ICS 33.050
CCS M 30

# 团　体　标　准

T/TAF 195—2023

# 支持支付业务的可穿戴设备安全规范

Security specifications for wearable devices supporting payment services

2023-11-24 发布　　2023-11-24 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：蚂蚁科技集团股份有限公司、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、百度在线网络技术（北京）有限公司、中国联合网络通信有限公司。

本文件主要起草人：孟飞、崔晓夏、林冠辰、袁琦、路晔绵、沈军强、张伟、黄乡崧、彭晋、李春强、王鲁克、熊健、刘小丽、田琛、刘献伦、郭建领、厉盛义。

# 引　言

随着物联网时代的到来，可穿戴智能终端越来越深入人们的生活，大量低功耗可支持支付业务的可穿戴设备（简称可穿戴设备）涌现在市场上，例如具备支付功能的智能手表、手环、VR设备等产品。但是由于这些设备碎片化非常严重，各个厂商采用的控制芯片、存储器、安全方案都不尽相同，存在支付安全隐患，限制了可穿戴支付应用生态发展，对于用户的使用体验、财产安全造成较大影响，并且阻碍整个行业生态的健康发展。

可穿戴支付是比较新兴的领域，支付又是高安全需求业务，目前国内外针对可穿戴支付的设备安全规范尚属空白，不能很好的指导可穿戴设备设计、开发、测试等工作，标准亟需补充。基于上述考虑制定本文件，一方面提高穿戴支付设备安全标准化水平，为穿戴支付设备产品的设计生产提供指导，为国内该领域的相关服务开发者提供安全的标准化开发方案，另一方面提升用户穿戴支付应用体验，切实保障用户财产安全。此外，该文件还能够提高整个穿戴支付物联网设备产业链的研发效率、减少上下游接口的磨合时间，帮助穿戴支付设备厂商和服务提供上提升服务能力，推动整个行业生态积极发展。

# 支持支付业务的可穿戴设备安全规范

## 1 范围

本文件规定了支持支付业务的可穿戴设备的安全功能要求，包括硬件安全、安全启动、安全更新、安全存储、访问控制、安全通信、业务安全、数据安全与个人信息保护要求。

本文件适用于支持支付业务的可穿戴设备的研发、设计、生产、测试等活动。

## 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—2022 信息安全技术 术语

GB/T 36651—2018 信息安全技术 基于可信环境的生物特征识别身份鉴别协议框架

## 3 术语和定义

GB/T 25069—2022界定的以及下列术语和定义适用于本文件。

3.1

**设备凭证 device certificate**

预置在芯片内部、用于提供设备身份信息的数据。

3.2

**支付凭证 payment certificate**

在设备和支付账号绑定过程中，由支付云平台下发的用于生成支付令牌的数据。

3.3

**支付令牌 payment token**

设备支付过程中，利用支付凭证动态生成的、用于支付云平台进行支付账户匹配、支付等操作的数据。

3.4

**可信环境 trusted environment**

设备上可保证加载到其内部数据的安全性如保密性、完整性和可用性的安全区域。

注：可信环境的实现方式可包括可信执行环境（TEE）、安全元件（SE）、可信密码模块（TCM）或其他具备安全边界的保护区域。

[来源：GB/T 36651—2018，3.1，有修改]

3.5

**支付云平台 payment cloud platform**

在可穿戴支付场景中负责与收款设备完成支付过程的云平台。

3.6

**安全存储区域 secure storage zone**

通过软件或硬件隔离技术与系统其他存储区域隔离的，为其上存储的数据提供安全保护的存储区域。

注：安全存储区域可以是外部安全芯片的存储区域，也可以是受安全隔离机制保护的存储区域。

## 4 缩略语

下列缩略语适用于本文件。

HUK：硬件唯一密钥（Hardware Unique Key）

SE：安全元件（Secure Element）

TCM：可信密码模块（Trusted Cryptography Module）

TEE：可信执行环境（Trusted Execution Environment）

## 5 可穿戴设备支付应用参考模型

典型的具备支付功能的可穿戴设备（简称可穿戴设备）应用参考模型见图1。典型应用参考模型中包含可穿戴设备、收款设备、支付云平台和手机支付APP四个参与主体，支付应用涉及到可穿戴支付交易、可穿戴支付个人管理和可穿戴支付平台管理三个功能角色管理。

