ZoTrus Technology Limited
301C, Block C, Building 2, Software Industrial Base, Hi-Tech Park,
Nanshan District, Shenzhen 518057, China
Tel: +86-755-2660 4080 Email: cps@zotrus.com

ZoTrus

Certificates Policy & Practice Statement

Version: 1.1

Status: Final Approved

Release Date：2022-06-28

Effective Date：2022-06-28

Updated Date: 2023-08-23

ZoTrus Technology Limited
301C, Block C, Building 2, Software Industrial Base, Hi-Tech Park,
Nanshan District, Shenzhen 518057, China
Tel: +86-755-2660 4080 Email: cps@zotrus.com

TABLE OF CONTENTS

1. Introduction

1.1 Overview

This document is the ZoTrus Certificate Policy (CP) & Certification Practice Statement (CPS) that outlines the legal, commercial, and technical principles and practices that ZoTrus employ in providing certification services that include, but are not limited to, approving, issuing, using, and managing of Digital Certificates and in maintaining a X.509 Certificate based Public Key Infrastructure (PKIX) in accordance with this Certificate Policies determined by ZoTrus. It also defines the underlying certification processes for Subscribers and describes ZoTrus' repository operations. The CPS is also a means of notification of roles and responsibilities for parties involved in Certificate based practices within the ZoTrus PKI.

For RSA/ECC algorithm certificates, TLS/SSL Certificates conforms to the current version of the Baseline Requirements (BR) and EV Guidelines (EVG). Code Signing Certificates conforms to the Code Signing BR. In the event of any inconsistency between this CPS and the other documents specified in this paragraph, those documents take precedence over this CPS. For the issuance of other certificate types, ZoTrus relies on the industry best practices and other standards.

For SM2 algorithm certificates, TLS/SSL Certificates conforms to GM/T 0024 and GB/T 38636 and refers to the current version of the Baseline Requirements (BR) and EV Guidelines (EVG). Code Signing Certificates refers to the Code Signing BR. In the event of any inconsistency between this CPS and the other documents specified in this paragraph, those documents take precedence over this CPS. For the issuance of other certificate types, ZoTrus relies on the industry best practices and other standards.

In case multiple or alternative methods or options are possible by the baseline requirements or guidelines in order to perform a certain task and/or multiple or alternative methods or options are offered in order to comply to those requirements and guidelines, ZoTrus reserves the right to choose any of the methods or options applicable at any times and may choose to change its procedures at all times and decide to do so on a case-to-case basis.

In pursuant to the IETF PKIX RFC 3647 CP/CPS framework, this document is divided into nine parts that cover the security controls and practices and procedures for certificate and timestamping services within the ZoTrus PKI. To preserve the outline specified by RFC 3647, sections that do not apply have the statement "Not applicable" or "No stipulation."

ZoTrus may publish additional certificate policies or certification practice statements as necessary to describe other product and service offerings. These supplemental policies and

statements are available to applicable users or relying parties through the online repositories. This CPS, related agreements referenced within this document are available online at www.zotrus.com/policy.

1.2 Document Name and Identification

This document is the ZoTrus Certificate Policy (CP) & Certification Practice Statement (CPS). It is also a means of notification of roles and responsibilities for parties involved in Certificate based practices within the ZoTrus PKI.

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

For RSA/ECC algorithm certificates OIDs found in Certificates reliant upon CAB Forum requirements and guidelines include the designated reserved policy identifiers in the Certificate Policy extension as specified in section 7.1.6 of the CAB Forum Baseline Requirements.

For SM2 algorithm certificates OID found in Certificates reliant the related GM and GB standards, and the SM2 certificate type and validation level OID found in Certificate reliant upon ZoTrus Trusted Root Program and related document.

1.2.1 Revisions

Ver.	Description	Adopted	Effective
1.0	Version 1.0 of the Certificate Practice Statement Adopted	2022.06.28	2022.06.28
1.1	Update office address, small change for some sentences	2023.08.23	2023.08.23

1.3 PKI Participants

1.3.1. Certification Authorities

In its role as a CA, ZoTrus provides Certificate services within the ZoTrus PKI. ZoTrus will:
• Conform its operations to the CPS (or other CA business practices disclosure), as the same may from time to time be modified by amendments published in the Repository,

• Issue and publish Certificates in a timely manner in accordance with the issuance times set out in this CPS,

• Upon receipt of a valid request to revoke the Certificate from a person authorized to request revocation using the revocation methods detailed in this CPS, revoke a Certificate issued for use within the ZoTrus PKI,

• Publish CRLs on a regular basis, in accordance with the applicable Certificate Policy and with provisions described in this CPS,

• Distribute issued Certificates in accordance with the methods detailed in this CPS,

• Update CRLs in a timely manner as detailed in this CPS,

• Notify Subscribers via email of the imminent expiry of their ZoTrus issued Certificate (for a period disclosed in this CPS).

1.3.2. Registration Authorities

Not applicable.

1.3.3. Subscribers

Subscribers of ZoTrus services are individuals or organizations that use PKI in relation with ZoTrus supported transactions and communications. Subscribers are parties that are identified in a certificate and hold the Private Key corresponding to the Public Key listed in the certificate. Prior to verification of identity and issuance of a certificate, a subscriber is an Applicant for the services of ZoTrus. Each Subscriber must agree the Subscriber Agreement with ZoTrus in related online page.

1.3.4. Relying Parties

Relying parties use PKI services in relation with ZoTrus certificates and reasonably rely on such certificates and/or digital signatures verifiable with reference to a Public Key listed in a subscriber certificate.

To verify the validity of a digital Certificate they receive, Relying Parties must refer to the CRL prior to relying on information featured in a Certificate to ensure that ZoTrus has not revoked the Certificate. The CRL location is detailed within the Certificate.

1.3.5. Other Participants

Not applicable.

1.4 Certificate Usage

1.4.1. Appropriate Certificate Uses

By accepting a certificate from ZoTrus, the subscriber agrees to the rules and regulations outlined in this policy and any accompanied agreement or document. The certificate shall be used lawfully in accordance with the terms of this document and relevant policies. Certificate usage must be consistent with the Key Usage field extensions included in the certificate (e.g., if a digital signature is not enabled then the certificate must not be used for signing). Subscribers shall protect their Private Keys from unauthorized use and shall discontinue use of the Private Key following expiration or revocation of the certificate.

Subscribers are notified hereby that electronic signatures can be legally binding. The extent to which they are trusted depends on local legislation. That means that legislation will decide on a case-by-case base whether they are legally binding. Because of these legal implications, subscribers must protect their Private Keys.

Renewing a certificate follows the same procedures as with a new certificate. Re-keying or reusing the same Private Key for any new or renewed certificate shall be avoided by the subscriber.

1.4.1.1. Certificate Types

TLS/SSL Certificates are typically used by server software for the identification of the server operator and the encrypting of sensitive information during its exposure at the networks.

Code Signing Certificates are typically used to sign software objects, macros, device drivers, firmware images, configuration files or mobile applications.

Document Signing Certificates are typically used to sign PDF documents or OFD documents.

S/MIME Certificates are typically used for signing and encryption of email. They are also referred to as email certificate and may be applicable for one or more purposes mentioned above depending on the key usage limit specified in the certificate.

Client Certificates are typically used for client authentication purpose.

IoT Certificates are typically used for IoT device authentication purpose, signing and encryption of IoT communication.

Time Stamping Certificates are used to ensure that the signing event took place at a

specific point in time.

Intermediate CA Certificates are used exclusively for the issuing and signing of end user certificates and Certificate Revocation Lists. Each CA certificate is responsible for the signing of a different validation level and different purpose.

CA Root Certificate is used to exclusively sign and issue the intermediate CA certificates and corresponding Certificate Revocation List.

1.4.1.2. Certificate Validation Level

T1 Validation Level Certificate provides modest assurances that the email originated from a sender with the specified email address or that the domain address belongs to the respective server IP address. These certificates provide no proof of the identity of the subscriber or of the organization. For email certificate and document signing certificate, it is a Mailbox-validated certificate. For SSL certificate, it is a domain-validated(DV) SSL certificate. In some document, this level certificate is named as Class 1 certificate.

T2 Validation Level Certificate provides medium assurances about the subscriber's identity and subscribers must prove their identity by various means, this level certificate is for individual only. In some document, this level certificate is named as Class 2 certificate.

T3 Validation Level Certificate provides a high level of assurance about the subscriber's identity in comparison with T1 and T2 certificates and are issued only to organizations to which the ZoTrus has verified its identity. In some document, this level certificate is named as Class 3 certificate.

T4 Validation Level Certificate, for email certificate and document signing certificate, it is sponsor-validated certificate, it provides an extended validation of high-level assurance about the subscriber's identity and its sponsor(organization) identity. For SSL Certificates, it is Extended Validation, the validation procedures and requirements of the Extended Validation Guidelines as published by the CA/Browser Forum.

1.4.2. Prohibited Certificate Uses

Certificates issued under the provisions of this CPS may not be used for: (i) any application requiring failsafe performance such as: (a) the operation of nuclear power facilities, (b) air traffic control systems, (c) aircraft navigation systems, (d) weapons control systems, or (e) any other system whose failure could lead to injury, death or environmental damage; or (ii) transactions where applicable law prohibits the use of encryption or digital certificates for such transactions or where otherwise prohibited by law.

T1 Validated Certificate including DV SSL Certificate, MV Email Certificate and MV Document Signing Certificate are not for use as a means of providing identity assurance.

1.5 Policy Administration

1.5.1. Organization Administering the Document

This CPS and the documents referenced herein are maintained by the ZoTrus Certificate Policy Authority (ZCPA).

1.5.2. Contact Person

The ZoTrus Policy Authority may be contacted at the following address:

Attn: Legal Counsel
ZoTrus Policy Authority
301C, Block C, Building 2, Software Industrial Base, Hi-Tech Park, Nanshan District, Shenzhen 518057, China
website: www.zotrus.com
Email: cps@zotrus.com

1.5.3. Person Determining CPS Suitability for the Policy

The ZCPA is responsible for determining the suitability of certificate policies illustrated within the CPS. The Authority is also responsible for determining the suitability of proposed changes to the CPS prior to the publication of an amended edition.

1.5.4. CPS Approval Procedures

The ZCPA approves the CPS and any amendments. Upon the ZCPA accepting such changes deemed by the CA's Policy Authority to have significant impact on the users of this CPS an updated edition of the CPS will be published at the ZoTrus repository (available at www.zotrus.com/policy). And controls are in place to reasonably ensure that the ZoTrus CPS is not amended and published without the prior authorization of the Certificate Policy Authority.

1.6 Definitions and Acronyms

All other definitions and acronyms are according to the Baseline Requirements and Extended

Validation Guidelines published at the CA/Browser Forum and related China GM and GB standard.

1.6.1. Definitions

Adobe Approved Trust List (AATL): A document signing certificate authority trust store created by the Adobe Root CA policy authority implemented from Adobe PDF Reader.

Affiliate: A corporation, partnership, joint venture, or other entity controlling, controlled by, or under common control with another entity, or an agency, department, political subdivision, or any entity operating under the direct control of a Government Entity.

Applicant: The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Applicant is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual certificate request.

Applicant Representative: A natural person or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant: (i) who signs and submits, or approves a certificate request on behalf of the Applicant, and/or (ii) who signs and submits a Subscriber Agreement on behalf of the Applicant, and/or (iii) who acknowledges the Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA or is the CA.

Application Software Supplier: A supplier of Internet browser software or other relying-party application software that displays or uses Certificates and incorporates Root Certificates.

Attestation Letter: A letter attesting that Subject Information is correct written by an accountant, lawyer, government official, or other reliable third party customarily relied upon for such information.

Audit Period: In a period-of-time audit, the period between the first day (start) and the last day of operations (end) covered by the auditors in their engagement. (This is not the same as the period of time when the auditors are on-site at the CA.) The coverage rules and maximum length of audit periods are defined in section 8.1.

Audit Report: A report from a Qualified Auditor stating the Qualified Auditor's opinion on whether an entity's processes and controls comply with the mandatory provisions of these Requirements.

Authorization Domain Name: The Domain Name used to obtain authorization for certificate issuance for a given FQDN. The CA may use the FQDN returned from a DNS CNAME lookup as the FQDN for the purposes of domain validation. If the FQDN contains a wildcard character,

then the CA MUST remove all wildcard labels from the left most portion of requested FQDN. The CA may prune zero or more labels from left to right until encountering a Base Domain Name and may use any one of the intermediate values for the purpose of domain validation.

Authorized Ports: One of the following ports: 80 (http), 443 (http), 25 (smtp), 22 (ssh).

Base Domain Name: The portion of an applied-for FQDN that is the first Domain Name node left of a registry-controlled or public suffix plus the registry-controlled or public suffix (e.g. "example.co.uk" or "example.com"). For FQDNs where the right-most Domain Name node is a gTLD having ICANN Specification 13 in its registry agreement, the gTLD itself may be used as the Base Domain Name.

Business Entity: Any entity that is not a Private Organization, Government Entity, or non-commercial entity as defined in the EV Guidelines. Examples include, but are not limited to, general partnerships, unincorporated associations, sole proprietorships, etc.

CAA: From RFC 6844 (http:tools.ietf.org/html/rfc6844): "The Certification Authority Authorization (CAA) DNS Resource Record allows a DNS Domain Name holder to specify the Certification Authorities (CAs) authorized to issue certificates for that domain. Publication of CAA Resource Records allows a public Certification Authority to implement additional controls to reduce the risk of unintended certificate mis-issue."

Certificate: An electronic document that uses a digital signature to bind a Public Key and an identity.

Certificate Data: Certificate requests and data related thereto (whether obtained from the Applicant or otherwise) in the CA's possession or control or to which the CA has access.

Certificate Management Process: Processes, practices, and procedures associated with the use of keys, software, and hardware, by which the CA verifies Certificate Data, issues Certificates, maintains a Repository, and revokes Certificates.

Certificate Policy: A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements.

Certificate Problem Report: Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.

Certificate Revocation List: A regularly updated time-stamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates.

Certificate System: A system used by a CA or Delegated Third Party to process, approve issuance of, or store certificates or certificate status information, including the database,

database server, and storage.

Certificate System Component: A individual element of a larger Certificate System used to process, approve issuance of, or store certificates or certificate status information. This includes the database, database server, storage devices, certificate hosting services, registration authority systems, and any other element used in certificate management.

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.

Certification Practice Statement: One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.

Certificate Transparency (CT): An Internet security standard for monitoring and auditing the issuance of digital certificates. The standard creates a system of public logs that seek to eventually record all TLS/SSL certificates issued by publicly trusted certificate authorities, allowing efficient identification of mistakenly or maliciously issued certificates.

Control: "Control" (and its correlative meanings, "controlled by" and "under common control with") means possession, directly or indirectly, of the power to: (1) direct the management, personnel, finances, or plans of such entity; (2) control the election of a majority of the directors ; or (3) vote that portion of voting shares required for "control" under the law of the entity's Jurisdiction of Incorporation or Registration but in no case less than 10%.

Country: Either a member of the United Nations OR a geographic region recognized as a Sovereign State by at least two UN member nations.

Cross Certificate: A certificate that is used to establish a trust relationship between two Root CAs.

CSPRNG: A random number generator intended for use in cryptographic system.

Delegated Third Party: A natural person or Legal Entity that is not the CA but is authorized by the CA to assist in the Certificate Management Process by performing or fulfilling one or more of the CA requirements found herein.

Digital Signature: To encode a message by using an asymmetric cryptosystem and a hash function such that a person having the initial message and the signer's Public Key can accurately determine whether the transformation was created using the Private Key that corresponds to the signer's Public Key and whether the initial message has been altered since the transformation was made.

Domain Authorization Document: Documentation provided by, or a CA's documentation of a communication with, a Domain Name Registrar, the Domain Name Registrant, or the person or entity listed in WHOIS as the Domain Name Registrant (including any private, anonymous, or proxy registration service) attesting to the authority of an Applicant to request a Certificate for a specific Domain Namespace.

Domain Contact: The Domain Name Registrant, technical contact, or administrative contract (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA record.

Domain Name: The label assigned to a node in the Domain Name System.

Domain Namespace: The set of all possible Domain Names that are subordinate to a single node in the Domain Name System.

Domain Name Registrant: Sometimes referred to as the "owner" of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the "Registrant" by WHOIS or the Domain Name Registrar.

Domain Name Registrar: A person or entity that registers Domain Names under the auspices of or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN), (ii) a national Domain Name authority/registry, or (iii) a Network Information Center (including their Affiliates, contractors, delegates, successors, or assigns).

