TrustAsia Certificate Policy and Certification Practice Statement for Global Trusted Service （CP&CPS）V1.3

May 18, 2021

TrustAsia Technologies, Inc.

Revision History

Version	Update content	Time	Editor	Approver	Comments
V1.1	Issue 1st version	2020/8/25	CPS compilation team	Security Policy Committee	
V1.2	• Update 2.2.2 to indicate that the serial number of the CRL is increasing. • Update the number for level 2.4 and 2.5. • Update 5.1.1, the implementation standard for the construction of the CA computer room. • Update 6.2.10, stating that the CA must not damage the CA private key restriction. • Update 9.14 to supplement applicable local laws and regulations	2020.10.23	CPS compilation team	Security Policy Committee	
• V1.3	• Full formatting adjustment to fully correspond to CA/B catalog • Update 1.1.1 Company introduction • Update 1.1.2 Certificate hierarchy • Update 1.2 OID Identification • Delete 2.5 high risk Repositories • Update 3.1.6 Recognition, Authentication, and Role of Trademarks • Update 3.2 Initial Identity Validation • Update 4.9.1.1 Certificate Revocation • Update 5.7.3 Recovery Procedures after Key Compromise • Add 6.1.1.2 RA Key Paire generation • Update 6.1.5 Key Sizes • Update 7.1.2 Certificate Content and Extensions; Application of RFC 5280 • Update 7.1.3 Algorithm Object Identifier • Replace original 8.7 Other Evaluation with new 8.7 Self-Evaluation • Add 10 Appendix A - Validation Requirements	2021.5.18	CPS compilation team	Security Policy Committee	

CONTENT

1. INTRODUCTION 1

1.1 OVERVIEW 1

1.1.1 Company Introduction 1

1.1.2 Service system/hierarchy 1

1.1.3 Certificate Policy(CP) and Certification Practice Statement(CPS) 4

1.2 DOCUMENT NAME AND IDENTFICATION 5

1.3 PKI PARTICIPANTS 5

1.3.1 Certification Authority 5

1.3.2 Registration Authority 6

1.3.3 Subscribers 6

1.3.4 Relying Parties 6

1.3.5 Other Participants 6

1.4 CERTIFICATE USAGE 6

1.4.1 Appropriate Certificate Usage 6

1.4.2 Prohibited Certificate Uses 7

1.4.3 Formal and test certificates 7

1.5 POLICY ADMINISTRATION 8

1.5.1 Organization Administering the Document 8

1.5.2 Contact Person 8

1.5.3 Person Determining CPS suitability for the policy 8

1.5.4 CPS Approval procedure 8

1.6 DEFINITIONS AND ACRONYMS 9

1.6.1 Definitions 9

1.6.2 Acronyms 10

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES 11

2.1 REPOSITORIES 11

2.2 PUBLICATION OF INFORMATION 11

2.2.1 Publication of Repositories 11

2.2.2 Publication of CRL 12

2.2.3 Publication of OCSP 12

2.3 TIME OR FREQUENCY OF PUBLICATION 12

2.3.1 Time or Frequency of Publication of CPS 12

2.3.2 Time or Frequency of Publication of CRL 12

2.3.3 Time or Frequency of Publication of OCSP 12

2.4 ACCESS CONTROLS ON REPOSITORIES 12

3. IDENTIFICATION AND AUTHENTICATION 13

3.1 NAMING 13

3.1.1 Type of Names 13

3.1.2 Need for Names to be Meaningful 14

3.1.3 Anonymity or pseudonymity of Subscribers 14

3.1.4 Rules for Interpreting Various Name Forms 14

3.1.5 Uniqueness of Names 14

3.1.6 Recognition, Authentication, and Role of Trademarks 15

3.2 INITIAL IDENTITY VALIDATION 15

3.2.1 Method to Prove Possession of Private Key *15*
3.2.2 Authentication of Organization and Domain Identity *15*
3.2.3 Authentication of Individual Identity *19*
3.2.4 Non-Verified Subscriber Information *20*
3.2.5 Validation of Authority *20*
3.2.6 Criteria for Interoperation or Certification *20*
3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS 20
3.3.1 Identification and Authentication got Routine Re-key *21*
3.3.2 Identification and Authentication for Re-key After Revocation *22*
3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST 22
3.5 IDENTIFICATION OF AUTHORIZED SERVICE INSTITUTIONS 22
4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 22
4.1 CERTIFICATE APPLICATION 22
4.1.1 Who Can Submit a Certificate Application *22*
4.1.2 Enrollment Process and Responsibilities *22*
4.2 CERTIFICATE APPLICATION PROCESSING 23
4.2.1 Performing Identification and Authentication Functions *23*
4.2.2 Approval or Rejection of Certificate Applications *24*
4.2.3 Time to Process Certificate Applications *24*
4.3 CERTIFICATE ISSUANCE 25
4.3.1 CA Actions during Certificate issuance *25*
4.3.2 Notification of CertifIicate Issuance *25*
4.4 CERTIFICATE ACCEPTANCE 25
4.4.1 Conduct Constituting Certificate Acceptance *25*
4.4.2 Publication of the certificate by the CA *26*
4.4.3 Notification of Certificate Issuance by the CA to Other Entities *26*
4.5 KEY PAIR AND CERTIFICATE USAGE 26
4.5.1 Subscriber Private Key and Certificate Usage *26*
4.5.2 Relying Party Public Key and Certificate Usage *26*
4.6 CERTIFICATE RENEWAL 27
4.6.1 Circumstance for Certificate Renewal *27*
4.6.2 Who May Request Renewal *27*
4.6.3 Processing Certificate Renewal Requests *28*
4.6.4 Notification of New Certificate Issuance to Subscriber *28*
4.6.5 Conduct Constituting Acceptance of a Renewal Certificate *28*
4.6.6 Publication of the Renewal Certificate by the CA *28*
4.6.7 Notification of Certificate Issuance by the CA to Other Entities *28*
4.7 CERTIFICATE RE-KEY 28
4.7.1 Circumstances for Certificate Re-key *28*
4.7.2 Who May Request Certification of a New public key *29*
4.7.3 Processing Certificate Re-keying Requests *29*
4.7.4 Notification of new certificate issuance to subscriber *29*
4.7.5 Conduct Constituting Acceptance of a Re-keyed certificate *29*
4.7.6 Publication of the Re-keyed certificate by the CA *29*
4.7.7 Notification of Certificate Issuance by the CA to Other Entities *29*

4.8 CERTIFICATE MODIFICATION 29
4.8.1 Circumstances for Certificate Modification *29*
4.8.2 Who May Request Certificate Modification *29*
4.8.3 Processing Certificate Modification Requests *29*
4.8.4 Notification of New Certificate Issuance to Subscriber *30*
4.8.5 Conduct Constituting Acceptance of Modified Certificate *30*
4.8.6 Publication of the Modified Certificate by the CA *30*
4.8.7 Notification of Certificate Issuance by the CA to Other Entities *30*
4.9 CERTIFICATE REVOCATION AND SUSPENSION 30
4.9.1 Circumstances for Revocation *30*
4.9.2 Who Can Request Revocation *32*
4.9.3 Procedure for Revocation Request *33*
4.9.4 Revocation Request Grace Period *33*
4.9.5 Time Within Which CA Must Process the Revocation Request *33*
4.9.6 Revocation Checking Requirement for Relying Parties *34*
4.9.7 CRL Issuance Frequency *34*
4.9.8 Maximum Latency for CRLs *34*
4.9.9 On-line Revocation/Status Checking Availability *34*
4.9.10 On-line Revocation Checking Requirements *34*
4.9.11 Other Forms of Revocation Advertisements Available *34*
4.9.12 Special Requirements related to Key Compromise *35*
4.9.13 Circumstances for Suspension *35*
4.9.14 Who Can Request Suspension *35*
4.9.15 Procedure for Suspension Request *35*
4.9.16 Limits on Suspension Period *35*
4.10 CERTIFICATE STATUS SERVICES 35
4.10.1 Operational Characteristics *35*
4.10.2 Service Availability *35*
4.10.3 Operational Features *35*
4.11 END OF SUBSCRIPTION 36
4.12 KEY ESCROW AND RECOVERY 36
4.12.1 Key Escrow and Recovery Policy and Practices *36*
4.12.2 Session Key Encapsulation and Recovery Policy and Practices *36*
5. MANAGEMENT, AND OPERATIONAL, AND PHYSICAL CONTROLS 36
5.1 PHYSICAL SECURITY CONTROLS 36
5.1.1 Site Location and Construction *36*
5.1.2 Physical Access *37*
5.1.3 Power and Air Conditioning *37*
5.1.4 Water exposures *38*
5.1.5 Fire Prevention and Protection *38*
5.1.6 Media Storage *38*
5.1.7 Waste Disposal *38*
5.1.8 Off-site Backup *38*
5.2 PROCEDURAL CONTROLS 38
5.2.1 Trusted Roles *38*

5.2.2 Number of Individuals Required per Task *39*
5.2.3 Identification and Authentication for Trusted Roles *39*
5.2.4 Roles Requiring Separation of Duties *39*
5.3 PERSONNEL CONTROLS 40
5.3.1 Qualifications, Experience, and Clearance Requirements *40*
5.3.2 Background Check Procedures *40*
5.3.3 Training Requirements and Procedures *41*
5.3.4 Retraining Frequency and Requirements *42*
5.3.5 Job Rotation Frequency and Sequence *42*
5.3.6 Sanctions for Unauthorized Actions *42*
5.3.7 Independent Contractor Controls *42*
5.3.8 Documentation Supplied to Personnel *42*
5.4 AUDIT LOGGING PROCEDURES 42
5.4.1 Types of Events Recorded *42*
5.4.2 Frequency for Processing and Archiving Audit Logs *43*
5.4.3 Retention Period for Audit Logs *44*
5.4.4 Protection of Audit Log *44*
5.4.5 Audit Log Backup Procedures *44*
5.4.6 Audit Log Accumulation System *44*
5.4.7 Notification to Event-Causing Subject *44*
5.4.8 Vulnerability Assessments *44*
5.5 RECORDS ARCHIVAL 45
5.5.1 Types of Records Archived *45*
5.5.2 Retention Period for Archive *45*
5.5.3 Protection of Archive *45*
5.5.4 Archive Backup Procedures *45*
5.5.5 Requirements for Time-stamping of Records *45*
5.5.6 Archive Collection System *46*
5.5.7 Procedures to Obtain and Verify Archive Information *46*
5.6 KEY CHANGEOVER 46
5.7 COMPROMISE AND DISASTER RECOVERY 46
5.7.1 Incident and Compromise Handling Procedures *46*
5.7.2 Recovery Procedures if Computing resources, software, and/or data are corrupted *47*
5.7.3 Recovery Procedures after Key Compromise *47*
5.7.4 Business Continuity Capabilities after a Disaster *47*
5.8 CA OR RA TERMINATION 47
6. TECHNICAL SECURITY CONTROLS 48
6.1 KEY PAIR GENERATION AND INSTALLATION 48
6.1.1 Key Pair Generation *48*
6.1.2 Private Key Delivery to Subscriber *48*
6.1.3 Public Key Delivery to Certificate Issuer *48*
6.1.4 CA Public Key Delivery to Relying Parties *48*
6.1.5 Key Sizes *49*
6.1.6 Public Key Parameters Generation and Quality Checking *49*
6.1.7 Key Usage Purposes *49*

