TrustAsia Certificate Policy and Certification Practice Statement for Global Trusted Service （CP&CPS）V1.7.2

April 25, 2024

TrustAsia Technologies, Inc.

CONTENTS

1. Introduction

1.1 Overview

1.1.1 Company Introduction

TrustAsia Technologies, Inc. (abbreviated as "TrustAsia") was established in April 2013. In December 2020, TrustAsia CA passed the qualification review by the State Cryptography Administration Office of Security Commercial Code Administration (abbreviated as OSCCA) and was granted the "Electronic Authentication Service License" by OSCCA (License number: 0060). In November 2021, TrustAsia CA obtained the “License for Electronic Certification Service Provider” issued by the Ministry of Industry and Information Technology (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 cyber security digital certificate and security monitoring solution provider. Its brand, TrustAsia, located in the field of information security, specializes in providing internationally renowned brand digital certificates and cyber security management solutions, which is recognized and trusted by the field of cyber security.

With the internationally standardized operational management and service level capability, we will provide globalized electronic authentication services for users with requirements on telecommunication and information security aspects in a variety of industries.

1.1.2 Service system/hierarchy

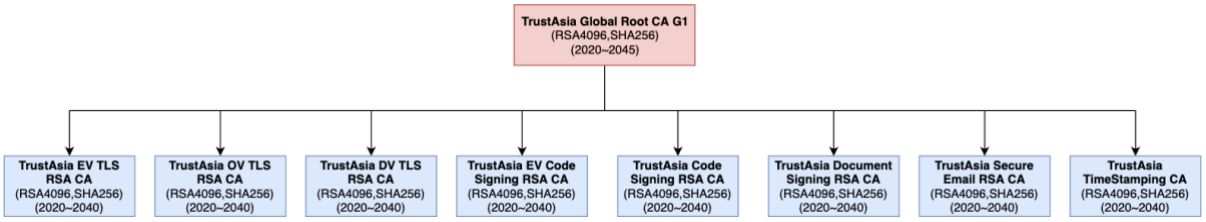
Under different application scenarios and algorithm, TrustAsia CA sets up the following root certificates：

1. TrustAsia Global Root CA G1
2. TrustAsia Global Root CA G2
3. TrustAsia Global Root CA G3
4. TrustAsia Global Root CA G4

Each root certificate does not issue the Subscriber certificates directly, and intermediate certificates are set up under each root certificate according to the different business scenarios to issue Subscriber certificates. Certificate details are available through the TrustAsia CA repositories. The root certificate architecture is as follows:

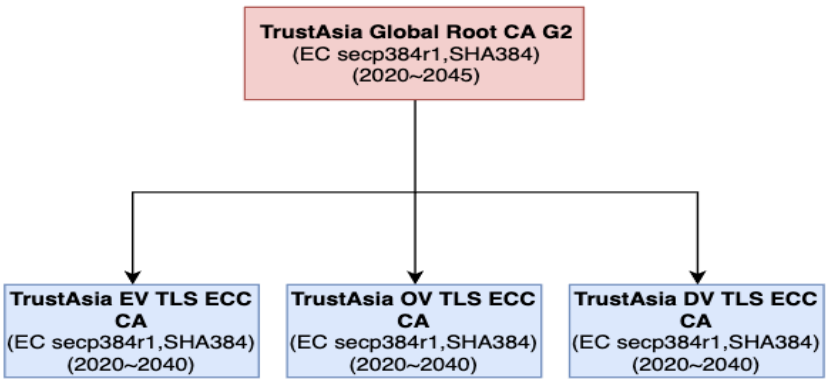
TrustAsia Global Root CA G1 is the root certificate of the RSA4096 with SHA256 algorithm for a period of 25 years. Different RSA intermediate certificates are set up according to the actual business type:

1. TrustAsia EV TLS RSA CA, issuing the RSA Extended Validation TLS Server Certificate.
2. TrustAsia OV TLS RSA CA, issuing the RSA Organization Validation TLS Server Certificate.
3. TrustAsia DV TLS RSA CA, issuing RSA Domain Validation TLS Server Certificate.
4. TrustAsia EV Code Signing RSA CA, issuing the RSA Extended Validation Code Signing Certificate.
5. TrustAsia Code Signing RSA CA, issuing the RSA Code Signing Certificate.
6. TrustAsia Document Signing RSA CA, issuing the RSA Document Signing Certificate.
7. TrustAsia Secure Email RSA CA, issuing the RSA Secure Email Certificate.
8. TrustAsia TimeStamping CA, issuing the RSA TimeStamp Certificate.



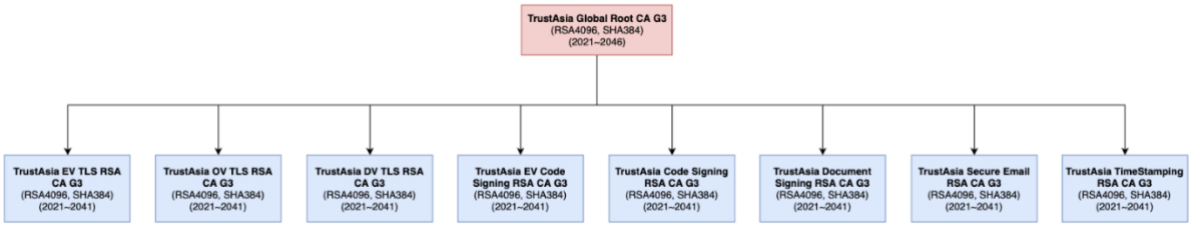
TrustAsia Global Root CA G2 is the root certificate of the ECDSA (P-384) with SHA384 algorithm for a period of 25 years. Different ECDSA intermediate certificates are set up according to the actual business type:

1. TrustAsia EV TLS ECC CA, issuing the ECC Extended Validation TLS Server Certificate.
2. TrustAsia OV TLS ECC CA, issuing the ECC Organization Validation TLS Server Certificate.
3. TrustAsia DV TLS ECC CA, issuing the ECC Domain Validation TLS Server Certificate.



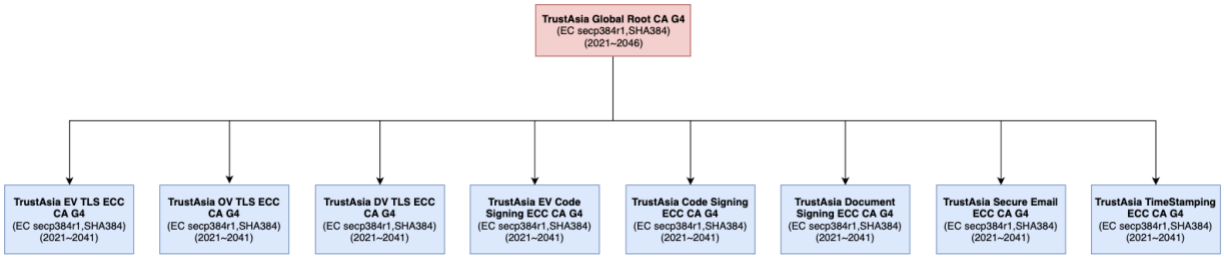
TrustAsia Global Root CA G3 is the root certificate of the RSA4096 with SHA384 algorithm for a period of 25 years. Different RSA intermediate certificates are set up according to the actual business type:

1. TrustAsia EV TLS RSA CA G3, issuing the RSA Extended Validation TLS Server Certificate.
2. TrustAsia OV TLS RSA CA G3, issuing the RSA Organization Validation TLS Server Certificate.
3. TrustAsia DV TLS RSA CA G3, issuing the RSA Domain Validation TLS Server Certificate.
4. TrustAsia EV Code Signing RSA CA G3, issuing the RSA Extended Validation Code Signing Certificate.
5. TrustAsia Code Signing RSA CA G3, issuing the RSA Code Signing Certificate.
6. TrustAsia Document Signing RSA CA G3, issuing the RSA Document Signing certificate.
7. TrustAsia Secure Email RSA CA G3, issuing the RSA Secure Email Certificate.
8. TrustAsia TimeStamping CA G3, issuing the RSA TimeStamp Certificate.



TrustAsia Global Root CA G4 is the root certificate of the ECDSA (P-384) with SHA384 algorithm for a period of 25 years. Different RSA intermediate certificates are set up according to the actual business type:

1. TrustAsia EV TLS ECC CA G4, issuing the ECC Extended Validation TLS Server Certificate.
2. TrustAsia OV TLS ECC CA G4, issuing the ECC Organization Validation TLS Server Certificate.
3. TrustAsia DV TLS RSA CA G4, issuing the ECC Domain Validation TLS Server Certificate.
4. TrustAsia EV Code Signing ECC CA G4, issuing the ECC Extended Validation Code Signing Certificate.
5. TrustAsia Code Signing ECC CA G4, issuing the ECC Code Signing Certificate.
6. TrustAsia Document Signing ECC CA G4, issuing the ECC Document Signing Certificate.
7. TrustAsia Secure Email ECC CA G4, issuing the ECC Secure Email Certificate.
8. TrustAsia TimeStamping　ECC CA G4，issuing the ECC TimeStamp Certificate.



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

This Certificate Policy and Certification Practice Statement (CP&CPS) is compiled with the "*Measures for the Administration of Electronic Certification Services*" and "*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, 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 these policies, guidelines and requirements:

1. The RFC3647 standard issued by the Internet Engineering Task Force (IETF)
2. The following latest requirements released by the CA/Browser Forum (https://cabforum.org/) (prior to this CP&CPS):
   - Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates
   - Network and Certificate System Security Requirements
   - Guidelines for the Issuance and Management of Extended Validation Certificates
   - Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates
   - Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates
3. Mozilla Root Store Policy
4. Microsoft Trusted Root Program
5. AATL Technical Requirements
6. Apple Root Certificate Program
7. Chrome Root Program
8. 360 Browser Root Certificate Program
9. Oracle Root Certificate Program

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 relevant

standard specifications, then the above officially issued specifications shall be prevailed. TrustAsia CA will notify the CA/Browser Forum if any of the provisions in the EV Guidelines is determined to be illegal by Chinese laws, regulations or government agencies.

1.2 Document name and identification

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

1.2.1 Certificate Policy Identification

Object	OID
Domain Validation SSL/TLS Server Certificate Policy Identification	2.23.140.1.2.1 1.3.6.1.4.1.44494.2.1.3
Organization Validation SSL/TLS Server Certificate Policy Identification	2.23.140.1.2.2 1.3.6.1.4.1.44494.2.1.2
Extended Validation SSL/TLS Server Certificate Policy Identification	2.23.140.1.1 1.3.6.1.4.1.44494.2.1.1
Organization Validation Code Signing Certificate Policy Identification	2.23.140.1.4.1 1.3.6.1.4.1.44494.2.2.1
Extended Validation Code Signing Certificate Policy Identification	2.23.140.1.3 1.3.6.1.4.1.44494.2.2.2
Adobe Document Signing Certificate Policy Identification	1.3.6.1.4.1.44494.2.3.1
S/MIME Basic Certificate Policy Identification	2.23.140.1.5.1.3 1.3.6.1.4.1.44494.2.4.3.3
S/MIME Individual Certificate Policy Identification	2.23.140.1.5.4.2 1.3.6.1.4.1.44494.2.4.6.2
S/MIME Enterprise Certificate Policy Identification	2.23.140.1.5.2.3 1.3.6.1.4.1.44494.2.4.4.3
S/MIME Enterprise Pro Certificate Policy Identification	2.23.140.1.5.3.2 1.3.6.1.4.1.44494.2.4.5.2
Timestamp Certificate Policy Identification	2.23.140.1.4.2 1.3.6.1.4.1.44494.2.5.1
Adobe Document Signing Timestamp Certificate Policy Identification	2.23.140.1.4.2 1.3.6.1.4.1.44494.2.5.2

1.2.2 Revision History

Release Date	Update Content	Version
2020-08-25	Issue initial version	V1.1

2020-10-23	• Update 2.2.2 Clarifying the CRL serial number is incremented • Update 2.4 and 2.5 section numbers • Update 5.1.1 Implementation standard for the construction of the CA computer room • Update 6.2.10 Clarifying the CA must not damage the CA private key restriction • Update 9.14 Adding applicable local laws and regulations	V1.2
2021-05-18	• Full formatting adjustment to fully correspond to CA/Browser catalog • Update 1 Revisions related to company introduction, certificate hierarchy and document identification OID • Update 3 Revisions related to recognition of trademarks and initial identity validation • Update 4.9 Certificate revocation • Update 5.7.3 Recovery procedures after key compromise • Update 6.1.5 Key sizes • Update 7 Clarifying certificate extensions and algorithm object identifier • Add Appendix A (10) Validation Requirements	V1.3
2021-10-28	• Update 1 Adding requirements this CP&CPS conforms with, clarifying that certificate application for the use of man-in-the-middle attack is prohibited • Update 2.2.3 Revisions related to OCSP publication frequency • Update 3 Clarifying validation of organization identity and wildcard domain, adding language about idoef property in CAA records • Update 4 Adding the implementation of identification and authentication, clarifying that all accounts that can directly issue certificates have deployed MFA, adding revocation circumstances and time limit for certificate revocation • Update 5 Clarifying types of events recorded, audit log and requirements for Timestamp Authority • Update 6 Clarifying requirements for key pair generation, RSA key size standards for Subscriber certificates, public key parameters generation and quality checking, key usage purposes, cryptographic module standards • Update 6.5.1 Deploying MFA for all accounts that can directly issue certificates, network security controls and requirements for time-stamping • Update 7.2.2 Addition of reasonCode extension • Update 9 Clarifying CGL and PI insurance, contents about Creative Commons license, indemnification scope for EV certificates • Update Appendix A (10) Validation requirements	V1.4
2022-05-24	• Update 1 Revisions related to company introduction, adding Timestamp Certificate OID and Document Signing Timestamp Certificate OID • Update 3 Clarifying approaches to Internationalized Domain Names and validation methods of email address, etc. • Update 5 Adding record and archived file types • Update 6 Adding relevant requirements for Code Signing Certificates, contents related to key protection and verification, clarifying S/MIME Certificates maximum validity period and Timestamp Certificates validity period • Update 7.1.4 Adding name forms related contents • Simplify revision history with removing "Editor" and "Comments" columns	V1.5

2022-12-15	• Full-text update, unifying the naming of "TrustAsia CA" and certain terms, adjusting formats and grammars to comply with the latest Baseline Requirements • Update 1 Adding OIDs of S/MIME Certificates • Update 2.3 Adjusting release frequency of CPS and Subscriber certificate CRL • Update 3 Adding Subject Distinguished Names of all types of certificates, clarifying relevant requirements for different S/MIME Certificates, adding private key possession proving of the ACME Protocol, adding requirements of validation information • Update 4 Adding description of authorization before certificate issuance by the Root CA and pre-issuance check for SSL/TLS Server Certificates, clarifying CRLReason usage, requirements for processing revocation request, requirements of certificate serial number in OCSP request, key compromise evidence of the ACME protocol • Update 5 Adding control goals of CA development and maintenance, certificate management and risk assessment, adding contents of risk assessment and business continuity plan, revisions related to types of records archived and retention period for archive, adding time limit for notifying relevant entities • Update 6 Adding requirements of pre-issuance check for key size and public key parameters, adding private key protection controls • Update 7 Adjusting extensions in Subscriber certificates, clarifying Precertificate in RFC5280, adding requirements of using algorithms • Update 8 Adding requirements needed to be conformed with for audit and contents related to communication and publishing of audit • Update Appendix A (10.2) Adjusting validation items of different types of Subscriber certificates • Add Appendix B (11) Presenting templates of different certificates contents	V1.6
2023-02-10	• Moving Revision History to Section 1.2.2 • Update Appendix B (11)	V1.6.1
2023-08-30	• Update 7 in accordance with SC-062 (The adjustments come into effect on September 1, 2023 along with SMC-001.) • Update the statements on OU field validation in Document Signing Certificate • Update definitions in Section 1.6 • Update the description in Section 2.4 • Update 3.2 Add verification requirements for "Principal Individual" in Business Entity, description for subject:organizationUnitName, and requirements of Personal Statement in application documents • Update 9.16.3 • Update Appendix B (11), making the order of certificate profiles consistent with that in BR and adding OCSP Responder Certificate Profile.	V1.7.0
2023-12-21	• Update 4.9 Comply with SC-063, effective on 2024-03-15 • Update 7.2 Add CRL related contents and requirements • Add SCT extension in certificate profiles	V1.7.1
2024-04-25	• Update 4.2.4 contents related to CAA in accordance with SMC05 • Update 5.4.1.1 clarifying router and firewall logging requirements in accordance with SC69v3 • Update 6.2.7 contents related to high risk changes in accordance with CSC-22 • Update protection requirements for timestamp private key in accoradace with CSC-24 • Update Appendix certificate profile	V1.7.2

1.3 PKI Participants

1.3.1 Certification Authority

Certification Authority (CA) refers to all entities authorized to issue public key certificates.

TrustAsia CA is a Certification Service Organization established according to law. It has become the main body of Certification activities by issuing digital certificates to all parties engaged in electronic transactions and providing digital certificate verification services.

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

1.3.2 Registration Authority

On behalf of CA, the Registration Authority (RA) establishes the certificate application process, including confirming the identity of the certificate applicant (Subscriber), approving or refusing the certificate application, approving the Subscriber's certificate revocation request or directly revoking the certificate, and approving the Subscriber's certificate update request.

In addition to assuming the role of CA, TrustAsia CA will act as RA, and no longer set up a separate RA.

1.3.3 Subscribers

Subscribers are all end-users who obtain certificates from TrustAsia CA, either individuals, institutions, or equipment. Contracts are usually signed between TrustAsia CA and Subscribers to obtain certificates and assume responsibility as certificate subscribers by subscribers.

Subscribers are not always identified in the certificate, such as when the certificate is issued to the employee of the organization. The subject of the certificate is the party specified in the certificate. As used in this article, Subscribers may refer to the subject of the certificate and the entity that signed the certificate contract with TrustAsia CA. Before verifying the identity and issuing the certificate, the Subscriber is the applicant. In the application of electronic signature, the electronic signer and the certificate holder are the same object (Subscriber).

1.3.4 Relying Parties

Relying parties are entities engaged in related activities based on trust in certificates and/or digital signatures issued by TrustAsia CA. The relying party can or may not be a Subscriber.

1.3.5 Other Participants

Other participants refer to other entities that provide related services for TrustAsia CA certification activities.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Usage

The certificate issued in accordance with this CP&CPS can be used for all identity authentication, encryption, access control, and digital signatures, specified by the key usage and extension key usage fields in the certificate.

1.4.2 Prohibited Certificate Uses

The digital certificate issued by TrustAsia CA is functionally limited and can only be used for the appropriate purpose of the principal identity represented by the certificate. For the utilization of certificates exceed the scope of this CP&CPS, it will not be protected by this CP&CPS.
The certificates issued by TrustAsia CA are prohibited from being used in any case of a violation of national laws, regulations or the destruction of national security, from being used for man-in-the-middle (MITM) attack, and from being used under any criminal activity or any related business prohibited by law, otherwise the legal consequences arising therefrom shall be borne by the Subscriber.

1.4.3 Formal and test certificates

TrustAsia CA certification system can provide formal certificates and test certificates. The formal certificate is issued by TrustAsia CA formal certification system and must be strictly authenticated in accordance with the provisions of CP&CPS.

The test certificate is issued by TrustAsia CA Test Certification system, and the certificate is untrustworthy. It is generally used to test the certificate application process, system applicability and technical feasibility, and cannot be used for any official purpose. Because the application scenarios in which digital certificates are used to process or protect information are very wide and different, relying parties must evaluate the applicability of their own application scenarios and the related risks in determining whether or not to issue certificates according to this CP&CPS. It covers different types of subscriber certificates and has different levels of protection. The following table describes the application scenarios for each certificate.

Certificate type	Application scenarios
Extended Validation SSL/ TLS Server Certificate	Execute strict audit to domain names and organization information, be applicable to scenarios involving serious consequences of transactions and sensitive information or data disclosure.
Organization Validation SSL/ TLS Server Certificate	Audit the authenticity of domain names and organization information, be applicable to scenarios involving privacy information and important data or where there is a risk of fraud.
Domain Validation SSL/ TLS Server Certificate	Review only the domain name for HTTPS data encryption transmission, be applicable to low-risk sites that do not involve trade or privacy information.
Extended Validation Code Signing Certificate	With hardware as the carrier, the user identifies the publisher of the software or code, supports the Windows10 kernel driver signing, and has a higher authentication level.
Organization Validation Code Signing Certificate	The user identifies the publisher of the software or code to protect the integrity of the software.
Document Signing Certificate	For Adobe document signing, you can display the signature information and verify the integrity of the document。
Secure Email Certificate	Be applicable to Email signing and encryption, protects the security of Email.

1.5 Policy Administration

1.5.1 Organization Administering the Document

The governing body of this CP&CPS is the TrustAsia CA Security PolicyCommittee, which is responsible for formulating, approving, issuing, implementing, updating and revoking this CP&CPS. The TrustAsia CA Security PolicyCommittee is composed of appropriate representatives from the management of the company who are responsible for operational security, technical security, customer service and talent security. The Committee is responsible for the daily work of the external consulting service of this policy document.

1.5.2 Contact Person

1.5.2.1 CP&CPS Contact Person

TrustAsia CA will be in strict control with the CP&CPS version and the designated department is responsible for matters related to it. Any questions, suggestions, etc. related to the CP&CPS can be contacted in the following manner.

Contact Department: Policy Department
Contact email address: 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 report and certificate revocation request must be submitted in one of the following ways, and certificate revocation request 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

TrustAsia CA Security Policy Committee is the main body of the policy formulation, and is also the highest authority to review and approve the CP&CPS.

1.5.4 CPS Approval procedure

This CP&CPS is compiled by the CP&CPS compilation team which is organized by Security Policy Committee of TrustAsia CA. When the compilation of this CP&CPS is finished, it will be submitted to Security Policy Committee for audit. After the approval by Security Policy Committee, it is published on the official website of TrustAsia CA.

This CP&CPS is revised annually in accordance with the country's policies and regulations, technical requirements, business development and the latest requirements of BR and EVG issued by CA/Browser Forum. The CP&CPS compilation team will prepare the CP&CPS revision contents according to the relevant conditions and submit to the Security Policy Committee for review. After the approval of the Committee, the version number is incremented, the release time, the effective time and the revision record are updated, and it is officially released on the website of TrustAsia CA.

1.6 Definitions and Acronyms

1.6.1 Definitions

Terms	Definitions
Security Policy Committee	It is the highest management and monitor function for CP&CPS and the decision-making agency pursuant to CP&CPS within the certification services system.
Certification Authority	An organization that is responsible for the creation, issuance, revocation, and management of certificates. The term applies equally to both Root CAs and Subordinate CAs.
Registration Authority	A Registration Authority (RA) is responsible for processing service requests from certificate applicants and certificate subscribers and submitting them to the certification authority for the final certificate applicant to establish registration process. RA is also responsible for identifying and verifying certificate applicants, initiating or transferring certificate revocation request, and approving certificate renewal or re-key request on behalf of the certification authority.

Certificate Policy	A set of named rules to indicate the applicability of certificates to a particular group or to an application type with the same security requirements. For example, a specific CP may indicate that a certain type of certificate is suitable for identifying participants engaged in enterprise-to-enterprise trading activities for products and services within a given price range.
Certification Practice Statement	One of several documents forming the governance framework in which certificates are created, issued, managed, and used.
Certification Path	An ordered sequence of certificates (containing the public key of the starting object in the path), and the public key of the end object can be obtained by processing the sequence.
Policy qualifier	Policy-dependent information may appear with CP identifiers in X.509 certificates. This information may contain the URL address of the available CP&CPS or dependency agreement, or the text of the certificate usage terms.
Certificate	An electronic document that uses a digital signature to bind a public key and an identity.
Electronic signature	It has the technical means to identify the identity of the signatory and indicate that the signatory recognizes the signature data.
Digital signature	An electronic signature implemented by encrypting and decrypting an electronic record using an asymmetric cryptographic system.
Electronic signature person	A person who holds an electronic signature and carries out an electronic signature in his or her name.
Electronic signature relying party	A person engaged in an activity based on a trust of an electronic signature certification or an electronic signature.
Public Key Infrastructure	A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of certificates and keys based on public key cryptography.
Key pair	Private key and associated public key
Private Key (Digital signature creation data)	The key of a key pair that is kept secret by the holder of the key pair, and that is used to create digital signatures and/or to decrypt electronic records or files that were encrypted with the corresponding public key.
Public Key (digital signature verification data)	The key of a key pair that may be publicly disclosed by the holder of the corresponding private key and that is used by a relying party to verify digital signatures created with the holder's corresponding private key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding private key.
Subscriber	A natural person or legal entity to whom a certificate is issued and who is legally bound by a Subscriber agreement.
Subscriber Agreement	An agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties.
Relying Party	Any natural person or legal entity that relies on a valid certificate. A relying party may or may not be a Subscriber.
Relying Party Agreement	An agreement that must be read and accepted by the relying party before verifying, relying on or using a certificate or accessing or using TrustAsia Information Base.

WebTrust	The current version of CPA Canada's WebTrust Program for Certification Authorities.
WHOIS	The agreement, as defined in RFC 3912, the registry data access protocol as defined in RFC 7482, or the information that the HTTPS website directly acquires from a domain name registrar or a registered management executing agency.
P-Label	A XN-Label that contains valid output of the Punycode algorithm (as defined in RFC 3492, Section 6.3) from the fifth and subsequent positions.
LDH-Label	From RFC 5890 (http://tools.ietf.org/html/rfc5890): "A string consisting of ASCII letters, digits, and the hyphen with the further restriction that the hyphen cannot appear at the beginning or end of the string. Like all DNS labels, its total length must not exceed 63 octets."

1.6.2 Acronyms

BR	Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates	公信证书的签发和管理基准要求
CA	Certification/Certificate Authority	电子认证服务机构
CAA	Certification Authority Authorization	认证机构授权
ccTLD	Country Code Top-Level Domain	国家顶级域名
CP	Certificate Policy	证书策略
CPS	Certification Practice Statement	电子认证业务规则
CRL	Certificate Revocation List	证书撤销列表
CSR	Certificate Signing Request	证书请求文件
DBA	Doing Business As	商业名称
DN	Distinguished Name	甄别名
DNS	Domain Name System	域名系统
EV	Extended Validation	扩展验证/增强验证
EVG	Guidelines for the Issuance and Management of Extended Validation Certificates	扩展验证证书签发与管理指南
FIPS	(US Government) Federal Information Processing Standard	(美国政府)联邦信息处理标准
FQDN	Fully Qualified Domain Name	完全限定域名
gTLD	Generic Top-Level Domain	通用顶级域名
IANA	Internet Assigned Numbers Authority	互联网编码分配机构
ICANN	Internet Corporation for Assigned Names and Numbers	互联网名字与编号分配机构
KM	Key Management	密钥管理
LDAP	Lightweight Directory Access Protocol	轻量级目录访问协议
LRA	Local Registration Authority	本地注册机构
OCSP	Online Certificate Status Protocol	在线证书状态协议
OID	object identifier	对象标识符
OSCCA	State Cryptography Administration Office of Security Commercial Code Administration of China	中国国家商用密码管理办公室
PIN	Personal Identification Number	个人身份识别码
PKCS	Public KEY Cryptography Standards	公共密钥密码标准
PKI	Public Key Infrastructure	公钥基础设施
RA	Registration Authority	注册机构

RFC	Request for Comments	请求评注标准(一种互联网建议标准)
SSL	Secure Sockets Layer	安全套接字
S/MIME	Secure/Multipurpose Internet Mail Extensions	安全/多用途邮件扩展
TLS	Transport Layer Security	传输层安全
TTL	Time to Live	IP 包的生存时间
X.509	The ITU-T standard for Certificates and their corresponding authentication	ITU-T 证书标准及其相应的认证

1.6.3 References

- The RFC3647 standard issued by the Internet Engineering Task Force (IETF)
- The following latest requirements released by the CA/Browser Forum (https://cabforum.org/) (prior to this CP&CPS):
  - Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates.
  - Network and Certificate System Security Requirements
  - Guidelines for the Issuance and Management of Extended Validation Certificates
  - Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates
  - Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates
- Mozilla Root Store Policy
- Microsoft Trusted Root Program
- AATL Technical Requirements
- Apple Root Certificate Program
- Chrome Root Program
- 360 Browser Root Certificate Program
- Oracle 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 CP&CPS shall be interpreted in accordance with RFC 2119.

This document omits time and time zones when listing effective requirements such as dates. Except when explicitly specified, the associated time with a date shall be 00:00:00 UTC+8 (Beijing Time).

2. Publication and Repository Responsibilities

2.1 Repositories

TrustAsia CA repositories are open to the public. It provides information services to subscribers and certificate application dependents. The repositories include, but is not

limited to, the following: CP&CPS, CRL, Subscriber Agreement, Dependent Party Agreement, Root Certificate, Intermediate CA Certificate and other information published as necessary by TrustAsia CA.

2.2 Publication of Information

2.2.1 Publication of Repositories

TrustAsia CA repositories will be posted on the official website (https://www.trustasia.com/cps) in a timely manner or in other possible forms as needed. The contents of the release include CA certificates, CP&CPS amendments and other materials, which must be consistent with CP&CPS and related laws and regulations.

2.2.2 Publication of CRL

TrustAsia CA issues a Subscriber's certificate and certificate revocation list (CRL) through HTTP. The Subscriber or relying party may obtain the CRL information from the CRL distribution point address in the certificate issued by TrustAsia CA. Each CRL issued by TrustAsia CA contains an incremental serial number.

