ICS 33.050
CCS M 30

团　体　标　准

T/TAF 127—2022

智能终端协同身份鉴别安全技术要求

Security technical requirements for smart terminal collaborative authentication

2022-09-15 发布　　2022-09-15 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。

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：中国信息通信研究院、华为技术有限公司、泰尔认证中心有限公司、荣耀终端有限公司、OPPO广东移动通信有限公司、北京三星通信技术研究有限公司、蚂蚁科技集团股份有限公司、北京快手科技有限公司。

本文件主要起草人：王思善、衣强、许东阳、傅山、刘陶、杜云、宁华、王艳红、武林娜、陈鑫爱、周飞、李可心、李京典、汪海、王浩仟、常琳、李杰强、赵晓娜、李根、吴越、林冠辰、落红卫。

引　言

随着移动终端及物联网技术的蓬勃发展，多种形态的智能终端设备逐渐走入消费者生活，特别随着PC、智能穿戴、智能音箱、智能电视、平板电脑、智能摄像头、智能门铃等设备的加入，多设备交互协同提供各种智慧化场景成为必然趋势。业界对多设备协同已经有了很多探索，如可穿戴免密解锁/授权批准/支付，手机与PC/PAD协同办公，手机向车机投屏互控，安防摄像头、门铃、大屏、音响联动实现访客识别通知等。

多设备协同能够提供更智能、便捷的用户操控体验，但是部分业务场景不可避免的会涉及到用户数据在不同设备间的流转，并且不同用户操作的风险等级也不尽相同。为了保证业务数据、资源访问时主体身份和权限的正确与合法性，需要对用户身份进行认证。

基于知识因素、拥有因素、生物因素这三类因素的用户身份鉴别技术，以及多种因素进行协同的多因素鉴别技术应用已经比较广泛。多设备场景下基于身份鉴别执行访问控制、业务风险控制，安全地设计开发多设备间的协同身份鉴别技术，同时保证业务操作体验在设备间的接续至关重要。

智能终端协同进行身份鉴别技术已经有了大量应用，但是业界目前并没有针对智能终端协同身份鉴别的统一技术标准，各个终端厂家和应用厂家自成体系，互联互通性差，也缺乏统一的评估准则，导致制造、开发和适配成本高昂。此外，有缺陷的设计也可能带来用户个人敏感信息或是设备数据泄露的风险，甚至是其他一系列严重的经济和社会后果。因此，本标准基于前期的调研报告的分析并结合业界实践，提出智能终端协同身份鉴别技术框架，规范协同身份鉴别技术多认证因素、多场景下的安全技术要求，为厂商在设计开发相应协同认证功能场景，或是业务利用协同认证进行业务访问控制、风险控制时给出参考依据，提高安全性，更好的服务用户，引导并促进协同身份鉴别技术的健康快速发展。

智能终端协同身份鉴别安全技术要求

1 范围

本文件规定了智能终端协同身份鉴别技术的总体框架、业务流程以及安全技术要求。

本文件适用于协同身份鉴别技术相关设计开发者，或是利用协同身份鉴别技术进行业务访问控制、风险控制方案设计开发的业务方。

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 5271.37—2021 信息技术 词汇 第37部分：生物特征识别

GB/T 18336.1—2015 信息技术 安全技术 信息技术安全评估准则 第1部分：简介和一般模型

GB/T 25069 信息安全技术 术语

GB/T 37036（所有部分） 信息技术 移动设备生物特征识别

GB/T 40660—2021 信息安全技术 生物特征识别信息保护基本要求

T/TAF 077.7—2020 APP 收集使用个人信息最小必要评估规范 人脸信息

T/TAF 097—2021 智能终端设备间互信操作技术要求

ISO/IEC 27040:2015 信息技术 安全技术 存储安全（Information technology—Security techniques—Storage security）

