ICS 33.050
CCS M 30

团　体　标　准

T/TAF 100-2021

智能终端设备间互操作数据保护技术要求

Data protection technical implementation requirement for interoperation between intelligent terminals

2021-12-13 发布　　2021-12-13 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：华为技术有限公司、中国信息通信研究院、郑州信大捷安信息技术股份有限公司。

本文件主要起草人：衣强、王思善、刘陶、杜云、宁华、张悦、刘献伦、李实。

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。本标准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，供移动终端厂商及业务应用开发厂商借鉴实施，以实现智能终端设备上的数据保护。

智能终端设备间互操作数据保护技术要求

1 范围

本文件规定了设备间互操作过程实现数据保护的要求。

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标准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。

YD/T 1699 移动终端信息安全技术要求

T/TAF 097-2021 智能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

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：本标准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安全概述

4.1 范围

智能终端上存储了用户在使用过程中产生的各种类型数据，本规范所指的数据由系统或应用软件生成的在智能终端系统上存储的数据，同时，数据还可在不同智能终端设备之间流转、使用。

4.2 智能终端设备互操作数据生命周期

数据的生命周期分为生成、存储、使用、传输、删除各阶段，根据数据在智能设备间的操作的过程，设备间互操作数据生命周期包括互操作前、互操作过程、互操作后，互操作前包括数据在源设备上的生成、存储、使用、删除过程，互操作过程包括数据传输过程，互操作后包括数据在目的设备上的生成、存储、使用、删除过程，图1给出了数据在源设备和目的设备间互操作的数据生命周期。

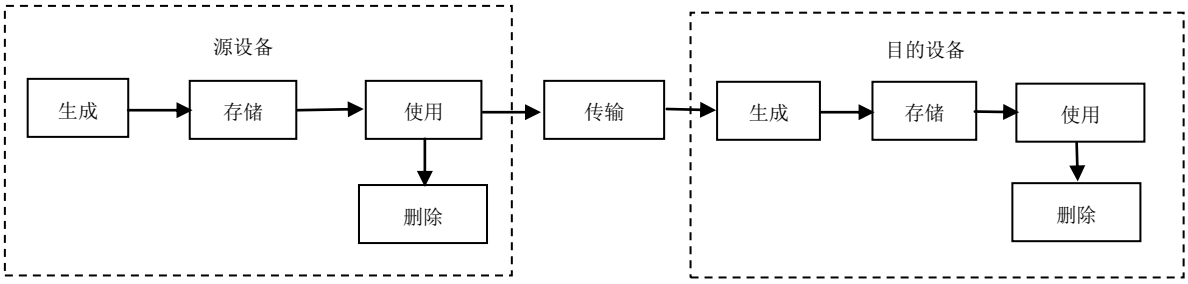

图1 设备间互操作数据生命周期

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。

存储：数据在智能终端设备上存留的过程。

使用：数据在智能终端设备上被访问、处理等操作的过程。

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。

传输：数据离开源智设备、转移到目的设备的过程。

4.3 智能终端设备间互操作数据安全风险

a) 数据泄露。数据在终端设备间存储、流转的过程中，若缺乏数据安全存储、数据加密传输等必要的安全机制，或实现的安全机制强度不足，攻击者利用系统或应用漏洞获取用户数据，导致数据被泄露，破坏系统上业务的正常运行，严重的，还可能由于一个终端上的数据泄露，攻击终端所在的网络，造成网络运行异常。另外，终端系统上保存了大量的用户隐私数据，如生物特征数据、用户设置密码等，若数据被泄露，可能给用户造成隐私、财产损失。

b) 数据篡改。用户在智能终端间互操作数据包括用户数据、系统数据、控制指令等，若在传输、存储、使用过程中，数据没有受到安全强度足够的保护，则攻击者可能篡改数据，影响终端系统正常功能的可用性，或实现非预期的恶意操控。

c) 数据不可使用。数据在终端设备上存储、使用过程中，可能面临DDos攻击或被删除的风险，导致数据不可用，数据在终端设备间进行互操作的过程中，若没有进行安全性保护，还可能出现通信链路阻塞，无法正常通信等风险，导致互操作业务无法开展。