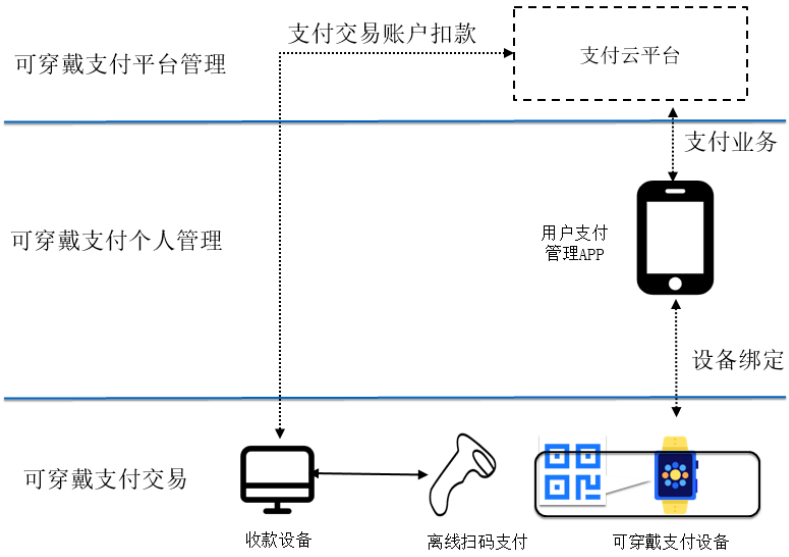


图 1 典型的可穿戴设备支付应用参考模型

具体到可穿戴设备，其支付应用包括两个阶段，分别是设备绑定阶段和支付业务交易阶段。

a) 在设备绑定阶段，可穿戴设备可直接或经过手机 APP 将设备凭证转发给支付交易平台，支付交易平台使用可穿戴设备的设备凭证将设备与用户支付账户进行绑定，并生成支付凭证下发给可穿戴设备；
b) 在支付业务交易阶段，可穿戴设备使用支付凭证与收款设备和支付交易平台完成交易，例如可穿戴设备动态生成支付令牌，如二维码。通过扫描设备扫描支付令牌后，收款设备和支付交易平台进行对应账户扣款操作来完成交易。

## 6 可穿戴设备安全威胁分析

可穿戴设备可能面临以下安全威胁：

a) 本地安全威胁，包括如下：
   1) 攻击者获取硬件调试能力，从而控制设备运行；
   2) 攻击者篡改或替换设备固件；
   3) 收集、存储的个人信息等敏感数据被泄露。
b) 远程通信安全威胁，包括如下：
   1) 攻击者篡改或替换固件更新包，或者使用包含已知漏洞的旧版本
   2) 固件替换固件更新包；
   3) 设备与手机/支付云平台之间的通信被劫持，造成设备绑定到其他的手机或云平台；
   4) 设备与手机/支付云平台之间的传输的支付凭证被泄露、篡改、伪造等。
c) 业务安全威胁，包括如下：
   1) 攻击者窃取设备，使用离线支付功能进行支付，损害用户利益；
   2) 用户账号与错误的设备进行绑定，从而损害用户利益；
   3) 攻击者窃取、篡改或替换设备上存储的设备凭证、支付凭证；
   4) 恶意应用非授权访问支付应用存储的支付凭证等数据。

