, TrustAsia CA recommends that users modify it themselves.

If the activation data for the Subscriber certificate private key is a password, these passwords must:

1. Be at least 8 characters long
2. Contain at least one lowercase letter
3. Not contain many identical characters
4. Not be identical to the operator's name
5. Not use numbers like birth dates or telephone numbers
6. Not contain long substrings from user name information

6.4.2 Activation Data Protection

For CA private key activation data (smart IC cards, PIN codes), TrustAsia CA ensures they are held by trusted personnel themselves in a reliable manner. All trusted personnel are required to memorize their passwords rather than writing them down or sharing them with others.

6.4.3 Other Aspects of Activation Data

When private key activation data is transmitted, it should be protected from loss, theft, modification, unauthorized disclosure, or unauthorized use during transmission.

When private key activation data is no longer needed, it will be destroyed and protected from loss, theft, disclosure, or unauthorized use during this process. The result of the destruction is that part or all of the activation data cannot be obtained directly or indirectly from residual information or media. For example, papers recording passwords must be shredded.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The information security management of the CA system, acting in accordance with the national standard "Cryptographic and Related Security Technical Specifications for Certificate Authority Systems", the "Electronic Authentication Service Management Measures" promulgated by the Ministry of Industry and Information Technology, the ISO 27001 information security management system requirements, and other relevant information security standards, has established comprehensive and complete security management policies and systems, which are implemented, reviewed, and recorded during operations. The primary technical security and control measures include: identification and authentication, logical access control, network access control, etc.

Multi-factor authentication is implemented for all accounts that can directly result in certificate issuance.

System operation and maintenance personnel log into the system through a bastion host to perform operations, ensuring that CA software and data files are secure, reliable, and not subject to unauthorized access.

Core systems must be physically separated from other systems, and production systems are logically isolated from other systems. This separation can prevent unauthorized network access. Firewalls are used to prevent unauthorized access to the production system network from both internal and external networks, restricting activities accessing the production system. Only trusted personnel in the CA system operation and management group with necessary work needs and system access can access the CA database via passwords.

6.5.2 Computer Security Rating

TrustAsia CA’s CA system and its operational environment have passed third-party security assessments and penetration tests, obtaining the corresponding test reports.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

TrustAsia CA’s software design and development process follows these principles:

1. Formulate an internal upgrade and change request system within the company, and require staff to strictly follow the process;
2. Formulate the company's internal procurement processes and management systems;
3. Developed programs must undergo strict and successful testing in the development environment before applying for deployment to the production environment;
4. Perform effective online backups before deploying changes;
5. Third-party verification and review;
6. Security risk analysis and reliability design.

6.6.2 Security Management Controls

TrustAsia CA has established various security policies, management systems, and processes to conduct security management of the certification system.

Information security management of the certification system operates strictly following the relevant operation management specifications of the State Cryptography Administration.

There are strict control measures over the use of the certification system. All systems are only put into secure use after rigorous testing and verification, and any modifications and upgrades are recorded on file.

TrustAsia CA regularly performs security inspections on the system to identify whether equipment has been compromised, whether security vulnerabilities exist, etc.

6.6.3 Life Cycle Security Controls

TrustAsia CA controls the research, development, and deployment of the certificate authentication system through internal change control processes to ensure the system is secure and reliable.

6.7 Network Security Controls

TrustAsia CA's certification system uses firewalls for system access control, IDS/IPS for network attack defense, bastion hosts for remote login permission management, and routers for network hierarchical control.

The certification system should only be open to designated services or personnel, granting only the minimum required access permissions.

The certification system should regularly undergo security vulnerability scanning and security device configuration audits, and related logs should be audited.

TrustAsia CA's network security controls comply with the CA/Browser Forum NCSSR.

6.8 Time-Stamping

The system time on TrustAsia CA computers should be updated using the Network Time Protocol (NTP) so that the system clock is synchronized at least once every 24 hours.

TrustAsia CA maintains an internal NTP server synchronized with external sources and maintains its clock precision to one second or less.

Furthermore, a dedicated authoritative Time Stamping Authority (TSA) of TrustAsia CA operates to provide timestamping services compliant with RFC 3161.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate Profile

Mark Certificates conform to the profile requirements specified in this section. Based on meeting the technical requirements stipulated in Sections 2.2, 6.1.5, and 6.1.6, TrustAsia CA issues certificates according to the following specifications in this chapter.

7.1.1 Version Number(s)

The certificate complies with the X.509 V3 certificate format, and the version information is stored in the certificate version format field.

7.1.2 Certificate Extensions

Based on the requirements of RFC 5280, TrustAsia CA applies the following configurations to all issued certificates.

