



# 中华人民共和国国家标准

GB/T 30266—2013/ISO/IEC 24787:2010

---

## 信息技术 识别卡 卡内生物特征比对

Information technology—Identification cards—On-card biometric comparison

(ISO/IEC 24787:2010, IDT)

2013-12-31 发布

2014-07-15 实施

中华人民共和国国家质量监督检验检疫总局 发布  
中国国家标准化管理委员会



目 次

前言 ..... III

引言 ..... IV

1 范围 ..... 1

2 符合性 ..... 1

3 规范性引用文件 ..... 1

4 术语和定义 ..... 2

5 缩略语 ..... 3

6 使用 ICC 的生物特征匹配体系结构 ..... 4

7 卡内比对应用的总体框架 ..... 6

8 协同工作..... 14

附录 A（规范性附录） 文件控制参数的一般 TLV 结构 ..... 16

附录 B（规范性附录） 卡内生物特征比对的安全策略 ..... 17

附录 C（资料性附录） 用于卡内比对的 APDU 示例 ..... 19

附录 D（资料性附录） 生物特征比对的软件共享接口 ..... 22

附录 E（资料性附录） 关于卡内比对安全机制的建议 ..... 24

附录 F（资料性附录） 协同工作的卡内比对体系结构 ..... 26

附录 G（资料性附录） 卡内生物特征比对机制实现示例 ..... 29

附录 H（资料性附录） 当需要时卡执行 WSR 会话的状态图 ..... 32





## 前 言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准使用翻译法等同采用 ISO/IEC 24787:2010《信息技术 识别卡 卡内生物特征比对》。

本标准做了下列编辑性修改：

- 删除国际标准前言，增加国家标准前言；
- 根据中文使用习惯，删除了国际标准的 4.2；
- 国际标准的 7.1.4.1.1 存在编辑性错误，7.1.4.1.1 修改为 7.1.4.2，相应地，国际标准的 7.1.4.2、7.1.4.3、7.1.4.4、7.1.4.5 分别修改为 7.1.4.3、7.1.4.4、7.1.4.5、7.1.4.6；
- 删除了国际标准的参考文献。

与本标准中规范性引用的国际文件有一致性对应关系的我国文件如下：

- GB/T 26237.1—2010 信息技术 生物特征识别数据交换格式 第 1 部分：框架(ISO/IEC 19794-1:2006,MOD)
- GB/T 26237.2—2011 信息技术 生物特征识别数据交换格式 第 2 部分：指纹细节点数据(ISO/IEC 19794-2:2005,NEQ)
- GB/T 26237.3—2011 信息技术 生物特征识别数据交换格式 第 3 部分：指纹型谱数据(ISO/IEC 19794-3:2006,MOD)

本标准由全国信息技术标准化技术委员会(SAC/TC 28)提出并归口。

本标准起草单位：中国电子技术标准化研究院、北京握奇智能科技有限公司。

本标准主要起草人：金倩、冯敬、高林、龙德帆、霍红文、乔申杰。

## 引 言

卡内生物特征比对,在 ISO/IEC 7816-11:2004《识别卡 集成电路卡 第 11 部分:通过生物方法的身份验证》中也称卡内匹配,是一种结合了集成电路卡(ICC)技术和生物技术的增强保密性的解决方案。生物特征比对过程在 ICC 内执行的情况下,它可以提供一个更安全的生物特征鉴别。与卡外比对(卡外匹配)相比,卡内比对不需要将 ICC 内的生物特征参考数据发送到接口设备上。因此,即使 ICC 丢失或被盗,存储在 ICC 内的生物特征参考数据也无法被复制,因而仍能保持其秘密性。

ISO/IEC 7816-11 和 ISO/IEC 19785-3《信息技术 公用生物特征识别交换格式框架(CBEFF) 第 3 部分:实体格式规范》覆盖了卡外比对和简单的卡内比对技术。使用在“真实”世界中获得的生物特征样本的最健全的生物比对过程需要很高的计算强度。相比之下,由于芯片低功耗、小尺寸的需求以及低成本卡的需求等阻碍了它们更快速的进步,使得 ICC 上能获得的 CPU 能力和其他资源的成长性会比较慢。将生物传感器嵌入到 ICC 上仍然是目前的技术挑战。

由于这些情况,工业界需要一个不包括卡外比对、系统和卡之间比对的新的标准用于卡内比对。本标准对以下内容进行了规定并提供了建议:

- 卡内比对过程的体系结构描述;
- 卡内比对过程协同工作的体系结构描述,协同工作可以通过预处理计算来减轻 ICC 的工作负载;
- 卡内比对阈值和其他安全管理问题的管理。

本文件的发布机构提请注意,声明符合本文件时,可能涉及到第 8 章与协同工作相关的专利的使用。

本文件的发布机构对于该专利的真实性、有效性和范围无任何立场。

该专利持有人已向 ISO 和 IEC 保证,他愿意同任何申请人在合理且无歧视的条款和条件下,就专利授权许可进行谈判。该专利持有人的声明已在 ISO 和 IEC 备案。相关信息可以通过以下联系方式获得:

Exploit Technologies Pte Ltd.,  
30 Biopolis Street,  
# 09-02 Matrix,  
Singapore 138671

请注意除上述专利外,本文件的某些内容仍可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

# 信息技术 识别卡 卡内生物特征比对

## 1 范围

本标准建立了

- 在集成电路卡(ICC)内实施生物特征样本比对和返回决策的需求;
- 卡内生物特征比对的安全策略。

本标准还建立了允许卡外预比对计算的命令和规则。

本标准未建立

- 卡外比对实现的需求;
- 卡内系统实现的需求;
- 存储和比对的指定形式需求。

## 2 符合性

一个卡内比对系统宣称符合本标准的前提是它应符合 7.1.2~7.1.5、7.2.1~7.2.8、8.1、8.2.2~8.2.3 的规定。

一张符合本标准的卡应:

- 采用以下两个数据集进行个人化:
  - 生物特征参考对象处理数据,如 7.1.2 所描述;
  - 用于生物特征验证的配置数据,如 7.1.3 所描述;
- 支持带多应用功能的 ICC 的共享接口,如 7.1.4 所描述;
- 支持重试计数器管理,如 7.1.5 所描述;
- 符合 7.2.1 和 7.2.8 中所规定的卡内比对实现的要求;
- 符合 8.1、8.2.2 和 8.2.3 中所规定的协同工作实现的要求。

生物特征鉴别可能会与其他鉴别机制,如 PIN 等共存。这种共存的规则应遵守的 GB/T 16649.4—2010。

生物特征数据应使用 GB/T 16649.4 中规定的文件结构或数据对象的形式来组织和管理:

- a) 如果生物特征数据以文件结构的形式来组织,则系统还应完全符合 ISO/IEC 7816-11 的规定;
- b) 如果生物特征数据以数据对象的形式来组织和管理,则卡应符合 GB/T 16649.4 中对数据对象处理的规定。

生物特征数据对象的编码应符合 ISO/IEC 7816-11 和 ISO/IEC 19785-3。

## 3 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 16649.4—2010 识别卡 集成电路卡 第 4 部分:用于交换的结构、安全和命令(ISO/IEC 7816-4:2005,IDT)

ISO/IEC 7816-11:2004 识别卡 集成电路卡 第 11 部分:通过生物方法的身份验证(Identifica-

tion cards — Integrated circuit cards — Part 11: Personal verification through biometric methods)

ISO/IEC 19785-1 信息技术 公用生物特征识别交换格式框架(CBEFF) 第1部分:数据元素规范(Information technology — Common Biometric Exchange Formats Framework — Part 1: Data element specification)

ISO/IEC 19785-3:2007 信息技术 公用生物特征识别交换格式框架(CBEFF) 第3部分:实体格式规范(Information technology — Common Biometric Exchange Formats Framework — Part 3: Patron format specifications)

ISO/IEC 19794 (所有部分) 信息技术 生物特征识别数据交换格式[Information technology — Biometric data interchange formats(all parts)]

ISO/IEC 29794-1:2009 信息技术 生物特征样本质量 第1部分:框架(Information technology — Biometric sample quality — Part 1: Framework)

## 4 术语和定义

下列术语和定义适用于本文件。

### 4.1

**辅助数据 auxiliary data**

依赖于生物特征形态,而且与生物特征参考有关,但不包含生物特征参考或生物特征样本的数据。  
示例:方向、尺度等数据。

### 4.2

**生物特征识别 biometrics**

基于行为特性和生物特性的个体自动识别。

[SC37 SD2 协调生物识别词汇]

### 4.3

**生物特征声称 biometric claim**

关于生物特征采集主体是或不是指定的或非指定的生物特征参考来源的声称。

[SC37 SD2 协调生物识别词汇]

### 4.4

**生物特征数据 biometric data**

处于任何处理阶段的生物特征样本或生物特征样本的聚集、生物特征参考、生物特征项或生物特征特性。

[SC37 SD2 协调生物识别词汇]

### 4.5

**生物特征数据格式 biometric data format**

表示生物特征数据的结构。

### 4.6

**生物特征信息模板 biometric information template**

关于相关生物特征数据的描述信息。

[ISO/IEC 7816-11:2004]

### 4.7

**生物特征产品标识符 biometric product identifier**

在 ISO/IEC 19785-1 注册机构注册的惟一标识符。

## 4.8

**生物特征特性 biometric property**

自动从生物特征样本中估计的或获得的生物特征数据主体的描述性属性。

[SC37 SD2 协调生物识别词汇]

## 4.9

**生物特征参考 biometric reference**

用于比对的、属于生物特征数据主体的一个或多个已存储的生物特征样本、生物特征模板或生物特征识别模型。

[SC37 SD2 协调生物识别词汇]

## 4.10

**生物特征验证系统 biometric verification system**

实施生物特征声称确认过程的系统。

[SC37 SD2 协调生物识别词汇]

## 4.11

**安装 installation**

当应用被上载到 ICC 后,执行安装规程的卡操作系统将需要的参数写入到 ICC 内的非易失存储器上。

## 4.12

**卡内比对 on-card comparison**

在 ICC 上执行比对和做出决策,在这种情况下,生物特征参考数据被保存在卡内以增强安全性和隐私性。

## 4.13

**卡外比对 off-card comparison**

在卡外通过生物特征验证系统对照存储在卡内的生物特征参考数据执行的生物特征比对。

## 4.14

**预比对计算 pre-comparison computation**

为加快随后的卡内生物特征数据比对过程而在 ICC 外执行的计算规程,该规程需要(开放的)卡内辅助数据来计算可供使用的元数据。

## 4.15

**协同工作 work-sharing**

将比对过程的计算工作分配在卡和生物特征接口设备之间。

注:协同工作卡内比对是卡内比对的一种类型。

## 4.16

**卡内系统 system-on-card**

生物特征验证系统(包括数据获取、处理和比对)完全位于卡内。

注:卡内系统比对是卡内比对的一种类型。

## 4.17

**归零数据 zeroize data**

已被消磁、擦除或覆写的电子化存储数据。

[ANSI X9.17]

## 5 缩略语

下列缩略语适用于本文件。

AID:应用标识符(application identifier)  
ADF:应用专用文件(application dedicated file)  
APDU:应用协议数据单元(application protocol data unit)  
AUT:鉴别(authenticate)  
BER:基本编码规则(basic encoding rules)  
BIT:生物特征信息模板(biometric information template)  
CRT:控制引用模板(control reference template)  
CPU:中央处理单元(central processing unit)  
DF:专用文件(dedicated file)  
DF.CIA:专用文件,密码信息应用(dedicated file, cryptographic information application)  
EF:基本文件(elementary file)  
FCI:文件控制信息(file control information)  
FCP:文件控制参数(file control parameter)  
FMR:错误匹配率(false match rate)  
ICC:集成电路卡(integrated circuit card)  
MAC:消息鉴别码(message authentication code)  
MSE:管理安全环境(manage security environment)  
RFU:保留供将来使用(reserved for future use)  
SW1-SW2:状态字节(status bytes)  
TLV:标记-长度-值(tag-length-value)  
WSCP:协同工作计算协议(work-sharing computation protocol)  
WSR:协同工作请求(work-sharing request)

## 6 使用 ICC 的生物特征匹配体系结构

### 6.1 概述

以下各条详细说明了进行生物特征匹配时,与 ISO/IEC 7816 兼容的卡与其生物特征验证系统之间功能分配的 4 种方式。仅 6.3 和 6.4 在本标准规定范围之内。

执行注册,即从采集用户的生物特征样本用于创建生物特征参考到上传用户信息到卡。这不适用于 6.5 中规定的卡内系统比对。

### 6.2 卡外比对

卡外比对是指在生物特征验证系统端执行生物特征验证。卡作为用户生物特征参考的存储设备。图 1 提供了此过程步骤的示意图。

为执行验证,生物特征验证系统将获取 ICC 的访问权限并读取用户的生物特征参考。生物特征验证系统的任务是采集生物特征样本并执行生物特征验证。如果生物特征验证成功,则生物特征验证系统将改变其安全状态,并可以从卡内下载进一步的信息以进行后续的交互。如果验证失败,进一步的访问将被拒绝。

通常使用密码算法在卡和生物特征验证系统之间做互鉴别。为了保护卡和生物特征验证系统之间的通信,在传输任何模板或数据之前应建立安全通道。

示例: 对于一个物理访问系统(如门禁系统),生物特征参考和访问码存储在 ICC 中。生物特征验证系统从卡上读取生物特征参考,并执行生物特征验证。如果验证成功,则生物特征验证系统从卡上读取访问码并将其发送到后台系统,从而将访问通道打开。

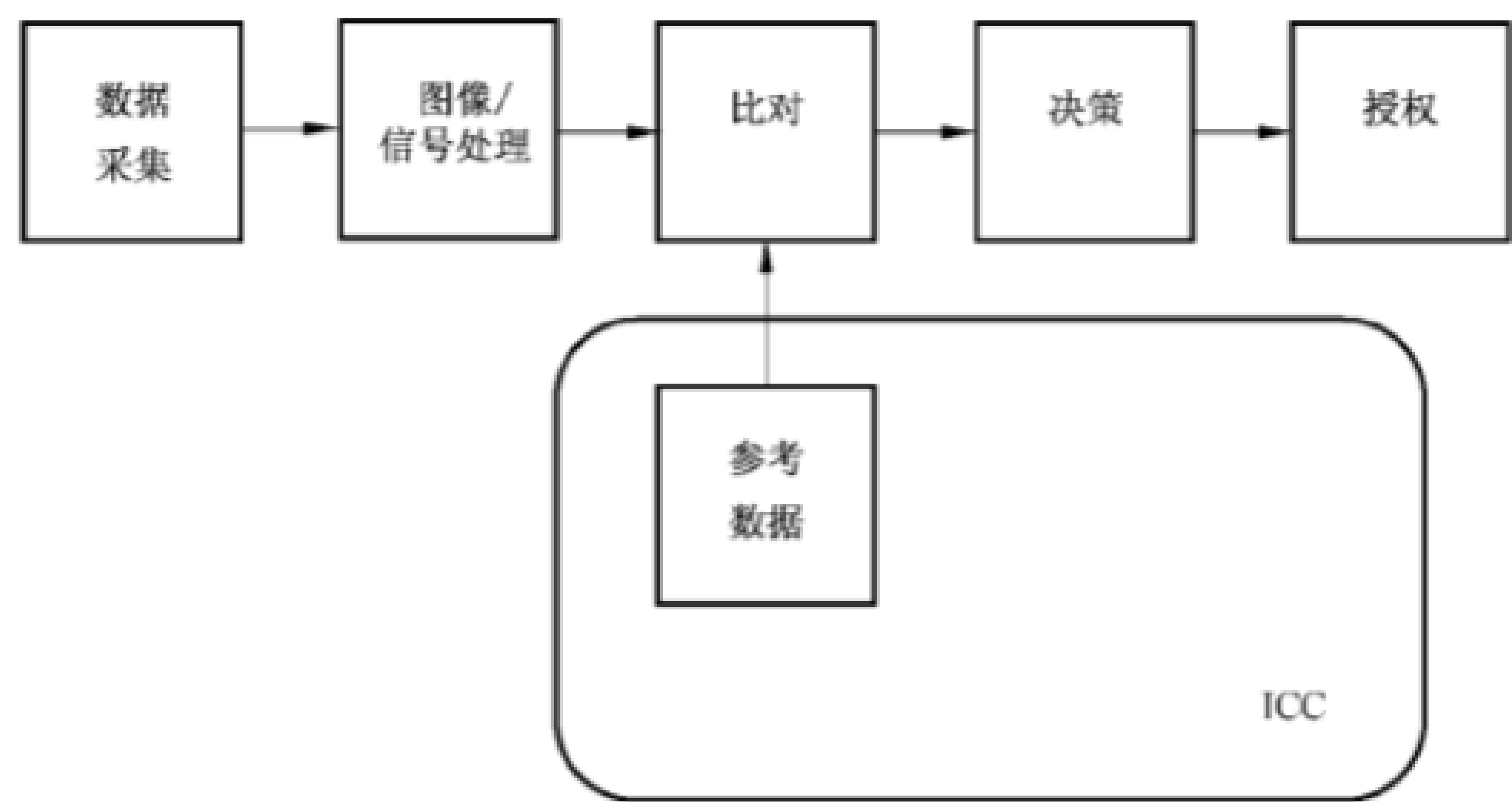


图 1 采用卡外匹配方式的生物特征鉴别通用体系结构

6.3 卡内比对(卡内无传感器)

