ICS 33.050
CCS M 30

团　体　标　准

T/TAF 126—2022

智能终端设备间互操作数据保护测试方法

Test methods for data protection of intelligent terminal interoperation

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。

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：胡重阳、马四英、衣强、李实、张悦、李战锋、杨佳霖、刘陶、杜云、王艳红、陈鑫爱、李京典、周飞、李可心、汪海、王浩仟、常琳、李杰强、宁华、刘献伦。

引　言

近年来，随着移动终端、智能家居的快速发展，每个用户可能拥有多个终端，如手机、手表、平板电脑等，加之扩展到家庭设备，如电视、路由器等，使得用户可操控的设备范围进一步扩大，覆盖家居、运动、办公、休闲、购物等多种场景。一方面，终端上的应用及服务日益丰富，另一方面为了给用户提供便利的体验，终端设备之间的交互也逐渐频繁，用户可以操控多个设备，也可以将一个终端设备上的操作无缝切换到另一个终端设备上，因此产生了大量数据在终端设备之间流转、使用的场景。

终端设备上的服务包含用户工作、生活多个方面，因此设备间交互涉及的数据种类也较多，从大的方面划分，包含个人信息、非个人信息，而个人信息的敏感程度又不尽相同，因此，在终端设备间对数据进行操作时，应保证数据在设备中互操作前、过程中、以及之后得到相应敏感等级的保护。T/TAF 100-2021基于设备间数据操作场景，根据数据的敏感程度、终端能力等给出可实施的数据保护技术要求，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 100-2021配套的测试方法，针对技术要求设计了科学的测试方法，用于测评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操作数据保护的落地实施，切实地保证用户设备间的数据安全。

智能终端设备间互操作数据保护测试方法

1 范围

本文件规定了设备间互操作过程中数据生成、存储、使用、传输和删除阶段数据保护的测试方法。

本文件适用于面向消费者的智能终端设备及移动设备应用程序在设备间进行数据相关操作时实现数据的安全存储、使用、删除等目标，也适用于评估机构基于本文件开展智能设备间数据安全的评估工作。

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。

T/TAF 097-2021 智能设备间互信操作技术要求

T/TAF 100-2021 智能终端设备间互操作数据保护技术要求

3 术语和定义

3.1

智能终端设备 intelligent terminal

包括CPU、RAM、非易失性存储器、内存控制器、中断控制器、时钟电路、I/O电路、各种通信接口及相关软件（操作系统、应用软件）、通信协议栈等在内的通信设备。

3.2

互操作 inter-operation

基于智能终端设备之间建立的连接，在智能终端设备间进行数据、实现业务功能的指令处理的过程。

注：本文件适用于智能终端设备间的数据处理操作。

3.3

加密密钥 encryption key

在智能终端设备间互操作场景下，用来对数据进行加密的符号序列。

3.4

根密钥 root key

在设备制造阶段写入的用于派生或保护加密密钥的符号序列。

4 智能终端设备间互操作数据保护测试分析

T/TAF 100-2021将智能终端上的数据分为4个风险等级（见表1），并定义了智能终端设备互操作数据生命周期中生成、存储、使用、传输、删除各阶段（见图1）终端及应用或服务处理不同风险等级数据需要满足的数据保护技术要求。

表1　智能终端设备数据风险等级分级原则

数据风险等级	分级原则	判定原则
4	业界法律法规中定义的特殊数据类型，涉及个人的最私密领域的信息或者一旦泄露、篡改、破坏、销毁可能会给个人或组织造成重大的不利影响的数据	对个人财产、声誉、生活状态以及生理和心理等方面产生重大的、不可消除的影响；或 对组织造成全部业务无法开展、重大经济损失，或对组织的全部用户产生负面影响，或对组织声誉构成特别严重影响。
3	数据的泄露、篡改、破坏、销毁可能会给个人或组织导致严峻的不利影响	对个人财产、声誉、生活状态以及生理和心理等方面可能产生重大影响、克服难度高、消除影响代价大。 对组织造成部分业务无法开展、严重经济损失，或对大部分组织用户产生负面影响，或对组织声誉造成严重影响。
2	数据的泄露、篡改、破坏、销毁可能会给个人或组织导致严重的不利影响	对个人财产、声誉、生活状态以及生理和心理等方面可能产生重大影响、克服有一定难度。 对组织造成个别业务无法开展、一定程度的经济损失，或对小部分组织用户产生负面影响，或对组织声誉构成一定威胁、造成一定影响。
1	数据的泄露、篡改、破坏、销毁可能会给个人或组织导致无不利影响、或导致有限的不利影响	对个人可能造成一定困扰、但可以克服，或不会造成困扰。 对组织造成轻微经济损失、不影响业务稳定或对组织没有影响。

