ICS 35.040
L 71

团 体 标 准

T/AI 111—2020

生物特征模板的安全使用要求

Secure using requirements of biometric template

2020－12－31 发布　　2020－12－31 实施

中关村视听产业技术创新联盟　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。

本文件由新一代人工智能产业技术创新战略联盟提出并归口。

本文件起草单位：青岛海信电子产业控股股份有限公司、西安电子科技大学、科大讯飞股份有限公司、云从科技集团股份有限公司、中国电子标准化研究院、北京大学、上海依图网络科技有限公司。

本文件主要起草人：陈维强、高雪松、朱辉、胡伟凤、张淯易、李祁、张紫铃、孟祥奇、孙菁、孙宗臣、马万钟、吴子阳、温浩、姚志强、李军、曹霖、李婧欣、田永鸿、赵春昊、张辰宇。

引　言

本文件只涉及与生物特征识别中生物特征模板的相关处理与存储。生物特征模板是指生物特征识别中参考的生物特征项的集合，已存储的生物特征项的集合，以及可直接与探针生物特征样本的生物特征项进行比对的数据。本文件中，也对生物特征探针、生物特征样本这些数据做出了安全要求，它们符合用户对生物特征模板广义上的认知，并且属于生物特征模板生存周期中的组成部分。在对安全性要求的同时，本文件也对生物特征识别的准确度和性能做出了要求。

本文件的目的是规范执行生物特征模板安全使用的最适合的要求和最佳的科学操作。目前，生物特征模板安全性的度量缺乏没有统一的方法，针对生物特征模板数据的也没有行业性建议。现存安全性的要求都是从整个生物特征识别系统的角度出发，过于笼统。且生物特征模板也不仅仅用于身份识别，需要更细的标准要求。

生物特征识别的种类有很多，常见的有指纹、人脸、虹膜、声纹、静脉等。每一个所产生的生物特征样本的形式、内容，以及对应的生物特征识别模型都不同。各个生物特征特性以及目前的研究应用现状也导致准确度与性能差异很大。这些差异导致本文件无法产生准确统一的安全性与可用性约束条件。因此，本文件抽象出所有生物特征识别的共性，针对生物特征识别中模板的生存周期进行了统一的定性，其理念和原则是广泛适用于各种生物特征模板的。

生物特征模板安全使用要求

1 范围

本文件规定了生物特征模板安全使用的目标和原则，及应用过程全生存周期中的管理措施和规范。

本文件针对生物特征识别系统提供生物特征模板使用的技术要求，适用于组织规范企业生物特征识别中针对生物特征模板的安全规范使用，也适用于网络安全相关主管部门、第三方评估机构等组织开展企业生物特征识别模板数据的安全监督管理、评估等工作。

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（包括所有的修改单）适用于本文件。

GB/T 20979—2019 信息安全技术 虹膜识别系统技术要求

GB/T 33767.4-2018 信息技术 生物特征样本质量 第4部分:指纹图像数据

GB/T 33767.5-2018 信息技术 生物特征样本质量 第5部分:人脸图像数据

GB/T 33767.6-2018 信息技术 生物特征样本质量 第6部分:虹膜图像数据

GB/T 37076—2018 信息安全技术 指纹识别系统技术要求

GB/T 38671—2020 信息安全技术 远程人脸识别系统技术要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

