ICS 33.050
CCS M 30

团　体　标　准

T/TAF 117—2022

智能终端设备间互信操作测试方法

Test methods for mutual trust operation between smart devices

2022-05-11 发布　　2022-05-11 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。

本文件中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、华为技术有限公司、郑州信大捷安信息技术股份有限公司。

本文件主要起草人：胡重阳、宁华、马四英、闫雪梅、衣强、李实、张悦、李战锋、刘献伦。

引　　言

随着智能终端设备相关应用场景及服务的不断发展，用户个人拥有的智能终端设备的种类和数量在不断增加，越来越多的应用场景和服务需要在不同的智能终端设备间建立通信连接。T/TAF 097-2021《智能终端设备间互信操作技术要求》针对智能终端设备间互信关系的建立、传递和解除各阶段提出了安全要求，为了评测智能终端设备是否满足技术要求规定的内容，特制定本文件。

本文件是T/TAF 097-2021《智能终端设备间互信操作技术要求》配套的测试方法，针对技术要求设计了科学的测试方法，用于评测设备满足技术要求的程度。通过本文件可以从测试角度保证设备间互信操作的落地实施，切实地保证用户设备间的通信安全。

智能终端设备间互信操作测试方法

1 范围

本文件规定了智能终端设备间安全建立、传递、解除互信关系各阶段的测试方法。

本文件适用于面向消费者的智能终端设备，个别条款不适用于特殊行业、专业应用，其他类似设备也可参考使用。

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。

T/TAF 097-2021 智能终端设备间互信操作技术要求

3 术语和定义

3.1

智能终端设备 intelligent terminal

具备网络接入功能，可进行信息采集和处理，支持数据通信的终端设备。

3.2

设备互信关系建立凭据 device trust relationship establishment credentials

在设备间互信关系建立过程中，用于验证设备可信身份的信息，形式包括但不限于：公私钥对、对称密钥、token、共享秘密等。

3.3

可信第三方 trusted third party

在双方通信设备之外，能够提供身份验证及证书签发功能的第三方服务器。

3.4

互信关系 mutual trust relationship

多个智能终端设备相互信任彼此来源且具有合法性身份。

3.5

可信设备列表 trusted device list

已建立互信关系的设备信息记录。

4 缩略语

下列缩略语适用于本文件。

RPMB：重放保护内存块（Replay Protected Memory Block）

SFS：安全文件系统（Secure File System）

TREC：互信关系建立凭据（Trust Relationship Establishment Credentials）

5 智能终端设备间互信操作测试分析

智能终端设备间互信关系建立的场景可以分为如下三种：

——场景 1：操作设备 A、设备 B，通过可信第三方服务器建立互信关系。

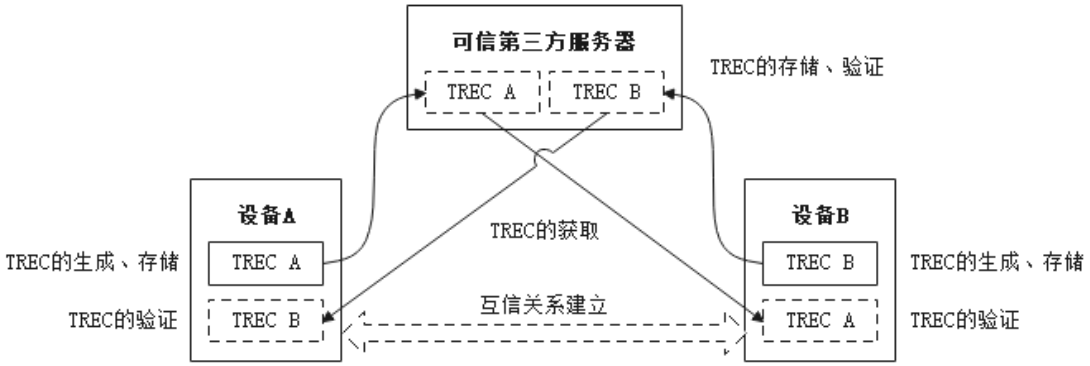

图1 基于可信第三方建立互信关系示意图

——场景 2：操作设备 C、设备 D，通过扫描二维码、输入预置 PIN 码、通过 NFC 触碰标签等形式，直接点对点交互建立互信关系。

——场景 3：操作设备 E、设备 F 通过可信第三方服务器/点对点方式建立互信关系，操作设备 F、设备 G 通过可信第三方服务器/点对点方式建立互信关系；操作设备 E、设备 G 通过设备 F 传递信息，进而建立互信关系。场景 3 可以拆解成场景 1/场景 2、场景 1/场景 2、端到端场景，见图 2。

