

ICS 35.110

M 11

**YD**

# 中华人民共和国通信行业标准

YD/T 3152-2016

---

## 网络电子身份标识 eID 移动应用接口 技术要求

Technical Requirements for eID Mobile Application Interface

2016-07-11 发布

2016-10-01 实施

---

中华人民共和国工业和信息化部 发布

## 目 次

前 言	II
引 言	III
1 范围	1
2 规范性引用文件	1
3 术语、定义和缩略语	1
4 eID移动应用服务	1
5 eID移动应用注册要求	2
6 eID移动应用接口	2
附录A（资料性附录） 接口调用示例	8
附录B（资料性附录） 移动应用接口函数交互图	9
附录C（规范性附录） 错误码定义	11
参考文献	14

广东省网络空间安全协会受控资料

## 前 言

本标准属于网络电子身份标识eID相关服务与应用接口系列标准之一，该系列标准包括：

- 《网络电子身份标识eID桌面应用接口技术要求》
- 《网络电子身份标识eID移动应用接口技术要求》
- 《网络电子身份标识eID验证服务接口技术要求》
- 《网络电子身份标识eID桌面应用接口测试方法》
- 《网络电子身份标识eID移动应用接口测试方法》
- 《网络电子身份标识eID验证服务接口测试方法》

本标准依据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。

本标准由中国通信标准化协会提出并归口。

本标准由公安部第三研究所、中国科学院软件研究所、北京中电华大电子设计有限责任公司、国防科学技术大学计算机学院、北京邮电大学、中国科学院信息工程研究所等单位起草。

本标准主要起草人：邹翔、杨明慧、汪志鹏、倪力舜、赵宏伟、高志刚、兰天、李树栋、落红卫、高峰、柳扬、全拥、邓璐、许晋、周薇、戴娇。

## 引 言

本技术要求旨在规范接口的命名；统一接口调用方式，方便eID移动应用接入；减少多个功能库的共用接口，减小维护成本；方便在此基础上添加新的功能接口。

本文件主要描述第三方应用通过移动终端访问eID卡的接口。第三方应用后台与eID服务平台的交互参见《网络电子身份标识eID验证服务接口技术要求》。

广东省网络空间安全协会受控资料

# 网络电子身份标识eID移动应用接口技术要求

## 1 范围

本标准规范了eID应用于移动应用的相关接口技术要求。

本标准适用于eID移动应用接口。

## 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。

YD/T 3150-2016 网络电子身份标识eID验证服务接口技术要求

YD/T 2592-2013 身份管理(IdM)术语

## 3 术语、定义和缩略语

### 3.1 术语和定义

YD/T 2592-2013界定的以及下列术语和定义适用于本文件。

#### 3.1.1

**eID 移动应用客户端 eID mobile application client**

在移动终端上实现eID实名认证、账号保护和安全登录服务的客户端软件。

### 3.2 缩略词

下列缩略语适用于本文件。

eID	electronic Identity	网络电子身份标识
eIDAuth		eID认证对象
hash		杂凑算法
idCarrier		载体唯一标识符
NFC	Near Field Communication	近距离无线通信
PIN	Personal Identification Number	个人识别码
ri	ResultInfo	返回结果对象
SDK	Software Development Kit	软件开发工具包

## 4 eID 移动应用服务

### 4.1 基本功能

eID移动应用服务主要为eID移动应用提供三个功能：实名认证、账号保护、安全登录。eID移动应用通过接口技术方法与eID交互，使用以下这三个服务功能。

### 4.2 移动实名认证

eID移动实名认证为eID移动应用提供安全便捷的移动端实名认证服务。用户下载eID移动应用客户端，安装并绑定自己的eID卡后，用户即可通过手机刷eID卡的方式进行eID移动应用的实名认证业务。