2.2.3 Publication of OCSP

TrustAsia CA provides Online Certificate Status Protocol (OCSP). Subscribers or relying parties can query the status information of certificates in real time.

2.3 Time or Frequency of Publication

2.3.1 Time or Frequency of Publication of CPS

TrustAsia CA CP&CPS can be obtained through repositories by 7d*24h. The release of CP&CPS is at least once every 365 days.
TrustAsia CA will follow the changes of the CA/Browser Forum standard on a regular basis and adjust the CP&CPS in a timely manner to meet the standard.

2.3.2 Time or Frequency of Publication of CRL

TrustAsia CA publishes CRL for Subscriber certificates on a daily basis; CRL for child CA certificates at least once every12 months. If the condition is that the child CA certificate being revoked occurs, the CRL for CA certificate must be updated within 24 hours.

2.4Access Controls on Repositories

The information in TrustAsia CA repositories is provided with query and access in a read-only manner.
With network security, secure system design and security policy, TrustAsia CA ensures that only authorized employees can add, delete, modify and publish the repositories.
All versions of CP&CPS, including the version history, will be disclosed in repositories.

3. Identification and Authentication

3.1 Naming

3.1.1 Type of Names

The digital certificate issued by TrustAsia CA complies with the X.509 standard and is assigned to the unique distinguished name of the certificate holder and is named in the X.500 standard. Its naming practices are compliant with RFC 5280, the Baseline Requirements, and the EVG. The certificate of TrustAsia CA contains the identification of the issuer and the certificate Subscriber's principal, identifies the identity and other attributes of the certificate applicant, and records its information in a different identification. The identity of the certificate holder is named and is included in the certificate subject in the form of a distinguished name and is the only distinguished name of the certificate holder.

For SSL/TLS server certificates, all domain names or IP addresses are added to the subject alias, while the Common Name is the primary or IP address and must be a domain name or IP address that appears in the subject alias. For Internationalized Domain Names (IDNs), TrustAsia CA may include the punycode version of the IDN as a subject name or subject alternative name.

In the subjectAltName extension or subject:commonName field of SSL/TLS server certificates, the reserved private IP addresses or internal names will not be included in them. In the dNSName entries of the certificate, the underscore ("_") characters will not be included in them.

For OV SSL/TLS server certificates, all domain names or IP addresses are added to the subject alias, while the Common Name is the primary or IP address and must be a domain name or IP address that appears in the subject alias.

In the subjectAltName extension or subject:commonName field of DV and EV SSL/TLS server certificates, IP addresses will not be included. EV SSL/TLS server certificates do not contain wildcard.

The naming rules and requirements of all types of certificates are documented in this CP&CPS and comply with the requirements of CA/Browser Forum.

Naming rules of issuer's DN are as follows:

Attribute	Value
Country (C)	CN
State (ST)	State of issuer (if included)
Locality (L)	Locality of issuer (if included)
Organization (O)	TrustAsia Technologies, Inc.
Common Name (CN)	Name of CA

Naming rules of Subscriber's DN are as follows:

Attribute	Value
Country (C)	Country or Region Code of Subscriber
State (ST)	State of Subscriber (if included)

Locality (L)	Locality of Subscriber (if included)
Organization (O)	Name of the Subscriber's organization
Organization Unit (OU)	Name of the Subscriber's organization unit (Document Signing Certificates)
Organization Identifier (OI)	Registration Reference for the organization (Organization-validated S/MIME Certificates)
Given Name (givenName)	An individual's legal given name (Individual-validated S/MIME Certificates and Organization-validated S/MIME Certificates that contain individual information)
Surname (surname)	An individual's legal surname (Individual-validated S/MIME Certificates and Organization-validated S/MIME Certificates that contain individual information)
Pseudonym (pseudonym)	An individual's pseudonym (Organization-validated S/MIME Certificates that contain individual information)
Email (E)	Subscriber's email address (if included)
Common Name (CN)	Domain name (SSL/TLS server certificate), organization name (Organization-validated certificate), individual name (Individual-validated certificate), or other identifiable names.

Naming rules of EV certificate Subscriber's DN are as follows:

Attribute	Value
Country (C)	Country or Region Code of Subscriber
State (ST)	State/Province of Subscriber (if included)
Locality (L)	Locality of Subscriber (if included)
Organization (O)	Name of Subscriber's legal organization
Business Category	Types of business: Private Organization, Government Entity, Business Entity and Non-Commercial Entity
Jurisdiction Country Name	Country Code of Subscriber's Jurisdiction of Incorporation or Registration Agency
Jurisdiction State Or Province Name	State or Province of Subscriber's Jurisdiction of Incorporation or Registration Agency
Jurisdiction Locality Name	Locality of Subscriber's Jurisdiction of Incorporation or Registration Agency
Serial Number	Subscriber's Registration Number/Subscriber's Incorporation or Registration Date
Common Name (CN)	Domain name (SSL/TLS server certificate), Organization Name (Organization-validated certificate), or other identifiable names.

3.1.2 Need for Names to be Meaningful

TrustAsia CA uses the DN (Distinguished Name) to identify the entity that is the subject of the certificate and the entity is the issuer of the certificate, The names in the DN have representative meanings and can be related to the identities and specific properties of the final entities that use the certificates. The common name identifies the end entity's particular name mentioned by this certificate. Identifier describes information of the specified entity with bound public key.

The name contained in Subscriber certificate has certain representative significance, and the principal identification name contained in it should be able to clearly determine the certificate holder and the network host server to be identified, or the Internet domain name, and can be identified by the relying party. The Distinguished Name of the subject shall comply with the requirements of laws and regulations and other relevant provisions.

1. The DNs to be used in DV SSL/TLS Server Certificates and S/MIME Basic Certificates include: domain names, public network IP or email addresses owned by the Subscriber, authenticated and verified as the critical information to identify the Subscriber
2. The DNs to be used in Individual-validated Document Signing Certificates and Individual-validated S/MIME Certificates include: email address owned by the Subscriber (S/MIME Certificates) and Subscriber's individual identity information, authenticated and verified as the critical information to identify the Subscriber
3. The DNs to be used in OV SSL/TLS Server Certificates, Code Signing Certificates, Organization-validated Document Signing Certificates and Organization-validated S/MIME Certificates include: domain names, public network IP (SSL/TLS Server Certificates) or email addresses (S/MIME Certificates), Subscriber's organization identity information and Subscriber's individual identity information (Organization-validated Document Signing Certificates that contain individual information, Sponsor-validated S/MIME Certificates), authenticated and verified as the critical information to identify the Subscriber
4. The DNs to be used in EV SSL/TLS Server Certificates and EV Code Signing Certificates include: domain names owned by the Subscriber (EV SSL/TLS Server Certificates) and Subscriber's organization identity information, authenticated and verified as the critical information to identify the Subscriber

3.1.3 Anonymity or pseudonymity of Subscribers

Subscribers of certificates described in this CP&CPS must use real names when applying for certificates. However, for Sponsor-validated S/MIME certificates, the value of DN can use assumed name for organization name, pseudonym for individual information; for Organization-validated S/MIME certificates, the value of DN can use assumed name for organization name. Both organization's assumed name and individual's pseudonym must be authenticated and validated by TrustAsia CA.

3.1.4 Rules for Interpreting Various Name Forms

A certificate issued by TrustAsia CA conforms to X.509 V3. The format of DN conforms to X.500, and naming rules of DN are defined by TrustAsia CA.

3.1.5 Uniqueness of Names

DN of certificate must be unique for different subscribers in TrustAsia CA trust domain, and same DNs cannot be allowed as the subject name of the certificates of different Subscribers. TrustAsia CA can issue more than one certificates using the unique DN for one Subscriber. When DN is not unique to different subscribers, the first applicant has the priority to use the DN, and the latter could add more additional information to distinguish from others.
The uniqueness of each subject name in the certificate is as follows:

SSL/TLS server certificate	The uniqueness of domain name is controlled by ICANN, an Internet name and digital address assignment organization.
S/MIME certificate	Requiring a unique email address combined or associated with a unique serial number.
Code Signing certificate	Requiring a unique organization name combined or associated with a unique serial number.
Document Signing certificate	Requiring a unique organization name combined or associated with a unique serial number.
Timestamp certificate	A unique hash and time or unique serial number is required to be assigned to the time stamp.

3.1.6 Recognition, Authentication, and Role of Trademarks

The certificate applicant shall not use names that may infringe upon others' intellectual property rights in their certificate application. The certificate issued by TrustAsia CA does not verify the Subscriber's right to use the trademark, nor responsible for resolving any trademark related disputes. TrustAsia CA can reject or revoke the relevant certificate in dispute with the trademark.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

The certificate applicant must prove that he or she properly holds the private key corresponding to the public key contained in the certificate by submitting the digitally signed PKCS#10 format Certificate Signature Request (CSR), or by signing the CSR provided to the Finalize method of the ACME Protocol defined in RFC 8555, Section 7.4.

3.2.2 Authentication of Organization and Domain Identity

3.2.2.1 Validation of the identity of the organization

Any organization (government agencies, public institutions, etc.), when applying for institution-based certificates in the name of the organization, should conduct strict identity authentication, such as verifying the authenticity of the trust database by querying the trusted database, identifying the identity material submitted by the applicant and other means of obtaining the applicant's clear identity information. The signature (official seal) of the applicant's own or the duly authorized certificate applicant's representative on the certificate application form of the institution-based Subscriber shall bear the relevant provisions of the certificate application and bear the corresponding responsibility.

For all certificates that contain organizational identity information, TrustAsia CA verifies the name and registration/business address of the organization. TrustAsia CA can perform different authentication methods according to the type of certificate requested by the organization, and the authentication methods refers to the CA/Browser Forum BR and EVG. Generally speaking, the higher the certificate category, the higher the security level. The stricter the authentication

method, and the more comprehensive the authentication content. TrustAsia CA selects one or more of the following items to verify the identity and address information of the organization:

1. An effective document issued by a government agency (including, but not limited to, a business license, a public institution legal person certificate, a unified social credit code certificate, etc.) or by issuing an authoritative third-party database of an effective document to confirm that the organization is a real, legal entity.
2. Obtain the address and contact information of the organization through the trusted third-party database, and contact the organization in the form of telephone, e-mail, postal letter, etc., so as to confirm the authenticity of the information provided by the applicant.
3. Validation of information through certified letters from qualified lawyers, accountants, etc.
4. Confirm the organization's address information through property bills, bank statements, government-issued tax bills, or other TrustAsia CA approved verification methods.
5. The third party is entrusted with the investigation of the organization, or the applicant is required to provide additional information and proof of the material.

In addition, if necessary, TrustAsia CA also sets up other required authentication methods and data. The applicant has an obligation to ensure the authenticity and validity of the application materials and to bear the relevant legal liability.
For Subscriber certificates issued by TrustAsia CA, TrustAsia CA establishes evaluation criteria to identify potentially high-risk fraud certificate requests. TrustAsia CA can directly reject certificate requests identified as "high risk".

3.2.2.1.1 Validation of Organization Identity for EV Certificates

1. Application requirements for EV Certificates
   TrustAsia CA does not issue EV certificates for IP addresses, wildcard domains and individuals. Organizations that make a request for an EV certificate should arrange the following roles to coordinate with TrustAsia CA for certificate issuance.
   a. Certificate Requester: The submitter of the EV certificate request and the person to contact with. A Certificate Requester is a natural person who is either an employee of the Applicant or an authorized agent who has express authority on behalf of the Applicant to submit an EV certificate request.
   b. Certificate Approver: The approver to approve the EV certificate request. A Certificate Approver is a natural person who is either an employee of the Applicant or an authorized agent who has express authority to represent the Applicant to approve the request.
   c. Contract Signer: The signer of the Subscriber Agreement. A Contract Signer is a natural person who is either an employee of the Applicant or an

authorized agent who has express authority to represent the Applicant to sign the Subscriber Agreement.

The Applicant may authorize one individual to occupy two or more of these roles. The Applicant may authorize more than one individual to occupy any of these roles.

2. Subject Distinguished Name Fields Requirements for EV Certificates
   a. subject:organizationName (OID 2.5.4.10) ; TrustAsia CA only accepts an effective document issued by an Incorporating Agency or Registration Agency (including but not limited to, a business license, a public institution legal person certificate, a unified social credit code certificate, etc.), or the name of the legal organization obtained through the database of an authoritative third-party who issues effective documents. The length limit for the text in the field is 64 characters. If the organization name by itself exceeds 64 characters, TrustAsia CA may abbreviate parts of the organization name, and/or omit non-material words in the organization name in such a way that the text in this field meets the length limit; provided that the abbreviations used are not misleading in the Jurisdiction of Incorporating Agency or Registration Agency and a Relying Party will not be misled into thinking that they are dealing with a different organization.
   b. subject:commonName (OID 2.5.4.3) ; For server certificates, TrustAsia CA only accepts a single Domain Name(s) owned or controlled by the Subject and to be associated with the Subject's server; IP address and wildcard are not allowed for EV Certificates. For code signing certificates, the text in this field shall be consistent with the text in the subject:organizationName (OID: 2.5.4.10) field.
   c. subject:businessCategory (OID: 2.5.4.15); TrustAsia CA categorizes the Applicant's business into four categories and identifies the category in the Subject. The four categories are "Private Organization", "Government Entity", "Business Entity" and "Non-Commercial Entity". TrustAsia CA verifies the Applicant's legal existence and identity in different ways according to its business category.
   d. subject:jurisdictionLocalityName (OID: 1.3.6.1.4.1.311.60.2.1.1); subject:jurisdictionStateOrProvinceName (OID: 1.3.6.1.4.1.311.60.2.1.2); subject:jurisdictionCountryName (OID: 1.3.6.1.4.1.311.60.2.1.3) TrustAsia CA has disclosed the values within these fields in the public document "Incorporating Agency and Registration Agency List V1.0" in its official website. These fields must not contain information that is not relevant to the level of the Incorporating Agency or Registration Agency. For example: The Jurisdiction of Incorporation for an Incorporating Agency or Jurisdiction of Registration for a Registration Agency that operates at the country level must include the country information (subject:jurisdictionCountryName) but must not include the state or province (subject:jurisdictionStateOrProvinceName) or locality information (subject:jurisdictionLocalityName). Similarly,

the Jurisdiction for the applicable Incorporating Agency or Registration Agency at the state or province level must include both country (subject:jurisdictionCountryName) and state or province information (subject:jurisdictionStateOrProvinceName), but must not include locality information (subject:jurisdictionLocalityName).
And, the Jurisdiction for the applicable Incorporating Agency or Registration Agency at the locality level must include all of these three fields information.

e. subject:serialNumber (OID: 2.5.4.5) ; TrustAsia CA has also disclosed the values within this field in the public document "Incorporating Agency and Registration Agency List V1.0" in its official website. TrustAsia CA only fills the Registration Number of the Jurisdiction of Incorporation or Registration in this field. If the jurisdiction of Incorporation or Registration does not provide a Registration Number, then the date of Incorporation or Registration shall be entered into this field.

To authenticate d and e fields, TrustAsia CA only accepts an effective document issued by an Incorporating Agency or Registration Agency (including but not limited to, a business license, a public institution legal person certificate, a unified social credit code certificate, etc.), or the information obtained through the database of an authoritative third-party that issues effective documents.

f. subject:localityName (OID: 2.5.4.7); subject:stateOrProvinceName (OID: 2.5.4.8); subject:countryName (OID: 2.5.4.6) In these fields, TrustAsia CA fills the physical address of the Subject's place of business or registration in this field. To confirm the physical location, TrustAsia CA verifies the information in accordance with Section 3.2.2.1.
g. subject:organizationalUnitName (OID: 2.5.4.11) is not included in TrustAsia CA EV certificate's DN.

TrustAsia CA does not include any other Subject Distinguished Name attributes except as specified in the EVG Section 9.2.

3. Verification Requirements for EV Certificates
   a. Verification of the Applicant Roles
      For EV certificates, TrustAsia CA verifies the name, title and authority of Certificate Requester, Certificate Approver and Contract Signer; and checks whether he or she is listed on the denial list or prohibited list of China. If he or she is listed, TrustAsia CA reserves the right to refuse to issue the certificate or ask for another person to contact with. TrustAsia CA will choose an appropriate method from the communication means in Section 3.2.2.1 to get connected with Certificate Requester or Certificate Approver and obtain an affirmative response sufficient to confirm the information accuracy.
   b. Verification of Signature on Subscriber Agreement and Certificate Requests

For EV certificates, TrustAsia CA requires that both the Subscriber Agreement and the Certificate Request must be signed. The Certificate Request must be signed by the Certificate Requester, and the Subscriber Agreement must be signed by an authorized Contract Signer. An authorized Certificate Approver must approve the Certificate Request. For the signing of Subscriber Agreement and Certificate Request, TrustAsia CA requires the Subscribers to complete signing in the order placement page; for the approval of Certificate Request by Certificate Approver, TrustAsia CA will send a link via email for online approval. TrustAsia CA will authenticate the signature in the process of validation.

c. Verification of the Applicant's ability to engage in business
For EV certificates, TrustAsia CA not only confirms the organization's legal and physical existence but also verifies the applicant's ability to engage in business. TrustAsia CA verifies the applicant's ability through verifying the operational existence of the Applicant, or its Affiliate/Parent/Subsidiary Company, by:
   i. Verifying that the Applicant, Affiliate, Parent Company, or Subsidiary Company has been in existence for at least three years, as indicated by the records of an Incorporating Agency or Registration Agency;
   ii. Verifying that the Applicant, Affiliate, Parent Company, or Subsidiary Company is listed in either a current QIIS or QTIS;
   iii. Verifying that the Applicant, Affiliate, Parent Company, or Subsidiary Company has an active current Demand Deposit Account with a Regulated Financial Institution by receiving authenticated documentation of the Applicant's, Affiliate's, Parent Company's, or Subsidiary Company's Demand Deposit Account directly from a Regulated Financial Institution; or
   iv. Relying on a Verified Professional Opinion Letter to the effect that the Applicant has an active current Demand Deposit Account with a Regulated Financial Institution.

d. Verification of Principal Individual of a Business Entity
For a Business Entity to request an EV certificate, TrustAsia CA requires the Principal Individual of the entity as the Certificate Approver. A Principal Individual can be an owner, legal representative, investor, director, or someone authorized in written form by such entity to take the role of Principal Individual. TrustAsia CA arranges a face-to-face validation with the Principal Individual in accordance with the requirements set forth in the EVG Section 11.11.3. The methods of face-to-face validation (those equivalent to face-to-face validation) include but are not limited to a video call, a video recording, in-person face-to-face validation, etc. During the face-to-face validation process, "Principal Individual" needs to provide government-issued identification documents and at least two secondary documentary evidences to verify his/her identity, one of which must be from a financial institution. Acceptable documents refer to the requirements

defined in EVG Section 11.2.2. “Principal Individual” needs to provide the original documents mentioned above as per the request by the validator and sign the application document about personal statement on the spot to complete validation

3.2.2.1.2 Validation of Organization Identity for Organization-validated S/MIME Certificates

1. Application Requirements
   Authentication of organization identity is required when applying for Organization-validated or Sponsor-validated S/MIME Certificates. The level of authentication requirements equals to that of other organization validation certificates. TrustAsia CA performs validation of the Applicant in accordance with the methods listed in Section 3.2.2.1.
2. Subject Distinguished Name Fields Requirements (Organization identity authentication)
   a. subject:commonName (OID:2.5.4.3) For Organization-validated S/MIME Certificates, TrustAsia CA only accepts the contents of subject:organizationName (OID:2.5.4.10); for Sponsor-validated S/MIME Certificates, TrustAsia CA accepts natural person’s legal name or pseudonym as the value of the field.
   b. subject:organizationName (OID:2.5.4.10) TrustAsia CA accepts the Subject’s full legal organization name and/or an Assumed Name as verified under Section 3.2.2.1. If both are included, the Assumed Name appears first, followed by the full legal organization name in parentheses. The value of the field must not exceed 64 characters. If exceeded, TrustAsia CA will abbreviate parts of the organization name, and/or omit non-material words in the organization name in such a way that the text in this field meets the length limit; provided that the abbreviations used are not misleading in the Jurisdiction of Incorporating Agency or Registration Agency and a Relying Party will not be misled into thinking that they are dealing with a different organization.
   c. subject:organizationIdentifier (OID:2.5.4.97) This field contains a Registration Reference for a Legal Entity assigned in accordance to the identified Registration Scheme. The specific contents include 3-character Registration Scheme identifier, 2-character country code, 2-character identifier for the subdivision of the nation and Registration Reference. Registration Scheme identifier includes NTR (National Trade Register), VAT (Value Added Tax), PSD (Payments Services Directive), LEI (Legal Entity Identifier), GOV (Government Entity) and INT (International Organization).
   d. subject:emailAddress (OID:1.2.840.113549.1.9.1) TrustAsia CA fills the email address for which the Subject applies certificate in this field. The email address will be verified under Section 3.2.2.9.

e. subject:stateOrProvinceName (OID:2.5.4.8); subject:localityName (OID:2.5.4.7); subject:countryName (OID:2.5.4.6) TrustAsia CA fills the physical address of the Applicant's place of business or registration in these fields. TrustAsia CA verifies the physical address under Section 3.2.2.1.

3. Verification Requirements
   a. Verification of Organization Information
      TrustAsia CA verifies the full legal name, operation status, registration agency and registration number, and business address of the Applicant. Verification methods and sources are the same as other organization validation certificates.
   b. Use of LEI Data
      In the case of organization information verification for Organization-validated or Sponsor-validated S/MIME Certificates, an LEI data reference can be used as a verification source with no region limitation. If an LEI data reference is used, the RegistrationStatus must be ISSUED, EntityStatus must be ACTIVE and ValidationSources must be FULLY_CORROBORATED. If ValidationSources entry is PARTIALLY_CORROBORATED, PENDING, or ENTITY_SUPPLIED_ONLY, an LEI cannot be used.
   c. Verification of Assumed Name
      TrustAsia CA accepts an Assumed Name when the Applicant applies for an Organization-validated or Sponsor-validated Certificates. TrustAsia CA imposes restrictions on Assumed Names, and only accepts stock short name of public companies or trademark names (only texts, images are not allowed) registered in the Trademark Office of National Intellectual Property Administration as the Assumed Name. In addition, if TrustAsia CA is aware of any possibility of the Assumed Name being ambiguous or repetitive, TrustAsia CA reserves the right to reject the certificate request that uses the certain Assumed Name.
   d. Verification of Unique Identifier
      TrustAsia CA verifies the Applicant's Registration Agency and Registration Number as the evidence of the field subject:organizationIdentifier (OID:2.5.4.97). TrustAsia CA obtains the related information through trusted verification sources and enters the identifier in accordance with the requirements specified in Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates. The specific verification sources have been disclosed in the Validation Resources in TrustAsia CA official website.
   e. Verification of Application Authorization
      When performing validation for Organization-validated S/MIME Certificates, TrustAsia CA will choose an appropriate method from the communication means in Section 3.2.2.1 to get connected with Certificate Requester and obtain an affirmative response sufficient to confirm the information accuracy.

3.2.2.1.3 Validation of Organization Identity for Organization-validated Document Signing Certificates

1. Application Requirements
   The level of authentication requirements of Organization-validated Document Signing Certificates equals to that of other organization validation certificates. TrustAsia CA performs validation of the Applicant in accordance with the methods listed in Section 3.2.2.1. For the Applicant that applies for Organization-validated Document Signing Certificate, apart from regular validation, TrustAsia CA performs face-to-face validation with the Certificate Requester.
2. Subject Distinguished Name Fields Requirements (Organization identity authentication)
   a. subject:commonName (OID:2.5.4.3); For Organization-validated Document Signing Certificates, TrustAsia CA only accepts the contents of subject:organizationName (OID:2.5.4.10); for Organization-validated Document Signing Certificates including individual information, TrustAsia CA only accepts the value of the fields subject:givenName (OID:2.5.4.42) with subject:surname (OID:2.5.4.4).
   b. subject:organizationName (OID:2.5.4.10); TrustAsia CA accepts an effective document issued by an Incorporation or Registration Agency (including but not limited to, a business license, a public institution legal person certificate, a unified social credit code certificate, etc.), or the information obtained through the database of an authoritative third-party that issues effective documents. The value of the field must not exceed 64 characters. If exceeded, TrustAsia CA will abbreviate parts of the organization name, and/or omit non-material words in the organization name in such a way that the text in this field meets the length limit; provided that the abbreviations used are not misleading in the Jurisdiction of Incorporating Agency or Registration Agency and a Relying Party will not be misled into thinking that they are dealing with a different organization.
   c. subject:stateOrProvinceName (OID:2.5.4.8); subject:localityName (OID:2.5.4.7); subject:countryName (OID:2.5.4.6) TrustAsia CA fills the physical address of the Applicant's place of business or registration in these fields. TrustAsia CA verifies the physical address under Section 3.2.2.1.
   d. subject:organizationalUnitName (OID: 2.5.4.11): TrustAsia CA fills in the full legal name of the affiliate of subject:organizationName in this field and performs validation with the methods defined in Section 3.2.2.1. TrustAsia CA can also fill in the name of Compliance Department of subject:organizationName in this field and the Applicant needs to provide supporting documents to verify such department name.
3. Verification Requirements
   a. Verification of Organization Information
      TrustAsia CA verifies the full legal name, operation status, registration agency and registration number, and business address of the Applicant.

Verification methods and sources are the same as other organization validation certificates.

b. Verification of Application Authority
When performing validation for Organization-validated Document Signing Certificates, TrustAsia CA will choose an appropriate method from the communication means in Section 3.2.2.1 to get connected with Certificate Requester and obtain an affirmative response sufficient to confirm the information accuracy.

c. Face-to-Face Validation
After authority verification is completed, TrustAsia CA performs a face-to-face validation with the Certificate Requester in accordance with the requirements set forth in the EVG Section 11.11.3. The methods of face-to-face validation (those equivalent to face-to-face validation) includes but are not limited to a video call, a video recording, in-person face-to-face validation, etc. In the process of face-to-face validation, the Certificate Requester is required to present his/her original ID document and sign the application document about personal statement on the spot to complete validation. In the case of applying for a Sponsor-validated Document Signing Certificate, the Individual included in the certificate is required to complete the face-to-face validation.

3.2.2.2 DBA/Tradename

Not applicable.

3.2.2.3 Validation of Country

If the certificate subject item contains a country field, TrustAsia CA will confirm the host country through the organization approval information provided by the applicant under the Section 3.2.2.1 of CP&CPS.

3.2.2.4 Validation of Domain Authorization or Control

When the user applies for an SSL certificate, TrustAsia CA verifies the Applicant's control of the domain name in the certificate applied for. The validation process is conducted by TrustAsia CA and will not be delegated to third parties.
TrustAsia CA does not support the validation of domains with .onion as the right-most Domain Label, and does not issue certificates to such domains.
TrustAsia CA maintains a record of the domain validation method used for each domain and the relevant BR version number.

3.2.2.4.1 Validating the Applicant as a Domain Contact

TrustAsia CA does not support this method.

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

In accordance with the definitions in BR Section 3.2.2.4.2, TrustAsia CA confirms the control over the domain name by sending a verification email to the Whois contact email. A unique Random Value is included in the verification email. The Subscriber visits the verification link containing the Random Value and click for approval to complete domain control validation.

The unique Random Value is generated by TrustAsia CA and its validity period is no more than 30 days from its creation. This method is suitable for validating wildcard domain names.

3.2.2.4.3 Phone Contact with Domain Contact

TrustAsia CA does not support this method.

3.2.2.4.4 Constructed Email to Domain Contact

In accordance with the definitions in BR Section 3.2.2.4.4, send a constructed email to domain contact.

Confirm the Applicant's control over the FQDN by

a. Sending an email to one or more addresses created by using "admin", "administrator", "webmaster", "hostmaster", or "postmaster" as the local part, followed by the at-sign ("@"), followed by an Authorization Domain Name; and
b. Including a Random Value in the email; and
c. The Applicant submitting (either by clicking or other means) Random Value to TrustAsia CA server to confirm receiving and authorization.

The unique Random Value is generated by TrustAsia CA and its validity period is no more than 30 days from its creation. This method is suitable for validating wildcard domain names.

3.2.2.4.5 Domain Authorization Document

TrustAsia CA does not support this method.

3.2.2.4.6 Agreed-Upon Change to Website

TrustAsia CA does not support this method.

3.2.2.4.7 DNS Change

In accordance with the definitions in BR Section 3.2.2.4.7, TrustAsia CA confirms the Applicant's control over the domain name by confirming the presence of a Random Value in a TXT or CNAME record.

The unique Random Value is generated by TrustAsia CA and its validity period is no more than 30 days from its creation. Once the FQDN has been validated using this method, TrustAsia CA issues certificates for this FQDN and other FQDNs that end with all the Domain Labels of the validated FQDN. This method is suitable for validating wildcard domain names.

3.2.2.4.8 IP Address

TrustAsia CA does not support this method.

3.2.2.4.9 Test Certificate

TrustAsia CA does not support this method.

3.2.2.4.10 TLS Using a Random Number

TrustAsia CA does not support this method.

3.2.2.4.11 Any other Method

TrustAsia CA does not support this method.

3.2.2.4.12 Validating Applicant as a Domain Contact

TrustAsia CA does not support this method.

3.2.2.4.13 Email to DNS CAA Contact

TrustAsia CA does not support this method.

