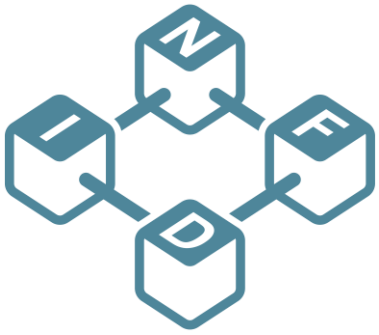
TECHNOLOGY ASSESSMENT BRIEF



Aliro and the NFID Foundation: Completing the Access Control Stack

Prepared by: NFID Foundation

NFID Foundation - Home

Salvatore (Sal) D'Agostino, IDmachines, Editor

March 2026

Version 1.0

Executive Summary

Two significant initiatives are reshaping how mobile devices interact with physical access control systems. **Aliro**, the Connectivity Standards Alliance's open communication protocol (v1.0 released February 18, 2026; CSA Document 26-42802-001), standardizes how a mobile device securely talks to an access reader—solving the transport problem. The **NFID Foundation**, a non-profit consortium advancing Self-Sovereign Identity for the security industry (launched April 2024), standardizes what the device presents and what it proves about the person behind it—solving the credential problem: binding authority, identity, identifiers, authorization, and authentication into a single, verifiable presentation.

These are not competing initiatives. They operate at different layers of the access control stack and are **naturally complementary**. Aliro is the secure pipe; NFID is the meaningful payload. Aliro tells a facility that a valid device is at the door. NFID tells the facility who is at the door, why that person should be granted access, and—through selective disclosure—only the minimum information needed to make that decision.

Together, they form a complete access control stack: Aliro providing cross-manufacturer device-to-reader interoperability, and NFID providing the decentralized credential layer that delivers **privacy by design**, **stronger cybersecurity**, **higher assurance including age verification**, **economic savings through wallet independence**, and **convergence of physical and digital access under a single holder-controlled credential**. Without a credential layer like NFID, Aliro is a better card reader. With it, Aliro becomes the front end of a fundamentally more trustworthy access system.

The Access Control Stack: Two Problems, Two Layers

Physical access control has always involved two distinct problems: how to communicate a credential securely (the transport layer) and what that credential means, who issued it, and what privileges it carries (the credential layer). Traditional PACS collapsed both into a single card—a proximity or smart card that was simultaneously the communication medium and the credential. The result was a system where the card was the identity, leading to well-known weaknesses: lost cards, cloned cards, shared cards, and no way to know who actually used the credential.

Mobile access control is now disaggregating these layers, creating an opportunity to solve each problem properly with purpose-built standards:

Layer	Problem Solved	Standard
Transport	How does a device securely communicate with a reader across manufacturers and platforms?	Aliro 1.0 (CSA) — NFC, BLE, UWB protocol with ECDSA/ECDH P-256 mutual authentication and AES-256-GCM encrypted channel
Credential	What is being presented, who issued it, what does it prove about the person, and what privileges does it carry?	NFID Foundation — Verifiable credentials, decentralized identifiers, and blockchain root of trust

A note on terminology: in access control, the word “identity” is often used loosely and risks conflating very different functions. What the credential layer actually encompasses is five distinct concepts that NFID binds together into a single verifiable presentation:

Concept	What It Means in Access Control
Authority	Who issued the credential and under what governance? A state DMV, a corporate HR system, an EU member state under eIDAS 2.0? The trust in the credential begins with the trust in its issuer.
Identity	The binding of a real person to their digital representation. The specific assertion that this credential belongs to this person—established through identity proofing performed by the issuing authority.
Identifier	The technical handle—a decentralized identifier (DID)—that refers to the person without revealing personal information. Unlike a badge number assigned by a facility, a DID is holder-controlled and portable.
Authorization	What privileges and attributes does the credential carry? Age over 21, building clearance level, contractor status—selectively disclosed based on what a specific access point requires.
Authentication	Proof that the person presenting the credential is the person bound to it. Cryptographic key possession in a Secure Element, optionally reinforced by biometric binding.