### 4.3 移动账号保护

#### 4.3.1 基本功能

eID的账号保护，即自建立eID第三方应用账号和eID之间的绑定关系起，一旦发生用户账号被盗或忘记密码的情况时，用户只需要刷eID卡就可以重置账号信息，让账号重新回到用户手中，eID账号保护包括账号绑定和账号找回两个过程。

#### 4.3.2 账号绑定

eID移动账号绑定为eID移动应用提供安全便捷的移动端账号绑定服务。用户下载eID移动应用客户端并安装后，即可通过手机刷eID卡的方式进行eID移动应用的账号绑定业务。

#### 4.3.3 账号找回

eID移动账号找回为eID移动应用提供安全便捷的移动端账号找回服务。用户下载eID移动应用客户端，安装并绑定自己的eID卡后，用户即可通过手机刷eID卡并输入PIN码的方式进行eID移动应用的账号找回业务。

### 4.4 移动安全登录

eID移动安全登录为eID移动应用提供安全便捷的移动端登录服务。用户下载eID移动应用客户端，安装并绑定自己的eID卡后，用户即可通过手机刷eID卡的方式进行eID移动应用的登录业务。

## 5 eID移动应用注册要求

第三方应用接入eID系统前，需联系eID服务平台进行注册。具体的规范描述见YD/T 3150-2016《网络电子身份标识eID验证服务接口技术要求》。

## 6 eID移动应用接口

### 6.1 接口函数列表

通过调用eID移动应用接口，eID移动应用可以实现eID基本服务功能的接入使用与应用改造。对于eID移动应用，可以通过以下两种层次访问eID卡：

- API层访问
- 应用层访问

通过这两种方式访问eID卡的应用接口函数如表1所示，接口函数交互图详见附录C。

表1 eID移动应用接口函数列

函数名	说明	对应章节
isSupportNFC	检测设备是否支持且开启NFC	6.2.2
openDevice	打开设备	6.2.3
closeDevice	关闭设备	6.2.4
geteIDNO	eID序列号获取	6.2.5
getIdCarrier	idCarrier获取	6.2.6
verifyPIN	PIN码校验	6.2.7
hash	杂凑算法	6.2.8
privateKeySign	私钥签名	6.2.9

表1 (续)

函数名	说明	对应章节
publicKeyVerify	公钥验证签名	6.2.10
getCertInfo	获取证书信息	6.2.11
getErrorDescription	获取结果码描述	6.2.12
getInstance	eIDAuth实例获取	6.3.2
isEIDAppInstalled	eID移动应用客户端安装判断	6.3.3
eIDAppEventListener	监听器实现	6.3.4
addListener	监听器添加	6.3.5
removeListener	监听器删除	6.3.6
startEIDApp	eID移动应用客户端启动	6.3.7
isEIDAppSupportAPI	最低版本要求	6.3.8
getVersion	SDK版本获取	6.3.9
getEIDAppSupportAPI	eID移动应用客户端最低版本号获取	6.3.10
getEIDAppVerCode	eID移动应用客户端版本号获取	6.3.11
getEIDAppVerName	eID移动应用客户端版本名获取	6.3.12

## 6.2 API 层访问

### 6.2.1 API 层访问接口方法

API层访问方式是将对eID卡的操作嵌入到移动应用中，由移动应用直接访问eID卡的方式。其接口是嵌入式SDK接口。对eID卡的操作方法包括：

- 检测设备是否支持且开启 NFC
- 打开设备
- 关闭设备
- 获取 eID 序列号
- 获取 idCarrier
- 校验 PIN 码
- 杂凑算法
- 私钥签名
- 公钥验证签名
- 获取证书信息
- 获取结果码描述