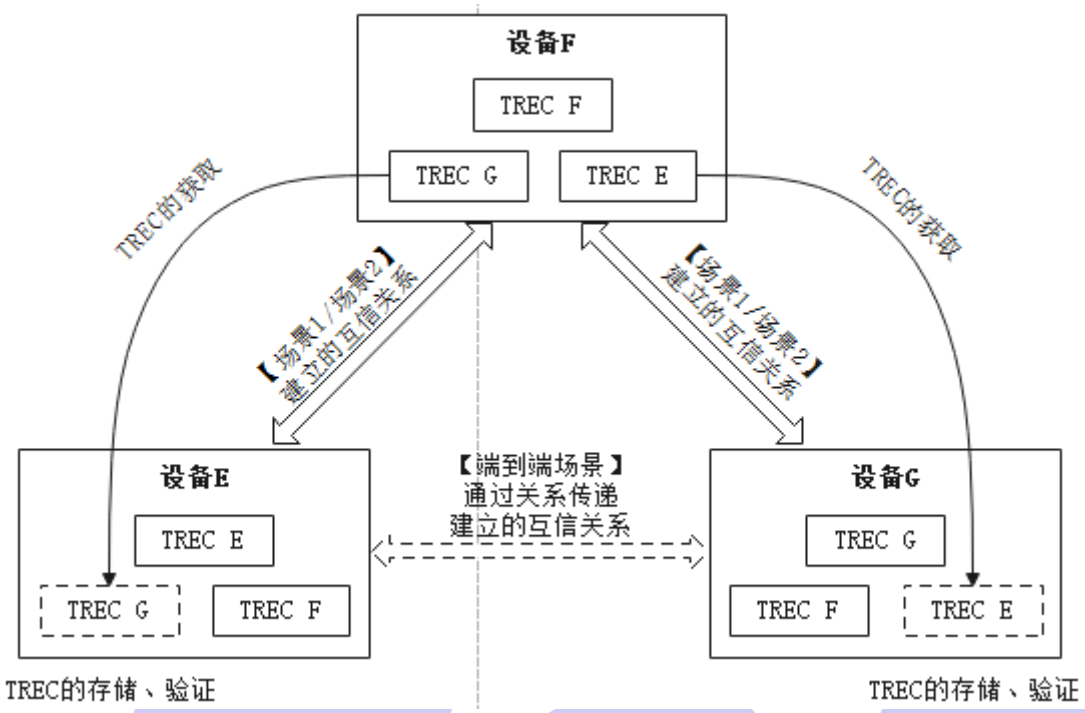

图2　互信关系传递示意图

T/TAF 097-2021 中智能终端设备间互信关系建立安全要求对应场景 1、场景 2，智能终端设备间互信关系传递安全要求对应场景 3，智能终端设备间互信关系解除安全要求对应场景 1、场景 2、场景 3。

综上，本文件测试方法的设计思路为：在测试项目中描述要评测的 T/TAF 097-2021 规则；测试步骤、预期结果描述评测场景和安全功能测试内容。本文件会从证明（检查文档）、验证两个角度测试安全功能的有效性，针对难以/无法开展验证型测试的安全功能仅采用证明型测试方法。另外在证明型测试活动中，厂商可以提供业界公认的认证/测评证书，替代设计文档、代码片段等资料，如：CC 认证、国家密码管理局的商用密码认证等。

