ICS 35.240.15
CCS L 70

中华人民共和国国家标准

GB/T 28826.4—2022

信息技术
公用生物特征识别交换格式框架
第4部分:安全块格式规范

Information technology—Common biometric exchange formats framework—Part 4:Security block format specifications

（ISO/IEC 19785-4:2010,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

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 28826《信息技术　公用生物特征识别交换格式框架》的第4部分。GB/T 28826已经发布了以下部分：

——第1部分：数据元素规范；

——第2部分：生物特征识别注册机构操作规程；

——第4部分：安全块格式规范。

本文件修改采用ISO/IEC 19785-4：2010《信息技术　公用生物特征识别交换格式框架　第4部分：安全块格式规范》。

本文件与ISO/IEC 19785-4：2010相比做了下述结构调整：

a) 5.8.2.1对应ISO/IEC 19785-4：2010的5.8.2的悬置段，5.8.2.2～5.8.2.3对应ISO/IEC 19785-4：2010的5.8.2.1～5.8.2.2；

b) 5.8.3.1对应ISO/IEC 19785-4：2010的5.8.3的悬置段，5.8.3.2～5.8.3.3对应ISO/IEC 19785-4：2010的5.8.3.1～5.8.3.2。

本文件与ISO/IEC 19785-4：2010的技术差异及其原因如下：

a) 在“范围”中增加了国内商用密码通用安全块格式（见第1章），以便于对本文件的理解和应用；

b) 在“术语和定义”中具体列出了“生物特征识别（的）、生物特征（的），生物特征识别，生物特征数据块，生物特征信息记录，CBEFF生物特征识别组织，安全块，安全块格式，安全块格式标识符，安全块格式所有者，标准生物特征数据头，BioAPI单元，ACBio实例，生物特征识别的鉴别上下文，生物特征处理单元，消息鉴别码”共15个术语的定义（见第3章），以便于对本文件的理解和应用；增加了“生物特征识别组织标识符”（3.6）和“对象标识符”（3.15），以便于对2个术语的区分理解和应用；

c) 在“缩略语”中具体体现了“ACBio、BDB、BPU、CBEFF、CRL、MAC、SB、SBH”共8个缩略语的全称和中文释义，以便于对本文件的理解和应用（见第4章），因此不再引用ISO/IEC 19785-1、ISO/IEC 24761、ISO/IEC 9798-6与REC 3852；

d) 在“缩略语”中增加了“ASN.1、BER、BioAPI、DER、PER、XER”共6个缩略语（见第4章），以便于对本文件的理解和应用；

e) 用规范性引用的GB/T 16262.1替换了ISO/IEC 8824-1（见5.8.1.1、7.8.1.1），以适应我国的技术条件；

f) 用规范性引用的GB/T 16263.1替换了ISO/IEC 8825-1（见5.4、6.4、6.8、7.4），以适应我国的技术条件；

g) 用规范性引用的GB/T 16263.2替换了ISO/IEC 8825-2（见5.4、6.4、7.4），以适应我国的技术条件；

h) 用规范性引用的GB/T 16263.4替换了ISO/IEC 8825-3（见5.4、6.4、7.4），以修改ISO/IEC 19785-4：2010的引用错误，并适应我国的技术条件；