3 术语和定义

GB/T 25069界定的以及下列术语和定义适用于本文件。

3.1

多模态 multi-modal

单个生物特征识别系统中的模态的三个组成成分中至少有两个是多重的。

注：多重意味着类型的差异。如2D人脸和3D人脸因为传感器类型、处理方法类型不同，属于不同的模态。

3.2

多模态融合 multi-modal fusion

一种基于多模态进行识别得到确定结果的生物特征识别技术。

3.3

多因素鉴别 multi-factor authentication

使用以下两个或多个因素的鉴别：

——知晓因素，“个人知道的”；
——拥有因素，“个人持有的”；
——生物因素，“个人是什么或能够做什么的”。
[来源：ISO/IEC 27040:2015，定义3.27]
注：每种因素下可以包括多种身份鉴别技术/鉴别方式，如针对生物因素，包括2D人脸识别，3D人脸识别，声纹识别等。

3.4

协同身份鉴别（协同鉴别） collaborative authentication

多设备配合执行一种或多种鉴别方式，或是在单设备上通过单因素或多因素实现的多种身份鉴别技术进行用户身份鉴别，以达到提升便捷性、或提升安全性、或在同等安全性下降低成本/硬件要求等目的。

3.5

鉴别数据 authentication data

用于验证用户所声称身份的信息。
[来源：GB/T 18336.1—2015，定义 3.1.7]

3.6

生物特征参考 biometric reference

属于生物特征数据主体并作为生物特征比对对象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模型。
[来源：GB/T 5271.37—2021，定义 3.3.16]

3.7

生物特征模板 biometric template

可直接与检测的生物特征项进行比对的已存储的生物特征项的集合。
[来源：GB/T 5271.37—2021，定义 3.3.22]

3.8

生物特征样本 biometric sample

在生物特征项提取之前的生物特征特性的模拟表示或数字表示。
[来源：GB/T 5271.37—2021，定义 3.3.21]

3.9

人脸识别数据 face recognition data

人脸图像及其处理得到的，可单独或与其他信息结合识别特定自然人或特定自然人身份的数据。

4 总体框架

4.1 概述

智能终端协同身份鉴别包括单因素单设备的协同鉴别、单因素多设备的协同鉴别、多因素单设备的协同鉴别、多因素多设备协同鉴别。协同身份鉴别技术中的协同，体现在设备的协同，或鉴别方式的协同。基于智能终端的多因素鉴别技术，无论是基于单设备或多设备实现，均适用于本文件定义的协同身份鉴别技术框架。当涉及单一因素时，该因素下多种鉴别方式的协同同样适用本文件定义的协同身份鉴别技术框架，例如生物特征这一因素下进一步细分的单模态多设备、多模态单设备均属于协同鉴别的场景。智能终端协同身份鉴别方式见表1。

典型的协同身份鉴别技术包括：

——单因素单设备：例如单设备生物特征多模态（人脸+声纹，人脸+虹膜）；

——单因素多设备：例如多设备协同执行口令或持有可信设备或多设备识别人脸等一种因素下的一种鉴别技术，或多设备生物特征多模态这类一种因素下的至少两种鉴别技术协同；

——多因素单设备：例如单设备上执行口令+生物特征识别、持有可信设备+口令、持有可信设备+生物特征识别；

——多因素多设备：例如多设备协同执行口令+生物特征识别、持有可信设备+口令、持有可信设备+生物特征识别。

表1 智能终端协同身份鉴别方式

类别	单因素	多因素
单设备	多种鉴别方式的协同	多种鉴别方式的协同
多设备	多设备间单一鉴别方式协同或多设备间多种鉴别方式的协同	多设备间多种鉴别方式的协同

4.2 技术框架

智能终端协同身份鉴别可以发生在单设备内或多设备之间，系统架构如图1所示，包括业务应用、协同鉴别系统、身份鉴别子系统、安全通信模块。其中，协同鉴别系统包括鉴别资源管理、方案评估、鉴别能力调度、结果评估等子功能模块。协同鉴别系统通过调度资源池中的身份鉴别子系统、安全通信模块完成协同身份鉴别。

