ICS 03.060
A11

团　　体　　标　　准

T/PCAC 0010-2021

移动金融基于声纹识别的安全应用评估规范

Testing specifications for voiceprint recognition based on security application for mobile finance

2021－06－29 发布　　2021－06－29 实施

中国支付清算协会　发布

目　　录

前　言

本规范由中国支付清算协会提出。

本标准由中国支付清算协会安全与技术标准专业委员会归口。

本标准起草单位：中国支付清算协会、清华大学、北京得意音通技术有限责任公司、公安部第三研究所、北京国家金融科技认证中心、国家应用软件产品质量监督检验中心、国家金融科技测评中心（银行卡检测中心）、中国银联股份有限公司、中国网络安全审查技术与认证中心。

本标准主要起草人：陈波、于沛、侯晓晨、高飞、薛宇、张媛、陈旭东、高展、郑方、邬晓钧、米青山、黄小妮、张艳、胡津铭、张健、李作全、孔昊、王秀君、张文博、李宇、邱雪涛、费志军、刘宇、魏少杰。

引　言

为保障手机银行等移动金融客户端应用软件声纹识别应用的标准符合性和安全性，中国人民银行组织相关单位制订了《JR/T 0164-2018 移动金融基于声纹识别的安全应用技术规范》，对于降低互联网金融的IT风险、保证互联网金融业务的连续性、提升终端用户体验、确保行业主管机构的有效监管，都具有非常积极的意义。

本评估规范依据JR/T 0164-2018中的功能、性能、安全要求，为金融行业安全建设和金融行业主管部门对声纹识别的安全技术评估提供参考，为第三方评估机构的安全检测评估提供指导和依据。

移动金融基于声纹识别的安全应用评估规范

1 范围

为保障在移动金融服务场景中声纹识别的安全应用，本文件规定声纹识别的功能、性能和安全等评估要求。

本文件适用于移动金融客户端应用软件利用声纹服务器开展声纹识别应用场景下，对客户端和声纹服务器的技术标准符合性和安全性评估，不包括电话或网络电话（VoIP）中涉及声纹识别的应用场景。其他证券、保险等金融类客户端应用软件可在适用场景中参照执行。

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。

GM/T 0021 动态口令密码应用技术规范

JR/T 0118 金融电子认证规范

JR/T 0164-2018 移动金融基于声纹识别的安全应用技术规范

3 术语和定义

GM/T 0021、JR/T 0118、JR/T 0164-2018界定的术语和定义适用于本文件。

4 声纹识别应用

4.1 概述

声纹识别是根据待识别语音的声纹特征鉴别该段语音所对应的说话人的过程，在移动金融服务中可用于用户的身份认证。

4.2 声纹识别应用流程

声纹识别应用流程应符合JR/T 0164-2018中4.2的规定。

4.3 声纹识别评估实施要求

为保证本文中评估项的评估结果在实际应用场景中具有参考价值，声纹识别系统的评估实施应符合附录E中的要求。

5 声纹服务器评估

5.1 功能评估

5.1.1 声纹注册

评估目的：检查声纹的注册过程，应包括语音信息的传输、声纹模型的建立、声纹特征存储和用户身份的绑定等。

评估方法：

1） 检查开发文档中对于声纹注册的相关要求及实现过程；
2） 查看传输时是否包含用户属性数据，如用户唯一性标识、移动设备标识等；
3） 查看存储的声纹模型或特征是否与用户属性数据形成映射关系。

通过标准：

1） 声纹信息在传输时包含用户的属性数据；注册时建立声纹模型，声纹模型或特征存储时与用户的属性数据形成映射关系。

5.1.2 声纹验证

评估目的：声纹的验证应包含动态声纹密码校验和声纹确认等，实现对关联账户主体身份的验证；动态声纹密码应由服务器端生成。

评估方法：

1） 检查开发文档中对于声纹验证的相关要求；
2） 查看声纹的验证功能是否包含动态声纹密码校验和声纹确认；
3） 查看动态声纹密码是否由服务器生成；
4） 查看动态声纹密码的有效期是否超过120秒；
5） 查看动态声纹密码的长度是否为6位或者8位；
6） 查看动态声纹密码是否可以连续重复；
7） 查看动态声纹密码在完成验证后是否及时清除。