3.2.2.4.14 Email to DNS TXT Contact

In accordance with the definitions in BR Section 3.2.2.4.14, TrustAsia CA sends a verification email to a DNS TXT Record Email Contact for the Authorization Domain Name selected to validate the FQDN, that is "validation-contactemail.ADN". A unique Random Value is included in the verification email. The Subscriber visits the verification link containing the Random Value and click for approval to complete domain control validation.
The unique Random Value is generated by TrustAsia CA and its validity period is no more than 30 days from its creation. Once the FQDN has been validated using this method, TrustAsia CA issues certificates for this FQDN and other FQDNs that end with all the Domain Labels of the validated FQDN. This method is suitable for validating wildcard domain names.

3.2.2.4.15 Phone Contact with Domain Contact

TrustAsia CA does not support this method.

3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact

TrustAsia CA does not support this method.

3.2.2.4.17 Phone Contact with DNS CAA Phone Contact

TrustAsia CA does not support this method.

3.2.2.4.18 Agreed-Upon Change to Website v2

In accordance with the definitions in BR Section 3.2.2.4.18, the Subscriber puts the specified verification file and a Random Value under the "/.well-known/pki-validation" directory of the Authorization Domain Name. If TrustAsia CA successfully accesses the specified verification contents over the default ports of HTTP/HTTPS protocol, then the Applicant's control over the FQDN is confirmed. The unique Random Value is generated by TrustAsia CA and its validity period is no more than 30 days from its creation. Once the FQDN has been validated using this method, TrustAsia CA issues certificates only for this FQDN. This method is not suitable for validating wildcard domain names. Redirects must be initiated at

the HTTP protocol layer. TrustAsia CA supports the redirects that are the result of a 301, 302 HTTP status code response. Redirects must be to resource URLs with either the “http” or “https” scheme, and must be to resource URLs accessed via Authorized Ports.

3.2.2.4.19 Agreed-Upon Change to Website – ACME

In accordance with the definitions in BR Section 3.2.2.4.19, TrustAsia CA confirms the Applicant’s control over a FQDN by validating domain control of the FQDN using the ACME HTTP Challenge method defined in Section 8.3 of RFC 8555.
The token (as defined in RFC 8555, Section 8.3) is generated by TrustAsia CA and its validity period is no more than 30 days from its creation.
Redirects must be initiated at the HTTP protocol layer. TrustAsia CA supports the redirects that are the result of a 301, 302 HTTP status code response. Redirects must be to resource URLs with either the “http” or “https” scheme, and must be to resource URLs accessed via Authorized Ports. This method is not suitable for validating wildcard domain names.

3.2.2.4.20 TLS Using ALPN

TrustAsia CA does not support this method.

3.2.2.5 Authentication for IP Address

TrustAsia CA accepts Subscribers to apply for SSL certificates using public IP, and public IP is not used to issue Domain Validation and Extended Validation certificates. The IP address used to apply for the certificate must be IANA compliant and cannot be a reserved IP.
TrustAsia CA maintains a record of the IP validation method used for each IP address and the relevant BR version number.

3.2.2.5.1 Agreed-Upon Change to Website

In accordance with the definitions in BR Section 3.2.2.5.1, the Subscriber puts the specified verification file and a Random Value under the “/.well-known/pki-validation” directory on the requested IP Address.
If TrustAsia CA successfully accesses the specified verification contents over the default ports of HTTP/HTTPS protocol, then the Applicant’s control over the requested IP Address is confirmed. The unique Random Value is generated by TrustAsia CA and its validity period is no more than 30 days from its creation.

3.2.2.5.2 Email, Fax, SMS, or Postal Mail to IP Address Contact

TrustAsia CA does not support this method.

3.2.2.5.3 Reverse Address Lookup

TrustAsia CA does not support this method.

3.2.2.5.4 Any Other Method

TrustAsia CA does not support this method.

3.2.2.5.5 Phone Contact with IP Address Contact

TrustAsia CA does not support this method.

3.2.2.5.6 ACME “http-01” method for IP Addresses

In accordance with the definitions in BR Section 3.2.2.5.6, TrustAsia CA confirms the Applicant’s control over the IP Address by performing the procedure documented for an “http-01” challenge in draft 04 of “ACME IP Identifier Validation Extension”, available at https://tools.ietf.org/html/draft-ietf-acme-ip-04#Section-4.

3.2.2.5.7 ACME “tls-alpn-01” method for IP Addresses

TrustAsia CA does not support this method.

3.2.2.6 Wildcard Domain Validation

TrustAsia CA verifies control over the domain name to the right of the wildcard, and the verification rules follow the regulations of this CP&CPS Section 3.2.2.4. TrustAsia CA can refuse to issue a certificate for it if the right side of the wildcard domain name is a top-level domain name or public suffix. TrustAsia CA will not issue EV certificates to wildcard Domain.

3.2.2.7 Accuracy of data sources

The data sources used in the forensic process will be published in the TrustAsia CA repository. Prior to the use of any data source as a dependent data source, TrustAsia CA assesses the dependability, accuracy and the resistance to alteration or falsification of that source. Following CA/Browser Forum and taking into account the following factors:

1. The number of years of information provided;
2. The frequency at which sources of information are updated;
3. Data providers and data collection purposes;
4. Availability and accessibility of data to the public;
5. The difficulty of falsifying or changing data.

3.2.2.8 Certification authority authorization record

Refer to Section 4.2.4 for TrustAsia CA policy on CAA records.

3.2.2.9 Authentication of E-mail Address

When the email address is used as the subject content or alternative name to apply for a certificate, TrustAsia CA will confirm the validity of the email address and confirm the Applicant's right to use the email address. Only after passing the validation can the Email entry be checked in the certificate.

1. Using Domain Validation
   TrustAsia CA confirms the Applicant’s control of email addresses by verifying the Applicant’s control over the FQDN part of the email address. TrustAsia CA only uses a domain validation process from Section 3.2.2.4.
2. Using Email Validation

TrustAsia CA confirms the Applicant’s control of email addresses by sending a URL containing a Random Value to the email address and then receiving an affirmative response utilizing the Random Value.

The specific validation steps are as follows:

a. TrustAsia CA System sends a control validation email to the requested email address. This email contains an approval link with a unique Random Value.
b. The Applicant receives the email and approves it via a link with a Random Value;
c. After TrustAsia CA System receives the approval from user, it will compare the Random Value sent with the Random Value in approval. If the result is consistent, then the email address is validated.

The Random Value is unique in each email, and the email containing a Random Value is only valid for 24 hours. The Random Value will be reset every time TrustAsia CA sends an email to the email address.

3.2.3 Authentication of Individual Identity

If the Applicant's identity is a natural person, TrustAsia CA will review the Applicant's name, address, and the authenticity of the certificate application. In the case of a personal identification certificate, TrustAsia CA will perform different identity authentication methods based on the different types of certificates applied by the individual. In general, the higher the certificate category, the higher the security level, the stricter the authentication method, and the more comprehensive the authentication content.

The Applicant needs to prove that he or she has control over some of the identity properties contained in the request, such as the e-mail address or domain name involved in the certificate in the certificate request. Applicants may also be required to submit clear copies of valid government-issued documents with photographs (such as identity cards, passports, driver's permits, military officers' certificates or other equivalent documents). TrustAsia CA verifies that copies of the documents match the requested names and that other relevant information is correct.

TrustAsia CA identifies and validates in one or more of the following ways:

1. The authenticity of the Applicant's certificate request is identified and verified by sending the relevant check code email or by telephone, mobile phone short message and other reliable means. TrustAsia CA does not confirm and guarantee the identity information other than the authentication information in the certificate issued is true, reliable and belonging to the Applicant himself;
2. Check whether the copy of the document submitted by the Applicant has any traces of tampering or forgery and, if necessary, verify the identity information provided by the Applicant through reliable means, such as consulting the authoritative third-party database, in order to ensure that the information provided by the applicant is consistent with the results of the verification;

3. Verify the Applicant's address through property bill, bank card statement or credit card bill or rely directly on identity documents issued by the government to confirm the address.
4. When the application information contains organization information. The Applicant may be required to submit a certificate of employment, or query a third-party database, or send a confirmation email to confirm the existence of the organization and whether the Applicant is a member of the organization.

In addition, if necessary, TrustAsia CA can also set up other required authentication methods and data. The Applicant has an obligation to ensure the authenticity and validity of the application materials and to bear the relevant legal liability.

For Subscriber certificates issued by TrustAsia CA, TrustAsia CA establishes evaluation criteria to identify potentially high-risk fraud certificate requests. TrustAsia CA can directly reject certificate requests identified as "high risk".

3.2.3.1 Validation of Individual Identity for Individual-validated S/MIME Certificates

1. Application Requirements
   TrustAsia CA only accepts Individual-validated S/MIME Certificate application by a natural person with full capacity for civil conduct. The Applicant needs to provide identity document to TrustAsia CA, and TrustAsia CA validates the Applicant’s identity document and the authenticity of the certificate request.
2. Subject Distinguished Name Fields Requirements
   a. subject:commonName (OID:2.5.4.3); TrustAsia CA only accepts the Applicant’s legal name as the value of the field. The Applicant’s name must be the same as the name on the provided identity document.
   b. subject:givenName (OID:2.5.4.42) and subject:surname (OID:2.5.4.4); TrustAsia CA only accepts the Applicant’s legal name.
   c. subject:emailAddress (OID:1.2.840.113549.1.9.1); TrustAsia CA fills the Applicant’s requested email address in this field. The email address is verified under Section 3.2.2.9.
   d. subject:countryName (OID:2.5.4.6); TrustAsia CA fills the country code of the country presented on the identity document that is provided by the Applicant in this field.
3. Verification Requirements
   Apart from validating all of the DN fields to be included in Individual-validated S/MIME Certificates, TrustAsia CA will collect the Applicant’s identity document and confirm the Certificate Request with the Applicant him/herself.
   a. Validation of Applicant Identity
      In terms of the methods of collecting Individual identity attributes, TrustAsia CA only accepts physical identity documents. The identity document types that TrustAsia CA accepts include Resident ID Card/Temporary Resident ID Card, Military ID Card, Driving License, Passport, Residence Permit for Hong Kong, Macao and Taiwan Residents,

Mainland Travel Permit for Hong Kong and Macao Residents, Mainland Travel Permit for Taiwan Residents, Foreigner's Permanent Resident ID Card and other government-issued identity documents. The physical identity document must contain a clear face photo, otherwise the document cannot be used as identity evidence. If there is no address on the identity document, the Applicant should provide identification documents to demonstrate the Applicant's address, and the documents accepted by TrustAsia CA include utility bills, bank statements, credit card statements, government-issued tax documents and other documents on which the Applicant's name, ID number and address are presented.

b. Application Confirmation
TrustAsia CA performs a face-to-face validation to confirm the identity attributes and the Certificate Request in accordance with the requirements set forth in the EV Guidelines Section 11.11.3. The methods of face-to-face validation (those equivalent to face-to-face validation) includes but are not limited to a video call, a video recording, in-person face-to-face validation, etc. In the process of face-to-face validation, the Certificate Requester is required to present his/her original ID document and sign the application document about personal statement on the spot to complete validation.

3.2.3.2 Validation of Individual Identity for Sponsor-validated S/MIME Certificates

1. Application Requirements
TrustAsia CA allows to include Individual information in Sponsor-validated S/MIME Certificates and the Individual information must be validated. The Individual included in the Certificate must have full capacity for civil conduct and obtain the authority from the Applicant's organization. The Applicant organization needs to complete organization validation under Section 3.2.2.1, and provides to TrustAsia CA the identity document of the Individual to be included in the Certificate. TrustAsia CA validates the identity document and the authenticity of the certificate request and authority.
2. Subject Distinguished Name Fields Requirements (Individual identity authentication)
    a. subject:commonName (OID:2.5.4.3); TrustAsia CA only accepts a natural person's legal name or pseudonym as the value of the field. If a legal name is used, it must be the same as the name on the provided identity document; if a pseudonym is used, the organization must provide an attestation document.
    b. subject:givenName (OID:2.5.4.42) and subject:surname (OID:2.5.4.4); TrustAsia CA only accepts the Applicant's legal name. The subject:pseudonym (OID:2.5.4.65) must not be present if the subject:givenName and/or subject:surname are present in the Certificate DNs.

c. subject:pseudonym (OID:2.5.4.65); TrustAsia CA accepts the use of pseudonyms for Inidividual identity information in Sponsor-validated S/MIME Certificates. The Applicant must provide evidence to demonstrate that the pseudonym is associated with the Individual's real identity information. The subject:pseudonym (OID:2.5.4.65) must not be present if the subject:givenName and/or subject:surname are present in the Certificate DNs.

3. Verification Requirements
   The Individual identity attributes included in Sponsor-validated S/MIME Certificate DNs should be authenticated under this Section. TrustAsia CA will collect the Individual's identity document and confirm the Certificate Request with the Individual him/herself.
   a. Validation of Individual Identity
      The methods of collecting identity documents are the same as the requirements set forth in Section 3.2.3.1. In addition, if a pseudonym will be present in the Certificate DN, the Applicant must provide the related evidence that is accepted by TrustAsia CA, such as an Authorization Letter and an Attestation, and is capable of demonstrating that the pseudonym is associated with the Individual's real identity information.
   b. Application and Authority Confirmation
      Apart from confirming the Individual authority through the communication means verified under Section 3.2.2.1, TrustAsia CA performs a face-to-face validation to validate the identity documents in accordance with the requirements set forth in the EVG Section 11.11.3. The methods of face-to-face validation (those equivalent to face-to-face validation) includes but are not limited to a video call, a video recording, in-person face-to-face validation, etc. In the process of face-to-face validation, the Certificate Requester is required to present his/her original ID document and sign the application document about personal statement on the spot to complete validation.

3.2.3.3 Validation of Individual Identity for Individual-validated Document Signing Certificates

1. Application Requirements
   TrustAsia CA only accepts Individual-validated Document Signing Certificate application by a natural person with full capacity for civil conduct. The Applicant needs to provide identity document to TrustAsia CA, and TrustAsia CA validates the Applicant's identity document and the authenticity of the certificate request.
2. Subject Distinguished Name Fields Requirements
   a. subject:commonName (OID:2.5.4.3) TrustAsia CA accepts the Applicant's legal name as the value of the field. The Applicant's name must be the same as the name on the provided identity document.
   b. subject:givenName (OID:2.5.4.42) and subject:surname (OID:2.5.4.4) TrustAsia CA only accepts the Applicant's legal name.

c. subject:countryName (OID:2.5.4.6) TrustAsia CA fills the country code of the country presented on the identity document that is provided by the Applicant in this field.

3. Verification Requirements

Apart from validating all of the DN fields to be included in Individual-validated Document Signing Certificates, TrustAsia CA will collect the Applicant's identity document and confirm the Certificate Request with the Applicant him/herself.

a. Validation of Applicant Identity

In terms of the methods of collecting Individual identity attributes, TrustAsia CA only accepts physical identity documents. The identity document types that TrustAsia CA accepts include Resident ID Card/Temporary Resident ID Card, Military ID Card, Driving License, Passport, Residence Permit for Hong Kong, Macao and Taiwan Residents, Mainland Travel Permit for Hong Kong and Macao Residents, Mainland Travel Permit for Taiwan Residents, Foreigner's Permanent Resident ID Card and other government-issued identity documents. The identity document must contain a clear face photo, otherwise the document cannot be used as identity evidence. If there is no address on the identity document, the Applicant should provide identification documents to demonstrate the Applicant's address, and the documents accepted by TrustAsia CA include utility bills, bank statements, credit card statements, government-issued tax documents and other documents on which the Applicant's name, ID number and address are presented.

b. Application Confirmation

TrustAsia CA performs a face-to-face validation to confirm the identity attributes and the Certificate Request in accordance with the requirements set forth in the EVG Section 11.11.3. The methods of face-to-face validation (those equivalent to face-to-face validation) includes but are not limited to a video call, a video recording, in-person face-to-face validation, etc. In the process of face-to-face validation, the Certificate Requester is required to present his/her original ID document and sign the application document about personal statement on the spot to complete validation.

3.2.3.4 Validation of Individual Identity for Organization-validated Document Signing Certificates Containing Individual Information

1. Application Requirements

TrustAsia CA allows to include Individual information in Organization-validated Document Signing Certificates and the Individual information must be validated. The Individual included in the Certificate must have full capacity for civil conduct and obtain the authority from the Applicant's organization. The Applicant organization needs to complete organization validation under Section 3.2.2.1, and provides to TrustAsia CA the identity document of the

Individual to be included in the Certificate. TrustAsia CA validates the identity document and the authenticity of the certificate request and authority.

2. Subject Distinguished Name Fields Requirements (Individual identity authentication)
   a. subject:commonName (OID:2.5.4.3); TrustAsia CA only accepts a natural person’s legal name as the value of the field. The legal name must be the same as the name on the provided identity document.
   b. subject:givenName (OID:2.5.4.42) and subject:surname (OID:2.5.4.4); TrustAsia CA only accepts the Applicant’s legal name.
3. Verification Requirements
   The Individual identity attributes included in Organization-validated Document Signing Certificate DNs should be authenticated under this Section. TrustAsia CA will collect the Individual’s identity document and confirm the Certificate Request with the Individual him/herself.
   a. Validation of Individual Identity
      The methods of collecting identity documents are the same as the requirements set forth in Section 3.2.3.1.
   b. Application and Authority Confirmation
      Apart from confirming the Individual authority through the communication means verified under Section 3.2.2.1, TrustAsia CA performs a face-to-face validation to validate the identity documents in accordance with the requirements set forth in the EVG Section 11.11.3. The methods of face-to-face validation (those equivalent to face-to-face validation) includes but are not limited to a video call, a video recording, in-person face-to-face validation, etc. In the process of face-to-face validation, the Certificate Requester is required to present his/her original ID document and sign the application document about personal statement on the spot to complete validation.

3.2.4 Non-Verified Subscriber Information

In general, in addition to the need for explicit and reliable authentication of the identity information required by the type of certificate. For the Subscriber information that is not required to be verified, TrustAsia CA does not commit to the authenticity of the relevant information and does not assume the relevant legal responsibility.

The information in the certificate must be verified with a trusted third-party source of information, and the unverified information must not be written to the certificate.

3.2.5 Validation of Authority

When an institutional Subscriber authorizes the Applicant's representative to handle the certificate business, TrustAsia CA will use the sources listed in Section 3.2.3 to obtain reliable means of communication to verify the authenticity of the Applicant's application. TrustAsia CA can confirm the authenticity of the certificate application directly with the Applicant's representative, or with the department with authority

within the Applicant's organization, such as the Applicant's main business office, the company's office, Human Resources Office, Information Technology Office or such other department as TrustAsia CA thinks fit.

TrustAsia CA also allows the Applicant to provide authorization letters, employment certificates or any equivalent means to verify that it belongs to the above-mentioned institution and that its representative conduct is authorized by the agency.

In addition, TrustAsia CA allows Applicants to designate independent individuals to apply for certificates. TrustAsia CA does not accept any request for a certificate beyond that authorization if the Applicant specifies in writing an independent individual who can apply for a certificate. Upon receipt of a verified written request from the Applicant, TrustAsia CA will provide the Applicant with a list of its authorized personnel.

3.2.6 Criteria for Interoperation or Certification

For other electronic certification services, they can interoperate with TrustAsia CA, but the CP&CPS of the electronic certification service must meet the TrustAsia CA CP&CPS requirements and a corresponding agreement must be signed with TrustAsia CA.
If there are relevant provisions in national laws and regulations, TrustAsia CA will strictly implement the provisions.
So far, TrustAsia CA has not issued any cross-certificate.

3.3 Identification and Authentication for Re-key Requests

Before the certificate expires, the Subscriber can request an update of the key. Upon receipt of a request to update the key, TrustAsia CA will create a new certificate that contains a new public key but the subject of the certificate is the same as the original certificate, and can selectively extend the validity of the certificate. TrustAsia CA can choose to reconfirm the Applicant according to the actual situation, or rely on the information previously provided or obtained.

The key update will cause the file or data encrypted with the original key pair to be unable to decrypt. Therefore, before applying for the key update, the Subscriber must confirm that the file or data encrypted with the original key pair has been decrypted, and TrustAsia CA will not be responsible for the loss caused by the original key pair.

3.3.1 Identification and Authentication got Routine Re-key

TrustAsia CA supports certificate Subscribers to make key update requests during the validity period, and Subscribers can choose to generate a new key pair to replace the key pair in use or the key pair that is about to expire.

There are two types of certificate key update: the reissue and the replacement.

1. **Certificate Reissue**

Subscribers need to apply for a certificate reissue in the following cases:
The reissue means that the certificate is within the validity period, and the Subscriber applies for the operation to update the certificate key.

- The Subscriber certificate (file) is lost or damaged or the Subscriber considers the original certificate and key to be insecure;
- Multiple deployment of a certificate by Subscriber requires the use of different key pairs;
- Subscribers need to obtain certificates with multiple algorithms (RSA、ECC);
- Subscribers need to add domain names (multi-domain SSL/TLS server certificates only);
- Other reasons approved by TrustAsia CA.

When a Subscriber needs to issue a replacement certificate, he/she should apply for a replacement certificate to TrustAsia CA on his/her own initiative. If the Subscriber's authenticated certificate registration information is within the validity period specified by CA/Browser Forum BR, TrustAsia CA will reissue the certificate based on its original information. If the time slot between the certified certificate registration information creation and initial verification has exceeded the CA/Browser Forum BR required verification validity period, the Subscriber identity shall be re-verified, and the verification process and requirements shall be the same as the initial application. The validity period of the replacement certificate is the same as that of the original certificate.

2. **Certificate Replacement**
   Replacement refers to the operation of the Subscriber applying for an update key within 30 days (inclusive) of the expiration of the certificate.
   Within 30 days (inclusive) before the expiration of the Subscriber Certificate, TrustAsia CA will notify the Subscriber of the certificate renewal operation by appropriate means. If the Subscriber's verified certificate registration information is within the validity period specified by CA/Browser Forum BR. TrustAsia CA will reissue the certificate to the Subscriber based on its original information. If the verified certificate registration information from the initial verification has exceeded the CA/Browser Forum BR specified verification validity period, the Subscriber identity needs to be re-validated, and the verification process and requirements are the same as the initial application. The new certificate will be valid from the date of renewal of the certificate until the expiration of the original certificate plus another certificate validity cycle.

3.3.2 Identification and Authentication for Re-key After Revocation

TrustAsia CA does not provide Re-key/renewal after revocation.

3.4 Identification and Authentication for Revocation Request

In TrustAsia CA's certificate business, a certificate revocation request can come from a Subscriber or from TrustAsia CA. In addition, TrustAsia CA has the right to initiate the revocation of a Subscriber certificate when there is a certificate required to be revoked for the reasons stated in this CP&CPS Section 4.9.1.1.
Subscribers submit requests to TrustAsia CA in certain ways, such as mail, fax, telephone, etc. TrustAsia CA confirms that the person or organization requesting to revoke the certificate is the Subscriber or its authorized person in a manner corresponding to the certificate safeguard level. Depending on the circumstances, one or more of the following can be used for confirmation: domain control verification, telephone, fax, e-mail, mailing or express delivery.

3.5 Identification of authorized Service institutions

TrustAsia CA acts as a certificate RA and no additional RA is established.

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 an Applicant may file a certificate application. The Applicant is responsible for any data provided to TrustAsia CA by it or the authorized representative.
The EV certificate request must be submitted by an authorized certificate applicant and approved by the certificate approver. The certificate application must be accompanied by a (written or electronic) Subscriber Agreement signed by the Contract Signer.

4.1.2 Enrollment Process and Responsibilities

1. Enrollment Process include:
   - Submit a certificate request;
   - Generating key pairs;
   - providing the public key (Signed CSR) of the key pair to TrustAsia CA;
   - Agree to the applicable Subscriber Agreement;
   - Pay any applicable fees.

2. Responsibilities
   - The Applicant shall know in advance the matters agreed upon in the Subscriber Agreement and this CP&CPS, in particular with regard to the scope of application, rights, obligations and guarantees of the certificate.
   - It is the responsibility of the Subscriber to provide authentic, complete and accurate certificate application information and material to TrustAsia CA.

- It is the responsibility of the registration agencies to check and examine the certificate application information and identification materials provided by the Subscriber.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

When TrustAsia CA receives a Subscriber's certificate request, the TrustAsia CA Verification Team will identify and authenticate the Subscriber's identity as required in Section 3.2 of the CP&CPS. TrustAsia CA maintains systems and processes to fully verify the identity of the Applicant in accordance with CP&CPS. The content of communication through telephone, fax or email will be stored securely together with the information provided by the Applicant directly through TrustAsia CA web interface or the API.

TrustAsia CA will establish and maintain a high-risk database list of SSL certificates based on certificates that have been denied or revoked for suspected or identified phishing or other fraudulent purposes, and will query the list information when accepting certificate applications. For Subscribers that appear in the list, TrustAsia CA has the right to reject the certificate request or perform additional authentication.

TrustAsia CA performs an CAA record check on each DNS Name in the issued certificate subject alias extension and determines whether the certificate application is approved according to the inspection method and results in Section 4.2.4 of the CP&CPS.

When conducting identity identification and authentication, the TrustAsia CA Verification Team will enforce rigorous control procedures for the separation of validation duties to ensure that no one person can single-handedly validate and authorize the issuance of an Individual-validated, Organization Validation or Extended Validation Certificate. One validation specialist will strictly follow the regulations as outlined in Section 3.2, and complete the initial validation of the certificate request. The validation content includes but is not limited to: utilizing a trusted database to examine information; completing the validation of the Applicant, Contract Signer, Certificate Requester and Certificate Approver; collecting and verifying all related information and documents. A second validation specialist will review the collected materials and check all of the validation items and validation procedures. The second specialist shall not participate in the information collection procedure. Only if the information is reviewed and approved by the second specialist can the certificate be issued. The entire procedure of identity identification and authentication conducted by the TrustAsia CA Verification Team will be recorded and be audited.

If some or all of the identity authentication data is not in the official language of TrustAsia CA, TrustAsia CA will use properly trained personnel with sufficient experience and judgment ability to complete the final cross-audit and due diligence.

After the verification is completed, the TrustAsia CA Verification Team will decide to accept, refuse the application or request the applicant to submit additional relevant materials based on the verification results.

For the purpose of authenticating the information contained in the Individual-validated, Organization Validation and Extended Validation Certificates, if the previous validation data or documentation obtained by TrustAsia CA from a source specified under Section 3.2 of this CP&CPS is no more than 398 days and has not changed, TrustAsia CA may use such data or documentation. If the domains, IP addresses and email addresses validated under Section 3.2 of this CP&CPS is no more than 398 days, such domains, IP addresses and email addresses do not need re-validation.

4.2.2 Approval or Rejection of Certificate Applications

4.2.2.1 Approval of Certificate Applications

After TrustAsia CA successfully completes verification steps for the certificate application, it means TrustAsia CA has approved the certificate application when a formal certificate is issued.

TrustAsia CA will approve the certificate requests, if the following conditions are met:

1. The application completely meets the requirements from CP&CPS Section 3.2 regarding the Subscriber's identification information and authentication.
2. Subscriber accepts or has no opposition regarding the content or requirements of the Subscriber Agreement.
3. Subscriber has paid applicable feesin accordance with the provisions.

4.2.2.2 Rejection of Certificate Applications

TrustAsia CA has the right to refuse the certificate application in case of the following situations:

1. The application does not meet the specifications of Subscriber’s identification and authentication in CP&CPS Section 3.2.
2. The Subscriber cannot provide the required identity documents.
3. The Subscriber opposes or does not accept the relevant content or requirements of the Subscriber Agreement.
4. The Subscriber has not paid or cannot pay the appropriate fees.
5. The requested certificates contain a new gTLD under consideration by ICANN (The Internet Corporation for Assigned Names and Numbers).
6. The utilization of the Subscriber's certificate does not comply with the laws and regulations of the place where it is located;
7. TrustAsia CA considers that the approval of the application will bring about controversies, legal disputes or losses to TrustAsia CA.

8. There are some insecure factors such as the length of the public key, algorithm that submitted by the application.

For rejected certificate applications, TrustAsia CA will email to notify subscribers that the certificate application has failed.

4.2.3 Time to Process Certificate Applications

Under normal circumstances, TrustAsia CA validates Subscriber information and issues certificates within a reasonable time frame. Unless otherwise stated in an agreement or other agreement with the Subscriber concerned, the processing time for the completion of the certificate application is not specified.

The time of certificate processing depends to a large extent on when the Subscriber provides the details and documents needed to complete the verification and whether to respond to the management requirements of TrustAsia CA in a timely manner. The application for a certificate will remain valid until it is rejected.

4.2.4 CAA Records

For SSL/TLS Server Certificates, TrustAsia CA conforms to the requirements specified in Section 3.2.2.8 of CA/Browser Forum BR. TrustAsia CA checks for DNS CAA records for each domain name in the Subject Name and Subject Alternative Name of the Certificate before issuance.

TrustAsia CA processes the “issue”, “issuewild”, “iodef” property tags as specified in RFC 8659 when processing CAA records.

When using ACME client for certificate request, CAA supports “accounturi” and “validationmethods” confirguration. “accounturi” managed by TrustAsia CA can be used to request certificate issuance and used as an object identification representing specific entity or relevant entity organization. “validationmethods” supports http-01 and dns-01.

When processing the property tags in CAA records, TrustAsia CA does not act on the contents of the “iodef” property tag. TrustAsia CA respects the critical flag and does not issue a certificate if an unrecognized property tag with this flag set is encountered.