卡内比对是指在卡内执行生物特征样本的验证。图 2 给出了此过程的示意图。ICC 的 CPU 应有足够的处理能力来执行匹配过程。注册过程与卡外比对相同或相似。

为执行卡内比对,生物特征验证系统采集生物特征样本并提取生物特征数据。所生成的生物特征数据被上载到卡内以供验证。验证过程在卡内执行。如果验证成功,则卡的安全状态被更新,并发送相应的信号到后台系统。

为了保护卡和生物特征验证系统之间的通信,建议采用一个安全、可信的通道(采用符合 ISO/IEC 7816 的安全报文传输、ISO/IEC 24761 定义的用于分布式比对验证的机制)。

示例:对于一张卡,它能使用一个永不脱离卡的密钥来生成数字签名。当一个请求发送到卡要求初始化生成数字签名时,卡端返回的响应报文为安全状态错误。这表明需要验证用户身份。用户将所需的生物特征样本呈现给生物特征验证系统以生成生物特征数据,之后将其传输给 ICC。ICC 将此新采集的生物特征数据与卡内存储的生物特征参考比对,如果比对成功,则 ICC 更新安全状态,该安全状态允许 ICC 在接收到相应的 APDU 报文后生成数字签名。

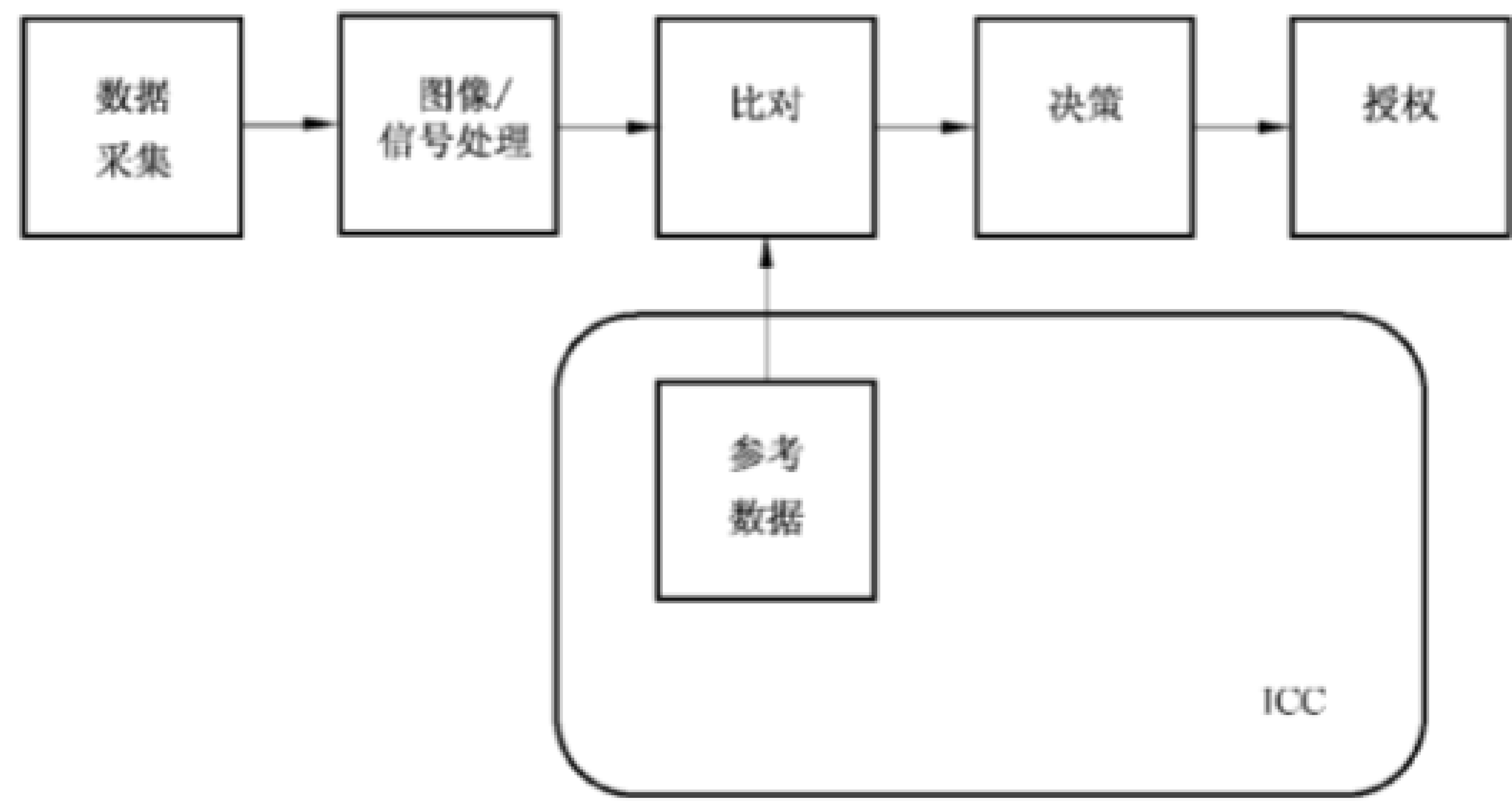


图 2 采用卡内匹配方式的生物特征鉴别通用体系结构

6.4 协同工作卡内比对

除比对规程不同外,协同工作卡内比对与卡内比对其他的过程相同。图 3 给出了此过程的示意图。当 ICC 不具备足够的处理能力执行生物特征数据比对时,可采用此类比对。某些需要大计算量的过程,例如一个数学变换,可以发送给生物特征验证系统执行该计算。计算的结果发送回 ICC 供卡内计算匹配程度和最终决策。在预比对计算过程中,卡和生物特征验证系统之间存在通信。安全、可信的通

道用于保护这种卡和终端之间的通信,除非在特定的操作环境中,明显地不需要此保护。附录 D 详细描述了协同工作的体系结构。

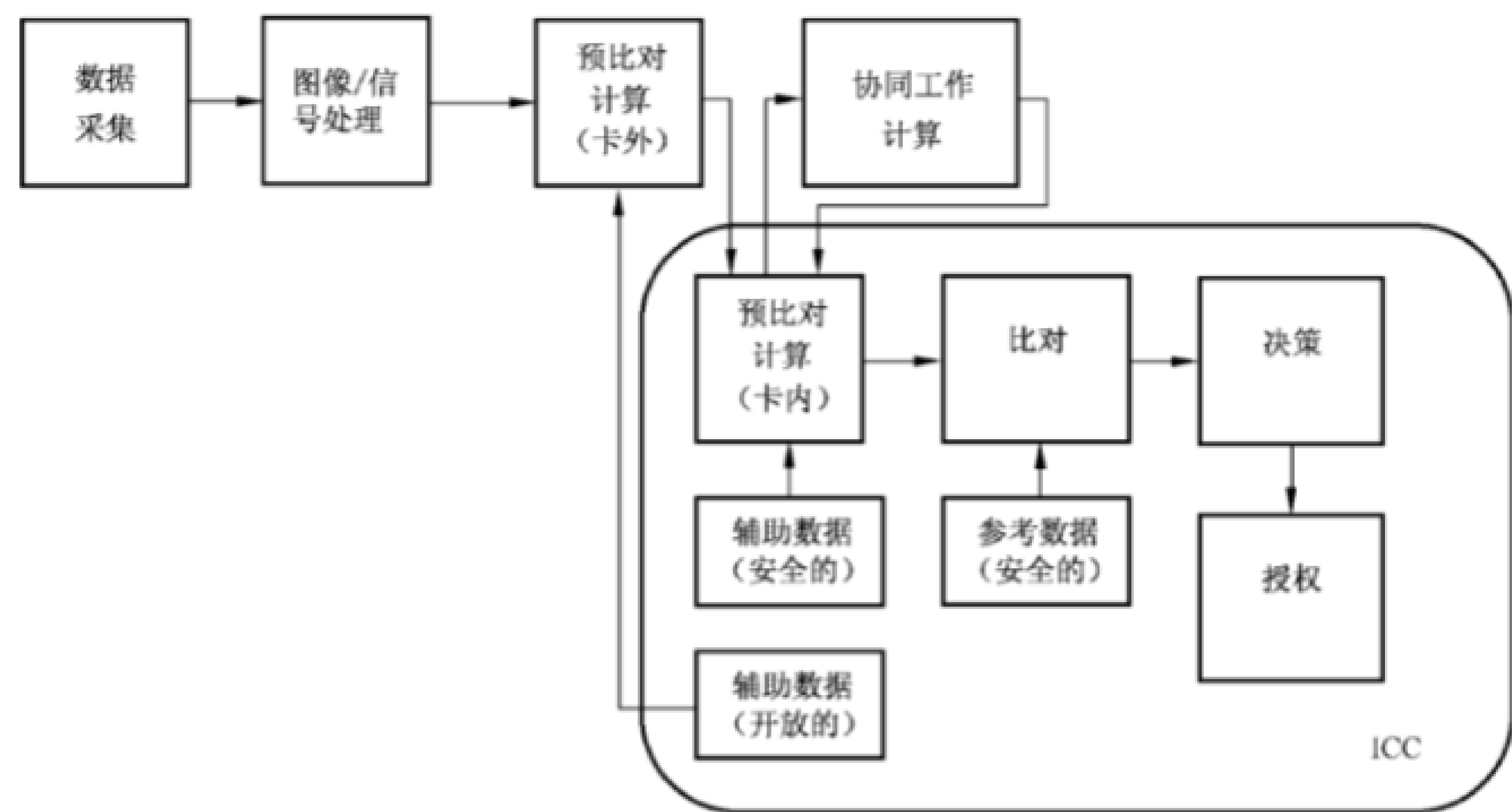


图 3 采用协同工作方式的生物特征鉴别通用体系结构

注：协同工作卡内比对应仅在：用到生物特征模式时，对于一个给定的应用，卡内比对过程的表现考虑所需的交易时间时不够优的情况下考虑。

6.5 卡内系统比对

卡内系统比对是指在卡内执行整个生物特征样本验证过程。图 4 给出了此过程的示意图。为执行卡内系统比对，卡内置的传感器采集生物特征样本并提取生物特征数据，生成的生物特征数据用于验证。验证过程在卡内执行。一旦卡完成验证，则卡的安全状态被更新。没有生物特征样本或生物特征参考数据被传递给卡或从卡内传出。

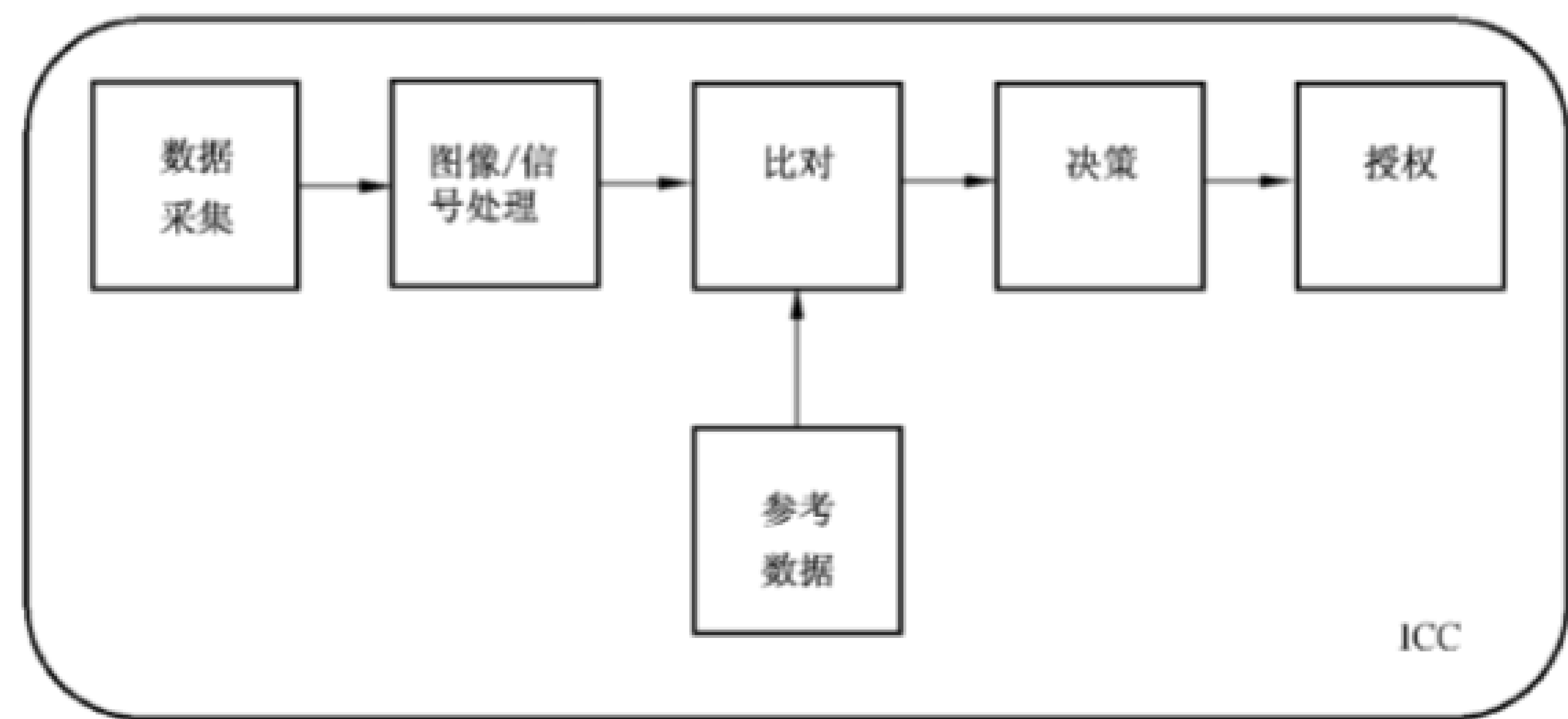


图 4 采用卡内系统匹配方式的生物特征鉴别通用体系结构

7 卡内比对应用的总体框架

7.1 用于卡内比对的数据

7.1.1 概述

7.1.2~7.1.5 规定了下列特性：



- 生物特征参考对象处理；
- 用于生物特征验证的配置数据；
- 支持多应用的共享接口；
- 重试计数器管理。

7.1.2 生物特征参考对象处理

考虑到生物特征参考互操作性的需求，卡内比对应使用 ISO/IEC 19794 相关部分定义的生物特征数据格式。附录 C 提供了一个示例。

除非在一些特别的操作环境中，明显不需要生物特征参考互操作性的情况下，可以不使用 ISO/IEC 19794 相关部分定义的生物特征数据格式。

注：推荐使用 ISO/IEC 19794 相关部分描述的压缩卡格式。

7.1.3 用于生物特征验证的配置数据

7.1.3.1 用于配置数据的数据对象

用于生物特征验证的配置数据由表 1 中描述的数据对象集组成。配置数据的获取应服从与存储此信息的逻辑数据结构相关的访问规则。如果配置数据可用，则它应存储在 BIT(见 ISO/IEC 7816-11)中。当在 BIT 的‘B1’(见 ISO/IEC 7816-11:2004)中存在时，配置数据应被编码，编码如表 1 所示。