Traditional access control systems typically handle only one or two of these concepts—often just an identifier and a rudimentary authentication (card tap). NFID’s architecture addresses all five, binding them cryptographically so that a single verifiable presentation at the reader carries the full chain: who issued it, who it belongs to, how to refer to them, what they’re authorized to do, and proof that the presenter is the rightful holder.

Neither layer operates in isolation from the infrastructure behind the reader. The access decisions that Aliro and NFID enable at the door still need to travel securely from reader to controller. **SIA OSDP** (Open Supervised Device Protocol) is already widely adopted for this purpose. Both Aliro and NFID can leverage this existing infrastructure, reducing development effort and accelerating market acceptance by building on a reader-to-controller channel that integrators and end users already trust and specify.

OSDP’s encrypted, bidirectional communication and supervisory monitoring also strengthen the overall security posture of a combined deployment. When both layers are present and OSDP secures the back channel, the result is an access control system where interoperability is guaranteed at the door (Aliro), trust is guaranteed in the credential (NFID), and the decision travels over an encrypted, monitored channel to the controller (OSDP). When only the transport layer is present, the system can verify that a device belongs—but not that a person does.

Aliro: The Transport Layer

What Aliro Does Well

Aliro is a standardized communication protocol and common credential format created by the CSA to enable interoperability between mobile devices, wearables, and access control readers from different manufacturers. Evolved from Apple's proprietary HomeKey implementation and a derivative of the UnifiedAccess protocol family, Aliro 1.0 (released February 18, 2026) specifies three communication configurations using NFC (tap-and-go), NFC + BLE (click-to-unlock), and NFC + BLE + UWB (hands-free with precise ranging via secure UWB ranging).

The protocol is built on strong cryptographic foundations specified in detail in the released v1.0 specification: ECDSA/ECDH with P-256 curves per FIPS 186-5 for digital signatures and key agreement, AES-256-GCM per NIST SP 800-38D for session encryption (with three derived session key types: ExpeditedSK, StepUpSK, and BleSK), compressed X.509 certificates in a custom profile0000 format for attestation, and mutual authentication ensuring both reader and device verify each other before exchanging data. The protocol operates in two phases: an expedited phase for fast key-based access decisions (subdivided into expedited-fast using cached Kpersistent symmetric keys and expedited-standard using ECDH key agreement), and a step-up phase based on ISO 18013-5 mdoc for presenting Credential Issuer-signed Access Documents containing access rules, schedules, and permissions encoded in CBOR. Private keys reside in device Secure Elements and never leave the device. Key derivation follows NIST SP 800-56A Rev 3 and HKDF per RFC 5869. The specification also references GlobalPlatform SCP11 Amendment F for secure channel operations.

With nearly 200 CSA member companies participating—including Apple, Google, Samsung, Allegion, ASSA ABLOY, dormakaba, Kastle Systems, LEGIC, NXP, and STMicroelectronics—and early products from Aqara, SwitchBot, and Nuki, Aliro represents a serious, well-backed effort to solve reader interoperability.

Aliro's contribution is real and valuable. The absence of a common mobile-to-reader protocol has been a genuine barrier to mobile access adoption, forcing proprietary lock-in at the reader level. Aliro removes this barrier.

What Aliro Leaves Unfinished

By design, Aliro addresses only the transport layer. The "credential" in Aliro is a device-bound cryptographic key stored in a Secure Element—not a verifiable claim about a person. While the released v1.0 specification does define an Access Document structure (based on ISO 18013-5 mdoc format) that can carry Credential Issuer-signed access rules, schedules, permissions, and an optional ID field, these are access-control-specific data elements within the Aliro namespace ("aliro-a")—not general-purpose identity attributes. The protocol carries no identity attributes in the W3C VC or SSI sense and supports no selective disclosure of identity data. However, Aliro's step-up phase is architecturally built on the ISO 18013-5 DeviceRequest/DeviceResponse framework — the same framework used by mDLs and EUDI

Wallet credentials — and its Access Documents employ CBOR encoding with integer-keyed maps for compactness, structurally analogous to NFID's own compact binary encoding. This architectural alignment represents the most natural integration point for NFID credentials: the step-up phase's document exchange is designed for extensibility via additional document types and namespaces.

