ICS 35.100.70

L 79

团　体　标　准

T/CHEAA 0001.4—202□

智能家居系统 云云互联互通

第 4 部分：设备配网身份验证技术要求

Smart home system - Cloud to cloud interconnection

Part 4: Technology requirements for device provisioning and authentication

征求意见稿（CD）

本稿完成日期 2023 年 5 月 29 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　发布

目　次

前　言

本文件按照 GB/T 1.1-2020 给出的规则起草。

T/CHEAA 0001《智能家居系统 云云互联互通》标准分为以下 4 个部分：

——第 1 部分：接口技术要求

——第 2 部分：信息安全技术要求与评估方法

——第 3 部分：用户界面设计指南

——第 4 部分：设备配网身份验证技术要求

本文件为 T/CHEAA 0001 的第 4 部分。

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。

本文件的发布机构对由于自愿采用本文件而引起的一切损失不承担任何责任及相关连带责任。

本文件由中国家用电器协会提出。

本文件由中国家用电器协会标准化委员会归口。

本文件起草单位：

本文件主要起草人：

本文件为首次发布。

引　言

随着越来越多的智能家用电器与互联网、物联网络连接，众多智能家居设备厂商都建立了自己独立的智能家居通信协议和云平台管理自己的智能家居设备，由于同一个家庭中会存在多个厂商的设备及多种控制终端，不兼容性导致用户的体验差，鉴于我国厂商的现状，在家庭本地形成统一的通信协议难度较大。

基于我国家电行业近六年来的探索实践，以及我国家电行业与我国通信行业的两大协会在标准领域的跨界合作，该系列标准提出了一套可使不同智能家居设备厂商智能系统间实现互联互通的轻量级解决方案，即规定了不同云平台之间互联互通的整体架构、基本规范和接口描述，从而使各厂商的人机交互系统和设备可通过云平台间的互联互通实现跨厂商、跨平台的操作及信息交互。该标准也将确保跨厂商设备交互的效率和有效性，为智能家居系统带来更好的用户体验，为其普及和发展奠定基础。

智能家居系统 云云互联互通

第 4 部分：设备配网身份验证技术要求

1 范围

本文件围绕智能家居云云互联互通的典型应用场景规定了设备配网及身份认证的流程及技术要求。

本文件适用于智能家居云云互联互通的典型应用场景下的设备配网及身份认证。

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 199—2018	移动互联网+智能家居系统 总体要求
IETF RFC 2616	超文本传输协议 （Hypertext Transfer Protocol HTTP/1.1）
IETF RFC 5246	传输层安全协议 1.2 版[The Transport Layer Security (TLS) Protocol Version 1.2]
IETF RFC 7159	JavaScript 对象标记数据交换格式 [The JavaScript Object Notation (JSON) Data Interchange Format]
IETF RFC 2818	基于安全传输层协议的超文本传输协议(HTTP over TLS)
IETF RFC 6749	OAuth 2.0 授权框架(The OAuth 2.0 Authorization Framework)
IETF RFC 6750	OAuth 2.0 授权框架短暂访问令牌的请求规则和注意事项 (The OAuth 2.0 Authorization Framework: Bearer Token Usage)
Swagger 2.0	表征状态转移接口规范 2.0 版(Swagger RESTful API Documentation Specification 2.0)
IETF RFC 7519	基于 JSON 对象格式的安全令牌[JSON Web Token(JWT)]

3 术语和定义及缩略语

3.1 术语和定义

3.1.1

智能家居系统 smart home system

以人们的居住环境为家庭平台，利用信息化技术将家庭中各种通信设备、家居设施、家用电器、环境监控、安保防护等电子装置连接到家庭智能化系统或云服务平台上进行集中的通信、监视、控制，和家庭事务管理，以给智能家居用户提供便利、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。

[YDB 199—2018，定义 3.1]

3.1.2

智能家居设备 smart home devices

通过有线或者无线方式连接到家庭网络的，并应用了智能化技术或具有了智能化能力/功能的家用和类似用途设备。

3.1.3

智能家居云服务平台　smart home application cloud

通过网络统一组织和灵活调用各种智能家居信息资源，实现智能家居信息大规模计算的处理方式。其利用分布式计算和虚拟资源管理等技术，通过网络将分散的ICT资源（包括计算与存储、应用运行平台、软件等）集中起来形成共享的智能家居资源池，并以动态按需和可度量的方式向用户提供服务。通常简称为云平台。