表 1 用于配置数据元的数据对象

标记	长度	有效值	描述
‘80’	‘01’~‘03’		生物特征验证数据的最大长度
‘81’	‘01’~‘03’		生物特征参考数据的最大长度
‘82’	1	‘00’-‘FF’	支持的生物特征模板的数量(‘00’-无信息)
‘83’	1	‘00’:无法重注册 ‘01’:可以重注册 其他值:RFU	指示标志重注册的可能性
‘85’	变长	如 ISO/IEC 29794-1 中所定义	如 ISO/IEC 19794 和 ISO/IEC 29794 系列标准相关部分定义的支持的验证数据质量的最小值
‘86’	1		重试计数器的初始值,指示支持的允许验证尝试次数的最大值
‘87’	变长		执行比较的内部质量限制
‘8F’	变长		专用数据
‘90’	变长	见表 3	生物特征鉴别类型,如果适用,还包括卡的性能
‘A4’	2	ISO/IEC 19785-2 中描述的注册管理机构的规定	保留供将来使用,由 SC37 规定的算法 ID

注：其他配置参数的编码，如：

- 执行生物特征验证所需的安全状态；
  - 执行生物特征注册所需的安全状态；
  - 验证成功后所设置的安全状态
- 不在本标准规定的范围之内。

7.1.3.2 生物特征比对算法参数

在生物特征验证之前,应从卡上读到生物特征比对参数集。表 2 和表 3 定义了卡内比对时 BIT 中的生物特征比对算法参数(标记‘91’/‘B1’在 ISO/IEC 19785-3:2007 的表 11.1 中),其中原始参数以标记‘91’开头,构建参数以标记‘B1’开头,并包含总长度。

表 2 用于生物特征比对算法参数的数据对象

标记	长度	有效值	描述
‘81’	*	*	ISO/IEC 19794 系列标准相关部分定义的生物特征数据的最小长度和最大长度
‘82’	*	*	如果适用,则为 ISO/IEC 19794 系列标准相关部分定义的生物特征数据的特征排序
‘83’	*	*	ISO/IEC 19794 系列标准相关部分定义的生物特征数据的特征处理信息
‘84’	*	*	ISO/IEC 19794 系列标准相关部分定义的对齐信息
‘85’	* *	* *	支持的最小验证数据质量(见表 1)
‘90’	1	见表 3	鉴别类型和算法强度
‘91’	2	‘0001’-‘FFFF’	最大响应时间,以毫秒为单位 <sup>a</sup>
<sup>a</sup> 卡执行的耗时操作应支持基于 ISO/IEC 7816-3 的合适的等待时间扩展。			

注 1: “\*”表示此变量在 ISO/IEC 19794 相关部分定义。

注 2: “\* \*”表示此变量在 ISO/IEC 19794 和 ISO/IEC 29794 相关部分定义。

卡内比对可能要求满足访问规则,包括为完成比对过程需要安全通道以保护命令和响应 APDU 的传输。这些传递卡上生物特征相关数据的 APDU 数据字段应按照本标准规定来编码。用于保护 APDU 的访问规则和安全报文传输应符合 GB/T 16649.4。

表 3 鉴别类型和识别能力

b7	b6	b5	b4	b3	b2	b1	b0	含 义
						x	x	鉴别类型
						0	0	卡内比对
						0	1	协同工作卡内比对
						1	0	卡内系统
						1	1	RFU
			x	x	x			FMR <sup>a</sup> 已声明
			0	0	0			无指示信息
			0	0	1			FMR 级别 1(最大)
			0	1	0			FMR 级别 2
			0	1	1			FMR 级别 3
			1	0	0			FMR 级别 4
			1	0	1			FMR 级别 5

表 3 (续)

b7	b6	b5	b4	b3	b2	b1	b0	含 义
			1	1	0			FMR 级别 6(最小)
			1	1	1			RFU
x	x	x						RFU
* 提供此值,使系统设计者能够为带特定卡内比对产品的不同应用设置不同的比对水平。								

制造商应宣布其 FMR 的值,为他们规定的分级。表 4 是一个 FMR 分级尺度的示例。

表 4 FMR 分级示例

分级	示例
FMR 级别 1	$FMR < 0.1$
FMR 级别 2	$FMR < 0.01$
FMR 级别 3	$FMR < 0.001$
FMR 级别 4	$FMR < 0.000\ 1$
FMR 级别 5	$FMR < 0.000\ 01$
FMR 级别 6	$FMR < 0.000\ 001$

7.1.3.3 生物特征产品标识符

生物特征产品标识符应是在 1~65 535 之间的整数,并应在符合 ISO/IEC 19785-1 的注册管理机构注册。

7.1.4 多应用的共享接口

7.1.4.1 概述

在可互操作的卡内比对系统中,一个可能的需求是不同应用在不同的配置数据下,使用同一个生物特征参考,如一个指纹模板。这种需求的实现是使用 ISO/IEC 7816 和其他生物特征相关标准定义的用于独立应用之间共享信息的访问规则参考和数据元。

7.1.4.2 比对信息

一个生物特征卡内比对系统可能需要补充参数,例如:

- 生物特征参考的指针;
- 比对参数,如:
  - 模板格式;
  - 拟采用的算法;
  - 阈值参数。

比对的最大分值可以被确定,或者一旦分值超过了阈值,比对可以返回成功结果。

这些参数与附录 E 中定义的密钥编号之间有一对一的关系。因此,有可能将这些参数附加到密钥编号上。

#### 7.1.4.3 文件控制参数

根据 GB/T 16649.4, 卡内的每个应用专用文件(ADF)、专用文件(DF)或基本文件(EF)都应具有表 A.1~表 A.3 中包含的文件控制参数(FCP)。依赖于命令参数, FCP 应在成功的 SELECT APDU 之后被返回。FCP 应包含符合 7.1.4.4 所规定的访问规则引用。附录 A 中的表总结了用于 DF 或 EF 的 FCP 的通用 TLV 结构。

#### 7.1.4.4 访问规则

为了能以特定访问模式来访问卡上受保护的资源, 访问规则应决定应该满足的安全条件(SC)。“NEVER”访问规则应与生物特征参考的读操作相关联。对于兼容本标准的卡, 访问规则应根据 GB/T 16649.4 来编码, 将安全条件与受保护的卡逻辑数据结构的访问模式相关联。一旦这些安全条件被满足, 外部应用就获得了以相应访问模式来访问受保护数据结构的安全状态。

注: “NEVER”访问规则在 GB/T 16649.4—2010 中表 20 和表 23 中定义。

当根据这些标准在卡上编码访问规则时, 应使用如下规则:

- 访问规则可以与任何 ADF, DF, EF 或受保护的数据对象相关联;
- 对于卡内比对应用, 存储应用的 ADF 所关联的 FCP 可以将访问规则编码以执行卡内生物特征比对;
- 对于卡内其他应用, 访问规则可以包含对一个鉴别控制引用模板(CRT AUT)的引用来保存生物特征信息模板的数据对象, 如 ISO/IEC 7816-11 规定的‘7F 60’;
- 如果需要, 生物特征信息模板(BIT)的获取应使用安全报文传输模板来保护, 如 ISO/IEC 7816-11 所规定。

注: “访问规则”在 GB/T 16649.4 中定义。

#### 7.1.4.5 二次转接

二次转接是一个可选的功能, 只有当符合本标准的卡不支持任何 7.2.8 和附录 B 要求的高安全性应用时, 它可提供此功能。二次转接指的是这样一种能力, 能使用不同的配置设置对应的不同访问规则以进行卡内生物特征比对。

GB/T 16649.4 为访问规则的规定提供了不同的可能性, 可申请二次转接功能的互操作实现。因此, 访问规则编码(以 ISO/IEC 7816-4 规定的压缩格式或扩展格式)访问模式之间的关系, 为那些指向生物特征参考的命令和要求满足的安全条件。根据 GB/T 16649.4, 这些安全条件可以指带一个鉴别控制引用模板的应用安全环境。本机制使不同的应用来指定不同的访问规则, 生物特征验证操作具有相同的生物特征参考。

图 5 举例示出了共享配置和生物特征参考。

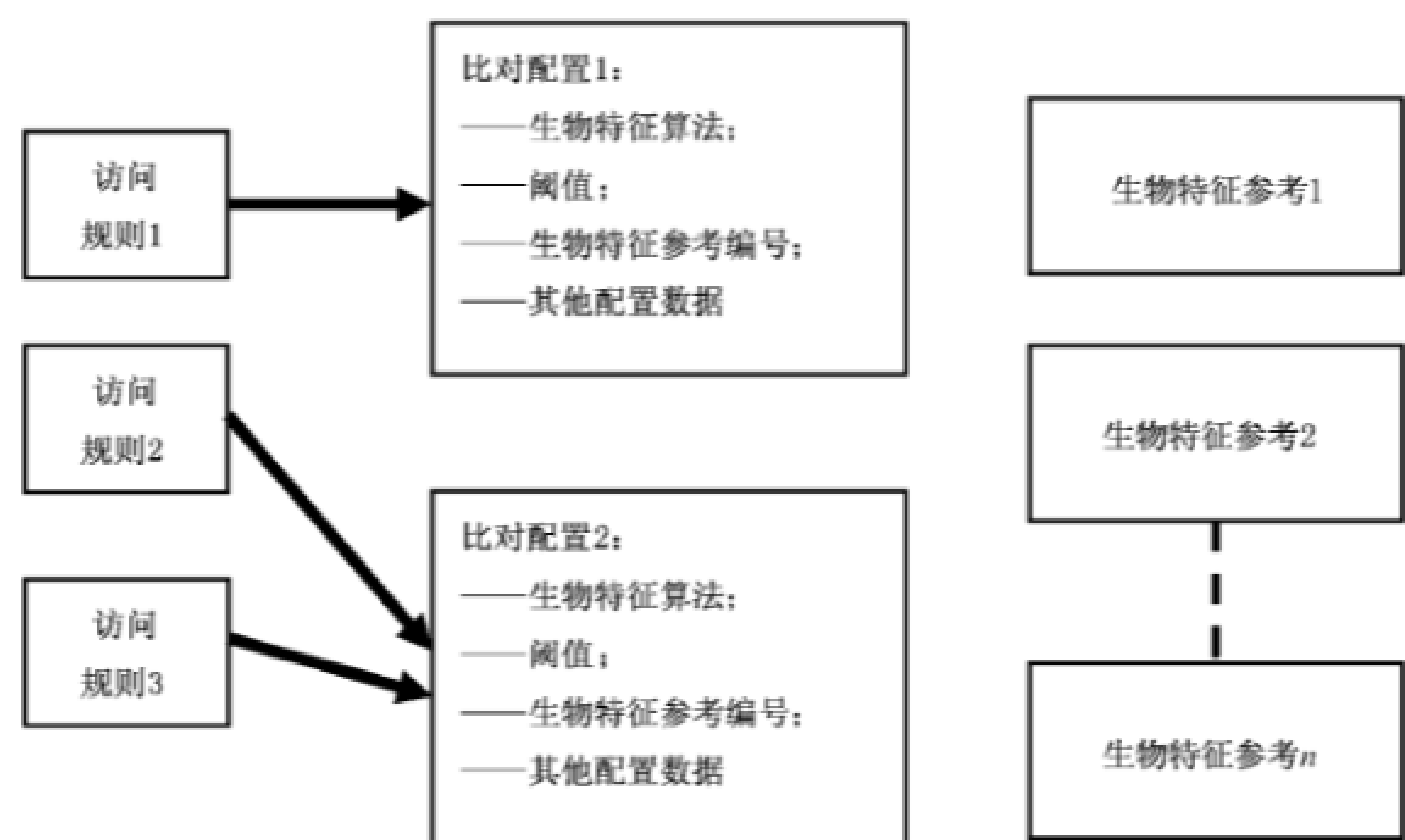


图 5 共享配置和生物特征参考示例

7.1.4.6 安全环境的使用

在 MSE SET 中使用的密钥编号决定：  
——引用模板；  
——安全级别。

在 GB/T 16649.4—2010 中，定义了生物特征鉴别的使用限定词（‘04’，见其表 35）。

在 ISO/IEC 7816-11:2004 中，执行生物特征比对的顺序在附录 B 中给出（见图 6，是 ISO/IEC 7816-11:2004 中图 B.6 的复制）。

命令/响应	含义
<div>SELECT&lt;File ID&gt; → OK ←</div>	FCI 扩展文件的选择
<div>READ BINARY → VIT    BIT ←</div>	获取验证需求信息模板 VIT 和生物特征信息模板 BIT
<div>MANAGE SE&lt;DO UQ    DO Alg.Reference    DO Key Reference&gt; → OK ←</div>	使用 Usage Qualifier UQ、算法引用和密钥引用来设置 CRT AT
<div>VERIFY&lt;生物特征鉴别数据&gt; → OK ←</div>	用户验证

图 6 不带安全报文传输的验证命令（示例）

然而，由于 ISO/IEC 7816-11 没有规定完整的注册过程，也就没有规定生物特征参考和比对参数的



内部存储方式。

在 GB/T 16649.4—2010 中表 33 定义了以下数据对象：

- ‘80’ 加密机制引用；
- 文件和密钥引用：
  - ‘81’—文件引用(GB/T 16649.4—2010 中 5.3.1.2 相同编码)；
  - ‘82’—DF 名称(见 GB/T 16649.4—2010 中 5.3.1.1)；
  - ‘83’—秘密密钥的引用(直接使用)；
    - 公钥的引用；
    - 参考数据的限定词；
  - ‘84’—计算会话密钥的引用；
    - 私钥的引用；
  - ‘A3’—密钥使用模板(见 GB/T 16649.4—2010)；
- 初始数据引用：未使用。

### 7.1.5 重试计数器管理

重试计数器管理定义了管理重试计数器机制的策略。这些策略是：

- a) 生物特征比对过程的持卡人应在重试计数器的控制之下,重试计数器决定针对某个给定的生物特征参考,验证过程是否可以继续使用。
- b) 重试计数器的初始值应与卡内生物特征参考相关联。
- c) 此关联可以使用 ISO/IEC 7816-15 分配给生物特征数据信息对象(BIO)的子类属性进行编码。
- d) 如果验证失败,重试计数器应减 1,并且应用应将包含剩余尝试次数的错误状态返回。
- e) 允许的重试次数应在状态字节 SW1-SW2=‘63 CX’(其中 X 为剩余次数)中编码,此状态字节是作为一个 VERIFY 命令的响应,并且根据 GB/T 16649.4 该响应的数据字段为空。
- f) 对生物特征参考成功的验证将重置其对应的重试计数器为初始值。

## 7.2 用于卡内比对的标准过程

### 7.2.1 用于卡内生物特征比对的应用标识符(AID)

卡应支持一个 AID。当卡内生物特征比对作为一个独立的应用实现时,它应根据 GB/T 16649.4 用一个 AID 来标识。卡内比对应用可以用 AID‘E8 28 81 C1 53 00’来选择。

