



中华人民共和国国家标准

GB/T 16649.11—2019

识别卡 集成电路卡 第 11 部分：通过生物特征识别 方法的身份验证

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

(ISO/IEC 7816-11:2017, MOD)

2019-08-30 发布

2020-03-01 实施

国家市场监督管理总局 发布
中国国家标准化管理委员会

目 次

前言 III

引言 V

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 符号和缩略语 3

5 生物特征验证及其相关过程的命令 4

6 数据元 9

附录 A（资料性附录） 生物特征验证过程 16

附录 B（资料性附录） 生物特征信息数据对象示例 19

附录 C（资料性附录） 生物特征信息模板中数据对象的标签列表 21

参考文献 22

前 言

GB/T 16649 分为以下几部分：

- 识别卡 带触点的集成电路卡 第 1 部分：物理特性(GB/T 16649.1)；
- 识别卡 带触点的集成电路卡 第 2 部分：触点的尺寸和位置(GB/T 16649.2)；
- 识别卡 带触点的集成电路卡 第 3 部分：电信号和传输协议(GB/T 16649.3)；
- 识别卡 集成电路卡 第 4 部分：用于交换的结构、安全和命令(GB/T 16649.4)；
- 识别卡 带触点的集成电路卡 第 5 部分：应用标识符的国家编号体系和注册规程(GB/T 16649.5)；
- 识别卡 带触点的集成电路卡 第 6 部分：行业间数据元(GB/T 16649.6)；
- 识别卡 带触点的集成电路卡 第 7 部分：用于结构化卡查询语言(SCQL)的行业间命令(GB/T 16649.7)；
- 识别卡 带触点的集成电路卡 第 8 部分：与安全相关的行业间命令(GB/T 16649.8)；
- 识别卡 集成电路卡 第 9 部分：用于卡管理的命令(GB/T 16649.9)；
- 识别卡 带触点的集成电路卡 第 10 部分：同步卡的电信号和复位应答(GB/T 16649.10)；
- 识别卡 集成电路卡 第 11 部分：通过生物特征识别方法的身份验证(GB/T 16649.11)；
- 识别卡 集成电路卡 第 12 部分：带触点的卡 USB 电气接口和操作规程(GB/T 16649.12)；
- 识别卡 集成电路卡 第 13 部分：在多应用环境中的应用管理命令(GB/T 16649.13)；
- 识别卡 集成电路卡 第 15 部分：密码信息应用(GB/T 16649.15)。

本部分为 GB/T 16649 的第 11 部分。

本部分按照 GB/T 1.1—2009 给出的规则起草。

本部分使用重新起草法修改采用 ISO/IEC 7816-11:2017《识别卡 集成电路卡 第 11 部分：通过生物特征识别方法的身份验证》。

本部分与 ISO/IEC 7816-11:2017 相比做了下列结构调整：

- 删除了第 6 章；
- 将第 7 章改为第 6 章。

本部分与 ISO/IEC 7816-11:2017 技术性差异及其原因如下：

- 关于规范性引用文件，本部分做了具有技术性差异的调整，以适应我国的技术条件，调整的情况集中反映在第 2 章“规范性引用文件”中，具体调整如下：
 - 增加引用了 GB/T 15694.1(见表 6、表 7 和表 C.1)；
 - 增加引用了 GB/T 16649.4—2010(见 5.1、5.2、5.3、5.4.1、6.3.1、表 1、表 6、表 7、表 C.1 和附录 B)；
 - 增加引用了 GB/T 30266—2013(见 5.2、A.1、表 3、表 5 和表 7)；
 - 增加引用了 ISO/IEC 7816-6(见 6.2 和表 6)；
 - 增加引用了 ISO/IEC 17839-3(见 5.2 和 5.4.6)；
 - 增加引用了 ISO/IEC 19785-3(见表 6、表 B.1 和附录 B)；
- 第 3 章中删除了术语“生物特征信息”“生物特征数据主体”和“原始数据”；
- 第 4 章中删除了缩略语 ACBio、BRT certificate、BDB、BPU、CCT、CT、DST、FCI、MAC、SM、SMT 和符号 I/O、L；
- 5.4.2 中删除了 SET INITIAL VALUES、GENERATE BIOMETRIC VALIDATION CER-

TIFICATE、GENERATE CONTROL VALUE 和 STORE BIOMETRIC INFORMATION
命令；

——将 6.1 标题改为“生物特征信息模板”；

——表 6 和表 7 中，默认标签分配机构修改为对应的国家标准化技术标委会 SAC/TC 28/SC 17。

本部分还做了下列编辑性修改：

——在表 6、表 7 和表 C.1 中，用 GB/T 26231—2017 代替引用的参考文献 ISO/IEC 8825-1；

——修改了参考文献。

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。

本部分由全国信息技术标准化技术委员会(SAC/TC 28)提出并归口。

本部分起草单位：中国电子技术标准化研究院、深圳眼神智能科技有限公司、楚天龙股份有限公司、北京智芯微电子科技有限公司、飞天诚信科技股份有限公司、大唐微电子技术有限公司、北京中电华大电子设计有限责任公司、北京握奇数据系统有限公司、上海密特印制有限公司、红天智能科技(天津)有限公司、紫光同芯微电子有限公司、中电智能卡有限责任公司、上海复旦微电子集团股份有限公司、金邦达有限公司。

本部分主要起草人：曹国顺、潘金华、蒋曲明、任程、王东山、朱鹏飞、杨春林、李斌、包乌日吐、张树蕊、白婧、张晓良、邴志刚、盛敬刚、周峥、胡波、李丹、邵兴、程文杰、夏立佳、王于波。

引 言

GB/T 16649 是规定集成电路卡参数和交换中集成电路卡使用的国家标准。集成电路卡是用于信息交换(该信息交换由外界和卡上集成电路之间商定)的识别卡。作为信息交换的结果,卡传送信息(计算结果、存储的数据),和/或更改其内容(数据存储、结果记忆)。

有 5 个部分规定了带触点的卡,其中 3 个部分规定了电接口:

- GB/T 16649.1 规定了带触点卡的物理特性;
- GB/T 16649.2 规定了触点的尺寸和位置;
- GB/T 16649.3 规定了异步卡的电接口和传输协议;
- GB/T 16649.10 规定了同步卡的电接口和复位应答;
- GB/T 16649.12 规定了 USB 卡的电接口和操作规程。

GB/T 16649 的其余部分均独立于物理接口技术。它们用于通过触点和/或射频访问的卡:

- GB/T 16649.4 规定了用于交换的结构、安全和命令;
- GB/T 16649.5 规定了应用提供者的注册;
- GB/T 16649.6 规定了用于交换的行业间数据元;
- GB/T 16649.7 规定了用于结构化卡查询语言的命令;
- GB/T 16649.8 规定了用于安全操作的命令;
- GB/T 16649.9 规定了用于卡管理的命令;
- GB/T 16649.11 规定了通过生物特征识别方法的身份验证;
- GB/T 16649.13 规定了用于管理应用程序的生命周期的命令;
- GB/T 16649.15 规定了密码信息应用。

识别卡 集成电路卡

第 11 部分:通过生物特征识别 方法的身份验证

1 范围

GB/T 16649 的本部分规定了安全相关的行业间命令,用于在集成电路卡中通过生物特征识别方法进行个人身份验证。针对卡作为生物特征参考的载体和/或对持卡者的生物特征探针(卡上生物特征比对)进行验证的装置,本部分也给出了其使用的数据结构和数据访问方法。

本部分适用于带生物特征识别技术卡的设计、生产、验证和测试。通过生物特征识别方法进行身份识别不属于本部分规定的范围。

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 15694.1 识别卡 发行者标识 第 1 部分:编号体系(GB/T 15694.1—1995,ISO/IEC 7812-1:1993,IDT)

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)

GB/T 30266—2013 信息技术 识别卡 卡内生物特征比对(ISO/IEC 24787:2010,IDT)