注意：厂商在提供设计文档、代码片段、测试报告、认证/测评证书等资料时，须符合业界惯例且保护自身商业秘密。

6　智能终端设备间互信关系建立、传递、解除的测试方法

6.1　智能终端设备间互信关系建立安全测试方法

6.1.1　测试项 a）：评测场景 1、场景 2 设备生成 TREC 的方法符合密码学要求

测试项目T/TAF 097-2021-6.3.1-a）：应使用符合密码学要求的安全的生成方法生成TREC，包括：使用符合密码学要求的安全随机数接口生成对称凭据，使用符合密码学要求的非对称密钥生成方法生成非对称凭据。

a）　测试步骤：

1）　步骤1：审查厂商提交的文档，查看被测智能终端的TREC设计文档，检查是否支持对称TREC、非对称TREC；

2）　步骤2：列出生成对称TREC的随机数接口，检查该接口是否为安全随机数接口（参考附录A）；

3） 步骤3：列出生成非对称TREC的非对称密钥的算法、密钥长度，检查算法、密钥长度是否符合国家和行业标准要求。

b） 预期结果：

1） 在步骤1之后，若智能终端支持对称TREC则须进行步骤2，支持非对称TREC则须进行步骤3，测评结果为“未见异常”；否则为“不符合要求”，测评结束；

2） 在步骤2之后，若智能终端生成对称TREC的随机数接口为安全随机数接口，测评结果为“未见异常”，否则为“不符合要求”，测评结束；

3） 在步骤3之后，若智能终端生成非对称TREC的非对称密钥生成方法符合国家和行业标准要求，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

6.1.2 测试项 b）：评测场景 1、场景 2 设备有加密、访问控制等机制保护 TREC 的使用

测试项目T/TAF 097-2021-6.3.1-b）：当TREC在智能终端设备上生成、存储后，设备应对TREC的使用提供加密、访问控制等安全保护机制，避免设备上的TREC被窃取或篡改。

a） 测试步骤：

1） 步骤1：审查厂商提交的文档，查看被测智能终端的TREC设计文档，检查是否采用了加密机制存储TREC，是否采用了行业通用的加密、访问控制技术保护了TREC；

2） 步骤2：按照场景1搭建测试环境，设备A使用未授权的测试程序读取本地设备的TREC，是否无法读取或读取为乱码；

3） 步骤3：按照场景2搭建测试环境，设备C使用未授权的测试程序读取本地设备的TREC，是否无法读取或读取为乱码。

b） 预期结果：

1） 在步骤1之后，若智能终端采用了行业通用的加密、访问控制机制保护了TREC，测评结果为“未见异常”，然后执行步骤2；否则为“不符合要求”，测评结束；

2） 在步骤2之后，若设备A上未授权的测试程序无法读取本地设备A的TREC或读取为乱码，测评结果为“未见异常”，然后执行步骤3；否则为“不符合要求”，测评结束；

3） 在步骤3之后，若设备C上未授权的测试程序无法读取本地设备C的TREC或读取为乱码，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

6.1.3 测试项 c）：评测场景 2 设备间安全通道双向认证，加密传输 TREC

测试项目T/TAF 097-2021-6.3.1-c）：通过直接点对点建立互信关系的方式，应通过设备间安全通道确保对端设备TREC获取的安全性。

——安全通道的建立应基于安全协议和设备间共享的机密信息，共享的机密信息应包括但不限于：输入预置PIN码/随机PIN码、通过扫码获得二维码中的共享信息、近场NFC交换的共享信息等。

——安全协议应采用有安全性证明的国际标准协议或业界通用协议，禁止采用私有协议。安全协议应为双向认证协议。

——TREC应通过上述建立的设备间安全通道进行加密传输。

a） 测试步骤：

1） 步骤1：审查厂商提交的文档，查看被测智能终端安全通道的设计文档，检查通道的建立是否基于业界通用的安全协议（参考附录B），检查设备间共享机密信息是否有泄露的风险；

2） 步骤2：审查厂商提交的文档，查看被测智能终端安全通道使用的安全协议的设计文档，检查是否为双向认证的国际标准协议或业界通用协议（参考附录B），是否为私有协议。

b） 预期结果：

1） 在步骤1之后，若智能终端安全通道的建立是基于安全协议，且设备间共享机密信息泄露风险低，测评结果为“未见异常”，然后执行步骤2；否则为“不符合要求”，测评结束；
2） 在步骤2之后，若智能终端安全通道使用的安全协议是双向认证的国际标准协议或业界通用协议，且不是私有协议，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