Aliro 1.0 does define a Credential Issuer trust framework with X.509 certificate chains: Access Documents are signed by a Credential Issuer key, the Credential Issuer may hold a certificate from a Credential Issuer CA, and Readers are provisioned to trust specific Credential Issuer public keys or CA certificates. The cryptographic mechanics of this trust chain are well specified. However, the specification is entirely silent on the governance layer above those mechanics:

- **No issuer registry:** There is no registry of Credential Issuers, no mechanism for discovering who is authorized to issue Access Documents, and no public record of which entities operate as Credential Issuer CAs. Any entity that can provision its public key or CA certificate onto a Reader becomes a trusted issuer for that Reader—with no external accountability.
- **No issuer qualification requirements:** The specification defines no criteria for what an entity must demonstrate to become a Credential Issuer or Credential Issuer CA. There are no governance requirements, no audit obligations, no transparency mandates, and no accountability framework.
- **No purpose limitation or legal basis:** The Access Document structure contains no data elements that communicate the purpose for which data is collected, the legal basis justifying the collection, or the retention and use policies that govern it.
- **No root-of-trust governance:** The Credential Issuer CA is a cryptographic root of trust, but the specification defines no requirements for how that root must be established, maintained, audited, or governed. There is no equivalent of the WebPKI's CA/B Forum baseline requirements, no equivalent of eIDAS trust lists, and no mechanism for revoking a misbehaving CA at the governance level. This governance gap is the most significant architectural difference between Aliro and NFID. While Aliro's cryptographic mechanics are sound, the absence of a governance layer above those mechanics means that the trust chain cannot be independently audited, issuer legitimacy cannot be externally verified, and regulated environments cannot demonstrate compliance with purpose limitation or legal-basis requirements.

In short, Aliro's issuer trust is mechanical—"this key signed this document, and this CA vouched for this key"—but not governed. The specification answers "can this signature be verified?" but not "should this entity be issuing credentials, under what authority, for what purposes, and with what accountability?"

Aliro does not specify how readers integrate with back end PACS systems, does not address access policy or identity management, and explicitly leaves everything behind the reader to existing infrastructure. In PACS terms, Aliro replaces the card-to-reader layer with a standardized mobile equivalent. The phone becomes a better card. The system behind the reader remains unchanged. SIA OSDP, already widely adopted for reader-to-controller communication, provides the existing infrastructure for this integration. NFID working group members have already demonstrated attestation data flowing over OSDP to standard access control panels.

Aliro 1.0 does include a “User Authentication” mechanism (Section 8.3.1.14), but its design reinforces rather than closes the person gap. The Reader sends an authentication_policy byte in the AUTH0 command with three defined values: “User device setting” (0x01, defer to the device’s own policy), “User device setting – secure action” (0x02, same but signals a lock/arm action), and “Force user authentication” (0x03, the device SHALL perform authentication or terminate). The specification states that the means of authenticating the user “are left to the User Device implementation” and “can include passcode or biometrics.”

However, this mechanism has five critical limitations. First, there is no verifiable proof: the signaling_bitmap returned in the AUTH1 response contains no bit indicating whether user authentication was actually performed—the Reader must trust the device’s implicit assertion. Second, the specification defines no biometric modality requirements, no template quality thresholds, no liveness or presentation attack detection requirements, and no false acceptance/rejection rate targets. Third, no biometric data of any kind transits the Aliro protocol; the Reader receives a cryptographic key assertion, never a biometric verification result. Fourth, a compromised or modified device could assert the key without performing authentication, and the Reader would have no way to distinguish this from a legitimately authenticated transaction. Fifth, even the “Force” policy (0x03) is explicitly recommended against for BLE+UWB passive entry flows—precisely the hands-free scenario where unauthorized device use is most likely.

What this means for Aliro: Aliro’s user authentication is a one-way hint from Reader to device, not a verifiable proof. Compare with PIV, where biometric matching per NIST SP 800-76-2 produces verifiable results, or FIDO2/WebAuthn, where the authenticator data includes a cryptographically bound userVerification flag. Aliro has neither server-verifiable nor reader-verifiable proof that the person holding the device is the authorized user. The person gap remains structurally open.