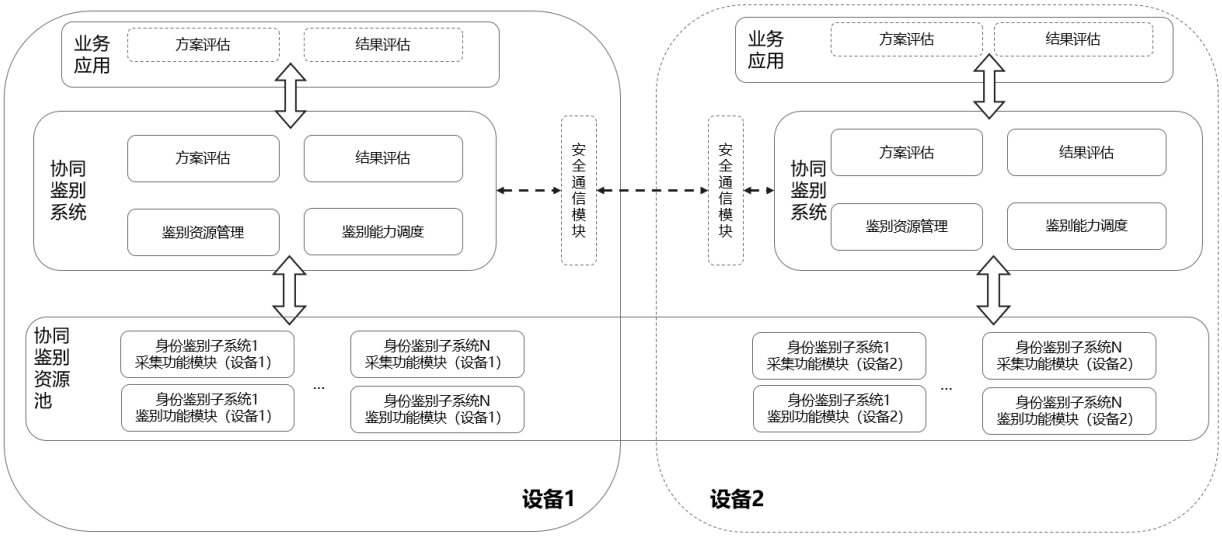

图1 系统架构

业务应用：身份鉴别功能的依赖方，根据业务诉求、业务风险等级和风控策略在业务中触发执行用户身份鉴别。业务应用可以自行根据终端当前具备的鉴别资源进行鉴别方案的评估，选择相应的多种身份鉴别方式进行协同鉴别，并自行评估协同身份鉴别结果是否满足业务需求。

协同鉴别系统：协同鉴别的核心执行单元，其中，鉴别资源管理主要提供对设备能够提供的各种鉴别资源进行管理和同步更新；方案评估根据终端当前具备的协同鉴别资源进行鉴别方案的评估，选择相应的一种或多种身份鉴别方式进行协同鉴别；鉴别能力调度主要负责对本设备或其他设备内的协同鉴别资源池进行调度，实现协同鉴别过程的采集、防伪、比对等操作；结果评估负责判断当次协同鉴别是否满足预定的策略，评估协同鉴别的结果；

安全通信模块：在多设备协同的场景下，负责完成设备间的互信关系的验证、通信密钥的协商等操作实现设备间的安全通信，保证待鉴别的凭证数据和其他业务消息的安全性。

协同鉴别资源池：终端上各种可参与协同鉴别的各种身份鉴别相关单元/系统的组合；本文件中，每个身份鉴别方式相关的单元/系统简称为一个身份鉴别子系统。每个鉴别子系统在协同鉴别资源池中，按照提供的功能，可抽象分为采集功能模块和鉴别功能模块（负责接收一个采集到的样本并与自身保存的凭证/生物特征参考进行比对）。

5　业务流程

5.1　概述

在建立了互信关系的智能终端设备间可以建立协同鉴别资源池，并执行协同身份鉴别。

同身份鉴别时，业务应用或协同鉴别系统根据业务类型进行风险等级评估，结合资源池可用的认证资源，评估并决策协同鉴别方案。在方案评估根据终端当前具备的协同鉴别资源进行鉴别方案的评估，选择相应的一种或多种身份鉴别方式进行协同鉴别。

5.2　单设备协同

5.2.1　单因素单设备协同

此场景主要是单因素下不同鉴别方式的协同鉴别。如下示意图2所示，身份鉴别子系统1和身份鉴别子系统2应该属于相同身份鉴别因素，但是对用户身份的鉴别结合了两个鉴别子系统的结果来综合评判。典型的场景是终端内部的生物特征多模态融合技术，如在单设备上进行2D人脸+声纹或是2D人脸+虹膜等属于相同生物因素下的协同。

