Aliro

Open, Certificate-Based Identity for Enterprise Access

Safetrust delivers interoperable physical and mobile credentials built on the Connectivity Standards Alliance Aliro standard, connecting physical access, mobile identity, and enterprise certificate infrastructure in one modern, identity-first platform.

What Is Aliro?

Aliro is the industry specification for access credentials and reader communication, developed by the Connectivity Standards Alliance with support from more than 400 partner organizations.

Safetrust operationalizes Aliro through Credential Manager, its cloud-based platform for issuing, managing, and trusting certificate-based credentials across mobile devices and readers. The result is interoperable, secure access that eliminates proprietary lock-in and aligns with enterprise PKI and Zero Trust principles.

Safetrust Inc. | safetrust.com
sales@safetrust.com

Why Is Aliro Important?

- **Eliminates reliance on shared secrets** through certificate-based authentication and mutual authentication between credential and reader
- **Enables cryptographically enforced trust** for federated identity across organizations, multi-tenant buildings, and supply chains
- **Supports unified credential management** for mobile and physical formats on a single platform, reducing duplication
- **Delivers cryptographic agility** with plans for post-quantum readiness (FIPS 203/204 alignment) so systems adapt without hardware replacement

How Does Aliro Work?

Aliro uses public-key cryptography to establish verifiable trust between credentials and readers. This protocol-based approach forms the foundation for scalable, interoperable access orchestration across devices and organizations.

- When a credential is created, a unique key pair is generated.
- The private key remains on the credential, while the public key is signed by the issuer and stored as a certificate.
- Readers are provisioned with the issuer's public certificate, enabling them to validate trusted credentials.
- When a credential is presented, the reader verifies its authenticity and performs mutual authentication with the credential.
- Once trust is established, credential data is securely transmitted.

Interoperability

Managing issuer public certificates on readers allows organizations to control which devices are authorized to read credentials. Credentials from one organization can be trusted across readers from multiple manufacturers, eliminating the need for complex symmetric key exchange.

No More Lock-in

Aliro removes dependency on proprietary secret keys tied to specific card or reader manufacturers. Credentials, whether physical or mobile, can be issued by one or more providers and used across a broad ecosystem of compatible readers.

Unified Platform

Aliro supports both mobile and card-based credentials within a single platform. In contrast, legacy approaches often require separate systems, leading to duplicated user records and, in many cases, different credential numbers for each format.

Safetrust Inc. | safetrust.com
sales@safetrust.com

Why Connected Readers Matter

Connected readers are required to support certificate lifecycle operations in alignment with enterprise certificate infrastructure, including issuance, renewal, and revocation.

Certificate-based systems follow established IT security practices such as defined expiration periods, renewal mechanisms, and revocation capabilities. Implementing Aliro with connected readers enables operational flexibility, including quick response to breaches and dynamic control of issuer credentials in multi-tenant environments. Manual, on-site certificate management is not scalable and introduces unacceptable delays in time-sensitive scenarios.

Aliro from Safetrust

Operationalizing Certificate-Based Identity for Your Access Platform

Mobile Credentials

Safetrust supports Aliro credentials via BLE on iOS and Android, and NFC on Android. NFC credentials are also supported in Safetrust Wallet, Apple Wallet, Google Wallet, and Samsung Wallet.

Physical Credentials

Safetrust supports Aliro on secure element cards from multiple silicon chip providers, with expanded enterprise availability through partnerships delivering certified physical credentials at scale. A lower-cost optimized option is planned for summer 2026.

FIDO2 and Legacy Compatibility

Safetrust extends Aliro beyond physical access by supporting FIDO2 for IT authentication and interoperability with legacy credential formats. Credential Manager unifies identity across physical and logical domains, enabling smooth migration from older technologies.

Federated Identity Across Organizations

Safetrust enables Aliro's federated identity model through Credential Manager, brokering trust via certificate exchange and centralized policy control, allowing credentials to be accepted across organizations without reissuance.

Certificate Management

Safetrust's cloud platform centralizes certificate lifecycle management, including issuance, rotation, revocation, and policy enforcement. This applies across both readers and credentials.

Interoperability

Safetrust supports flexible credential issuance models, including customer-managed issuers, Safetrust-managed issuance, or third-party issuers. In all cases, certificates are securely provisioned and managed through Credential Manager, enabling trusted use of credentials across compatible readers.

Cryptographic Agility

Safetrust delivers cryptographic agility through centralized certificate management and over-the-air policy updates, enabling adoption of new standards (including post-quantum readiness) without hardware replacement.

Safetrust Inc. | safetrust.com
sales@safetrust.com

Summary

Aliro establishes an open, certificate-based standard for interoperable, chip-independent access credentials. Safetrust operationalizes this standard through Credential Manager, delivering centralized certificate lifecycle management, federated trust, and unified identity across physical and logical access.

By combining Aliro's interoperability with cloud-based orchestration, Safetrust enables organizations to securely issue, manage, and trust credentials across devices and environments, eliminating proprietary dependencies and serving as the control plane for scalable, certificate-based access architectures.

Continue Exploring Aliro

Visit safetrust.com/aliro for the latest resources, including webinars, press releases, blogs, white paper, and the latest deployment updates. Request a demo to see it in action.

Safetrust Inc. | safetrust.com
sales@safetrust.com