

ICS 35.200

CCS M30

团体标准

T/CHEAA 00□□—202□

智能家居本地互联互通技术要求

Technical Requirements for Local Interconnection of Smart Home

征求意见稿（CD）

本稿完成日期 2025 年 2 月 28 日

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上

202□-□□-□□发布

202□-□□-□□实施

中国家用电器协会

版权声明

本文件的版权归中国家用电器协会所有，任何单位和个人未经许可，不得进行技术文件的纸质和电子等任何形式的复制、印刷、出版、翻译、传播、发行、合订和宣贯等，也不得未经允许采用其具体内容编制中国家用电器协会以外各类标准和技术文件。如有以上需要请与版权所有方联系。

邮箱：bzfg@cheaa.org

电话：010-51696557

目 次

前言	IV
引言	V
1 范围	1
2 规范性引用文件.....	1
3 术语和定义.....	2
4 缩略语.....	3
5 智能家居本地互联互通架构.....	3
5.1 本地互联互通网络架构.....	3
5.2 本地互联互通功能架构.....	4
5.3 本地互联互通业务流程.....	5
5.4 本地互联互通软件架构.....	5
6 智能家居本地互联互通技术要求.....	6
6.1 发现.....	6
6.1.1 发现流程.....	6
6.1.2 技术要求.....	7
6.2 配网.....	7
6.2.1 配网流程.....	7
6.2.2 技术要求.....	8
6.3 身份认证.....	8
6.3.1 身份认证流程.....	8
6.3.2 技术要求.....	9
6.4 权限管理.....	9
6.4.1 权限配置流程.....	9
6.4.2 管理域.....	10
6.4.3 角色.....	11
6.4.4 ACL（访问控制列表）.....	11
6.5 标识及寻址.....	11
6.5.1 设备终端标识符.....	11
6.5.2 控制终端标识符.....	12
6.5.3 管理域标识符.....	12
6.5.4 组标识符.....	12
6.6 会话管理.....	12
6.6.1 会话流程.....	12
6.6.2 技术要求.....	13
6.7 消息.....	14
6.7.1 消息流程.....	14
6.7.2 消息帧格式.....	14
6.7.3 技术要求.....	15
6.8 模型.....	15
6.8.1 模型的架构.....	15

6.8.2 模型的要求.....	16
7 智能家居本地互联互通安全要求.....	16
7.1 通用要求.....	16
7.2 证书.....	16
7.3 身份认证协议.....	16
7.4 会话密钥.....	17
7.5 加密算法.....	17
附录 A （资料性）智能家居本地互联互通控制权限授权流程	18
附录 B （资料性）智能家居本地互联互通设备模型	19
B.1 属性.....	19
B.2 方法.....	19
B.3 事件.....	19
B.4 服务.....	20

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这些专利的责任。

本文件由中国家用电器协会提出并归口。

本文件主要起草单位：

本文件主要起草人：

引 言

智能家居互联互通是指不同品牌、不同类型的智能家居终端、智能家居网关、智能家居云平台采用统一的标准协议实现控制指令、数据的传输和一致性解析，从而形成统一的智能家居应用和服务的生态。现阶段智能家居硬软硬件厂商众多，产品和服务种类繁多，且厂商出于对设备和用户数据保护的需求，以及市场竞争的目的，智能家居互联互通存在着不同的架构体系、标准协议和技术方案，形成了多个不能相互联通的智能家居生态系统，也成为制约智能家居行业发展的关键因素。

智能家居互联互通按照技术方案，可以分为智能家居本地网络互联互通、智能家居设备终端与智能家居云平台的互联互通、智能家居云平台之间的云云互联互通三种技术方案。本地互联互通不依赖于广域网及智能家居云服务平台，实现智能家居设备的互联互通，与基于云平台的互联互通共同形成智能家居全场景互联互通方案，从而满足不同的智能家居业务场景需求。

智能家居本地互联互通技术要求

1 范围

本文件规定了智能家居本地网络中的互联互通的功能框架和技术要求。

本文件适用于智能家居本地网络互联互通的典型应用场景。

注：本标准中的本地网络基于 IP 网络协议，对于采用非 IP 网络接入协议的智能家居设备，在进行 IP 协议转化后，适用于本文件的规定。非 IP 网络接入协议转换为 IP 网络接入协议，不在本文件规定范围内。

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。

T/CHEAA 0001.1—2023|T/CCSA 260.1—2023 智能家居系统 云云互联互通 第1部分：接口技术要求

T/CHEAA 0038-2024|T/CCSA 592-2024 智能家居系统 基于 Soft-AP 技术的 WLAN 终端快速配网技术要求

T/CHEAA 0030-2024|T/CCSA 525-2024 智能家居系统 基于 NFC 的 WLAN 终端快速配网技术要求

GB/T 39579-2020 公众电信网 智能家居应用技术要求

GB/T 41387-2022 信息安全技术 智能家居通用安全规范

GB/T 35273-2020 信息安全技术 个人信息安全规范

GB/T 40979-2021 智能家用电器个人信息保护要求和测评方法

IEEE 2785-2023 智能家居系统架构框架和通用要求（IEEE Standard for Architectural Framework and General Requirements for Smart Home Systems）

IETF RFC 6763 基于 DNS 的服务发现协议（DNS-Based Service Discovery, DNS-SD）

IETF RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

IETF RFC 2616 超文本传输协议 (Hypertext Transfer Protocol HTTP/1.1)