6.1.4 测试项 d）：评测场景 1 三方服务器校验设备身份合法性，传输协议安全有效

测试项目T/TAF 097-2021-6.3.1-d）：通过可信第三方建立互信关系的方式，应确保对端设备TREC获取的安全性。

——当设备向第三方服务器请求下发对端设备TREC时，可信第三方服务器应验证请求建立互信关系的设备身份合法性。

——可信第三方服务器应下发与被请求设备相对应的合法TREC。

——设备通过可信第三方服务器获取对端设备TREC，设备与可信第三方服务器之间进行通信时使用的安全协议应采用有安全性证明的国际标准协议或业界通用协议（如：TLS v1.2及以上），禁止采用私有协议。安全协议宜为双向认证协议。

a） 测试步骤：
1） 步骤1：审查厂商提交的文档，查看被测智能终端通过可信第三方服务器获取对端设备TREC的设计文档，检查可信第三方服务器是否采用典型技术（如：证书、签名等）验证了请求设备的身份合法性，可信第三方服务器是否下发了对应设备的合法TREC；
2） 步骤2：审查厂商提交的文档，查看被测智能终端与可信第三方服务器之间进行通信时使用的安全协议的设计文档，检查是否为有安全性证明的国际标准协议或业界通用协议（参考附录B），是否为私有协议；
3） 步骤3：按照场景1搭建测试环境，基于设备A、B建立互信关系的时间点，分别查看设备A、B上的服务器返回的消息/日志，检查服务器是否已校验了设备A、B身份合法性；
4） 步骤4：按照场景1搭建测试环境，设备A通过测试程序给服务器发送仿冒的身份信息，检查服务器是否可以拒绝设备A的请求。

b） 预期结果：
1） 在步骤1之后，若可信第三方服务器采用了典型技术验证请求设备的身份合法性，且可信第三方服务器下发了对应设备的合法TREC，测评结果为“未见异常”，然后执行步骤2；否则为“不符合要求”，测评结束；
2） 在步骤2之后，若智能终端与可信第三方服务器之间进行通信时的安全协议是有安全性证明的国际标准协议或业界通用协议，且不是私有协议，测评结果为“未见异常”，然后执行步骤3；否则为“不符合要求”，测评结束；
3） 在步骤3之后，若获取到的消息/日志证明服务器校验了设备A、设备B身份合法性，测评结果为“未见异常”，然后执行步骤4；否则为“不符合要求”，测评结束；
4） 在步骤4之后，若服务器拒绝了设备A的请求，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

6.1.5 测试项 e）：评测场景 1 设备校验了对端 TREC 的完整性

测试项目T/TAF 097-2021-6.3.1-e）：当设备收到由可信第三方下发的对端设备的TREC后，应校验对端设备TREC的完整性。

a） 测试步骤：
1） 步骤1：审查厂商提交的文档，查看被测智能终端收到由可信第三方服务器下发的对端设备的TREC的设计文档，是否采用典型技术（如：签名、哈希等）校验了TREC的完整性；

2） 步骤2：按照场景1搭建测试环境，基于设备A、B建立互信关系的时间点，查看设备A上的日志，检查是否校验了设备B TREC的完整性；
3） 步骤3：按照场景1搭建测试环境，通过测试程序篡改设备B的TREC然后发给设备A，检查设备A是否拒绝了设备B非法的TREC。

b） 预期结果：
1） 在步骤1之后，若智能终端采用典型技术校验了对端设备TREC的完整性，测评结果为“未见异常”，然后执行步骤2；否则为“不符合要求”，测评结束；
2） 在步骤2之后，若日志显示设备A采用设计文档所述的技术，校验了设备B TREC的完整性，测评结果为“未见异常”，否则为“不符合要求”，测评结束；
3） 在步骤3之后，若设备A拒绝了设备B非法的TREC，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