- 7.1.2.1 Root Certificate Profile
- 7.1.2.2 Subordinate CA Certificate Profile
- 7.1.2.3 Subscriber Certificate Profile

7.1.2.1 Root CA Certificate Profile

See Section 11.1.

7.1.2.2 Subordinate CA Certificate Profile

See Section 11.2.

7.1.2.3 Subscriber Certificate Profile

See Section 11.3.

7.1.3 Algorithm Object Identifiers

7.1.3.1 Subject Public Key Info

The following requirements apply to subjectPublicKeyInfo in certificates or precertificates. Other encodings are not used.

7.1.3.1.1 RSA

TrustAsia CA uses the rsaEncryption (OID: 1.2.840.113549.1.1.1) algorithm identifier to indicate an RSA key and explicitly displays NULL. When encoded, the hexadecimal encoding for the RSA key algorithm identifier is 300d06092a864886f70d0101010500.

7.1.3.1.2 ECDSA

TrustAsia CA uses the id-ecPublicKey (OID: 1.2.840.10045.2.1) algorithm identifier to indicate an ECDSA key.

Parameters are encoded using the curve name:

- For P-256 keys, the curve is secp256r1 (OID: 1.2.840.10045.3.1.7).
- For P-384 keys, the curve is secp384r1 (OID: 1.3.132.0.34).

When encoded, the key identification for ECDSA is the following hexadecimal encoding:

- P-256 key: 301306072a8648ce3d020106082a8648ce3d030107
- P-384 key: 301006072a8648ce3d020106052b81040022

7.1.3.2 Signature Algorithm Identifier

Objects signed by TrustAsia CA private keys and the derived content signatures all conform to the algorithm used in context.

In particular, all following objects and fields:

1. The signatureAlgorithm field of a certificate or precertificate.
2. The signature field of a tbsCertificate.
3. The signatureAlgorithm field of a CertificateList.
4. The signature field of a tbsCertList.
5. The signatureAlgorithm field of an OCSP response.

7.1.3.2.1 RSA

TrustAsia CA uses two RSA signature algorithms and encodings, as follows:

Signature Algorithm	OID	Hexadecimal Encoding
SHA-256 with RSA	1.2.840.113549.1.1.11	300d06092a864886f70d01010b0500
SHA-384 with RSA	1.2.840.113549.1.1.12	300d06092a864886f70d01010c0500

7.1.3.2.2 ECDSA

TrustAsia CA uses two ECDSA signature algorithms and encodings, as follows:

Signature Algorithm	OID	Hexadecimal Encoding
SHA-256 with ECDSA	1.2.840.10045.4.3.2	300a06082a8648ce3d040302
SHA-384 with ECDSA	1.2.840.10045.4.3.3	300a06082a8648ce3d040303

7.1.4 Name Forms

This section describes the encoding rules applicable to all certificates issued by the CA. Further

restrictions may be specified in Section 7.1.2, but these restrictions do not supersede these requirements.

For each valid certification path (as defined by RFC 5280 Section 6) from TrustAsia CA:

- For each certificate in the certification path, the encoded content of the Issuer Distinguished Name field of the certificate is 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 the certificate is byte-for-byte identical among all certificates whose Subject Distinguished Name can be compared according to RFC 5280 Section 7.1, including expired and revoked certificates.

When encoding a Name:

- Each Name contains an RDNSequence.
- Each RelativeDistinguishedName contains exactly one AttributeTypeAndValue.
- Each Name does not contain more than one instance of a given AttributeTypeAndValue across all RelativeDistinguishedNames.

7.1.5 Name Constraints

This extension is not used.

7.1.6 Certificate Policy Object Identifier

7.1.6.1 Reserved Certificate Policy Identifiers

See Section 1.2 of this CP&CPS.

7.1.7 Usage of Policy Constraints Extension

Not applicable.

7.1.8 Policy Qualifiers Syntax and Semantics

Not applicable.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

Not applicable.

7.2 CRL Profile

TrustAsia CA generates and publishes CRLs according to the following profile.

The CRL covers all certificates issued by the CA. If CRL partitions are used, the aggregation of these partitions equals the complete CRL. The CA does not issue CRLs indirectly.

Attribute		Presence	Description
tbsCertList			
	version	Present	v2 version
	signature	Present	
	issuer	Present	Matches the issuing CA subject byte-for-byte
	thisUpdate	Present	The issue date of the CRL
	nextUpdate	Present	No more than 10 days for Subscriber certificates, no more than 12 months for Subordinate certificates
	revokedCertificates	Not used	
	extensions	Present	See table below
signature		Present	

7.2.1 Version Number(s)

TrustAsia CA's Certificate Revocation List complies with the X.509 v2 version and format requirements.