### 6.2.2 检测设备是否支持且开启 NFC

函数名：isSupportNFC。

输入：当前上下文环境。

输出：返回结果。

说明：为0表示支持NFC；1表示不支持NFC；2表示支持但未开启NFC。

### 6.2.3 打开设备

函数名：openDevice。

输入：NFC发现的卡。

输出：返回结果对象ri。

说明：例如，ri.errorCode为0表示成功；非0表示失败。

#### 6.2.4 关闭设备

函数名：closeDevice。

输入：无。

输出：返回结果对象ri。

说明：例如，ri.errorCode为0表示成功；非0表示失败。

#### 6.2.5 获取 eID 序列号

函数名：geteIDNO。

输入：无。

输出：返回结果对象ri。

说明：例如，ri.errorCode为0表示成功，可通过ri.result得到eID序列号信息（48字节）；非0表示失败。

#### 6.2.6 获取 idCarrier

函数名：getIdCarrier。

输入：无。

输出：返回结果对象ri。

说明：例如，ri.errorCode为0表示成功，可通过ri.result得到idCarrier信息(12字节)；非0表示失败。

#### 6.2.7 校验 PIN 码

函数名：verifyPIN。

输入：string类型的待验证eID卡的PIN码值，一般是4~12位数字。

输出：返回结果对象ri。

说明：例如，ri.errorCode为0表示该PIN码与卡实际PIN一致；非0表示不一致。

#### 6.2.8 杂凑算法

函数名：hash。

输入：字符型或字符串类型的签名模式，需要根据具体的要求计算杂凑值。

输出：返回结果对象ri。

说明：例如，ri.errorCode为0表示计算hash值成功，可通过ri.result得到新的签名；非0表示计算hash值失败。

#### 6.2.9 私钥签名

函数名：privateKeySign。

输入：要签名的十六进制字符串或字节类型数组。

输出：返回结果对象ri。

说明：例如错误代码ri.errorCode为0表示签名成功，可以通过result拿到签名结果；非零表示签名失败。

#### 6.2.10 公钥验证签名

函数名：publicKeyVerify。

输入：原文数据的十六进制字符串，和验签数据的十六进制字符串。

返回：返回结果对象ri。

说明：例如ri为true表示验签成功，false表示验签失败。

### 6.2.11 获取证书信息

函数名：getCertInfo。

输入：获取到的证书信息。

输出：返回结果对象ri。

说明：例如，错误代码ri.errorCode为0表示获取证书信息成功；非零表示获取证书信息失败。

### 6.2.12 获取结果码的描述

函数名：getErrorDescription。

输入：结果码errorCode。

返回：返回结果码描述的字符串。

说明：结果码参考附录C《错误码定义》。

## 6.3 应用层访问

### 6.3.1 应用层访问接口方法

应用层访问方式是由移动应用调用eID移动应用客户端以访问eID卡的方式。其接口是交互式SDK接口。接口方法包括：

- 获取 eIDAuth 实例
- 判断 eID 移动应用客户端是否安装
- 实现监听器
- 添加监听器
- 删除监听器
- 启动 eID 移动应用客户端
- 判断当前安装的 eID 移动应用客户端是否符合 SDK 所支持的最低版本要求
- 获取 SDK 版本
- 获取 SDK 所支持的 eID 移动应用客户端最低版本号
- 获取当前安装的 eID 移动应用客户端版本号
- 获取当前安装的 eID 移动应用客户端版本名

