ICS 33.050
M 30

团　体　标　准

T/TAF 087-2021

智能可穿戴设备安全　儿童电话手表安全技术要求和测试评估方法

Security of smart wearable devices—Security technical requirements and assessment methods for children's watch phone

2021-05-12 发布　　2021－05－12 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、广东小天才科技有限公司、北京奇虎科技有限公司、福州物联网开放实验室有限公司、上海兆言网络科技有限公司。

本文件主要起草人：宁华、刘陶、吴怡、周俊华、周裕亮、姚一楠、周晓彤、李戎。

引　言

儿童安全问题在全球都是一个非常热门的话题，每年针对儿童的安全问题国家都会制定一些相应举措，但仍旧不能够避免儿童走丢等问题的发生。伴随着可穿戴设备的兴起，儿童智能手表也在市场大潮中崛起。儿童手表兼具电话功能，具有智能作用，自身具有安全，便于携带等特点，同时随儿童电话手表的不断发展，逐渐增加了定位和通话功能，因此受到广大家长的喜爱，而且对于大部分的家长来说购买电话手表的初衷是为了保证幼儿的安全. 但是，儿童电话手表产业刚刚起步，但所面临的安全威胁也日趋凸显，针对儿童电话手表的恶意攻击种类不断更新，儿童隐私信息泄露、中间人攻击、恶意远程操控等事件反复曝光，给用户信息和人身安全带来极大困扰。儿童电话手表的信息安全问题已成为制约产业发展的重要因素之一。目前国内儿童电话手表市场发展快速，产品类别繁多，安全防护水平参差不齐。

本文件旨在规范儿童电话手表的安全防护能力，通过提高儿童电话手表自身的安全防护水平，以防范各类安全威胁，避免用户的利益受到损害，同时防止儿童电话手表对网络安全产生不利影响。

本文件的制定能够为儿童电话手表采购者、生产厂商、评估机构提供了一个多方认可的，通用的儿童电话手表设计开发安全要求，儿童电话手表可参考本文件进行设计、开发，评估机构可依据本文件开展对儿童电话手表的安全评估，设备采购者可采信基于本文件的评估结果。

智能可穿戴设备安全　儿童电话手表安全技术要求和测试评估方法

1　范围

本文件规定了儿童电话手表的终端设备安全能力的技术要求，包括儿童电话手表硬件安全能力、操作系统安全能力、外围接口安全能力、控制程序安全能力、服务器端安全能力、无线通信安全能力、家长和儿童个人数据保护安全能力等。

本文件适用于儿童电话手表终端设备，个别条款不适用于特殊行业、专业应用，其他类似设备也可参考使用。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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。

YDB 200-2018 可穿戴无线通信设备通用技术要求和测试方法 腕戴式设备ISO/IEC 18092 Information technology-Telecommunications and information exchange between systems — Near Field Communication — Interface and Protocol (NFCIP-1)

USB-IF USB2.0 USB2.0 Electrical Test Specification

Bluetooth SIG 蓝牙安全管理协议测试规范（Security Manager Protocol (SM) Bluetooth Test Specification）

Bluetooth SIG 蓝牙通用属性协议测试规范（Generic Attribute Profile (GATT) Bluetooth Test Specification）

Bluetooth SIG 蓝牙属性协议测试规范（Attribute Profile (GATT) Bluetooth Test Specification）

Bluetooth SIG 蓝牙通用接入协议测试规范（Generic Access Profile (GAP) Bluetooth Test Specification）

3　术语、定义和缩略语

3.1 术语和定义

3.1.1

儿童电话手表　children's watch phone

面向14周岁以下儿童设计，具有定位、通话、即时通讯等基本功能，使用客户识别模块（SIM卡或eSIM），采用公共运营商网络且具备手表基本形态特征的电子通讯产品，具备家长端控制程序。

3.1.2

儿童电话手表控制程序　children's watch phone control program

安装在家长手机或平板等智能终端，能够实现某项或某几项特定任务的程序，主要是进行手表功能设置、查看定位和孩子之间的沟通交流等。

3.1.3

儿童电话手表服务器端 children's watch phone server

连接儿童电话手表和家长控制程序桥梁，提供绑定、定位等后台服务。

3.2 缩略语

下列缩略语适用于本文件。

ADB：安卓调试桥（Android Debug Bridge）
API：应用程序编程接口（Application Programming Interface）
APP：移动应用程序（Application）
DDOS：分布式拒绝服务攻击（Distributed Denial Of Service Attack）
DNS：域名系统（Domain Name System）
MAC：媒体存取控制位址（Media Access Control Address）
NFC：近场通信（Near Field Communication）
SQL：结构化查询语言（Structured Query Language）
USB：通用串行总线（Universal Serial Bus）
WLAN：无线局域网（Wireless Local Area Network）
XSS：跨站脚本攻击（Cross Site Scripting）

