

ICS 35.040  
L 80  
备案号:38316—2013



# 中华人民共和国密码行业标准

GM/T 0018—2012

---

## 密码设备应用接口规范

Interface specifications of cryptography device application

2012-11-22 发布

2012-11-22 实施

---

国家密码管理局 发布

## 目 次

前言 .....	III
引言 .....	IV
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 .....	2
5 算法标识和数据结构 .....	2
5.1 算法标识定义 .....	2
5.2 设备信息定义 .....	2
5.3 密钥分类及存储定义 .....	3
5.3.1 设备密钥与用户密钥 .....	3
5.3.2 密钥加密密钥 .....	3
5.3.3 会话密钥 .....	3
5.4 RSA 密钥数据结构定义 .....	3
5.5 ECC 密钥数据结构定义 .....	5
5.6 ECC 加密数据结构定义 .....	5
5.7 ECC 签名数据结构定义 .....	6
5.8 ECC 加密密钥对保护结构 .....	6
6 设备接口描述 .....	7
6.1 密码设备应用接口在公钥密码基础设施应用技术体系框架中的位置 .....	7
6.2 设备管理类函数 .....	7
6.2.1 打开设备 .....	7
6.2.2 关闭设备 .....	8
6.2.3 创建会话 .....	8
6.2.4 关闭会话 .....	8
6.2.5 获取设备信息 .....	8
6.2.6 产生随机数 .....	8
6.2.7 获取私钥使用权限 .....	9
6.2.8 释放私钥使用权限 .....	9
6.3 密钥管理类函数 .....	9
6.3.1 导出 RSA 签名公钥 .....	10
6.3.2 导出 RSA 加密公钥 .....	10
6.3.3 产生 RSA 密钥对并输出 .....	10
6.3.4 生成会话密钥并用内部 RSA 公钥加密输出 .....	11
6.3.5 生成会话密钥并用外部 RSA 公钥加密输出 .....	11
6.3.6 导入会话密钥并用内部 RSA 私钥解密 .....	12
6.3.7 基于 RSA 算法的数字信封转换 .....	12
6.3.8 导出 ECC 签名公钥 .....	13

6.3.9	导出 ECC 加密公钥 .....	13
6.3.10	产生 ECC 密钥对并输出 .....	13
6.3.11	生成会话密钥并用内部 ECC 公钥加密输出 .....	14
6.3.12	生成会话密钥并用外部 ECC 公钥加密输出 .....	14
6.3.13	导入会话密钥并用内部 ECC 私钥解密 .....	14
6.3.14	生成密钥协商参数并输出 .....	15
6.3.15	计算会话密钥 .....	15
6.3.16	产生协商数据并计算会话密钥 .....	16
6.3.17	基于 ECC 算法的数字信封转换 .....	17
6.3.18	生成会话密钥并用密钥加密密钥加密输出 .....	17
6.3.19	导入会话密钥并用密钥加密密钥解密 .....	18
6.3.20	销毁会话密钥 .....	18
6.4	非对称算法运算类函数 .....	18
6.4.1	外部公钥 RSA 运算 .....	19
6.4.2	内部公钥 RSA 运算 .....	19
6.4.3	内部私钥 RSA 运算 .....	20
6.4.4	外部密钥 ECC 验证 .....	20
6.4.5	内部密钥 ECC 签名 .....	21
6.4.6	内部密钥 ECC 验证 .....	21
6.4.7	外部密钥 ECC 公钥加密 .....	21
6.5	对称算法运算类函数 .....	22
6.5.1	对称加密 .....	22
6.5.2	对称解密 .....	23
6.5.3	计算 MAC .....	23
6.6	杂凑运算类函数 .....	24
6.6.1	杂凑运算初始化 .....	24
6.6.2	多包杂凑运算 .....	24
6.6.3	杂凑运算结束 .....	25
6.7	用户文件操作类函数 .....	25
6.7.1	创建文件 .....	25
6.7.2	读取文件 .....	25
6.7.3	写文件 .....	26
6.7.4	删除文件 .....	26
7	安全要求 .....	27
7.1	密钥管理要求 .....	27
7.2	密码服务要求 .....	27
7.3	设备状态要求 .....	27
7.4	其他安全要求 .....	27
附录 A	(规范性附录) 函数返回代码定义 .....	28
参考文献	.....	29

## 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。

本标准中的附录 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：卫士通信息产业股份有限公司、无锡江南信息安全工程技术中心、上海格尔软件股份有限公司、北京数字认证股份有限公司、兴唐通信科技股份有限公司、山东得安计算机技术有限公司、北京海泰方圆科技有限公司。

本标准主要起草人：刘平、李元正、徐强、谭武征、李述胜、李玉峰、高志权、柳增寿。

## 引 言

本标准的目标是为公钥密码基础设施应用体系框架下的服务类密码设备制定统一的应用接口标准,通过该接口调用密码设备,向上层提供基础密码服务。为该类密码设备的开发、使用及检测提供标准依据和指导,有利于提高该类密码设备的产品化、标准化和系列化水平。

本标准凡涉及密码算法相关内容,按国家有关法规实施。

# 密码设备应用接口规范

## 1 范围

本标准规定了公钥密码基础设施应用技术体系下服务类密码设备的应用接口标准。

本标准适用于服务类密码设备的研制、使用,以及基于该类密码设备的应用开发,也可用于指导该类密码设备的检测。

## 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 0009 SM2 密码算法使用规范

## 3 术语和定义

以下术语和定义适用于本文件。

### 3.1

**算法标识 algorithm identifier**

用于对密码算法进行唯一标识的符号。

### 3.2

**非对称密码算法/公钥密码算法 asymmetric cryptographic algorithm/public key cryptographic algorithm**  
加解密使用不同密钥的密码算法。

### 3.3

**解密 decipherment/decryption**

加密过程对应的逆过程。

### 3.4

**设备密钥 device key pair**

存储在设备内部的用于设备管理的非对称密钥对,包含签名密钥对和加密密钥对。

### 3.5

**加密 encipherment/encryption**

对数据进行密码变换以产生密文的过程。

### 3.6

**密钥加密密钥 key encrypt key; KEK**

对密钥进行加密保护的密钥。

### 3.7

**公钥基础设施 public key infrastructure; PKI**

用公钥密码技术建立的普遍适用的基础设施,为用户提供证书管理和密钥管理等安全服务。

### 3.8

**私钥访问控制码 private key access password**

用于验证私钥使用权限的口令字。