ICS 33.050
CCS M 30

团　体　标　准

T/TAF 165—2023

智能终端协同身份鉴别安全测试方法

Test methods for security technical requirements for smart terminal collaborative authentication

2023-04-26 发布　　2023-04-26 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、泰尔认证中心有限公司、郑州信大捷安信息技术股份有限公司。

本文件主要起草人：刘珍、胡重阳、王嘉义、马四英、李战锋、衣强、李实、魏凡星、姜慧格、常琳、钱康、李俊宏、宁华、刘献伦。

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，多设备交互协同能够提供更智能、便捷的用户操控体验。在进行多设备交互时，不可避免的会涉及到用户数据在不同设备间的流转，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。

T/TAF 127—2022制定了智能终端协同身份鉴别技术框架，规范了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，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。为了测评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 127—2022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协同身份鉴别安全技术的落地实施，切实地保证智能终端协同身份鉴别的安全。

智能终端协同身份鉴别安全测试方法

1 范围

本文件规定了智能终端协同身份鉴别安全总体安全要求、资源池管理安全要求和协同鉴别系统安全要求的测试方法。

本文件适用于面向消费者的智能终端设备，用于指导智能终端设备厂商和评测机构开展智能终端协同身份鉴别安全的测评工作。

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 25069 信息安全技术 术语

T/TAF 117—2022 智能终端设备间互信操作测试方法

T/TAF 127—2022 智能终端协同身份鉴别安全技术要求

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　智能终端协同身份鉴别安全测试概述

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。多设备之间协同进行一种身份鉴别技术时，又可以分为3种模式：

a)　模式1：访问入口设备采集，数据属主设备认证；

b)　模式2：访问入口设备采集和认证，数据属主设备接受结果；

c)　模式3：访问入口设备没有采集和认证能力，请求数据属主设备完成采集和认证。

遍历这些鉴别组合、模式，提炼出11种智能终端协同身份鉴别方式（见表1）。

表1　智能终端协同身份鉴别方式

类别	单因素	多因素

表 1　智能终端协同身份鉴别方式（续）

类别	单因素	多因素
单设备协同	场景1.1-单因素单设备协同（如：因素1+因素1）	场景1.2-多因素单设备协同（如：因素1+因素2）
多设备协同模式1	场景2.1-单因素多设备单鉴别方式协同模式1（如：因素1鉴别方式1+因素1鉴别方式1）	场景2.3-多因素多设备协同模式1（如：因素1+因素2）
	场景2.2-单因素多设备多鉴别方式协同模式1（如：因素1鉴别方式1+因素1鉴别方式2）	
多设备协同模式2	场景3.1-单因素多设备单鉴别方式协同模式2（如：因素1鉴别方式1+因素1鉴别方式1）	场景3.3-多因素多设备协同模式2（如：因素1+因素2）
	场景3.2-单因素多设备多鉴别方式协同模式2（如：因素1鉴别方式1+因素1鉴别方式2）	
多设备协同模式3	场景4.1-单因素多设备单鉴别方式协同模式3（如：因素1鉴别方式1+因素1鉴别方式1）	场景4.3-多因素多设备协同模式3（如：因素1+因素2）
	场景4.2-单因素多设备多鉴别方式协同模式3（如：因素1鉴别方式1+因素1鉴别方式2）	

根据智能终端协同身份鉴别方式使用的因素个数、设备个数及使用的协同鉴别模式的不同，可以提炼出以下11种场景：

——场景1.1：单因素单设备协同，在一台设备上，选择多个相同的身份鉴别因素进行身份认证。（组网图见附录A.1，技术标准见T/TAF 127—2022，5.2.1图2）

——场景1.2：多因素单设备协同，在一台设备上，选择多个不同的身份鉴别因素进行身份认证。（组网图见附录A.2，技术标准见T/TAF 127—2022，5.2.2图3）

——场景2.1：单因素多设备单鉴别方式协同模式1，业务入口设备2采集因素1的身份鉴别信息，发送给设备3，设备3进行认证。（组网图见附录A.3，技术标准见T/TAF 127—2022，5.3.1图4，5.3.3图7）

——场景2.2：单因素多设备多鉴别方式协同模式1，业务入口设备2采集因素1的多种身份鉴别信息，发送给设备3，设备3进行认证。（组网图见附录A.4，技术标准见T/TAF 127—2022，5.3.1图5，5.3.3图7）

——场景2.3：多因素多设备协同模式1，业务入口设备2采集多个不同因素的身份鉴别信息，发送给设备3，设备3进行认证。（组网图见附录A.5，技术标准见T/TAF 127—2022，5.3.2图6，5.3.3图7）

——场景3.1：单因素多设备单鉴别方式协同模式2，业务入口设备2采集因素1的身份鉴别信息，完成认证后，将认证结果发送给设备3，设备3进行确认。（组网图见附录A.6，技术标准见T/TAF 127—2022，5.3.1图4，5.3.3图8）

——场景3.2：单因素多设备多鉴别方式协同模式2，业务入口设备2采集因素1的多个身份鉴别信息，完成认证后，将认证结果发送给设备3，设备3进行确认。（组网图见附录A.7，技术标准见T/TAF 127—2022，5.3.1图5，5.3.3图8）

——场景3.3：多因素多设备协同模式2，业务入口设备2采集多个因素的身份鉴别信息，完成认证后，将认证结果发送给设备3，设备3进行确认。（组网图见附录A.8，技术标准见T/TAF 127—2022，5.3.1图6，5.3.3图8）

——场景4.1：单因素多设备单鉴别方式协同模式3，访问入口设备2没有采集和认证能力，请求设备3采集因素1的身份鉴别信息，设备3完成认证后，将认证结果发送给设备2，设备2进行确认。（组网图见附录A.9，技术标准见T/TAF 127—2022，5.3.1图4，5.3.3图9）

——场景4.2：单因素多设备多鉴别方式协同模式3，访问入口设备2没有采集和认证能力，请求设备3采集因素1的多个身份鉴别信息，设备3完成认证后，将认证结果发送给设备2，设备2进行确认。（组网图见附录A.10，技术标准见T/TAF 127—2022，5.3.1图5，5.3.3图9）

——场景4.3：多因素多设备协同模式3，访问入口设备2没有采集和认证能力，请求设备3采集多个因素的身份鉴别信息，设备3完成认证后，将认证结果发送给设备2，设备2进行确认。（组网图见附录A.11，技术标准见T/TAF 127—2022，5.3.1图6，5.3.3图9）

综上，本文件测试方法的设计思路为：以安全技术要求和应用场景为维度组织测试项（技术标准和测试项的映射关系见附录B.1），在测试项中描述要测评的T/TAF 127—2022，6章节，测试步骤、预期结果描述测评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，针对可以开展验证型测试的安全功能同时采用证明型与验证型两种测试方法，按照场景搭建测试环境时，提炼出2种部署预置条件的方式（见表2）；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/评测证书，替代设计文档、代码片段等资料，如：CC认证等。

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

表2　智能终端协同身份鉴别安全测试环境预置条件

测试场景	单设备协同（含场景1.1、1.2）	多设备协同模式1（含场景2.1、2.2、2.3）	多设备协同模式2（含场景3.1、3.2、3.3）	多设备协同模式3（含场景4.1、4.2、4.3）
预置条件	a） 设备1开启协同身份鉴别功能； b） 设备1已录入并启用协同身份鉴别业务使用的身份认证凭据； c） 设备1上协同身份鉴别功能的外部依赖（如权限）满足要求，可以正常执行协同身份鉴别功能。	a） 设备2、设备3开启协同身份鉴别功能； b） 多设备协同模式1、多设备协同模式3组网在设备3上录入并启用协同身份鉴别业务使用的身份认证凭据；多设备协同模式2组网在设备2上录入并启用协同身份鉴别业务使用的身份认证凭据； c） 设备2、设备3已建立设备间互信关系； d） 设备2、设备3上协同身份鉴别功能外部依赖（如权限）满足要求，可以正常执行协同身份鉴别功能。		

5　智能终端协同身份鉴别安全测试方法

5.1　总体安全要求测试方法

5.1.1　测试项a)：测评设备间协同鉴别资源池建立前已建立设备间互信关系

测试要求T/TAF 127—2022-6.1-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。本要求的测试方法如下：

注：互信关系的评测见T/TAF 117—2022。

a） 测试步骤：

1） 步骤1：检查厂商提交的文档，查看设备间资源池建立的设计文档（或业界公认的认证/评测证书），是否确保已经建立了设备间互信关系；
2） 步骤2：按照多设备协同模式1组网搭建测试环境，在智能终端设备2、设备3上使用日志/命令行/测试应用等测试工具查看是否已经建立了设备间互信关系；
3） 步骤3：按照多设备协同模式2组网搭建测试环境，在智能终端设备2、设备3上使用日志/命令行/测试应用等测试工具查看是否已经建立了设备间互信关系；
4） 步骤4：按照多设备协同模式3组网搭建测试环境，在智能终端设备2、设备3上使用日志/命令行/测试应用等测试工具查看是否已经建立了设备间互信关系。

b） 预期结果：
1） 步骤1之后，若可以确保设备间资源池建立前已建立设备间互信关系，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2、设备3已经建立了设备间互信关系，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2、设备3已经建立了设备间互信关系，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2、设备3已经建立了设备间互信关系，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

5.1.2 测试项 b)：测评本地身份鉴别子系统加入资源池前已完成凭据录入并正式启用

测试要求 T/TAF 127—2022-6.1-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。本要求的测试方法如下：

a） 测试步骤：
1） 步骤1：检查厂商提交的文档，查看本地身份鉴别子系统加入资源池的设计文档，是否确保加入资源池前已完成凭据录入并正式启用；
2） 步骤2：按照单设备协同组网搭建测试环境，遍历设备1上协同身份鉴别业务使用的所有凭据录入入口，查看是否已录入凭据并正式启用；
3） 步骤3：按照多设备协同模式1组网搭建测试环境，遍历设备3上协同身份鉴别业务使用的所有凭据录入入口，查看是否已录入凭据并正式启用；
4） 步骤4：按照多设备协同模式2组网搭建测试环境，遍历设备2上协同身份鉴别业务使用的所有凭据录入入口，查看是否已录入凭据并正式启用；
5） 步骤5：按照多设备协同模式3组网搭建测试环境，遍历设备3上协同身份鉴别业务使用的所有凭据录入入口，查看是否已录入凭据并正式启用。

b） 预期结果：
1） 在步骤1之后，若可以确保身份鉴别子系统在加入资源池前已完成录入凭据并正式启用，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1上所有协同身份鉴别业务使用的凭据都已录入并正式启用，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3上所有协同身份鉴别业务使用的凭据都已录入并正式启用，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2上所有协同身份鉴别业务使用的凭据都已录入并正式启用，然后执行步骤5；否则为“不符合要求”，测评结束；
5） 在步骤5之后，若设备3上所有协同身份鉴别业务使用的凭据都已录入并正式启用，测评结果为“未见异常”；否则为“不符合要求”，测评结束。

5.1.3 测试项 c)：测评生物特征参考的采集、存储、使用、销毁等遵从现行规定

测试要求 T/TAF 127—2022-6.1-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。本要求的测试方法如下：

a） 测试步骤：

1） 步骤1：检查厂商提交的文档，查看生物特征类凭据处理的设计文档（或业界公认的认证/评测证书），是否确保生物特征参考的采集、存储、使用、销毁等要求遵从现行规定（参考：GB/T 37036、GB/T 40660—2021）。

b） 预期结果：

1） 在步骤1之后，若能确保生物特征参考的采集、存储、使用、销毁等要求遵从现行规定，测评结果为“未见异常”，否则测评结果为“不符合要求”，测评结束。

注：不使用生物特征进行协同身份鉴别的终端设备，无需测试。

5.1.4 测试项 d)：测评生物特征样本基于安全通道在建立资源池的设备间传输

测试要求 T/TAF 127—2022-6.1-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；本要求的测试方法如下：

注：基于指纹的身份鉴别应使用本地模式。

a） 测试步骤：

1） 步骤1：检查厂商提交的文档，查看多设备协同采集生物特征样本传输的设计文档（或业界公认的认证/评测证书），是否基于指纹的身份鉴别使用的是本地模式，其它生物特征样本仅在建立资源池的设备间通过安全通道传输；