4 安全能力框架及目标

4.1 主要安全风险

儿童电话手表系统由远程服务器端、儿童电话手表终端和家长端控制程序三部分组成，总体框架如下图1所示。

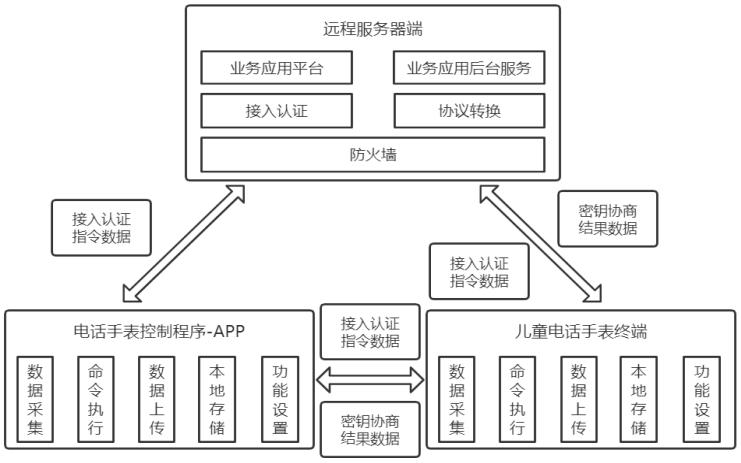

图 1 儿童电话手表应用总体框架图

儿童电话手表的安全风险存在于硬件、操作系统、应用软件、外围接口、远程服务器端、无线通信、家长数据&儿童数据七个方面。各层次所面临的主要风险见表1。

表 1 儿童电话手表重要安全风险

对象	主要安全风险
硬件	• 材料安全，有毒有害物质； • 非授权的访问； • 功能失效、设备不可用； • 假冒设备。
操作系统	• 非授权的访问； • 审计数据丢失； • 恶意代码攻击； • 非法软件安装； • 端口爆破，手表被控制。
应用软件	• 脱壳、二次编译； • 软件漏洞； • 恶意代码攻击； • 假冒软件。
外围接口	• 非授权访问； • 恶意代码攻击。
远程服务端	• DNS 劫持、内容劫持； • SQL 注入、XXS 攻击、非法访问； • 数据泄露； • DDOS 攻击，重放攻击，中间人攻击。
无线通信	• 通信数据泄露、篡改、丢失； • 传输中断、拦截、篡改、伪造； • DDOS 攻击，重放攻击，中间人攻击； • 虚假路由； • 通信协议漏洞。
家长&儿童数据	• 家长&儿童数据泄露； • 未经同意私自和过度采集用户数据。

4.2 安全能力框架

图2为儿童电话手表设备安全能力框架图，主要包括7个部分，最底层是设备硬件安全能力，之上为操作系统安全能力，其中外围接口安全能力涉及操作系统和硬件安全能力两个层面，再上为应用层安全能力，最顶层为远程服务器端&无线通信安全能力，家长&儿童数据保护安全能力涉及以上各个层面。

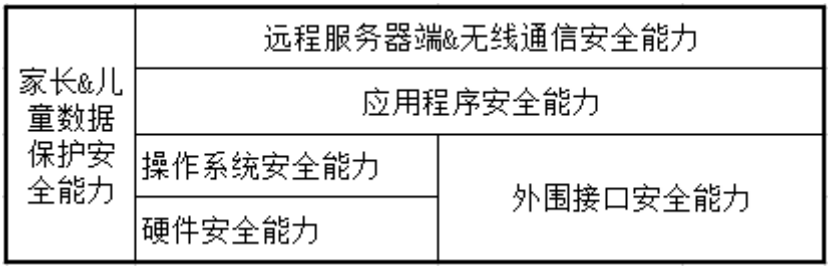

图 2 儿童电话手表设备安全能力框架图

4.3 安全目标

4.3.1 儿童电话手表硬件安全目标

儿童电话手表硬件安全目标一是保证材料器件本身的安全性，如材料、电磁、电池和可靠性等，切实保证儿童佩戴安全性；二是保障儿童电话手表使用的电路和芯片在实现数据运算和数据存储等功能时的安全性，能够对抗针对加解密操作的密码分析攻击、侧信道攻击、故障注入攻击等破坏数据保密性和完整性的安全威胁，保证儿童电话手表所存储的关键数据不被泄露或篡改。

4.3.2 儿童电话手表操作系统安全目标

操作系统安全目标是通过符合儿童电话手表应用场景的身份权限管理和访问控制机制，正确地响应授权操作和处理异常行为，达到操作系统对系统资源调用的监控、保护、提醒的目的，确保涉及安全的系统行为在受控状态下，不会出现用户未经授权的执行，或者用户不可控行为的执行。还需要保证儿童电话手表终端设备对要安装在其上的应用软件可进行来源的识别，对已经安装在其上的应用软件可以进行敏感行为的控制。另外还要确保预置在儿童电话手表设备中的应用软件无损害用户利益和危害网络安全的行为，例如：未经授权敏感信息采集、越权数据操作、向外传送用户数据等行为。最后操作系统还应保证自身的升级是受控的。