IETF RFC 2818 基于传输层安全协议的超文本传输协议 (HTTP over TLS)

RFC 5246 传输层安全协议 1.2 版 (The Transport Layer Security (TLS) Protocol Version 1.2)

RFC 7959 资源受限应用协议中的分块传输 (Block-Wise Transfers in the Constrained Application Protocol (COAP))

ISO/IEC PRF 20922 消息队列遥测传输 (Message Queuing Telemetry Transport (MQTT))

3 术语和定义

下列术语和定义适用于本文件。

3.1 智能家居 smart home

以人们的居住环境为平台，利用信息化技术将家庭中各类终端，如通信设备、家居设施、家用电器、环境监控设备、安保防护设备等电子装置连接到家庭智能化系统或云平台上进行监视、控制，和家庭事务管理，为用户提供便利、安全、环保、节能、舒适、高效的家庭生活的设备、网络、平台、应用的总称。

[来源：T/CHEAA 0001.1—2023|T/CCSA 260.1—2023, 3.1, 有修改]

3.2 智能家居本地互联互通 Local Interconnection of smart home

智能家居终端在本地网络中采用统一的架构、协议及流程实现身份认证，控制指令和数据的传输及一致性解析。

3.3 智能家居终端 Smart Home Terminal

连接到家庭网络、协同提供智能家居业务的各种设备的逻辑实体。是智能家居控制终端、设备终端的统称。

[来源：GB/T 39579—2020, 3.4, 有修改]

3.4 智能家居控制终端 Smart Home Control Terminal

与智能家居的用户交互，根据接收的用户指令或预先配置的任务，通过本地网络对设备终端进行管理或控制的逻辑实体。

注：常见的控制终端包括运行在智能手机、网关、家庭信息箱、中控或带屏幕的家电等物

理实体设备上的应用软件。

[来源：GB/T 41387—2022, 3.4 有修改]

3.5 智能家居设备终端 Smart Home Device Terminal

具有本地网络接入能力，接收控制终端指令并执行特定功能的逻辑实体。

注：常见的智能家居设备终端包括运行在智能家电、智能传感器、家居设备等物理实体设备上的应用软件。

4 缩略语

下列缩略语适用于本文件。

ACL	Access Control List	访问控制列表
AES	Advanced Encryption Standard	高级加密标准
BLE	Bluetooth Low Energy	蓝牙低功耗
CoAP	Constrained Application Protocol	受限应用协议
HTTP	Hypertext Transfer Protocol	超文本传输协议
IP	Internet Protocol	互联网协议
MAC	Media Access Control	媒介访问控制
MQTT	Message Queuing Telemetry Transport	消息队列遥测传输
NFC	Near Field Communication	近场通信
PLC	Power Line Communication	电力线通信
SM4	SM4 Block Cipher Algorithm	国密 SM4 分组密码算法
Soft AP	Soft Access Point	软接入点
TCP	Transmission Control Protocol	传输控制协议
TLS	Transport Layer Security	传输层安全
UDP	User Datagram Protocol	用户数据包协议
UUID	Universally Unique Identifier	通用唯一标识符
WLAN	Wireless Local Area Network	无线局域网
XMPP	Extensible Messaging and Presence Protocol	可扩展通讯和表示协议

5 智能家居本地互联互通架构

5.1 本地互联互通网络架构

智能家居本地互联互通网络架构包括智能家居控制终端和设备终端。控制终端对设备终端进行控制和管理。智能家居本地互联互通网络架构如图 1 所示。

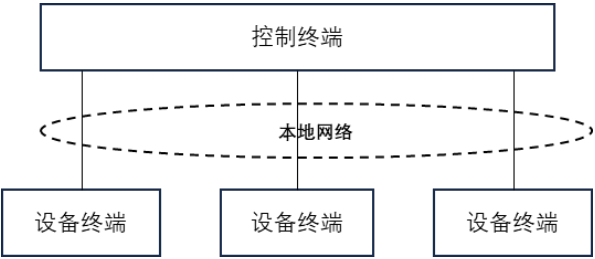


图 1 智能家居本地互联互通网络架构示例

5.2 本地互联互通功能架构

本地互联互通功能框架基于 IP 网络实现智能家居终端间的互联互通，为智能家居应用提供支撑服务。本地互联互通功能框架包括发现、配网、身份认证、标识与寻址、连接管理、模型、消息、会话管理、权限管理、安全等功能组件。智能家居本地互联互通功能架构如图 2 所示。

