ICS 33.050
M 30

团　体　标　准

T/TAF 064-2020

智能音箱产品安全能力技术要求和测试方法

Technical Requirements and Test Methods for Security Capabilities of Smart Speaker

2020-08-24 发布　　2020-08-24 实施

电信终端产业协会　发布

目　　次

前　言

本标准按照 GB/T 1.1-2009给出的规则编写。

本标准中的某些内容可能涉及专利。本标准的发布机构不承担识别这些专利的责任。

本标准由电信终端产业协会提出并归口。

本标准起草单位：中国信息通信研究院、北京百度网讯科技有限公司、北京奇虎科技有限公司、阿里巴巴(中国)有限公司

本标准主要起草人：刘陶、宁华、王剑、李笑如、周飞、杜云、王艳红、武林娜、黄天宁、孙伟超、王海棠、吴月升、唐佳伟

智能音箱产品安全能力技术要求和测试方法

1. 范围

本标准规定了智能音箱安全能力技术要求和测试方法，包括硬件安全能力、操作系统安全能力、应用层安全能力、通信安全能力及用户数据安全保护能力，并对安全能力进行了分级，制定了相应的测试方法。

本标准适用于提供互联网内容服务的智能音箱设备。

本标准适用于智能音箱的设计、开发、测试和评估。

本标准仅提出智能音箱安全能力技术要求和测试方法，对具体技术实现方式不作规定。

2. 规范性引用文件

下列文件对于本标准的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本标准。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本标准。

GB/T 35273	个人信息安全规范
YD/T 2407-2013	移动智能终端安全能力技术要求
YD/T 2408-2013	移动智能终端安全能力测试方法
YDB 201-2018	智能家居终端设备安全能力技术要求

3. 术语、定义和缩略语

3.1. 术语和定义

3.1.1.

智能音箱 smart speaker

以音箱为载体，利用计算机网络、互联网、音视频等技术，具备语音识别、语音交互、自然语言理解、语音合成等功能，能够为用户提供信息等服务的设备。

3.1.2.

智能音箱操作系统 operator system of smart speaker

智能音箱最基本的系统软件，提供控制和管理智能音箱各种硬件和软件资源的能力，并提供其上运行的应用程序的开放接口。

3.1.3.

应用软件 application software

智能音箱内，能够利用智能音箱操作系统提供的开发接口，实现某项或某几项特定任务的计算机程序或代码片段。包含智能音箱预置应用软件，以及互联网信息服务提供者提供的可以通过网站、应用商店等移动应用分发平台下载、安装、升级的应用软件。

3.1.4.

预置应用 pre-installed application

智能音箱内，在主屏幕和辅助屏界面（不包含进入界面后，通过菜单进入或者调起的功能）有用户交互入口并且可独立使用的应用软件。

3.1.5.

第三方应用 third-party application

指非智能音箱厂商或与互联网信息服务提供者合作在智能音箱出厂前安装在其系统中的应用软件，以及非系统升级时新增加的应用软件。

3.1.6.

用户 user

使用智能音箱资源的自然人。

3.1.7.

用户数据 user data

智能音箱上存储的用户信息，包括由用户在本地生成的数据、为用户在本地生成的数据、在用户许可后由外部进入用户数据区的数据等。

3.1.8.

控制单元 control unit

进行用户和音箱指令交互的单元。

注：通过控制单元，用户可以操控智能音箱，如开启、关闭音箱，或者下载应用等。控制单元可能部署在移动智能终端上，也可能部署在云端上。

3.1.9.

隐藏语音命令 hidden voice command

由攻击者发出，对用户来说无法理解，但可以被设备理解的指令。

3.2. 缩略语

下列缩略语适用于本文件。

API	应用程序编程接口	Application Programming Interface
APP	应用	Application

AI	人工智能	Artificial Intelligence
CNVD	国家信息安全漏洞共享平台	China National Vulnerability Database
CNNVD	中国国家信息安全漏洞库	China National Vulnerability Database of Information Security
CPU	中央处理器	Central Processing Unit
HTTP	超文本传输协议	Hyper Text Transfer Protocol
HTTPS	以安全为目标的 HTTP 通道	Hyper Text Transfer Protocol over Secure Socket Layer
ROM	只读内存	Read Only Memory
SQL	结构化查询语言	Structured Query Language
SSL	安全套接层	Secure Socket Layer
TEE	可信执行环境	Trusted Execution Environment
TLS	安全传输协议	Transport Layer Security
Web	万维网	World Wide Web
WLAN	无线局域网	Wireless Local Area Networks

4. 智能音箱安全架构

4.1. 概述

图1为智能音箱安全能力框架，主要包含5个部分：最底层是智能音箱硬件安全能力，之上为操作系统安全能力，顶层为应用层安全能力和控制端安全能力，通信安全能力及上述4个层面，用户数据安全保护能力涉及上述5个层面。

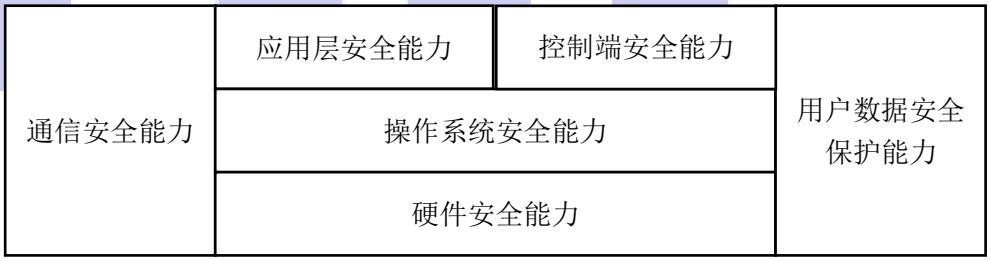

图 1. 智能音箱产品安全能力框架

其中：

a) 硬件安全能力：在芯片级保障智能音箱存储及处理芯片安全，避免芯片内的操作系统、数据、程序等被非法获取或者篡改；

b) 操作系统安全能力：操作系统包含常规智能操作系统，以及嵌入智能操作系统中提供相应开放接口供应用程序（框架应用程序，如免安装应用等）使用的框架。操作系统安全能力是确保操作系统自身无损害用户利益和危害网络及终端的行为，以及提供操作系统对系统资源的监控、保护和提醒，确保涉及安全的系统行为总是在受控的状态下，不会出现用户在不知情的情况下执行某种行为，或者在用户不可控的情况下执行某种行为；

c) 应用层安全能力：应用层安全能力是要保证智能音箱对要安装在其上的应用程序可进行来源的识别，对已经安装或加载在其上的应用程序可以进行敏感行为的控制。另外，还要确保预置在智能音箱中的应用程序无损害用户利益和危害网络或终端安全的行为；

d) 控制端安全能力：控制段安全能力是要保证智能音箱控制端软硬件安全以及控制端与服务器、控制端与音箱之间的传输安全；

e) 通信安全能力：保障智能音箱采用的 WLAN、蓝牙等通信协议安全能力满足相应的国家标准或标准组织规定。此外，应确保用户对外围接口的连接及数据传输的可知和可控；

f) 用户数据安全保护能力：用户数据安全保护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、不被非法获取、不被非法篡改。