## 7 可穿戴设备安全架构

为保证上述可穿戴支付应用场景的安全运行，可穿戴设备应提供相应的安全功能，具体安全架构如图2所示。

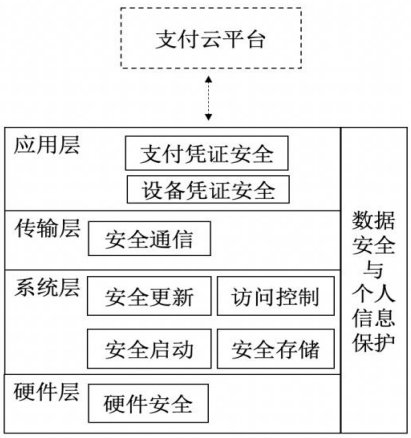


图 2 可穿戴设备安全架构

安全架构从下到上可分为四层：

——硬件层提供硬件安全，包括HUK、调试接口等；

——系统层提供核心安全服务，包括安全启动、安全更新、安全存储、访问控制等；

——传输层提供安全通讯机制；

——应用层提供主要包括可穿戴支付场景使用到的设备凭证和支付凭证的安全要求。

此外，可穿戴设备还应提供业务安全、数据安全与个人信息保护功能，这两部分的安全功能可能涉及如下安全服务：

——业务安全主要包括可穿戴支付场景使用到的设备凭证和支付凭证的安全要求；

——数据安全与个人信息保护功能主要涉及可穿戴设备对收集的用户个人信息以及其他数据的安全保护能力。

## 8 可穿戴设备安全要求和测试方法

### 8.1 概述

本章规定了可穿戴设备安全分级和安全技术要求。

### 8.2 安全分级

依据敏感数据存储的安全性，可将本章的安全技术要求分为三个等级，其中一级可使用软件加密算法实现数据的安全存储，二级应使用硬件机制保护存储数据的安全，三级应提供硬件保护机制和代码逻辑安全机制。具体分级情况可见表1。

**表 1 安全技术要求分级表**

| 安全技术要求 | | 一级 | 二级 | 三级 |
|---|---|---|---|---|
| 硬件层安全要求 | 硬件安全要求 | 8.3.1 | 8.3.1 | 8.3.1 |
| 系统层安全要求 | 安全启动要求 | 8.3.2.1 a) | 8.3.2.1 a)b) | 8.3.2.1 a)c) |
| | 安全更新要求 | 8.3.2.2 a)d)f) | 8.3.2.2 a)b)d)f) | 8.3.2.2a),c)-e)f) |
| | 安全存储要求 | 8.3.2.3 a) | 8.3.2.3 a)-c) | 8.3.2.3 |
| | 访问控制要求 | 8.3.2.4 a) | 8.3.2.4 | 8.3.2.4 |
| 传输层安全要求 | 安全通信要求 | 8.3.3 | 8.3.3 | 8.3.3 |
| 应用层业务安全要求 | 设备凭证安全要求 | 8.3.4.1 | 8.3.4.1 | 8.3.4.1 |
| | 支付凭证安全要求 | 8.3.4.2 a)b) | 8.3.4.2 a)b) | 8.3.4.2 |
| 数据安全要求 | 数据安全与个人信息保护要求 | 8.3.5 | 8.3.5 | 8.3.5 |
| 密码算法安全要求 | 密码算法安全要求 | 8.3.6 | 8.3.6 | 8.3.6 |

