

**NFC读取护照流程说明书**

安徽中科智链信息科技有限公司

目 录

[一.护照简介 1](#_Toc512588574)

[二.协议与命令 1](#_Toc512588575)

[2.1命令结构说明 1](#_Toc512588576)

[2.2 CAPDU结构说明 1](#_Toc512588577)

[2.3响应数据结构说明 2](#_Toc512588578)

[2.4 RAPDU结构说明 2](#_Toc512588579)

[三.流程分析 3](#_Toc512588580)

[3.1激活NFC 3](#_Toc512588581)

[3.2寻卡 4](#_Toc512588582)

[3.3文件应用选择 4](#_Toc512588583)

[3.4加密 5](#_Toc512588584)

[3.5发送加密数据 5](#_Toc512588585)

[3.6常见RAPDU状态码含义参考 5](#_Toc512588586)

[参考文献 6](#_Toc512588587)

# 一.护照简介

目前，我国在全国各地办理的电子护照，不同地方采用不同的电子芯片，其电子芯片目前分为A型和B型两种，但都根据《ISO/IEC-14443》《ISO/IEC-7816》《ICAO-DOC-9303（机读旅行证件）》三个国际标准协议文件制定，可在国际通用，以下的信息读取和校验过程都是基于这三个标准文件。

港澳通行证的验证方式和护照是一致的，使用同样的协议解析，目前已知的港澳通行证芯片为A卡。

# 二.协议与命令

本次读取护照信息使用的NFC芯片型号是PN532，NFC与护照芯片的通讯协议遵循了《ISO/IEC-14443》和《ISO/IEC-7816》的标准，以下分析了命令数据和响应数据的结构说明，以便大家快速了解命令与响应的结构和含义。

## 2.1命令结构说明

报头 + 命令长度 + 命令长度校验 + （发送标志 + 命令 + 参数 + 数据(CAPDU)） + 命令校验 +结尾

**例:** （获取随机数指令）00 00 FF 08 F8 D4 40 01 00 84 00 00 08 5F 00

00 00 FF报头

08 命令长度

F8 命令长度校验（100 - 04）

D4 发送命令的标志

40 操作命令

1. 目标卡的逻辑号

00 84 00 00 08（CAPDU）命令

E1 命令校验（从D4开始，加到命令数据，去后两位，100减去此值）

00 报尾

## 2.2 CAPDU结构说明

CLA + INS + P1 + P2 + Lc + Data + Le

**例：**00 84 00 00 08

00 84 请求一个随机数

00 00 参数1，参数2，不同命令中意义不一

(空) 或是后续数据字段的长度

(空) 或是鉴别相关的数据

08 Le是响应预期最大字节数，此命令若无响应数据，仅有结果状态，则此为空

## 2.3响应数据结构说明

报头 + 响应数据长度 + 响应数据长度校验 + (响应标志+响应命令+RAPDU) + 响应数据校验 + 报尾

**例：**00 00 FF 00 FF 00

* 1. 00 FF 0D F3 D5 41 00 A9 50 19 5C 47 C5 C0 01 90 00 1F 00

00 00 FF 00 FF 00 ACK响应

00 00 FF 报头

0D 响应数据长度

F3 响应数据长度校验(100-0D)

D5 响应数据标志

41 响应命令标志(此处值为 操作命令+1，即40 + 1)

00 命令响应状态（00为发送成功）

A9 50 19 5C 47 C5 C0 01 （返回的8位随机数）

1. 00 是APDU响应的状态（90 00 表示成功响应）

1F 表示数据校验（同发送数据校验的算法）

00 报尾

## 2.4 RAPDU结构说明

Data + SW1 + SW2

**例:** A9 50 19 5C 47 C5 C0 01 90 00

A9 50 19 5C 47 C5 C0 01 期待响应的数据

90 00 结果状态，此为执行结果正确

其他响应状态，如6A 82代表未找到文件，69 86不满足命令执行条件，以上CAPDU和RAPDU可到相关文档中查看。

参考:《电子钱包电子存折应用卡片规范》第11页，文库链接 <https://wenku.baidu.com/view/ceb843a24afe04a1b171de46.html> ；

