

WHITE PAPER



# Open Connectivity Foundation 通用云接口

2020-10-20

OPEN CONNECTIVITY  
FOUNDATION

# 目录

前言 .....	2
业务场景 .....	2
概述 .....	2
客户端云 .....	3
设备云 .....	3
技术要求 .....	3
概述 .....	3
基本要求 .....	4
云和云的关联（用户视角） .....	4
发现和获取云上托管的设备 .....	5
设备互操作：获取和更新 .....	5
保持同步：事件 .....	6
参考实现“plgd” .....	7
认证项目 .....	8

## 前言

根据国际数据公司（IDC）的预测，到 2024 年，用于云服务以及围绕云的专业和管理服务的支出将超过 1 万亿美元。随着 416 亿台物联网设备在 2025 年前被部署，连接到云的智能家居设备的数量也将不断增加，消费者越来越需要一个集成的智慧生态系统。

实现不同厂商的物联网设备之间的大规模互操作，云云互联是一种简单有效的方法。厂商只需要在云上开发 API，而不需要改变设备和云的现有技术架构。

但也有新挑战。厂商正在耗费越来越多的时间和资源，为不同的合作伙伴开发不同的云云互联 API，以满足业务的需求。而这些 API 之间，通常只有细微的差别。

为了解决这个问题，Open Connectivity Foundation (OCF) 于 2020 年 8 月推出业界首个开放的云云互联规范——OCF 通用云接口（Universal Cloud Interface, UCI），并同时发布了其开源的参考实现和认证项目。

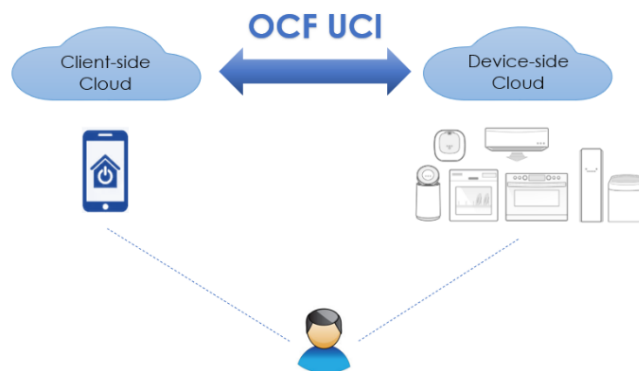
本白皮书旨在为读者提供 OCF 通用云接口的全面描述，包括业务场景、技术要求、参考实现和认证项目。

## 业务场景

### 概述

在现今各种 B2B 商业合作中，云云互联已成为重要的技术解决方案。例如，如果用户想在汽车仪表盘上打开家里的空调，就可以通过汽车制造商和家电制造商的云云互联来实现。与其他技术方案相比，云云互联不需要对现有设备进行修改，也不需要建立公共的云平台或网关。厂商还可以轻松地管理他们的数据，包括哪些数据可以与合作伙伴共享，哪些不能共享。

随着 OCF 通用云接口的发布，云云互联变得更加简单。使用 OCF 通用云接口的云可以互相通信，满足各种业务需求，并节约定制开发的成本。



OCF 通用云接口的使用场景中有两类云：客户端云（Client-side Cloud）和设备云（Device-side Cloud）。

## 客户端云

在 OCF 规范中，客户端云也称原始云，它是承载用户客户端（如，智能手机和智能音箱）的云。通过 OCF 通用云接口，客户端可以控制用户托管在设备云上的设备并接收来自它们的通知。使用客户端云的通常是物联网解决方案提供商或应用程序提供商。