[YDB 199—2018，定义3.3]

3.1.4

云云互联互通　cloud to cloud interconnection

通过公开的标准协议，使各个厂商可实现各自云平台间信息的直接交互，使用户可通过任意厂商的应用实现对各个厂商设备及服务的添加、控制、信息获取等交互功能。

3.1.5

控制终端　master controlling terminal

在智能家居环境中，以本地或者远程方式综合管理或控制各家居应用终端，主要实现将使用者的操作或控制行为转换成实际指令信号，并协调云服务平台的智能化应用服务资源，下发至应用终端以供其执行具体操作。可包括智能家居App、智能音箱、大屏等。

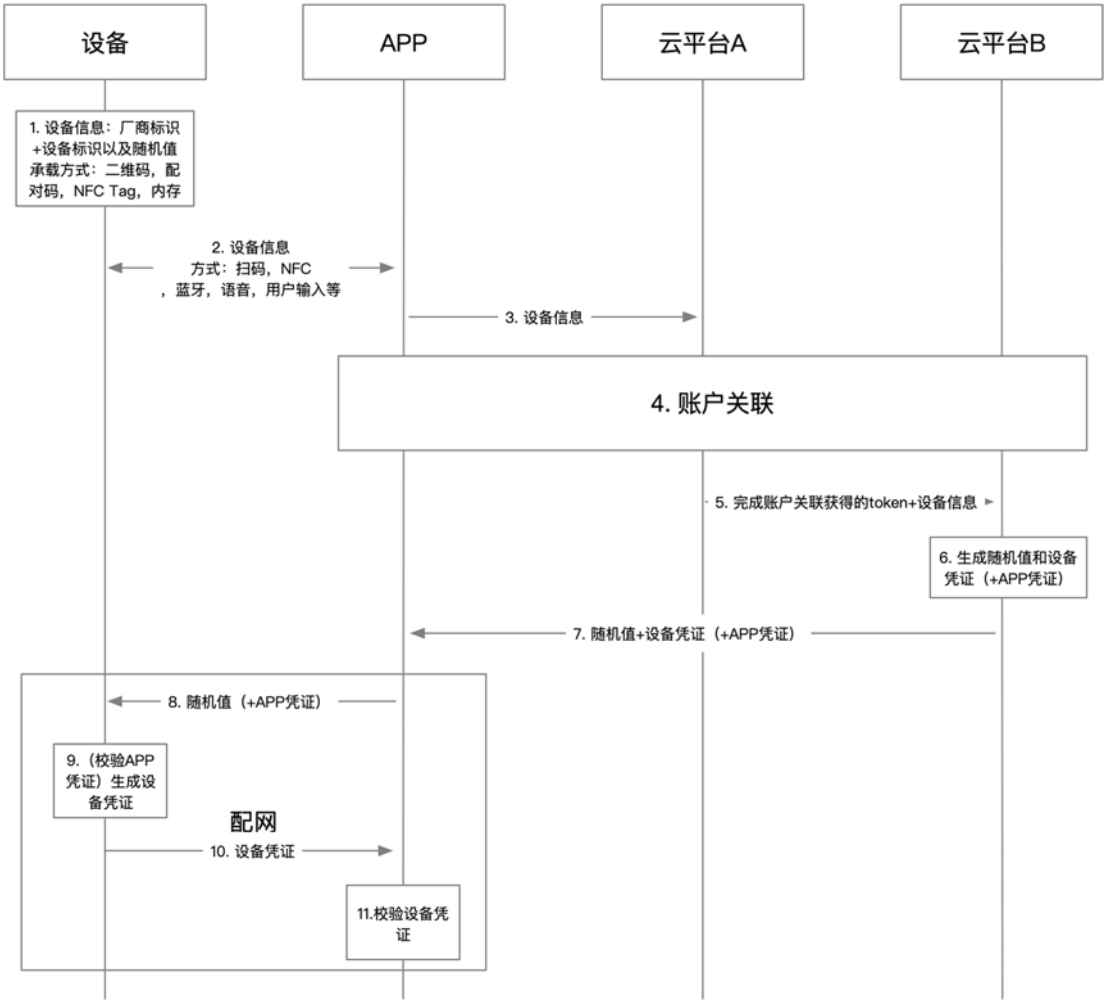
3.2　缩略语

下列缩略语适用于本文件。

API	Application Programming Interface	应用程序接口
APP	Application	应用程序
ASCII	American Standard Code for Information Interchange	美国标准信息交换代码
HMAC	Hash-based Message Authentication Code	基于散列的消息验证码
ICT	Information Communications Technology	信息和通信技术
JSON	JavaScript Object Notation	JavaScript 对象标记
URL	Uniform Resource Locator	统一资源定位符

4　总体流程

目前采用设备许可码的方式，设备许可码(License)由设备的云平台生成(云平台B)，出厂时在应用终端侧进行预置。同时，设备云需保留应用终端唯一标识与设备许可码（License）之间的对应关系，具体流程如下：



标引序号说明：

1. 设备预先存储必要设备信息：厂商标识+设备标识以及随机值（可选用于认证 app），承载方式宜为：机器上二维码，机器人的刻印配对码，NFC 标签以及在设备 flash 里存储等。