5. 智能音箱安全能力技术要求

5.1. 基本要求

智能音箱应通过给用户提示和让用户确认的方式来防范安全威胁，当操作系统自身或第三方应用调用相关功能时，操作系统应具备给用户提示和让用户确认的能力。

本章所提及的给用户提示和用户确认，除明确声明外，均指由系统自身或者第三方应用调用相关功能时，操作系统所应具备的能力。对于第三方应用通过调用操作系统提供的人—机接口执行的操作，认为是在用户知情的情况下执行的操作，已经给用户提示并得到用户的确认。

给用户的提示可以是图标、文字、语音或其他明显的提示方式。在操作执行期间，提示应足够引起用户的注意。对于不具备主界面的智能音箱，应在控制单元进行用户提示和确认或在说明书中提供详细说明。

用户确认应使用户有选择的权利，即用户应能确认也能取消。

若用户使用语音交互控制操作系统或第三方应用调用相关功能，则认为用户已进行确认。

用户确认如无特别说明，则认为以下三种确认方式均可：

— 应用软件每一次调用行为发生时进行确认；

— 应用软件首次调用行为发生时确认，本确认在一定时间内有效，确认应针对每一个调用行为单独确认；

— 应用软件首次安装或调用行为发生时确认，本确认对该软件长期有效，确认应针对每一个调用行为单独确认。

对于应用软件安全配置中用户设置为允许访问的操作，也认为是在用户知情的情况下执行的操作，已经得到用户的确认。

对于移动通信网络连接、无线局域网络连接、无线外围接口的开启操作在任何情况下都应给用户提示并经用户确认。

5.2. 硬件安全能力

5.2.1. 可调试物理接口安全

a) 智能音箱可调式物理接口配置为限制使用，访问时需进行认证；

b) 智能音箱保留可调式物理接口，非拆机状态下不可访问；

c) 智能音箱保留可调式物理接口，采用一定的物理方式对接口进行保护，如去除部分接口器件，使调试接口不可用。

5.2.2. 硬件存储安全

a) 应支持对存储芯片内固件的签名和签名验证；

b) 硬件平台应具备用于存储校验密钥等敏感信息的安全存储区域。

5.2.3. 防物理攻击

a) 智能音箱密码模块应具备抵抗物理攻击能力，防止密钥或加解密操作过程数据的泄漏。攻击手段包括但不限于旁路攻击和故障注入攻击。

5.2.4. 根密钥生成与保护

a) 若智能音箱存在根密钥，则根密钥应随机生成实现一机一密；

b) 根密钥应存储并运行于软硬件安全区域内，如白盒、TEE、安全芯片等，不可被非授权访问。

5.3. 操作系统安全能力

5.3.1. 调用控制安全能力

5.3.1.1. 通信类功能受控机制

a) 应用软件调用通信类功能时，应遵照 YD/T 2407 要求在用户确认的情况下执行操作，通信类功能包括但不限于拨打电话、三方通话、发送短信、发送邮件。

5.3.1.2. 网络连接

a) 应用软件调用开启网络连接功能时，智能音箱应提供开关，可开启/关闭网络连接；或智能音箱支持用户使用语音交互的方式控制网络连接开关；

b) 应给用户相应的提示，当用户确认后连接方可开启；

c) 当网络连接处于已连接状态，若智能音箱具备图像人机交互界面，则应在图像人机交互界面上给用户相应的状态提示；若智能音箱不具备图像人机交互界面，则应通过控制端或说明书中说明等方式提示用户当前数据连接状态；

d) 当网络正在传送数据时，智能音箱应给与用户一定的状态提示。

5.3.1.3. 本地敏感功能受控机制

a) 应用软件调用定位功能时，智能音箱应在用户确认的情况下才能调用；

b) 通话录音是指在通话状态下录取线路上双方的话音。当应用软件调用通话录音时，应在用户确认的情况下才能开启；

c) 应用软件或操作系统调用本地录音功能时，应在用户确认的情况下才能启动录音操作。若用户通过语音明确发出录音指令，则认为已经进行了用户确认；

d) 后台截屏是指应用软件后台运行时截取前台屏幕内容。当应用软件调用后台截屏时，应在用户确认的情况下才能启动截屏操作；

e) 对于具备摄像头的智能音箱，当应用软件启动拍照或摄像功能时，智能音箱应给用户相应的提示（图像预览、指示灯、声音或图标等），在用户确认的情况下方可执行拍照或摄像操作；

f) 智能音箱应提供接收短信控制能力，应用软件调用接收短信控制功能应在用户确认的情况下执行。

5.3.2. 安全启动

a) 智能音箱应对安全启动代码进行完整性验证，当验证通过后执行安全启动过程。

5.3.3. 系统配置安全

a) 智能音箱应关闭非必要远程访问控制接口。

5.3.4. 系统与固件更新安全

a) 进行系统与固件更新时，应对更新文件的来源和完整性进行校验，包括验证更新包的文件大小、版本号和签名；

b) 进行系统与固件更新，当发生更新失败时，不应出现系统不可用的情况；

c) 应不支持在线的从高版本的操作系统降级到低版本的操作系统；

d) 进行系统与固件更新时，应对更新包文件进行加密。

5.3.5. 漏洞修复

a) 系统出厂时应保证不包含有 CNVD 与 CNNVD 6 个月前公布的高危漏洞；

b) 应通过升级、更新等手段，支持紧急系统缺陷及漏洞的修复。

5.3.6. 端口安全

a) 默认开启防火墙按需进行服务端口的打开或放系统端口时进行访问控制。

5.3.7. 对抗性攻击防护

a) 智能音箱语音识别功能应具备抵抗对抗性攻击的能力，如隐藏语音攻击。

5.3.8. 机器学习模型安全

a) 应对机器学习模型进行安全保护，以保护机器学习模型不被非法窃取；

b) 机器学习模型参数或预测 API 接口应具备一定的访问控制机制，不可被公开获取，保护 AI 模型安全。

5.4. 应用层安全能力

5.4.1. 应用软件安全配置能力要求

智能音箱或智能音箱控制单元可提供机制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、发送彩信、开启移动通信网络数据连接开关、开启WLAN网络连接开关、开启无线外围接口开关、调用移动通信网络数据连接、调用WLAN网络连接、调用无线外围接口、开启通话录音、开启本地录音、后台截屏、拍照/摄像、读取用户本机号码、读取电话本数据、读取通话记录、读取短信数据、读取上网记录、读取日程表数据、读取定位信息、读取媒体影音数据（如照片、视频和音频）、读取生物特征识别信息（如指纹识别、人脸识别等）、读取设备唯一可识别信息、读取应用软件列表、删除或修改用户电话本数据、删除或修改通话记录、删除或修改短信数据、删除或修改日程表数据的行为。