7.2.2 CRL and CRL Entry Extensions

CRL Extensions:

Extension	Presence	Critical	Description
authorityKeyIdentifier	Yes	No	Matches the SubjectKeyIdentifier of the issuing CA byte-for-byte
CRLNumber	Yes	No	A monotonically increasing non-negative integer up to 2^159
IssuingDistributionPoint	*	-	See Section 7.2.2.1 of this CP&CPS

Revoked Certificate Component:

Component	Presence	Description
serialNumber	Yes	Matches the serial number of the revoked certificate byte-for-byte
revocationDate	Yes	Usually the revocation date. If TrustAsia CA has sufficient evidence that the private key of the certificate was compromised prior to the revocation date, this date will be backdated to the compromise date.
crlEntryExtensions	Maybe	See crlEntryExtensions component table below

crlEntryExtensions Component:

CRL Entry Extension	Presence	Description
reasonCode	Maybe	Not present when the reason code is 0; this reason code is the default option provided as specified in the Subscriber Agreement. When the reason code is otherwise, it is present and non-critical.

7.2.2.1 Issuing Distribution Point

TrustAsia CA does not use this extension when using a complete CRL. This extension is enabled when CRL partitions are used.

7.3 OCSP Profile

If the OCSP response is for a Root CA or Subordinate CA certificate (including cross-certified Subordinate CA certificates), and that certificate has been revoked, then the revocationReason field MUST be present within the RevokedInfo of the CertStatus.

The CRLReason indicated contains a permitted value for CRLs as specified in Section 7.2.2.

7.3.1 Version Number(s)

OCSP Version 1 defined by RFC 6960.

7.3.2 OCSP Extensions

Consistent with RFC 6960. The singleExtensions of an OCSP response do not contain the reasonCode (OID 2.5.29.21) CRL entry extension.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

TrustAsia CA at all times:

1. Complies with the guidelines of the latest version of the BIMI Group MCR;
2. Complies with the WebTrust audit requirements specified in this chapter;
3. Obtains a CA operation license authorized by the Ministry of Industry and Information Technology (MIIT).

8.1 Frequency or Circumstances of Assessment

TrustAsia CA performs the following audits and assessments:

1. Performs an annual security vulnerability assessment covering systems, physical sites, operational management, etc., and takes measures based on the assessment report to mitigate operational risks.
2. Performs an annual operational quality assessment to ensure the reliability, security, and controllability of operational services.
3. Performs a quarterly internal audit sampling at least 1 certificate or 3% of the certificates, whichever is greater.
4. Performs an annual operational risk assessment to identify internal and external threats, evaluate the likelihood of threat events occurring and the resulting damages, and develop and implement handling plans based on the risk assessment results.
5. In addition to internal audits and assessments, TrustAsia CA engages an independent audit firm to conduct an external audit and assessment annually in accordance with the WebTrust audit specifications for CAs and Mark Certificates.

8.2 Identity/Qualifications of Assessor

Internal audits and assessments are executed by the internal audit and assessment group of TrustAsia CA.

External audits are handled by an organization possessing the following qualifications:

1. Independent auditing entity;
2. Must be a licensed and qualified assessment agency with a good reputation in the industry;
3. Familiar with computer information security systems, communication network security requirements, PKI technology, standards, and operations;
4. Possess professional technology and tools to check system operation performance;
5. Qualified for WebTrust audits;
6. Holds 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 work positions of internal auditors must not overlap with those of the organization’s system administrators, business administrators, and business operators.

The external assessor and TrustAsia CA have a mutually independent relationship, and both parties have no conflicts of interest that could affect the objectivity of the assessment.

8.4 Topics Covered by Assessment

The internal audit work involves the following:

1. Whether operational workflows and systems are strictly adhered to;
2. Whether certification operations are strictly conducted according to the CP&CPS, business specifications, and security requirements;
3. Whether various logs and records are complete, and whether there are issues;
4. Whether there are other potential security risks.

The third-party audit firm conducts an independent audit on TrustAsia CA in accordance with the WebTrust for CA and MC specifications.

8.5 Actions Taken as a Result of Deficiency

For issues identified in the organization’s internal audit results, the audit and assessment group is responsible for supervising the improvements by the relevant responsible departments.

After the third-party audit firm completes its assessment, TrustAsia CA rectifies issues based on the work report and undergoes a re-audit and assessment.

8.6 Communication of Results

TrustAsia CA makes the audit report publicly available within three months after the end of the audit period. If the delay exceeds three months, TrustAsia CA provides an explanatory letter signed by the qualified auditor.