2. APP 通过扫码，NFC，Wi-Fi Beacon，蓝牙，语音输入，用户手动输入，图像识别等方式获得设备信息。

3. APP 将设备信息发给云平台 A。

4. 云平台 A 通过厂商标识获得云平台 B 地址，配合 APP 与云平台 B 完成账户关联流程。

5. 云平台 A 将通过账户关联获得的云平台 B 的 token 和设备信息发送给云平台 B。

6. 云平台 B 通过获得的设备信息生成用于认证设备的随机值和设备凭证，通过从云平台 A 获取到的随机值生成用于验证 APP 的凭证（可选）。

7. 云平台 B 将随机值和设备凭证和 APP 凭证（可选）发给 APP （可通过云平台 A 转发）。

以下步骤在配网流程中进行：

8. APP 将获得到随机值和 APP 凭证（可选）发给设备。

9. 如果设备获得了 APP 凭证需要校验凭证的合法性，根据随机值生成设备凭证。

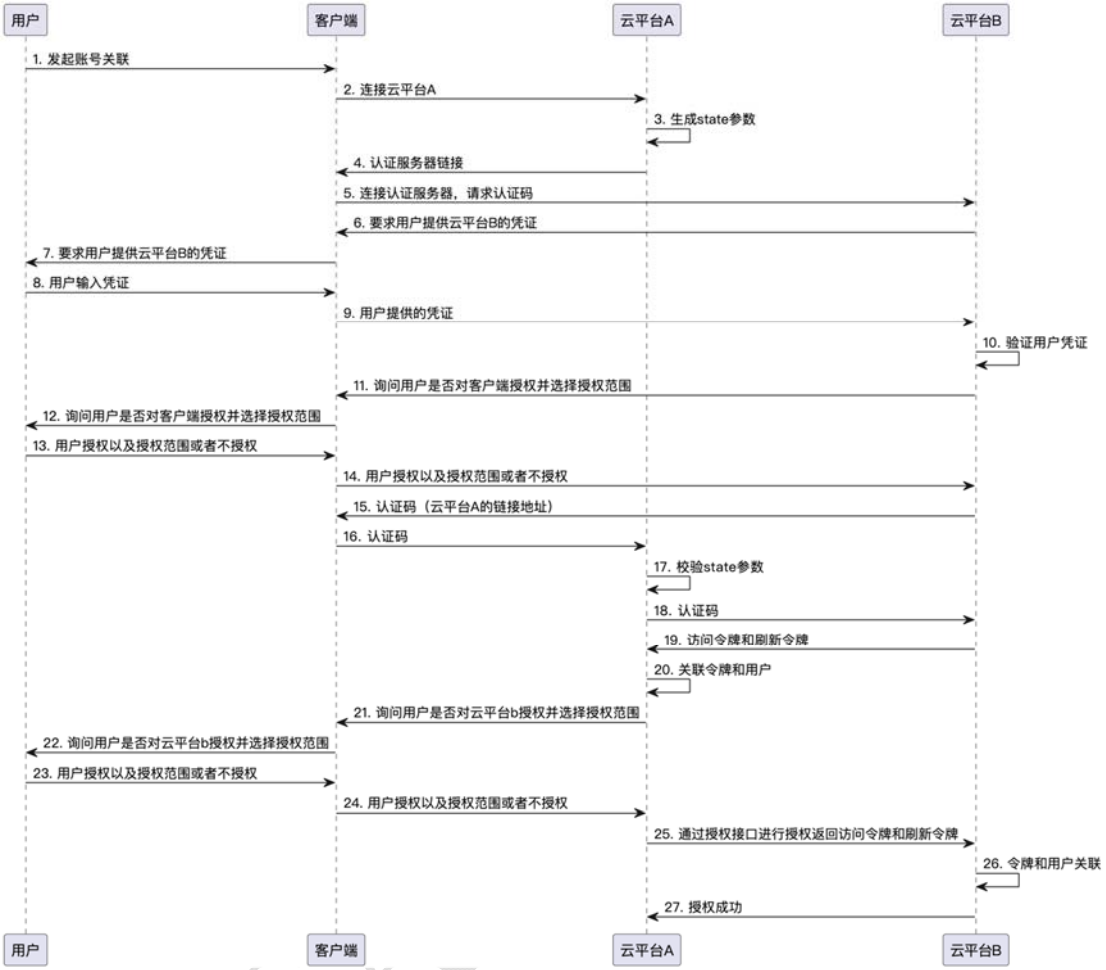
10. 设备将设备凭证发给 APP

11. APP 校验获得的设备凭证，合法后进行配网。

图 1 设备配网身份验证流程示意图

5 账户关联流程

在账户关联过程中，用户需要将云平台 B 的设备控制权限授权给云平台 A，同时也可以将在云平台 A 的设备控制权限授权给云平台 B，具体流程如下：



标引序号说明：

1. 用户发起账号关联。
2. APP 连接云平台 A。
3. 云平台 A 生成 state 参数。
4. 云平台 A 将认证服务器（云平台 B）链接发给 APP。
5. APP 连接认证服务器（云平台 B）请求认证码。

6-10 用户通过云平台 B 在 APP 上提供的界面进行登陆。

11-16 云平台 B 根据用户授权范围返回认证码。

17-19 云平台 A 校验 state 参数后向云平台 B 请求访问令牌和刷新令牌。

20. 云平台 A 关联令牌和用户。

21-24 云平台 A 询问用户将用户在云平台 A 的设备控制权授权给云平台 B。