注：AID 源于根据 GB/T 16649.4 和附录 A 的标准的对象标识符。

### 7.2.2 读取生物特征参考数据

在一个卡内生物特征比对应用中,不应为比对而赋予对生物特征参考的读取权限。与生物特征参考有关的辅助数据(开放的)可以根据应用的需要被读取。

### 7.2.3 注册

注册是创建并存储一个生物特征参考的过程。在卡内比对系统中,该过程包括：

- a) 向 ICC 传送一个或多个生物特征模板并将其存储在卡上；
- b) 传送并存储为执行生物特征比对所需的任何其他参数(例如,比对阈值、质量保证参数等)。

依赖于 ICC 的能力,信号处理可以被分离在生物特征接口设备和 ICC 之间。在所有情况下,所有的生物特征数据应通过安全和可信的通道或在可信的环境中传输到卡,以确保用户的隐私。建议在

注册之后直接执行一个验证测试以测试过程的质量。

ISO/IEC 7816-11 包含了生物特征数据注册到卡上的指导。

为了更新用户的生物特征数据,重注册可能发生。在此情况下,应应用注册规则。

#### 7.2.4 验证

验证是生物特征数据与生物特征参考的比对。在卡内比对系统中,比对应在 ICC 内执行。生物特征参考可以包含注册的多数性,例如,同一个人的多个指纹或者虹膜和人脸的不同的形态等。

生物特征比对需要应用文件结构中定义的访问条件。这些条件应优先通过应用文件结构中定义的互鉴别或外部鉴别来满足。用于验证的生物特征数据宜使用 GB/T 16649.4 规定的安全报文传输来传送到卡内。

应使用 VERIFY 命令(根据 GB/T 16649.4—2010)来初始化卡内比对过程。如果比对成功,则卡的安全状态可以根据安全条件相应设置。为了避免爬坡(hill-climb)攻击,应使用重试计数器,除非在特定操作环境下这种计数器测量的需求明显不要求。如果比对失败,重试计数器应递减,并可以在响应状态字中返回。如果重试计数器到达 0,则进一步的验证尝试应被阻塞。重试计数器可以通过使用 GB/T 16649.4—2010 所述的解阻塞方法来重置。

#### 7.2.5 卡内比对应用的终止

当终止一个卡内比对应用时,卡内包含的仅针对此应用的生物特征参考数据的逻辑数据结构应被置为不可访问的,如果可能,这些数据应被清零。

#### 7.2.6 比对过程和结果输出

##### 7.2.6.1 比对过程

整个比对过程应在卡内进行。

##### 7.2.6.2 比对结果

比对结果应是给出的生物特征数据比对分值与预定义的为达安全级别所确定的阈值之间的比对结果。如果比对分值高于预定义的阈值,则 VERIFY 响应 APDU 中的 SW1-SW2 应被置为‘90 00’。否则,SW1-SW2 应符合 ISO/IEC 7816 的错误代码。

#### 7.2.7 安全需求和生物特征参考管理

安全需求和生物特征参考的管理策略为:

- a) 生物特征参考的安全访问条件应不允许此数据被任何命令读出;
- b) 为了更新生物特征参考数据,应使用注册所适用的规则;
- c) 应只在预定义的安全状态下执行生物特征验证;
- d) 对每个存储的生物特征参考的引用可以有一个独立的重试计数器;并且
- e) 不同应用的重试计数器可以相互独立。这意味着如果一个重试计数器失效了,针对同一生物特征数据的其他应用的重试计数器也会保持不变。

#### 7.2.8 阈值管理

阈值管理定义了管理阈值参数和相关机制的策略。应遵守以下策略:

- a) 如果卡上有使用相同生物特征参考的卡内生物特征比对的多个应用,则这些应用应使用一个唯一的阈值和单个与该生物特征参考相关联的重试计数器。

注：本标准确认由于商业或实现的原因，可以存在对同一生物特征参考有不同阈值的需求。如果是这种情况，则可以应用附录 B 中给出的策略，特别是 SP2。

- b) 在第一次装载卡内生物特征鉴别应用期间，配置参数应为内部质量限制定义一个参数用于执行比对。
- c) 在应用的装载阶段期间，应定义用于二次转接的访问规则，尤其是对特定比对阈值中不同配置的上下文。
- d) 在验证期间，为了确定真实性，应考虑如 7.1.3.2 中描述的下列参数：
  - 1) 生物特征比对算法参数；和
  - 2) 鉴别类型和识别能力。
- e) 从配置数据宜得到积极的生物特征验证的结果可达到的安全水平。主机应在初始验证之前选择其应用所需的安全级别。
- f) 本条款所描述的阈值参数在卡内验证期间不应产生变化。

## 8 协同工作

### 8.1 运行时协同工作机制

在协同工作卡内比对体系结构中，比对应在 ICC 中执行。预比对计算可以在生物特征验证系统中完全或部分执行，这依赖于特定的 ICC 生物特征验证系统的设计。8.2.2~8.2.3 描述的 ENVELOPE 命令可以用来发现所支持的 WSR 协议是否可用。如 6.4 所述，生物特征数据的两部分被存于 ICC 中。保密部分，包含生物特征参考，不应被发送到生物特征验证系统。辅助数据（开放）部分，包含生物特征属性，可以使用 WSR 协议发送到卡外并被生物特征接口设备处理以加快处理时间。预比对计算和运行时协同工作都应使用此机制来实现。附录 F 中描述了一个协同工作体系结构的示例。图 F.2 表明了根据图 3 的协同工作的机制。对其他不同的协同工作体系结构，图 F.2 并不适用。GB/T 16649.4—2010 中 8.6“卡发起的字节串”所规定的 APDU 命令和响应，应被用来支持 WSR 协议。卡可以在单个 APDU 会话中发送多个 WSR 请求到本地生物特征验证系统。在开始 WSR 函数（功能）调用之前，相应的用于计算的数据应被传输到 APDU 缓冲区中。在图 7 中，每个箭头的括号中的数值指示了顺序。当一个 WSR 协议被发现（见 8.2.2）或被选择（见 8.2.3）时，如下序列总结了 WSR 协议：

- (1) 卡接收一个需要 WSR 的生物特征比对命令，并内部调用其 WSR 函数（功能）。
- (2) 卡操作系统把响应字节‘62 XX’返回给生物特征验证系统，以通知卡正确确认 WSR 请求的初始化，如步骤(1)。卡要求生物特征验证系统取回‘XX’字节，并期望一个响应。
- (3)和(4) 收到‘62 XX’后，生物特征验证系统应发送 GET DATA 命令（‘00 CB 00 00 XX’）到卡上，并将中间数据从卡中取出。为了取回卡中可用的‘XX’字节，接口设备应发送一个 GET DATA 命令，该命令的 P1-P2 为‘0000’，Le 字段为‘XX’。如果在接收来自外界的数据之前卡仍然需要传送数据，则卡应发送 SW1-SW2=‘62 XY’并重复步骤(3)和(4)。
- (5) 一旦生物特征验证系统处理完中间数据，则设备应将处理后的数据返回给卡。生物特征验证系统应使用 PUT DATA 命令（‘00 DB 00 00 YY …’）将处理后的数据发送回卡，以继续卡内比对过程。接口设备应发送一个 PUT DATA 命令，命令的 P1-P2 为‘0000’，Le 字段为‘YY’。如果外界还未传输完所有的数据，则 PUT DATA 应被链接并重复步骤(5)。
- (6) 如果卡仍需要 WSR，则卡操作系统重复执行步骤(2)开始的生物特征比对函数。如果不是，则见下面内容。
- (7) 如果卡不再需要 WSR，则卡应响应 SW1-SW2，作为对步骤(1)开始的接收到的生物特征比对命令的响应。

WSR 协议的状态图参见附录 H。



其中,XX 是发送给生物特征验证系统的中间数据的字节数;YY 是返回给卡的处理后的数据的字节数。

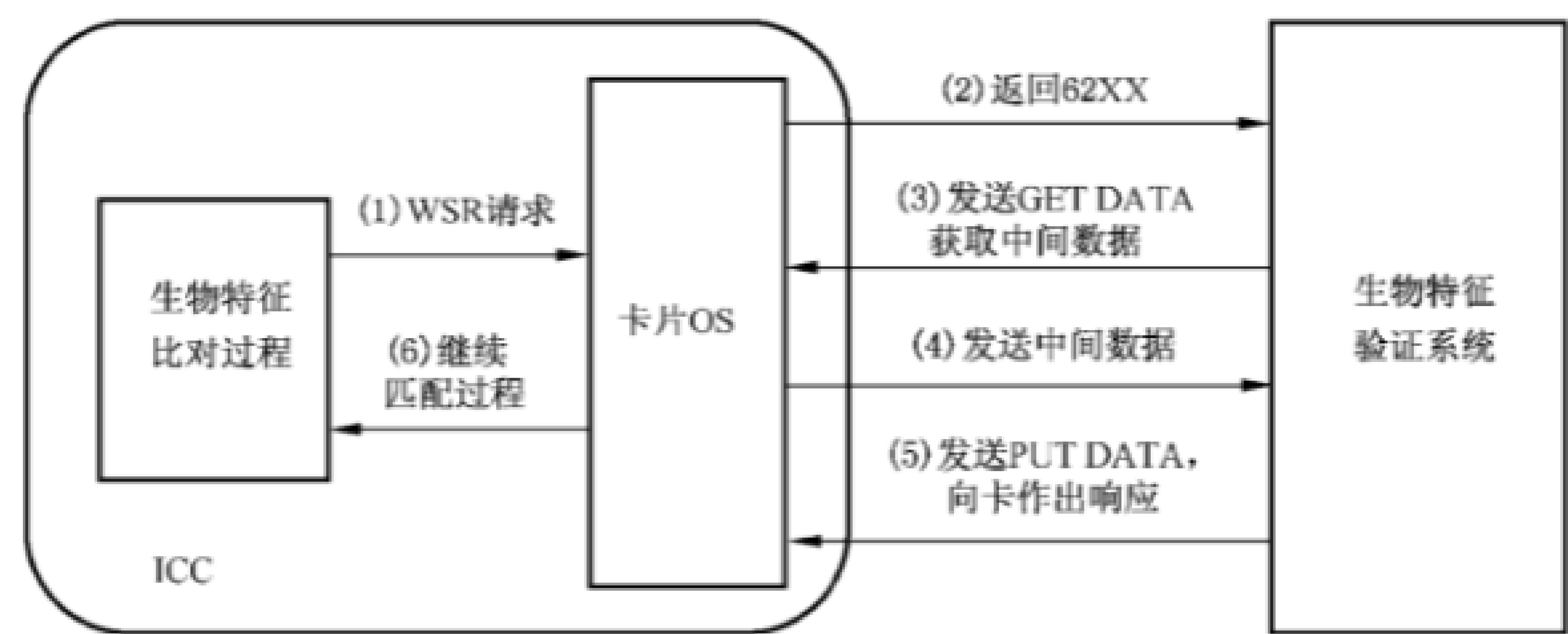


图 7 WSR 机制

8.2 协同工作管理

8.2.1 概述

卡内比对应用可能需要管理规程来使生物特征验证系统知道 WSR 协议是否可用和明确调用一个给定的 WSR 协议。这种情况下,可以使用唯一对象标识符(OID)来让生物特征验证系统在生物特征比对过程中接收 WSR 请求。因此,应有一个属于 OID 树的足够精确的规范来允许 WSR 协议的实现,这意味着此规范有一个唯一的 OID。

8.2.2 协同工作过程发现

对需要卡内生物特征鉴别的应用相关联的特定 WSR 协议的支持,可以将 OID 封装在所构造的应用模板(标记‘61’)中的私有数据(标记‘73’)版本中,被在 DIR 文件中读出或通过标准 GET DATA 命令恢复;在通道 0 上,它应是:

‘00’ ‘CB’ ‘2F’ ‘00’ ‘02’ ‘5C’ ‘00’ ‘00’

注: ISO/IEC 7816-15 在私有数据中为了其他目的使用了此类编码。

8.2.3 协同工作过程操作

需要卡内生物特征比对的应用应在当前被选择。接口设备应知晓(根据 8.1)WSR 协议可用。为了根据 8.1 选择一个 WSR 协议,接口设备可以发送一个封装了 WSR 协议的 OID 的 odd ENVELOPE 命令到卡。在通道 0 上,它应为:

‘00’ ‘C3’ ‘00’ ‘00’ <Lc> ‘06’ <Lc-2> < WSR 协议的 OID >

命令的成功(响应为‘90 00’)说明了:

- 卡已理解 OID,因此支持被引用的 WSR 协议;
- 对执行此协议已准备就绪,例如,它处于应用工作流程的正确位置,并且充分的安全环境已设置。

所有其他的 SW1 SW2 值,要么是拒绝支持所引用的 WSR 协议,要么是拒绝其使用的时机。推荐使用 SW1 SW2 = ‘6A’ ‘81’。如果卡成功执行 ENVELOPE 命令,则 ENVELOPE APDU 命令数据字段的 OID 应标识定义 WSR 协议的规范。

附录 A  
(规范性附录)  
文件控制参数的一般 TLV 结构

表 A.1~表 A.3 是 GB/T 16649.4—2010 定义的用于访问规则的编码,它包含了访问模式数据对象,后随着一个或多个安全条件数据对象。

表 A.1 用于 DF 的 FCI 的一般 TLV 结构

标记	长度	值		
62	x	标记	长度	值
		82	1	‘38’文件描述符
		83	2	文件 ID
		84	‘01’到‘10’	DF 名称(AID)
		8A	1	5

表 A.2 用于格式化 EF 的 FCI 的一般 TLV 结构

标记	长度	值		
62	x	标记	长度	值
		82	5	文件描述符(1 个字节) 41 00 记录长度最大值(1 个字节) 记录计数最大值(1 个字节)
		83	2	文件 ID
		85	2	最大长度
		88	1	短 EF ID
		8A	1	5(启用状态)
		A1	变长	带访问规则引用的数据对象

表 A.3 用于透明 EF 的 FCI 的一般 TLV 结构

标记	长度	值		
62	x	标记	长度	值
		80	2	透明 EF 的内存空间
		82	1	透明 EF 的文件描述符
		83	2	文件 ID
		88	1	短 EF ID
		8A	1	5
		A1	x	带访问规则引用的数据对象

附 录 B  
(规范性附录)  
卡内生物特征比对的安全策略

B.1 简介

本附录为使用卡内生物特征比对的 ICC 应用定义了安全策略的最小集。就像将要说明的那样,考虑不同的体系结构,尽管有些策略可以运用于所有情况,但也有一些其他的策略仅适用于一些特定的体系结构。

在本介绍中,将提供一个对于不同体系结构的总体看法,并用一个表格来将那些体系结构对应到以下条款中的具体安全策略中来。不同的结构可被分类为:

- a) 将生物特征参考作为一个全局元素。它包括以下情况:
  - 1) 使用卡内生物特征比对的单应用卡。
  - 2) 使用一个单一比对配置(例如:相同的阈值、相同的重试计数器等)的卡内生物特征比对的多应用卡。在这种情况下,如果一个应用阻止了卡内生物特征比对机制,那么所有使用相同验证机制的应用都会受到影响。另一方面,如果一个应用有一次成功的验证,那么所有应用的重试计数器都将被重置。
- b) 将生物特征参考作为一个本地元素。它包括以下情况:
  - 1) 每个应用都有它自己的生物特征参考结构,包括生物特征参考数据、配置数据(如阈值)、重试计数器的最大值、重试计数器等。
  - 2) 所有应用仅共享相同的生物特征参考数据,但每个应用都有它自己的配置数据(比对配置数据),它包括了不同的阈值、重试计数器等。