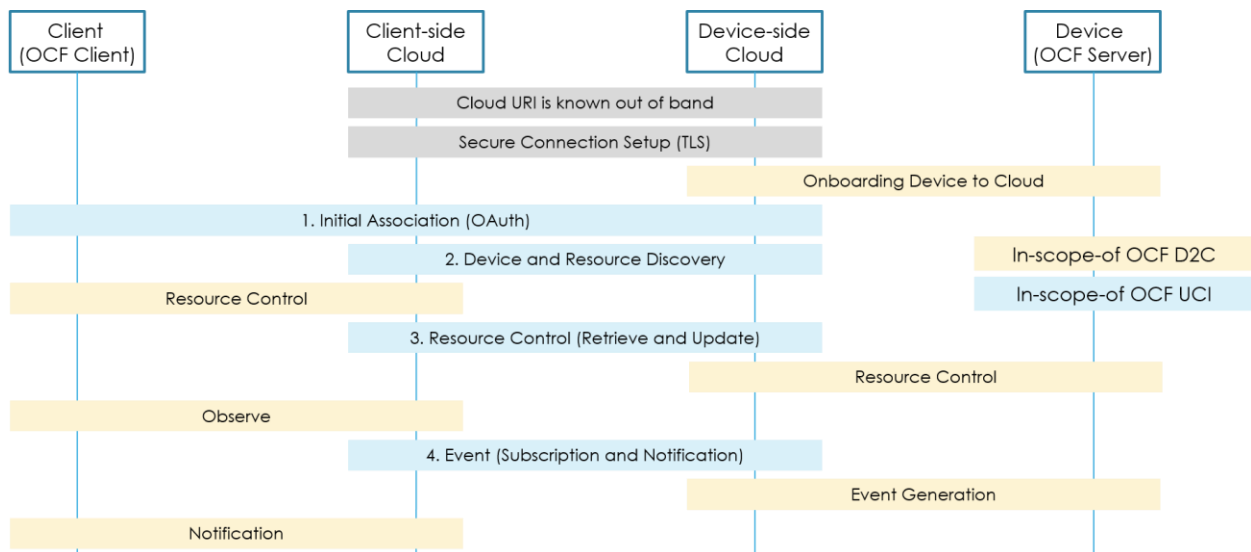
## 设备云

在 OCF 规范中，设备云也称目标云，它是托管用户设备（如，智能家电和传感器）的云。通过 OCF 通用云接口，设备可以向客户端云上的客户端开放其资源（如，开关）的控制权，并上报动态信息。使用设备云的通常是物联网设备制造商。

# 技术要求

## 概述

OCF 通用云接口是一组应用程序接口（Application Programming Interface, API），用于帮助物联网行业避免实现和维护大量的、同时运行的、专有或自定义的编程接口。OCF 通用云接口由安全的且符合行业标准的基础技术构建而成，由 OAuth2.0 提供必要的身份验证，由 HTTPS 提供安全连接。这组定义清晰的 API 实现了设备信息的获取和更新，及设备事件的订阅。API 的使用独立于数据模型，因此所有 OCF 已发布和将发布的数据模型都可用于这组 API。数据模型是对 RESTful 动词的有效负载的描述，OCF 通用云接口透传数据模型，不对其做任何修改（如，在获取设备信息时）。有效负载使用的媒体类型可通过 HTTP 机制的 Accept 报头协商确定。至少 JSON 和 CBOR 受到支持。

