ICS 35.040
CCS L 80

中华人民共和国密码行业标准

GM/T 0094—2020

公钥密码应用技术体系框架规范

Public key cryptographic application technology framework specification

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。

本文件起草单位：格尔软件股份有限公司、飞天诚信科技股份有限公司、北京信安世纪科技股份有限公司、长春吉大正元信息技术股份有限公司、上海交通大学、成都卫士通信息产业股份有限公司、北京数字认证股份有限公司、北京海泰方圆科技股份有限公司、北京国脉信安科技有限公司、北京握奇智能科技有限公司、国民技术股份有限公司、北京天融信网络安全技术有限公司、山东得安信息技术有限公司。

本文件主要起草人：郑强、朱鹏飞、张庆勇、赵丽丽、李强、罗俊、傅大鹏、蒋红宇、药乐、张渊、付月鹏、雷晓峰、马洪富。

公钥密码应用技术体系框架规范

1 范围

本文件规定了公钥密码应用技术体系框架，给出该框架内各组成部分及其逻辑关系。

本文件适用于公钥密码应用技术体系的建设及相关标准的制修订，并指导应用系统的密码应用。

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 35275 信息安全技术 SM2密码算法加密签名消息语法规范

GM/Z 4001 密码术语

3 术语和定义

GM/Z 4001界定的以及下列术语和定义适用于本文件。

3.1

属性管理系统 attribute authority system

用来产生、签发、发布、更新和撤销属性证书的管理系统。

3.2

访问控制 access control

按照特定策略，允许或拒绝用户对资源访问的一种机制。

3.3

证书认证系统 certificate authentication system

对数字证书的签发、发布、更新、撤销等数字证书全生命周期进行管理的系统。

3.4

通用密码应用支撑 common cryptography application support

向典型密码应用支撑和上层应用提供加解密、签名验签等通用密码功能。

3.5

密码设备 cryptography device

包括密码机、密码卡和智能密码终端等设备。

3.6

身份鉴别 authentication

确认一个实体所声称身份的过程。

3.7

典型密码应用支撑 typical cryptography application support

由电子证据、身份鉴别、电子签章、访问控制和时间戳等组成，为上层应用提供对应的密码应用支撑。