表 B.1 列出了上面提到的不同体系结构和本附录中定义的安全策略之间的关系。

表 B.1 卡内生物特征比对体系结构与安全策略的映射

	SP1:全局比对配置数据	SP2:本地比对配置数据
a.1	X	
a.2	X	
b.1		X
b.2		X

下列条款定义了一般的安全策略:策略 SP1 及策略 SP2。

B.2 卡内生物特征比对的一般安全策略(common security policies, CSP)

- 在任何情况下,以下的最低安全策略都可行:
- 不允许任何应用发送生物特征参考到 ICC 外部(见 7.2.2)。
  - 7.1.5 中规定的策略应被用来实现重试计数器机制。
  - 所有应用都应使用可用的安全机制来创建生物特征参考(注册)、更新生物特征参考(再次注册)或与生物特征参考比对(验证)。特别是:

- 安全报文传输的建立应优先于上面提到的任何操作(GB/T 16649.4)。
- 所有关于卡内生物特征比对的数据交换都应鉴别其完整性。
- 所有生物特征数据都应被加密传送给 ICC,以确保其机密性(ISO/IEC 24761:2009)。

——卡操作系统可能有一个解阻塞卡内生物特征比对的机制。如果是这种情况,解阻塞程序应“清零”ICC 中的生物特征参考,并请求一次新的注册。

### B.3 全局比对配置数据的安全策略(SP1)

对生物特征参考作为全局验证机制的应用,无需为确定一个比对配置而建立一个二次转接。此外,应执行以下策略:

- 对于使用相同生物特征参考进行卡内生物特征比对的多应用卡,如果任何使用生物特征参考的应用都是一个高安全应用,则所有应用都应使用一个唯一的阈值,并且使用与生物特征参考相关的一个单一重试计数器,见 7.2.8 a)。
- 所有配置数据都与生物特征参考相链接。特别是:
  - 验证阈值;
  - 验证重试次数的最大值;
  - 重试计数器;
  - 比对算法的所有参数。
- 任何使用卡内生物特征比对机制并且包含这些生物特征参考的应用都不可以单独改变配置数据。
- 当重试计数器到达零时,卡内生物特征比对机制会被阻止,因而所有使用生物特征参考来验证的应用都将无法运行那些被卡内生物特征比对所保护的操作。
- 一个成功的生物特征参验证会重置相关的重试计数器到其初始值,无论哪个应用都可实现这样的成功验证。

### B.4 本地比对配置数据的安全策略(SP2)

当一张卡上的应用请求卡内生物特征比对的一个独立控制,但同时共享同一个生物特征参考时,应执行以下策略:

- 使用二次转接机制的所有应用将拥有它们自己的比对配置数据,包括,并至少要有:
  - 阈值;
  - 重试计数器。
- 不允许配置共享相同生物特征数据的应用,那将产生不同阈值,但是共享相同的重试计数器。
- 一个应用使用生物特征参考,不应对其他应用的安全性和完整性产生影响。更需明确的是:
  - 当一个应用成功验证生物特征参考的任何时候,只有用于这个应用的重试计数器会被重置到其初始值。
  - 当一个应用验证生物特征参考数据失败的任何时候时,只有用于这个应用的重试计数器会减少一个单位值。
  - 如果一个应用的重试计数器到达零时,只有这个应用可以阻止之后卡内生物特征比对的验证命令的执行。
- 所有应用可以根据需要改变它的比对配置数据,不需要修改任何与它共享同个生物特征参考的其他应用的比对配置数据。

附录 C  
(资料性附录)  
用于卡内比对的 APDU 示例

表 C.1 是符合现有标准的一个示例 APDU 的结构。  
VERIFY 命令 APDU 用来发送一个指纹细节点模板给 ICC。它具有以下结构：

表 C.1 命令 APDU 结构

CLA	INS	P1	P2	Lc	数据
0x00	0x20 0x21 <sup>a</sup>	0x00	0x00	长度	Lc 字节
注 1：Le 字段为空，因为在 GB/T 16649.4 中 VERIFY 命令没有返回响应数据，而是仅向接口设备返回了状态字。					
注 2：使用中的生物特征在 BIT 内部指示。					
<sup>a</sup> 如果数据字段包含透明无格式数据，则使用标记 0x20，而标记 0x21 则是指明数据字段是按 BER-TLV 编码的。					

数据字段包含验证数据。ICC 的性能或许能够隐约的被知道。推荐的方法是保留一个 BIT，它可以采用使用标记 0x7F60 的 GET DATA 命令公开地从卡内读出，也可以向外界发送关于卡性能的信息，例如：支持卡内比对，无论期望的数据格式和格式类型是什么以及 ICC 是否想要有序的细节点。关于 BIT 的详细内容见 ISO/IEC 7816-11。

数据字段中的模板应为按 BER-TLV 编码的。以下标记与编码相关：

- 0x7F2E 生物特征参考；
- 0x5F2E 生物特征数据；
- 0x81/0xA1 标准格式的生物特征数据(原始的/已构建的)；
- 0x82/0xA2 私有格式的生物特征数据(原始的/已构建的)。

如果发送一个标准的细节点数据集给卡，数据字段采用表 C.2 的编码。

表 C.2 标准细节点的数据字段

标记生物特征参考	数据对象的长度	标记标准化的生物特征数据	细节点数据的长度	细节点数据
0x5F2E	L+2	0x81	L	

图 C.1 示出了一个标出了细节点方位的指纹图片。





图 C.1 标出细节点方位的指纹图像

细节点可以用度量单位来测量,并被压缩成卡格式,以便于卡内使用。这样便可以得到以下数据(16 进制):

5D 69 2D A1 43 2F AA 82 2F 6F 48 2F 43 49 35 96 45 37 AF 81 48 B0 BF 48 96 48 48 5D 89 4A  
9C 43 4D 7C 6A 4D 63 6A 4D 19 45 4F 73 8B 50 91 42 54 85 6B 57 6B AA 58 86 B2 58 7D 70 59  
36 82 5B 8C 57 5E 94 9C 5F 73 71 61 61 66 64 4C 9C 69 97 9B 6F A5 9D 70 33 B9 72 50 96 74 92  
58 7D 27 59 7E 9D 59 80 66 93 83 4A 56 86 8E 56 90 3D 74 9A 3A 76

ISO/IEC 19794-2 的类型 6 格式用于编码细节点。细节点方位在凸起结构的分歧点以及凸起结构的终点。这与地面原理类似,可以被一个人工的指纹检测器和普遍使用于最多供方的指纹算法所用。每个细节点由 3 个一组的字节所表示。第一个细节点有水平方位 0x5D,垂直方位 0x69,分歧及方位类型都存储于 0x2D 中。

一共发现了 35 个细节点,总计细节点尺寸是  $3 \times 35 = 105$  字节,16 进制为 0x69。

数据加到上述结构后得到如图 C.2 所示结构的命令:

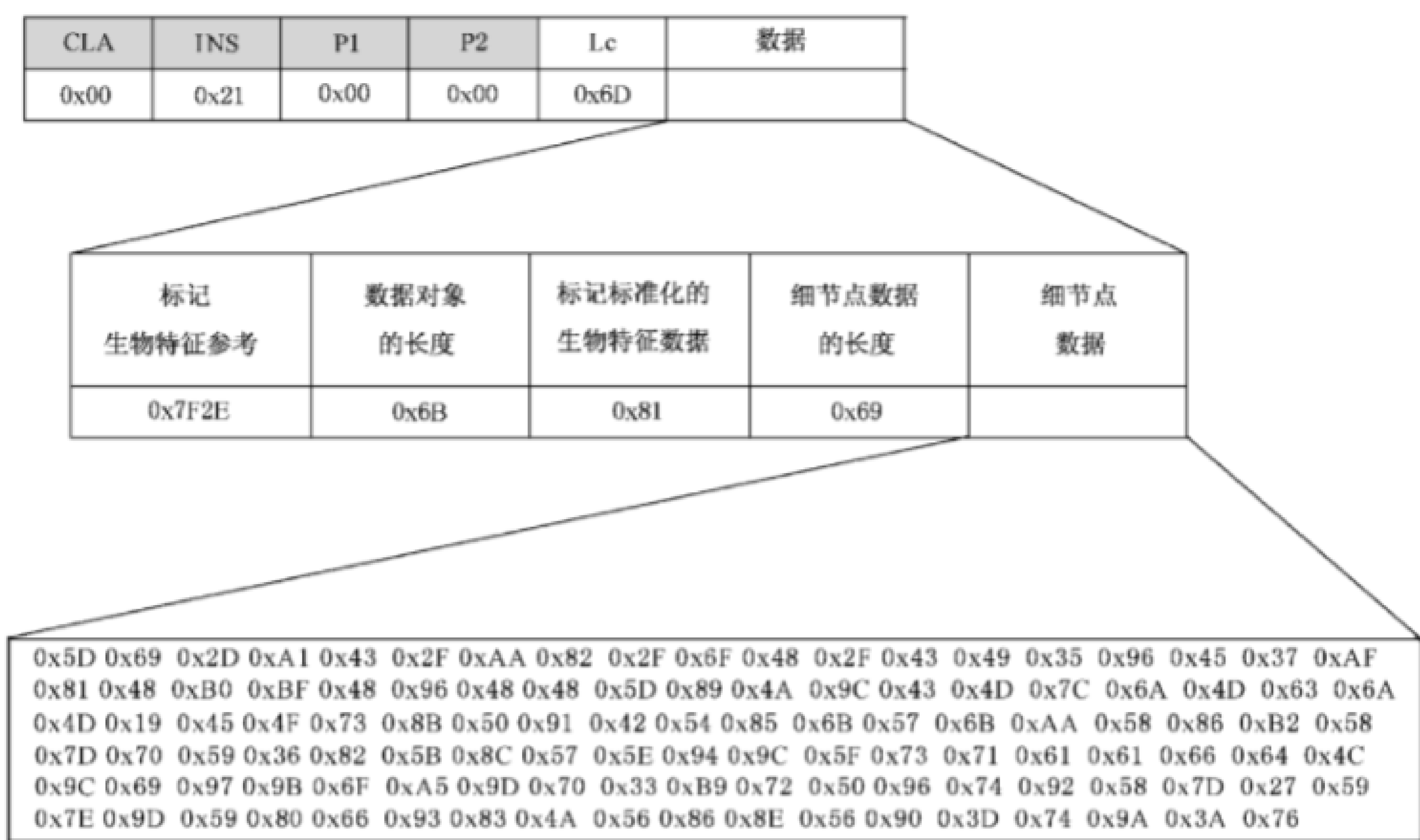


图 C.2 用于卡内比較的 APDU 结构

所有命令：

0x00 0x21 0x00 0x00 0x6D 0x7F 0x2E 0x6B 0x81 0x69 0x5D 0x69 0x2D 0xA1 0x43 0x2F 0xAA  
0x82 0x2F 0x6F 0x48 0x2F 0x43 0x49 0x35 0x96 0x45 0x37 0xAF 0x81 0x48 0xB0 0xBF 0x48  
0x96 0x48 0x48 0x5D 0x89 0x4A 0x9C 0x43 0x4D 0x7C 0x6A 0x4D 0x63 0x6A 0x4D 0x19 0x45  
0x4F 0x73 0x8B 0x50 0x91 0x42 0x54 0x85 0x6B 0x57 0x6B 0xAA 0x58 0x86 0xB2 0x58 0x7D  
0x70 0x59 0x36 0x82 0x5B 0x8C 0x57 0x5E 0x94 0x9C 0x5F 0x73 0x71 0x61 0x61 0x66 0x64  
0x4C 0x9C 0x69 0x97 0x9B 0x6F 0xA5 0x9D 0x70 0x33 0xB9 0x72 0x50 0x96 0x74 0x92 0x58  
0x7D 0x27 0x59 0x7E 0x9D 0x59 0x80 0x66 0x93 0x83 0x4A 0x56 0x86 0x8E 0x56 0x90 0x3D  
0x74 0x9A 0x3A 0x76

对于编码细节点和构建命令还存在其他的可能性，可以使用可选特征或属性数据。  
对于这些可选项，为便于使用来自不同供方的技术的应用实现互操作，应在应用框架中给出指南。

附 录 D  
(资料性附录)  
生物特征比对的软件共享接口

D.1 概述

在一个多应用 ICC 中,通过建立防火墙机制来保护每个应用的敏感数据。该机制的优点在于它能阻止恶意应用访问另一应用的数据。但是该机制也存在一个可信应用想要与另一可信应用共享一个方法/数据的问题。拥有一个安全的共享接口或软件防火墙可以允许应用之间只分享被选择过的方法/数据,这样也可保护敏感数据被访问。这对于生物特征应用与其他应用在卡内共享结果或生物特征数据是至关重要的。

D.2 共享接口机制

通过共享界面共享函数/数据的方法在下文中描述。图 D.1 示出了一张有两个应用的卡。共享生物特征应用创建了两套函数/数据:非共享函数用于自身的访问,可共享函数/数据可被其他应用有限访问。可共享函数来自于共享界面。另一个普通应用想要使用生物特征应用的共享函数/数据,它也会创建两套函数/数据:非共享函数适用于自身的方法,可共享函数/数据用于使用其他应用的方法。

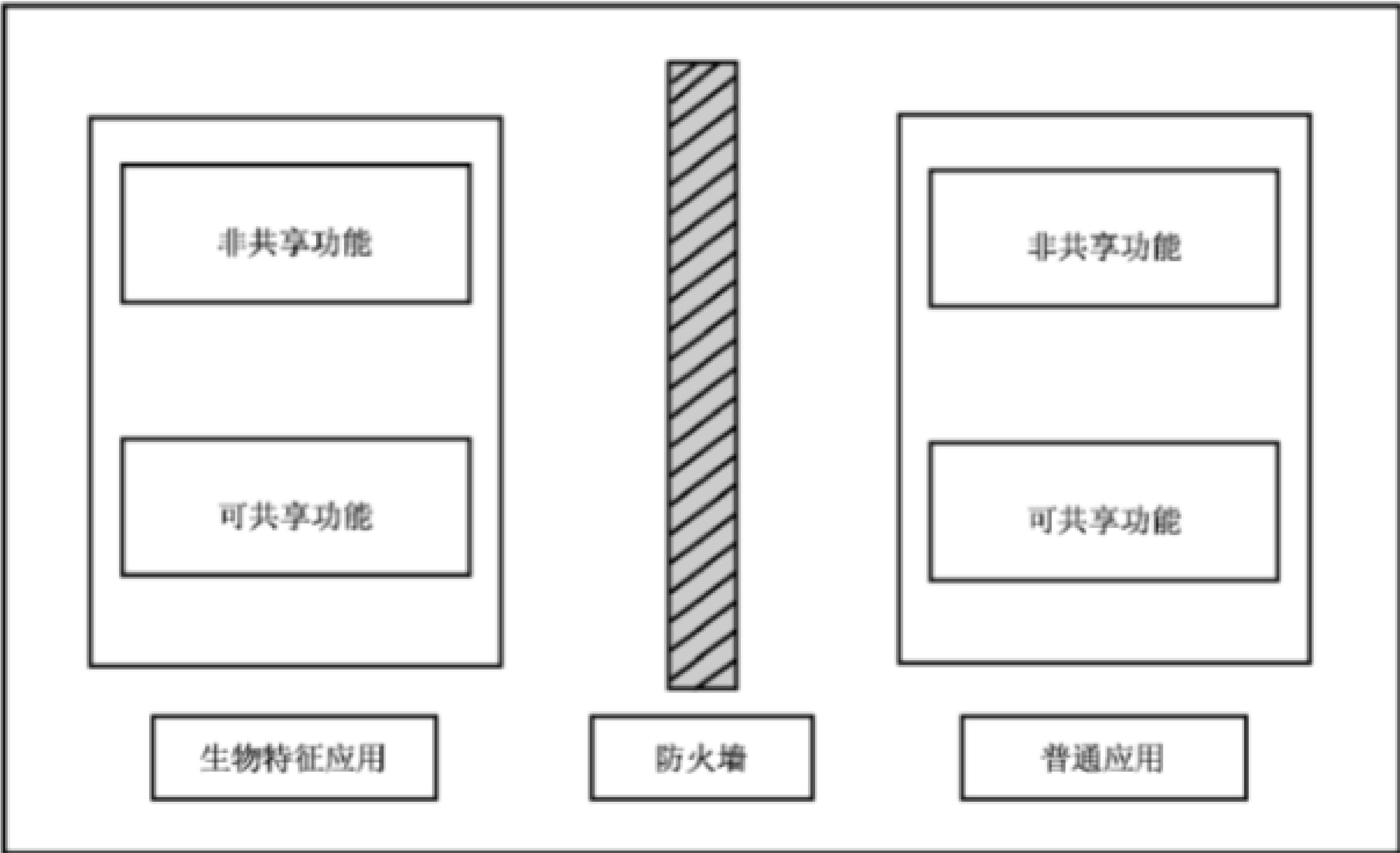


图 D.1 卡内应用

普通应用可调用生物特征应用的共享函数。操作系统检查并转发请求给生物特征应用。生物特征应用接收请求并决定它是否与其他请求者共享其共享函数。如果生物特征应用发现请求可获准,那么会提供一个参考给它的共享函数;否则返回错误。操作系统将这个参考转发给请求者(普通应用)。图 D.2 说明了这个过程。