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS 50
6.2.1 Cryptographic Module Standards and Controls *50*
6.2.2 Private Key (n out of m) Multi-person Control *50*
6.2.3 Private Key Escrow *50*
6.2.4 Private Key Backup *50*
6.2.5 Private Key Archival *50*
6.2.6 Private Key Transfer into or from a Cryptographic Module *50*
6.2.7 Private Key Storage on Cryptographic Module *50*
6.2.8 Activating Private Keys *51*
6.2.9 Deactivating Private Keys *51*
6.2.10 Destroying Private Keys *51*
6.2.11 Cryptographic Module Capabilities *51*
6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT 51
6.3.1 Public Key Archival *51*
6.3.2 Certificate Operational Periods and Key Pair Usage Periods *51*
6.4 ACTIVATION DATA 52
6.4.1 Activation Data Generation and Installation *52*
6.4.2 Activation Data Protection *52*
6.4.3 Other Aspects of Activation Data *53*
6.5 COMPUTER SECURITY CONTROLS 53
6.5.1 Specific Computer Security Technical Requirements *53*
6.5.2 Computer Security Rating *54*
6.6 LIFE CYCLE TECHNICAL CONTROLS 54
6.6.1 System Development Controls *54*
6.6.2 Security Management Controls *54*
6.6.3 Life Cycle Security Controls *54*
6.7 NETWORK SECURITY CONTROLS 55
6.8 TIME-STAMPING 55
7. CERTIFICATE, CRL, AND OCSP PROFILES 55
7.1 CERTIFICATE PROFILE 55
7.1.1 Version Number(s) *55*
7.1.2 Certificate Content and Extensions; Application of RFC 5280 ..... *55*
7.1.3 Algorithm Object Identifiers *58*
7.1.4 Name Forms *59*
7.1.5 Name Constraints *59*
7.1.6 Certificate Policy Object Identifier *59*
7.1.7 Usage of Policy Constraints Extension *59*
7.1.8 Policy Qualifiers Syntax and Semantics *59*
7.1.9 Processing Semantics for the Critical Certificate Policies Extension *59*
7.2 CRL PROFILE 59
7.2.1 Version Number(s) *59*
7.2.2 CRL and CRL Entry Extensions *59*
7.3 OCSP PROFILE 60
7.3.1 Vision Number(s) *60*
7.3.2 OCSP Expansions *60*

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS 60
8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENTS 60
8.2 IDENTITY/QUALIFICATION OF ASSESSOR 60
8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY 61
8.4 TOPICS COVERED BY ASSESSMENT 61
8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY 61
8.6 COMMUNICATION OF RESULTS 61
8.7 SELF-AUDITS 61
9. OTHER BUSINESS AND LEGAL MATTERS 62
9.1 FEES 62
9.1.1 Certificate Issuance or Renewal Fees 62
9.1.2 Certificate access Fees 62
9.1.3 Revocation or Status information access Fees 62
9.1.4 Fees for Other Services 62
9.1.5 Refund Policy 62
9.2 FINANCIAL RESPONSIBILITY 62
9.2.1 Insurance Coverage 62
9.2.2 Other Assets 63
9.2.3 Insurance or Warranty Coverage for End-Entities 63
9.3 CONFIDENTIALITY OF BUSINESS INFORMATION 63
9.3.1 Scope of Confidential Information 63
9.3.2 Information Not Within the Scope of Confidential Information 63
9.3.3 Responsibility to Protect Confidential Information 63
9.4 PRIVACY OF PERSONAL INFORMATION 64
9.4.1 Privacy Plan 64
9.4.2 Information Treated as Private 64
9.4.3 Information Not Deemed Private 64
9.4.4 Responsibility to Protect Private Information 64
9.4.5 Notice and Consent to Use private Information 64
9.4.6 Disclosure Pursuant to Judicial or Administrative Process 64
9.4.7 Other Information Disclosure Circumstances 64
9.5 INTELLECTUAL PROPERTY RIGHTS 65
9.6 REPRESENTATIONS AND WARRANTIES 65
9.6.1 CA Representations and Warranties 65
9.6.2 RA Representations and Warranties 66
9.6.3 Subscriber Representations and Warranties 66
9.6.4 Relying party Representations and Warranties 67
9.6.5 Representations and Warranties of Other Participants 67
9.7 DISCLAIMERS OF WARRANTIES 67
9.8 LIMITATIONS OF LIABILITY 68
9.9 INDEMNITIES 68
9.9.1 Indemnification scope 68
9.9.2 Indemnification by Subscribers 69
9.9.3 Indemnification by Relying Parties 69
9.10 TERM AND TERMINATION 70

9.10.1 Term *70*
9.10.2 Termination *70*
9.10.3 Effect of Termination and Survival *70*
9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS 70
9.12 AMENDENTS 70
9.12.1 Prodedure for Amendment *70*
9.12.2 Notification Mechanism and Period *71*
9.12.3 Circumstances under which OID Must Be Changed *71*
9.12.4 Circumstance under which CPS Must Be Changes *71*
9.13 DISPUTE RESOLUTION PROVISIONS 71
9.14 GOVERNING LAW 71
9.15 COMPLIANCE WITH APPLICABLE LAW 71
9.16 MISCELLANEOUS PROVISIONS 72
9.16.1 Entire Agreement *72*
9.16.2 Assignment *72*
9.16.3 Serverability *72*
9.16.4 Enforcement *72*
9.16.5 Force Majeure *72*
9.17 OTHER PROVISIONS 72
10. APPENDIX A - VALIDATION REQUIREMENTS 73
10.1 VALIDATION ITEMS AND REQUIREMENTS 73
10.2 SUBSCRIBER CERTIFICATES AND VALIDATION ITEMS 75

1. Introduction

1.1 Overview

1.1.1 Company Introduction

TrustAsia Technologies, Inc. (abbreviated as TrustAsia) was established in April 2013, with ISO27001 information security management system certification and ISO 9001 quality management system certification, is an outstanding domestic cyber security digital certificate and security monitoring solution provider.
TrustAsia is a brand in the field of information security, specializing 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 sets up the following root certificates：

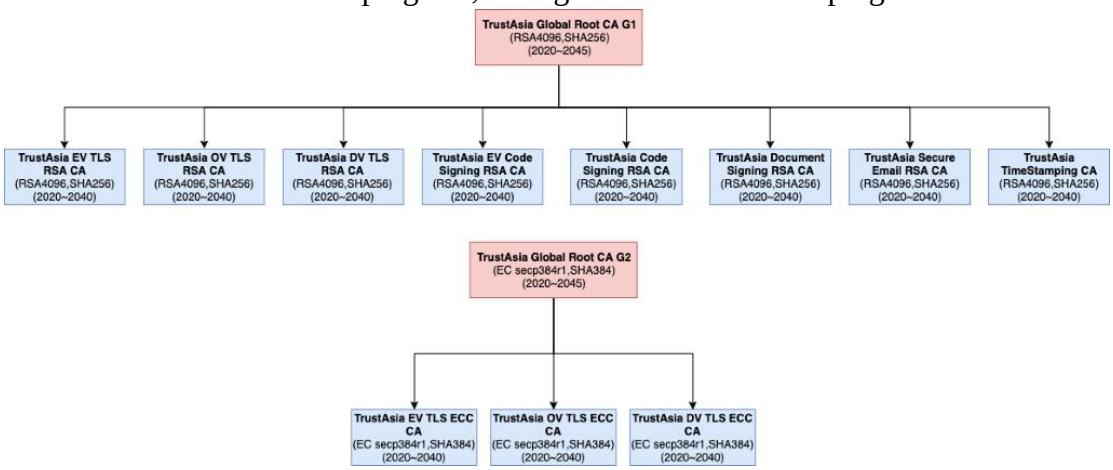
- TrustAsia Global Root CA G1
- TrustAsia Global Root CA G2
- TrustAsia Global Root CA G3
- TrustAsia Global Root CA G4

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 database. 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:

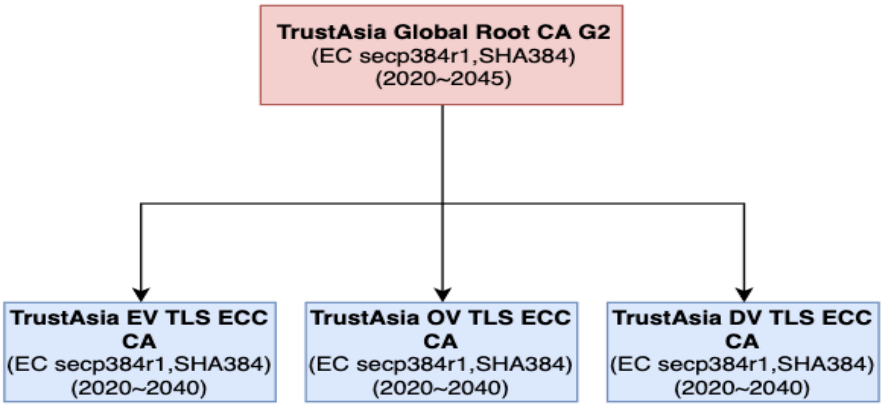
- TrustAsia EV TLS RSA CA, Issuing the RSA Extended Validation TLS Server Certificate.
- TrustAsia OV TLS RSA CA, issuing the RSA Organization Validation TLS Server Certificate.
- TrustAsia DV TLS RSA CA, issuing RSA Domain Validation TLS Server Certificate.
- TrustAsia EV Code Signing RSA CA, issuing the RSA Extended Validation Code Signing Certificates.
- TrustAsia Code Signing RSA CA, issuing the RSA code signing certificate.

- TrustAsia Document Signing RSA CA, issuing the RSA document signing certificates.
- TrustAsia Secure Email RSA CA, issuing the RSA Security Email Certificate.
- TrustAsia TimeStamping CA, issung the RSA TimeStamping 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:

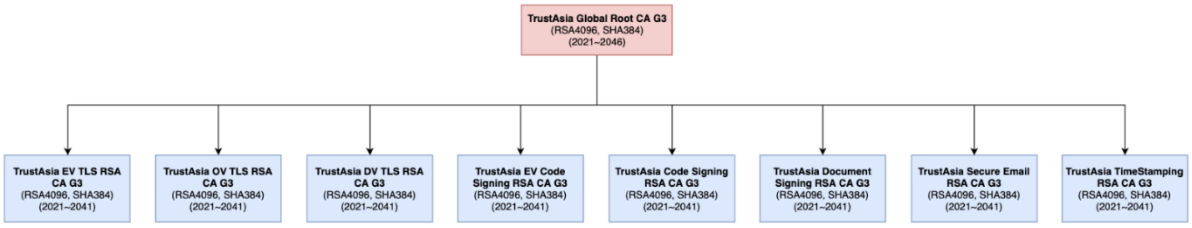
- TrustAsia EV TLS ECC CA, issuing the ECC Extended Validation TLS Server Certificate.
- TrustAsia OV TLS ECC CA, issuing the ECC Organization Validation TLS server certificate.
- TrustAsia DV TLS ECC CA, issuing the ECC Domain Validation TLS server certificate.