通过标准：

1） 声纹的验证包含动态声纹密码校验和声纹确认。动态声纹密码由服务器生成、有效期不超过120秒、长度宜6位或者8位，动态声纹密码中的字符无连续重复，如″…11…″，服务器连续生成的动态声纹密码无重复；
2） 动态声纹密码在验证完成后被立即清除。

5.1.3 声纹变更

评估目的：应具有声纹的变更功能，即服务器端重新进行声纹模型训练以实现对原有声纹信息的更新。

评估方法：

1） 检查开发文档中对于声纹变更的相关要求；
2） 查看是否具有声纹变更的功能。

通过标准：

1） 系统具有根据定义的模型更新机制对声纹模型进行变更的功能。支持用户主动发起的声纹变更。

5.1.4 声纹注销

评估目的：应具有声纹的注销功能，且注销后应删除与用户相关的声纹信息或做匿名化处理，不应重复使用。

评估方法：

1） 检查开发文档中对于声纹注销的相关要求；
2） 查看声纹注销后是否删除或匿名化与用户相关的声纹信息，并查看是否可以重复使用。

通过标准：

1） 声纹注销后，立即删除或匿名化与用户相关的声纹信息，并且未重复使用。

5.2 性能评估

5.2.1 基本性能指标

评估目的：检查基本性能指标是否满足相关规范要求。

评估方法：

1) 检查开发文档中对于基本性能指标的相关要求；

——参考附录A建立语音样本库，查看声纹验证过程中的错误接受率(FAR)；

——参考附录A建立语音样本库，查看声纹验证过程中错误拒绝率(FRR)。

通过标准：

1) 基本性能指标同时满足FAR≤0.5%，FRR≤3.0%。

5.2.2 采样指标

评估目的：检查采样指标是否满足相关规范要求。

评估方法：

1) 检查开发文档中对于采样率和采样精度的相关要求；
2) 查看实际采样率和采样精度。

通过标准：

1) 系统支持采样率16kHz，采样精度16bit。

5.2.3 有效语音长度

评估目的：检查声纹注册和验证时的有效语音长度。

评估方法：

1) 检查开发文档中对于声纹注册和验证时有效语音长度的相关要求；
2) 查看实际声纹注册时的有效语音长度；
3) 查看实际声纹验证时的有效语音长度。

通过标准：

1) 系统进行声纹注册时要求有效语音长度宜大于等于5000ms，进行声纹验证时要求有效语音长度大于等于1000ms。

5.2.4 系统响应时间

评估目的：检查声纹注册和验证时的系统响应时间。

评估方法：

1) 检查开发文档中对于声纹注册和验证时系统响应时间的相关要求；
2) 查看开发文档，确认正常工作情况下系统在单台服务器上支持的最大并发数量，使用单台服务器进行声纹处理，按此最大并发数量进行测试，查看注册和验证的系统响应时间；

通过标准：

1) 声纹注册时的系统最大响应时间≤3000ms，声纹验证时的系统最大响应时间≤2000ms；
2) 在评估方法中描述的最大并发情况下系统可稳定运行48小时以上，且响应时间满足 1)中要求。

5.2.5 语音信息质量判断

评估目的：检查是否具有语音信息质量判断的能力。

评估方法：

1) 检查开发文档中对于语音信息质量判断机制的说明；
2) 通过尝试不同截幅比例、信噪比、完整程度的语音信息，查看是否可以判断该语音信息的质量。

通过标准：

1) 具有根据截幅比例、信噪比、完整程度等判断语音信息质量的能力。

5.2.6 抗噪音能力

评估目的：检查是否具有抗噪音能力。

评估方法：

1) 检查开发文档中对于抗噪音能力机制的描述；
2) 基于基本性能指标测试时设置的阈值等系统参数，参考附录B建立语音样本库，尝试在不同噪音环境下对声纹信息进行验证；使用FAR与FRR评价系统的抗噪音能力：
   ——检测环境噪音40-50分贝下的FAR、FRR；
   ——检测环境噪音51-60分贝下的FAR、FRR。