6.1.6 测试项 f）：评测场景 1、场景 2 设备加密存储了收到的 TREC

测试项目T/TAF 097-2021-6.3.1-f）：当设备收到对端设备的TREC后，应使用设备提供的安全保护能力对收到的TREC进行加密存储，确保收到的设备TREC在智能终端设备中的存储安全性，如：将收到的TREC加密后存储于设备安全环境内。

a） 测试步骤：
1） 步骤1：审查厂商提交的文档，查看被测智能终端存储TREC的安全设计文档，是否采用安全存储技术（如：安全芯片、RPMB、SFS等）保护了TREC；
2） 步骤2：按照场景1搭建测试环境，设备A使用未授权的测试程序读取本地存储的设备B的TREC，是否无法读取或读取为乱码；
3） 步骤3：按照场景2搭建测试环境，设备C使用未授权的测试程序读取本地存储的设备D的TREC，是否无法读取或读取为乱码；

b） 预期结果：
1） 在步骤1之后，若智能终端按照业界惯例保障了TREC的安全性，测评结果为“未见异常”，然后执行步骤2；否则为“不符合要求”，测评结束；
2） 在步骤2之后，若设备A上未授权的测试程序无法读取本地存储的设备B的TREC或读取为乱码，测评结果为“未见异常”，然后执行步骤3；否则为“不符合要求”，测评结束；
3） 在步骤3之后，若设备C上未授权的测试程序无法读取本地存储的设备D的TREC或读取为乱码，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

6.1.7 测试项 g）：评测场景 1、场景 2 设备基于验证 TREC 的有效性建立互信关系

测试项目T/TAF 097-2021-6.3.1-g）：智能终端设备间互信关系的建立应基于对双方设备有效TREC的验证。

a） 测试步骤：
1） 步骤1：审查厂商提交的文档，查看被测智能终端设备间建立互信关系的设计文档，是否采用典型技术（如：证书、签名、Token等）验证了TREC的有效性；
2） 步骤2：按照场景1搭建测试环境，基于设备A、B之间建立互信关系的时间点，分别查看设备A、B上的日志，检查是否在建立互信关系前验证了对方TREC的有效性；
3） 步骤3：按照场景1搭建测试环境，通过测试程序篡改设备A本地存储的设备B的TREC，设备A、B尝试建立互信关系，检查建立互信关系是否失败；
4） 步骤4：按照场景2搭建测试环境，基于设备C、D之间建立互信关系的时间点，分别查看设备A、B上的日志，检查是否在建立互信关系前验证了对方TREC的有效性；

5） 步骤5：按照场景2搭建测试环境，通过测试程序篡改设备C本地存储的设备D的TREC，设备C、D尝试建立互信关系，检查建立互信关系是否失败。

b） 预期结果：

1） 在步骤1之后，若智能终端采用典型技术验证了TREC的有效性，测评结果为“未见异常”，然后执行步骤2；否则为“不符合要求”，测评结束；

2） 在步骤2之后，若设备A、B上日志显示采用了设计文档所述的技术，验证了对方TREC的有效性，测评结果为“未见异常”，然后执行步骤3；否则为“不符合要求”，测评结束；

3） 在步骤3之后，若设备A、B建立互信关系失败，测评结果为“未见异常”，然后执行步骤4；否则为“不符合要求”，测评结束；

4） 在步骤4之后，若设备C、D上日志显示采用了设计文档所述的技术，验证了对方TREC的有效性，测评结果为“未见异常”，否则为“不符合要求”，然后执行步骤5，测评结束。

5） 在步骤5之后，若设备C、D建立互信关系失败，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

6.1.8 测试项 h）：评测场景 1、场景 2 设备基于对端 TREC 建立安全连接，传输数据

测试项目T/TAF 097-2021-6.3.1-h）：互信关系建立后，当智能终端设备建立设备间通信连接时，应基于设备双方获取的对端设备TREC建立安全的连接，以确保数据的传输安全。

a） 测试步骤：

1） 步骤1：审查厂商提交的文档，查看被测智能终端设备间建立安全连接的设计文档，是否是采用业界安全密码学原理（如：密钥派生PBKDF迭代次数不低于10000次，密钥协商ECDH密钥长度不低于256，基于非对称密钥体系的密钥协商协议Station-To-Station协议等）利用对端设备TREC建立的。