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:

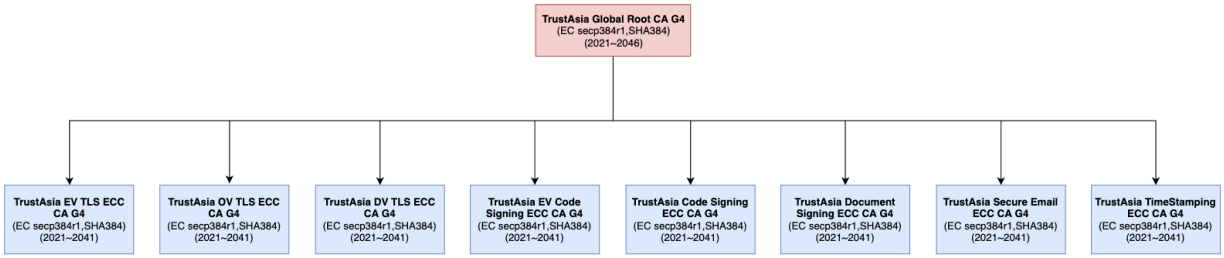
- TrustAsia EV TLS RSA CA G3, issuing the RSA Extended Validation TLS Server Certificate.
- TrustAsia OV TLS RSA CA G3, issuing the RSA Organization Validation TLS server certificate.

- TrustAsia DV TLS RSA CA G3, issuing the RSA Domain Validation TLS server certificate.
- TrustAsia EV Code Signing RSA CA G3, issuing the RSA Extended Validation Code Signing Certificates.
- TrustAsia Code Signing RSA CA G3, issuing the RSA code signing certificate.
- TrustAsia Document Signing RSA CA G3, issuing the RSA document signing certificates.
- TrustAsia Secure Email RSA CA G3, issuing the RSA Security Email Certificate.
- TrustAsia TimeStamping CA G3, issung the RSA TimeStamping 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:

- TrustAsia EV TLS ECC CA G4, issuing the ECC Extended Validation TLS Server Certificate.
- TrustAsia OV TLS ECC CA G4, issuing the ECC Organization Validation TLS server certificate.
- TrustAsia DV TLS RSA CA G4, issuing the ECC Domain Validation TLS server certificate.
- TrustAsia EV Code Signing ECC CA G4, issuing the ECC Extended Validation Code Signing Certificates.
- TrustAsia Code Signing ECC CA G4, issuing the ECC code signing certificate.
- TrustAsia Document Signing ECC CA G4, issuing the ECC document signing certificates.
- TrustAsia Secure Email ECC CA G4, issuing the ECC Security Email Certificate.
- TrustAsia TimeStamping ECC CA G4，issung the ECC TimeStamping certificate.



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

The overall structure of this Certificate Policy and Certification Practice Statement (CP&CPS) conforms to the Code of Certification Practice Statement(trial) issued by the Ministry of Industry and Information Technology, and strictly complies with the “Electronic Signature Law of the People's Republic of China”, "Measures for the Administration of Electronic Certification Services", "Measures for the Administration of Cipher Codes for Electronic Certification Services" and other related laws and regulations, as well as the requirements of the Ministry of Industry and Information Industry and the Cryptography Administration, and the framework of RFC3647.

This CP&CPS describes how TrustAsia 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/） (before 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.
3. Mozilla Root Store Policy
4. Microsfot 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 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.

1.2 Document name and identfication

Object	OID
Domain Validation SSL/TLS Certificate Policy Identification	2.23.140.1.2.1 1.3.6.1.4.1.44494.2.1.3
Organization Validation SSL/TLS Certificate Policy Identification	2.23.140.1.2.2 1.3.6.1.4.1.44494.2.1.2
Extended Validation SSL/TLS 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
Class 1 Secure Email Certificate Policy Identification	1.3.6.1.4.1.44494.2.4.1
Class 2 Secure Email Certificate Policy Identification	1.3.6.1.4.1.44494.2.4.2
Time-stamping Certificate Policy Identification	1.3.6.1.4.1.44494.2.5.1

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 agents of multiple CA, TrustAsia 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'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 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, either individuals, institutions, or equipments. Contracts are usually signed between TrustAsia 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. 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. The relying party can or may not be a subscriber.
Other participants refer to other entities that provide related services for TrustAsia certification activities.

1.3.5 Other Participants

Other participants refer to other entities that provide related services for TrustAsia 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 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 CPS, it will not be protected by this CP&CPS.
The certificates issued by TrustAsia are prohibited from being used in any case of a violation of national laws, regulations or the destruction of national security, and are prohibited 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 certification system can provide formal certificates and test certificates.

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

The test certificate is issued by TrustAsia 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 user 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 Security Strategy Committee, which is responsible for formulating, approving, issuing, implementing, updating and revoking this CP&CPS. The Asia Integrity Security Strategy Committee 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 strategy department 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 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 issue 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 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 CPS compilation team which is organized by Security Policy Committee of TrustAsia. When the compilation of this CP&CPS is

finished, which is submitted to Security Policy Committee for audit. After the approval by Security Policy Committee, it is published on the official website of TrustAsia.

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 EV Guideline issued by CA/B Forum, and the CP&CPS preparation team will prepare the CP&CPS revision contents according to the relevant conditions. 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.

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 Roots 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.

1.6.2 Acronyms

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	证书撤消列表
CSR	Certificate Signing Request	证书请求文件

DBA	Doing Business As	商业名称
DNS	Domain Name System	域名系统
EV	Extended Validation	扩展验证/增强验证
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
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

2. Publication and Repository Responsibilities

2.1 Repositories

TrustAsia 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.

2.2 Publication of Information

2.2.1 Publication of Repositories

TrustAsia repositories will be posted on the official website (https://www.trustasia.com) 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 issues a subscriber's certificate and certificate revocation list (CRL) through HTTP, and the subscriber or relying party may obtain the CRL information from the CRL distribution point address in the certificate issued by TrustAsia. Each CRL issued by TrustAsia contains an incremental serial number.

2.2.3 Publication of OCSP

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

2.3.2 Time or Frequency of Publication of CRL

TrustAsia publishes CRL for subscriber certificates at least once in 7 days; CRL for child CA certificates at least once in 12 months, If the condition is that the child CA certificate being revoked occurs, the CRL for releasing CA certificate must be updated within 24 hours.

2.3.3 Time or Frequency of Publication of OCSP

As soon as the subscriber certificate issued by TrustAsia is issued, it can be downloaded. Subscribers can obtain the issued certificate through email or the certificate service site provided by TrustAsia, and inquire about the status of the certificate through OCSP.

The OCSP response data for subscriber certificates is updated at least once in 4 days, with a maximum validity period of not more than 10 days.
The OCSP response data for intermediate CA certificates is updated at least once in 12 months, and will be updated within 24 hours if the CA certificate is revoked.

In the case of emergency, the release time and frequency of the other contents of repositories shall be determined independently by TrustAsia, which should be immediate, efficient and consistent with the requirements of the national laws.

2.4 Access Controls on Repositories

The information in TrustAsia repositories is provided with query and access in a read-only manner.

With network security, secure system design and security policy, TrustAsia ensures that only authorized employees can add, delete, modify and publish the repositories.

3. Identification and Authentication

3.1 Naming

3.1.1 Type of Names

The digital certificate issued by TrustAsia 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. The certificate of TrustAsia 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 screening 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, and the generic 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 TLS/SSL certificate, the reserved private IP addresses or internal names should not be included in them. In the dNSName entries of the certificate, the underscore ("_") characters should not be included in them.
The subjectAltName extension of DV and EV TLS/SSL certificates cannot include IP address.

Naming rules of issuer's DN are as follows:

Attribute	Value
Country（C）	CN
State（S）	State of issuer (if included)
Local（L）	Local of issuer (if included)
Organization（O）	TrustAsia Technologies, Inc.
Organization Unit (OU)	TrustAsia Certificate contains various issuers depend on subscriber types, applications and regions to issue the certificate.
Common Name（CN）	Name of CA

Naming rules of subscriber's DN are as follows:

Attribute	Value
Country（C）	CN
State（S）	State of subscriber (if included)
Local（L）	Local of subscriber (if included)
Organization（O）	Organization where subscriber subordinates for certain one;
Organization Unit（OU）	OU of subscriber subordinates;
Email（E）	Subscriber's email address (if included)

Common Name（CN）	Domain name (SSL/TLS certificate), organization name (organization certificate), individual name (individual certificate), or other identifiable names.

3.1.2 Need for Names to be Meaningful

TrustAsia uses the DN field 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 identification name of the subject shall comply with the requirements of laws and regulations and other relevant provisions.

3.1.3 Anonymity or pseudonymity of Subscribers

Subscribers of certificates described in this CP&CPS may not use anonymous or pseudonyms when applying for certificates.

3.1.4 Rules for Interpreting Various Name Forms

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

3.1.5 Uniqueness of Names

DN of certificate must be unique for different subscribers in TrustAsia trust domain, and same DNs cannot be allowed as subscriber's subject name. TrustAsia 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.
Client certificate	Requires a unique email address or organization name to be combined or associated with a unique serial number.
Code signing certificate (including document signing certificate)	The only organization name and address or unique organization name is required to be combined or associated with a unique serial number.
Timestamp certificate	A unique hash and time or unique sequence 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 does not verify the subscriber's right to use the trademark, nor responsible for resolving any trademark related disputes. TrustAsia 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) .

3.2.2 Authentication of Organization and Domain Identity

3.2.2.1 Identification 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. Identify 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 should verify the name and registration or business address of the organization. TrustAsia can perform different authentication methods according to the type of certificate requested by the organization. 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 can select 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 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 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, TrustAsia establishes evaluation criteria to identify potentially high-risk fraud certificate requests. TrustAsia can directly reject certificate requests identified as "high risk".

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 will confirm the host country through the organization approval information provided by the applicant under the section 3.2.2 of CP&CPS.