### 8.3 安全技术要求

#### 8.3.1 硬件安全要求

可穿戴设备硬件层应满足以下安全要求：

a) 设备应具备HUK，该HUK应用于实现固件和芯片绑定；

b) HUK长度不应低于128bit；

c) HUK可由芯片硬件生成或存于OTP区域；

d) 设备应在出厂前关闭物理调试接口或者禁用物理调试功能；

e） 硬件固件不应通过物理接口（如串口等）提取出来。

### 8.3.2 系统层安全要求

#### 8.3.2.1 安全启动要求

可穿戴设备的安全启动功能，应满足以下要求：

a） 应支持镜像文件完整性校验，校验通过后方可加载运行，校验机制应采用哈希算法；

b） 应支持镜像文件来源验证，验证通过后方可加载运行，验证机制应采用对称密码算法；

c） 应支持镜像文件来源验证，验证通过后方可加载运行，验证机制应采用非对称密码算法。

注：此处涉及的镜像文件为系统启动过程中镜像文件，一般包括ROM、Bootloader、主镜像文件。其中b)和c)的区别在于验签机制采用的算法安全性不同，非对称密码算法安全性高于对称密码算法安全性。

#### 8.3.2.2 安全更新要求

可穿戴设备安全更新应满足以下要求：

a） 应支持升级镜像文件完整性校验，校验通过后方可进行镜像文件升级，校验机制应采用哈希算法；

b） 应支持升级镜像文件来源验证，验证通过后方可进行镜像文件升级，验证机制应采用对称密码算法；

c） 应支持升级镜像文件来源验证，验证通过后方可进行镜像文件升级，验证机制应采用非对称密码算法；

d） 镜像文件升级失败应保证设备可使用可运行的版本正常运行；

e） 应提供镜像文件版本防回滚机制，防止通过升级机制将镜像文件进行版本降级；

f） 如通过手机等代理设备进行镜像文件安全验证的，应在可穿戴设备和代理设备之间建立安全的传输通道，保障镜像文件传输时不被篡改。

注：可穿戴设备可支持设备自主安全更新或代理设备（如可穿戴设备绑定的手机）安全更新，镜像文件安全性可以由可穿戴设备或者代理设备进行验证。

#### 8.3.2.3 安全存储要求

可穿戴设备应提供安全存储能力，满足以下要求：

a） 应使用基于密码学的安全机制保障存储数据的机密性和完整性；

b） 应使用硬件保护机制（如TEE、SE等）防止存储数据被篡改或泄露；

c） 应保证安全存储区域与系统非安全存储区域之间的物理隔离；

d） 应提供数据防回滚机制。

注：防回滚机制用于保证当前数据是最新数据，而不能被过期数据更新。

#### 8.3.2.4 访问控制要求

可穿戴设备应提供访问控制机制，满足以下要求：

a） 设备宜具备身份认证访问控制机制，包括但不限于锁屏密码、为支付应用设置应用锁、在唤起支付功能时进行生物识别身份认证等；

b） 应提供针对应用资源的访问控制机制，除明确授权情况外，应阻止一个应用对另一个应用资源的访问。

注：此处的应用资源主要指应用运行过程中生成和存储的数据，例如属于当前应用的支付凭证。

### 8.3.3 传输层安全要求

可穿戴设备应提供安全通信机制，满足以下要求：

a) 可穿戴设备与手机等其他设备进行数据交互时其他设备应基于设备凭证对该可穿戴设备进行身份验证并构建安全的数据传输通道；

b) 应使用安全的通信协议，并且对通信数据加密，保障数据的完整性和机密性。

#### 8.3.4 应用层业务安全要求

##### 8.3.4.1 设备凭证安全要求

可穿戴设备应具备设备凭证，用于设备绑定过程中的设备身份识别。设备凭证安全要求如下：

a) 设备凭证中应包含设备唯一标识符，以保证支付云平台可以据此识别和管理可穿戴设备；

b) 设备凭证中应包含设备证书等安全凭证，用于设备绑定过程中服务端对设备身份进行验证；

c) 设备凭证的存储应满足8.3.2.3中的要求；

d) 设备凭证应与芯片进行绑定，防止设备被克隆。

##### 8.3.4.2 支付凭证安全要求

可穿戴设备应具备支付凭证，满足以下要求：

a) 支付凭证的存储应满足8.3.2.3中的要求；

b) 设备解绑或设备恢复出厂设置时，应删除支付凭证且无法恢复；

c) 应在可信环境中完成基于支付凭证生成支付令牌的过程。

#### 8.3.5 数据安全与个人信息保护要求

支持支付功能的可穿戴设备对其上数据的处理应满足以下要求：

a) 设备若需收集用户敏感个人信息，应确保有完备的隐私政策，确保用户知情并单独同意；如涉及收集不满十四周岁未成年人信息的，应当征得未成年人的父母或其他监护人同意；