ISO/IEC 2382-37:2017 信息技术 词汇 第 37 部分:生物特征识别(Information technology—Vocabulary—Part 37:Biometrics)

ISO/IEC 7816-4:2013 识别卡 集成电路卡 第 4 部分:用于交换的结构、安全和命令(Identification cards—Integrated circuit cards—Part 4:Organization,security and commands for interchange)

ISO/IEC 7816-6 识别卡 集成电路卡 第 6 部分:用于交换的行业间数据元(Identification cards—Integrated circuit cards—Part 6:Interindustry data elements for interchange)

ISO/IEC 17839-3 信息技术 识别卡 卡上生物特征识别系统 第 3 部分:逻辑信息交换机制(Information technology—Identification cards—Biometric system-on-card—Part 3:Logical information interchange mechanism)

ISO/IEC 19785-3 信息技术 公用生物特征识别交换格式框架 第 3 部分:实体格式规范(Information technology—Common biometric exchange formats framework—Part 3:Patron format specification)

3 术语和定义

GB/T 16649.4—2010、ISO/IEC 2382-37:2017 和 ISO/IEC 7816-4:2013 界定的以及下列术语和定义适用于本文件。

3.1

生物识别特征 biometric characteristic

个体生物学的和行为的特征,该特征可被检测,并且可以从中提取有区别的、可重复的生物特征项(3.4),从而达到生物特征验证(3.9)的目的。

3.2

生物特征比对 biometric comparison

估算、计算或测量生物特征探针(3.6)与生物特征参考(3.7)之间的相似度或相异度。

3.3

生物特征数据 biometric data

处于任何处理阶段的生物特征样本(3.8)或生物特征样本的聚集。

示例:生物特征参考(3.7)、生物特征探针(3.6)、生物特征项(3.4)。

3.4

生物特征项 biometric feature

从生物特征样本(3.8)中提取的,用于生物特征比对(3.2)的数值或标记。

3.5

生物特征项提取 biometric feature extraction

应用于生物特征样本(3.8)的过程,目的是分离并输出可重复性和辨别性的数值或标记,它们可与从其他生物特征样本提取的数据做比较。

[ISO/IEC 2382-37:2017,定义 3.5.4]

3.6

生物特征探针 biometric probe

在生物特征验证(3.9)过程中的、与生物特征参考(3.7)进行生物特征比对(3.2)的数据。

注:ISO/IEC 7816-11:2004 使用“生物特征验证数据”术语。

3.7

生物特征参考 biometric reference

在登记期间存储在卡上的一个或多个数据对象,表示被鉴别人的、任何生物识别特征(3.1)的生物特征数据(3.3)。

注:ISO/IEC 7816-11:2004 使用“生物特征参考数据”术语。

3.8

生物特征样本 biometric sample

先于生物特征项提取(3.5)的,模拟的或数字的生物识别特征(3.1)的表示。

3.9

生物特征验证 biometric verification

生物特征探针(3.6)与生物特征参考(3.7)进行一对一生物特征比对(3.2)的验证过程。

3.10

数据采集 data acquisition

从一个生物识别特征(3.1)中收集或尝试收集信号(3.17)并将其转换为一个生物特征样本(3.8)集的过程。

3.11

动态生物特征验证 dynamic biometric verification

对被鉴别人的动态行为进行的生物特征验证(3.9)过程。

注:动态行为包括:语音、签名时序数据等具有动态变化特征的行为。这些行为可用于固定模式的静态生物特征验证(3.18)。

3.12

登记过程 enrolment processing

按照登记策略创建和存储生物特征参考(3.7)的行为。

3.13

外部采集的 externally-captured

通过卡外数据采集(3.10)获取的。

3.14

反馈机制 feedback mechanism

通过卡上状态字,将用于补充的详细错误、警告或进度信息通知卡上生物特征识别系统之外的装置的机制。

[ISO/IEC 17839-3:2016,定义 3.2]

3.15

内部采集的 internally-captured

通过卡上数据采集(3.10)获取的。

3.16

传感器 sensor

获取生物识别特征(3.1)并将其转换为信号(3.17)的装置。

3.17

信号 signal

模拟或数字输出的序列,其变化代表编码信息。

3.18

静态生物特征验证 static biometric verification

对被鉴别人的生理(即静态)特征或已登记的、预设的行为的生物特征验证(3.9)。

注 1: 生理特征包括人脸、指纹、虹膜、静脉等。

注 2: 已登记的、预设的行为包括:具有固定模式的步态、语音、签名时序数据等。

3.19

模板 template

构成结构化 BER-TLV 数据对象值字段的 BER-TLV 数据对象的集合。

注:“模板”是指一个已建立的数据对象值字段,不宜与已处理的生物特征数据(3.3)样本混淆。

[ISO/IEC 7816-4:2013,定义 3.58]

4 符号和缩略语

下列符号和缩略语适用于本文件。

AID:应用标识符(Application Identifier)

ASN.1:抽象语法记法一(Abstract Syntax Notation One)

AT:用于鉴别的控制引用模板(Control Reference Template for Authentication)

BER:ASN.1 的基本编码规则(Basic Encoding Rules of ASN.1)

BHT:生物特征数据头模板(Biometric Header Template)

CBEFF:公用生物特征交换格式框架(Common Biometric Exchange Formats Framework)

DF:专用文件(Dedicated File)

DO:BER-TLV 数据对象(BER-TLV Data Object)

ICC:集成电路卡(Integrated Circuit Card)

ID:标识符(Identifier)

MSE:管理安全环境(MANAGE SECURITY ENVIRONMENT)

OID:对象标识符(Object Identifier)

PBO:执行生物特征识别操作(PERFORM BIOMETRIC OPERATION)

RFU:留待(Reserved for Future Use by ISO/IEC JTC 1/SC 17)

TLV:标签-长度-值(Tag, Length, Value)

VIDO:验证信息数据对象(Verification Requirement Information Data Object)

VIT:验证信息模板(Verification Requirement Information Template)

5 生物特征验证及其相关过程的命令

5.1 概述

在 5.4 中介绍的执行生物特征识别操作(PBO)命令,描述了用于登记(将生物特征数据存储在 ICC 中)和验证(生物特征数据与 ICC 中存储的参考数据之间的比对)的生物特征操作命令。生物特征数据的存储和比对可按 GB/T 16649.4—2010 中规定的命令(例如:PUT DATA,用于存储的 UPDATE BINARY,用于比对的 VERIFY)实现。

5.2 静态生物特征验证过程命令

用于静态验证过程(参见附录 A)的命令应是 VERIFY 命令(见 GB/T 16649.4—2010)或执行生物特征识别操作(PBO)相关的操作命令,例如,5.4 中介绍的生物特征探针的比对。当使用 VERIFY 命令且外部已获取生物特征数据时,VERIFY 命令应包含作为生物特征探针的生物特征数据,其数据字段用于比对,编码在 6.1 和 6.2 定义。生物特征识别的算法标识符应是:

- 隐式已知的;
- 定义在用于鉴别的控制引用模板(AT)中的安全环境(SE)内;
- 定义在生物特征信息模板(见 GB/T 30266—2013)中的命令数据内;
- 定义在用于鉴别的控制引用模板(AT)中的命令数据内。

生物特征参考限定词是:

- 定义在用于鉴别的控制引用模板(AT)中的安全环境(SE)内;
- 定义在 VERIFY 或 PBO 命令中的 P2 参数;
- 定义在生物特征信息模板中的命令数据内(见 6.1);
- 定义在生物特征数据模板中的命令数据内(见 6.2);
- 定义在用于鉴别的控制引用模板(AT)中的命令数据内。

生物特征探针可被编码为 BER-TLV 数据对象(见表 9),存储于生物特征信息模板(见表 6 和表 7)或生物特征信息模板组模板(见表 8)中。

ICC 卡上或卡外获取的生物特征数据都可以进行比对。对于内部采集的生物特征探针的比对,宜通过 5.4.6 中的 PBO 命令,实现 ISO/IEC 17839-3 中规定的反馈机制。

