ICS 33.050
CCS M 30

团　体　标　准

T/TAF 193—2023

酒店民宿行业智能对话设备信息安全技术要求

Information security technique requirements of smart dialogue devices for hotel and homestay industry

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：百度在线网络技术（北京）有限公司、中国信息通信研究院、联想（北京）有限公司、郑州信大捷安信息技术股份有限公司、中国电信股份有限公司广东研究院、蚂蚁科技集团股份有限公司、北京京东世纪贸易有限公司。

本文件主要起草人：远超、穆亚敏、王振杰、袁琦、王海棠、夏良钊、闫晗、郭建领、于欢、张宏星、田琛、李汝鑫、林巍巍、刘献伦、康亮、邹一心、骆媛媛、李明扬、龚昕羽、林冠辰、李然。

酒店民宿行业智能对话设备信息安全要求

1 范围

本文件规定了酒店民宿行业智能对话设备的信息安全技术要求，包括应用设备安全、网络传输安全、控制安全、数据与隐私安全和安全运营要求。

本文件涉及的酒店民宿行业智能对话设备包含有语音对话功能的智能无屏音箱、智能有屏音箱、智能中控屏等。

本文件适用于酒店民宿行业智能对话设备的研发、测试、验收和运维。

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 35273—2020 信息安全技术 个人信息安全规范

GB/T 41807—2022 信息安全技术 声纹识别数据安全要求

GB/T 41387—2022 信息安全技术 智能家居通用安全规范

GB/T 41388—2022 信息安全技术 可信执行环境

3 术语和定义

下列术语和定义适用于本文件。

3.1

可信执行环境 trusted execution environment

基于硬件级隔离及安全启动机制，为确保安全敏感应用相关数据和代码的机密性、完整性、真实性和不可否认性目标构建的一种软件运行环境。其中，硬件级隔离是指基于硬件安全扩展机制，通过对计算资源的固定划分或动态共享，保证隔离资源不被富执行环境访问的一种安全机制。

[来源：GB/T 41388—2022，3.3]

3.2

安全启动 secure boot

在系统启动过程中，为验证系统启动过程每一阶段所加载代码的真实性、完整性而提供的一种安全机制。

[来源：GB/T 41388—2022，3.7]

3.3

固件 firmware

功能上独立于主存储器，通常存储在只读存储器（ROM）中的指令和相关数据的有序集。

[来源：GB/T 25069—2022，3.225]

3.4

传输层安全协议 transport layer security protocol

一种作为安全套接层协议后继的正式互联网协议。

[来源：GB/T 25069—2022，3.82]

3.5

服务端 service platform

支持酒店民宿行业智能对话服务的软硬件基础设施，通过与智能对话设备、移动控制端协同，实现应用服务。

[来源：GB/T 41387—2022，3.3，有修改]

3.6

移动控制端 mobile controller

与酒店民宿行业智能对话设备的用户交互，根据接收的用户指令或预先配置的任务，通过服务端向智能对话设备发出指令的应用。

[来源：GB/T 41387—2022，3.4，有修改]

4 缩略语

下列缩略语适用于本文件。

ASLR：地址空间布局随机化（Address Space Layout Randomization）

HTTPS：以安全为目标的 HTTP 通道（Hyper Text Transfer Protocol over Secure Socket Layer）

NX：堆栈不可执行（No Execute）

OTA：空中下载技术（Over-The-Air）

PIE：地址无关代码（Position-Independent Executable）

SELinux：安全增强型Linux（Security-Enhanced Linux）

SIP：会话发起协议（Session initialization Protocol）

SRTP：安全实时传输协议（Secure Real-time Transport Protocol）

TLS：传输层安全协议（Transport Layer Security）

5 设备安全

酒店民宿行业智能对话设备的运行系统由智能对话设备、服务端、移动控制端组成。用户可以通过移动控制端向服务端发起控制请求，服务端下发控制命令至智能对话设备，由智能对话设备执行；用户可以通过移动控制端直接向智能对话设备下发控制命令，由智能对话设备执行；智能对话设备可以向其他智能对话设备转发控制命令。

智能对话设备的信息安全要求包括硬件安全、系统安全、应用安全和通信安全；智能对话设备和服务端之间交互的信息安全要求包括更新安全、通信安全和控制安全；智能对话设备和移动控制端之间交互的信息安全要求包括通信安全和控制安全；智能对话设备之间交互的信息安全要求包括通信安全和控制安全；运行系统整体的信息安全要求包括数据与隐私安全和安全运营。典型安全框架参见图1。