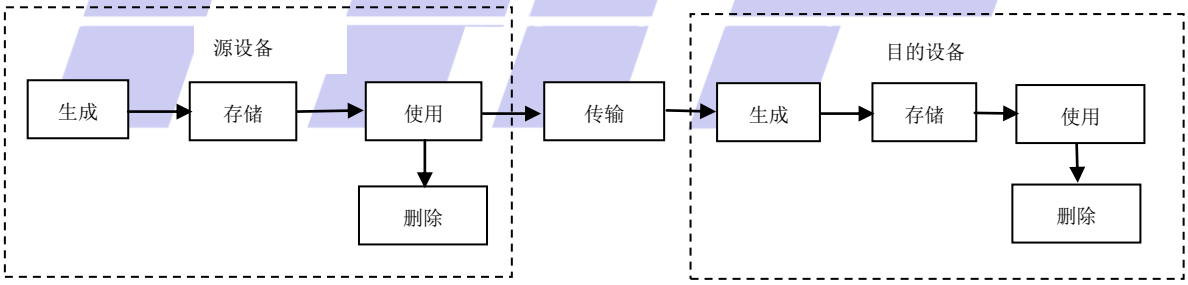

图1　设备间互操作数据生命周期

智能终端设备互操作数据生命周期分成如下五个阶段：

a） 生成：智能终端和其上的应用软件通过采集、直接生成、从其它终端接收或其它方式转入等方式产生数据的过程；

b） 存储：数据在智能终端设备上存留的过程；

c） 使用：数据在智能终端设备上被访问、处理等操作的过程；

d） 传输：数据离开源智设备、转移到目的设备的过程；

e） 删除：数据在智能终端设备上被销毁，保证其不可被检索、访问、恢复的状态。

同时，除了传输阶段的一般性要求，针对传输阶段基于近距离连接（见图2）和基于远端连接两种数据互操作方式（见图3），也制定了相关数据保护技术要求。

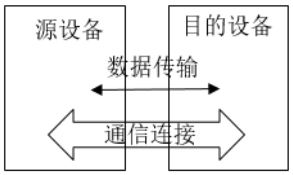

图2　终端设备间基于近距离连接进行数据互操作

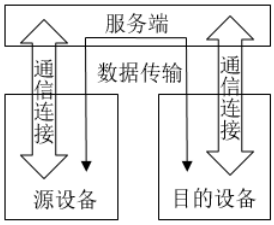

图3　终端设备之间基于远端连接进行数据互操作

综上，本文件中测试方法以数据生命周期、测试对象、数据风险等级三个维度组织测试项（见表2），在测试项中描述要测评的T/TAF 100-2021规则，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；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　智能终端设备互操作数据保护测试项

<table>
<tr><td rowspan="2">数据生命周期</td><td rowspan="2">测试对象</td><td colspan="4">数据风险等级</td></tr>
<tr><td>4级</td><td>3级</td><td>2级</td><td>1级</td></tr>
<tr><td>生成阶段</td><td>应用或服务</td><td colspan="4">5.1.1　测试项a）：测评生成数据的应用或服务确认数据风险等级</td></tr>
<tr><td rowspan="9">存储阶段</td><td rowspan="3">终端</td><td colspan="4">5.2.1　测试项a）：测评不同智能终端设备间的根密钥的唯一性</td></tr>
<tr><td colspan="4">5.2.2　测试项b）：测评智能终端根密钥存储和运行的安全性</td></tr>
<tr><td colspan="2">5.2.3　测试项c）：测评终端支持标记数据风险等级能力（3级及以上风险等级数据）</td><td colspan="2">无</td></tr>
<tr><td rowspan="6">应用或服务</td><td colspan="4">5.2.4　测试项d）：测评生成数据的应用或服务应标记数据的风险等级</td></tr>
<tr><td colspan="4">5.2.5　测试项e）：测评确保终端安全等级支持待存储数据的最高风险等级</td></tr>
<tr><td colspan="2">5.2.6　测试项f）：测评生成数据的应用或服务按照文件级进行数据的加密存储（3级及以上风险等级数据）</td><td colspan="2">5.2.7　测试项g）：测评数据加密存储（2级及以下风险等级数据）</td></tr>
<tr><td colspan="3">5.2.8　测试项h）：测评加密密钥存储和运行在硬件隔离的安全环境（3级及以上风险等级数据）</td><td>无</td></tr>
<tr><td colspan="4">5.2.9　测试项i）：测评加密密钥使用根密钥进行保护且根密钥唯一</td></tr>
</table>

表2　智能终端设备互操作数据保护测试项（续）

<table>
<tr><th rowspan="2">数据生命周期</th><th rowspan="2">测试对象</th><th colspan="4">数据风险等级</th></tr>
<tr><th>4级</th><th>3级</th><th>2级</th><th>1级</th></tr>
<tr><td rowspan="2">使用阶段</td><td>终端</td><td colspan="3">5.3.1　测试项a）：测评数据在智能终端设备被访问时被系统的自主访问控制机制保护（2级及以上风险等级数据）</td><td>无</td></tr>
<tr><td>应用或服务</td><td>5.3.2　测试项b）：测评数据被本地应用或服务访问时，具备数据访问权限的用户才能访问数据（4级风险等级数据）</td><td>5.3.3　测试项c）：测评数据被本地应用或服务访问时，具备数据访问权限的用户才能访问数据，或访问该数据的用户曾被系统验证过且对访问的应用标识进行验证（3级风险等级数据）</td><td>5.3.4　测试项d）：测评数据被本地应用或服务访问时，访问该数据的用户曾被系统验证过（2级风险等级数据）</td><td>无</td></tr>
<tr><td>传输阶段（一般要求）</td><td>应用或服务</td><td colspan="3">5.4.1.1　测试项a）：测评安全通道传输数据的机密性以及完整性（2级及以上风险等级数据）</td><td>5.4.1.2　测试项b）：测评安全通道传输数据的完整性（1级风险等级数据）</td></tr>
<tr><td rowspan="8">传输阶段（基于近距离连接）</td><td>终端</td><td colspan="3">5.4.2.1　测试项c）：测评数据传输前源设备确保目的设备的合法性并与目的设备建立互信关系（2级及以上风险等级数据）</td><td>无</td></tr>
<tr><td rowspan="7">应用或服务</td><td colspan="4">5.4.2.2　测试项d）：测评源设备向目的设备发送数据并在目的设备存储时的安全等级检查</td></tr>
<tr><td colspan="4">5.4.2.3　测试项e）：测评目的设备从源设备向自身传输并存储数据时的安全等级检查</td></tr>
<tr><td colspan="4">5.4.2.4　测试项f）：测评终端之间数据自动传输及存储的安全要求</td></tr>
<tr><td colspan="4">5.4.2.5　测试项g）：测评源设备上的应用或服务传输数据同时将数据风险等级传输到目的设备</td></tr>
<tr><td colspan="4">5.4.2.6　测试项h）：测评生物特征模板数据不在设备间传输</td></tr>
<tr><td colspan="3">5.4.2.7　测试项i）：测评数据被其他设备的应用或服务访问时对访问数据的用户身份进行验证（2级及以上风险等级数据）</td><td rowspan="2">5.4.2.9　测试项k）：数据被其他设备的应用或服务访问时可不进行身份验证（1级风险等级数据）</td></tr>
<tr><td colspan="3">5.4.2.8　测试项j）：同账号下多设备间数据访问已完成对访问用户的身份认证可不进行身份验证（2级及以上风险等级数据）</td></tr>
<tr><td>传输阶段（基于远端连接）</td><td>应用或服务</td><td>5.4.3.1　测试项l）：测评数据在源设备上加密，在目的设备上解密，且远端服务器不可解密（4级风险等级数据）</td><td>5.4.3.2　测试项m）：测评数据通过加密通道传输及加密存储在服务器（3级风险等级数据）</td><td colspan="2">无</td></tr>
<tr><td>删除阶段</td><td>应用或服务</td><td colspan="2">5.5.1　测试项a）：测评应用或服务应确保数据在智能终端设备上彻底删除（3级及以上风险等级数据）</td><td colspan="2">无</td></tr>
</table>