3.2.2.4 Validation of Domain Authorization or Control

When the user applies for an SSL certificate, TrustAsia needs to verify the applicant's control of the domain name in the certificate applied for. The verification of domain name ownership follows the principles set out in section 3.2.2.4 of CA/B Forum BR:

1. The root domain of the domain name must be the legal root domain published by ICANN.
2. The domain name format must follow the FQDN standard, or there is only one *. the wildcard domain name located on the leftmost side of the FQDN.
3. Domain name control can be verified in any of the following ways:

   a. Domain name management mailbox

   TrustAsia will verify the domain name control right by sending a verification email with a random value to any of the following mailboxes:

   - Whois contact email(BR 3.2.2.4.2) of the domain name to be verified, or the default administrator email(BR 3.2.2.4.4)
   - Administrator@Domain name to be verified
   - Admin@Domain name to be verified
   - Postmaster@Domain name to be verified
   - Hostmaster@Name to be verified
   - Webmaster@Domain name to be verified
   - Domain contact email (BR 3.2.2.4.14) for "_validation-contactemail.domain-to-be-validated" TXT resolution via DNS query.

After the subscriber receives the verification email, enter the domain verification link and click on approval to complete the domain ownership verification.

b. DNS validation code (BR 3.2.2.4.7)

The subscriber can complete the domain ownership verification by checking the specified TXT or CNAME record with a random value for the domain name to be verified.

c. HTTP/ HTTPS validation code (BR 3.2.2.4.6)

The subscriber places the designated verification file and random verification value under the designated directory /.well-known/pki-validation/ of the domain name site to be verified.

TrustAsia can successfully access the specified verification content through the default port of the HTTP/HTTPS protocol to complete the domain name ownership verification.

If the domain name completes the ownership verification in this way, TrustAsia may only can issue a certificate for this domain name. This verification method does not apply to verification with wildcard domain names.

4. Do not support the verification of ".onion" as the rightmost label, and do not issue this kind of certificate.

3.2.2.5 Authentication for IP Address

TrustAsia 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. Verification of the right to use IP address follows the principles in chapter 3.2.2.5 of CA/B Forum BR:

TrustAsia validates the right to use IP in any of the following ways:

1. TrustAsia will verify the IP control right by sending a verification email to Whois contact email. The verification email contains a unique random value, and when the subscriber receives the verification message, they access the verification link with the random value and click approve to complete the IP control verification.
2. HTTP/ HTTPS validation code (BR 3.2.2.5.1)

   Subscriber put specified verification file and random verification code under specified directory /.well-known/pki-validation/ at the IP site to be verified.

   TrustAsia can successfully access specified authentication content through the default port of the HTTP/HTTPS protocol, which means the domain name ownership verification can be completed.

3.2.2.6 Wildcard Domain Validation

TrustAsia verifies control over the domain name to the right of the wildcard, and the verification rules follow the regulations of this CP&CPS 3.2.2.4. TrustAsia 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.

3.2.2.7 Accuracy of data sources

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

TrustAsia follows the regulations of section 3.2.2.8 of CA/ B Forum BR, and the domain names of all subject name and alternate name in the certificate application are checked by the DNS CAA record 8 hours earlier before the certificate is issued. TrustAsia processes the "issue," "issuewild," "iodef" attribute tags in CAA records according to the regulations of RFC8659.

If there is an "iodef" tag in the CAA record, TrustAsia will communicate with the subscriber to determine whether to issue the certificate, but may not send a report to the address in the "iodef" attribute label.

TrustAsia will refuse to issue a certificate when the CAA response data has the "issue", "issuewild" attribute tags, and the tag content does not contain “trustasia.com".

TrustAsia are permitted to treat a record lookup failure as permission to issue if:

1. The failure is outside the CA’s infrastructure; and
2. The lookup has been retried at least once; and
3. The domain’s zone does not have a DNSSEC validation chain to the ICANN root.

3.2.2.9 Validation E-mail Address

When the email address is applied for as the subject content of the certificate, TrustAsia will confirm the validity of the email address and audit the applicant's right to use the email address. Only after passing the audit can the Email entry be checked in the certificate. The specific audit steps are as follows:

1. After the applicant completes the generation of the CSR file, the system detects the mail address and automatically sends a random value to the mail address, which is generated by the system and unique.
2. The applicant receives the mail and approves it via a link with a random code;
3. After the CA system of TrustAsia receives the approval from user, it will compare the random code sent with the random code in approval. If the result is consistent, the email is approved.

The mail with the original random value can be repeatedly transmitted without any change in the overall content of the recipient and the mail. The random value in the message shall start on the day of the generation and the validity period shall not exceed 30 days.

3.2.3 Authentication of Individual Identity

If the applicant's identity is a natural person, TrustAsia will review the applicant's name, address, and the authenticity of the certificate application. In the case of a personal identification certificate, TrustAsia 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 more strict 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 verifies that copies of the documents match the requested names and that other relevant information is correct.

TrustAsia 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 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 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, TrustAsia establishes evaluation criteria to identify potentially high-risk fraud certificate requests. TrustAsia can directly reject certificate requests identified as "high risk".

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 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 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 will use the sources listed in Chapter 3.2.3 to obtain reliable means of communication to verify the authenticity of the applicant's application certificate. TrustAsia 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 thinks fit.

TrustAsia may also allow 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 allows applicants to designate independent individuals to apply for certificates. TrustAsia 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 shall 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, but the CP&CPS of the electronic certification service must meet the TrustAsia CP requirements and sign the corresponding agreement with TrustAsia.
If there are provisions in national laws and regulations, TrustAsia will strictly implement the relevant provisions.
So far, TrustAsia 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 will create a new certificate that contains the new public key but the subject matter of the certificate is the same as the original certificate, and can selectively extend the validity of the certificate. TrustAsia 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 will not be responsible for the loss caused by the original key pair.

3.3.1 Identification and Authentication got Routine Re-key

TrustAsia supports certificate subscribers during the validity period to make key update requests, 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.

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

When a subscriber needs to issue a replacement certificate, he/she should apply for a replacement certificate to TrustAsia on his/her own initiative. If the subscriber's authenticated certificate registration information is within the CA/B Forum BR certification period, TrustAsia 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/B 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 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/B Form BR. TrustAsia will reissue the

certificate to the subscriber based on its original information. If the verified certificate registration information distance from the initial verification has exceeded the CA/B Form BR specified verification validity period, the subscriber identity needs to be re-validated, 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 does not provide Re-key/renewal after revocation.

3.4 Identification and Authentication for Revocation Request

In TrustAsia's certificate business, a certificate revocation request can come from a subscriber or from TrustAsia. In addition, TrustAsia has the right to initiate the revocation of a subscriber certificate when it has a certificate that requires revocation for the reasons stated in this CP&CPS 4.9.1.1.
Subscribers submit requests to TrustAsia in certain ways, such as mail, fax, telephone, etc., TrustAsia confirms that the person or organization 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 name control verification, telephone, fax, e-mail, mailing or express delivery.

3.5 Identification of authorized Service institutions

TrustAsia 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 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 signatory.

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;
- 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, CP and this 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.
   - 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 receives a subscriber's certificate request, the TrustAsia Verification Team will identify and authenticate the subscriber's identity as required in Section 3.2 of the CP&CPS. TrustAsia 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 applicant through the web interface of TrustAsia or all the information provided directly by the API.

TrustAsia 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 has the right to reject certificates and request or perform additional authentication.

TrustAsia 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 3.2.2.8 of the CP&CPS.

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

After the verification is completed, the TrustAsia verification team will review all certificate application information and related documents, and according to the verification results decide to accept, refuse the application or request the applicant to submit additional relevant materials.

For the purpose of authenticating the information contained in the OV and EV SSL certificates, TrustAsia may use data or supporting documentation obtained from a source designated by TrustAsia in accordance with section 3.2 of this CP&CPS if the data or supporting documentation has not been obtained by TrustAsia for more than 398 days and the information has not changed.

4.2.2 Approval or Rejection of Certificate Applications

4.2.2.1 Approval of Certificate Applications

After TrustAsia's registration authority successfully completes verification steps for the certificate application and submits a certificate request, when TrustAsia formally issues certificates, it means TrustAsia has approved the certificate application.

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

1. The application shall completely meet 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's agreement.
3. Subscriber has paid already in accordance with the provisions.

4.2.2.2 Rejection of Certificate Applications

If the following circumstances happened, TrustAsia 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 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's 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 considers that the approval of the application will bring about controversies, legal disputes or losses to TrustAsia.
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 will email to notify subscribers that the certificate application has failed.

4.2.3 Time to Process Certificate Applications

Under normal circumstances, TrustAsia 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 in a timely manner. The application for a certificate will remain valid until it is rejected.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate issuance

TrustAsia 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 does not issue the final entity certificate directly from its root certificate.
Record the SSL/TLS server certificate to be trusted in Chrome 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 TLS certificates, after the pre-certificate is issued the CA will use certificate checking tools such as x509lint, zlint, cablint, etc. to check the pre-certificate and block the issuance of non-compliant certificates.

4.3.2 Notification of CertifIicate Issuance

TrustAsia provides certificates in any secure manner within a reasonable time after release. Typically, TrustAsia 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 certificate service website, and complete downloading the certificate to the digital certificate carrier.
2. TrustAsia downloads the certificate instead 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 delivers the certificate to the subscriber as a release of the certificate. TrustAsia will chooses 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.

Follow the regulations on the information base mechanism in chapters 2.4 and 2.5 of this CPS, TrustAsia will 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 is authorized to maintain and manage its integrity. If required by relevant laws and regulations such as confidentiality laws. TrustAsia 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 will not notice to 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, 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, a certificate update may be made from 30 days (inclusive) prior to the expiration of the certificate. If the subscriber choose 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 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 CPS, then TrustAsia may verify 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 CPS, the certificate renewal request will be verified in accordance with the process and requirements of the certificate initial application by TrustAsia.

If the original certificate of the subscriber has expired, verify according to the process and requirements of the initial application of the certificate 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 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:
   1) The original certificate of the subscriber exists and is issued by TrustAsia;
   2) the certificate update request is within the license period;
   3) 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 will process according to the provisions of Chapter 3.3.1 of this CP&CPS. TrustAsia 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 can approve 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 one certificate multiple deployments, 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 name 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 certificate and whose certificate has not expired.

4.7.3 Processing Certificate Re-keying Requests

The process of certificate key update request is completed by the process of certificate update request in TrustAsia. 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. If the name of the authority needs to be changed, the subscriber needs to apply for a new certificate again.

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 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 will re-verify the certificate information. If the application

data of the original certificate are available and not expired (the application data of OV and EV certificate is valid for 398 days, the application data of DV certificate need 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 will audit and verify the certificate process and requirements in accordance with the initial application process and requirements. Then,TrustAsia will reissue 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

TrustAsia shall revoke the certificate within 24 hours if one or more of the following occurs:

1. The subscriber requests in writing that TrustAsia revoke the certificate;
2. The subscriber notifies TrustAsia that the original certificate request was not authorized and does not retroactively grant authorization;
3. TrustAsia obtained evidence that the subscriber private key corresponding to the certificate public key was compromised.
4. TrustAsia is made aware of a demonstrated or proven method that 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);
5. TrustAsia is proof that control of the domain name or IP address contained in the certificate is no longer reliable;

TrustAsia shall revoke the certificate within 24 hours if one or more of the following occurs, and the certificate must be revoked within 5 dyas.

