移动终端数字证书应用标准

总体框架

Digital certificate application standard

for mobile terminal

General framework specification

中国电子认证服务产业联盟

2017 年 11 月

目　　录

前　言

《移动终端数字证书应用标准》分为5个部分：

——第1部分：总体框架；

——第2部分：标识规范；

——第3部分：密码服务接口规范；

——第4部分：证书应用综合服务接口规范；

——第5部分：数字证书认证接口规范。

本部分是《移动终端数字证书应用标准》的第1部分，它描述了移动终端数字证书应用的技术体系框架，说明了体系框架各组成部分的层次结构和逻辑关系。

本部分的附录A是规范性附录。

本部分凡涉及密码算法相关内容均符合国家密码管理主管部门对密码管理的要求。

本部分由中国电子认证服务产业联盟委员会提出并归口。

本部分的主要起草单位：北京创原天地科技有限公司、上海数字证书认证中心、贵州省电子证书有限公司、东方新诚信数字认证中心有限公司、新疆数字证书认证中心(有限公司)、福建省数字安全证书管理有限公司、江西省数字证书有限公司、河南信息安全电子认证中心、南京一证通科技有限公司、河北省电子认证有限公司、广东数安时代科技股份有限公司、广西壮族自治区数字证书认证中心有限公司、山东省数字证书认证管理有限公司、陕西省数字证书认证中心、浙江省数字安全证书管理有限公司、内蒙古网信电子认证有限责任公司、安徽省电子认证管理中心有限责任公司、东方中讯数字证书认证有限公司、湖北省数字证书认证管理中心有限公司、北京世纪速码信息科技有限公司、深圳市电子商务安全证书管理有限公司。

引　言

随着互联网移动化，基于PKI技术体系的移动终端数字证书服务，得到了越来越多的应用。作为一个新的应用领域，由于缺乏顶层的设计，没有相关的标准和规范作为指导，相关产品研制方、应用方和集成方对数字证书在移动互联网的应用都有各自的理解，对于具体的接口和协议都有各自的实现，导致各厂家同类产品间接口差别大，不能实现互联互通，应用方只能绑定到某一个产品，后期更换数字证书产品的成本较高；各数字证书认证中心对外的接口都有自己的特殊性，对接适配工作繁多，实现业务接入周期较长，这些都限制了数字证书在移动终端应用的推广，不利于整个产业的健康发展。因此迫切需要建立一套完整、自主、科学的移动终端数字证书应用标准，为我国移动互联网信息化建设提供可靠的密码支撑。

建立和完善移动终端数字证书应用标准系列规范,一方面为中国电子认证服务产业联盟的行业或团体密码相关标准编制工作提供方向性指导，另一方面给密码及数字证书产业单位的科研、生产、检测，以及为其行业用户提供数字证书及密码应用标准指南。另外，也可以有效解决移动信息系统整体安全问题，有利于推动信息安全产业的发展。

通过对PKI体系进行总体研究、统一规划和协调编制，形成基于PKI体系的移动终端数字证书应用标准系列规范。系列规范把PKI安全特性作为标准服务向用户提供，任何需要身份真实性、数据机密性、数据完整性以及行为不可否认性等服务的应用不必再关心复杂的数学模型和运算，提高应用系统开发效率，推动信息系统的快速发展。

本部分由范围、规范性引用文件、术语和定义、移动终端数字证书应用技术体系框架、框架内系列规范、附录A和参考文献等章节组成。

移动终端数字证书应用标准

总体框架

1 范围

《移动终端数字证书应用标准 总体框架》规定了基于移动终端数字证书应用的技术体系框架，给出了各组成部分及其层次结构和逻辑关系。

《移动终端数字证书应用标准》适用于基于Android和iOS平台的移动智能终端，适用于其规定范围内的所有参与主体及其使用的相关密码产品和技术。这里的参与主体包括终端密码服务平台、移动终端设备和证书管理平台、数字证书认证系统、业务系统以及业务APP。

移动终端数字证书应用技术体系重点对终端密码服务平台对外提供的密码服务接口、证书应用综合服务接口、数字证书认证系统对终端密码设备和证书管理平台提供的接口进行定义。对于业务APP与业务系统、业务系统与终端密码设备和证书管理平台的接口不进行定义。

2 规范性引用文件

下列文件中的条款通过本部分的引用而成为本部分的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本部分。凡是不注日期的引用文件，其最新版本适用于本部分。

GM/T 0028-2014 密码模块安全技术要求

3 术语和定义

下列术语仅适用于本部分。

3.1.