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。

注1:“个体”限指人。

注2:生物特征识别涵盖从开始注册到得到验证结果全周期流程。

注3:由于识别过程中通常使用生物特征模板进行比对，本文件中生物特征识别与生物特征模板识别等同。

3.2

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。

3.3

生物特征数据库 biometric database

生物特征数据记录存储的数据库。

3.4

生物特征数据记录　biometric data record

包含生物特征数据的数据记录。

注：一个生物特征数据记录可能包括非生物特征数据，例如，生物特征参考。

3.5

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。

3.6

生物特征样本　biometric sample

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

3.7

生物识别特征　biometric characteristic

个体生物学和行为的特征，该特征可被检测，并且可以从中提取与他人有区别的、可重复的生物特征项，从而达到个体自动识别的目的。

示例：生物识别特征包括:指纹脊线结构、脸型、声音、面部皮肤纹理构造、掌型、指形、虹膜结构、手部静脉血管结构、手掌脊状结构、视网膜图案，动态手写签名等。

3.8

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。

注 1：生物特征项是一次完成的生物特征项提取的输出。

注 2：这一术语的使用宜与其在模式识别和数学领域的使用相一致。

注 3：生物特征项集也可被看作是一个最终的生物特征样本。

3.9

生物特征探针　biometric probe

输入到算法的、与生物特征参考数据进行比对的生物特征数据。

注：术语“比对”是指生物特征识别意义上的比对。

3.10

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。

3.11

生物特征识别模型　biometric model

依据生物特征数据主体，由生物特征项产生的已存储的函数。

3.12

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，可直接与探针生物特征样本的生物特征项进行比对。

注 1：生物特征参考包括图像或其他被采集的生物体特征样本，狭义上，它的原始、增强或压缩形式都不是生物特征模板。

注 2：狭义上，生物特征项通常不被看作是生物特征模板，除非它们被储存用作参考。本文件广义上认为生物特征项是生物特征模板前阶段的产物，也归属于生物特征模板的范畴。

3.13

错误接受率　false accept rate

在进行生物特征探针与生物特征参考的比对过程中，对于本不该接收的比对(即结果应为拒绝的比对)错误地判定为接受的次数与总测试次数(不同手指)的比率的测定值。

3.14

错误拒绝率　false reject rate

在进行生物特征探针与特征参考的比对过程中，对于本不该拒绝的比对(即结果应为接受的比对)错误地判定为拒绝地次数与总测试次数

3.15

不可逆性 irreversibility

根据生物特征样本创建生物特征模板的变换的性质，使得变换的生物特征模板的知识不能用于确定关于生物特征样本的任何信息。

3.16

爬山攻击 climb attack

在一个有输入和输出的黑盒环境下，根据输出结果的规律不断调整输入数据，使得输出结果逐渐接近期望并最终得到期望的输出结果。

4 缩略语

下列缩略语适用于本文件。

FAR:错误接受率(False Accept Rate)

FRR:错误拒绝率(False Reject Rate)

