ICS 35.240
A 90

GA

# 中华人民共和国公共安全行业标准

GA/T XXXX—XXXX

# 信息安全技术 双接口鉴别卡安全技术要求

Information security technology Security technology requirements for dual-interface authentication card

（报批稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中华人民共和国公安部　发布

# 目　　次

前言 ..... II
1 范围 ..... 1
2 规范性引用文件 ..... 1
3 术语和定义 ..... 1
4 缩略语 ..... 1
5 双接口鉴别卡描述 ..... 2
6 安全功能要求 ..... 2
6.1 通用安全功能要求 ..... 2
6.2 接触式安全功能要求 ..... 4
6.3 非接触式安全功能要求 ..... 4
7 安全保障要求 ..... 5
7.1 开发 ..... 5
7.2 指导性文档 ..... 5
7.3 生命周期支持 ..... 6
7.4 测试 ..... 7
7.5 脆弱性评定 ..... 7
参考文献 ..... 8

# 前　言

本标准按照GB/T 1.1-2009给出的规则起草。

本标准由公安部网络安全保卫局提出。

本标准由公安部信息系统安全标准化技术委员会归口。

本标准起草单位：公安部计算机信息系统安全产品质量监督检验中心、公安部第三研究所。

本标准主要起草人：郭运尧、杨元原、陆臻、沈亮、顾健。

# 信息安全技术 双接口鉴别卡安全技术要求

## 1 范围

本标准规定了双接口鉴别卡的安全功能要求、安全保障要求。

本标准适用于双接口鉴别卡的设计、开发及测试。

## 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。

GB/T 18336.3－2015 信息技术 安全技术 信息技术安全评估准则 第3部分：安全保障要求

GB/T 25069－2010 信息安全技术 术语

## 3 术语和定义

GB/T 18336.3－2015和GB/T 25069－2010界定的以及下列术语和定义适用于本文件。

3.1

**双接口鉴别卡 dual-interface authentication card**

同时具有接触和非接触式两个接口的智能卡，并且此类卡带有至少一个非接触与接触式应用。

3.2

**应用软件 application software**

架构基于芯片操作系统之上，实现智能卡的应用功能的软件。

3.3

**持卡者 cardholder**

按照既定目的使用接触式应用的最终用户。

3.4

**发行者 issuer**

承担产品的发行、产品的作废等职责的管理员用户。

## 4 缩略语

下列缩略语适用于本文件。

CAD：卡接收设备（Card Acceptor Device）

DIAC：双接口鉴别卡（Dual-Interface Authentication Card）

PIN：个人身份识别码（Personal Identification Number）

# 5 双接口鉴别卡描述

双接口鉴别卡是一个多应用双接口的智能卡，该卡同时具备接触式和非接触式两种接口，且两种接口可分别应用于不同的应用场景中，至少包含以下方面：

a) 非接触式应用实现的访问只能通过非接触式接口实现；
b) 接触式应用访问只能通过接触式接口实现，并要求持卡人输入 PIN 码，使卡与主机系统完成双向鉴别，从而完成对智能卡的验证。