对以上调用行为进行控制至少有允许调用和禁止调用两种状态。推荐允许调用、每次调用时询问用户和禁止调用3种状态。对于应用软件升级前后共有的调用行为，智能音箱应保证其安全配置状态在升级前后一致。

5.4.2. 软件安装安全

a) 应不允许安装未签名应用或者不受信任的代码，禁止自动安装第三方应用软件；
b) 若支持安装第三方开发者功能或应用，则应确保安装包的完整性和来源的真实性；或智能音箱不支持安装第三方开发者功能或应用；
c) 预置应用软件不应存在后门的隐藏接口，不应存在 CNVD 和 CNNVD 三个月前公布的高危漏洞。

5.4.3. 软件更新安全

a) 预置应用进行更新时，应对更新包进行版本号、签名和文件大小校验；
b) 进行预置应用软件更新时，应对软件更新包进行加密。

5.4.4. 预置应用软件安全要求

5.4.4.1. 收集用户数据

预置应用软件不应有未向用户明示且未经用户同意，擅自收集用户个人信息的行为。

5.4.4.2. 修改用户数据

预置应用软件不应有未向用户明示且未经用户同意，擅自修改用户个人信息的行为。

5.4.4.3. 用户数据录入保护

支付类预置应用软件输入认证/支付密码等敏感信息时，需采取技术措施防止密码被截获，并不得在智能音箱界面上显示明文。

5.5. 通信安全能力

5.5.1. 外围接口安全能力要求

5.5.1.1. 外围接口开启/关闭受控机制

对于具备蓝牙功能的智能应具备开关，可开启/关闭蓝牙等终端所支持的无线连接方式。

5.5.1.2. 外围接口连接建立的确认机制

当通过外围接口（仅适用于蓝牙）与不同设备进行第一次连接时，智能音箱能够发现该连接并给用户相应的提示，当用户确认建立连接时，连接才可建立。

5.5.1.3. 外围接口数据传输的受控机制

当智能音箱与其他设备已经通过外围接口（如蓝牙）实现连接，此时通过无线外围接口进行文件数据传输时，智能音箱应给用户相应的提示。

5.5.2. 数据传输安全

a) 智能音箱应支持对控制端的身份认证，以防止非授权的操作；
b) 智能音箱应支持与云平台、家居设备和控制单元之间的双向身份认证；
c) 智能音箱应使用安全传输协议对通过公共网络传输的用户数据，进行机密性及完整性保护；
d) 应抵抗因编程语言固有缺陷造成的安全漏洞，如使用可抵抗内存安全漏洞的传输层安全协议。

5.5.3. 上传数据安全

a) 应通过将上传服务器地址设置为不可配置等方法，防止攻击者将用户使用人工智能功能时的交互数据上传指向非授权地址。

5.6. 控制端安全保护能力要求

5. 6. 1. 控制端应用安全

a) 控制端应用应符合 YD/T 3228-2017《移动应用软件安全评估方法》标准相应级别要求。

5.6.2. 控制端设备安全

a) 控制端设备应符合 YD/T 2407《移动智能终端安全能力技术要求》标准相应级别要求。

5.7. 用户数据安全保护能力要求

5.7.1. 智能音箱用户数据安全保护基本要求

a) 智能音箱操作系统和应用软件收集、使用用户数据的，应当明确告知用户收集、使用信息的目的、方式和范围，查询、更正信息的渠道以及拒绝提供信息的后果等事项。
b) 智能音箱操作系统和应用软件不得收集其提供服务所必需以外的用户数据或者将数据用于提供服务之外的目的，不得以欺骗、误导或者强迫等方式或者违反法律、行政法规以及双方的约定收集、使用信息。
c) 智能音箱操作系统和应用软件在用户终止使用电信服务或者互联网信息服务后，应当停止对用户个人信息的收集和使用，并为用户提供注销号码或者账号的服务。

5.7.2. 文件类用户数据授权访问

若智能音箱提供文件类用户数据的授权访问能力，则第三方应用访问被保护的用户数据时，应在用户确认的情况下才能访问。文件类用户数据包括图片、视频、音频和文档等。

5.7.3. 用户数据的存储安全

未经授权的任何实体应不能从智能音箱的加密存储区域的数据中还原出用户数据的真实内容。

5.7.4. 用户个人信息的共享、转让

a) 智能音箱在进行用户个人信息共享、转让之前，应事先征得用户的授权同意。共享、转让经去标识化处理的个人信息，且确保数据接收方无法重新识别个人信息主体的除外；
b) 个人信息控制者应准确记录和保存个人信息的共享、转让情况，包括共享、转让的日期、规模、目的，以及数据接收方基本情况等。

