ICS 33.050
CCS M 30

团　体　标　准

T/TAF 012—2023
代替 T/TAF 012—2017

移动智能终端指纹框架接口测试方法

Test methods for fingerprint framework interface of smart mobile terminal

2023-02-08 发布　　2023-02-08 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。

本文件代替T/TAF 012—2017《移动智能终端指纹框架接口测试方法》，与T/TAF 012—2017相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 增加了可信执行环境术语和定义（见 3.1）；
b) 增加了富执行环境术语和定义（见 3.2）；
c) 增加了错误接受率术语和定义（见 3.3）；
d) 增加了错误拒绝率术语和定义（见 3.4）；
e) 增加了国密算法测试要求（见 7.3.10、7.3.11）。

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：蚂蚁科技集团股份有限公司、中国信息通信研究院、荣耀终端有限公司、华为技术有限公司、郑州信大捷安信息技术股份有限公司、安谋科技（中国）有限公司。

本文件主要起草人：林冠辰、彭晋、李志雄、张武、窦方钰、朱凯、邱晗若、傅山、王嘉义、魏凡星、邓太生、李志超、王思善、刘为华、王骏超。

本文件及其所代替文件的历次版本发布情况为：

——本文件于2017年首次发布；
——本次为第一次修订。

移动智能终端指纹框架接口测试方法

1 范围

本文件规范了移动智能终端REE指纹接口的测试架构和测试方法，包括测试环境和测试案例。

本文件适用于移动智能终端REE指纹接口的测试。

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 41388-2022 信息安全技术 可信执行环境 基本安全规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

可信执行环境 trusted execution environment

移动智能终端上基于硬件级隔离及安全启动机制，为确保安全敏感应用相关数据和代码的机密性、完整性、真实性和不可否认性目标构建的一种软件运行环境。

注：硬件级隔离是指基于硬件安全扩展机制，通过对计算资源的固定划分或动态共享，保证隔离资源不被富执行环访问的一种安全机制。

[来源：GB/T 41388-2022，3.3，有改写]

3.2

富执行环境 rich execution environment

移动智能终端上为应用程序提供基础功能和计算资源的一种软件软件环境。

注：富执行环境是相对可信执行环境独立存在的运行环境。

[来源：GB/T 41388-2022，3.4，有改写]

3.3

错误接受率 false acceptance rate

指纹样本特征与存储的指纹模板的比对过程中，发生错误接受结果的比对次数与总比对次数的比值。

3.4

错误拒绝率 false rejection rate

指纹样本特征与存储的指纹模板的比对过程中，发生错误拒绝结果的比对次数与总比对次数的比值。

4 缩略语

下列缩略语适用于本文件。

API：应用程序接口（Application Program Interface）
FAR：错误接受率（False Acceptance Rate）
FRR：错误拒绝率（False Rejection Rate）
REE：富执行环境（Rich Execution Environment）