4.4 智能终端设备间互操作数据安全影响因素

终端设备间互操作是指在终端设备间进行数据处理操作的行为，使得数据可以在终端设备之间流转、读取、编辑等操作，从而实现设备控制、用户数据共享等功能。

对于面向消费者的终端设备，其上运行不同业务类型，不同业务类型涉及广泛的数据类型，包括语音图像数据、位置轨迹数据、运动健康数据、生物特征数据、账户凭证等数据类型，因此数据的风险等级各不相同，数据在终端设备间处理过程中的安全保护要求也不同。

同时，数据在设备间处理涉及到数据在不同设备上的生成、存储、使用，而设备作为数据的存储介质，为数据提供基本的保护能力，因此当终端设备的安全能力不同时，对其上数据安全也产生较大差异。

本文件在规定终端设备间数据保护要求时，考虑了数据风险等级因素、终端设备安全能力因素，从数据生命周期对移动终端及其上应用软件提出要求，图1给出了上述各因素之间的关系。

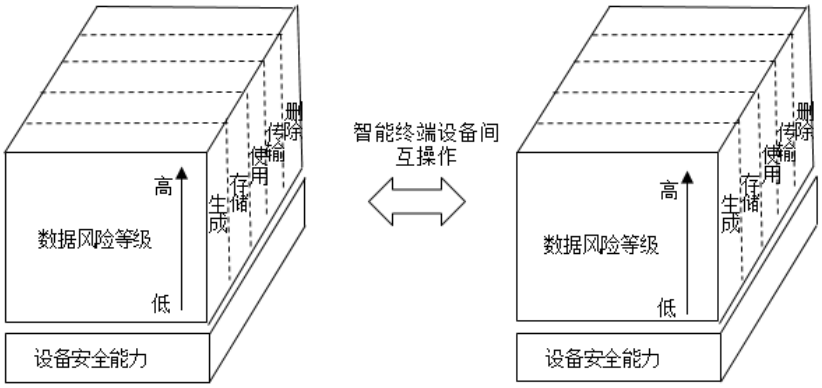

图2　智能设备间互操作数据安全影响因素

5　智能终端设备数据分级原则

数据安全主要从数据的机密性、完整性、可用性三个属性进行评估，机密性是对数据进行加密等控制手段进行保护，防止未授权的访问或披露；完整性是防止信息被非法篡改或销毁；可靠性是确保信息能够及时可靠的被访问和使用，目前业界的评估依据是数据遭到泄露或破坏给组织、个人所带来的影响，综合分析对数据机密性、完整性、可用性造成的影响从而确定数据的风险等级。一般而言，移动终端上的数据风险等级可分为4级，其分级原则是：

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、不可消除的不利影响；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不利影响，或对组织声誉构成特别严重不利影响。
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不利影响、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不利影响，或对组织声誉造成严重不利影响。
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不利影响、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

表1　智能终端设备数据风险等级分级原则（续）

数据风险等级	分级原则	判定原则
		失，或对小部分组织用户产生不利影响，或对组织声誉构成一定威胁、造成一定不利影响。
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不利影响、但可以消除，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不利影响。

数据风险等级示例可参考附录。

6　智能终端设备间互操作设备安全能力

终端设备从所具备的安全能力、所能抵御的风险角度分为不同安全能力级别，而终端设备上的数据安全与数据所在的终端设备的安全能力级别直接相关，如敏感数据应在安全隔离环境中进行加密存储、并受到访问控制机制管理等，要求终端设备具备较高的安全能力等级，而对于公开数据则没有上述要求。反之，对于安全能力较高的终端设备可支持存储、使用敏感等级高的数据，安全能力等级低的设备不建议存储、使用敏感等级高的数据，即终端设备不同安全等级具备不同的可支持的数据风险等级范围。

根据业界最佳实践及相关标准规范，从所具备的安全能力、所能抵御的风险角度，终端设备的安全能力宜划分为5个等级。

具体定义可参考YD/T 1699《移动终端信息安全技术要求》。

7　智能终端设备间数据传输方式

智能终端设备基于终端设备之间建立的连接进行数据传输、共享等操作，智能终端设备之间的连接包含近距离连接、远端连接两种方式，终端设备之间建立连接的方式不同，其上数据传输的方式也不同。

数据在终端设备之间进行操作时，数据所在的原始设备称之为源设备；数据所传输到的目标设备称之为目的设备。

当终端设备间建立近距离端到端通信连接时，可实现基于终端设备间之间近距离连接传输数据，进行设备间互操作，如下图3所示。

当源设备通过远端服务器与目的设备建立连接时，终端设备之间的交互需要通过远端服务器中转实现数据在终端设备之间的传输，实现终端设备之间基于远端连接的方式进行数据互操作，如图4所示。