Enterprise RA: An employee or agent of an organization unaffiliated with the CA who authorizes issuance of Certificates to that organization.

Expiry Date: The "Not After" date in a Certificate that defines the end of a Certificate's Validity Period.

Fully-Qualified Domain Name: A Domain Name that includes the labels of all superior nodes in the Internet Domain Name System.

Government Entity: A government-operated Legal Entity, agency, department, ministry, branch, or similar element of the government of a country, or political subdivision within such country (such as a state, province, city, county, etc.).

Hardware Security Module (HSM): An HSM is type of secure crypto processor targeted at managing digital keys, accelerating crypto processes in terms of digital signings/second and for providing strong authentication to access critical keys for server applications.

High Risk Certificate Request: A Request that the CA flags for additional scrutiny by reference

to internal criteria and databases maintained by the CA, which may include names at higher risk for phishing or other fraudulent usage, names contained in previously rejected certificate requests or revoked Certificates, names listed on the Miller Smiles phishing list or the Google Safe Browsing list, or names that the CA identifies using its own risk-mitigation criteria.

Internal Name: A string of characters (not an IP address) in a Common Name or Subject Alternative Name field of a Certificate that cannot be verified as globally unique within the public DNS at the time of certificate issuance because it does not end with a Top Level Domain registered in IANA's Root Zone Database.

High Security Zone: An area (physical or logical) protected by physical and logical controls that appropriately protect the confidentiality, integrity, and availability of the CA's or Delegated Third Party Private Key or cryptographic hardware.

Issuing CA: In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA.

Key Compromise: A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, an unauthorized person has had access to it, or there exists a practical technique by which an unauthorized person may discover its value. A Private Key is also considered compromised if methods have been developed that can easily calculate it based on the Public Key (such as a Debian weak key, see http://wiki.debian.org/SSLkeys) or if there is clear evidence that the specific method used to generate the Private Key was flawed.

Key Generation Script: A documented plan of procedures for the generation of a CA Key Pair.

Key Pair: The Private Key and its associated Public Key.

Legal Entity: An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country's legal system.

Object Identifier: A unique alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object class.

OCSP Responder: An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol.

Online Certificate Status Protocol: An online Certificate-checking protocol that enables relying-party application software to determine the status of an identified Certificate. See also OCSP Responder.

Parent Company: A company that Controls a Subsidiary Company.

Private Key: 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: 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.

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.

Publicly Trusted Certificate: A Certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely-available application software.

Qualified Auditor: A natural person or Legal Entity that meets the requirements of Section 8.3.

Qualified Government Information Source: A database maintained by a Government Entity.

Qualified Government Tax Information Source: A Qualified Governmental Information Source that specifically contains tax information relating to Private Organizations, Business Entities, or Individuals.

Qualified Independent Information Source: A regularly updated and current, publicly available, database designed for the purpose of accurately providing the information for which it is consulted, and which is generally recognized as a dependable source of such information.

Random Value: A value specified by a CA to the Applicant that exhibits at least 112 bits of entropy.

Registered Domain Name: A Domain Name that has been registered with a Domain Name Registrar.

Registration Authority (RA): Any Legal Entity that is responsible for identification and authentication of Subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA may assist in the certificate application process or revocation process or both. When "RA" is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.

Reliable Data Source: An identification document or source of data used to verify Subject Identity Information that is generally recognized among commercial enterprises and governments as reliable, and which was created by a third party for a purpose other than the Applicant obtaining a Certificate.

Reliable Method of Communication: A method of communication, such as a postal/courier delivery address, telephone number, or email address, that was verified using a source other than the Applicant Representative.

Relying Party: Any natural person or Legal Entity that relies on a Valid Certificate. An Application Software Supplier is not considered a Relying Party when software distributed by such supplier merely displays information relating to a Certificate.

Relying Party Agreement: The Relying Party Agreement is an agreement that must be read and accepted by a Relying Party prior to validating, relying on or using a Certificate and is available for reference at https://www.zotrus.com/CPS/relying_party.htm.

Repository: An online database containing publicly disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information (CRL).

Request Token: A value derived in a method specified by the CA which binds this demonstration of control to the certificate request.

- The Request Token SHALL incorporate the key used in the certificate request.
- A Request Token MAY include a timestamp to indicate when it was created.
- A Request Token MAY include other information to ensure its uniqueness.
- A Request Token that includes a timestamp SHALL remain valid for no more than 30 days from the time of creation.
- A Request Token that includes a timestamp SHALL be treated as invalid if its timestamp is in the future.
- A Request Token that does not include a timestamp is valid for a single use and the CA SHALL NOT re-use it for a subsequent validation.

The binding SHALL use a digital signature algorithm or a cryptographic hash algorithm at least as strong as that to be used in signing the certificate request.

Required Website Content: Either a Random Value or a Request Token, together with additional information that uniquely identifies the Subscriber, as specified by the CA.

Requirements: The Baseline Requirements found in this document.

Reserved IP Address: An IPv4 or IPv6 address that the IANA has marked as reserved:

http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml
http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml

Root CA: The top-level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.

Root Certificate: The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.

Secure Zone: An area (physical or logical) protected by physical and logical controls that appropriately protect the confidentiality, integrity, and availability of Certificate Systems.

Security Support Systems: A system used to provide security support functions, such as authentication, network boundary control, audit logging, audit log reduction and analysis, vulnerability scanning, and anti-virus.

Signed Certificate Timestamp (SCT): A timestamp and promise from a Certificate Transparency operator to add the submitted precertificate to the log within a specified time period, the signing algorithm is ECC algorithm.

SM2 Algorithm: A set of public key cryptographic algorithms based on elliptic curves, the algorithms parameters are published by China State Cryptography Administration Office, it includes SM2 algorithm for key exchange, SM3 algorithm for message authentication and SM4 algorithm for encryption.

SM2 Browser: A browser that supports SM2 algorithm and SM2 SSL certificate.

SM2 Certificates: The X.509 certificates that use SM2 algorithm including SM2 SSL Certificate, SM2 Code Signing Certificate, SM2 Email Certificate, SM2 Document Signing Certificate etc.

SM2 Certificate Transparency: A Certificate Transparency mechanism for SM2 SSL certificate including SM2 Certificate Transparency Log system using SM2 algorithm to generate the CT log key and sign the SCT data.

SM2 Signed Certificate Timestamp (SM2 SCT): A timestamp and promise from a SM2 Certificate Transparency operator to add the submitted precertificate to the log within a specified time period, the signing algorithm is SM2 algorithm.

Sovereign State: A state or country that administers its own government, and is not dependent upon, or Subject to, another power.

Subject: The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation

of the Subscriber.

Subject Identity Information: Information that identifies the Certificate Subject. Subject Identity Information does not include a Domain Name listed in the subject AltName extension or the subject commonName field.

Subordinate CA: A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.

Subscriber: A natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement or Terms of Use.

Subscriber Agreement: An agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties.

Subsidiary Company: A company that is controlled by a Parent Company.

Technically Constrained Subordinate CA Certificate: A Subordinate CA certificate which uses a combination of Extended Key Usage settings and Name Constraint settings to limit the scope within which the Subordinate CA Certificate may issue Subscriber or additional Subordinate CA Certificates.

Terms of Use: Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with these Requirements when the Applicant/Subscriber is an Affiliate of the CA or is the CA.

Trusted Platform Module (TPM): A hardware cryptographic device which is defined by the Trusted Computing Group. https://www.trustedcomputinggroup.org/specs/TPM.

Test Certificate: A Certificate with a maximum Validity Period of 30 days and which: (i) includes a critical extension with the specified Test Certificate CABF OID (2.23.140.2.1), or (ii) is issued under a CA where there are no certificate paths/chains to a Root Certificate Subject to these Requirements.

Trustworthy System: Computer hardware, software, and procedures that are: reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy.

Unregistered Domain Name: A Domain Name that is not a Registered Domain Name.

Valid Certificate: A Certificate that passes the validation procedure specified in RFC 5280.

Validation Specialists: Someone who performs the information verification duties specified by these Requirements.

Validity Period: The period of time measured from the date when the Certificate is issued until the Expiry Date.

WebTrust Program for CAs: The then-current version of the AICPA/CICA WebTrust Program for Certification Authorities.

WebTrust Seal of Assurance: An affirmation of compliance resulting from the WebTrust Program for CAs.

Wildcard Certificate: A Certificate containing an asterisk (*) in the left-most position of any of the Subject Fully-Qualified Domain Names contained in the Certificate.

Wildcard Domain Name: A Domain Name consisting of a single asterisk character followed by a single full stop character ("*.") followed by a Fully-Qualified Domain Name.

Zone: A subset of Certificate Systems created by the logical or physical partitioning of systems from other Certificate Systems.

X.509: The standard of the ITU-T (International Telecommunications Union-T) for Certificates.

1.6.2. Acronyms

AICPA	American Institute of Certified Public Accountants
API	Application Programming Interface
CA	Certification Authority
CAA	Certification Authority authorization
ccTLD	Country Code Top-Level Domain
CICA	Canadian Institute of Chartered accountants
CP	Certificate Policy
CPS	Certification Practice statement
CRL	Certificate Revocation List
DBA	Doing Business As
DNS	Domain Name system
EKU	Extended Key Usage
EV	Extended Validation
FIPS	(US Government) Federal Information Processing tandard
FQDN	Fully-Qualified Domain Name
IM	Instant Messaging
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and numbers

ISO	International Organization for Standardization
NIST	(US Government) National Institute of Standards and technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
QGIS	Qualified Government Information Source
QGTIS	Qualified Government Tax Information source
QIIS	Qualified Independent Information Source
RA	Registration Authority
RFC	Request for Comments
S/MIME	Secure MIME (Multipurpose Internet Mail Extensions) SSL Secure Sockets Layer
TLD	Top-Level Domain
TLS	Transport Layer Security
VOIP	Voice Over Internet Protocol

1.6.3 Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in these Requirements shall be interpreted in accordance with RFC 2119.

2.Publication and Repository Responsibilities

2.1 Repositories

ZoTrus publishes a repository of legal notices regarding its PKI services, including this CPS, certificates, CRLS, agreements and notices, references within this CPS as well as any other information it considers essential to its services. The ZoTrus legal repository may be accessed at www.zotrus.com/policy.

2.2 Publication of Certification Information

ZoTrus manages and makes publicly available directories of revoked certificates using Certificate Revocation Lists (CRLs). All CRLs issued by ZoTrus are X.509 v2 CRLs, in particular as profiled in RFC3280. Users and relying parties are strongly urged to consult the directories of revoked certificates at all times prior to relying on information featured in a certificate. The CRL distribution points are included in the certificates.

2.3 Time or Frequency of Publication

CA Certificates are published in a repository as soon as possible after issuance. ZoTrus updates and publishes a new CRL every 7 days or whenever a CA Certificate is revoked. The CRL of root and intermediate CA certificates may be valid for one year and shall be updated accordingly.

The last CRL of issuer certificates which reach end-of-life (expired) shall remain published available for a period of 365 days. Such last CRL shall be archived with other related records of the expired issuer certificate.

New or modified versions of the CP/CPS, Subscriber Agreements, or Relying Party Warranties are typically published within seven days after their approval.

This CPS is updated at least once every year. Even if no other changes are made to the contents of this CPS, ZoTrus will increment the version number and update the release date, effective date, and the revision records of this CPS.

2.4 Access Controls on Repositories

Read-only access to the repository is unrestricted. Logical and physical controls prevent unauthorized write access to repositories.

2.5 Accuracy of Information

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

3. Identification and Authentication

3.1 Naming

3.1.1. Type of Names

ZoTrus Certificates are issued with Subject DNs (Distinguished Names) which meet the requirements of X.500 naming, RFC-822 naming and X.400 naming. CNs (Common Names) respect name space uniqueness and are not misleading. However, some Certificates

Common Names may also include RFC2460 (IP version 6) or RFC791 (IP version 4) addresses.

Wildcard SSL Certificates include a wildcard asterisk character as the first character in a CN or SAN. Before issuing a Certificate with a wildcard character (*) in the CN or SAN, ZoTrus follows best practices to determine if the wildcard character occurs in the first label position to the left of a "registry-controlled" label or "public suffix". (e.g. "*.com", "*.co.uk", see RFC 6454 Section 8.2 for further explanation.) and, if it does, it will reject the request if that Domain Namespace is not owned or controlled by the Subscriber.

3.1.2. Need for Names to be Meaningful

ZoTrus uses distinguished names that identify both the entity (i.e., person, organization, device, or object) that is the Subject of the Certificate and the entity that is the issuer of the Certificate.

3.1.3. Anonymity or Pseudonymity of Subscribers

Generally, ZoTrus does not issue anonymous or pseudonymous Certificates; however, for IDNs, ZoTrus may include the Punycode version of the IDN as a Subject name. ZoTrus may also issue other pseudonymous end-entity certificates if they are allowed by policy and any applicable name space uniqueness requirements are met.

3.1.4. Rules for Interpreting Various Name Forms

Distinguished Names in Certificates shall be interpreted using X.500 standards and ASN.1 syntax. See RFC 2253 and RFC 2616 for further information on how X.500 distinguished names in certificates are interpreted as Uniform Resource Identifiers and HTTP references.

3.1.5. Uniqueness of Names

Name uniqueness is ensured through the use of either the Common Name attribute of the Subject Field for server certificates, the emailAddress attribute of the Subject Field for S/MIME certificates and the Common Name and Organization attribute of the Subject Field for code signing certificates.

3.1.6. Recognition, Authentication, and Role of Trademarks

ZoTrus performs sanity and fraud prevention checks in order to limit accidental issuing of certificates whose domain or organization names might be misleading and/or might be used to perform an act of fraud, identity theft or infringement of trademarks.

Subscribers may not request Certificates with any content that infringes the intellectual property rights of a third party. ZoTrus does not require that an Applicant's right to use a trademark be verified. ZoTrus reserves the right to revoke any Certificate that is involved in a dispute.

3.2 Initial Identity Validation

ZoTrus may perform identification of the Applicant or for services including CA chaining services using any legal means of communication or investigation necessary to identify the Legal Entity or individual. ZoTrus may refuse to issue a Certificate in its sole discretion.

3.2.1. Method to Prove Possession of Private Key

Subscribers must prove possession of the Private Key corresponding to the Public Key being registered either as a Certificate Signing Request (CSR) in PKCS#10 format or as a Signed Public Key and Challenge (SPKAC).

3.2.2. Authentication of Organization Identity and Domain Identity

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

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

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

- Subscriber Agreement, signed (if applying out of bands)

3.2.2.1. Domain and IP Address Verification

3.2.2.1.1. Domain Verification

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

1. Email, Fax, SMS, or Postal Mail to Domain Contact as defined in section 3.2.2.4.2 of the Baseline Requirements.
   Communicating directly with the Domain Name Registrant using a postal address, email address, or telephone number provided by the Domain Name Registrar.
   Confirming the Applicant's control over the FQDN by sending a Random Value via email, fax, SMS, or postal mail to a recipient identified as a Domain Contact and then receiving a confirming response utilizing the Random Value. The Random Value, which is unique, is generated by ZoTrus and remains valid for use in a confirming response for no more than 30 days from its generation.

2. Constructed email to domain contact as defined in section 3.2.2.4.4 of the Baseline Requirements.
   Communicating directly with the Domain Contact confirming the Applicant's control over the requested FQDN using a constructed email address by:
   (1) sending an email to one or more addresses created by using 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the at-sign ("@"), followed by an Authorization Domain Name,
   (2) including a Random Value in the email, and
   (3) having the Applicant submit (by clicking or otherwise) the Random Value to ZoTrus' servers to confirm receipt and authorization.
   The Random Value, which is unique, is generated by ZoTrus and remains valid for use in a confirming response for no more than 30 days from its generation.

3. DNS Change as defined in section 3.2.2.4.7 of the Baseline Requirements.
   Confirming the Applicant's control over the requested FQDN by confirming the presence of a Random Value or Request Token in a DNS CNAME or TXT record for an Authorization Domain Name or an Authorization Domain Name that is prefixed with a label that begins with an underscore character. The Random Value, which is unique, is generated by ZoTrus and remains valid for no more than 30 days from its generation.

4. IP Address as defined in section 3.2.2.4.8 of the Baseline Requirements.
   Confirming the Applicant's control over the requested FQDN by confirming that the Applicant controls an IP address returned from a DNS lookup for A or AAAA records for the FQDN. This method is not used for validating wildcard domain names.