5 生物特征模板全生存周期流程

5.1 生物特征模板全生存周期流程概述

生物特征模板全生存周期的基本组成和相互关系如图 1 所示。

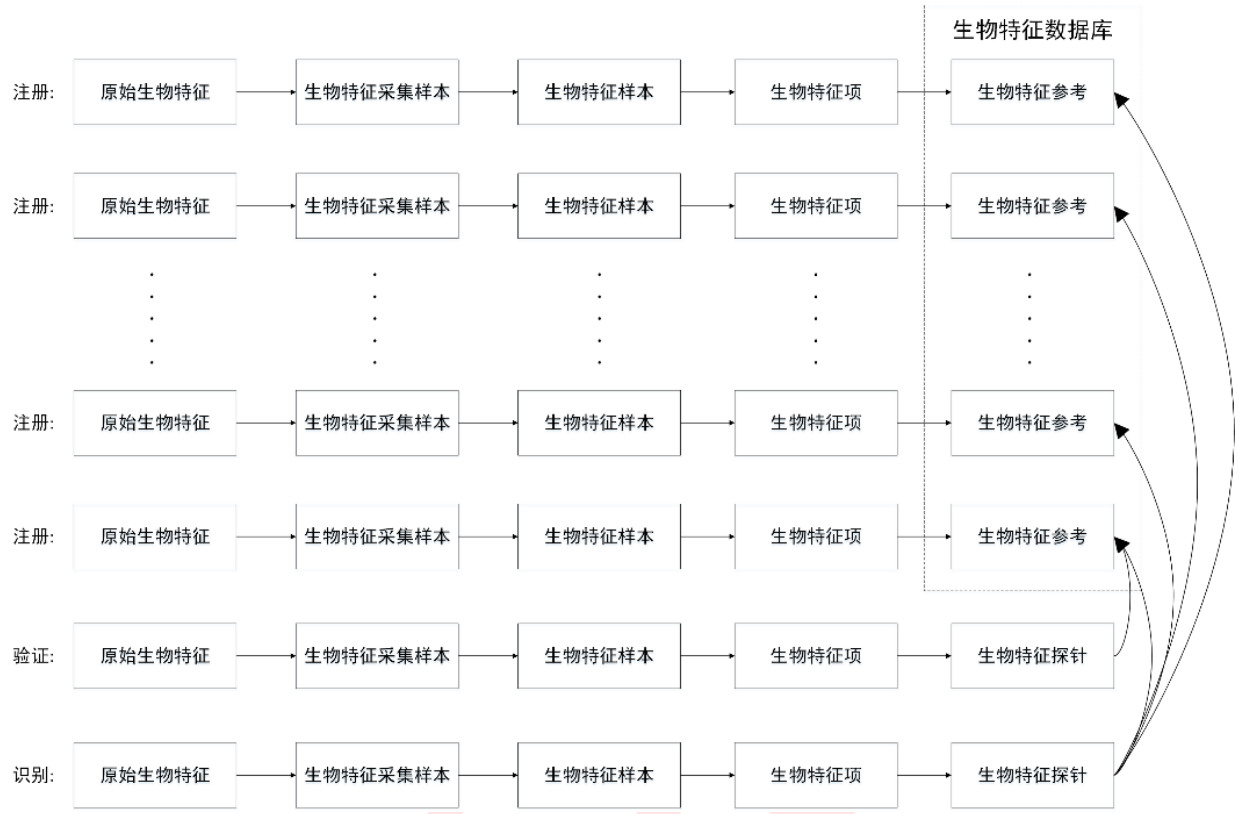

图 1 生物特征模板全生存周期流程框图

狭义上的生物特征模板指参考的生物特征项的集合和已存储的生物特征项的集合，并且模板可直接与探针生物特征样本的生物特征项进行比对。生物特征参考包括图像或其他被采集的生物体特征样本，狭义上，它的原始、增强或压缩形式都不是生物特征模板，生物特征项通常不被看作是生物特征模板，除非它们被储存用作参考。广义上，图中所提的原始生物特征、生物特征采集样本、生物特征样本、生物特征项、生物特征参考，生物特征探针等都属于生物特征模板的范畴。

5.2 生物特征模板生存周期各阶段

5.2.1 生物特征采集

输入设备或传感器从用户采集生物特征信息，将其转化成适合生物特征识别系统其他部分进行处理的形式，实现信息的转换。

5.2.2 生物特征处理

系统接收原始生物特征数据，将数据转换成生物特征比对所需要的生物特征样本，包含生物特征采集样本处理、生物特征提取等方面。

生物特征采集样本处理方面针对生物特征进行增强、下采样、压缩、转化成数据交换格式标准等处理操作，形成生物特征样本。

生物特征提取功能针对经过标准化处理的生物特征样本分离并输出可重复性和辨别性的数值或标记，形成生物特征项，组成生物特征模板。

5.2.3 生物特征注册

根据生物特征处理提供的信息，进行生物特征注册处理，并将生物特征数据信息进行存储。

5.2.4 生物特征识别

根据生物特征处理后的生物特征探针，以及经数据存储提供的生物特征参考，进行生物特征识别比对。比较所产生的分数值表明生物特征样本和生物特征参考匹配的程度。

5.2.5 生物特征决策

接收从生物特征识别模块输出的比对数值，根据设置的生物特征识别决策策略，为生物特征识别应用产生一个“声称者是否为其所声称身份”的是非决定。生物特征识别策略包括：

a） 匹配阈值；
b） 每次识别所允许的匹配尝试次数；
c） 每个声称者注册的参考模板数目；
d） 在匹配过程中使用内部控制，用以检测生物特征模板是否相同；
e） 使用集成决策模型，使用多次参考模板。

5.2.6 生物特征模板存储

存储模块为用户存储注册的生物特征参考。根据生物特征比对的需要，可以对登记生物特征参考进行增加、删除和检索功能。根据系统架构和预期的功能，可为单个用户保存一个或大量生物特征模板。

生物特征模板可存储在：

a） 生物特征设备中的物理保护媒体；
b） 计算机系统的常规数据库；
c） 令牌存储的设备，例如智能卡。

5.2.7 生物特征模板更改

根据用户提供的新的生物特征，进行相同步骤的生物特征注册处理，并且将存储模块中存储的旧生物特征模板进行替换。

5.2.8 生物特征模板删除

根据用户账号删除的需要，先对用户身份进行认证，认证成功后实现存储模块中生物特征模板的删除，或者做匿名化处理，使得该特征模板无法被检索。

5.2.9 生物特征传输

实现各模块、各环节以及其他信息系统间的通信与数据传输。

5.3 生物特征模板应用

5.3.1 生物特征模板登记

生物特征模板登记，也可称为生物特征模板注册，是指将用户身份与生物特征参考数据绑定并保存的过程。依据生物特征模板是否允许更新，生物特征模板登记可分为初始登记和再登记。

