ICS 35.040
CCS L 80

GM

中华人民共和国密码行业标准

GM/T 0085—2020

基于 SM9 标识密码算法的技术体系框架

Identity-based cryptographic algorithm SM9 based on technology system framework

2020-12-28 发布　　2021-07-01 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。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

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：上海信息安全工程技术研究中心、北京国脉信安科技有限公司、西安工业大学、长春吉大正元信息技术股份有限公司、上海格尔软件股份有限公司、中国科学院自动化研究所苏州研究院、北京海泰方圆科技有限公司、航天信息股份有限公司、深圳奥联信息安全技术有限公司。

本文件主要起草人：袁峰、王晓春、封维端、张立圆、郭保安、容晓峰、赵丽丽、郑强、汪雪林、蒋红宇、蔡先勇、张庆盛、唐静、袁文恭。

引　言

基于标识的密码技术(Identity-Based Cryptography,IBC)是一种公钥密码技术,利用椭圆曲线双线性对理论,由用户的标识和一组公开的数学参数计算出用户的公钥,相应的用户私钥则由用户标识、一组公开的数学参数和一个域范围内的秘密值(系统私钥等参数)计算出来。IBC 公钥能被任一个具有相应算法和公开参数的实体计算出来,实现用户身份与密钥对直接绑定的密码技术。

该密码技术可实现公钥密码的基本功能包括:数字签名与验证、数据加密与解密、密钥协商、密钥封装与传送等。在 IBC 技术体系中,用户的私钥通常不在自身管理的密码设备中产生,而是由密钥管理基础设施 KMS 统一产生并下载给用户。用户的公钥可依据用户标识和规范算法及参数实时生成。

本文件的目标是为基于 SM9 标识密码算法的 IBC 技术提供技术应用框架、密钥管理基础设施建设框架和标准体系研制框架。

本文件仅从理论研究和技术应用的角度描述了相关内容,不涉及具体的管理和标准内容编制细节。

基于SM9标识密码算法的技术体系框架

1 范围

本文件描述了基于SM9标识密码算法的IBC技术应用框架、标识密码密钥管理系统的框架以及基于SM9标识密码算法应用所涉及的标准规范。

本文件适用于基于SM9标识密码算法的应用体系建设、产品和系统研制、标识密码密钥管理系统建设管理和相关标准研制、查询提供参考。

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。

GM/T 0044.1 SM9标识密码算法 第1部分：总则

GM/T 0044.2 SM9标识密码算法 第2部分：数字签名算法

GM/T 0044.3 SM9标识密码算法 第3部分：密钥交换协议

GM/T 0044.4 SM9标识密码算法 第4部分：密钥封装机制和公钥加密算法

GM/T 0086 基于SM9标识密码算法的密钥管理系统技术规范

GM/Z 4001 密码术语

3 术语和定义

GM/T 0044.1～GM/T 0044.4和GM/Z 4001界定的以及下列术语适用于本文件。

3.1

基于标识的密码 identity-based cryptography；IBC

在指定应用范围内基于用户/实体唯一性身份标识和系统主密钥而生成用户密钥的密码机制。

3.2

公开参数服务 public parameter service；PPS

为IBC系统的用户提供包括密码算法参数、系统策略和用户标识变化等相关公开信息的服务。

4 缩略语

下列缩略语适用于本文件。

KMS：标识密钥管理系统(Key Management Server)

PPS：公共参数服务器(Public Parameter Server)

5 基本特征

IBC是一种公钥密码技术，它能由用户/实体(以下统称用户)的标识和一组公开的数学参数计算出