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

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。

本文件采用 GM/T 0044.1～GM/T 0044.4 标识密码算法。可支持数字签名与验证、数据加密与解密、密钥协商、密钥封装与传送等密码运算，可实现公钥密码的基本功能。

6 IBC 技术体系框架

IBC 技术体系框架主要有以下方面的内容：密码基础技术，密码设备服务、通用密码服务、典型密码服务，基础设施支撑这三个部分的有机结合。该体系以密码基础技术为依托，利用密码设备提供密码运算服务，以标准接口形式为应用提供统一的身份鉴别、数据加解密、数据签名验签等服务。其中典型和通用密码服务依靠基础设施支撑平台的密钥管理基础设施、时间戳系统获取密钥生成、系统参数和时间管理等基础服务。见图 1。

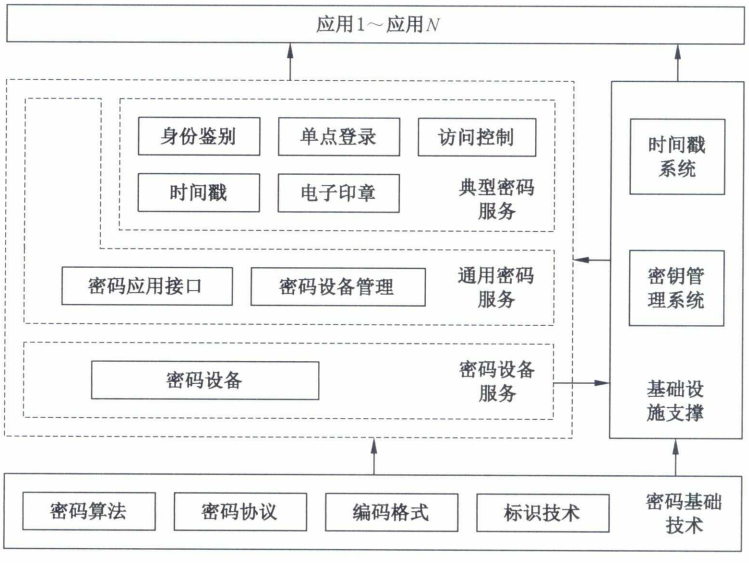

图 1 IBC 技术体系框架

IBC 技术体系框架中的三部分定义：

密码基础技术中的密码算法实现、应用理论是整个架构基础，为 IBC 技术提供标准密码算法、算法应用所需的各种协议、基础编码格式、基本标识定义等底层支撑。该部分能够直接服务其他各个部分。

基础设施支撑部分是 IBC 技术信任源点，为 IBC 技术应用提供私钥生成服务、IBC 系统参数和标识状态发布服务、可信时间服务等。该部分依靠技术基础部分的理论、密码设备部分和接口部分的计算支持完成信任源点的功能服务，并用于支撑 IBC 技术的各种应用。

密码设备服务由密码机、密码卡、智能密码终端等设备组成，通过标准的密码设备应用接口向通用密码服务层提供基础密码服务。

主要功能包括密钥生成、密码运算等服务。

密码设备通过统一的设备管理接口来接受通用密码服务层的密码设备管理。

密码设备应具备密钥加载、存储、更新、备份和恢复等功能并保障密钥在密码设备中的安全。

通用密码服务由通用密码服务和密码设备管理服务组成，为上层应用提供与底层具体密码设备透明的密码服务和设备管理服务。

通用密码服务通过统一的密码服务接口向典型密码服务层和应用层提供标识认证、信息的机密性、

完整性和不可否认性等通用密码服务，将上层的密码服务请求转化为具体的基础密码操作请求，通过统一的密码设备应用接口调用相应密码设备实现具体的密码运算和密钥操作。

密码设备管理向上层管理应用提供统一的设备管理应用接口，为实现远程密钥管理、设备维护、设备监控等上层管理应用提供设备管理功能，将上层管理应用的管理请求转换为标准的消息调用，通过安全通道实现管理应用与密码设备间的消息传递。