5. Email to DNS CAA contact as defined in section 3.2.2.4.13 of the Baseline Requirements.
   Confirming the Applicant's control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value. The Random Value MUST be sent to a DNS CAA Email Contact. The relevant CAA Resource Record Set MUST be found using the search algorithm defined in RFC 8659 Section 3.
   The Random Value, which is unique, is generated by ZoTrus and remains valid for no more than 30 days from its generation.

6. Email to DNS TXT contact as defined in Section 3.2.2.4.14 of the Baseline Requirements.
   Confirming the Applicant's control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value.
   Random Value MUST be sent to an email address identified as a DNS TXT record email contact for the Authorization Domain Name selected to validate the FQDN.
   The Random Value, which is unique, is generated by ZoTrus and remains valid for no more than 30 days from its generation.

7. Phone contact with domain contact as defined in Section 3.2.2.4.15 of the Baseline Requirements.
   Confirming the Applicant's control over the FQDN by calling the domain contact´s phone number and obtain a confirming response to validate the AND.
   In the event of reaching voicemail, ZoTrus will leave a Random Value and the ADNs being validated and then receiving a confirming response utilizing the Random Value.
   The Random Value, which is unique, is generated by ZoTrus and remains valid for no more than 30 days from its generation.

8. Phone contact with DNS TXT record phone contact as defined in Section 3.2.2.4.16 of the Baseline Requirements.
   Confirming the Applicant's control over the FQDN by calling the DNS TXT record phone contact´s phone number and obtain a confirming response to validate the ADN.
   In the event of reaching voicemail, ZoTrus will leave a Random Value and the ADNs being validated and then receiving a confirming response utilizing the Random Value.
   The Random Value, which is unique, is generated by ZoTrus and remains valid for no more than 30 days from its generation.

9. Phone contact with DNS CAA phone contact as defined in Section 3.2.2.4.17 of the Baseline Requirements.
   Confirming the Applicant's control over the FQDN by calling the DNS CAA phone contact´s phone number and obtain a confirming response to validate the ADN. The relevant CAA Resource Record Set MUST be found using the search algorithm defined in RFC 8659 Section 3.
   In the event of reaching voicemail, ZoTrus will leave a Random Value and the ADNs being validated and then receiving a confirming response utilizing the Random Value.
   The Random Value, which is unique, is generated by ZoTrus and remains valid for no more than 30 days from its generation.

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

Requirements.
Confirming the Applicant's control over the requested FQDN by verifying that the Request Token or Random Value is contained in the contents of a file. Confirming that the Request Token or Random Value is located on the Authorization Domain Name, under the HTTP[S]://<Authorization Domain>/.well-known/pki-validation/ over port 80 (HTTP) or 443 (HTTPS). The Random Value, which is unique, is generated by ZoTrus and remains valid for use for no more than 30 days from its generation.
This method is not used for validating wildcard domain names.

11. Agreed-upon change to website – ACME as defined in section 3.2.2.4.19 of the Baseline Requirements.
Confirming the Applicant's control over the FQDN by validating domain control of the FQDN using the ACME HTTP Challenge method as defined in section 8.3 of RFC 8555. The token (as defined in section 8.3 of the RFC 8555) is generated by ZoTrus and remains valid for use for no more than 30 days from its generation.
This method is not used for validating wildcard domain names.

12. TLS using ALPN as defined in section 3.2.2.4.20 of the Baseline Requirements.
Confirming the Applicant's control over a FQDN by validating domain control of the FQDN by negotiating a new application layer protocol using the TLS Application- Layer Protocol Negotiation (ALPN) Extension [RFC7301] as defined in RFC 8737. The token (as defined in RFC 8737, section 3) SHALL NOT be used for more than 30 days from its creation.
This method is not used for validating wildcard domain names.

3.2.2.1.2. IP Address Verification

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

1. Agreed-upon change to website as defined in section 3.2.2.5.1 of the Baseline requirements.
Confirming the Applicant's control over the requested IP Address by confirming the presence of a Request Token or Random Value contained in the content of a file or webpage in the form of a meta tag under the "/.well-known/pki-validation" directory, or another path registered with IANA for the purpose of validating control of IP Addresses, on the IP Address that is accessible by the CA via HTTP/HTTPS over an Authorized Port. The Request Token or Random Value SHALL NOT appear in the request.
When a Random Value, which is unique, is used it remains valid for use for no more than 30 days from its generation.

2. Email, Fax, SMS, or Postal Mail to IP Address Contact as defined in section 3.2.2.5.2 of the Baseline Requirements.
Confirming the Applicant's control over the IP Address by sending a Random Value via

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

3. Reverse address lookup as defined in section 3.2.2.5.3 of the Baseline Requirements.
   Confirming the Applicant's control over the IP Address by obtaining a Domain Name associated with the IP Address through a reverse-IP lookup on the IP Address and then verifying control over the FQDN using a method permitted under Section 3.2.2.1.1 above.

4. Phone contact with IP Address contact as defined in section 3.2.2.5.5 of the Baseline Requirements.
   Confirming the Applicant's control over the IP Address by calling the IP Address contact´s phone number and obtain a confirming response to validate the IP Address. ZoTrus makes the call to a phone number identified by the IP Address Registration Authority as the IP Address contact.
   In the event of reaching voicemail, ZoTrus will leave a Random Value and the IP Address being validated and then receiving a confirming response utilizing the Random Value.
   The Random Value, which is unique, is generated by ZoTrus and remains valid for no more than 30 days from its generation.

5. ACME "http-01" method for IP Addresses as defined in section 3.2.2.5.6 of the Baseline Requirements.
   Confirming the Applicant's control over the IP Address by performing the procedure documented for a "http-01" challenge in draft 04 of "ACME IP Identifier Validation Extension", available at https://tools.ietf.org/html/draft-ietf-acme-ip-04#section-4.

6. ACME "tls-alpn-01" method for IP Addresses as defined in section 3.2.2.5.7 of the Baseline Requirements.
   Confirming the Applicant's control over the IP Address by performing the procedure documented for a "tls-alpn-01" challenge in draft 04 of "ACME IP Identifier Validation Extension", available at https://tools.ietf.org/html/draft-ietf-acme-ip- 04#section-4.

3.2.2.2. Validating control over mailbox via email

ZoTrus MAY confirm the Applicant's control over each Mailbox Field to be included in a Certificate by sending a Random Value via email and then receiving a confirming response utilizing the Random Value.
Control over each Mailbox Address SHALL be confirmed using a unique Random Value. The Random Value SHALL be sent only to the email address being validated and SHALL not be shared in any other way.

The Random Value SHALL be unique in each email. The Random Value SHALL remain valid for use in a confirming response for no more than 24 hours from its creation.
The Random Value SHALL be reset upon each instance of the email sent by ZoTrus to a Mailbox Address, however all relevant Random Values sent to that Mailbox Address MAY remain valid for use in a confirming response within the validity period described in this Section. In addition, the Random Value SHALL be reset upon first use by the user if intended for additional use as an authentication factor following the Mailbox Address verification.

3.2.2.3. Authentication of Organization Identity for OV SSL/TLS, Code Signing, Document Signing, and Device Certificates

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

(1) A government agency in the jurisdiction of the Applicant's legal creation, existence or recognition;

(2) A third party database that is periodically updated and considered a Reliable Data Source;

(3) A site visit by the CA or a third party who is acting as an agent for the CA; or,

(4) An attestation letter;

For the other certificate types, ZoTrus MAY use the same documentation (BRs and Code Signing BRs) or additional documentation like the AATL from Adobe.

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

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

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

3.2.2.4. Authentication of Organization Identity for EV SSL/TLS and EV Code Signing Certificates

Before issuing an EV Certificate, ZoTrus ensures that all Subject organization information to be included in the EV Secure Server, or Code Signing Certificate conforms to the requirements of, and is verified in accordance with the CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates (commonly referred to as the EV Guidelines) and/or the Baseline Requirements For The Issuance And Management Of Publicly Trusted Code Signing Certificates (commonly referred to as Code Signing BR) as applicable.
ZoTrus will verify:

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

For purposes of verifying the Applicant's Legal Existence/Jurisdiction of Incorporation or Registration information ZoTrus uses the data sources as published at www.zotrus.com/policy.

3.2.2.5. Wildcard domain validation

ZoTrus has established and follows a documented procedure that determines if a wildcard character in a CN or subjectAltName of type DNS-ID occurs in the first label position to the left of a "registry-controlled" label or "public suffix" (e.g. ".com",".com.cn", see RFC 6454 Section 8.2 for further explanation). If a wildcard falls within the label immediately to the left of a registry-controlled or public suffix, ZoTrus refuses issuance unless the applicant proves its rightful control of the entire Domain Namespace.

3.2.2.6. Data source accuracy

All data sources are evaluated for reliability, accuracy, and for their protection from alteration and falsification before they are used for any identification or authentication purposes. Data sources are revalidated in accordance with the CAB Forum BR for secure server or code signing certificates or EVG documentation or other best practices documentation.

3.2.3. Authentication of Individual Identity

Authentication of an individual identity is performed through the validation processes specified below and depends on the type of Certificate. Applications for ZoTrus Certificates are supported by appropriate documentation to establish the identity of an Applicant.
The following elements are critical information elements for a ZoTrus Certificate issued to an individual:

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

3.2.3.1. Domain and IP Address Verification

Same as section 3.2.2.1 for Organizational Applicants.

3.2.3.2. Individual Identity Verification for IV SSL/TLS Secure Server, Code Signing, Document Signing, and Device Certificates

In addition to the verification of domain control using the procedures listed above in section 3.2.2.1 of this CPS, if the Applicant is a natural person, ZoTrus verifies the identity and address of the Applicant in accordance with the Baseline Requirements (BRs for Secure Server certificates and Code Signing BRs for Code Signing certificates), using:

(1) Verify the Applicant's name using a legible copy, which discernibly shows the Applicant's face, of at least one currently valid government issued photo ID (passport, driver's license, military ID, national ID or equivalent document type)

(2) Verify the Applicant's address using a form of identification that ZoTrus determines to be reliable such as a government ID, utility bill, or bank or credit card statement. ZoTrus MAY rely on the same government issued ID that was used to verify the Applicant's name.

ZoTrus MAY accept or require, at its discretion, other official documentation supporting an application, possibly including, but not limited to, requiring face to face verification of the Applicant's identity before an authorized agent of ZoTrus, an attorney, a CPA, a Latin notary, a notary public or equivalent. Such face-to-face verification SHALL be required prior to issuance of a Document Signing Certificate.

ZoTrus verifies the certificate request with the Applicant using a Reliable Method of Communication.

3.2.3.3. Individual Identity Verification for EV SSL/TLS Secure Server or EV Code Signing Certificate

ZoTrus does not issue EV SSL/TLS Certificate or EV Code Signing Certificates to Individual Applicants.

3.2.4. Non-Verified Subscriber Information

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

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

3.2.5. Validation of Authority

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

3.2.5.1. S/MIME / Client Certificates

The request is verified via email sent to the email address to be contained in the Certificate Subject.

3.2.5.2. Domain Registrant Authorization of SSL/TLS Server Certificates

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

3.2.5.3. OV SSL/TLS Server, Code Signing, and Document Signing Certificates

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

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

technology offices, or other department that ZoTrus deems appropriate.

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

3.2.5.4. EV SSL/TLS Server and Code Signing Certificates

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

The request for EV Code Signing certificates is verified in accordance with the CA/B Forum Baseline Requirements For The Issuance And Management Of Publicly Trusted Code Signing Certificates section 11.2.

3.2.6. Criteria for Interoperation or Certification

Not applicable.

3.3 Identification and Authentication for Re-Key Requests

3.3.1. Identification and Authentication for Routine Re-Key

Subscribers should not reuse Private Keys for successive certificates after expiration thereof and it's highly recommended to create a new key for every certificate.

3.3.2. Identification and Authentication for Re-Key After Revocation

Private Keys of certificates which were revoked should not be reused.

3.4 Identification and Authentication for Revocation Request

See Sections 4.9.1 through 4.9.3 for information about Certificate revocation procedures.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1. Who Can Submit a Certificate Application

Any individual who is the Subject of the certificate or any authorized representative of an organization or entity.

ZoTrus SHALL maintain an internal database of all previously revoked Certificates and previously rejected certificate requests due to suspected phishing or other fraudulent usage or concerns. ZoTrus SHALL use this information to identify subsequent suspicious certificate requests.

4.1.1.1. Subscriber Agreement Requirements

By accepting a certificate from ZoTrus, the subscriber agrees to the rules and regulations outlined in this policy and any accompanied agreement or document. The certificate shall be used lawfully in accordance with the terms of this CP and the relevant CP statements. The certificate Applicants can acknowledge the acceptance of CP and CPS electronically on ZoTrus website. Certificate usage must be consistent with the Key Usage field extensions included in the certificate (e.g., if a digital signature is not enabled then the certificate must not be used for signing). Subscribers shall protect their Private Keys from unauthorized use and shall discontinue use of the Private Key following expiration or revocation of the certificate.

4.1.1.2. Certificate Request Requirements for DV/IV/OV SSL Certificates

Accept the Subscriber Agreement Requirements and demonstration of possession and/or exclusive control of the Private Key corresponding to the Public Key.

4.1.2. Enrollment Process and Responsibilities

ZoTrus maintains systems and processes that sufficiently authenticate the Applicant's identity for all Certificate types that present the identity to Relying Parties. Applicants must submit sufficient information to allow ZoTrus to successfully perform the required verification. ZoTrus shall protect communications and securely store information presented by the Applicant during the application process in compliance with the ZoTrus Privacy Policy.

In no particular order, the enrollment process includes:

1) Generating a suitable Key Pair using a suitably secure platform;
2) Generating a Certificate Signing Request (CSR) using an appropriately secure tool;
3) Submitting a request for a Certificate type and appropriate application information;
4) Agreeing to a Subscriber Agreement or other applicable terms and conditions; and
5) Paying any applicable fees.

4.2 Certificate Application Processing

4.2.1. Performing Identification and Authentication Functions

ZoTrus maintains systems and processes to sufficiently authenticate the Applicant's identity in compliance with this CPS. Initial vetting may be performed by ZoTrus' validation team as set forth in Section 3.2. All communications sent through as email are securely stored along with all information presented directly by the Applicant via the ZoTrus web interface or API. Future applications for Certificates are authenticated using single (username and password) or multi-factor (Certificate in combination with username/password) authentication techniques.

Before the issuance of any SSL certificate, ZoTrus checks the DNS for the existence of a CAA record for each dNSName in the SubjectAltName extension, according to the RFC 6844 requirements. In case the certificate is issued, it will be done before the TTL of the CAA registry, and in any case in no more than 8 hours. ZoTrus always processes "issue" and "issuewild" tags, and may not dispatch reports of issuance requests to the contact(s) listed in the "iodef" tag. The CAA records that identify domains for which ZoTrus is authorized to issue are "zotrus.com". For more information about CAA, see Section 3.2.2.8 CAA records.

4.2.2. Approval or Rejection of Certificate Applications

Following successful completion of all required validations of a certificate application, ZoTrus approves an application for a digital certificate.

If the validation of a certificate application fails, ZoTrus rejects the certificate application. ZoTrus reserves the right to reject applications to issue a certificate to Applicants if, on its own assessment and may do so without incurring any liability or responsibility for any loss or expenses arising as a result of such refusal. Applicants whose applications have been rejected may subsequently re-apply.

ZoTrus may reject requests based on potential brand damage to ZoTrus in accepting the request. ZoTrus may also reject applications for Certificates from Applicants who have previously been rejected or have previously violated a provision of their Subscriber Agreement. ZoTrus is under no obligation to provide a reason to an Applicant for rejection of a Certificate Request.

Subscribers are required to check the Certificate's contents for accuracy prior to using the certificate.

4.2.3. Time to Process Certificate Applications

ZoTrus makes reasonable efforts to confirm certificate application information and issue the Certificates within a reasonable time frame. This greatly dependents on the Applicant providing the necessary details and documentation in a timely manner. Upon the receipt of the necessary details and documentation, ZoTrus aims to confirm submitted application data and to complete the validation process and issue or reject a certificate application.

The following is the approximate processing time:

T1 Validation Level Certificates	30 minutes
T2 Validation Level Certificates	50 minutes
T3 Validation Level Certificates	4 hours
T4 Validation Level Certificates	one business day

4.3 Certificate Issuance

4.3.1. CA Actions During Certificate Issuance

ZoTrus offers different certificate types to make use of SSL and S/MIME technology for secure online transactions, secure electronic document, and secure email respectively. Prior to the issuance of a certificate, ZoTrus will validate an application in accordance with this CPS which may involve the request by ZoTrus to the Applicant for relevant official documentation supporting the application.