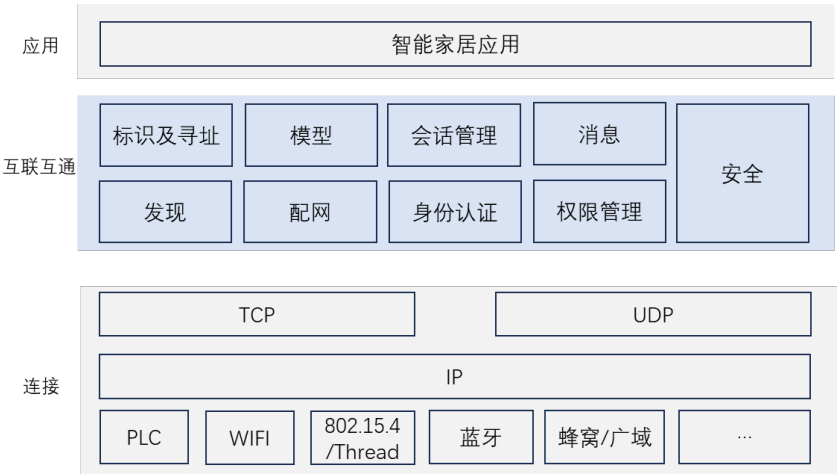


图 2 智能家居本地互联互通功能架构示例

发现：实现控制终端发现设备终端，设备终端发现控制终端的功能。如控制终端发现待配网设备终端，控制终端发现已配网设备终端，以及待配网设备终端发现控制终端。

配网：控制终端向待配网设备终端发送本地网络配置信息，使待配网设备终端接入本地局域网络的功能。

身份认证：控制终端与设备终端实现双向身份认证，确定身份合法性。

权限管理：用户控制权限的配置，包括管理域、访问控制列表等。

标识与寻址：设备终端的唯一标识符，用于该设备终端的寻址。

模型：用于描述设备终端的功能特征和运行状态，由若干属性、方法、事件组成。其中，属性是描述设备终端的功能特征和运行状态的基本数据单元。方法是描述设备终端可供调

用的特定功能。事件是终端设备主动上报的特定信息，包括通知、告警、故障。

消息：控制终端与设备终端间的信息传输的功能。

会话管理：控制终端与设备终端建立的安全连接， 用于后续通信的安全保护。

安全：实现本地互联互通的控制终端、设备终端之间的通信及信息安全、个人数据保护的功能。

5.3 本地互联互通业务流程

控制终端通过发现流程发现设备终端，通过配网流程配置设备终端接入本地网络，通过身份认证流程验证设备终端身份合法性，并对设备终端进行权限的配置。控制终端与设备终端建立会话连接。在会话建立完成后，控制终端与设备终端可以进行消息交互。智能家居本地互联互通流程如图 3 所示。

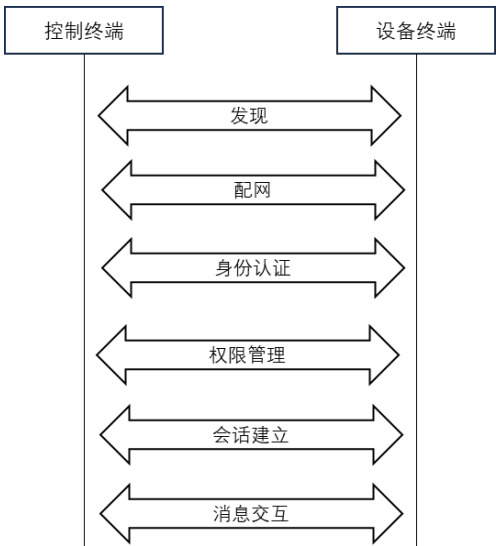


图 3 智能家居本地互联互通流程示例

需要注意的是，发现流程可以在任何阶段由控制终端或设备终端发起。

5.4 本地互联互通软件架构

本地互联互通软件架构采用客户端（Client）/服务器（Server）架构。控制终端作客户端，设备终端作为服务器。控制终端与用户进行交互，向设备终端发送请求，调用设备终端所提供的功能操作、订阅通知等服务。设备终端接收控制终端的服务调用请求，执行并向控制终端返回结果。同时，设备终端也能够主动向控制终端发送通知。本地互联互通软件架构如图 4 所示。

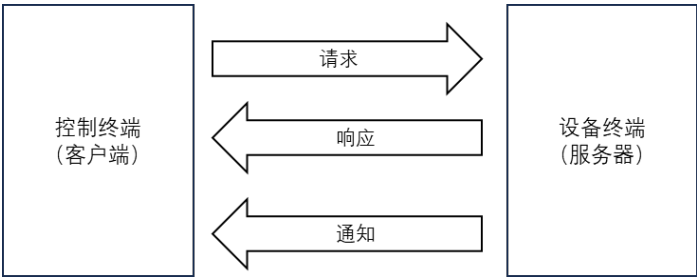


图 4 本地互联互通软件架构示例

控制终端和设备终端是逻辑实体，可以分别部署在不同的物理实体设备上，也可以同时部署在一个物理实体设备上，例如带屏冰箱同时部署控制终端和设备终端，控制终端对部署在智能空调上的设备终端进行控制和管理，如图 5 所示。