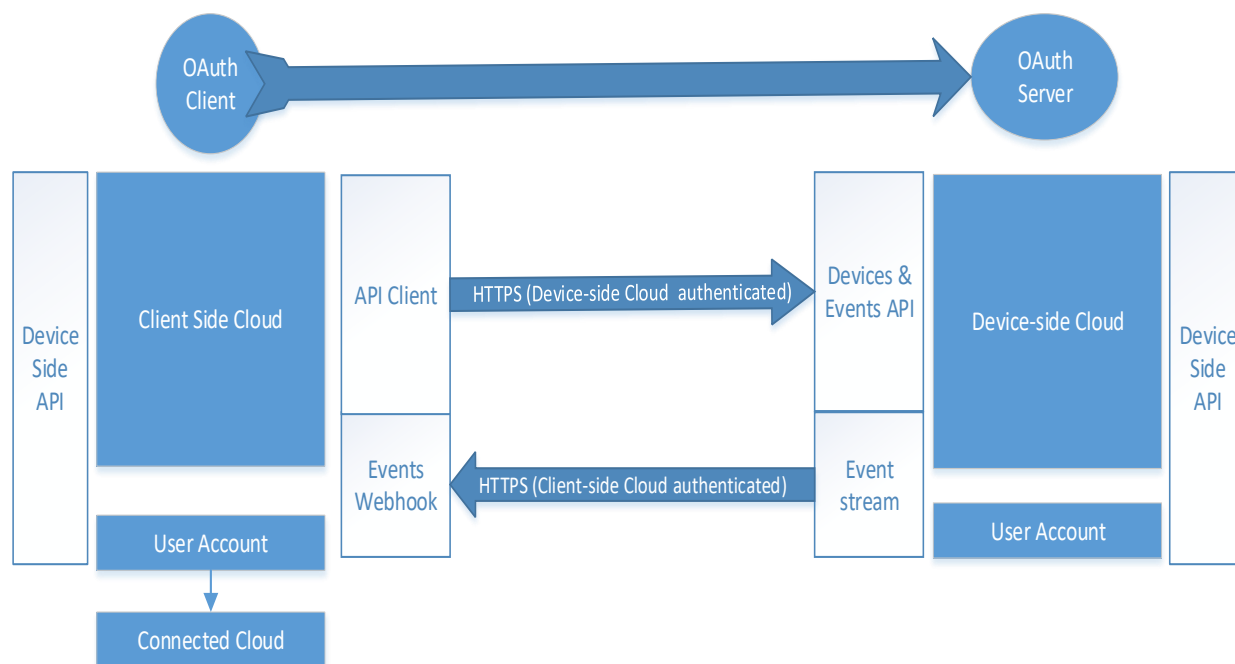


## 基本要求

如前所述，OCF 通用云接口是一组基于 HTTPS 的 RESTful 风格的 API。我们用 OpenAPI 2.0 撰写了这组 API 的机器可读的定义。

客户端云与设备云通信，使用的凭证信息来自基于 OAuth2.0 的用户帐户关联过程，该凭证信息同时存在于两个云上。云云之间的所有请求都通过 HTTPS 进行，且含有 OAuth2.0 提供的承载令牌（用于身份验证）。

云云之间交互的有效负载的格式，使用标准 HTTP 机制协商确定。设备和资源由 OCF 规范定义，该规范部分采用了 Open API 2.0 的定义。有效负载可以（至少）使用 JSON 或 CBOR 编码。