### 6.3.2 eIDAuth 获取

eIDAuth是eID认证对象,是调用者与eID移动应用客户端之间传递数据的桥梁。

函数名：getInstance。

输入：context类型的当前eID移动应用客户端的运行上下文。

输出：eIDAuth实例。

### 6.3.3 eID 移动应用客户端安装判断

函数名：isEIDAppInstalled。

输入：无。

输出：布尔类型的返回值，true表示安装；false表示未安装。

说明：建议在启动eID移动应用客户端之前作检查，判断eID移动应用客户端是否安装。

#### 6.3.4 监听器实现

应通过实现下列接口来监听eID移动应用客户端事件消息：

函数名：eIDAppEventListener。

输入：string类型的第三方应用包名，启动eID移动应用客户端时传入的；integer类型的eID移动应用客户端事件消息结果码。

输出：无。

说明：建议先检查传入的第三方应用包名字符串是否与自己的应用包名完全一致，如果一致，则处理；如果不一致，则可以忽略。

#### 6.3.5 监听器添加

函数名：addListener。

输入：string类型的移动应用的包名；eID移动应用客户端事件消息监听器（6.3.4中所述）。

输出：integer类型的返回码，0表示成功；非0表示失败。

说明：如果用户需要监听，应增加一个派生类实现EIDAppEventListener接口，从而通过其参数获取事件消息。添加监听器后可以收到eID移动应用客户端的事件消息，例如认证结果信息。