b) 收集的数据应满足最小化原则，不应超范围、超频次进行数据收集；

c) 数据的存储应具备访问控制机制或使用符合8.3.2.3的安全存储机制；

d) 数据的共享、提供、公开应具备合理性和必要性，并应征得用户同意；

e) 数据的传输应满足8.3.3的要求，必要时应对敏感数据进行加密或脱敏后再传输；

f) 收集、使用、传输阶段所使用的敏感数据的缓存数据，应该提供自动删除或者授权用户手动删除功能。

#### 8.3.6 密码算法安全要求

本文件涉及的密码算法应符合法律、法规的规定，符合国家相关管理机构和相关国家标准、行业标准的要求，保障密码算法在应用中的合规性、正确性和有效性。

### 8.4 安全测试方法

#### 8.4.1 硬件安全

可穿戴设备硬件安全检测方法和结果判定如下：

a) 检测方法如下：

1) 查看设备是否具备 HUK，HUK 是否应用于实现固件和芯片绑定；

1) 查看 HUK 长度是否低于 128bit；

2) 查看 HUK 是否由芯片硬件生成或存于 OTP 区域；

3) 查看设备是否关闭物理调试接口或者禁用物理调试功能；

4） 查看硬件固件是否可以通过物理接口（如串口等）提取出来。

b） 预期结果如下：

1） 设备具备 HUK，切该 HUK 应用于实现固件和芯片绑定；

2） HUK 长度不低于 128bit；

3） HUK 可由芯片硬件生成或存于 OTP 区域；

4） 设备关闭物理调试接口或者禁用物理调试功能；

5） 硬件固件不能通过物理接口（如串口等）提取出来。

c） 结果判定：

实际测试结果与相关预期结果一直则判定为符合，其他情况判定为不符合。

### 8.4.2 系统层安全

#### 8.4.2.1 安全启动

可穿戴设备安全启动检测方法和结果判定如下：

a） 检测方法如下：

1） 检查镜像文件完整性校验是否校验通过后才可加载运行，校验机制是否采用哈希算法；

2） 查看镜像文件是否支持来源验证，是否验证通过后才能加载运行，验证机制是否采用对称密码算法；

3） 查看镜像文件是否支持来源验证，是否验证通过后才能加载运行，验证机制是否采用非对称密码算法。

b） 预期结果如下：

1） 支持镜像文件完整性校验，校验通过后才能加载运行，校验机制采用哈希算法；

2） 支持镜像文件来源验证，验证通过后才能加载运行，验证机制采用对称密码算法；

3） 支持镜像文件来源验证，验证通过后才能加载运行，验证机制采用非对称密码算法。

c） 结果判定：

实际测试结果与相关预期结果一直则判定为符合，其他情况判定为不符合。

#### 8.4.2.2 安全更新

可穿戴设备安全更新检测方法和结果判定如下：

a） 检测方法如下：

1） 查看是否支持升级镜像文件完整性校验，是否校验通过后才可进行镜像文件升级，校验机制是否采用哈希算法；