The audit report satisfies the requirements specified elsewhere in Section 8.6 of this CPS and contains the following explicitly labeled information:

1. Name of the organization being audited;
2. Name and address of the organization performing the audit;
3. SHA-256 fingerprints of all Root and Subordinate CA certificates (including cross-certificates) within the scope of the audit;
4. The audit standards, with version numbers, used to audit each certificate (and related key);

5. A list of the CA policy documents referenced during the audit, along with their version numbers;
6. Whether the audit assessment is for a period of time or a point in time;
7. The start date and end date of the audit period, for an audit covering a period of time;
8. The date of the point in time, for some point in time;
9. The date the report was issued, which must follow the end date or the point in time date.

TrustAsia CA ensures that an authoritative English version of the audit report, provided by the qualified auditor, is publicly available. The report is provided in PDF format and is text-searchable for all required information. Each SHA-256 fingerprint in the audit report consists of uppercase letters and does not contain colons, spaces, or line breaks.

8.7 Self-Audits

TrustAsia CA will continuously conduct self-audits and strictly control service quality according to relevant international and domestic standards and the provisions of the CP&CPS through at least an annual internal risk assessment and at least a quarterly self-supervisory random inspection. The self-audit assesses whether electronic certification activities from the end of the previous review period to the initial stage of the current audit period comply with relevant regulations. The sample size for the random inspection should not be less than 1 certificate or 3% of the total number of certificates issued during the period, whichever is greater.

Any revisions to this CP&CPS become officially effective upon publication to TrustAsia CA's online repository and remain effective until replaced by a new version or until TrustAsia CA ceases operations.

9.10.2 Termination

This CP&CPS terminates when TrustAsia CA ceases operations.

9.10.3 Effect of Termination and Survival

After this CP&CPS terminates, its effect will simultaneously terminate, but for legal facts occurring before the date of termination, the provisions on the responsibilities of the parties and the exemption of responsibilities in this CP&CPS still apply, including but not limited to the contents involving auditing, confidential information, privacy protection, intellectual property rights, and limited liability clauses for compensation in the CP&CPS, which continue to be effective after this CP&CPS terminates.

When certain provisions in the CP&CPS, Subscriber Agreement, Relying Party Agreement, and other agreements become invalid due to certain reasons, such as content modification or conflict with applicable laws, it does not affect the legal validity of other provisions in the documents.

9.11 Individual Notices and Communications with Participants

TrustAsia CA will individually notify Subscribers and Relying Parties via email or other methods when necessary, such as proactively revoking Subscriber certificates, discovering that the Subscriber used the certificate for unauthorized purposes, or other violations of the Subscriber Agreement by the Subscriber.

9.12 Amendments

9.12.1 Procedure for Amendment

Authorized by the TrustAsia CA Security Policy Committee, the CPS writing group reviews this CP&CPS at least annually to ensure it complies with national laws, regulations, the requirements of competent authorities, relevant international standards, and the actual needs of certification business operations.

For modifications and updates to this CP&CPS, the CPS writing group proposes revision suggestions. After approval by the TrustAsia CA Security Policy Committee, the CPS writing group is responsible for completing the revisions. The revised CP&CPS is officially published after being approved by the TrustAsia CA Security Policy Committee.

9.12.2 Notification Mechanism and Period

The revised CP&CPS will be published immediately on TrustAsia CA's official website upon approval. For modifications that require notification via email, mail, media, etc., TrustAsia CA will notify relevant parties within a reasonable time, which should ensure minimal impact on the concerned parties.

9.12.3 Circumstances Under Which OID Must Be Changed

TrustAsia CA has the sole authority to determine whether an amendment to the CP&CPS requires a change to the OID.

9.12.4 Circumstances Under Which Business Rules Must Be Modified

Circumstances under which TrustAsia CA must modify this CP&CPS include: inconsistencies between relevant contents in the CP&CPS and governing laws, explicit change or adjustment requirements from national regulatory authorities regarding the organization's certification business, etc.

9.13 Dispute Resolution Provisions

If disputes arise among end entities such as TrustAsia CA, Certificate Subscribers, and Relying Parties during electronic certification activities, they should first be resolved through friendly negotiation based on the agreement. If negotiation fails, they may be resolved through legal channels.

Any litigation brought against TrustAsia CA regarding any dispute involving this CP&CPS shall be submitted by the parties to the jurisdiction of the People's Court at the location where TrustAsia CA's industrial and commercial registration is located.

9.14 Governing Law

TrustAsia CA's CP&CPS is governed by the laws and regulations of the People's Republic of China.

9.15 Compliance with Applicable Law

Regardless of where TrustAsia CA's Certificate Subscribers, Relying Parties, and other entities reside and where they use TrustAsia CA's certificates, the execution, interpretation, and procedural validity of this CP&CPS are subject to the laws and regulations of the People's Republic of China and the requirements of the national information security competent authorities. Any disputes with TrustAsia CA involving this CP&CPS are governed by the laws of the People's Republic of China.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

The complete document structure of this CP&CPS includes three parts: title, table of contents, and main body. Alternative content following modifications to the table of contents and main body will fully replace all previous parts and be placed on TrustAsia CA's website for reference and browsing.