通过标准：

1) 具有在不同噪音环境下对声纹信息进行验证的能力，参考附录F，FAR、FRR数值越小表明抗噪音能力越强。

5.2.7 抗时变能力

评估目的：检查是否具有因时间变化而导致声音变化的正确处理能力。

评估方法：

1) 检查开发文档中关于抗时变能力的机制说明。
2) 基于基本性能指标测试时设置的阈值等系统参数，参考附录C建立语音样本库，尝试在一定时间变化范围内对相同声音来源的声纹信息进行验证。
3) 使用FAR与FRR评价系统的抗时变能力：
   ——检测3个月后的FAR、FRR；
   ——检测6个月后的FAR、FRR；
   ——检测9个月后的FAR、FRR；
   ——检测12个月后的FAR、FRR。

通过标准：

1) 具有在一定时间变化范围内对相同声音来源的声纹信息进行验证的能力，参考附录F，FAR、FRR数值越小表明抗时变能力越强。

5.3 安全评估

5.3.1 声纹信息采集

5.3.1.1 基本要求

评估目的：确保声纹信息采集满足相关安全要求。

评估方法：

1) 检查开发文档中关于声纹信息采集的安全要求；
2) 查看声纹信息采集时是否使用了动态声纹密码；
3) 查看在声纹注册时，声纹信息采集是否使用多组动态声纹密码。

通过标准：

1) 声纹信息在采集时使用动态声纹密码；声纹注册时，宜使用多组动态声纹密码采集声纹信息，但不宜超过5组。

5.3.2 声纹信息传输

评估目的：检查声纹信息在传输时是否可以保证传输过程中的安全性。

评估方法：

1) 查看声纹识别接口的调用情况。

通过标准：

1) 声纹识别接口仅限于服务器端之间内部调用，未暴露在公共、开放的网络上。

5.3.3 声纹信息存储

评估目的：评估声纹信息是否满足安全存储要求。

评估方法：

1) 查看服务器对于声纹模型的保存方式；
2) 查看服务器对留存语音信息的保护措施和对留存声纹模型信息的保存时间。

通过标准：

1) 服务器对声纹信息进行加密保存，并防止声纹模型的未授权访问、泄露、篡改或者毁损；
2) 服务器留存语音信息时进行了加密或采取高强度安全防护措施，防止语音信息的未授权访问、泄露、篡改或者毁损；对留存的语音信息进行去标识化或脱敏处理，确保对外不可用；
3) 服务器留存的声纹模型信息保存时间为实现目的所必需的最短时间。

5.3.4 声纹信息处理

5.3.4.1 基本要求

评估目的：评估声纹信息在处理时，是否满足安全要求。

评估方法：

1) 查看开发文档中对于声纹信息处理的安全要求；
2) 尝试对声纹模型配置参数进行非授权的访问和篡改；
3) 查看声纹注册、验证、变更和注销各个环节是否对关键操作信息进行日志记录；
4) 检查是否具有失败处理措施，并确认失败处理机制是否有效。

通过标准：

1) 采取有效措施防止声纹模型配置参数的未授权访问、泄露、篡改；
2) 声纹注册、验证、变更和注销各个环节对关键操作信息进行日志记录；
3) 具有合理的失败处理措施，具有限制失败次数的机制，如果超过限制次数，则触发相应的失败控制机制。

5.3.4.2 防攻击能力

评估目的：检查系统是否具备抵御常见攻击的能力。

评估方法：

1) 检查开发文档中关于抗攻击能力的安全要求；
2) 基于基本性能指标测试时设置的阈值等系统参数，参考附录D建立语音样本库，尝试通过语音模仿的方式，查看系统是否可以抵御语音模仿攻击；
3) 参考附录D建立语音样本库，尝试通过语音转换及合成的方式，查看系统是否可以抵御语音转换及合成攻击；
4) 参考附录D建立语音样本库，尝试通过录音的方式，查看系统是否可以抵御录音欺诈攻击；
5) 参考附录D建立语音样本库，尝试通过录音拼接的方式，查看系统是否可以抵御录音拼接欺诈攻击。
6) 使用FAR与FRR评价系统的防攻击能力。