This creates four gaps that the credential layer must fill:

- **The person gap:** Who is holding the device? Aliro’s authentication_policy mechanism is a non-verifiable hint, not an answer. The Reader has no way to confirm that user authentication occurred.
- **The attribute gap:** Is the person authorized for this space, at this time, with these qualifications? Aliro carries no attributes to evaluate.
- **The assurance gap:** How confident is the facility that the credential is legitimate, current, and presented by its rightful holder? Aliro provides device-level assurance only.
- **The trust governance gap:** Who authorized the Credential Issuer? Under what governance framework does it operate? Aliro’s cryptographic trust chain has no governance layer above it—no registry, no qualification criteria, no legal-basis requirements, and no mechanism for holders or relying parties to evaluate issuer legitimacy beyond raw key possession.

NFID Foundation: The Credential Layer That Completes the Stack

What the NFID Foundation Provides

The NFID Foundation is a non-profit consortium launched in April 2024, dedicated to advancing Self-Sovereign Identity within the security industry. Founded by PassiveBolt CEO Kabir Maiga, with founding members including LEGIC, PDQ, TECH5, ZKTeco USA, Z-bit Systems, and IDmachines, the Foundation builds upon W3C, DIF, Trust over IP, and OpenWallet Foundation standards while addressing the critical gap those bodies have not covered: firmware and microcontroller implementations for the embedded devices that make up physical access control infrastructure. The working group meets biweekly and includes expertise spanning semiconductors, smart locks, biometrics, access control panels, identity management, and system integration. The Foundation defines open specifications and publishes reference implementations; member companies build independent commercial products and services on these specifications.

The NFID technology stack provides exactly the credential layer that Aliro's transport needs:

- **Decentralized Identifiers (DIDs):** Unique, non-transferable identifiers for persons, organizations, and devices. Published to a blockchain with no single point of failure. The holder proves control via private keys—not via a platform wallet or CA hierarchy.
- **Verifiable Credentials (Attestations):** Cryptographically verifiable credentials operating through the issuer/holder/verifier trust triangle. Organizations issue credentials; holders receive, store, and manage them; any entity can verify authenticity using registry-published public keys—without contacting the issuer.
- **Verifiable Trust Registry:** A registry architecture designed for decentralized identity resolution, hosting public cryptographic elements for independent verification. Unlike Aliro's bilateral provisioning model—where issuer trust is established privately between a Credential Issuer and whoever configures the Reader—NFID's registry architecture is designed to be public, discoverable, and independently auditable.
- **mdoc and W3C Credential Acceptance:** Explicit support for credentials in the ISO 18013-5 mdoc format—including mobile driver's licenses, digital passports, national identity cards, and EU Digital Identity (EUDI) Wallet credentials—as well as W3C Verifiable Credentials.
- **Firmware Verification Libraries:** A planned Foundation-published reference implementation (targeted for 2026 release) enabling hardware manufacturers to verify NFID attestations on embedded devices with limited computational power—enabling any Aliro-compatible reader to also verify NFID credentials without additional hardware.
- **Standardized Schemas:** A common credential format for physical access control and beyond, ensuring interoperability across the security industry.

How NFID Fills Aliro's Four Gaps

The person gap: NFID binds the credential to a person's decentralized identifier, not to a device. Biometric verification occurs on the holder's device before the credential is released—and unlike Aliro's authentication_policy hint, NFID's presentation security requirements are issuer-defined policies embedded in the credential itself — ensuring biometric verification is mandated by the credential's trust chain before the credential is released, rather than relying on a per-transaction reader hint with no verifiable proof of compliance. The facility knows a verified person—not just a valid phone—is at the door.

The attribute gap: NFID credentials carry verifiable attributes—employer affiliation, access authorization, age assertions, regulatory training, clearance levels—any of which can be selectively disclosed per transaction. Critically, the NFID Access Attestation data model includes explicit fields (externalCredentialId and externalCredentialData) for bridging to existing PACS infrastructure. These attributes allow an NFID attestation to carry a backward-compatible credential identifier — such as a card number or site-specific token — that legacy panels and controllers can consume through their native access decision logic. This means NFID does not require rip-and-replace: a facility can accept NFID attestations at the reader while its existing panel infrastructure processes a familiar credential format behind the reader. Beyond static attributes, the NFID Access Attestation data model defines granular, time-bound access authorizations with embedded schedule configurations (time-based, day-of-week, weekly, and exception-based patterns with recurrence rules) and access modifiers (administrator privileges, emergency override, extended door time, privacy exemption, remote unlock, and biometric/PIN exemption flags) — all encoded in a compact CBOR binary format optimized for resource-constrained embedded devices. This level of access control granularity, purpose-built for physical security, goes substantially beyond Aliro's capabilities bitmask and schedule model.