典型密码服务由身份鉴别、单点登录、访问控制、时间戳和电子签章等服务组成，为上层应用提供对应的密码服务。典型密码服务层使用的密码功能通过调用通用密码服务实现。

身份鉴别通过标准接口为上层应用提供身份查询、身份解析、身份验证等身份鉴别服务。

单点登录通过标准接口为上层应用提供登录凭据的产生、获取、验证等服务，在相互间存在信任关系的应用系统之间实现单点登录和单点注销。

访问控制通过标准接口为上层应用提供系统资源的访问控制，实现用户管理、资源管理、访问控制策略管理和用户授权等功能。

时间戳通过标准接口为上层应用和典型密码服务层其他组成部分提供与时间戳系统无关的时间戳加盖、验证等时间认证服务。

电子签章通过标准接口为上层应用和典型密码服务层其他组成部分提供电子签章生成与验证服务。

7 密钥管理系统框架

7.1 密钥管理系统关系结构

有层次的密钥管理系统(KMS)结构可分为两级，第一级是上级 KMS，第二级是应用(即下级)KMS，形成扁平化结构。独立部署的 KMS 自己即为根同时直接作为应用 KMS。见图 2。

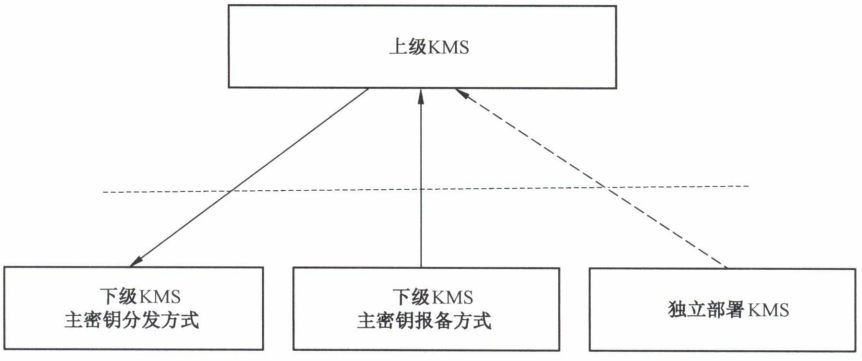

图 2 密钥基础设施关系架构图

密钥管理系统技术规范见 GM/T 0086。

分发方式是指下级 KMS 通过下列流程向其上级 KMS 申请产生主密钥对并签名。

报备方式是指下级 KMS 产生一对主密钥，并通过下列流程由其上级 KMS 对其主公钥签名。

独立部署的标识密钥管理系统可以自行产生主密钥和设置应用层主密钥。

7.2 上级标识密钥管理系统

上级标识密钥管理系统分为分级管理的 KMS 系统和独立 KMS 应用系统两种。

a) 分级管理的 KMS 系统

上级标识密钥管理系统包括上级 KMS 和上级 PPS 发布系统。

上级 KMS 是 IBC 体系的信任基础，以离线方式独立运行。对应用基础设施进行分类管控，为密钥分发方式应用 KMS 产生主私钥。

上级 PPS 发布系统发布本根规定的基准算法参数、所有通过本根注册的应用 KMS 系统的信息、PPS 地址和状态，形成统一管理架构和完整部署结构，为各个应用 IBC 系统提供互认和互信查询列表。

b） 独立 KMS 应用系统

独立密钥管理基础设施包括应用 KMS 和应用 PPS 发布系统。

独立 KMS 是自身为本 IBC 体系的信任源点，以在线方式独立运行为应用提供密钥签发管理服务。

独立 PPS 发布系统发布本根规定的基准算法参数、用户密钥状态信息，为应用提供参数和密钥信息查询服务。

7.3 下级应用密钥管理系统

下级应用密钥管理基础设施分为密钥分发方式、密钥报备方式、独立部署方式三种。

a） 密钥分发方式应用 KMS

密钥分发方式应用 KMS 应向上级 KMS 申请注册，并由上级 KMS 自上而下签发应用主私钥，由根统一管控。

IBC 业务系统标明能够为用户提供安全可靠的服务时，应采用已经注册过的 KMS 系统为其签发私钥。

b） 密钥报备方式应用 KMS

密钥报备方式应用 KMS 为按照某一上级 KMS 发布的公共参数，自生成应用根密钥，并向该上级 KMS 报备其公钥，接受上级 KMS 的监督管理。

c） 独立部署方式应用 KMS

独立部署方式应用 KMS 为自生成根密钥并自行管理，无需向任何根报备。但应采用 GM/T 0044 中的曲线、参数。独立部署方式应用 KMS 如需要时，可向某上级 KMS 报备申请，通过安全加固和安全审查，具备向上级 KMS 报备的条件后，变换为密钥报备方式。

