



# 中华人民共和国国家标准

GB/T 41815.2—2022

## 信息技术 生物特征识别呈现 攻击检测 第2部分：数据格式

Information technology—Biometric presentation attack detection—  
Part 2:Data formats

(ISO/IEC 30107-2:2017,MOD)

2022-10-12发布

2023-05-01实施

国家市场监督管理总局  
国家标准化管理委员会 发布

## 目 次

前言 .....	I
引言 .....	II
1 范围 .....	1
2 规范性引用文件 .....	1
3 术语和定义 .....	1
4 符合性 .....	1
5 数据元素 .....	2
<b>5.1 概述</b> .....	2
<b>5.2 PAD 输出</b> .....	2
<b>5.3 PAD 输入</b> .....	4
附录 A (规范性)标准格式 .....	7
附录 B(资料性) PAD 编码示例 .....	17
参考文献 .....	19

## 前 言

本文件按照GB/T 1.1—2020《标准化工作导则第1部分：标准化文件的结构和起草规则》的规定起草。

本文件是GB/T 41815《信息技术 生物特征识别呈现攻击检测》的第2部分。GB/T 41815已经发布了以下部分：

- 第1部分：框架；
- 第2部分：数据格式；
- 第3部分：测试与报告。

本文件修改采用ISO/IEC 30107-2:2017《信息技术. 生物特征识别呈现攻击检测第2部分：数据格式》。

本文件与ISO/IEC 30107-2:2017的技术差异及其原因如下：

- 用规范性引用的GB/T 5271.37替换了ISO/IEC 2382—37(见第3章),增加可操作性；
- 用规范性引用的GB/T 41815.1替换了ISO/IEC 30107-1(见第3章),以适应我国的技术条件,增加可操作性；
- 用规范性引用的GB/T 16262.1替换了ISO/IEC 8824-1(见附录A.1.1),以适应我国的技术条件,增加可操作性；
- 用规范性引用的GB/T 16263.1替换了ISO/IEC 8825-1(见附录A.1.1、附录A.1.3),以适应我国的技术条件,增加可操作性。

本文件做了下列编辑性改动：

- 增加了5.2.2、5.2.3、5.2.5、5.2.6、5.3.8的注。

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专利的责任。

本文件由全国信息技术标准化技术委员会(SAC/TC 28)提出并归口。

本文件起草单位：中国电子技术标准化研究院、云从科技集团股份有限公司、上海商汤智能科技有限公司、厦门市美亚柏科信息股份有限公司、武汉虹识技术有限公司、北京旷视科技有限公司、深圳爱酷智能科技有限公司、福州数据技术研究院有限公司、广东九联科技股份有限公司、广州麦仑信息科技有限公司、杭州海康威视数字技术股份有限公司、惠州学院、蚂蚁科技集团股份有限公司、新大陆数字技术股份有限公司、北京曙光易通技术有限公司、北京中科虹霸科技有限公司、杭州景联文科技有限公司、哈尔滨理工大学、广州广电运通金融电子股份有限公司、北京集创北方科技股份有限公司、上海依图网络科技有限公司、西安凯虹电子科技有限公司、深圳市铭图创新科技有限公司、北京万里红科技股份有限公司、上海点与面智能科技有限公司。

本文件主要起草人：钟陈、史春腾、李军、蒋慧、陈晨、陈子泮、王文峰、宋继伟、刘倩颖、易开军、梅敬青、杨春林、郑文强、何强、崔峰科、彭晋、王…、任文奇、黄剑锋、林冠辰、蔡春水、于雪平、李星光、刘云涛、宋方方、罗中良、张亚浩、张玮、樊磊、赵春昊、胥建民、李清顺、张小亮、程治国、蒋燕、全嫚丽、罗恒。

## 引 言

以可能干扰生物特征识别系统的预期策略的方式向生物特征采集子系统呈现假体或人体特征的过程称为呈现攻击。GB/T 41815关注用于呈现攻击的自动检测机制。这些机制被称作呈现攻击检测(PAD)机制。