ZoTrus does not issue end entity certificates directly from its Root Certificates. ZoTrus logs its issued RSA/ECC SSL Certificates in Certificate Transparency Log Systems and log its issued SM2 SSL Certificates in SM2 Certificate Transparency Log Systems. Databases and CA processes occurring during certificate issuance are protected from unauthorized modification. After issuance is complete, the certificate is stored in a database and sent to the Subscriber.

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

ZoTrus shall notify the Subscriber of the issuance of a Certificate at an email address which was supplied by the Subscriber during the enrollment process or by any other equivalent method. The email may contain the Certificate itself or a link to download depending upon the workflow of the Certificate requested.

4.4 Certificate Acceptance

4.4.1. Conduct Constituting Certificate Acceptance

ZoTrus shall inform the Subscriber that she/he may not use the Certificate until the Subscriber has reviewed and verified the accuracy of the data incorporated into the Certificate. Unless the Subscriber notifies ZoTrus within seven (7) days from receipt, the Certificate is deemed accepted.

4.4.2. Publication of the Certificate by the CA

ZoTrus publishes all CA Certificates in its repository (www.zotrus.com/root). ZoTrus publishes end-entity Certificates by delivering them to the Subscriber.

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

No other publication or notification to others occurs.

4.5 Key Pair and Certificate Usage

4.5.1. Subscriber Private Key and Certificate Usage

Subscribers must protect their Private Keys from unauthorized use and shall discontinue use of the Private Key following expiration or revocation of the certificate.

Subscribers are notified hereby that electronic signatures can be legally binding. The extent to which they are trusted depends on local legislation. That means that legislation will decide on a case-by-case base whether or not they are legally binding. Because of these legal implications, subscribers must protect their Private Keys.

4.5.2. Relying Party Public Key and Certificate Usage

Reliance on a certificate must be reasonable under the circumstances. If the circumstances indicate a need for additional assurances, the relying party must obtain such assurances for such reliance to be deemed reasonable. Before any act of reliance, relying parties shall independently assess:

1) That the certificate is being used in accordance with the Key Usage field extensions included in the certificate (e.g., if a digital signature is not enabled then the certificate may not be relied upon for validating a Subscriber's signature).
2) The status of the end entity certificate and all the CA certificates in the chain that issued the certificate. If any of the certificates in the certificate chain have been revoked, the relying party shall not rely on the end user certificate or other revoked

certificates in the certificate chain.

4.6 Certificate Renewal

Renewing a certificate follows the same procedures as with a new certificate.

4.6.1. Circumstances for Certificate Renewal

Not applicable.

4.6.2. Who May Request Renewal

Not applicable.

4.6.3. Processing Certificate Renewal Requests

Not applicable.

4.6.4. Notification of New Certificate Issuance to Subscriber

Not applicable.

4.6.5. Conduct Constituting Acceptance of a Renewal Certificate

Not applicable.

4.6.6. Publication of the Renewal Certificate by the CA

Not applicable.

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

Not applicable.

4.7 Certificate Re-Key

ZoTrus treats certificate re-key requests as requests for the issuance of a new Certificate. Re-keying or reusing the same Private Key for any new or renewed certificate shall be avoided by the subscriber.

4.7.1. Circumstances for Certificate Re-Key

Not applicable.

4.7.2. Who May Request Certification of a New Public Key

Not applicable.

4.7.3. Processing Certificate Re-Keying Requests

Not applicable.

4.7.4. Notification of New Certificate Issuance to Subscriber

Not applicable.

4.7.5. Conduct Constituting Acceptance of a Re-Keyed Certificate

Not applicable.

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

Not applicable.

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

Not applicable.

4.8 Certificate Modification

ZoTrus does not modify previously issued certificates. Any request for certificate modification will be treated as a request for the issuance of a new Certificate.

4.8.1. Circumstances for Certificate Modification

Not applicable.

4.8.2. Who May Request Certificate Modification

Not applicable.

4.8.3. Processing Certificate Modification Requests

Not applicable.

4.8.4. Notification of New Certificate Issuance to Subscriber

Not applicable.

4.8.5. Conduct Constituting Acceptance of Modified Certificate

Not applicable.

4.8.6. Publication of the Modified Certificate by the CA

Not applicable.

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

Not applicable.

4.9 Certificate Revocation and Suspension

4.9.1. Circumstances for Revocation

Revocation of a certificate is to permanently end the operational period of the certificate prior to reaching the end of its stated Validity Period. A certificate will be revoked when the information it contains is suspected to be incorrect or compromised.

4.9.1.1. Reasons for Revoking a Subscriber Certificate

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

1. The Subscriber requests in writing that ZoTrus revoke the Certificate;
2. The Subscriber notifies ZoTrus that the original certificate request was not authorized and does not retroactively grant authorization;
3. ZoTrus obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise;

4. ZoTrus 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. ZoTrus obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address in the Certificate should not be relied upon.

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

1. The Certificate no longer complies with the requirements of Section 6.1.5 and Section 6.1.6;
2. ZoTrus obtains evidence that the Certificate was misused;
3. ZoTrus is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use;
4. ZoTrus 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. ZoTrus is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
6. ZoTrus is made aware of a material change in the information contained in the Certificate;
7. ZoTrus is made aware that the Certificate was not issued in accordance with these Requirements or the CA's Certificate Policy or Certification Practice Statement;
8. ZoTrus determines or is made aware that any of the information appearing in the Certificate is inaccurate;
9. ZoTrus' right to issue Certificates under these Requirements expires or is revoked or terminated, unless ZoTrus has made arrangements to continue maintaining the CRL Repository;
10. Revocation is required by ZoTrus' Certificate Policy and/or Certification Practice Statement; or
11. ZoTrus is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed.

4.9.1.2. Reasons for Revoking a Subordinate CA Certificate

ZoTrus SHALL revoke a Subordinate CA Certificate within 7 days if one or more of the following occurs:

1. The Subordinate CA requests revocation in writing;
2. The Subordinate CA notifies ZoTrus that the original certificate request was not authorized and does not retroactively grant authorization;

3. ZoTrus obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Section 6.1.5 and Section 6.1.6;
4. ZoTrus obtains evidence that the Certificate was misused;
5. ZoTrus is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with this document or the applicable Certificate Policy or Certification Practice Statement;
6. ZoTrus determines that any of the information appearing in the Certificate is inaccurate or misleading;
7. ZoTrus or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
8. ZoTrus' or Subordinate CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless ZoTrus has made arrangements to continue maintaining the CRL Repository; or
9. Revocation is required by ZoTrus' Certification Practice Statement.

4.9.2. Who Can Request Revocation

Certificate revocation can be requested by the subscriber of the certificate or by any other entity presenting proof of knowledge of circumstances for revocation. Additionally, Subscribers, Relying Parties, Application Software Suppliers, and other third parties may submit Certificate Problem Reports informing ZoTrus of reasonable cause to revoke the certificate. ZoTrus may also at its own discretion revoke Certificates.

4.9.3. Procedure for Revocation Request

Subscribers may request revocation of a certificate by using the online utility provided at the ZoTrus website. ZoTrus makes every reasonable effort to verify the claims, reason, and identity of the requester.

The subscriber can check the revocation status in his/her ZoTrus account. Upon the revocation of a subscriber's certificate, the newly revoked certificate is recorded and an updated CRL shall be issued. Notification of revocation of a certificate to others than the subscriber and Subject of the certificate, beyond the published CRL, are generally not performed.

ZoTrus maintains a continuous 24X7 ability to internally respond to any high priority revocation requests. If appropriate, ZoTrus forwards complaints to law enforcement.

4.9.4. Revocation Request Grace Period

ZoTrus may grant and extend revocation grace periods on a case-by-case basis.

4.9.5. Time Within Which CA Must Process the Revocation Request

ZoTrus maintains 24 x 7 ability to respond internally to a high-priority Certificate Problem Report and, where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a Certificate that is the Subject of such a complaint. ZoTrus will begin investigation procedures for a suspected Key Compromise or misuse of a Certificate within 24 hours of receipt of the report.

ZoTrus decides whether revocation or other action is warranted based on at least the following criteria:

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

4.9.6. Revocation Checking Requirements for Relying Parties

Relying parties must verify the certificate against the revocation list (CRL), check against expiry time, certificate chain, the validity check of the certificates in the chain and the identification of the domain and email.

4.9.7. CRL Issuance Frequency

The corresponding Certificate Revocation Lists (CRL) of subscriber certificates are updated at least every seven (7) days or every time a certificate is revoked, whichever comes first. And the value of the nextUpdate field MUST NOT be more than seven days beyond the value of the thisUpdate field. The CRL is published via Internet download. Each intermediate CA issues its own corresponding CRL for the certificates issued. The CRL distribution points are included in the certificates.

The CRL of intermediate CA certificates is updated at least once every twelve (12) months and within 24 hours after revoking an intermediate CA certificate, and the value of the nextUpdate field is not more than 12 months beyond the value of the thisUpdate field.

The last CRL of issuer certificates which reach end-of-life (expired) shall remain published

available for a period of 365 days. Such last CRL shall be archived with other related records of the expired issuer certificate.

4.9.8. Maximum Latency for CRLs

Certificate Revocation Lists is published at the on-line repository within a commercially reasonable time after generation. This is generally done automatically and within three (3) hours after generation of a new CRL.

4.9.9. On-Line Revocation/Status Checking Availability

ZoTrus only provides CRL service about the status of a certificate.

4.9.10. On-Line Revocation Checking Requirements

Relying parties must verify the certificate against the revocation list (CRL), check against expiry time, certificate chain, the validity check of the certificates in the chain and the identification of the domain and email.

4.9.11. Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12. Special Requirements Related to Key Compromise

ZoTrus uses commercially reasonable methods to inform Subscribers that their Private Key may have been Compromised. This includes cases where new vulnerabilities have been discovered or where ZoTrus at its own discretion decides that evidence suggests a possible Key Compromise has taken place. Where Key Compromise is not disputed, ZoTrus shall revoke Issuing CA Certificates or Subscriber end entity Certificates within 24 hours and publish online CRLs within one hour of creation.

4.9.13. Circumstances for Suspension

Certificates issued to subscriber may be either valid, expired or revoked. ZoTrus does not perform certificate suspension and subscribers are advised to request a new certificate in case of expiration or revocation of previously valid certificates.

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

ZoTrus provides a Certificate status service in the form of a CRL distribution point only. ZoTrus MUST NOT remove the revocation entries on a CRL until after the Expiry Date of the revoked Certificate.

4.10.2. Service Availability

ZoTrus provides 24x7 certificate status services, and the response time is of ten seconds or less.

4.10.3. Operational Features

No stipulation.

4.11 End of Subscription

A Subscriber may terminate its subscription to certificate services by allowing the term of a Certificate or applicable agreement to expire without renewal. A Subscriber may also voluntarily revoke a Certificate as explained in Section 4.9.

4.12 Key Escrow and Recovery

ZoTrus does not create or store the Subscriber's private key for publicly trusted SSL/TLS Server Certificates. In general, ZoTrus does not provide key escrow or key backup services. ZoTrus expects an Applicant to generate key-pairs in its own environment and to pass only the Public Key to ZoTrus for inclusion in the Certificates issued.

4.12.1. Key Escrow and Recovery Policy and Practices

For Email security cloud service and document security cloud service, ZoTrus will provide key escrow service for the Private Keys of the Email encrypting certificate and Document Signing certificate. The Escrowed Private Keys SHALL be stored in encrypted form. ZoTrus SHALL protect escrowed Private Keys from unauthorized disclosure.

ZoTrus SHALL recover Subscriber Private Keys only under the circumstances permitted within this CPS that subscriber MUST validate the email account control for getting the stored Private Key for this email address.

For Document Cloud Signing service, the subscriber must validate the related service account control for using the stored Private Key to sign the document HASH data.

4.12.2. Session Key Encapsulation and Recovery Policy and Practices

Not stipulation.

5. Facility, Management, and Operational Controls

5.1 Physical Controls

5.1.1. Site Location and Construction

ZoTrus has one machine rooms in Shenzhen, it operates under a security policy designed to provide reasonable assurance of the detection, deterrence and prevention of unauthorized logical or physical access to CA related facilities. Physical barriers are used to segregate secure areas within buildings and are constructed so as to extend from real floor to real ceiling to prevent unauthorized entry. External walls of the site are of solid construction.

5.1.2. Physical Access

The hardware is located in a dedicated, resistant server room. Access to the facility by individuals (personnel and others) is strictly controlled and restricted to authorized and trusted personnel only. Maintenance and other services applied to the cryptographic devices and server systems must be authorized by the CEO or CTO of ZoTrus or equally authorized caretaker of the ZoTrus PKI. Physical access to the server infrastructure and facilities shall be logged and signed by at least one other witness on the four eyes principal. Otherwise, physical access to the systems shall be avoided.

5.1.3. Power and Air Conditioning

The locality is fully air conditioned to prevent overheating and to maintain a suitable humidity level. Primary and secondary power supplies ensure continuous, uninterrupted access to electric power. Electricity power backup (UPS) is supported by an external, independent electricity power source for cases of prolonged power outages.

5.1.4. Water Exposures

All server equipment and devices are elevated above the ground. No water lines exist above equipment.

5.1.5. Fire Prevention and Protection

Fire alarm and intrusion prevention equipment are installed, maintained and available at the premise.

5.1.6. Media Storage

The server room is monitored by a closed-circuit camera and television monitoring system with recording capabilities and records shall be archived in a rolling and increasing mode.

Daily backup of its CA related data that are rotated and stored according to either on-site or off-site according to an established backup rotation schedule.

5.1.7. Waste Disposal

ZoTrus implemented procedures for the disposal of waste (paper, media, or any other waste) in order to prevent the unauthorized use of, or access to, or disclosure of waste containing confidential information.

5.1.8. Off-Site Backup

ZoTrus backs up much of its information to a secure, off-site location that is sufficiently distant to escape damage from a disaster at the primary location. The CA Private Keys and activation data is backed up in a rolling fashion and secure manner and stored off-site in separate safety vaults accessible only by trusted personnel.

5.2 Procedural Controls

5.2.1. Trusted Roles

ZoTrus follows personnel and management practices that provide reasonable assurance of the trustworthiness and competence of their employees and of the satisfactory performance of their duties. Personnel acting in trusted roles include CA, TSA, and CMS system administration personnel, and personnel involved with identity vetting and the issuance and revocation of Certificates. The functions and duties performed by persons in trusted roles are distributed so that one person alone cannot circumvent security measures or subvert the security and trustworthiness of the PKI or TSA operations. All personnel in trusted roles must be free from conflicts of interest that might prejudice the impartiality of the ZoTrus PKI's operations. Trusted roles are appointed by senior management. A list of personnel appointed to trusted roles is maintained and reviewed annually.

5.2.2. Number of Persons Required per Task

Handling of CA Private Keys (throughout the entire CA key lifecycle) requires the involvement of at least two trusted persons. Physical and logical access controls exist for the key activation material in order to maintain multi-party control over the Hardware Security Modules containing CA Private Keys.

The signing of Intermediate Certificates and Certificate Revocation Lists covering the Intermediate CAs shall be performed exclusively by an executive officer and in attendance of at least one witness.

5.2.3. Identification and Authentication for Each Role

Personnel in trusted roles must authenticate themselves to CA, TSA, and CMS system before they are allowed access to the components of the system necessary to perform their trusted roles.

5.2.4. Roles Requiring Separation of Duties

The signing of CA Root Certificates, Intermediate Certificates and Certificate Revocation Lists covering the Intermediate CAs shall be performed exclusively by an executive officer of ZoTrus and attendance by at least one witness.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

ZoTrus employs enough personnel that possess the expert knowledge, experience and

qualifications necessary for the offered services, as appropriate to the job function. ZoTrus personnel fulfil the requirement through expert knowledge, experience and qualifications with formal training and education, actual experience, or a combination of the two. Trusted roles and responsibilities, as specified in Section 5.2.1 are documented in job descriptions. ZoTrus personnel (both temporary and permanent) have job descriptions defined from the viewpoint of separation of duties and least privilege, determining position sensitivity based on the duties and access levels, background screening and employee training and awareness. ZoTrus personnel are formally appointed to trusted roles by senior management responsible for security.

The job descriptions include skills and experience requirements. Managerial personnel are employed who possess experience or training in electronic signature technology and familiarity with security procedures for personnel with security responsibilities and experience with information security and risk assessment sufficient to carry out management functions.

The ZCPA is responsible and accountable for ZoTrus' PKI operations and ensures compliance with this CPS. ZoTrus' personnel and management practices provide reasonable assurance of the trustworthiness and competence of its employees and of the satisfactory performance of their duties.

