ICS 35.040
L 71

MH

中华人民共和国民用航空行业标准

MH/T 0045.4—2013

民航电子政务数字证书服务及技术规范 第4部分：证书应用集成

Specifications for CAAC e-government digital certificate service and technique
Part 4：Certificate application integration

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4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：张威、张超、魏申、于清洋、李涵。

民航电子政务数字证书服务及技术规范
第4部分：证书应用集成

1 范围

MH/T 0045的本部分规定了民航电子政务数字证书应用集成总体要求、集成内容及集成接口要求。民航电子政务内网数字证书有关要求不在本部分中涉及。

本部分适用于民航电子政务数字证书应用中间件的设计和实现，指导证书认证服务机构和信息系统开发商实现基于数字证书的安全登录、数字签名和加密解密等安全功能。

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/Z 0001 密码术语

GM/T 0018 密码设备应用接口规范

GM/T 0019 通用密码服务接口规范

GM/T 0020 证书应用综合服务接口规范

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/Z 0001、GM/T 0018、GM/T 0019、GM/T 0020和MH/T 0045.1界定的术语定义适用于本文件。

4 证书应用集成规范

4.1 集成目标

证书应用集成的集成目标如下：

a) 在用户名和口令认证方式基础上，引入数字证书技术，建立基于数字证书的身份认证机制，确保系统访问控制的高安全性和高可靠性；

b) 考虑对民航电子政务信息系统的重要操作环节和重要数据实现基于数字证书的数字签名功能，保护数据的完整性，并为后期纠纷处理及责任认定提供合法电子证据；

c) 对民航电子政务信息系统的重要敏感信息实现基于数字证书的数据加密功能，确保敏感信息在传输和存储阶段的安全性。

4.2 集成要求

在证书应用集成时，应根据民航电子政务信息系统的业务特点和业务需求，确定需要改造的业务系统数量及名称、确定需要使用证书认证的用户及范围、确定需要加密签名的重要操作环节和数据，具体集成要求如下：

a) 民航电子政务信息系统在集成数字证书的安全功能时，首先应实现基于数字证书的身份认证功能；
b) 对于具有操作行为责任认定、证据保存需求的民航电子政务信息系统，应实现基于数字证书的数字签名的功能；
c) 对于具有数据加密和解密需求的民航电子政务信息系统，应实现基于数字证书的信息加密、信息解密功能；
d) 对于具有可信时间需求的民航电子政务信息系统，应集成时间戳功能；
e) 对于具有信息共享需求的多个应用系统，可采用统一的身份认证模式，实现统一的身份认证管理、用户信息共享和单点登录等功能。

4.3 集成内容

4.3.1 基于数字证书的身份认证

证书登录认证过程中，应完成以下安全认证工作：

a) 证书保护口令校验；
b) 每次登录认证是基于随机数的签名和验证，防止重放攻击；
c) 验证用户证书的信任链；
d) 验证用户证书有效期；
e) 基于最新的证书撤销列表，验证用户证书是否被注销；
f) 验证证书信息是否在信息系统中具有对应的用户账户及操作权限。

在证书应用集成时，应实现用户安装和使用的方便性，如证书介质的即插即用功能。

4.3.2 数字签名和验证

民航电子政务信息系统中关键业务数据和操作的数字签名，应满足相关政策法规规定的书面形式、原件形式及文件保存等要求，至少应包括数据原文、电子签名、可信时间等内容，并可在需要时查询、阅读、下载、验证，具备作为电子证据的真实性、可靠性和可验证性。

数字签名可以和图章结合起来应用，实现电子签章功能，从而实现电子签名的可视化管理，方便用户查看、审阅和验证。

4.3.3 数据加密和解密

数据加密时应采用对称算法和非对称算法相结合的方式，既保障加密机制的安全性、密钥分发的方便性，同时又提高了加解密操作的效率。根据业务需求，可使用单个数字证书加密，也可使用多个数字证书对数据共同加密，形成密文数据。

密文数据应安全存储在数据库或磁盘上，待解密时间达到后方可解密。数据解密时，须使用数字证书对应的密码设备或证书介质解密。如果证书介质损坏或丢失，电子认证服务机构应在安全可控的前提下，为用户及时提供密钥恢复服务。

4.3.4 时间戳应用

认证服务机构提供的时间戳服务应基于可靠的标准时间源，确保时间的准确和可信。

4.3.5 密码设备应用

民航电子政务信息系统在使用数字证书安全功能时，应基于密码设备提供的密码服务。密码设备包括客户端用户使用的证书介质和服务器端使用的密码设备。

客户端证书介质是指具有密码许可资质的USB Key、智能IC卡等PC终端上的密码设备，以及符合国家密码政策管理规定的SIM卡、SD卡等手机终端上的密码设备。证书介质应用接口应支持所有主流操作系统，并符合GM/T 0018的要求。

服务器端密码设备是指具有密码许可资质的加密机、加密卡等，应支持所有主流操作系统，并符合GM/T 0018的要求。

通用密码服务接口调用证书介质应用接口或密码设备应用接口，实现对底层密码设备和证书介质的调用，应支持所有主流操作系统，并符合GM/T 0019的要求。

4.4 证书应用接口规范

4.4.1 证书介质应用接口

证书介质应用接口是客户端证书介质的底层应用接口，该接口应符合GM/T 0018的要求。

证书介质应用接口适用于USB Key等终端密码设备上，应支持操作终端类的主流操作系统。

4.4.2 密码设备应用接口

密码设备应用接口是服务器端密码设备（如加密机）的底层应用接口，该接口应在符合RSA程序设计接口（PKCS#11）技术规范的基础上，符合GM/T 0018的要求。

密码设备应用接口适用于加密机等服务器的密码设备上，应支持服务器类的主流操作系统。

4.4.3 通用密码接口

通用密码接口是屏蔽了底层不同密码设备类型和底层接口的通用中间件，该接口应符合GM/T 0019的要求。

通用密码接口适用于客户端和服务器端使用，应支持主流操作系统。

4.4.4 客户端组件接口

客户端控件接口是供民航电子政务信息系统直接调用的高级接口，适用于客户端程序使用，应支持操作终端类的主流操作系统，该接口应符合GM/T 0020的要求。

客户端控件与服务端组件对应，其主要功能函数包括：配置管理、数字证书解析、签名与验证、数据加密与解密、加密信息的语法规则(PKCS#7)数据信封、XML数据的签名与验证、文件签名与加解密等。

4.4.5 服务端组件接口

服务器端组件接口是供民航电子政务信息系统直接调用的高级接口，适用于服务器端程序使用，应支持主流操作系统，该接口应符合GM/T 0020的要求。

服务器端组件接口的主要功能函数与客户端控件接口对应，包括：配置管理、数字证书解析、签名与验证、数据加密与解密、PKCS#7数据信封、XML数据的签名与验证、文件签名与加解密等。