5.3 动态生物特征验证过程命令

为获取挑战,应使用 GB/T 16649.4—2010 中定义的 GET CHALLENGE 命令或 5.4 中定义的 PBO 命令,挑战需要用户做出响应(参见附录 A)。

在 GB/T 16649.4—2010 中,P1 设置为‘00’表示未提供信息,例如,在发出命令之前已知生物特征识别算法。P1 的其他值为 RFU。

生物特征验证过程的挑战类型依赖于算法,例如,一个声纹短语或击键表达。如果挑战要求使用

GET CHALLENGE 命令,那么 GET CHALLENGE 命令的参数 P1 应标识出生物特征识别算法。如果挑战要求使用 PBO 命令,生物特征识别算法应是以下其中一种:

- 隐式已知的;
- 定义在用于鉴别的控制引用模板中的安全环境(SE)内。

相应的算法可通过 MSE 命令(例如 AT 的 SET 操作、命令数据字段中的 DO 用户限定词和 DO 引用算法)交替地选择使用。

当接收一个生物特征挑战后,EXTERNAL AUTHENTICATE 命令或 PBO 命令将被发送到 ICC 中。命令数据字段发送相关的生物特征探针。

5.4 执行生物特征识别操作命令

5.4.1 PBO 命令的通用定义

一个或多个 PBO 命令可用于生物特征验证及其相关过程,命令和响应见表 1 和表 2。PBO 命令按照 P1 所指示的值,启动各种类型的生物特征识别操作以及其他相关操作。

表 1 执行生物特征识别操作命令-响应对

命令和响应		含义
命令	CLA	在 ISO/IEC 7816-4:2013 的 5.4.1 中定义
	INS	‘2E’
	P1	功能编号和用例变量(见表 4)
	P2	见表 2
	L _c 字段	当 N _c 编码为 0 时不存在,N _c 编码大于 0 则存在
	命令数据字段	根据 P1 字段决定不存在或存在
	L _c 字段	当 N _c 编码为 0 时不存在,N _c 编码大于 0 则存在
响应	响应数据字段	根据 P1 字段决定不存在或存在
	SW1-SW2	在 GB/T 16649.4—2010 的表 5 和表 6 中定义,例如:‘6281’、‘6282’、‘6700’、‘6981’、‘6982’、‘6A81’、‘6A82’、‘6A83’

表 1 中,P1 表示与生物特征识别相关的单一操作,表 2 中,P2 以 GB/T 16649.4-2010 定义基本安全操作命令的相同方式对生物特征参考进行限制。

表 2 PBO 命令的 P2

P2								含 义
b8	b7	b6	b5	b4	b3	b2	b1	
0	0	0	0	0	0	0	0	无信息提供
0	—	—	—	—	—	—	—	全局生物特征参考(例如:MF 细节)
1	—	—	—	—	—	—	—	特定生物特征参考(例如:应用 DF 细节)
—	×	×	—	—	—	—	—	00(任何其他值为 RFU)
—	—	—	×	×	×	×	×	限定词,例如:生物特征参考号

PBO 命令可以优先于 MSE 命令,以设置合适的参数。例如:MSE 命令设置一个对安全环境(SE)进行鉴别的有效控制引用模板(AT)。当执行 PBO 命令时,该 SE 利用生物特征参考的限定词传送生

物特征识别用户验证的指示。

5.4.2 PBO 命令的操作

- 表 3 和表 4 列出的 PBO 操作的功能见下述解释。
- STORE BIOMETRIC REFERENCE
 - UPDATE BIOMETRIC REFERENCE
 - PBO 命令的 STORE BIOMETRIC REFERENCE 和 UPDATE BIOMETRIC REFERENCE 操作用于对外部采集的生物特征数据进行登记。
 - CAPTURE AND STORE BIOMETRIC REFERENCE
 - CAPTURE AND UPDATE BIOMETRIC REFERENCE
 - PBO 命令的 CAPTURE AND STORE BIOMETRIC REFERENCE 和 CAPTURE AND UPDATE BIOMETRIC REFERENCE 操作用于对内部采集的生物特征数据进行登记。
 - COMPARE BIOMETRIC PROBE
 - PBO 命令的 COMPARE BIOMETRIC PROBE 操作用于将外部采集的生物特征探针与生物特征参考进行比对。
 - CAPTURE AND COMPARE BIOMETRIC PROBE
 - PBO 命令的 CAPTURE AND COMPARE BIOMETRIC PROBE 操作用于将内部采集的生物特征探针与生物特征参考进行比对。
 - RETRIEVE BIOMETRIC REFERENCE
 - PBO 命令的 RETRIEVE BIOMETRIC REFERENCE 操作用于从 ICC 中检索生物特征参考。
 - GET BIOMETRIC CHALLENGE
 - PBO 命令的 GET BIOMETRIC CHALLENGE 操作用于在动态生物特征验证情况下，在 COMPARE BIOMETRIC PROBE 或 CAPTURE AND COMPARE BIOMETRIC PROBE 操作之前，获取生物特征识别挑战。
 - SET BIOMETRIC PARAMETER
 - CONTINUE CAPTURE
 - ABORT CAPTURE
 - PBO 命令的 SET BIOMETRIC PARAMETER、CONTINUE CAPTURE 和 ABORT CAPTURE 操作用于反馈机制。

表 3 PBO 命令与响应数据字段

操作	命令数据字段		响应数据字段	
STORE BIOMETRIC REFERENCE(见 5.4.3.1)		生物特征参考为：	—	无
	DO‘7F2E’	生物特征数据模板		
	DO‘7F60’	生物特征信息模板		
	DO‘7F61’	生物特征信息模板组模板		
UPDATE BIOMETRIC REFERENCE(见 5.4.3.1)		生物特征参考为：	—	无
	DO‘7F2E’	生物特征数据模板		
	DO‘7F60’	生物特征信息模板		
	DO‘7F61’	生物特征信息模板组模板		

表 3 (续)

操作	命令数据字段		响应数据字段	
CAPTURE AND STORE BIOMETRIC REFERENCE (见 5.4.3.2)	—	无	—	无
CAPTURE AND UPDATE BIOMETRIC REFERENCE (见 5.4.3.2)	—	无	—	无
COMPARE BIOMETRIC PROBE (见 5.4.5.1)	DO‘7F2E’ DO‘7F60’ DO‘7F61’	生物特征探针为:	—	无
		生物特征数据模板 生物特征信息模板 生物特征信息模板组模板		
CAPTURE AND COMPARE BIOMETRIC PROBE(见 5.4.5.2)	—	无	—	无
RETRIEVE BIOMETRIC REFERENCE(见 5.4.4)	—	无	DO‘7F60’ DO‘7F61’	生物特征参考为: 生物特征信息模板 生物信息模板组模板
GET BIOMETRIC CHALLENGE (见 5.4.5.1 和 5.4.5.2)	—	无	DO‘53’/ DO‘73’	生物特征挑战模板(原始的/构造的)
SET BIOMETRIC PARAMETER (见 5.4.6)	DO‘B1’	配置数据元的数据对象	—	无
CONTINUE CAPTURE(见 5.4.6)	—	无	—	无
ABORT CAPTURE (见 5.4.6)	—	无	—	无
<p>注 1: 生物特征数据模板 DO‘7F2E’在表 9 中定义。</p> <p>注 2: 生物特征信息模板 DO‘7F60’在表 6 和表 7 中定义。</p> <p>注 3: 生物特征信息模板组模板在表 8 中定义。</p> <p>注 4: 在生物特征信息模板 DO‘7F60’中嵌入的 DO‘B1’,作为配置数据元的数据对象在 GB/T 30266—2013 中定义。</p>				