5　智能终端设备间互操作数据保护测试方法

5.1 生成阶段

5.1.1 测试项 a）：测评生成数据的应用或服务确认数据风险等级

测试项T/TAF 100-2021-9.1.1-a）：数据在终端设备上生成后，生成数据的应用或服务应确认其风险等级。

a） 测试步骤：

1） 步骤1：检查厂商提交的文档，查看应用或服务在智能终端设备上生成数据的设计文档，是否确认了所生成数据的风险等级；

2） 步骤2：在智能终端设备上遍历被测应用或服务生成的数据，通过日志/命令行等测试工具查看对应的标签，检查是否符合此数据类型对应的风险等级（可参考T/TAF 100-2021附录A）。

b） 预期结果：

1） 在步骤1之后，若应用或服务在智能终端设备上生成数据后确认了所生成数据的风险等级，测评结果为“未见异常”，执行步骤2；否则为“不符合要求”，测评结束；

2） 在步骤2之后，若应用或服务在智能终端设备标记的数据符合对应的风险等级，测评结果为“未见异常”；否则为“不符合要求”，测评结束。

5.2 存储阶段

5.2.1 测试项 a）：测评不同智能终端设备间的根密钥的唯一性

测试项T/TAF 100-2021-9.1.2-a）：移动终端应确保不同终端设备间的根密钥的唯一性。

a） 测试步骤：

1） 步骤1：检查厂商提交的文档，查看智能终端根密钥的设计文档，是否确保不同智能终端设备间的根密钥唯一。

b） 预期结果：

1） 在步骤1之后，若可以确保不同智能终端设备间的根密钥唯一，测评结果为“未见异常”；否则为“不符合要求”，测评结束。

5.2.2 测试项 b）：测评智能终端根密钥存储和运行的安全性

测试项T/TAF 100-2021-9.1.2-b）：移动终端需确保根密钥存储和运行的安全性，根密钥需存储和运行在硬件隔离的安全环境，终端不支持硬件隔离的安全环境，可通过其它主流的密钥保护技术实现，如软件、或软硬件结合的方式，根密钥的访问需具备访问控制机制，如仅密钥管理模块可访问根密钥。

a） 测试步骤：

1） 步骤1：检查厂商提交的文档，查看智能终端根密钥的设计文档，是否确保根密钥存储和运行的安全性，包括：1）根密钥存储和运行在硬件隔离的安全环境，或其他主流的密钥保护技术（如TEE，软token等），2）根密钥的访问具备访问控制机制；

2） 步骤2：使用具有根密钥访问权限的测试应用或服务访问根密钥，检查是否可以访问；

3） 步骤3：使用不具有根密钥访问权限的测试应用或服务访问根密钥，检查是否无法访问。

b） 预期结果：

1） 在步骤1之后，若智能终端可以确保根密钥存储和运行的安全性，执行步骤2；否则为“不符合要求”，测评结束；

2） 在步骤2之后，若具有根密钥访问权限的测试应用或服务访问根密钥成功，执行步骤3；否则为“不符合要求”，测评结束；

3） 在步骤3之后，若不具有根密钥访问权限的测试应用或服务访问根密钥失败，测评结果为“未见异常”；否则为“不符合要求”，测评结束。

5.2.3 测试项 c）：测评终端支持标记数据风险等级能力（3 级及以上风险等级数据）

测试项T/TAF 100-2021-9.1.2-c）：涉及处理3级及以上风险等级数据的终端应支持标记数据风险等级能力。

a） 测试步骤：

1） 步骤1：检查厂商提交的文档，查看智能终端系统的设计文档，是否支持标记数据风险等级能力；

2） 步骤2：使用测试应用或服务通过终端支持的标记数据风险等级能力分别标记1-4级风险等级的数据，检查是否可以标记。

b） 预期结果：

1） 在步骤1之后，若智能终端设备支持标记数据风险等级能力，执行步骤2；否则为“不符合要求”，测评结束；

2） 在步骤2之后，若测试应用或服务可以通过终端支持的标记数据风险等级能力正确标记1-4风险等级的数据，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）：测评生成数据的应用或服务应标记数据的风险等级

测试项T/TAF 100-2021-9.1.2-d）：生成数据的应用或服务应标记数据的风险等级，标记的方式依据数据的存储方式，且采取就高不就低原则，如数据以文件方式存储，则以文件粒度按照文件中包含的数据最高风险等级进行标记。

数据存储在TEE或芯片级安全存储器件的情况除外。

a） 测试步骤：

1） 步骤1：检查厂商提交的文档，查看应用或服务在智能终端设备上存储数据的设计文档，是否依据数据的存储方式标记了所生成数据的风险等级，且采取就高不就低原则；

2） 步骤2：在智能终端设备上遍历被测应用或服务生成的数据，通过日志/命令行等测试工具查看对应的标签，检查是否符合此数据类型对应的风险等级（可参考T/TAF 100-2021附录A）。

b） 预期结果：

1） 在步骤1之后，若应用或服务在智能终端设备上存储数据时标记了数据的风险等级，且采取就高不就低原则，执行步骤2；否则为“不符合要求”，测评结束；

2） 在步骤2之后，若应用或服务在智能终端设备标记的数据符合对应的风险等级，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）：测评确保终端安全等级支持待存储数据的最高风险等级

测试项T/TAF 100-2021-9.1.2-e）：生成数据的应用或服务应确保终端安全等级支持待存储数据的最高风险等级，若终端安全等级不支持待存储数据的最高风险等级，生成数据的应用或服务应在用户确认前提下存储。