2） 步骤2：按照多设备协同模式1组网搭建测试环境，执行协同身份鉴别业务，通过网络抓包工具抓取设备2和设备3之间传输的生物特征样本并篡改，检查数据是否加密传输，篡改后是否导致协同身份鉴别失败。

b） 预期结果：

1） 在步骤1之后，若基于指纹的身份鉴别使用的是本地模式，其它生物特征样本使用安全传输通道在建立资源池的设备间传输，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，若传输的生物特征样本为密文，篡改后导致协同身份鉴别失败，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

注：不使用生物特征或生物特征不涉及跨设备传输时，无需测试。

5.1.5 测试项 e)：测评协同身份鉴别技术不应用于身份凭证凭据录入/修改/删除场景

测试要求 T/TAF 127—2022-6.1-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。本要求的测试方法如下：

a） 测试步骤：

1） 步骤1：检查厂商提交的文档，查看协同身份鉴别技术使用场景的设计文档，是否用于身份鉴别凭据录入/修改/删除场景；

2） 步骤2：按照单设备协同组网搭建测试环境，遍历设备1上所有身份鉴别入口，分别进行凭据录入、修改、删除的操作，使用日志/命令行/测试应用等测试工具查看是否使用了协同身份鉴别技术进行身份认证；

3） 步骤3：按照多设备协同模式1组网搭建测试环境，遍历设备3上所有身份鉴别入口，分别进行凭据录入、修改、删除的操作，使用日志/命令行/测试应用等测试工具查看是否使用了协同身份鉴别技术进行身份认证；
4） 步骤4：按照多设备协同模式2组网搭建测试环境，遍历设备2上所有身份鉴别入口，分别进行凭据录入、修改、删除的操作，使用日志/命令行/测试应用等测试工具查看是否使用了协同身份鉴别技术进行身份认证；
5） 步骤5：按照多设备协同模式3组网搭建测试环境，遍历设备3上所有身份鉴别入口，分别进行凭据录入、修改、删除的操作，使用日志/命令行/测试应用等测试工具查看是否使用了协同身份鉴别技术进行身份认证。

b） 预期结果：
1） 在步骤1之后，若协同身份鉴别技术未应用于身份鉴别凭据录入/修改/删除场景，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1上在录入、修改、删除凭据时，未使用协同身份鉴别技术进行身份认证，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3上在录入、修改、删除凭据时，未使用协同身份鉴别技术进行身份认证，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2上在录入、修改、删除凭据时，未使用协同身份鉴别技术进行身份认证，然后执行步骤5；否则为“不符合要求”，测评结束；
5） 在步骤5之后，若设备3上在录入、修改、删除凭据时，未使用协同身份鉴别技术进行身份认证，测评结果为“未见异常”；否则为“不符合要求”，测评结束。

5.1.6 测试项 f)：测评协同鉴别功能开启应获得用户单独同意

测试要求 T/TAF 127—2022-6.1-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。本要求的测试方法如下：

a） 测试步骤：
1） 步骤1：检查厂商提交的文档，检查协同鉴别功能管理的设计文档，协同鉴别功能是否默认关闭，且在用户单独同意下才能开启；
2） 步骤2：按照单设备协同组网搭建测试环境，设备1升级新版本，检查协同鉴别功能是否默认关闭；
3） 步骤3：设备1打开协同鉴别功能，检查是否在提示用户并获得用户同意的情况下才可使用协同鉴别功能；
4） 步骤4：设备1打开协同鉴别功能，检查是否在用户拒绝的情况下无法使用协同鉴别功能；
5） 步骤5：按照多设备协同模式1组网搭建测试环境，设备3升级新版本，在设备3上检查协同鉴别功能是否默认关闭；
6） 步骤6：设备3打开协同鉴别功能，检查是否在提示用户并获得用户同意的情况下才可使用协同鉴别功能；
7） 步骤7：设备3打开协同鉴别功能，检查是否在用户拒绝的情况下无法使用协同鉴别功能；
8） 步骤8：按照多设备协同模式2组网搭建测试环境，设备2升级新版本，在设备2上检查协同鉴别功能是否默认关闭；
9） 步骤9：设备2打开协同鉴别功能，检查是否在提示用户并获得用户同意的情况下才可使用协同鉴别功能；
10）步骤10：设备2打开协同鉴别功能，检查是否在用户拒绝的情况下无法使用协同鉴别功能；

11）步骤11：按照多设备协同模式3组网搭建测试环境，设备3升级新版本，在设备3上检查协同鉴别功能是否默认关闭；

12）步骤12：设备3打开协同鉴别功能，检查是否在提示用户并获得用户同意的情况下才可使用协同鉴别功能；

13）步骤13：设备3打开协同鉴别功能，检查是否在用户拒绝的情况下无法使用协同鉴别功能。

b） 预期结果：

1） 在步骤1之后，若协同鉴别功能默认关闭，且在用户单独同意下才能开启，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，若协同鉴别功能默认关闭，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，打开协同鉴别功能，若在提示用户并获得同意的情况下可以使用协同鉴别功能，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，打开协同鉴别功能，若在用户拒绝的情况下无法使用协同鉴别功能，然后执行步骤5；否则为“不符合要求”，测评结束；

5） 在步骤5之后，若协同鉴别功能默认关闭，然后执行步骤6；否则为“不符合要求”，测评结束；

6） 在步骤6之后，打开协同鉴别功能，若在提示用户并获得同意的情况下可以使用协同鉴别功能，然后执行步骤7；否则为“不符合要求”，测评结束；

7） 在步骤7之后，打开协同鉴别功能，若在用户拒绝的情况下无法使用协同鉴别功能，然后执行步骤8；否则为“不符合要求”，测评结束；

8） 在步骤8之后，若协同鉴别功能默认关闭，然后执行步骤9；否则为“不符合要求”，测评结束；

9） 在步骤9之后，打开协同鉴别功能，若在提示用户并获得同意的情况下可以使用协同鉴别功能，然后执行步骤10；否则为“不符合要求”，测评结束；

10）在步骤10之后，打开协同鉴别功能，若在用户拒绝的情况下无法使用协同鉴别功能，然后执行步骤11；否则为“不符合要求”，测评结束；

11）在步骤11之后，若协同鉴别功能默认关闭，然后执行步骤12；否则为“不符合要求”，测评结束；

12）在步骤12之后，打开协同鉴别功能，若在提示用户并获得同意的情况下可以使用协同鉴别功能，然后执行步骤13；否则为“不符合要求”，测评结束；

13）在步骤13之后，打开协同鉴别功能，若在用户拒绝的情况下无法使用协同鉴别功能，然后执行步骤14；否则为“不符合要求”，测评结束。

5.1.7 测试项 g)：测评用户不进行协同身份鉴别时，不禁止其他业务的正常使用

测试要求 T/TAF 127—2022-6.1-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。本要求的测试方法如下：

a） 测试步骤：

1） 步骤1：检查厂商提交的文档，查看协同鉴别功能的设计文档，不进行协同鉴别功能时是否影响其它业务的正常使用，是否告知可替代处理流程；

2） 步骤2：按照单设备协同组网搭建测试环境，在设备1上不进行协同身份鉴别功能，检查是否告知可替代处理流程（如本地认证），并尝试使用依赖身份鉴别功能的业务，检查是否正常；

3） 步骤3：按照多设备协同模式1组网搭建测试环境，在设备3上不进行协同身份鉴别功能，检查是否告知可替代处理流程（如本地认证），并尝试使用依赖身份鉴别功能的业务，检查是否正常；

4） 步骤4：按照多设备协同模式2组网搭建测试环境，在设备2上不进行协同身份鉴别功能，检查是否告知可替代处理流程（如本地认证），并尝试使用依赖身份鉴别功能的业务，检查是否正常；

5） 步骤5：按照多设备协同模式3组网搭建测试环境，在设备3上不进行协同身份鉴别功能，检查是否告知可替代处理流程（如本地认证），并尝试使用依赖身份鉴别功能的业务，检查是否正常。

b） 预期结果：

1） 在步骤1之后，若不进行协同鉴别功能时，有告知用户可替代处理流程，并不影响其它业务的正常使用，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1上不进行协同鉴别功能时，有告知用户可替代处理流程，并不影响依赖身份鉴别功能的业务的正常使用，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3上不进行协同鉴别功能时，有告知用户可替代处理流程，并不影响依赖身份鉴别功能的业务的正常使用，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2上不进行协同鉴别功能时，有告知用户可替代处理流程，并不影响依赖身份鉴别功能的业务的正常使用，然后执行步骤5；否则为“不符合要求”，测评结束；

5） 在步骤5之后，若设备3上不进行协同鉴别功能时，有告知用户可替代处理流程，并不影响依赖身份鉴别功能的业务的正常使用，测评结果为“未见异常”；否则为“不符合要求”，测评结束。

5.2 资源池管理安全要求测试方法

5.2.1 测试项 a)：测评终端设备对不同身份鉴别子系统的鉴别能力强度进行区分

测试要求 T/TAF 127—2022-6.2-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。本要求的测试方法如下：

a） 测试步骤：

1） 步骤1：检查厂商提交的文档，查看身份鉴别子系统鉴别能力的设计文档，是否对不同身份鉴别子系统提供的鉴别能力进行强度区分(可参考T/TAF 127—2022，附录A) 。

b） 预期结果：

1） 在步骤1之后，若终端设备对身份鉴别子系统鉴别能力进行强度区分，测评结果为“未见异常”；否则为“不符合要求”，测评结束。

注：此项为建议项，不强制要求满足。

5.2.2 测试项 b)：测评终端设备对不同身份鉴别子系统在采集、比对、存储等环境的软硬件环境的安全性进行区分

测试要求 T/TAF 127—2022-6.2-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。本要求的测试方法如下：

a） 测试步骤：

1） 步骤1：检查厂商提交的文档，查看身份鉴别子系统在采集、比对、存储环节的设计文档，是否对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（可参考T/TAF 127—2022，附录A.2）。

b） 预期结果：

1） 在步骤1之后，若终端设备对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，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

注：此项为建议项，不强制要求满足。

5.2.3 测试项 c)：测评加入资源池的身份鉴别子系统具备身份标识

测试要求 T/TAF 127—2022-6.2-c)：加入资源池的身份鉴别子系统应具备身份标识。本要求的测试方法如下：

a） 测试步骤：

1） 步骤1：检查厂商提交的文档，查看资源池管理的设计文档，加入资源池的身份鉴别子系统是否具备身份标识；

2） 步骤2：按照单设备协同组网搭建测试环境，在设备1上通过日志/命令行/测试应用等测试工具查看资源池的所有身份鉴别子系统是否都具备身份标识；

3） 步骤3：按照多设备协同模式1组网搭建测试环境，在设备2、设备3上通过日志/命令行/测试应用等测试工具查看资源池的所有身份鉴别子系统是否都具备身份标识；

4） 步骤4：按照多设备协同模式2组网搭建测试环境，在设备2、设备3上通过日志/命令行/测试应用等测试工具查看资源池的所有身份鉴别子系统是否都具备身份标识；

5） 步骤5：按照多设备协同模式3组网搭建测试环境，在设备2、设备3上通过日志/命令行/测试应用等测试工具查看资源池的所有身份鉴别子系统是否都具备身份标识。

b） 预期结果：

1） 在步骤1之后，若加入资源池的身份鉴别子系统都具备身份标识，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1上资源池的所有身份鉴别子系统都具备身份标识，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2、设备3上资源池的所有身份鉴别子系统都具备身份标识，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2、设备3上资源池的所有身份鉴别子系统都具备身份标识，然后执行步骤5；否则为“不符合要求”，测评结束；

5） 在步骤5之后，若设备2、设备3上资源池的所有身份鉴别子系统都具备身份标识，测评结果为“未见异常”；否则为“不符合要求”，测评结束。

5.2.4 测试项 d)：测评加入资源池的身份鉴别子系统具备资源池设备间的认证凭证

测试要求 T/TAF 127—2022-6.2-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。本要求的测试方法如下：

a） 测试步骤：

1） 步骤1：检查厂商提交的文档，查看身份鉴别子系统的设计文档，是否确保加入资源池的身份鉴别子系统具备资源池设备间的认证凭证；

2） 步骤2：按照多设备协同模式1组网搭建测试环境，在设备2、设备3上通过日志/命令行/测试应用等测试工具查看资源池的所有身份鉴别子系统是否具备资源池设备间的认证凭证；