b） 预期结果：

1）在步骤1之后，若智能终端设备间的安全连接是按照业界安全密码学原理利用对端设备TREC建立的，测评结果为“未见异常”；否则为“不符合要求”，测评结束。

6.1.9 测试项 i）：评测场景 1、场景 2 设备建立互信关系后，清除了缓存的 TREC

测试项目T/TAF 097-2021-6.3.1-i）：互信关系建立完成后，为防止TREC泄漏，应及时清除缓存中的设备TREC信息，清除方式应包括但不限于：覆盖/重写缓存。

a） 测试步骤：

1） 步骤1：审查厂商提交的文档，查看被测智能终端设备建立互信关系后清除缓存中TREC的代码片段，是否采用业界通用的覆盖/重写技术（如：全0/全1/随机数覆写、加密后丢密钥等）清除了TREC的缓存。

b） 预期结果：

1） 在步骤1之后，若智能终端设备建立互信关系后，采用业界通用的覆盖/重写技术清除了缓存中的TREC，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

6.2 智能终端设备间互信关系传递安全测试方法

6.2.1 测试项 a）：评测场景 3 满足本文件 6.1 章节测试项 c）、测试项 d）、测试项 e）、测试项 f）、测试项 g）、测试项 h）、测试项 i）

测试项目T/TAF 097-2021-6.3.2-a）：应满足（T/TAF 097-2021）6.3.1中c),d),e),f),g),h),i)的要求。

注：此规则约束的是场景3，场景3可以拆解成场景1/场景2、场景1/场景2、端到端场景（见图2）；（T/TAF 097-2021）6.3.1中c),d),e)三条技术要求约束的是场景3中的场景1/场景2，这部分测试内容跟本文件6.1章节评测场景1、场景2的内容相同（见测试项c）、测试项d）、测试项e））。所以本测试项不再重复测试这些内容，而是聚焦测试（T/TAF 097-2021）6.3.1中f),g),h),i)的规则。

另外，场景3中设备满足（T/TAF 097-2021）6.3.1中f),g),h),i)的规则的测试方法跟本文件6.1章节f),g),h),i)，直接参考对应章节评测即可。

6.2.2 测试项 b）：评测场景 3 设备校验了收到的 TREC 来自已建立互信关系的可信设备

测试项目T/TAF 097-2021-6.3.2-b）：当设备通过关系传递获得其他设备TREC时，设备应确保收到的TREC来自已建立互信关系的可信设备。

a） 测试步骤：

1） 步骤1：审查厂商提交的文档，查看被测智能终端设备间互信关系传递的设计文档，设备是否会基于通用技术（如：签名、消息验证码HMAC等）验证TREC来源于已建立互信关系的可信设备；

2） 步骤2：按照场景3搭建测试环境，基于设备E、G建立互信关系的时间点，查看设备E上日志，检查是否检验了设备G的TREC来自可信设备F；

3） 步骤3：按照场景3搭建测试环境，在设备F上运行测试程序转变成不可信的非法设备，设备F将设备G的TREC传递给设备E，检查设备E是否拒绝了此TREC，是否跟设备G建立互信关系失败。

b） 预期结果：

1） 在步骤1之后，若智能终端设备会基于通用技术验证TREC来源于已建立互信关系的可信设备，测评结果为“未见异常”，然后执行步骤2；否则为“不符合要求”，测评结束；

2） 在步骤2之后，若日志显示设备E采用设计文档所述的技术，校验了设备G的TREC来自可信设备F，测评结果为“未见异常”，然后执行步骤3；否则为“不符合要求”，测评结束；

3） 在步骤3之后，若设备E拒绝了非法设备F传递的TREC，且跟设备G建立互信关系失败，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

6.3 智能终端设备间互信关系解除安全测试方法

6.3.1 测试项 a）：评测场景 1、场景 2、场景 3 设备解除互信关系后，安全删除对端设备的 TREC

测试项目T/TAF 097-2021-6.3.3-a）：当设备间互信关系解除后，应将对端设备TREC从本地彻底删除，并确保无法被复原，删除方式应包括但不限于：覆盖/重写存储单元/存储区。

a） 测试步骤：

基于等价类遍历设备间互信关系解除的方式，解除方式包括但不限于：主动解除绑定/注销账号/恢复出厂/卸载互信关系业务，执行如下测试步骤：

1） 步骤1：审查厂商提交的文档，查看被测智能终端互信关系解除的设计文档，是否采用通用技术（如：全0/全1/随机数覆写、加密后丢密钥等）彻底删除了对端设备TREC；

