零信技术（深圳）有限公司
中国深圳市南山区软件产业基地 2 栋 C 座 301C
Tel: +86-755-2660 4080　　Email: cps@zotrus.com

零信技术内网数字证书认证业务规则(CPS)

(版本: 1.0，发布日期：2024 年 1 月 24 日，生效日期：2024 年 1 月 24 日)

1. 概述

本 CPS 适用于零信技术内网根证书签发的 RSA 和 SM2 算法内网专用数字证书。两个内网证书专用顶级根证书同公网顶级根一样严格遵循 CPS 生成根密钥和根证书、生成中级根证书，共用同一套 CA 系统，用户证书身份认证、证书生命周期管理、安全控制和机房管理等等都遵循零信技术 CPS(www.zotrus.com/policy)及相关国际标准和国家标准。本 CPS 仅补充说明同公网 SSL 证书不同之处，对于内网 SSL 证书的签发管理以本 CPS 为准。

1. 内网证书采用的 OID 标识

零信技术已向国家 OID 注册中心申请中国国别国际 OID: **1.2.156.157933** 和向国际组织 IANA 申请了企业 OID: **1.3.6.1.4.1.57933**, 具体分配给内网 SM2 算法和 RSA 算法数字证书的情况如下:

(1) 中级根证书 OID：
　　1.2.156.157933.8. <cert-type>
　　1. 3.6.1.4.1.57933.8. <cert-type>
(2) 用户证书 OID：
　　1.2.156.157933.8. <cert-type>.<cert-class>
　　1.3.6.1.4.1.5793.8. <cert-type>.<cert-class>

<cert-type>: 证书类型：1: SSL 证书; 2: 代码签名证书; 3: 邮件证书; 4: 文档签名证书
　　5: 客户端证书；6: 时间戳证书
<cert-class>: 证书级别：1: T1; 2: T2; 3: T3; 4: T4，对应 SSL 证书的 DV/IV/OV/EV 认证

2. 内网根证书信息

零信技术新增2个内网证书专用自签顶级根证书:

(1) **AAA Intranet SM2 Root**
(2) **AAA Intranet RSA Root**

目前仅用于签发SM2算法和RSA算法DV/OV/EV 三类内网SSL证书，这2个根证书已经预置到零信浏览器信任中。可以从零信官网下载: https://www.zotrus.com/root。

3. 内网证书 AIA 和 CRL 信息

两个根证书签发的中级根证书和用户证书的 AIA 和 CRL 同公网数字证书一样部署在腾讯云，由腾讯云 CDN 为用户提供证书吊销信息查询和证书签发 CA 证书下载服务。

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

© 2024 零信技术（深圳）有限公司

4. 内网证书吊销服务

支持国际标准和国家标准的 SSL 证书吊销服务，用户可以在零信官网申请相应的证书吊销服务。

5. 国密证书透明服务

零信内网 SSL 证书全部支持国密证书透明，内嵌零信浏览器信任的国密证书透明日志签名数据 SCT，SCT 数量遵循零信浏览器对公网 SSL 证书的规定。

6. 内网 SSL 证书费用

零信技术提供自动化配置免费内网 SSL 证书和收费内网 SSL 证书的 HTTPS 加密自动化服务，请用户访问零信官网查询相关产品费用。

7. 内网 SSL 证书用户协议

用户必须遵循零信 CPS 9.6.3 中的用户协议。

8. 内网 SSL 证书 CN 字段和 SAN 字段有关规则

内网 SSL 证书的 CN 字段和 SAN 字段同公网 SSL 证书有所不同，遵循以下规则：

(1) 证书 CN 字段为内网 SSL 证书主域名，必须是一个公网域名，用户必须依据公网 SSL 证书 CPS 完成域名控制权验证；

(2) 证书 SAN 字段除了必须有主域名外，可以包含内网 IP 地址，主机名和内网域名，这些都不验证，但是如果 SAN 字段包含了公网 IP 地址和公网域名，则每一个公网域名和公网 IP 地址都需要依据公网 SSL 证书 CPS 完成域名或 IP 地址验证。其中内网 IP 地址包括：

- 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) 内网主机名和内网域名可以是中文，但必须遵守国家有关命名规定。

9. 内网 SSL 证书有效期

内网 SSL 证书有效期支持 1-5 年，具体有：90 天、365 天、730 天、1461 天 和 1826 天。不受公网 SSL 证书有效期为 397 天的限制，用户选购多少年有效期的证书就实际签发多年有效期的内网 SSL 证书。

© 2024 零信技术（深圳）有限公司