ICS 33.050
CCS M 30

团 体 标 准

T/TAF 097-2021

智能终端设备间互信操作技术要求

Technical requirements for mutual trust operation between smart devices

2021-08-17 发布 2021-08-17 实施

电信终端产业协会 发布

目　　次

前言 II
引言 III
1 范围 1
2 规范性引用文件 1
3 术语和定义 1
4 缩略语 1
5 智能终端设备间互信关系框架及目标 2
6 智能终端设备间互信关系管理安全要求 2
6.1 智能终端设备间互信关系生命周期 2
6.2 智能终端设备间互信关系建立方式 4
6.3 智能终端设备间互信关系生命周期管理安全要求 4

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这些专利的责任。

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。

本文件主要起草人：衣强、李实、傅山、刘陶、宁华。

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。为确保在智能终端设备间传输的数据、指令等信息的安全，需确保建立通信连接的设备的身份合法性和通信连接的安全可靠性。由于不同智能终端设备形态及使用场景不尽相同，设备间建立互信关系的方式存在差异，为保证建立互信关系的设备都是用户本人持有的可信设备，同时，针对目前不同类型的智能终端设备间的互信关系建立和管理方式参差不齐的现状，特制定本文件。

本文件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安全要求，为设备间互操作提供安全基础，保证用户设备间的通信安全。

智能终端设备互信操作技术要求

1 范围

本文件规定了智能终端设备间互信关系在建立、传递、解除各阶段的安全要求。

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

本文件没有规范性引用文件。

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。

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

5 智能终端设备间互信关系框架及目标

根据不同应用和服务的需求，智能终端设备间存在互操作的场景。为确保设备间互操作的安全性，智能终端设备需要确认与其进行互操作的对端设备是可信设备，这就需要在智能终端设备间建立互信关系。智能终端设备间互信关系建立的目标是在设备互操作场景下，保证设备间进行互操作的通信安全性。

智能终端设备间互信关系框架包括智能终端设备间互信关系的建立、传递和解除，互信关系各阶段的本质是对TREC（互信关系建立凭据）的操作，涉及设备TREC（互信关系建立凭据）的生成、存储、获取、验证和删除等操作，互信关系的建立阶段包括TREC的生成、存储、获取、验证操作；互信关系的传递阶段包括TREC的获取、存储、验证操作；互信关系的解除阶段包括TREC的删除操作。TREC的各操作定义及目标如下，如图1所示：

——TREC生成操作：指智能终端设备通过自身产生、或从可信第三方服务器端获取等方式获得该智能终端设备的TREC的过程，其安全目标是确保TREC来源可信；

——TREC获取操作：指获得所要建立的互信关系中其它设备的TREC，用以进行对其它设备验证的目的，获取方式包括但不限于进行公钥传递、使用有数学/密码学理论支撑的安全协议进行协商等，其安全目标是确保对其他设备TREC获取过程的安全性；

——TREC存储操作：指智能终端设备保存设备TREC的过程，包括保存自身设备的TREC、以及保存互信关系中其它设备的TREC，其安全目标是确保TREC被安全的存储在设备中；