P1 的 b8(Bit8)设置为 0 表示通用用例。P1 的 b8 设置为 1 表示为具体用例(见表 4)。P1 设置为‘00’和‘FF’表示 RFU。

表 4 PBO 命令的 P1 编码

P1								含 义
b8	b7	b6	b5	b4	b3	b2	b1	
0	×	×	×	×	×	×	×	通用用例
1	×	×	×	×	×	×	×	具体用例
×	0	0	0	0	0	1	0	STORE BIOMETRIC REFERENCE(存储生物特征参考)
×	0	0	0	0	0	1	1	UPDATE BIOMETRIC REFERENCE(修改生物特征参考)
×	0	0	0	0	1	0	0	CAPTURE AND STORE BIOMETRIC REFERENCE(采集并存储生物特征参考)
×	0	0	0	0	1	0	1	CAPTURE AND UPDATE BIOMETRIC REFERENCE(采集并修改生物特征参考)
×	0	0	0	0	1	1	0	COMPARE BIOMETRIC PROBE(比对生物特征探针)
×	0	0	0	0	1	1	1	CAPTURE AND COMPARE BIOMETRIC PROBE(采集并比对生物特征探针)
×	0	0	0	1	0	0	0	RETRIEVE BIOMETRIC REFERENCE(检索生物特征参考)
×	0	0	0	1	1	0	0	GET BIOMETRIC CHALLENGE(获取生物特征挑战)
×	0	0	0	1	1	0	1	SET BIOMETRIC PARAMETER(设置生物特征参数)
×	0	0	0	1	1	1	0	CONTINUE CAPTURE(继续采集)
×	0	0	0	1	1	1	1	ABORT CAPTURE(中止采集)
×	×	×	×	×	×	×	×	其他值留待

5.4.3 生物特征参考的登记

5.4.3.1 外部采集的生物特征数据登记

STORE BIOMETRIC REFERENCE 和 UPDATE BIOMETRIC REFERENCE 的 PBO 操作命令在表 3 和表 4 中定义,用于外部采集的生物特征数据的登记和卡上相关的生物特征信息以及生物特征参考结果的存储。

5.4.3.2 内部采集的生物特征数据登记

CAPTURE AND STORE BIOMETRIC REFERENCE 和 CAPTURE AND UPDATE BIOMETRIC REFERENCE 的 PBO 操作命令在表 3 和表 4 中定义,用于内部采集的生物特征数据的登记和卡上相关的生物特征信息以及生物特征参考结果的存储。

5.4.4 生物特征参考的检索

RETRIEVE BIOMETRIC REFERENCE 的 PBO 操作命令在表 3 和表 4 中定义,用于从卡上检索

生物特征参考。

5.4.5 生物特征探针的比对

5.4.5.1 外部采集的生物特征探针的比对

COMPARE BIOMETRIC PROBE 的 PBO 操作命令在表 3 和表 4 中定义,用于外部采集的生物特征探针与生物特征参考的比对。在动态生物特征验证过程中,表 3 和表 4 中定义的 GET BIOMETRIC CHALLENGE 的 PBO 操作命令用于在 COMPARE BIOMETRIC PROBE 操作之前获取生物特征识别挑战。

5.4.5.2 内部采集的生物特征探针的比对

CAPTURE AND COMPARE BIOMETRIC PROBE 的 PBO 操作命令在表 3 和表 4 中定义,用于内部采集的生物特征探针与生物特征参考的比对。在动态生物特征验证过程中,表 3 和表 4 中定义的 GET BIOMETRIC CHALLENGE 的 PBO 操作命令用于在 CAPTURE AND COMPARE BIOMETRIC PROBE 操作之前获取生物特征识别挑战。

5.4.6 生物特征采集过程中的反馈机制

由于在生物特征登记或比对过程中采集生物特征数据时需要用户交互,以及无法预测时间行为的原因,因此,宜使用 ISO/IEC 17839-3 规定的反馈机制。在表 3 和表 4 中定义的 PBO 命令 SET BIOMETRIC PARAMETER、CONTINUE CAPTURE 和 ABORT CAPTURE 等用于反馈机制。

表 5 给出了 SET BIOMETRIC PARAMETER 的 PBO 操作命令细节,该命令用于 ISO/IEC 17839-3 中定义的应用超时等级管理。

表 5 利用 SET BIOMETRIC PARAMETER 的 PBO 操作命令设置应用超时等级

操作	P1	命令数据字段		响应数据字段	
SET BIOMETRIC PARAMETER (设置应用超时等级)	'0D'	DO'89'	应用超时等级见 GB/T 30266—2013 如果数据对象为空,那么应用超时等级 是隐式已知的	—	无

6 数据元

6.1 生物特征信息模板

生物特征信息模板提供了与生物特征数据相关的描述性信息。它是在验证过程之前卡对检索命令做出的响应。表 6 和表 7 定义了生物特征信息的数据对象。

生物特征信息模板可以包括生物特征数据(见 6.2)。在进行卡外比对时,因为卡外验证需要同时具有生物特征参考及其信息,所以生物特征参考宜包含在生物特征信息模板中。在卡上比对和卡外系统需要某个生物特征参考相关信息的情况下,无生物特征数据的生物特征信息模板和生物特征参考宜分开存储在 ICC 中,以防该生物特征参考被检索。

表 6 生物特征信息模板中的生物特征信息 DOs(隐式标签分配编码)

标签	长度	值			状态
‘7F60’	变长	生物特征信息模板			
		标签	长度	值	
		‘80’	1	生物特征验证的引用算法	可选项
		‘83’	1	生物特征验证的引用数据限定词	可选项
		‘A0’	变长	留待,用于本文件中定义的生物特征信息 DOs	可选项
		‘06’	变长	标签分配机构(见 ISO/IEC 7816-6): ——对象标识符(OID,编码参见 GB/T 26231 中的规定);	如果‘A1’存在,这些数据对象中的其中一个 是必选的
		‘41’	变长	——国家编码(编码参见 GB/T 2659 中的规定)和可选的国家数据;	
		‘42’	变长	——发卡机构标识码(编码和注册遵循 GB/T 15694.1 中的规定)和可选的发卡机构数据;	
		‘4F’	变长	——应用标识符(AID,编码在 GB/T 16649.4—2010 中的规定)。 默认标签分配机构为 SAC/TC 28/SC 17。	
		‘A1’	变长	由标签分配机构定义的生物特征信息 DOs(必选指示,见上) TLV 编码的实体格式见 ISO/IEC 19785-3 中的规定	必选项,如果‘A0’不存在
				标签	长度
		‘8x’/‘Ax’ ‘9x’/‘Bx’	变长 变长	由标签分配机构定义的 DOs (原始的/构造的) (原始的/构造的)	数据对象相关
‘5F2E’/‘7F2E’	变长	生物特征数据(见 6.2)			必选项,生物特征探针或在卡外比对情况下的被检索的生物特征参考

表 7 生物特征信息模板中的生物特征信息 DOs(显式标签分配编码)

标签	长度	值					状态
‘7F60’	变长	生物特征信息模板					
		标签	长度	值			
		‘80’	1	生物特征验证的引用算法			可选项
		‘83’	1	生物特征验证的引用数据限定词			可选项
		‘A0’	变长	留待,用于本文件中定义的生物特征信息 DOs			可选项
		‘A1’	变长	其他标准定义的生物特征信息 DOs			必选项,如果‘A0’不存在
				标签	长度	值	
				‘78’	变长	兼容标签分配机构	
						标签	长度
						‘06’	变长
						对象标识符 (OID, 编码参见 GB/T 26231 中的规定)	
						‘41’	变长
						国家编码 (编码参见 GB/T 2659 中的规定) 和可选的国家数据	
						‘42’	变长
						发卡机构标识码 (编码和注册遵循 GB/T 15694.1 中规定) 和可选的发卡机构数据	
						‘4F’	变长
						应用标识符 (AID, 编码在 GB/T 16649.4—2010 中规定)	
				‘70’	变长	由标签分配机构定义的生物特征信息 DOs	
						‘B1’	变长
				生物特征信息 DOs 符合 GB/T 30266—2013 中规定			
		‘5F2E’/ ‘7F2E’	变长	生物特征数据(见 6.2)			必选项,生物特征探针或在卡外比对情况下的被检索的生物特征参考