5.7.5. 用户数据的彻底删除

智能音箱提供数据彻底删除功能，以保证被删除的用户数据不可再恢复出来。

6. 智能音箱安全能力测试方法

6.1. 硬件安全能力测试项

6.1.1. 可调试物理接口安全测试

6.1.1.1. 测试项 HW-1

测试评价内容：

智能音箱可调式物理接口配置为限制使用，访问时需进行认证。

测试评价方法：

a) 审查厂商提交的文档，查看被测智能音箱接口设计；
b) 模拟用户通过调试命令连接可调式物理接口；查看是否对用户身份进行识别和校验。

测试评价结果：

a) 若可调式物理接口对访问行为进行了限制，则本项判为合格。

测试评价等级：

一级、二级。

6.1.1.2. 测试项 HW-2

测试评价内容：

智能音箱保留可调式物理接口，非拆机状态下不可访问。

测试评价方法：

a) 审查厂商提交的文档，查看被测智能音箱接口设计；

b) 模拟用户通过调试命令连接可调式物理接口，查看是否可访问。

测试评价结果：

a) 若非拆机状态下，可调试物理接口不可访问，则本项判为合格。

测试评价等级：

三、四级。

6.1.1.3. 测试项 HW-3

测试评价内容：

智能音箱保留可调式物理接口，采用一定的物理方式对接口进行保护，如去除部分接口器件，使调试接口不可用。

测试评价方法：

a) 审查厂商提交的文档，查看被测智能音箱接口设计；

b) 将音箱进行硬件拆分，检查是否不存在可用的接口或者串口可对设备进行连接调试。

测试评价结果：

a) 若不存在可对设备调试的接口或者串口，则本项判为合格；

测试评价等级：

五级。

6.1.2. 硬件存储安全测试

6.1.2.1. 测试项 HS-1

测试评价内容：

应支持对存储芯片内固件的签名和签名验证。

测试评价方法：

a) 审查厂商提交的文档，查看存储芯片固件安全设计；

b) 模拟攻击者修改操作系统引导分区文件，将修改后的引导分区文件刷入操作系统，查看系统是否允许刷入。

测试评价结果：

a) 若不可以刷入修改后的引导分区文件，则本项判为合格。

测试评价等级：

三级、四级、五级。

6.1.2.2. 测试项 HS-2

测试评价内容：

硬件平台应具备用于存储校验密钥等敏感信息的安全存储区域。

测试评价方法：

a) 审查厂商提交的文档，查看智能音箱采用的安全芯片型号；

b) 核查该安全芯片是否具备安全存储区。

测试评价结果：

a) 若智能音箱采用的安全芯片存在安全存储区，则本项判为合格。

测试评价等级：

五级。

6.1.3. 防物理攻击安全测试

测试评价内容：

智能音箱密码模块应具备抵抗物理攻击能力，防止密钥或加解密操作过程数据的泄漏。攻击手段包括但不限于旁路攻击和故障注入攻击。

测试评价方法：

a) 审查厂商提交的文档，验证厂商已声明硬件具有防护非侵入、半侵入和侵入式等物理攻击的能步力；

b) 通过实验验证关键硬件具有抵抗旁路攻击、错误注入攻击的能力，旁路攻击包括但不限于—简单功耗分析（SPA）、差分功耗分析（DPA）、相关功耗分析（CPA）、电磁辐射分析（EMA）、模板分析等，错误注入攻击包括但不限于—时钟毛刺分析、电压毛刺分析、光信号分析、电磁信号分析等；

c) 查看是否存在信息泄漏，包括但不限于密钥。

测试评价结果：

a) 若智能音箱密码模块具备抵抗物理攻击的能力，则本项判为合格。

测试评价等级：

五级

6.1.4. 根密钥生成与保护安全测试

6.1.4.1. 测试项 KEY-1

测试评价内容：

a) 若智能音箱存在根密钥，则根密钥应随机生成实现一机一密。

测试评价方法：

a) 审查厂商提交的文档，验证厂商已声明根密钥随机生成并保证一机一密。

测试评价结果：

a) 若智能音箱根密钥随机生成且保证一机一密，则本项判为合格。

测试评价等级：

二、三、四、五级。

6.1.4.2. 测试项 KEY-2

测试评价内容：

a) 根密钥应存储并运行于软硬件安全区域内，如白盒、TEE、安全芯片等，不可被非授权访问。

测试评价方法：

a) 审查厂商提交的文档，查看根密钥的是否存储并运行于软硬件安全区域内，如白盒、TEE、安全芯片等，不可被非授权访问。

测试评价结果：

a) 若智能音箱根密钥存储并运行于安全区域，则本项判为合格。

测试评价等级：

四、五级。

6.2. 操作系统安全能力测试项

6.2.1. 调用控制安全能力

6.2.1.1. 通信类受控机制测试

参考 YD/T 2408 《移动智能终端安全能力测试方法》 4.3.1.1.1 ，4.3.1.1.2,4.3.1.1.3,4.3.1.1.4,4.3.1.1.5执行。

测试评价等级：

一、二、三、四、五级。

6.2.1.2. 网络连接测试

6.2.1.2.1. 测试项 NC-1

测试评价内容：

a) 应用软件调用开启网络连接功能时，智能音箱应提供开关，可开启/关闭网络连接；或智能音箱支持用户使用语音交互的方式控制网络开关；

b) 应给用户相应的提示，当用户确认后连接方可开启。

测试评价方法：

a) 查看智能音箱是否提供开关或语音交互的方式，开启/关闭网络数据连接；

b) 查看智能音箱开启网络数据连接功能时，是否给用户相应提示；

c) 验证是否只有用户确认后连接方可开启。

测试评价结果：

a) 若智能音箱提供开启/关闭通信网络数据连接功能，开启网络连接功能时会给用户相应提示，且只有用户确认后连接方可开启，则本项判为合格。

测试评价等级：

一、二、三、四、五级。

6.2.1.2.2. **测试项** NC-2

测试评价内容：

当网络连接处于已连接状态，若智能音箱具备图像人机交互界面，则应在图像人机交互界面上给用户相应的状态提示；若智能音箱不具备图像人机交互界面，则应通过控制端或说明书中说明等方式提示用户当前数据连接状态。

测试评价方法：

a) 将智能音箱设置为移动通信网络数据连接状态；

b) 查看主界面或其它方式，提示了当前数据连接状态。

测试评价结果：

a) 若智能音箱具备移动通信网络数据连接状态提示，则本项判为合格。

测试评价等级：

二、三、四、五级。

6.2.1.2.3. **测试项** NC-3

测试评价内容：

当网络正在传送数据时，智能音箱应给与用户一定的状态提示。

测试评价方法：

a) 将智能音箱设置为移动通信网络数据连接状态，并开启应用向外传输数据；

b) 查看主界面或其它方式，提示了当前数据传送状态。

测试评价结果：

a) 若智能音箱具备移动通信网络数据传送状态提示，则本项判为合格。

测试评价等级：

一、二、三、四、五级。

6.2.1.3. **本地敏感功能受控机制测试**

6.2.1.3.1. 测试项 LS-1

测试评价内容：

a) 应用软件调用定位功能时，智能音箱应在用户确认的情况下才能调用；
b) 通话录音是指在通话状态下录取线路上双方的话音。当应用软件调用通话录音时，应在用户确认的情况下才能开启；
c) 应用软件或操作系统调用本地录音功能时，应在用户确认的情况下才能启动录音操作。若用户通过语音明确发出录音指令，则认为已经进行了用户确认。

参考YD/T 2408 《移动智能终端安全能力测试方法》4.3.1.2.1，4.3.1.2.2,4.3.1.2.3,执行。

测试评价等级：

一、二、三、四、五级。

6.2.1.3.2.…测试项 LS-2

测试评价内容：

后台截屏是指应用软件后台运行时截取前台屏幕内容。当应用软件调用后台截屏时，应在用户确认的情况下才能启动截屏操作。

测试评价方法：

a) 查看被测智能音箱是否提供后台截屏功能；
b) 查看智能音箱提供后台截屏功能，是否给与用户相应提示；
c) 验证是否只有用户明确同意之后，才会使用后台截屏功能。

测试评价结果：

a) 若智能音箱提供后台截屏功能，使用该功能时会给与用户一定的提示，且只有在用户明确同意时才会启用该功能，则本项判定合格；
b) 若智能音箱不提供后台截屏功能，则该项判定合格。