本文件构建了用于传达呈现攻击检测方法类型和呈现攻击检测方法结果的通用数据格式。本文件规定了在呈现攻击检测数据格式中数据元素的含义，见第5章。其中包括基于ASN.1中可扩展规范的带标记的二进制PAD数据格式，见附录A中 A.1；基于XML模式定义的文本PAD数据格式，见附录A中 A.2。规范性附录A包括正式的编码规范，资料性附录B给出了编码示例。

GB/T 41815《信息技术生物特征识别呈现攻击检测》规定了生物特征识别领域呈现攻击检测相关的框架、数据格式、测试相关的内容，以便于对呈现攻击检测功能的设计及其能力的评估。GB/T 41815拟由三个部分构成。

- 第1部分：框架。目的在于建立生物特征识别系统中呈现攻击检测相关的整体框架。
- 第2部分：数据格式。目的在于规范呈现攻击检测相关的数据格式。
- 第3部分：测试与报告。目的在于明确呈现攻击检测能力评估时需要考虑的各种因素以及评估原则和方法。

对呈现攻击检测相关对象进行标准化，需要首先从整体上明确呈现攻击检测框架以指导对攻击的分类及工具的定义，其次为了将相关数据元素进行交换和共享，需要定义明确、统一的数据格式，最后在对呈现攻击检测能力进行评估时需要明确测试对象、测试环境以及测试指标，指导对呈现攻击检测能力进行科学、客观的评估。

# 信息技术 生物特征识别呈现 攻击检测 第2部分：数据格式

## 1 范围

本文件规定了在生物特征识别中使用二进制格式和可扩展标记语言(XML)表示呈现攻击检测所使用具体机制以及检测结果的可用于交换的通用数据格式。

本文件适用于规范不同应用领域中传感器采集生物特征识别特性时涉及的与呈现攻击检测相关的数据。

本文件不适用于规范呈现攻击检测数据在存储和传输过程中关于真实性、完整性和机密性相关信息。

注：虽然解决安全问题超出了本文件的范围，但可见GB/T28826.1,通过将PAD数据编码为包含可选安全块的生物特征信息记录来保护PAD数据。

## 2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 5271.37 信息技术 词汇 第37部分：生物特征识别(GB/T 5271.37—2021,ISO/IEC 2382—37:2017,MOD)

GB/T 16262.1 信息技术抽象语法记法一(ASN.1) 第1部分：基本记法规范(GB/T 16262.1—2006,ISO/IEC 8824-1:2002,IDT)

GB/T 16263.1 信息技术 ASN.1 编码规则 第1部分：基本编码规则(BER)、正则编码规则(CER)和非典型编码规则(DER)规范(GB/T 16263.1—2006,ISO/IEC 8825-1:2002,IDT)

GB/T 41815.1 信息技术生物特征识别呈现攻击检测第1部分：框架(GB/T 41815.1—2022,ISO/IEC 30107-1:2016,IDT)

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

注：GB/T 28826.1—2012 信息技术 公用生物特征识别交换格式框架 第1部分：数据元素规范(ISO/IEC 19785-1:2006,MOD)

ISO 80000(所有部分)量和单位(Quantities and units)

## 3 术语和定义

GB/T 5271.37和GB/T 41815.1界定的术语和定义适用于本文件。

## 4 符合性

如果呈现攻击检测(PAD)数据块分别满足第5章和附录A中 A.1 或 A.2 的相关要求，则它符合本

文件。

## 5 数据元素

### 5.1 概述

第5章包含了对于由PAD子系统产生的并由可信系统使用的数据的描述。此类数据可能会在子系统的任何处理环节产生。因此，生物特征样本可用的PAD数据可能在生物特征样本采集及后续处理的任何阶段发生变化。PAD子系统有数据输入(例如阈值，生物特征样本，二级数据流，如电导系数、反射率、电感、心电图、质询/响应对等的度量)并提供输出数据。