3） 步骤3：按照多设备协同模式2组网搭建测试环境，在设备2、设备3上通过日志/命令行/测试应用等测试工具查看资源池的所有身份鉴别子系统是否具备资源池设备间的认证凭证；

4） 步骤4：按照多设备协同模式3组网搭建测试环境，在设备2、设备3上通过日志/命令行/测试应用等测试工具查看资源池的所有身份鉴别子系统是否具备资源池设备间的认证凭证。

b） 预期结果：

1） 在步骤1之后，若能确保加入资源池的身份鉴别子系统具备资源池设备间的认证凭证，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2、设备3上资源池的所有身份鉴别子系统都具备资源池设备间的认证凭证，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2、设备3上资源池的所有身份鉴别子系统都具备资源池设备间的认证凭证，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2、设备3上资源池的所有身份鉴别子系统都具备资源池设备间的认证凭证，测评结果为“未见异常”；否则为“不符合要求”，测评结束。

5.2.5 测试项 e)：测评身份鉴别子系统身份标识和可用状态具备安全同步机制

测试要求 T/TAF 127—2022-6.2-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。本要求的测试方法如下：

a） 测试步骤：

1） 步骤1：检查厂商提交的文档，查看资源池管理的设计文档，身份鉴别子系统的身份标识和可用状态变化时，是否具备安全同步机制；

2） 步骤2：按照单设备协同组网搭建测试环境，遍历录入设备1上协同身份鉴别业务使用的身份认证凭据，通过日志/命令行/测试应用等测试工具查看设备1上资源池中是否新增该凭据对应的身份鉴别子系统的身份标识和可用状态；

3） 步骤3：依次使设备1上协同身份鉴别业务使用的身份鉴别子系统锁定，通过日志/命令行/测试应用等测试工具查看设备1上资源池中该凭据对应的身份鉴别子系统的可用状态是否同步更新为锁定状态；

4） 步骤4：依次使设备1上协同身份鉴别业务使用的身份鉴别子系统解锁定，通过日志/命令行/测试应用等测试工具查看设备1上资源池中该凭据对应的身份鉴别子系统的可用状态是否同步更新为可用状态；

5） 步骤5：按照多设备协同模式1组网搭建测试环境，遍历录入设备3上协同身份鉴别业务使用的身份认证凭据，通过日志/命令行/测试应用等测试工具查看设备2、设备3上资源池中是否新增该凭据对应的身份鉴别子系统的身份标识和可用状态；

6） 步骤6：依次使设备3上协同身份鉴别业务使用的身份鉴别子系统锁定，通过日志/命令行/测试应用等测试工具查看设备2、设备3上资源池中该凭据对应的身份鉴别子系统的可用状态是否同步更新为锁定状态；

7） 步骤7：依次使设备3上协同身份鉴别业务使用的身份鉴别子系统解锁定，通过日志/命令行/测试应用等测试工具查看设备2、设备3上资源池中该凭据对应的身份鉴别子系统的可用状态是否同步更新为可用状态；

8） 步骤8：按照多设备协同模式2组网搭建测试环境，遍历录入设备2上协同身份鉴别业务使用的身份认证凭据，通过日志/命令行/测试应用等测试工具查看设备2、设备3上资源池中是否新增该凭据对应的身份鉴别子系统的身份标识和可用状态；

9） 步骤9：依次使设备2上协同身份鉴别业务使用的身份鉴别子系统锁定，通过日志/命令行/测试应用等测试工具查看设备2、设备3上资源池中该凭据对应的身份鉴别子系统的可用状态是否同步更新为锁定状态；

10） 步骤10：依次使设备2上协同身份鉴别业务使用的身份鉴别子系统解锁定，通过日志/命令行/测试应用等测试工具查看设备2、设备3上资源池中该凭据对应的身份鉴别子系统的可用状态是否同步更新为可用状态；

11） 步骤11：按照多设备协同模式3组网搭建测试环境，遍历录入设备3上协同身份鉴别业务使用的身份认证凭据，通过日志/命令行/测试应用等测试工具查看设备2、设备3上资源池中是否新增该凭据对应的身份鉴别子系统的身份标识和可用状态；

12） 步骤12：依次使设备3上协同身份鉴别业务使用的身份鉴别子系统锁定，通过日志/命令行/测试应用等测试工具查看设备2、设备3上资源池中该凭据对应的身份鉴别子系统的可用状态是否同步更新为锁定状态；

13） 步骤13：依次使设备3上协同身份鉴别业务使用的身份鉴别子系统解锁定，通过日志/命令行/测试应用等测试工具查看设备2、设备3上资源池中该凭据对应的身份鉴别子系统的可用状态是否同步更新为可用状态。

b） 预期结果：

1） 在步骤1之后，若身份鉴别子系统的身份标识和可用状态变化时，具备安全同步机制，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1录入新的身份认证凭据时，资源池列表新增该凭据对应的身份认证标识和可用状态，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1身份鉴别子系统锁定时，资源池列表中身份鉴别子系统的可用状态同步更新为锁定状态，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1身份鉴别子系统解锁定时，资源池列表中身份鉴别子系统的可用状态同步更新为可用状态，然后执行步骤5；否则为“不符合要求”，测评结束；

5） 在步骤5之后，若设备3录入新的身份认证凭据时，设备2、设备3资源池列表新增该凭据对应的身份认证标识和可用状态，然后执行步骤6，否则为“不符合要求”，测评结束；

6） 在步骤6之后，若设备3身份鉴别子系统锁定时，设备2、设备3资源池列表中身份鉴别子系统的可用状态同步更新为锁定状态，然后执行步骤7；否则为“不符合要求”，测评结束；

7） 在步骤7之后，若设备3身份鉴别子系统解锁定时，设备2、设备3资源池列表中身份鉴别子系统的可用状态同步更新为可用状态，然后执行步骤8；否则为“不符合要求”，测评结束；

8） 在步骤8之后，若设备2录入新的身份认证凭据时，设备2、设备3资源池列表新增该凭据对应的身份认证标识和可用状态，然后执行步骤9，否则为“不符合要求”，测评结束；

9） 在步骤9之后，若设备2身份鉴别子系统锁定时，设备2、设备3资源池列表中身份鉴别子系统的可用状态同步更新为锁定状态，然后执行步骤10；否则为“不符合要求”，测评结束；

10） 在步骤10之后，若设备2身份鉴别子系统解锁定时，设备2、设备3资源池列表中身份鉴别子系统的可用状态同步更新为可用状态，然后执行步骤11；否则为“不符合要求”，测评结束；

11） 在步骤11之后，若设备3录入新的身份认证凭据时，设备2、设备3资源池列表新增该凭据对应的身份认证标识和可用状态，然后执行步骤12，否则为“不符合要求”，测评结束；

12） 在步骤12之后，若设备3身份鉴别子系统锁定时，设备2、设备3资源池列表中身份鉴别子系统的可用状态同步更新为锁定状态，然后执行步骤13；否则为“不符合要求”，测评结束；

13） 在步骤13之后，若设备3身份鉴别子系统解锁定时，设备2、设备3资源池列表中身份鉴别子系统的可用状态同步更新为可用状态，测评结果为“未见异常”；否则为“不符合要求”，测评结束。

5.2.6 测试项 f)：测评身份鉴别子系统的可用状态发生变化时，及时从资源池中移除该子系统

测试要求 T/TAF 127—2022-6.2-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。本要求的测试方法如下：

a） 测试步骤：

1） 步骤1：检查厂商提交的文档，查看资源池设计文档，检查资源池中身份鉴别子系统的可用状态变化时，是否从资源池中移除该子系统；

2） 步骤2：按照单设备协同组网搭建测试环境，遍历删除设备1上协同身份鉴别业务使用的身份认证凭据，通过日志/命令行/测试应用等测试工具查看设备1上资源池是否移除了该身份认证凭据对应的子系统；

3） 步骤3：按照多设备协同模式1组网搭建测试环境，遍历删除设备3上协同身份鉴别业务使用的身份认证凭据，通过日志/命令行/测试应用等测试工具查看设备2、设备3上资源池是否移除了该身份认证凭据对应的子系统；

4） 步骤4：按照多设备协同模式2组网搭建测试环境，遍历删除设备2上协同身份鉴别业务使用的身份认证凭据，通过日志/命令行/测试应用等测试工具查看设备2、设备3上资源池是否移除了该身份认证凭据对应的子系统；

5） 步骤5：按照多设备协同模式3组网搭建测试环境，遍历删除设备3上协同身份鉴别业务使用的身份认证凭据，通过日志/命令行/测试应用等测试工具查看设备2、设备3上资源池是否移除了该身份认证凭据对应的子系统。

b） 预期结果：

1） 在步骤1之后，若资源池中身份鉴别子系统的可用状态变化时，资源池会移除该子系统，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1资源池中列表中不包括该凭据对应的身份鉴别子系统，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2、设备3的资源池中列表和身份标识中不包括该凭据对应的身份鉴别子系统和身份标识，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2、设备3的资源池中列表和身份标识中不包括该凭据对应的身份鉴别子系统和身份标识，然后执行步骤5；否则为“不符合要求”，测评结束；

5） 在步骤5之后，若设备2、设备3的资源池中列表和身份标识中不包括该凭据对应的身份鉴别子系统和身份标识，测评结果为“未见异常”；否则为“不符合要求”，测评结束。

5.2.7 测试项 g)：测评设备间的互信关系发生变化时，及时对资源池的相关信息进行同步

测试要求 T/TAF 127—2022-6.2-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。本要求的测试方法如下：

a） 测试步骤：

1） 步骤1：检查厂商提交的文档，查看资源池设计文档，检查设备间互信关系发生变化时，是否及时对资源池的相关信息进行同步；

2） 步骤2：按照多设备协同模式1组网搭建测试环境，建立设备间互信关系，通过日志/命令行/测试应用等测试工具查看设备2、设备3上资源池是否包括对端设备的资源池信息；
3） 步骤3：按照多设备协同模式1组网搭建测试环境，解除设备间互信关系，通过日志/命令行/测试应用等测试工具查看设备2、设备3上资源池是否不包括对端设备的资源池信息；
4） 步骤4：按照多设备协同模式2组网搭建测试环境，建立设备间互信关系，通过日志/命令行/测试应用等测试工具查看设备2、设备3上资源池是否包括对端设备的资源池信息；
5） 步骤5：按照多设备协同模式2组网搭建测试环境，解除设备间互信关系，通过日志/命令行/测试应用等测试工具查看设备2、设备3上资源池是否不包括对端设备的资源池信息；
6） 步骤6：按照多设备协同模式3组网搭建测试环境，建立设备间互信关系，通过日志/命令行/测试应用等测试工具查看设备2、设备3上资源池是否包括对端设备的资源池信息；
7） 步骤7：按照多设备协同模式3组网搭建测试环境，解除设备间互信关系，通过日志/命令行/测试应用等测试工具查看设备2、设备3上资源池是否不包括对端设备的资源池信息。

b） 预期结果：

1） 在步骤1之后，若设备间互信关系发生变化时，资源池中的相关信息及时进行了同步，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，若建立设备互信关系时，设备2、设备3的资源池信息包括了对端设备的资源池信息，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，若解除设备互信关系时，设备2、设备3的资源池信息不包括对端设备的资源池信息，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，若建立设备互信关系时，设备2、设备3的资源池信息包括了对端设备的资源池信息，然后执行步骤5；否则为“不符合要求”，测评结束；
5） 在步骤5之后，若解除设备互信关系时，设备2、设备3的资源池信息不包括对端设备的资源池信息，然后执行步骤6；否则为“不符合要求”，测评结束；
6） 在步骤6之后，若建立设备互信关系时，设备2、设备3的资源池信息包括了对端设备的资源池信息，然后执行步骤7；否则为“不符合要求”，测评结束；
7） 在步骤7之后，若解除设备互信关系时，设备2、设备3的资源池信息不包括对端设备的资源池信息，测评结果为“未见异常”；否则为“不符合要求”，测评结束。