图2　单因素单设备协同

5.2.2　多因素单设备协同

此场景是多因素下不同鉴别方式的在单设备上协同鉴别，可以为业务提供更高可信度的用户身份鉴

别能力和风险控制因素。如下图 3 所示，通过在一台设备上选择多种鉴别方法进行多因素鉴别，来满足高安业务的身份验证需求或是达到单模态需要更高软硬件成本才能达到的可信度。典型的场景例如单设备协同执行口令+生物特征识别、持有可信设备+口令、持有可信设备+生物特征识别等。

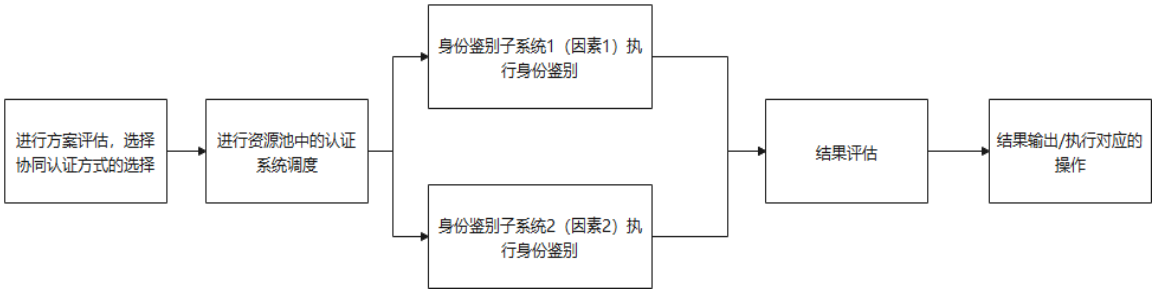

图3　多因素单设备协同

5.3　多设备协同

5.3.1　单因素多设备协同

单因素多设备是指通过单因素下一种（图4）或多种（图5）鉴别方式，在多设备（一个以上）间协同完成身份鉴别，图4和图5为两个设备间协同鉴别的示意流程。

如图4所示，设备1和设备2协同操作，基于一种鉴别方式完成用户身份鉴别，该两台设备协同工作模式见5.3.3。典型场景是PC访问手机上的数据时通过口令或人脸识别快速鉴别手机用户身份、或是智能门铃和电视/手机等设备协同工作，识别并提示门外访客身份等。

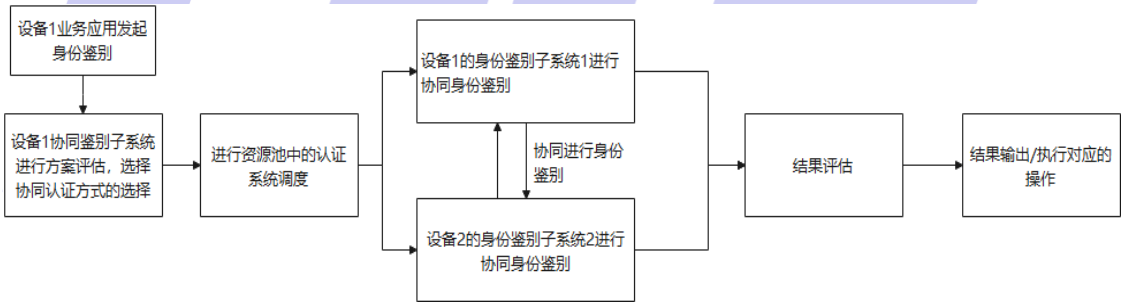

图4　基于一种鉴别方式的多设备协同身份鉴别

图5的场景下，设备1和设备2上的身份鉴别子系统1和身份鉴别子系统2属于同一身份鉴别因素下的两种鉴别方式，两台设备使用这两种鉴别方式配合完成协同鉴别。每种鉴别方式该两台设备协同的工作模式见5.3.3，典型的场景如两台设备配合以生物特征因素下的2D人脸+声纹的方式完成用户鉴别。