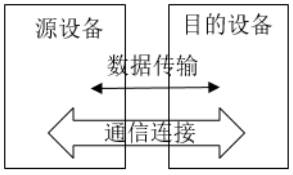

图3　终端设备间基于近距离连接进行数据互操作

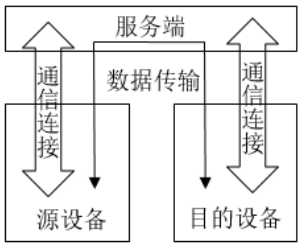

图4　终端设备之间基于远端连接进行数据互操作

8　智能终端设备间互操作数据安全目标

智能终端设备间互操作过程，应保证数据在源设备、目的设备的机密性、完整性和可用性，为实现上述三方面的数据安全，智能终端设备间互操作的数据安全目标是：

a)　数据在智能设备（包括源设备、目的设备）上存储、使用应具备与数据风险等级相应的安全保护措施。

b)　数据从源设备转移到目的设备的情况，应确保源设备、目的设备是可信设备，并确保传输安全。

c)　数据删除过程中，高敏感等级数据应确保安全、彻底删除。

9　智能终端设备间互操作数据安全要求

9.1　智能终端设备间互操作各生命周期要求

9.1.1　生成阶段

终端或其上的应用/服务在数据生成阶段处理各风险等级数据满足如下要求：

表2　智能终端设备互操作数据安全要求-数据生成阶段

要求对象	4级	3级	2级	1级
应用或服务	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。			

9.1.2　存储阶段

终端或其上的应用/服务在数据存储阶段处理各风险等级数据满足如下要求：

表3　智能终端设备互操作数据安全要求-数据存储阶段

要求对象	4级	3级	2级	1级
终端	a)　移动终端应确保不同终端设备间的根密钥的唯一性。 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。			
	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。		无	无

表3　智能终端设备互操作数据安全要求-数据存储阶段（续）

要求对象	4级	3级	2级	1级
应用或服务	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。 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附录B。			
	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。 g) 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。 h) 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。		i) 数据应加密存储。 j) 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。 k) 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。	l) 数据应加密存储。 m) 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。

9.1.3　使用阶段

终端或其上的应用/服务在数据使用阶段处理各风险等级数据满足如下要求：

表4　智能终端设备互操作数据安全要求-数据使用阶段

要求对象	4级	3级	2级	1级
终端	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。			无
应用或服务	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。	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。	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。	

9.1.4 传输阶段

9.1.4.1 传输阶段一般要求

终端或其上的应用/服务在数据传输阶段处理各风险等级数据满足如下要求，适用于基于近距离连接的互操作、基于远端连接的智能设备间互操作。

表5 智能终端设备互操作数据安全要求-数据传输阶段

要求对象	4级	3级	2级	1级
应用或服务	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。			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。

9.1.4.2 基于近距离连接的数据互操作方式传输阶段其它要求

基于近距离连接的智能设备间互操作，终端或其上的应用/服务在数据传输阶段处理各风险等级数据还需满足如下要求：

表6 智能终端设备互操作数据安全要求-基于近距离连接数据传输阶段

要求对象	4级	3级	2级	1级
终端	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《智能设备间互信操作技术要求》。			无
应用或服务	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。 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。 若目的设备不能支持待传输数据的最高风险等级，则需在源设备用户确认的前提下进行数据传输。 d) 在支持账号登陆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。 e) 数据从源数据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。 f) 生物特征模板数据，如指纹模板，不宜在设备间传输。			
	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。 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			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。

表6　智能终端设备互操作数据安全要求-基于近距离连接数据传输阶段（续）

要求对象	4级	3级	2级	1级
	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。			

9.1.4.3　基于远端连接的数据互操作方式传输阶段其它要求

基于远端连接的智能设备间互操作，终端或其上的应用/服务在数据传输阶段处理各风险等级数据还需满足如下要求：

表7　智能终端设备互操作数据安全要求-基于远端连接数据传输阶段

要求对象	4级	3级	2级	1级
应用或服务	a)　对于风险等级等级为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。	b)　对于风险等级等级为3级的数据，若涉及在远端服务器存储的情况，则应在远端服务器加密存储。	无	无