PAD相关的数据包括输入和输出数据流。输出数据可能包括：

- PAD数据是否可用的提示(超出固有嵌入生物特征信号的数据)；
- PAD决策结果是否已经作出的指示，如果是，则说明决策的性质；
- PAD分数；
- 部分PAD结果的向量；
- 生物特征样本附带的任何扩展的PAD数据；
- PAD机制的标识符(PAD机制供应商标识符，PAD机制标识符，PAD扩展数据机制供应商标识符及PAD扩展数据机制标识符)。

输入数据可能包括：

- 采集的背景信息——注册、验证及辨识过程；
- 采集过程的监督/监控级别；
- 当前风险级别，例如最近的攻击活动；
- PAD准则的分类，即准则对所有受试者(全局)是通用的，或对各自受试者，或者是未知的
- PAD处理过程中所使用的任何外部参数；
- 给予数据采集主体的任何质询；
- PAD数据采集日期和时间；
- 采集设备的标识符(采集设备供应商标识符，采集设备型号标识符和采集设备序列号)。

注：由于生物特征样本与PAD数据之间存在宽松的空间和时间绑定，因此PAD输出数据不需要仅与单个采集的生物特征样本相关。PAD数据也可能适用于同样过程下获得的其他样本。

如果记录中包括物理和/或化学量级，则量值应按照ISO 80000(所有部分)规定的国际单位制(SI)中的单位予以表达。

### 5.2 PAD输出

#### 5.2.1 PAD决策

是否存在：可选的

抽象值：ATTACK,NO\_ATTACK,FAILURE\_TO\_COMPUTE

注：带标记的二进制格式的抽象值的编码定义见附录A中A.1。使用XML的抽象值的编码定义见附录A中A.2。

内容：如果存在，此数据元素应指示PAD子系统是否检测到呈现攻击企图。抽象值“ATTACK”应指示PAD子系统检测到了呈现攻击企图。抽象值“NO\_ATTACK”应指示PAD子系统未检测到呈现攻击企图。抽象值“FAILURE\_TO\_COMPUTE”应指示PAD决策过程已经失败。

#### 5.2.2 PAD机制供应商标识符

适用性：可选的

抽象值：整数1~65535

内容：如果存在，此数据元素应标识 PAD 机制供应商。供应商标识符应按照ISO/IEC 19785-1的要求在其指定的生物特征识别注册机构登记。

注：国内相关标识符向GB/T 28826.2—2020中指定的机构申请登记。

### 5.2.3 PAD机制标识符

是否存在：有条件的。当且仅当PAD 机制供应商标识符存在时，应包含该数据元素。

抽象值：整数1~65535

内容：如果存在，此数据元素应标识PAD 机制(在ISO/IEC 19785-1中称为PAD 技术)。PAD 机制标识符应由PAD 机制供应商指定。

表1列出了与特定供应商无关的PAD 方法的PAD 机制标识符，对于在表1中列出的PAD 机制标识符，ISO/IEC JTC 1/SC 37生物特征识别组织标识符[即257(0101Hex)]，应被用作PAD 机制供应商标识符。这些标识符已经在ISO/IEC 19785-1中确定的生物特征识别注册机构进行了登记。

注：国内相关标识符向GB/T 28826.2—2020中指定的机构申请登记。

表 1 与特定供应商无关的PAD 方法的PAD 机制标识符

PAD机制供应商标识符	PAD机制标识符	描述
257(0101He)	1(0001Hex)	质询/无意识响应
257(0101He)	2(0002Hex)	质询/主动响应
257(0101 μ a)	3(0003Hex)	挑战质询/是什么和知道什么的组合响应
257(0101na)	4(0004Hex)	活体非刺激观察

### 5.2.4 PAD得分

是否存在：可选的

抽象值：整数0~100和FAILURE\_TO\_COMPUTE

内容：如果存在，此数据元素应以0~100的分数指示 PAD 结果。正常应呈现产生较低的分数，呈现攻击应产生更高的分数。抽象值“FAILURE\_TO\_COMPUTE” 应指示PAD 得分计算失败。

如果PAD 得分为“FAILURE\_TO\_COMPUTE”，那么，如果存在PAD 决策值，则PAD 决策值也应为“FAILURE\_TO\_COMPUTE”。