生物特征模板登记过程包括：

a） 生物特征样本采集；
b） 生物特征提取；
c） 生物特征质量评价，如果不合格则重新采集；

d) 生物特征模板生成与存储；
e) 测试登记是否成功；
f) 若初始登记不合格，判断是否进行重复采集、登记等操作。

5.3.2 生物特征模板识别

生物特征模板识别的过程是试图确定某使用者是否已经注册在系统中，如果是则确定其身份。
生物特征模板识别包括以下步骤：
a) 生物特征样本采集；
b) 生物特征提取；
c) 生物特征质量评价；
d) 比对生物特征探针与系统中的待比对生物特征参考模板；
e) 判断是否有匹配上的身份；
f) 根据生物特征识别决策策略和输出的比对得分判断是否识别结论。

5.3.3 生物特征模板验证

在生物特征模板验证过程中，用户提交所声称的身份和进行验证所需要的生物特征。通常基于所声称的身份，系统提取用户的生物特征模板，并将其与从所采集生物特征样本产生的特征进行比较，确定用户是否确实是所声称身份的拥有者。
生物特征模板包括以下步骤：
a) 生物特征样本采集；
b) 生物特征提取；
c) 生物特征质量评价，如果不合格则重新采集；
d) 比对生物特征探针与其所声称身份的对应生物特征参考模板；
e) 判断相似度是否超过确定的门限阈值；
f) 根据生物特征识别决策策略和比对得分判断是否匹配。

6 安全威胁

6.1 概述

生物特征模板属于个人隐私信息，并且具有高度敏感性。如图 2 所示，是生物特征身份鉴别系统的基本流程，在该流程当中，有八个可能被攻击的环节，对生物特征模板的安全造成威胁。

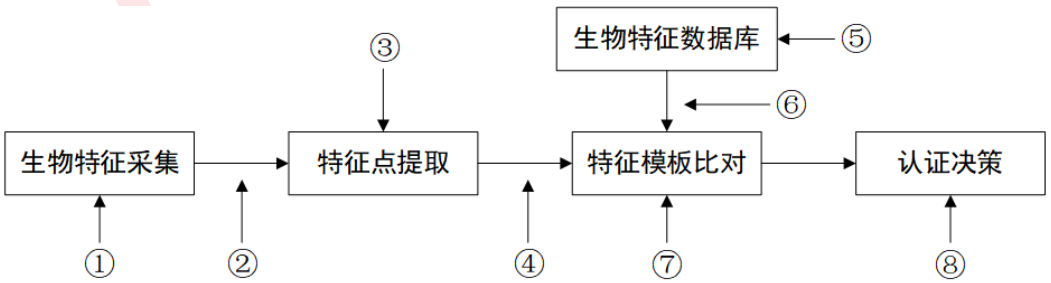

图 2 生物特征识别流程

6.2 基于身份伪造的安全威胁

在生物特征身份鉴别系统中，攻击者可能在多个环节伪装自己的身份以获取用户的生物特征模板，具体包括：

a) 当身份鉴别涉及用户、服务器和可信第三方时，攻击者冒充可信第三方去访问服务器，并获取用户的生物特征模板，例如图 2 中的攻击点⑤；或者攻击者冒充合法用户从可信第三方获取认证信息，从而更改服务器中存储的用户特征模板，例如图 2 中的攻击点⑤；
b) 攻击者冒充合法物联网设备来采集用户的原始生物特征，例如图 2 中的攻击点①；
c) 攻击者冒充合法服务器来获取用户的原始生物特征，例如图 2 中的攻击点②。

6.3 基于窃听的安全威胁

生物特征模板在通信信道传输的过程中，将面临信道被窃听或者信道被恶意控制的风险，从而导致用户的个人隐私信息泄露，造成安全威胁。具体包括：

a) 攻击者窃听通信信道，并试图获取合法用户的生物特征模板，例如图 2 中的攻击点②、④、⑥；
b) 攻击者窃听通信数据后，通过重放攻击以通过认证，例如图 2 中的攻击点②、④。

6.4 基于身份伪造和窃听的组合安全威胁

在生物特征身份鉴别系统中，攻击者可能结合身份伪造和窃听进行组合攻击，具体包括：

a) 攻击者通过窃听通信信道获取合法用户的生物特征模板，然后生成一个合法的恶意用户账号，并利用该账号对身份鉴别系统展开攻击；
b) 攻击者通过窃听信道获取合法用户的生物特征模板，从而冒充合法用户。