4.3.3 儿童电话手表外围接口安全目标

外围接口包括无线外围接口和有线外围接口。外围接口的安全目标是确保用户对外围接口的连接及数据传输的可知和可控。

4.3.4 儿童电话手表控制程序安全目标

手表控制程序安全目标是要保证控制程序在终端设备中运行的安全性，例如：对应用控制程序进行加固和签名，防止二次编译和假冒APP等恶意行为另外还应保证本地数据存储的安全性，例如：本地数据库、本地资源文件和缓存等。

4.3.5儿童手表服务器端安全目标

儿童电话手表远程服务器端安全目标是要保证服务器端遭受到攻击和破坏时也能正常提供服务，另外还需要保证服务器端数据的完整性和可用性，此外还需要保证遭受到意外如机房断电、业务异常等能够快速恢复服务。

4.3.6 儿童电话手表无线通信安全目标

无线通信安全目标是要保证儿童电话手表远程服务器端与控制程序APP和手表终端设备之间数据传输的机密性、完整性和真实性，采用必要数据加密和完整性校验等手段进行安全防护，且加密算法强度应满足国家相关规范，防止认证、标识、口令、隐私等敏感数据在无线传输过程中被获取甚至篡改。

4.3.7 儿童电话手表用户数据保护安全目标

用户数据保护安全目标是要保证用户数据的安全存储，确保用户数据不被非法访问、获取和篡改，同时能够通过安全备份机制保证用户数据的可靠恢复。

4.3.8 儿童电话手表终端设备能耗保护安全目标

终端设备能耗保护安全目标是要保证终端电池的正常、稳定消耗，避免由于外部的蓄意攻击而导致电池非预期耗尽。

5 安全能力技术要求

5.1 基本配置要求

5.1.1 儿童电话手表远程服务器端基本配置要求

与儿童电话手表控制程序和终端捆绑使用，承载控制程序和终端接入控制功能的服务器基本配置要求如下：

a) 应支持所连接应用设备的注册和管理；
b) 应支持所连接控制程序和终端运行状态收集上报，如设备标识、位置信息、固件版本、系统版本、网络类型、用户信息等；
c) 应支持对接入的控制程序和终端，实现软件升级、固件更新等功能；
d) 应支持对接入的控制程序和终端进行注销、禁用和锁定管理，当接入设备丢失时，登录、访问等敏感数据应被自动擦除，防止恶意利用。
e) 应配置 WAF 防火墙、主机入侵检测等安全防护手段。

5.1.2 儿童电话手表控制设备基本配置要求

儿童电话手表控制程序基本配置要求如下：

a) 应支持与儿童电话手表远程服务器端之间的通信认证和密钥协商功能；
b) 应支持与儿童电话手表远程服务器端之间的接入认证功能；

5.1.3 儿童电话手表终端基本配置要求

a) 应支持与儿童电话手表服务器之间的接入认证功能；
b) 应支持与儿童电话手表服务器之间的通信认证和密钥协商功能；

5.2 硬件安全能力

5.2.1 硬件功能安全

硬件功能实现应与提供给用户的用户手册相一致，不应存在未声明或隐藏的功能。例如应关闭隐藏调试功能，防止厂商在未获得用户授权的情况下获得对芯片内存的访问或芯片功能更改的能力。

5.2.2 硬件设计安全

硬件设计安全要求包括但不限于：

a) 硬件内部模块的安全属性和芯片间通信协议等安全敏感实现应不存在设计原理上的缺陷，例如由于随机数的随机性较差而导致的弱密钥等；
b) 密码算法的安全性应符合相关国家和行业标准要求，密钥的产生、分发、使用、存储、销毁应有相应安全保障机制。
c) 在非必要情况下，不在空口以明文方式广播真实终端信息，特别是能标识具体终端设备的 MAC 地址等信息。
d) 终端应具有防物理攻击能力，防止信息泄漏。攻击手段包括但不限于非侵入式攻击、半侵入式攻击和侵入式攻击；设备的加密模块支持防旁路攻击，以及抵抗错误注入攻击。

5.2.3 芯片安全能力

芯片安全能力要求包括但不限于：

a) 对于支持安全模块的芯片，应具备物理写保护的功能，防止固件代码、用户数据、密钥等敏感数据被篡改；
b) 宜具备安全启动硬件保护能力。
c) 芯片宜使用拆卸存迹硬质涂层，防止直接观察、探测芯片内容，并在企图拆卸或移动芯片后留下证据。