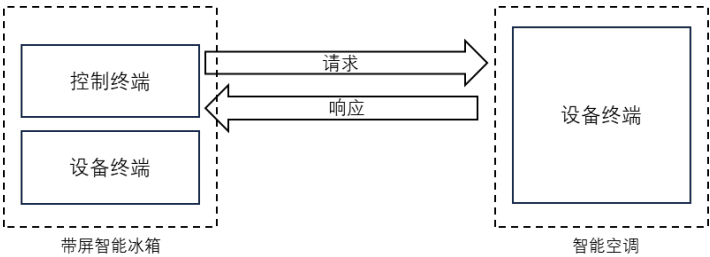


图 5 设备终端与控制终端的部署示例

6 智能家居本地互联互通技术要求

6.1 发现

6.1.1 发现流程

发现流程用于控制终端发现设备终端。控制终端发送发现请求，设备终端收到发现请求后进行响应。设备终端也可主动发起通知宣告该设备终端的存在。发现流程如图 6 所示。

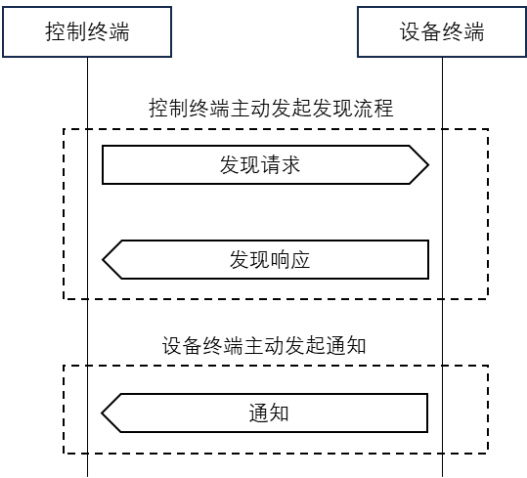


图 6 发现流程示例

设备终端存在不同的网络接入状态，应根据不同的网络接入状态遵循不同的发现流程及技术要求。设备终端的网络状态如表 1 所示。

表 1 设备终端网络状态示例

网络接入状态	说明
待配网	设备终端处于待配网状态
已配网	设备终端已接入本地网络，但是还未通过身份认证
已认证	设备终端已经通过身份认证，接入到控制终端的管理域中

6.1.2 技术要求

待配网状态设备终端的发现技术要求如下：

（a）对于支持 Soft AP 配网的终端，设备终端应工作在 Soft AP 模式下，发送 WLAN 信标帧，控制终端根据信标帧中的 SSID 进行设备发现；

（b）对于支持蓝牙配网的终端，设备终端通过蓝牙广播报文来实现设备发现，广播数据中包括服务 UUID 和自定义信息；

（c）对于支持 NFC 配网的终端，控制终端应工作在主动模式下，通过近距离距离接触设备终端，通过检测帧发现设备终端，并读取设备终端信息实现设备发现；

已配网和已认证状态设备终端的发现技术要求如下：

（a）控制终端应主动发起发现流程，通过广播或组播的方式发送发现请求。设备终端应支持发现请求的监听，在收到发现请求后，应进行响应。响应消息中应当包含该设备的网络状态信息，如配网状态（待配网、已配网、已认证）、产品信息（厂商 ID、产品 ID、MAC 地址等）等。

（b）控制终端应支持特定设备终端的发现，发现请求中应当包括该设备终端的 MAC 地址。该产品 MAC 地址可以通过二维码、NFC、蓝牙等方式获取；

（c）发现流程宜采用 IETF RFC 6763 规定的基于 DNS 的服务发现协议（DNS-Based Service Discovery, DNS-SD）。

6.2 配网

6.2.1 配网流程

配网流程是待配网设备终端获取本地网络配置信息，接入本地网络的功能。在配网前，通过发现流程（6.1 节）发现进入待配网状态的设备终端，配网流程如图 7 所示。

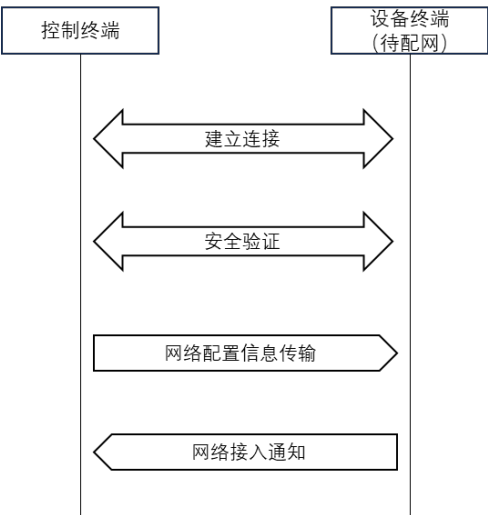


图 7 配网流程示例

6.2.2 技术要求

- 配网的技术要求如下：
- (a) 控制终端与处于待配网状态的设备终端应当至少支持一种建立连接的方式，连接方式可以是 Soft-AP、NFC、蓝牙等；
 - (b) 控制终端与待配网设备终端建立连接后应当进行安全验证，数据传输应当进行加密，避免明文传输；
 - (c) 网络配置信息应至少包括接入本地无线网络的 SSID 和密码；
 - (d) 待配网设备终端获取到网络配置信息并接入本地网络后，应当向控制终端发送网络接入通知；
 - (e) 基于 Soft-AP 的配网宜参照 T/CHEAA 0038-2024|T/CCSA 592-2024；
 - (f) 基于 NFC 的配网宜参照 T/CHEAA 0030-2024|T/CCSA 525-2024；
 - (g) 基于蓝牙的配网宜参照《智能家居系统 基于蓝牙的 WLAN 终端快速配网技术要求》（送审稿）。

6.3 身份认证

6.3.1 身份认证流程

控制终端和设备终端应进行身份合法性的双向认证，即控制终端对设备终端的身份合法性进行验证，设备终端对控制终端的身份合法性进行验证。通过认证请求和响应实现控制终端对设备终端，设备终端对控制终端的身份信息进行验证。身份认证的流程如图 8 所示。