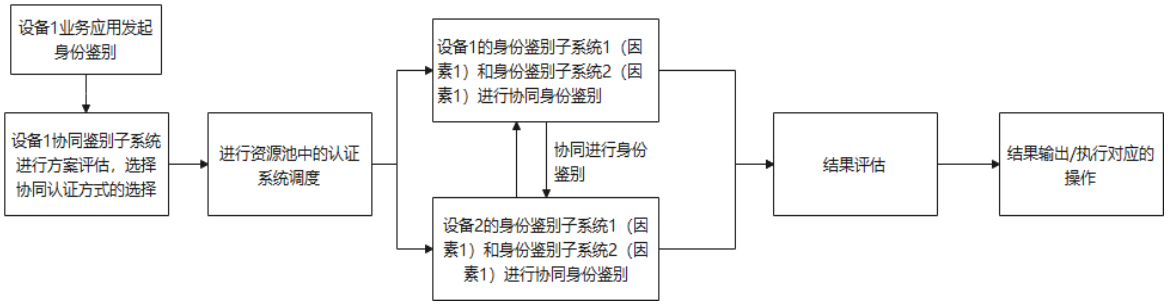

图5　基于单因素下多种鉴别方式的多设备协同身份鉴别

5.3.2　多因素多设备协同

多因素多设备是指多设备间通过多因素下多种鉴别方式协同完成用户身份鉴别（图6）。其中，设备1和设备2上的身份鉴别子系统1和身份鉴别子系统2属于不同身份鉴别因素下的两种鉴别方式，两台设备使用这两种鉴别方式配合完成协同鉴别。每种鉴别方式该两台设备协同的工作模式见5.3.3，典型场景如多设备协同执行口令+生物特征识别、持有可信设备+口令、持有可信设备+生物特征识别等多种因素的协同鉴别。

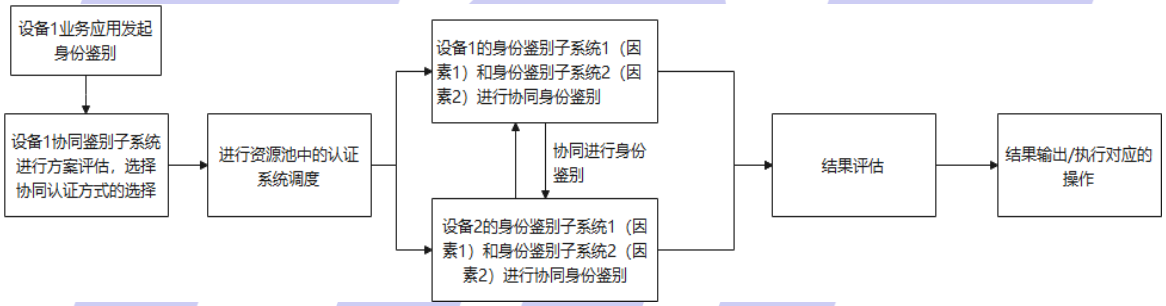

图6　基于多因素多设备协同身份鉴别

5.3.3　多设备协同工作模式

多设备之间协同进行一种身份鉴别技术时，一般可以分为以下三种模式：

a)　模式 1：访问入口设备 1 采集，数据属主设备 2 认证。其中，访问入口设备为有协同认证业务需求（如访问数据或认证用户），发起协同认证的设备，数据属主设备为需要根据协同认证结果对特定业务操作进行授权的被访问设备，见图 7。此模式下，与设备 2 建立了互信关系的设备 1，可以认为是设备 2 上身份鉴别子系统的一个采集单元；