The assurance gap: When the credential originates from a government mDL, digital passport, or EUDI Wallet, the identity proofing behind it was performed by a state authority to the highest assurance level. The NFID credential carries this assurance forward cryptographically.

The trust governance gap: NFID's verifiable registry is architected to provide what Aliro's Credential Issuer framework lacks: a public, discoverable, auditable record of who is issuing credentials and under what authority. Issuers publish their DIDs and associated governance assertions to the blockchain. The Trust over IP governance framework that NFID builds upon defines requirements for purpose limitation, legal basis, and accountability that Aliro's specification does not address. When a government authority issues a credential through the NFID ecosystem, the governance chain is traceable: the issuing authority is identifiable, its authorization is verifiable, and the legal framework under which it operates is discoverable—not merely assumed from the presence of a provisioned public key.

Use Case: The Turnstile as Access Gate and Age Gate

Consider how the combined stack works in practice. A turnstile at the entrance to a venue, campus, or regulated space needs to perform two functions: verify access authorization and confirm the entrant meets an age requirement.

With Aliro Alone

The turnstile authenticates a device key via NFC/BLE and opens if the key is valid. There is no way to verify the person's age. A separate age verification system must be deployed alongside. Two systems, two points of friction, two cost centers, and no cryptographic link between the access decision and the age check.

With Aliro + NFID

The person presents a verifiable credential—from an NFID-issued attestation, a government mDL, a digital passport, or a EUDI Wallet—**over Aliro's secure communication channel**. In a single transaction, the turnstile's reader simultaneously verifies access authorization and confirms an age assertion through selective disclosure. The holder does not reveal their full date of birth, name, or photo; the verifier receives only a cryptographically signed "over 21" or "over 18" assertion. The turnstile opens for authorized, age-verified individuals in a single tap—one system, one interaction, one cryptographic proof chain.

Privacy Benefits

- **Data minimization by design:** Selective disclosure is designed to ensure only the minimum attributes required for a specific access decision are revealed.
- **No centralized PII database:** Credentials are held by the person and verified cryptographically. The facility operator dramatically reduces its PII footprint compared to traditional PACS — identity verification occurs cryptographically, and any enrollment data required for access management is minimized to operational necessity rather than stored as a centralized identity database.
- **Consent-based sharing:** Every credential presentation requires the holder's active consent. Critically, the NFID framework supports purpose limitation and legal-basis communication that Aliro's Access Document structure does not.
- **No phone-home surveillance:** Credential verification occurs locally between holder device and reader using registry-published public keys.

What this means for Aliro: Aliro provides the encrypted communication channel that protects NFID's minimal data disclosures in transit. Without NFID's selective disclosure, there is no identity data to protect—but also no identity data to use.

Cybersecurity Benefits

- **Person-bound credentials eliminate the leading PACS attack vector:** Aliro's device-bound PKI keys are harder to clone than legacy cards, but the device can still be used by someone other than the authorized person. Aliro's authentication_policy mechanism (Section 8.3.1.14) sends a hint to the device requesting passcode or biometric verification but provides no verifiable proof back to the Reader that it occurred—a compromised or shared device can assert the key without authentication. NFID's credentials are bound to a decentralized identifier with on-device biometric verification before credential release, producing a cryptographically signed attestation that the verified holder is presenting.
- **Blockchain-anchored anti-forgery:** A forged NFID credential cannot reference a valid DID in the immutable trust registry. Two layers of defense.
- **No single point of CA failure—and no ungoverned CA trust:** Aliro's X.509 PKI relies on Certificate Authorities, but the specification defines no governance requirements for those CAs—no registry, no qualification criteria, no audit obligations, no transparency mandates. NFID's decentralized trust registry has no single CA to compromise, and issuer legitimacy is publicly verifiable against the blockchain registry.
- **Reduced attack surface:** Without a centralized PII database, there is no honeypot for attackers. Credential verification is local and cryptographic at both layers.
- **Revocation at both layers:** Aliro 1.0 defines a Revocation Document mechanism (Credential Issuer-signed, with ValidityIteration for lifecycle management) alongside standard X.509 CRL/OCSP; NFID provides complementary revocation of identity credentials via the verifiable data registry.