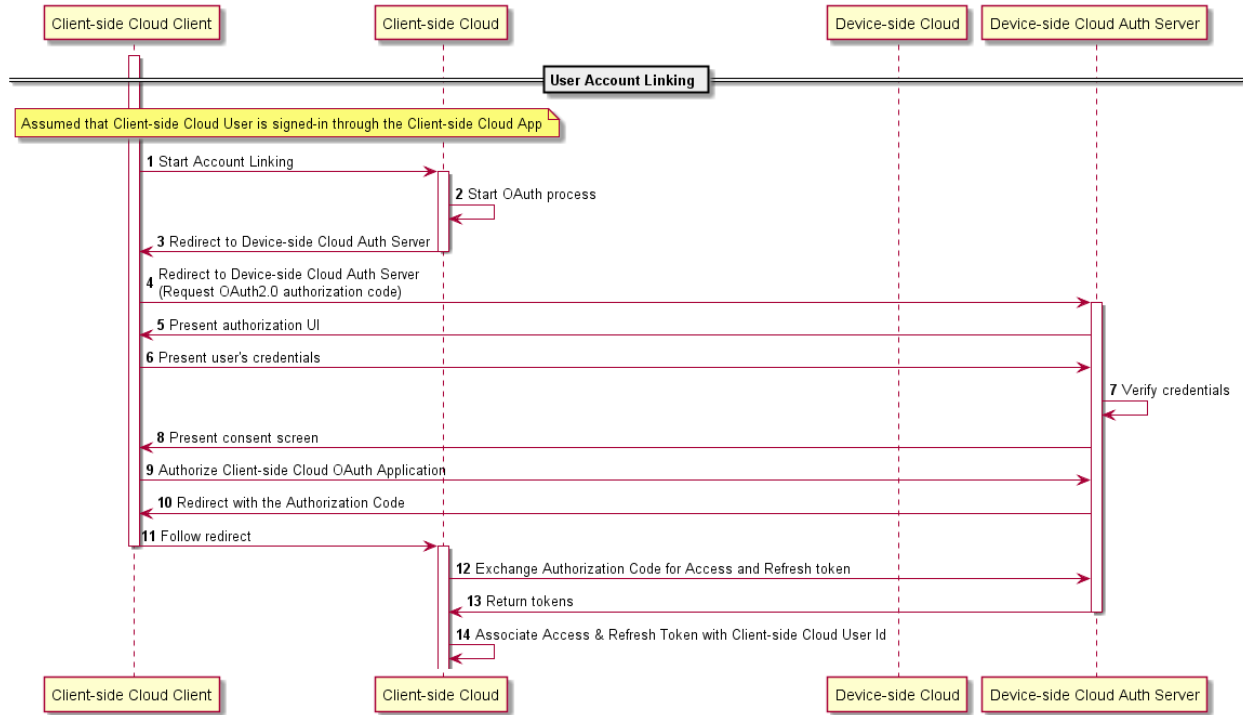
## 云和云的关联（用户视角）

假设一个用户在分属不同供应商的两个云上都拥有账户，且每个账户都关联有不同的应用程序或设备。用户希望用一个客户端（或应用程序）就能对其两个账户下的所有设备进行控制，而不希望对不同账户的设备使用不同的客户端（或应用程序）。通过连接客户端云的账户和设备云的设备，用户可在应用程序上把设备添加到账户下（无需考虑云的不同），这是由标准的 OAuth2.0 授权码授权流程实现的。

**帐户关联 API** 是把用户在设备云上托管的设备与用户在客户端云上的用户标识进行关联的机制。帐户关联仅限于客户端云和设备云之间，相关信息不能被代理到第三方云上。

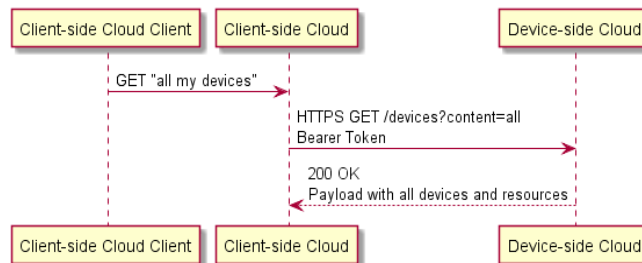
客户端云的 OAuth2.0 客户端在设备云的成功注册依赖于双方建立信任并共享必要的客户端参数（如，客户端标识、客户端密钥和允许的重定向 URI）和 OAuth2.0 令牌端点，这些由 OAuth 规范（IETF RFC 6749）定义。OCF 通用云接口的帐户关联由 OAuth2.0 授权码授权流程实现。帐户关联过程需要用户的明确同意，这在跨域的联合身份验证中非常重要，可确保恶意的客户端无法获得授权。

帐户关联后，用户可通过客户端云请求其在设备云上的设备，因为此时客户端云可以代表设备云上的用户帐户（向设备发出请求）。



## 发现和获取云上托管的设备

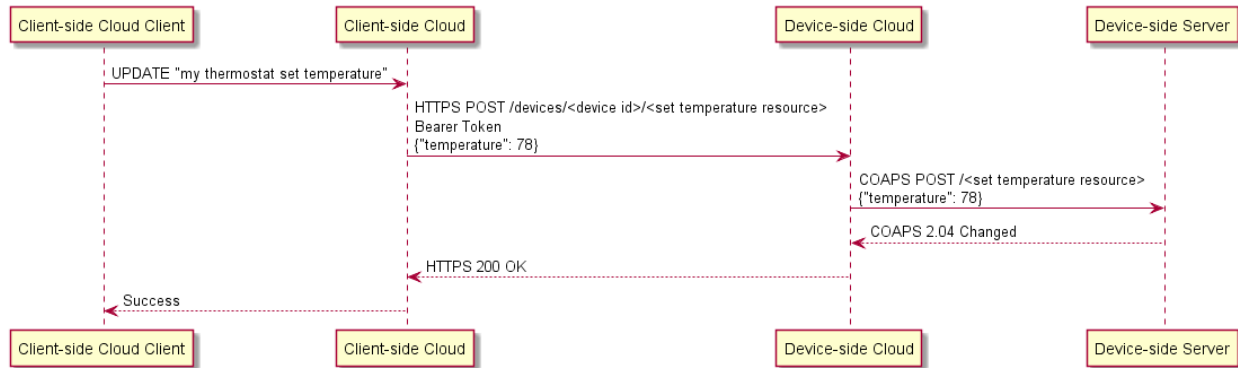
帐户关联后，客户端云可调用设备云提供的**设备 API** 来获取完整的设备信息。一个 HTTP GET 请求足以触发所需的 HTTP 响应，该响应包含用户（在设备云上）托管的设备信息，及这些设备的资源和当前状态。从用户体验的角度，用户操作同一云平台下的设备，和操作关联云平台下的设备，体验是一致的。