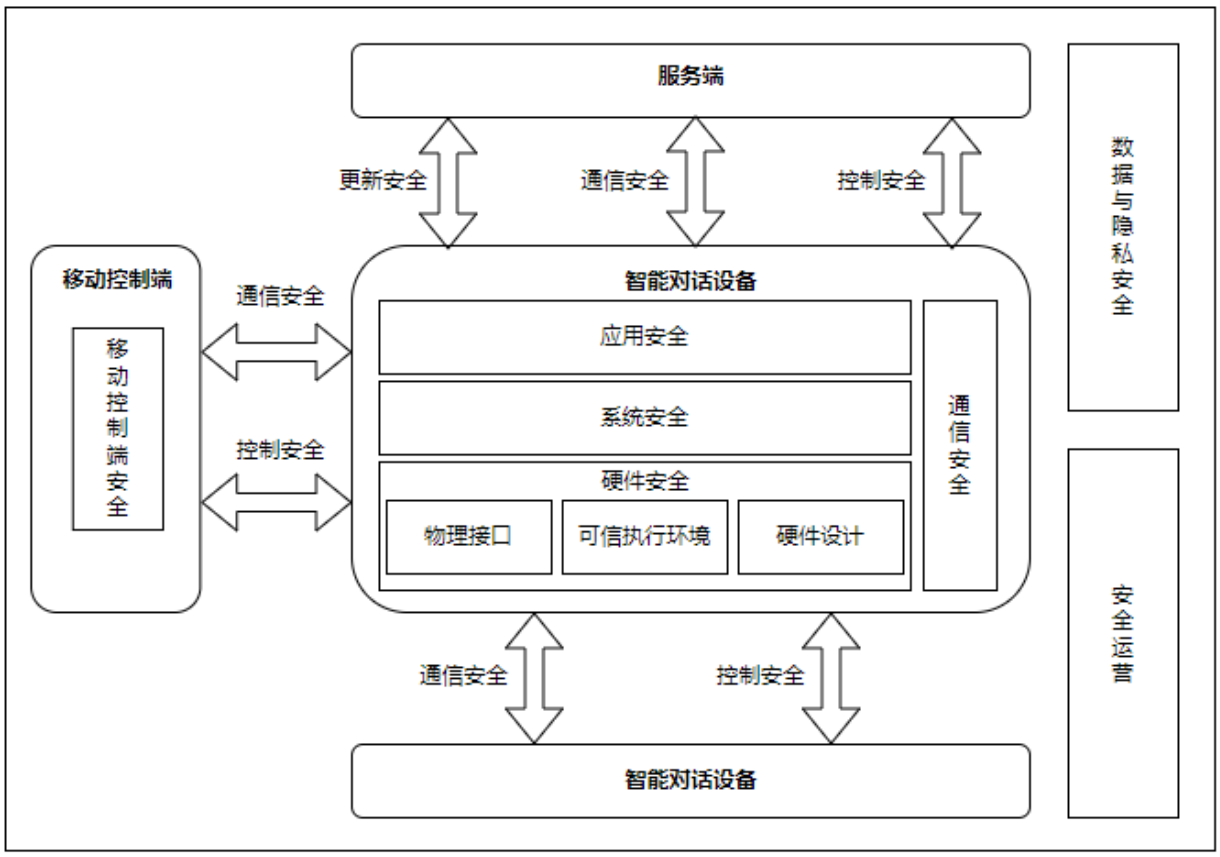

图 1　酒店民宿行业智能对话设备安全框架

5.1　硬件安全

5.1.1　物理接口

物理接口应满足以下要求：

a)　接口设计中应不对外暴露物理调试接口器件；

b)　应遵循最小化原则，禁用非必须的物理接口；

c)　应对箱体内的可调试接口添加访问验证，接口要求默认禁用。

5.1.2　可信执行环境

可信执行环境应满足以下要求：

a)　应支持安全启动，仅允许加载通过完整性校验的固件；

b)　应使用支持可信执行环境的硬件平台。

5.1.3　硬件设计

硬件设计应满足以下要求：

a)　应移除摄像头部件，或添加用户可控的摄像头物理遮挡措施；

b)　若存在摄像头、麦克风部件，应具备用于展示摄像头、麦克风的工作状态的状态指示器；

c） 宜具备控制电源的物理开关按键，包括物理按键或触控按键等；
d） 每一个物理接口均有标识，且有功能说明，无未向用户声明的物理接口。

5.2 系统安全

系统安全应满足以下要求：
a） 应开启 SELinux 或其他类似的强制访问控制策略，按组为系统进程配置不同的访问权限；
b） 应开启 ASLR 保护措施；
c） 应关闭 SSH、Telnet、FTP 等远程控制服务，关闭非必要的端口；
d） 应移除或隐藏开发者选项入口；
e） 应仅支持酒店授权或许可的渠道和方式安装软件/插件。