5.3 儿童电话手表操作系统安全能力

5.3.1 安全启动

在启动过程中，所有启动程序（例如引导程序、内核镜像、基带固件等）必须通过完整性校验才可以加载运行，防止加载并运行未经授权的恶意程序。

5.3.2 安全调用控制

安全调用控制能力要求包括但不限于：

a) 终端操作系统应具备用户授权的安全调用机制。在用户授权情况下，才可调用终端所连接的智能设备（如手机、平板电脑等）中的通讯录、短信、电话、邮件、及移动网络连接等功能。
b) 终端应提供机制，支持对所安装的第三方应用软件的调用行为进行配置，包括对拨打电话、发起三方通话、发送短信、接收短信、调用移动通信网络数据连接、调用定位功能、进行通话录音、本地录音、访问电话本、访问通话记录、访问日程表、访问短信和访问彩信等的控制。

5.3.3 应用程序安装

应用程序安装要求包括：

a）系统在应用安装时需要获得用户授权，未授权或被用户拒绝的应用，系统应拒绝安装；

b）若系统支持对未经认证签名的软件下载和安装，在进行应用软件安装前应能对应用软件的签名进行验证；

c）应用安装时，权限分配采取授权最小化原则，系统应能禁止所有未被允许权限的使用。

d）本章节不适用于不支持应用安装的儿童手表。

5.3.4 应用程序启动

应能防止未经授权或认证的的应用软件启动。

5.3.5 应用程序卸载

应用程序卸载要求包括：

a） 卸载应用软件必须卸载彻底，不应在系统中留下应用软件的临时文件和活动程序或模块；

b） 本章节不适用于不支持应用卸载的儿童手表。

5.3.6 安全日志记录及审计控制

安全日志记录及审计控制要求包括但不限于：

a） 宜具备记录用户对设备操作的能力，记录包括但不限于以下内容：用户对设备操作时所使用的帐号、操作时间、操作内容以及操作结果等；

b） 设备在异常关机、重启、文件系统损坏时产生的告警信息宜自动记入日志；

c） 对于具备文件系统的系统，应具备按帐号分配日志文件读取的能力，防止日志文件被非法读取。仅允许管理员帐号对日志文件进行删除操作；

d） 审计日志应具有循环机制，避免因为日志满而遗漏新事件记录。

5.3.7 系统更新机制

操作系统应具备更新机制，且更新前应得到用户确认，要求包括但不限于：

a） 系统更新时，应对更新文件的来源和完整性进行校验，并应具有原始数据备份能力，能够进行必要的回滚操作，避免更新失败导致系统失效，更新前是否备份可交由用户决定；

b） 系统更新失败时，应保证系统的可用性并给予用户相应的提示；

c） 系统应具备通过补丁或软件升级的方式消除或缓解高危及以上等级安全漏洞的能力。

5.3.10 预置应用软件安全要求

预装应用软件不应存在后门等隐藏接口，不应存在 CNVD、CNNVD 六个月之前公布的高危以上漏洞，不应含有非授权收集或泄露用户信息、非法数据外传等恶意行为。

5.4 应用控制程序安全能力

5.4.1 应用软件签名认证

应用软件签名认证机制要求包括但不限于：

a) 应对应用程序进行签名认证，确保软件的真实和完整性，防止恶意篡改。

b) 应对应用程序进行加壳加固，防止应用源码泄漏和二次打包。

5.4.2 应用软件数据安全要求

应用软件数据要求包括但不限于：

a) 应对应用程序资源文件、本地数据库和缓存等进行加密，且密码算法的安全性应符合相关国家和行业标准要求。

b) 应对应用程序缓存本地的日志文件做脱敏和加密处理，且密码算法的安全性应符合相关国家和行业标准要求。

5.5 外围接口安全能力

5.5.1 ADB

终端设备应关闭ADB端口或通过远程服务器端认证的方式打开ADB端口防止黑客恶意攻击破坏终端设备。

5.6 无线通信安全能力

5.6.1 协议安全一致性

所采用 WLAN、蓝牙、ZigBee 等无线通信协议应支持设备授权认证、加密传输等安全扩展功能，协议安全相关部分应正确实现与相关标准一致。

5.6.2 传输保密性

传输保密性要求包括但不限于：

a) 儿童电话手表终端设备、控制应用程序与服务端三者之间通信配对时应对密钥进行加密传输，防止密钥泄露；

b) 所采用安全协议，应符合国家相关标准规范，不能使用已被证实安全风险较高的安全协议，如 WEP 等；

c) 宜支持传输通道加密功能，使用安全传输层协议建立数据传输通道，且不得使用不安全的传输层协议，如 SSL3.0、TLS1.1 及以下，或使用 TLS1.2 中的弱密码套件。

d) 宜支持媒体内容加密功能，对敏感的视频、音频和消息内容进行加密，且不得使用不安全的密码算法和杂凑算法，如 AES-ECB、DES、RC4、SHA-1、MD5 等。