## 设备互操作：获取和更新

通过 OCF 通用云接口获取和更新设备时，设备的资源和属性及其操作方式遵循 OCF 规范的定义。由于 OCF 资源使用机器可读的 OpenAPI 2.0 定义，因此有丰富的自动化工具链和代码生成技术可供使用。

下面的示意图展示了如何更新设备云上托管的设备的资源。



## 保持同步：事件

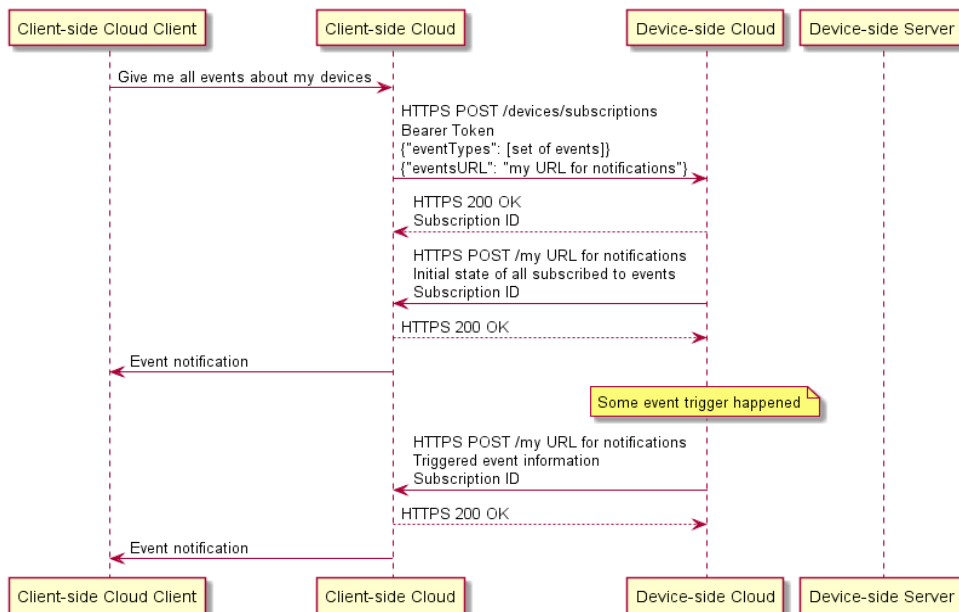
通过 OCF 通用云接口的**事件 API**，客户端云可以订阅设备云上的设备的事件，以使客户端获得设备状态动态信息的推送，免去客户端重复请求这些信息的必要。

对事件的订阅分为三个维度：订阅所有设备的事件、订阅单个设备的事件、订阅设备特定资源的事件。

所有设备的事件，包括设备上线、设备离线、设备注册和设备退出。单个设备的事件，包括资源发布和资源隐藏。特定资源的事件，包括该资源的所有变化。当设备云检测到被订阅的事件发生变化时，就发送通知到客户端云指定的 URL。

所有通知都有 HMAC 签名保护，以避免恶意参与者的攻击。

下面的流程图描述了这一过程。



## 参考实现“plgd”

一个可互操作的物联网平台要能适应多种通信协议，并且是安全、有弹性、可扩展且支持多租户的。参考实现“plgd”（读作“plugged”）是一个云原生物联网平台，实现了 OCF 通用云接口的所有要求并具有更多功能，可在 <https://github.com/plgd-dev/cloud> 上查阅。

