证签技术（深圳）有限公司
中国深圳市南山区高新区科技生态园 9 栋 A1 座 2702A
Tel: +86-755-2660 4080　　Email: cps@cersign.com

证签技术 SM2 算法数字证书认证业务规则(CPS)

(版本: 1.0, 发布日期：2022 年 6 月 28 日，生效日期：2022 年 6 月 28 日)

1. 概述

本 CPS 适用于证签技术国密 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证签技术 CPS(www.cersign.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)。

1. 国密 SM2 根证书采用的 OID 标识

证签技术已向国家 OID 注册中心申请到中国国别国际 OID: **1.2.156.157672**, 具体分配如下:

1) CPS 版本 OID：
   1.2.156.157672.1.1.<major-version>.<minor-version>
2) 特殊用途 OID：
   1.2.156.157672.2.<number>
3) 中级根证书 OID：
   1.2.156.157672.3. <cert-type>
4) 用户证书 OID：
   1.2.156.157672.3. <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

2. 国密 SM2 根证书信息

证签技术拥有 8 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 8 个根证书已经预置到零信浏览器中。可以从证签官网下载: https://www.cersign.com/root。

3. 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。

4. 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。

5. 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，用户可以在证签官网申请相应的证书吊销服务。

6. 国密证书透明服务

证签国密 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。

7. 国密 SM2 证书费用

证签技术同时提供免费 SM2 用户证书和收费证书服务，请用户访问证签官网查询相关证书费用。

8. 国密 SM2 证书用户协议

用户必须遵循证签 CPS 9.6.3 中的用户协议。

证签技术（深圳）有限公司

2022 年 6 月