5.7 家长&儿童数据保护安全能力

家长&儿童数据保护安全能力包括但不限于：

a) 儿童电话手表控制程序对用户数据中个人信息的收集应取得家长明示同意不仅限于 APP 启动时弹窗等方式，应向家长提供个人信息收集撤回同意功能且撤回同意后数据采集应立即停止。

b) 儿童电话手表终端设备采集 14 岁以下儿童数据时应取得家长端明示同意，应向家长提供撤回同意功能且撤回同意后数据采集应立即停止。

c) 儿童电话手表终端设备在将位置、健康等个人信息存储在终端内部时，应为保存个人信息的文件设置适当的权限，以防止未授权的访问。存储生物特征等敏感个人信息时，应安全存储或进行数据隔离等要求；

d) 儿童电话手表终端设备若通过公共网络传输用户数据，应对数据进行加密，确保信息在网络传输过程中的安全；

e) 儿童电话手表控制程序不应有未向家长明示且未经用户同意，擅自修改个人信息的行为，且控制程序应提供账户注销功能，账户注销后用户数据应删除或做匿名化处理。

6 测试评估方法

6.1 总体说明

测试方法与技术要求一一对应，在技术要求中，每条技术要求对应的测试评价由检测方法和预期结果组成。

6.2 儿童电话手表硬件安全测试评价方法

6.2.1 硬件功能安全

硬件功能安全的测评方法和结果判定如下：

a) 检测方法：

1) 审查厂商提交的用户手册，查看硬件功能实现是否与用户手册一致。

2) 审查厂商提交的文档，查看是否存在未声明或隐藏的功能，检查具备调试功能的接口，在出场时是否设置为默认关闭状态。

b) 结果判定：

1) 硬件功能实现是否与用户手册一致。满足为“符合”，其他情况为“不符合”。

2) 硬件功能不存在未声明或隐藏功能，调试功能接口关闭。满足为“符合”，其他情况为“不符合”。

6.2.2 硬件设计安全

硬件设计安全的检测方法和结果判定如下：

a) 检测方法：

1) 审查厂商提交的文档，查看硬件内部模块实现，安全属性和通信协议等安全敏感实现是否存在设计缺陷。

2) 审查厂商提交的文档，查看密码算法的安全性设计，是否符合国家或行业标准要求，使用安全保障机制保护密钥生产、分发、使用、存储、销毁等过程。

3) 审查厂商提交的文档，查看数据传输功能，是否在空口以明文方式广播终端信息，如终端设备的 MAC 地址等。

b) 结果判定：

1) 硬件内部模块安全敏感实现不存在设计缺陷。满足为“符合”，其他情况为“不符合”。

2) 密码算法的安全性设计符合国家或行业标准要求，满足为“符合”，其他情况为“不符合”。

3) 在非必要情况下，不在空口以明文方式广播真实终端信息。满足为“符合”，其他情况为“不符合”。

6.2.3 芯片安全能力

芯片安全的检测方法和结果判定如下：

a) 检测方法：

1) 对于支持安全模块的芯片，尝试篡改芯片内部固件数据，验证固件芯片是否具有物理写保护的功能。

2) 审查厂商提交的文档，查看芯片是否使用拆卸存迹硬质涂层，可以防止直接观察、探测芯片内容，并在企图拆卸或移动芯片后留下证据。

3) 审查厂商提交的文档，查看出厂前是否擦除主控芯片表面的型号、厂商等信息，增加破解难度。

4) 审查厂商提交的文档，查看是否具备安全启动硬件保护能力。

b) 结果判定：

1) 支持安全模块的芯片，固件芯片具有物理写保护的功能，防止固件被篡改。满足为“符合”，其他情况为“不符合”。

2) 芯片使用拆卸存迹硬质涂层，防止直接观察、探测芯片内容，并在企图拆卸或移动芯片后留下证据。满足为“符合”，其他情况为“不符合”。

3) 出厂前擦除主控芯片表面的型号、厂商等信息，增加破解难度；满足为“符合”，其他情况为“不符合”。

4) 具备安全启动硬件保护能力。满足为“符合”，其他情况为“不符合”。

6.3 儿童电话手表操作系统安全测试评价方法

6.3.1 安全启动

操作系统安全启动认证的检测方法和结果判定如下：

a) 检测方法：

1) 审查厂商提交的文档，查看儿童电话手表是否具有安全启动机制；在非授权的条件下修改启动分区，重新启动操作系统；检查修改的代码是否可以通过完整性验证。

b) 结果判定：

1) 儿童电话手表具有安全启动机制，在非授权的条件下修改启动分区，重新启动操作系统，修改后的代码不能通过完整新验证，系统无法正常启动。满足为“符合”，其他情况为“不符合”。

6.3.2 安全调用控制

操作系统权限限制的检测方法和结果判定如下：

a) 检测方法：

1) 创建多个用户账户，验证用户权限分配是否遵循最小权限原则，普通用户是否只拥有系统赋予的最小权限，尝试越权操作，该越权操作是否被禁止。单用户系统不适用。

2) 在系统上申请安装应用，验证是否需要获得用户授权才能安装；如果用户未授权或者用户拒绝安装该应用，系统是否拒绝安装应用。在应用安装时，验证权限分配是否采取授权最小化原则，系统是否禁止所有未被允许权限的使用。