注: 如果 DO‘A1’下的兼容标签分配机构 DO‘78’不存在,则默认的标签分配机构为 SAC/TC 28/SC 17。

在显式标签分配编码的情况下,附录 C 中所示的标签可以存在于生物特征信息模板中(见表 7)。

如果同一应用程序中存在多个生物特征信息模板,则应将其分组如表 8 所示。
其他的生物特征信息模板示例参见附录 B。

表 8 生物特征信息模板组模板

标签	长度	值			状态
‘7F61’	变长	生物特征信息模板组模板			
		标签	长度	有效值	
		‘02’	变长	组中的生物特征信息模板数	必选项
		‘7F60’	变长	生物特征信息模板 1	有条件的
		
		‘7F60’	变长	生物特征信息模板 <i>n</i>	有条件的

6.2 生物特征数据

生物特征数据按 ISO/IEC 7816-6 中规定的 DO‘5F2E’或 DO‘7F2E’进行编码。表 9 表示的生物特征数据 DOs 可包含在生物特征信息模板(见 6.1)中。

表 9 生物特征数据 DOs

标签	长度	值			状态
‘7F2E’	变长	生物特征数据模板			
		标签	长度	值	
		‘80’/‘A0’	变长	对持卡人进行提示的挑战, DO ‘A0’ 见表 10	可选项, 针对动态生物特征验证
		‘5F2E’	变长	生物特征数据	如果使用了模板, 至少一个 DOs 存在。同一个标签号可能在模板中多次出现
		‘81’/‘A1’	变长	标准化格式的生物特征数据(原始的/构造的)	
		‘82’/‘A2’	变长	专有格式的生物特征数据(原始的/构造的)	
		‘83’	1	生物特征参考限定词	如果生物特征数据模板不在生物特征信息模板中, 则该 DO 可能存在

如表 9 所示,生物特征数据可以分解为一部分为标准化格式,另一部分为专有格式,因此,使用专有格式的生物特征数据可以实现更优性能和/或调用内部数据。标准化格式和专有格式的生物特征数据的使用如图 1 所示。本例分别描述了嵌入卡中的两种引用算法。两种算法属于相同的生物特征类型,例如指纹,但都可以通过使用不同的专有格式和标准化格式的生物特征数据来计算验证结果。当接口设备仅支持算法 A 时,可以根据 ICC 返回的引用算法确定 VERIFY 命令的数据字段中的生物特征探针。

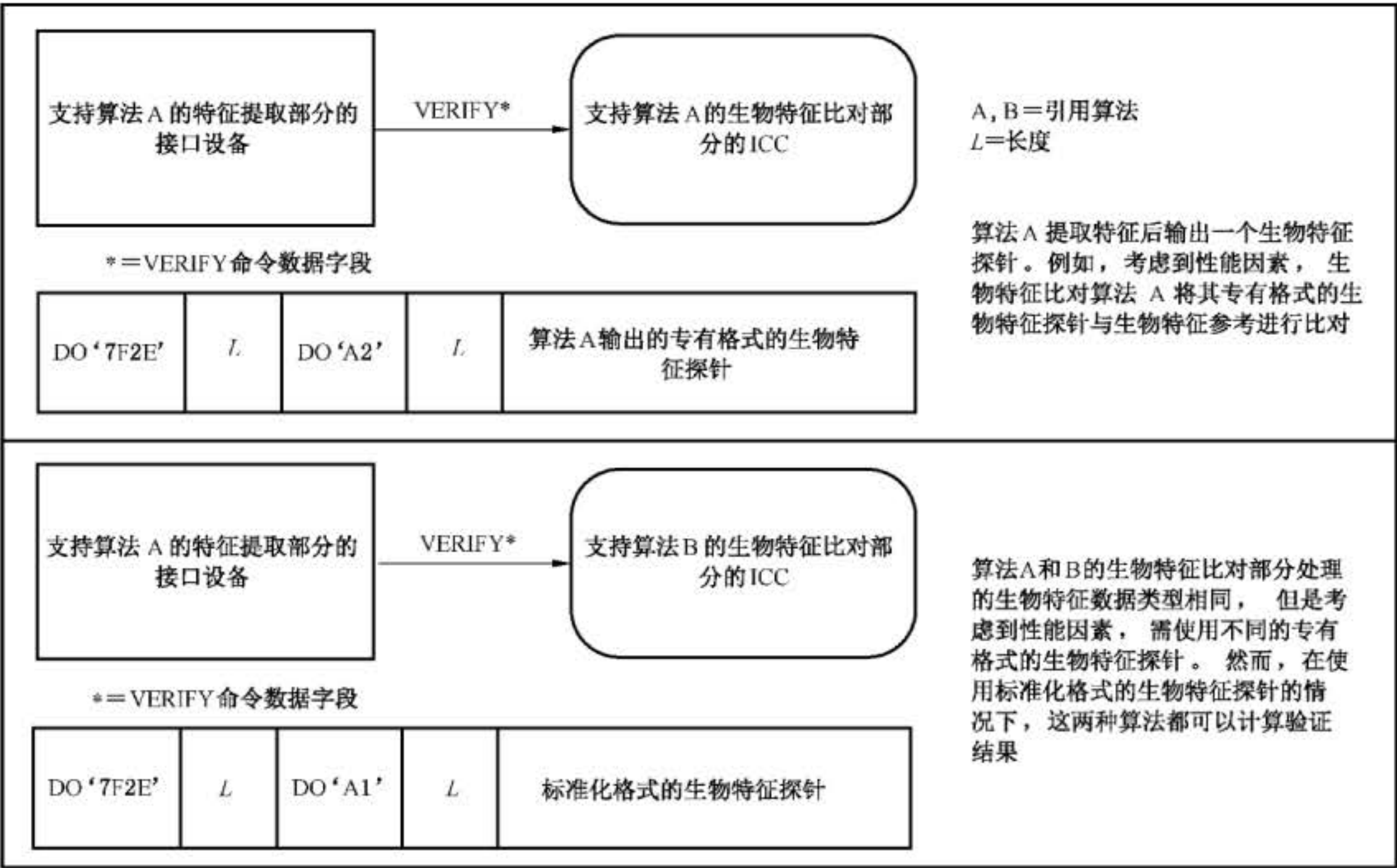


图 1 使用标准化和专有格式的生物特征数据

持卡人生物特征参考和标准化格式的生物特征探针的结构和编码依赖于生物特征类型(例如,人脸特征、指纹),这超出了本部分的范围。

在动态生物特征验证过程中的用于对持卡人进行提示的生物特征挑战,宜按照 DO 'A0' 或 DO '80' 进行编码(见 5.3)。生物特征挑战模板的样本如表 10 所示。

表 10 生物特征挑战模板

标签	长度	值		
'A0'	变长	挑战模板		
		标签	长度	值
		'90'	变长	挑战限定词 '00' = 未提供信息(未指定); '01' = UTF8 编码(默认); 其他,留待
		'80'	变长	挑战

6.3 验证信息

6.3.1 目的

当前的验证信息可由以下对象提供：
——验证信息数据对象 VIDO(标签 '96', 原始的);或

——验证信息模板 VIT(标签‘A6’,构造的)。

VIDO 或 VIT 可包含在 GB/T 16649.4—2010 定义的相应 DF 文件控制信息中,或可以存储在包含扩展文件控制信息的 EF 中。为此,在用于 DF 的文件控制参数(FCP)模板 DO‘62’下的 DO‘87’,作为包含扩充文件控制信息的 EF 标识符,在 GB/T 16649.4—2010 中定义。VIDO 和 VIT 包含使用生物特征参考的启用/禁用验证要求的信息。为了切换该验证信息状态,可使用在 GB/T 16649.4—2010 中定义的 ENABLE VERIFICATION REQUIREMENT/DISABLE VERIFECATION REQUIREMENT 命令。VIDO 和 VIT 还包含指示是否允许(可用/不可用)进一步验证的信息。