5 系统技术架构

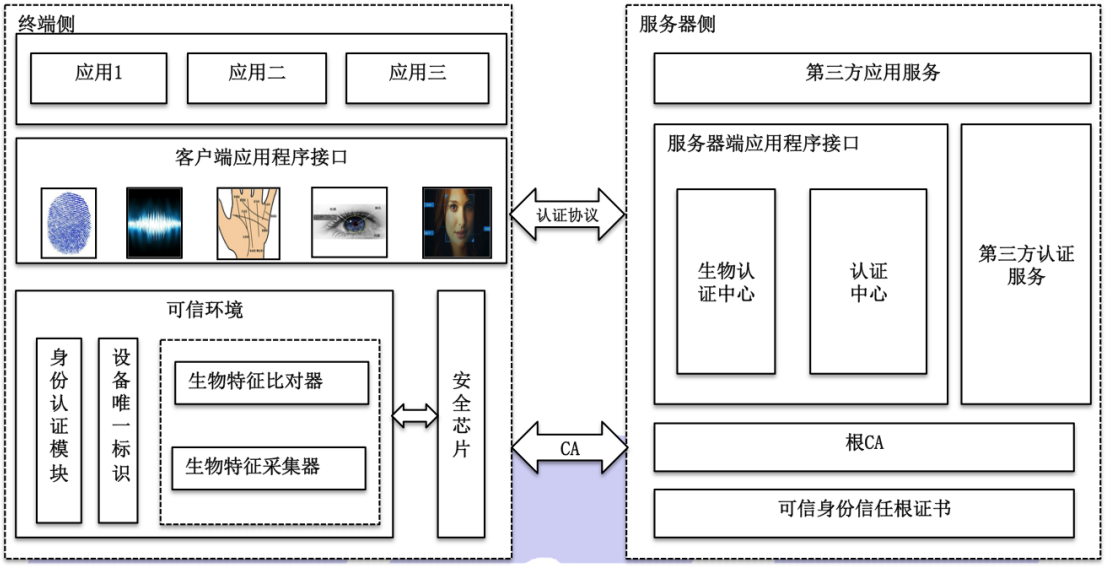

图1 系统技术架构

基于生物识别的移动智能终端身份认证技术架构见图1。架构包含两部分，终端侧及服务器侧。终端侧包含应用业务层、生物识别中间件、及安全基础层。服务器侧包含应用业务服务层、生物识别认证服务及第三方认证服务层、根 CA 及可信身份信任根证书。生物识别应用层通过认证协议完成身份认证，PKI 作为底层基础设施提供完整性、安全性及可追溯性。

6 测试坏境

6.1 测试架构

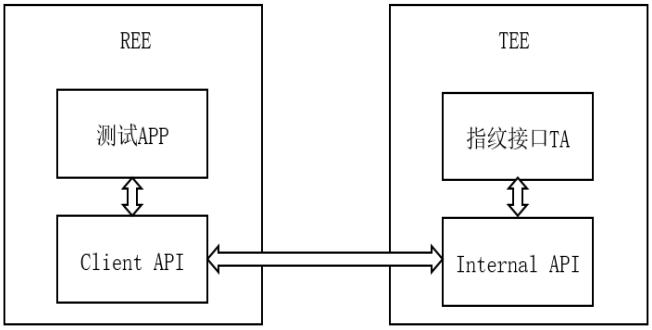

图2 测试架构

测试架构见图2。通过在REE开发测试APP，执行核心案例，实现指纹框架接口测试，具体测试架构如图2所示。

6.2 测试要求

应满足在 FAR≤1/50000 的情况下 FRR≤3%。

7 测试要求

7.1 测试错误码

测试错误码见表1。

表1 测试错误码

错误码	值	说明
ERR_SUCCESS	0x00000000	成功
ERR_UNKNOWN	0x7A000001	未知错误
ERR_BAD_ACCESS	0x7A000002	访存错误
ERR_BAD_PARAM	0x7A000003	参数错误
ERR_UNKNOWN_CMD	0x7A000004	不能识别的命令
ERR_BUF_TOO_SHORT	0x7A000005	Buffer长度不足
ERR_OUT_OF_MEM	0x7A000006	内存分配失败
ERR_TIMEOUT	0x7A000007	超时错误
ERR_HASH	0x7A000008	Hash错误
ERR_SIGN	0x7A000009	签名错误
ERR_VERIFY	0x7A00000A	验签错误
ERR_KEY_GEN	0x7A00000B	生成密钥错误
ERR_READ	0x7A00000C	读文件错误
ERR_WRITE	0x7A00000D	写文件错误
ERR_ERASE	0x7A00000E	删除文件错误
ERR_NOT_MATCH	0x7A00000F	生物特征本地不匹配
ERR_GEN_RESPONSE	0x7A000010	生成返回值失败
ERR_GET_DEVICEID	0x7A000011	获取设备ID失败
ERR_GET_LAST_IDENTIFIED_ID	0x7A000012	获取最近一次认证通过结果失败
ERR_AUTHENTICATOR_SIGN	0x7A000013	Authenticator签名失败
ERR_GET_ID_LIST	0x7A000014	获取id列表失败
ERR_UN_INITIALIZED	0x7A000015	未初始化错误
ERR_NO_OPTIONAL_LEVEL	0x7A000016	本地无服务端支持的level