i) 用规范性引用的GB/T 28826.1替换了ISO/IEC 19785-1（见5.8.1.3），以适应我国的技术条件；

j) 增加了规范性引用文件GB/T 28826.2—2020（见7.2、7.4），以规范国内商用密码通用安全块

格式的登记要求；

k) 增加了规范性引用文件 GB/T 32918.2(见 7.8.3.1)，以规范国内商用密码通用安全块格式的登记要求；

l) 增加了规范性引用文件 GB/T 33560—2017(见 7.8.3.2.1、7.8.3.2.2)，以规范国内商用密码通用安全块格式的登记要求；

m) 增加了规范性引用文件 GB/T 35275—2017(见 7.8.3.2.1、7.8.3.2.2)，以规范国内商用密码通用安全块格式的登记要求；

n) 增加了规范性引用文件 GB/T 38635.2(见 7.8.3.1)，以规范国内商用密码通用安全块格式的登记要求；

o) 将 ISO/IEC 19785-2 从资料性引用修改为规范性引用，因为 ISO/IEC 19785-2 规定的登记操作规程是规范性要求；

p) 增加了对于国内商用密码算法的支持，为适用国家密码体系(见第 7 章)；

q) 增加了“国内商用密码通用安全块格式的 ASN.1 代码”(见附录 B)，为说明 ASN.1 国内商用密码安全块格式的具体内容。

本文件做了下列编辑性改动：

a) 将 ISO/IEC 19785-4:2010/CORR1:2013《信息技术　公用生物特征识别交换格式框架　第 4 部分：安全块格式规范》的技术勘误 1 纳入到相应条款中，并在改动过的条款的外侧页边空白位置用垂直双线(||)标示，根据技术勘误删除原附录 B；

b) 删除了对 ISO/IEC 19785-2《信息技术　公用生物特征识别交换格式框架　第 2 部分：生物特征识别注册机构操作规程》的资料性引用。

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：北京曙光易通技术有限公司、江苏赛西科技发展有限公司、北京数字认证股份有限公司、中国银联股份有限公司、中国电子技术标准化研究院、人力资源和社会保障部信息中心、北京眼神智能科技有限公司、北京得意音通技术有限责任公司、广州广电运通金融电子股份有限公司、北京中科虹霸科技有限公司、联想中天科技有限公司、上海商汤智能科技有限公司、圣点世纪科技股份有限公司、上海依图网络科技有限公司、福建海景科技开发有限公司。

本文件主要起草人：张大朋、刘倩颖、王文峰、刘旭华、于雪平、宋继伟、詹榜华、戚文彬、张亚浩、钟陈、王思翔、韩烽、王智飞、宋方方、郑方、张玮、校利虎、宁静、蒋慧、胡文矛、刘亦珩、黄来青、夏冰冰、费志军、杨波、于欢、张辰宇、谢德坤。

引　言

基于生物特征的身份验证系统和应用程序有望支持来自不同供应商的多种生物特征识别设备。公用生物特征识别交换格式框架(CBEFF)通过简化生物特征数据交换,促进了由不同供应商开发的生物特征识别应用程序和系统的互操作性。

GB/T 28826《信息技术　公用生物特征识别交换格式框架》拟由4个部分构成。

——第1部分:数据元素规范。目的在于定义能够实现生物识别数据交换的标准化项目。

——第2部分:生物特征识别注册机构操作规程。目的在于规定用于国内的生物特征识别登记标识符、登记机构、登记程序、登记申请、登记维护的要求。

——第3部分:维护者格式规范。目的在于对CBEFF生物特征识别组织ISO/IEC JTC 1/SC 37定义的、根据ISO/IEC 19785-2登记的三种维护者格式规范进行说明。

——第4部分:安全块格式规范。目的在于对CBEFF生物特征识别组织ISO/IEC JTC 1/SC 37定义的、根据ISO/IEC 19785-2登记的两种安全块格式,以及全国信息技术标准化委员会生物特征识别分技术委员会(SAC/TC 28/SC 37)定义的、根据GB/T 28826.2—2020登记的一种安全块格式规范进行说明。

本文件作为CBEFF的第4部分,规定了生物特征数据的完整性和加密性。用于生物特征验证和识别的生物特征数据来自受信的来源,传输过程中不受干扰并且确保完整性。可根据安全策略的不同确定是否对生物特征数据进行加密。

为了确保互操作性,在GB/T 28826.1中规定了通用生物特征交换格式框架(CBEFF),用来将元数据与一个或多个生物特征数据块(BDB)相关联。在GB/T 28826.1中定义了完整性和加密选项,以及包含与这些选项相关的安全信息的安全块(SB)的概念,但没有规定安全块的格式和详细内容。

从一个CBEFF维护者格式开始,有以下几点说明。

首先,如果该维护者格式确定CBEFF数据元素CBEFF_BDB_encryption_options(生物特征数据块加密选项)的抽象值指定为NO ENCRYPTION(无加密),并且CBEFF数据元素CBEFF_BIR_integrity_options(生物特征信息记录完整性选项)指定为NO INTEGRITY(不完整),则该维护者格式不需要安全块。