测试评价等级：

一、二、三、四、五级。

6.2.1.3.3. 测试项 LS-3

测试评价内容：

a) 对于具备摄像头的智能音箱，当应用软件启动拍照或摄像功能时，智能音箱应给用户相应的提示（图像预览、指示灯、声音或图标等），在用户确认的情况下方可执行拍照或摄像操作；
b) 智能音箱应提供接收短信控制能力，应用软件调用接收短信控制功能应在用户确认的情况下执行。

参考YD/T 2408 《移动智能终端安全能力测试方法》4.3.1.2.4，4.3.1.2.5执行。

测试评价等级：

一、二、三、四、五级。

6.2.2. 安全启动测试

测试评价内容：

智能音箱应对安全启动代码进行完整性验证，当验证通过后执行安全启动过程。

测试评价方法：

a) 审查厂商提交的文档，查看被智能音箱是否具有安全启动机制；
b) 在非授权的条件下修改启动分区，重新启动操作系统；
c) 检查修改的代码是否可以通过完整性验证。

测试评价结果：

a) 若非授权条件下修改的代码不能通过完整性验证，则本项判为合格。

测试评价等级：

三级、四级、五级。

6.2.3. 系统配置安全测试

测试评价内容：

智能音箱应关闭非必要远程访问控制接口。

测试评价方法：

a) 审查厂商提交的文档，查看被测智能音箱是否开启了非必要远程访问控制接口；
b) 使用接口扫描工具对智能音箱进扫描，查看是否能在用户不允许的情况下开启非必要远程访问控制接口。

测试评价结果：

a) 若非必要远程登陆接口默认关闭，则本项判为合格。

测试评价等级：

一级、二级、三级、四级、五级。

6.2.4. 系统与固件更新安全测试

6.2.4.1. 测试项 OS-1

测试评价内容：

进行系统与固件更新时，应对更新文件的来源和完整性进行校验，包括验证更新包的文件大小、版本号和签名。

测试评价方法：

a) 审查厂商提交的文档，查看被测智能音箱是否提供了系统与固件更新时的完整性校验功能；
b) 模拟攻击者在未授权的情况下进行系统与固件更新包进行修改，查看是否可以成功刷入；
c) 模拟攻击者通过劫持替换系统与固件更新包，查看伪造的系统与固件更新包是否被刷入。

测试评价结果：

a) 若步骤测试方法 b)和 c)均不可成功刷入修改或替换后的系统与固件更新包，则本项判为合格。

测试评价等级：

一级、二级、三级、四级、五级。

6.2.4.2. 测试项 OS-2

测试评价内容：

进行系统与固件更新，当发生更新失败时，不应出现系统不可用的情况。

测试评价方法：

a) 审查厂商提交的文档，查看被测智能音箱是否提供了系统与固件更新失败时的处理机制；
b) 模拟终端进行系统与固件更新失败操作，查看智能音箱是否进入到系统不可用的状态。

测试评价结果：

a) 若智能音箱有相应的机制，在系统与固件更新失败时，可防止终端进入到系统不可用的状态，则本项判为合格。

测试评价等级：

一级、二级、三级、四级、五级。

6.2.4.3. 测试项 OS-3

测试评价内容：

应不支持在线的从高版本的操作系统降级到低版本的操作系统。

测试评价方法：

a) 审查厂商提交的文档，查看被测智能音箱是否提供了在线从高版本的操作系统降级到低版本的操作系统的机制；
b) 模拟用户尝试通过在线方式刷入低版本的系统包，查看是否可以成功刷入。

测试评价结果：

a) 若用户不可以通过在线方式刷入低版本的系统包，则本项判为合格

测试评价等级：

五级。

6.2.4.4. 测试项 OS-4

测试评价内容：

进行系统与固件更新时，应对更新包文件进行加密。

测试评价方法：

a) 审查厂商提交的文档，查看被测智能音箱是否提供对系统与固件更新包加密的功能；

b) 对系统与固件更新包进行解析，检查是否可以获取正常的文件格式。

测试评价结果：

a) 若对系统与固件更新包进行解析后，不可以获取正常的文件格式，则本项判为合格。

测试评价等级：

五级。

6.2.5. 漏洞修复安全测试

6.2.5.1. 测试项 LX-1

测试评价内容：

系统出厂时应保证不包含有CNVD与CNNVD 6个月前公布的高危漏洞。

测试评价方法：

a) 使用已知漏洞自动检测工具，对所有音箱设备进行漏洞扫描；
b) 结合 CNVD 与 CNNVD 漏洞库，判断是否存在 6 个月前公布的高危漏洞。

测试评价结果：

a) 进行漏洞扫描后，若不存在 6 个月前公布的高危漏洞，则本项判为合格。

测试评价等级：

一级、二级、三级、四级、五级。

6.2.5.2. 测试项 LX-2

测试评价内容：

应通过升级、更新等手段，支持紧急系统缺陷及漏洞的修复。

测试评价方法：

a) 审查厂商提交的文档，查看是否开启防火墙；
b) 检测智能音箱是否存在紧急系统缺陷的解决方法。

测试评价结果：

a) 若厂商提供系统缺陷及漏洞的及时修复机制且系统不存在两周内的紧急系统缺陷，则本项判为合格。

测试评价等级：

三级、四级、五级。

6.2.6. 端口安全测试

测试评价内容：

默认开启防火墙按需进行服务端口的打开或放系统端口时进行访问控制。

测试评价方法：

a) 审查厂商提交的文档，查看是否支持服务端口按需打开或访问控制机制；
b) 使用接口扫描工具对智能音箱进行扫描，检查所有开启的接口是否存在可疑行为，是否可以访问可疑端口。

测试评价结果：

a) 若不存在开启的可疑端口，或访问可疑端口需要进行访问控制，则本项判为合格。

测试评价等级：

四级、五级。

6.2.7. 对抗性攻击防护安全测试

测试评价内容：

智能音箱语音识别功能应具备抵抗对抗性攻击的能力，如隐藏语音攻击。

测试评价方法：

a) 模拟攻击者，尝试进行隐藏语音命令攻击操作，如使用大于 20KHZ 的超声波，查看是否可以控制智能音箱执行相应的操作。

测试评价结果：

a) 若智能音箱不可执行相应操作，则本项判为合格。

测试评价等级：

五级。

6.2.8. 机器学习模型安全测试

6.2.8.1. 测试项 MS-1

测试评价内容：

应对机器学习模型进行安全保护，以保护机器学习模型不被非法窃取。

测试评价方法：

a) 审查厂商提交的文档，查看智能音箱是否采用了安全机制对机器学习模型进行了保护；
b) 尝试利用公共访问接口的方式，对智能音箱机器学习模型进行构造。

测试评价结果

a) 若不可成功构造智能音箱机器学习模型，则本项判为合格。

测试评价等级：

五级。

6.2.8.2. 测试项MS-2

测试评价内容：

机器学习模型参数或预测 API 接口应具备一定的访问控制机制，不可被公开获取，保护 AI 模型安全。

测试评价方法：

a) 检查厂商提交的文档，查看智能音箱是否采用了安全机制对机器学习模型进行了保护；

b) 尝试利用公共访问接口的方式，对智能音箱机器学习模型进行构造。

测试评价结果:

a) 在步骤 a)之后，若未进行安全保护，测评结果为“不符合要求”，测评结束；否则进行步骤 b)；

b) 在步骤 b)之后，若未能进行成功构造模型算法，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

测试评价等级：

五级。

6.3. 应用层安全能力测试项

6.3.1. 应用软件安全配置能力要求

参考YD/T 2408 《移动智能终端安全能力测试方法》4.5.1执行。

测试评价等级：

四级、五级。

6.3.2. 软件安装安全测试

6.3.2.1. 测试项 AP-1

测试评价内容：

应不允许安装未签名应用或者不受信任的代码，禁止自动安装第三方应用软件。

测试评价方法：

a) 审查厂商提交的文档，智能音箱是否提供第三方应用安装能力；

b) 检测系统设置选项中是否默认关闭未知来源安装，不存在静默安装接口。

测试评价结果：

a) 若智能音箱不提供第三方应用安装能力，则本项判为合格；

b) 若智能音箱默认关闭未知来源安装且不存在静默安装接口，则本项判为合格。

测试评价等级：

一级、二级、三级、四级、五级。

6.3.2.2. 测试项 AP-2

测试评价内容：

若支持安装第三方开发者功能或应用，则应确保安装包的完整性和来源的真实性；或智能音箱不支持安装第三方开发者功能或应用。

测试评价方法：

a) 审查厂商提交的文档，查看智能音箱是否提供第三方应用安装能力；
b) 在未授权的情况下对第三方应用安装包进行修改，查看是否可以成功安装第三方应用；
c) 通过 DNS 劫持或 HTTP 劫持替换第三方应用安装包，或伪造安装包，查看是否可以成功安装第三方应用。

测试评价结果：

a) 若智能音箱不提供第三方应用安装能力，则本项判为合格；
b) 若测试评价方法 b)和 c)均不可成功安装第三方应用，则本项判为合格。

测试评价等级：

一级、二级、三级、四级、五级。

6.3.2.3. 测试项 AP-3

测试评价内容：

预置应用软件不应存在后门的隐藏接口，不应存在 CNVD 和 CNNVD 三个月前公布的高危漏洞。

测试评价方法：

a) 使用自动化扫描工具扫描并验证智能音箱预置应用是否存在 CNVD 和 CNNVD 三个月前公布的高危漏洞。

测试评价结果：

a) 若扫描后，确认智能音箱不存在 CNVD 和 CNNVD 三个月前公布的高危漏洞，则本项判为合格。

测试评价等级：

四级、五级。

6.3.3. 软件更新安全测试

6.3.3.1. 测试项 AU-1

测试评价内容：

预置应用进行更新时，应对更新包进行版本号、签名和文件大小校验。

测试评价方法：

a) 审查厂商提交的文档，查看智能音箱是否提供预置应用能力；

b) 逆向分析预置软件更新包的代码，查看是否对预置软件进行了签名等完整性保护措施；

c) 劫持替换预置应用软件的更新包，查看修改后的更新包是否可以安装。

测试评价结果：

a) 若智能音箱不提供预置应用能力，则本项判为合格；

b) 若在测试方法 b）中提供了完整性保护措施，且测试方法 c）不可安装修改后的更新包，则本项判为合格。

测试评价等级：

二级、三级、四级、五级。

6.3.3.2. 测试项 AU-2

测试评价内容：

进行预置应用软件更新时，应对软件更新包进行加密。

测试评价方法：

a) 审查厂商提交的文档，查看智能音箱是否提供预置应用能力；

b) 对软件预置更新包进行解析，检查是否可以获取正常的文件格式。

测试评价结果：

a) 若智能音箱不提供预置应用能力，则本项判为合格；

b) 若在测试方法 b）中不可获取正常的预置软件更新包格式，则本项判为合格。

测试评价等级：

五级。

6.3.4. 收集用户数据测试

参考YD/T 2408 《移动智能终端安全能力测试方法》4.5.4.1执行。

测试评价等级：

一级、二级、三级、四级、五级。

6.3.5. 修改用户数据测试

参考YD/T 2408 《移动智能终端安全能力测试方法》4.5.4.2执行。

测试评价等级：

一级、二级、三级、四级、五级。

6.3.6. 用户数据录入保护测试

测试评价内容：

支付类预置应用软件输入认证/支付密码等敏感信息时，需采取技术措施防止密码被截获，并不得在智能音箱界面上显示明文。

测试评价方法：

a) 查看智能音箱中预置应用软件中是否存在支付类的应用软件；

b) 若存在支付类预置应用软件，查看在该软件进行输入认证/支付密码等敏感信息时，是否采取了技术措施防止密码被截获，且在智能音箱界面上是否不显示敏感信息或者对敏感信息进行加密处理。

测试评价结果：

a) 若智能音箱不存在支付类预置应用软件，则该项判定合格；

b) 若智能音箱存在支付类预置应用软件，在进行敏感信息输入时对该信息进行保护措施，且在终端界面上无法显示敏感信息或者敏感信息进行加密处理，则该项判定合格。

测试评价等级：

四级、五级。

6.4. 通信安全能力测试项

6. 4. 1. 外围接口安全能力要求测试

6.4.1.1. 外围接口开启/关闭受控机制测试

参考YD/T 2408 《移动智能终端安全能力测试方法》4.4.1.1执行。

测试评价等级：

一级、二级、三级、四级、五级。

6.4.1.2. 外围接口连接建立的确认机制测试

参考YD/T 2408 《移动智能终端安全能力测试方法》4.4.1.2执行。

测试评价等级：

一级、二级、三级、四级、五级。

6.4.1.3. 外围接口数据传输的受控机制测试

参考YD/T 2408 《移动智能终端安全能力测试方法》4.4.1.4执行。

测试评价等级：

三级、四级、五级。

6.4.2. 数据传输安全测试

6.4.2.1. 测试项 WC-1

测试评价内容：

智能音箱应支持对控制端的身份认证，以防止非授权的操作。

测试评价方法：

a) 审查厂商提交的文档，查看智能音箱是否具备对控制端的认证功能；
b) 在未进行智能音箱对控制端身份认证的情况下，通过控制端操作智能音箱，查看是否可以成功。

测试评价结果：

a) 若在未进行智能音箱对控制端身份认证的情况下，不可通过控制端操作智能音箱，则本项判为合格。

测试评价等级：

一级、二级、三级、四级、五级。

6.4.2.2. 测试项 WC-2

测试评价内容：

智能音箱应支持与云平台、家居设备和控制单元之间的双向身份认证。

测试评价方法：

a) 审查厂商提交的文档，查看是否具备智能音箱与云平台、家居设备和控制单元之间的双向身份认证功能；
b) 在未进行智能音箱对控制端双向身份认证的情况下，进行智能音箱与控制端之间的交互，查看是否可以成功。