### 5.2.5 PAD扩展数据机制供应商标识符

是否存在：有条件的。仅当PAD 扩展数据存在时，应包含该数据元素。

抽象值：整数1~65535

内容：如果存在，此数据元素应标识 PAD 扩展数据中使用的PAD 机制供应商。供应商标识符应按照ISO/IEC 19785-1的要求在其指定的生物特征识别注册机构登记。

注：国内相关标识符向GB/ T28826.2—2020中指定的机构申请登记。

### 5.2.6 PAD扩展数据机制标识符

是否存在：有条件的。仅当PAD 扩展数据供应商标识符存在时，应包含该数据元素。

抽象值：整数1~65535

内容：如果存在，此数据元素应标识PAD 扩展数据使用的 PAD 机制。PAD 扩展数据机制标识符应由PAD 扩展数据机制供应商分配。PAD 机制标识符宜按照 ISO/IEC 19785-1的要求在其指定的生物特征识别注册机构登记。

注1:ISO/IEC 19785-1中规定的生物特征产品标识符的登记是可选的。

注2:国内相关标识符向GB/T 28826.2—2020中指定的机构申请登记。

### 5.2.7 PAD扩展数据

是否存在：可选的

抽象值：任何八位位组字符串

内容：如果存在，此数据元素应包含上述定义的数据元素不能表述的PAD 相关附加信息。此数据结构由辨识机制供应商定义。

## 5.3 PAD输入

### 5.3.1 采集背景

是否存在：可选的

抽象值：ENRLOMENT、VERIFICATION、IDENTIFICATION

内容：如果存在，此数据元素应指示采集过程背景信息。抽象值ENRLOMENT 应表示采集过程背景信息为注册。VERIFICATION 应表示采集过程背景信息为生物特征验证。IDENTIFICATION 应表示采集过程背景信息为生物特征辨识。

### 5.3.2 监控等级

是否存在：可选的

抽象值：UNKNOWN,CONTROLLED,ASSISTED,OBSERVED,UNATTENDED

内容：如果存在，此数据元素应指示采集过程的监督/监控级别。生物特征鉴别可在表2所示各种条件下执行。

表 2 设备监控模式

抽象值	描述
UNKNOWN	无已知信息
CONTROLLED	操作者控制生物特征采集主体来获取生物特征样本
ASSISTED	有人向提交生物特征特性的生物特征采集主体提供帮助
OBSERVED	有人监督设备操作，但不提供帮助
UNATTENDED	无人在场监督或提供帮助
<ul style="list-style-type: none"> <li>· 这一类包括通过遥感观察用户与生物特征采集系统的交互，例如视频监控，也称为远程呈现。</li> </ul>	