3) 当不同的应用进程或数据之间进行访问时，验证系统是否具有访问控制机制，不同应用程序的进程及数据是否禁止随意互访。

4) 审查厂商提交的文档，查看系统是否禁止预留任何的未公开帐号，所有帐号都必须可被操作系统管理。

5) 审查厂商提交的文档，查看是否禁止存在绕过正常认证机制直接进入到系统的隐秘通道，如：特定接口、特定客户端、特殊 URL 等。

b) 结果判定：

1) 对于支持多个用户账户的系统，用户权限分配遵循最小权限原则，普通用户只拥有系统赋予的最小权限，禁止越权操作。满足为“符合”，其他情况为“不符合”。

2) 系统在应用安装时需要获得用户授权，未授权或被用户拒绝的应用，系统拒绝安装。应用安装时，权限分配采取授权最小化原则，系统可以禁止所有未被允许权限的使用。满足为“符合”，其他情况为“不符合”。

3) 系统对不同的应用进程及数据之间实施适当的访问控制管理，不同应用程序的进程及数据不能随意互访。满足为“符合”，其他情况为“不符合”。

4) 系统禁止预留任何的未公开帐号，所有帐号都必须可被操作系统管理。满足为“符合”，其他情况为“不符合”。

5) 禁止存在绕过正常认证机制直接进入到系统的隐秘通道，如：特定接口、特定客户端、特殊 URL 等。满足为“符合”，其他情况为“不符合”。

6.3.3 应用程序安装

应用程序安装的检测方法和结果判定如下：

a) 检测方法：

1) 检查儿童电话手表是否支持应用程序安装。

2) 尝试在设备中安装应用程序，检查应用安装时系统是否需要获得用户授权，未授权或被用户拒绝的应用，检查系统是否拒绝安装。

3) 审查厂商提交的文档，检查系统是否支持对未经认证签名的软件下载和安装，若支持，检查软件安全前是否对应用软件的签名进行验证。

4) 尝试在设备中安装应用程序，检查各权限分配是否采取授权最小化原则，当权限未被允许时，检查系统是否可使用此权限。

b) 结果判定

1) 设备支持应用安装。满足则继续测评，不满足则结束此项测评

2) 安装应用时系统需要获得用户授权，用户拒绝应用安装后，系统拒绝此应用安装。满足为“符合”，其他情况为“不符合”。

3) 系统支持对未经认证签名的软件下载和安装时，应用软件安全前系统会对应用软件的签名进行验证。满足为“符合”，其他情况为“不符合”。
4) 应用程序安装符合授权最小化原则，当权限未被允许是，系统不可使用此权限。满足为“符合”，其他情况为“不符合”。

6.3.4 应用程序启动

应用程序启动的检测方法和结果判定如下：

a) 检测方法：
   1) 审查厂商提供的文档，检查是否存在安全机制防止未经授权或认证的应用软件启动。
b) 结果判定
   1) 存在安全机制防止未经授权或认证的应用软件启动。满足则继续测评，不满足则结束此项测评。
   2) 满足第一步的条件下，查看未经授权或认证的应用软件是否能启动，满足为“符合”，其他情况为“不符合”。

6.3.5 应用程序卸载

应用程序卸载的检测方法和结果判定如下：

a) 检测方法：
   1) 检查儿童电话手表是否支持应用卸载。
   2) 若支持应用卸载，在儿童电话手表上卸载应用程序，评估其是否能完全卸载，即没有可执行代码或者不必要的文件驻留在终端。
b) 结果判定
   1) 设备支持应用卸载。满足则继续测评，不满足则结束此项测评
   2) 卸载应用软件后，应用图标、应用进程等可执行代码或不必要的文件是否完全删除。满足为“符合”，其他情况为“不符合”。

6.3.6 安全日志记录及审计控制

日志安全的检测方法和结果判定如下：

a) 检测方法：
   1) 当用户对设备进行操作时，检查是否进行了日志记录，记录内容是否至少包含用户对设备操作时所使用的帐号、操作时间、操作内容以及操作结果，且记录应符合 GB/T 35273-2020 中对个人信息的安全要求。
   2) 检查设备在异常关机、重启、文件系统损坏时产生的告警信息，是否自动记入日志。
   3) 检查设备当为日志分配的存储空间耗尽时，是否按操作系统用户的设置决定采取的措施，包括报警并丢弃未记录的信息、暂停日志录入、覆盖以前的日志等。

b) 结果判定：
   1) 当用户对设备进行操作时，设备对其进行了日志记录，记录内容至少包含用户对设备操作时所使用的帐号、操作时间、操作内容以及操作结果，且记录应符合 GB/T 35273-2020 中对个人信息的安全要求。满足为“符合”，其他情况为“不符合”。