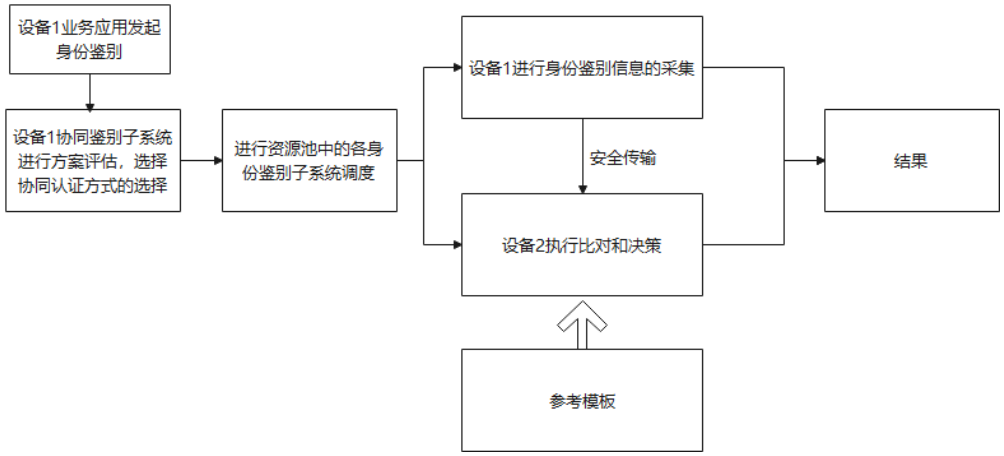

图7 多设备协同工作模式1

b) 模式 2：访问入口设备 1 采集和认证，数据属主设备 2 接受结果。此模式下，与设备 2 建立了互信关系的设备 1，可以认为是设备 2 上的一个身份鉴别子系统，为设备 2 提供用户身份鉴别能力，见图 8；

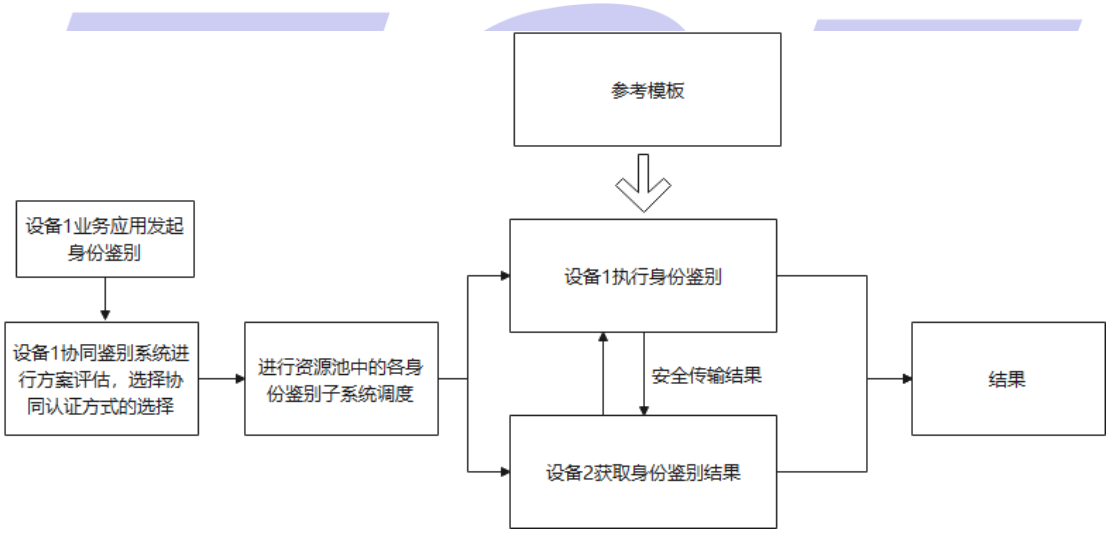

图8 多设备协同工作模式2

c) 模式 3：访问入口设备 1 没有采集和认证能力，请求数据属主设备 2 完成采集和认证。此模式下，访问设备 1 触发在属主设备 2 完成用户身份鉴别（图 9）。