#### 6.3.6 监听器删除

接口 removeListener。

输入：无。

输出：无。

说明：当不再监听eID移动应用客户端事件消息时，必须删除监听器。

#### 6.3.7 eID 移动应用客户端启动

函数名：startEIDApp。

输入：string类型的待授权认证的数据字符串；string类型的保留字段。

输出：integer类型的返回码，0表示成功；非0表示失败。

#### 6.3.8 最低版本要求

函数名：isEIDAppSupportAPI。

输入：无。

输出：布尔类型的返回码，true表示符合；false表示不符合。

说明：判断当前安装的eID移动应用客户端是否符合SDK所支持的最低版本，建议先调用isEIDAppInstalled来判断eID移动应用客户端是否已安装。

#### 6.3.9 SDK 版本获取

函数名：getVersion。

输入：无。

输出：string类型的版本字符串，形如1.0.0.0。

#### 6.3.10 最低版本号获取

函数名：getEIDAppSupportAPI。

输入：无。

输出：int类型的版本号。

说明：获取SDK所支持的eID移动应用客户端最低版本号。

#### 6.3.11 eID 移动应用客户端版本号获取

函数名：getEIDAppVerCode。

输入：无。

输出：int类型的版本号值，如果未安装，则返回错误码。

说明：获取当前安装的eID移动应用客户端版本号。

#### 6.3.12 eID 移动应用客户端版本名获取

函数名：getEIDAppVerName。

输入：无。

输出：string类型的版本字符串，如果未安装，则返回null。

说明：获取当前安装的eID移动应用客户端版本名称。

广东省网络空间安全协会受控资料

附 录 A  
(资料性附录)  
接口调用示例

用java语言编写的接口调用简单示例如下（应用层访问方式）：

```

package com.example.test;
import com.trimps.eid.sdk.openapi.EIDAppEventListener;
import com.trimps.eid.sdk.openapi.EIDAuth;
.....
public class MainActivity
extends Activity
implements EIDAppEventListener {
    private static final String TAG = MainActivity.class.getName();
    EIDAuth auth = null;
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_main);
        auth = EIDAuth.getInstance(this);
        auth.addListener(this.getPackageName(), this);
        boolean code = auth.isEIDAppInstalled();
        Log.d(TAG, "eID App installed : " + code);
        code = auth.isEIDAppSupportAPI();
        Log.d(TAG, "can be supported by SDK : " + code);
        int verCode = auth.getEIDAppVerCode();
        Log.d(TAG, "verCode = " + verCode);
        String verName = auth.getEIDAppVerName();
        Log.d(TAG, "verName = " + verName);
        int ret = auth.startEIDApp("subo4110", "");
        Log.d(TAG, "ret = " + ret);
        //...
    }
    public boolean onCreateOptionsMenu(Menu menu) {
        getMenuInflater().inflate(R.menu.main, menu);
        return true;
    }
    public void onError(String arg0, int arg1) {
        Log.d(TAG, "onError - yourPkgName = " + arg0);
        Log.d(TAG, "onError - code = " + arg1);
    }
    protected void onDestroy() {
        auth.removeListener();
        super.onDestroy();
    }
}
}

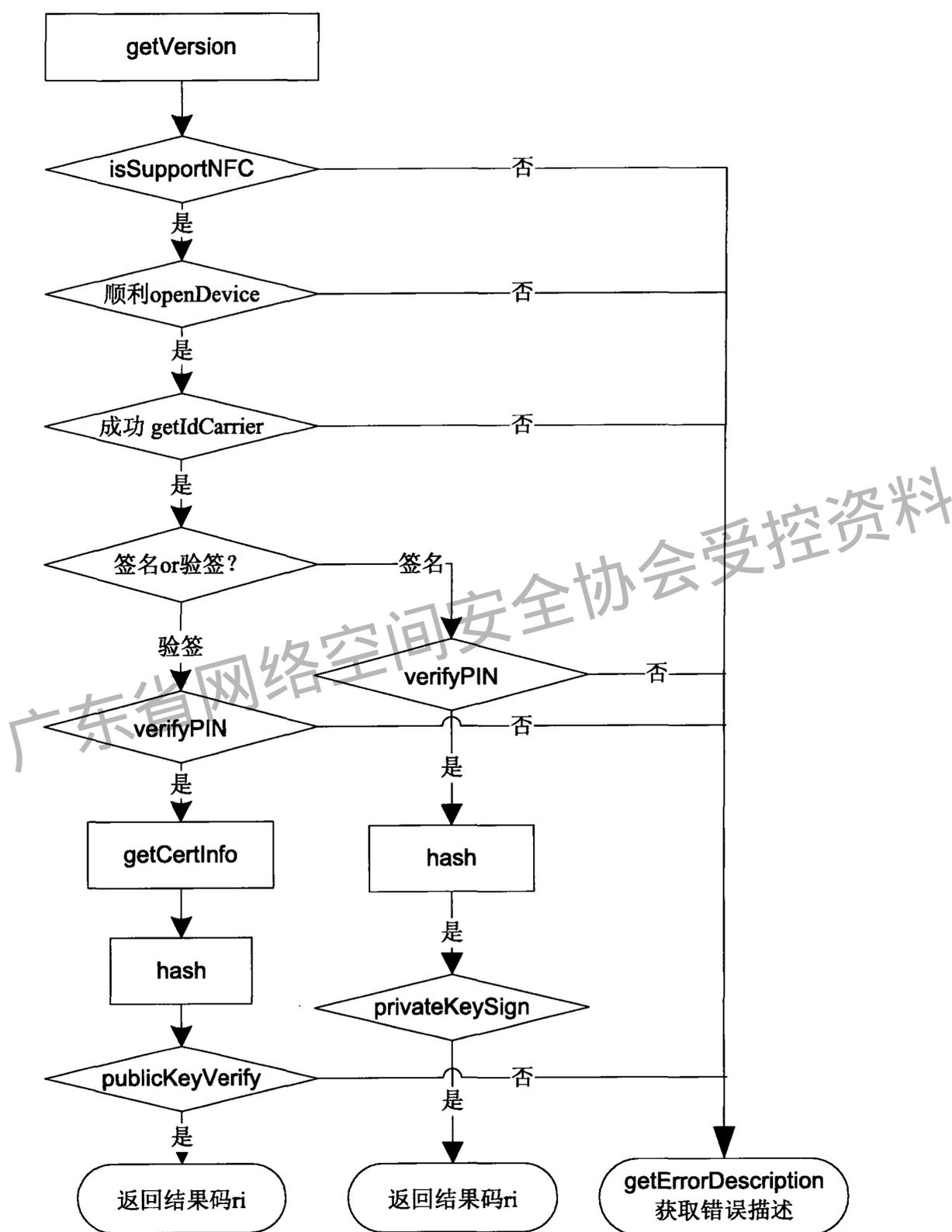
```

附录 B  
(资料性附录)