测试评价结果：

a) 若在未进行双向身份认证的情况下，不可进行智能音箱与控制端之间的交互，则本项判为合格。

测试评价等级：

三级、四级、五级。

6.4.2.3. 测试项 WC-3

测试评价内容：

智能音箱应使用安全传输协议对通过公共网络传输的用户数据，进行机密性及完整性保护。

测试评价方法：

a) 审查厂商提交的文档，查看智能音箱是否采用安全机制对公共网络传输的用户数据进行了机密性及完整保护；
b) 功在用户进行数据采集功能时，进行网络抓包，检查是否对传输的用户数据进行机密性和完整性保护。

测试评价结果：

a) 解析抓取的网络数据包，若对数据进行了机密性和完整性保护，则符合要求。

测试评价等级：

一级、二级、三级、四级、五级。

6.4.2.4. 测试项 WC-4

测试评价内容：

应抵抗因编程语言固有缺陷造成的安全漏洞，如使用可抵抗内存安全漏洞的传输层安全协议。

测试评价方法：

a) 审查厂商提交的文档，查看智能音箱的传输层安全协议实现是否采用了一定机制避免因编程语言固有缺陷造成的安全漏洞；
b) 使用因编程语言固有缺陷造成的安全漏洞对传输层安全协议进行攻击，查看是否造成用户信息泄漏。

测试评价结果：

a) 若使用测试评价方法 b)对传输层协议进行攻击，而未造成用户信息泄漏，则本项判为合格。

测试评价等级：

三级、四级、五级。

6.4.3. 上传数据安全测试

测试评价内容：

应通过将上传服务器地址设置为不可配置等方法，防止攻击者将用户使用人工智能功能时的交互数据上传指向非授权地址。

测试评价方法：

a) 审查厂商提交的文档，查看智能音箱是否采用了安全机制防止攻击者将数据上传到自己的服务器；
b) 模拟攻击者，尝试修改数据上传服务器地址，查看是否可以成功接收到用户数据。

测试评价结果：

a) 若不可成功接收到用户数据，则本项判为合格。

测试评价等级：

三级、四级、五级。

6.5. 控制端安全保护能力要求测试项

6.5.1. 控制端应用安全测试

测试评价内容：

控制端应用应符合 YD/T 3228-2017《移动应用软件安全评估方法》标准相应级别要求。

测试评价方法：

a) 查看客户是否能提供 YD/T 3228-2017《移动应用软件安全评估方法》相应级别的符合性证明。

测试评价结果：

a) 如能提供，则本项判为合格。

测试评价等级：

一、二、三、四、五级。

6.5.2. 控制端设备安全测试

测试评价内容：

控制端应用应符合 YD/T 2407《移动智能终端安全能力技术要求》标准相应级别要求。

测试评价方法：

a) 查看客户是否能提供 YD/T 2407《移动智能终端安全能力技术要求》相应级别的符合性证明。

测试评价结果：

a) 如能提供，则本项判为合格。

测试评价等级：

一、二、三、四、五级。

6.6. 用户数据安全保护能力要求测试项

6.6.1. 智能音箱用户数据安全保护基本要求测试

6.6.1.1. 测试项 YHB-1

测试评价内容：

a) 智能音箱操作系统和应用软件收集、使用用户数据的，应当明确告知用户收集、使用信息的目的、方式和范围，查询、更正信息的渠道以及拒绝提供信息的后果等事项。

测试评价方法：

a) 检查智能音箱操作系统和应用软件收集、使用用户数据的，是否明确告知用户收集、使用信息的目的、方式和范围，查询、更正信息的渠道以及拒绝提供信息的后果等事项。

测试评价结果：

a) 如能提供，则本项判为合格。

测试评价等级：

一、二、三、四、五级。

6.6.1.2. 测试项 YHB-2

测试评价内容：

智能音箱操作系统和应用软件不得收集其提供服务所必需以外的用户数据或者将数据用于提供服务之外的目的，不得以欺骗、误导或者强迫等方式或者违反法律、行政法规以及双方的约定收集、使用信息。

测试评价方法：

a) 检查智能音箱操作系统和应用软件是否收集其提供服务所必需以外的用户数据或者将数据用于提供服务之外的目的，不得以欺骗、误导或者强迫等方式或者违反法律、行政法规以及双方的约定收集、使用信息