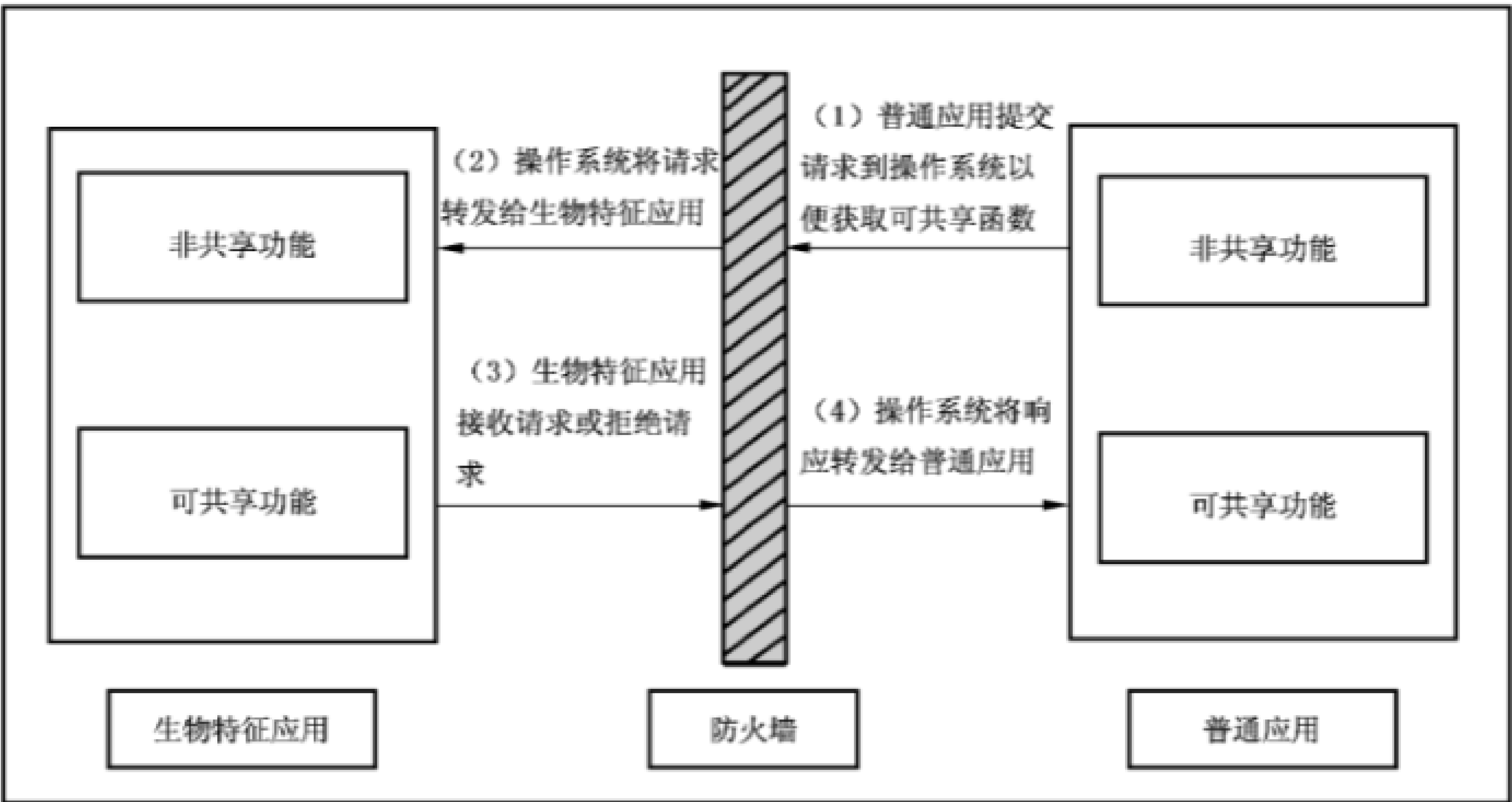


图 D.2 访问已共享的目标

一旦普通应用获得该参考,它就可以使用生物特征应用所提供的共享函数/数据。普通应用可以通过共享函数来获得生物特征比对分数以实现传送或获取授权用户用于传输所需的信息。共享函数可共享的时间取决于操作系统或增加安全的生物特征应用,如图 D.3 中所述。

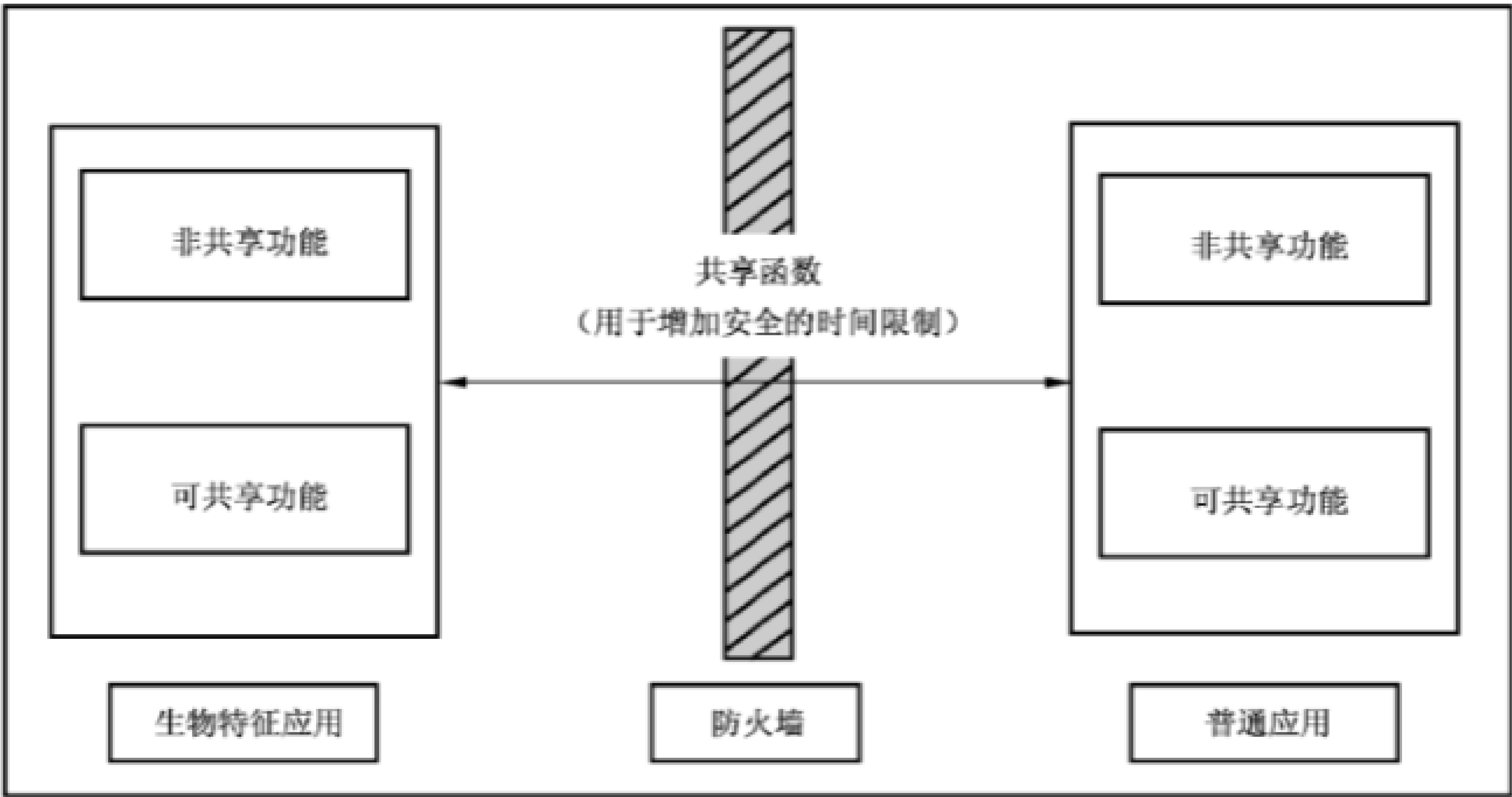


图 D.3 对象的成功共享

例如,一旦生物特征应用完成了生物特征验证,一个比对分数就会被算出并存储在程序中。普通应用可以访问生物特征应用来获取比对分数,它是经过防火墙来访问共享函数实现的。防火墙会首先检测请求者的访问能力(普通应用),然后允许它从生物特征应用那里获取比对分数(在成功验证的基础上)。防火墙由卡内操作系统控制。

## 附录 E

### (资料性附录)

#### 关于卡内比对安全机制的建议

##### E.1 概述

本附录意在介绍与卡内比对识别卡共同工作时考虑的安全机制。如本标准所提到的,由于对生物特征信息有隐私限制,因此强烈推荐采用安全机制。

读者应同时参考其他安全相关的标准,以获取执行这些安全机制所需的所有技术细节。读者也可通过参考 ISO/IEC 7816 来了解有关集成电路卡的命令和机制的信息(如第 4、8、11 和 15 部分),以及有关的我国和国际信息安全标准。

##### E.2 双向鉴别

当两个实体交换数据时,试图保证安全首先需要考虑的就是双方之间的相互信任。因此,当开始通信时,一个机制用于终端信任卡,另一个机制用于卡信任终端,这两个机制均要被用到。这些机制被称为内部鉴别和外部鉴别。当两个机制同时使用时,就被称为双向鉴别。

为了创建一个安全通道,双向鉴别通常终止于一个会话密钥的产生。为了避免重放攻击,这种会话密钥在不同的会话中应完全不同。一些用于双向鉴别的算法需要卡和终端双方均产生随机数或伪随机数。

一旦一个安全通道在卡和终端之间建立起来,下面的机制就可达成成功的更高级别。

##### E.3 报文完整性

在 APDU 的交换过程中,黑客可能会试图截取报文并且根据他们自身的利益来更改报文内容,例如,通过重新发送之前的生物特征样本来获取访问卡信息和/或服务的权利。为了避免这种攻击,建议卡和终端都要检查所接收到的 APDU 的完整性。

一种执行检查的方法是对 APDU 签名,包括报头和数据,可以使用对称加密算法,并将已获取的签名附加到已交换的数据上。使用双向鉴别过程中创建的会话密钥,可以避免以上提到的攻击。

##### E.4 机密性

完整性被推荐用于所有的 APDU 交换,但是有时需要用到一些更高的安全级别。特别关键的是那些将生物特征模板或生物特征样本从读写器传输到卡(或在卡外比对中从卡传输到读写器)的 APDU。在这类报文中,数据在原始格式的状态下不应被传送,但是可以使用可用的最高安全级别来加密,从而增强系统内的机密性。

例如,如果使用对称加密算法,数据可以和双向鉴别中获取的会话密钥一起被加密(在建立一个安全通道时)。完整性检查仍然被推荐,因此完整性适用于所传输数据的加密前和加密后。

### E.5 使用带保密密钥的 MAC 防止重放攻击

推荐在 ICC 中实现保护机制来防止重放攻击。一种避免重放攻击的可行方法是使用与一个随机数和一个保密密钥相关联的生物特征数据的报文鉴别代码(MAC)。终端可从卡上获得随机数,并计算一个与随机数(卡上的)和保密密钥相连接的生物特征数据的 MAC。保密密钥存储在应用和卡上。在通信过程中,只有随机数和 MAC 是必需传输的。当卡接收到生物特征数据和 MAC 时,在进行生物特征比对之前,首先宜在卡内验证 MAC。

如果攻击者能够获取生物特征数据,甚至来自卡的随机数和来自之前匹配过程的 MAC,但是在不知道保密密钥的情况下,攻击者仍然无法产生一个正确的 MAC 来完成下一次的验证。

然而,这种方法的前提是假设终端是被信任的,并能自己保持一个保密密钥,该方法可被视为是“安全通道”的一种。

注:考虑到工作环境,该方法是可选的。

附 录 F  
(资料性附录)  
协同工作的卡内比对体系结构

F.1 概述

协同工作是卡内比对的一种特殊情况,它把生物特征比对过程的工作量分配在 ICC 和接口设备上。上述的机制使得卡可以使用本地生物特征验证系统,这通常是指一台 PC 或拥有更强处理能力的嵌入式处理器,以便协助加载密集函数的计算。卡和本地生物特征验证系统共同工作来加速整体的生物特征比对并将注册的生物特征信息的安全性和私密性考虑在内。在协同工作的体系结构下,比对过程应在 ICC 中进行。

F.2 卡内比对的协同工作体系结构

图 F.1 示出了协同工作的卡内比对体系结构的框图。大部分协同工作的卡内比对所使用的元件与纯卡内比对所使用的元件相同,除了以下两个部分:

- 生物特征数据,在注册过程中被存储于卡内,分为保密部分和开放部分。保密部分指的是关键的、具有唯一性的生物特征参考,而开放部分没有那么关键,因为它无法用来恢复保密部分中的数据。保密部分,即生物特征参考,以 ISO 格式存储。开放部分,包含生物特征属性,其目的是加速卡的比对过程并将其发送到本地生物特征验证系统。
- 比对过程产生了一些生物特征验证系统端的计算来加速比对。