数字证书认证系统 certificate authority system

数字证书认证系统是对生命周期内的公钥证书进行全过程管理的系统。

3.2.

密码边界 cryptographic boundary

明确定义的连续边线，该边线建立了密码模块的物理和/或逻辑边界，并包括了密码模块的所有硬件、软件和/或固件部件。

3.3.

密码模块 cryptographic module

模块 module

实现了安全功能的硬件、软件和/或固件的集合，并且被包含在密码边界内。

3.4.

硬件 hardware

包含在密码边界内，用以处理程序和数据的物理设备/部件。

3.5.

硬件模块 hardware module

主要由硬件构成的模块，其中还可以包含固件。

3.6.

软件 software

密码模块的可执行代码，它存储于易擦除的介质中，在执行期间可以对介质上的软件进行写和修改操作。易擦除介质包括但不限于固态存储器、硬盘等。

3.7.

软件模块 software module

仅由软件组成的模块。

3.8.

富操作系统 Rich OS

高级操作系统执行环境，允许终端用户下载和运行应用。

如Android，Linux， Symbian OS， Microsoft Windows， iOS 等。

3.9.

可信执行环境 Trusted Execution Environment

可信执行环境（Trusted Execution Environment，简称TEE），与Rich OS并行运行的独立执行环境，并为富操作系统提供安全服务。对富操作系统下的软硬件安全资源和应用实现隔离访问和保护。

3.10.

协同密钥运算

将密钥拆分成两部分，分别存储在服务端和移动端，使用时进行协同计算，密钥不会在任何一方完整出现，即参与运算的任何一方都不会拿到完整的密钥。

4 移动终端数字证书应用技术体系

4.1 概述

移动终端数字证书应用技术体系包括终端侧和平台侧，其中终端侧由终端密码服务平台和业务APP构成；平台侧由数字证书认证系统、终端密码设备和证书管理平台及业务系统构成。其中终端密码服务平台与终端密码设备和证书管理平台组合起来作为服务提供者为各行业应用提供密码运算和证书综合服务。

