

Aliro 简介

Aliro 是一种全新的标准化凭证与通信协议，旨在提供更可靠、流畅、具备互操作性的移动凭证体验，为安全访问奠定基础。该协议由连接标准联盟（Connectivity Standards Alliance, CSA）携手多家专业科技公司共同支持，致力于提升移动设备与门禁读卡器之间的兼容性，并将用户便利性与安全性确立为基本设计原则。

首个 [Aliro 1.0 协议](#) 于 2026 年 2 月 26 日发布，是一种统一、安全的数字门禁控制方法，适用于住宅和商业环境。

基于通用通信协议与长期落地验证的技术：

Aliro 支持近场通信 (NFC) 技术，可轻触开门；支持蓝牙低功耗 (Bluetooth LE) 技术，可进行身份验证；并支持超宽带 (UWB) 技术，助力实现基于位置的免提解锁。

Aliro 有助于在不同厂商的硬件及移动平台之间实现一致而流畅的“轻触进门”体验。该标准定义了统一的信令协议，减少了数字门禁生态中开发者和消费者的摩擦。

物理门禁控制系统的互操作性、用户体验与 Aliro 1.0 验证:

随着移动凭证、标准化凭证框架以及互联设备生态系统的广泛采用,物理门禁控制系统 (Physical Access Control Systems, PACS) 正经历快速演进。诸如 Aliro 1.0 等框架,以及蓝牙低功耗、近场通信和超宽带等长期落地验证的无线技术,正在让跨越用户、设备和基础设施的可互操作门禁体验成为可能。

PACS 原始设备制造商 (OEM) 正面临日益增长的压力,需要在多样化的部署环境中同时应对以下方面的要求:规范一致性、互操作性、强健的安全性以及直观的用户体验。

UL Solutions 通过提供第三方测试服务,助力 PACS OEM 证明其设备符合 Aliro 1.0 的各项要求。

我们的测试内容:

CSA-IoT Aliro 1.0 支持

- 按照 Aliro 1.0 规范进行测试
- 评估基于 Aliro 的移动凭证在用户设备与读卡器之间的交互表现。

连接性与互操作性

- 测试 Wi-Fi、Bluetooth、NFC 以及基于 IP 的通信行为,验证其是否符合 Aliro 规范要求
- 设备对设备、设备对平台的互操作性:涵盖读卡器、控制器、移动设备及应用程序在内的生态系统交互

我们支持的用例:

- PACS 面板、读卡器和门禁设备
- 基于 Aliro 1.0 的门禁生态系统
- 移动凭证和基于钱包的门禁解决方案
- 企业、商用及校园级部署





UL Solutions 是少数几家获得授权的实验室之一。我们在互联技术端到端测试服务方面拥有十多年的专业经验, 支持的技术包括 Bluetooth、Matter、Thread 和 Zigbee 等。

自 CSA Aliro 认证计划启动以来, UL Solutions 即获授权, 可开展 Aliro 认证测试。UL Solutions 根据 CSA 认证政策中规定的方法, 为读卡器和用户设备提供认证测试。

CSA 授予的 Aliro 认证类型

1. Aliro 产品硬件解决方案

- 指至少助力实现了 Aliro 规范中各项强制性要求的硬件设计。提交测试的 Aliro 硬件解决方案应为完整的方案（最终产品）。

2. Aliro 软件组件解决方案

- 指在支持的操作环境 (SOE) 上下文中运行, 且符合 Aliro 软件组件各项强制性要求的软件产品。
- 其本身不应为可证明 / 可调试的 Aliro 硬件设备。
- 目前, 只有 Aliro 软件组件计划下的“用户设备”功能可获得认证。

若某个 Aliro 解决方案可同时作为 Aliro 产品硬件解决方案, 以及在 SOE 上运行的 Aliro 软件组件解决方案, 则该方案可针对两种类型分别进行认证。否则, 该解决方案应作为 Aliro 产品硬件解决方案进行认证。

下图说明了 Aliro 产品硬件解决方案与 Aliro 软件组件解决方案之间的认证差异。



图形来源: 认证机构, 连接性标准联盟 (CSA-IoT), 认证政策文件

Aliro 从属认证计划

Aliro 不对网络层和应用层解决方案分别开展认证。Aliro 硬件解决方案的认证依赖于从属认证计划(DCP)所提供的从属认证。

从属认证为 Aliro 硬件解决方案开发者提供了一种机制,使其能够证明产品的连接能力(包括硬件与软件)已按照 Aliro 对各类连接能力选项的基本要求取得了认证。这一机制允许由集成电路制造商、模块或平台提供商,或 Aliro 硬件解决方案制造商完成认证。当此类经过外部认证的组件被用于产品中时,其认证即被继承,成为 Aliro 解决方案的一部分。

Aliro 当前支持的从属认证计划如下:

1. NFC Forum 认证计划: (认证版本 C14 或以上):

- 读卡器设备的 NFC 部分至少应获得 CCC 数字钥匙读卡器设备的认证。
- 用户设备的 NFC 部分至少应获得 NFC Forum 设备要求第 3.3 版中定义的 CCC 数字钥匙 CE 设备认证。

2. 蓝牙技术联盟 (Bluetooth SIG): 对于符合 Bluetooth 相关定义的最终产品类型,Bluetooth LE 版本应为 v4.2 或以上。

- UWB PHY/MAC: Aliro UWB 功能遵循 [FiRa Consortium](#) 在 Core Certification Release 4.0 或以上版本中的定义。读卡器设备的 UWB 部分应获得 Aliro UWB 功能(读卡器设备)的认证。
- 用户设备的 UWB 部分应获得 Aliro UWB 功能(用户设备)的认证。

在申请对新增或经修订 / 更新的 Aliro 解决方案进行 CSA 认证的过程中,将核实各 Aliro 硬件解决方案所支持连接能力是否符合从属认证的要求。



认证流程

Aliro 认证对 CSA 成员公司开放。通过认证的产品，其申请公司将被授予 Aliro 认证状态。认证权益包括获得使用 Aliro 认证标志的许可。

1

测试

- 完成开发并选择一家授权测试实验室 (ATL)，例如 UL Solutions，按照 Aliro 规范进行产品测试。
- ATL 根据 CSA-Aliro 的测试计划、规范、认证政策及程序安排并执行测试。
- 在成功获取相关认证数据后，ATL 将最终产品测试结果提交至 CSA 进行终审。

2

向 CSA 提交申请：

- 申请人应通过 CSA 认证门户填写并提交认证申请，申请材料包括 PICS、DoC、DCP (从属认证)、声明及认证费用。

3

审核

- CSA 对 ATL 提交的测试结果以及申请人提交的相应申请进行审查。
- 与测试结果相关的问题将转发给 ATL 审批。
- 若提交的测试结果符合 Aliro 规范要求，CSA 将在收到结果后的两到三周内向申请人签发产品证书，该产品将立即列入 CSA 的认证产品公共数据库中。