2） 步骤2：按照场景1搭建测试环境，设备A通过测试程序读取本地设备B TREC的存储单元/存储区，导出到文本11，设备A、B解除互信关系，设备A再次读取原设备B TREC的存储单元/存储区导出到文本12，对比文本11、文本12，检查是否采用设计文档所述技术彻底删除了对端的TREC；

3） 步骤3：按照场景2搭建测试环境，设备C通过测试程序读取本地设备D TREC的存储单元/存储区，导出到文本21，设备C、D解除互信关系，设备C再次读取原设备D TREC的存储单

元/存储区导出到文本22，对比文本21、文本22，检查是否采用设计文档所述技术彻底删除了对端的TREC；

4） 步骤4：按照场景3搭建测试环境，设备E通过测试程序读取本地设备G TREC的存储单元/存储区，导出到文本31，设备E、G解除互信关系，设备E再次读取原设备G TREC的存储单元/存储区导出到文本32，对比文本31、文本32，检查是否采用设计文档所述技术彻底删除了对端的TREC。

b） 预期结果：

1） 在步骤1之后，若被测智能终端在解除互信关系后，彻底删除了对端设备TREC，测评结果为“未见异常”，然后执行步骤2；否则为“不符合要求”，测评结束；

2） 在步骤2之后，若设备A采用设计文档所述技术彻底删除了设备B的TREC，测评结果为“未见异常”，然后执行步骤3；否则为“不符合要求”，测评结束；

3） 在步骤3之后，若设备C采用设计文档所述技术彻底删除了设备D的TREC，测评结果为“未见异常”，然后执行步骤4；否则为“不符合要求”，测评结束；

4） 在步骤4之后，若设备E采用设计文档所述技术彻底删除了设备G的TREC，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

6.3.2 测试项 b）：评测场景 1、场景 2、场景 3 设备在可信设备列表中，删除了解除互信关系的设备

测试项目T/TAF 097-2021-6.3.3-b）：解除了互信关系的设备相关信息应从可信设备列表中删除。

a） 测试步骤：

遍历设备间互信关系解除的方式（包括：主动解除绑定/注销账号/恢复出厂/卸载互信关系业务等），执行如下步骤：

1） 步骤1：按照场景1搭建测试环境，设备A解除跟设备B的互信关系，设备A、设备B上查看可信设备列表是否删除掉了对端设备信息；

2） 步骤2：按照场景2搭建测试环境，设备C解除跟设备D的互信关系，设备C、设备D上查看可信设备列表是否删除掉了对端设备信息；

3） 步骤3：按照场景3搭建测试环境，设备E解除跟设备G的互信关系，设备E、设备G上查看可信设备列表是否删除掉了对端设备信息。

b） 预期结果：

1） 在步骤1之后，若设备A、设备B的可信设备列表删除掉了对端设备信息，测评结果为“未见异常”，然后执行步骤2；否则为“不符合要求”，测评结束。

2） 在步骤2之后，若设备C、设备D的可信设备列表删除掉了对端设备信息，测评结果为“未见异常”，然后执行步骤3；否则为“不符合要求”，测评结束。

3） 在步骤3之后，若设备E、设备G的可信设备列表删除掉了对端设备信息，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

附录 A
（资料性）
常见的安全和不安全随机数接口

已知常见的安全随机数接口有：类Unix平台/dev/random、Windows平台CryptGenRandom、OpenSSL的RAND_bytes或RAND_priv_bytes、OpenSSL FIPS模块中实现的各种DRBG、JDK的java.security.SecureRandom等。

已知常见的不安全随机数接口有：C标准库函数random()、rand()以及Java的java.util.Random类等。

附录 B
（资料性）
常见的安全和不安全协议

已知常见的安全协议有：SFTP、TLS1.2、TLS1.3、SNMPv3、SSHv2等。

已知常见的不安全协议有：TFTP、FTP、Telnet、SSL2.0、SSL3.0、TLS1.0、TLS1.1、SNMPv1/v2、SSHv1等。

电信终端产业协会团体标准

智能终端设备间互信操作测试方法

T/TAF 117—2022

*

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