7.2 接口测试

7.2.1 获取设备 ID

测试方法如下：

a) 测试编号：7.2.1；
b) 测试项目：获取设备 Id 测试；
c) 项目要求：验证是否满足定义的获取设备 Id 接口要求；
d) 测试条件：应提供获取设备 Id 的测试说明；
e) 测试步骤：验证获取设备 Id 是否满足规范要求。具体测试步骤如下：
   1) 步骤 1：调用获取设备 Id 并暂存结果；
   2) 步骤 2：调用获取设备 Id 并暂存结果；
   3) 步骤 3：比较步骤 1 的结果和步骤 2 的暂存结果；
   4) 步骤 4：重复步骤 2-3。

f） 预期结果：执行完步骤 3 之后，如果结果均相等，则该评测结果为“未见异常”，否则评测结果为“异常”。

7.2.2 获取设备型号

测试方法如下：

a） 测试编号：7.2.2；
b） 测试项目：获取设备型号测试；
c） 项目要求：验证是否满足定义的获取设备型号接口要求；
d） 测试条件：应提供获取设备型号的测试说明；
e） 测试步骤：验证获取设备型号是否满足规范要求。具体测试步骤如下：
   1） 步骤 1：调用获取设备型号接口并暂存结果；
   2） 步骤 2：调用获取设备型号接口并暂存结果；
   3） 步骤 3：比较步骤 1 的暂存结果和步骤的暂存结果；
   4） 步骤 4：重复步骤 2-3。
f） 预期结果：执行完步骤 3 之后，如果结果均相等，则评测结果为“未见异常”，否则评测结果为“异常”。

7.2.3 获取客户端协议版本

测试方法如下：

a） 测试编号：7.2.3；
b） 测试项目：获取客户端协议版本测试；
c） 项目要求：验证是否满足定义的获取客户端协议版本接口要求；
d） 测试条件：应提供获取客户端协议版本的测试说明；
e） 测试步骤：验证获取客户端协议版本是否满足规范要求。具体测试步骤如下：
   1） 步骤 1：调用获取客户端协议版本并暂存结果；
   2） 步骤 2：调用获取客户端协议版本并暂存结果；
   3） 步骤 3：比较步骤 1 的暂存结果和步骤 2 的暂存结果；
   4） 步骤 4：重复步骤 2-3。
f） 预期结果：执行完步骤 3 后，如果结果均相等，则该评测结果为“未见异常”。否则评测结果为“异常”。

7.2.4 获取客户端支持的生物验证类型

测试方法如下：

a） 测试编号：7.2.4；
b） 测试项目：获取客户端支持的生物验证类型接口测试；
c） 项目要求：验证是否满足定义的获取客户端支持的生物验证类型接口要求；
d） 测试条件：应提供获取客户端支持的生物验证类型接口的测试说明；
e） 测试步骤：验证获取客户端支持的生物验证类型接口是否满足规范要求。具体测试步骤如下：
   1） 步骤 1：在支持指纹的设备上调用该接口并暂存结果；
   2） 步骤 2：相同设备上调用该接口并暂存结果；
   3） 步骤 3：比较步骤 1 的暂存结果和步骤 2 的暂存结果；
   4） 步骤 4：重复步骤 2-3。
f） 预期结果：执行完步骤 3 后，如果比较结果均相等且结果为支持指纹，则评测结果为“未见异常”，否则结果为“异常”。

7.2.5 启动指纹/虹膜管理应用

测试方法如下：

a） 测试编号：7.2.5；

b) 测试项目：启动指纹/虹膜管理应用测试；
c) 项目要求：验证是否满足定义的启动指纹/虹膜管理应用的接口要求；
d) 测试条件：应提供启动指纹/虹膜管理应用的测试说明；
e) 测试步骤：验证启动指纹/虹膜管理应用是否满足规范要求。具体测试步骤如下：
   1) 步骤 1：在支持指纹的设备上以指纹为入参调用该接口，暂存结果；
   2) 步骤 2：在支持指纹的设备上以虹膜为入参调用该接口，暂存结果；
   3) 步骤 3：在支持虹膜的设备上以虹膜为入参调用该接口，并暂存结果；
   4) 步骤 4：在支持虹膜的设备上以指纹为入参调用该接口，并暂存结果。
f) 预期结果：步骤 1 的结果为成功，且步骤 2 的结果为失败，且步骤 3 的结果为成功，且步骤 4 的结果为失败，则评测结果为“未见异常”，否则，评测结果为“异常”。