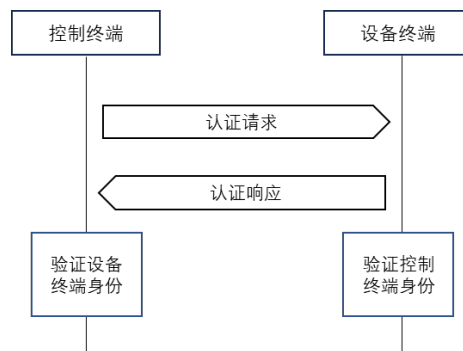


图 8 身份认证流程示例

6.3.2 技术要求

身份认证的技术要求如下：

- (a) 设备终端在出厂前应当内置证书用于控制终端对设备终端进行身份认证；
- (b) 控制终端应内置控制终端的证书，用于设备终端对控制终端进行身份认证；
- (c) 控制终端向设备终端发送身份认证请求，请求中至少包括控制终端的证书；
- (d) 设备终端向控制终端发送身份认证响应，响应中至少包括设备终端的证书；
- (e) 控制终端对设备终端证书进行验证，包括检查证书的签名是否是由信任的 CA 签发的，证书是否过期或被吊销等情况。如果验证失败，控制终端终止连接并提示用户证书错误。如果验证成功，可以继续权限配置流程（6.4 节），或会话建立流程（6.6 节）；
- (f) 设备终端对控制终端证书进行验证，包括检查证书的签名是否是由信任的 CA 签发的，证书是否过期或被吊销等情况。如果验证失败，设备终端拒绝控制终端的权限配置（6.4 节）或会话建立流程（6.6 节）。如果验证成功，可以继续权限配置流程或会话建立流程。

6.4 权限管理

6.4.1 权限配置流程

设备终端身份认证通过后，控制终端对设备终端进行权限配置。权限配置主要包括：控制终端为设备终端分配所属管理域的管理域标识符、设备终端标识符、组标识符以及 ACL（访问控制列表）等信息。权限配置流程如图 9 所示。

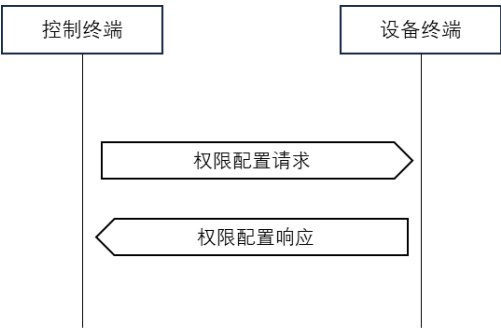


图 9 权限配置流程示例

6.4.2 管理域

控制终端对设备终端的进行控制和管理，由控制终端管理和控制的设备终端的集合称为该控制终端的管理域，在同一个管理域中，将采用相同的安全策略及管理域标识符。一个设备终端可以被多个控制终端控制和管理，因此一个设备终端可以加入多个管理域。管理域如图 10 所示。

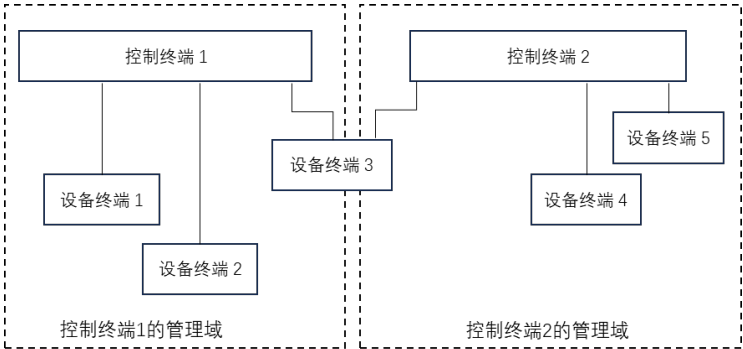


图 10 管理域示例

在图 10 中，设备终端 3 属于控制终端 1 的管理域。控制终端 2 将设备终端 3 加入到控制终端 2 的管理域中，需要向设备终端 3 发起身份认证以及权限配置的流程，如图 11 所示。

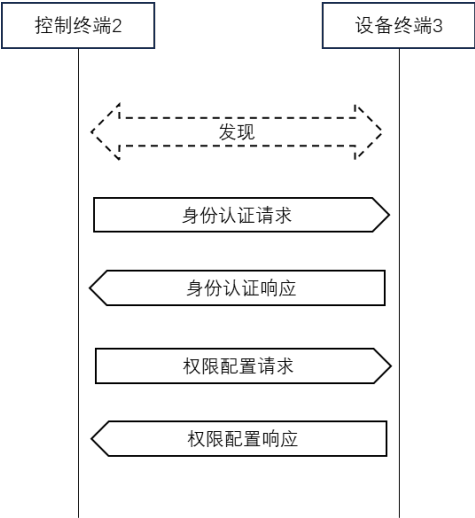


图 11 设备终端加入多管理域示例图

6.4.3 角色

角色分为管理员和非管理员两种。建立管理域的控制终端默认具有管理员角色，即对管理域中的设备终端的控制和管理具有最高权限，包括设备终端 ACL 的配置和修改的权限。非管理员即普通使用者，基于 ACL 的规则对设备终端进行控制，不能对设备终端的 ACL 进行配置和修改。