当设置了生物特征验证的最大尝试次数,并且连续生物验证失败的次数达到最大值时,生物特征参考是不可用的。为了将不可用状态切换到可用状态,如果安全属性允许,则可以使用 RESET RETRY COUNTER 命令。

注: P2 字段是 ENABLE VERIFICATION REQUIREMENT 或 DISABLE VERIFECATION REQUIREMENT 命令的限定词,即引用数据或秘密号。在当前安全环境中,用于鉴别的有效控制引用模板(AT)的用户限定词可以指示用户鉴别是基于密码(秘密)还是基于生物特征的(生物特征参考)。在当前 SE 中可以通过 MANAGE SECURITY ENVIRONMENT 命令来处理此用户限定词。

6.3.2 验证信息数据对象(VIDO)

验证信息数据对象(VIDO)中的值字段的第 1 个字节表示生物特征参考的验证信息(见表 11 和表 12)。该字节 b8 位表示启用/禁用生物特征参考(见表 12)的验证信息(如果存在),该信息被 VIDO 值字段第 3 个字节引用。b8 后面的每个比特位表示生物特征参考的验证信息,并依次被第 3 个字节后面的每个字节引用。

VIDO 值字段中的第 2 个字节表示可用的生物特征参考(见表 13)。该字节的 b8 位表示被 VIDO 值字段第 3 个字节引用的生物特征参考可用/不可用(如果存在)。b8 后面的每个比特位表示生物特征参考的验证信息,并依次被第 3 个字节后面的每个字节引用。

生物特征参考限定词在 VIDO 的值字段中最多为 8 个。当生物特征参考限定词的数量小于 8 时,从第 1 字节和第 2 个字节的 b8 位开始对应数量的比特位有效。

表 11 验证信息 DO 的编码

标签	长度	值			
		第 1 个字节	第 2 个字节	第 3 个字节	...
‘96’	3~10	验证信息字节	可用生物特征参考字节	生物特征参考限定词 对应于第 1 个字节 和第 2 个字节的 b8 位	...

表 12 验证信息字节的编码

b8	b7	b6	b5	b4	b3	b2	b1	含义
1	—	—	—	—	—	—	—	使用第 3 个字节(如果存在)引用的生物特征参考的启用验证信息
—	1	—	—	—	—	—	—	使用第 4 个字节,其他同上
—	—	1	—	—	—	—	—	使用第 5 个字节,其他同上
—	—	—	1	—	—	—	—	使用第 6 个字节,其他同上
—	—	—	—	1	—	—	—	使用第 7 个字节,其他同上

表 12 (续)

b8	b7	b6	b5	b4	b3	b2	b1	含义
—	—	—	—	—	1	—	—	使用第 8 个字节,其他同上
—	—	—	—	—	—	1	—	使用第 9 个字节,其他同上
—	—	—	—	—	—	—	1	使用第 10 个字节,其他同上

表 13 可用生物特征参考字节的编码

b8	b7	b6	b5	b4	b3	b2	b1	含义
1	—	—	—	—	—	—	—	由第 3 个字节(如果存在)引用可用的生物特征参考
—	1	—	—	—	—	—	—	使用第 4 个字节,其他同上
—	—	1	—	—	—	—	—	使用第 5 个字节,其他同上
—	—	—	1	—	—	—	—	使用第 6 个字节,其他同上
—	—	—	—	1	—	—	—	使用第 7 个字节,其他同上
—	—	—	—	—	1	—	—	使用第 8 个字节,其他同上
—	—	—	—	—	—	1	—	使用第 9 个字节,其他同上
—	—	—	—	—	—	—	1	使用第 10 个字节,其他同上

6.3.3 验证信息模板(VIT)

验证信息模板用于支持超过 8 个的生物特征参考限定词(见表 14)。它由一个或多个基于生物特征的鉴别模板 DO‘A4’组成。基于生物特征的鉴别模板 DO‘A4’,由验证要求数据对象 DO‘81’、可用的生物特征参考限定词数据对象 DO‘82’和生物特征参考限定词数据对象 DO‘83’组成。DO‘81’、DO‘82’和 DO‘83’最多存在于 DO‘A4’中一次。其他数据对象可存在于 DO‘A4’中。

表 14 验证信息模板的编码

标签	长度	值			
‘A6’	变长	验证信息模板			
		标签	长度	值	
		‘A4’	变长	基于生物特征的鉴别模板	
				标签	长度
				值	
				‘81’	1
				验证要求数据对象: ——‘00’:禁用验证要求; ——‘01’:启用验证要求; ——其他值,留待	
				‘82’	1
				可用的生物特征参考限定词数据对象: ——‘00’:不可用的生物特征参考限定词; ——‘01’:可用的生物特征参考限定词; ——其他值,留待	
				‘83’	1
				生物特征参考限定词数据对象	
		‘A4’	变长	基于生物特征的鉴别模板	