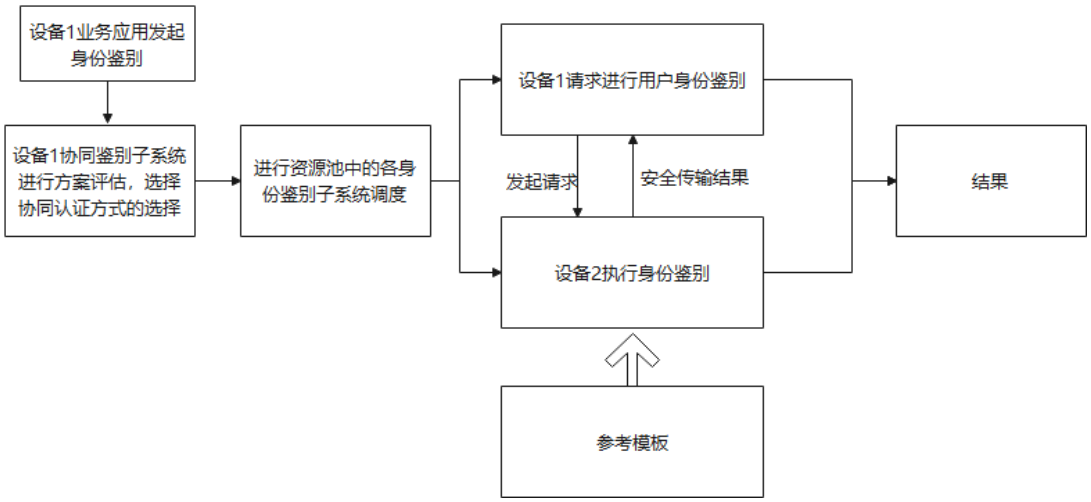

图9　多设备协同工作模式3

6　安全技术要求

6.1　总体安全要求

总体安全要求如下：

a) 应仅在建立互信关系的设备间建立资源池并进行协同身份鉴别，互信关系的建立方式可参考T/TAF 097—2021 的要求；

b) 智能终端设备本地的身份鉴别子系统，应在完成凭证录入正式启用后，才具备加入资源池的条件；

c) 对于生物特征类凭证，生物特征参考的采集、存储、使用、销毁等要求应遵从现行规定，不宜在多设备间传输生物特征参考，对于法律法规禁止远程身份鉴别模式的场景下，应仅使用本地模式；

d) 在执行协同鉴别的过程中，当涉及多设备协同采集生物特征样本（如人脸、声纹）的场景，采集到的样本应仅在建立资源池的设备间通过安全通道传输。具体传输安全要求宜参考GB/T 40660—2021、GB/T 37036、T/TAF 077.7—2020 等现行标准中“远程模式”或“本地+远程模式”下传输安全要求；

注：基于指纹的身份鉴别应使用本地模式。

e) 协同身份鉴别技术，不应在身份鉴别子系统的身份鉴别凭证录入/修改/删除的场景使用；

f) 协同鉴别功能的开启操作应告知用户并获得用户的单独同意，若通过开关的方式管理协同鉴别功能开启，则开关应默认关闭；

g) 用户不进行协同身份鉴别时，不应禁止用户其他业务的正常使用，仅可停止相关功能，并应告知可替代处理流程。

6.2　资源池管理安全要求

协同鉴别资源池应满足以下要求：

a) 宜对资源池中不同身份鉴别子系统提供的鉴别能力的强度进行区分，使方案评估模块和结果评估模块根据鉴别能力给出更准确的给出判断。鉴别能力的强度可参考附录 A；

b) 宜对资源池中不同身份鉴别子系统在进行采集、比对、存储等环节时的软硬件环境的安全性进行区分，使方案评估模块和结果评估模块根据环境安全性更准确的给出判断；

c) 加入资源池的身份鉴别子系统应具备身份标识；
d) 加入资源池的身份鉴别子系统应具备资源池设备间的认证凭证，用于证明数据（采集的数据或给出的鉴权结果）来源安全可靠；
e) 资源池中身份鉴别子系统的身份标识和身份鉴别子系统的可用状态应具备安全同步机制；
f) 当身份鉴别子系统的可用状态发生变化时，应及时从资源池中移除该子系统；
g) 当设备间的互信关系发生变化时，应及时对资源池的相关信息进行同步。

6.3 协同鉴别系统安全要求

系统应满足以下要求：
a) 应结合资源池中的可用资源，根据协同鉴别方案选择策略来选定协同鉴别方案和 5.3.3 章的协同身份鉴别的工作模式；
b) 应根据选定的协同鉴别方案和工作模式决定对资源池中身份鉴别子系统的采集和鉴别能力进行调度；
c) 协同鉴别方案选择的策略宜支持动态配置；
d) 配置到协同鉴别系统的策略应具备完整性保护机制；
e) 5.3.3 中的模式 2 下，应保证访问入口设备执行的鉴别方式整体的安全性和强度不低于在属主设备独立执行该类鉴别方式时的安全性和强度；