1. TrustAsia 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.;
2. TrustAsia obtains evidence that the certificate was misused;

3. TrustAsia is made aware that a subscriber has violated one or more of its material obligations under the subscriber agreement and CP/CPS;
4. TrustAsia is made aware of any circumstance indicating that use of a fully-qualified domain name or IP address in the certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a domain name registrant's right to use the domain name, a relevant licensing or services agreement between the domain name registrant and the applicant has terminated, or the domain name registrant has failed to renew the domain name);
5. TrustAsia is made aware that a wildcard certificate has been used to authenticate a fraudulently misleading subordinate fully-qualified domain name;
6. TrustAsia is made aware of a material change in the information contained in the certification.
7. TrustAsia is made aware that the certificate was not issued in accordance with Baseline Requirements or TrustAsia's CP&CPS;
8. TrustAsia considers that any information that appears in the certificate is inaccurate, untrue or misleading;
9. TrustAsia's right to issue certificates under Baseline Requirements expires or is revoked or terminated, unless TrustAsia has made arrangements to continue maintaining the CRL/OCSP Repository.
10. TrustAsia CP&CPS requires revocation of subscriber certificate;
11. TrustAsia is made aware of a proven method that the compromise of the subscriber's private key, or clear evidence that the specific method used to generate subscriber's private key was flawed.
12. TrustAsia ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the certificate;
13. 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;
14. After TrustAsia has fulfilled its call obligation, the subscriber has still not paid the service charge.
15. 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).
16. CA obtain evidence or be informed that the subscriber has suspicious code in the software who signs.

4.9.1.2 Reasons for the revocation of Intermediate CA certificates

In the event of one or more of the following conditions, TrustAsia shall revoke the intermediate CA certificate within 7 days:

1. The formal written application of the intermediate certification authority shall be revoked;

2. The intermediate certificate authority finds and informs TrustAsia that the initial certificate request is not authorized and cannot be traced back to the authorization act;
3. TrustAsia obtained evidence that the intermediate CA private key corresponding to the certificate public key had been damaged or that it no longer met the relevant requirements of sections 6.1.5 and 6.1.6 of Baseline Requirements;
4. TrustAsia obtained evidence that the certificate had been misused;
5. TrustAsia was informed 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 considers that any information that appears in the intermediate CA certificate is inaccurate, untrue, or misleading;
7. TrustAsia ceased operations for any reason and did not enter into an agreement with another CA to provide a certificate revocation service;
8. TrustAsia's power to issue certificates in accordance with Baseline Requirements is invalidated, or revoked or terminated, unless it continues to maintain the CRL/OCSP database;
9. This CP or the corresponding 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, RA, TrustAsia, 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 of reasonable grounds to revoke the certificates.

For incidents involving malware, TrustAsia will take 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

5. The subscriber submits the application form of certificate revocation and the related identification material to TrustAsia, and the reasons for revocation should be described in the application form;
6. TrustAsia shall authenticate the certificate revocation request in accordance with the provisions of Chapter 3.4 of this CPS;
7. TrustAsia should publish it to the certificate revocation list in time after accomplishing the certificate revocation.
8. After the certificate is revoked, TrustAsia will notify the subscriber by e-mail and other appropriate means. If the subscriber is not reached, TrustAsia can announce the revoked certificate through the website if necessary.
9. TrustAsia 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 will apply 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 CPS;
2. When the private key corresponding to the root certificate or intermediate CA certificate of TrustAsia appears 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 draws the certificate problem report, TrustAsia shall organize the investigation and decide whether to revoke the certificate according to the result of the investigation;
4. After the certificate has been revoked, TrustAsia will notify the final subscriber certificate of its revocation and the reasons for its revocation by appropriate means, including mail, telephone, etc.; if the subscriber cannot be contacted, TrustAsia may announce the revoked certificate through the website if necessary;
5. TrustAsia provides 7*24 hours of certificate problem reporting and processing services, which can be reported through the contact information provided in Chapter 1.5.2 of this CP&CPS.

4.9.4 Revocation Request Grace Period

TrustAsia does not support a revocation request grace period.

4.9.5 Time Within Which CA Must Process the Revocation Request

TrustAsia 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.

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 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, 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

The CRL release cycle for subscriber certificates is at least once in 7 days, and it is valid for no more than 10 days.
For intermediate certificates, the CRL release cycle is at least once in 6 months, and it is valid for no more than 12 months. If there is a revocation of intermediate certificates, CRL should be updated within 24 hours.

4.9.8 Maximum Latency for CRLs

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

4.9.9 On-line Revocation/Status Checking Availability

TrustAsia provides Online Certificate Status Protocol for the subscriber certificate and 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 offers the OCSP service using both the Get and Post methods.
The OCSP response data for subscriber certificates is updated at least once in 4 days, with a maximum validity period of not more than 10 days.
The OCSP response data for intermediate CA certificates shall be updated at least once in 12 months, and will be updated within 24 hours if the CA certificate is revoked.
If the OCSP responder receives a request for status of a certificate that has not been issued, then the responder should not respond with a “good” status.

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 can require subscribers to use OCSP binding to access OCSP services according to the provisions in RFC4366.

4.9.12 Special Requirements related to Key Compromise

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

1. The private key itself
2. CSR signed with a compromised private key, CSR generic name is “Proof of Private Key Compromise for TrustAsia”

4.9.13 Circumstances for Suspension

TrustAsia 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 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 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, EVSSL certificate chain can be downloaded in no more than 3 seconds through an analogue telephone line.

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 shall be deemed that the user terminated the use of the certificate services provided by TrustAsia:

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 during the validity period of the certificate, TrustAsia 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 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 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

5.1 Physical Security Controls

5.1.1 Site Location and Construction

The TrustAsia’s data center and system shall be 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'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 open.

5.1.2 Physical Access

In the data center of TrustAsia, installing with 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

TrustAisa 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 also has a diesel engines can meet the requirement that 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’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

TrustAsica 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 complete various linkage actions related to the system.

5.1.6 Media Storage

TrustAsia 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 shall shred 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 backups the coresystem data, audit log data at off-site location by offline media. The storage facilities fulfill the description of 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. These roles include but are not limited to:

1. Key and cryptographic devices personnel, which are responsible for the management of CA keys, certificates life-cycle and cryptographic devices;

2. Authentication and customer service personnel, which are responsible for the validation of subscriber certificates, and customer support services;
3. System maintenance personnel, which are responsible for the maintenance of the hardware and software of CA system;
4. Security management personnel, which are responsible for the area security and daily physical security management;
5. Security audit personnel, which are responsible for the audit of the operations;
6. Human resource management personnel, which 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 strictly defines the controls of core missions in specific standards. Multiple trusted roles shall be 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 authenticates CA and RA systems before allowing the trusted roles access and execute 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. Roles requiring segregation of duties include but are not limited to：

	Key and cryptographic devices personnel	Validation & Customer Service Personnel	System Maintenance Personnel	Security Management Personnel	Security Auditor Personnel	Human Resource Management Personnel
Key and cryptographic devices personnel	——	NO	NO	NO	YES	NO
Validation and Customer Service Personnel	NO	——	NO	NO	NO	NO
System Maintenance Personnel	NO	NO	——	NO	NO	NO
Security Management Personnel	NO	NO	NO	——	NO	NO
Security Auditor Personnel	YES	NO	NO	NO	——	NO
Human Resource Management Personnel	NO	NO	NO	NO	NO	——

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

The qualification requirements of person who undertakes trusted role in TrustAsia 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 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's related training and examination before they start their work.

5.3.2 Background Check Procedures

TrustAsia or 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 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 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 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. Disaster recovery and business continuity management
5. Job responsibilities requirements
6. Baseline of CA/Browser Forum
7. The laws, regulations, standards and procedures of electronic certification service in China.
8. Other needs of training

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. Related personnel for operating authentication system should have the training of relevant skills and knowledge at least once a year. In addition, TrustAsia 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 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 systems, perform authorization businesses without or beyond the permission, once the above circumstances are confirmed by TrustAsia, we will immediately revoke the login certificates and simultaneously terminate the system access authorization. TrustAsia 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 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 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 supports all basic event auditing capabilities of its CA and applications to document the following events. TrustAsia will record manually if the application does not record automatically.

These events include but not limited to:

1. Management events in key's life cycle, including,

- Generation, backup, storage, recovery, usage, revocation, archiving, destruction, private key leakage, etc.

2. Management events in cryptography device’s life cycle, including
   - Receiving, installation, uninstallation, activation, usage, repair, etc. for equipment.
3. The certificate application events, including
   - The subscriber accepts subscriber’s agreement, the applied company, application data verification, application and validation data preservation, etc.
4. Management events of certificate life cycle, including
   - Application, approval, update, revocation, etc.
5. System security events including:
   - Successful or unsuccessful access attempts for CA system,
   - Unauthorized access attempts for CA system network,
   - Unauthorized access attempts for CA system files,
   - Operation (read, write or delete, etc.) for restricted and sensitive documents or records,
   - System crash, hardware failures and other abnormal events.
6. Security events recorded via firewalls and routers.
7. System operating events, including:
   - Startup and shutdown,
   - Creation or deletion of permission, configuration or modification of password.
8. Access to CA facilities, including
   - The access of authorized
   - The unauthorized personnel and attendants, and the access to security storage facilities.
9. Management record of trusted roles and personnel, including
   - The network account application,
   - System permission application, modification, and creation,
   - 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.

5.4.2 Frequency for Processing and Archiving Audit Logs

TrustAsia checks and summarizes the system's automatic log and operators' manual records once a month.

TrustAsia 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 keeps the audit log of the CA service properly, and the audit log related to the certificate is retained for at least 10 years after the certificate expired.

5.4.4 Protection of Audit Log

TrustAsia audit logs are stored in the database with backup, including audit information and event records in related documents.
TrustAsia 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's system log is backed up to the log server in real time, and to the different places weekly. The manual electronic records are backed up to SVN, and the manual paper records are archived and saved in a special filing cabinet.

5.4.6 Audit Log Accumulation System

Regarding the electronic audit information, TrustAsia'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 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 has the right to decide whether to notify subjects related to the event.

5.4.8 Vulnerability Assessments

According to security events found by the audit, TrustAsia will conduct the annual security vulnerability assessment of the system, physical sites, operation management, etc., and take measures to reduce the operational risk based on the assessment report.

5.5 Records Archival

5.5.1 Types of Records Archived

TrustAsia archives the following types of records:

1. Documents of certificate system building and upgrading;
2. Certificates
3. Life cycle management records of subscriber certificates;
4. Audit records;
5. CP&CPS;
6. Employee materials, including but not limited to materials of background investigation, employment, training, etc.;
7. Various external and internal evaluation documents.