7.2.6 获取校验数据测试

测试方法如下：

a) 测试编号：7.2.6；
b) 测试项目：获取校验数据测试；
c) 项目要求：验证 TA 是否满足定义的获取校验数据接口要求；
d) 测试条件：应提供获取校验数据的测试说明；
e) 测试步骤：验证获取校验数据接口是否满足规范要求。具体测试步骤如下：
   1) 步骤 1：在不支持任何生物验证的设备上调用该接口并暂存结果；
   2) 步骤 2：在仅支持指纹验证的设备上调用该接口并暂存结果；
   3) 步骤 3：在仅支持虹膜验证的设备上调用该接口并暂存结果；
   4) 步骤 4：在同时支持指纹和虹膜验证的设备上调用该接口并暂存结果。
f) 预期结果：步骤 1 的结果为空，且步骤 2 的结果为指纹数据，且步骤 3 的结果为虹膜数据，且步骤 4 的结果为指纹+虹膜数据，则该评测为“未见异常”。否则评测结果为“异常”。

7.2.7 指纹注册测试

测试方法如下：

a) 测试编号：7.2.7；
b) 测试项目：指纹注册接口测试；
c) 项目要求：验证是否满足定义的指纹注册接口要求；
d) 测试条件：应提供指纹注册接口的测试说明；
e) 测试步骤：验证指纹注册接口是否满足规范要求。具体测试步骤如下：
   1) 步骤 1：构造服务端数据为入参，在支持指纹的设备上调用该接口；
   2) 步骤 2：用错误的手指验证并暂存结果；
   3) 步骤 3：重复步骤 2 多次并暂存结果；
   4) 步骤 4：重新调用该接口并使用正确的手指验证并暂存结果；
   5) 步骤 5：构造伪造签名的数据为入参，调用该接口并暂存结果。
f) 预期结果：步骤 2 的结果为“提示用户重试”，且步骤 3 的结果为“校验失败”，且步骤 4 的结果为“校验成功”，且步骤 5 的结果为“校验失败”，则该评测为“未见异常”。否则评测结果为“异常”。

7.2.8 指纹校验

测试方法如下：

a) 测试编号：7.2.8；
b) 测试项目：指纹校验测试；
c) 项目要求：验证是否满足定义的指纹校验接口要求；
d) 测试条件：应提供指纹校验接口的测试说明；
e) 测试步骤：验证指纹校验接口是否满足规范要求。具体测试步骤如下：
   1) 步骤 1：构造服务端数据为入参，在支持指纹的设备上调用该接口；
   2) 步骤 2：用错误的手指验证并暂存结果；

3) 步骤 3：重复步骤 2 多次并暂存结果；
4) 步骤 4：重新调用该接口并使用正确的手指验证并暂存结果；
5) 步骤 5：构造伪造签名的数据为入参，调用该接口并暂存结果。

f) 预期结果：步骤 2 的结果为“提示用户重试”，且步骤 3 的结果为“校验失败”，且步骤 4 的结果为“校验成功”，且步骤 5 的结果为“校验失败”，则该评测为“未见异常”。否则评测结果为“异常”。

7.2.9 指纹注销

测试方法如下：

a) 测试编号：7.2.9；
b) 测试项目：指纹注销测试；
c) 项目要求：验证是否满足定义的指纹注销的接口要求；
d) 测试条件：应提供指纹注销接口的测试说明；
e) 测试步骤：验证指纹注销接口是否满足规范要求。具体测试步骤如下：
1) 步骤 1：构造服务端数据为入参，在支持指纹的设备上调用该接口；
2) 步骤 2：构造伪造签名的数据为入参，调用该接口并暂存结果。
f) 预期结果：步骤 1 的结果为“校验成功”，且步骤 2 的结果为“校验失败”，则该评测为“未见异常”。否则评测结果为“异常”。

7.3 性能测试

7.3.1 获取设备型号性能

测试方法如下：

a) 测试编号：7.3.1；
b) 测试项目：获取设备型号接口的性能测试；
c) 项目要求：验证是否满足定义的获取设备型号接口的性能要求；
d) 测试条件：应提供获取设备型号性能的测试说明；
e) 测试步骤：验证获取设备型号接口的性能是否满足规范要求。具体测试步骤如下：
步骤 1：调用获取设备型号并记录调用耗时；
f) 预期结果：步骤 1 的耗时在 2ms 以内，则评测结果为“未见异常”。否则评测结果为“异常”。

