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 Intranet Digital Certificate CPS

(Version: 1.0, Release Date: Jan. 24, 2024, Effective Date: Jan. 24, 2024)

1. Overview

This CPS is applicable to RSA and SM2 algorithm intranet digital certificates issued by ZoTrus Intranet Root CA Certificate. The two root CA certificates for intranet strictly follow the same CPS for internet to generate root keys and root certificates, generate intermediate root certificates, and share the same CA system, and all follow ZoTrus Technology CPS (www.zotrus.com/policy) and related international and national standards for end user certificate identity validation, certificate lifecycle management, security control, and computer room management. This CPS only describers the difference from the public trusted SSL certificate, and this CPS shall prevail for the issuance and management of the intranet SSL certificates.

2. The OID used by the Intranet Certificates

ZoTrus has applied to the China National OID Registry for China OID: **1.2.156.157933** and to the international organization IANA for international OID: **1.3.6.1.4.1.57933**, which are assigned to the intranet SM2 algorithm and RSA algorithm digital certificates as follows:

1) ZoTrus Intermediate root certificate (Issuer CA) OID：
   1.2.156.157933.8. <cert-type>
   1.3.6.1.4.1.57933.8. <cert-type>

2) ZoTrus User certificate OID：
   1.2.156.157933.8. <cert-type>.<cert-class>
   1.3.6.1.4.1.57933.8. <cert-type>.<cert-class>

<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

3. Intranet Root CA Certificate Information

ZoTrus has created two self-signed root CA certificates for intranet certificates:
(1) **AAA Intranet SM2 Root** **(2) AAA Intranet RSA Root**
which are currently only used to issue SM2 algorithm and RSA algorithm DV/OV/EV three types of intranet SSL certificates, and these two root CA certificates have been included and trusted by ZT Browser. It can be downloaded from the ZoTrus official website: https://www.zotrus.com/root。

4. Intranet Certificates AIA and CRL Information

The AIA and CRL of the intermediate root certificate and the end user certificate issued by the two root CA certificates are deployed on Tencent Cloud like the publicly trusted digital certificate, and Tencent Cloud CDN provides users with certificate revocation information query and certificate issuing CA certificate download services.

(1) AIA URL: aia.zotrus.cn (2) CRL URL: crl.zotrus.cn

5. Intranet Certificates Revocation Service

SSL certificate revocation service supports international and national standards, and users can apply for the corresponding certificate revocation service on the ZoTrus official website.

6. SM2 Certificate Transparency Log Service

All ZoTrus intranet SSL certificates support SM2 certificate transparency, embedded certificate transparency log signature data SCT trusted by ZT Browser, and the number of SCTs follows ZT Browser's regulations for publicly trusted SSL certificates.

7. Intranet SSL Certificate Fee

ZoTrus provides HTTPS automation service for automatic configuration of intranet SSL certificates and paid intranet SSL certificates, please visit the official website of ZoTrus to inquire about the relevant product fees.

8. Intranet SSL Certificate User Agreement

Users must comply with the User Agreement in ZoTrus CPS 9.6.3.

9. The Rules for CN and SAN Field of the Intranet SSL Certificate

The CN and SAN fields of an intranet SSL certificate are different from the publicly trusted SSL certificate, it subjects to the following rules:

(1) The CN field of the certificate is the primary domain name of the intranet SSL certificate, which must be a public domain name(FQDN), and the user must complete the domain name control verification based on the publicly trusted SSL certificate CPS.

(2) In addition to the primary domain name, the SAN field of the certificate can contain the private IP address, host name, and private domain name, which are not validated, but if the SAN field contains a public IP address and a public domain name, each public domain name and public IP address needs to be validated according to the publicly trusted SSL certificate CPS. The Intranet IP addresses include:

- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255

(3) The intranet host name and intranet domain name can be in Chinese, but they must comply with the relevant national naming regulations.

10. Validity Period of the Intranet SSL Certificate

Intranet SSL certificates can be valid for 1-5 years, including 90 days, 365 days, 730 days, 1461 days, and 1826 days. There is no restriction on the validity period as publicly trusted SSL certificate of 397 days, and the intranet SSL certificate with a validity period of many years will be issued as many years as the user purchases.