TrustAsia CA does not issue a certificate if there is a “issue” or “issuewild” tag in CAA records and these tags do not contain “trustasia.com”.

For S/MIME Certificates, starting on September 15, 2024, TrustAsia CA processes the “issuemail” property tag in CAA records, as specified in RFC 9495, prior to issuing a certificate that includes an email address. The “issuemail” property tag does not conflict with “issue” and “issuewild” in SSL/TLS Server Certificates.

If there is the “issuemail” tag in CAA records, TrustAsia CA does not issue a certificate to an email address beyond domain names included in “issuemail”.

TrustAsia CA treats a record lookup failure as permission to issue a certificate if:

1. The failure is outside the TrustAsia CA’s infrastructure; and
2. The lookup has been retried at least once by TrustAsia CA; and

3. The domain’s zone does not have a DNSSEC validation chain to the ICANN root.

TrustAsia CA issues a certificate within the validity period of the CAA record (the TTL of the CAA record, or 8 hours, whichever is greater). TrustAsia CA documents potential issuances that were prevented by a CAA record in sufficient detail to provide feedback to the CA/Browser Forum on the circumstances, and dispatches reports of such issuance requests to the contact(s) stipulated in the CAA iodef record(s), if present. TrustAsia CA only supports mailto: scheme in the iodef record. CAA record is not applicable for Code Signing Certificates, Document Signing Certificates and Timestamp Certificates.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate issuance

Certificate issuance by the Root CA requires an individual authorized by the CA (i.e. the CA system operator, system officer, or PKI administrator) to deliberately issue a direct command in order for the Root CA to perform a certificate signing operation. For Subscriber Certificates, TrustAsia CA confirms the source of the certificate request before issuing it.
In the process of issuing, the RA administrator is responsible for the examination and approval of the certificate application, and sends the request for issuing the certificate to the certificate issuing system of CA through the operation of the RA system. The certificate issuance request information sent by the RA to the CA must have the authentication and information confidentiality measures of RA, and ensure that the request is sent to the correct CA certificate issuing system. After obtaining the certificate issuance request, the CA certificate issuing system authenticates and decrypts the information from RA.

TrustAsia CA does not issue the end-entity certificate directly from its root certificate. The SSL/TLS Server Certificate to be trusted in Chrome is recorded in two or more certificate transparency databases.
Databases and CA processes that occur during certificate issuance are protected against unauthorized modifications.

For valid certificate issuance requests, the CA Certificate Issuing System will send it to the Subscriber.
For SSL/TLS Server Certificates, TrustAsia CA performs pre-issuance linting to check a tbsCertificate (To Be Signed Certificate) and conduct manual review if an error is found, to prevent mis-issuance that violates BR.
TrustAsia CA has deployed Multi-Factor Authentication (MFA) for all the accounts that can directly issue certificates.

4.3.2 Notification of Certificate Issuance

TrustAsia CA provides certificates in any secure manner within a reasonable time after release. Typically, TrustAsia CA will email the certificate to the e-mail address specified by the Subscriber during the certificate 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.
Subscribers are deemed to accept issued certificates, including, but not limited to:

1. Subscribers visit the specialized TrustAsia CA certificate service website, and complete downloading the certificate to the digital certificate carrier.
2. TrustAsia CA downloads the certificate on behalf of the Subscriber, with the permission of the Subscriber, and sends the certificate to the Subscriber through the security carrier.
3. After the notification of sending the certificate to the Subscriber is received, the Subscriber downloads the certificate through the notice.
4. The Subscriber accepted the manner in which the certificate was obtained and did not object to the certificate or the contents of the certificate.

4.4.2 Publication of the certificate by the CA

TrustAsia CA delivers the certificate to the Subscriber as a release of the certificate. TrustAsia CA will choose to publish the certificate on multiple Certificate Transparency Log servers, as required by Google and Apple, in accordance with different utilization scenarios of Subscribers' certificates.

TrustAsia CA follows the regulations on the information base mechanism in Section 2.4 and 2.5 of this CP&CPS to issue certificates to Subscribers. Only personnel in roles authorized by CA can monitor and manage the high-risk database or alternate issuance mechanism of the information database. At the same time, the personnel in roles are authorized to maintain and manage its integrity. If required by relevant laws and regulations such as confidentiality laws, TrustAsia CA will comply with relevant requirements and make its certificate in a searchable state after obtaining the Subscriber's consent.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

TrustAsia CA does not notify other entities.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

After receiving the certificate issued by TrustAsia CA, the Subscriber shall take reasonable measures to properly keep the key pair and control its use authorization. The Subscriber shall use the key pair within the scope of the protocol, laws and regulations, CP&CPS.

4.5.2 Relying Party Public Key and Certificate Usage

The relying party shall consider the overall situation and the risk of loss before relying on the certificate.
When the relying party has received the message with digital signature, the party has the obligation to carry out the following operations to confirm:

1. Obtain digital signature's corresponding certificate and trust chain.
2. Verify the validity of the certificate to ensure that the certificate is used within the validity period.
3. Confirm that the signature's corresponding certificate is the one trusted by the relying party.
4. Confirm whether the signature corresponding certificate has been revoked by querying the CRL or OCSP.
5. Certificate usage is suitable for the corresponding signature.
6. Use certificate's public key to verify the signature.
7. Consider other information specified in this CP&CPS or elsewhere.

If the above conditions are not met, it is the duty of the relying party to refuse the signature information.

4.6 Certificate Renewal

4.6.1 Circumstance for Certificate Renewal

For a Subscriber certificate issued by TrustAsia CA, a certificate update may be made from 30 days (inclusive) prior to the expiration of the certificate. If the Subscriber chooses to keep using the original key pair to re-issue the certificate, the Subscriber needs to ensure that the security of its key pair is not compromised. As of 30 days (inclusive) prior to the expiration of the certificate, TrustAsia CA will notify the Subscriber of the renewal of the certificate by way of a mail notification.

If the Subscriber does not change the certificate subject alias name and the related identity information when the certificate renewal request is submitted, and the verification time of the original certificate does not exceed the period specified in Section 4.2.1 of this CP&CPS, then TrustAsia CA verifies the information of the update certificate with reference to the data and the supporting documents verified by the original certificate.

Where the Subscriber needs to change some of the certificate information when submitting the certificate renewal request or the validation limitation of the original certificate has exceeded the time limit specified in Section 4.2.1 of this CP&CPS, the certificate renewal request will be verified in accordance with the process and requirements of the certificate initial application by TrustAsia CA.

If the original certificate of the Subscriber has expired, verification in accordance with the process and requirements of the initial application of the certificate is required when applying for the certificate again.

4.6.2 Who May Request Renewal

The entity requesting the renewal of the certificate is a Subscriber or other authorized representative who has applied for a TrustAsia CA certificate, and the remaining validity of the certificate is less than 30 days (inclusive).

4.6.3 Processing Certificate Renewal Requests

For certificate update, the processing procedure includes application identification and authentication, certificate information verification and certificate issuance.

1. The identification and authentication of the application shall be based on the following aspects:
   a. The original certificate of the Subscriber exists and is issued by TrustAsia CA;
   b. The certificate update request is within the license period;
   c. A Subscriber can submit sufficient information to be able to identify the original certificate, such as a Subscriber's alias name, certificate sequence number, etc.
2. For the processing procedure of certificate information verification, TrustAsia CA will process according to the provisions of Section 3.3.1 of this CP&CPS. TrustAsia CA may also choose to verify according to the general initial certificate application process according to the specific application situation of Subscriber certificate update.
3. TrustAsia CA approves the issuance of the certificate only after all the above authentication and verification have been passed.

4.6.4 Notification of New Certificate Issuance to Subscriber

See CP&CPS Section 4.3.2

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

See CP&CPS Section 4.4.1.

4.6.6 Publication of the Renewal Certificate by the CA

See CP&CPS Section 4.4.2.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

See CP&CPS Section 4.4.3.

4.7 Certificate Re-key

4.7.1 Circumstances for Certificate Re-key

The Subscriber can choose the certificate rekey service when the Subscriber's certificate is as follows:

1. The Subscriber certificate (file) is missing or damaged or the Subscriber considers that the original certificate and key is unsafe;
2. In case of multiple deployments for a single certificate, the Subscriber needs to use different key pairs;
3. Subscribers need to obtain certificate with multiple algorithms (RSA、ECC);
4. Subscriber needs to add domain name (only for multi-domain SSL/TLS server certificate);
5. The Subscriber certificate is about to expire and it is believed that the key needs to be updated when the certificate is updated;
6. Other situations that may result in key updates.

4.7.2 Who May Request Certification of a New public key

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

4.7.3 Processing Certificate Re-keying Requests

The processing of certificate key update request is completed by the process of certificate update request in TrustAsia CA. See CP&CPS Section 4.6.3.

4.7.4 Notification of new certificate issuance to Subscriber

See CP&CPS Section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-keyed certificate

See CP&CPS Section 4.4.1.

4.7.6 Publication of the Re-keyed certificate by the CA

See CP&CPS Section 4.4.2.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

See CP&CPS Section 4.4.3.

4.8 Certificate Modification

4.8.1 Circumstances for Certificate Modification

Certificate change means that the Subscriber's certificate is within its validity period, the alternate name of the certificate extension information is changed with nonupdated key, but the certificate is reissued.

The Subscriber’s request to change the name of the certificate authority is not accepted by TrustAsia CA. If the name of the authority needs to be changed, the Subscriber needs to apply for a new certificate.

4.8.2 Who May Request Certificate Modification

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

4.8.3 Processing Certificate Modification Requests

When the Subscriber submits the application for modification of certificate information, TrustAsia CA will re-verify the certificate information. If the application data of the original certificate are available and not expired (the application data of Individual-validated, OV and EV certificate is valid for 398 days, the application data of DV certificate needs to be verified every time), the original information can be examined and verified by reference to the original data. If the above information is unavailable or overdue, then TrustAsia CA will perform validation in accordance with the initial application process and requirements before reissuing a new certificate.

4.8.4 Notification of New Certificate Issuance to Subscriber

See CP&CPS Section 4.3.2.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

See CP&CPS Section 4.4.1.

4.8.6 Publication of the Modified Certificate by the CA

See CP&CPS Section 4.4.2.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

See CP&CPS Section 4.4.3.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

4.9.1.1 Reasons for Revoking a Subscriber Certificate

Unless the CRLReason is “unspecified (0)”, a CRLReason must be included in the “reasonCode” extension of the CRL entry.

Only the following CRLReasons may be present in the CRL “reasonCode” extension:

1. keyCompromise (RFC 5280 CRLReason #1):
   Indicates that it is known or suspected that the Subscriber’s Private Key has been compromised;
2. affiliationChanged (RFC 5280 CRLReason #3):
   It is intended to be used to to indicate that the Subject’s name or other Subject Identity Information in the Certificate has changed, but there is no cause to suspect that the Certificate’s Private Key has been compromised;
3. superseded (RFC 5280 CRLReason #4):
   It is intended to be used to indicate when the Certificate Subscriber has requested a new Certificate to replace an existing Certificate, or TrustAsia CA obtains reasonable evidence that the validation of domain authorization or control for any FQDN or IP address in the Certificate should not be relied upon, or TrustAsia CA has revoked the Certificate for compliance reasons.
4. cessationOfOperation (RFC 5280 CRLReason #5):
   It is intended to be used when the website with the Certificate is shut down prior to the expiration of the Certificate, or if the Subscriber no longer owns or controls the domain name in the Certificate prior to the expiration of the Certificate;
5. privilegeWithdrawn (RFC 5280 CRLReason #9):
   It is intended to be used when there has been a subscriber-side infraction that has not resulted in keyCompromise. The privilegeWithdrawn reasonCode will not be made available to the Subscriber as a revocation reason option.

TrustAsia CA lists the above-mentioned revocation reason options in the Subscriber Agreement and provides explanation about when to choose each option. Tools that TrustAsia CA provides to the Subscriber allows for these options to be easily specified when the Subscriber requests revocation of their Certificate, with the default value being that no revocation reason is provided (i.e. the default corresponds to the CRLReason “unspecified (0)” which results in no reasonCode extension being provided in the CRL).

1. TrustAsia CA revokes the certificate within 24 hours if one or more of the following occurs and uses the corresponding CRLReason:

a. The Subscriber requests in writing that TrustAsia CA revoke the certificate (CRLReason “unspecified (0)”, or another reason specified by the Subscriber);
b. The Subscriber notifies TrustAsia CA that the original certificate request was not authorized and does not retroactively grant authorization (CRLReason #9 “privilegeWithdrawn”);
c. TrustAsia CA obtains evidence that the Subscriber’s private key corresponding to the certificate public key was compromised (CRLReason #1 “keyCompromise”).
d. TrustAsia CA has a method to verify the leak of the Subscriber’s private key and such method can easily compute the Subscriber’s private key based on the public key in the certificate (such as a Debian weak key, see https://wiki.debian.org/SSLkeys), or there is clear evidence that the specific method used to generate the private key was flawed (CRLReason #1 “keyCompromise”);
e. TrustAsia CA obtains reasonable evidence that the validation of control for any domain name or IP address in the certificate should not be relied upon (CRLReason #4 “superseded”).

2. TrustAsia CA should revoke the certificate within 24 hours and must revoke the certificate within 5 days if one or more of the following occurs, and uses the corresponding CRLReason.
   a. TrustAsia CA is informed that the certificate no longer complies with the relevant requirements of Section 6.1.5 and 6.1.6 of the Baseline Requirements, or no longer complies with the current root certificate policy of the relying party, such as Mozilla, Google, Microsoft, Apple, Adobe, Oracle, 360, etc. (CRLReason #4 “superseded”);
   b. TrustAsia CA obtains evidence that the certificate was misused (CRLReason #9 “privilegeWithdrawn”);
   c. TrustAsia CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement and CP/CPS (CRLReason #9 “privilegeWithdrawn”);
   d. TrustAsia CA is made aware of any circumstance indicating that use of a fully-qualified domain name, IP address 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, the domain name registrant has failed to renew the domain name, or the use of email address in the certificate by the Subscriber is no longer legally permitted) (CRLReason #5 “cessationOfOperation”);
   e. TrustAsia CA is made aware that a wildcard certificate has been used to authenticate a fraudulently misleading subordinate fully-qualified domain name (CRLReason #9 “privilegeWithdrawn”);

f. TrustAsia CA is made aware of a material change in the information contained in the certificate (CRLReason #9 “privilegeWithdrawn”).
g. TrustAsia CA is made aware that the certificate was not issued in accordance with Baseline Requirements or TrustAsia CA’s CP&CPS (CRLReason #4 “superseded”);
h. TrustAsia CA determines that any information that appears in the certificate is inaccurate, untrue or misleading (CRLReason #9 “privilegeWithdrawn”);
i. TrustAsia CA's right to issue certificates under Baseline Requirements expires or is revoked or terminated, unless TrustAsia CA has made arrangements to continue maintaining the CRL/OCSP Repository (CRLReason “unspecified (0)”);
j. Apart from the circumstances specified in this Section 4.9.1.1, revocation is required by TrustAsia CA’s CP&CPS (CRLReason “unspecified (0)”);
k. TrustAsia CA is made aware of a proven method that exposes the Subscriber’s private key to compromise or there is clear evidence that the specific method used to generate the private key was flawed (CRLReason #1 “keyCompromise”);
l. TrustAsia CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the certificate (CRLReason #9 “privilegeWithdrawn”);
m. The performance of duties in CP&CPS is delayed or hindered by force majeure; natural disasters; failure of computers or communications; changes in laws, regulations or other laws; acts of government; or other reasons beyond personal control and posing a threat to the information of others (CRLReason #4 “superseded”);
n. After TrustAsia CA has fulfilled its call obligation, the Subscriber has still not paid the service charge (CRLReason #9 “privilegeWithdrawn”);
o. The technical content or format of the certificate poses an unacceptable risk to the application software supplier or relying party (for example, the CA/Browser Forum may determine that the deprecated encryption/signature algorithm or key size will bring unacceptable. Therefore, such certificates should be revoked within a given time and replaced by CA) (CRLReason #4 “superseded”);
p. CA obtains evidence or be informed that the Subscriber has suspicious code in the software which has been signed (CRLReason #9 “privilegeWithdrawn”).

4.9.1.2 Reasons for the revocation of Intermediate CA certificates

In the event of one or more of the following conditions, TrustAsia CA revokes the Intermediate CA certificate within 7 days:

1. The Intermediate CA requests revocation in writing;
2. The Intermediate CA finds and informs TrustAsia CA that the original certificate request was not authorized and does not retroactively grant authorization;

3. TrustAsia CA obtains evidence that the Intermediate CA private key corresponding to the certificate public key suffered a key compromise or no longer complies with the requirements of BR Section 6.1.5 and Section 6.1.6;
4. TrustAsia CA obtains evidence that the certificate wasmisused;
5. TrustAsia CA is made aware that the issuance of the intermediate certificate failed to meet the Baseline Requirements, or the Intermediate CA failed to comply with CP/ CPS;
6. TrustAsia CA determines that any information that appears in the Intermediate CA certificate is inaccurate, untrue, or misleading;
7. TrustAsia CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the certificate;
8. TrustAsia CA's right to issue certificates in accordance with Baseline Requirements expires, or is revoked or terminated, unless it continues to maintain the CRL/OCSP Repository;
9. This CP&CPS requires the revocation of the Intermediate CA certificate.
10. The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk).

4.9.2 Who Can Request Revocation

The Subscribers, TrustAsia CA, or judicial officials authorized by judicial institutions can initiate revocation. Additionally, relying parties, application software suppliers, anti-virus organizations and other third parties may submit certificate problem reports informing TrustAsia CA of reasonable reasons to revoke the certificates.

For incidents involving malware, TrustAsia CA takes the following measures:

1. Contact the software publisher within 1 working day after learning of the incident, and request a reply within 72 hours.
2. Determine the number of affected relying parties within 72 hours of learning about the incident.
3. If a reply from the publisher is received, the CA and the publisher determine a "reasonable date" for the revocation
4. If no response is received from the issuer, the CA will notify the issuer that the CA will revoke the certificate within 7 days, unless it has written evidence that this will have a significant impact on the public.

4.9.3 Procedure for Revocation Request

4.9.3.1 The Subscriber actively proposed to revocation application

1. The Subscriber submits the application form of certificate revocation and the related identification material to TrustAsia CA, and the reasons for revocation should be described in the application form;
2. TrustAsia CA authenticates the certificate revocation request in accordance with the provisions of Section 3.4 of this CP&CPS;

3. TrustAsia CA publishes it to the Certificate Revocation List in time after accomplishing the certificate revocation;
4. After the certificate is revoked, TrustAsia CA will notify the Subscriber by e-mail and other appropriate means. If the Subscriber is not reached, TrustAsia CA can announce the revoked certificate through the website if necessary.
5. TrustAsia CA provides a 7 * 24-hour certificate revocation application service, and the Subscriber may apply for a certificate revocation through the contact information provided in Section 1.5.2 of this CP&CPS.

4.9.3.2 The Subscriber is forced to revoke the certificate

1. TrustAsia CA applies for a revocation of the certificate through the internal process when it has sufficient reason to be sure that the Subscriber certificate is forced to be revoked in the Section 4.9.1.1 of this CP&CPS;
2. When the private key corresponding to the Root Certificate or Intermediate CA Certificate of TrustAsia CA is exposed to security risk, the Subscriber certificate can be revoked directly after approval by the competent department of national electronic certification service.
3. When a third party such as a relying party, a judicial institution, an application software provider, an anti-virus mechanism and the like submits a Certificate Problem Report, TrustAsia CA organizes the investigation and decides whether to revoke the certificate according to the result of the investigation;
4. After the certificate has been revoked, TrustAsia CA will notify the end Subscriber of its certificate revocation and the reasons for its revocation by appropriate means, including email, telephone, etc.; if the Subscriber cannot be contacted, TrustAsia CA may announce the revoked certificate through the website if necessary;
5. TrustAsia CA provides 7*24 hours of certificate problem reporting and processing services, which can be reported 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

TrustAsia CA will investigate within 24 hours of receipt of the revocation request or certificate issue report to determine whether to revoke the certificate or take other reasonable measures. If the circumstances described in Section 4.9.1.1 (1) occur, TrustAsia CA will revoke the certificate within 24 hours.

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 report on the findings to both the Subscriber and the entity who initiated the revocation request.

After reviewing the facts and circumstances, TrustAsia CA will work with the Subscriber and any entity reporting the revocation request to establish whether or not the certificate will be revoked or other appropriate processing measures will be taken.

If the certificate is determined to be revoked, the period from receipt of the revocation request or revocation-related notice to published revocation will not exceed the time frame set forth in Section 4.9.1.1.
The date which TrustAsia CA will revoke the certificate considers the following criteria:

1. The nature of the alleged problem (scope, context, severity, magnitude, risk of harm);
2. The consequences of revocation (direct and collateral impacts to Subscribers and Relying Parties);
3. The number of revocation requests received about a particular certificate or Subscriber;
4. The entity making the complaint (for example, a complaint from a law enforcement official that a Web site is engaged in illegal activities carries more weight than a complaint from a consumer alleging that they didn't receive the goods they ordered); and
5. Relevant legislation.

4.9.6 Revocation Checking Requirement for Relying Parties

Certificate Revocation List CRL, as public information, does not have the security setting of reading permission, and the relying party is free to query according to the needs, including querying the Certificate Revocation List, querying the certificate status through the TrustAsia CA designated website, querying the online certificate status protocol (OCSP), and so on.
Before trusting this certificate, the relying party should actively check the status of the certificate according to the latest published CRL of TrustAsia CA, and also need to verify the reliability and integrity of the CRL to confirm the validity of the certificate.

4.9.7 CRL Issuance Frequency

CRL is available via a publicly-accessible HTTP URL. Within twenty-four hours of issuing the first certificate, the CA will generate and publish either:

- A full and complete CRL; or
- Partitioned CRLs that, when aggregated, represent the equivalent of a full and complete CRL.

CA issuing Subscriber Certificates will:

1. Update and publish a new CRL at least every four days;
2. Update and publish a new CRL within twenty-four hours after recording a certificate as revoked.

CA issuing CA Certificates will:

1. Update and publish a new CRL at least every twelve months;
2. Update and publish a new CRL within twenty-four hours after recording a certificate as revoked.

CA will continue issuing CRLs until one of the following is true:

- All Subordinate CA Certificates containing the same subject public key are expired or revoked; or
- The corresponding Subordinate CA private key is destroyed.

4.9.8 Maximum Latency for CRLs

TrustAsia CA CRL is automatically released to the public network after it is generated. The validity is usually within 1 hour and does not exceed 24 hours.

4.9.9 On-line Revocation/Status Checking Availability

TrustAsia CA provides Online Certificate Status Protocol for the Subscriber certificate and it is in accordance with the RFC6960 standard. The response data of the OCSP is signed by the parent CA certificate of the queried certificate or signed by the OCSP responder certificate issued by the parent CA of the query certificate.

4.9.10 On-line Revocation Checking Requirements

TrustAsia CA offers the OCSP service using both the Get and Post methods.
The OCSP response data for Subscriber certificates is updated at least once every 4 days, with a maximum validity period of no more than 10 days.
The OCSP response data for Intermediate CA certificates will be updated at least once every 12 months, and will be updated within 24 hours if the CA certificate is revoked.
If the OCSP responder receives a request for the status of a certificate serial number that is “unused”, then the responder will not respond with a “good” status. If the OCSP responder is for a CA that is not Technically Constrained in line with BR, the responder must not respond with a “good” status for such requests.
The OCSP responder will provide a definitive response about “reserved” certificate serial numbers, as if there was a corresponding certificate that matches the Precertificate [RFC6962].
A certificate serial number within an OCSP request is one of the following three options:

1. “assigned” if a certificate with that serial number has been issued by the Issuing CA, using any current or previous key associated with that CA subject; or
2. “reserved” if a Precertificate [RFC6962] with that serial number has been issued by
    a. the Issuing CA; or
    b. a Precertificate Signing Certificate [RFC6962] associated with the Issuing CA; or
3. “unused” if neither of the previous conditions are met.

4.9.11 Other Forms of Revocation Advertisements Available

If the network access volume is high in the usage scenario of the Subscriber certificate, TrustAsia CA will require Subscribers to use OCSP stapling to access OCSP services according to the provisions in RFC4366.

4.9.12 Special Requirements related to Key Compromise

If the Subscriber or TrustAsia CA discovers or suspects the compromise of the private key, immediate measures should be taken to revoke the compromised key certificate and reissue the certificate in accordance with CP&CPS requirements. Any relying party discovers a private key compromise can report to TrustAsia CA via an email (revoke@trustasia.com) and the email needs to provide evidence of a private key compromise:

1. The private key itself
2. CSR signed with the compromised private key, CSR common name is “Proof of Private Key Compromise for TrustAsia”
3. Key compromise demonstrated via the certificate revocation method of the ACME Protocol defined in RFC 8555 Section 7.6.

4.9.13Circumstances for Suspension

TrustAsia CA does not support 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 can be obtained through CRL and OCSP responses. For revoked certificates, TrustAsia CA does not delete its revocation records in CRL and OCSP until the certificate expires.

4.10.2 Service Availability

The round-the-clock Status Service of Certificates is provided. TrustAsia CA runs and maintains its CRL and OCSP capabilities with sufficient resources to provide 10 seconds or less response time under normal working conditions.

Under normal network conditions, the CRL of the EV CS, EV SSL certificate chain can be downloaded in no more than 3 seconds through an analogue telephone line.

TrustAsia CA maintains a continuous 7*24 ability to respond internally to a high-priority certificate problem, and where appropriate, forwards such a complaint to law enforcement authorities, and/or revoke a certificate that is the subject of such a complaint.

4.10.3 Operational Features

The OCSP responder may not apply to all of the types of certificates.

4.11 End of Subscription

The following conditions will be deemed that the user terminated the use of the certificate services provided by TrustAsia CA:

1. Failure to renew the service charge on time after the expiration of the certificate;
2. No certificate update or key update is carried out after the certificate expires;
3. The certificate was revoked before it expires.

Once the user terminates the certificate authentication service of TrustAsia CA during the validity period of the certificate, TrustAsia CA will revoke the Subscriber's certificate in real time and publish it in accordance with the CRL publishing policy after approving its termination request.

TrustAsia CA keeps detailed records of the certificate revocation operation and regularly archives the certificates and corresponding Subscriber data after subscription termination.

4.12 Key Escrow and Recovery

TrustAsia CA does not host the private key of any digital certificate Subscriber, so it does not provide key recovery service.

4.12.1 Key Escrow and Recovery Policy and Practices

Not applicable.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5. Management, and Operational, and Physical Controls

The CA/Browser Forum’s Network and Certificate System Security Requirements are incorporated by reference as if fully set forth herein. TrustAsia CA develops, implements, and maintains a comprehensive security program designed to:

1. Protect the confidentiality, integrity, and availability of certificate data and certificate management processes;
2. Protect against anticipated threats or hazards to the confidentiality, integrity, and availability of the certificate data and certificate management processes;

3. Protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of any certificate data or certificate management processes;
4. Protect against accidental loss or destruction of, or damage to, any certificate data or certificate management processes; and
5. Comply with all other security requirements applicable to the CA by law.

The certificate management process of TrustAsia CA includes:

1. physical security and environmental controls;
2. system integrity controls, including configuration management, integrity maintenance of trusted code, and malware detection/prevention;
3. network security and firewall management, including port restrictions and IP address filtering;
4. user management, separate trusted-role assignments, education, awareness, and training; and
5. logical access controls, activity logging, and inactivity time-outs to provide individual accountability.

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

1. identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any certificate data or certificate management processes;
2. assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the certificate data and certificate management processes; and
3. assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.

Based on the risk assessment, TrustAsia CA develops, implements, and maintains a security plan consisting of security procedures, measures, and products designed to achieve the objectives set forth above and to manage and control the risks identified during the risk assessment, commensurate with the sensitivity of the certificate data and certificate management processes. The security plan includes administrative, organizational, technical, and physical safeguards appropriate to the sensitivity of the certificate data and certificate management processes. The security plan also takes into account then-available technology and the cost of implementing the specific measures, and implements a reasonable level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected.

5.1 Physical Security Controls

5.1.1 Site Location and Construction

The TrustAsia CA's data center and system are constructed in accordance with the following standard:

1. <*Specification for computer field*>（GB 2887-89）
2. <*Code for design of electronic information System Room*>（GB 50174- 2008）

3. <*Code for Fire Prevention in Design of Interior Decoration of Buildings*>（GB50222-95）
4. <*Code for design of low voltage electrical installations*>（GBJ50054-95）
5. <*Technical requirements and test methods of electromagnetic shielding room for handling confidential information* > Level C（BMB3-1999）
6. <*General Specification for Computer field*> (GB/T 2887-2011)
7. <*Code for Design Protection of Structures Against Lightning*> (GB/50057-2010)

5.1.1.1 Public Area

The entrance and power distribution of TrustAsia CA's locate at this public area, where adopting keycard or fingerprint access control system.

5.1.1.2 Management Service Area

Service area is a working area for RA operator and administrators. Entering this area requires two reliable administrators to use keycard and fingerprint authentication with access log records.

5.1.1.3 Core Area

Core area, the area of CA operation and administration with keycard and fingerprint authentication. Certificate authentication system, encryption equipment, and other cryptographic devices are settled in this area. The CA signature servers, CA database servers, and other core devices are installed in the shielding zone. Only two authorized and specified administrators have rights to access this area by both keycard and fingerprint, to ensure that sensitive operations cannot be completed by a single person in the shielded area.