通过标准：

1) 在声纹确认过程中，能够抵御攻击者模仿说话人、试图以说话人的身份通过声纹验证的攻击行为；
2) 在声纹确认过程中，能够抵御攻击者通过机械的、电子的方法产生人造语音的攻击行为，如语音转换及合成技术；
3) 在声纹确认过程中，能够抵御播放已录制好的目标用户声音并尝试通过声纹验证的攻击行为；
4) 在声纹确认过程中，能够抵御将已录制好的目标用户录音片段拼接成待验证语音播放并尝试通过声纹验证的攻击行为。
5) 参考附录F，FAR、FRR数值越小表明防攻击能力越强。

5.3.5 声纹信息删除

评估目的：检查声纹信息的删除是否满足相关安全要求。
评估方法：
1) 检查开发文档中关于声纹信息删除的安全要求；
2) 尝试删除声纹信息，查看删除后的声纹信息是否可以被检索、访问。
通过标准：
1) 删除后的声纹信息不可检索、访问。

6 客户端软件评估

6.1 功能评估

6.1.1 声纹注册

评估目的：检查声纹的注册过程，应包括语音信息的采集、传输等功能。
评估方法：
1) 检查开发文档中对于声纹注册的相关要求；
2) 查看用户在注册前是否需要对身份进行认证；
3) 查看用户在注册前是否取得用户的明示同意；
4) 查看传输时是否包含用户属性数据，如用户唯一性标识、移动设备标识等；
5) 查看注册完成后，注册用声纹信息是否被及时清除。
通过标准：
1) 具有声纹注册功能，声纹注册前对用户身份进行认证、且经过用户的明示同意；
2) 声纹信息在传输时包含用户的属性数据。注册完成后，注册用声纹信息被立即清除。

6.1.2 声纹验证

评估目的：声纹的验证应包含动态声纹密码校验和声纹确认等，实现对关联账户主体身份的验证。
动态声纹密码应由服务器端生成。
评估方法：
1) 检查开发文档中对于声纹验证的相关要求；
2) 查看声纹的验证功能是否包含动态声纹密码校验和声纹确认；
3) 查看动态声纹密码是否由服务器生成；
4) 查看动态声纹密码的有效期是否超过120秒；
5) 查看动态声纹密码的长度是否为6位或者8位；
6) 查看动态声纹密码是否可以连续重复。
通过标准：
1) 声纹的验证包含动态声纹密码校验和声纹确认；

2) 动态声纹密码由服务器生成、有效期不超过120秒、长度宜6位或者8位，动态声纹密码中的字符无连续重复，如″…11…″，服务器连续生成的动态声纹密码无重复。

6.1.3 声纹变更

评估目的：应具有声纹的变更功能，即服务器端重新进行声纹模型训练以实现对原有声纹信息的更新。

评估方法：

1) 检查开发文档中对于声纹变更的相关要求；
2) 查看是否具有声纹变更的功能；
3) 用户主动发起变更前是否对用户身份进行认证；
4) 用户主动发起变更前是否取得用户的明示同意。

通过标准：

1) 具有声纹变更的功能，发起变更前应对用户身份进行认证、并且取得用户的明示同意。

6.1.4 声纹注销

评估目的：应具有声纹的注销功能，且注销后应删除与用户相关的声纹信息或做匿名化处理，不应重复使用。

评估方法：

1) 检查开发文档中对于声纹注销的相关要求；
2) 查看声纹信息控制者主动发起对声纹的注销功能时，是否明确告知用户注销原因、注销时间及注销后声纹信息处理方式；
3) 查看用户主动发起对声纹的注销功能前，是否对用户身份进行认证并且取得用户的明示同意；
4) 查看声纹注销后是否删除与用户相关的声纹信息，并查看是否可以重复使用。

通过标准：

1) 声纹信息控制者主动发起对声纹的注销时，明确告知用户注销原因、注销时间及注销后声纹信息处理方式；
2) 用户主动发起对声纹的注销前，对用户身份进行认证并且取得用户的明示同意，告知用户注销后声纹信息的处理方式；
3) 声纹注销后，立即删除与用户相关的声纹信息或做匿名化处理，并且不应重复使用。