# 6 安全功能要求

## 6.1 通用安全功能要求

### 6.1.1 应用接口限制

非接触式应用的所有数据只能通过非接接口与外部实体进行通讯；接触式应用的所有数据只能通过接触接口与外部实体进行通讯。

### 6.1.2 应用程序的隔离

任何应用程序的代码或数据，不得被其他应用程序访问和操作，除非该应用程序已被显式地授权访问相应的代码或数据。

### 6.1.3 身份鉴别

#### 6.1.3.1 鉴别失败处理

当失败的用户身份鉴别尝试次数达到规定的数值时，产品应能够终止鉴别会话过程。

#### 6.1.3.2 鉴别信息重用

产品应能防止与鉴别机制有关的鉴别信息被重复使用。

#### 6.1.3.3 重鉴别

产品应在下述条件下重新鉴别用户：

a) 智能卡会话终止；
b) 智能卡重置。

### 6.1.4 安全管理

#### 6.1.4.1 安全功能管理

产品应仅限于授权用户对以下安全功能进行管理：

a) 应用软件管理；
b) 智能卡生命周期管理；
c) 密钥管理；
d) PIN 码管理。

#### 6.1.4.2 安全属性的管理

产品应仅允许授权用户单向更新智能卡生命周期状态，修改应用软件生命周期状态、用户权限、PIN码状态等安全属性。

#### 6.1.4.3 静态属性初始化

产品应为安全属性提供一个受限的默认值，并仅允许授权用户修改这些默认值。

#### 6.1.4.4 安全角色

产品应能够维护持卡者、发行者和运行环境上下文等安全角色。

### 6.1.5 用户数据保护

#### 6.1.5.1 访问控制策略

产品应确保安全功能涉及的所有操作都被访问控制策略所涵盖，主体应能够按照预定义的访问控制策略访问客体。

#### 6.1.5.2 基于安全属性的访问控制

产品应基于主体和客体的安全属性，提供明确的访问保障能力和拒绝访问能力。

#### 6.1.5.3 数据保密性

产品安全功能应对用户数据执行保密性处理。

#### 6.1.5.4 数据完整性

产品安全功能应对用户数据执行完整性校验。

### 6.1.6 自保护能力

#### 6.1.6.1 安全功能检测

产品应在初始化时，运行一套自检程序以证明产品运行的正确性。

#### 6.1.6.2 失效保护

产品应在下列失效情况发生时，能够自动恢复到一个安全状态：

a) 鉴别数据完整性的破坏；
b) 缓冲区溢出；
c) 资源不可用；
d) 违反产品安全策略的行为；
e) 智能卡从 CAD 中意外拔出；
f) 异常环境条件（频率、电压、温度）；
g) 安全功能检测故障。

#### 6.1.6.3 旁路攻击抵抗

产品应能够抵抗攻击者通过指令耗时、功率消耗和电磁辐射等方式发起的旁路攻击。

#### 6.1.6.4 扰动攻击抵抗

产品应能够抵抗攻击者通过激光、时钟毛刺和电压毛刺等方式发起的扰动攻击。

#### 6.1.6.5 物理攻击抵抗

产品应能够抵抗攻击者通过逆向分析、物理篡改、物理探针等方式发起的物理攻击。

### 6.1.7 密码支持

#### 6.1.7.1 密钥生成

产品的密钥生成应符合国家密码管理的有关规定。

#### 6.1.7.2 密钥销毁

对于不再使用的密钥，产品应提供密钥销毁功能。

#### 6.1.7.3 密码算法

产品执行的加密、解密、签名、验签等密码算法应符合国家密码管理的有关规定。

## 6.2 接触式安全功能要求

### 6.2.1 持卡者鉴别

#### 6.2.1.1 鉴别时机

在访问产品受保护资源前应进行身份鉴别，应允许用户执行下述动作：

a) 建立逻辑通道；
b) 选择智能卡中的接触式应用软件；
c) 建立安全通道。

#### 6.2.1.2 鉴别机制

应采用基于PIN码的持卡者身份鉴别，持卡者PIN码鉴别成功后，才允许执行其他授权操作。

### 6.2.2 身份验证的时效性和真实性

产品应能验证身份验证时的验证过程的时效性和真实性，应具备以下能力：

a) 检测 PIN 验证过程的时效性和真实性的能力；
b) 验证授权消息时效性和真实性，且能核实证据的能力。

## 6.3 非接触式安全功能要求

### 6.3.1 鉴别时机

在访问产品受保护资源前应进行身份鉴别，应允许用户执行下述动作：

a) 建立逻辑通道；
b) 选择智能卡中的非接触式应用软件；
c) 建立安全通道。

### 6.3.2 身份鉴别

产品应能采取授权协议机制完成身份鉴别。

# 7 安全保障要求

## 7.1 开发

### 7.1.1 安全架构

开发者应提供产品安全功能的安全架构描述，安全架构描述应满足以下要求：

a) 与产品设计文档中对安全功能实施抽象描述的级别一致；
b) 描述与安全功能要求一致的产品安全功能的安全域；
c) 描述产品安全功能初始化过程为何是安全的；
d) 证实产品安全功能能够防止被破坏；
e) 证实产品安全功能能够防止安全特性被旁路。

### 7.1.2 功能规范

开发者应提供完备的功能规范说明，功能规范说明应满足以下要求：

a) 完全描述产品的安全功能；
b) 描述所有安全功能接口的目的与使用方法；
c) 标识和描述每个安全功能接口相关的所有参数；
d) 描述安全功能接口相关的安全功能实施行为；
e) 描述由安全功能实施行为处理而引起的直接错误消息；
f) 证实安全功能要求到安全功能接口的追溯；
g) 描述安全功能实施过程中，与安全功能接口相关的所有行为；
h) 描述可能由安全功能接口的调用而引起的所有直接错误消息。

### 7.1.3 实现表示

开发者应提供全部安全功能的实现表示，实现表示应满足以下要求：

a) 提供产品设计描述与实现表示实例之间的映射，并证明其一致性；
b) 按详细级别定义产品安全功能，详细程度达到无须进一步设计就能生成安全功能的程度；
c) 以开发人员使用的形式提供。

### 7.1.4 产品设计

开发者应提供产品设计文档，产品设计文档应满足以下要求：

a) 根据子系统描述产品结构；
b) 标识和描述产品安全功能的所有子系统；
c) 描述安全功能所有子系统间的相互作用；
d) 提供的映射关系能够证实设计中描述的所有行为能够映射到调用它的安全功能接口；
e) 根据模块描述安全功能；
f) 提供安全功能子系统到模块间的映射关系；
g) 描述所有安全功能实现模块，包括其目的及与其他模块间的相互作用；
h) 描述所有实现模块的安全功能要求相关接口、其他接口的返回值、与其他模块间的相互作用及调用的接口；
i) 描述所有安全功能的支撑或相关模块，包括其目的及与其他模块间的相互作用。