7.3.2 获取客户端协议版本性能

测试方法如下：

a) 测试编号：7.3.2；
b) 测试项目：获取客户端协议版本接口的性能测试；
c) 项目要求：验证是否满足定义的获取客户端协议版本接口的性能要求；
d) 测试条件：应提供获取客户端协议版本性能的测试说明；
e) 测试步骤：验证获取客户端协议版本接口的性能是否满足规范要求。具体测试步骤如下：
步骤1：调用获取客户端协议版本接口并记录调用耗时；
f) 预期结果：步骤 1 的耗时在 2ms 以内，则评测结果为“未见异常”。否则评测结果为“异常”。

7.3.3 获取客户端支持的生物验证类型性能

测试方法如下：

a) 测试编号：7.3.3；
b) 测试项目：获取客户端及支持的生物验证类型接口的性能测试；
c) 项目要求：验证是否满足定义的获取客户端支持的生物验证类型接口的性能要求；
d) 测试条件：应提供获取客户端及支持的生物验证类型性能的测试说明；

e） 测试步骤：验证获取客户端及支持的生物验证类型接口是否满足规范要求。具体测试步骤如下：
步骤 1：调用获取客户端及支持的生物验证类型接口，并记录调用耗时；
f） 预期结果：步骤 1 结果的耗时在 5ms 以内，则评测结果为“未见异常”。否则评测结果为“异常”。

7.3.4 获取校验数据性能

测试方法如下：
a） 测试编号：7.3.4；
b） 测试项目：获取校验数据性能测试；
c） 项目要求：验证是否满足定义的获取校验数据的性能要求；
d） 测试条件：应提供获取校验数据性能的测试说明；
e） 测试步骤：验证获取校验数据接口的性能是否满足规范要求。具体测试步骤如下：
步骤1：调用获取校验数据接口，并记录调用耗时。
f） 预期结果：步骤 1 结果的耗时在 5ms 以内，则评测结果为“未见异常”。否则评测结果为“异常”。

7.3.5 指纹注册性能

测试方法如下：
a） 测试编号：7.3.5；
b） 测试项目：指纹注册的性能测试；
c） 项目要求：验证是否满足定义的指纹注册的性能要求；
d） 测试条件：应提供指纹注册性能的测试说明；
e） 测试步骤：验证指纹注册接口的性能是否满足规范要求。具体测试步骤如下：
步骤1：调用指纹注册接口，并记录调用耗时。
f） 预期结果：步骤 1 结果的耗时在 5s 以内，则评测结果为“未见异常”。否则评测结果为“异常”。

7.3.6 指纹校验性能

测试方法如下：
a） 测试编号：7.3.6；
b） 测试项目：指纹校验的性能测试；
c） 项目要求：验证是否满足定义的指纹校验的性能要求；
d） 测试条件：应提供指纹校验性能的测试说明；
e） 测试步骤：验证指纹校验接口的性能是否满足规范要求。具体测试步骤如下：
步骤 1：调用指纹校验接口，并记录调用耗时。
f） 预期结果：步骤 1 结果的耗时在 2s 以内，则评测结果为“未见异常”。否则评测结果为“异常”。

7.3.7 指纹注销性能

测试方法如下：
a） 测试编号：7.3.7；
b） 测试项目：指纹注销的性能测试；
c） 项目要求：验证是否满足定义的指纹注销的性能要求；
d） 测试条件：应提供指纹注销性能的测试说明；
e） 测试步骤：验证指纹注销接口的性能是否满足规范要求。具体测试步骤如下：
步骤1：调用指纹注销接口，并记录调用耗时。
f） 预期结果：步骤 1 结果的耗时在 1s 以内，则评测结果为“未见异常”。否则评测结果为“异常”。

7.3.8 RSA 密钥签名算法性能

测试方法如下：

a) 测试编号：7.3.8；
b) 测试项目：RSA 密钥签名算法性能测试；
c) 项目要求：验证是否满足定义的 RSA 密钥签名算法的性能要求；
d) 测试条件：应提供 RSA 密钥签名算法性能的测试说明；
e) 测试步骤：验证 RSA 密钥签名算法的性能是否满足规范要求。具体测试步骤如下：
   1) 步骤 1：随机生成 byte 数组；
   2) 步骤 2：以暂存的密钥句柄拼凑 RSA 密钥签名接口的入参；
   3) 步骤 3：根据步骤 2 的结果调用 RSA 密钥签名接口并暂存结果；
   4) 步骤 4：从步骤 2 的暂存结果中解析状态码和生成的签名并暂存。
f) 预期结果：在步骤 4 后，如果状态码为 ERR_SUCCESS，且步骤 3-4 的耗时低于 200ms,则该评测为“未见异常”。否则评测结果为“异常”。(具体错误原因参考错误码定义)