6.2 性能评估

6.2.1 采样指标

评估目的：检查采样指标是否满足相关规范要求。

评估方法：

1) 检查开发文档中对于采样率和采样精度的相关要求；
2) 查看实际采样率和采样精度。

通过标准：

1) 采样率为16kHz，采样精度为16bit。

6.3 安全评估

6.3.1 声纹信息采集

6.3.1.1 基本要求

评估目的：确保声纹信息采集满足相关安全要求。

评估方法：

1) 检查开发文档中关于声纹信息采集的安全要求；
2) 查看声纹信息采集时是否使用了动态声纹密码；
3) 查看采集完成后，是否立即对声纹信息进行加密处理；
4) 尝试通过其他设备或者程序非授权获取声纹信息，验证是否成功；
5) 尝试通过其他设备或者程序篡改声纹信息，验证是否成功；
6) 查看在声纹注册时，声纹信息采集是否使用多组动态声纹密码。

通过标准：

1) 声纹信息在采集时使用动态声纹密码。采集完成后，立即对声纹信息进行加密处理。无法通过其他设备或者程序非授权获取声纹信息，无法通过其他设备或者程序篡改声纹信息。声纹注册时，宜使用多组动态声纹密码采集声纹信息，但不宜超过5组。

6.3.1.2 身份认证要求

评估目的：声纹注册采集语音信息前，是否使用多种要素验证用户身份。

评估方法：

1) 检查开发文档中对于声纹注册采集语音前身份认证的相关要求；
2) 查看声纹注册采集语音信息前，采用何种方式验证用户身份。

通过标准：

1) 身份认证满足以下方式之一：
   ——采用符合 JR/T 0118 的数字证书，并组合交易密码等至少一种其他认证要素；
   ——采用符合 GM/T 0021 的动态令牌设备，并组合交易密码等至少一种其他认证要素；
   ——至少组合两种认证要素（其中至少一种为动态认证要素，如动态验证码、基于客户行为的动态挑战应答等），并采用短信、数据（如手机银行、即时通讯、邮件）等至少两种不同通信渠道。

6.3.1.3 明示同意要求

评估目的：声纹信息采集前，是否向用户明示，明确告知声纹信息收集、使用信息的目的、方式和范围。

评估方法：

1) 检查开发文档中对于明示同意的相关规定；
2) 尝试采集用户的声纹信息，查看采集声纹信息前是否需要用户的明示同意；
3) 查看明示信息中是否明确告知用户声纹信息收集、使用信息的目的、方式和范围。

通过标准：

1) 在采集用户声纹信息前，向用户明确告知声纹信息收集、使用信息的目的、方式和范围。

6.3.2 声纹信息传输

评估目的：检查声纹信息在传输时是否可以保证传输过程中的安全性。

评估方法：

1) 检查开发文档中关于声纹信息传输的安全要求；
2) 查看传输时采用的协议是否为安全的网络通讯协议。

通过标准：

1) 采用安全传输协议，保证声纹信息传输时的完整性和保密性。

6.3.3 声纹信息存储

评估目的：评估声纹信息是否满足安全存储要求。

评估方法：

1) 检查开发文档中对于声纹信息存储的安全要求；
2) 查看客户端应用软件是否留存声纹信息；
3) 查看制度文档中关于发生声纹信息遗失、泄露或者毁损等情况时所采取的补救措施；
4) 查看制度文档中关于声纹境内存储和向境外提供的要求。

通过标准：

1) 客户端应用软件未留存任何形式的声纹信息，声纹信息包含但不限于声纹注册、声纹验证、变更等过程中使用的声纹信息；
2) 制度文档中具有对发生声纹信息遗失、泄露或者毁损等情况的补给措施，并及时告知用户。境内运营中采集和产生的声纹信息境内存储，制度文档中具有向境外提供的相关安全规定，且满足法律法规要求。

6.3.4 声纹信息处理

6.3.4.1 基本要求

评估目的：评估声纹信息在处理时，是否满足安全要求。

评估方法：

1) 查看开发文档中对于声纹信息处理的安全要求；
2) 查看在发起声纹变更、注销前是否需要验证用户身份；
3) 检查是否具有失败处理措施，并确认失败处理机制是否有效；
4) 检查制度文档中对于声纹信息的使用范围以及安全保护的规定。