2) 设备在异常关机、重启、文件系统损坏时产生的告警信息，自动记入日志。满足为“符合”，其他情况为“不符合”。
3) 当为日志分配的存储空间耗尽时，可按操作系统用户的设置决定采取的措施，包括报警并丢弃未记录的信息、暂停日志录入、覆盖以前的日志等。满足为“符合”，其他情况为“不符合”。

6.3.7 系统更新机制

操作系统更新安全机制的检测方法和结果判定如下：

a) 检测方法：
1) 审查厂商提交的文档，查看操作系统是否具有自动或者手动更新功能；如果具有自动更新功能，在授权的条件下，检查是否可以自动更新操作系统；如果具有手动更新功能，在授权的条件下，检查是否可以手动更新操作系统。
2) 修改更新文件的来源，在授权的条件下，进行系统更新，检查是否可以通过校验，完成更新；修改更新文件的内容，在授权的条件下，进行系统更新，检查是否可以通过完整性校验，完成更新。
3) 尝试推送不正确的固件给设备，使升级失败，验证设备是否恢复到之前可用的版本，并提示更新失败的信息。
4) 审查厂商提交的文档，查看操作系统是否具备通过补丁或软件升级的方式消除高危及以上等级安全漏洞的能力。

b) 结果判定：
1) 操作系统具备自动或者手动更新功能，通过自动或者手动，能够实现操作系统升级。满足为“符合”，其他情况为“不符合”。
2) 修改更新文件的来源，在授权的条件下，进行系统更新，未通过校验，更新失败；修改更新文件的内容，在授权的条件下，进行系统更新，未通过校验，更新失败。满足为“符合”，其他情况为“不符合”。
3) 推送不正确的固件给设备，使升级失败，设备可以恢复到之前可用的版本，并提示更新失败的信息。满足为“符合”，其他情况为“不符合”。
4) 操作系统具备通过补丁或软件升级的方式消除高危及以上等级安全漏洞的能力。满足为“符合”，其他情况为“不符合”。

6.3.8 预置应用软件安全要求

预置应用软件安全的检测方法和结果判定如下：

a) 检测方法：
1) 使用检测工具检测预置应用软件是否存在 CNVD、CNNVD 六个月之前公布的高危以上漏洞。验证是否具备根据新曝光漏洞自动或手动安装升级补丁的能力。
2) 运行预置应用软件，如果应用软件在使用过程中需要收集与用户敏感信息，如用户名、密码、银行账号、身份证信息等数据，评估其是否在明示用户且经用户确认后执行，该评估过程可在控制程序或终端设备实现。
3) 检查预置应用软件是否具有读取用户电话本数据、通话记录、短信、定位等信息的权限或功能。直接运行或通过其他方式唤醒应用程序，评估各上传行为是否明示且要求用户确认

b) 结果判定：

1) 使用检测工具检测预置应用软件不存在 CNVD、CNNVD 六个月之前公布的高危以上漏洞。且验证具备根据新曝光漏洞自动或手动安装升级补丁的能力。满足为“符合”，其他情况为“不符合”。
2) 预置应用软件收集用户敏感信息前明示了用户，且用户可以有效确认或拒绝，确认过程可以在控制程序或终端设备完成。满足为“符合”，其他情况为“不符合”。
3) 若被测预置应用软件具备上传用户电话本、通话记录、短信、定位等行为，软件向用户明示且要求用户确认。满足为“符合”，其他情况为“不符合”。

6.4 应用控制程序安全能力测试评价方法

应用控制程序安全能力的检测方法和结果判定如下：

a) 检测方法：
1) 检查应用是否具备防伪冒、防应用二次打包/篡改、防逆向反编译等能力。
2) 尝试越权操作，检查是否可以操作；尝试非法身份操作，检查是否可以操作。
3) 检查在日志和配置文件中，是否明文记录设备密码、设备认证信息等关键安全信息。
4) 与儿童电话手表应用服务平台进行数据交互时，检查在通信时是否采用安全网络协议。
5) 检查是否具有防止身份验证数据被暴力攻击的能力。
6) 检查是否具备对输入数据格式的恶意代码检验能力，输入不安全的数据，是否会进行过滤处理。
7) 审查厂商提交的文档，查看是否禁止使用业界已知的不安全的密码算法。
8) 审查厂商提交的文档，查看是否具备应用安全事件的实时监测和应用审计能力。

b) 结果判定：
1) 应用具备防伪冒、防应用二次打包/篡改、防逆向反编译等能力。满足为“符合”，其他情况为“不符合”。
2) 对应用进行越权操作，操作失败；使用非法身份操作，操作失败。满足为“符合”，其他情况为“不符合”。
3) 在日志和配置文件中，对设备密码、设备认证等关键安全信息进行加密存储。满足为“符合”，其他情况为“不符合”。
4) 与儿童电话手表应用服务平台进行数据交互时，在通信时采用安全网络协议。满足为“符合”，其他情况为“不符合”。
5) 具有防止身份验证数据被暴力攻击的能力。满足为“符合”，其他情况为“不符合”。
6) 具备对输入数据格式的恶意代码检验能力，输入不安全的数据，会进行过滤处理。满足为“符合”，其他情况为“不符合”。
7) 禁止使用业界已知的不安全的密码算法。满足为“符合”，其他情况为“不符合”。
8) 具备应用安全事件的实时监测和应用审计能力。满足为“符合”，其他情况为“不符合”。