终端安全等级与可支撑的数据风险等级可参考T/TAF 100-2021附录B。

a） 测试步骤：

1） 步骤1：检查厂商提交的文档，查看应用或服务在智能终端设备上存储数据的设计文档，是否判断智能终端设备的安全等级支持待存储数据的最高风险等级；

2） 步骤2：使用被测应用或服务在安全等级支持待存储数据的最高风险等级的智能终端设备上存储数据，检查是否可以直接存储；

3） 步骤3：使用被测应用或服务在安全等级不支持待存储数据的最高风险等级的智能终端设备上存储数据，检查是否在提示用户并获取用户同意的情况下可以存储；
4） 步骤4：使用被测应用或服务在安全等级不支持待存储数据的最高风险等级的智能终端设备上存储数据，检查是否在用户拒绝的情况下无法存储。

b） 预期结果：
1） 在步骤1之后，若应用或服务判断了智能终端设备的安全等级是否支持待存储数据的最高风险等级，执行步骤2；否则为“不符合要求”，测评结束；
2） 在步骤2之后，若应用或服务可以直接存储，执行步骤3；否则为“不符合要求”，测评结束；
3） 在步骤3之后，若应用或服务在提示用户并获取用户同意的情况下可以存储数据，执行步骤4；否则为“不符合要求”，测评结束；
4） 在步骤4之后，若应用或服务在用户拒绝的情况下无法存储，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）：测评生成数据的应用或服务按照文件级进行数据的加密存储（3 级及以上风险等级数据）

测试项T/TAF 100-2021-9.1.2-f）：生成数据的应用或服务应按照文件级进行数据的加密存储。

a） 测试步骤：
1） 步骤1：检查厂商提交的文档，查看应用或服务在智能终端设备上存储数据的设计文档，3级及以上风险等级数据是否按照文件级进行数据的加密存储；
2） 步骤2：通过日志/命令行等测试工具查看智能终端设备中被测应用或服务3级及以上风险等级数据，检查是否按照文件级加密存储为密文。

b） 预期结果：
1）在步骤1之后，若应用或服务对3级及以上风险等级数据按照文件级进行了数据的加密存储，执行步骤2；否则为“不符合要求”，测评结束；
2） 在步骤2之后，若应用或服务对3级及以上风险等级数据按照文件级加密存储为密文，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）：测评数据加密存储（2 级及以下风险等级数据）

测试项T/TAF 100-2021-9.1.2-i/l）：数据应加密存储。

a） 测试步骤：
1） 步骤1：检查厂商提交的文档，查看应用或服务在智能终端设备上存储数据的设计文档，2级及以下风险等级数据是否对数据加密存储；
2） 步骤2：通过日志/命令行等测试工具查看智能终端设备中被测应用或服务2级及以下风险等级数据，检查是否加密存储为密文。

b） 预期结果：
1） 在步骤1之后，若应用或服务对2级及以下风险等级数据进行了加密存储，执行步骤2；否则为“不符合要求”，测评结束；
2） 在步骤2之后，若应用或服务2对级及以下风险等级数据加密存储为密文，测评结果为“未见异常”；否则为“不符合要求”，测评结束。

5.2.8 测试项 h）：测评加密密钥存储和运行在硬件隔离的安全环境（3 级及以上风险等级数据）

测试项T/TAF 100-2021-9.1.2-g/j）：(文件)加密密钥需存储和运行在硬件隔离的安全环境。

终端不支持硬件隔离的安全环境，可在用户确认的前提下进行相应的安全运行和存储。

a） 测试步骤：

1） 步骤1：检查厂商提交的文档，查看应用或服务在智能终端设备上存储数据的设计文档，是否在终端支持硬件隔离的安全环境条件下将（文件）加密密钥存储和运行在硬件隔离的安全环境，或终端不支持硬件隔离的安全环境需用户确认才能进行安全运行和存储；

2） 步骤2：使用被测应用或服务在终端支持硬件隔离的安全环境条件下进行（文件）加密密钥的存储和运行，检查是否可以存储和运行成功；

3） 步骤3：使用被测应用或服务在终端不支持硬件隔离的安全环境条件下进行（文件）加密密钥的存储和运行，检查是否在提示用户并获取用户同意情况下存储和运行成功；

4） 步骤4：使用被测应用或服务在终端不支持硬件隔离的安全环境条件下进行（文件）加密密钥的存储和运行，检查是否在用户拒绝的情况下无法存储和运行。

b） 预期结果：

1） 在步骤1之后，若应用或服务在终端支持硬件隔离的安全环境条件下将（文件）加密密钥存储和运行在硬件隔离的安全环境，或在终端不支持硬件隔离的安全环境需用户确认才能进行安全运行和存储，执行步骤2；否则为“不符合要求”，测评结束；

2） 在步骤2之后，若应用或服务可以存储和运行成功，执行步骤3；否则为“不符合要求”，测评结束；

3） 在步骤3之后，若应用或服务在提示用户并获取用户同意情况下可以存储和运行，执行步骤4；否则为“不符合要求”，测评结束；

4） 在步骤4之后，若应用或服务在用户拒绝的情况下无法存储和运行，测评结果为“未见异常”；否则为“不符合要求”，测评结束。

5.2.9 测试项 i）：测评加密密钥使用根密钥进行保护且根密钥唯一

测试项T/TAF 100-2021-9.1.2-h/k/m）：(文件)加密密钥应使用根密钥进行保护，根密钥应确保不同终端设备间的唯一性。

a） 测试步骤：

1） 步骤1：检查厂商提交的文档，查看应用或服务在智能终端设备上存储数据的设计文档，是否使用根密钥对(文件)加密密钥进行保护，且不同智能终端设备间的根密钥唯一。

b） 预期结果：

1） 在步骤1之后，若应用或服务使用了根密钥对(文件)加密密钥进行保护，且不同智能终端设备间的根密钥唯一，测评结果为“未见异常”；否则为“不符合要求”，测评结束。

5.3 使用阶段

5.3.1 测试项 a）：测评数据在智能终端设备被访问时被系统的自主访问控制机制保护（2 级及以上风险等级数据）

测试项T/TAF 100-2021-9.1.3-a）：终端应支持自主访问控制机制，数据在终端设备被访问时应被终端系统的自主访问控制机制所保护。

a） 测试步骤：

1） 步骤1：检查厂商提交的文档，查看智能终端系统的设计文档，是否2级及以上风险等级数据在智能终端设备被访问时被系统的自主访问控制机制所保护；

2） 步骤2：使用智能终端系统自主访问控制列表中有权限的应用或服务访问2级及以上风险等级数据数据，检查是否可以访问；

3） 步骤3：使用智能终端系统自主访问控制列表中没有权限的应用或服务访问2级及以上风险等级数据数据，检查是否无法访问。

b） 预期结果：

1） 在步骤1之后，若2级及以上风险等级数据在智能终端设备被访问时被智能终端系统的自主访问控制机制所保护，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2级及以上风险等级数据可以被智能终端系统自主访问控制列表中有权限的应用或服务访问，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2级及以上风险等级数据无法被智能终端系统自主访问控制列表中没有权限的应用或服务访问，测评结果为“未见异常”；否则为“不符合要求”，测评结束。