5.5.2 Retention Period for Archive

For different archived records, the retention periods are different. For system operation event records and system security event records, the archives will be retained to complete the security vulnerability assessment or audit consistency.

1. Archiving for management events in subscriber certificate life cycle will be kept for more than 10 years.
2. Archiving for management events in CA Certificate and key life cycle will be kept for not less than life cycle of CA certificate and key.
3. Archiving retention period of subscriber certificates data will not be less than 10 years after the expiration of certificates.
4. CA key and certificate archiving will be kept for 10 more years after the end-of-life cycle.

5.5.3 Protection of Archive

TrustAsia 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 shall be made regularly and backup files shall be stored in different places; the manual electronic records shall 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

All the TrustAsia records are labelled with time, and the time will either be added manually by the operators or automatically by system.

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 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 valid period of TrustAsia'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 CPS, TrustAsia will start the key renewal process and replace the already expired CA key pair. The key changeover of TrustAsia 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. Generate a new key pair and issue a new higher CA certificate.
3. 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.
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 has stipulated the corresponding incident and compromise handling procedures, and formulated various emergency response plans as following:

1. The emergency plan of the power system;
2. The emergency plan of Internet failure;
3. The hardware failure emergency plan;
4. System backup and recovery emergency plan;
5. Key emergency plan, etc.

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

TrustAsia 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 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 to revoke the certificate, or immediately notify TrustAsia revoke the certificate by telephone, etc., and reapply for a new certificate according to the relevant process. TrustAsia will issue certificate revocation information according to Section 4.9 of this CP&CPS.
2. When TrustAsia finds that the entity certificate private key of the subscriber certificate is compromised, TrustAsia 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 will issue certificate revocation information according to Section 4.9 of this CP&CPS.
3. When the private key of TrustAsia root CA or subordinate CA is compromised, TrustAsia 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 will restore some services within 48 hours in accordance with the business continuity plan.

5.8 CA or RA Termination

When TrustAsia need 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 must:

1. Determine the service undertaking unit;
2. Draft the termination statement;
3. Notify the relevant entities;
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 approved and licensed by OSCCA, in a physically secure environment and under the control of multiple trusted persons. The generation, management, storage, backup and recovery of the key pair shall comply with the relevant regulations of FIPS140-2. Since FIPS140-2 is not a standard approved and accepted by OSCCA and OSCCA implements a strict management of state's cryptographic products, TRUSTASIA only applies part of the provisions of FIPS140-2 under the permission of OSCCA. Specifically, the product manual of the device is for your reference. Hardware Security Module used for key generation must be evaluated and certified by OSCCA. The generation of the CA key pairs are witnessed by key administrators, several trusted personnel and independent third-party auditors of TrustAsia, and completed in accordance with key generation procedures in TrustAsia shield computer room. The procedures and operations related to key pair generation shall be video recorded and archived.

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. If a subscriber submits a PKCS#10 file of weak Algorithm during application, TrustAsia will reject the application and recommend the user to generate a new key pair.
TrustAsia does not generate key pairs for Subscribers.

6.1.2 Private Key Delivery to Subscriber

Not applicable.

6.1.3 Public Key Delivery to Certificate Issuer

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

6.1.4 CA Public Key Delivery to Relying Parties

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

6.1.5 Key Sizes

To ensure the security strength of the keys, TrustAsia's different types of certificate keys follow 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	2048, 3072, 4096
ECC Curve	P-384	P-384	P-256, P-384

6.1.6 Public Key Parameters Generation and Quality Checking

Public key parameters shall be generated by using the cryptographic hardware and media with the license from OSCCA and shall follow generation norms and standards of these equipment. Regarding the parameter quality check, since keys are generated and stored using the cryptographic hardware and media with the license from OSCCA, the parameters have already met the requirements on high security level.

6.1.7 Key Usage Purposes

X.509v3 certificate issued by TrustAsia includes key usage extensions, and their usage conforms to RFC5280 Standard. Regarding the purposes specified by TrustAsia 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. the CRL (ARL) of the root CA and the subordinate CA.

Except as stipulated in the Baseline Requirements, Root CA Private Keys are not used to sign CS、EV CS、EV SSL certificates or create CS、EV Signatures

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

1. subscriber certificate;
2. PKI system function certificate with specific purposes (e.g. OCSP certificate);
3. subscriber CRL.

The subscriber's key can be used to provide security services, such as identity authentication, information encryption and signatur, 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

6.2.1 Cryptographic Module Standards and Controls

TrustAsia keys are generated using the encryption modules approved and licensed by OSCCA, follows regulations of <GM/T 0028-2014 Security requirements for cryptographic modules>, FIPS140-2 Standard. Information details provided by the equipment manufacturer.

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 neither allows escrow for the root private key or CA private key, nor provides escrow service of private key for subscribers.

6.2.4 Private Key Backup

TrustAsia 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 does not archive private keys of subscriber certificates.

6.2.6 Private Key Transfer into or from a Cryptographic Module

TrustAsia's key pair is generated, saved and used on the hardware cryptographic module. In order to achieve recovery, TrustAsia backs up the CA key according to the operation specification provided by the encryption equipment manufacturer. Besides, TrustAsia 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

TrustAsia’s private keys shall be stored on the hardware cryptographic module that meets the requirements of OSCCA in an encrypted form, and the use of private keys shall also be conducted on the hardware cryptographic module.

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, 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’s private key ends, TrustAsia 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

TrustAsia uses the cryptographic products approved and permitted by OSCCA, and OSCCA is responsibility for the evaluation of cryptographic module.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

For TrustAsia 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 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	No stipulation	397 days
OV SSL/TLS	No stipulation	397 days
EV SSL/TLS	No stipulation	397 days
Document Signing	No stipulation	39 months
CodeSigning	No stipulation	39 months
EV CodeSigning	No stipulation	39 months
S/MIME	No stipulation	39 months

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 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), must be kept in reliable way and by trusted personnel. 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 should 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.

Dual-factor authentication mechanism shall be utilized in the login process to validate the digital certificate and username/password of user. TrustAsia assign each user of CA/RA system a unique account with minimum permissions according to the requirements of user.

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's 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 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

The operation specifications of software development, which refer to ISO15408 standard, implement relevant plan and development control.

6.6.2 Security Management Controls

TrustAsia 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 shall strictly follow 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 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 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’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 should only open to specific services and personnel with the minimum access authority.

The certification system should regularly scan security vulnerabilities, check the configuration of security devices, and audit the system logs.

6.8 Time-Stamping

The digital certificate and CRL issued by the TrustAsia certification system contain date information, which is digitally signed. The authentication system log and operation log have corresponding time identification. These time-stampings do not adopt the digital time stamp technology based on password.
The time source of the authentication system is Coordinated Universal Time（UTC）.

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

The format of TrustAsia certificates conforms to ITU-T X.509 V3, ITU-T and RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
TrustAsia generates non-sequential certificate serial numbers greater than zero containing 64 bits of output from a CSPRNG.

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; Application of RFC 5280

In addition to the certificate standard items and standard extension items, TrustAsia also uses customized extensions.

7.1.2.1 Root CA Certificate

1. basicConstraints
   The "basicContraints" extension in the root CA certificate is marked as critical. The "CA" field of this extension isA True" and the "pathLenConstraint" field is not set.
2. keyUsage

The "keyUsage" in the root CA certificate is a critical extension, and the usage is set to: KeyCertSign, CRLSign. The root CA private key is not used for signing OCSP responses.

3. certificatePolicies
   This extension is not set for the root CA certificate.
4. extKeyUsage
   This extension is not set for the root CA certificate.

7.1.2.2 Subordinate CA Certificate

1. certificatePolicies
   The subordinate CA certificates have the "CertificatePolicies" extension, which is a non-critical extension. Different policy identifiers are set according to the different usage of subordinate CA certificates.
2. CRLDistributionPoints
   The subordinate CA certificates have the "CRLDistributionPoints" extension, which is a non-critical extension. This extension will contain the HTTP URL of the CA's CRL service.
3. authorityInformationAccess
   The subordinate CA certificates have the "authorityInformationAccess" extension, which is a non-critical extension. This extension will contain the HTTP URL of the issuing CA's certificate (AccessMethod=1.3.6.1.5.5.7.48.2) and the HTTP URL of the issuing CA's OCSP responder(AccessMethod=1.3.6.1.5.7.48.1).
4. basicConstraints
   The subordinate CA certificates have the "basicConstraints" extension, which is a critical extension. The "CA" field in this extension is set to "True" and the "PathLenConstraint" field is set to a specific value as needed.
5. keyUsage
   The Subordinate CA certificates have the "keyUsage" extension, which is a critical extension. Usage settings are: DigitalSignature, KeyCertSign, CRLSign.
6. nameConstraints
   This extension is not set for the Subordinate CA certificates.
7. extKeyUsage
   The subordinate CA certificates have the "extKeyUsage" extension, which is a non-critical extension. TrustAsia sets up special subordinate certificates for issuing TLS certificates, code signing certificates, email certificates, time-stamp signing certificates, and document signing certificates (see 1.1.2). Different "extKeyUsage" extension is set according to the different usage of subordinate CA certificate.

The usage of subordinate CA certificate / extKeyUsage	Sub CA cert for issuing time-stampe signing cert	Sub CA cert for issuing (EV) code signing cert	Sub CA cert for issuing TLS cert	Sub CA cert for issuing secure eamil cert	Sub CA cert for issuing document signing cert

Server Authentication 1.3.6.1.5.5.7.3.1	×	×	√	×	×
Client Authentication 1.3.6.1.5.5.7.3.2	×	×	√	√	×
Code Signing 1.3.6.1.5.5.7.3.3	×	√	×	×	×
Secure Email 1.3.6.1.5.5.7.3.4	×	×	×	√	×
Time-Stamping 1.3.6.1.5.5.7.3.8	√	×	×	×	×
PDF Signing 1.2.840.113583.1.1.5	×	×	×	×	√
MS Document Signing 1.3.6.1.4.1.311.10.3.12	×	×	×	√	√

8. authorityKeyIdentifier
   The subordinate CA certificates have the "authorityKeyIdentifie" extension, which is a non-critical extension. This extension contains only the "KeyIdentifier" field.

7.1.2.3 Subscriber Certificate

1. certificatePolicies
   The subscriber certificates have the "CertificatePolicies" extension, which is a non-critical extension. Different policy identifiers are set according to the different usage of subscriber certificates.(see section 1.2)
2. CRLDistributionPoints
   The subscriber certificates have the "CRLDistributionPoints" extension, which is a non-critical extension. This extension will contain the HTTP URL of the CA's CRL service
3. authorityInformationAccess
   The subscriber certificates have the "authorityInformationAccess" extension, which is a non-critical extension. This extension will contain the HTTP URL of the issuing CA's certificate (AccessMethod=1.3.6.1.5.5.7.48.2) and the HTTP URL of the issuing CA's OCSP responder(AccessMethod=1.3.6.1.5.7.48.1)
4. basicConstraints
   The subscriber certificates have the "basicConstraints" extension, which is a critical extension. The "CA" field in this extension is set to "False".
5. keyUsage
   The subscriber certificates have the "keyUsage" extension, which is a critical extension. Different "keyUsage" extension can be set depending on the subscriber certificate usage.