通过标准：

1) 用户主动发起声纹变更、注销前，采用了JR/T 0164—2018 7.1.2 中要求的身份认证方式验证用户身份；
2) 具有合理的失败处理措施，在失败时进行相应提示并限制连续失败次数（宜不超过5次），如果超过限制次数，则触发相应的失败控制机制；
3) 除法律规定外，声纹信息未被转让，未用于声纹注册、验证、变更、注销之外的其他用途；未向其他客户端应用软件提供声纹信息。

附 录 A

为了验证FAR和FRR等指标，需要建立一个专门的语音样本库用于测试。语音样本库是指包含一定数量的对声纹确认算法进行性能评测的语音样本的集合。

本测试集所有语音录制需要在安静室内环境进行采集。

具体要求包括：

a) 语音样本库应充分考虑性别、年龄、地域分布、不同拾音设备等因素；

b) 采集对象人数不少于500人；

c) 语音内容采用动态声纹密码，生成过程及内容应符合采集要求；

d) 每人采集10段语音用于声纹注册，采集10段语音用于声纹确认。

附 录 B

为了验证系统的抗噪音能力，需要建立一个专门的语音样本库用于测试。语音样本库是指包含一定数量的对声纹确认算法进行性能评测的语音样本的集合。

具体要求包括：

a) 语音样本库应充分考虑不同噪音来源（交通运输噪声、工业机械噪声、城市建筑噪声、社会生活和公共场所噪声、家用电器造成的室内噪声等）、不同噪音强度、不同拾音设备等因素；

b) 采集对象人数不少于50人；

c) 语音内容采用动态声纹密码，生成过程及内容应符合采集要求；

d) 每人在安静室内环境下采集10段语音用于声纹注册，每人在安静室内环境下采集10段语音用于声纹验证，基于不同噪音来源，每人在不同噪音强度下（40分贝-50分贝、51分贝-60分贝）分别采集10段语音，用于抗噪音能力的验证。

附 录 C

为了验证系统的抗时变能力，需要建立一个专门的语音样本库用于测试。语音样本库是指包含一定数量的对声纹确认算法进行性能评测的语音样本的集合。

本测试集所有语音录制需要在安静室内环境进行采集。

具体要求包括：

a) 语音样本库应充分考虑性别、起始采样时的年龄、时间变化、不同拾音设备等因素；

b) 采集对象人数不少于50人；

c) 语音内容采用动态声纹密码，生成过程及内容应符合采集要求；

d) 每人分别在连续12个月内每月进行采集：首月每人采集10段语音用于声纹注册，每人采集10段语音用于声纹验证；后续月份每人采集10段语音，用于抗时变能力的验证。

附 录 D

为了验证系统的抗攻击能力，需要建立四个专门的语音样本库用于测试。语音样本库是指包含一定数量的对声纹确认算法进行性能评测的语音样本的集合。

本测试集所有语音录制需要在安静室内环境进行采集并考虑使用不同拾音设备。

具体要求包括：

a) 防语音模仿攻击语音样本库

——模仿人与被模仿人人数各不少于20人；

——语音内容采用动态声纹密码，生成过程及内容应符合采集要求；

——在安静录音环境下，每个被模仿人采集10段语音用于声纹注册，每个被模仿人采集10段语音用于被模仿，每个模仿人按照对应被模仿人说话方式、语气语调等采集10段语音，用于防语音模仿能力的验证。

b) 防语音转换及合成攻击语音样本库

——采集对象人数不少于20人；

——语音内容采用动态声纹密码，生成过程及内容应符合采集要求；

——在安静录音环境下，每人采集10段语音用于声纹注册，每人分别采集10段转换及合成后的语音和正常语音，用于防语音转换及合成能力的验证。

c) 防录音欺诈攻击语音样本库

——采集对象人数不少于20人；

——语音内容采用动态声纹密码，生成过程及内容应符合采集要求；

——在安静录音环境下，每人采集10段语音用于声纹注册，每人分别采集10段录音和正常语音用于声纹验证，用于防录音欺诈的验证。

d) 防录音拼接欺诈攻击语音样本库

——采集对象人数不少于20人；

——语音内容采用动态声纹密码，生成过程及内容应符合采集要求；

——在安静录音环境下，每人采集10段语音用于声纹注册，每人分别采集10段录音用于声纹验证和拼接合成，使用语音拼接工具对语音进行拼接生成10段待验证语音，用于防录音拼接欺诈的验证。