5.3.2 测试项 b）：测评数据被本地应用或服务访问时，具备数据访问权限的用户才能访问数据（4级风险等级数据）

测试项T/TAF 100-2021-9.1.3-b）：数据被本地应用或服务访问时，生成数据的应用或服务应对访问用户身份进行验证，确保具备数据访问权限的用户才能访问数据。

a） 测试步骤：

1） 步骤1：检查厂商提交的文档，查看生成数据的应用或服务在智能终端设备上使用数据的设计文档，在4级风险等级数据被本地应用或服务访问时，是否对访问用户身份进行验证；

2） 步骤2：使用未进行身份验证的用户访问被测应用或服务的4级风险等级数据，检查是否无法访问；

3） 步骤3：使用进行过身份验证且具备数据访问权限的用户访问被测应用或服务的4级风险等级数据，检查是否可以访问；

4） 步骤4：使用进行过身份验证但不具备数据访问权限的用户访问被测应用或服务的4级风险等级数据，检查是否无法访问。

b） 预期结果：

1） 在步骤1之后，若生成数据的应用或服务的4级风险等级数据被本地应用或服务访问时，对访问用户身份进行了验证，执行步骤2；否则为“不符合要求”，测评结束；

2） 在步骤2之后，若未进行身份验证的用户无法访问被测应用或服务的4级风险等级数据，测评结果为“未见异常”，执行步骤3；否则为“不符合要求”，测评结束；

3） 在步骤3之后，若进行过身份验证且具备数据访问权限的用户可以访问被测应用或服务的4级风险等级数据，测评结果为“未见异常”，执行步骤4；否则为“不符合要求”，测评结束；

4） 在步骤4之后，若进行过身份验证但不具备数据访问权限的用户无法访问被测应用或服务的4级风险等级数据，测评结果为“未见异常”；否则为“不符合要求”，测评结束。

5.3.3 测试项 c）：测评数据被本地应用或服务访问时，具备数据访问权限的用户才能访问数据，或访问该数据的用户曾被系统验证过且对访问的应用标识进行验证（3 级风险等级数据）

测试项T/TAF 100-2021-9.1.3-c）：数据被本地应用或服务访问时，生成数据的应用或服务应对用户身份进行验证，确保具备数据访问权限的用户才能访问数据；或应确保访问数据用户曾被系统验证过（如终端开机后已验证用户身份），并对访问的应用标识进行验证，确保只有生成该数据的应用才能访问数据。

a） 测试步骤：

1） 步骤1：检查厂商提交的文档，查看生成数据的应用或服务在智能终端设备上使用数据的设计文档，在3级风险等级数据被本地应用或服务访问时，是否对访问用户身份进行验证；

2） 步骤2：使用未进行身份验证的用户访问被测应用或服务的3级风险等级数据，检查是否无法访问；
3） 步骤3：使用进行过身份验证且具备数据访问权限的用户访问被测应用或服务的3级风险等级数据，检查是否可以访问；
4） 步骤4：使用进行过身份验证但不具备数据访问权限的用户访问被测应用或服务的3级风险等级数据，检查是否无法访问；
5） 步骤5：检查厂商提交的文档，查看应用或服务在智能终端设备上使用数据的设计文档，数据被本地应用或服务访问时，是否确保访问3级风险等级数据用户曾被系统验证过，并对访问的应用标识进行验证；
6） 步骤6：访问数据用户曾被系统验证过的情况下，使用生成该数据的应用访问被测应用或服务的3级风险等级数据，检查是否可以访问；
7） 步骤7：访问数据用户曾被系统验证过的情况下，使用非生成该数据的应用访问被测应用或服务的3级风险等级数据，检查是否无法访问。

b） 预期结果：
1） 在步骤1之后，若生成数据的应用或服务的3级风险等级数据被本地应用或服务访问时，对访问用户身份进行了验证，执行步骤2；否则执行步骤5；
2） 在步骤2之后，若未进行身份验证的用户无法访问被测应用或服务的3级风险等级数据，执行步骤3；否则为“不符合要求”，测评结束；
3） 在步骤3之后，若进行过身份验证且具备数据访问权限的用户可以访问被测应用或服务的3级风险等级数据，执行步骤4；否则为“不符合要求”，测评结束；
4） 在步骤4之后，若进行过身份验证但不具备数据访问权限的用户无法访问被测应用或服务的3级风险等级数据，测评结果为“未见异常”；否则为“不符合要求”，测评结束；
5） 在步骤5之后，若确保了访问3级风险等级数据用户曾被系统验证过，并对访问的应用标识进行了验证，执行步骤6；否则为“不符合要求”，测评结束；
6） 在步骤6之后，若访问数据用户曾被系统验证过，生成该数据的应用可以访问被测应用或服务的3级风险等级数据，执行步骤7；否则为“不符合要求”，测评结束；
7） 在步骤7之后，若访问数据用户曾被系统验证过，非生成该数据的应用无法访问被测应用或服务的3级风险等级数据，测评结果为“未见异常”；否则为“不符合要求”，测评结束。

5.3.4 测试项 d）：测评数据被本地应用或服务访问时，访问该数据的用户曾被系统验证过（2 级风险等级数据）

测试项T/TAF 100-2021-9.1.3-d）：数据被本地应用或服务访问时，生成数据的应用或服务应确保访问该数据的用户曾被系统验证过，如终端开机后已验证用户身份。

a） 测试步骤：
1） 步骤1：检查厂商提交的文档，查看生成数据的应用或服务在智能终端设备上使用数据的设计文档，在2级风险等级数据被本地应用或服务访问时，是否确保访问数据用户曾被系统验证过；
2） 步骤2：访问数据用户曾被系统验证过的情况下，使用生成该数据的应用访问被测应用或服务的2级风险等级数据，检查是否可以访问；
3） 步骤3：访问数据用户未被系统验证过的情况下，使用生成该数据的应用访问被测应用或服务的2级风险等级数据，检查是否无法访问。

b） 预期结果：

1）在步骤1之后，若生成数据的应用或服务确保了访问2级风险等级数据用户曾被系统验证过，执行步骤2；否则为“不符合要求”，测评结束；
2） 在步骤2之后，若访问数据用户曾被系统验证过，生成该数据的应用可以访问被测应用或服务的2级风险等级数据，执行步骤3；否则为“不符合要求”，测评结束；
3） 在步骤3之后，若访问数据用户未被系统验证过，生成该数据的应用无法访问被测应用或服务的2级风险等级数据，测评结果为“未见异常”；否则为“不符合要求”，测评结束。