Android App《Passport-Reader-Master》源码中PassportApduService.java文件的sendGetChallenge()方法，如图1所示。

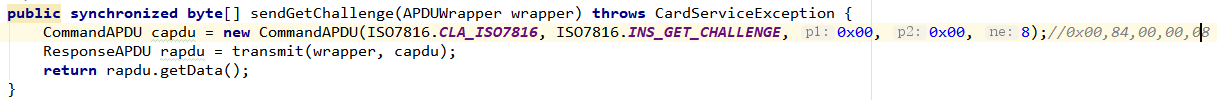


图1 Android源码

# 三.流程分析

护照信息验证的流程如下图2所示，除了在激活NFC和寻卡过程中不会返回40 01超时错误，其他操作过程中若返回40 01超时错误时，需要重新寻卡。

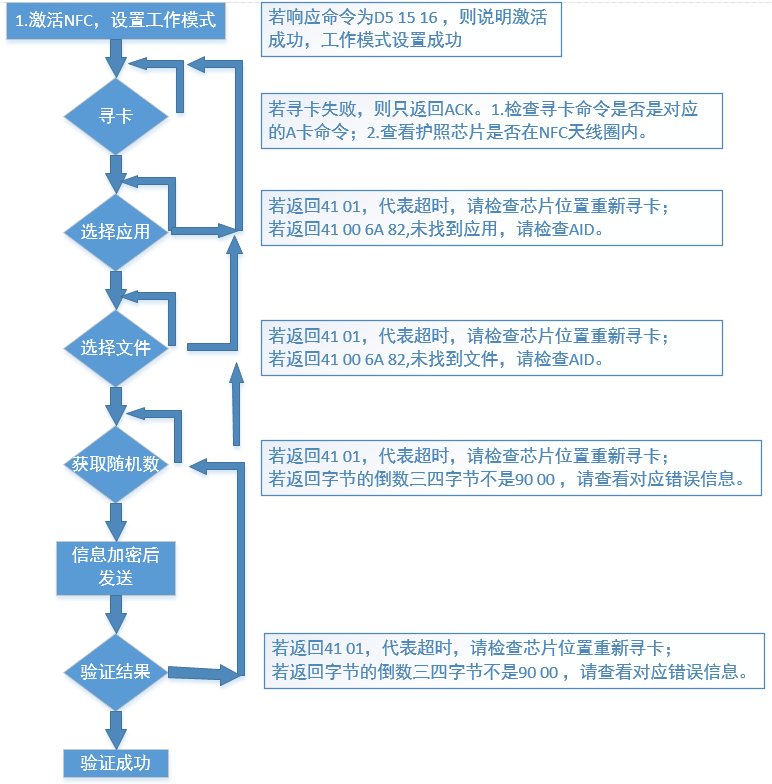


图2 护照信息验证流程简图

## 3.1激活NFC

我们采用的是NFC芯片型号是PN532，激活命令如下:

55 55 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF 03 FD 17 00

该命令用于通过配置内部串行数据开关来选择数据流路径。模式定义了使用SAM（安全访问模块）的方式，14是设置NFC模式命令，01代表选择普通模式（默认），02代表虚拟卡，03代表有线卡，04代表双卡，设置完成后NFC芯片处于待机模式。

若无返回信息，请检查COM口是否选择正确，是否插好通电。返回D5 15即NFC唤醒成功。

参考：《科星NFC模块用户手册V2.0》3.1.3节

## 3.2寻卡

A卡的寻卡命令为: 00 00 FF 04 FC D4 4A 01 00 E1 00 ;

B卡的寻卡命令为: 00 00 FF 05 FB D4 4A 01 03 00 DE 00 ;