测试评价结果：

a) 如能提供，则本项判为合格。

测试评价等级：

一、二、三、四、五级。

6.6.1.3. 测试项 YHB-3

测试评价内容：

智能音箱操作系统和应用软件在用户终止使用电信服务或者互联网信息服务后，应当停止对用户个人信息的收集和使用，并为用户提供注销号码或者账号的服务。

测试评价方法：

a) 查看智能音箱操作系统和应用软件在用户终止使用电信服务或者互联网信息服务后，是否停止对用户个人信息的收集和使用，并为用户提供注销号码或者账号的服务。

测试评价结果：

a) 如能提供，则本项判为合格。

测试评价等级：

一、二、三、四、五级。

6.6.2. 文件类用户数据授权访问测试

测试评价内容：

若智能音箱提供文件类用户数据的授权访问能力，则第三方应用访问被保护的用户数据时，应在用户确认的情况下才能访问。文件类用户数据包括图片、视频、音频和文档等。

测试评价方法：

a) 将图片、视频、音频和文档等文件类用户数据的授权访问功能进行加密保护；

b) 使用第三方应用软件尝试访问被保护的图片、视频、音频和文档；

c) 使用数据线连接 PC，采用多种方式修改破解加密文件。

测试评价结果：

a) 在步骤 b）：在用户确认后第三方应用软件可访问被保护的图片、视频、音频和文档；

b) 在步骤 c）：文件无法被正常访问；

c) 如果满足以上预期结果，则该项目评测结果为“未见异常”，反之该项目评测结果为“不符合要求”。

测试评价等级：

三、四、五级。

6.6.3. 用户数据的存储安全测试

测试评价内容：

未经授权的任何实体应不能从智能音箱的加密存储区域的数据中还原出用户数据的真实内容。

测试评价方法：

a) 将智能音箱的应用数据存储于加密存储区；

b) 将加密后的应用数据采用未授权方式导出到其他设备（如本地计算机）上，用文本编辑软件打开并查看器是否以密文方式存储。

测试评价结果：

a) 在步骤 b），使用文本编辑软件应无法还原应用文件；

b) 满足以上预期结果，则该项目评测结果为“未见异常”，反之该项目评测结果为“不符合要求”。

测试评价等级：

三、四、五级。

6.6.4. 用户个人信息的共享、转让测试

6.6.4.1. 测试项 GX-1

测试评价内容：

智能音箱在进行用户个人信息共享、转让之前，应事先征得用户的授权同意。共享、转让经去标识化处理的个人信息，且确保数据接收方无法重新识别个人信息主体的除外；

测试评价方法：

a) 若个人信息进行共享或转让时，测尝试转移个人信息，查看是否在用户的授权同意后，才进行用户数据共享、转让；

b) 检查厂商提供的文档，检查个人信息是否经去标识化处理后共享、转让，且确保数据接收方

无法重新识别个人信息主体的除外。

测试评价结果：

a) 如能提供，则本项判为合格。

测试评价等级：

二、三、四、五级。

6.6.4.2. 测试项 GX-2

测试评价内容：

个人信息控制者应准确记录和保存个人信息的共享、转让情况，包括共享、转让的日期、规模、目的，以及数据接收方基本情况等。

测试评价方法：

a) 检查智能音箱是否准确记录和保存个人信息的共享、转让情况；
b) 如果存在记录，检查记录内容是否包括共享、转让的日期、规模、目的，以及数据接收方基本情况等。

测试评价结果：

a) 如能提供，则本项判为合格。

测试评价等级：

二、三、四、五级。

6.6.5. 用户数据的彻底删除测试

测试评价内容：

智能音箱提供数据彻底删除功能，以保证被删除的用户数据不可再恢复出来。

测试评价方法：

a) 在智能音箱中预先存入测试数据，使用数据读取工具对用户存储介质进行原始数据的读取；
b) 通过智能音箱的彻底删除功能对用户数据执行彻底删除操作；
c) 再次使用数据读取工具对用户存储介质进行数据读取。

测试评价结果：

a) 如能提供，则本项判为合格。

测试评价等级：

四、五级。

7. 智能音箱安全能力分级

7.1. 概述

智能音箱所支持的安全能力划分为 5 个等级，第五级是最高等级。智能音箱可选支持到不同的等级。达到相应等级的智能音箱应在说明书上进行明确的标识，参见附录 A 的内容。

7.2. 安全能力分级

根据智能音箱所支持的安全能力的程度，将智能音箱安全能力自低到高划分为5个等级。在每一等级定义了智能音箱在相应等级对应的安全能力的最小集合，也就是智能音箱必须支持该集合中的所有安全能力才能标识为该级别，例如：达到第五级的智能音箱应支持本标准第5张所定义的所有安全能力。具体的等级划分详见表1。

表1 智能音箱安全能力分级

安全能力		安全能力等级				
		一级	二级	三级	四级	五级
1	5.2.1 可调式物理接口安全 a)	√	√			
2	5.2.1 可调式物理接口安全 b)			√	√	
3	5.2.1 可调式物理接口安全 c)					√
4	5.2.2 硬件存储安全 a)			√	√	√
5	5.2.2 硬件存储安全 b)					√
6	5.2.3 防物理攻击 a)					√
7	5.2.4 根密钥生成与保护 a)		√	√	√	√
8	5.2.4 根密钥生成与保护 b)				√	√
9	5.3.1.1 通信类功能受控机制 a)	√	√	√	√	√
10	5.3.1.2 网络连接 a)	√	√	√	√	√
11	5.3.1.2 网络连接 b)	√	√	√	√	√
12	5.3.1.2 网络连接 c)		√	√	√	√
13	5.3.1.2 网络连接 d)	√	√	√	√	√
14	5.3.1.3 本地敏感功能受控机制 a)	√	√	√	√	√
15	5.3.1.3 本地敏感功能受控机制 b)	√	√	√	√	√
16	5.3.1.3 本地敏感功能受控机制 c)	√	√	√	√	√
17	5.3.1.3 本地敏感功能受控机制 d)	√	√	√	√	√
18	5.3.1.3 本地敏感功能受控机制 e)	√	√	√	√	√
19	5.3.1.3 本地敏感功能受控机制 f)	√	√	√	√	√
20	5.3.2 安全启动 a)			√	√	√
21	5.3.3 系统配置安全 a)	√	√	√	√	√
22	5.3.4 系统与固件更新安全 a)	√	√	√	√	√
23	5.3.4 系统与固件更新安全 b)	√	√	√	√	√
24	5.3.4 系统与固件更新安全 c)					√
25	5.3.4 系统与固件更新安全 d)					√
26	5.3.5 漏洞修复 a)	√	√	√	√	√
27	5.3.5 漏洞修复 b)			√	√	√
28	5.3.6 端口安全 a)				√	√

29	5.3.7 对抗性攻击防护 a)					√
30	5.3.8 机器学习模型安全 a)					√
31	5.3.8 机器学习模型安全 b)					√
32	5.4.1 应用软件安全配置能力要求				√	√
33	5.4.2 软件安装安全 a)	√	√	√	√	√
34	5.4.2 软件安装安全 b)	√	√	√	√	√
35	5.4.2 软件安装安全 c)				√	√
36	5.4.3 软件更新安全 a)		√	√	√	√
37	5.4.3 软件更新安全 b)					√
38	5.4.4.1 收集用户数据	√	√	√	√	√
39	5.4.4.2 修改用户数据	√	√	√	√	√
40	5.4.4.3 用户数据录入保护				√	√
41	5.5.1.1 外围接口开启/关闭受控机制	√	√	√	√	√
42	5.5.1.2 外围接口连接建立的确认机制	√	√	√	√	√
43	5.5.1.3 外围接口数据传输的受控机制			√	√	√
44	5.5.2 数据传输安全 a)	√	√	√	√	√
45	5.5.2 数据传输安全 b)			√	√	√
46	5.5.2 数据传输安全 c)	√	√	√	√	√
47	5.5.2 数据传输安全 d)			√	√	√
48	5.5.3 上传数据安全 a)			√	√	√
49	5.6.1 控制端应用安全	√	√	√	√	√
50	5.6.2 控制端设备安全	√	√	√	√	√
51	5.7.1 智能音箱用户数据安全保护基本要求 a)	√	√	√	√	√
52	5.7.1 智能音箱用户数据安全保护基本要求 b)	√	√	√	√	√
53	5.7.1 智能音箱用户数据安全保护基本要求 c)	√	√	√	√	√
54	5.7.2 文件类用户数据的访问授权			√	√	√
55	5.7.3 用户数据的存储安全			√	√	√
56	5.7.4 用户个人信息的共享、转让 a)		√	√	√	√
57	5.7.4 用户个人信息的共享、转让 b)		√	√	√	√
58	5.7.5 用户数据的彻底删除				√	√

电信终端产业协会团体标准

智能音箱产品安全能力技术要求和测试方法

T/TAF 064-2020

*

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