ICS 35.040
L 80

中华人民共和国国家标准

GB/T 36322—2018

信息安全技术
密码设备应用接口规范

Information security technology—
Cryptographic device application interface specifications

2018-06-07 发布　　2019-01-01 实施

国家市场监督管理总局
中国国家标准化管理委员会　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。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)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、四川大学、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、山东得安信息技术有限公司、北京三未信安科技发展有限公司、海泰方圆科技有限公司、山东大学。

本标准主要起草人:刘平、罗俊、龚勋、李元正、徐强、郑强、李述胜、李玉峰、孔凡玉、马洪富、高志权、徐明翼、柳增寿、蒋红宇。

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。

本标准中涉及密码算法的相关内容，按照国家有关法规实施。

信息安全技术
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。

GB/T 33560 信息安全技术 密码应用标识规范

3 术语和定义

下列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 asymmetric cryptographic algorithm/public key cryptographic algorithm

公钥密码算法

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 encryption key

对密钥进行加密保护的密钥。

3.7

公钥基础设施 public key infrastructure

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。