

## 沃通 CA 国密 SM2 证书认证业务规则(CPS)

(版本: 1.1, 发布日期: 2019 年 4 月 30 日, 生效日期: 2019 年 4 月 30 日)

### 1. 概述

本 CPS 适用于沃通 CA 自签国密 SM2 根证书签发的各种 SM2 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沃通 CA 自签 RSA 根证书系统的通过 WebTrust 国际审计的 CPS (WoTrus CPS), 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

沃通 CA 已向国家 OID 注册中心申请到中国国别国际 OID: **1.2.156.150570**, 具体分配如下, 其中:

<cert-type>: 证书类型: 1: SSL 证书; 2: 代码签名证书; 3: 客户端证书; 4: 时间戳证书;  
5: PDF/OFD 文档证书; 6: OCSP 证书  
<cert-class>: 证书级别: 1: V1; 2: V2; 3: V3; 4: V4

##### 1) CPS 版本 OID:

1.2.156.150570.1.1.<major-version>.<minor-version>

##### 2) 其他特殊用途 OID:

###### (1) 密信根认证计划证书级别 OID:

V1 级别证书: 1.2.156.150570.11

V2 级别证书: 1.2.156.150570.12

V3 级别证书: 1.2.156.150570.13

V4 级别证书: 1.2.156.150570.14

###### (2) PDF/OFD 文档双证书签名

国密签名: 1.2.156.150570.2.2.1

国密时间戳: 1.2.156.150570.2.2.2

###### (3) 密信阅读器识别 OID: 1.2.156.150570.2.9

##### 3) 中级根证书 OID:

(1) 沃通自用根: 1.2.156.150570.3. <cert-type>

(2) 密信自用根: 1.2.156.150570.8. <cert-type>

(3) 东方新诚信 CA: 1.2.156.150570.101. <cert-type>

(4) 安信数字科技(东方新诚信 CA): 1.2.156.150570.102. <cert-type>

(5) 华测 CA: 1.2.156.150570.103. <cert-type>

(6) 江西 CA: 1.2.156.150570.104. <cert-type>

(7) 新疆 CA: 1.2.156.150570.105. <cert-type>

(8) 中认环宇 CA: 1.2.156.150570.106. <cert-type>

(9) 福建 CA: 1.2.156.150570.107. <cert-type>

(10) 国富安 CA: 1.2.156.150570.108. <cert-type>

4) 用户证书 OID:

(1) 沃通自用: 1.2.156.150570.3. <cert-type>.<cert-class>

(2) 密信自用: 1.2.156.150570.8. <cert-type>.<cert-class>

(3) 东方新诚信: 1.2.156.150570.101. <cert-type>.<cert-class>

(4) 安信数字科技(东方新诚信 CA): 1.2.156.150570.102. <cert-type>.<cert-class>

(5) 华测 CA: 1.2.156.150570.103. <cert-type>.<cert-class>

(6) 江西 CA: 1.2.156.150570.104. <cert-type>.<cert-class>

(7) 新疆 CA: 1.2.156.150570.105. <cert-type>.<cert-class>

(8) 中认环宇 CA: 1.2.156.150570.106. <cert-type>.<cert-class>

(9) 福建 CA: 1.2.156.150570.107. <cert-type>.<cert-class>

(10) 国富安 CA: 1.2.156.150570.108. <cert-type>.<cert-class>

## 2. 国密 SM2 根证书信息

沃通 CA 拥有以下两个自签顶级根证书，用于签发各种业务所需的 SM2 证书，这两个根证书已经预置到 360 浏览器、密信浏览器、密信阅读器和密信(电子邮件客户端)中。可以从沃通官网下载: <https://www.wotrus.com/root>。

SM2 根证书 1:

公用名称: 国密 SM2 根证书

单位名称: 沃通电子认证服务有限公司

序列号: 0081C354BD60B92CBB5E8155A34238FAD4

指纹(SHA1): F69A41CE24A0FDCE4054803D331842C7372C0CCE

SM2 根证书 2:

公用名称: MeSince Identity CA SM2

单位名称: MeSince Technology Limited

序列号: 43F8C49C0C80E568850879ADA4E7FD95

指纹(SHA1): 47DFB05E073B791422856FD2281FCC6B0B8F9E8B

## 3. 国密 SM2 AIA, CRL 和 OCSP 信息

中级根证书和用户证书的 AIA、CRL 和 OCSP 都采用国密 SM2 证书和 SM2 算法，并部署在沃通通过 WebTrust 国际审计的同一套系统中，只是加密算法不同。

## 4. 国密 SM2 时间戳服务

采用国际标准 RFC3161 协议并采用国密 SM2 时间戳证书和加密算法提供国密标准时间戳服务，此服务同沃通通过 WebTrust 国际审计的时间戳服务系统为同一套系统，只是加密算法不同。

## 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，用户可以在沃通官网和密信官网申请相应的证书吊销服务。

## 6. 国密 SM2 证书费用

沃通同时提供免费 SM2 用户证书和收费证书服务，请用户访问沃通官网和密信官网查询相关证书费用。

## 7. 国密 SM2 证书用户协议

用户必须遵循国际标准的 WoTrus CPS 9.6.3 中的用户协议和国家标准的 WoTrus DCA CPS 中的用户协议。