ICS 33.050
M 30

团　体　标　准

T/TAF 079-2021

移动智能终端及应用软件生物特征识别安全规范

Smart mobile terminal and application software biometric recognition security specification

2021-01-08 发布　　2021-01-08 实施

电信终端产业协会　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。

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。

本文件由电信终端产业协会提出并归口。

本文件起草单位：中国信息通信研究院、蚂蚁科技集团股份有限公司、高通无线通信技术(中国)有限公司、OPPO广东移动通信有限公司、北京三星通信技术研究有限公司、维沃移动通信有限公司、北京奇虎科技有限公司、国民认证科技（北京）有限公司、阿里巴巴(中国)有限公司。

本文件主要起草人：傅山、王嘉义、宁华、刘陶、王艳红、杜云、林冠辰、王江胜、李根、吴越、吴春雨、贾科、姚一楠、李俊、黄天宁。

引　　言

随着移动通信技术的快速发展，移动互联网应用正逐渐渗透到人们生活、工作的各个领域，个人信息安全问题成为各方关注的重点。越来越多的移动智能终端及应用软件使用生物特征识别实现身份认证等功能，生物特征识别信息是个人信息的重要部分。

生物特征识别信息与个人身份高度绑定，且具有不可变更的特点，生物特征识别信息的泄露或滥用将带来严重的社会问题，移动智能终端及应用软件的生物特征识别信息保护安全规范迫在眉睫。

移动智能终端及应用软件生物特征识别安全规范

1 范围

本文件规定了移动智能终端及移动应用软件开展收集、存储、使用、共享、转让、公开披露、注销等生物特征识别信息处理活动应遵循的原则和安全要求。

本文件适用于各种制式的移动智能终端，个别条款不适用于特殊行业、专业应用，其他终端也可参考使用。

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 26238－2010 信息技术 生物特征识别术语

GB/T 35273－2020 信息安全技术 个人信息安全规范

3 术语和定义

GB/T 26238－2010和GB/T 35273－2020界定的以及下列术语和定义适用于本文件。

3.1

移动智能终端 smart mobile terminal

能够接入移动通信网，具有能够提供应用程序开发接口的操作系统，并能够安装和运行应用软件的移动终端。

3.2

生物特征识别 biometric recognition

基于个体的行为特征和生物学特征，对该个体进行的自动识别。

3.3

生物特征识别系统 biometric system

基于个体的行为特征和生物学特征进行自动识别的系统。

3.4

生物特征样本 biometric sample

先于生物特征项提取，且从生物特征采集子系统获得的模拟的或数字的生物识别特征的表示。

3.5

生物特征数据主体 biometric data subject

在生物特征识别系统内的包含生物特征信息的个人。

3.6

生物特征项　biometric feature

从生物特征样本中提取的，用于比对的数值或标记。

3.7

生物特征模板　biometric template

参考的生物特征项的集合，已存储的生物特征项的集合。

3.8

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。

3.9

生物特征识别信息　biometric information

对自然人的物理、生物或行为特征进行技术处理得到的、能够单独或者与其他信息结合识别该自然人身份的个人信息。本部分对处于任何处理阶段的生物特征样本、生物特征参考、生物特征项或生物特性的通称。

3.10

生物特征识别信息控制者　biometric information controller

有能力决定生物特征识别信息处理目的、方式等的组织或个人。

3.11

身份鉴别　identity authentication

在计算机及计算机网络系统中确认操作者身份真实性的过程，在本文件中指以人为主体的生物特征身份鉴别。包括在实体可以在域中进行注册和识别之前，确定所声称身份真实性的信任程度的过程。