非管理员获得设备控制的权限，需要由管理员同意授权。其权限授权流程，不在本标准的规定范围内，可参考附录 A。

6.4.4 ACL（访问控制列表）

控制终端在权限配置过程中为设备终端配置 ACL，用于标识不同角色的控制端对设备终端服务的访问权限。

ACL 的要求如下：

- （a）ACL 在设备终端出厂时应为空，在控制终端权限配置后被创建；
- （b）ACL 应当包括设备终端的服务列表（见 6.8 节）、控制终端标识符、访问权限；
- （c）访问权限应包括：可读、可写、可读写；
- （d）ACL 中服务及相关属性、方法、事件不能超出该设备终端设备模型定义的范围；
- （e）非管理员角色的控制终端不能对 ACL 进行配置和修改。

6.5 标识及寻址

6.5.1 设备终端标识符

设备终端标识符的要求如下：

- (a) 设备终端标识符应能够唯一的标识该设备终端；
- (b) 设备终端标识符应由控制终端统一分配；
- (c) 设备终端标识符应用于在控制终端管理域中的设备寻址。

6.5.2 控制终端标识符

控制终端标识符要求如下：

- (a) 控制终端标识符应当能够唯一的标识该控制终端；
- (b) 控制终端标识符应用于控制终端的寻址。

6.5.3 管理域标识符

管理域标识符要求如下：

- (a) 管理域标识符应能够唯一的标识该控制终端的管理域；
- (b) 管理域标识符由控制终端生成，并同步至该管理域内的设备终端。

6.5.4 组标识符

组标识符应由控制终端生成，并同步至该管理域内的设备终端，用于特定组播组的寻址。

6.6 会话管理

6.6.1 会话流程

设备终端身份认证通过后，控制终端与设备终端建立会话，用于后续一系列消息的关联以及消息通信的安全保护。控制终端也可以终止会话。会话建立和终止的流程如图 11 所示。

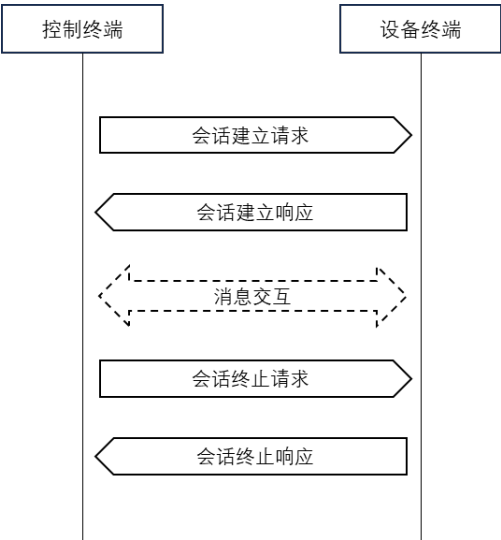


图 11 会话流程示例

会话建立过程中，可能不止进行一次请求/响应的交互流程，主要依赖于所采用的的密钥交互协议。

会话分为单播会话和组播会话。单播会话用于控制端与一个设备终端间的消息通信，组播会话用于一个控制终端与多个设备终端同时进行消息通信，如图 12 所示。

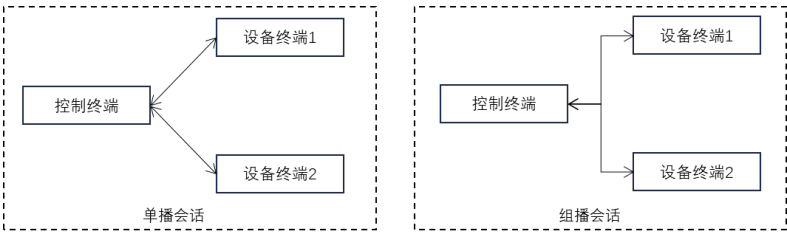


图 12 单播会话与组播会话示例

6.6.2 技术要求

- 单播会话的技术要求如下：
- (a) 控制终端应支持单播会话的建立和终止；
 - (b) 由控制终端在发起单播会话建立请求前，控制终端应生成会话标识符，以及单播会话加密的密钥对；
 - (c) 控制终端向设备终端发起单播会话建立请求，请求消息中至少包括会话标识符、控制端管理域标识符、设备终端标识符、所支持的密钥交互协议；
 - (d) 会话标识符在控制终端的管理域中，能够唯一的标识一个会话；
 - (e) 控制终端与设备终端应采用密钥交换协议进行会话加密密钥的安全传输；
 - (f) 设备终端应对会话建立请求进行响应。响应消息中至少应当包括会话建立结果状态码；

(e) 控制终端应通过会话终止来结束当前会话。会话终止后，会话标识符、会话密钥对应当被释放。

组播会话的技术要求如下：

- (a) 控制终端应支持组播会话的建立和终止；
- (b) 由控制终端在发起组播会话建立请求前，控制终端应生成组播会话标识符，以及组播会话加密的密钥对；
- (c) 控制终端向设备终端发起组播会话建立请求，请求消息中至少包括组播会话标识符、控制端管理域标识符、组标识符、所支持的密钥交互协议；
- (d) 组播会话标识符在控制终端的管理域中，能够唯一的标识一个组播会话；
- (e) 控制终端与设备终端应采用密钥交换协议进行组播会话加密密钥的安全传输；
- (f) 设备终端应对组播会话建立请求进行响应。响应消息中至少应当包括会话建立结果状态码；
- (e) 控制终端应通过会话终止来结束当前组播会话。会话终止后，会话标识符、会话密钥对应被释放。