7.3.9 RSA 密钥验签算法性能

测试方法如下：

a) 测试编号：7.3.9；
b) 测试项目：RSA 密钥验签算法性能测试；
c) 项目要求：验证是否满足定义的 RSA 密钥验签算法的性能要求；
d) 测试条件：应提供 RSA 密钥验签算法性能的测试说明；
e) 测试步骤：验证 RSA 密钥验签算法的性能是否满足规范要求。具体测试步骤如下：
   1) 步骤 1：根据暂存的密钥句柄，以及暂存的签名结果拼凑 RSA 验签接口的入参；
   2) 步骤 2：以步骤 1 的入参调用 RSA 验签接口并暂存结果；
   3) 步骤 3：从步骤 2 暂存结果中解析返回值状态码。
f) 预期结果：在步骤 3 后，如果状态码为 ERR_SUCCESSS，且步骤 2-3 的耗时低于 100ms，则该评测为“未见异常”。否则评测结果为“异常”。(具体错误原因参考错误码定义)

7.3.10 SM2 密钥签名算法性能

测试方法如下：

a) 测试编号：7.3.10；
b) 测试项目：SM2 密钥签名算法性能测试；
c) 项目要求：验证是否满足定义的 SM2 密钥签名算法的性能要求；
d) 测试条件：应提供 SM2 密钥签名算法性能的测试说明；
e) 测试步骤：验证 SM2 密钥签名算法的性能是否满足规范要求。具体测试步骤如下：
   1) 步骤 1：随机生成 byte 数组；
   2) 步骤 2：以暂存的密钥句柄拼凑 SM2 密钥签名接口的入参；
   3) 步骤 3：根据步骤 2 的结果调用 SM2 密钥签名接口并暂存结果；
   4) 步骤 4：从步骤 2 的暂存结果中解析状态码和生成的签名并暂存。
f) 预期结果：在步骤 4 后，如果状态码为 ERR_SUCCESS，且步骤 3-4 的耗时低于 200ms,则该评测为“未见异常”。否则评测结果为“异常”。(具体错误原因参考错误码定义)

7.3.11 SM2 密钥验签算法性能

测试方法如下：

a) 测试编号：7.3.11；
b) 测试项目：SM2 密钥验签算法性能测试；
c) 项目要求：验证是否满足定义的 SM2 密钥验签算法的性能要求；
d) 测试条件：应提供 SM2 密钥验签算法性能的测试说明；
e) 测试步骤：验证 SM2 密钥验签算法的性能是否满足规范要求。具体测试步骤如下：
   1) 步骤 1：根据暂存的密钥句柄，以及暂存的签名结果拼凑 SM2 验签接口的入参；

2） 步骤 2：以步骤 1 的入参调用 SM2 验签接口并暂存结果；
3） 步骤 3：从步骤 2 暂存结果中解析返回值状态码。

f） 预期结果：在步骤 3 后，如果状态码为 ERR_SUCCESSS，且步骤 2-3 的耗时低于 100ms，则该评测为“未见异常”。否则评测结果为“异常”。(具体错误原因参考错误码定义)

7.3.12 校验器签名算法性能

测试方法如下：

a） 测试编号：7.3.12；
b） 测试项目：校验器签名算法性能测试；
c） 项目要求：验证是否满足定义的校验器签名算法的性能要求；
d） 测试条件：应提供校验器签名算法性能的测试说明；
e） 测试步骤：验证校验器签名算法的性能是否满足规范要求。具体测试步骤如下：
1） 步骤 1：随机生成一个 byte 数组；
2） 步骤 2：以步骤 1 的结果为入参调用标准 SHA256 算法；
3） 步骤 3：从步骤 2 的结果拼凑校验器签名接口的入参；
4） 步骤 4：以步骤 3 的结果调用校验器签名接口并暂存结果；
5） 步骤 5：从步骤 4 的结果中解析出状态码。
f） 预期结果：在步骤 5 后，如果状态码为 ERR_SUCCESS，且步骤 4-5 的耗时低于 200ms，则该评测为“未见异常”。否则评测结果为“异常”。(具体错误原因参考错误码定义)