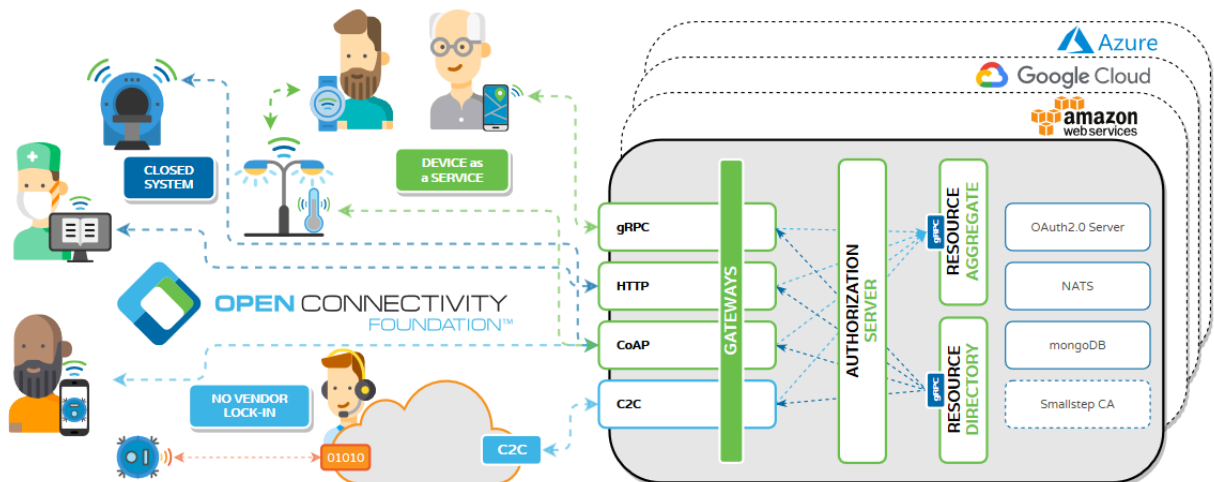
plgd 云平台默认支持 OCF 通用云接口，和 OCF 规范所规定的设备到云的连接。此外，plgd 云平台还公开了它的 gRPC 网关，及一个可用于所有平台（包括移动平台）的 plgd 客户端库，以方便开发人员建立如下端到端的解决方案：

- 客户端和设备在本地的连接，
- 客户端和设备通过云的连接，
- 客户端和设备通过云云互联的连接。

该物联网平台的部署方式有无限可能性。较低的内存和 CPU 占用降低了运营成本，使其不仅能做托管部署，也能部署在基于树莓派的网关上供家庭使用。还可以扩展到标准部署场景，如在使用 k8s 的大型云平台上进行“公共”部署，或在自己的基础设施上进行“离线”部署。

OCF 标准化 API（设备到云 API 和通用云接口 API），配以明智的技术选择（go-lang 和 MongoDB）和设计模式（Event Sourcing 和 CQRS），共同构成了这个成熟且互操作的物联网平台。

部署物联网平台需锁定供应商已成为历史，OCF 规范和 plgd 参考实现提供的端到端解决方案，实现了跨平台和跨域的安全的物联网连接。让使用者避免了必须选择特定部署模型甚至托管供应商的困境。希望物联网供应商在封闭的生态系统中制造越来越多碎片的时代一去不返，因为要支持所有平台的不同接口，对许多公司来说是昂贵的。若使用 plgd 云平台集成其他标准化的物联网系统，还能通过互联产生更多收益。





## 认证项目

为了确保云平台的合规性和互操作性，OCF 建立了通用云接口的认证项目。该项目利用了 OCF 现有的设备认证项目的成熟部分，如一般性认证程序、一致性测试工具（CTT）的框架和授权测试实验室等，使得一旦 OCF 通用云接口的技术细节完成（或更新）并发布，其认证项目就能快速部署。

OCF 在定义通用云接口时，同样致力于将技术要求转化为测试用例。编写测试用例是为了对所有必要技术要求进行全面测试。随着测试用例的开发，需要开发人员在 CTT 中同步集成引擎更新。这是一项十分复杂的工作，因为要测试客户端云，CTT 必须完全模拟设备云，反之亦然。经过大量的开发工作和内部测试，OCF 现已能对厂商的云平台进行测试认证。

早在 2019 年 12 月，OCF 就举办了首次针对通用云接口的多供应商互操作性测试活动（MVITE）。当时由于 OCF 对 CTT 的实现以及厂商对通用云接口的实现都处于早期阶段，因此进行了大量的故障排除工作，并确定了很多在 OCF 规范和 CTT 实现中需要更正的细节。几个月后的 2020 年 5 月，OCF 举办线上 MVITE，再次对通用云接口规范及其 CTT 测试用例进行验证。

2020 年 8 月，通用云接口认证项目正式发布，那时已知的遗留问题都已解决。希望认证通用云接口的 OCF 成员公司可登录 OCF 认证管理系统（<https://cms.openconnectivity.org>）提交待测云平台的接口给授权测试实验室。通过认证的公司及其云平台将在 OCF 认证产品清单上公布（<https://www.openconnectivity.org/certified-products>）。