Management and operational support personnel involved in timestamp operations possess experience with information security and risk assessment and knowledge of timestamping technology, digital signature technology, mechanisms for calibration of time stamping clocks with UTC, and security procedures. The ZCPA ensures that all individuals assigned to trusted roles have the experience, qualifications, and trustworthiness required to perform their duties under this CPS.

5.3.2 Background Check Procedures

ZoTrus verifies the identity of each employee appointed to a trusted role and performs a background check prior to allowing such person to act in a trusted role. ZoTrus requires everyone to appear in-person before a human resources employee whose responsibility it is to verify identity. The human resources employee verifies the individual's identity using government-issued photo identification (e.g., resident identity card and/or passports etc.). Background checks include employment history, education, and criminal background. The highest education degree obtained is verified regardless of the date awarded. Based upon the information obtained during the background check, the human resources administration department makes an adjudication decision, as to whether the individual is suitable for the position to which they will be assigned.

ZoTrus requires that all individuals assigned to trusted roles to provide proof non-criminal

record or non-criminal statement every year.

5.3.3 Training Requirements

ZoTrus provides skills training to all employees involved in ZoTrus' PKI and CMS operations. The training relates to the person's job functions and covers:

1) basic Public Key Infrastructure (PKI) knowledge,
2) software versions used by ZoTrus,
3) authentication and verification policies and procedures,
4) ZoTrus security principals and mechanisms,
5) disaster recovery and business continuity procedures,
6) common threats to the validation process, including phishing and other social engineering tactics, and
7) applicable industry and government guidelines.

Training is provided via a mentoring process involving senior members of the team to which the employee belongs.

ZoTrus maintains records of who received training and what level of training was completed. Validation Specialist must have the minimum skills necessary to satisfactorily perform validation duties before being granted validation privileges. All Validation Specialist are required to pass an internal examination on the ZoTrus Validation Operational Guide prior to validating and approving the issuance of Certificates.

Where competence is demonstrated in lieu of training, ZoTrus maintains supporting documentation.

5.3.4 Retraining Frequency and Requirements

Employees must maintain skill levels that are consistent with industry-relevant training and performance programs in order to continue acting in trusted roles. ZoTrus makes all employees acting in trusted roles aware of any changes to ZoTrus' operations. If ZoTrus' operations change, ZoTrus will provide documented training, in accordance with an executed training plan, to all employees acting in trusted roles.

5.3.5. Job Rotation Frequency and Sequence

No stipulation.

5.3.6. Sanctions for Unauthorized Actions

ZoTrus employees failing to comply with this CPS, whether through negligence or malicious intent, are Subject to administrative or disciplinary actions, including termination of employment or criminal sanctions. If a person in a trusted role is cited by management for unauthorized or inappropriate actions, the person will be immediately removed from the trusted role pending management review. After management has reviewed and discussed the incident with the employee involved, management may reassign that employee to a non-trusted role or dismiss the individual from employment as appropriate.

5.3.7. Independent Contractor Requirements

No stipulation.

5.3.8. Documentation Supplied to Personnel

Personnel in trusted roles are provided with the documentation necessary to perform their duties, including a copy of this CPS, and other technical and operational documentation needed to maintain the integrity of ZoTrus' CA operations. Personnel are also given access to information on internal systems and security documentation, identity vetting policies and procedures, discipline-specific books, treatises and periodicals, and other information.

5.4 Audit Logging Procedures

5.4.1. Types of Events Recorded

Audit log files shall be generated for all events relating to the security and services of the CA. Where possible, the security audit logs shall be automatically generated. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits.

ZoTrus SHALL record at least the following events:

1. CA certificate and key lifecycle events, including:
   (1) Key generation, backup, storage, recovery, archival, and destruction;
   (2) Certificate requests, renewal, and re-key requests, and revocation;
   (3) Approval and rejection of certificate requests;
   (4) Cryptographic device lifecycle management events;
   (5) Generation of Certificate Revocation Lists;
   (6) Introduction of new Certificate Profiles and retirement of existing Certificate Profiles.

2. Subscriber Certificate lifecycle management events, including:

(1) Certificate requests, renewal, and re-key requests, and revocation;
(2) All verification activities stipulated in these Requirements and the CA's CPS;
(3) Approval and rejection of certificate requests;
(4) Issuance of Certificates;
(5) Generation of Certificate Revocation Lists.

3. Security events, including:
(1) Successful and unsuccessful PKI system access attempts;
(2) PKI and security system actions performed;
(3) Security profile changes;
(4) Installation, update and removal of software on a Certificate System;
(5) System crashes, hardware failures, and other anomalies;
(6) Firewall and router activities; and
(7) Entries to and exits from the CA facility.

5.4.2. Frequency for Processing and Archiving Audit Logs

The ZoTrus internal auditor administrator reviews the system log at least once a month. And the audit logs are automatically archived in the system's database.

5.4.3. Retention Period for Audit Log

ZoTrus SHALL retains audit logs for at least two (2) years.

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

5.4.4. Protection of Audit Log

ZoTrus audit logs are stored with HASH data or timestamp data in the database with backup, including audit information and event records in related documents. ZoTrus carries out strictly the measures of physical and logical access control to ensure that only personnel authorized by ZoTrus can be access to the records being reviewed. These records are strictly protected from unauthorized access, reading, modification and deletion, and all PDF documents are digitally signed with timestamped for the technical guarantee of log temper-proof.

5.4.5. Audit Log Backup Procedures

Log data is backed up daily in a rolling and increasing mode, including critical system data or any other sensitive information, like personal data and event log files. Archives and other materials of critical system data important for recovery in case of a disaster are encrypted transferred and stored at another off-site facility.

5.4.6. Audit Collection System (Internal vs. External)

No stipulation.

5.4.7. Notification to Event-Causing Subject

No stipulation.

5.4.8. Vulnerability Assessments

ZoTrus' Security Program MUST include an annual risk assessment that:

1) Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate data or Certificate Management Processes;
2) Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and
3) Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that ZoTrus has in place to control such risks.

Based on the Risk Assessment, ZoTrus implements and maintains a Security Plan consisting of security procedures, measures, and products designed to achieve the objectives set forth above and to reasonably manage and control the risks identified during the Risk Assessment, commensurate with the sensitivity of the data and processes, as well as the complexity and scope of the activities of ZoTrus.

The Security Plan includes administrative, organizational, technical, and physical safeguards appropriate to the size, complexity, nature, and scope of the ZoTrus' business. The Security Plan also considers the available technology and the cost of implementing the specific measures and implements a reasonable level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected.

5.5 Records Archival

5.5.1. Types of Records Archived

ZoTrus SHALL archive all audit logs (as set forth in Section 5.4.1).
Additionally, ZoTrus SHALL archive:

(1) Documentation related to the security of Certificate Systems, Certificate Management Systems, Root CA Systems, and other Systems; and
(2) Documentation related to verification, issuance, and revocation of certificate requests and Certificates.

5.5.2. Retention Period for Archive

Archived audit logs (as set forth in Section 5.5.1 SHALL be retained for a period of at least two (2) years from their record creation timestamp, or as long as they are required to be retained per Section 5.4.3, whichever is longer.

Additionally, ZoTrus retains, for at least two (2) years:

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

Such records may be retained in electronic, in paper-based format or any other format that ZoTrus may see fit.

5.5.3. Protection of Archive

Archive records are stored at a secure off-site location and are maintained in a manner that prevents unauthorized modification, substitution, or destruction.

5.5.4. Archive Backup Procedures

Same as 5.4.5

5.5.5. Requirements for Time-Stamping of Records

System times are updated using the Network Time Protocol (NTP) to synchronize system clocks at least once every day. All recorded events are time-stamped in the events and audit logs. Irrespective of timestamping methods, all logs must have data indicating the time at which the event occurred.

5.5.6. Archive Collection System (Internal or External)

Archive information is collected internally.

5.5.7. Procedures to Obtain and Verify Archive Information

Records are archived and maintained in a form that prevents unauthorized modification, substitution, or destruction. Such records may be retained in electronic, in paper-based format or any other format that ZoTrus may see fit.

5.6 Key Changeover

Key changeover procedures enable the smooth transition from expiring CA Certificates to new CA Certificates. Towards the end of the CA Private Key's lifetime, ZoTrus ceases using its expiring CA Private Key to sign Certificates (well in advance of expiration) and uses the old Private Key only to sign CRLs. A new CA signing Key Pair is commissioned, and all subsequently issued certificates and CRL's are signed with the new private signing key. Both the old and the new Key Pairs may be concurrently active. This key changeover process helps minimize any adverse effects from CA Certificate expiration. The corresponding new CA Public Key certificate is provided to subscribers and relying parties through the delivery methods detailed in Section 6.1.4.

5.7 Compromise and Disaster Recovery

5.7.1. Incident and Compromise Handling Procedures

In the event that a CA Private Key is suspected to have been compromised, ZoTrus' CEO or COO will immediately convene an emergency Incident Response Team to assess the situation to determine the degree and scope of the incident and take appropriate actions. Those include collection of information related to the incident, investigation, informing law enforcement and other interested parties, further prevention, and short-term corrections, compiling and issuing of a critical events report. In case it was determined that a CA Private Key was compromised, the affected key shall be revoked (where possible) and a replacement issued after appropriate solutions are implemented to prevent recurrence.

ZoTrus maintains an Incident Response Plan and a Disaster Recovery Plan, which set out the procedures necessary to ensure business continuity, to notify affected stakeholders, and to reasonably protect Application Software, Suppliers, Subscribers, and Relying Parties in the event of a disaster, security compromise, or business failure. ZoTrus annually tests, reviews, and updates its business continuity plan and its security plans and makes them available to its auditors upon request.

The business continuity plan includes:
1). The conditions for activating the plan;
2). Emergency procedures;
3). Fallback procedures;
4). Resumption procedures;
5). A maintenance schedule for the plan;
6). Awareness and education requirements;
7). The responsibilities of the individuals;
8). Recovery time objective (RTO);
9). Regular testing of contingency plans;
10). A plan to maintain or restore the CA's business operations in a timely manner following interruption to or failure of critical business processes;
11). A requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location;
12). A definition of acceptable system outage and recovery times;
13). The frequency at which backup copies of essential business information and software are taken;
14). The distance of recovery facilities to the CA's main site; and
15). Procedures for securing an affected facility following a disaster and prior to restoring a secure environment either at the original or a remote site.

5.7.2. Recovery Procedures if Computing Resources, Software, and/or Data Are Corrupted

ZoTrus performs system back-ups on daily basis. Back-up copies are made of CA Private Keys and are stored off-site in a secure location. In the event of a disaster whereby the CA operations become inoperative, ZoTrus will re-initiate its operations on replacement hardware using backup copies of its software, data and CA Private Keys at a comparable, secured facility.

5.7.3. Recovery procedures after Key Compromise

In the event that the Root CA Private Key of ZoTrus is compromised, ZoTrus will:
- Immediately cease using the compromised key material;
- Revoke all Certificates signed with the compromised key;
- Take commercially reasonable steps to notify all Subscribers of the Revocation; and

- Take commercially reasonable steps to cause all Subscribers to cease using, for any purpose, any such Certificates.

Once the compromised key material has been replaced and a secure operation of the CA in question has been established, the CA may re-issue the revoked certificates following the procedure for initially providing the certificates.

5.7.4. Business Continuity Capabilities After a Disaster

The disaster recovery plan deals with the business continuity as described in Section 5.7.1.

5.8 CA or RA Termination

In the event of termination of a ZoTrus CA business, ZoTrus provides notice to all customers prior to the termination and:

1) Stops delivering Certificates according to and referring to this CPS;
2) Archives all audit logs and other records prior to termination;
3) Destroys all Private Keys upon termination;
4) Ensures archive records are transferred to an appropriate authority;
5) Uses secure means to notify customers and Application Software Suppliers to delete all trust anchors.

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

ZoTrus Generates the Root CA key as required:

1) prepare and follow a Key Generation Script and
2) have a Qualified Auditor witness the Root CA Key Pair generation process or record a video of the entire Root CA Key Pair generation process.
3) generate the keys in a physically secured environment as described in this CPS;
4) generate the CA keys using personnel in trusted roles under the principles of multiple person control and split knowledge;
5) generate the CA keys within cryptographic modules meeting the applicable technical and business requirements as disclosed in this CPS;

6) log its CA key generation activities; and
7) maintain effective controls to provide reasonable assurance that the Private Key was generated and protected in conformance with the procedures described in this CPS and its Key Generation Script.

6.1.1.2 RA Key Pair Generation

No stipulation.

6.1.1.3 Subscriber Key Pair Generation

In general, unless otherwise noted in this CPS, Subscriber is solely responsible for the generation of an asymmetric cryptographic key pair (RSA, ECDSA or SM2) appropriate to the Certificate type being applied for. During application, the Subscriber will generally be required to submit a Public Key and other personal / corporate details in the form of a Certificate Signing Request (CSR).

TLS/SSL Certificate requests are usually generated using the key generation facilities available in the Subscriber's webserver software. Client Certificate requests are usually generated using the cryptographic service provider module software present in popular browsers, although they may also be submitted as a PKCS#10 or SPKAC.

Key pairs for Code Signing Certificates and End Entity Certificates issued pursuant to Adobe Approved Trust List requirements SHALL be generated, stored and used in a crypto module that meets or exceeds the requirements of FIPS 140-2 level 3 or Common Criteria EAL 4+. Acceptable methods of satisfying this requirement include (but are not limited to) the following:
• ZoTrus ships a suitable hardware crypto module, with a preinstalled key pair, in the form of a smartcard or USB device or similar;
• The Subscriber counter-signs certificate requests that can be verified by using a manufacturer's certificate or manufacturers key indicating that the subscriber key is managed in a suitable hardware module;
• The Subscriber provides a suitable IT audit indicating that its operating environment achieves a level of security at least equivalent to that of FIPS 140-2 level 3.

ZoTrus SHALL reject a certificate request if one or more of the following conditions are met:
(1) The Key Pair does not meet the requirements set forth in Section 6.1.5 and/or Section 6.1.6;
(2) There is clear evidence that the specific method used to generate the Private Key was flawed;
(3) ZoTrus is aware of a demonstrated or proven method that exposes the Applicant's Private Key to compromise;
(4) ZoTrus has previously been made aware that the Applicant's Private Key has suffered a

Key Compromise, such as through the provisions of Section 4.9.1;

(5) ZoTrus is aware of a demonstrated or proven method to easily compute the Applicant's Private Key based on the Public Key (such as a Debian weak key, see https://wiki.debian.org/SSLkeys).

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

6.1.2. Private Key Delivery to Subscriber

Where Subscriber keys are generated on ZoTrus' servers, they are delivered to the Subscriber over an encrypted communication. Subscribers may produce and prepare their own Private Keys and certificate signing requests (CSR) for server certificates and client certificates and submit them via SSL secured connection to CA system. In this case, Private Key delivery to the subscriber is unnecessary.

6.1.3. Public Key Delivery to Certificate Issuer

An issued certificate is either delivered through an on-line collection method or retrieved from the provided on-line interfaces. A subscriber is deemed to have accepted a certificate when delivered and installed into client or server software or when retrieved from the on-line interfaces.

6.1.4. CA Public Key Delivery to Relying Parties

The public Root CA keys and intermediate CA Public Keys are published from the following repository: www.zotrus.com/root/
The public Root CA keys shall be embedded within popular software applications, making special root distribution mechanisms unnecessary.

6.1.5. Key Sizes

ZoTrus supports RSA key length of 2048 bits or more, supports ECC key length of 256 bits or more, supports SM2 key length of 256 bits.

6.1.6. Public Key Parameters Generation and Quality Checking

ZoTrus' CA keys SHALL be generated within at least a FIPS 140-2 Level 3 or Common Criteria EAL 4+ certified HSM for RSA/ECC algorithm, or a China Commercial Cryptography Product Certification certified HSM for SM2 algorithm.

(1) RSA: ZoTrus confirms that the value of the public exponent is an odd number equal to 3 or more. Additionally, the public exponent SHOULD be in the range between 2^16 +1 and 2^256-1. The modulus SHOULD also have the following characteristics: an odd number, not the power of a prime, and have no factors smaller than 752. [Source: Section 5.3.3, NIST SP 800-89].
(2) ECC: ZoTrus confirms the validity of all keys using either the ECC Full Public Key Validation Routine or the ECC Partial Public Key Validation Routine. [Source: Sections 5.6.2.3.2 and 5.6.2.3.3, respectively, of NIST SP 800-56A: Revision 2].
(3) SM2: ZoTrus confirms the validity of all keys using either the SM2 Full Public Key Validation Routine or the SM2 Partial Public Key Validation Routine. [Source: GB/T 32918, 32905, GM/T 0015].