移动应用接口函数交互图

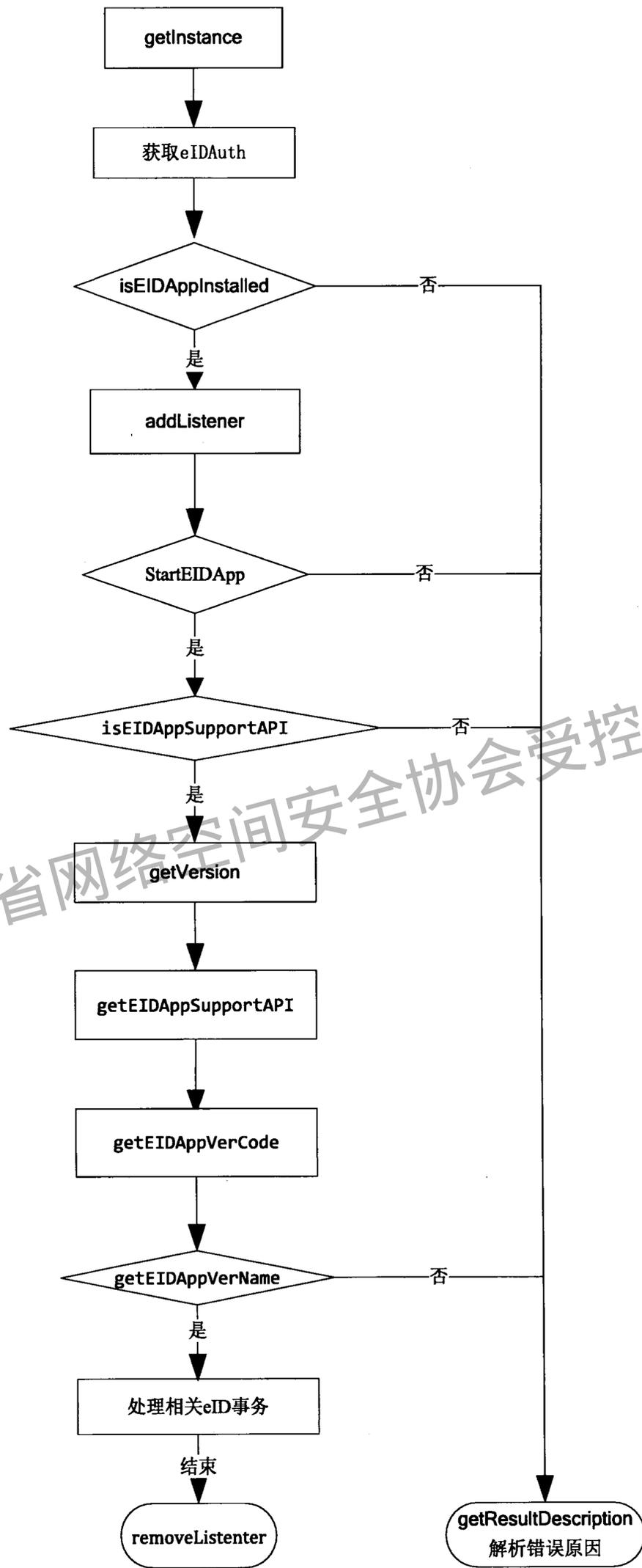
eID移动应用调用移动应用接口可以实现eID基本服务功能的接入使用与应用改造。对于eID移动应用，可以通过以下API层或应用层的移动应用接口访问eID卡。