3.12

删除　delete

在实现日常业务功能所涉及的系统中去除个人信息的行为，使其保持不可被检索、访问的状态。

3.13

匿名化　anonymization

通过对个人信息的技术处理，使得个人信息主体无法被识别或者关联，且处理后的信息不能被复原的过程。个人信息经匿名化处理后所得的信息不属于个人信息。

3.14

不可链接性　unlinkability

两个或多个生物特征识别参考的特性，无法相互链接或与各自的信息主体链接。

3.15

不可逆性 irreversibility

从生物特征样本进行技术处理生成其他信息时，所生成信息具有的、从生成信息无法推断出生物特征样本任何信息的特征。

4 生物特征识别模态和系统框架

4.1 生物特征识别模态

生物特征识别系统根据一个或多个生理（身体的物理特性，例如指纹）或者行为（个体所做的事情，例如步态）特征对个体进行自动识别。

生理特征包括但不限于：

—— 指纹；
—— 人脸；
—— 虹膜；
—— 声纹；
—— 手型；
—— 指静脉/掌静脉；
—— 视网膜；
—— DNA；
—— 掌纹。

行为特征包括但不限于：

—— 签名；
—— 步态；
—— 语音。

为了验证或辨识个体，生物特征识别系统处理生物特征样本以便与存储的生物特征参考进行比对。生物特征参考可以是一个或一组生物特征样本、生物特征模板或生物特征识别模型。

4.2 生物特征识别系统框架

图1是移动智能终端与应用软件的生物特征识别系统框架。

生物特征识别系统主要由移动智能终端和远端服务器的若干功能模块构成，主要包括生物特征采集模块、生物特征存储模块、生物特征比对模块等。其中，由生物特征采集装置采集生物特征、提取生物特征项，经由生物特征采集模块将生物特征参考存储在生物特征存储模块中，生物特征比对模块实现对生物特征项与生物特征模板的比对。

移动智能终端生物识别主要包括本地识别和远程识别两种方案。本地识别方案中，生物特征采集装置采集后的信息通过移动智能终端内的生物特征采集模块进行样本采集和特征项提取；通过生物特征存储模块进行信息存储和本地保护；通过生物特征比对模块进行阈值比对分析，最后将比对结果传输给移动应用完成生物特征识别。

在远程识别方案中，生物特征采集装置采集后的信息传输到远端服务器，用于后续的生物特征项提取、生物特征存储和生物特征比对。也可在移动智能终端上完成生物特征项提取后，传输给远端服务器。最后远端服务器将分析结果传输给移动应用完成生物特征识别。

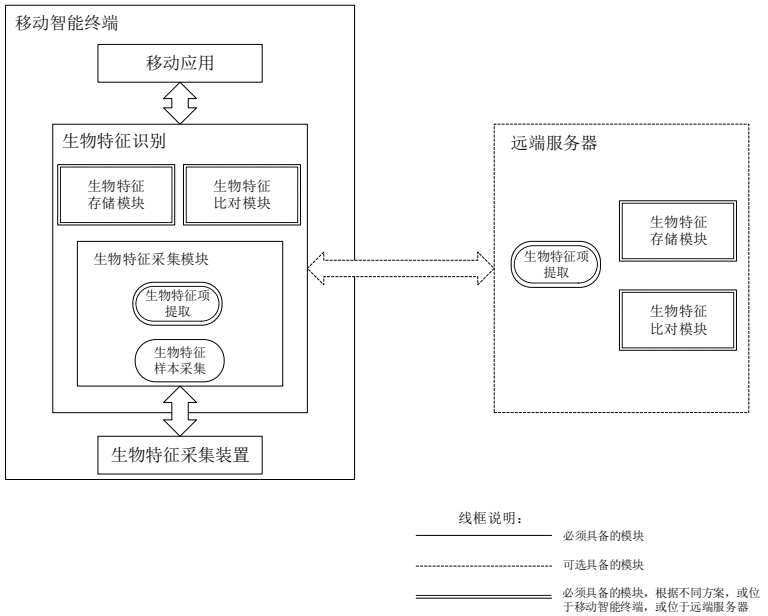

图1　生物特征识别系统框架

5　生物特征识别信息的收集

对生物特征识别信息控制者的要求包括：

a) 不应强制或诱导生物特征识别信息主体进行生物特征识别。生物特征识别信息主体不进行生物特征识别时，不应禁止用户的正常使用，仅可停止访问生物特征识别相关功能，并应告知可替代处理流程；