6.5 基于服务可用性的安全威胁

在生物特征身份鉴别系统中，攻击者可能针对认证服务器等设备展开攻击，导致身份鉴别系统无法正常工作。具体包括：

a) 攻击者通过发送大量信息以堵塞合法用户的认证请求，令合法用户无法正常提交认证请求，最终导致认证服务不可用，例如图 2 中的攻击点②；
b) 攻击者通过对传感器等设备实施物理破坏，导致物联网终端无法正常工作，例如图 2 中的攻击点①；
c) 攻击者通过盗窃终端设备并通过破解以获取用户的生物特征，例如图 2 中的攻击点①；
d) 攻击者利用木马病毒将预先选定好的模板直接覆盖特征提取器的处理结果，也称为假冒攻击，例如图 2 中的攻击点③。

7 安全要求

7.1 安全分级

本文件将生物特征模板使用的基本功能、性能和安全要求分为基本级和增强级。增强级要求包括了基本级要求的内容。

本文件中凡涉及密码算法的相关内容，按国家有关法律实施；凡涉及采用密码技术解决机密性、完整性、真实性、不可否认性需求的应符合密码相关国家标准和行业标准。

7.2 生物特征模板安全基本原则

生物特征模板控制者在使用生物特征模板时应遵守合法、正当、必要的原则，具体包括：采取技术和其他必要措施保障生物特征模板的安全，确保生物特征主体个人的权益不受侵害，保护生物特征模板

的安全性、完整性和可用性；具有明确、清晰、具体的生物特征数据使用目的；以清晰易懂的方式公开生物特征模板的使用范围、目的和规则，接受外部监督。

7.3 基本级要求

7.3.1 生物特征采样数据脱敏

生物特征数据在采集后应该进行脱敏操作，包括但不限于：

a) 在采集后对模板数据应使用无损或有损的脱敏机制进行相关操作，降低模板数据的敏感性；
b) 脱敏的数据，应能满足如下安全级别：无法利用这些数据做重构、爬山等欺骗攻击，进而无法威胁所有用户所注册的生物特征识别系统；
c) 应在对生物特征模板脱敏之后，及时删除脱敏之前的原始生物特征模板，让原始的特征模板仅存在于采集阶段；
d) 应采用可抗模板碰撞攻击、重放攻击的脱敏机制，保证统一原始模板不同的脱敏结果模板无关联性。

7.3.2 生物特征数据记录加密

生物特征数据在进行存储时应进行加密操作，包括但不限于：

a) 生物特征识别认证端存储的生物特征模板必须经过加密以密文的形式存储于数据库中；
b) 应在存储数据库被攻破的前提下，能够抵抗重放攻击、模板碰撞攻击、密钥反演攻击等攻击方式，保证密文模板之间的无关联性；
c) 应让攻击者根据密文模板进行重构、模板碰撞等欺骗攻击时的拒绝率达到相应规范中的要求。例如，GB/T 38671—2020 中规定人脸识别的活体检测攻击拒绝率应不小于 99%。

7.3.3 全生存周期中密文传输

生物特征数据在进行传输时应使用密文传输，包括但不限于：

a) 在整个生物特征模板的生存周期，通信信道中传输的生物特征模板应进行加密，以密文的形式传输；
b) 应进行加入时间戳、签名等措施抵抗中间人攻击等传送过程攻击；
c) 应保证信道被窃听或者信道被恶意控制的情况下，传输的密文生物特征模板不会泄露用户原始生物特征模板的任何信息；
d) 注册及认证过程中应保证传输模板之间无关联，能够抵抗模板碰撞等攻击。

7.3.4 分布式环境下的安全性要求

在分布式环境下，模板在存储或比对的过程中均应需要满足应有的安全要求，确保用户生物特征模板的保密性和完整性不被非法窃取或篡改。

模板存储或比对的位置是可选的，不同的位置有其不同的优势和劣势。针对云端、本地、分布式等部署方式，模板需要满足以下几个安全要求：

a) 模板存储时应该以密文的形式进行存储；
b) 模板比对时应该以密文的形式进行比对；
c) 用户的生物特征模板与用户的身份标识信息应该分库存储，满足不可链接性；
d) 在比对阶段，比对模块拿到的特征模板应该是满足不可逆性，并且模板之间应该是不可链接的。

