

零信技术 SM2 算法数字证书认证业务规则(CPS)

(版本: 1.1, 发布日期: 2022 年 6 月 28 日, 生效日期: 2022 年 6 月 28 日, 更新日期: 2024 年 1 月 24 日)

1. 概述

本 CPS 适用于零信技术国密 SM2 根证书签发的各种 SM2 算法数字证书。所有 CA 系统、根密钥生成、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, 唯一不同的是加密算法不是采用 RSA 算法, 而是采用国密 SM2 算法(SM2/SM3/SM4)。

2. 国密 SM2 根证书采用的 OID 标识

零信技术已向中国国家 OID 注册中心申请到中国国别国际 OID: **1.2.156.157933**, 具体分配如下:

- 1) CPS 版本 OID:
1.2.156.157933.1.1.<major-version>.<minor-version>
- 2) 特殊用途 OID:
1.2.156.157933.2.<number>
- 3) 中级根证书 OID:
1.2.156.157933.3. <cert-type>
- 4) 用户证书 OID:
1.2.156.157933.3. <cert-type>.<cert-class>
<cert-type>: 证书类型: 1: SSL 证书(SSL); 2: 代码签名证书(Code); 3: 邮件证书(Mail);
4: 文档签名证书(Doc); 5: 客户端证书(Client); 6: 时间戳证书(TS)
<cert-class>: 证书级别: 1: T1; 2: T2; 3: T3; 4: T4
- 5) 零信根认证计划证书级别 OID:
1.2.156.157933.11, DV SSL, 对应 CABF DV SSL OID: 2.23.140.1.2.1
1.2.156.157933.12, IV SSL, 对应 CABF IV SSL OID: 2.23.140.1.2.3
1.2.156.157933.13, OV SSL, 对应 CABF OV SSL OID: 2.23.140.1.2.2
1.2.156.157933.14, EV SSL, 对应 CABF EV SSL OID: 2.23.140.1.1
1.2.156.157933.22, IV Code, 对应 CABF Code BR OID: 2.23.140.1.4.1
1.2.156.157933.23, OV Code, 对应 CABF Code BR OID: 2.23.140.1.4.1
1.2.156.157933.24, EV Code, 对应 CABF Code EV OID: 2.23.140.1.3
1.2.156.157933.31, MV Mail, 对应 CABF S/MIME MV strict OID: 2.23.140.1.5.1.3
1.2.156.157933.32, IV Mail, 对应 CABF S/MIME IV strict OID: 2.23.140.1.5.4.3
1.2.156.157933.33, OV Mail, 对应 CABF S/MIME OV strict OID: 2.23.140.1.5.2.3
1.2.156.157933.34, SV Mail, 对应 CABF S/MIME SV strict OID: 2.23.140.1.5.3.3
1.2.156.157933.41, MV Doc, 对应 CABF S/MIME MV multipurpose OID: 2.23.140.1.5.1.2
1.2.156.157933.42, IV Doc, 对应 CABF S/MIME IV multipurpose OID: 2.23.140.1.5.4.2
1.2.156.157933.43, OV doc, 对应 CABF S/MIME OV multipurpose OID: 2.23.140.1.5.2.2
1.2.156.157933.44, SV Doc, 对应 CABF S/MIME SV multipurpose OID: 2.23.140.1.5.3.2
1.2.156.157933.3.6.3, 时间戳云服务证书, 对应 CABF Code BR OID: 2.23.140.1.4.1

3. 国密 SM2 根证书信息

零信技术拥有 9 个国密 SM2 算法自签顶级根证书，用于签发各种业务所需的 SM2 证书，这 9 个根证书已经预置到零信浏览器中。可以从零信官网下载：

<https://www.zotrus.com/root>。

4. 国密 SM2 AIA 和 CRL 信息

中级根证书和用户证书的 AIA 和 CRL 都采用国密 SM2 算法，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。

AIA 网址：aia.zotrus.cn CRL 网址：crl.zotrus.cn

5. 国密 SM2 时间戳服务

遵循国家标准 GB/T 20520-2006，参考国际标准 RFC3161 协议，采用国密 SM2 时间戳证书和 SM2 算法提供国密标准时间戳服务，部署在腾讯云和天翼云，通过 CDN 为用户提供服务。

6. 国密 SM2 证书吊销服务

支持国际标准和国家标准的 SM2 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。

7. 国密证书透明服务

零信国密 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。

8. 国密证书自动化服务

零信国密 SSL 证书和国密邮件证书支持《自动化证书管理协议》国密标准草案实现证书自动化申请、验证和部署。

9. 国密 SM2 证书费用

零信技术不为用户提供国密 SSL 证书，而是在相关产品和服务中为用户自动配置国密证书，证书费用包含在相关产品和服务中，请用户访问零信官网查询相关产品和服务费用。

10. 国密 SM2 证书用户协议

用户必须遵循零信 CPS 9.6.3 中的用户协议及相关产品和服务协议。