ICS 35.030
CCS L 80

GM

中华人民共和国密码行业标准

GM/T 0130—2023

基于SM2算法的无证书及隐式证书公钥机制

Certificateless and implicit-certificate-based public key mechanisms based on the SM2 algorithms

2023-12-04 发布　　2024-06-01 实施

国家密码管理局　　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：深圳奥联信息安全技术有限公司、兴唐通信科技有限公司、国汽（北京）智能网联汽车研究院有限公司、国家工业信息安全发展研究中心、中汽数据（天津）有限公司、中国电力科学研究院有限公司、北京信安世纪科技股份有限公司、中国石油勘探开发研究院、北京汽车研究总院有限公司、北京数字认证股份有限公司、北京国脉信安科技有限公司、国家电网能源互联网技术研究院、中国测绘科学研究院、中国科学院信息工程研究所、北京邮电大学、中国大唐集团科学技术研究总院有限公司、大唐微电子技术有限公司、大唐移动通信设备有限公司、大唐高鸿数据网络技术股份有限公司、格尔软件股份有限公司、大唐电信科技股份有限公司、中国信息通信研究院、中国移动研究院、中安网脉（北京）技术股份有限公司、广州汽车集团股份有限公司汽车工程研究院、中汽研软件测评（天津）有限公司、联通智网科技股份有限公司、上汽通用五菱汽车股份有限公司、握奇数据股份有限公司、三未信安科技股份有限公司、中国联通中讯邮电咨询设计院有限公司、青岛国创智能家电研究院有限公司、国家信息安全技术研究中心、北京江南天安科技有限公司、博雅中科（北京）信息技术有限公司、安徽问天量子科技股份有限公司。

本文件主要起草人：程朝辉、万兆泽、刘建行、陈雪鸿、赵万里、翟峰、汪宗斌、冯梅、王冲华、袁峰、李志虎、马照亭、刘奇旭、谭儒、徐国爱、张永强、郑强、李峰、郑丽娟、王妮娜、张金池、陈中林、周光涛、巩军、邵学彬、邓宇、徐晖、沈天珺、于润东、田野、李增欣、但波、熊开新、张渊、车业蒙、王首媛、王亮、李冰、金添、郭忠泉、浦雨三、李雪雁、刘会议。

引　言

Al-Riyami 和 Paterson 在 2003 年提出无证书公钥密码(Certificateless-Public Key Cryptography)。无证书公钥系统不依赖数字证书验证用户的标识和公钥绑定关系的真实性并且密钥生成中心不具有密钥委托功能。扩展后的无证书公钥密码模型和安全定义允许基于标准公钥密码算法构造无证书公钥机制。

隐式证书(Implicit Certificate)不包括证书签发机构的签名且证书处理者需要根据证书中的数据计算得出证书拥有者的公钥。

本文件描述基于 SM2 算法构造的无证书公钥机制和隐式证书公钥机制。

本文件的发布机构提请注意,声明符合本文件时,可能涉及与第 6 章、第 7 章相关的 ZL 2017 10792638.7 专利的使用。

本文件的发布机构对于该专利的真实性、有效性和范围无任何立场。

该专利持有人已向本文件的发布机构承诺,他愿意同任何申请人在合理且无歧视的条款和条件下,就专利授权许可进行谈判。该专利持有人的声明已在本文件的发布机构备案。相关信息可以通过以下联系方式获得:

专利持有人姓名:深圳奥联信息安全技术有限公司

地址:深圳市宝安区宝兴路海纳百川 B 座 16 楼

请注意除上述专利外,本文件的某些内容仍可能涉及专利。本文件的发布机构不承担识别专利的责任。

基于SM2算法的无证书及隐式证书公钥机制

1 范围

本文件规定基于SM2算法的无证书及隐式证书公钥机制，包括密钥生成与校验机制、数字签名机制、公钥加密机制。

本文件规定的数字签名机制适用于商用密码应用中的数字签名和验证，加密机制适用于商用密码应用中的消息加解密。本文件规定的机制特别适合带宽和计算资源受限的应用环境。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 32918.1—2016 信息安全技术 SM2椭圆曲线公钥密码算法 第1部分：总则

GB/T 32918.2—2016 信息安全技术 SM2椭圆曲线公钥密码算法 第2部分：数字签名算法

GB/T 32918.4—2016 信息安全技术 SM2椭圆曲线公钥密码算法 第4部分：公钥加密算法

GB/T 32918.5—2017 信息安全技术 SM2椭圆曲线公钥密码算法 第5部分：参数定义

GB/T 32905 信息安全技术 SM3密码杂凑算法

GB/T 32915 信息安全技术 二元序列随机性检测方法

3 术语和定义

GB/T 32918.1、GB/T 32918.2、GB/T 32918.4界定的以及下列术语和定义适用于本文件。

3.1

密钥生成中心 key generation center；KGC

负责选择椭圆曲线系统参数、生成主密钥并产生用户部分私钥和声明公钥的可信机构。

3.2

标识 identity

由实体无法否认的信息组成，如实体的可识别名称、电子邮箱、身份证号、电话号码、街道地址等，可唯一确定一个实体身份的信息。

标识可进一步包括其他辅助信息，如标识用途、标识有效期等。

注：[来源：GB/T 38635.1—2020，3.1]

3.3

主密钥 master key

处于无证书密码系统密钥分层结构最顶层的密钥，包括系统主私钥和系统主公钥，其中系统主公钥公开，系统主私钥由KGC秘密保存。

3.4

用户的声明公钥 user's claimed public key

用于与椭圆曲线系统参数、系统主公钥、用户的标识一起计算用户实际公钥的公开值。

注：用户的声明公钥在隐式证书中也称为公钥还原数据。