The separate buffer prevents electromagnetic leakage when shielded door opens.

5.1.2 Physical Access

TrustAsia CA data center installs electronic access system with the following functions:

1. The access control of each door is controlled by means of identification card and fingerprint identification;
2. There are log records for the entry and exit of every door;
3. Doors of the service area, the management area and the core area are all equipped with forcible entry alarm and overtime alarm;
4. The whole access control system is connected to UPS, and emergency power supply is provided by UPS at the time of power interruption.

The whole area also has a video surveillance system, no blind spot monitoring, the important channels inside and outside the site to implement 7*24 hours of uninterrupted video recording. All video information is retained for at least 3 months, and videos of major events are archived separately for inquiries. Set illegal intrusion detection alarm, environmental control detection alarm, sound and light alarm, while notifying operation and maintenance personnel.

5.1.3 Power and Air Conditioning

TrustAsia CA has a safe and reliable power supply system and an electric power reserve system to ensure the normal power supply for 7*24 hours and to provide normal services in the case of power supply interruptions in the power supply system.

In addition, TrustAsia CA also has a diesel engine which can meet the requirement of all racks lasting for more than 12 hours under full load. The machine room is equipped with air conditioning system to control the temperature and humidity in the operation facilities, and the power is configured according to the number of cabinets in each machine room and the full load of the equipment.

5.1.4 Water exposures

The water leakage alarm system is deployed at 1.45M above the ground in TrustAsia CA's machine room. and equipped with a leakage alarm system. Once flood occurs, the system will immediately give an alarm to notify the relevant personnel to take emergency measures.

5.1.5 Fire Prevention and Protection

TrustAsia CA machine room adopts the cabinet type heptafluoropropane automatic fire extinguishing device. The system collects fire-fighting data through the temperature and smoke fire detectors in the machine room, meanwhile it provides the system with real-time processing of the alarm data of the user's automatic fire alarm terminal and the system operation status data.
The system has two starting modes, automatic and manual operation, realizing the real-time detection and monitoring of network system and the setting of manual and automatic control mode of the system. It completes various linkage actions related to the system.

5.1.6 Media Storage

TrustAsia CA keeps the media storing software and data, archiving, auditing, or backup information in security facilities. These facilities are protected by appropriate physical and logical access control, allowing only the access of two authorized personnel and preventing these media from accidental compromise.

5.1.7 Waste Disposal

TrustAsia CA shreds sensitive files and materials out of use before processing to make the information unrecoverable. Before the disposal, cryptographic devices shall be initialized first and then be destroyed physically as per the method provided by the manufacturer.
At least 2 trusted personnel are present when processing the invalid content.

5.1.8 Off-site Backup

TrustAsia CA backups the coresystem data, audit log data at off-site location by offline media. The storage facilities fulfill the description of Section 5.1.7 media storage.

5.2 Procedural Controls

5.2.1 Trusted Roles

In the process of providing certification service, roles that essentially affect key operations, such as certificate issuance, use, administration, revocation, etc. will be regarded as trusted roles by TrustAsia CA. These roles include but are not limited to:

1. Authentication and customer service personnel, who are responsible for the validation of Subscriber certificates, and customer support services;
2. Key and cryptographic devices personnel, who are responsible for the management of CA keys, certificates life-cycle and cryptographic devices;
3. System maintenance personnel, who are responsible for the maintenance of the hardware and software of CA system;
4. Security management personnel, who are responsible for the area security and daily physical security management;
5. Security audit personnel, who are responsible for the audit of the operations;
6. Human resource management personnel, who are responsible for conducting the background investigation on trusted roles and the management of personnel security.

Trusted personnel are nominated by management position. The list of trusted personnel will be maintained and supervised every year.

5.2.2 Number of Individuals Required per Task

TrustAsia CA strictly defines the controls of core missions in specific standards. Multiple trusted roles are required to jointly complete the sensitive operation. For example:

1. Access to shielding area: set 2 trusted personnel access modes;
2. Identification, audit and certificate issuance: two trusted personnel are required to complete the work together;
3. Safe to save root key activation data: set to 2 trusted person open mode;
4. For operation and storage of the key cryptographic equipment, it requires at least three of five trusted persons to operate;
5. For background operation of the certificate issuance system, it requires at least two trusted persons to operate;
6. For system operation and maintenance personnel requires at least one person to operate, and one person to monitor and record.

5.2.3 Identification and Authentication for Trusted Roles

TrustAsia CA authenticates CA and RA systems before allowing the trusted roles access and executing the system, such as:

1. For the physical access of trusted personnel, the access card and fingerprint identification are used to identify and determine the corresponding authority.

2. For the trusted person who manages the Subscriber's certificate life cycle, the certificate management is completed by using the corresponding digital certificate to access the system.
3. For the system maintenance personnel, using their own accounts and passwords to log into the system through the bastion machine for maintenance.

5.2.4 Roles Requiring Separation of Duties

In order to ensure security of the systems, it should follow the trusted role segregation principle that the trusted role must be assumed by different personnel in TrustAsia CA. Roles requiring segregation of duties include but are not limited to, Subscriber identity validation, Subscriber identity validation review, system maintenance, CA key management, security auditor, etc.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

The qualification requirements of person who undertakes trusted role in TrustAsia CA are as follows:

1. Good social and working background.
2. Complying with state’s laws and regulations. Obeying TrustAsia’s unified arrangement and management.
3. Complying with the TrustAsia CA related security management norms, regulations and specifications.
4. Having good personalities and working attitudes, with good working experience.
5. A good team player.
6. Staff in key and core positions must have related working experience, or pass TrustAsia CA’s related training and examination before they start their work.

5.3.2 Background Check Procedures

TrustAsia CA may work with relevant government departments and investigation agencies to complete background checks on trusted employees. All trusted employees and those applying for transfer in must agree in writing to carry out background investigation. The background investigation must meet the requirements of laws and regulations, and the investigation contents, methods and personnel engaged in the investigation shall not violate laws and regulations. Background investigation shall use legal means to verify the background information of personnel through relevant organizations and departments as far as possible.

The background investigation is divided into basic investigation and comprehensive investigation. The basic survey includes work experience, career recommendation, education and social relations. In addition to the basic investigation items, the comprehensive investigation includes the investigation of criminal records, social relations and social security. It is necessary to conduct a comprehensive investigation on the key positions of the public trust certificate business.

HR review procedure includes:

1. The HR department is responsible for confirming candidate's personal information. Candidates should provide the following information: resume, the highest degree graduation certificate, degree certificate, qualification certificate and identity card and other related valid certificates.
2. The HR department identifies the authenticity of the information provided by candidates through telephone, correspondence, network, visits and other forms.
3. In the background investigation, if TrustAsia finds the following circumstances, TrustAsia can directly refuse qualifications of trusted personnel:
   - There is fabricating facts or information
   - With evidence of the unreliable staff
   - Use illegal identification or education, qualifications
   - The behavior of serious dishonesty in the work
4. The HR department checks candidates through on-site assessment, daily observation, situational test and other methods. Appropriate arrangement is made according to the investigation result.
5. After the review, TrustAsia CA signs a confidentiality agreement with employee in order to restrain employee not to reveal any confidential and sensitive information of CA certificate services. At the same time, TrustAsia CA will also be in accordance with the relevant organization regulations of personnel management and make job examination on in-service staff who assumed trusted role, so as to continuously review these employees' trustworthiness and working ability.

5.3.3 Training Requirements and Procedures

In order to make the relevant personnel competent for their work, TrustAsia CA has a special training program for all the personnel of the trusted roles. The training contents include:

1. Basic knowledge of Public Key Infrastructure (PKI);
2. CP&CPS and related standards and procedures;
3. Authentication and the policies and procedures of verification;
4. Security management policies and mechanisms;
5. Disaster recovery and business continuity management;
6. Job responsibilities requirements;
7. Baseline Requirements of CA/Browser Forum, EVG and others;
8. The laws, regulations, standards and procedures of electronic certification service in China;
9. Other needs of training.

Each Validation Specialist must complete all the trainings above to ensure that his or her performs validation duties satisfactorily. All Validation Specialists must pass the periodic examinations arranged by TrustAsia CA to ensure that he or she has the necessary skills and abilities to fulfill their obligations.

5.3.4 Retraining Frequency and Requirements

For persons acting as trusted roles or other important roles, they shall be trained at least once a year by TrustAsia CA. Related personnel for operating authentication system should have the training of relevant skills and knowledge at least once a year. In addition, TrustAsia CA will provide ongoing training for employees irregularly according to system upgrade, strategy adjustment and other requirements.

5.3.5 Job Rotation Frequency and Sequence

TrustAsia CA will define and change the Job rotation cycle and the sequence based on the organization security management strategy.

5.3.6 Sanctions for Unauthorized Actions

When the circumstances that in-service staff use TrustAsia CA systems, perform authorization businesses without or beyond the permission, once the above circumstances are confirmed by TrustAsia CA, TrustAsia CA will immediately revoke the login certificates and simultaneously terminate the system access authorization. TrustAsia CA makes the implementation of the official notice criticism, fine, dismissal and submit judicial institutions and other measures depend on the seriousness of unauthorized behavior.

5.3.7 Independent Contractor Controls

TrustAsia CA doesn't hire external personnel engaged in the work related to certificate validation for now.

5.3.8 Documentation Supplied to Personnel

During the training or retraining, TrustAsia CA provides materials including but not limited to the following categories:

1. CP&CPS and related agreements and standards;
2. Employee handbook;
3. Job descriptions, work flow and regulations;
4. Internal operating files, including business continuous management, disaster recovery programs, etc.;
5. Security management regulations and etc.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

TrustAsia CA records details of the actions taken to process a certificate request and to issue a certificate, including all information generated, the documents received in relation with the certificate request, the time and date, and the personnel involved. TrustAsia CA will record manually if the application does not record automatically. These events include but not limited to:

1. CA certificate and key lifecycle management events, including

a. Key generation, backup, storage, recovery, archiving, and destruction;
b. Certificate requests, renewal, re-key requests, and revocation;
c. Approval and rejection of certificate request, including successful or unsuccessful certificate practice;
d. Cryptographic device lifecycle management events, including device receiving, installation, uninstallation, activation, use and maintenance;
e. Generation of CRL entries;
f. Signing of OCSP Responses;
g. Introduction of new certificate profiles and retirement of existing certificate profiles.

2. Subscriber lifecycle management events, including
   a. Certificate requests, renewal, re-key requests and revocation;
   b. All verification activities stipulated in CA/Browser Forum Baseline Requirements and this CP&CPS;
   c. Acceptance and rejection of certificate requests, including accepting Subscriber Agreement, verification of application materials, and storage of application and verification materials;
   d. Issuance of certificates;
   e. Generation of CRL entries; and
   f. Signing of OCSP Responses.
3. Security events, including
   a. Successful and unsuccessful PKI system access attempts;
   b. PKI and security system actions performed;
   c. Security profile changes;
   d. Installation, update and removal of software on a Certificate System;
   e. System crashes, hardware failures, and other anomalies;
   f. Firewall and router activities; and
   g. Entries to and exits from the CA facility, including the access of authorized and unauthorized personnel and security storage device.
4. System operating events, including:
   a. Startup and shutdown;
   b. Creation or deletion of permission, configuration or modification of password;
   c. Unauthorized access and access attempts to CA system network;
   d. Unauthorized access and access attempts to system files;
   e. Reading, writing or deletion of secure and sensitive files or records.
5. Management record of trusted roles and personnel, including
   a. The network account application;
   b. System permission application, modification, and creation;
   c. The changes of personnel status.

Generally, the log records shall include:

1. Date and time of record;
2. The serial number of the record;

3. The identity of the entity making the log;
4. Description of the recorded content.

5.4.1.1 Router and Firewall Activities Logs

TrustAsia CA router and firewall activities logs include at least the following:

1. Successful and unsuccessful login attempts to routers and firewalls;
2. Logging of all administrative actions performed 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 systems events and errors, including hardware failures, software crashes, and system restarts.

5.4.2 Frequency for Processing and Archiving Audit Logs

TrustAsia CA checks and summarizes the system's automatic log and operators' manual records once a month.
TrustAsia CA tracks and handles the system security log once a month to check violations of policies and other major events.

5.4.3 Retention Period for Audit Logs

TrustAsia CA and its Timestamp Authority retain the following logs for at least two years:

1. CA certificate and key lifecycle management event records (as set forth in Section 5.4.1-1) after the later occurrence of:
   a. The destruction of the CA Private Key; or
   b. The revocation or expiration of the final CA Certificate in that set of Certificates that have an X.509v3 basicConstraints extension with the CA field set to true and which share a common Public Key corresponding to the CA Private Key.
2. Subscriber Certificate lifecycle management event records (as set forth in Section 5.4.1-2) after the revocation or expiration of the Subscriber Certificate.
3. Timestamp Authority data records (as set forth in Section 5.5.5) after the revocation or renewal of the Timestamp Certificate private key.
4. Any security event records (as set forth in Section 5.4.1-3 and for Timestamp Authority security event records set forth in Section 5.5.5-3) after the event occurred.

Note: While these requirements set the minimum retention period, TrustAsia and the Timestamp Authority will choose a greater value as more appropriate in order to be able to investigate possible security or other types of incidents that will require retrospection and examination of past events.

5.4.4 Protection of Audit Log

TrustAsia CA audit logs are stored in the database with backup, including audit information and event records in related documents.
TrustAsia CA carries out strictly the measures of physical and logical access control to ensure that only personnel authorized by TrustAsia can be access to the records being reviewed. These records are strictly protected from unauthorized access, reading, modification and deletion.

5.4.5 Audit Log Backup Procedures

TrustAsia CA's system log is backed up to the log server in real time, and to the different places weekly. The manual paper records are archived periodically and saved in a special filing cabinet.

5.4.6 Audit Log Accumulation System

Regarding the electronic audit information, TrustAsia CA's log server can collect and archive the following logs:

1. certificate management system;
2. certificate issuing system;
3. certificate accepting system;
4. telecommunication system;
5. certificate acceptance system;
6. access control system;
7. Website and database security management system;
8. other systems that need to be audited.

Regarding paper audit information, there is a special filing cabinet for collection and archival.

5.4.7 Notification to Event-Causing Subject

When TrustAsia CA detects the attack, it will record the attacker's behaviors, trace the attacker to the extent permitted by the law, and retain the right to take the corresponding countermeasures. TrustAsia CA has the right to decide whether to notify subjects related to the event.

5.4.8 Vulnerability Assessments

TrustAsia CA performs an annual risk assessment that:

1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any certificate data or certificate management processes;
2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the certificate data and certificate management processes; and
3. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that TrustAsia CA has in place to counter

such threats. Based on the risk assessment, TrustAsia CA develops, implements, and maintains a security plan consisting of security procedures, measures, and products designed to achieve the objectives set forth above and to manage and control the risks identified during the risk assessment. The security plan includes administrative, organizational, technical, and physical safeguards appropriate to the sensitivity of the certificate data and certificate management processes. The security plan also takes into account then-available technology and the cost of implementing the specific measures, and implements a reasonable level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected.

5.5 Records Archival

5.5.1 Types of Records Archived

TrustAsia CA archives all audit logs as set forth in Section 5.4.1, and additionally retains the following types of records in its archives, including but not limited to:

1. Documentation related to the security of the Certificate Systems, Certificate Management Systems, Root CA Systems, and Delegated Third Party Systems; and
2. Documentation related to the verification, issuance, and revocation of certificate requests and certificates.

5.5.2 Retention Period for Archive

Archived audit logs (as set forth in Section 5.5.1) will be retained for a period of at least two years from their record creation timestamp, or as long as they are required to be retained per Section 5.4.3, whichever is longer.

TrustAsia CA retains the following for at least two years:

1. All archived documentation related to the security of Certificate Systems, Certificate Management Systems, Root CA Systems and Delegated Third Party Systems (as set forth in Section 5.5.1); and
2. All archived documentation relating to the verification, issuance, and revocation of certificate requests and certificates (as set forth in Section 5.5.1) after the later occurrence of:
    a. such records and documentation were last relied upon in the verification, issuance, or revocation of certificate requests and certificates; or
    b. the expiration of the Subscriber Certificates relying upon such records and documentation.

5.5.3 Protection of Archive

TrustAsia CA has secure physical and logical protection measures and strict management procedures for various electronic and paper filing documents, ensuring that the archived documents will not be compromised and preventing unauthorized access, alteration, deletion or other tampering behaviors.

5.5.4 Archive Backup Procedures

Backups of electronic archiving records generated by the system will be made regularly and backup files will be stored in different places; the manual electronic records will be archived in SVN.
For written archive materials, backup is not required, yet strict measures are required to protect their security and prevent deletion, alteration, etc. of archives and their backups.

5.5.5 Requirements for Time-stamping of Records

TrustAsia CA will automatically timestamp its records based on the system time as they are created (non-cryptographic time-stamping). The time on TrustAsia CA's time source server is synchronized to the universal coordinated time (UTC) recognized by National Measurement Institute.

The Timestamp Authority of TrustAsia CA will log the following information and make these records available to its qualified auditor as proof of the Timestamp Authority's compliance with the Baseline Requirements.

1. Physical or remote access to a timestamp server, including the time of the access and the identity of the individual accessing the server,
2. History of the timestamp server configuration,
3. Any attempt to delete or modify timestamp logs,
4. Security events, including:
    a. Successful and unsuccessful Timestamp Authority access attempts;
    b. Timestamp Authority server actions performed;
    c. Security profile changes;
    d. System crashes and other anomalies; and
    e. Firewall and router activities;
5. Revocation of a TimeStamp certificate,
6. Major changes to the timestamp server's time, and
7. System startup and shutdown.

5.5.6 Archive Collection System

For system-generated electronic records, they are synchronized to the log server in real time and backed up to the off-site every week.
For electronic records, the SVN server completes the collection and backup work.
For written archive materials, they are collected and archived into the management area.

5.5.7 Procedures to Obtain and Verify Archive Information

TrustAsia CA takes physical and logical access control methods to ensure that only the authorized personnel can approach the archive information and strictly prohibit unauthorized operations such as access, reading, alteration and deletion, etc.

5.6 Key Changeover

The validity period of TrustAsia CA's root certificate is not more than 25 years. The end time of any certificate issued by it, including CA certificate and Subscriber certificate, does not exceed the end time of the root certificate, and the end time of any Subscriber certificate issued by CA certificate does not exceed the end time of CA certificate.
When the lifetime of the key pair that corresponds to the CA certificate exceeds the maximum life cycle specified in this CP&CPS, TrustAsia CA will start the key renewal process and replace the already expired CA key pair. The key changeover of TrustAsia CA is carried out in the following ways:

1. The higher CA will stop issuing a new subordinate CA certificate ("the date of stopping issuance") before the expiration time of its private key is less than the lifetime of the subordinate CA key.
2. After "the date of stopping certificate issuance", a new CA key will be adopted for issuing certificates for the approved Subordinate CA or Subscriber certificate request.
3. Generate a new key pair and issue a new higher CA certificate.
4. The higher CA continues to use the original CA private key to issue CRL until the last certificate issued by the original private key expires.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

TrustAsia CA documents a business continuity and disaster recovery procedures designed to notify and reasonably protect Application Software Suppliers, Subscribers, and Relying Parties in the event of a disaster, security compromise, or business failure. TrustAsia CA does not publicly disclose its business continuity plans but its business continuity plan and security plans are available to the auditors upon request. TrustAsia CA annually tests, reviews and updates these procedures.

The business continuity plan includes:

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

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

5.7.2 Recovery Procedures if Computing resources, software, and/or data are corrupted

TrustAsia CA has backed up the resources, software and/or data of the service system and other important systems, and has developed the corresponding emergency handling process. In case of network failure, system and software compromise, database failure, etc., or a disaster caused by force majeure, TrustAsia CA will implement the recovery in accordance with the disaster recovery plan.

5.7.3 Recovery Procedures after Key Compromise

1. When the certificate Subscriber finds that the entity certificate private key is compromised, the Subscriber must immediately stop using the private key and immediately visit certificate service sites of TrustAsia CA to revoke the certificate, or immediately notify TrustAsia CA revoke the certificate by telephone, etc., and reapply for a new certificate according to the relevant process. TrustAsia CA will issue certificate revocation information according to Section 4.9 of this CP&CPS.
2. When TrustAsia CA finds that the entity certificate private key of the Subscriber certificate is compromised, TrustAsia CA will immediately revoke the certificate and notify the certificate Subscriber; the Subscriber must immediately stop using the private key and reapply for a new certificate according to the relevant process. TrustAsia CA will issue certificate revocation information according to Section 4.9 of this CP&CPS.
3. When the private key of TrustAsia CA root CA or subordinate CA is compromised, TrustAsia CA will handle the emergency according to key emergency plan, and notify the relying party such as Microsoft, Mozilla, Google, Apple, Adobe, Oracle, 360 through various ways.

5.7.4 Business Continuity Capabilities after a Disaster

In the event of a major disaster at the physical site, TrustAsia CA will restore some services within 48 hours in accordance with the business continuity plan.

5.8 CA or RA Termination

When TrustAsia CA needs to stop their business, they will work strictly in accordance with the requirements of Electronic Signature Law of the People's Republic of China and the relevant regulations on the business suspension for certification authorities.
Before termination, TrustAsia CA will:

1. Determine the service undertaking unit;
2. Draft the termination statement of TrustAsia CA;
3. Notify the relevant entities which are involved in the TrustAsia CA termination at least 90 days in advance (such as Microsoft, Mozilla, Google, Apple, Adobe, Oracle, 360);
4. Process the archive records;
5. Stop the service of CA system;
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

The key pairs of CAs are generated within the cryptographic devices that meet the FIPS140-2 Level 3 standard, in a physically secure environment. The generation, management, storage, backup and recovery of the key pair comply with the relevant regulations of FIPS140-2.

The generation of the CA key pairs is witnessed by multiple key administrators, several trusted personnel and qualified independent third-party auditors, and is completed in accordance with a key pair generation script prepared by TrustAsia CA in advance in TrustAsia CA shield computer room. The procedures and operations related to CA key pair generation shall be video recorded, and the qualified independent third-party auditor should issue a report opining that the CA key pair generation process and the controls by TrustAsia CA are able to 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

Subscriber’s key pairs are generated by the built-in key generation mechanism of Subscriber's server or other equipment. TrustAsia CA does not generate a Server Certificate key pair for a Subscriber.

For Code Signing, EV Code Signing and Document Signing certificates, subscribers should ensure that private keys are generated in a cryptographic module that meets or exceeds the following standards:

- FIPS 140-2 Level 2, or
- CC EAL 4+

TrustAsia CA rejects a certificate request if one or more of the following conditions occur:

1. The key pair does not meet the requirements set forth in Section 6.1.5 or 6.1.6 in this CP&CPS;
2. There is clear evidence that the specific method used to generate the private key was flawed;
3. TrustAsia CA has a demonstrated or proven method that indicates the leak of the private key;
4. TrustAsia CA has previously been made aware that the private key has suffered a key compromise, such as through the provisions of Section 4.9.1.1;
5. TrustAsia CA is aware of a demonstrated or proven method to easily compute the private key based on the public key (such as a Debian weak key, see https://wiki.debian.org/SSLkeys).

6.1.2 Private Key Delivery to Subscriber

TrustAsia CA does not generate or deliver the key pair on behalf of the Subscriber.

6.1.3 Public Key Delivery to Certificate Issuer

As part of the certificate application process, subscribers generate key pair and submit the public key to TrustAsia CA in CSR.

6.1.4 CA Public Key Delivery to Relying Parties

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

6.1.5 Key Sizes

To ensure the security strength of the keys, TrustAsia CA uses a linting tool to perform key size check before certificate issuance, ensuring that TrustAsia CA's different types of certificate keys meet the following standards:

Certificate Type	ROOT Certificate	Subordinate Certificate	Subscriber Certificate
Digest Algorithm	SHA256, SHA384	SHA256, SHA384	SHA256, SHA384
RSA Key Size	4096	3072, 4096 (For Code Signing and EV Code Signing certificates, the minimum key size is 4096 bits.)	2048, 3072, 4096 (For Code Signing and EV Code Signing certificates, the minimum key size is 3072 bits.
ECC Curve	P-384	P-384	P-256, P-384

6.1.6 Public Key Parameters Generation and Quality Checking

TrustAsia CA and Subscribers shall generate public keys in accordance with the regulations stipulated in Section 6.1.1 in this CP&CPS. Public key parameters are generated by compliant devices/platforms to ensure parameter quality. Public keys must meet the requirements stipulated in Section 6.1.5.
TrustAsia CA uses linting tools to check public key parameters before the issuance of a certificate to ensure that the public key parameters meet the following requirements:

- For RSA public keys:
  1. The public exponent is an odd number equal to 3 or more.
  2. The public exponent is in the range between 2^16+1 and 2^256-1.
  3. The modulus is an odd number.
  4. The minimum modulus size is 2048 bits and is an integer multiple of 8.
  5. The modulus is not the power of a prime.
  6. The modulus has no factors smaller than 752.
- For ECDSA public keys:
  The validity of all ECDSA keys is confirmed using either the ECC Full Public Key Validation Routine or the ECC Partial Public Key Validation Routine.

6.1.7 Key Usage Purposes

X.509v3 certificate issued by TrustAsia CA includes key usage extensions, and their usage conforms to RFC5280 Standard. Regarding the purposes specified by TrustAsia CA in key usage extensions of the issued certificate, the certificate Subscriber shall use the key according to specified purposes.
The root CA key is generally used to issue the following certificates and CRL:

1. self-signed certificate representing the root CA;
2. subordinate CA certificate and cross certificate;
3. OCSP Responder Certificates.

The subordinate CA key is generally used to issue the following certificates and CRL:

1. Subscriber certificate;
2. TimeStamp signing certificate;
3. OCSP Responder Certificate;

The Subscriber's key can be used to provide security services, such as identity authentication, information encryption and signature, non-repudiation and information integrity; the encryption key pair can be used to encrypt and decrypt information.
The combination usage of signature key and encryption key can achieve security mechanisms such as identity authentication, authorization management and responsibility identification.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

TrustAsia CA implements physical and logical safeguards to prevent unauthorized certificate issuance. Regarding protection of the CA private key outside the validated system or device specified above, TrustAsia CA stores the encrypted key shards in the physical devices of different entities to prevent disclosure of the private key. TrustAsia CA encrypts its private key with an algorithm and key-length that, according to the state of the art, are capable of withstanding cryptanalytic attacks for the residual life of the encrypted key or key part.

6.2.1 Cryptographic Module Standards and Controls

Cryptographic modules used by TrustAsia CA for CA key pairs and timestamp key pairs meet the FIPS 140-2 Level 3 standards.
Cryptographic modules used for code signing, EV code signing and document signing certificates meet or exceed the following standards:

- FIPS 140-2 Level 2, or
- CC EAL 4+

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

The generation, update, revocation, backup and restoration of TrustAsia CA private key are controlled by a multi-person mechanism, with the management authority of the private key distributed to 5 key administrators, and only when at least 3 or more of the key administrators are present and permitting, can the private key be operated by inserting the administrators 's IC card or USBKey and entering the PIN code.

6.2.3 Private Key Escrow

TrustAsia CA does not escrow private keys.

6.2.4 Private Key Backup

TrustAsia CA backups for the root private key and the CA private key， generate backup ciphertext files and backup authority recovery IC cards or USBKey according to the operation specification provided by the encryption equipment manufacturer and save them in the company's safe box (or bank safe deposit box and other location that security levels are not lower than the local backup).

6.2.5 Private Key Archival

TrustAsia CA does not archive private keys of Subscriber certificates. The private keys of all CA certificates will not be archived by third parties.

6.2.6 Private Key Transfer into or from a Cryptographic Module

TrustAsia CA's key pair is generated, saved and used on the hardware cryptographic module. In order to achieve recovery, TrustAsia CA backs up the CA key according to the operation specification provided by the encryption equipment manufacturer. Besides, TrustAsia CA also has strict key management process to control the replication of CA key pair. All these measures have effectively prevented the loss, theft, alteration, unauthorized disclosure, and unauthorized use of CA private key.

6.2.7 Private Key Storage on Cryptographic Module

6.2.7.1 CA Private Key Storage

TrustAsia CA private keys are stored in a hardware cryptographic module that meets the requirements of FIPS 140-2 level 3 in an encrypted form, and the use of private keys are also conducted in the hardware cryptographic module.

6.2.7.2 Timestamp Authority Private Key Storage

TrustAsia CA protects its private keys for timestamp authorities in accordance with the requirements stipulated in Section 6.2.7.1 in this CP&CPS.

6.2.7.3 Private Key Storage for Signing Services

For EV Code Signing Certificates, Code Signing Certificates and Document Signing Certificates, Signing Services will ensure that the hardware cryptographic module utilized when a Subscriber's private key is generated, stored and used, conforms to at least FIPS 140-2 Level 3 or Common Criteria EAL 4+. Subscribers should use one of the following techniques to satisfy this requirement:

1. Use of a hardware cryptographic module, verified by means of a FIPS or Common Criteria certificate.
2. A cloud-based key generation and protection solution with the following requirements:
    a. Key creation, storage, and usage of private key must remain within the security boundaries of the cloud solution's hardware cryptographic module that conforms to the specified requirements;
    b. Subscription at the level that manages the private key must be configured to log all access, operations, and configuration changes on the resources securing the private key.
3. Signing Services provided by TrustAsia CA.