6.5 儿童电话手表外围接口安全测试评价方法

6.5.1 ADB

ADB 的检测方法和结果判定如下：

a) 检测方法：

1) 调试终端 ADB 端口，检查在默认情况下 ADB 端口是否为关闭状态，并不可开启或可通过远程服务器认证方式打开 ADB 端口。

b) 结果判定：

1) 默认情况下终端 ADB 端口为关闭状态，并不可开启或可通过远程服务器认证方式打开 ADB 端口。满足为“符合”，其他情况为“不符合”。

6.6 无线通信安全测试评价方法

6.6.1 协议安全一致性

协议安全一致性的检测方法和结果判定如下：

a) 检测方法：

1) 检查设备采用的 WLAN、蓝牙、ZigBee 等无线通信协议是否支持设备授权认证、加密传输等安全扩展功能。

2) 检查设备协议安全部分实现是否与相关标准一致。

b) 结果判定

1) 设备采用的通信协议支持设备授权认证、加密传输等安全扩展功能。满足为“符合”，其他情况为“不符合”。

2) 设备协议安全部分实现与相关标准一致。满足为“符合”，其他情况为“不符合”。

6.6.2 传输保密性

传输保密性的检测方法和结果判定如下：

a) 检测方法：

1) 审查厂商提交的文档，查看通信配对时，儿童电话手表终端、控制应用程序和服务端三者之间是否具备对密钥加密传输的保护能力

2) 检查采用的安全协议是否符合国家相关标准规范。

3) 审查厂商的产品技术文档，是否提供安全传输层协议来建立传输通道；配置安全传输层协议后，通过网络抓包检查，判断是否使用不被认可的协议或密码套件。

4) 审查厂商的产品技术文档，是否具备媒体内容加密模块，是否使用安全的加密算法和模式；配置媒体加密后，通过终端检测和网络抓包，判断是否实现安全的加密算法和模式。

b) 结果判定

1) 儿童电话手表终端、控制应用程序和服务端三者之间具备密钥加密传输的能力。满足为“符合”，其他情况为“不符合”。

2) 安全协议符合国家相关标准规范。满足为“符合”，其他情况为“不符合”。

3) 具备认可的安全传输层协议功能且有效实现。满足为“符合”，其他情况为“不符合”。

4) 具备认可的媒体内容加密功能且有效实现。满足为“符合”，其他情况为“不符合”。

6.7 家长&儿童数据保护安全能力测试评价方法

家长&儿童数据保护安全的检测方法和结果判定如下：

a) 检测方法：

1） 查看厂商提供的控制程序收集家长数据是否提前征得同意，且撤回同意后是否立即停止收集数据。
2） 查看厂商提供的终端设备收集儿童数据是否取得家长端应用控制程序明示同意，且撤回同意后是否立即停止收集数据。
3） 查看厂商提供数据管理制度和数据存储等，是否多敏感数据设置权限和单独存放等安全隔离措施。
4） 查看厂商提供控制程序和终端设备在数据传输过程中是否采用加密或者 HTTPS 等安全传输措施。
5） 查看厂商提供的控制程序是否未经允许私自修改个人信息，账户注销后是否还能继续登录或保留用户个人信息，匿名化除外。

b） 结果判定：

1） 厂商控制程序有明示同意等提示且撤回同意后停止收集数据。满足为“符合”，其他情况为“不符合”。
2） 厂商提供证明敏感数据授权访问和安全隔离措施。满足为“符合”，其他情况为“不符合”。
3） 通过相关技术手段不仅限于抓包等查看是否采用安全的传输方法传输用户数据。满足为“符合”，其他情况为“不符合”。
4） 无未经允许修改个人信息且账户注销后不能继续登录使用，无其他个人信息留存。满足为“符合”，其他情况为“不符合”。

参 考 文 献

[1] YD/T2407-2013 移动智能终端安全能力技术要求
[2] GB/T 35273-2020 信息安全技术个人信息安全规范
[3] GB/T 34975-2017 信息安全技术移动智能终端应用软件安全技术要求和测试评价方法
[4] GB/T 22239-2019 信息安全技术网络安全等级保护基本要求
[5] YD/T 1699-2007 移动终端信息安全技术要求
[6] YD/T 1760-2012 数字移动终端外围接口数据交换技术要求
[7] YD/T 3228-2017 移动应用软件安全评估方法
[8] YD/T 3082-2016 移动智能终端上的个人信息保护技术要求

电信终端产业协会团体标准

智能可穿戴设备安全 儿童电话手表安全技术要求和测试评估方法

T/TAF 087-2021

*

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