Certificate Type / KeyUsage	TLS Cert	(EV)CS Signing Cert	Secure Email Cert	Time-Stamp Signing Cert	Document Signing Cert
0 Digital Signature	√	√	√	√	√
1 Non Repudiation	×	×	×	×	√
2 Key Encipherment (ECC algorithm has no KU)	√	×	√	×	×
3 Data Encipherment	×	×	×	×	×
4 Key Agreement	×	×	×	×	×

5 Key Cert Sign	×	×	×	×	×
6 CRL Sign	×	×	×	×	×
7 Encipher Only	×	×	×	×	×
8 Decipher Only	×	×	×	×	×

6. extKeyUsage

   The subscriber certificates have the "extKeyUsage" extension, which is a non-critical extension.. Different "extKeyUsage" extension is set according to the different type and usage of subscriber certificate.

Cert Type / extKeyUsage	time-stampe signing cert	code signing cert	Server cert	secure eamil cert	document signing cert
Server Authentication 1.3.6.1.5.5.7.3.1	×	×	√	×	×
Client Authentication 1.3.6.1.5.5.7.3.2	×	×	√	√	×
Code Signing 1.3.6.1.5.5.7.3.3	×	√	×	×	×
Secure Email 1.3.6.1.5.5.7.3.4	×	×	×	√	×
Time-Stamping 1.3.6.1.5.5.7.3.8	√	×	×	×	×
PDF Signing 1.2.840.113583.1.1.5	×	×	×	×	√
MS Document Signing 1.3.6.1.4.1.311.10.3.12	×	×	×	×	√

7. authorityKeyIdentifier

   The subscriber certificates have the "authorityKeyIdentifie" extension, which is a non-critical extension. This extension contains only the "KeyIdentifier" field.

7.1.2.4 All Certificates

All certificates issued by TrustAsia are set in accordance with RFC 5280. The keyUsage, extKeyUsage and other certificate extensions in the certificate comply with the provisions in section 7.1.2.1, 7.1.2.2, 7.1.2.3.

7.1.3 Algorithm Object Identifiers

TrustAsia Certificates are signed using one of the following algorithms:

SHA-256 with RSA	1.2.840.113549.1.1.11
SHA-384 with RSA	1.2.840.113549.1.1.12
SHA-256 with ECDSA	1.2.840.10045.4.3.2
SHA-384 with ECDSA	1.2.840.10045.4.3.3

TrustAsia and Subscribers may generate Key Pairs using the following method:

RSA	1.2.840.113549.1.1.1
ECDSA	1.2.840.10045.2.1

7.1.4 Name Forms

Name of certificate issued by TrustAsia is formatted in accordance with RFC5280 and CA/B Forum Baseline Requirements Section 7.1.4.

7.1.5 Name Constraints

No stipulation

7.1.6 Certificate Policy Object Identifier

See 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

TrustAsia issues CRL regularly for the subscribers to query

7.2.1 Version Number(s)

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

7.2.2 CRL and CRL Entry Extensions

Consistent with ITU X.509 and RFC3280 regulations.

1. CRL version: It refers to version information of CRL, TrustAsia adopts CRL V2 corresponding to X.509 V3 certificate.
2. Signature algorithm: TrustAsia adopts SHA256withRSA, SHA384withRSA, SHA384withECDSA algorithms.
3. Issuer: It refers to DN of issuing authority, including country, province, city, organization, department and common name, etc.
4. Effective time: It refers to date/time which indicates CRL issuing time.
5. Update time: It refers to date/time which indicates next issuing time of CRL. (It's an enforced field in this CPS).
6. Certificate Revocation List: It refers to a list of revoked certificates. The list contains certificate serial number and certificate revocation date and time.
7. Issuer Unique Identifier: It is used to authenticate the public key which is used to verify signature of CRL. It can distinguish different keys used by the same CA.

7.3 OCSP Profile

The OCSP service is provided by the TrustAsia 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.

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

8.1 Frequency or Circumstances of Assessments

TrustAsia conducts the following audits and assessments:

1. TrustAsia 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 conducts an annual operation quality assessment to ensure the reliability, safety and controllability of the operation service.
3. TrustAsia 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/B Forum, TrustAsia carries out BR self-assessment once a year.
5. TrustAsia 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 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 also employs an auunal independent audit firm to conduct external audit and evaluation in accordance with WebTrust's audit specifications for CA.

8.2 Identity/Qualification of Assessor

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

External auditors which TrustAsia 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. Qualified for WebTrust audit.

8.3 Assessor's relationship to Assessed Entity

Segregation of duties is required between the TrustAsia auditors, and the TrustAsia system administrators, business administrators, and business operators.
The external evaluators and TrustAsia 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's audit contents include:

1. Whether operation procedures and processes strictly followed
2. Whether strictly following the CPS, business specifications and security requirements when conducting authentication services
3. Whether all kinds of logs and records are preserved and if there is any question
4. If there's any other potential security risks

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

8.5 Actions taken as a result of deficiency

Audit assessment group monitors responsible departments for improvements and complete status of issues that were mentioned in audit reports.
If assessments of a third-party auditor firm are completed, TrustAsia will rectify in accordance with the audit reports. TrustAsia will be evaluated again after the rectification.

8.6 Communication of Results

Audit results are formally informed to relevant departments of TrustAsia and related RA. TrustAsia will notify the subscribers of any potential security risks timely.
After the assessment from a third-party auditor firm is completed, the final audit report will be provided to TrustAsia. If TrustAsia completes the rectification and reevaluation, the final audit results will be published on the official website.

8.7 Self-Audits

TrustAsia will conduct ongoing self-audits and strictly control the service quality bby performing internal risk asscssment on at least an annual basis and self-consorship sampling on at least a quarterly vasis according to international and domestic relevant standards and the CP&CPS. The self-audti assesses wherther 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 of the sampling 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 can charge subscriber certification fees for digital authentication service provided. TrustAsia may change its fees at anytime in accordance with the applicable customer agreement, market and administration.
If the price specified in TrustAsia agreements with subscribers is different from the one published, the agreement price prevails.

9.1.2 Certificate access Fees

Currently, TrustAsia doesn't charge for inquiry during the certificate validation period. If the subscriber has special requests, which makes TrustAsia to pay extra fees, TrustAsia will interact with the subscriber for appropriate charges.

9.1.3 Revocation or Status information access Fees

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

9.1.4 Fees for Other Services

TrustAsia provides certificate storage media and related services to subscribers. TrustAsia declares the prices of above items in the agreements signed with subscribers or other entities.
Other services fees that TrustAsia may or will charge, will inform the subscribers timely.

9.1.5 Refund Policy

In the event that TrustAsia is unable to perform the Subscriber Contract or use the Subscriber Certificate due to TrustAsia's fault, TrustAsia will reimburse the Subscriber for the cost incurred. In the event that TrustAsia is not the cause, the Subscriber will be required to make a refund, subject to the terms of the Subscriber Agreement.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

TrustAsia provides certificate subscribers with use guarantee. If the user suffers losses in using the certificate due to the reason of TrustAsia, TrustAsia will provide compensation to the certificate subscriber (see section 9.9 of this CP&CPS for details)

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

If TrustAsia violates the provisions of this CPS, certificate subscribers, relying party and other entities can request that TrustAsia shall assume the liability for compensation (except for statutory or contractual exemption). After confirmation, TrustAsia can compensate for the entity. Limitations of compensation are as follows:

1. All the compensation obligation of TrustAsia 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 can reset the compensation maximum amount. TrustAsia will notify relevant parties immediately after the reset.
2. TrustAsia only assumes compensation liabilities when the certificate is valid.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

In the electronic certification service provided by TrustAsia, the following information is treated as confidential information:

1. TrustAsia subscriber's digital signature and decryption key
2. Audit records including local logs, server logs, archive logs information, which is treated by TrustAsia as confidential information. These records can only be accessed by security auditors and business administrators. Unless for law requirements, this information cannot be released outside of the company
3. Other individual and company information preserved by TrustAsia and RA and 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 treats the following information as non-confidential information:

1. Information in the certificate and CRL issued by TrustAsia
2. Information in certificate policy supported by TrustAsia and recognized by CPS
3. Information that is permitted by TrustAsia, only used by TrustAsia subscribers and published at the TrustAsia official website
4. Others: The confidentiality of TrustAsia information depends on particular data items and applications.

9.3.3 Responsibility to Protect Confidential Information

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

9.4.2 Information Treated as Private

TrustAsia considers all personal information of individuals not publicly provided in the relevant certificate or CRL content as private information. TrustAsia uses appropriate safeguards and reasonable care to protect private information.

9.4.3 Information Not Deemed Private

Certificate information held by subscribers and certificate status information are not considered as privacy information.

9.4.4 Responsibility to Protect Private Information

TrustAsia has the responsibility and obligation for proper custody and protection of the certificate applicant personal privacy described in section 9.4.2.

9.4.5 Notice and Consent to Use private Information

TrustAsia takes appropriate steps to protect the certificate subscriber's personal privacy, and takes reliable security measures to protect stored personal privacy information. TrustAsia 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 subscriber, unless base on provisions of the law or government.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

TrustAsia 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 to provide some particular customer support services such as mailing materials, TrustAsia needs to send the subscriber's name, mailing address and other related information to a third-party such as mailing company.

9.5 Intellectual Property Rights

1. TrustAsia reserves and remains full intellectual property rights for all the certificates and software offered by TrustAsia.
2. TrustAsia holds ownership, the right of name, the right to share the benefits for certificate system software.
3. TrustAsia has the right to decide to use which software system.
4. All the information published at TrustAsia website is TrustAsia property. Without written permission of TrustAsia, others cannot repost them for commercial activities.
5. Certificates and CRLs issued by TrustAsia are both the properties controlled by TrustAsia.
6. External operation management strategy and specification are TrustAsia properties.
7. The distinguished name (hereinafter referred to as DN), used to express the TrustAsia domain entity in the directory and the certificate issued to the terminal in the domain entity are the properties of TrustAsia.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

During the process of providing electronic certification service activities, TrustAsia 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 must be in line with all substantive requirements of the CPS;
4. Will not issue certificates that mislead a Relying Party about the certificate information verified by the CA;
5. Informs subcribers any known events, which will fundamentally affect the validity and reliability of the certificate;
6. Revokes the certificate according to this CPS;
7. Verify the applicants' identities according to this CPS;
8. If TrustAsia is not associated with the subscriber,the subscriber and TrustAsia are parties to a legally valid and enforceable subscriber agreement that satisfies the BRs and other requirements published by the CA/Browser Forum, or , if TrustAsia and subscribers are the same entity or are affiliated, the applicant representative acknowledged the terms of use;
9. Maintains 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 guarantees that the subscriber information in the certificate are accurate except the unauthenticated subscriber information.