2） 查看是否支持升级镜像文件来源验证，是否验证通过后才可进行镜像文件升级，验证机制是否采用对称密码算法；

3） 查看是否支持升级镜像文件来源验证，是否验证通过后方可进行镜像文件升级，验证机制是否采用非对称密码算法；

4） 查看镜像文件升级失败后，设备是否可使用升级前的版本正常运行；

5） 查看是否提供镜像文件版本防回滚机制，是否可以通过升级机制将镜像文件进行版本降级；

6） 如通过手机等代理设备进行镜像文件安全验证的，查看可穿戴设备和代理设备之间是否建立安全的传输通道，是否保障镜像文件传输时不被篡改。

b） 预期结果如下：

1） 支持升级镜像文件完整性校验，仅校验通过后才可进行镜像文件升级，校验机制采用哈希算法；

2） 支持升级镜像文件来源验证，仅验证通过后才可进行镜像文件升级，验证机制采用对称密码算法
3） 支持升级镜像文件来源验证，仅验证通过后方可进行镜像文件升级，验证机制采用非对称密码算法；
4） 镜像文件升级失败后，设备可使用升级前的版本正常运行；
5） 镜像文件版本防回滚，不能通过升级机制将镜像文件进行版本降级。
6） 如通过手机等代理设备进行镜像文件安全验证的，可穿戴设备和代理设备之间建立了安全的传输通道，镜像文件传输时不被篡改。

c） 结果判定如下：
实际测试结果与相关预期结果一直则判定为符合，其他情况判定为不符合。

#### 8.4.2.3 安全存储

可穿戴设备安全存储检测方法和结果判定如下：

a） 检测方法如下：
1） 查看是否基于密码学的安全机制进行数据加密存储；
2） 查看是否使用硬件保护机制（如 TEE、SE 等）存储数据；
3） 查看安全存储区域与系统非安全存储区域之间是否物理隔离；
4） 查看是否提供数据防回滚机制。

b） 预期结果如下：
1） 提供存储数据的机密性和完整性保护；
2） 使用硬件保护机制（如 TEE、SE 等）防止存储数据被篡改或泄露；
3） 安全存储区域与系统非安全存储区域之间进行了物理隔离；
4） 提供了数据防回滚机制。

c） 结果判定如下：
实际测试结果与相关预期结果一直则判定为符合，其他情况判定为不符合。

#### 8.4.2.4 访问控制

可穿戴设备访问控制检测方法和结果判定如下：

a） 检测方法如下：
1） 查看设备是否具备身份认证访问控制机制，包括但不限于锁屏密码、为支付应用设置应用锁、在唤起支付功能时进行生物识别身份认证等；
2） 查看是否提供针对应用资源的访问控制机制，是否存在无授权情况外一个应用对另一个应用资源可进行访问的情况。

b） 预期结果如下：
1） 设备具备身份认证访问控制机制，包括但不限于锁屏密码、为支付应用设置应用锁、在唤起支付功能时进行生物识别身份认证等；
2） 提供针对应用资源的访问控制机制，无授权情况下一个应用无法对另一个应用资源进行访问。