7.4 增强级要求

7.4.1 生物特征采样数据脱敏

生物特征数据在采集后应该进行脱敏操作，包括但不限于：

a) 在采集后对模板数据应使用无损或有损的脱敏机制进行相关操作，降低模板数据的敏感性；
b) 脱敏的数据，应能满足如下安全级别：无法利用这些数据做重构、爬山等欺骗攻击，进而无法威胁所有用户所注册的生物特征识别系统；
c) 应在对生物特征模板脱敏之后，及时删除脱敏之前的原始生物特征模板，让原始的特征模板仅存在于采集阶段；
d) 应采用可抗模板碰撞攻击、重放攻击的脱敏机制，保证统一原始模板不同的脱敏结果模板无关联性；
e) 脱敏后生物特征模板可抵抗机器学习分析，攻击者无法从中分析出生理、情绪等数据。

7.4.2 生物特征数据记录加密

生物特征数据在进行存储时应进行加密操作，包括但不限于：

a) 生物特征识别认证端存储的生物特征模板必须经过加密，以密文的形式存储于数据库中；
b) 应在存储数据库被攻破的前提下，能够抵抗重放攻击、模板碰撞攻击、密钥反演攻击等攻击方式，保证模板的密文之间的无关联性；
c) 应让攻击者根据密文模板进行重构、模板碰撞等欺骗攻击时的拒绝率达到相应规范中的要求。例如，GB/T 38671—2020 中规定人脸识别的活体检测攻击拒绝率应不小于 99%。

7.4.3 全生存周期中密文传输

生物特征数据在进行传输时应使用密文传输，包括但不限于：

a) 在整个生物特征模板的生存周期，通信信道中传输的生物特征模板应进行加密，以密文的形式传输；
b) 应进行加入时间戳、签名等措施抵抗中间人攻击等传送过程攻击；
c) 应保证信道被窃听或者信道被恶意控制的情况下，传输的密文生物特征模板不会泄露用户原始生物特征模板的任何信息；
d) 注册及认证过程中应保证传输模板之间无关联，能够抵抗模板碰撞等攻击；
e) 执行传输数据包验证功能，检验生物特征模板的完整性。

7.4.4 分布式环境下的安全性要求

在分布式环境下，模板在存储或比对的过程中均应需要满足应有的安全要求，确保用户生物特征模板的保密性和完整性，不被非法窃取或篡改。

模板存储或比对的位置是可选的，不同的位置有其不同的优势和劣势。针对云端、本地、分布式等部署方式，模板需要满足以下几个安全要求：

a) 模板存储时应该以密文的形式进行存储；
b) 模板比对时应该以密文的形式进行比对；
c) 用户的生物特征模板与用户的身份标识信息应该分库存储，满足不可链接性；
d) 在比对阶段，比对模块拿到的特征模板应该是满足不可逆性，并且模板之间应该是不可链接的。

8 管理要求

8.1 基本级要求

8.1.1 生物特征模板产生

生物特征模板在产生的过程中应满足：

a) 应为生物特征模板分配唯一的与用户对应的标识符；
b) 收集生物特征信息时，应向用户告知收集、使用生物特征信息的目的、方式和范围等规则，并获得用户的明示授权同意；
c) 生物特征模板产生前应排查数据库中是否有其他用户的模版与其相似度超过阈值，不同用户的生物特征模板不能相同；
d) 模板签发者应在所产生的生物特征模板中标明唯一的模板签发者身份标识；
e) 模板应包含足够的生物特征项，以保证能够满足上述生物特征模板识别的准确率；
f) 产生生物特征模板所需的各类参数应可通过上述安全要求进行修改和加强。

8.1.2 生物特征模板分发

生物特征模板的所有分发模式均应确保模板安全，包括但不限于：

a) 若使用集中模式，生物特征模板集中存储，应确认生物特征模板安全分发到集中存储的位置；
b) 若使用分布式，生物特征模板传输到多个地方，应确认模板安全分发到所有存储位置；
c) 若使用令牌模式，模板存储在可移动的媒体中，应确认模板被安全地注入到设备中且令牌被安全地签发给用户。

8.1.3 生物特征模板存储

生物特征模板的存储过程应满足：

a) 存储期限应为实现用户授权使用的目的所必需的最短时间，法律法规另有规定或者用户另行授权同意的除外；
b) 管理员应将用户身份标识与生物特征模板信息分开存储并加强访问和使用的管理权限；
c) 当管理者停止运营时，应将所存储的生物特征模板进行删除或匿名化处理。