TrustAsia is not responsible for the assessment of whether a certificate is used within an appropriate scope. Subscriber and relying party ensure the certificate is used for appropriate purposes based on the 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 makes following commitments:

1. The registration process provided for subscribers is compliant with all the substantive requirements of TrustAsia CP&CPS.
2. When generating certificates, TrustAsia 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 in time according to the provisions of CP&CPS.

9.6.3 Subscriber Representations and Warranties

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

1. Acknowledged and accepted all the terms and conditions of TrustAsia "certificate application responsibility" and CP&CPS.
2. The subscribers use digital signatures if the certificate is valid.
3. All information that subscriber provides to registration authority during certificate application process must be true, 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 take jointly responsibility. The subscriber is responsible for notifying TrustAsia and its authorized certification services agencies any false statements and omissions made by the agent.
4. Each signature is generated using the private key corresponding to the public key included in certificate by subscribers themselves. The certificates shall be valid at the moment of singing, i.e. certificate is not revoked or expired. The private key for the certificate is accessed and used by the subscriber itself.
5. Subscribers ensure that they don't engage in business performed by the issuing agency (or similar institutions) unless they sign written agreements with the issuing agency on such matters.
6. Once the certificate is accepted, the subscriber 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. Prohibited for rejecting any statements, changes, updates and upgrades published by TrustASia, including but not limited to modification of strategies and standards as well as additions and deletions of certificated services.
8. The subscribers only uses certificate for the authorized or other lawful purpose within the range specified by this CP&CPS.
9. The subscriber use secure and reasonable measures to prevent the private key from loss, disclosure, alteration and other events.
10. For the SSL/TLS certifcates, the subscribers undertake and obligation and warranty to install the certicates only on servers that are accessible that the accessible at the subjectALTName(s) listed in the certificates.
11. Subscribers of code singing certificates shall promptly request the revocation of their certificates by TrustAsia in case of the following situations: 1) any information in the certificate is or becomes incorrect or inaccurate; 2)there is any misuse or compromise of the subscriber's private key associated with the public key included in the certificate; 3) there is evidence that such code signing certificxates are used to sigh suspicious codes.

9.6.4 Relying party Representations and Warranties

1. Abide by 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 rust the certificate.
4. Before trust a certificate, verify whether the certificate is revoked or not through querying CRL or OCSP.
5. The relying party is willing to compensate TrustAsia 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. Prohibited for rejecting any statements, changes, updates and upgrades published by TrustAsia, 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 abide by all provisions of this CP&CPS.

9.7 Disclaimers of Warranties

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

1. Do not guarantee the statements of certificate subscribers, relying party and other.
2. Do not guarantee any 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 responsibility 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 can exempt from liability.
6. When digital certificates issuing errors, delays, interruptions, inability to issue, or suspension or termination of all or part of certificate services due to technical failures such as TrustAsia's equipments or network failures. The causes of "technical failure" specified in this paragraph include but not limited to: the TrustAsia's equipments or network failures caused by related companies such as power, telecommunication, communication departments, hacker attack.
7. TrustAsia has carefully obey 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, TrustAsia 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 violated statement in CP&CPS section 9.6.1, certificat4e subscribers, relying parties and other entities can request TrustAsia assume compensation liabilities (except for statutory and contractual exeptions). The payoff limit from legal responsibility of direct losses: in any case, the compensation for each server certificate must not exceed 10 times the purchase price of the certificate market. If the following circumstances occure, TrustAsia will assume limited compensation liability:

1. TrustAsia 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, but TrustAsia issues certificates with error information and the error leads to losses of the subscriber or relying party.
3. After TrustAsia knows the fact that subscriber provides fake registration information or data, TrustAsia 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, which leads to the subscriber or relying party suffing losses.
5. TrustAsia fails to revoke certificates in time, which leads to relying party suffering losses.

In addition, TrustAsia's compensation limitations are as follow:

1. All the compensation obligation of TrustAsia shall not exceed the insurance coverage stipulated in section 9.2.1. The maximum amount of compensation can

be reset by TrustAsia based on different situations. TrustAsia will notify related parties immediately after the reset.

2. For the losses caused by subscribers or relying party, TrustAsia does not assume responsibilities. Subscribers or relying themselves should assume their own responsibilities.
3. TrustAsia takes the responsibilities only during the validity of the certificate.

9.9.2 Indemnification by Subscribers

If the following situations cause losses to TrustAsiua or relying party, subscribers shall assume the compensation liability:

1. TrustAsia and its authorized service agencies or third-party suffer losses due to unreal information, such as deliberate, negligent or malicious provision of unreal information, by applying for certificates.
2. TrustAsia 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 and its authorized service agencies or third-party of the leakage and loss of private keys with knowing the facts; and due to handing keys to others inappropriately.
3. Subscribers violate the CP&CPS and related operation practices when using certificates as well as using the certificates activies outside of 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 to this information of certificate revocation published by TrustAsia, if TrustAsia operates in accordance with requirements of the CPS, subscribers must assume any responsibility of looses according to this CP&CPS.
5. Unreal, incomplete or inaccurate information provided by subscribers.
6. Subscribers continue to use the certificates and do not notify TrustAsia and relying parties promptly when information in the certificates is changed.
7. The private key is compromised, damaged, stolen, disclosed, and etc. due to not taking effective protection measures.
8. Subscribers continue to use the certificate and do not notify TrustAsia and relying parties promptly when they are 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 the use of certificates for illegal and criminal activities.

9.9.3 Indemnification by Relying Parties

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

1. Obligations defined in the CP&CPS and agreements between TrustAsia and relying parties are not fulfilled.

2. TrustAsia 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 effect when it is released on TrustAsia's online repository. It will be effective until the new version of CP&CPS released.

9.10.2 Termination

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

9.10.3 Effect of Termination and Survival

After the termination of this CPS, its effect will be terminated at the same time, but 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 CPS, as well as limited liability clauses relating to indemnification, and are still valid after this CP&CPS is terminated.
When some provisions in CPS, subscriber agreements, relying party agreements and other agreements become invalid due to some reason, 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, TrustAsia will notify individual subscribers and relying parties by email or other ways, when TrustAsia revoking the certificates, discovering the other usage of certificates by subscribers and other behaviors against the subscriber agreement.

9.12 Amendents

9.12.1 Prodedure for Amendment

As authorized by TrustAsia 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 actural needs of certification business operations.

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

9.12.2 Notification Mechanism and Period

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

9.12.3 Circumstances under which OID Must Be Changed

The TrustAsia 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 Changes

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

9.13 Dispute Resolution Provisions

If TrustAsia, certificate subscribers, relying parties and other entities have disputes in the electronic certification activities, should solve through amicable negotiation according to the agreement. If coordination fails, these parties should reach out to the legal authorities. Any prosecutions against TrustAsia over any disputes arising from this CP&CPS should be governed by the people's court in the place where TrustAsia is registered.

9.14 Governing Law

The CP&CPS of TrustAsia 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 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 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'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 placed at the TrustAsia official website for brosing.

9.16.2 Assignment

TrustAsia 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.

9.16.3 Serverability

If any provisions of this CP&CPS are held invalid or unenforceable by a competent court or tribunal, the remainder of the CP&CPS will remain valid and enforceable. Each provision of this CP&CPS that provides for a limitation of liability, disclaimer of a warranty, or an exclusion of damages is severable and independent of any other provision.

9.16.4 Enforcement

TrustAsia declare that if an entity such as a certificate subscriber or relying party fails to implement a provision in this CPS, it is not considered that the entity will not implement that or other provision 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 CPS, then TrustAsia will not be responsible for such incidents.

9.17 Other Provisions

TrustAsia has final interpretation rights to this CP&CPS.

10. Appendix A - Validation Requirements

10.1 Validation items and requirements

TrustAsia requires the following 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 CPS section 3.2.2.9.
Organizational Validation	• Verify the city of the state province in which the organization operates. • Verify that the organization is legally existing and operating. • Verify telephone numbers, fax numbers, email addresses or postal delivery addresses as verified means of communication for the organization. Comply with CP&CPS section 3.2.2.1 and BR requirements.
Extended Validation	• Verify that the applicant has the ability to participate in the business by verifying the operational presence of the applicant, or co-signer, parent or subsidiary. The validation is performed by： • Verifying the type of applicant and must be one of the following: private organization, government entity, business entity, non-commercial entity. • Verifying the applicant's registered address and registration code through a reliable databank published by TrustAsia • Verify that the applicant, affiliate, parent company or subsidiary has been in existence for at least 3 years based on the records of the registration or registration authority. • Verifying that the applicant, co-signer, parent or subsidiary is listed in QIIS or QTIS. • Verify that the applicant, affiliate, parent or subsidiary has an active current financial account with the financial institution by receiving confirmatory documentation from the regulated financial institution regarding the applicant, affiliate, parent or subsidiary; or • Verify through a verified legal opinion letter that the applicant has a valid current deposit account with the regulated financial institution. • Comply with EV-Guidelines requirements.

IndividuaI Identity Validation	• Verify individual identity according to CP&CPS section 3.2.3.
Operator Validation	• Verify the name and title of the certificate application operator (if applicable), 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 application operator.
Approver Validation	• Verify the name and title of the certificate application approver, as well as verify that it is the applicant's agent._ • Verify by contacting the certificate application approver that the certificate application operator has explicit authorization from the applicant to enter into a subscriber agreement (or other relevant contractual responsibility) on behalf of the applicant and the authority to be authorized to submit the certificate application._ • Comply with EV-Guidelines requirements.
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 request manager, certificate request approver, or applicant's jurisdiction of 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 individual_ • 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, 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 TLS	OV TLS	EV TLS	Code Signing	EV Code Signing	Document Signing	Class 1 S/MIME	Class 2 S/MIME
CSR Validation	Y	Y	Y	Y	Y	Y	Y	Y
Domain/IP validation	Y	Y	Y	N	N	N	N	N
CAA Validation	Y	Y	Y	N	N	N	N	N
Email Address Validation	N	N	N	N	N	N	Y	Y
Organizational Validation	N	Y	Y	Y	Y	Y	N	Y
Extended Validation	N	N	Y	N	Y	N	N	N
Individual Identity Validation	N	N	N	N	N	N	N	Y
Operator Validation	N	Y	Y	Y	Y	Y	N	Y
Approver Validation	N	N	Y	N	Y	N	N	N
High risk validation	Y	Y	Y	Y	Y	Y	Y	Y
Lawyer Identity Validation [1]	N	O	O	O	O	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