9.16.2 Assignment

TrustAsia CA declares that according to the rights and obligations of the certification entities detailed in this CP&CPS, the parties cannot make assignments in any way without the prior written consent of TrustAsia CA.

9.16.3 Severability

In the event of a conflict between a requirement of this CP&CPS and the laws, regulations, or government orders of any jurisdiction within mainland China (hereinafter referred to as "Laws"), TrustAsia CA will modify any conflicting requirement to the minimum extent necessary to make it legally effective within that jurisdiction. This applies only to operations or certificate issuances subject to that Law. In such cases, TrustAsia CA will immediately (and prior to issuing certificates under the modified requirement) detail the specific Law in Section 9.16.3 of this CP&CPS, as well as the related modifications specifically implementing these requirements.

Furthermore, TrustAsia CA will (and prior to issuing certificates under the modified requirement) notify the BIMI Group Working Group of the newly added relevant content in its CPS by sending a message and receiving a confirmation receipt, so that the BIMI Group Working Group may consider possible revisions to the MCR accordingly.

Any modification made by TrustAsia CA based on the MCR shall be terminated if either of the following occurs:

1. The relevant Law no longer applies;
2. The MCR is revised such that the CA can comply with both.

In such cases, the following three tasks must be completed within 90 days (as stated above):

1. Make the corresponding practice changes;
2. Modify the CA's CPS;
3. Notify the BIMI Group Working Group.

9.16.4 Enforcement

TrustAsia CA states that if Certificate Subscribers, Relying Parties, and other entities fail to enforce a provision of this CP&CPS, it shall not be deemed that the entity will not enforce that or other provisions in the future.

9.16.5 Force Majeure

If a violation, delay, or inability to perform the warranty liabilities stipulated in this CP&CPS is caused by force majeure such as war, plague, fire, earthquake, or natural disaster, TrustAsia CA will not be responsible for such events.

9.17 Other Provisions

TrustAsia CA holds the right of final interpretation of this CP&CPS.

10. Appendix A – Validation Requirements

10.1 Validation Items and Requirements

TrustAsia CA's authentication requirements for Subscriber certificates are as follows:

Authentication Item	Authentication Requirement
CSR Validation	Validate CSR signature data Validate CSR public key length Validate whether the CSR public key is a weak key
Domain Validation	Validate domain control according to CPS 3.2.2.5
CAA Validation	Validate CAA according to CPS 4.2.4

Authentication Item	Authentication Requirement
Organization Validation	Verify whether the applicant's name is legally compliant Verify whether the applicant is legally existing and operating Verify the country, province, city, and address of the applicant's location Verify the telephone number, fax number, email address, or postal delivery address as the applicant's verified communication method Organization registration jurisdiction validation (country, state/province of registration, place of registration, registration number) Name, title, and authorization validation of the Certificate Approver and Contract Signer 1. Certificate Approver: Validate their name and title, and validate their authority to approve certificate applications 2. Contract Signer: Validate their name and title, and validate their authority to enter into the Subscriber Agreement (or other relevant contractual obligations) on behalf of the applicant Signature validation of the Subscriber Agreement and certificate request Validation of the applicant organization's operational capability Identification and validation of the applicant organization's business category 1. Private Organization: Legal existence, organization name, registration number, registering agency 2. Government Entity: Legal existence, organization name, registration number 3. Business Entity: Legal existence, organization name, registration number, Principal Individual 4. Non-Commercial Entity: Legal existence, organization name, registration number Face-to-face validation of the "Principal Individual" of a business entity: `Face-to-face validation of the Contract Signer or Certificate Approver` Follow relevant sections on organization validation in CPS 3.2.2
Prior Use Mark Validation	Validate mark type, prior use period, mark source, color limitations, mark representation Follow Section 3.2.2.7.1 of CPS

Authentication Item	Authentication Requirement
Modified Registered Mark Validation	Validate mark type, country or region of trademark registration, trademark office name, trademark number, color limitations, mark representation Follow Section 3.2.2.7.2 of CPS
Registered Mark Validation	Validate mark type, country or region of trademark registration, legal citations, trademark office name, trademark number, color limitations, trademark representation Follow CPS 3.2.2.8.1
Government Mark Validation	Verify mark type, specific citation of the act/regulation/treaty or government action and specific URL source, government mark ownership or license, trademark representation, color limitations, legal jurisdiction of the government entity establishing the government mark (country of the act, state/province of the act, locality of the act) Follow CPS 3.2.2.8.2
Individual Identity Validation	Validate individual identity according to CPS 3.2.3
Certificate Requester Validation	Validate the name and title of the certificate application requester, and validate their agency for the applicant; Confirm relevant information about the applicant and the type of certificate requested by contacting the certificate application requester.