6.7 消息

6.7.1 消息流程

本地互联互通采用请求/响应消息和通知消息实现通信，控制终端作为请求消息的发起方，向设备终端发送请求消息。设备终端作为响应方，向控制终端反馈响应消息。设备终端也能够向控制终端发送通知消息。本地互联互通通信流程如图 13 所示。

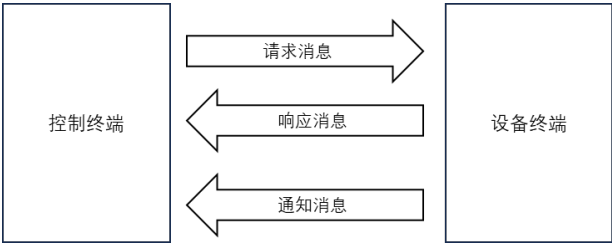


图 13 智能家居本地互联互通消息流程示例

消息分为单播消息和组播消息。单播消息用于控制终端与特定设备终端的消息通信，组播消息用于控制终端与多个设备终端的消息通信。

6.7.2 消息帧格式

消息帧包括三个部分：消息头、消息负荷以及消息尾，如图 14 所示。

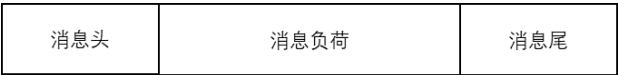


图 14 消息帧格式示例

消息头定义了该消息的基本信息，如消息类型、长度等。消息负荷为该消息承载的智能家居业务应用数据，如控制指令等。消息尾用于消息完整性校验，即对消息进行完整性校验算法计算后得出的数据。

6.7.3 技术要求

- 消息的要求如下：
- (a) 消息头中应至少包括：消息长度、消息类型、会话标识符（见 6.5 节）、消息计数器、管理域标识符等。单播消息中应包括设备终端标识符。组播消息应包括组播标识符。
 - (b) 消息应通过消息计数器检测消息是否为重传；
 - (c) 消息应设置最大长度，超出最大长度的消息应通过传输层协议进行分段处理；
 - (d) 消息通信应具有重传机制；
 - (e) 消息应加密传输；
 - (f) 消息负荷中的设备终端操作命令应符合设备模型中的定义（见 6.8 节）；
 - (g) 消息应包含消息完整性校验；
 - (h) 消息流程及消息帧格式应能够映射到特定的传输协议，如 HTTP、CoAP、XMPP、MQTT 等；

6.8 模型

6.8.1 模型的架构

设备模型描述设备终端的功能特征和运行状态，其逻辑架构如图 15 所示。

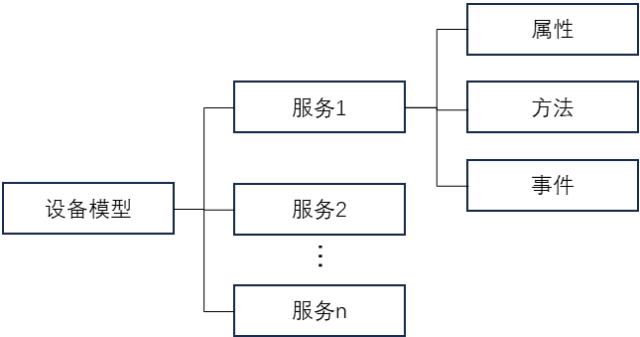


图 15 模型架构示例

- 设备模型对应于设备终端，其功能特征和运行状态等可以通过若干服务的集合来描述。
- (a) 服务描述一个独立且有意义的功能集合，由若干属性、方法、事件组成；

- (b) 属性描述设备终端的功能特征和运行状态的基本数据单元。
- (c) 方法描述设备终端可供调用的特定功能，此类功能不能通过单个属性的读写来完成。
- (d) 事件用于设备终端主动上报的特定信息，包括通知、告警、故障。

6.8.2 模型的要求

模型的要求如下：

- (a) 一个服务至少应包含属性、方法、事件中的一个元素；
- (b) 服务宜采用名称、属性列表、方法列表、时间来进行描述；
- (c) 服务应在不同类型的设备终端间复用；
- (d) 属性宜采用名称、数据类型、访问权限（可读、可写、可通知）、可取值（最大值、最小值、步进单位）、单位、默认值等来描述；
- (e) 方法宜采用名称、输入参数、输出参数来描述；
- (f) 事件宜采用名称、事件类型（通知、告警、故障）、输出参数来描述。

模型结构见附录 B。

7 智能家居本地互联互通安全要求

7.1 通用要求

智能家居本地互联互通应满足以下通用的安全要求及数据保护要求：

- (a) 应符合 GB/T 41387—2022 中第 5 章、第 6 章、第 8 章的相关要求；
- (b) 应符合 GB/T 35373—2020 中第 5 章-第 8 章，GB/T 40979-2021 第 5 章的要求。

7.2 证书

设备终端应当内置证书，用于身份认证。证书的要求如下：

- (a) 应采用符合国家法律法规、相关标准、行业标准要求的证书颁发机构。证书可采用统一证书颁发机制或采用多根 CA 互信机制；
- (b) 设备终端出厂前需预置根 CA 证书、中间 CA 证书（如采用多根 CA 互信机制，则不要求中间 CA 证书）以及设备证书；
- (c) 证书应采用 X.509 格式，宜采用 v3 版本。