6.2.7.4 Subscriber Private Key Protection and Verification

6.2.7.4.1 Subscriber Private Key Protection

For Code Signing, EV Code Signing and Document Signing Certificates, Subscribers shall provide TrustAsia CA with contractual representation to show one of the following techniques will be used to satisfy private key protection requirements:

1. Subscriber provides TrustAsia CA with an auditable statement which shows Subscriber private key is generated and stored in a hardware cryptographic module that conforms to at least the following standards:
    - FIPS 140-2 level 2, or
    - Common Criteria EAL 4+
2. A cloud-based key generation and protection solution with the following requirements:
    a. Key creation, storage, and usage of private key must remain within the security boundaries of the cloud solution's hardware cryptographic module that conforms to the specified requirements;
    b. Subscription at the level that manages the private key must be configured to log all access, operations, and configuration changes on the resources securing the private key.
3. Subscriber uses a Signing Service which meets the requirements of Section 6.2.7.3 in this CP&CPS.

6.2.7.4.2 Subscriber Private Key Verification

TrustAsia CA uses one of the following methods to confirm that Subscriber private key protection meets the above requirements:

- The Subscriber provides key attestation generated by an HSM manufacturer to demonstrate that the private key corresponding to the Subscriber's CSR is generated in a non-exportable way using a suitable HSM.
- The Subscriber uses a TrustAsia CA prescribed crypto library, software and HSM combination for the key pair generation and storage.
- TrustAsia CA relies on a report provided by the Applicant that is signed by an auditor who is approved by TrustAsia CA and who has IT and security training or is a CISA witnesses the key pair creation in a suitable hardware cryptographic module solution including a cloud-based key generation and protection solution.
- The Subscriber provides an agreement that they use a Signing Service meeting the requirements of Section 6.2.7.3 in this CP&CPS.

6.2.8 Activating Private Keys

The TrustAsia CA private key is stored in the hardware cryptographic module, and activation needs to be achieved using the encrypted device's operator privileges as per Section 6.2.2 of this CP&CPS, where at least half of the key administrators are present and permitted. When the CA private key is required (online or offline), the key administrators is required to provide the operator IC card or USBKey and enter the PIN to do so.

6.2.9 Deactivating Private Keys

Regarding private keys of TrustAsia CA, when CA system sends logout instruction to the cryptographic module or when the cryptography management software sends close instruction to the cryptographic module, or when the hardware cryptographic module that stores private keys is power off, private keys enter the inactivated state. The operation of removing the private key is performed when at least half of the key administrators are present and permitting, and the key administrator logs into the server cryptographic machine using an administrator card containing his or her own PIN.

6.2.10 Destroying Private Keys

After the life cycle of TrustAsia CA's private key ends, TrustAsia CA will continue to keep the CA private key in a backup hardware cryptographic module and archive it, and the other CA private key backups are safely destroyed. Meanwhile, all PIN codes and IC cards or USBKey, etc. for activating the private key must be destroyed. Before the commercial purpose of the CA private key or its application has lost its value or the legal liability expires, the CA shall not destroy its private key.
An archived CA private key needs to be securely destroyed with the involvement of multiple trusted personnel after its archival period has expired, or when a backup or copy of the CA private key is no longer in use for a valid business purpose. the

destruction of the CA private key will ensure that the CA private key is completely removed from the hardware cryptographic module, leaving no residual information.

6.2.11 Cryptographic Module Capabilities

See Section 6.2.1

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

For TrustAsia CA public key archiving, please refer to Section 5.5.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The maximum validity period of TrustAsia CA certificates:

Type	Private Key Usage Periods	Certificate Valid Period
Publicly Trusted Root CA	No stipulation	25 years
Publicly Trusted Sub-CA	No stipulation	20 years
DV SSL/TLS Server Certificates	No stipulation	397 days
OV SSL/TLS Server Certificates	No stipulation	397 days
EV SSL/TLS Server Certificates	No stipulation	397 days
Document Signing Certificates	No stipulation	39 months
Code Signing Certificates	No stipulation	39 months
EV Code Signing Certificates	No stipulation	39 months
S/MIME Certificates	No stipulation	27 months
Timestamp Certificates	15 months	135 months

Effective April 15, 2025, private keys associated with Timestamp Certificates issued for greater than 15 months will be removed from the hardware cryptographic module protecting the private key within 18 months after issuance of the Timestamp Certificate. For Timestamp Certificates issued on or after June 1, 2024, TrustAsia CA will log the removal of the private key from the hardware cryptographic module through means of a key deletion ceremony performed by TrustAsia CA and witnesses and signed-off by at least two trusted role members.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The TrustAsia CA private key activation data is generated by the encryption device in accordance with the operating specifications provided by the manufacturer of the encryption device and with the permission of at least half of the key managers present.

The activation data of the Subscriber's private key, including the password used to download the certificate (provided in the form of a password envelope, etc.), the USB key, the login password of the IC card, etc., must be generated in a safe and reliable environment. These activation data are delivered to subscribers in a safe and

reliable way, such as offline face-to-face delivery, postal delivery, etc. For non-one-time use activation data, TrustAsia CA recommends that users modify it by themselves.

If Subscriber's certificate private key is password, then all the protection password should follow the following principles:

1. Contain at least eight characters
2. Contain one lowercase letter at least
3. Not contain many of the same characters
4. Not be the same as operator's name
5. Not use birthdays, telephone numbers
6. Longer substring in username information

6.4.2 Activation Data Protection

Activation data of CA private key (smart IC card and PIN code) is kept in reliable way and by trusted personnel by TrustAsia CA. All the trusted personnel are requested to remember password instead of marking it down or sharing with others. Subscriber's activation data must be generated in the safe and reliable environment and be properly safeguarded or destroyed, and cannot be leaked to others. If the certificate Subscriber uses a password or PIN to protect private key, the Subscriber should take good care of password or PIN to prevent the leakage or theft. If the certificate Subscriber uses biological characteristics to protect the private key, the Subscriber should also pay attention to prevent his/her biological characteristics from illegal obtaining.

6.4.3 Other Aspects of Activation Data

Activation of private key shall be protected from loss, theft, modification, unauthorized disclosure, or unauthorized usage during the transmission.
The activation data of private key which is no longer used will be destroyed and protected from theft, disclosure or unauthorized use during the destruction. The result of destruction is that some or all of activation data can't be recovered directly or indirectly from the residual information and medium, papers recorded with passwords must be shredded.
For the security reasons, the rules of certificate applicant activate data of lifecycle as below:

1. The password used to apply for certificate becomes invalid after successful application.
2. The password used to protect the private key, or IC card, USB Key, could be modified by Subscriber at any time based on business application, and should be modified three months after the validity.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

Information security management of TrustAsia certification system meets <*Specifications Related Security Technology Certificate Authentication System*> published by OSCCA, <*Measures for the Administration of Electronic Certification Services*> published by Ministry of Industry and Information Technology, standards of information security in ISO 27001 and security standards of other relevant information. TrustAsia draws up comprehensive and perfect security management strategies and standards, which have been implemented, reviewed and recorded within operation. The main security technologies and control measures include: Identification and authentication, logic access control, physical access control, management of personnel's responsibilities decentralization, network access control, etc.

Multi-Factor Authentication is used for all the accounts capable of certificate issuance.

For the system operation staffs, log in to the system through the bastion machine to ensure that the CA software and data files are safe and reliable, and will not be accessed without authorization.

Core system must be separated physically from other systems and the production system must be separated from other system logically. This separation can prohibit network access except for specific applications. The usage of firewall is to prevent the intrusion from the internal and external network production system and restrict activities of access production system. Only trusted persons in operation and management group of CA system, when necessary to access the system can access the CA database using password.

6.5.2 Computer Security Rating

TrustAsia CA system and its operating environment have passed third-party security assessments and penetration testing, and have received appropriate test reports.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

Software design and development of TrustAsia CA process follows principles:

1. Establish internal system of corporation about update, alteration and application. The employees should follow this system strictly.
2. Establish internal purchasing process and management system of corporation.
3. After the programs have passed strict test in development environment, they can be deployed to production environment.
4. Effective online backup must be done before deployment changes.
5. Verification and review of third-party
6. The security risk analysis and reliability design

6.6.2 Security Management Controls

TrustAsia CA has developed a variety of security strategies, management systems and processes for security management of the certification system.
The information security management of the authentication system strictly follows the relevant operation management specifications of OSCCA.
The usage of authentication system has strict control measures. All systems are tested and verified strictly before use. Any modification and upgrade will be recorded.
TrustAsia CA conducts regular security checks on the system to identify whether the equipment has been intruded, whether there are security vulnerabilities, and etc.

6.6.3 Life Cycle Security Controls

TrustAsia CA controls the R&D and online work of certificate certification system through internal change control process to ensure the safety and reliability of the system.

6.7 Network Security Controls

TrustAsia CA's certification system adopts firewall to implement access control, IDS/IPS to resist network attack, bastion host to manage the authority of remote-logging, and router to layer the intranet.
The certification system only opens to specific services and personnel with the minimum access authority.
The certification system regularly scans security vulnerabilities, checks the configuration of security devices, and audits the system logs.
The network security controls by TrustAsia CA comply with the CA/Browser Forum's Network and Certificate System Security Requirements (NCSSR).

6.8 Time-Stamping

The system time on TrustAsia CA computers is updated using the Network Time Protocol (NTP) in order to synchronize system clocks at least once every 24 hours.
An internal NTP server is maintained by TrustAsia CA that synchronizes with external sources and maintains the accuracy of its clock within one second or less.
In addition, there is a dedicated Timestamp Authority (TSA) of TrustAsia CA in operation in order to provide timestamp services in accordance to RFC 3161.

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

TrustAsia CA meets the technical requirements set forth in Section 2.2, 6.1.5 and 6.1.6, and effective 2023-09-01, TrustAsia CA issues certificates in accordance with the requirements specified in this Section.

7.1.1 Version Number(s)

All Certificates are X.509 Version 3 certificate. The version information is listed in the version field of the certificate.

7.1.2 Certificate Content and Extensions

In accordance with the requirements specified in RFC5280, the profiles in the following sections cover all certificates issued by TrustAsia CA.

- 7.1.2.1 Root CA Certificate Profile
- 7.1.2.3 Technically Constrained Non-TLS Subordinate CA Certificate Profile
- 7.1.2.6 TLS Subordinate CA Certificate Profile
- 7.1.2.7 Subscriber Certificate Profile
- 7.1.2.8 OCSP Responder Certificate Profile
- 7.1.2.9 Precertificate Profile

7.1.2.1 Root CA Certificate Profile

See Section 11.1.

7.1.2.1.1 Root CA Validity

See Section 11.1.

7.1.2.1.2 Root CA Extensions

See Section 11.1.

7.1.2.1.3 Root CA Authority Key Identifier

See Section 11.1.

7.1.2.1.4 Root CA Basic Constraints

See Section 11.1.

7.1.2.2 Cross-Certified Subordinate CA Certificate Profile

No stipulation.

7.1.2.2.1 Cross-Certified Subordinate CA Validity

No stipulation.

7.1.2.2.2 Cross-Certified Subordinate CA Naming

No stipulation.

7.1.2.2.3 Cross-Certified Subordinate CA Extensions

No stipulation.

7.1.2.2.4 Cross-Certified Subordinate CA Extended Key Usage – Unrestricted

No stipulation.

7.1.2.2.5 Cross-Certified Subordinate CA Extended Key Usage – Restricted

No stipulation.

7.1.2.3 Technically Constrained Non-TLS Subordinate CA Certificate Profile

TrustAsia CA issues not only TLS Certificates, but also Code Signing Certificates, S/MIME Certificates, Document Signing Certificates, TimeStamp Certificates, and OCSP Responder Certificates. See Appendix 11.2 for the profiles.

7.1.2.3.1 Technically Constrained Non-TLS Subordinate CA Certificate Extensions

See Section 11.2.

7.1.2.3.2 Technically Constrained Non-TLS Subordinate CA Certificate Policies

See Section 11.2.

7.1.2.3.3 Technically Constrained Non-TLS Subordinate CA Certificate Extended Key Usage

See Section 11.2.

7.1.2.4 Technically Constrained Precertificate Signing CA Certificate Profile

No stipulation.

7.1.2.4.1 Technically Constrained Precertificate Signing CA Extensions

No stipulation.

7.1.2.4.2 Technically Constrained Precertificate Signing CA Extended Key Usage

No stipulation.

7.1.2.5 Technically Constrained TLS Subordinate CA Certificate Profile

No stipulation.

7.1.2.5.1 Technically Constrained TLS Subordinate CA Extensions

No stipulation.

7.1.2.5.2 Technically Constrained TLS Subordinate CA Name Constraints

No stipulation.

7.1.2.6 TLS Subordinate CA Certificate Profile

See Section 11.2.

7.1.2.6.1 TLS Subordinate CA Extensions

See Section 11.2.

7.1.2.7 Subscriber Certificate Profile

TrustAsia CA issues TLS Certificates, see Appendix 11.3 for the profile. In addition, TrustAsia CA issues Code Signing Certificates, S/MIME Certificates, Document Signing Certificates, and TimeStamp Certificates and OCSP Responder Certificates which are for other usage, see Appendix 11.3 for the profiles.

7.1.2.7.1 Subscriber Certificate Types

The types of TLS Certificates include: Domain Validated (DV), Organization Validated (OV), Extended Validation (EV). TrustAsia CA currently does not issue Individual Validated (IV) certificates.
The types of Code Signing Certificates include: Code Signing (CS), Extended Validation Code Signing (EVCS).
The types of S/MIME Certificates include: Mailbox Validation (MV), Individual Validation (IV), Organization Validation (OV), Sponsor Validation (SV).
Other types include: Document Signing Certificate (DS), TimeStamp Certificate and OCSP Responder Certificate.

7.1.2.7.2 Domain Validated

See Section 11.3.1.

7.1.2.7.3 Individual Validated

No stipulation.

7.1.2.7.4 Organization Validated

See Section 11.3.2.

7.1.2.7.5 Extended Validation

See Section 11.3.3.

7.1.2.7.6 Subscriber Certificate Extensions

See Section 11.3.

7.1.2.7.7 Subscriber Certificate Authority Information Access

See Section 11.3.

7.1.2.7.8 Subscriber Certificate Basic Constraints

See Section 11.3.

7.1.2.7.9 Subscriber Certificate Certificate Policies

See Section 11.3. All Reserved Certificate Policy Identifier are defined and documented in this CPS Section 1.2.1. All Subscriber Certificates have the policyQualifiers field (id-qt-cps:1.3.6.1.5.5.7.2.1), and the content is the URL for this CPS.

7.1.2.7.10 Subscriber Certificate Extended Key Usage

See Section 11.3.

7.1.2.7.11 Subscriber Certificate Key Usage

See Section 11.3.

7.1.2.7.12 Subscriber Certificate Subject Alternative Name

See Section 11.3. The zero-length Domain Label representing the root zone of the Internet Domain Name System is not included in dNSName.

7.1.2.8 OCSP Responder Certificate Profile

See Section 11.3.11.

7.1.2.8.1 OCSP Responder Validity

See Section 11.3.11.

7.1.2.8.2 OCSP Responder Extensions

See Section 11.3.11.

7.1.2.8.3 OCSP Responder Authority Information Access

No stipulation.

7.1.2.8.4 OCSP Responder Basic Constraints

See Section 11.3.11.

7.1.2.8.5 OCSP Responder Extended Key Usage

See Section 11.3.11.

7.1.2.8.6 OCSP Responder id-pkix-ocsp-nocheck

See Section 11.3.11.

7.1.2.8.7 OCSP Responder Key Usage

See Section 11.3.11.

7.1.2.8.8 OCSP Responder Certificate Policies

No stipulation.

7.1.2.9 Precertificate Profile

A Precertificate is a signed data structure that can be submitted to a Certificate Transparency log, as defined by RFC 6962. A Precertificate appears structurally identical to a Certificate, with the exception of a special critical poison extension in the extensions field, with the OID of 1.3.6.1.4.1.11129.2.4.3. This extension ensures that the Precertificate will not be accepted as a Certificate by clients conforming to RFC 5280. The existence of a signed Precertificate can be treated as evidence of a corresponding Certificate also existing, as the signature represents a binding commitment by TrustAsia CA that it may issue such a Certificate.

A Precertificate is created after a CA has decided to issue a Certificate, but prior to the actual signing of the Certificate. TrustAsia CA will construct and sign a Precertificate corresponding to the Certificate, for purposes of submitting to Certificate Transparency Logs. TrustAsia CA will use the returned Signed Certificate Timestamps to then alter the Certificate's extensions field, adding a

Signed Certificate Timestamp List, as defined in Section 7.1.2.11.3 and as permitted by the relevant profile, prior to signing the Certificate.

Once a Precertificate is signed, relying parties are permitted to treat this as a binding commitment from TrustAsia CA of the intent to issue a corresponding Certificate, or more commonly, that a corresponding Certificate exists. A Certificate is said to be corresponding to a Precertificate based upon the value of the tbsCertificate contents, as transformed by the process defined in RFC 6962, Section 3.2.

TrustAsia CA will not issue a Precertificate unless it is willing to issue a corresponding Certificate, regardless of whether it has done so. The Precertificate will be issued directly by the Issuing CA.

The encoded values of the Precertificate Profile are byte-for-byte identical to that of the corresponding Certificate.The fields of Precertificate Profile are the same as the ones in TLS Certificate Profile as seen in Appendix 11.3. The serialNumber field of the Precertificate is identical to that of the corresponding Certificate. For the extensions of Precertificate Profile, see Section 7.1.2.9.1.

7.1.2.9.1 Precertificate Profile Extensions – Directly Issued

Extension	Presence	Critical	Description
Precertificate Poison (OID: 1.3.6.1.4.1.11129.2.4.3)	Must	Y	
Signed Certificate Timestamp List	Must Not	-	
Any other extension	-	-	The order, criticality, and encoded values of all other extensions are byte-for-byte identical to the extensions field of the Certificate.

7.1.2.9.2 Precertificate Profile Extensions –Precertificate CA Issued

No stipulation.

7.1.2.9.3 Precertificate Poison

The Precertificate contains the Precertificate Poison extension (OID: 1.3.6.1.4.1.11129.2.4.3). This extension has an extnValue OCTET STRING which is exactly the hex-encoded bytes 0500, the encoded representation of the ASN.1 NULL value, as specified in RFC 6962, Section 3.1.

7.1.2.9.4 Precertificate Authority Key Identifier

The Precertificate is directly issued by Issuing CA, and the authorityKeyIdentifier extension of the Precertificate is identical to the Issuing CA certificate's subjecyKeyIdentifier.

7.1.2.10 Common CA Fields

Before issuing a certificate, TrustAsia CA will ensure the certificate contents, including the contents of each field, complies in whole with all of the requirements of at least one Certificate Profile documented in Section 7.1.2.

7.1.2.10.1 CA Certificate Validity

See Section 11.2.

7.1.2.10.2 CA Certificate Naming

See Section 11.2.

7.1.2.10.3 CA Certificate Authority Information Access

See Section 11.2.

7.1.2.10.4 CA Certificate Basic Constraints

See Section 11.2.

7.1.2.10.5 CA Certificate Certificate Policies

See Section 11.2. Certificates have the policyQualifiers field (id-qt-cps: 1.3.6.1.5.5.7.2.1), and the content is the URL for this CPS.

7.1.2.10.6 CA Certificate Extended Key Usage

See Section 11.2.

7.1.2.10.7 CA Certificate Key Usage

See Section 11.2.

7.1.2.10.8 CA Certificate Name Constraints

No stipulation.

7.1.2.11 Common Certificate Fields

Before issuing a certificate, TrustAsia CA will ensure the certificate contents, including the contents of each field, complies in whole with all of the requirements of at least one Certificate Profile documented in Section 7.1.2.

7.1.2.11.1 Authority Key Identifier

See Section 11.3.

7.1.2.11.2 CRL Distribution Points

See Section 11.3.

7.1.2.11.3 Signed Certificate Timestamp List

If present, the Signed Certificate Timestamp List extension contents is an OCTET STRING containing the encoded SignedCertificateTimestampList, as specified in RFC 6962, Section 3.3.
Each SignedCertificateTimestamp included within the SignedCertificateTimestampList is for a PreCert LogEntryType that corresponds to the current certificate.

7.1.2.11.4 Subject Key Identifier

See Section 11.3.

7.1.2.11.5 Other Extensions

See Section 11.3.

7.1.3 Algorithm Object Identifiers

7.1.3.1 SubjectPublicKeyInfo

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

7.1.3.1.1 RSA

TrustAsia CA indicates an RSA key using the rsaEncryption (OID: 1.2.840.113549.1.1.1) algorithm identifier, and it is an explicit NULL. When encoded, the AlgorithmIdentifier for RSA keys is byte-for-byte identical with the following hex-encoded bytes: 300d06092a864886f70d0101010500.

7.1.3.1.2 ECDSA

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

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

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

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

7.1.3.2 Signature AlgorithmIdentifier

All objects signed by TrustAsia CA Private Key conform to these requirements on the use of the AlgorithmIdentifier or AlgorithmIdentifier-derived type in the context of signatures.

In particular, it applies to all of the following objects and fields:

- The signatureAlgorithm field of a Certificate or Precertificate.
- The signature field of a TBSCertificate (for example, as used by either a Certificate or Precertificate).

- The signatureAlgorithm field of a CertificateList
- The signature field of a TBSCertList
- The signatureAlgorithm field of a BasicOCSPResponse.

7.1.3.2.1 RSA

TrustAsia CA uses two RSA signature algorithms and encodings:

Signature Algorithm	OID	Hex-encoded bytes
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:

Signature Algorithm	OID	Hex-encoded bytes
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 details encoding rules that apply to all Certificates issued by a CA. Further restrictions may be specified within Section 7.1.2, but these restrictions do not supersede these requirements.

7.1.4.1 Name Encoding

For every valid Certification Path (as defined by RFC 5280, Section 6), TrustAsia CA applies the following rules:

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

When encoding a Name:

- Each Name contains an RDNSequence.
- Each RelativeDistinguishedName contains exactly one AttributeTypeAndValue.
- Each RelativeDistinguishedName, if present, is encoded within the RDNSequence in the order that it appears in Section 7.1.4.2, see Appendix B.
- Each Name does not contain more than one instance of a given AttributeTypeAndValue across all RelativeDistinguishedNames unless explicitly allowed in these Requirements.

7.1.4.2 Subject Attribute Encoding

The attributes in TLS/CS Certificates issued by TrustAsia CA comply with the requirements for encoding and order in the table below. For other certificates, see Appendix B for the corresponding certificate templates. Subject Distinguished Name Fields (Common Name) contains a single IP address or Fully-Qualified Domain Name that is one of the values contained in the Certificate's subjectAltName extension.

Attribute	OID	Specification	Encoding Requirements	Max Length
countryName	2.5.4.6	RFC 5280	PrintableString	2
stateOrProvinceName	2.5.4.8	RFC 5280	UTF8String or PrintableString	128
localityName	2.5.4.7	RFC 5280	UTF8String or PrintableString	128
organizationName	2.5.4.10	RFC 5280	UTF8String or PrintableString	64
commonName	2.5.4.3	RFC 5280	UTF8String or PrintableString	64

Encoding and order requirements for EV selected attributes are as follows:

Attribute	OID	Specification	Encoding Requirements	Max Length
businessCategory	2.5.4.15	X.520	UTF8String or PrintableString	128
jurisdictionCountry	1.3.6.1.4.1.311.60.2.1.3	EVG	PrintableString	2
jurisdictionStateOrProvince	1.3.6.1.4.1.311.60.2.1.2	EVG	UTF8String or PrintableString	128
serialNumber	2.5.4.5	RFC 5280	PrintableString	64

7.1.4.3 Subscriber Certificate Common Name Attribute

Common Name contains one entry that is one of the values contained in the Certificate's subjectAltName extension. The value of the field is encoded as follows:

- If the value is an IPv4 address, then the value is encoded as an IPv4Address as specified in RFC 3986, Section 3.2.2.
- If the value is an IPv6 address, then the value is encoded in the text representation specified in RFC 5952, Section 4.
- If the value is a Fully-Qualified Domain Name or Wildcard Domain Name, then the value is encoded as a character-for-character copy of the dNSName entry value from the subjectAltName extension. Specifically, all Domain Labels of the Fully-Qualified Domain Name or FQDN portion of the Wildcard Domain Name are encoded as LDH Labels, and for P-Labels, their Unicode representation will not be used.

7.1.4.4 Other Subject Attributes

See Section 11.3.

7.1.5 Name Constraints

No stipulation.

7.1.6 Certificate Policy Object Identifier

7.1.6.1 Reserved Certificate Policy Identifiers

See this CP&CPS Section 1.2.

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

No stipulation.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2 CRL Profile

Effective 2024-03-15, TrustAsia CA issues CRL in accordance with the profile specified as the following.

CRL includes all certificates issued by the CA. If issuing partitioned CRLs, the combined scope of those CRLs is equivalent to that of a full and complete CRL. The CA will not issue indirect CRLs.

Field		Presence	Description
tbsCertList			
	version	Must	v2
	signature	Must	
	issuer	Must	Byte-for-byte identical to the subject field of the Issuing CA
	thisUpdate	Must	The issue date of the CRL
	nextUpdate	Must	For CRLs covering Subscriber Certificates, 7 days after the thisUpdate. For CRLs covering Subordinate CA Certificates, 12 months after the thisUpdate.
	revokedCertificate	Not use	
	extensions	Must	See the table below
signature		Must	

7.2.1 Version Number(s)

CRL issued by TrustAsia CA is formatted in accordance with X.509 v2.

7.2.2 CRL and CRL Entry Extensions

Table: CRL Extensions

Extension	Presence	Critical	Description
authorityKeyIdentifier	Must	N	Byte-for-byte identical to the subjectKeyIdentifier field of the Issuing CA
CRLNumber	Must	N	An integer greater than or equal to zero and less than 2^159, and convey a strictly increasing sequence
IssuingDistributionPoint	*	-	See Section 7.2.2.1

Table: revokedCertificates Component

Component	Presence	Description
serialNumber	Must	Byte-for-byte identical to the serialNumber contained in the revoked certificate
revocationDate	Must	Normally, the date and time revocation occurred. If TrustAsia CA has sufficient evidence to determine that the private key of the certificate was compromised prior to the revocation date that is indicated in the RL entry for that certificate, the revocationDate field will be backdated.
crlEntryExtensions	Maybe	See the crlEntryExtensions table below

Table: crlEntryExtensions Component

CRL Entry Extension	Presence	Description
reasonCode	Maybe	See the table below for CRLReasons. If reasonCode value is 0, not present; and this reason code is the default option specified in the Subscriber Agreement. If reasonCode value is other values, the field presents and is not marked critical.

Table: CRLReasons

RFC5280 reasonCode	Value	Description
unspecified	0	Default option
keyCompromise	1	Indicates that it is known that the Subscriber's private key has been compromised. If there is any other reasons occurred except for key compromise, then reasonCode keycompromise will be used.

affiliationChanged	3	Indicates the Subject's name or other Subject identity information in the certificate has changed
Superseded	4	Indicates that the certificate is being replaced because: the Subscriber has requested a new certificate, TrustAsia CA has reasonable evidence that the validation of domain authorization or control for any FQDN or IP address in the certificate should not be relied upon, or the CA has revoked the certificate for compliance reasons such as the certificate does not comply with these Baseline Requirements or CPS.
cessationOfOperation	5	Indicates that the website with the certificate is shut down prior to the expiration of the certificate, or if the Subscriber no longer owns or controls the domain name in the certificate prior to the expiration of the certificate.
certificateHold	6	Not applicable
privilegeWithdrawn	9	Indicates that there has been a subscriber-side infraction that has not resulted in keyCompromise, such as the certificate Subscriber provided misleading information in their certificate request or has not upheld their material obligations under the Subscriber Agreement or Terms of Use.

7.2.2.1 CRL Issuing Distribution Point

This extension will not be used when TrustAsia CA issues a full and complete CRL. When issuing partitioned CRLs, this extension will be used.

7.3 OCSP Profile

The OCSP service is provided by the TrustAsia CA certification system, and the issued OCSP response conforms to RFC6960 standard, which defines a standard request and response information format to confirm the certificate status.
If the certificate in an OCSP response has been revoked, the revocation reason will be included in the revocation information.

7.3.1 Vision Number(s)

OCSP V1 version defined by RFC6960

7.3.2 OCSP Expansions

Consistent with RFC6960

8. Compliance Audit and Other Assessments

TrustAsia CA abides by the following rules at all times:

1. Issue certificates and operate the public key infrastructure in accordance with all applicable laws and jurisdictions.
2. Comply with all the requirements in this CP&CPS
3. Comply with the Audit requirements in this CP&CPS; and
4. Licensed as a CA in Chinese jurisdiction where it operates, by Ministry of Industry and Information Technology.

8.1 Frequency or Circumstances of Assessments

TrustAsia CA conducts the following audits and assessments:

1. TrustAsia CA conducts an annual security vulnerability assessment to assess the system, physical site, operation management and other aspects to reduce the operational risk according to the assessment report.
2. TrustAsia CA conducts an annual operation quality assessment to ensure the reliability, safety and controllability of the operation service.
3. TrustAsia CA conducts an annual internal assurance audit, at least 3% of the certificate samples shall be taken.
4. According to the requirements of BR on CA/Browser Forum, TrustAsia CA carries out BR self-assessment once a year.
5. TrustAsia CA audits the physical control, key management, operation control and assurance implementation once a year to determine whether the actual situation is consistent with the predetermined standards and requirements, and take actions according to the review results.
6. TrustAsia CA conducts an annual operational risk assessment to identify internal and external threats, assess the possibility of threat events and damage caused, and formulate and implement a disposal plan according to the risk assessment results.
7. In addition to internal audit and evaluation, TrustAsia CA also employs an independent audit firm to conduct external audit and evaluation once a year in accordance with WebTrust's audit specifications for CA.