5.3 协同鉴别系统安全要求测试方法

5.3.1 鉴别系统要求

5.3.1.1 测试项 a)：测评协同鉴别系统结合资源池中的可用资源根据协同鉴别方案选择策略选定协同鉴别方案和协同身份鉴别的工作模式

测试要求 T/TAF 127—2022-6.3-鉴别系统要求-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。本要求的测试方法如下：

a） 测试步骤：

1） 步骤1：检查厂商提交的文档，查看协同鉴别系统方案评估的设计文档，是否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协同身份鉴别的工作模式；
2） 步骤2：按照单设备协同组网分别搭建单设备单因素协同、单设备多因素协同测试环境，在设备1通过日志/命令行/测试应用等测试工具读取协同鉴别方案选择策略，查看是否正确匹配相应的场景；

3） 步骤3：按照多设备协同模式1组网分别搭建多设备单因素单鉴别方式协同、多设备单因素多鉴别方式协同、多设备多因素协同测试环境，在设备2通过日志/命令行/测试应用等测试工具读取协同鉴别方案选择策略，查看是否正确匹配相应的场景；

4） 步骤4：按照多设备协同模式2组网分别搭建多设备单因素单鉴别方式协同、多设备单因素多鉴别方式协同、多设备多因素协同测试环境，在设备2通过日志/命令行/测试应用等测试工具读取协同鉴别方案选择策略，查看是否正确匹配相应的场景；

5） 步骤5：按照多设备协同模式3组网分别搭建多设备单因素单鉴别方式协同、多设备单因素多鉴别方式协同、多设备多因素协同测试环境，在设备2通过日志/命令行/测试应用等测试工具读取协同鉴别方案选择策略，查看是否正确匹配相应的场景。

b） 预期结果：

1） 在步骤1之后，若协同鉴别系统结合了资源池的可用资源，并根据协同鉴别方案选择策略来选定协同鉴别方案和协同身份鉴别的工作模式，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1上读取的协同鉴别方案选择策略匹配当前测试场景的协同鉴别方案和协同身份鉴别工作模式，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2上读取的协同鉴别方案选择策略匹配当前测试场景的协同鉴别方案和协同身份鉴别工作模式，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2上读取的协同鉴别方案选择策略匹配当前测试场景的协同鉴别方案和协同身份鉴别工作模式，然后执行步骤5；否则为“不符合要求”，测评结束；

5） 在步骤5之后，若设备2上读取的协同鉴别方案选择策略匹配当前测试场景的协同鉴别方案和协同身份鉴别工作模式，测评结果为“未见异常”；否则为“不符合要求”，测评结束。

5.3.1.2 测试项 b)：测评协同鉴别系统根据选定的协同鉴别方案和工作模式对资源池中身份鉴别子系统的采集和鉴别能力进行调度

测试要求 T/TAF 127—2022-6.3-鉴别系统要求-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。本要求的测试方法如下：

a） 测试步骤：

1） 步骤1：检查厂商提交的文档，查看协同鉴别方案评估设计文档，在对资源池身份鉴别子系统的采集和鉴别能力进行调度时，是否按照选定的协同鉴别方案和工作模式进行的调度；

2） 步骤2：按照单设备协同组网搭建测试环境，执行协同身份鉴别业务，在设备1上通过日志/命令行/测试应用等测试工具查看调度的身份鉴别子系统采集和鉴别模块是否和选定的协同鉴别方案和工作模式要求的采集和鉴别模块一致；

3） 步骤3：按照多设备协同模式1组网搭建测试环境，执行协同身份鉴别业务，在设备2、设备3上通过日志/命令行/测试应用等测试工具查看调度的身份鉴别子系统采集和鉴别模块是否和选定的协同鉴别方案和工作模式要求的采集和鉴别模块一致；

4） 步骤4：按照多设备协同模式2组网搭建测试环境，执行协同身份鉴别业务，在设备2、设备3上通过日志/命令行/测试应用等测试工具查看调度的身份鉴别子系统采集和鉴别模块是否和选定的协同鉴别方案和工作模式要求的采集和鉴别模块一致；

5） 步骤5：按照多设备协同模式3组网搭建测试环境，执行协同身份鉴别业务，在设备2、设备3上通过日志/命令行/测试应用等测试工具查看调度的身份鉴别子系统采集和鉴别模块是否和选定的协同鉴别方案和工作模式要求的采集和鉴别模块一致。

b） 预期结果：

1） 在步骤1之后，若协同鉴别系统在对资源池身份鉴别子系统的采集和鉴别能力进行调度时，是否按照选定的协同鉴别方案和工作模式进行调度，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，若实际调度的身份鉴别子系统采集模块和鉴别模块和选定的协同鉴别方案和工作模式的要求一致，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，若实际调度的身份鉴别子系统采集模块和鉴别模块和选定的协同鉴别方案和工作模式的要求一致，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，若实际调度的身份鉴别子系统采集模块和鉴别模块和选定的协同鉴别方案和工作模式的要求一致，然后执行步骤5，否则为“不符合要求”，测评结束；
5） 在步骤5之后，若实际调度的身份鉴别子系统采集模块和鉴别模块和选定的协同鉴别方案和工作模式的要求一致，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

5.3.1.3 测试项 c)：测评协同鉴别方案选择的策略支持动态配置

测试要求 T/TAF 127—2022-6.3-鉴别系统要求-c)：协同鉴别方案选择的策略宜支持动态配置。本要求的测试方法如下：

a） 测试步骤：
1） 步骤1： 检查厂商提交的文档，查看协同鉴别方案评估设计文档，协同鉴别方案选择的策略是否支持动态配置。
2） 步骤2：按照单设备协同组网搭建测试环境，根据设计方案中的动态配置方法，修改协同鉴别方案选择策略，执行协同身份鉴别业务，在设备1上通过日志/命令行/测试应用等测试工具查看实际使用的协同鉴别方案选择策略和修改后的策略是否一致；
3） 步骤3：按照多设备协同模式1组网搭建测试环境，根据设计方案中的动态配置方法，修改协同鉴别方案选择策略，执行协同身份鉴别业务，在设备2、设备3上通过日志/命令行/测试应用等测试工具查看实际使用的协同鉴别方案选择策略和修改后的策略是否一致；
4） 步骤4：按照多设备协同模式2组网搭建测试环境，根据设计方案中的动态配置方法，修改协同鉴别方案选择策略，执行协同身份鉴别业务，在设备2、设备3上通过日志/命令行/测试应用等测试工具查看实际使用的协同鉴别方案选择策略和修改后的策略是否一致；
5） 步骤5：按照多设备协同模式3组网搭建测试环境，根据设计方案中的动态配置方法，修改协同鉴别方案选择策略，执行协同身份鉴别业务，在设备2、设备3上通过日志/命令行/测试应用等测试工具查看实际使用的协同鉴别方案选择策略和修改后的策略是否一致。

b） 预期结果：
1） 在步骤1之后，若协同鉴别方案的策略支持动态配置，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，若实际使用的协同鉴别方案策略和修改后的策略一致，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，若实际使用的协同鉴别方案策略和修改后的策略一致，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，若实际使用的协同鉴别方案策略和修改后的策略一致，然后执行步骤5；否则为“不符合要求”，测评结束；
5） 在步骤5之后，若实际使用的协同鉴别方案策略和修改后的策略一致，测评结果为“未见异常”；否则为“不符合要求”，测评结束。

注：此项为建议项，不强制要求满足。

5.3.1.4 测试项 d)：测评配置到协同鉴别系统的策略具备完整性保护机制

测试要求 T/TAF 127—2022-6.3-鉴别系统要求-d)：配置到协同鉴别系统的策略应具备完整性保护机制。本要求的测试方法如下：

a） 测试步骤：

1） 步骤1：检查厂商提交的文档，查看协同鉴别方案评估设计文档，协同鉴别系统的策略是否具有完整性保护；

2） 步骤2：按照单设备协同组网搭建测试环境，在设备1上使用命令行/测试应用等测试工具对策略进行篡改，执行协同身份鉴别业务，检查是否能执行成功；

3） 步骤3：按照多设备协同模式1组网搭建测试环境，在设备2上使用命令行/测试应用等测试工具对策略进行篡改，执行协同身份鉴别业务，检查是否能执行成功；

4） 步骤4：按照多设备协同模式2组网搭建测试环境，在设备2上使用命令行/测试应用等测试工具对策略进行篡改，执行协同身份鉴别业务，检查是否能执行成功；

5） 步骤5：按照多设备协同模式3组网搭建测试环境，在设备2上使用命令行/测试应用等测试工具对策略进行篡改，执行协同身份鉴别业务，检查是否能执行成功。

b） 预期结果：

1） 在步骤1之后，若协同鉴别系统的策略有进行完整性保护，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，若协同鉴别系统的策略篡改后协同身份鉴别业务执行失败，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，若协同鉴别系统的策略篡改后协同身份鉴别业务执行失败，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，若协同鉴别系统的策略篡改后协同身份鉴别业务执行失败，然后执行步骤5；否则为“不符合要求”，测评结束；

5） 在步骤5之后，若协同鉴别系统的策略篡改后协同身份鉴别业务执行失败，测评结果为“未见异常”；否则为“不符合要求”，测评结束。

5.3.1.5 测试项 e)：测评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

测试要求 T/TAF 127—2022-6.3-鉴别系统要求-e)：5.3.3 中的模式 2 下，应保证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。本要求的测试方法如下：

a） 测试步骤：

1） 步骤1：检查厂商提交的文档，查看入口设备执行的协同鉴别方案设计文档和属主设备独立执行该鉴别方式的设计文档，对比二者的安全性和强度（如：身份鉴别子系统的执行环境，FAR/FRR/SAR等），是否确保入口设备执行的协同鉴别方式整体的安全性和强度不低于属主设备独立执行该鉴别方式时的安全性和强度。

b） 预期结果：

1） 在步骤1之后，若能确保入口设备执行的鉴别方式整体的安全性和强度不低于属主设备独立执行该鉴别方式时的安全性和强度；测评结果为“未见异常”，否则为“不符合要求”，测评结束。

5.3.2 鉴别能力调度要求

5.3.2.1 测试项 a)：测评身份鉴别子系统采集的数据在发出时携带身份鉴别子系统提供的认证凭证

测试要求 T/TAF 127—2022-6.3-鉴别能力调度要求-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）。本要求的测试方法如下：

a） 测试步骤：

1） 步骤1：检查厂商提交的文档，查看协同鉴别能力调度的设计文档，在发送身份鉴别子系统采集的数据时，是否有携带身份鉴别子系统提供的认证凭证；

2） 步骤2：按照单设备协同组网搭建测试环境，执行协同身份鉴别功能，在设备1上通过日志/命令行/测试应用等测试工具查看身份鉴别子系统采集的数据在发出时是否携带了身份鉴别子系统提供的认证凭证；

3） 步骤3：按照多设备协同模式1组网搭建测试环境，执行协同身份鉴别功能，在设备2上通过日志/命令行/测试应用等测试工具查看身份鉴别子系统采集的数据在发出时是否携带了身份鉴别子系统提供的认证凭证；

4） 步骤4：按照多设备协同模式2组网搭建测试环境，执行协同身份鉴别功能，在设备2上通过日志/命令行/测试应用等测试工具查看身份鉴别子系统采集的数据在发出时是否携带了身份鉴别子系统提供的认证凭证；

5） 步骤5：按照多设备协同模式3组网搭建测试环境，执行协同身份鉴别功能，在设备3上通过日志/命令行/测试应用等测试工具查看身份鉴别子系统采集的数据在发出时是否携带了身份鉴别子系统提供的认证凭证。

b） 预期结果：

1） 在步骤1之后，若身份鉴别子系统采集的数据在发送时，有携带身份鉴别子系统的认证凭证，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，若设备1上身份鉴别子系统采集的数据在发送时，有携带身份鉴别子系统提供的认证凭证，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2上身份鉴别子系统采集的数据在发送时，有携带身份鉴别子系统提供的认证凭证，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2上身份鉴别子系统采集的数据在发送时，有携带身份鉴别子系统提供的认证凭证，然后执行步骤5；否则为“不符合要求”，测评结束；