——TREC验证操作：指基于生成和获取的设备TREC，建立互信关系的智能终端设备彼此验证身份合法性的过程，其安全目标是确保TREC在使用过程中的安全性；

——TREC删除操作：指擦除终端设备上的设备TREC，使其不可被访问、使用等的过程，其安全目标是确保TREC被彻底删除。

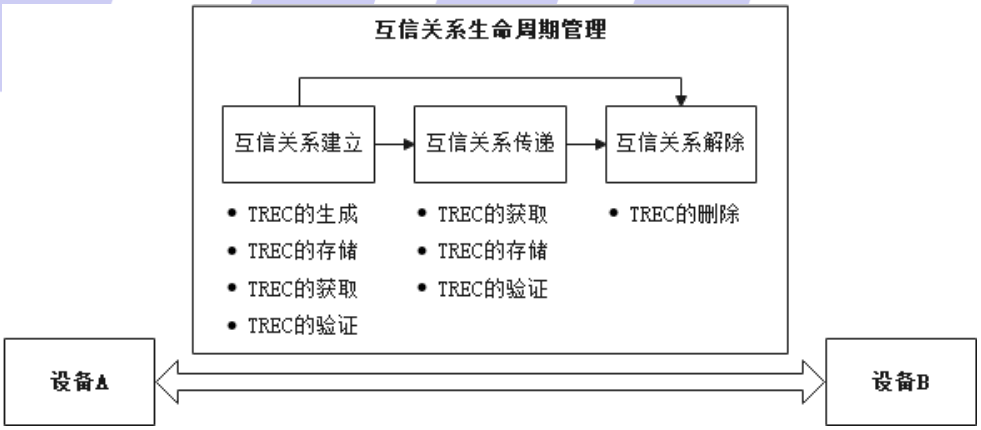

图1 互信操作框架图

6 智能终端设备间互信关系管理安全要求

6.1 智能终端设备间互信关系生命周期

6.1.1 互信关系建立

智能终端设备互信关系建立阶段的安全目标是确保只有用户本人的设备或来源及身份可信的设备间建立互信关系，而对于非用户本人的设备且来源及身份不可信的设备无法与其他设备间建立互信关系。

智能终端设备互信关系建立包括设备TREC的生成、存储、获取、验证操作。如图2所示，需要建立互信关系的设备生成各自的设备TREC，并通过安全协议或交换公钥等方式获取对端设备TREC，基于收到的设备TREC验证对端设备身份，将验证通过的设备信息加入信任设备列表，完成设备间互信关系的建立。

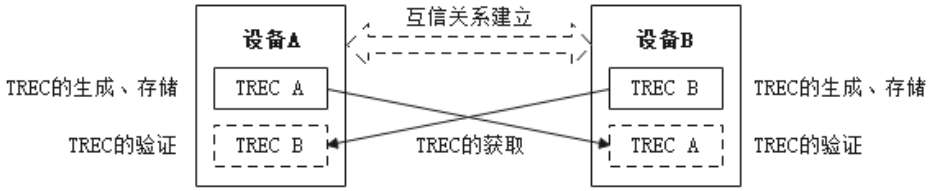

图2　互信关系建立示意图

6.1.2　互信关系传递

智能终端设备互信关系传递阶段的安全目标是确保互信关系只能在来源及身份可信的设备间进行传递。该阶段包括设备TREC的获取、存储、验证等操作。

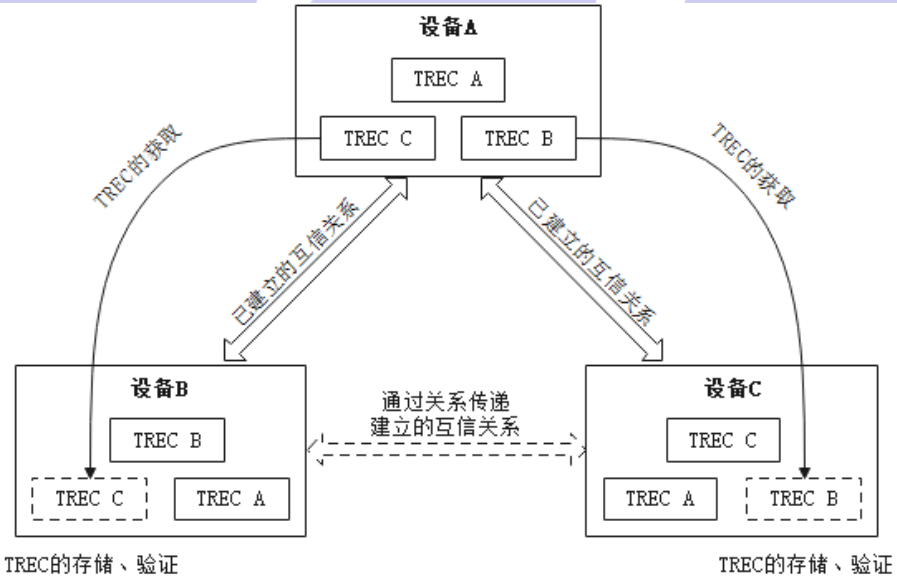

图3　互信关系传递示意图

如图3所示，设备A分别与设备B和设备C建立了互信关系，通过互信关系传递，设备A可以帮助设备B和设备C之间建立互信关系，使设备B和设备C可以进行互操作。设备A需要将设备B的TREC传递给设备C，同时将设备C的TREC传递给设备B，设备B和设备C验证收到的TREC来自共同的可信设备A，即完成设备B和设备C间互信关系的建立。