25. 云平台 A 通过授权接口将授权访问令牌和刷新令牌发送给云平台 B。
26. 云平台 B 将令牌和用户关联。
27. 授权成功。

图 2 账户关联流程示意图

6 账户关联接口

6.1 总体介绍

账户关联接口是把用户在云平台B上的设备与用户在云平台A上的用户标识进行关联的机制。账户关联成功后，云平台A从云平台B获得访问令牌（Access Token）和更新令牌（Refresh Token）。访问令牌使用承载令牌（Bearer Token），用于在云平台B上确定用户（及其使用的客户端）的身份。

账户关联宜参考IETF RFC 6749第4.1节使用OAuth 2.0授权码授权流程。账户关联的前提条件包括用户在云平台A的客户端在云平台B上已注册成功，且已获得必要的参数，如客户端标识（client_id）、客户端密钥（client_secret）、重定向URI、及令牌端点（token endpoint）。

注：本文件的范围不包含授权码授权流程的前提条件，客户端注册成功（IETF RFC 6749第2节）。

账户关联过程还应满足以下要求：

1) 所有请求访问令牌和更新令牌的命令应包含客户端标识和客户端密钥，且宜参照 IETF RFC 6749 中 2.3.1 的规定使用 Authorization Header 和 Basic 机制在请求命令中携带客户端标识和客户端密钥。
2) 所有授权请求应按照 IETF RFC 6749 中 4.1.1 的规定包含状态（State）参数，云平台 A 客户端用其来维护账号关联过程中请求和回调之间的状态。
3) 所有在账号关联过程发送的请求命令、响应命令和错误码都应符合 RFC 6749 的界定。
4) 客户端不应对请求命令的 Body 进行编码。
5) 当访问令牌过期但更新令牌仍然有效时，云平台 A 可以通过云平台 B 的 OAuth 2.0 令牌端点请求新的访问令牌。当更新令牌过期或不可用，且访问令牌也无法获得时，云平台 A 应按照 IETF RFC 6749 的有关要求移除与云平台 B 上的设备的所有关联。