5） 在步骤5之后，若设备3上身份鉴别子系统采集的数据在发送时，有携带身份鉴别子系统提供的认证凭证，测评结果为“未见异常”；否则为“不符合要求”，测评结束。

5.3.2.2 测试项 b)：测评协同鉴别系统接收到某个鉴别子系统采集的数据使用认证凭证验证数据来源的合法性

测试要求 T/TAF 127—2022-6.3-鉴别能力调度要求-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。本要求的测试方法如下：

a） 测试步骤：

1） 步骤1：检查厂商提交的文档，查看协同鉴别能力调度的设计文档，在接收到身份鉴别子系统采集的数据时，是否验证数据来自于资源池内的合法鉴别子系统；

2） 步骤2：按照单设备协同组网搭建测试环境，在设备1上使用命令行/测试应用等测试工具篡改身份鉴别子系统采集的数据，同时在设备1上通过日志/命令行/测试应用等测试工具查看协同鉴别系统使用认证凭证对采集数据来源的验证结果是否为来自非法鉴别子系统；

3） 步骤3：按照多设备协同模式1组网搭建测试环境，在设备2上使用命令行/测试应用等测试工具篡改身份鉴别子系统采集的数据，同时在设备2上通过日志/命令行/测试应用等测试工具查看协同鉴别系统使用认证凭证对采集数据来源的验证结果是否为来自非法鉴别子系统；

4） 步骤4：按照多设备协同模式2组网搭建测试环境，在设备2上使用命令行/测试应用等测试工具篡改身份鉴别子系统采集的数据，同时在设备2上通过日志/命令行/测试应用等测试工具查看协同鉴别系统使用认证凭证对采集数据来源的验证结果是否为来自非法鉴别子系统；

5） 步骤5：按照多设备协同模式3组网搭建测试环境，在设备3上使用命令行/测试应用等测试工具篡改身份鉴别子系统采集的数据，同时在设备3上通过日志/命令行/测试应用等测试工具查看协同鉴别系统使用认证凭证对采集数据来源的验证结果是否为来自非法鉴别子系统。

b） 预期结果：

1） 在步骤1之后，若接收到身份鉴别子系统采集的数据时，协同鉴别系统有使用认证凭证验证数据是否来自于资源池内的合法鉴别子系统，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，若采集数据被篡改时，设备1上协同鉴别系统使用认证凭证对采集数据来源的验证结果为来自非法鉴别子系统，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，若采集数据被篡改时，设备2协同鉴别系统使用认证凭证对采集数据来源的验证结果为来自非法鉴别子系统，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，若采集数据被篡改时，设备2协同鉴别系统使用认证凭证对采集数据来源的验证结果为来自非法鉴别子系统，然后执行步骤5；否则为“不符合要求”，测评结束；

5） 在步骤5之后，若采集数据被篡改时，设备3协同鉴别系统对采集数据来源的验证结果为来自非法鉴别子系统，测评结果为“未见异常”；否则为“不符合要求”，测评结束。

5.3.2.3 测试项 c)：测评鉴别子系统的鉴别结果在发出时携带身份鉴别子系统提供的认证凭证

测试要求 T/TAF 127—2022-6.3-鉴别能力调度要求-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）。本要求的测试方法如下：

a） 测试步骤：

1） 步骤1：检查厂商提交的文档，查看协同鉴别能力调度的设计文档，在发送身份鉴别子系统的鉴别结果时，是否有携带身份鉴别子系统提供的认证凭证；

2） 步骤2：按照单设备协同组网搭建测试环境，执行协同身份鉴别功能，在设备1上通过日志/命令行/测试应用等测试工具查看鉴别子系统的鉴别结果在发出时是否携带了身份鉴别子系统提供的认证凭证；

3） 步骤3：按照多设备协同模式1组网搭建测试环境，执行协同身份鉴别功能，在设备3上通过日志/命令行/测试应用等测试工具查看鉴别子系统的鉴别结果在发出时是否携带了身份鉴别子系统提供的认证凭证；

4） 步骤4：按照多设备协同模式2组网搭建测试环境，执行协同身份鉴别功能，在设备2上通过日志/命令行/测试应用等测试工具查看鉴别子系统的鉴别结果在发出时是否携带了身份鉴别子系统提供的认证凭证；

5） 步骤5：按照多设备协同模式3组网搭建测试环境，执行协同身份鉴别功能，在设备3上通过日志/命令行/测试应用等测试工具查看鉴别子系统的鉴别结果在发出时是否携带了身份鉴别子系统提供的认证凭证。

b） 预期结果：

1） 在步骤1之后，若身份鉴别子系统的鉴别结果在发送时，有携带身份鉴别子系统的认证凭证，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，若设备1上鉴别子系统的鉴别结果在发送时，有携带身份鉴别子系统提供的认证凭证，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3上鉴别子系统的鉴别结果在发送时，有携带身份鉴别子系统提供的认证凭证，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2上鉴别子系统的鉴别结果在发送时，有携带身份鉴别子系统提供的认证凭证，然后执行步骤5；否则为“不符合要求”，测评结束；

5） 在步骤5之后，若设备3上鉴别子系统的鉴别结果在发送时，有携带身份鉴别子系统提供的认证凭证，测评结果为“未见异常”；否则为“不符合要求”，测评结束。

5.3.2.4 测试项 d)：测评协同鉴别系统接收到某个鉴别子系统发送的鉴别结果使用认证凭证验证数据来源合法性

测试要求 T/TAF 127—2022-6.3-鉴别能力调度要求-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。本要求的测试方法如下：

a） 测试步骤：

1） 步骤1：检查厂商提交的文档，查看协同鉴别能力调度的设计文档，在接收到身份鉴别子系统的鉴别结果时，是否使用认证凭证验证数据来源是否来自资源池内的合法鉴别子系统；

2） 步骤2：按照单设备协同组网搭建测试环境，在设备1上使用命令行/测试应用等测试工具篡改身份鉴别子系统发送的鉴别结果，同时在设备1上通过日志/命令行/测试应用等测试工具查看协同鉴别系统使用认证凭证对鉴别结果来源的验证结果是否为来自非法鉴别子系统；

3） 步骤3：按照多设备协同模式1组网搭建测试环境，在设备3上使用命令行/测试应用等测试工具篡改身份鉴别子系统发送的鉴别结果，同时在设备3上通过日志/命令行/测试应用等测试工具查看协同鉴别系统使用认证凭证对鉴别结果来源的验证结果是否为来自非法鉴别子系统；

4） 步骤4：按照多设备协同模式2组网搭建测试环境，在设备2上使用命令行/测试应用等测试工具篡改身份鉴别子系统发送的鉴别结果，同时在设备2上通过日志/命令行/测试应用等测试工具查看协同鉴别系统使用认证凭证对鉴别结果来源的验证结果是否为来自非法鉴别子系统；

5） 步骤5：按照多设备协同模式3组网搭建测试环境，在设备3上使用命令行/测试应用等测试工具篡改身份鉴别子系统发送的鉴别结果，同时在设备3上通过日志/命令行/测试应用等测试工具查看协同鉴别系统使用认证凭证对鉴别结果来源的验证结果是否为来自非法鉴别子系统。

b） 预期结果：

1） 在步骤1之后，若接收到身份鉴别子系统的鉴别结果时，有使用认证凭证验证鉴别结果是否来自于资源池内的合法鉴别子系统，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，若鉴别结果被篡改时，设备1上协同鉴别系统使用认证凭证对鉴别结果来源的验证结果为来自非法鉴别子系统，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，若鉴别结果被篡改时，设备3上协同鉴别系统使用认证凭证对鉴别结果来源的验证结果为来自非法鉴别子系统，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，若鉴别结果被篡改时，设备2上协同鉴别系统使用认证凭证对鉴别结果来源的验证结果为来自非法鉴别子系统，然后执行步骤5；否则为“不符合要求”，测评结束；
5） 在步骤5之后，若鉴别结果被篡改时，设备3上协同鉴别系统使用认证凭证对鉴别结果来源的验证结果为来自非法鉴别子系统，测评结果为“未见异常”；否则为“不符合要求”，测评结束。

5.3.2.5 测试项 e)：测评多设备间传输鉴别数据的保留和用途

测试要求 T/TAF 127—2022-6.3-鉴别能力调度要求-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。本要求的测试方法如下：

a） 测试步骤：
1） 步骤1：检查厂商提交的文档，查看协同鉴别能力调度的设计文档，是否确保多设备间传输的鉴别数据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；
2） 步骤2：按照多设备协同模式1组网搭建测试环境，在设备3上通过日志/命令行/测试应用等测试工具检查鉴别数据（采集的身份鉴别信息和鉴别结果）仅用于进行用户身份鉴别，在提示用户并获得用户同意后才保留或用于其它用途；
3） 步骤3：按照多设备协同模式1组网搭建测试环境，在设备3上通过日志/命令行/测试应用等测试工具检查鉴别数据（采集的身份鉴别信息和鉴别结果）仅用于进行用户身份鉴别，在用户拒绝的情况下不保留或用于其它用途；
4） 步骤4：按照多设备协同模式2组网搭建测试环境，在设备3通过日志/命令行/测试应用等测试工具检查鉴别数据（鉴别结果）仅用于进行用户身份鉴别，在提示用户并获得用户同意后才保留或用于其它用途；
5） 步骤5：按照多设备协同模式2组网搭建测试环境，在设备3通过日志/命令行/测试应用等测试工具检查鉴别数据（鉴别结果）仅用于进行用户身份鉴别，在用户拒绝的情况下不保留或用于其它用途；
6） 步骤6：按照多设备协同模式3组网搭建测试环境，在设备2通过日志/命令行/测试应用等测试工具检查鉴别数据（鉴别结果）仅用于进行用户身份鉴别，在提示用户并获得用户同意后才保留或用于其它用途；
7） 步骤7：按照多设备协同模式3组网搭建测试环境，在设备2通过日志/命令行/测试应用等测试工具检查鉴别数据（鉴别结果）仅用于进行用户身份鉴别，在用户拒绝的情况下不保留或用于其它用途。

b） 预期结果：
1） 在步骤1之后，若能确保多设备间传输的鉴别数据仅用于进行用户身份鉴别，除非明确告知同意外，不会保留或用于其它用途，然后执行步骤2；否则测评结果为“不符合要求”，测评结束；
2） 在步骤2之后，若设备间传输的鉴别数据（采集的身份鉴别信息和鉴别结果）在用户同意后，才做保留或用于其它用途，然后执行步骤3；否则测评结果为“不符合要求”，测评结束；
3） 在步骤3之后，若设备间传输的鉴别数据（采集的身份鉴别信息和鉴别结果）在用户不同意时，仅用于进行用户身份鉴别，不会保留或用于其它用途，然后执行步骤4；否则测评结果为“不符合要求”，测评结束；

4） 在步骤4之后，若设备间传输的鉴别数据（鉴别结果）在用户同意后，才做保留或用于其它用途，然后执行步骤5；否则测评结果为“不符合要求”，测评结束；
5） 在步骤5之后，若设备间传输的鉴别数据（鉴别结果）在用户不同意时，仅用于进行用户身份鉴别，不会保留或用于其它用途，然后执行步骤6；否则测评结果为“不符合要求”，测评结束；
6） 在步骤6之后，若设备间传输的鉴别数据（鉴别结果）在用户同意后，才做保留或用于其它用途，然后执行步骤7；否则测评结果为“不符合要求”，测评结束；
7） 在步骤7之后，若设备间传输的鉴别数据（鉴别结果）在用户不同意时，仅用于进行用户身份鉴别，不会保留或用于其它用途，测评结果为“未见异常”；否则测评结果为“不符合要求”，测评结束。