5.4 传输阶段

5.4.1 传输阶段一般要求

5.4.1.1 测试项 a）：测评安全通道传输数据的机密性以及完整性（2 级及以上风险等级数据）

测试项T/TAF 100-2021-9.1.4.1-a）：终端设备上的应用或服务应采用安全通道进行数据传输，保证传输数据的机密性以及完整性。

a） 测试步骤：
1） 步骤1：检查厂商提交的文档，查看应用或服务在智能终端设备上传输2级及以上风险等级数据的设计文档，是否使用安全通道进行数据传输，并保证传输数据的机密性以及完整性；
2） 步骤2：通过网络抓包工具拦截2级及以上风险等级传输数据并篡改，检查数据是否加密传输，篡改后是否导致传输失败。

b） 预期结果：
1） 在步骤1之后，若应用或服务使用了安全通道进行2级及以上风险等级数据传输，并保证传输数据的机密性以及完整性，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2级及以上风险等级传输数据为密文，篡改后导致传输失败，测评结果为“未见异常”；否则为“不符合要求”，测评结束。

5.4.1.2 测试项 b）：测评安全通道传输数据的完整性（1 级风险等级数据）

测试项T/TAF 100-2021-9.1.4.1-b）：终端设备上的应用或服务应采用安全通道进行数据传输，保证传输数据的完整性。

a） 测试步骤：
1） 步骤1：检查厂商提交的文档，查看应用或服务在智能终端设备上传输1级风险等级数据的设计文档，是否使用安全通道进行数据传输，并保证传输数据的完整性；
2） 步骤2：通过网络抓包工具拦截1级风险等级传输数据并篡改，检查数据篡改后是否导致传输失败。

b） 预期结果：
1） 在步骤1之后，若应用或服务使用了安全通道进行1级风险等级数据传输，并保证传输数据的完整性，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1级风险等级数据篡改后导致传输失败，测评结果为“未见异常”；否则为“不符合要求”，测评结束。

5.4.2 基于近距离连接的数据互操作方式其它要求

5.4.2.1 测试项 c）：测评数据传输前源设备确保目的设备的合法性并与目的设备建立互信关系（2 级及以上风险等级数据）

测试项T/TAF 100-2021-9.1.4.2-a）：在设备间传输风险等级为2级及以上级别数据，传输前源设备应确保目的设备的合法性，并与目的设备完成双向认证、建立互信关系。

注：终端设备间建立互信关系要求参考T/TAF 097-2021。

a） 测试步骤：

1） 步骤1：检查厂商提交的文档，查看智能终端基于近距离连接传输数据的设计文档，在设备间传输风险等级为2级及以上级别数据时，是否源设备在传输前确保目的设备的合法性，并与目的设备完成双向认证、建立互信关系。

b） 预期结果：

1） 在步骤1之后，若设备间传输风险等级为2级及以上级别数据时，源设备在传输前确保了目的设备的合法性，与目的设备完成双向认证、建立互信关系，测评结果为“未见异常”；否则为“不符合要求”，测评结束。

5.4.2.2 测试项 d）：测评源设备向目的设备发送数据并在目的设备存储时的安全等级检查

测试项T/TAF 100-2021-9.1.4.2-b）：源设备的应用或服务向目的设备发送数据、且数据在目的设备存储时，源设备的应用或服务应确保目的设备支持待传输数据的最高风险等级。

数据传输到目的设备后，在目的设备存储前，目的设备的应用或服务应确保源设备支持传输数据的最高风险等级。

若目的设备或源设备无法支持传输数据的最高风险等级，则需在对端设备用户确认的前提下进行传输或存储。

a） 测试步骤：

1） 步骤1：检查厂商提交的文档，查看应用或服务在智能终端设备上基于近距离连接传输数据的设计文档，源设备的应用或服务向目的设备发送数据、且数据在目的设备存储时，1）源设备的应用或服务是否判断目的设备的安全等级支持待存储数据的最高风险等级，2）目的设备的应用或服务是否判断源设备的安全等级支持待存储数据的最高风险等级；

2） 步骤2：在目的设备和源设备同时支持传输数据的最高风险等级的情况下传输数据或存储数据，检查是否可以直接传输或存储；

3） 步骤3：在目的设备或源设备无法支持传输数据的最高风险等级的情况下传输数据或存储数据（参考T/TAF 100-2021附录B），检查是否在对端设备提示用户并获取用户同意的情况下可以传输或存储；

4） 步骤4：在目的设备或源设备无法支持传输数据的最高风险等级的情况下传输数据或存储数据（参考T/TAF 100-2021附录B），检查是否用户在拒绝的情况下无法传输和存储。

b） 预期结果：

1） 在步骤1之后，若源设备的应用或服务和目的设备的应用或服务都判断了是否支持待存储数据的最高风险等级，执行步骤2；否则为“不符合要求”，测评结束；

2） 在步骤2之后，若目的设备和源设备同时支持传输数据的最高风险等级的情况下，应用或服务可以直接传输或存储，执行步骤3；否则为“不符合要求”，测评结束；

3） 在步骤3之后，若目的设备或源设备无法支持传输数据的最高风险等级的情况下，应用或服务在对端设备提示用户并获取用户同意的情况下可以传输或存储，执行步骤4；否则为“不符合要求”，测评结束；

4） 在步骤4之后，若目的设备或源设备无法支持传输数据的最高风险等级的情况下，应用或服务在用户拒绝的情况下无法传输和存储，测评结果为“未见异常”；否则为“不符合要求”，测评结束。