8 IBC 技术标准

8.1 分类概述

基于 SM9 标识密码算法的 IBC 技术标准规范包括基础类型和应用类型两大类别，这些标准中有拟研制新研制，对已发布标准的拟修订和已发布标准。

8.2 基础类

8.2.1 总体框架类

本文件的目标是为基于 SM9 标识密码算法的 IBC 技术提供密钥管理基础设施建设规划、标准研制提供总体框架。本文件仅从理论研究和技术应用的角度给出标识密码密钥管理系统的建设规划以及 IBC 技术体系所需的标准，不涉及具体的管理和标准内容编制细节，其架构见表 1。

表 1　总体框架

大类	小类	名称	文件编号	备注
基础类型	算法标准类	SM9 标识密码算法	GM/T 0044.1～GM/T 0044.4	已有
		SM3 密码杂凑算法	GM/T 0004—2012	已有
		SM4 分组密码算法	GM/T 0002—2012	已有
	编码类	密码应用标识规范	GM/T 0006—2012	修订
		标识密码应用标识规范		制定
		SM9 密码算法加密签名消息语法规范		制定
		SM9 密码算法 XML 加密签名消息语法与处理规范		制定
		标识密码应用编码规范		制定
	服务类	智能密码钥匙技术规范	GM/T 0027—2014	修订
		密码模块安全技术要求	GM/T 0028—2014	修订
		服务器密码机技术规范	GM/T 0030—2014	修订
		智能密码钥匙密码应用接口规范	GM/T 0016—2012	修订
		智能密码钥匙密码应用接口数据格式规范	GM/T 0017—2012	修订
	接口类	密码设备应用接口规范	GM/T 0018—2012	修订
		通用密码服务接口规范	GM/T 0019—2012	修订
		签名验签服务器技术规范	GM/T 0029—2014	
		SM9 密码算法使用规范		制定
		IBC 公开参数访问规范		制定
	密码协议类	基于 IBC 技术的身份鉴别协议规范		制定
		安全通信协议规范	GM/T 0022—2014 GM/T 0023—2014 GM/T 0024—2014 GM/T 0025—2014	修订
	基础设施类规范	基于标识的密钥基础设施规范		制定
		时间戳接口规范	GM/T 0033—2014	修订
应用类型		基于 SM9 密码算法的安全电子签章密码技术规范		制定
		电子邮件密码技术规范		制定
		密码模块安全技术要求	GM/T 0028—2014	已有

8.2.2 算法标准类

SM9 标识密码算法

见 GM/T 0044.1～GM/T 0044.4。

SM3 密码杂凑算法

见 GM/T 0004。

SM4 分组密码算法

见 GM/T 0002。

8.2.3 编码类

密码应用标识规范

修订类。对已发布 GM/T 0006 进行修订，增加 SM9 密码算法相关的内容。规范密码应用有关的算法标识、密钥标识、设备标识、数据标识、协议标识、角色标识等的表示和使用。

标识密码应用标识规范

制定类。对基于标识的密码安全应用的标识编码格式进行规范，用于指导不同应用领域在使用标识密码技术时遵循统一的标识编码格式。

SM9 密码算法加密签名消息语法规范

制定类。定义使用 SM9 密码算法的加密签名消息语法，具体包括 SM9 签名数据类型、数字信封数据类型、签名及数字信封数据类型、加密数据类型、密钥协商类型。用于指导使用 SM9 标识密码算法进行加密和签名操作时对操作结果的标准化封装。

SM9 密码算法 XML 加密签名消息语法与处理规范

制定类。主要定义在应用层基于 XML 封装传输 SM9 密码算法的加密签名的消息语法。用于指导使用 XML 对 SM9 加密和签名消息结果的标准化封装和处理。

标识密码应用编码规范

制定类。主要定义与接口的函数名称及不同系统分配的错误代码区间，用于规范开发和用户的使用。

8.2.4 密码服务类

智能密码钥匙技术规范

修订类。对已发布 GM/T 0027—2014 进行修订，增加基于 IBC 技术的智能密码钥匙的相关术语，增加规范 IBC 智能密码钥匙功能要求、硬件要求、软件要求、性能要求、安全性要求等有关内容。

密码模块安全技术要求

见 GM/T 0028—2014。

服务器密码机技术规范

修订类。对已发布 GM/T 0030—2014 进行修订，增加基于 IBC 技术的密码机的相关术语，规范 IBC 密码机功能要求、硬件要求、软件要求、性能要求及安全性要求等有关内容。