Authentication Item	Authentication Requirement
High-Risk Validation	Query the internal database storing all previously revoked certificates and rejected certificate applications to identify subsequent suspicious certificate applications. Identify "High-Risk Applicants" using the validation methods outlined below and take additional reasonably necessary precautions to ensure such applicants are appropriately validated: Identify high-risk applications by querying a list of organization names frequently associated with phishing, fraud, or other deceptive behaviors, and automatically flag certificate applications matching the list for further investigation prior to issuance. Adopt information recognized by the organization’s high-risk criteria to flag suspicious certificate applications. Perform additional validation on any certificate application flagged as suspicious or high-risk according to documented procedures. Determine whether the entity is identified as applying for a Mark Certificate from a high-risk area of concern. Mark Certificates will not be issued if the applicant, Certificate Requester, Certificate Approver, Contract Signer, or the applicant’s registration jurisdiction or place of business falls under the following circumstances: • On any government denied list, prohibited persons list, or other list prohibiting business dealings with that organization or individual in the country where the CA operates; or • For the registration jurisdiction, the country where the registering agency or place of business is located is one with which business dealings are prohibited by the laws of the CA’s jurisdiction.
Attorney Identity Validation	Verify attorney-related information, check the attorney’s practice certificate, or query the registration and filing status of their practice certificate, and confirm their practice status with their law firm; Verify the authenticity and accuracy of the signed attorney letter with the attorney. This validation must be performed if an attorney letter is used.

11. Appendix B – Certificate Profiles

11.1 Root Certificate

Certificate Field		Critical Extension	Content
Version			v3
Serial Number			Contains a CSPRNG of at least 64 bits
Issuer			Matches the subject byte-for-byte
TBSCertificate Signature			TrustAsia Verified Mark RSA Root CA: sha384withRSA TrustAsia Verified Mark ECC Root CA: sha384withECDSA
Validity: notBefore			Day of the generation ceremony
Validity: notAfter			25 years
Subject	Common Name (CN)		TrustAsia Verified Mark RSA/ECC Root CA
	Organization (O)		TrustAsia Technologies, Inc.
	Country (C)		CN
Public Key Info			RSA4096 (OID: 1.2.840.113549.1.1.1) or secp384r1 (OID: 1.3.132.0.34)
Signature Algorithm			Matches the TBSCertificate Signature
Extension: subjectKeyIdentifier		Non-critical	160-bit SHA-1 hash of the subjectPublicKey, per RFC 5280
Extension: basicConstraints		Critical	Subject Type=CA Path Length Constraint=None
Extension: keyUsage		Critical	keyCertSign, cRLSign

11.2 Subordinate Certificate

Certificate Field	Critical Extension	Content
Version		v3
Serial Number		Contains a CSPRNG of at least 64 bits
Issuer		Matches the Subject info of the issuing CA byte-for-byte

Certificate Field		Critical Extension	Content
TBSCertificate Signature			TrustAsia Verified Mark RSA CA 2026: sha384withRSA TrustAsia Verified Mark ECC CA 2026: sha384withECDSA
Validity: notBefore			Day of the generation ceremony
Validity: notAfter			20 years
Subject	Common Name (CN)		TrustAsia Verified Mark RSA CA 2026 or TrustAsia Verified Mark ECC CA 2026
	Organization (O)		TrustAsia Technologies, Inc.
	Country (C)		CN
Public Key Algorithm			RSA4096 (OID: 1.2.840.113549.1.1.1) or secp384r1 (OID: 1.3.132.0.34)
Signature Algorithm			Matches the TBSCertificate Signature
Extension: subjectKeyIdentifier		Non-critical	160-bit SHA-1 hash of the subjectPublicKey, per RFC 5280
Extension: authorityKeyIdentifier		Non-critical	Matches the subjectKeyIdentifier of the signing certificate
Extension: certificatePolicies		Non-critical	Policy Identifier=Any Policy (2.5.29.32.0)
Extension: basicConstraints		Critical	Subject Type=CA Path Length Constraint=0
Extension: keyUsage		Critical	keyCertSign, cRLSign
Extension: extKeyUsage		Non-critical	id-kp-BIMIInternet
Extension: authorityInfoAccess		Non-critical	ICA AccessMethod=1.3.6.1.5.5.7.48.2 URL=http://ica.vmc.trustasia.com/<Issuername>.crt OCSP AccessMethod=1.3.6.1.5.5.7.48.1 URL=http://ocsp.vmc.trustasia.com/<Issuername>
Extension: cRLDistributionPoints		Non-critical	CRL HTTP URL=http://crl.vmc.trustasia.com/<Issuername>.crl