5.4.2.3 测试项 e）：测评目的设备从源设备向自身传输并存储数据时的安全等级检查

测试项T/TAF 100-2021-9.1.4.2-c）：目的设备的应用或服务从源设备向自身传输并存储数据时，源设备的应用或服务应确保目的设备支持待传输数据的最高风险等级。

a） 测试步骤：

1） 步骤1：检查厂商提交的文档，查看应用或服务在智能终端设备上基于近距离连接传输数据的设计文档，当目的设备的应用或服务从源设备向自身传输并存储数据时，源设备的应用或服务是否判断目的设备的安全等级支持待存储数据的最高风险等级；

2） 步骤2：使用安全等级支持待存储数据的最高风险等级的目的设备从源设备向自身传输并存储数据，检查是否可以直接传输并存储；

3） 步骤3：使用安全等级不支持待存储数据的最高风险等级的目的设备从源设备向自身传输并存储数据，检查是否无法传输并存储。

b） 预期结果：

1） 在步骤1之后，若源设备的应用或服务判断了目的设备的安全等级是否支持待存储数据的最高风险等级，执行步骤2；否则为“不符合要求”，测评结束；

2） 在步骤2之后，若安全等级支持待存储数据的最高风险等级的目的设备可以从源设备向自身直接传输并存储数据，执行步骤3；否则为“不符合要求”，测评结束；

3） 在步骤3之后，若安全等级不支持待存储数据的最高风险等级的目的设备无法从源设备向自身传输并存储数据，测评结果为“未见异常”；否则为“不符合要求”，测评结束。

5.4.2.4 测试项 f）：测评终端之间数据自动传输及存储的安全要求

测试项T/TAF 100-2021-9.1.4.2-d）：在支持账号登录的终端之间进行多个设备间自动传输、存储数据时，同账号下终端可进行自动传输，非同账号下终端之间，应用或服务应在用户确认的前提下进行数据自动传输。

注：多设备间数据自动传输应满足本节b）要求，自动传输数据场景下不需要每次传输均经过用户确认。

a） 测试步骤：

1） 步骤1：检查厂商提交的文档，查看应用或服务在智能终端设备上基于近距离连接传输数据的设计文档，在支持账号登录的终端之间进行多个设备间自动传输、存储数据时，1）同账号下终端是否可进行自动传输，2）非同账号下终端之间，是否在用户确认的前提下才能进行数据自动传输；

2） 步骤2：被测应用或服务在同账号登录的终端之间进行自动传输及存储数据，检查是否可以自动传输和存储；

3） 步骤3：被测应用或服务在非同账号登录的终端之间进行自动传输及存储数据，检查是否在提示用户并获取用户同意的情况下可以自动传输和存储；

4） 步骤4：被测应用或服务在非同账号登录的终端之间进行自动传输及存储数据，检查是否在用户拒绝的情况下无法自动传输和存储。

b） 预期结果：

1） 在步骤1之后，若同账号下终端可进行自动传输，非同账号下终端之间在用户确认的前提下才能进行数据自动传输，执行步骤2；否则为“不符合要求”，测评结束；

2） 在步骤2之后，在同账号登录的终端之间进行自动传输及存储数据，若可以自动传输和存储，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，在非同账号登录的终端之间进行自动传输及存储数据，若在提示用户并获取用户同意的情况下可以自动传输和存储，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，在非同账号登录的终端之间进行自动传输及存储数据，若在用户拒绝的情况下无法自动传输和存储，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。

5.4.2.5 测试项 g）：测评源设备上的应用或服务传输数据同时将数据风险等级传输到目的设备

测试项T/TAF 100-2021-9.1.4.2-e）：数据从源设备传输到目的设备的过程中，源设备上的应用或服务应确保数据风险等级传输到目的设备。

a） 测试步骤：

1） 步骤1：检查厂商提交的文档，查看应用或服务基于近距离连接传输数据的设计文档，在数据从源数据传输到目的设备的过程中，是否将数据风险等级传输到目的设备；

2） 步骤2：使用被测应用或服务从源设备传输数据到目的设备，检查目的设备是否可以同时接收到数据的风险等级，且与源设备相同。

b） 预期结果：

1） 在步骤1之后，若应用或服务在数据从源数据传输到目的设备的过程中将数据风险等级传输到目的设备，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，若目的设备是否可以同时接收到数据的风险等级且与源设备相同，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。

5.4.2.6 测试项 h）：测评生物特征模板数据不在设备间传输

测试项T/TAF 100-2021-9.1.4.2-f）：生物特征模板数据，如指纹模板，不宜在设备间传输。

a） 测试步骤：

1） 步骤1：检查厂商提交的文档，查看应用或服务基于近距离连接传输数据的设计文档，是否在设备间传输生物特征模板数据（如指纹模板）。

b） 预期结果：

1） 在步骤1之后，若应用或服务没有在设备间传输生物特征模板数据，测评结果为“满足要求”；否则测评结果为“未满足要求”。

注：此项为建议项，不强制要求满足。

5.4.2.7 测试项 i）：测评数据被其他设备的应用或服务访问时对访问数据的用户身份进行验证（2级及以上风险等级数据）

测试项T/TAF 100-2021-9.1.4.2-g）：风险等级为2级及以上级别的数据被其它设备的应用或服务访问时，应对访问数据的用户身份进行验证，确保拥有该数据、或具有访问权限的用户才能访问数据。

a） 测试步骤：

1） 步骤1：检查厂商提交的文档，查看应用或服务在智能终端设备上使用数据的设计文档，在风险等级为2级及以上级别的数据被其它设备的应用或服务访问时，是否对访问用户身份进行验证；

2） 步骤2：使用未进行身份验证的用户通过其它设备的应用或服务访问被测应用或服务风险等级为2级及以上级别的数据，检查是否无法访问；

3） 步骤3：使用进行过身份验证且具备数据访问权限的用户通过其它设备的应用或服务访问被测应用或服务风险等级为2级及以上级别的数据，检查是否可以访问；

4） 步骤4：使用进行过身份验证但不具备数据访问权限的用户通过其它设备的应用或服务访问被测应用或服务风险等级为2级及以上级别的数据，检查是否无法访问。

b） 预期结果：

1） 在步骤1之后，若应用或服务风险等级为2级及以上级别的数据被其它设备的应用或服务访问时，对访问数据的用户身份进行了验证，执行步骤2；否则为“不符合要求”，测评结束；
2） 在步骤2之后，若未进行身份验证的用户无法通过其它设备的应用或服务访问被测应用或服务风险等级为2级及以上级别的数据，执行步骤3；否则为“不符合要求”，测评结束；
3） 在步骤3之后，若进行过身份验证且具备数据访问权限的用户可以通过其它设备的应用或服务访问被测应用或服务风险等级为2级及以上级别的数据，执行步骤4；否则为“不符合要求”，测评结束；
4） 在步骤4之后，若进行过身份验证但不具备数据访问权限的用户无法通过其它设备的应用或服务访问被测应用或服务风险等级为2级及以上级别的数据，测评结果为“未见异常”；否则为“不符合要求”，测评结束。