鉴别能力调度应满足以下要求：
a) 身份鉴别子系统采集的数据，在发出时应携带身份鉴别子系统提供的认证凭证（如采集模块私钥提供的签名）；
b) 接收到某个鉴别子系统采集的数据，应使用认证凭证（如采集模块的公钥），验证数据是否是来自于资源池内的合法鉴别子系统；
c) 鉴别子系统的鉴别结果，在发出时应携带身份鉴别子系统提供的认证凭证（如采集模块私钥提供的签名）；
d) 接收到某个鉴别子系统发送的鉴别结果，应使用认证凭证（如采集模块的公钥），验证数据是否是来自于资源池内的合法鉴别子系统；
e) 当涉及多设备间传输鉴别数据时，鉴别数据应仅用于进行用户身份鉴别，除非明确告知同意外，不应保留或用于其它用途；

结果评估应满足以下要求：
a) 应结合协同鉴别评估策略，对一个或多个鉴别子系统给出的鉴别结果进行综合评估。针对不同的认证方式，可基于 FAR/FRR/SAR 等指标，和认证模块所处的设备安全等级，综合评估认证结果；
b) 可向业务应用返回对应的认证结果，由业务应用使用应用自己保存的评估策略执行判断。

附 录 A
（资料性）
业务风险等级评估和认证方案能力等级评估

A.1 业务风险等级评估

业务风险等级直接影响认证系统所采取的认证方式，参考NIST《数字身份指南》（SP800-63），给出评估业务风险等级方法。其中，风险分类的维度包括：

——造成不便或名誉影响
——经济损失或组织可信度影响
——影响组织的项目或公共利益
——未授权的敏感信息泄露
——人身安全
——违法犯罪

风险等级的分类的如表A.1所示：

表A.1 风险操作等级划分

影响类型	风险等级		
	低	中	高
造成不便或名誉影响	低	中	高
经济损失或组织可信度影响	低	中	高
影响组织的项目或公共利益	N/A	低/中	高
未授权的敏感信息泄露	N/A	低/中	高
人身安全	N/A	低	中/高
违法犯罪	N/A	低/中	高

综合风险操作等级评估，可以对业务风险等级进行评估。根据业务风险等级，协同鉴别调度模块会结合资源池（包含设备可用的采集器、认证器资源），为业务提供足够安全的认证能力，以适配业务风险等级。

A.2 认证方案能力等级评估

针对认证能力等级评估，根据不同认证凭证达到的错误接受率FAR（False Accept Rate）、错误拒绝率FRR(False Reject Rate)、欺骗接受率SAR（Spoof Accept Rate），将用户身份鉴别方法从认证能力本身的维度分为不同的认证方案能力等级，认证方案能力等级将作为认证场景判断主体信任等级的重要依据。不同认证方式的认证指标示例如下表A.2所示。其中，性能指标参考安卓兼容性定义文档（Compatibility Definition Document，CDD）要求。

表A.2 不同认证方式性能举例

认证方式举例	性能指标
纯数字口令（6 位锁屏 PIN） 数字+字母组合密码 可信持有物（OPT、USB KEY 及同等类型）	FAR = 0 FRR = 0 SAR = 0

表A.2　不同认证方式性能举例（续）

认证方式举例	性能指标
3D 人脸/指纹认证；	FAR ≤ 0.002% FRR ≤ 10% SAR ≤ 7%
2D 人脸认证；	FAR ≤ 0.002% FRR ≤ 10% 7% < SAR ≤ 20%
行为认证； 骨声纹认证; 基于佩戴和测距的可信持有物的持有状态； 佩戴检测；	FAR ≤ 1% FRR ≤ 10% SAR ≤ 20%
声纹认证； PPG 认证；	FAR ≤ 3% FRR ≤ 10% 7% ≤ SAR ≤ 20%

同时，一个身份鉴别子系统内分为数据采集，特征提取，特征比对，特征存储，结果签发几个执行单元，每个执行单元本身的运行、存储环境安全，以及各执行单元间的通信安全都是判断整个认证方案安全等级的依据。根据硬件环境差异，执行单元运行环境包括：高安全硬件可信环境（SE），硬件可信执行环境（TEE、SGX），有访问控制的执行环境，无访问控制的运行环境（RTOS）。整体认证方案的安全等级会根据各执行单元运行环境安全强度，综合评估。

参 考 文 献

[1] NIST SP800-63 (all parts)　Digital Identity Guidelines

电信终端产业协会团体标准

智能终端协同身份鉴别安全技术要求

T/TAF 127—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