7.3.13 校验器验签算法性能

测试方法如下：

a） 测试编号：7.3.13；
b） 测试项目：校验器验证签名算法性能测试；
c） 项目要求：验证是否满足定义的校验器验签算法的性能要求；
d） 测试条件：应提供校验器验签算法性能的测试说明；
e） 测试步骤：验证校验器验签算法的性能是否满足规范要求。具体测试步骤如下：
1） 步骤 1：随机生成一个 byte 数组；
2） 步骤 2：以步骤 1 的结果为入参调用标准 SHA256 算法；
3） 步骤 3：以根证书临时签发一个二级证书；
4） 步骤 4：用步骤 3 的二级证书私钥对步骤 2 的结果进行签名；
5） 步骤 5：以步骤 2 的结果、步骤 4 的签名结果、步骤 3 的二级证书拼凑校验器验签算法的入参；
6） 步骤 6：根据步骤 5 的入参调用校验器验签接口并暂存结果；
7） 步骤 7：从步骤 6 的结果中解析出状态码。
f） 预期结果：在步骤 7 后，如果状态码为 ERR_SUCCESS，且步骤 6-7 的耗时低于 100ms，则该评测为“未见异常”。否则评测结果为“异常”。(具体错误原因参考错误码定义)

7.3.14 获取最近一次认证通过的指纹模板 ID 性能测试

测试方法如下：

a） 测试编号：7.3.14；
b） 测试项目：获取最近一次认证通过的指纹模板 ID 性能测试；
c） 项目要求：验证是否满足定义的获取最近一次认证通过的指纹模板 ID 的性能要求；
d） 测试条件：应提供获取最近一次认证通过指纹模板 ID 性能的测试说明；
e） 测试步骤：验证获取最近一次认证通过的指纹模板 ID 的性能是否满足规范要求。具体测试步骤如下：
1） 步骤 1：提前录入手指 A 到系统指纹库中；
2） 步骤 2：以手指 A 验证指纹；
3） 步骤 3：调用获取最近一次认证通过的指纹模板 ID 接口并暂存结果；
4） 步骤 4：从结果中解析状态码和指纹模板 ID。

f） 预期结果：在步骤 4 后，如果状态码为 ERR_SUCCESS，且步骤 2-4 的耗时低于 260ms，则评测结果为“未见异常”。否则评测结果为“异常”。(具体错误原因参考错误码定义)

7.3.15 获取指纹库中录入的指纹模板 ID 集性能测试

测试方法如下：

a） 测试编号：7.3.15；
b） 测试项目：获取指纹库中录入的指纹模板 ID 集性能测试；
c） 项目要求：验证是否满足定义的获取系统中录入的指纹模板 ID 集的性能要求；
d） 测试条件：应提供获取系统中录入的指纹模板 ID 集性能的测试说明；
e） 测试步骤：验证获取系统中录入的指纹模板 ID 集的性能是否满足规范要求。具体测试步骤如下：
   1） 步骤 1：提前录入若干手指到系统指纹库中；
   2） 步骤 2：调用获取系统中录入的指纹模板 ID 集接口并暂存结果；
   3） 步骤 3：从结果中解析状态码和指纹模板 ID 集。
f） 预期结果：在步骤 3 后，如果状态码为 ERR_SUCCESS，且步骤 2-3 耗时低于 100ms，则评测结果为“未见异常”。否则评测结果为“异常”。(具体错误原因参考错误码定义)

7.3.16 获取设备 ID 性能测试

测试方法如下：

a） 测试编号：7.3.16；
b） 测试项目：获取设备 ID 性能测试；
c） 项目要求：验证设备 ID 获取的性能；
d） 测试条件：应提供获取设备 ID 性能的测试说明；
e） 测试步骤：验证设备 ID 获取的性能是否满足规范要求。具体测试步骤如下：
   1） 步骤 1：调用获取设备 ID 接口并暂存结果；
   2） 步骤 2：从步骤 1 的结果中解析出状态码和设备 ID。
f） 预期结果：在步骤 2 后，如果状态码为 ERR_SUCCESS，且步骤 1-2 耗时低于 100ms，则评测结果为“未见异常”，否则评测结果为“异常”(具体错误原因参考错误码定义)。

电信终端产业协会团体标准

移动智能终端指纹框架接口测试方法

T/TAF 012—2023

*

电信终端产业协会印发
地址：北京市西城区新街口外大街 28 号
电话：010-82052809
电子版发行网址：www.taf.org.cn