5.4.2.8 测试项 j）：同账号下多设备间数据访问已完成对访问用户的身份认证可不进行身份验证（2级及以上风险等级数据）

测试项T/TAF 100-2021-9.1.4.2-h）：基于账号体系的系统中，同一账号下多个设备间数据访问认为已完成对访问用户的身份认证，以支持多用户设备作为入口访问其它设备上的数据的情况除外。

多用户设备指可被多个用户使用的设备，如电视、大屏、PC等。

注：此条标准属同账号下多设备间数据访问的例外情况，无需测评。

5.4.2.9 测试项 k）：数据被其他设备的应用或服务访问时可不进行身份验证（1 级风险等级数据）

测试项T/TAF 100-2021-9.1.4.2-i）：1级风险等级数据被其它设备的应用或服务访问时，可不进行身份验证。

注：此条标准属于低风险等级数据的例外情况，无需测评。

5.4.3 基于远端连接的数据互操作方式其它要求

5.4.3.1 测试项 l）：测评数据在源设备上加密，在目的设备上解密，且远端服务器不可解密（4 级风险等级数据）

测试项T/TAF 100-2021-9.1.4.3-a）：对于风险等级为4级的数据，应用或服务宜确保数据在源设备上加密，在目的设备上解密，确保远端服务器不可解密。

a） 测试步骤：
1） 步骤1：检查厂商提交的文档，查看应用或服务基于远端连接传输数据的设计文档，是否对风险等级为4级的数据在源设备上加密，在目的设备上解密，确保远端服务器不可解密；
2） 步骤2：使用被测应用或服务基于远端连接向目的设备传输风险等级为4级的数据，检查传输后的数据是否与源设备相同；
3） 步骤3：通过网络抓包工具拦截风险等级为4级的传输数据，检查数据是否加密传输，若涉及在远端服务器存储，通过日志/命令行等测试工具查看远端服务器风险等级为4级的数据，检查是否加密存储；
4） 步骤4：使用解密工具尝试解密远端服务器风险等级为4级的数据，检查是否可以解密。

b） 预期结果：
1） 在步骤1之后，若应用或服务对风险等级为4级的数据在源设备上加密，在目的设备上解密，确保远端服务器不可解密，执行步骤2；否则为“不符合要求”，测评结束；

2） 在步骤2之后，若向目的设备传输后的数据与源设备相同，执行步骤3；否则为“不符合要求”，测评结束；

3） 在步骤3之后，若风险等级为4级的数据在终端设备与远端服务器之间加密传输，且涉及在远端服务器存储情况下加密存储，测评结果为“未见异常”；否则为“不符合要求”，测评结束；

4）在步骤4之后，若尝试解密远端服务器风险等级为4级的数据失败，测评结果为“未见异常”；否则为“不符合要求”，测评结束。

5.4.3.2 测试项 m）：测评数据通过加密通道传输及加密存储在服务器（3 级风险等级数据）

测试项T/TAF 100-2021-9.1.4.3-b）：对于风险等级为3级的数据，应用或服务应确保通过终端设备与远端服务器之间的加密通道传输，若涉及在远端服务器存储的情况，则应加密存储在远端服务器。

a） 测试步骤：

1） 步骤1：检查厂商提交的文档，查看应用或服务基于远端连接传输数据的设计文档，是否对风险等级为3级的数据通过智能终端设备与远端服务器之间的加密通道传输，涉及在远端服务器存储的情况，是否加密存储在远端服务器；

2） 步骤2：使用被测应用或服务基于远端连接向目的设备传输风险等级为3级的数据，检查传输后的数据是否与源设备相同；

3） 步骤3：通过网络抓包工具拦截风险等级为3级的传输数据，检查数据是否加密传输，若涉及在远端服务器存储，通过日志/命令行等测试工具查看远端服务器风险等级为3级的数据，检查是否加密存储。

b） 预期结果：

1） 在步骤1之后，若应用或服务对风险等级为3级的数据通过智能终端设备与远端服务器之间的加密通道传输，涉及在远端服务器存储的情况，加密存储在远端服务器，执行步骤2；否则为“不符合要求”，测评结束；

2） 在步骤2之后，若向目的设备传输后的数据与源设备相同，执行步骤3；否则为“不符合要求”，测评结束；

3） 在步骤3之后，若风险等级为3级的数据在终端设备与远端服务器之间加密传输，且涉及在远端服务器存储情况下加密存储，测评结果为“未见异常”；否则为“不符合要求”，测评结束。

5.5 删除阶段

5.5.1 测试项 a）：测评应用或服务应确保数据在智能终端设备上彻底删除（3 级及以上风险等级数据）

测试项T/TAF 100-2021-9.1.5-a）：终端设备上的应用或服务应确保数据在终端设备上彻底删除，禁止使用标志位方式删除。

a） 测试步骤：

1） 步骤1：检查厂商提交的文档，查看应用或服务删除保存在智能终端设备上的3级及以上风险等级数据的设计文档，是否使用了安全删除的方式（如覆盖/重写）；

2） 步骤2：读取被测应用或服务存储3级及以上风险等级数据的ROM单元/区域，检查删除操作后该区域数据二进制数值是否无法恢复成原数据二进制数值（如全0/全1）。

b） 预期结果：

1） 在步骤1之后，若应用或服务对3级及以上风险等级数据使用了安全删除的方式，执行步骤2；否则为“不符合要求”，测评结束；

2） 在步骤2之后，若应用或服务删除操作后3级及以上风险等级数据二进制数值无法恢复成原数据二进制数值，测评结果为“未见异常”；否则为“不符合要求”，测评结束。

电信终端产业协会团体标准

智能终端设备间互操作数据保护测试方法

T/TAF 126—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