### 5.3.3 风险等级

是否存在：可选的

抽象值：整数0~100

内容：如果存在，此数据元素应将风险等级表示为0~100的得分，较低分数表示较低风险，较高分数表示较高风险。若风险等级未知，则此数据元素应不存在。



该内容被模糊地定义，以便系统开发人员可自身设计定性或定量风险评估方法。

#### 5.3.4 PAD准则类别

是否存在：可选的

抽象值：UNKNOWN,INDIVIDUAL,COMMON。

内容：如果存在，此数据元素应被使用来区分PAD 决策准则是针对特定的生物特征采集主体还是对所有的生物特征采集主体通用的。表3给出了此数据元素抽象值的具体描述。

**表 3 PAD 准则类别抽象值**

抽象值	描述
UNKNOWN	准则是未知的
INDIVIDUAL	准则是针对特定的生物特征采集主体
COMMON	准则是对所有的生物特征采集主体通用的

#### 5.3.5 PAD参数

是否存在：可选的

抽象值：任何可输出字符串

内容：如果存在，此数据元素应指示任何用于做出PAD 决策的外部参数，如：阈值。

#### 5.3.6 PAD质询

是否存在：可选的

抽象值：一个或多个可输出字符串

内容：如果存在，此数据元素应指示给予数据采集主体的任何质询。

#### 5.3.7 PAD数据获取日期和时间

是否存在：可选的

抽象值：2000-01-01T00:00:00Z 到3000-12-31T23:59:59Z

注：抽象值按ISO 8601的扩展日期时间格式。“Z”代表UTC(世界协调时)指示器。

内容：如果存在，此数据元素应指示在UTC 中开始获取 PAD 数据日期和时间，精确度为1 s。

#### 5.3.8 采集设备供应商标识符

是否存在：可选的

抽象值：整数1~65535

内容：如果存在，此数据元素应标识采集设备供应商。供应商标识符应按照ISO/IEC 19785-1的要求在其指定的生物特征识别注册机构登记。

注：国内相关标识符向 GB/T 28826.2—2020中指定的机构申请登记。

#### 5.3.9 采集设备模型标识符

是否存在：有条件的。仅当存在采集设备提供商标识符时，应包括该数据元素。

抽象值：整数1~65535

内容：如果存在，此数据元素应标识采集设备型号。采集设备型号标识符应由采集设备的供应商

分配。

#### 5.3.10 采集设备序列号

是否存在：可选的

抽象值：任何可输出字符串

内容：如果存在，此数据元素应标识采集设备。

## 附录 A (规范性) 标准格式

### A.1 带标记的二进制编码

#### A.1.1 总体要求

定义独立于位级表示的数据格式(抽象语法)很有用,这使得:

- a) 在适当的情况下使用不同的编码;
- b) 使用不同的内存表示,相应的使用结构用C、C++或Java 编程语言易处理;
- c) 有多种工具用于这些格式的实现;
- d) 在无大端硬件体系结构的机器上的内存表示更容易;
- e) 对格式中的值的描述更易理解。

PAD信息的抽象语法在GB/T 16262.1抽象语法记法1(ASN.1) 模块的A.1.2 中指定。采用带标记的二进制格式的PAD 数据应通过将ASN.1 区分编码规则(DER)(在GB/T 16263.1中规定)应用于A.1.2中 ASN.1 模块里定义的类型值来获得。在A.1.3 中给出了DER 的概要。所得的编码以表格形式显示在A.1.4 中。在冲突的情况下, A.1.2 中给出的ASN.1 模块优先使用。

使用抽象语法模式时,工具可以在值的编码和内存表示之间进行转换。将ASN.1 模块转换为编程语言数据结构的工具称为ASN.1 编译器,由执行内存值和指定编码之间转换的运行程序支持。此类工具可以在多个硬件平台上和多种编程语言上使用,并且由多个供应商提供。

为了保持向后兼容性,即基于新版本格式的工具能够读取和理解基于旧版本格式的PAD 数据,在新版本中,不应修改A.1.2 给出的ASN.1 模块中指定的任何元素。如果在本文件的稍后版本中需要向SET、SEQUENCE或CHOICE 添加新项,则应在扩展标记“…”之后将其添加到末尾。为了保持前向兼容性,即基于旧版本格式的工具能够基于新版本格式读取PAD 数据,读取PAD 数据的工具应忽略未知数据元素。

#### A.1.2 ASN.1中 PAD 信息的抽象语法

经认定的ASN.1 模块能按本文件恢复。

一 该ASN.1 规范已使用OSS ASN.1工具进行了对其ASN.1 标准的符合性进行了核查。

PADDataFormatModule

{GB standard 41815.2 data-formats(2)modules(0)pad-data(0)version(0)}

DEFINITIONS

IMPLICIT TAGS ::=

BEGIN

PADData::=[APPLICATION	98]SET{	
pADDecision	[0]PADDecision	OPTIONAL,
pADScoreBlockSequence	[1]PADScoreBlockSequence	OPTIONAL,
pADExtendedDataSequence	[2]PADExtendedDataSequence	OPTIONAL,
captureContext	[3]CaptureContext	OPTIONAL,
supervisionLevel	[4]SupervisionLevel	OPTIONAL,
riskLevel	[5]RiskLevel	OPTIONAL,

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：<https://d.book118.com/076115132141010200>