b) 收集生物特征识别信息前，应通过隐私协议或弹窗明示等方式单独向生物特征识别信息主体告知以下信息，并征得生物特征识别信息主体的明示同意：

1) 收集、使用生物特征识别信息的目的、方式、类型和范围，以及授权存储时间等规则；

2) 收集的生物特征识别信息处理方式的描述；

3) 控制者的联系信息，至少包括的信息有：组织机构信息、联系方式；

4) 生物特征识别信息主体实现查看、修改、撤回其生物特征识别授权同意的方式；

c) 不应超出向生物特征识别信息主体明示的范围收集生物特征识别信息；

d) 当收集生物特征识别信息的范围或用途发生变化时，应在变化之后的首次采集时更新明示告知的内容并征得同意。

6　生物特征识别信息的存储

对生物特征识别信息控制者的要求包括：

a) 应将生物特征识别信息与生物特征识别信息主体的身份信息分开存储，并进行完整性保护；

b) 同一生物特征识别信息主体的多传感器生物特征识别信息应分开存储；

c) 生物特征识别信息在不同应用、数据库间应保证不可链接性；

d) 不应直接存储生物特征识别样本；

e) 生物特征模板应进行加密存储，并采用授权访问方式读取；

f) 生物特征识别比对前应进行生物特征项的完整性校验，采用有效的安全机制确保生物特征识别

信息的保密性和完整性，及时清除比对过程产生的临时数据（如比对得分等数据）并确保不可恢复；

g) 存储生物特征识别比对信息时，可通过减少特征提取、使用假名标识符等方式保证不可逆性，并进行加密存储；

h) 应只存储满足生物特征识别信息主体授权同意的目的所需的最少生物特征识别信息；

i) 若采用远程识别方案，除上述要求外，还应在远端服务器上采取加密、访问控制、逻辑隔离等方式对生物特征比对模块进行保护。

7 生物特征识别信息的使用

对生物特征识别信息控制者的要求包括：

a) 应使用多样化或可更新等方式进行生物特征识别比对，且多样更新产生的生物特征识别信息应具备不可逆性和不可链接性；

b) 不应基于生物特征识别信息生成用户画像，以及基于生物特征识别信息自身进行个性化推荐；

c) 生物特征识别信息的处理应符合以下要求：

1) 原则上应在本地处理生物特征识别信息，仅向服务器返回比对结果；

2) 若存在远程传输需求，应对必要性进行评估，应向生物特征识别信息主体明示告知信息处理方式，并进行数据加密、去标识化处理；

d) 传输生物特征识别信息时，应对通讯对方的真实身份进行鉴别，鉴别通过后应建立安全通道保证传输过程中的保密性和完整性；

e) 不同模块间以及模块与应用服务器进行生物特征识别信息的传输时，应采取有效安全机制防止重放攻击，如不可预测随机数、时间戳或挑战/应答等方式；

f) 应支持对使用生物特征识别信息的日志记录功能，记录内容包括但不限于事件主体、事件时间、事件类型、事件是否成功等要素。日志存储期限应符合相关法律法规的要求。

8 生物特征识别信息的委托处理、共享、转让、公开披露

对生物特征识别信息控制者的要求包括：

a) 委托第三方处理生物特征识别信息时，应预先向生物特征识别信息主体告知第三方相关信息，所涉生物特征识别信息的类型和数量、委托处理目的、委托时限等，并获得生物特征识别信息主体的明示同意；

b) 生物特征识别信息原则上不应共享、转让，宜仅提供与生物特征识别主体相关联的身份验证结果或经过匿名化处理的生物特征识别信息；

c) 生物特征识别信息共享时不应与用户相关联，应进行匿名化处理；

d) 委托第三方处理生物特征识别信息，以及嵌入第三方工具处理生物特征识别信息时，应优先选择具备同等或更高生物特征识别信息保护能力的第三方机构；

e) 确需共享、转让生物特征识别信息时，应单独向生物特征识别信息主体告知目的、涉及的生物特征识别信息类型、接收方的具体身份和数据安全能力等，应定期对共享、转让生物特征识别信息的必要性进行评估，并在获得明示同意后进行；

f) 在委托时限内，如果授权的第三方机构发生变化或共享信息的范围用途发生变化，应及时更新明示告知的内容并征得同意；

g) 委托到期后，应及时对生物特征识别信息进行删除；

h) 不应公开披露生物特征识别信息。

9 生物特征识别信息的删除

a) 在以下条件满足其中之一时，应及时对生物特征识别信息进行删除：
   1) 超出授权同意的生物特征识别信息存储时间；
   2) 共享或转让生物特征识别信息被评估为不必要；
b) 删除操作应便于生物特征识别信息主体查找，删除应便于用户操作；
c) 应向生物特征识别信息主体提供仅删除生物特征识别信息的功能，并明示告知删除的渠道及相关管理制度，如申请删除的步骤、信息的使用范围、信息的保存时间、信息的处理措施、审核处理周期、结果反馈方式等；
d) 删除发起前应进行身份验证，删除过程收集的个人信息，不应超出采集时所提供的范围；
e) 不应设置不合理的删除条件，如仅提供现场办理、设置冻结期等；
f) 宜具备应急处置能力，例如，提供远程撤销授权或删除生物特征识别信息的功能，防止设备丢失引发个人生物识别信息泄露。
g) 原则上不应具备分模态删除功能，如仅删除单一模态生物特征识别信息，删除后不宜限制用户的正常使用，不宜拒绝再次使用该模态生物特征识别功能。

参 考 文 献

[1] ISO/IEC 30136-2018 Information technology- Performance testing of biometric template protection schemes

[2] GB/T 37036.2-2018 信息技术 移动设备生物特征识别 第2部分：指纹

[3] GB/T 37036.3-2018 信息技术 移动设备生物特征识别 第3部分：人脸

电信终端产业协会团体标准

移动智能终端及应用软件生物特征识别安全规范

T/TAF 079-2021

*

电信终端产业协会印发
地址：
电话：
电子版发行网址：