6.1.3　互信关系解除

智能终端设备互信关系解除阶段的安全目标是确保设备的TREC在互信关系解除后能够被彻底删除且无法恢复，以保证设备TREC不会被泄露，从而确保设备间互信关系的可靠性。该阶段主要涉及设备TREC的删除操作。如图4所示，解除了互信关系的设备，需要确保将对端设备的TREC从本地删除，并从信任设备列表中删除对端设备相关信息。

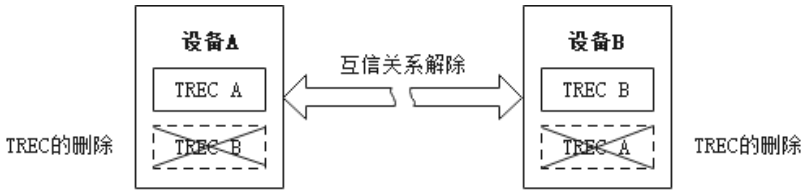

图4　互信关系解除示意图

6.2　智能终端设备间互信关系建立方式

6.2.1　智能终端设备间基于可信第三方建立互信关系

被多个设备共同信任的可信第三方可以帮助建立设备间互信关系。该方式需要设备通过账号登录可信第三方服务器。如图5所示，设备A和设备B可以将各自的TREC上传到共同信任的可信第三方服务器（如：账号服务器）。当设备A和设备B向该服务器提出对端设备TREC的下发请求时，该服务器将设备A的TREC下发给设备B，并将设备B的TREC下发给设备A，以使设备A和设备B获取彼此的设备TREC。

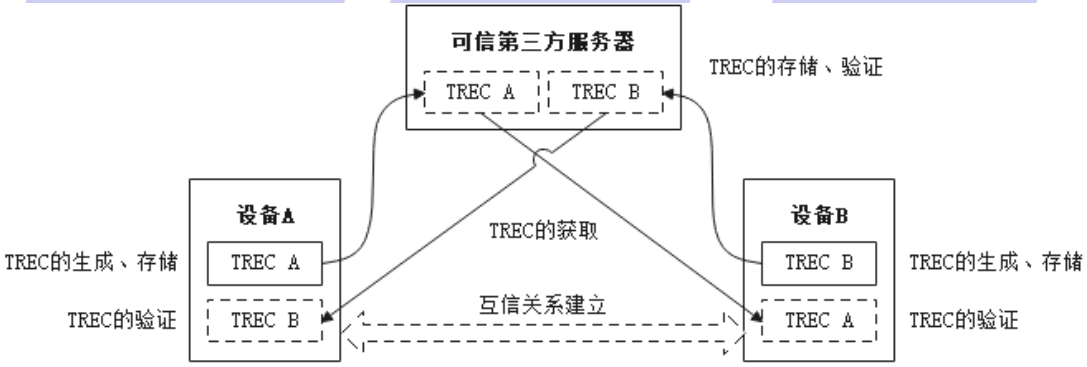

图5　基于可信第三方建立互信关系示意图

6.2.2　智能终端设备间直接点对点建立互信关系

多个智能终端设备在没有任何第三方参与的情况下，通过设备间直接点对点交互的方式建立的互信关系，如图2所示，形式包括但不限于：扫描二维码、输入预置PIN码、通过NFC触碰标签等。

6.3　智能终端设备间互信关系生命周期管理安全要求

6.3.1　智能终端设备间互信关系建立安全要求

智能终端设备间的互信关系建立主要涉及设备TREC的生成、获取、存储和验证操作，为确保互信关系建立的可靠性和安全性，对互信关系建立阶段的安全要求如下。

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。

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。

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。
   1)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。
   2）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。
   3）TREC应通过上述建立的设备间安全通道进行加密传输。
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。
   1）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。
   2）可信第三方服务器应下发与被请求设备相对应的合法TREC。
   3）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。
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。
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。
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。
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。
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。

6.3.2 智能终端设备间互信关系传递安全要求

智能终端设备间的互信关系传递主要涉及设备TREC的获取、存储和验证操作，为确保互信关系传递的可靠性和安全性，对互信关系传递阶段的安全要求如下。

a) 应满足5.3.1中c),d),e),f),g),h),i)的要求。
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。

6.3.3 智能终端设备间互信关系解除安全要求

智能终端设备间的互信关系解除主要涉及设备TREC的删除操作。为确保TREC被彻底删除，对互信关系解除阶段的安全要求如下。

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。
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。

电信终端产业协会团体标准

智能终端设备间互信操作技术要求

T/TAF 097-2021

*

版权所有 侵权必究

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