ICS 35.040
L 80
备案号：38317—2013

GM

中华人民共和国密码行业标准

GM/T 0019—2012

通用密码服务接口规范

Universal cryptography service interface specification

2012-11-22 发布　　2012-11-22 实施

国家密码管理局　　发布

目　　次

前言 …… Ⅰ
引言 …… Ⅱ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　符号和缩略语 …… 1
5　算法标识和数据结构 …… 2
5.1　算法标识与常量定义 …… 2
5.2　密码服务接口数据结构定义和说明 …… 2
6　密码服务接口 …… 4
6.1　通用密码服务接口在公钥密码基础设施应用技术体系框架中的位置 …… 4
6.2　密码服务接口组成和功能说明 …… 5
7　密码服务接口函数定义 …… 6
7.1　环境类函数 …… 6
7.2　证书类函数 …… 8
7.3　密码运算类函数 …… 15
7.4　消息类函数 …… 35
附录A（规范性附录）　密码服务接口错误代码定义 …… 45
参考文献 …… 47

前　言

本标准依据 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。

本标准的附录 A 为规范性附录。

本标准由国家密码管理局提出并归口。

本标准起草单位：北京数字认证股份有限公司、上海格尔软件股份有限公司、北京海泰方圆科技有限公司、无锡江南信息安全工程技术中心、上海数字证书认证中心有限公司、卫士通信息产业股份有限公司、山东得安信息技术有限公司、国家信息安全工程技术研究中心。

本标准主要起草人：刘平、李述胜、谭武征、柳增寿、徐强、刘承、李元正、高志权、孔凡玉、袁峰。

本标准凡涉及密码算法相关内容，按照国家有关法规实施。

引　言

本标准依托于密码设备层的GM/T 0018《密码设备应用接口规范》和GM/T 0016《智能密码钥匙密码应用接口规范》，为典型密码服务层和应用层规定了统一的通用密码服务接口。

通用密码服务接口在公钥密码基础设施支撑的前提下，向应用系统和典型密码服务层提供各类通用的密码服务，有利于密码服务接口产品的开发，有利于应用系统在密码服务过程中的集成和实施，有利于实现各应用系统的互联互通。

通用密码服务接口规范

1 范围

本标准规定了统一的通用密码服务接口。

本标准适用于公开密钥应用技术体系下密码应用服务的开发,密码应用支撑平台的研制及检测,也可用于指导直接使用密码设备的应用系统的开发。

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 0006 密码应用标识规范

GM/T 0015 基于 SM2 密码算法的数字证书格式规范

GM/T 0018 密码设备应用接口规范

GM/T 0016 智能密码钥匙密码应用接口规范

GM/T 0010 SM2 密码算法加密签名消息语法规范

GM/T 0009 SM2 密码算法使用规范

PKCS #7:Cryptographic Message Syntax

3 术语和定义

下列术语和定义适用于本文件。

3.1

数字证书 digital certificate

由认证权威数字签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及一些扩展信息的数字文件。

3.2

用户密钥 user key

存储在设备内部的用于应用密码运算的非对称密钥对,包含签名密钥对和加密密钥对。

3.3

容器 container

密码设备中用于保存密钥所划分的唯一性存储空间。

4 符号和缩略语

下列缩略语适用于本文件:

API Application Program Interface 应用程序接口,简称应用接口

CA Certification Authority 证书认证机构

CN Common Name 通用名