附 录 E

声纹识别系统评估实施要求如下：

a) 部署要求

——声纹厂商负责送检系统的部署调试，部署调试完成后，不应再重新设置系统，直至检测结束。如出现测试不通过，检测机构须重置测试服务器，清空所有数据，由声纹厂商重新部署调整后，再次开始测试；

——检测机构应在同一配置的声纹识别系统中，完成所有评估条款。

b) 语音集准备

为了测试基本性能指标、语音质量评估、抗噪音、抗时变、防攻击等评估项，检测机构应按附录A-D中的要求准备相应性能评估的语音数据集，语音数据来源应可靠（避免出现数据作弊情况），语音数据经人工检查标注无误。

c) 测试用例生成

应按如下2个步骤生成完整测试用例。

——检测机构基于A-D语音样本库独立地生成随机顺序的4类测试用例列表。每类测试用例列表生成生成时均需注意：

应保证每个说话人的声纹注册用例在该说话人的声纹验证用例之前；

避免将全部声纹注册用例排列在一起，不同说话人的声纹注册用例与声纹验证用例随机交叉；

应控制声纹验证测试的正例与反例比例，避免某类用例数量过少；

抗时变测试用例列表中应保证每个说话人的验证语音是按时间间隔由小到大排列。

——检测机构应将基于A-D语音样本库生成的各个测试用例列表随机合并，生成一个完整的全项测试用例列表，用于声纹识别测试。

d) 测试记录及结果统计

检测机构应使用统一的声纹注册和声纹验证接口对完整的全项测试用例列表进行测试，记录每一个用例的系统输出结果和用时，统计结果时按基本性能指标、语音质量评估、抗噪音、抗时变、防攻击等评估项分开独立进行统计。

提取基本性能指标相关的测试记录，得到FAR≤0.5%条件下的阈值与相应FRR值。

基于上述条件下获取的阈值，确定语音质量检测、抗噪音、抗时变、防攻击等检测项的检测结果。

声纹识别系统服务出现故障即为评估结束，测试不通过。

分别绘制整个测试过程中声纹注册和声纹验证的系统响应时间曲线，标记声纹注册的平均系统响应时间和声纹验证的平均系统响应时间。

记录整个测试过程中，系统的CPU、内存占用情况。

附 录 F

声纹识别系统抗噪音能力建议参考范围：

环境噪音强度	FAR	FRR
40-50分贝	≤0.5%	≤3.0%
51-60分贝	≤0.5%	≤3.3%

声纹识别系统抗时变能力建议参考范围：

时间变化范围	FAR	FRR
3个月后	≤0.5%	≤5.0%
6个月后	≤0.5%	≤5.0%
9个月后	≤0.5%	≤5.0%
12个月后	≤0.5%	≤5.0%

声纹识别系统抗攻击能力建议参考范围：

声纹攻击类型	FAR	FRR
语音模仿	≤0.5%	≤3.0%
语音转换及合成	≤0.5%	≤3.0%
录音欺诈	≤0.5%	≤3.0%
录音拼接欺诈	≤0.5%	≤3.0%

参 考 文 献

[1] 中华人民共和国网络安全法（全国人民代表大会常务委员会 2016年11月7日发布，2017年6月1日实施）

[2] GB/T 25069—2010 信息安全技术 术语

[3] GB/T 35273—2017 信息安全技术 个人信息安全规范

[4] GA/T 893—2010 安防生物特征识别应用术语

[5] GA/T 1179—2014 安防声纹确认应用算法技术要求和测试方法

[6] JR/T 0068—2012 网上银行系统信息安全通用规范

[7] JR/T 0071—2012 金融行业信息系统信息安全等级保护实施指引

[8] JR/T 0092—2012 中国金融移动支付 客户端技术规范

[9] SJ/T 11380—2008 自动声纹识别（说话人识别）技术规范

[10] JR/T 0171—2020 个人金融信息保护技术规范