ICS 35.040
L 80
备案号：62992—2018

GM

中华人民共和国密码行业标准

GM/T 0057—2018

基于 IBC 技术的身份鉴别规范

Identity authentication specifications based on IBC technology

2018-05-02 发布　　2018-05-02 实施

国家密码管理局　　发 布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

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这些专利的责任。

本标准由密码行业标准化技术委员会提出并归口。

本标准起草单位：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、无锡江南信息安全工程技术研究中心、中油瑞飞信息技术有限责任公司。

本标准起草人：袁峰、药乐、容晓峰、杜志强、王一曲、蒋楠、王建、崔广印、金一、万进。

本标准凡涉及密码算法的相关内容，按国家有关法规实施，凡涉及采用密码技术解决保密性、完整性、真实性、不可否认性需求的须遵循密码相关国家标准和行业标准。

引　言

本标准是IBC(Identity-Based Cryptography)基于标识的密码技术系列标准之一,本标准依托于GM/T 0044 SM9标识密码算法,面向应用系统中基于IBC技术和SM9算法进行的身份鉴别时涉及的鉴别需求。

鉴于标识密码技术的特点,规定了两种单向身份鉴别要求和一个双向身份鉴别要求。本标准还在附录中给出了利用IBC技术进行鉴别时需要访问公开参数服务(PPS)的基本流程和相关密码数据结构,用于公开参数和标识状态查询。

基于 IBC 技术的身份鉴别规范

1 范围

本标准规定了使用基于标识的密码技术的身份鉴别要求。

本标准适用于使用基于标识的密码技术的身份鉴别领域。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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 SM9 标识密码算法

3 术语和定义

下列术语和定义适用于本文件。

3.1

标识 identity

可确定一个对象身份的唯一信息，例如电子邮箱地址、手机号码、指纹数据等。

3.2

SM9 密码算法 SM9 algorithm

由 GM/T 0044 定义的一种算法。

3.3

公开参数服务 public parameter service

用于发布基于标识的密码技术中公开参数、私钥生成策略、用户标识信息和状态等数据的应用服务。

4 缩略语

下列缩略语适用于本文件。

ASN.1 抽象语法标记(Abstract Syntax Notation One)

IBC 基于标识的密码技术(Identity-Based Cryptography)

IRI 国际化资源标识符(Internationalized Resource Identifiers)

OID 对象标识符(Object identifier)

PKG 私钥生成(Private Key Generation)

PPS 公开参数服务(Public Parameter Service)

URI 统一资源标识符(Uniform Resource Identifier)

5 标识结构

标识数据格式的 ASN.1 定义为：