c） 结果判定如下：
实际测试结果与相关预期结果一直则判定为符合，其他情况判定为不符合。

### 8.4.3 传输层安全

可穿戴设备传输层安全通信检测方法和结果判定如下：

a） 检测方法如下：

1） 将可穿戴设备与手机等设备进行数据交互，查看是否基于设备凭证对该可穿戴设备进行身份验证并是否构建数据安全传输通道；

2） 查看支持数据和机密性完整性保护的安全通信协议，是否对通信数据加密。

b） 预期结果如下：

1） 可穿戴设备与手机等其他设备进行数据交互时，其他设备基于设备凭证对该可穿戴设备进行了身份验证并构建了数据安全传输通道；

2） 使用了安全通信协议进行数据交互，对通信数据进行了加密。

c） 结果判定如下：

实际测试结果与相关预期结果一直则判定为符合，其他情况判定为不符合。

### 8.4.4 应用层业务安全

#### 8.4.4.1 设备凭证安全

设备凭证安全检测方法和结果判定如下：

a） 检测方法如下：

1） 查看设备凭证中是否包含设备唯一标识符；

2） 查看设备凭证中是否包含设备证书；

3） 存储安全测试按照 8.4.2.3 a）中的方法进行测试；

4） 查看设备凭证是否与芯片进行绑定。

b） 预期结果如下：

1） 设备凭证中包含设备唯一标识符；

2） 设备凭证中包含设备证书；

3） 设备凭证存储安全预期结果见 8.4.2.3 b）；

4） 设备凭证与芯片进行绑定。

c） 结果判定如下：

实际测试结果与相关预期结果一直则判定为符合，其他情况判定为不符合。

#### 8.4.4.2 支付凭证安全要求

可穿戴设备应具备支付凭证并保障支付凭证安全，满足以下要求：

a） 检测方法如下：

1） 支付凭证存储安全测试按照 8.4.2.3 a）中的方法进行测试；

2） 将设备解绑或恢复出厂设置，查看是否删除支付凭证且无法恢复；

3） 查看基于支付凭证生成支付令牌的过程是否在可信环境中完成。

b） 预期结果如下：

1） 支付凭证存储安全预期结果见 8.4.2.3 b）；

2） 将设备解绑或恢复出厂设置，支付凭证删除且无法恢复；

3） 基于支付凭证生成支付令牌的过程在可信环境中完成。

c） 结果判定如下：

实际测试结果与相关预期结果一直则判定为符合，其他情况判定为不符合。

### 8.4.5 数据安全与个人信息保护要求

数据安全与个人信息保护检测方法和结果判定如下：

a） 检测方法如下：

1） 查看是否有完备的隐私政策，隐私政策是否涵盖如下内容：设备若需收集用户敏感个人信息，需用户授权并单独同意，如涉及收集不满十四周岁未成年人信息的，应当征得未成年人的父母或其他监护人同意；
2） 查看收集的数据是否满足最小化原则，是否有超范围、超频次数据收集；
3） 查看数据的存储是否具备访问控制机制或参照 8.4.2.3 a）的检测方法进行测试；
4） 查看数据的共享、提供、公开是否具备合理性和必要性，并是否征得用户同意；
5） 数据传输测试按照 8.4.2.5 a）的测试方法，查看必要的情况下是否有这对敏感数据进行加密或脱敏后再传输；
6） 查看收集、使用、传输阶段所使用的敏感数据的缓存数据，是否可以自动删除或者授权用户进行手动删除。

b） 预期结果如下：
1） 具备完备的隐私政策，隐私政策是否涵盖如下内容：设备若需收集用户敏感个人信息，需用户授权并单独同意，如涉及收集不满十四周岁未成年人信息的，应当征得未成年人的父母或其他监护人同意；
2） 收集的数据满足最小化原则，不存在超范围、超频次数据收集的行为；
3） 数据的存储具备访问控制机制或参照 8.4.2.3 b）的预期结果；
4） 数据的共享、提供、公开具备合理性和必要性，并征得用户同意；
5） 数据传输测试按照 8.4.2.5 a）的测试方法，必要的情况下有针对敏感数据进行加密或脱敏后再传输；
6） 收集、使用、传输阶段所使用的敏感数据的缓存数据，可以自动删除或者授权用户进行手动删除。

c） 结果判定如下：
实际测试结果与相关预期结果一直则判定为符合，其他情况判定为不符合。

### 8.4.6 密码算法安全要求

密钥算法安全检测方法和结果判定如下：

a） 检测方法如下：
查看密码算法是否符合法律、法规的规定，符合国家相关管理机构和相关国家标准、行业标准的要求，密码算法在应用中是否满足合规性，正确性和有效性。

b） 预期结果如下：
符合法律、法规的规定，符合国家相关管理机构和相关国家标准、行业标准的要求，密码算法在应用中满足合规性，正确性和有效性。

c） 结果判定如下：
实际测试结果与相关预期结果一直则判定为符合，其他情况判定为不符合。

# 电信终端产业协会团体标准

# 支持支付业务的可穿戴设备安全规范

T/TAF 195—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