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

CA certificates include key usage extension fields to specify the purposes for which the CA Certificate may be used and to technically limit the usage of the certificate when used with X.509v3 compliant software. Reliance on key usage extension fields is dependent on correct software implementations of the X.509v3 standard and is outside of the control of ZoTrus. Key usages are specified in the Certificate Profile set forth in Section 7.1.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1. Cryptographic Module Standards and Controls

The Private Keys of the Intermediate CA certificates are stored in Hardware Security Modules (HSM) FIPS 140-2 Level 3 certified devices for RSA/ECC algorithm, or a China Commercial Cryptography Product Certification certified HSM for SM2 algorithm.
It is used for the signing of Subscriber Certificates and the online Certificate Revocation Lists. For recovery and archival purpose, the Private Keys of the Intermediate CA certificates are also cloned and stored off-line according to the same procedure as the CA root key.

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

ZoTrus' authentication mechanisms are protected securely when not in use and may only be accessed by actions of multiple trusted persons. The HSMs are configured to require 2 from 3 management key to be present.

Backups of CA Private Keys are securely stored off-site and require two-person access. Re-activation of a backed-up CA Private Key (unwrapping) requires the same security and multi-person control as when performing other sensitive CA Private Key operations.

6.2.3. Private Key Escrow

ZoTrus does not escrow its signature keys. Subscribers may not escrow their private signature keys.

6.2.4. Private Key Backup

If required for business continuity ZoTrus backs up Private Keys under the same multi-person control as the original Private Key.

6.2.5. Private Key Archival

Private Keys belonging to ZoTrus are not archived by parties other than ZoTrus.

6.2.6. Private Key Transfer into or From a Cryptographic Module

All root keys must be generated by and in a cryptographic module. Private Keys can't be exported from the cryptographic module. For backup, use the same type HSM device to clone as backup HSM, the clone operation requires at least two-person access.

6.2.7. Private Key Storage on Cryptographic Module

ZoTrus stores CA Private Keys on at least a FIPS 140-2 level 3 device for RSA/ECC algorithm, or a China Commercial Cryptography Product Certification certified HSM for SM2 algorithm.

6.2.8. Activating Private Key

ZoTrus' Private Keys are activated according to the specifications of the cryptographic module manufacturer. Activation data entry is protected from disclosure.

Subscribers are solely responsible for protecting their Private Keys. Subscribers should use a strong password or equivalent authentication method to prevent unauthorized access or use of the Subscriber's Private Key. At a minimum, Subscribers are required to authenticate themselves to the cryptographic module before activating their Private Keys. See also Section 6.4.

6.2.9. Deactivating Private Key

ZoTrus' Private Keys are deactivated via logout procedures on the applicable HSM device

when not in use. Root Private Keys are further deactivated by removing them entirely from the storage partition on the HSM device. ZoTrus never leaves its HSM devices in an active unlocked or unattended state.

Subscribers should deactivate their Private Keys via logout and removal procedures when not in use.

6.2.10. Destroying Private Key

ZoTrus personnel, acting in trusted roles, destroy CA Private Keys when no longer needed. Subscribers shall destroy their Private Keys when the corresponding Certificate is revoked or expired or if the Private Key is no longer needed.

ZoTrus may destroy a Private Key by deleting it from all known storage partitions. ZoTrus also zeroizes the HSM device according to the specifications of the hardware manufacturer. This reinitializes the device and overwrites the data with binary zeros. If the zeroization or re-initialization procedure fails, ZoTrus will crush, shred, and/or incinerate the device in a manner that destroys the ability to extract any Private Key.

6.2.11. Cryptographic Module Capabilities

See Section 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1. Public Key Archival

ZoTrus archives Public Keys from Certificates.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

All certificates and corresponding keys shall have maximum Validity Periods (not exceeding):

- Root CA 25 years
- Sub CA 10-15 years
- Subscriber Certificates: for SSL Certificate, it has a Validity Period no greater than 398 days. For code signing and client certificate, it has a Validity Period no greater than 39 months.

Pursuant to Section 5.6 CA Private Keys are retired from signing subordinate certificates

before the periods listed above to accommodate the key changeover process (i.e., the retiring CA Private Key is still used to sign CRLs to provide validation services for certificates issued with that retiring CA Private Key.)

6.4 Activation Data

6.4.1. Activation Data Generation and Installation

ZoTrus activates the cryptographic module containing its CA Private Keys according to the specifications of the hardware manufacturer. This method has been evaluated as meeting the requirements of FIPS 140-2 Level 3 for RSA/ECC algorithm or China Commercial Cryptography Product Certification certified HSM for SM2 algorithm. The cryptographic hardware is held under two-person control as explained in Section 5.2.2 and elsewhere in this CPS. ZoTrus will only transmit activation data via an appropriately protected channel and at a time and place that is distinct from the delivery of the associated cryptographic module.

All ZoTrus personnel and Subscribers are instructed to use strong passwords and to protect PINs and passwords. ZoTrus employees are required to create non-dictionary, alphanumeric passwords with a minimum length and to change their passwords on a regular basis.

6.4.2. Activation Data Protection

ZoTrus protects data used to unlock Private Keys from disclosure using a combination of cryptographic and physical access control mechanisms. Protection mechanisms include keeping activation mechanisms secure using role-based physical control. All PIN codes and USB key PINs are kept in sealed envelopes, which are placed in locked Safe Box and taken out by the CEO or CTO when used. ZoTrus locks accounts used to access secure CA processes if a certain number of failed password attempts occur.

6.4.3. Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1. Specific Computer Security Technical Requirements

ZoTrus implements various access codes, smart cards, electronic tokens and physical locks

in multiple combinations thereof for facility access, workstations, CA administration programs, server administration programs and monitoring devices to restrict and control access according to the defined roles and permissions.

6.5.2. Computer Security Rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1. System Development Controls

Development of the CA related infrastructures, hardware, libraries, programs, protective programs are performed by personnel with the appropriate knowledge and training. Changes to configuration files and settings, sources, binaries, and hardware components must be reviewed and approved by the management team. Modifications to the processes and certificates are tested for eventual flaws. Maintenance and other activities on hardware the CA require prior approval by the management team and are logged accordingly, monitored, and recorded.

6.6.2. Security Management Controls

ZoTrus has mechanisms in place to control and monitor the security-related configurations of its CA systems. Change control processes consist of change control data entries that are processed, logged, and tracked for any security-related changes to CA systems, firewalls, routers, software and other access controls. In this manner, ZoTrus can verify whether a change to the system has been properly evaluated for risk mitigation and authorized by management.

6.6.3. Life Cycle Security Controls

No stipulation.

6.7 Network Security Controls

The CA root key(s) are kept off-line and brought out from coffer only when necessary to sign intermediate CAs or periodic CRLs. Firewalls and boundary control devices are configured to allow access only by the IP addresses, ports, protocols, and commands required for the trustworthy provision of PKI services by such systems.

6.8 Time Stamping

All ZoTrus components are regularly synchronized with a reliable time service. ZoTrus operates a trusted Time-Stamping Authority (TSA) that compliant with RFC 3161. The RSA/ECC TSA Certificate shall be in a FIPS 140-2 level 3 HSM, SM2 TSA certificate shall be in a HSM certified by China Commercial Cryptography Product Certification. ZoTrus TSA provides RFC 3161 compliant timestamps and Authenticode Timestamp for RSA algorithm and provides GB/T 20520 compliant timestamp service for SM2 algorithm.

For RFC 3161 compliant timestamps, ZoTrus includes a unique integer for each newly generated timestamp token. ZoTrus only timestamps hash representations of data, not the data itself. Information can be hashed for time - stamping using SHA-256 with RSA encryption and 2048-bit key size for signature creation. (SHA-1, SHA-256, SHA-384 and SHA-512 are supported for RFC 3161-based requests.) ZoTrus does not examine the imprint being time-stamped other than to check the imprint's length.

For GB/T 20520 compliant timestamps, ZoTrus includes a unique integer for each newly generated timestamp token. ZoTrus only timestamps hash representations of data, not the data itself. Information can be hashed for time - stamping using SM3 with SM2 encryption and 256-bit key size for signature creation. ZoTrus does not examine the imprint being time-stamped other than to check the imprint's length.

No warranty is offered, and no liability will be accepted for any use of the ZoTrus free TSA service which is made other than using a ZoTrus issued certificates, except contracted TSA users.

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

For RSA/ECC certificate, ZoTrus conforms to RFC 5280, Internet X.509 Public Key Infrastructure Certificate and CRL Profile. Certificate extensions and their criticality, as well as cryptographic algorithm object identifiers, are populated according to the IETF RFC 5280 standards. In cases where stipulations of RFC 5280 and the applicable CA/Browser Forum Baseline Requirements differ, the Baseline Requirements notion will be adhered to.

For SM2 certificate, ZoTrus conforms to GM/T 0015, refers to RFC 5280, Internet X.509 Public Key Infrastructure Certificate and CRL Profile. Certificate extensions and their criticality, as well as cryptographic algorithm object identifiers, are populated according to

the GB/T 32918, GB/T 32905, GB/T 32907, GB/T 33560. For SSL certificates, ZoTrus conforms to GM/T 0024, GB/T 38636.

ZoTrus generates non-sequential Certificate serial numbers greater than zero (0) containing at least 64 bits of output from a CSPRNG.

7.1.1. Version Number(s)

All certificates are X.509 version 3 certificates.

7.1.2. Certificate Extensions

ZoTrus issues Certificates in compliance with RFC 5280 and GM/T 0015 and applicable best practice. Criticality also follows best practice to prevent unnecessary risks to Relying Parties when applied to name constraints.

7.1.2.1 Root CA Certificate

Duration: 25 years
Algorithm: SHA-256, P-384 (ECC with SHA-384), SM2
Key size: 4096 bits, P-384, SM2 256
Serial number: non-sequential greater than zero and containing at least 64 bits of output from a CSPNRG

As per CABF BRs 7.1.2.1 and RFC 5280

- **basicConstraints:** MUST be present as critical extension. The CA field MUST be set to true. The pathLenConstraint field SHOULD NOT be present.
- **keyUsage:** MUST be present as critical extension. Bit positions for keyCertSign and cRLSign MUST be set.
- **certificatePolicies:** This extension SHOULD NOT be present.
- **extendedKeyUsage:** This extension MUST NOT be present.
- **Subject information:**
- **commonName (OID 2.5.4.3):** This field MUST be present, and the contents SHOULD be an identifier for the certificate such that the certificate's Name is unique across all certificates issued by the issuing certificate.
- **countryName (OID 2.5.4.6):** This field MUST contain the two-letter ISO 3166-1 country code for the country in which the CA's place of business is located.
- **organizationName (OID 2.5.4.10):** This field MUST be present and the contents MUST contain either the Subject CA's name or DBA as verified under Section 3.2.2.2.

7.1.2.2 Subordinate CA Certificate

Duration: 10 - 15 years
Algorithm: SHA-256, P-256 (ECC with SHA-256), SM2
Key size: 2048 bits, P-256, SM2 256
Serial number: non-sequential greater than zero and containing at least 64 bits of output from a CSPNRG

For TLS/SSL certificate, as per CABF BRs 7.1.2.2 and RFC 5280

- **cerificatePolicies:** This extension MUST be present and SHOULD NOT be marked critical
- **cRLDistributionPoints:** This extension MUST be present and MUST NOT be marked critical. It MUST contain the HTTP URL of the CA's CRL service.
- **authorityInformationAccess:** this extension MUST be present. It MUST NOT be marked critical, and it MUST contain the HTTP URL of the Issuing CA's certificate.
- **basicConstraints:** This extension MUST be present and MUST be marked critical. The CA field MUST be set true. The pathLenConstraint field MAY be present.
- **keyUsage:** This extension MUST be present and MUST be marked critical. Bit positions for keyCertSign and cRLSign MUST be set. If the Subordinate CA Private Key is used for signing OCSP responses, then the digitalSignature bit MUST be set.
- **extKeyUsage**: The id-kp-serverAuth and id-kp-clientAuth [RFC5280] value MUST be present. anyExtendedKeyUsage MUST NOT be present. Other values SHOULD NOT be present. This extension SHOULD be marked non-critical.
- **Subject information:**
- **commonName (OID 2.5.4.3):** This field MUST be present and the contents SHOULD be an identifier for the certificate such that the certificate's Name is unique across all certificates issued by the issuing certificate.
- **countryName (OID 2.5.4.6):** This field MUST contain the two-letter ISO 3166-1 country code for the country in which the CA's place of business is located.
- **organizationName (OID 2.5.4.10):** This field MUST be present and the contents MUST contain either the Subject CA's name or DBA as verified under Section 3.2.2.2.

For code signing certificate, as per Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates 7.1.2.2

- **cerificatePolicies**: This extension MUST be present and SHOULD NOT be marked critical
- **cRLDistributionPoints**: This extension MUST be present and MUST NOT be marked critical. It MUST contain the HTTP URL of the CA's CRL service.
- **authorityInformationAccess**: this extension MUST be present. It MUST NOT be marked critical, and it MUST contain the HTTP URL of the Issuing CA's certificate.
- **basicConstraints**: This extension MUST be present and MUST be marked critical. The cA field MUST be set true. The pathLenConstraint field MAY be present.
- **keyUsage**: This extension MUST be present and MUST be marked critical. Bit positions for keyCertSign and cRLSign MUST be set. If the Subordinate CA Private Key is used for signing OCSP responses, then the digitalSignature bit MUST be set.
- **extKeyUsage**: The id-kp-codeSigning [RFC5280] value MUST be present. anyExtendedKeyUsage MUST NOT be present. Other values SHOULD NOT be present.

This extension SHOULD be marked non-critical.

- **Subject information:**
- **commonName (OID 2.5.4.3):** This field MUST be present and the contents SHOULD be an identifier for the certificate such that the certificate's Name is unique across all certificates issued by the issuing certificate.
- **countryName (OID 2.5.4.6):** This field MUST contain the two-letter ISO 3166-1 country code for the country in which the CA's place of business is located.
- **organizationName (OID 2.5.4.10):** This field MUST be present and the contents MUST contain either the Subject CA's name or DBA as verified under Section 3.2.2.2.

For timestamping certificate, as per Baseline Requirements for the Issuance and Management of Publicly - Trusted Code Signing Certificates 7.1.2.2

- **cerificatePolicies**: This extension MUST be present and SHOULD NOT be marked critical
- **cRLDistributionPoints**: This extension MUST be present and MUST NOT be marked critical. It MUST contain the HTTP URL of the CA's CRL service.
- **authorityInformationAccess**: this extension MUST be present. It MUST NOT be marked critical, and it MUST contain the HTTP URL of the Issuing CA's certificate.
- **basicConstraints**: This extension MUST be present and MUST be marked critical. The cA field MUST be set true. The pathLenConstraint field MAY be present.
- **keyUsage**: This extension MUST be present and MUST be marked critical. Bit positions for keyCertSign and cRLSign MUST be set. If the Subordinate CA Private Key is used for signing OCSP responses, then the digitalSignature bit MUST be set.
- **extKeyUsage**: The id-kp-timeStamping [RFC5280] value MUST be present. anyExtendedKeyUsage MUST NOT be present. Other values SHOULD NOT be present. This extension SHOULD be marked non-critical.
- **Subject information:**
- **commonName (OID 2.5.4.3):** This field MUST be present and the contents SHOULD be an identifier for the certificate such that the certificate's Name is unique across all certificates issued by the issuing certificate.
- **countryName (OID 2.5.4.6):** This field MUST contain the two-letter ISO 3166-1 country code for the country in which the CA's place of business is located.
- **organizationName (OID 2.5.4.10):** This field MUST be present and the contents MUST contain either the Subject CA's name or DBA as verified under Section 3.2.2.2.

For Client certificate, as per RFC 5280

- **cerificatePolicies**: This extension MUST be present and SHOULD NOT be marked critical
- **cRLDistributionPoints**: This extension MUST be present and MUST NOT be marked critical. It MUST contain the HTTP URL of the CA's CRL service.
- **basicConstraints**: This extension MUST be present and MUST be marked critical. The CA field MUST be set true. The pathLenConstraint field MAY be present.
- **keyUsage**: This extension MUST be present and MUST be marked critical. Bit positions for keyCertSign and cRLSign MUST be set. If the Subordinate CA Private Key is used for signing OCSP responses, then the digitalSignature bit MUST be set.

