ICS 35.040
L 80
备案号：62990—2018

中华人民共和国密码行业标准

GM/T 0055—2018

电子文件密码应用技术规范

File cryptographic technical specification

2018-05-02 发布　　2018-05-02 实施

国家密码管理局　　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。

本标准由密码行业标准化技术委员会提出并归口。

本标准起草单位：上海颐东网络信息有限公司、北京海泰方圆科技有限公司、深圳奥联科技有限公司、北京书生公司、北京宇讯佳通科技有限责任公司、深圳宝嘉电子设备有限公司、北京兴唐通信科技股份有限公司、上海格尔软件股份有限公司。

本标准主要起草人：刘平、谢永泉、姜海舟、宋明华、柳增寿、刘海生、蒋健、夏东山、刘宁胜、曹学武、杨茂江、孙志辉。

引　言

本标准中涉及的文件为广义的文件对象，与文件的具体格式无关。

在涉及文件处理及流转的应用系统中，存在着密码协议不统一、密码接口应用混乱、密码服务处理层次不清晰等问题，从而导致文件在不同应用系统之间进行交互时，出现兼容性和安全失控等问题。

为保证文件在处理过程中的规范性、兼容性、安全性和可控性，本标准提出了一种标签与文件绑定的安全控制机制，实现了文件全生命周期的机密性、完整性、有效性和抗抵赖性等安全控制。

本标准描述了基于标签的安全电子文件系统架构和应用系统如何通过中间件，调用相应的基础密码服务和个性密码服务，实现对文件的安全操作，由中间件为应用系统提供统一、规范的密码服务，有利于应用系统、中间件和密码服务开发单位专注于自身技术的开发，促进技术的产品化。

电子文件密码应用技术规范

1 范围

本标准不规范应用系统的安全性，也不规定具体的文件类型。

本标准适用于关注文件对象自身安全的相关标准规范和应用，也适用于安全电子文件密码服务中间件的开发和检测，可用于指导使用该中间件的应用系统的开发。

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 0009 SM2 密码算法使用规范

GM/T 0015 基于 SM2 密码算法的数字证书格式规范

GM/T 0017 智能密码钥匙密码应用接口数据格式规范

GM/T 0019 通用密码服务接口规范

GM/T 0031 安全电子签章密码技术规范

PKCS#1 RSA Cryptography Standard

PKCS#5 Password-based Encryption Standard

3 术语和定义

下列术语和定义适用于本文件。

3.1

应用系统 application system

以文件为处理对象，对文件进行创建、修改、授权、阅读、签批、盖章、打印、添加水印、流转、存档和销毁等操作的系统。

3.2

文件/电子文件 file

以数字方式表示的、对特定的使用对象有特定意义的实体。它可以是各类公文、票据、数字作品等。

3.3

标签 label

和文件绑定的一段数字实体，用于标识文件的属性和状态，定义文件的操作对象、操作行为及访问权限，记录文件处理环节中操作者的操作行为，确保文件在创建、修改、授权、阅读、签批、盖章、打印、添加水印、流转、存档和销毁等操作中始终处于安全可控的状态，为应用系统提供追溯和审计的依据。

3.4

操作者 operator

对文件进行创建、修改、授权、阅读、签批、盖章、打印、添加水印、流转、存档和销毁等操作的行为主