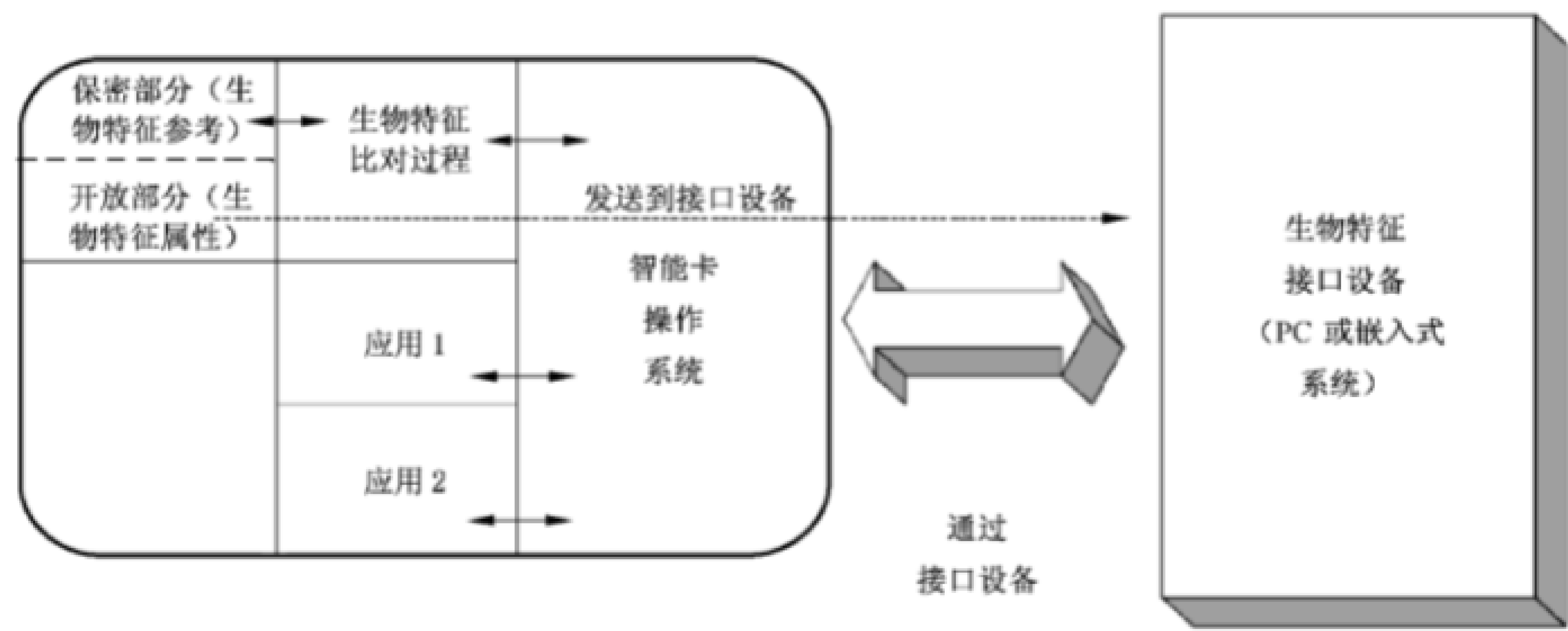


图 F.1 协同工作的卡内比对框图

在图 F.1 中的虚线箭头指示开放部分是可以被传送到生物特征验证系统的。开放部分应与请求一起从本地生物特征验证系统中发出。为了同时保证模板的安全和节省内存空间,开放部分可在被存储前预加密并且压缩。

### F.3 用于卡内比对的协同工作策略的类型

#### F.3.1 概述

有两种类型的协同工作策略可用于卡内比对。一种是预对计算,另一种是在比对运行时实行协同工作。6.4 中的图 3 示意性地表示了协同工作卡内比对的体系结构。

#### F.3.2 预比对计算

某些生物特征,如指纹,需要在比对前进行模板核准。这类过程被称作预比对计算,就是说在真正的比对过程前,需要一定的计算。为了计算预比对,需要一些来自于指纹注册时的信息。数据的开放部分可被用来执行此类操作。

示例:基于使用波文的指纹识别的模式可以使用开放部分存储已选择的波文。这样减少的维度部分可以被传输到本地生物特征验证系统来对输入的模板执行转化核准。

#### F.3.3 运行时的协同工作

在预比对计算过程中,有些计算是计算密集型的。低端卡也许没有足够的计算能力在短时间内处理这类计算。因此,为了加速比对过程,卡可以发出一些中间数据到本地生物特征验证系统进行计算。

### F.4 协同工作计算协议

协同工作计算协议(WSCP)说明了使用协同工作来执行卡内比对的顺序。在启用 WSCP 之前,建议本地生物特征验证系统和卡应运行双向鉴别来确认比对过程及本地生物特征验证系统都是真正获得授权的可执行卡内比对的程序。

图 F.2 总体示出了 WSCP 被分为两个部分。第一个部分是预比对计算部分。它涉及四个步骤。第一步是本地生物特征验证系统发出一个命令到卡上来启用比对程序。一旦卡接收到命令,卡会将模板的开放部分发回到本地生物特征验证系统。在生物特征验证系统接收到模板的开放部分后,生物特征验证系统会使用开放模板来执行必要的操作,例如旋转式转化以及创建输入模板等。然后输入模板会被发送到卡上开始卡内比对。步骤(1)~步骤(4)是生物特征验证系统和卡之间的标准数据处理。因此,原有的 GB/T 16649.4—2010 的 APDU 命令和响应对于处理在预比对计算中的开放部分的传送操作已经足够了。

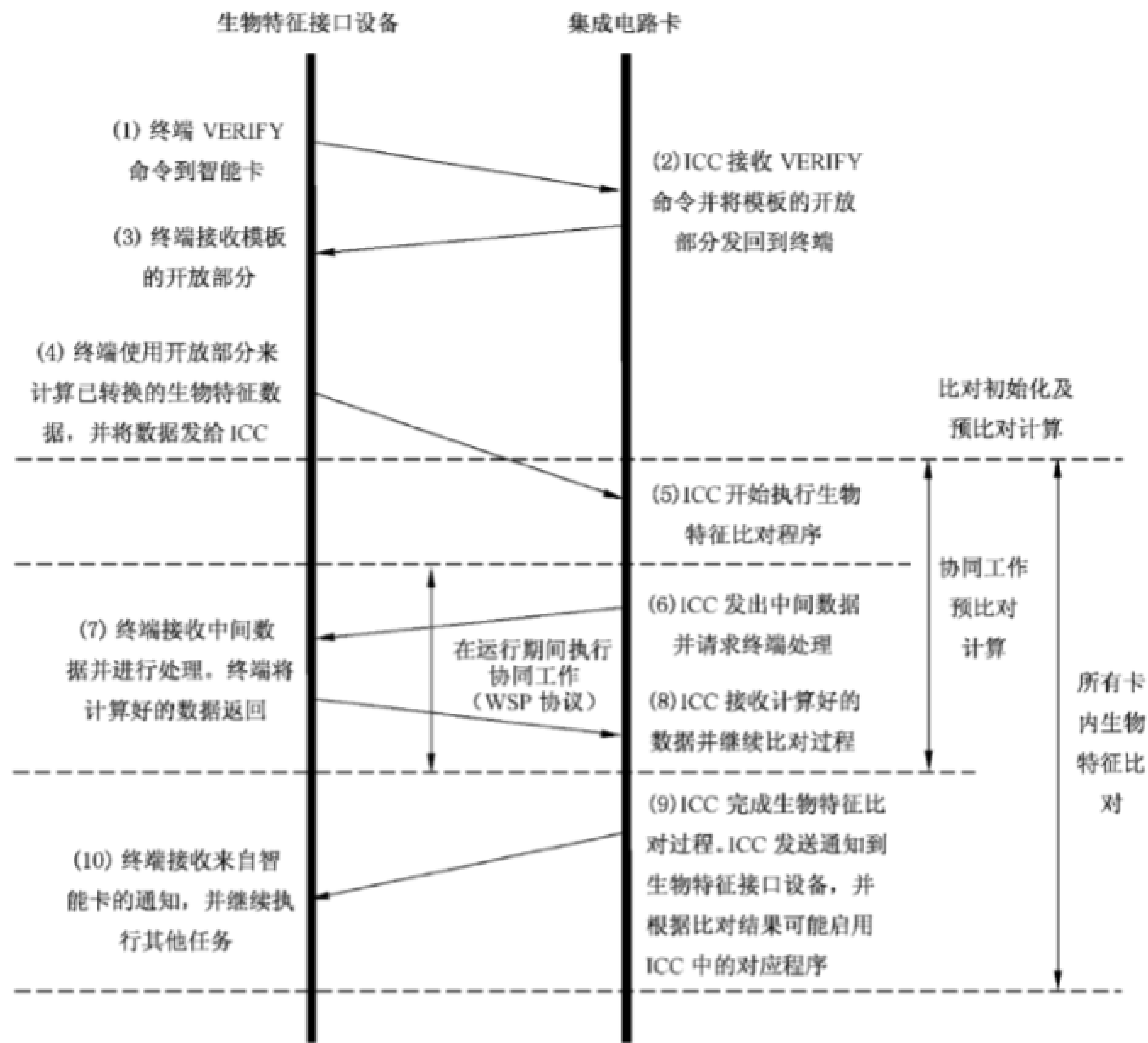


图 F.2 所有协同工作的计算协议

在步骤(5)中，卡在完成预比对过程后开始比对计算。在比对过程中，如果卡需要计算计算密集型函数，则 WSR 协议可以用来请求来自于生物特征验证系统的协同工作。如果卡不需要执行这种函数，则过程可以跳过步骤(6)~(8)，而直接到步骤(9)。步骤(6)、(7)和(8)是使本地生物特征验证系统执行 WSR 的过程，但是如果这些函数都不能应用，那么可以直接跳到步骤(9)。在步骤(6)中，卡发送了协同工作请求和中间数据到本地生物特征验证系统。本地生物特征验证系统在步骤(7)中一起接收了请求和中间数据，之后应执行所请求的函数来处理中间数据。一旦生物特征验证系统端的处理结束了，生物特征验证系统应在步骤(8)中将结果发送到卡，卡会继续执行比对过程。当卡完成了步骤(9)中的比对分数计算时，卡应通知本地生物特征验证系统生物特征比对已完成。在步骤(10)中，本地生物特征验证系统可以继续使用卡内比对的结果来进行接下来的任务。

附 录 G  
(资料性附录)  
卡内生物特征比对机制实现示例

G.1 简介

本附录提供了 3 个示例来介绍如何实现与卡的安全状态相关的卡内生物特征比对机制。这些示例通过状态流程图来说明,其中,圆圈表示安全状态,箭头表示操作及操作所得的结果,两者都意味着状态间的转换。

注释会被简化表示,如 SS 表示安全状态。安全状态会被标上数字,其中,0 为初始状态,数字越大,安全状态的限制也越严格。

为了简单的解释示例,将会使用阈值。当一次生物特征比对完成后,比对分数(cs)会被用来与一个适当的阈值(th)进行比较。如果  $cs > th$ ,则访问被批准,否则将拒绝访问。如果卡中的应用使用一个以上的阈值,则可用符号 th1 及 th2 等来表示,如果  $th2 > th1$ ,这表示 th2 的限制更加严格。

在所有情况下,如本标准所推荐的那样,如果没有预先建立安全通道并且用于进一步的操作,那么任何生物特征比对都不会被批准。

G.2 单一应用,同类使用

首先本标准从最简单的示例开始,卡内一个单一应用的使用,只含一个单一验证级别(单一阈值)。在图 G.1 中安全状态流程被表示了出来。当其他操作可能运行于初始 SS 中时,生物特征验证仅在通过建立安全通道获得一个更高级别的 SS 后执行。在这个 SS 中,用户可能会使用一个 VERIFY 命令。如果访问被批准,便可获得一个更高级别的 SS,并且可以运行需要此级别 SS 或稍低级别 SS 的操作。

如果生物特征验证不成功,则会报一个安全错误,从而回到初始 SS,需要在下一个验证尝试完成前建立一条新的安全通道。此外,生物特征比对的重试计数器会减少一个单位值,如果不允许重试的话,生物特征比对机制会被阻塞。

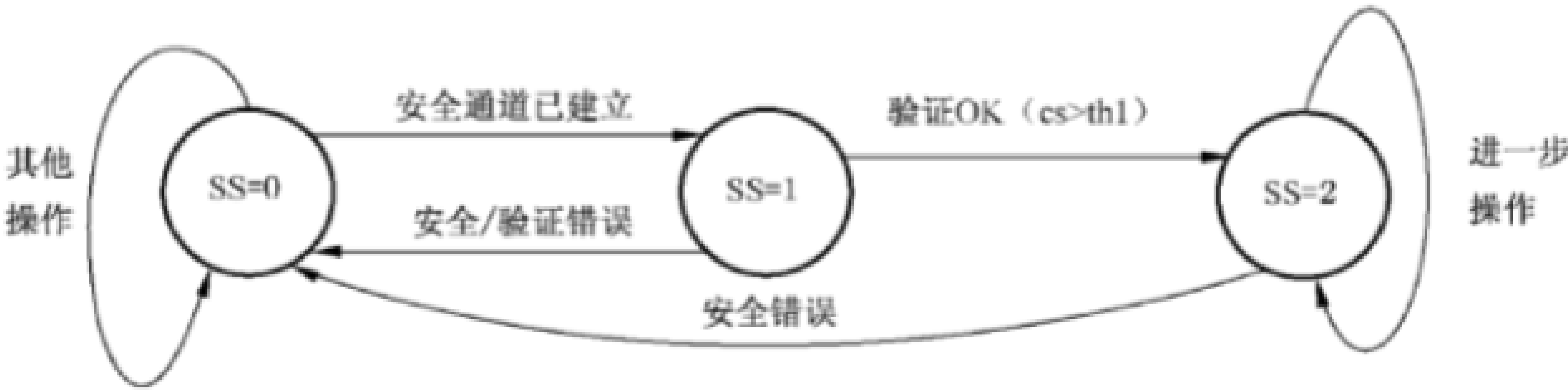


图 G.1 单一应用,同类使用的安全状态流程图

G.3 单一应用,不同使用

在此,本标准将介绍一个更高级别的示例(见图 G.2)。如果一个卡内的单一应用想使用生物特征比对来获取访问信息或特定操作的权利,不同操作需要不同的安全级别是可能的。在这种情况下,应用可能想要通过生物特征比对过程所提供的精确性来选取不同的安全级别。如果是这样的话,可以通过选择两个不同阈值:th1 和 th2 来选取两个不同的级别,举例来说,如果  $th2 > th1$ ,那么 th2 的限制更加

严格。

在建立安全通道后,得到  $SS=1$ 。在此  $SS$  值中,可以执行一次生物特征比对。完成这个操作后,可能会有三种不同情况发生。如果  $cs$  小于或等于  $th1$ ,则访问会被拒绝,相关的重试计数器值会递减,并回到初始  $SS$ 。如果  $cs$  大于  $th1$  但小于或等于  $th2$ ,那么只允许级别 1 的操作,只要其他操作一直需要一个稍低级别的  $SS$ ,就会一直持续下去。只有当  $cs$  大于  $th2$  时,才允许级别 2 的操作,同样是会持续下去,只要其他操作一直需要一个稍低级别的  $SS$ 。