9.1.5　删除阶段

终端或其上的应用/服务在数据删除阶段处理各风险等级数据满足如下要求：

表8　智能终端设备互操作数据安全要求-数据删除阶段

要求对象	4级	3级	2级	1级
应用或服务	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。		无	无

附 录 A
（资料性）
数据类型及数据风险等级示例

根据本文件第 5 章的定级原则，表 A.1 给出不同类型数据的风险等级，同时，给出数据是否是用户个人信息的参考。

表A.1 数据类型及数据风险等级示例

数据类型	是否是个人信息	级别	实例
敏感身份标识	是	4	身份证号码、军官证号码、 社会/保险保障号码、驾照号码、护照号码、签证授权编号、口令及密码
生物特征	是	4	DNA、指纹、面部特征、声纹、虹膜、行为特征等
健康信息	是	4	体脂、血压、血糖、心率、血氧、医疗记录、生理周期等
金融账号标识	是	4	银行账号、支付账号等
运动信息	是	3	运动目标、运动类型、步数、运动距离、运动时长等
用户行为特征	是	3	兴趣爱好、行为习惯等
精确位置	是	3	经纬度、轨迹
通信内容	是	3	通话语音、短信内容、电子邮件内容、及时通信内容、语音消息等
通信记录	是	3	来去电号码、通话记录
通讯录	是	3	联系人列表、好友群组、黑名单群组等
多媒体数据	是	3	图片及图片信息、音视频、日历日程、备忘录、文档、文件
浏览记录	是	3	网页浏览记录、新闻浏览记录等
密钥	否	3	系统密钥等密钥信息
不可变更硬件标识符	是	3	SN、IMEI、SIM 卡标识
账号信息	是	2	微信账号、微博账号等
头像昵称	是	2	昵称姓名、头像图片信息
家庭、工作相关信息	是	2	婚姻状况、家庭成员、工作类型、工作单位等
身高体重等个人信息	是	2	身高数据、体重数据
粗略位置	是	2	基站标识、小区标识、公网 IP 地址、SSID 等信息
联系方式	是	2	电话号码、邮件地址等
快递及相关信息	是	2	快递地址 寄\收件人电话 寄\收件人姓名等
地址信息	是	2	工作地址、家庭地址等
个人消费记录、财税信息	是	2	交易和消费记录、信贷记录、征信信息等
合约、订阅信息	是	2	订阅关系、订阅的服务信息、合约信息等

表A.1　数据类型及数据风险等级示例（续）

数据类型	是否是个人信息	级别	实例
权益信息	是	2	折扣券等其它权益
服务、行为记录	是	2	播放记录、收藏记录、用户提交信息、查询结果等
其它设备标识符	是	2	androidID 等
网络地址	是	2	IP 地址、蓝牙 MAC 地址、wifi MAC 地址
临时认证凭据	否	2	短信验证码、登录验证码等
一般个人信息	是	1	性别、国籍、教育程度等
区域位置信息	是	1	国家标识、运营商标识、城市、村镇等
用户配置信息	是	1	开关、布局、分辨率等设备配置信息，应用个性化配置信息
系统信息	否	1	系统临时文件/数据、系统文件、日志、版本、系统状态/运行记录
应用信息	否	1	应用标识符、应用文件、应用状态/运行记录
设备信息	否	1	设备类型、设备状态/运行记录
网络信息	否	1	网络状态信息

附 录 B
（资料性）
设备安全等级与数据风险等级对应表

根据设备安全等级分级原则，5 级、4 级设备具备了最高、或最完整的设备安全能力和风险抵御能力，因此可传输所有风险等级数据；3 级设备具备了较强的安全能力和风险抵御能力，除最高风险等级的数据外，其它等级数据均可以存储、使用在该等级设备中；2 级设备具备了一定的安全能力，而 4、3 级风险等级数据涵盖了用户生物特征、健康信息、多媒体信息、通讯录等高敏感等级数据，不应存储在 2 级等级设备中，因此 2 级设备可存储、使用 1 级和 2 级风险等级数据；1 级设备仅具备了基础的安全能力，无法抵御一般的风险攻击，仅可存储最低风险等级的数据。

表B.1 设备安全等级可支持的数据风险等级表

设备安全能力级别	5	4	3	2	1
数据风险等级	所有级别	所有级别	1-3	1-2	1

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技术要求

T/TAF 100—2021

*

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