8.2 Identity/Qualification of Assessor

Cross department audit assessment group organized by TrustAsia CA Security Policy Committee performs internal audit of TrustAsia CA.

External auditors which TrustAsia CA hires shall have the following qualifications:

1. Independence from the subject of the audit;
2. Must be an authority which has been licensed and has a good reputation;
3. Understand computer information security system, communication network security requirements, PKI technology, and related standards and operations;
4. Have the expertise and tools to check the system operation and functionality;
5. Have the Qualification for WebTrust audit.

8.3 Assessor's relationship to Assessed Entity

Segregation of duties is required between the TrustAsia CA auditors, and the TrustAsia CA system administrators, business administrators, and business operators.
The external evaluators and TrustAsia CA are independent from each other. There are no any stakes that could affect the objectivity of the assessment between the above two.

8.4 Topics Covered by Assessment

TrustAsia CA's audit contents include:

1. Whether operation procedures and processes are strictly followed.
2. Whether the CP&CPS, business specifications and security requirements are strictly followed when conducting authentication services.
3. Whether all kinds of logs and records are preserved and if there are any problems occurred.
4. If there have any potential security risks.

Third-party audit firms perform assessments and evaluations on TrustAsia CA to be compliant with CA requirements of WebTrust.

8.5 Actions taken as a result of deficiency

For the issues mentioned in the internal audit report of TrustAsia CA, the assessment team will be responsible for supervising related departments' improvements afterwards.
After the evaluation from a third-party audit firm had been completed, TrustAsia CA will carry out rectification according to the evaluation report, and the second audit and evaluation will be taken.

8.6 Communication of Results

TrustAsia CA needs to release the audit report within three months after the end of auditing. If it was delayed more than three months, TrustAsia CA will provide explanation document which was signed by a qualified auditor.
The audit report should satisfy the requirements in Section 8.6 of this CP&CPS, include the following information that was clearly identified.

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

TrustAsia CA will ensure an authoritative English language version of the publicly available audit information will be provided by the qualified auditor and it is publicly available.
The report will be available as a PDF, and is text searchable for all information required. Each SHA-256 fingerprint within the audit report is uppercase letters and does not contain colons, spaces or line feeds. The audit report will be submitted to CCADB within 7 working days.

8.7 Self-Audits

TrustAsia CA will conduct ongoing self-audits and strictly control the service quality by performing internal risk assessment on at least an annual basis and self-censorship sampling on at least a quarterly basis according to international and domesticstandards and the CP&CPS ones. The self-audit will evaluate whether the electronic certification activities from the end of the last review period to the initial period of the current audit period meet the relevant regulations. The sample size shall not be less than 3% of the total number of certificates issued during the period.

9. Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

TrustAsia CA will charge Subscriber certification's fees based on the digital authentication service provided. The price standard depends on the regulations of marketing and management departments.
If the price specified in TrustAsia CA's agreements with Subscribers is different from the one published, the agreement price shall prevail.

9.1.2 Certificate access Fees

During the validity of the certificates, TrustAsia CA does not charge for certificate inquiries. If the Subscriber has special requests, which may charge extra fees, TrustAsia CA will negotiate with the Subscriber for proper charges.

9.1.3 Revocation or Status information access Fees

TrustAsia CA does not charge any fees for the acquirement of Certificate Revocation List (CRL).

9.1.4 Fees for Other Services

If TrustAsia CA provides certificate storage media and related services to Subscribers, the price will be specified in agreements with Subscribers or other entities. Other services fees that TrustAsia CA may or will charge, will inform the Subscribers timely.

9.1.5 Refund Policy

In the event that TrustAsia CA is unable to perform the Subscriber Contract or the usage of Subscriber Certificate is disabled due to TrustAsia CA's fault, TrustAsia CA will refund fees to the Subscriber. If the fault does not lead by TrustAsia CA andthe Subscriber wants to require a refund, the terms of the Subscriber Agreement shall prevail.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

TrustAsia CA maintains Commercial General Liability insurance with a policy limit of at least two million US dollars in coverage and Errors and Omissions/Professional Liability insurance with a policy limit of at least five million US dollars in coverage.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

If TrustAsia CA violates the provisions of this CP&CPS, certificate Subscribers can request let TrustAsia CA to bear the accountability for compensation (except for statutory or contractual exemption). After confirmation, TrustAsia CA will compensate for the entity. Limitations of compensation are as follows:

1. All the compensation obligation of TrustAsia CA shall not exceed the insurance coverage stipulated in Section 9.2.1. The amount of compensation shall not be higher than the compensation maximum amount. TrustAsia CA can reset the compensation maximum amount depends on various situations. The new compensation will inform the Subscribers immediately.
2. TrustAsia CA only bears compensation accountabilities when the certificate is valid.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

For the electronic certification services provided by TrustAsia CA, the following information is treated as confidential information:

1. The undisclosed content in certificates, which is the information that Subscribers submit or agreements they signed when applying certificates.
2. Audit records including local logs, server logs and archive logs information. These records can only be accessed by security auditors and business administrators. Unless for law requirements, this information cannot be released outside the company.

3. Individual and company information preserved by TrustAsia CA and its affiliated RA should be treated as confidential. Unless for law requirements, this information cannot be released to the public.

9.3.2 Information Not Within the scope of Confidential Information

TrustAsia CA treats the following information as non-confidential:

1. Information that has been disclosed in the certificate and CRL issued by TrustAsia CA.
2. Information in certificate policy supported by TrustAsia CA and recognized by CP&CPS.
3. Information that is permitted by TrustAsia CA and only can be used by TrustAsia CA's Subscribers and published at the TrustAsia CA's official website.
4. Other confidentiality of TrustAsia CA's information depends on particular data items and applications.

9.3.3 Responsibility to Protect Confidential Information

TrustAsia CA has the responsibility and obligation to protect the confidential information described in Section 9.3.1.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

TrustAsia CA respects the privacy of certificate Subscriber's personal data and guarantees to fully comply with the relevant national laws and regulations. In the meantime, TrustAsia CA requires all employees to strictly comply with security and confidentiality standards for personal privacy.

9.4.2 Information Treated as Private

TrustAsia CA will consider all personal information which is undisclosed in the relevant certificate or CRL content as private. TrustAsia CA uses appropriate safeguards and reasonable degree of cautious to protect private information.

9.4.3 Information Not Deemed Private

Certificate information held by Subscribers and certificate status information is not considered as privacy information.

9.4.4 Responsibility to Protect Private Information

TrustAsia CA has the responsibility and obligation for proper custody and protection of the certificate applicant's privacy described in Section 9.4.2.

9.4.5 Notice and Consent to Use private Information

TrustAsia CA takes appropriate steps to protect the certificate Subscriber's personal privacy, and takes reliable security measures to protect stored personal privacy

information. TrustAsia CA guarantees not to provide the certificate Subscriber's personal information, except personal information written in the certificate, to unrelated third parties (including companies and individuals) without the permission of certificate Subscribers, unless based on provisions of the law or government.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

TrustAsia CA may need to provide relevant information to law-enforcement officials and administrative-enforcement officials without subscribers' knowledge, in accordance with the administrative regulations, rules, decisions, orders, and etc. due to the law requirements.

9.4.7 Other Information Disclosure Circumstances

If certificate Subscriber requires TrustAsia CA to provide some particular customer support services such as mailing materials. TrustAsia CA may need to send the Subscriber's name, mailing address and other related information to a third-party such as express company.

9.5 Intellectual Property Rights

1. TrustAsia CA reserves and remains full intellectual property rights for all the certificates and software offered by TrustAsia CA.
2. TrustAsia CA holds ownership, the right of name and the right to share the benefits for certificate system software.
3. TrustAsia CA has the right to decide which software system can be used.
4. All the information published at TrustAsia CA's website is TrustAsia CA's property. Without written permission of TrustAsia CA, others cannot repost them for any commercial activities.
5. Certificates and CRLs issued by TrustAsia CA are both the properties controlled by TrustAsia CA.
6. External operation management strategy and specification are TrustAsia CA's properties.
7. The Distinguished Name (DN) used to express the TrustAsia CA's domain entity in the directory and the certificate issued to the terminal in the domain entity are the properties of TrustAsia CA.
8. This CP&CPS adopts Attribution-NoDerivs 4.0 (CC BY-ND 4.0) for permission.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

During the process of providing electronic certification service activities, TrustAsia CA makes following commitments:

1. Comply with the laws and regulations such as the "Electronic Signature Law of the People's Republic of China", accept the guidance of the competent authorities of the industry, and take corresponding legal responsibility for the issued digital certificate.

2. In accordance with the requirements of the "Administrative Measures for Electronic Certification Services", audit the consistency between the registration agency's electronic certification business and CP&CPS.
3. Certificates issued to subscribers by TrustAsia CA must be in line with all substantive requirements of the CP&CPS.
4. Will not issue certificates that mislead a Relying Party about the certificate information verified by the CA.
5. Inform Subscribers the events that will fundamentally affect the validity and reliability of the certificate.
6. Revoke the certificate timely according to this CP&CPS.
7. Verify the applicants' identities according to this CP&CPS.
8. If TrustAsia CA has no affiliated relationship with Subscriber, then the Subscriber and TrustAsia CA can be called legal and enforceable two valid agreement parties. The Subscriber agreement is compliance with requirements (such as BR) that published on CA/Browser Forum. If TrustAsia CA and the Subscriber are the same entity or have affiliated relationship, the application representative acknowledged the terms of use.
9. Maintain a 24x7 publicly-accessible repository with current information regarding the status (valid or revoked) of all unexpired certificates.

After the certificate has issued to the public, TrustAsia CA guarantees that the Subscriber information in the certificate is accurate except the unverified Subscriber information.
TrustAsia CA is not responsible for the assessment of whether a certificate is used within an appropriate scope. Subscriber and relying party shall ensure the certificate is used for appropriate purposes based on Subscriber agreements and relying party agreements.

9.6.2 RA Representations and Warranties

During participation in the process of electronic certification services, registration authority of TrustAsia CA makes following commitments:

1. The registration process provided for Subscribers is compliant with all the substantive requirements of TrustAsia CA's CP&CPS.
2. When generating certificates, TrustAsia CA does not allow the inconsistencies between certificate information and certificate applicant information due to mistakes of registration authority.
3. Registration authority will submit the applications of revocation, update and other services to TrustAsia CA in time according to the provisions of CP&CPS.

9.6.3 Subscriber Representations and Warranties

Once Subscribers accept a certificate issued by TrustAsia CA, the Subscriber is considered to make the following commitments to TrustAsia CA, registration authority and related parties who trust the certificate:

1. Acknowledged and accepted all the terms and conditions of TrustAsia CA "certificate application responsibility" and CP&CPS.
2. The Subscribers can use digital signatures during the period ofthe certificate is valid.
3. All information that Subscriber provides to the registration authority during certificate application process must be reliable, complete and accurate. The Subscriber is willing to take legal responsibility for any false or forged information. If there is an agent, then both the Subscriber and agent shall take joint responsibility. The Subscriber is responsible for notifying TrustAsia CA and its authorized certification services agencies any false statements and omissions made by the agent.
4. Each signature which uses the corresponding private key of public key is generated by Subscribers themselves. When signing their names, Subscribers need to ensure that the private key can only be used and visited by themselves. The certificate must valid, which means it is not expired or revoked.
5. Subscribers need to ensure that they don't engage in business performed by the issuing agency (or similar institutions) unless they have signed agreements with the issuing agency on such matters.
6. Once the certificate is accepted, Subscribers should assume the following responsibilities: always maintain control of their private keys; use trustworthy systems; and take reasonable precautions to prevent the loss, disclosure, alteration, or unauthorized usage of the private keys.
7. Subscribers are prohibited for rejecting any statements, changes, updates and upgrades published by TrustAsia CA, including but not limited to modification of strategies and standards as well as additions and deletions of certificated services.
8. Subscribers only use certificate for the authorized or other lawful purpose within the range specified by this CP&CPS.
9. Subscribers should use secure and reasonable measures to prevent the private key from loss, disclosure, alteration and other events.
10. For the SSL/TLS Server certificates, Subscribers have responsibilities and obligations to ensure that the certificates should be only installed on the servers that are accessible at the subAltName(s) listed in the certificates.
11. Subscribers of code signing certificates shall promptly apply the revocation of their certificates to TrustAsia CA in case of the following situations:
    1) information in the certificate is or will become incorrect or inaccurate;
    2) misuse or damage of the Subscriber's private key associated with the public key included in the certificate;
    3) evidence that such code signing certificates are used to sigh suspicious codes.

9.6.4 Relying party Representations and Warranties

1. Comply with all provisions of this CP&CPS.
2. Ensure that the certificate is used in prescribed scope and duration.
3. Verify certificate's trust chain before trust the certificate.

4. Before trust a certificate, verify whether the certificate is revokedthrough querying CRL or OCSP.
5. The relying party is willing to compensate TrustAsia CA for the losses and accept liabilities for any loss of self or others, due to negligence or other reasons violating the terms of a reasonable inspection.
6. The relying party is prohibited for rejecting any statements, changes, updates and upgrades published by TrustAsia CA, including but not limited to modification of strategies and standards as well as additions and deletions of certificate services.

9.6.5 Representations and Warranties of Other Participants

Other participants engaged in electronic certification activities must promise to comply with all provisions of this CP&CPS.

9.7 Disclaimers of Warranties

Except for the commitments declared in CP&CPS Section 9.6.1, TrustAsia CA does not assume any other forms of guarantee and obligation:

1. Do not guarantee the statements of certificate subscribers, relying party and other participants.
2. Do not make any security guarantees for the software used in electronic certification activities.
3. Do not assume any liability when certificate is used beyond the prescribed purposes.
4. Do not assume any responsibilities for service interruption and customer losses caused by force majeure, such as war, natural disasters, etc.
5. When Subscriber violates the commitments defined in CP&CPS Section 9.6.3. or relying party violates the commitments defined in CP&CPS Section 9.6.4, TrustAsia CA can exempt from liability.
6. When digital certificates have errors, delays, interruptions, inability to issue, or suspension or termination of all or part of certificate services due to technical failures of TrustAsia CA’s equipment or network failures. The reasons of "technical failure" specified in this paragraph include but not limited to: the TrustAsia’s equipment or network failures caused by related companies such as power, telecommunication, communication departments, hacker attack.
7. TrustAsia CA has carefully obeyed the regulations of digital certificate by national laws, but still cause losses.

9.8 Limitations of Liability

If the certificate Subscriber and the relying party specialized in civil activities suffered losses due to electronic certification services provided by TrustAsia CA. TrustAsia CA will assume limited compensation liability no more than the amount stipulated in the CP&CPS Section 9.9.

9.9 Indemnities

9.9.1 Indemnification scope

If TrustAsia CA violated statement in CP&CPS Section 9.6.1, certificate subscribers, relying parties and other entities can request TrustAsia CA to assume compensation liabilities (except for statutory and contractual exemption). The upper limit of legal liability for direct losses:

- In any case, the compensation for each server certificate must not exceed 10 times the purchase price of the certificate market.
- The compensation for each EV certificate per Subscriber or relying party shall be no less than two thousand US dollars.

If the following circumstances occurred, TrustAsia CA will assume limited compensation liability:

1. TrustAsia CA issues certificates to a third-party instead of the Subscriber by mistake, which leads to the losses of the Subscriber or relying party.
2. If Subscriber submits accurate and true information to TrustAsia CA, but TrustAsia CA issues certificates with wrong information and this fault leads to losses of the Subscriber or relying party.
3. After TrustAsia CA knows the fact that Subscriber provides fake registration information or data, TrustAsia CA still issues certificate, which leads to relying party suffering losses.
4. If the private key of the certificate is deciphered, stolen or disclosed due to TrustAsia CA's fault, which leads to the Subscriber or relying party suffering losses.
5. TrustAsia CA fails to revoke certificates in time, which leads to relying party suffering losses.

In addition, TrustAsia CA's compensation scope is as follows:

1. All the compensation obligation of TrustAsia CA shall not exceed the insurance coverage stipulated in Section 9.2.1. The maximum amount of compensation can be reset by TrustAsia CA based on different situations. TrustAsia CA will notify related parties immediately after the reset.
2. For the losses caused by subscribers or relying parties, TrustAsia CA does not assume responsibilities. Subscribers or relying parties themselves should assume their own responsibilities.
3. TrustAsia CA takes the responsibilities only during the validity of the certificate.

9.9.2 Indemnification by Subscribers

If the following situations cause losses to TrustAsia CA or relying parties, subscribers shall assume the compensation liability:

1. When Subscribers were applying for certificates, due to deliberate, negligent or malicious provision of false information, which leads to the losses of TrustAsia CA or third parties.
2. TrustAsia CA and its authorized service agencies or third-party suffer losses due to disclosure and loss of private keys deliberately and by mistake; due to not informing TrustAsia CA and its authorized service agencies or third-party of the leakage and loss of private keys with knowing the facts; or due to handing keys to others inappropriately.
3. Subscribers violate the regulations in this CP&CPS and related operation practices when using certificates as well as using the certificatesoutside the scope of activities which described in the CP&CPS.
4. If the certificate is used for illegal transactions or causes disputes during the period from revocation requests submitted by the subscribers or other entities authorized by TrustAsia CA to this information of certificate revocation published by TrustAsia CA. Meanwhile, TrustAsia CA operates in accordance with requirements of the CP&CPS, subscribers must assume all responsibilities of losses according to this CP&CPS.
5. Unreal, incomplete or inaccurate information provided by Subscribers.
6. Subscribers continue to use the certificates when information in the certificates is changed and do not notify TrustAsia CA and relying parties promptly.
7. The private key is compromised, damaged, stolen, disclosed, etc. due to not taking effective protection measures.
8. Subscribers continue to use the certificate and do not notify TrustAsia CA and relying parties promptly when they were made aware that private keys are lost or at the risk of being compromised.
9. The certificate has expired but is still in use.
10. The Subscriber’s certificate information infringes upon the intellectual property rights of a third-party.
11. Using Certificated beyond specified scope, such as using certificates for illegal and criminal activities.

9.9.3 Indemnification by Relying Parties

If the following circumstances lead to the losses of TrustAsia CA or Subscribers, relying party shall be assumed compensation responsibility:

1. Obligations defined in the CP&CPS and agreements between TrustAsia CA and relying parties are not followed.
2. TrustAsia CA and its authorized service agencies or a third-party suffer losses due to inappropriate reviews against the CP&CPS.
3. Trust certificates in unreasonable circumstances. For example, relying party still trusts the certificate with knowing that the certificate usage is beyond its scope or period or the certificate has or may have been stolen.
4. Relying party does not verify trust chains of the certificates.
5. Relying party does not check whether a certificate is revoked through querying CRL or OCSP.

9.10 Term and Termination

9.10.1 Term

This CP&CPS and any amendments will immediately become effective when it is released on TrustAsia CA's online repository. It will become effective until the new version of CP&CPS released.

9.10.2 Termination

When TrustAsia CA terminates electronic certification services, this CP&CPS is terminated.

9.10.3 Effect of Termination and Survival

After the termination of this CP&CPS, its effect will be terminated at the same time. The legal facts that occur before the date of termination, the provisions of the responsibility of the parties and the exemption of liability in this CP&CPS are still applicable, including, but not limited to, the contents of audit, confidential information, privacy protection, intellectual property, etc. in CP&CPS, as well as limited liability clauses relating to indemnification, are still valid after this CP&CPS is terminated.

When some provisions in CP&CPS, for example, Subscriber agreements, relying party agreements and other agreements become invalid due to some reasons, such as content modifications or conflict with applicable laws, they do not affect the force of law of other provisions in the corresponding document.

9.11 Individual Notices and Communications with Participants

If necessary, when TrustAsia CA needs to revoke the certificate, or detect the Subscriber has used the certificate for illegal activities which violates the Subscriber agreement. TrustAsia CA will notify individual subscribers and relying parties by email or other ways.

9.12 Amendments

9.12.1 Procedure for Amendment

As authorized by TrustAsia CA Security Policy Committee, CP&CPS composition team reviews this CP&CPS at least once a year to ensure that the CP&CPS meets the requirement of national laws, regulations and administration department as well as relevant international standards; to ensure it meets actual needs of certification business operations.

Revisions and updates of the CP&CPS should be initiated by the CP&CPS compliance team and approved by TrustAsia CA Security Policy Committee. The revised CP&CPS shall be officially released after being approved by TrustAsia CA Security Policy Committee.

9.12.2 Notification Mechanism and Period

After approval of the revised CP&CPS, it will be released on TrustAsia CA's official website synchronously. For the modification notified by email, mail, media and other ways, TrustAsia CA shall notify the relevant parties in time, which ensures that the relevant parties have minimum negative influence.

9.12.3 Circumstances under which OID Must Be Changed

The TrustAsia CA is solely responsible for determining whether an amendment to the CP&CPS requires and OID change.

9.12.4 Circumstance under which CPS Must Be Changed

The situations that TrustAsia CA must modify this CP&CPS include: discrepancies between CP&CPS and governing laws, clear requirements of changes or adjustments for TrustAsia CA's certification services initiated by national regulatory departments.

9.13 Dispute Resolution Provisions

If TrustAsia CA, certificate subscribers, relying parties and other entities have disputed in the electronic certification activities, should be solved through amicable negotiation according to the agreement. If coordination fails, these parties should reach out to the legal authorities.

Any prosecutions against TrustAsia CA over any disputes arising from this CP&CPS should be governed by the people's court in the place where TrustAsia CA is registered.

9.14 Governing Law

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

9.15 Compliance with Applicable Law

Regardless of the place of residence for the subscribers, relying parties and other entities or place to use of the TrustAsia CA's certificates, the execution, explanation and procedure should be compliant with laws and regulations of the People's Republic of China and the requirements of the national information security authority. Any disputes involved by TrustAsia CA and its RA in relation to his CP&CPS should also be compliant with laws of the People's Republic of China.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

Complete document structure of TrustAsia CA's CP&CPS includes three parts: titles, table of contents and main contents. Modified alternative content of the table of contents and the main contents will completely replace all previous parts. The previous parts would be displayed in the TrustAsia CA's official website for browsing.

9.16.2 Assignment

TrustAsia CA declares that the rights and obligations of the parties to the accredited entity as detailed in this CP&CPS may not be assigned by any means without the prior written consent of TrustAsia CA.

9.16.3 Severability

In the event of a conflict between the Requirements in this CP&CPS and a law, regulation or government order (hereinafter 'Law') of China mainland, TrustAsia CA will modify any conflicting requirement to the minimum extent necessary to make the requirement valid and legal in the jurisdiction. This applies only to operations or certificate issuances that are subject to that Law. In such event, TrustAsia CA will immediately (and prior to issuing a certificate under the modified requirement) include in Section 9.16.3 of this CP&CPS a detailed reference to the Law, and the specific modification to these Requirements implemented by TrustAsia CA.

TrustAsia CA (prior to issuing a certificate under the modified requirement) will notify the CA/Browser Forum of the relevant information newly added to this CP&CPS by sending a message to questions@cabforum.org and receiving confirmation that it has been posted to the Public Mailing List and is indexed in the Public Mail Archives available at https://cabforum.org/pipermail/public/ (or such other email addresses and links as the Forum may designate), so that the CA/Browser Forum may consider possible revisions to these Requirements accordingly.

Any modification to CA practice enabled under this section will be discontinued if and when the Law no longer applies, or these Requirements are modified to make it possible to comply with both them and the Law simultaneously. An appropriate change in practice, modification to this CP&CPS and a notice to the CA/Browser Forum, as outlined above, will be made by TrustAsia CA within 90 days.

9.16.4Enforcement

TrustAsia CA declares that if an entity such as a certificate Subscriber or relying party fails to implement a provision in this CP&CPS, it is not considered that the entity will not implement that or other provisions in the future.

9.16.5 Force Majeure

If force majeure, such as war, plague, fire, earthquake and natural disaster, results in violation, delay or failure to perform the warranty liability under this CP&CPS, then TrustAsia will not be responsible for such incidents.

9.17 Other Provisions

TrustAsia CA has final interpretation rights to this CP&CPS.

10. Appendix A - Validation Requirements

10.1 Validation items and requirements

TrustAsia CA requires the following items for Subscriber certificate authentication.

Validation items	Validation Requirements
CSR Validation	Validate CSR signature data. Validate CSR public key size. Validate that whether the CSR public key is a weak key or not.
Domain/IP validation	Validate domain control according to CP&CPS Section 3.2.2.4. Validate IP control according to CP&CPS Section 3.2.2.5.
CAA Validation	Validate CAA record according to CP&CPS Section 3.2.2.8.
Mailbox Validation	Validate email address control according to CP&CPS Section 3.2.2.9.
Organizational Validation	Verify that the name of the applicant is legal Verify that the applicant is legally existing and operating Verify the city, province, state and country where the applicant is located and its physical address Verify telephone numbers, fax numbers, email addresses or postal delivery addresses as the verified communication means for the applicant Comply with CP&CPS Section 3.2.2.1, Baseline Requirements and EV Guidelines
Extended Validation	Verify the Jurisdiction of Incorporation or Registration (country, state/province of registration, registration locality, registration number) Verify the name, title and authority of Certificate Approver and Contract Signer 1. Certificate Approver: verify the name and title, and the authority of approving certificate requests 2. Contract Signer: verify the name and title, and the authority of entering into the Subscriber Agreement (and any other relevant contractual obligations) on behalf of the applicant Verify the signature on Subscriber Agreement and Certificate Requests Verify the applicant's ability to engage in the business Identify and verify the applicant's business category 1. Private Organization: Legal Existence, Organization Name, Registration Number, Registered Agent 2. Government Entity: Legal Existence, Entity Name, Registration Number 3. Business Entity: Legal Existence, Organization Name, Registration number, Principal Individual 4. Non-commercial Entity: Legal Existence, Entity Name, Registration Number Face-to-face validation of Principal Individual for Business Entity Comply with CP&CPS 3.2.2.1 and Baseline Requirements and EV Guidelines

Individual Identity Validation	Verify individual identity according to CP&CPS Section 3.2.3.
Certificate Requester Validation	Verify the name and title of the certificate requester, as well as verify that he/she is the applicant's agent. Confirm the relevant information about the applicant and the type of certificate to be applied for by contacting the certificate requester.
High risk validation	Query the internal database for all previously revoked certificates and rejected certificate applications to identify subsequent suspect certificate applications. Identify "high-risk applicants" using the verification methods shown below and take additional precautions reasonably necessary to ensure that such applicants are properly verified. Identify high-risk applications by querying a list of relevant agency names that are often used in phishing scams or otherwise deceptive practices, and automatically flag certificate applications that match the list for further investigation prior to issuance. Use the information identified by the Agency's high-risk criteria to flag suspicious certificate applications. Perform additional validation of any certificate applications flagged as suspicious or high-risk based on documented procedures. Determine if the entity is identified as applying for a code-signing certificate from a high-risk area of concern. Not issue an EV SSL certificate if the applicant, Certificate Requester, Certificate Approver, Contract Signer or the applicant's jurisdiction of incorporation or registration or place of business has: • Is on any government denial list, prohibited persons list, or other list of countries within the CA's operating jurisdiction that prohibit business with the organization or individualor，or • For the registration jurisdiction, the country where the registration authority or business is located, the laws of the CA jurisdiction prohibit doing business with it.
Lawyer Identity Validation	Verify the information related to the lawyer, check the lawyer's practice certificate or check the registration and records of the lawyer’s practice certificate, and confirm the practice status with his or her law firm. Check the authenticity and accuracy of the signed lawyer's letter with the lawyer.

10.2 Subscriber certificates and validation items

Items to be verified for various types of Subscriber certificates.