在任何情况下,当报了一个安全错误时, $SS$  就会回到初始值,并且一个新的安全通道会被建立来处理受限的操作。

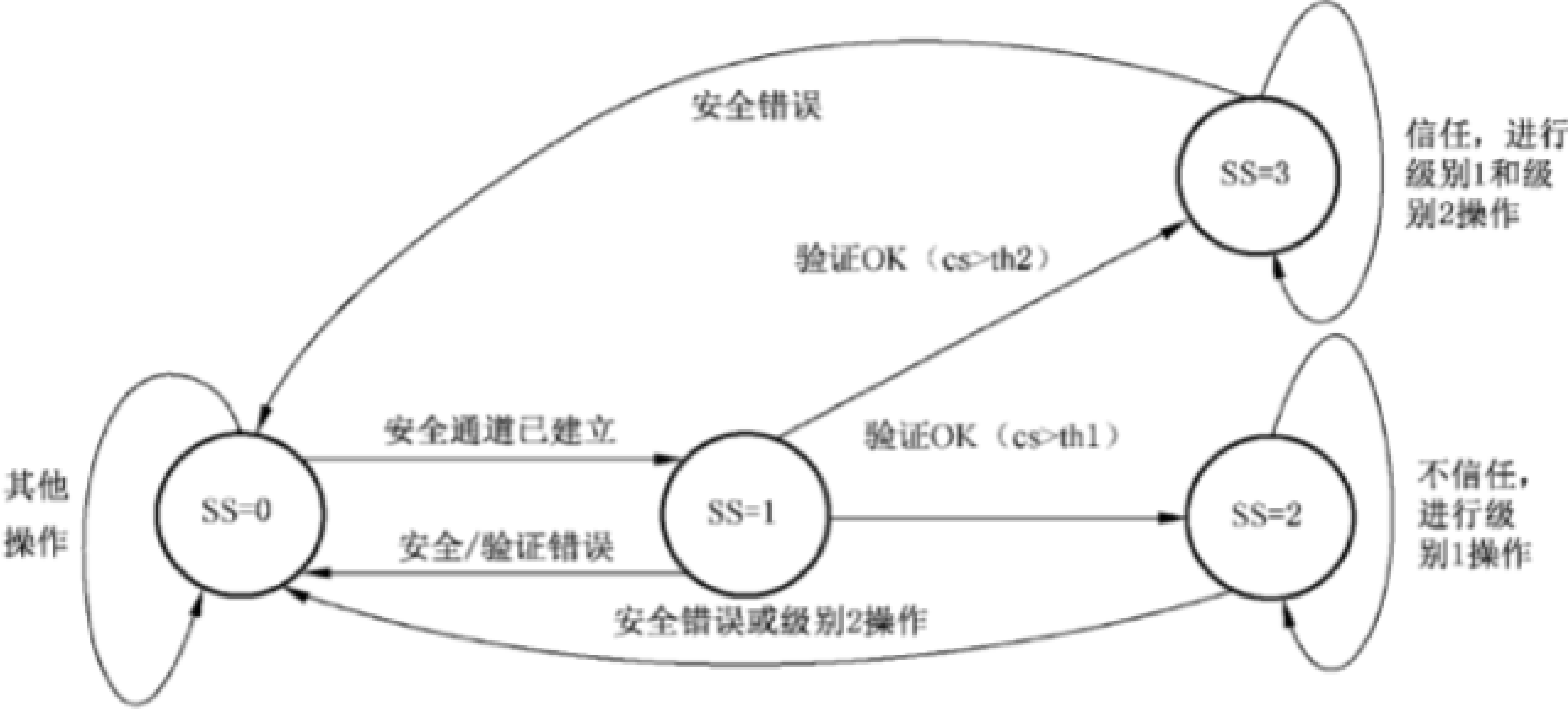


图 G.2 单一应用,不同使用的安全状态流程图

G.4 多应用

最复杂的情况就是一个多应用 ICC,并且每一个应用都有它特定的阈值级别和重试计数器来到达它自身的  $SS$  值从而达成不同的安全级别,同时又使用相同的生物特征参考数据。

过程与以上描述的单一应用不同,使用类似,唯一不同的是与不同阈值及重试计数器的拥有者相关。每个阈值和每个重试计数器影响的只是某一个应用,这样可以避免修改一个应用而影响到其他应用的功能。一个应用的  $SS$  不会被其他应用影响,因为一旦一个新的应用被选定后, $SS$  就会回到其初始级别。因此,在一个应用被选定后,如果要使用一些受限的操作,那么应当建立一个新的安全通道,在那之后,可以使用 `VERIFY` 命令来执行一次生物特征比对。这样比对的结果是,在之前已提到过,将有以下可能性:

- 如果检测没有成功( $cs < th1$ ):
  - a) 减少重试计数器单位值,但只是与现在已选应用相关的计数器。
  - b) 如果重试计数器到达 0 值,那么阻止生物特征检测程序。
- 如果检测成功了,已选应用程序的重试计数器会被重置,并且:
  - a) 如果  $th2 < cs < th1$ ,那么将会到达  $SS$  级别 1 并且会批准请求此类  $SS$  的操作。
  - b) 如果  $cs > th2$ ,那么将会到达  $SS$  级别 2,然后会批准所有的操作(级别 1 和级别 2)。

这在图 G.3 中得到说明:



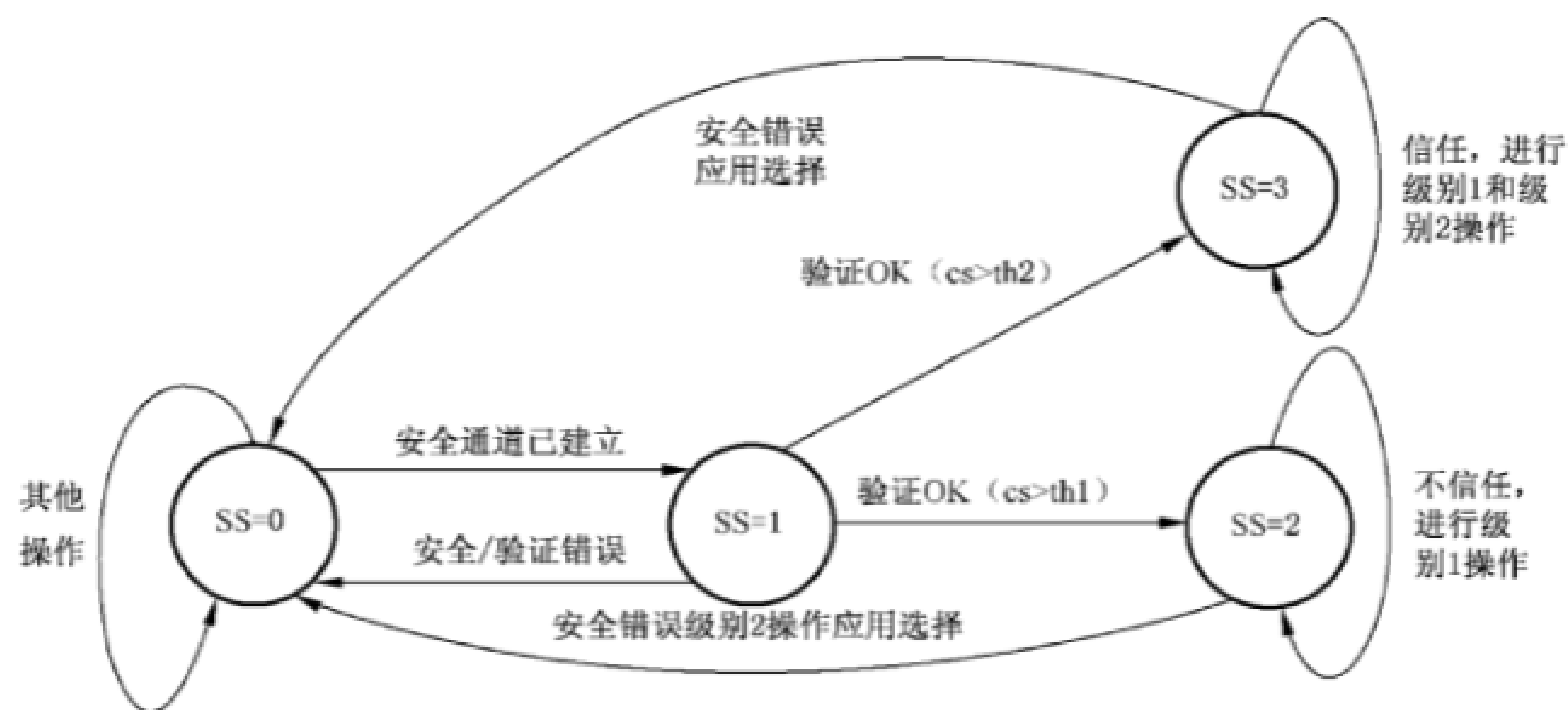


图 G.3 多应用的安全状态流程图

附 录 H  
(资料性附录)  
当需要时卡执行 WSR 会话的状态图

图 H.1 示出了卡执行 WSR 会话的状态图。

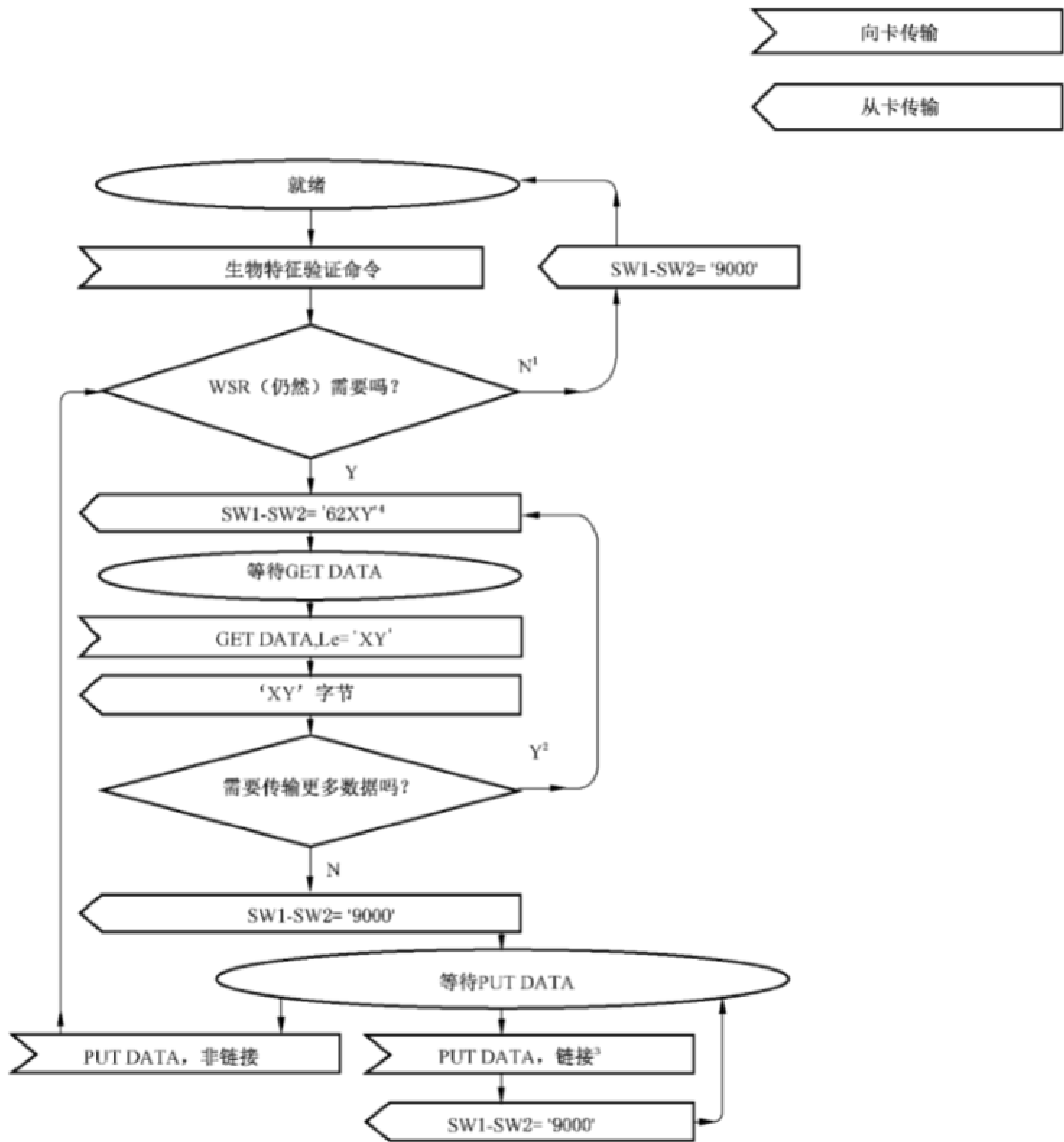


图 H.1 卡执行 WSR 会话的状态图

图中：

- <sup>1</sup> 命令不需要 WSR, 或 WSR 会话已结束。
- <sup>2</sup> 当一个 GET DATA 命令不够时的处理机制在 GB/T 16649.4 中定义。
- <sup>3</sup> 当一个 PUT DATA 命令不够时的处理机制在 GB/T 16649.4 中定义。
- <sup>4</sup> 本标准要求发送充分的 GET DATA 命令, 但是在 GB/T 16649.4 中仅仅是推荐的。

如果这里描述的语法不被考虑,例如因为一个命令被拒绝,或者如果外界发送一个 GET DATA 失败,则卡预期返回“就绪”状态。

---

中 华 人 民 共 和 国  
国 家 标 准  
信息技术 识别卡 卡内生物特征比对  
GB/T 30266—2013/ISO/IEC 24787:2010

\*

中国标准出版社出版发行  
北京市朝阳区和平里西街甲2号(100013)  
北京市西城区三里河北街16号(100045)

网址:www.gbl68.cn

服务热线:400-168-0010

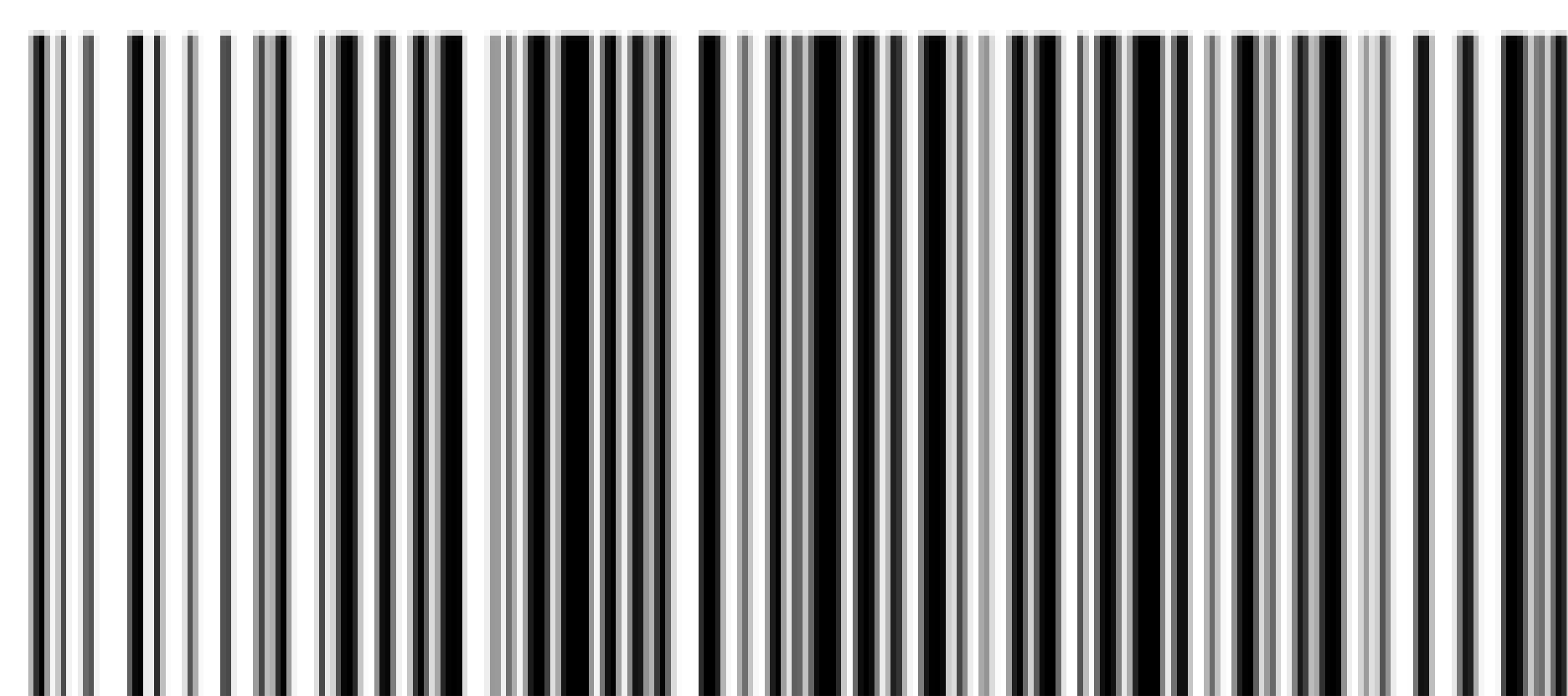
010-68522006

2014年4月第一版

\*

书号:155066·1-48798

版权专有 侵权必究



GB/T 30266-2013