ICS 35.040
L 71

MH

中华人民共和国民用航空行业标准

MH/T 0045.3—2013

民航电子政务数字证书服务及技术规范 第3部分：USB Key介质

Specifications for CAAC e-government digital certificate service and technique
Part 3: USB Key medium

2013－11－11 发布　　2014－03－01 实施

中国民用航空局　发布

前　言

MH/T 0045《民航电子政务数字证书服务及技术规范》分为四个部分：

——第1部分：服务；

——第2部分：数字证书模板；

——第3部分：USB Key介质；

——第4部分：证书应用集成。

本部分为第3部分。

本部分按照GB/T 1.1-2009给出的规则起草。

本部分由中国民用航空局综合司提出。

本部分由中国民用航空局航空器适航审定司批准立项。

本部分由中国民航科学技术研究院归口。

本部分起草单位：中国民用航空局信息中心、北京数字认证股份有限公司。

本部分主要起草人：陈黎萍、魏申、张超、李涵、于飞。

民航电子政务数字证书服务及技术规范
第3部分：USB Key介质

1 范围

MH/T 0045 的本部分规定了民航电子政务数字证书介质的硬件技术参数要求，以及对驱动程序及介质接口的要求。民航电子政务内网数字证书介质有关要求不在本标准内涉及。

本部分适用于民航电子政务数字证书认证服务机构、数字证书介质供应商。

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，仅所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 0016 智能密码钥匙密码应用接口数据格式规范

GM/T 0017 智能密码钥匙密码应用接口规范

MH/T 0045.1 民航电子政务数字证书服务及技术规范 第1部分 服务

3 术语和定义

GM/T 0016、GM/T 0017和MH/T 0045.1界定的的术语定义适用于本文件。

4 硬件要求

4.1 组成

硬件部分主要包括USB Key产品外壳、接口电路及内部芯片及固化在芯片里的操作系统COS。

4.2 基本要求

民航电子政务数字证书USB Key应满足以下基本要求：

——应通过国家密码管理局产品鉴定并具备国家商用密码非对称密码算法(SM2)支持的产品型号；

——证书介质供应商应根据民航局证书认证服务机构对证书介质的管理要求，对介质外观进行统一设置；

——介质外形尺寸相当或小于58 mm×18 mm×8 mm（长×宽×高），总体要求外观美观大方；

——宜采用环保材质，色泽鲜明，坚固耐用，不含铅、汞、铬等有害物质；

——介质外观应印制中国民航航徽和“民航电子政务数字证书”字样。

4.3 技术指标要求

民航电子政务数字证书USB Key应满足的技术指标要求见表1：

表1 USB Key 技术指标要求

序号	要求	备注
1	主芯片位数	≥8 位
	主芯片型号	应采用国家密码管理局批准型号的芯片
	用户空间	≥64K Bytes
	VID	2 字节 16 进制字符
	PID	2 字节 16 进制字符
	硬件接口	符合 USB 接口规范，不需额外插电。
	传输模式	支持 USB 协议控制传输或块传输
	传输速率	USB 全速或高速
2	功耗	≤300 mW
	存放温度	(-20～80) ℃
	工作温度	(-20～45) ℃
	湿度要求	10%～90% 不结露
	工作电压	4.5 V～5.5 V
	数据存储年限	至少 10 年
	读写次数	至少 10 万次
	适用浏览器	适用当前主流浏览器
	适用操作系统	适用当前主流操作系统
3	非对称算法	硬件实现 RSA1024、RSA2048、SM2(256 位)
	对称算法	硬件实现国家商用密码分组加密算法(SM1)、国家商用密码分组加密算法(SM4)
	杂凑算法	硬件实现 SHA-1、SHA-256、国家商用密码杂凑算法算法(SM3)
	RSA 公私钥对生成时间（1024 位）	8 位芯片≤3 s；32 位芯片≤2 s
	RSA 签名时间（1024 位）	8 位芯片≥8 次/s；32 位≥20 次/s
	RSA 验签时间（1024 位）	8 位芯片≥12 次/s；32 位≥35 次/s
	RSA 公私钥对生成时间（2048 位）	8 位芯片≤17 s/次；32 位≤12 s
	RSA 签名时间（2048 位）	8 位芯片≥4 次/s；32 位≥10 次/s
	RSA 验签时间（2048 位）	8 位芯片≥15 次/s；32 位≥25 次/s
	SM2 公私钥对生成时间（256 位）	8 位芯片≤0.6 s；32 位≤0.1 s
	SM2 签名时间（256 位）	8 位芯片≥20 次/s；32 位≥30 次/s
	SM2 验签时间（256 位）	8 位芯片≥14 次/s；32 位≥20 次/s
	硬件真随机数发生器	支持
4	安全性要求	用户口令连续 10 次输错后应自动锁死。
5	文件系统	支持删除，删除后文件所占空间实时回收 每个文件拥有独立的创建、读、写权限
	支持证书和标准	X.509 V3 标准证书格式
	可存储证书数量	≥10 个
	可存储非对称密钥对数量	≥10 个
	文件数量限制	≥32 个
	文件大小限制	≥16K 字节

5 软件要求

5.1 驱动程序

数字证书认证服务机构提供的驱动安装程序应满足以下要求：

a) 安装程序中应包括必要的驱动、客户端证书应用接口、证书管理工具等内容。证书管理工具的功能至少包含修改介质口令和查看证书的功能。

b) 安装程序的提示文字应简洁易懂、便于理解，安装菜单清晰合理、方便查找，操作系统桌面上应有证书管理工具的快捷方式。

c) 安装程序应支持主流操作系统，支持简体中文和英文两种语言。

d) 安装程序应能够自动识别用户操作系统的版本并自动安装相应兼容性组件。

5.2 证书介质接口

证书介质接口函数应遵守GM/T 0017和GM/T 0016的函数定义和数据结构定义，提供设备管理、访问控制、文件管理和密码服务等相关密码服务接口。