- **extKeyUsage**: The id-kp-emailProtection and/or id-kp-clientAuth [RFC5280] value MUST be present. anyExtendedKeyUsage , serverAuth , codeSigning , timeStamping MUST NOT be present.
- **Subject information:**
- **commonName (OID 2.5.4.3):** This field MUST be present and the contents SHOULD be an identifier for the certificate such that the certificate's Name is unique across all certificates issued by the issuing certificate.
- **countryName (OID 2.5.4.6):** This field MUST contain the two-letter ISO 3166-1 country code for the country in which the CA's place of business is located.
  organizationName (OID 2.5.4.10): This field MUST be present and the contents MUST contain either the Subject CA's name or DBA as verified under Section 3.2.2.2.

7.1.2.3 Subscriber Certificate

Serial number: non-sequential greater than zero and containing at least 64 bits of output from a CSPNRG

For TLS/SSL certificate, as per CABF BRs 7.1.2.3

- **certificatePolicies**: This extension MUST be present and SHOULD NOT be marked critical
- **cRLDistributionPoint**: This extension MAY be present. If present, it MUST NOT be marked critical, and it MUST contain the HTTP URL of the CA's CRL service.
- **authorityInformationAccess**: This extension MUST be present. It MUST NOT be marked critical, and it MUST contain the HTTP URL of the Issuing CA's certificate.
- **basicConstraints (optional):** The CA field MUST NOT be true.
- **keyUsage (optional):** If present, bit positions for keyCertSign and cRLSign MUST NOT be set.
- **extKeyUsage(required):** Either the value id-kp-serverAuth [RFC5280] or id-kp-clientAuth [RFC5280] or both values MUST be present. id-kp-emailProtection [RFC5280] MAY be present. Other values SHOULD NOT be present.

For code signing certificate, as per Baseline Requirements for the Issuance and management of Publicly-Trusted Code Signing Certificates 7.1.2.2

- **certificatePolicies:** This extension MUST be present and SHOULD NOT be marked critical
- **cRLDistributionPoint:** This extension MAY be present. If present, it MUST NOT be marked critical, and it MUST contain the HTTP URL of the CA's CRL service.
- **authorityInformationAccess:** this extension MUST be present. It MUST NOT be marked critical, and it MUST contain the HTTP URL of the Issuing CA's certificate.
- **basicConstraints (optional):** The cA field MUST NOT be true.
- **keyUsage (required):** This extension MUST be present and MUST be marked critical. The bit positions for digitalSignature MUST be set. Bit positions for keyCertSign and cRLSign MUST NOT be set. All other bit positions SHOULD NOT be set.
- **extKeyUsage(required)**: The value id-kp-codeSigning [RFC5280] MUST be present and

MUST be marked critical. The value anyExtendedKeyUsage MUST NOT be present.

For timestamping certificate, as per Baseline Requirements for the Issuance and management of Publicly-Trusted Code Signing Certificates 7.1.2.2

- **certificatePolicies:** This extension MUST be present and SHOULD NOT be marked critical
- **cRLDistributionPoint:** This extension MAY be present. If present, it MUST NOT be marked critical, and it MUST contain the HTTP URL of the CA's CRL service.
- **authorityInformationAccess:** this extension MUST be present. It MUST NOT be marked critical, and it MUST contain the HTTP URL of the Issuing CA's certificate.
- **basicConstraints (optional):** The cA field MUST NOT be true.
- **keyUsage (required):** This extension MUST be present and MUST be marked critical. The bit positions for digitalSignature MUST be set. Bit positions for keyCertSign and cRLSign MUST NOT be set. All other bit positions SHOULD NOT be set.
- **extKeyUsage(required)**: The value id-kp-timeStamping [RFC5280] MUST be present and MUST be marked critical. The value anyExtendedKeyUsage MUST NOT be present.

For client certificate, as per RFC 5280

- **cerificatePolicies:** This extension MUST be present and SHOULD NOT be marked critical
- **cRLDistributionPoints:** This extension MUST be present and MUST NOT be marked critical. It MUST contain the HTTP URL of the CA's certificate.
- **basicConstraints (optional):** The CA field MUST NOT be true.
- **keyUsage(required)**: This extension MUST be present and MUST be marked critical. The bit positions for digitalSignature MUST be set.
- **extKeyUsage(required):** The id-kp-emailProtection and/or id-kp-clientAuth [RFC5280] value MUST be present. anyExtendedKeyUsage, serverAuth, codeSigning, timeStamping MUST NOT be present.

7.1.2.4 All Certificates

All other fields and extensions MUST be set in accordance with RFC 5280. ZoTrus does not issue a Certificate with:

- Extensions that do not apply in the context of the public Internet (such as an extendedKeyUsage value for a service that is only valid in the context of a privately managed network).
- semantics that, if included, will mislead a Relying Party about the certificate information verified by the CA (such as including extendedKeyUsage value for a smart card, where the CA is not able to verify that the corresponding Private Key is confined to such hardware due to remote issuance).

7.1.2.5 Application of RFC 5280

For purposes of clarification, a Precertificate, as described in RFC 6962 – Certificate

Transparency, shall not be considered to be a "certificate" subject to the requirements of RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile under this CPS.

7.1.3. Algorithm Object Identifiers

ZoTrus issues certificates using the following algorithm identifiers including SHA256 With RSA, SHA384 With RSA, ECDSA With SH256, ECDSA With SH384, SM3 With SM2.

7.1.4. Name Forms

ZoTrus issues Certificates with name forms compliant to RFC 5280. Within the domain of each Issuing CA, ZoTrus includes a unique non-sequential Certificate serial number that exhibits at least 20 bits of entropy.

7.1.4.1.Name Encoding

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

• For each Certificate in the Certification Path, the encoded content of the Issuer Distinguished Name field of a Certificate SHALL be byte-for-byte identical with the encoded form of the Subject Distinguished Name field of the Issuing CA certificate.

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

7.1.4.2.Subject Information – Subscriber Certificates

By issuing the Certificate, ZoTrus represents that it followed the procedure set forth in its Certificate Policy and/or Certification Practice Statement to verify that, as of the Certificate's issuance date, all of the Subject Information was accurate.

7.1.4.3.Subject Information – Root Certificates and Subordinate CA Certificates

By issuing Root Certificate and a Subordinate CA Certificate, ZoTrus represents that it followed the procedure set forth in its Certificate Policy and/or Certification Practice Statement to verify that, as of the Certificate's issuance date, all of the Subject Information was accurate.

7.1.5. Name Constraints

No stipulation.

7.1.6. Certificate Policy Object Identifier

An object identifier (OID) is a unique number that identifies an object or policy. The OID **1.3.6.1.4.1.57933** is for ZoTrus RSA/ECC algorithm certificates, the OID **1.2.156.157933** is for ZoTrus SM2/RSA/ECC algorithm certificates. ZoTrus issues certificates contain the following OIDs / OID arcs:

1) ZoTrus cps version：
   1.3.6.1.4.1.57933.1. <major-version>.<minor-version>
   1.2.156.157933.1. <major-version>.<minor-version>
2) ZoTrus special purpose OID：
   1.3.6.1.4.1.57933.2.<number>
   1.2.156.157933.2.<number>
3) ZoTrus Intermediate root certificate (Issuer CA) OID：
   1.3.6.1.4.1.57933.3. <cert-type>
   1.2.156.157933.3. <cert-type>
4) ZoTrus User certificate OID：
   1.3.6.1.4.1.57933.3. <cert-type>.<cert-class>
   1.2.156.157933.3. <cert-type>.<cert-class>

Definition:

<cert-type>: 1: SSL; 2: Code; 3: Email; 4: Document; 5: Client; 6: Timestamp
<cert-class>: 1: Class 1/T1; 2: Class 2/T2; 3: Class 3/T3; 4: Class 4/T4

Digitally Signed Object	**Object Identifier**
SSL Certificates Issuing CA	**1.2.156.157933.3.1**
Domain Validation SSL Certificates	1.2.156.157933.3.1.1 1.2.156.157933.11
Individual Validation SSL Certificates	1.2.156.157933.3.1.2 1.2.156.157933.12
Organization Validation SSL Certificates	1.2.156.157933.3.1.3 1.2.156.157933.13
Extended Validation SSL Certificates	1.2.156.157933.3.1.4 1.2.156.157933.14
Code Signing Certificate Issuing CA	**1.2.156.157933.3.2**
Individual Validation Code Signing Certificates	1.2.156.157933.3.2.2 1.2.156.157933.22

Organization Validation Code Signing Certificates	1.2.156.157933.3.2.3 1.2.156.157933.23
Extended Validation Code Signing Certificates	1.2.156.157933.3.2.4 1.2.156.157933.24
Email Certificates Issuing CA	**1.2.156.157933.3.3**
Mailbox Validation Email Certificates	1.2.156.157933.3.3.1 1.2.156.157933.31
Individual Validation Email Certificates	1.2.156.157933.3.3.2 1.2.156.157933.32
Organization Validation Email Certificates	1.2.156.157933.3.3.3 1.2.156.157933.33
Sponsor Validation Email Certificates	1.2.156.157933.3.3.4 1.2.156.157933.34
Document Signing Certificates Issuing CA	**1.2.156.157933.3.4**
Mailbox Validation Document Signing Certificates	1.2.156.157933.3.4.1 1.2.156.157933.41
Individual Validation Document Signing Certificates	1.2.156.157933.3.4.2 1.2.156.157933.42
Organization Validation Document Signing Certificates	1.2.156.157933.3.4.3 1.2.156.157933.43
Sponsor Validation Document Signing Certificates	1.2.156.157933.3.4.4 1.2.156.157933.44
Client Certificates Issuing CA	**1.2.156.157933.3.5**
Mailbox/Mobile Validation Client Certificates	1.2.156.157933.3.5.1 1.2.156.157933.31
Individual Validation Client Certificates	1.2.156.157933.3.5.2 1.2.156.157933.32
Organization Validation Client Certificates	1.2.156.157933.3.5.3 1.2.156.157933.33
Sponsor Validation Client Certificates	1.2.156.157933.3.5.4 1.2.156.157933.34
Timestamping Certificates Issuing CA	**1.2.156.157933.3.6**

Time Stamping SM2 Certificates for code signing	1.2.156.157933.3.6.2
Time Stamping SM2 Certificates for email signing	1.2.156.157933.3.6.3
Time Stamping SM2 Certificates for document signing	1.2.156.157933.3.6.4
Time Stamping RSA Certificates for email signing	1.2.156.157933.3.6.6

The OID arcs 2.23.140.* is the CA/Browser Forum OID, the OID arcs 1.2.156.157933.* is ZoTrus Technology OID. The Certificate MAY also contain additional policy identifier(s) defined by ZoTrus or other entities.

7.1.7. Usage of Policy Constraints Extension

No stipulation.

7.1.8. Policy Qualifiers Syntax and Semantics

ZoTrus certificates may include a brief statement describing limitations of liability, limitations in the value of transactions to be accomplished, validation period, and intended purpose of the certificate and disclaimers of warranty that may apply.

7.1.9. Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2 CRL Profile

ZoTrus RSA/ECC certificate issues version 2 CRLs that contain the following fields:

- Version: v2
- Signature Algorithm: SHA256 With RSA
- Issuer: Identification of the CA issuing the CRL
- Last Update: Time of CRL issue
- Next Update: Time of next CRL issue (7 days)
- Revoked certificates: Listing of information for revoked certificates
- Revocation Date: Date of Revocation

ZoTrus SM2 certificate issues version 2 CRLs that contain the following fields:

- Version: v2
- Signature Algorithm: SM3 With SM2

- Issuer: Identification of the CA issuing the CRL
- Last Update: Time of CRL issue
- Next Update: Time of next CRL issue (7days)
- Revoked certificates: Listing of information for revoked certificates
- Revocation Date: Date of Revocation

7.2.1 Version Number(s)

ZoTrus issues version 2 CRLs.

7.2.2 CRL and CRL Entry Extensions

- Authority Key Identifier: Issuing CA Key Identifier
- CRL Number: a monotonically increasing sequence number.

7.3 OCSP Profile

Due to the privacy protection concern, ZoTrus does not provide OCSP service for all certificates.

8. Compliance Audit and Other Assessments

The practices specified in this CPS are designed to meet or exceed the requirements of generally accepted and developing industry standards including the AICPA/CICA WebTrust Program for Certification Authorities, ANS X9.79:2001 PKI Practices and Policy Framework, and other industry standards related to the operation of CAs.

As part of its Security Program, ZoTrus controls its service quality each quarter by performing ongoing self-audits against a randomly selected sample of at least three percent (3%) of the T2/T3/T4 validation level certificates it has issued in the period beginning immediately after the last sample was taken.

8.1 Frequency and Circumstances of Assessment

An annual audit is or will be performed by an independent external auditor to assess ZoTrus' compliance with the AICPA/CICA WebTrust program for Certification Authorities for RSA/ECC algorithm certificates. For SM2 algorithm certificates, ZoTrus is or will comply with the related audit requirement according to China related regulations.

8.2 Identity/Qualifications of Assessor

For RSA/ECC algorithm certificates, ZoTrus' CA compliance audits are performed by WebTrust License Practitioners that:

1) Independence from the subject of the audit;
2) The ability to conduct an audit that addresses the criteria specified in an Eligible Audit as stipulated in section 8 of this document;
3) Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function;
4) Certified, accredited, licensed, or otherwise assessed as meeting the qualification requirements of auditors under the audit scheme;
5) Bound by law, government regulation, or professional code of ethics.

For SM2 algorithm certificates, ZoTrus' CA compliance internal audits are performed by ZoTrus Certificate Policy Authority, the external audits are performed by related organization that is qualified by related administrative authority in China according to the related regulations.

8.3 Assessor's Relationship to Assessed Entity

ZoTrus' external auditor does not have a financial interest, business relationship, or course of dealing that could foreseeably create a significant bias for or against ZoTrus.

8.4 Topics Covered by Assessment

Topics covered by the annual audit include but are not limited to the following:

1) CA business practices disclosure,
2) Service integrity,
3) CA environmental controls,
4) CA key life cycle management, and
5) Certificate life cycle management.

8.5 Actions Taken as a Result of Deficiency

Upon detection of deficiencies and possible weaknesses of the CA infrastructure and/or established procedures as a result of internal or external auditing or in case of non-compliance thereof, ZoTrus shall take corrective measures and actions in order to correct deficiencies and ensure future compliance within a reasonable timeframe. ZoTrus shall record, approve, and report any corrective action steps taken and/or action steps that are anticipated to correct the non-compliant areas. The annual audit shall confirm the improvements and corrective measures taken.

8.6 Communications of Results

The results of each audit are reported to the ZCPA and to any third-party entities which are entitled by law, regulation, or agreement to receive a copy of the audit results. On an annual basis, ZoTrus submits a report of its audit compliance to various parties if need. Such results shall be available no later than three (3) months after the end of the Audit Period. In the event of a delay greater than three months, ZoTrus shall provide an explanatory letter signed by the Qualified Auditor.

8.7 Self-Audits

ZoTrus monitors its adherence to this CPS by performing self-audits on at least a quarterly basis against a randomly selected sample of the greater of one certificate or at least three percent (3%) of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken.

9. Other Business and Legal Matters

9.1 Fees

9.1.1. Certificate Issuance or Renewal Fees

ZoTrus charges Subscriber fees for some of the certificate services it offers, including issuance, renewal. Such fees are detailed on the official ZoTrus websites (www.zotrus.com).

9.1.2. Certificate Access Fees

ZoTrus may charge a reasonable fee for access to its certificate databases.

9.1.3. Revocation or Status Information Access Fees

ZoTrus does not charge fees for the revocation of a certificate or for a Relying Party to check the validity status of a ZoTrus issued certificate using Certificate Revocation Lists. ZoTrus retains its right to apply changes to such fees.

9.1.4. Fees for Other Services

No stipulation.

9.1.5. Refund Policy

Subscribers must request refunds within 30 days after a Certificate issues. After receiving the refund request, ZoTrus may revoke the Certificate and refund the amount paid by the Applicant, minus any applicable application processing fees.

9.2 Financial Responsibility

9.2.1. Insurance Coverage

ZoTrus provides certificate use guarantee to subscribers. If the user suffers losses in using the certificate due to ZoTrus' fault, ZoTrus will provide compensation to the certificate subscriber and relying party. The total compensation fee does not exceed 10 times of the purchase cost.

9.2.2. Other Assets

No stipulation.

9.2.3. Insurance or Warranty Coverage for End-Entities

In case of erroneous issuance of a digital certificate that resulted in a loss to a relying party, relying parties may be eligible for compensation, the aggregate indemnity cap does not exceed that specified in this CPS 9.2.1.

ZoTrus administers all claims on a first-come first-serve basis. Your reliance on multiple products and services used on the same website are mutually exclusive. Payments made to you or another Relying Party by ZoTrus will decrease the amount available under the Aggregate Limit to all other Relying Parties. If the Aggregate Limit is met, then you waive ZoTrus of any liability for all remaining unreimbursed unauthorized charges, regardless of whether any amount was actually paid to you.