5.3.3 结果评估要求

5.3.3.1 测试项 a)：测评结果评估模块根据协同鉴别评估策略对鉴别结果综合评估

测试要求 T/TAF 127—2022-6.3-结果评估要求-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。本要求的测试方法如下：

a） 测试步骤：
1） 步骤1：检查厂商提交的文档，查看协同鉴别系统结果评估设计文档，是否结合协同鉴别评估策略，对鉴别子系统给出的鉴别结果进行综合评估；
2） 步骤2：按照单设备协同组网搭建测试环境，执行协同身份鉴别功能，在设备1上通过日志/命令行/测试应用等测试工具查看鉴别结果评估是否结合协同鉴别评估策略对一个或多个鉴别子系统的鉴别结果进行的综合评估；
3） 步骤3：按照多设备协同模式1组网搭建测试环境，执行协同身份鉴别功能，在设备3上通过日志/命令行/测试应用等测试工具查看鉴别结果评估是否结合协同鉴别评估策略对一个或多个鉴别子系统的鉴别结果进行的综合评估；
4） 步骤4：按照多设备协同模式2组网搭建测试环境，执行协同身份鉴别功能，在设备2上通过日志/命令行/测试应用等测试工具查看鉴别结果评估是否结合协同鉴别评估策略对一个或多个鉴别子系统的鉴别结果进行的综合评估；
5） 步骤5：按照多设备协同模式3组网搭建测试环境，执行协同身份鉴别功能，在设备3上通过日志/命令行/测试应用等测试工具查看鉴别结果评估是否结合协同鉴别评估策略对一个或多个鉴别子系统的鉴别结果进行的综合评估。

b） 预期结果：
1） 在步骤1之后，若协同鉴别系统结果评估有根据协同鉴别评估策略对鉴别子系统给出的鉴别结果进行综合评估，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，若鉴别结果评估结合了协同鉴别评估策略对一个或多个鉴别子系统的鉴别结果进行的综合评估，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，若鉴别结果评估结合了协同鉴别评估策略对一个或多个鉴别子系统的鉴别结果进行的综合评估，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，若鉴别结果评估结合了协同鉴别评估策略对一个或多个鉴别子系统的鉴别结果进行的综合评估，然后执行步骤5，否则为“不符合要求”，测评结束；
5） 在步骤5之后，若鉴别结果评估结合了协同鉴别评估策略对一个或多个鉴别子系统的鉴别结果进行的综合评估，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

5.3.3.2 测试项 b)：测评结果评估模块可向业务应用返回认证结果

测试要求 T/TAF 127—2022-6.3-结果评估要求-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。本要求的测试方法如下：

a） 测试步骤：

1） 步骤1：检查厂商提交的文档，查看协同鉴别系统结果评估的设计文档，协同鉴别系统是否可向业务应用返回对应的认证结果，由业务应用使用应用保存的评估策略执行判断；

2） 步骤2：按照单设备协同组网搭建测试环境，执行协同身份鉴别功能，在设备1上通过日志/命令行/测试应用等测试工具查看协同鉴别系统是否向业务应用返回对应的认证结果；

3） 步骤3：按照多设备协同模式1组网搭建测试环境，执行协同身份鉴别功能，在设备3上通过日志/命令行/测试应用等测试工具查看协同鉴别系统是否向业务应用返回对应的认证结果；

4） 步骤4：按照多设备协同模式2组网搭建测试环境，执行协同身份鉴别功能，在设备2上通过日志/命令行/测试应用等测试工具查看协同鉴别系统是否向业务应用返回对应的认证结果；

5） 步骤5：按照多设备协同模式3组网搭建测试环境，执行协同身份鉴别功能，在设备3上通过日志/命令行/测试应用等测试工具查看协同鉴别系统是否向业务应用返回对应的认证结果。

b） 预期结果：

1） 在步骤1之后，若协同鉴别系统可以向业务返回对应的认证结果，由业务应用使用自己保存的评估策略执行 ，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，若协同鉴别系统有向业务应用返回对应的认证结果，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，若协同鉴别系统有向业务应用返回对应的认证结果，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，若协同鉴别系统有向业务应用返回对应的认证结果，然后执行步骤5，否则为“不符合要求”，测评结束；

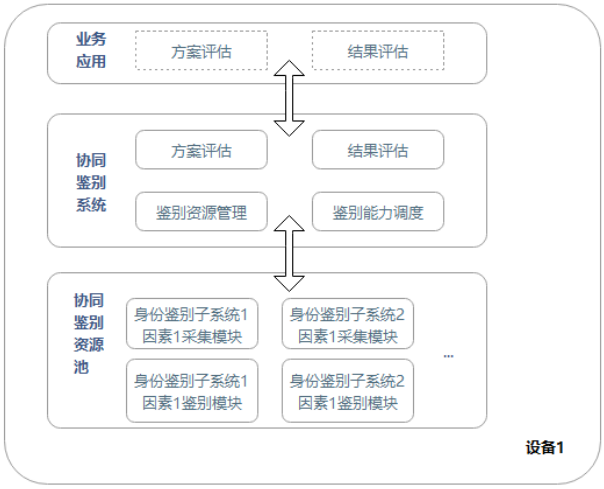
5） 在步骤5之后，若协同鉴别系统有向业务应用返回对应的认证结果，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

注：此项为建议项，不强制要求满足。

附 录 A
（规范性）
协同身份鉴别方式组网

A.1 单因素单设备协同组网

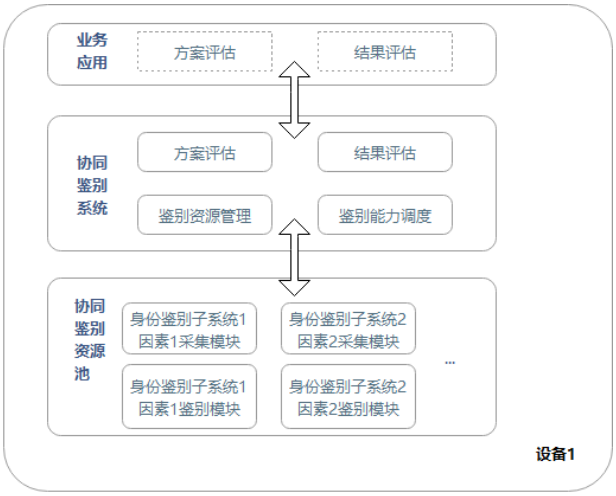
此场景是单因素下不同鉴别方式的协同鉴别，如下图A.1所示，身份鉴别子系统1和身份鉴别子系统2应该属于相同身份鉴别因素1，但是对用户身份的鉴别结合了两个鉴别子系统的结果来综合评判。



图A.1 单因素单设备协同组网

A.2 多因素单设备协同组网

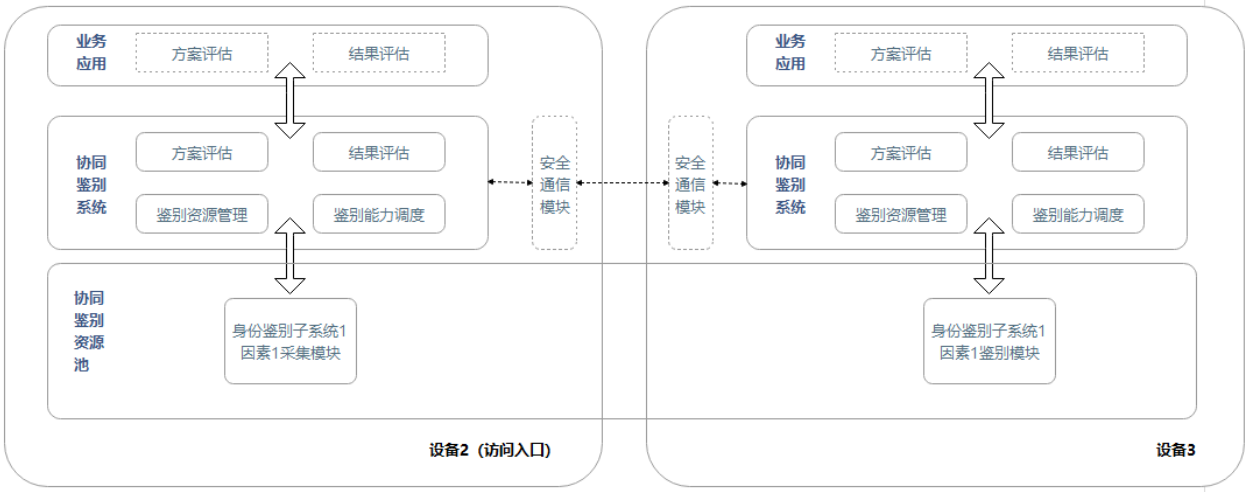
此场景是多因素下不同鉴别方式的在单设备上协同鉴别，可以为业务提供更高可信度的用户身份鉴别能力和风险控制因素。如下图 A.2 所示，通过在一台设备上选择多种鉴别方法进行多因素鉴别，来满足高安业务的身份验证需求或是达到单模态需要更高软硬件成本才能达到的可信度。



图A.2 多因素单设备协同组网

A.3 单因素多设备单鉴别方式协同模式 1 组网

此场景是单因素下单鉴别方式在多设备上基于模式 1 进行的协同鉴别，设备 2 为访问入口设备，设备 3 为数据属主设备。如下图 A.3 所示，设备 2 与设备 3 已建立互信关系，设备 2 有协同认证业务需求（如访问数据或认证用户）时，发起协同认证并进行协同身份鉴别因素 1 的采集，设备 3 对设备 2 采集的协同身份鉴别因素 1 进行认证，并根据协同认证结果对特定业务操作进行授权。



图A.3　单因素多设备单鉴别方式协同模式1组网

A.4 单因素多设备多鉴别方式协同模式 1 组网

此场景是单因素下多鉴别方式在多设备上基于模式 1 进行的协同鉴别，设备 2 为访问入口设备，设备 3 为数据属主设备。如下图 A.4 所示，设备 2 与设备 3 已建立互信关系，设备 2 有协同认证业务需求（如访问数据或认证用户）时，发起协同认证并进行协同身份鉴别子系统 1 和协同身份鉴别子系统 2 的因素 1 采集，设备 3 对设备 2 采集的协同身份鉴别因素 1 进行认证，并根据协同认证结果对特定业务操作进行授权。

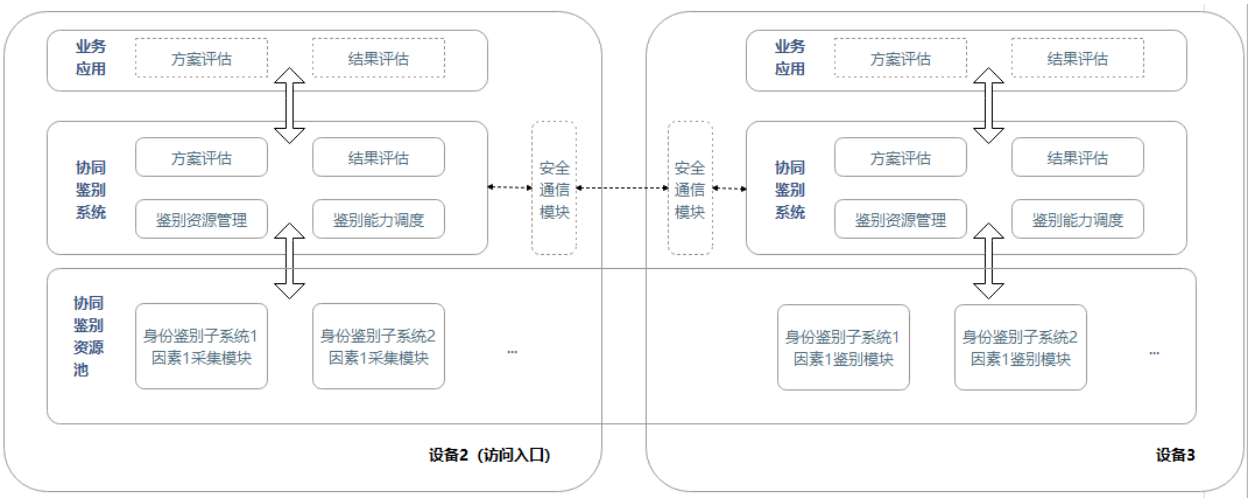


图 A.4　单因素多设备多鉴别方式协同模式 1 组网

A.5 多因素多设备协同模式 1 组网

此场景是多因素下多鉴别方式在多设备上基于模式 1 进行的协同鉴别，设备 2 为访问入口设备，设备 3 为数据属主设备。如下图 A.5 所示，设备 2 与设备 3 已建立互信关系，设备 2 有协同认证业务需求（如访问数据或认证用户）时，发起协同认证并进行协同身份鉴别子系统 1 因素 1 和协同身份鉴别子系统 2 的因素 2 采集，设备 3 对设备 2 采集的协同身份鉴别因素 1 和因素 2 进行认证，并根据协同认证结果对特定业务操作进行授权。