11.3 Subscriber (End Entity) Certificate

Certificate Field	Critical Extension	Content
Version		v3
Serial Number		Contains a CSPRNG of at least 64 bits
TBSCertificate Signature		sha256withRSA or sha384withRSA or sha384withECDSA
Issuer		Matches the Subject of the issuing CA byte-for-byte
Validity: notBefore		Difference from the issuance time is no more than 24 hours
Validity: notAfter		See Section 6.3.2
Subject		See Subject Content Table in this section
Public Key Info		RSA 2048, 3072, or 4096; or ECDSA P-256 or P-384
Signature Algorithm		Matches the TBSCertificate
Extension: subjectKeyIdentifier	Non-critical	160-bit SHA-1 hash of the subjectPublicKey, per RFC 5280
Extension: authorityKeyIdentifier	Non-critical	Matches the subjectKeyIdentifier of the signing certificate
Extension: certificatePolicies	Non-critical	[1] Policy Identifier=1.3.6.1.4.1.44494.2.7 policyQualifier=https://www.trustasia.com/cps [2] Policy Identifier=1.3.6.1.4.1.53087.1.1
Extension: basicConstraints	Critical	Subject Type=End Entity
Extension: subjectAltName	Non-critical	Must be of type dNSName, cannot be a wildcard, must not use internal domain names or reserved IPs
Extension: extKeyUsage	Non-critical	id-kp-BIMIInternet
Extension: Signed Certificate Timestamp List	Non-critical	Matches the precertificate LogEntryType
Extension: authorityInfoAccess	Non-critical	ICA AccessMethod=1.3.6.1.5.5.7.48.2 URL=http://ica.vmc.trustasia.com/<Issuername>.crt OCSP AccessMethod=1.3.6.1.5.5.7.48.1 URL=http://ocsp.vmc.trustasia.com/<Issuername>
Extension: cRLDistributionPoints	Non-critical	CRL HTTP URL=http://crl.vmc.trustasia.com/<Issuername>.crl
Extension: logotype extension (1.3.6.1.5.5.7.1.12)	Non-critical	Verified SVG trademark compliant with RFC 6170

Subject Content:

		Common Mark Certificate		Verified Mark Certificate	
Common Name (CN)		Verified organization name or word mark			
Organization (O)		Verified organization, may be DBA (Doing Business As)			
Street (Street)		Verified street of the organization			
Locality (L)		Verified city of the organization, optional if ST is present			
State/Province (ST)		Verified province of the organization, optional if L is present			
Country (C)		Verified country of the organization			
Organizational Unit (OU)		Optional			
Business Category businessCategory		One of the following 4: Private Organization or Government Entity or Business Entity or Non-Commercial Entity			
JOI	City of Registration	City of the registration jurisdiction, must include province and country			
	State/Province of Registration	State/Province of the registration jurisdiction, must include country			
	Country of Registration	Country of the registration jurisdiction			
Serial Number (serialNumber)		See description in Section 3.2.2			
Legal Entity Identifier (LEI)		Optional			
Organization Identifier (OI)		Optional			
Mark Type		Prior Use Mark Certificate	Modified Registered Mark Certificate	Registered Mark Certificate	Government Mark Certificate

			Common Mark Certificate		Verified Mark Certificate	
	Prior Use Mark Source URL		Verified trademark URL			
	Trademark Registration Location			Country or region of the Trademark Office	Country or region of the Trademark Office	
	Trademark Office Name			Optional when the applicable Trademark Office is unique	Optional when the applicable Trademark Office is unique	
	Trademark Identifier			Trademark Identifier	Trademark Identifier	
	Statute/Government Information (SGI)	Locality of the Statute				Locality of the statute, must include province/state
		State/Province of the Statute				State/Province of the statute, must include country
		Country Code of the Statute				Country of the statute
	Statute Citation					Statute, regulation, or treaty cited by the mark
	Statute URL					Mark URL, optional

12. MARK CERTIFICATES TERMS OF USE

Mark Certificates Terms of Use ("MC Terms")

All **Mark Asserting Entities (MAEs)**, as a condition to obtaining a Mark Certificate, agree to these MC Terms. Any and all use, display, or reliance by **Consuming Entities**, **Relying Parties**, and any other persons on any Mark Certificate (and any mark representation, other data, or information therein) is contingent upon acceptance of these MC Terms. **OID 1.3.6.1.4.1.53087.1.1** within the Mark Certificate incorporates these MC Terms by reference. If any person does not agree to these MC Terms, they shall not obtain, use, publish, or rely on any Mark Certificate or any mark representation or any other data or information within a Mark Certificate.