6.2 访问令牌的授权范围

本文件定义了一组 OAuth 2.0 访问令牌的授权范围，如表 10 所示。账户关联过程中，云平台 A 可以请求这组授权范围中的一个或多个，或厂商自定义的授权范围。若云平台 B 提供的授权范围不同于云平台 A 请求的授权范围，则访问令牌中应包含前者。若云平台 B 支持不指定授权范围的访问令牌请求，则当其从云平台 A 收到这样的请求时，所提供的访问令牌应包含表 1 中所有的授权范围。

表 1 访问令牌的授权范围

授权范围的名称	授权范围的描述
r:*	读取
w:*	更新

表 2 给出了每个 API 端点对应的访问令牌的授权范围。例如，若云平台 A 发送 GET 请求到 API 端点“/v1/devices”，则云平台 A 得到的访问令牌一定包含授权范围“r:*”或相关的厂商自定义授权范围。

表 2 API 端点对应的访问令牌授权范围

API 端点	HTTP 请求类型	授权范围
/v1/devices	GET	r:*

/v1/devices/{deviceID}	GET	r:*
/v1/devices/status	POST	r:*
/v1/devices/operation	POST	w:*
/v1/devices/subscriptions	POST	r:*
	DELETE	r:*
/v1/devices/{deviceID}/{DeviceAttr}/subscriptions	POST	r:*
	DELETE	r:*

厂商若要对表 1 的访问令牌授权范围进行扩展，可在其名称中（星号*前）添加厂商特定信息，如“r:xyz:*”。厂商自定义授权范围不属于本文件范围，但可以包含在对访问令牌的请求命令中。若用户同意云平台 A 的授权范围“w:*”，则代表其也同意所有衍生的授权范围，如"w:xyz:*"。

6.3 授权接口

本接口用于云平台 A 将用户在云平台 A 的设备权限授权给云平台 B，此权限可以使用户通过云平台 B 控制用户接入云平台 A 的设备。接口说明如表 3 所示，请求参数如表 4 所示，响应参数如表 5 所示，返回码和返回信息如表 6 所示。

表 3 接口说明

HTTP Method	接口访问地址
POST	/v1/reverseauth

表 4 请求参数

位置	参数	值类型	必填	说明
Header	Accept		是	发送者可接受的一种或多种 MIME 类型，用于指示响应消息的负载可使用的 MIME 类型。
Header	Content-Type	String	否	命令负载所使用的 MIME 类型。
Header	Access Token		是	通过账户关联过程获取的访问令牌，通过 JWT Bearer Token 承载。
Header	appId	String	否	云平台 A 为云平台 B 分配的 ID
Header	timeStamp	Unix 时间戳	否	消息时间戳
Header	openId	string	否	用户标识
Header	signature	string	否	使用 HmacSHA256 签名算法对字符串进行签名，得到对应的签名数组再使用 base64 进行编码，密钥使用云平台 B 为云平台 B 的 APP 应用生成的 client Secret。
Body	access_token	string	是	访问云平台 A 设备的访问令牌，通过 JWT Bearer Token 承载。
Body	refresh_token	string	否	刷新令牌
Body	expire_in	时间戳	是	过期时间

表 5 响应参数

位置	参数	值类型	必填	说明
Header	Content-Type	String	否	命令负载所使用的 MIME 类型。

表 6 返回码和返回信息

返回码	返回信息	适用场景
200	所有设备的设备信息和设备状态	请求成功。
400	出错原因（可选）	请求的格式不正确。
401	出错原因（可选）	请求是未经授权的，如访问令牌错误或缺失。
403	出错原因（可选）	访问令牌的授权范围不正确。
406	出错原因（可选）	请求中 Accept 指定的媒体类型不受支持。
503	出错原因（可选）	所请求的服务不可用。
504	出错原因（可选）	所请求的设备不可用。
厂商可按照 IETF RFC 2818 自定义。		