Beyond the coverage of the certificate insured warranty above, ZoTrus denies any responsibility for damages or impairments resulting from its operation and assumes no financial responsibility with respect of the use of any issued certificate or provided service.

9.3 Confidentiality of Business Information

9.3.1. Scope of Confidential Information

The following information is considered confidential and protected against disclosure using a reasonable degree of care:

1) Private Keys;
2) Activation data used to access Private Keys or to gain access to the CA system;
3) Business continuity, incident response, contingency, and disaster recovery plans;
4) Other security practices used to protect the confidentiality, integrity, or availability of information;
5) Information held by ZoTrus as private information in accordance with Section 9.4;
6) Audit logs and archive records; and
7) Transaction records, financial audit records, and external or internal audit trail records and any audit reports (with the exception of an auditor's letter confirming the effectiveness of the controls set forth in this CPS).

9.3.2. Information Not Within the Scope of Confidential Information

Any information not listed as confidential is considered public information. Published Certificate and revocation data is considered public information.

9.3.3. Responsibility to Protect Confidential Information

ZoTrus' employees, agents, and contractors are responsible for protecting confidential information and are contractually obligated to do so. Employees receive training on how to handle confidential information.

9.4 Privacy of Personal Information

9.4.1. Privacy Plan

ZoTrus respects the privacy of individuals and entities and shall not disclose personal details of certificate Applicants or other identifying information it retains from and about them to third parties.

9.4.2. Information Treated as Private

Any information about subscribers that is not publicly available through the content of the issued certificate, certificate directory and Certificate Revocation Lists, shall be treated as private and regarded as protected information.

9.4.3. Information Not Deemed Private

Private information does not include certificates, CRLs, or their contents.

9.4.4. Responsibility to Protect Private Information

Obtained private details and information shall not be used without the consent of the party to whom that information applies beyond the tasks ZoTrus has to perform for successful validation and verification purpose. ZoTrus shall save and secure subscriber information it retains from compromise and disclosure to third parties and shall comply with applicable local privacy laws for the protection of such information.

9.4.5. Notice and Consent to Use Private Information

Personal information obtained from an Applicant during the application or identity verification process is considered private information if the information is not included in a Certificate. ZoTrus will only use private information after obtaining the Subject's consent or as required by applicable law or regulation. All Subscribers must consent to the global transfer and publication of any personal data contained in a Certificate.

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

If disclosure is necessary in response to judicial, administrative, or other legal process during the discovery process in a civil or administrative action, such as subpoenas, interrogatories, requests for admission, and requests for production of documents, ZoTrus shall be entitled to disclose private information to law officials without penalty.

9.4.7. Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property rights

Digital certificates which are the result of the operations of ZoTrus, are at any given time and remain during their whole lifetime the property of ZoTrus. Ownership of digital certificates issued by and through the operations of ZoTrus can't be claimed by subscribers, relying parties, software vendors or any other party. Issuance of a certificate to the end user gives the subscriber the right to use the issued certificate(s), Subjected to the requirements and obligations set forth in this policy, acceptance of the terms and conditions of ZoTrus as published on the related web site(s) and to the extent of the key

usage and extended key usage fields of the certificate, until expiration or revocation of the certificate, whichever comes first. ZoTrus exclusively retains the copyright of all certificates produced, created, published, and issued by ZoTrus at all times and all rights are reserved.

9.6 Representations and Warranties

9.6.1. CA Representations and Warranties

ZoTrus uses this CPS and applicable Subscriber Agreements to convey legal conditions of usage of issued Certificates to Subscribers and Relying Parties. All parties including ZoTrus and Subscribers warrant the integrity of their respective Private Key(s). If any such party suspects that a Private Key has been Compromised, they will immediately notify ZoTrus.

ZoTrus represents and warrants to Certificate Beneficiaries, during the period when the Certificate is valid, ZoTrus has complied with its CPS in issuing and managing the Certificate.

(1) **Right to Use Domain Name or IP Address or email address:** That, at the time of issuance, ZoTrus (i) implemented a procedure for verifying that the Applicant either had the right to use, or had control of, the Domain Name(s) or IP address(es) or email address listed in the Certificate's Subject field and Subject AltName extension (or, only in the case of Domain Names, was delegated such right or control by someone who had such right to use or control); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in ZoTrus' CPS;

(2) **Authorization for Certificate:** That, at the time of issuance, ZoTrus (i) implemented a procedure for verifying that the Subject authorized the issuance of the Certificate and that the Applicant Representative is authorized to request the Certificate on behalf of the Subject; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in ZoTrus' CPS;

(3) **Accuracy of Information:** That, at the time of issuance, ZoTrus (i) implemented a procedure for verifying the accuracy of all of the information contained in the Certificate (with the exception of the Subject: organizationalUnitName attribute); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in ZoTrus' CPS;

(4) **No Misleading Information:** That, at the time of issuance, ZoTrus (i) implemented a procedure for reducing the likelihood that the information contained in the Certificate's Subject: organizationalUnitName attribute would be misleading; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in ZoTrus' CPS;

(5) **Identity of Applicant:** That, if the Certificate contains Subject Identity Information, ZoTrus (i) implemented a procedure to verify the identity of the Applicant; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in ZoTrus' CPS;

(6) **Subscriber Agreement:** That, if ZoTrus and Subscriber are not Affiliates, the Subscriber and CA are parties to a legally valid and enforceable Subscriber Agreement that satisfies the Baseline Requirements, or, if ZoTrus and Subscriber are Affiliates, the Applicant Representative acknowledged and accepted the Terms of Use;

(7) **Status:** That ZoTrus maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates; and

(8) **Revocation:** That ZoTrus will revoke the Certificate for any of the reasons specified in the Baseline Requirements and other guidelines as applicable.

9.6.2. RA Representations and Warranties

No stipulation.

9.6.3. Subscriber Representations and Warranties

Prior to being issued and receiving a Certificate, subscribers are solely responsible for any misrepresentations they make to third parties and for all transactions that use Subscriber's Private Key, regardless of whether such use was authorized. Subscribers are required to notify ZoTrus if a change occurs that could affect the status of the Certificate. Subscribers represent to ZoTrus, Application Software Vendors, and Relying Parties that, for each Certificate, the Subscriber will:

(1) **Accuracy of Information:** Subscriber will provide accurate and complete information at all times to ZoTrus, both in the Certificate Request and as otherwise requested by ZoTrus in connection with issuance of a Certificate.

(2) **Protection of Private Key:** Subscriber shall take all reasonable measures to maintain sole control of, keep confidential, and properly protect at all times the Private Key to be included in the requested Certificate(s) and any associated activation data or device, e.g. password or token;

(3) **Acceptance of Certificate:** Subscriber shall review and verify the Certificate contents for accuracy.

(4) **Use of Certificate:** Subscriber shall install the SSL Certificate only on servers that are accessible at the Subject AltName(s) listed in the Certificate or shall install the S/MIME Certificate only for the email address at Subject AltName(s) listed in the Certificate, and

use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement or Terms of Use.

(5) **Reporting and Revocation:** Subscriber shall
(a) promptly request revocation of the certificate, and cease using it and its associated Private Key, if there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate; and
(b) promptly request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate.

(6) **Termination of Use of Certificate:** Subscriber shall promptly cease use of Private Key associated with the Public Key in the Certificate upon revocation of that Certificate for reasons of Key Compromise.

(7) **Responsiveness:** Subscriber shall respond to ZoTrus' instructions concerning Key Compromise or Certificate misuse within a specified time period.

(8) **Acknowledgment and Acceptance:** ZoTrus is entitled to revoke the Certificate immediately if the Subscriber violates the terms of the Subscriber Agreement or Terms of Use or if ZoTrus discovers that the Certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware.

9.6.4. Relying Party Representations and Warranties

Each Relying Party represents that, prior to relying on a ZoTrus Certificate, it:

1) Obtained sufficient knowledge on the use of digital Certificates and PKI,
2) Studied the applicable limitations on the usage of Certificates and agrees to ZoTrus' limitations on liability related to the use of Certificates,
3) Has read, understands, and agrees to the ZoTrus Relying Party Agreement and this CPS,
4) Verified both the ZoTrus Certificate and the Certificates in the certificate chain using the relevant CRL,
5) Will not use a ZoTrus Certificate if the Certificate has expired or been revoked, and
6) Will take all reasonable steps to minimize the risk associated with relying on a digital signature, including only relying on a ZoTrus Certificate after considering:
   a) applicable law and the legal requirements for identification of a party, protection of the confidentiality or privacy of information, and enforceability of the transaction,
   b) the intended use of the Certificate as listed in the certificate or this CPS,
   c) the data listed in the Certificate,
   d) the economic value of the transaction or communication,
   e) the potential loss or damage that would be caused by an erroneous identification or a loss of confidentiality or privacy of information in the application, transaction, or communication,

f) the Relying Party's previous course of dealing with the Subscriber,
g) the Relying Party's understanding of trade, including experience with computer-based methods of trade, and
h) any other indicia of reliability or unreliability pertaining to the Subscriber and/or the application, communication, or transaction.

Any unauthorized reliance on a Certificate is at a party's own risk.

9.6.5. Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

EXCEPT AS EXPRESSLY STATED IN SECTION 9.6.1, ALL CERTIFICATES AND ANY RELATED SOFTWARE AND SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE". TO THE MAXIMUM EXTENT PERMITTED BY LAW, ZOTRUS DISCLAIMS ALL EXPRESS AND IMPLIED WARRANTIES, INCLUDING ALL WARRANTIESOF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON- INFRINGEMENT. ZOTRUS DOES NOT WARRANT THAT ANY SERVICE OR PRODUCT WILL MEET ANY EXPECTATIONS OR THAT ACCESS TO CERTIFICATES WILL BE TIMELY OR ERROR-FREE. ZoTrus does not guarantee the availability of any products or services and may modify or discontinue any product or service offering at any time. A fiduciary duty is not created simply because an entity uses ZoTrus' services.

9.8 Limitations of Liability

ZoTrus gives no guaranties whatsoever about the security or suitability of the services provided that are identified by a certificate issued by ZoTrus or the use of thereof, including but not limited to the use of its websites and programs or any other service offered currently or in the future. The certification services are operated according to the highest possible levels of security and to the highest industry standards, but without any warranty.

Relying parties have sufficient information to make an informed decision as to the extent to which they choose to rely on the information in a certificate, and as such are solely responsible for deciding whether or not to rely on such information, and therefore shall bear the legal consequences of their failure to perform the Relying Party Obligations outlined in this policy.

Under no circumstances, including negligence, shall ZoTrus or its contributors be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits;

or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this or other services, even if advised of the possibility of such damage.

9.9 Indemnities

9.9.1. Indemnification by ZoTrus

ZoTrus shall defend, indemnify, and hold harmless each Application Software Vendor for any and all claims, damages, and losses suffered by such Application Software Vendor related to a Certificate issued by ZoTrus, regardless of the cause of action or legal theory involved. This shall not apply, however, to any claim, damages, or loss suffered by such Application Software Vendor related to a Certificate issued by ZoTrus where such claim, damage, or loss was directly caused by such Application Software Vendor's software displaying as not trustworthy a Certificate that is still valid, or displaying as trustworthy: (1) a Certificate that has expired, or (2) a Certificate that has been revoked (but only in cases where the revocation status is currently available from the online repository, and the software either failed to check such status or ignored an indication of revoked status).

9.9.2. Indemnification by Subscribers

To the extent permitted by law, each Subscriber shall indemnify ZoTrus, its partners, and any Trusted Root entities, and their respective directors, officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable attorney's fees, related to (i) any misrepresentation or omission of material fact by Subscriber, regardless of whether the misrepresentation or omission was intentional or unintentional; (ii) Subscriber's breach of the Subscriber Agreement, this CPS, or applicable law; (iii) the Compromise or unauthorized use of a Certificate or Private Key caused by the Subscriber's negligence; or (iv) Subscriber's misuse of the Certificate or Private Key.

9.9.3. Indemnification by Relying Parties

To the extent permitted by law, each Relying Party shall indemnify ZoTrus, its partners, and any cross-signed entities, and their respective directors, officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable attorney's fees, related to the Relying Party's (i) breach of the Relying Party Agreement, this CPS, or applicable law; (ii) unreasonable reliance on a Certificate; or (iii) failure to check the Certificate's status prior to use.

9.10 Term and Termination

9.10.1. Term

This CPS and any amendments to the CPS are effective when published to ZoTrus' online repository and remain in effect until replaced with a newer version.

9.10.2. Termination

This CPS and any amendments remain in effect until replaced by a newer version.

9.10.3. Effect of Termination and Survival

ZoTrus will communicate the conditions and effect of this CPS's termination via the ZoTrus Repository. The communication will specify which provisions survive termination. At a minimum, all responsibilities related to protecting confidential information will survive termination. All Subscriber Agreements remain effective until the Certificate is revoked or expired, even if this CPS terminates.

9.11 Individual Notices and Communications with Participants

Unless otherwise specified by agreement between the parties, Participants shall use commercially reasonable methods to communicate with each other, taking into account the criticality and subject matter of the communication.

9.12 Amendments

9.12.1. Procedure for Amendment

ZoTrus is responsible for determining the suitability of certificate policies illustrated within this document. ZoTrus is also responsible for determining the suitability of proposed changes to the policy and practice statements prior to the publication of an amended version.

Subscribers and relaying parties will not be notified of impending changes of the policy. The policy is legally binding from the moment of its publication.

This CPS is reviewed annually. Amendments are made by posting an updated version of the CPS to the online repository. Controls are in place to reasonably ensure that the policy and practice statements are not amended and published without the prior authorization by the management of ZoTrus.

9.12.2. Notification Mechanism and Period

ZoTrus posts CPS revisions to its website. ZoTrus does not guarantee or set a notice-and-comment period and may make changes to this CPS without notice and without changing the version number. Major changes affecting accredited Certificates are announced and approved by the accrediting agency prior to becoming effective. The ZCPA is responsible for determining what constitutes a material change of the CPS.

9.12.3. Circumstances Under Which OID Must be Changed

The ZCPA is solely responsible for determining whether an amendment to the CPS requires an OID change.

9.13 Dispute Resolution Provisions

Disputes arising in relation to certificates issued according to the related Guidelines as published by the CA/Browser Forum shall be treated according to those guidelines and only to the extend and scope set forth by those guidelines. This may include different interpretation of applicable laws and the locality of jurisdiction. The parties may however agree to solve disputes under different applicable laws and jurisdiction.

9.14 Governing Law

Any party involved shall try to resolve all disputes that might arise in a spirit of cooperation without formal procedures. Any legal dispute which cannot be resolved without formal procedures shall take place in China or at a different location if the parties agree or are ordered to do so by law.

9.15 Compliance with Applicable Law

This CPS shall be subject to applicable national, state, local and foreign laws, rules, regulations, ordinances, decrees, and orders including but not limited to restrictions on exporting or importing software, hardware, or technical information.

9.16 Miscellaneous Provisions

9.16.1. Entire Agreement

This CPS shall be interpreted consistently within the boundaries of business customs,

commercial reasonableness under the circumstances, and intended usage of the product or service described herein. Appendices and definitions to this CPS are for all purposes an integral and binding part of the CPS.

9.16.2. Assignment

Parties to this CPS may not assign any of their rights or obligations under this CPS or applicable agreements without the written consent by ZoTrus.

9.16.3. Severability

Interpretation of legal disputes arising from the operation of ZoTrus shall be treated according to the China legal system and laws.

If any term of this policy should be invalid under applicable laws, the affected term shall be replaced by the closest match according to applicable laws and the validity of the other terms should not be affected.

9.16.4. Enforcement (attorney's fees and waiver of rights)

ZoTrus may seek indemnification and attorneys' fees from a party for damages, losses, and expenses related to that party's conduct. ZoTrus' failure to enforce a provision of this CPS does not waive ZoTrus' right to enforce the same provision later or right to enforce any other provision of this CPS. To be effective, waivers must be in writing and signed by ZoTrus.

9.16.5. Force Majeure

ZoTrus incurs no liability if it is prevented, forbidden or delayed from performing, or omits to perform, any act or requirement by reason of: any provision of any applicable law, regulation or order; civil, governmental or military authority; the failure of any electrical, communication or other system operated by any other party over which it has no control; fire, flood, or other emergency condition; strike; acts of terrorism or war; act of god; or other similar causes beyond its reasonable control and without its fault or negligence.

9.17 Other Provisions

No Stipulation.