What this means for Aliro: Aliro's mutual authentication and Secure Element protection are genuine security improvements. NFID adds an identity authentication layer on top, closing the "who is holding the device" gap. Together, the system authenticates the device and the person.

Higher Assurance and Age Assurance

- **Government-proofed identity at the source:** When the credential originates from a government mDL, digital passport, or EUDI Wallet, the identity proofing was performed by a state authority to the highest assurance level.
- **Automated age assurance at the highest achievable level:** A signed "over 21" assertion from a government-issued credential is a cryptographically verifiable claim backed by government identity proofing—delivered over Aliro's authenticated, encrypted channel.
- **Continuous assurance without re-enrollment:** Verifiable credentials carry their own proof of validity. Each presentation is independently verified.
- **Audit trail with privacy:** Verifiable proof that an age check was performed—for compliance—without storing personal identity data.

What this means for Aliro: Aliro provides transport-level assurance. NFID provides identity-level assurance. A facility requiring age gating, identity verification, or regulatory compliance needs both.

Economic Benefits

- **Wallet-independent architecture:** NFID's credential model reduces dependency on any single platform's credential infrastructure, giving organizations flexibility in how credentials are delivered and eliminating per-user platform licensing as a cost driver.
- **Zero-touch onboarding:** NFID's verifiable credentials enable arrival with a pre-issued credential and access through Aliro's reader with zero manual enrollment.
- **Reduced breach liability:** By eliminating centralized PII databases, NFID removes the primary breach target.
- **Multi-function infrastructure:** A single Aliro + NFID turnstile replaces separate PACS reader and age verification systems.
- **No hardware lock-in:** NFID firmware libraries enable any manufacturer's Aliro-compatible reader to also verify identity credentials.

What this means for Aliro: Aliro reduces reader interoperability costs. NFID extends those savings by removing the credential tax, enabling zero-touch onboarding, and consolidating multiple verification functions into a single reader interaction.

Beyond the Door: Identity Convergence Across Physical and Digital Access

Aliro addresses physical access exclusively—doors, locks, entry points. Logical access is entirely out of scope. NFID's credential layer, however, is **not limited to physical access**. Because the credential is a W3C Verifiable Credential bound to a DID, the same identity infrastructure can authorize door access via Aliro, network login, application authentication, document signing, visitor verification, and cross-organizational trust.

Because NFID accepts any mdoc-format credential, a person arriving at an Aliro+NFID access point can present their **digital passport, EUDI Wallet credential, mDL, or any government-issued mdoc** as the identity basis for physical access—and use that same credential for logical access elsewhere. This creates the convergence that enterprise security teams have sought: **one identity, all access, physical and digital**.

Bringing It Together: The Turnstile Scenario

Function	Aliro Only	NFID Only	Aliro + NFID
Transport security	Mutual authentication, encrypted channel	Depends on available reader protocol	Aliro's encrypted channel protects NFID credential in transit
Access authorization	Device key valid / invalid	Person's verifiable credential checked	Device AND person authenticated
Age verification	Not possible	Signed age assertion via selective disclosure	Signed age assertion over secure channel in same tap
Identity assurance	Device-level only	Government-level identity proofing inherited	Transport + identity assurance combined
Privacy	No identity data exchanged	Selective disclosure; no PII stored	Minimal attributes over encrypted channel; no PII stored
Credential source	Platform wallet key	Any VC, mDL, passport, EUDI Wallet	Any credential, any wallet, any transport
Platform fees	Platform credential licensing	None	None — wallet-independent
Systems required	PACS reader + separate age system	Identity-aware reader	Single Aliro+NFID reader
Audit compliance	Access log only	Verifiable proof without PII	Complete audit trail, privacy-preserving