8.1.4 生物特征模板终止

生物特征模板应能够终止使用，包括但不限于：

a) 应分配安全管理员拥有终止生物特征模板的权限；
b) 应规定安全管理员终止生物特征模板的安全策略；
c) 终止生物特征模板时应确认拥有者的身份和终止者的授权；
d) 当可行的时候，在发生生物特征模板终止的时候通知用户；
e) 用户应当有权力终止生物特征模板使用；
f) 当生物特征模板终止时，将对应的所有模板的实例被清除。

8.1.5 生物特征模板更新

生物特征模板更新的过程中应满足：

a) 生物特征模板更新前应终止当前生物特征模板；
b) 产生新生物特征模板后应确认成功分发；

c） 在更新过程应采取安全措施保证用户生物特征模板的安全；

d） 保证模板可撤销性：应给用户随时提供认证端模板撤销、重新注册、更换模板等服务，且保证前后模板无相关性。

8.2 增强级要求

8.2.1 生物特征模板产生

生物特征模板在产生的过程中应满足：

a） 只应将获准进行登记的用户的生物特征作为生物特征模板存入生物特征数据库；

b） 应为生物特征模板分配唯一的与用户对应的标识符；

c） 收集生物特征信息时，应向用户告知收集、使用生物特征信息的目的、方式和范围等规则，并获得用户的明示授权同意，**并应确保用户的明示同意是在其完全知情的基础上给出的；**

d） 生物特征模板产生前应排查数据库中是否有其他用户的模版与其相似度超过阈值，不同用户的生物特征模板不能相同；

e） 提供对生物特征模板签名的功能，标明唯一的登记模板签发者身份标识符；

f） 模板应包含足够的生物特征项，以保证能够满足上述生物特征模板识别的准确率；

g） 产生生物特征模板所需的各类参数应可通过上述安全要求进行修改和加强；

h） 应确保当其产生的登记模板因为某些原因不能使用时，最少数目和类型的可替代、降级鉴别要求可通过安全要求进行加强。

8.2.2 生物特征模板分发

生物特征模板的所有分发模式均应确保模板安全，包括但不限于：

a） 若使用集中模式，生物特征模板集中存储，应确认生物特征模板安全分发到集中存储的位置；

b） 若使用分布式，生物特征模板传输到多个地方，应确认模板安全分发到所有存储位置；

c） 若使用令牌模式，模板存储在可移动的媒体中，应确认模板被安全地注入到设备中且令牌被安全地签发给用户。

8.2.3 生物特征模板存储

生物特征模板的存储过程应满足：

a） 存储期限应为实现用户授权使用的目的所必需的最短时间，法律法规另有规定或者用户另行授权同意的除外；

b） 管理员应将用户身份标识与生物特征模板信息分开存储并加强访问和使用的管理权限；

c） 存储时应采用加密等安全措施，采用密码技术时应符合密码管理相关国家标准；

d） 当管理者停止运营时，应将所存储的生物特征模板进行删除或匿名化处理。

8.2.4 生物特征模板终止

生物特征模板应能够终止使用，包括但不限于：

a） 应分配安全管理员拥有终止生物特征模板的权限；

b） 应规定安全管理员终止生物特征模板的安全策略；

c） 终止生物特征模板时应确认拥有者的身份和终止者的授权；

d） 当可行的时候，在发生生物特征模板终止的时候通知用户；

e） 用户应当有权力终止生物特征模板使用；

f） 当生物特征模板终止时，将对应的所有模板的实例被清除。

8.2.5 生物特征模板更新

生物特征模板更新的过程中应满足：

a） 生物特征模板更新前应终止当前生物特征模板；

b） 产生新生物特征模板后应确认成功分发；

c） 在更新过程应采取安全措施保证用户生物特征模板的安全；

d） 保证模板可撤销性：应给用户随时提供认证端模板撤销、重新注册、更换模板等服务，且保证前后模板无相关性。

参考文献

[1] GB/T 26238-2010 信息技术 生物特征识别术语

[2] GB/T 29268.2-2012 信息技术 生物特征识别性能测试和报告 第2部分：技术与场景评价的测试方法

[3] GB/T 33767.1-2017 信息技术 生物特征样本质量 第1部分：框架

[4] ISO/IEC 29100 Information technology — Security techniques — Privacy framework