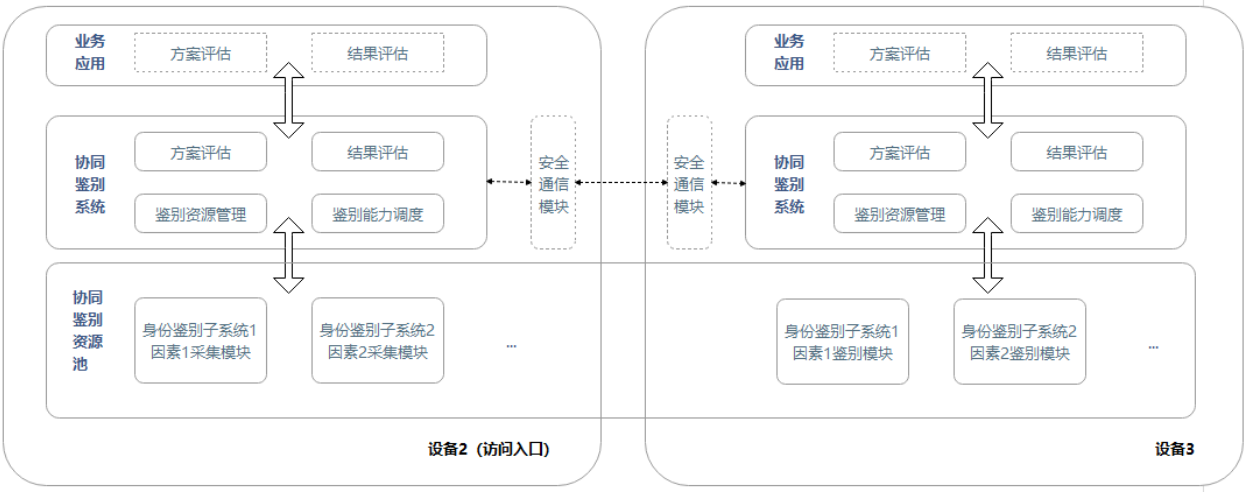


图 A.5　多因素多设备协同模式 1 组网

A.6 单因素多设备单鉴别方式协同模式 2 组网

此场景是单因素下单鉴别方式在多设备上基于模式 2 进行的协同鉴别，设备 2 为访问入口设备，设备 3 为数据属主设备。如下图 A.6 所示，设备 2 与设备 3 已建立互信关系，设备 2 有协同认证业务需求（如访问数据或认证用户）时，发起协同认证并进行协同身份鉴别因素 1 的采集和认证，设备 3 接收协同认证结果并根据结果对特定业务操作进行授权。

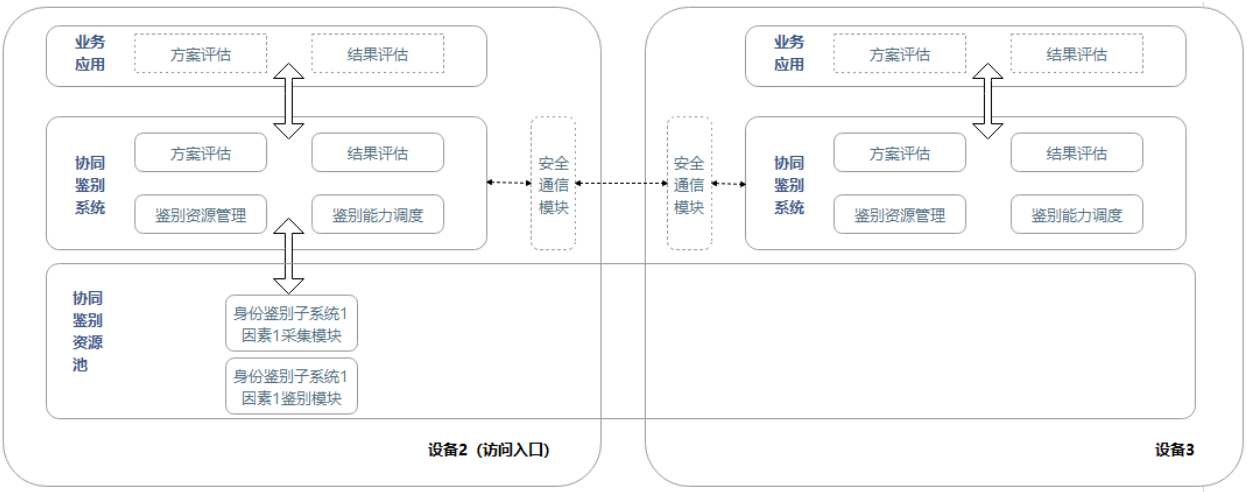


图 A.6　单因素多设备单鉴别方式协同模式 2 组网

A.7 单因素多设备多鉴别方式协同模式 2 组网

此场景是单因素下多鉴别方式在多设备上基于模式 2 进行的协同鉴别，设备 2 为访问入口设备，设备 3 为数据属主设备。如下图 A.7 所示，设备 2 与设备 3 已建立互信关系，设备 2 有协同认证业务需求（如访问数据或认证用户）时，发起协同认证并进行协同身份鉴别子系统 1 和协同身份鉴别子系统 2 的因素 1 采集和认证，设备 3 接收协同认证结果并根据认证结果对特定业务操作进行授权。

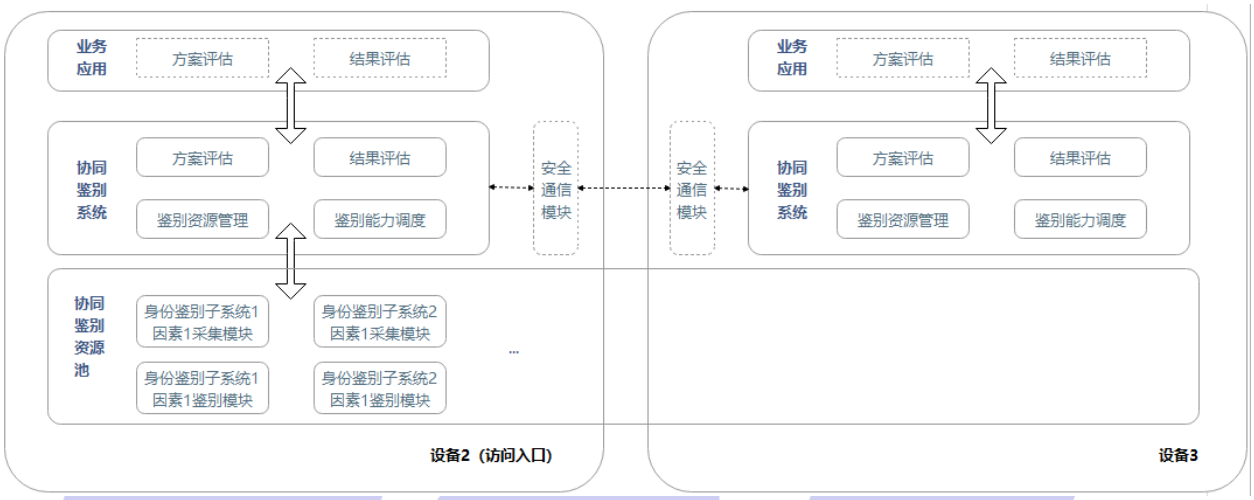


图 A.7　单因素多设备多鉴别方式协同模式 2 组网

A.8 多因素多设备协同模式 2 组网

此场景是多因素下多鉴别方式在多设备上基于模式 2 进行的协同鉴别，设备 2 为访问入口设备，设备 3 为数据属主设备。如下图 A.8 所示，设备 2 与设备 3 已建立互信关系，设备 2 有协同认证业务需求（如访问数据或认证用户）时，发起协同认证并进行协同身份鉴别子系统 1 因素 1 和协同身份鉴别子系统 2 的因素 2 采集和认证，设备 3 接收协同认证结果并根据认证结果对特定业务操作进行授权。

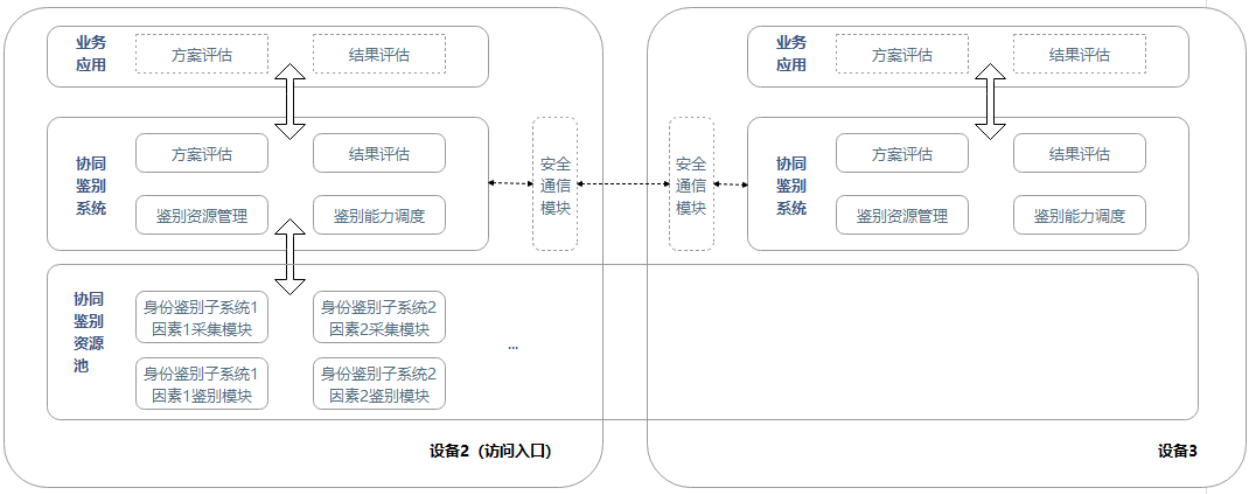


图 A.8　多因素多设备协同模式 2 组网

A.9 单因素多设备单鉴别方式协同模式 3 组网

此场景是单因素下单鉴别方式在多设备上基于模式 3 进行的协同鉴别，设备 2 为访问入口设备但无

采集和认证能力，设备 3 为数据属主设备。如下图 A.9 所示，设备 2 与设备 3 已建立互信关系，设备 2 有协同认证业务需求（如访问数据或认证用户）时，发起协同认证请求设备 3 进行协同身份鉴别子系统 1 因素 1 的采集和认证，设备 3 根据协同认证结果对特定业务操作进行授权。

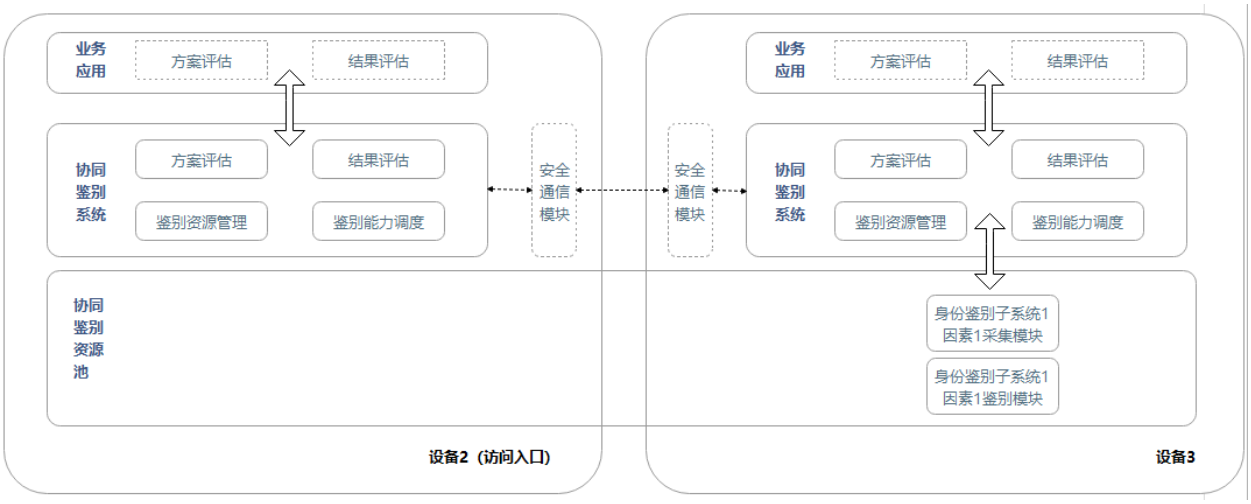


图 A.9　单因素多设备单鉴别方式协同模式 3 组网

A.10 单因素多设备多鉴别方式协同模式 3 组网

此场景是单因素下多鉴别方式在多设备上基于模式 3 进行的协同鉴别，设备 2 为访问入口设备但无采集和认证能力，设备 3 为数据属主设备。如下图 A.10 所示，设备 2 与设备 3 已建立互信关系，设备 2 有协同认证业务需求（如访问数据或认证用户）时，发起协同认证请求设备 3 进行协同身份鉴别子系统 1 和协同身份鉴别子系统 2 的因素 1 的采集和认证，设备 3 根据协同认证结果对特定业务操作进行授权。