移动终端数字证书应用体系框架如图1所示。

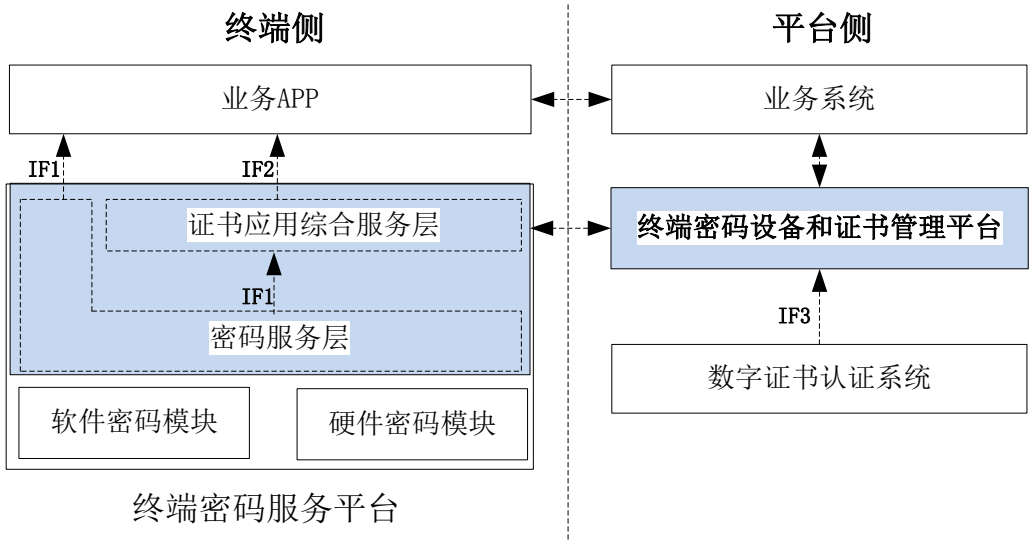

图1. 移动终端数字证书应用技术体系框架

4.2 终端密码服务平台

终端密码服务平台依托底层密码模块通过密码服务层和证书应用综合服务层向上层业务APP提供密码运算、密钥管理服务及证书应用综合服务。

底层密码模块包含软件密码模块和硬件密码模块。硬件密码模块包含：SDKey、USBKey、SIMKey、蓝牙KEY、音频KEY以及TEE+SE等。密码模块安全要求遵循国密行标《GM/T 0028-2014 密码模块安全技术要求》，因此，密码模块相关技术要求不在本标准进行规定要求。

密码服务层是底层密码模块向上提供基础密码运算、密钥存储、产生及管理等服务的接口层。密码服务层兼容支撑软件密码模块和硬件密码模块等密码模块。当前版本密码服务层仅支持软件密码模块。

证书综合服务层依托于密码服务层，向上为业务APP提供统一的、与密码协议无关、与密钥管理无关、与密码设备管理无关的高级密码服务。

密码服务层和证书综合服务层都可直接对上层业务APP提供服务。

4.3 终端密码设备和证书管理平台

终端密码设备和证书管理平台一方面连接数字证书认证系统为证书综合服务层提供证书管理服务，另一方面配合密码服务层实现协同密钥运算服务。

4.4 数字证书认证系统

数字证书认证系统为终端密码设备和证书管理平台提供基础的证书管理服务。

4.5 业务 APP

业务APP是指集成使用终端密码服务平台的第三方业务系统APP。第三方业务系统包括：银行、第三方支付、医疗、社保、税务、政务移动办公等。

4.6 业务系统

业务系统是直接为终端用户提供业务办理的第三方系统。一方面它支撑其APP，提供相关的业务功能；另一方面与终端密码设备和证书管理平台交互，实现相关信息同步。

4.7 接口说明

移动终端数字证书应用标准中的接口定义如表 1 所示。

表 1 移动终端数字证书应用标准中的接口定义

接口	描述	是否在本体系范围内
IF1	终端密码服务平台对外提供的密码服务接口	是
IF2	终端密码服务平台对外提供的证书应用综合服务接口	是
IF3	数字证书认证系统对终端密码设备和证书管理平台提供的接口	是
	终端密码服务平台与终端密码设备和证书管理平台之间的接口	否
	业务系统与终端密码设备和证书管理平台之间的接口	否
	业务 APP 与业务系统之间的接口	否

5 框架内的系列规范

本框架内的系列规范包括：

密码服务接口规范；

证书应用综合服务接口规范；

数字证书认证系统接口规范；

此外，为规范标识（如算法标识、密钥标识、设备标识、数据标识、协议标识、角色标识等）的表示和使用，还应制订标识规范。

附录 A（规范性附录）

错误代码区间划分

本框架内分配的错误代码区间为：

密码服务接口：0x0A000000～0x0AFFFFFFFF

证书应用综合服务接口：0x0B000000～0x0BFFFFFFFF

数字证书认证系统接口：0x0C000000～0x0CFFFFFFFF

返回代码正确为0，非零用错误代码区间表示。

参考文献

[1] GB/T 25069-2010 信息安全技术 术语

[2] GB/T 25056-2010 信息安全技术 证书认证系统密码及其相关安全技术规范

[3] GB/T 25055-2010 信息安全技术 公钥基础设施安全支撑平台技术框架

[4] GB/T 26855-2011 信息安全技术 公钥基础设施 证书策略与认证业务声明框架