1. Definitions

Capitalized terms have the meanings provided in Section 1.6 of the Mark Certificates Requirements.

2. Limited Reproduction and Display Rights

Subject to the terms, conditions, and restrictions of the MC Requirements and these MC Terms, the MAE hereby grants:

1. **To the Issuing CA**: A limited, non-exclusive, worldwide license to issue Mark Certificates containing the MC Mark and to log the certificates in a limited number of **Certificate Transparency (CT) Logs** as required by the MC Requirements.
2. **To Consuming Entities**: A limited, non-exclusive, worldwide license to use the MC Mark in conjunction with internal logo identification systems, and to host, store, reproduce, display, process, and (to the extent permitted by Section 3.1) modify the MC Mark when directly visually associated with communications, correspondence, or services authored or provided by the MAE; and such communications, etc. must originate from or pass through the identical domain name included in the "Subject Alternative Name (SAN)" field of the Mark Certificate.
3. **To Certificate Transparency Log Operators** (if different from the Issuing CA): A limited, non-exclusive, worldwide license to retain copies of Mark Certificates and to reproduce them to support the long-term public record of these issued certificates and to permit public audit of the verification of Mark Certificates.

No other licenses are granted to any other party or for any other use.

3. License Restrictions and Conditions

Any Consuming Entity that incorporates or intends to incorporate the MC Mark into its products and services through issued and published Mark Certificates agrees that the relevant licenses it receives are subject to and conditioned upon the following restrictions:

1. **Quality Control and Equal Treatment**: When displaying the mark representation obtained from a published Mark Certificate, a Consuming Entity **shall not distort** it, shall not change its color or background, shall not modify its transparency, and shall not alter it in any way other than adjusting its size, proportions, or cropping it in a manner consistent with other mark representations. If a Consuming Entity displays a word mark obtained from a published Mark Certificate, it must do so in a neutral manner and consistently with the word marks of all other

Mark Certificates displayed in the same visual environment. A Consuming Entity may display the mark without the word mark, but **shall not display the word mark alone without displaying the mark**.

2. **No Implication of Partnership or Relationship**: Unless expressly agreed otherwise between the Consuming Entity and the MAE, the MC Mark or any other content of the Mark Certificate shall not be used or displayed in any manner that reasonably implies any relationship between the Consuming Entity and the MAE other than the pure licensor-licensee relationship created by these MC Terms.
3. **CRL or OCSP Queries**: The Consuming Entity must check the **Certificate Revocation List (CRL)** maintained by the CA **no less frequently than once every 7 days** to determine whether the Mark Certificate has been revoked.
4. **Lawful Use**: The Consuming Entity may only use the mark representation from the Mark Certificate in accordance with applicable laws.
5. **Sufficient Ownership or License**: The **MAE warrants** that the MC Mark published via the Mark Certificate represents a **registered mark** (and word mark, if any) for which the MAE owns or has obtained sufficient licenses to grant the limited licenses in these MC Terms; and if the MAE ceases to own or ceases to have sufficient licenses for the relevant registered mark (or word mark), the MAE will **immediately revoke** the Mark Certificate. The MAE shall defend and be liable for any intellectual property or other claims against any Consuming Entity, Relying Party, or CA arising out of the content of the MAE's application for the Mark Certificate.
6. **No Obligation to Display**: The MAE acknowledges that Consuming Entities have no obligation to display the MC Mark in published communications associated with domains owned or controlled by the MAE, even if the communication or message has been confirmed to originate from the MAE and an appropriate MC Mark can be obtained and securely displayed from the corresponding Mark Certificate. A Consuming Entity may choose to display or not display the MC Mark under these MC Terms.
7. **Termination**: Upon revocation or expiration of the Mark Certificate, the MAE shall immediately cease publishing or using the Mark Certificate, and the licenses granted to Consuming Entities in Section 2.2 above **shall terminate**. If a Consuming Entity violates any provision of these MC Terms, the licenses granted to that Consuming Entity in Section 2.2 shall also **terminate automatically and immediately**. Upon termination of the license, the Consuming Entity must immediately cease any and all use of the MC Mark.
8. **Updates to MC Requirements and MC Terms**: The MC Requirements and MC Terms may be updated from time to time. The parties agree that the versions of the MC Requirements and MC Terms in effect at the time the Mark Certificate was issued shall apply until the date of expiration or revocation of that Mark Certificate. Any entity obtaining, using, publishing, or relying on a Mark Certificate is responsible for reviewing and familiarizing itself with any updated versions of the MC Requirements and MC Terms from time to time.