	DV SSL/ TLS Server	OV SSL/ TLS Server	EV SSL/ TLS Server	Code Signing	EV Code Signing	Document Signing	MV Strict S/MIME	OV Strict S/MIME	IV Multipurpose S/MIME	SV Multipurpose S/MIME
CSR Validation	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Domain/IP validation	Y	Y	Y	N	N	N	N	N	N	N
CAA Validation	Y	Y	Y	N	N	N	N	N	N	N
Email Address Validation	N	N	N	N	N	N	Y	Y	Y	Y

Organizational Validation	N	Y	Y	Y	Y	Y	N	Y	N	Y
Extended Validation	N	N	Y	N	Y	N	N	N	N	N
Individual Identity Validation	N	N	N	N	N	N	N	N	Y	Y
Certificate Requester Validation	N	Y	Y	Y	Y	Y	N	Y	N	Y
High risk validation	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Lawyer Identity Validation [1]	N	O	O	O	O	O	N	O	N	O

Notes：

Y: Perform this validation

N: No need to perform this validation

O: Determine if this validation needs to be performed based on the situation

[1] This validation is required if using a lawyer's letter

11. Appendix B – Certificate Profiles

11.1 Root Certificate Profile

Root Certificate Field		Critical Extension	Contents
Version			v3
Serial Number			Contain at least 64 bits CSPRNG
Issuer			Byte-for-byte match with Subject
TBSCertificate Signature			TrustAsia Global Root CA G1:sha256withRSA TrustAsia Global Root CA G2:sha384withECDSA TrustAsia Global Root CA G3:sha384withRSA TrustAsia Global Root CA G4:sha384withECDSA
Validity: notBefore			The day of certificate generation
Validity: notAfter			25 years
Subject	Common Name (CN)		TrustAsia Global Root CA G1 | G2 | G3 | G4
	Organization(O)		TrustAsia Technologies, Inc.
	Country(C)		CN
Public Key Information			G1 and G3:RSA4096 (OID: 1.2.840.113549.1.1.1) G2 and G4:secp384r1 (OID: 1.3.132.0.34)
Signature Algorithm			Encoded value must be byte-for-byte identical to the tbsCertificate.signature
Extension: authorityKeyIdentifier		Not Critical	Match subjectKeyIdentifier
Extension: subjectKeyIdentifier		Not Critical	160-bit SHA-1 hash of subjectPublicKey per RFC5280
Extension: basicConstraints		Critical	Subject Type= CA Path Length Constraint=None
Extension: keyUsage		Critical	keyCertSign, cRLSign

11.2 Intermediate Certificate Profile

Intermediate Certificate Field		Critical Extension	Contents
Version			v3
Serial Number			Contain at least 64 bits CSPRNG
Issuer			Byte-for-byte match the Subject of Issuing CA
TBSCertificate Signature			G1: sha256withRSA G3: sha384withRSA G2 or G4: sha384withECDSA
Validity: notBefore			The day of certificate generation
Validity: notAfter			No later than the notAfter of the signing certificate
Subject	Common Name (CN)		See Section 1.1.2
	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			Encoded value must be byte-for-byte identical to the tbsCertificate.signature
Extension: subjectKeyIdentifier		Not Critical	160-bit SHA-1 hash of subjectPublicKey per RFC 5280
Extension: authorityKeyIdentifier		Not Critical	Match subjectKeyIdentifier of the signing certificate
Extension: certificatePolicies		Not Critical	• For Intermediate CA that issues Code Signing, the extension is: Policy Identifier=2.23.140.1.4.1 Policy Identifier=1.3.6.1.4.1.44494.2.2.1 • For Intermediate CA that issues EV Code Signing, the extension is: Policy Identifier=2.23.140.1.3 Policy Identifier=1.3.6.1.4.1.44494.2.2.2 • For Intermediate CA that issues other certificates, the extension is: Policy Identifier=Any Policy (2.5.29.32.0)
Extension: basicConstraints		Critical	Subject Type=CA Path Length Constraint=0
Extension: keyUsage		Critical	digitalSignature, keyCertSign, cRLSign
Extension: extKeyUsage		Not Critical	Must exist. • For issuing SSL/TLS types, the extension is: Server Authentication 1.3.6.1.5.5.7.3.1 Client Authentication 1.3.6.1.5.5.7.3.2 • For issuing Code Signing Certificates, the extension is: Code Signing 1.3.6.1.5.5.7.3.3 • For issuing S/MIME Certificates, the extension is: Email Protection 1.3.6.1.5.5.7.3.4 Client Authentication 1.3.6.1.5.5.7.3.2 MS Document Signing 1.3.6.1.4.1.311.10.3.12 • For issuing Document Signing Certificates, the extension is: PDF Signing 1.2.840.113583.1.1.5 MS Document Signing 1.3.6.1.4.1.311.10.3.12 • For issuing Timestamp Certificates, the extension is:

		Time-Stamping 1.3.6.1.5.5.7.3.8
Extension: authorityInfoAccess	Not Critical	ICA AccessMethod=1.3.6.1.5.5.7.48.2 URL=http://ica.wt.trustasia.com/<Issuername>.crt OCSP AccessMethod=1.3.6.1.5.5.7.48.1 URL=http://ocsp.wt.trustasia.com/<Issuername>
Extension: cRLDistributionPoints	Not Critical	CRL HTTP URL=http://crl.wt.trustasia.com/<Issuername>.crl

11.3Subscriber (End-Entity) Certificate Profiles

11.3.1 DV SSL/TLS Server Certificate Profile

Certificate Field		Critical Extension	Contents
Version			v3
Serial Number			Contain at least 64 bits CSPRNG
TBSCertificate Signature			sha256withRSA or sha384withRSA or sha256withECDSA or sha384withECDSA
Issuer			Byte-for-byte match the Subject of Issuing CA
Validity: notBefore			A value within 24 hours of the certificate signing operation
Validity: notAfter			No longer than 397 days
Subject	Common Name (CN)		Must contain in the derived value of subjectAltName
Public Key Information			RSA2048｜3072｜4096 or ECDSA P-256｜P-384
Signature Algorithm			Encoded value must be byte-for-byte identical to the tbsCertificate.signature
Extension: subjectKeyIdentifier		Not Critical	160-bit SHA-1 hash of subjectPublicKey per RFC 5280
Extension: authorityKeyIdentifier		Not Critical	Match subjectKeyIdentifier of the signing certificate
Extension: certificatePolicies		Not Critical	[1] Policy Identifier=2.23.140.1.2.1 [2] Policy Identifier=1.3.6.1.4.1.44494.2.1.3
Extension: basicConstraints		Critical	Subject Type=End Entity Path Length Constraint=None
Extension: subjectAltName		Not Critical	dNSName is allowed. Contain FQDN or wildcard domain name validated under Section 3.2.2.4. The Internal domain name cannot be used.
Extension: keyUsage		Critical	digitalSignature, keyEncipherment (only RSA)
Extension: extKeyUsage		Not Critical	Server Authentication 1.3.6.1.5.5.7.3.1 Client Authentication 1.3.6.1.5.5.7.3.2
Extenstion: Signed Certificate Timestamp List		Not Critical	Optional extension, match LogEntryType in the precertificate
Extension: authorityInfoAccess		Not Critical	ICA AccessMethod=1.3.6.1.5.5.7.48.2 URL=http://ica.wt.trustasia.com/<Issuername>.crt OCSP AccessMethod=1.3.6.1.5.5.7.48.1 URL= http://ocsp.wt.trustasia.com/<Issuername>
Extension: cRLDistributionPoints		Not Critical	CRL HTTP URL= http://crl.wt.trustasia.com/<Issuername>.crl

11.3.2 OV SSL/TLS Server Certificate Profile

Certificate Field		Critical Extension	Contents
Version			v3
Serial Number			Contain at least 64 bits CSPRNG
TBSCertificate Signature			sha256withRSA or sha384withRSA or sha256withECDSA or sha384withECDSA
Issuer			Byte-for-byte match the Subject of Issuing CA
Validity: notBefore			A value within 24 hours of the certificate signing operation
Validity: notAfter			No longer than 397 days
Subject	Country (C)		Country code of the organization registration/business address validated under Section 3.2
	State (ST)		State or province of the organization registration/business address validated under Section 3.2
	Locality (L)		Locality of the organization registration/business address validated under Section 3.2
	Organization (O)		Organization name validated under Section 3.2
	Common Name (CN)		Must contain in the derived value of subjectAltName
Public Key Information			RSA2048｜3072｜4096 or ECDSA P-256｜P-384
Signature Algorithm			Encoded value must be byte-for-byte identical to the tbsCertificate.signature
Extension: subjectKeyIdentifier		Not Critical	160-bit SHA-1 hash of subjectPublicKey per RFC5280
Extension: authorityKeyIdentifier		Not Critical	Match subjectKeyIdentifier of the signing certificate
Extension: certificatePolicies		Not Critical	[1] Policy Identifier=2.23.140.1.2.2 [2] Policy Identifier=1.3.6.1.4.1.44494.2.1.2
Extension: basicConstraints		Critical	Subject Type=End Entity Path Length Constraint=None
Extension: subjectAltName		Not Critical	dNSName or IPAddress type only. When dNSName type, this value shall contain an FQDN or wildcard domain name validated under Section 3.2.2.4, and an internal name cannot be used. When IPAddress type, if the value is an IPv4 address, the value must be encoded to an IPv4Address as specified in RFC 3986 Section 3.2.2; if the value is an IPv6 address, then the value must be encoded in the textual format as specified in RFC 5952 Section 4.
Extension: keyUsage		Critical	digitalSignature, keyEncipherment (only for RSA)
Extension: extKeyUsage		Not Critical	Server Authentication 1.3.6.1.5.5.7.3.1 Client Authentication 1.3.6.1.5.5.7.3.2
Extension: Signed Certificate Timestamp List		Not Critical	Optional extension, match LogEntryType in the precertificate
Extension: authorityInfoAccess		Not Critical	ICA AccessMethod=1.3.6.1.5.5.7.48.2 URL=http://ica.wt.trustasia.com/<Issuername>.crt OCSP AccessMethod=1.3.6.1.5.5.7.48.1 URL= http://ocsp.wt.trustasia.com/<Issuername>
Extension: cRLDistributionPoints		Not Critical	CRL HTTP URL= http://crl.wt.trustasia.com/<Issuername>.crl

11.3.3 EV SSL/TLS Server Certificate Profile

Certificate Field		Critical Extension	Contents
Version			v3
Serial Number			Contain at least 64 bits CSPRNG
TBSCertificate Signature			sha256withRSA or sha384withRSA or sha256withECDSA or sha384withECDSA
Issuer			Byte-for-byte match the Subject of Issuing CA
Validity: notBefore			A value within 24 hours of the certificate signing operation
Validity: notAfter			No longer than 397 days
Subject	businessCategory		Business category of the organization validated under Section 3.2
	jurisdictionCountryName		Country code of the jurisdiction of organization registration validated under Section 3.2
	jurisdictionStateOrProvinceName		State or province of the jurisdiction of organization registration validated under Section 3.2
	jurisdictionLocalityName		Locality of the jurisdiction of organization registration validated under Section 3.2
	serialNumber		Registration number of the organization validated under Section 3.2
	Country (C)		Country code of the organization registration/business address validated under Section 3.2
	State (ST)		State or province of the organization registration/business address validated under Section 3.2
	Locality (L)		Locality of the organization registration/business address validated under Section 3.2
	Organization (O)		Organization name validated under Section 3.2
	Common Name (CN)		Must contain in the derived value of subjectAltName
Public Key Information			RSA2048｜3072｜4096 or ECDSA P-256｜P-384
Signature Algorithm			Encoded value must be byte-for-byte identical to the tbsCertificate.signature
Extension: subjectKeyIdentifier		Not Critical	160-bit SHA-1 hash of subjectPublicKey per RFC5280
Extension: authorityKeyIdentifier		Not Critical	Match subjectKeyIdentifier of the signing certificate
Extension: certificatePolicies		Not Critical	[1] Policy Identifier=2.23.140.1.1 [2] Policy Identifier=1.3.6.1.4.1.44494.2.1.1
Extension: basicConstraints		Critical	Subject Type=End Entity Path Length Constraint= None
Extension: subjectAltName		Not Critical	Must be dNSName type only. Cannot be wildcard type, cannot use internal domain name or reserved IP
Extension: keyUsage		Critical	digitalSignature, keyEncipherment (only RSA)
Extension: extKeyUsage		Not Critical	Server Authentication 1.3.6.1.5.5.7.3.1 Client Authentication 1.3.6.1.5.5.7.3.2
Extension: Signed Certificate Timestamp List		Not Critical	Optional extension, match LogEntryType in the precertificate
Extension: authorityInfoAccess		Not Critical	ICA AccessMethod=1.3.6.1.5.5.7.48.2 URL=http://ica.wt.trustasia.com/<Issuername>.crt OCSP AccessMethod=1.3.6.1.5.5.7.48.1 URL= http://ocsp.wt.trustasia.com/<Issuername>

Extension: cRLDistributionPoints	Not Critical	CRL HTTP URL= http://crl.wt.trustasia.com/<Issuername>.crl

11.3.4 OV Code Signing Certificate Profile

Certificate Field		Critical Extension	Contents
Version			v3
Serial Number			Contain at least 64 bits CSPRNG
TBSCertificate Signature			sha256withRSA or sha384withRSA or sha256withECDSA or sha384withECDSA
Issuer			Byte-for-byte match the Subject of Issuing CA
Validity: notBefore			A value within 24 hours of the certificate signing operation
Validity: notAfter			No longer than 39 months
Subject	Country(C)		Country code of the organization registration/business address validated under Section 3.2
	State (ST)		State or province of the organization registration/business address validated under Section 3.2
	Locality (L)		Locality of the organization registration/business address validated under Section 3.2
	Organization (O)		Organization name validated under Section 3.2
	Common Name (CN)		Legal name validated under Section 3.2
Public Key Information			RSA 3072｜4096 or ECDSA P-256｜P-384
Signature Algorithm			Encoded value must be byte-for-byte identical to the tbsCertificate.signature
Extension: subjectKeyIdentifier		Not Critical	160-bit SHA-1 hash of subjectPublicKey per RFC5280
Extension: authorityKeyIdentifier		Not Critical	Match subjectKeyIdentifier of the signing certificate
Extension: certificatePolicies		Not Critical	[1] Policy Identifier= 2.23.140.1.4.1 [2] Policy Identifier=1.3.6.1.4.1.44494.2.2.1
Extension: basicConstraints		Critical	Subject Type=End Entity Path Length Constraint=None
Extension: keyUsage		Critical	digitalSignature
Extension: extkeyUsage		Not Critical	Code Signing 1.3.6.1.5.5.7.3.3
Extension: authorityInfoAccess		Not Critical	ICA AccessMethod=1.3.6.1.5.5.7.48.2 URL=http://ica.wt.trustasia.com/<Issuername>.crt OCSP AccessMethod=1.3.6.1.5.5.7.48.1 URL= http://ocsp.wt.trustasia.com/<Issuername>
Extension: cRLDistributionPoints		Not Critical	CRL HTTP URL= http://crl.wt.trustasia.com/<Issuername>.crl

11.3.5 EV Code Signing Certificate Profile

Certificate Field		Critical Extension	Contents
Version			v3
Serial Number			Contain at least 64 bits CSPRNG
TBSCertificate Signature			sha256withRSA or sha384withRSA or sha256withECDSA or sha384withECDSA
Issuer			Byte-for-byte match the Subject of Issuing CA
Validity: notBefore			A value within 24 hours of the certificate signing operation
Validity: notAfter			No longer than 39 months
Subject	businessCategory		Business category of the organization validated under Section 3.2
	jurisdictionCountryName		Country code of the jurisdiction of organization registration validated under Section 3.2
	jurisdictionStateOrProvinceName		State or province of the jurisdiction of organization registration validated under Section 3.2
	jurisdictionLocalityName		Locality of the jurisdiction of organization registration validated under Section 3.2
	serialNumber		Registration number of the organization validated under Section 3.2
	Country(C)		Country code of the organization registration/business address validated under Section 3.2
	State (ST)		State or province of the organization registration/business address validated under Section 3.2
	Locality (L)		Locality of the organization registration/business address validated under Section 3.2
	Organization (O)		Organization name validated under Section 3.2
	Common Name (CN)		Legal name validated under Section 3.2
Public Key Information			RSA 3072｜4096 or ECDSA P-256｜P-384
Signature Algorithm			Encoded value must be byte-for-byte identical to the tbsCertificate.signature
Extension: subjectKeyIdentifier		Not Critical	160-bit SHA-1 hash of subjectPublicKey per RFC5280
Extension: authorityKeyIdentifier		Not Critical	Match subjectKeyIdentifier of the signing certificate
Extension: certificatePolicies		Not Critical	[1] Policy Identifier=2.23.140.1.3 [2] Policy Identifier=1.3.6.1.4.1.44494.2.2.2
Extension: basicConstraints		Critical	Subject Type=End Entity Path Length Constraint= None
Extension: keyUsage		Critical	digitalSignature
Extension: extKeyUsage		Not Critical	Code Signing 1.3.6.1.5.5.7.3.3
Extension: authorityInfoAccess		Not Critical	ICA AccessMethod=1.3.6.1.5.5.7.48.2 URL=http://ica.wt.trustasia.com/<Issuername>.crt OCSP AccessMethod=1.3.6.1.5.5.7.48.1 URL= http://ocsp.wt.trustasia.com/<Issuername>
Extension: cRLDistributionPoints		Not Critical	CRL HTTP URL= http://crl.wt.trustasia.com/<Issuername>.crl

11.3.6 S/MIME Basic Certificate Profile

Certificate Field		Critical Extension	Contents
Version			v3
Serial Number			Contain at least 64 bits CSPRNG
TBSCertificate Signature			sha256withRSA or sha384withRSA or sha256withECDSA or sha384withECDSA
Issuer			Byte-for-byte match the Subject of Issuing CA
Validity: notBefore			A value within 24 hours of the certificate signing operation
Validity: notAfter			No longer than 825 days
Subject	Common Name (CN)		rfc822Name email address validated under Section 3.2
	Email (E)		
Public Key Information			RSA2048｜3072｜4096 or ECDSA P-256｜P-384
Signature Algorithm			Encoded value must be byte-for-byte identical to the tbsCertificate.signature
Extension: subjectKeyIdentifier		Not Critical	160-bit SHA-1 hash of subjectPublicKey per RFC5280
Extension: authorityKeyIdentifier		Not Critical	Match subjectKeyIdentifier of the signing certificate
Extension: certificatePolicies		Not Critical	[1] Policy Identifier=2.23.140.1.5.1.3 [2] Policy Identifier=1.3.6.1.4.1.44494.2.4.3.3
Extension: basicConstraints		Critical	Subject Type=End Entity Path Length Constraint=None
Extension: subjectAltName		Not Critical	Include rfc822Name email address
Extension: keyUsage		Critical	digitalSignature, nonRepudiation, keyEncipherment (Only RSA), keyAgreement (Only ECC)
Extension: extKeyUsage		Not Critical	Email Protection 1.3.6.1.5.5.7.3.4
Extension: authorityInfoAccess		Not Critical	ICA AccessMethod=1.3.6.1.5.5.7.48.2 URL=http://ica.wt.trustasia.com/<Issuername>.crt OCSP AccessMethod=1.3.6.1.5.5.7.48.1 URL= http://ocsp.wt.trustasia.com/<Issuername>
Extension: cRLDistributionPoints		Not Critical	CRL HTTP URL= http://crl.wt.trustasia.com/<Issuername>.crl

11.3.7 S/MIME Individual Certificate Profile

Certificate Field		Critical Extension	Contents
Version			v3
Serial Number			Contain at least 64 bits CSPRNG
TBSCertificate Signature			sha256withRSA or sha384withRSA or sha256withECDSA or sha384withECDSA
Issuer			Byte-for-byte match the Subject of Issuing CA
Validity: notBefore			A value within 24 hours of the certificate signing operation
Validity: notAfter			No longer than 825 days
Subject	Common Name (CN)		Legal name of the Applicant validated under Section 3.2
	givenName		Individual's legal given name validated under Section 3.2
	surname		Individual's legal surname validated under Section 3.2
	Email		rfc822Name email address validated under Section 3.2
	Country (C)		Country code of the Applicant's nationality validated under Section 3.2
Public Key Information			RSA2048｜3072｜4096 or ECDSA P-256｜P-384
Signature Algorithm			Encoded value must be byte-for-byte identical to the tbsCertificate.signature
Extension: subjectKeyIdentifier		Not Critical	160-bit SHA-1 hash of subjectPublicKey per RFC5280
Extension: authorityKeyIdentifier		Not Critical	Match subjectKeyIdentifier of the signing certificate
Extension: certificatePolicies		Not Critical	[1] Policy Identifier=2.23.140.1.5.4.2 [2] Policy Identifier=1.3.6.1.4.1.44494.2.4.6.2
Extension: basicConstraints		Critical	Subject Type=End Entity Path Length Constraint=None
Extension: subjectAltName		Not Critical	Include rfc822Name email address
Extension: keyUsage		Critical	digitalSignature, nonRepudiation, keyEncipherment (Only RSA), keyAgreement (Only ECC)
Extension: extKeyUsage		Not Critical	Email Protection 1.3.6.1.5.5.7.3.4 Client Authentication 1.3.6.1.5.5.7.3.2
Extension: authorityInfoAccess		Not Critical	ICA AccessMethod=1.3.6.1.5.5.7.48.2 URL=http://ica.wt.trustasia.com/<Issuername>.crt OCSP AccessMethod=1.3.6.1.5.5.7.48.1 URL= http://ocsp.wt.trustasia.com/<Issuername>
Extension: cRLDistributionPoints		Not Critical	CRL HTTP URL= http://crl.wt.trustasia.com/<Issuername>.crl

11.3.8 S/MIME Enterprise Certificate Profile

Certificate Field		Critical Extension	Contents
Version			v3
Serial Number			Contain at least 64 bits CSPRNG
TBSCertificate Signature			sha256withRSA or sha384withRSA or sha256withECDSA or sha384withECDSA
Issuer			Byte-for-byte match the Subject of Issuing CA
Validity: notBefore			A value within 24 hours of the certificate signing operation
Validity: notAfter			No longer than 825 days
Subject	Common Name (CN)		Organization name validated under Section 3.2
	Organization (O)		Organization name validated under Section 3.2
	Organization Identifier (OI)		Organization registration number validated under Section 3.2 (Refer to S/MIME Baseline Requirements)
	Email		rfc822Name email address validated under Section 3.2
	Locality (L)		Locality of the organization registration/business address validated under Section 3.2
	State (ST)		State or province of the organization registration/business address validated under Section 3.2
	Country (C)		Country code of the organization registration/business address validated under Section 3.2
Public Key Information			RSA2048｜3072｜4096 or ECDSA P-256｜P-384
Signature Algorithm			Encoded value must be byte-for-byte identical to the tbsCertificate.signature
Extension: subjectKeyIdentifier		Not Critical	160-bit SHA-1 hash of subjectPublicKey per RFC5280
Extension: authorityKeyIdentifier		Not Critical	Match subjectKeyIdentifier of the signing certificate
Extension: certificatePolicies		Not Critical	[1] Policy Identifier=2.23.140.1.5.2.3 [2] Policy Identifier=1.3.6.1.4.1.44494.2.4.4.3
Extension: basicConstraints		Critical	Subject Type=End Entity Path Length Constraint=None
Extension: subjectAltName		Not Critical	Include rfc822Name email address
Extension: keyUsage		Critical	digitalSignature, nonRepudiation, keyEncipherment (Only RSA), keyAgreement (Only ECC)
Extension: extKeyUsage		Not Critical	Email Protection 1.3.6.1.5.5.7.3.4
Extension: authorityInfoAccess		Not Critical	ICA AccessMethod=1.3.6.1.5.5.7.48.2 URL=http://ica.wt.trustasia.com/<Issuername>.crt OCSP AccessMethod=1.3.6.1.5.5.7.48.1 URL= http://ocsp.wt.trustasia.com/<Issuername>
Extension: cRLDistributionPoints		Not Critical	CRL HTTP URL= http://crl.wt.trustasia.com/<Issuername>.crl

11.3.9 S/MIME Enterprise Pro Certificate Profile

Certificate Field		Critical Extension	Contents
Version			v3
Serial Number			Contain at least 64 bits CSPRNG
TBSCertificate			sha256withRSA or sha384withRSA or sha256withECDSA or sha384withECDSA
Issuer			Byte-for-byte match the Subject of Issuing CA
Validity: notBefore			A value within 24 hours of the certificate signing operation
Validity: notAfter			No longer than 825 days
Subject	Common Name (CN)		Applicant's name or pseudonym (2.5.4.65) validated under Section 3.2, choose between the two
	Organization (O)		Organization name validated under Section 3.2
	Organization Identifier (OI)		Organization registration number validated under Section 3.2 (Refer to S/MIME Baseline Requirements)
	givenName		Individual's legal given name validated under Section 3.2
	surname		Individual's legal surname validated under Section 3.2
	pseudonym		Applicant's personal pseudonym validated under Section 3.2. This field must not be present if the Applicant's name is present in the Certificate DN.
	Email		rfc822Name email address validated under Section 3.2
	Locality (L)		Locality of the organization registration/business address validated under Section 3.2
	State (ST)		State or province of the organization registration/business address validated under Section 3.2
	Country (C)		Country code of the organization registration/business address validated under Section 3.2
Public Key Information			RSA2048｜3072｜4096 or ECDSA P-256｜P-384
Signature Algorithm			Encoded value must be byte-for-byte identical to the tbsCertificate.signature
Extension: subjectKeyIdentifier		Not Critical	160-bit SHA-1 hash of subjectPublicKey per RFC5280
Extension: authorityKeyIdentifier		Not Critical	Match subjectKeyIdentifier of the signing certificate
Extension: certificatePolicies		Not Critical	[1] Policy Identifier=2.23.140.1.5.3.2 [2] Policy Identifier= 1.3.6.1.4.1.44494.2.4.5.2
Extension: basicConstraints		Critical	Subject Type=End Entity Path Length Constraint=None
Extension: subjectAltName		Not Critical	Must include rfc822Name email address
Extension: keyUsage		Critical	digitalSignature, nonRepudiation, keyEncipherment (Only RSA), keyAgreement (Only ECC)
Extension: extKeyUsage		Not Critical	Email Protection 1.3.6.1.5.5.7.3.4 Client Authentication 1.3.6.1.5.5.7.3.2
Extension: authorityInfoAccess		Not Critical	ICA AccessMethod=1.3.6.1.5.5.7.48.2 URL=http://ica.wt.trustasia.com/<Issuername>.crt OCSP AccessMethod=1.3.6.1.5.5.7.48.1 URL= http://ocsp.wt.trustasia.com/<Issuername>
Extension: cRLDistributionPoints		Not Critical	CRL HTTP URL= http://crl.wt.trustasia.com/<Issuername>.crl

11.3.10 Document Signing Certificate Profile

Certificate Field		Critical Extension	Contents
Version			v3
Serial Number			Contain at least 64 bits CSPRNG
TBSCertificate Signature			sha256withRSA or sha384withRSA or sha256withECDSA or sha384withECDSA
Issuer			Byte-for-byte match the Subject of Issuing CA
Validity: notBefore			A value within 24 hours of the certificate signing operation
Validity: notAfter			No longer than 39 months
Subject	Common Name (CN)		Applicant name validated under Section 3.2 Organization name validated under Section 3.2
	serialNumber		Applicant's encrypted identity information, if any
	givenName		Individual's legal given name validated under Section 3.2 (Individual-validated and Organization-validated containing individual information)
	surname		Individual's legal surname validated under Section 3.2 (Individual-validated and Organization-validated containing individual information)
	Organization (O)		Organization name validated under Section 3.2 (Organization-validated and Organization-validated containing individual information)
	Organization Unit (OU)		Subsidiary bodies/department names validated under Section 3.2 (Organization-validated and Organization-validated containing individual information)
	Locality (L)		Locality of the organization registration/business address validated under Section 3.2 (Organization-validated and Organization-validated containing individual information)
	State (ST)		State or province of the organization registration/business address validated under Section 3.2 (Organization-validated and Organization-validated containing individual information)
	Country (C)		Country code of the organization registration/business address and nationality (Individual-validated) validated under Section 3.2
Public Key Information			RSA2048｜3072｜4096 or ECDSA P-256｜P-384
Signature Algorithm			Encoded value must be byte-for-byte identical to the tbsCertificate.signature
Extension: subjectKeyIdentfier		Not Critical	160-bit SHA-1 hash of subjectPublicKey per RFC5280
Extension: authorityKeyIdentifier		Not Critical	Match subjectKeyIdentifier of the signing certificate
Extension: certificatePolicies		Not Critical	Policy Identifier=1.3.6.1.4.1.44494.2.3.1
Extension: basicConstraints		Critical	Subject Type=End Entity Path Length Constraint=None
Extension: keyUsage		Critical	digitalSignature, nonRepudiation
Extension: extKeyUsage		Not Critical	PDF Signing 1.2.840.113583.1.1.5 MS Document Signing 1.3.6.1.4.1.311.10.3.12

Extension: authorityInfoAccess	Not Critical	ICA AccessMethod=1.3.6.1.5.5.7.48.2 URL=http://ica.wt.trustasia.com/<Issuername>.crt OCSP AccessMethod=1.3.6.1.5.5.7.48.1 URL= http://ocsp.wt.trustasia.com/<Issuername>
Extension: cRLDistributionPoints	Not Critical	CRL HTTP URL= http://crl.wt.trustasia.com/<Issuername>.crl
Extension: timeStamping	Not Critical	TimeStamping URL RSA: http://tsa.wt.trustasia.com/aatl-rsag3/<TSCert's SerialNumber> TimeStamping URL ECC： http://tsa.wt.trustasia.com/aatl-eccg4/<TSCert's SerialNumber>
Extension: ArchiveRevInfo	Not Critical	This extension is supported.

11.3.11 OCSP Responder Certificate Profile

Certificate Field		Critical Extension	Contents
Version			v3
Serial Number			Contain at least 64 bits CSPRNG
TBSCertificate Signature			sha384withRSA or sha384withECDSA
Issuer			Byte-for-byte match the Subject of Issuing CA
Validity: notBefore			A value within 24 hours of the certificate signing operation
Validity: notAfter			No longer than 398 days
Subject	Common Name (CN)		<CA Common Name>-OCSP Responder
	Organization (O)		TrustAsia Technologies, lnc.
	Country (C)		CN
Public Key Information			RSA 2048｜3072｜4096 or ECDSA P-256｜P-384
Signature Algorithm			Encoded value must be byte-for-byte identical to the tbsCertificate.signature
Extension: subjectKeyIdentfier		Not Critical	160-bit SHA-1 hash of subjectPublicKey per RFC5280
Extension: authorityKeyIdentifier		Not Critical	Match subjectKeyIdentifier of the signing certificate
Extension: basicConstraints		Critical	Subject Type=End Entity Path Length Constraint=None
Extension: keyUsage		Critical	digitalSignature
Extension: extKeyUsage		Not Critical	OCSP Signing (1.3.6.1.5.5.7.3.9)
Extension: id-pkix-ocsp-nocheck (1.3.6.1.5.5.7.48.1.5)		Not Critical	0x0500