7.3 身份认证协议

控制终端与设备终端的双向身份认证，宜采用 TLS1.2 协议及以上版本。

7.4 会话密钥

会话建立后，会生成临时的密钥，用于后续消息通信的安全加密。会话密钥应采用密钥交换协议生成和传输会话密钥，宜采用 DH、SIGMA 协议。

7.5 加密算法

消息通信的加密算法宜使用 SM4、AES 256 密码算法。

附录 A

(资料性)

智能家居本地互联互通控制权限授权流程

当非管理员角色的控制终端 2 对设备终端进行控制，如图 A.1 步骤如下：

(1) 控制终端 2 对管理员角色的控制终端 1 请求控制权限，或设备终端 1 向设备终端 2 发起权限授权请求；

(2) 设备终端 1 对设备终端 2 进行必要的身份验证；

(3) 验证通过后，控制终端 1 配置设备终端的 ACL，加入控制终端 2 的相关控制权限；

(4) 设备终端收到控制终端 2 的控制请求后，根据控制终端 2 的标识符验证其权限。

验证通过后，可以对设备终端进行相应的操作。

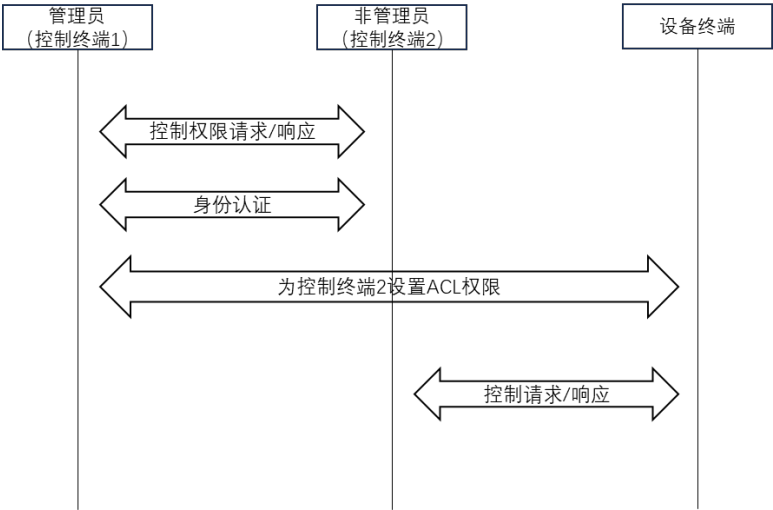


图 A.1 控制权限授权流程示例

附录 B

(资料性)

智能家居本地互联互通设备模型

B.1 属性

属性可采用如下字段进行描述：

- (a) 名称 (name)：属性的唯一标识，采用字符串形式；
- (b) 数据类型 (dataType)：属性值的数据类型；
- (c) 显示名称 (label)：属性的显示名称，通常用中文表示；
- (d) 可取值 (valueRange)：整型和浮点型属性的可取值范围，采用最小值 (minValue)、最大值 (maxValue) 和步进 (step) 表示；
- (e) 取值列表 (valueList)：布尔型和枚举型属性的可取值列表，包含每项可取值及其对应的取值描述；
- (f) 字符串长度 (length)：字符串型属性的长度约束，包括最小长度 (minLen) 和最大长度 (maxLen)；
- (g) 字符串格式 (format)：字符串型属性的格式约束，例如日期、IP 地址等；
- (h) 单位 (unit)：整型和浮点型属性的单位；
- (i) 默认值 (default)：属性的默认取值。

B.2 方法

方法可采用如下字段进行描述：

- (a) 名称 (name)：方法的唯一标识，采用字符串形式，命名规则详见第 8 章；
- (b) 显示名称 (label)：方法的显示名称，通常用中文表示；
- (c) 输入参数 (inParamter)：方法输入参数列表，输入参数可以为 0 个或者多个；
- (d) 输出参数 (outParamter)：方法输出参数列表，输出参数可以为 0 或者多个。

B.3 事件

事件可采用如下字段进行描述：

- (a) 名称 (name)：事件的唯一标识，采用字符串形式；
- (b) 显示名称 (label)：事件的显示名称，通常用中文表示；
- (c) 事件类型 (eventType)：事件类型，包括 0-通知事件（如衣服已洗完）、1-告

警事件（如烟雾告警）、2-故障事件（如温度传感器故障）；

（d）输出参数（outParameter）：事件输出参数列表，输出参数可以为 0 或者多个。

B.4 服务

服务由属性、方法、事件组成，一个服务至少应包含属性、方法、事件中的一个元素。

服务可以在不同类型的设备终端间复用。

服务可采用如下字段进行描述：

（a）名称（name）：服务的唯一标识，采用字符串形式；

（b）显示名称（label）：服务的显示名称，通常用中文表示；

（c）属性列表（propertyList）：服务包含的属性列表，其中每一属性应包含属性名称以及在本服务中是否为必选；

（d）方法列表（actionList）：服务包含的方法列表，其中每一方法应包含方法名称以及在本服务中是否为必选；

（e）事件列表（eventList）：服务包含的事件列表，其中每一事件应包含事件名称以及在本服务中是否必选。

参考文献

- [1] 《智能家居系统 基于蓝牙的 WLAN 终端快速配网技术要求》（送审稿）
-