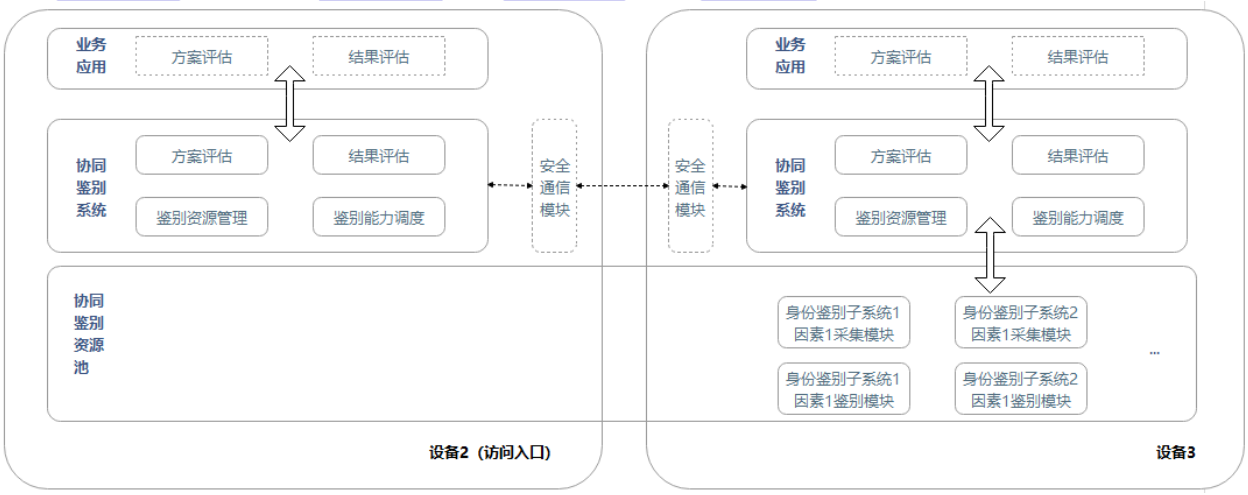


图 A.10　单因素多设备多鉴别方式协同模式 3 组网

A.11 多因素多设备协同模式 3 组网

此场景是多因素下多设备上基于模式 3 进行的协同鉴别，设备 2 为访问入口设备但无采集和认证能力，设备 3 为数据属主设备。如下图 A.11 所示，设备 2 与设备 3 已建立互信关系，设备 2 有协同认证

业务需求（如访问数据或认证用户）时，发起协同认证请求设备 3 进行协同身份鉴别子系统 1 因素 1 和协同身份鉴别子系统 2 的因素 2 的采集和认证，设备 3 根据协同认证结果对特定业务操作进行授权。

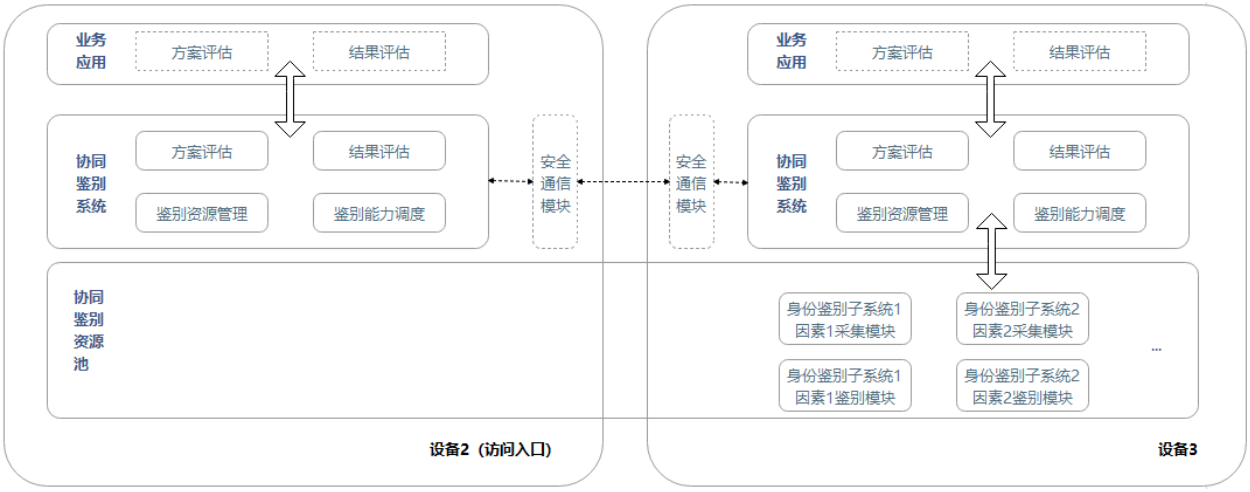


图 A.11　多因素多设备协同模式 3 组网

附 录 B
（规范性）
智能终端协同身份鉴别安全测试项

B.1 智能终端协同身份鉴别安全测试项

T/TAF 127—2022 将协同身份鉴别安全要求分为总体安全要求、资源池管理安全要求、协同鉴别系统安全要求，不同的安全技术要求适用的协同身份鉴别场景不同，如 T/TAF 127—2022，6.1.a 只适用于多设备场景（含多设备协同模式 1，多设备协同模式 2 和多设备协同模式 3）。为了清晰展示安全技术要求适用的测试场景，整理出技术要求和测试场景的映射关系（见表 B.1）。

表 B.1 智能终端协同身份鉴别安全测试项

<table>
<tr><th>安全技术要求</th><th>编号</th><th>单设备协同（含场景 1.1、1.2）</th><th>多设备协同模式 1（含场景 2.1、2.2、2.3）</th><th>多设备协同模式 2（含场景 3.1、3.2、3.3）</th><th>多设备协同模式 3（含场景 4.1、4.2、4.3）</th></tr>
<tr><td rowspan="8">总体安全要求测试</td><td>6.1.a</td><td colspan="4">5.1.1 测试项 a)：测评设备间协同鉴别资源池建立前已建立设备间互信关系</td></tr>
<tr><td>6.1.b</td><td colspan="4">5.1.2 测试项 b)：测评本地身份鉴别子系统加入资源池前已完成凭据录入并正式启用</td></tr>
<tr><td>6.1.c</td><td colspan="4">5.1.3 测试项 c)：测评生物特征参考的采集、存储、使用、销毁等遵从现行规定</td></tr>
<tr><td>6.1.d</td><td>无</td><td>5.1.4 测试项 d)：测评生物特征样本基于安全通道在建立资源池的设备间传输</td><td>无</td><td>无</td></tr>
<tr><td>6.1.e</td><td colspan="4">5.1.5 测试项 e)：测评协同身份鉴别技术不应用于身份凭证凭据录入/修改/删除场景</td></tr>
<tr><td>6.1.f</td><td colspan="4">5.1.6 测试项 f)：测评协同鉴别功能开启应获得用户单独同意</td></tr>
<tr><td>6.1.g</td><td colspan="4">5.1.7 测试项 g)：测评用户不进行协同身份鉴别时，不禁止其他业务的正常使用</td></tr>
<tr><td rowspan="6">资源池管理安全要求测试</td><td>6.2.a</td><td colspan="4">5.2.1 测试项 a)：测评终端设备对不同身份鉴别子系统的鉴别能力强度进行区分</td></tr>
<tr><td>6.2.b</td><td colspan="4">5.2.2 测试项 b)：测评终端设备对不同身份鉴别子系统在采集、比对、存储等环境的软硬件环境的安全性进行区分</td></tr>
<tr><td>6.2.c</td><td colspan="4">5.2.3 测试项 c)：测评加入资源池的身份鉴别子系统具备身份标识</td></tr>
<tr><td>6.2.d</td><td>无</td><td colspan="3">5.2.4 测试项 d)：测评加入资源池的身份鉴别子系统具备资源池设备间的认证凭证</td></tr>
<tr><td>6.2.e</td><td colspan="4">5.2.5 测试项 e)：测评身份鉴别子系统身份标识和可用状态具备安全同步机制</td></tr>
<tr><td>6.2.f</td><td colspan="4">5.2.6 测试项 f)：测评身份鉴别子系统的可用状态发生变化时，及时从资源池中移除该子系统</td></tr>
<tr><td>6.2.g</td><td>无</td><td colspan="3">5.2.7 测试项 g)：测评设备间的互信关系发生变化时，及时对资源池的相关信息进行同步</td></tr>
<tr><td rowspan="2">协调鉴别系统安全要求测试</td><td>6.3-鉴别系统要求-a</td><td colspan="4">5.3.1.1 测试项 a)：测评协同鉴别系统结合资源池中的可用资源根据协同鉴别方案选择策略选定协同鉴别方案和协同身份鉴别的工作模式</td></tr>
<tr><td>6.3-鉴别系统要求-b</td><td colspan="4">5.3.1.2 测试项 b)：测评协同鉴别系统根据选定的协同鉴别方案和工作模式对资源池中身份鉴别子系统的采集和鉴别能力进行调度</td></tr>
</table>

表 B.1　智能终端协同身份鉴别安全测试项（续）

安全技术要求	编号	单设备协同（含场景 1.1、1.2）	多设备协同模式 1（含场景 2.1、2.2、2.3）	多设备协同模式 2（含场景 3.1、3.2、3.3）	多设备协同模式 3（含场景 4.1、4.2、4.3）
	6.3-鉴别系统要求-c	5.3.1.3　测试项 c)：测评协同鉴别方案选择的策略支持动态配置			
	6.3-鉴别系统要求-d	5.3.1.4　测试项 d)：测评配置到协同鉴别系统的策略具备完整性保护机制			
协调鉴别系统安全要求测试	6.3-鉴别系统要求-e	无	无	5.3.1.5　测试项 e)：测评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	无
	6.3-鉴别能力调度要求-a	5.3.2.1　测试项 a)：测评身份鉴别子系统采集的数据在发出时携带身份鉴别子系统提供的认证凭证			
	6.3-鉴别能力调度要求-b	5.3.2.2　测试项 b)：测评协同鉴别系统接收到某个鉴别子系统采集的数据使用认证凭证验证数据来源的合法性			
	6.3-鉴别能力调度要求-c	5.3.2.3　测试项 c)：测评鉴别子系统的鉴别结果在发出时携带身份鉴别子系统提供的认证凭证			
	6.3-鉴别能力调度要求-d	5.3.2.4　测试项 d)：测评协同鉴别系统接收到某个鉴别子系统发送的鉴别结果使用认证凭证验证数据来源合法性			
	6.3-鉴别能力调度要求-e	无	5.3.2.5　测试项 e)：测评多设备间传输鉴别数据的保留和用途		
	6.3-结果评估要求-a	5.3.3.1　测试项 a)：测评结果评估模块根据协同鉴别评估策略对鉴别结果综合评估			
	6.3-结果评估要求-b	5.3.3.2　测试项 b)：测评结果评估模块可向业务应用返回认证结果			

参 考 文 献

[1] GB/T 37036（所有部分） 信息技术 移动设备生物特征识别
[2] GB/T 40660—2021 信息安全技术 生物特征识别信息保护基本要求
[3] 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
[4] T/TAF 097—2021 智能终端设备间互信操作技术要求

电信终端产业协会团体标准

智能终端协同身份鉴别安全测试方法

T/TAF 165—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