8.2.5 密码应用接口类

智能密码钥匙密码应用接口规范

修订类。对已发布 GM/T 0016—2012 进行修订，增加基于 SM9 密码体制的智能密码钥匙应用接口，描述应用接口的函数、数据类型、参数的定义和设备的安全要求。

智能密码钥匙密码应用接口数据格式规范

修订类。对已发布 GM/T 0017—2012 进行修订，增加基于 SM9 算法的智能 IC 卡应用接口，描述

应用接口的函数、数据类型、参数的定义和设备的安全要求。

密码设备应用接口规范

修订类。对已发布 GM/T 0018—2012 进行修订，增加基于 SM9 标识密码算法的密码设备应用接口，描述应用接口的函数、数据类型、参数的定义和设备的安全要求。

通用密码服务接口规范

修订类。对已发布 GM/T 0019—2012 进行修订，增加定义 IBC 应用与密码设备无关的统一密码应用接口，屏蔽密码应用支撑接口中的密码设备特性，以密码应用支撑接口为基础，服务于各种设施平台、各种 IBC 应用。

签名验签服务器技术规范

修订类。对已发布 GM/T 0029—2014 进行修订，增加基于 SM9 标识密码算法的签名验签服务器应用接口，描述应用接口的函数、数据类型、参数的定义和设备的安全要求。

8.2.6 应用协议类

SM9 密码算法使用规范

制定类。描述 SM9 密码算法的使用方法，给出 SM9 的密钥对、密钥数据结构、签名数据结构、加密数据结构、密钥封装数据格式等。用于指导 SM9 密码算法的使用，以及支持 SM9 密码算法的设备和系统的研发和检测。

IBC 公开参数访问规范

制定类。规范向 PPS 服务查询、下载相关信息的协议和格式。规范 IBC 公开参数服务系统(PPS)的内容结构、逻辑关系、业务流程、系统管理、数据格式等。为建设、检测 PPS 提供技术支撑。

基于 IBC 技术的身份鉴别协议规范

制定类。面向应用系统中基于 IBC 技术和 SM9 标识密码算法进行身份认证时涉及的鉴别需求，基于标识密码技术的特点，重点规范包括单向鉴别和双向鉴别在内的身份鉴别技术，并给出利用 IBC 技术进行鉴别时访问 PPS 的基本流程和相关密码协议，用于公开参数和标识状态查询。

安全通信协议规范

修订类。规范基于 IBC 的安全通信技术，具体包括通信数据的加解密协议及完整性保护协议。

对已发布的 GM/T 0022—2014、GM/T 0023—2014、GM/T 0024—2014、GM/T 0025—2014 VPN 类进行修订，修改其规范的引用部分，明确引用 SM9 标识密码算法规范和 SM9 标识密码算法使用规范；在预主密钥协商阶段，明确相对于交换证书时所交互的 IBC 信息。明确相关 IBC 数据的获取方式、组成和编码等信息。以利于将 SM9 纳入 SSL VPN 技术体系之后，服务端和客户端之间实现互联互通。

8.2.7 基础设施类规范

时间戳接口规范

修订类。对已发布 GM/T 0033—2014 进行修订，增加时间戳基于 SM9 的签名和验证的协议和接口，并补充包括时间戳机构、证书持有者和信赖者，并规范时间戳的产生及使用流程。

基于 SM9 标识密码算法的密钥管理系统技术规范

制定类。规范基于 IBC 技术的密钥管理系统的内容结构、逻辑关系、业务流程、系统管理、各种协议、数据包格式等。为建设、检测密钥管理基础设施提供技术支撑。

8.3 应用类

电子签章技术规范

制定类。虽然已发布 GM/T 0031—2014，但由于增加基于 IBC 密码体制的电子签章的基本概念、

总体技术要求、数据格式设计、接口规范等，与数字证书系统的电子印章系统在使用时有较大差异，需要另行制定，并明确基于IBC密码体制电子签章实现的安全性要求。

电子邮件密码技术规范

制定类。安全邮件系统是IBC技术在实际应用中一个主要领域。本文件主要对使用IBC技术的安全邮件系统，包括体系架构、功能、数据流、数据格式、密钥管理等在内的核心内容进行规范，指导基于IBC的邮件系统和产品的开发和使用。

中华人民共和国密码
行业标准
基于SM9标识密码算法的技术体系框架
GM/T 0085—2020
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)68533533 发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 1 字数 28千字
2021年5月第一版 2021年5月第一次印刷
*
书号:155066·2-35879 定价 18.00 元

GM/T 0085-2020

码上扫一扫 正版服务到