B.1 API层接口函数交互图



图B.1 API层接口函数交互图

B.2 应用层接口函数交互图



图B.2 应用层接口函数交互图

附 录 C  
(规范性附录)  
错误码定义

0x6282	文件长度<Le
0x6283	选择文件无效
0x6284	FCI格式与P2指定的不符
0x6581	内存错误
0x6700	Lc或Le有错
0x6882	不支持安全报文
0x6901	(命令不接受)无效状态
0x6981	命令与文件结构不相容
0x6982	安全状态不满足
0x6983	卡片锁定
0x6984	引用数据无效
0x6985	使用条件不满足
0x6986	不满足命令执行的条件(不是当前的EF)
0x6987	安全报文数据项丢失
0x6988	安全报文数据项不正确
0x6A80	数据域参数不正确
0x6A81	功能不支持
0x6A82	没有找到文件
0x6A83	没有找到记录
0x6A84	没有足够的空间
0x6A86	P1,P2参数不正确
0x6A88	未找到引用数据
0x6B00	参数错误(偏移地址超出了EF)
0x6CXX	长度错误(Le不正确,'XX'表示实际长度)
0x6D00	不正确的INS
0x6E00	不正确的CLA
0x6F00	数据无效
0x9302	MAC无效
0x9303	应用已被永久锁定

前两个字节为0xe01X(0-3)时表示自定义错误，其中0xe010表示卡片层错误，0xe011表示上下文环境错误，0xe012表示统一接口层错误，0xe013表示卡片设备层错误。后2字节表示具体错误信息如下：

0x0000	操作成功
0x0001	未知错误

0x0002	函数不支持
0x0003	卡对象错误
0x0004	卡设备对象错误
0x0005	参数错误
0x0006	数据长度错误
0x0007	算法错误
0x0008	填充或反填充错误
0x0009	初始化向量错误
0x000A	密钥错误
0x000B	对称算法模式错误
0x000C	错误的角色
0x000D	文件ID错误
0x000E	目录名错误
0x000F	指定的文件已存在
0x0010	指定的文件不存在
0x0011	密钥类型错误
0x0012	指定的容器已存在
0x0013	指定的容器不存在
0x0014	无效的容器
0x0015	未完成初始化
0x0016	枚举设备错误
0x0017	设备句柄错误
0x0018	设备名错误
0x0019	无法找到设备
0x001A	打开设备失败
0x001B	加载函数地址错误
0x001C	没有足够的内存
0x001D	PIN码长度错误
0x001E	文件偏移错误
0x001F	会话密钥索引错误
0x0020	用户已取消
0x0021	打开互斥错误
0x0022	无法找到已打开的设备
0x0023	未找到能力文件
0x0024	设备名错误
0x0025	文件系统错误
0x0026	指定的算法与密钥类型不匹配

0x0027	不允许插入多个设备
0x0028	计算错误
0x0029	没有绑定SN
0x0030	设备错误
0x0031	读取HashMap错误
0x0032	读取eID号错误
0x0033	填充类型错误
0x0034	填充数据长度错误
0x0035	反填充数据错误
0x0036	未打开设备
0x0037	Eid卡已被锁定
0x0038	PIN校验失败

广东省网络空间安全协会受控资料

## 参 考 文 献

- [1] GB/T 16649.1-2006 识别卡.带触点的集成电路卡.第 1 部分: 物理特性
  - [2] GB/T 16649.2-2006 识别卡.带触点的集成电路卡.第 2 部分: 触点的尺寸和位置
  - [3] GB/T 16649.3-2006 识别卡.带触点的集成电路卡.第 3 部分: 电信号和传输协议
  - [4] GB/T 16649.4-2006 识别卡.带触点的集成电路卡.第 4 部分: 用于交换的结构、安全和命令
  - [5] GB/T 16649.6-2001 识别卡.带触点的集成电路卡.第 6 部分: 行业间数据元
- 

广东省网络空间安全协会受控资料

广东省网络空间安全协会受控资料

中华人民共和国  
通信行业标准  
网络电子身份标识 eID 移动应用接口技术要求  
YD/T 3152-2016

\*

人民邮电出版社出版发行  
北京市丰台区成寿寺路11号邮电出版大厦  
邮政编码：100164  
北京康利胶印厂印刷  
版权所有 不得翻印

\*

开本：880×1230 1/16 2016年10月第1版  
印张：1.5 2016年10月北京第1次印刷  
字数：34千字

15115·1178

定价：20元

本书如有印装质量问题，请与本社联系 电话：(010)81055492