附录 A
(资料性附录)
生物特征验证过程

A.1 登记和验证过程

登记过程的通用体系结构(示意图)如图 A.1 和图 A.2 所示。

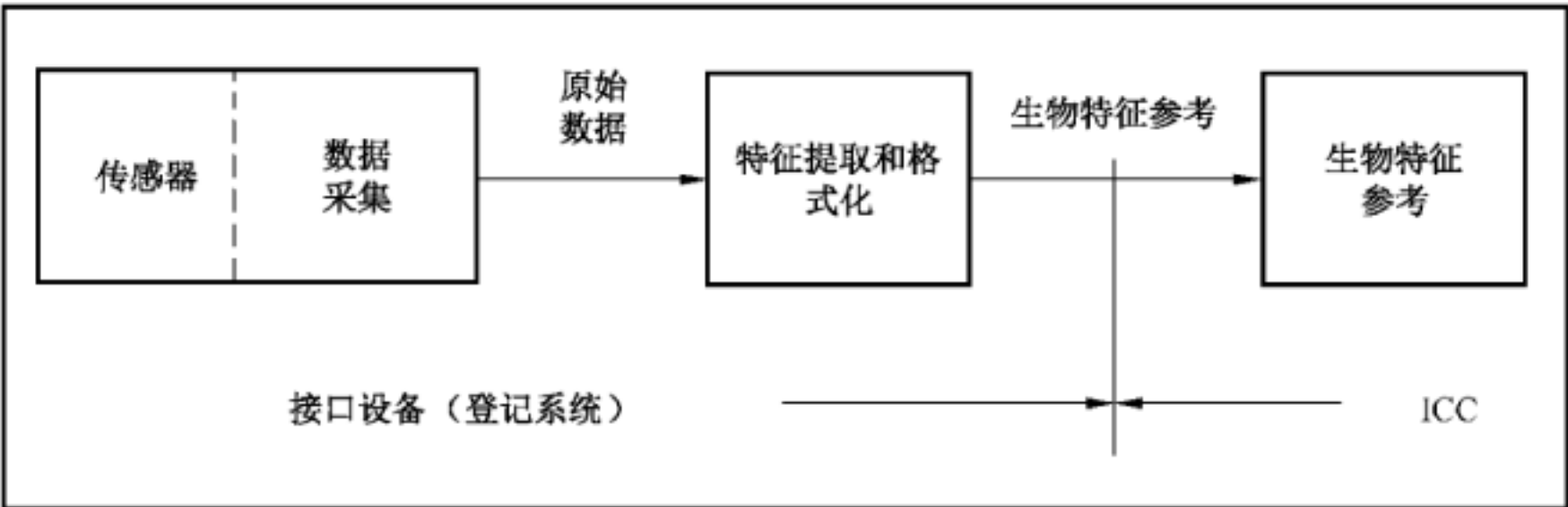


图 A.1 基于外部采集生物特征数据的登记通用体系结构

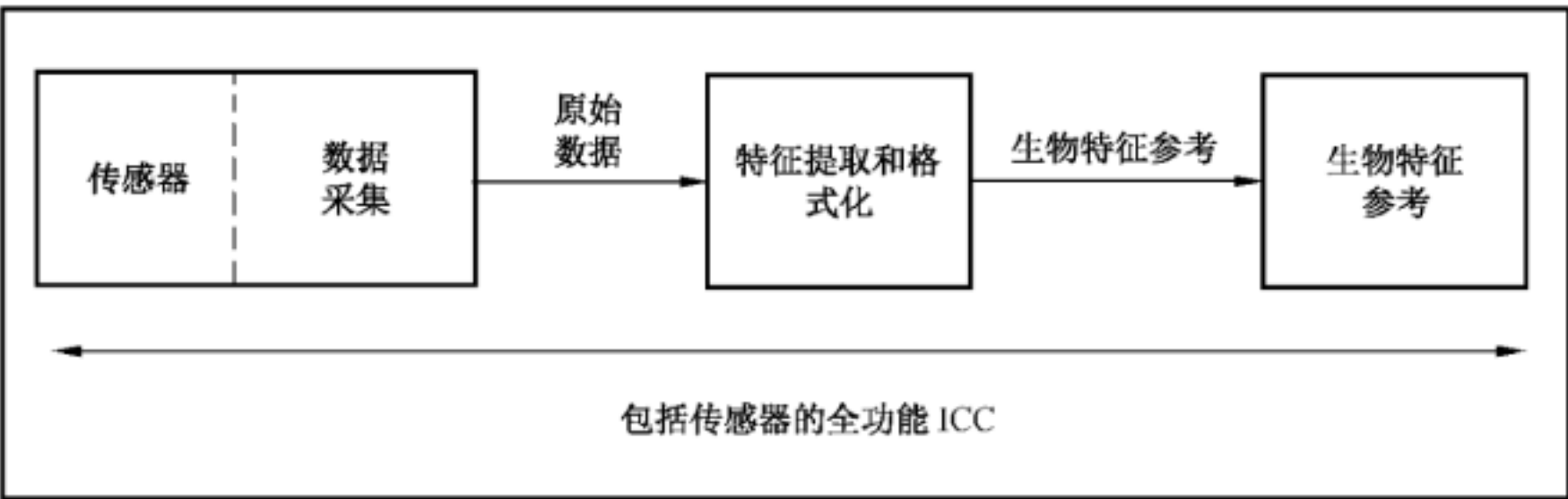


图 A.2 基于内部采集生物识别数据的登记通用体系结构

如图 A.1 所示,在对外部采集的生物特征数据登记时,由于生物特征样本的数据量较大,通常在卡外进行处理。处理过程是进行生物特征项的提取和格式化,为后续使用。在登记过程或后续阶段,生物特征参考数据将被以一种安全的方式发送到卡进行存储和后续使用。

如图 A.2 所示,包含传感器和数据采集模块的 ICC,能够登记内部采集的生物特征数据。此种情况下,整个生物特征参考数据的采集、处理和存储都在卡上进行。

对于这两种方案,可在登记过程中存储与生物特征验证相关的参数。

生物特征参数可存储在卡上:

- 在卡个人化阶段;
- 发卡阶段。

GB/T 30266—2013 给出了一个简化的验证流程。

A.2 生物特征验证方法分类

生物特征模式可分为两种类型。

第一类(A类)特征的主要特点为：

- 唯一的,不可修改的；
- 可选的,如果存在同类的几个样本(如拇指、食指等)；
- 公共的,如果需要采集或测量各种生物特征(如人脸、耳型、指纹),即各种生物特征探针和卡之间建立可信通道。