除去响应的ACK6个字节，若寻卡成功，则返回24个字节的数据。若以A卡的命令寻B卡，则只返回6位ACK响应，反之亦然。

参考：《科星NFC模块用户手册V2.0》3.1.4节；《PN532 User Manual》7.3.5节

## 3.3文件应用选择

电子机读旅行证件中的信息存储在[ISO/IEC 7816-4]定义的文件系统中。该文件系统按层次结构包括专用文件（DF）和基本文件（EF）。专用文件（DF）包含基本文件或其他专用文件。选择性的主文件（MF）可以是文件系统的根目录。

1. **Send Select Applet：**

00 00 FF 0F F1 D4 40 01 00 A4 04 0C 07 A0 00 00 02 47 10 01 36 00

电子机读旅行证件应用应通过使用作为预留 DF 名的应用标识符（AID）来选择。应用标识符应包括国际标准化组织根据[ISO/IEC7816-5]分配的注册应用标识符和本文件中规定的专有应用标识符扩展项（PIX）。电子机读旅行证件应用的全AID是A0 00 00 02 47 10 01。

1. **Send Select File：**

00 00 FF 0A F6 D4 40 01 00 A4 02 0C 02 01 1E 18 00

有两种方法读取来自电子机读旅行证件的数据：通过选择该文件，然后读取数据，或通过使用短文件标识符直接读取数据。对于电子机读旅行证件，支持短文件标识符是必要的，因此建议使用短文件标识符。此处没有使用短文件标识符。

**c. Send Get Challenge：**

00 00 FF 08 F8 D4 40 01 00 84 00 00 08 5F 00

获取随机数，用于和护照进行通讯加密验证。

参考：《Doc9303-机读旅行证件-第七版-2015年 第10部分》3.9节

Android App《Passport-Reader-Master》源码中PassportApduService.java文件的

sendSelectFile()方法，sendSelectApplet()方法和sendGetChallenge()方法。

## 3.4加密

个人的证件信息的极为重要，护照的信息读取安全也必须加密。我国电子护照遵循《ICAO-DOC-9303（机读旅行证件）》的标准，所以护照的安全验证问题也遵循相关ISO标准文件的要求。

为了防止护照信息被随意读取，需要根据护照的编号、有效日期和持有者生日三个数据加密，生成公钥和私钥，根据SHA-1（安全散列算法）生成keySeed，再根据keySeed生成kEnc和kMac。本地生成1个8字节随机数组和1个16字节随机数组，把这两个随机数组和从护照芯片获取的随机数字进行拼接加密，通过APDU发送个护照芯片验证。

参考: Android App《Passport-Reader-Master》源码中PassportService.java的doBAC()方法，PassportApduService.java的sendMutualAuth()方法。

《Doc9303-机读旅行证件-第七版-2015年 第10部分》3.9.3节

## 3.5发送加密数据

把上一流程生成的加密数据利用APDU发送给护照芯片进行验证，发送验证数据的命令格式如下:

CLA + INS + P1 + P2 + dataLength + data + expectedDataLength

00 82 00 00 28 + data + 28

如果接收到长度为42的RAPDU，即响应数据+sw1+sw2，如果最后两个字节是90 00 则证明验证成功。

参考: 百度文库:《电子钱包电子存折应用卡片规范》 <https://wenku.baidu.com/view/2be43622af45b307e871978a.html>

第10页6.2.6节

## 3.6常见RAPDU状态码含义参考

|  |  |  |
| --- | --- | --- |
| **SW1** | **SW2** | **含义** |
| 90 | 00 | 命令执行成功/正确 |
| 6A | 82 | 未找到文件 |
| 69 | 82 | 不满足安全状态 |
| 69 | 84 | 引用数据无效 |
| 69 | 86 | 不满足命令执行条件 |

参考: 百度文库:《电子钱包电子存折应用卡片规范》 <https://wenku.baidu.com/view/2be43622af45b307e871978a.html>

第4部分

# 参考文献

《PN532 User Manual》- PN532芯片的官方pdf文档

《科星NFC模块用户手册V2.0》

《Doc9303-机读旅行证件-第七版-2015年 第10部分》

百度文库:《电子钱包电子存折应用卡片规范》 <https://wenku.baidu.com/view/2be43622af45b307e871978a.html>