5.3 应用安全

应用安全应满足以下要求：
a） 应默认禁止应用获取系统的超级用户权限；
b） 若支持应用版本回滚，应仅能由指定服务平台发起回滚；
c） 应在系统应用编译选项中开启 PIE、NX 等保护措施。

5.4 更新安全

更新安全应满足以下要求：
a） 应仅支持云端远程 OTA 方式更新系统固件，例如酒店民宿本地服务器、设备厂商云端服务器等；
b） 应禁止来源不可信的更新包安装；
c） 应使用加密通信链路传输更新包文件；
d） 应在系统固件更新时，对更新包文件进行完整性校验；
e） 应禁止对系统版本进行降级更新；
f） 在系统固件升级失败后，应能支持设备恢复至原版本状态。

6 通信安全

6.1 网络通信安全

6.1.1 通用安全

通用安全应符合以下要求：
a） 智能对话设备和云端、智能对话设备和移动控制端、智能对话设备和其他智能对话设备、智能对话设备和被控设备之间的网络通信，应使用加密传输协议传输控制指令及敏感数据；
b） 在使用 HTTPS 协议时，应对服务端证书进行合法性校验。

6.1.2 呼叫业务安全

呼叫业务安全应符合以下要求：
a） 应使用 TLS 加密 SIP 数据流，避免泄露手机号码等敏感信息；
b） 应使用 SRTP 或其他加密协议传输语音流。

6.2 蓝牙、Zigbee安全

蓝牙、Zigbee 安全应符合以下要求：

a) 若支持蓝牙功能，应具备开启/关闭蓝牙功能的开关，宜默认关闭蓝牙功能；
b) 在与其他设备进行蓝牙配对时，应给予用户提示，并经过用户确认；
c) 若支持 Zigbee 功能，应采用 Zigbee 安全模式。

7 控制安全

7.1 设备交互控制安全

设备与云端交互控制安全应符合以下要求：

a) 设备应支持与云端的双向身份认证
b) 设备应在酒店云端注册后，才允许使用客房控制等涉及与酒店内其他设备、服务人员交互的功能；
c) 应支持对交互控制数据的合法性校验；
d) 应对交互控制数据进行加密；
e) 应对交互控制数据采用防重放机制。

7.2 移动控制端安全

移动控制端安全应符合以下要求：

a) 移动控制端应使用正式版本；
b) 移动控制端应支持远程 OTA 方式更新；
c) 移动控制端应基于 HTTPS 或其他加密协议传输更新包；
d) 移动控制端应支持对更新包进行完整性校验；
e) 移动控制端在使用 HTTPS 协议时，应对服务端证书进行合法性校验。

8 数据与隐私安全

8.1 隐私协议

隐私协议应符合以下要求：

a) 应根据酒店行业的特殊情况，分别为智能对话设备、移动控制端单独制定隐私协议；
b) 应在界面的固定路径展示隐私政策（或其链接），用户进入主功能界面后，通过 4 次（含）以内的点击等操作，能够访问到隐私政策；
c) 无屏智能对话设备的隐私协议应以纸质文件等方式向用户展示。

注：如酒店作为数据处理者，隐私协议应以酒店协议为准。

8.2 用户数据生命周期安全

用户数据生命周期安全应符合以下要求：

a) 应在酒店客户入住时，解耦数据与用户个人身份，如数据初始化等；
b) 应禁止采集用户个人身份信息；

c） 应对用户产生的数据进行匿名化处理；
d） 在酒店客户退房、用户调用销毁功能时，应支持删除用户数据，以便于对用户产生的数据进行销毁；
e） 应支持远程数据销毁与设备禁用功能，用于在丢失、挪用等场景下销毁用户数据；
f） 涉及用户声纹信息处理活动的，应符合 GB/T 41807—2022 中 7.1、8.1、9.1 的相关要求。

9 安全运营

9.1 日志审计安全

智能对话设备涉及到的用户访问记录、浏览记录、设备操作记录等形成的日志应符合 GB/T 35273—2020 中 10.6 规定的对个人信息处理者的要求。

9.2 应急响应

智能对话设备运营者应制定合理的应急响应流程，宜涵盖事件处理过程的每个阶段，包括准备、检测、遏制、根除、恢复、跟踪。

电信终端产业协会团体标准

酒店民宿行业智能对话设备信息安全技术要求

T/TAF 193—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