第二类(B类)特征的主要特点为：

- 唯一的,但可修改的；
- 基于挑战的,如动态验证。

A类生物特征示例：

- 耳廓；
- 人脸特征；
- 指型；
- 指纹；
- 手型；
- 虹膜；
- 掌纹；
- 视网膜；
- 静脉。

B类生物特征示例：

- 击键；
- 唇动；
- 签名图像；
- 声纹；
- 笔迹(签名)。

考虑到卡和设备之间存在不同的信息交换,采用如下分类：

- 静态生物特征验证,使用A类和B类；
- 动态生物特征验证,使用B类。

图 A.3 和图 A.4 说明了在卡上比对和决策处理生物特征的情况下,静态和动态生物特征验证之间的差别。

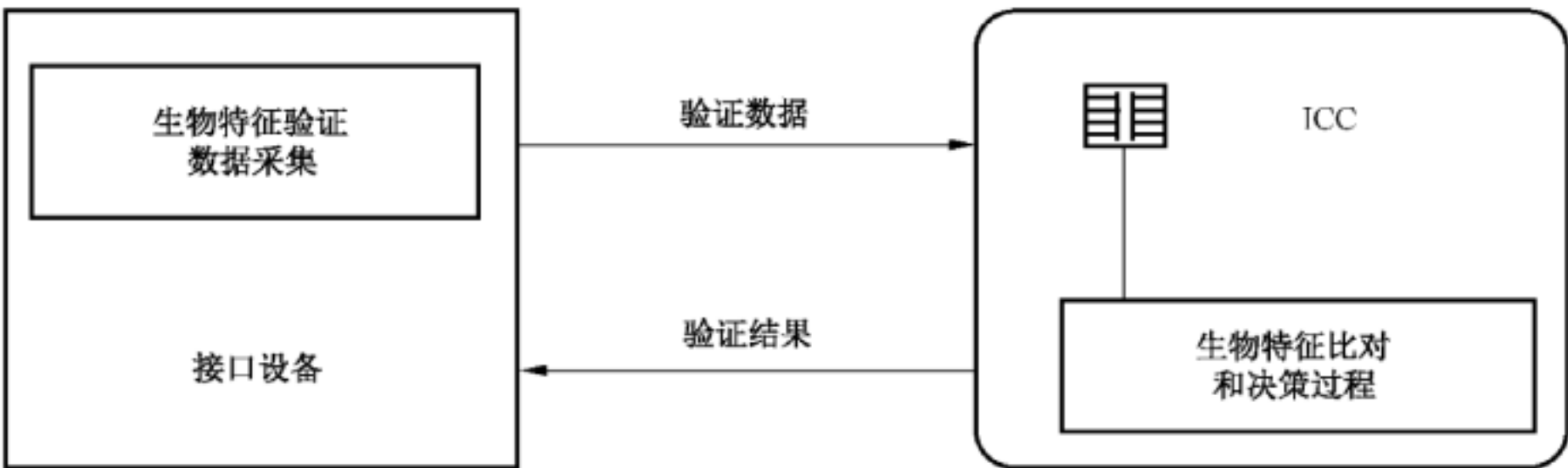


图 A.3 基于卡上比对的静态生物特征验证过程示例



图 A.4 基于卡上比对的动态生物特征验证过程示例

图 A.5 是基于卡上生物特征识别系统,使用 PBO 命令的动态生物特征验证示例。

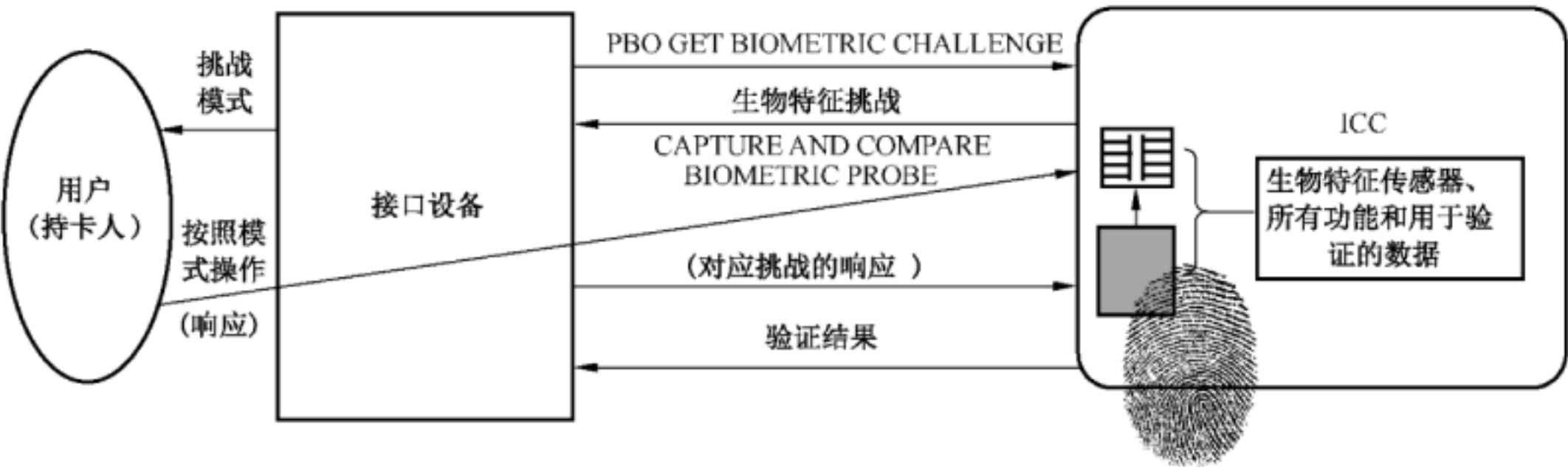


图 A.5 基于卡上生物特征识别系统,使用 PBO 命令的动态生物特征验证过程示例

附录 B
(资料性附录)
生物特征信息数据对象示例

本附录给出了基于公用生物特征交换格式框架(CBEFF)的生物特征信息数据,基于 TLV 的实体格式见 ISO/IEC 19785-3。

在验证之前,可以从 ICC 提供的详细数据中检索出相关的信息,在验证过程中,外部可获得该详细数据。表 B.1 为生物特征信息模板组模板的示例。模板组模板内可包含几个生物特征信息模板。其中一个生物特征信息模板可包含 ISO/IEC 19785-3 中基于 TLV 实体格式的生物特征信息。

对于标准化结构的生物特征探针,如果其后面存在厂商定义的特定结构的生物特征探针,那么宜使用嵌套的 BHT 结构,如表 B.1 所示。

表 B.1 含有嵌套 BHT 结构的生物特征信息模板,适用于生物特征探针的标准化格式和专有格式(示例)

标签	长度	值						
‘7F60’	变长	生物特征信息模板						
		标签	长度	值				
		‘80’	1	引用算法				
		‘83’	1	引用数据限定词				
		‘A1’	变长	BHT（等级 1）				
				标签	长度	值		
				通用 DOs, 见 ISO/IEC 19785-3		
				‘A1’	变长	BHT 1（等级 2）		
						标签	长度	值
						‘87’	2	生物特征探针格式所有者, 例: ISO/IEC JTC 1/SC 37 中的格式所有者标识符
						‘88’	2	生物特征探针格式类型, 由格式所有者定义
				‘A2’	变长	BHT 2（等级 2）		
						标签	长度	值
						‘87’	2	生物特征探针格式所有者, 例如卡商
						‘88’	2	生物特征探针格式类型, 由格式所有者定义

对于多种生物特征项(多模态或组合生物特征)验证的情况,为了访问指定的数据或密钥,需要通过使用包含嵌套生物特征信息模板的组合模板,并发送多个 VERIFY 命令或 PBO 命令完成验证。如表 B.2 所示,隶属于相关联的受保护对象的安全属性(见 GB/T 16649.4—2010),定义了宜被成功验证的生物特征项组合。

表 B.2 包含嵌套生物特征信息模板的模板组模板,适用于含有各自生物特征参考数据
限定词的多个生物特征探针(示例)

标签	长度	值								
‘7F61’	变长	生物特征信息模板组模板								
		标签	长度	值						
		‘02’	1	‘02’=生物特征信息模板个数						
		‘7F60’	变长	生物特征信息模板 1						
				标签	长度	值				
				‘80’	1	引用算法				
				‘83’	1	引用数据限定词				
				‘A1’	变长	BHT				
						标签	长度	值		
							
						‘81’	1~3	生物特征类型,例如指纹		
						‘82’	1	生物特征子类型,例如右手食指指纹		
						‘87’	2	生物特征探针格式所有者		
						‘88’	2	生物特征探针格式类型,由格式所有者定义		
		‘7F60’	变长	生物特征信息模板 2						
				标签	长度	值				
				‘80’	1	引用算法				
				‘83’	1	引用数据限定词				
				‘A1’	变长	BHT				
						标签	长度	值		
							
						‘81’	1~3	生物特征类型,例如指纹		
						‘82’	1	生物特征子类型,例如左手食指指纹		
						‘87’	2	生物特征探针格式所有者		
						‘88’	2	生物特征探针格式类型,由格式所有者定义		

附 录 C
(资料性附录)

生物特征信息模板中数据对象的标签列表

表 C.1 给出了生物特征数据对象的标签列表,详细说明见 CBEFF(见 ISO/IEC 19785-3 规定的基于 TLV 格式的实体格式)。在生物特征处理过程中,这些标签用于将详细的信息引用到生物特征信息模板(见表 6 和表 7)中。

表 C.1 生物特征信息模板中 DOs 的标签列表

标签	生物特征数据对象	状态
‘53’/‘73’	生物特征负载(原始的/构造的)	可选项
‘80’	生物特征验证的引用算法	可选项
‘83’	引用数据限定词	可选项
‘A0’	留待,用于本文件中定义的生物特征信息 DOs	可选项
‘A1’	其他标准定义的生物特征信息 DOs	必选项,如果‘A0’不存在
仅用于 DO‘A1’		
‘78’	兼容标签分配机构	必选项,如果‘A1’存在
‘70’	生物特征信息 DOs 由标签分配机构说明	可选项
仅用于 DO‘78’		
‘06’	对象标识符(OID,编码参见 GB/T 26231 中的规定)	上述选择至多一种
‘41’	国家编码(编码参见 GB/T 2659 中的规定)和可选的国家数据	
‘42’	发卡机构标识码(编码和注册在 GB/T 15694.1 中规定)	
‘4F’	应用标识符(AID,编码在 GB/T 16649.4-2010 中规定)	
仅用于 DO‘70’(见 ISO/IEC 19785-3)		
‘80’	实体数据头版本	必选项(若无,使用默认值)
‘81’	生物特征类型	可选项
‘82’	生物特征子类	可选项,只能用生物特征类型
‘83’	创建时间(年月日)	可选项
‘84’	创建人	可选项
‘85’	有效期(年月日)	可选项
‘86’	产品 ID(产品所有者和产品类型的关联,标识创建生物特征参考的产品)	可选项
‘87’	格式所有者(生物特征数据的格式所有者)	必选项,如果‘A1’存在
‘88’	格式类型(格式所有者指定的生物特征数据的格式类型)	必选项,如果‘A1’存在
‘90’	索引(用于在卡外的应用环境中引用此生物数据集的唯一标识符)	可选项
‘91’/‘B1’	生物特征匹配算法参数(原始的/构造的)	可选项

参 考 文 献

- [1] GB/T 2659 世界各国和地区名称代码
 - [2] GB/T 26231 信息技术 开放系统互连 对象标识符(OID)的国家编号体系和操作规程
 - [3] ISO/IEC 7816(all parts) Identification cards—Integrated circuit cards
 - [4] ISO/IEC 7816-1 Identification cards—Integrated circuit cards—Part 1: Cards with contacts—Physical characteristics
-

中 华 人 民 共 和 国
国 家 标 准
识别卡 集成电路卡
第 11 部分:通过生物特征识别
方法的身份验证

GB/T 16649.11—2019

*

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(100029)
北京市西城区三里河北街 16 号(100045)

网址:www.spc.org.cn

服务热线:400-168-0010

2019 年 7 月第一版

*

书号: 155066 • 1-63238

版权专有 侵权必究



GB/T 16649.11—2019