## 7.2 指导性文档

#### 7.2.1 操作用户指南

开发者应提供明确和合理的操作用户指南，操作用户指南与为评估而提供的其他所有文档保持一致，对每一种用户角色的描述应满足以下要求：

a) 描述在安全处理环境中被控制的用户可访问的功能和特权，包含适当的警示信息；
b) 描述如何以安全的方式使用产品提供的可用接口；
c) 描述可用功能和接口，尤其是受用户控制的所有安全参数，适当时指明安全值；
d) 明确说明与需要执行的用户可访问功能有关的每一种安全相关事件，包括改变安全功能所控制实体的安全特性；
e) 标识产品运行的所有可能状态（包括操作导致的失败或者操作性错误），以及它们与维持安全运行之间的因果关系和联系；
f) 充分实现安全目的所执行的安全策略。

#### 7.2.2 准备程序

开发者应提供产品及其准备程序，准备程序描述应满足以下要求：

a) 描述与开发者交付程序相一致的安全接收所交付产品必需的所有步骤；
b) 描述安全安装产品及其运行环境必需的所有步骤。

### 7.3 生命周期支持

#### 7.3.1 配置管理能力

开发者的配置管理能力应满足以下要求：

a) 为产品的不同版本提供唯一的标识；
b) 使用配置管理系统对组成产品的所有配置项进行维护，并唯一标识配置项；
c) 提供配置管理文档，配置管理文档描述用于唯一标识配置项的方法；
d) 配置管理系统提供一种自动方式来支持产品的生成，通过该方式确保只能对产品的实现表示进行已授权的改变；
e) 配置管理文档包括一个配置管理计划，配置管理计划描述如何使用配置管理系统开发产品。实施的配置管理与配置管理计划相一致；
f) 配置管理计划描述用来接受修改过的或新建的作为产品组成部分的配置项的程序。

#### 7.3.2 配置管理范围

开发者应提供产品配置项列表，并说明配置项的开发者。配置项列表应包含以下内容：

a) 产品、安全保障要求的评估证据和产品的组成部分；
b) 实现表示、安全缺陷报告及其解决状态。

#### 7.3.3 交付程序

开发者应使用一定的交付程序交付产品，并将交付过程文档化。在给用户方交付产品的各版本时，交付文档应描述为维护安全所必需的所有程序。

#### 7.3.4 开发安全

开发者应提供开发安全文档。开发安全文档应描述在产品的开发环境中，为保护产品设计和实现的保密性和完整性所必需的所有物理的、程序的、人员的和其他方面的安全措施。

#### 7.3.5 生命周期定义

开发者应建立一个生命周期模型对产品的开发和维护进行的必要控制，并提供生命周期定义文档描述用于开发和维护产品的模型。

#### 7.3.6 工具和技术

开发者应明确定义用于开发产品的工具，并提供开发工具文档无歧义地定义实现中每个语句的含义和所有依赖于实现的选项的含义。

### 7.4 测试

#### 7.4.1 测试覆盖

开发者应提供测试覆盖文档，测试覆盖描述应满足以下要求：

a) 表明测试文档中所标识的测试与功能规范中所描述的产品的安全功能间的对应性；
b) 表明上述对应性是完备的，并证实功能规范中的所有安全功能接口都进行了测试。

#### 7.4.2 测试深度

开发者应提供测试深度的分析。测试深度分析描述应满足以下要求：

a) 证实测试文档中的测试与产品设计中的安全功能子系统和实现模块之间的一致性；
b) 证实产品设计中的所有安全功能子系统、实现模块都已经进行过测试。

#### 7.4.3 功能测试

开发者应测试产品安全功能，将结果文档化并提供测试文档。测试文档应包括以下内容：

a) 测试计划，标识要执行的测试，并描述执行每个测试的方案，这些方案包括对于其他测试结果的任何顺序依赖性；
b) 预期的测试结果，表明测试成功后的预期输出；
c) 实际测试结果和预期的一致性。

#### 7.4.4 独立测试

开发者应提供一组与其自测安全功能时使用的同等资源，以用于安全功能的抽样测试。

### 7.5 脆弱性评定

基于已标识的潜在脆弱性，产品能够抵抗具有增强型基本攻击潜力的攻击者的攻击。

# 参 考 文 献

[1] Machine Readable Traval Document Platform Protection Profile, Version 1.00, HMGovernment, UK, 2009. UNKT-DO-0002

[2] GB/T 20276-2016 信息安全技术 具有中央处理器的IC卡嵌入式软件安全技术要求

[3] GB/T 22186-2016 信息安全技术 具有中央处理器的IC卡芯片安全技术要求