其次,如果该维护者格式在某些情况下需要包含安全块,则该维护者格式可以将其指定为本文件中定义的其中一种安全块格式或者其他安全块格式,或者可以包含CBEFF数据元素CBEFF_SB_format_owner(安全块格式所有者)和CBEFF_SB_format_type(安全块格式类型),来标识采用的是本文件定义的某种安全块格式还是某些其他安全块格式。

最后,除了本文件规定的安全块格式,可能还有许多满足不同需求的CBEFF安全块格式。例如,在ISO/IEC 24713-3中为国际劳工组织海员简介定义的安全块格式。有关国际登记的安全块格式的完整列表,请参阅IBIA网站https://www.ibia.org/cbeff/iso/sb-format-identifiers;有关国内登记的安全块格式的完整列表,请参阅网站http://sc37.cesinet.com/biometrics/regProduct。

本文件给出了三种常用的安全块格式:通用安全块格式、只包含签名的安全块格式和国内商用密码通用安全块格式。

第一种安全块格式是通用安全块格式,设计得尽量通用。该格式采用RFC 3852加密消息语法(CMS),包含了用于加密和完整性的可选元素,并对RFC 3852的EnvelopedData、EncryptedData、SignedData和AuthenticatedData进行了某些修改,以满足与CBEFF一致的生物特征信息安全性表达要求。通用安全块格式还可以选择包含ISO/IEC 24761中规定的生物特征(ACBio)实例的身份验证上

下文。ACBio 也使用 RFC 3852 加密消息语法方案。通过包含 ACBio 实例，可以确定生成认证用生物特征的系统的安全级别。可选择使用 ACBio 实例是提供远程生物认证基础设施（TAI）的重要组成部分。

第二种安全块格式是只包含签名的安全块格式，也是使用 RFC 3852 定义的。

第三种安全块格式是采用国内商用密码消息语法定义的国内商用密码通用安全块格式，包含了用于加密和完整性的可选元素，不支持 ACBio 实例。

信息技术
公用生物特征识别交换格式框架
第4部分:安全块格式规范

1 范围

本文件给出了由CBEFF生物特征识别组织ISO/IEC JTC 1/SC 37定义的,根据ISO/IEC 19785-2登记的两种安全块格式,并给出了其登记的安全块格式标识符。

注:安全块格式标识符记录在维护者格式的SBH中(或由该维护者格式定义为唯一可用的安全块格式)。

通用安全块格式提供了BDB是否加密以及SBH和BDB是否需要完整性校验的规范,该格式采用国际RFC系列密码消息语法,也能包含符合ISO/IEC 24761的ACBio实例。安全块包含用于加密和/或完整性在内的所有必要的安全参数。

它不限制用于加密或完整性的算法和参数,但提供了如何记录此类算法和参数值的方式。

对于特定的应用领域,如何确定安全块生成器可以使用哪些算法和参数范围,从而确定安全块使用者要支持的算法和参数范围是一个分析问题,超出了本文件的范围。

只包含签名的安全块格式与通用安全块格式类似,虽然限制更大,但更简单,特别是不能包含ACBio实例,也不支持BDB加密。

本文件还给出了由SAC/TC28/SC37定义的、根据GB/T 28826.2—2020登记的一种安全块格式:国内商用密码通用安全块格式。

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 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 16263.2 信息技术 ASN.1编码规则 第2部分:紧缩编码规则(PER)规范(GB/T 16263.2—2006, ISO/IEC 8825-2:2002,IDT)

GB/T 16263.4 信息技术 ASN.1编码规则 第4部分:XML编码规则(XER)(GB/T 16263.4—2015, ISO/IEC 8825-4:2008,IDT)

GB/T 28826.1 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(GB/T 28826.1—2012, ISO/IEC 19785-1:2006,MOD)

注:GB/T 28826.1—2012被引用的内容与ISO/IEC 19785-1:2006被引用的内容没有技术上的差异。

GB/T 28826.2—2020 信息技术 公用生物特征识别交换格式框架 第2部分:生物特征识别注册机构操作规程

GB/T 32918.2 信息安全技术 SM2椭圆曲线公钥密码算法 第2部分:数字签名算法