Standards and Specifications Landscape

Standard / Spec	Aliro (Transport Layer)	NFID (Credential Layer)
W3C Verifiable Credentials	Not used (Access Document uses mdoc/CBOR, not VC)	Core credential format
W3C Decentralized Identifiers	Not used	Foundation of identity model
ISO 18013-5 (mdoc)	Step-up phase uses mdoc DeviceRequest/Response for Access Documents	Accepts mdoc credentials: mDLs, passports, national IDs, EUDI Wallet
EUDI Wallet (eIDAS 2.0)	No relationship	EUDI mdoc credentials accepted; bridge to EU government digital IDs
DIF / ToIP / OpenWallet	No relationship	Builds upon; extends to embedded/firmware
Apple HomeKey	Direct ancestor; Aliro generalizes cross-platform	Independent
CCC Digital Key	Sibling; shared UnifiedAccess lineage	Independent
Matter (CSA)	Complementary for remote lock management	Independent
SIA OSDP	Compatible; reader decisions travel to controller over OSDP	Compatible; identity-rich decisions travel over OSDP
X.509 / ECDSA / ISO 7816	ECDSA/ECDH P-256, compressed X.509 (profile0000), ISO 7816-4 APDUs	Uses public-key cryptography; not X.509-dependent Note: Both Aliro and NFID build on the ISO 18013-5 framework, using it for different purposes — Aliro for access-specific data exchange, NFID for identity-rich credential presentation. This shared foundation defines the technical integration path between the two layers.

Industry Participation

Aliro (Transport Layer)

Nearly 200 CSA member companies. Key participants: Apple, Google, Samsung (platforms); Allegion, ASSA ABLOY, dormakaba, Kastle Systems (access control); LEGIC, NXP, STMicroelectronics, Nordic, Infineon, Qualcomm, Qorvo (silicon/smart card). Early products from Aqara, SwitchBot, Nuki.

NFID Foundation (Credential Layer)

Founding members: PassiveBolt (Web3 access control), LEGIC (semiconductor/smart card), PDQ (smart locks), TECH5 (biometrics), ZKTeco USA (biometric readers/locks), Z-bit Systems (physical security), IDmachines (identity management/physical security). dormakaba is active in both ecosystems. SIA education partnerships for industry adoption. Several other credential and access standards initiatives are active in adjacent spaces, including LEAF and PKOC. NFID's differentiation is its identity-first approach — consuming government-issued identity at the point of access — rather than defining a new credential format or transport protocol.

The Path Forward: Toward a Complete Stack

The released Aliro 1.0 specification does not include a mechanism to carry verifiable credentials as a payload—its credential format is a device-bound PKI key, and its Access Document structure carries only access-control-specific data elements within the "aliro-a" namespace. However, the architectural foundation is significant: Aliro's step-up phase already uses the ISO 18013-5 DeviceRequest/DeviceResponse framework, the same framework used by mDL and EUDI Wallet credentials.

The **architectural alignment is now concrete, not hypothetical**: Aliro provides a secure, authenticated, AES-256-GCM encrypted channel between device and reader with an mdoc-based document exchange mechanism already in place; NFID provides a verifiable, privacy-preserving credential to transmit over that channel. The integration point is the step-up phase's DeviceRequest/DeviceResponse exchange, which is designed for extensibility via additional document types and namespaces.

Several market forces are driving toward this convergence:

- **Regulatory momentum:** Privacy laws increasingly require purpose limitation and transparency about legal basis—all native to NFID's SSI model, none addressed by Aliro's transport layer. Aliro's Credential Issuer framework provides no mechanism for communicating purpose, legal basis, or governance context.
- **Government digital ID at scale:** As millions of mDLs, digital passports, and EUDI Wallet credentials enter circulation in mdoc format, facilities will need readers that can accept these credentials. Aliro's readers need a credential layer to do so.
- **Enterprise convergence demand:** Security teams are seeking unified credential frameworks across physical and logical access. Aliro provides the physical entry point; NFID provides the credential fabric.
- **Economic pressure:** The cost pressure associated with platform-dependent credentialing creates demand for wallet-independent identity solutions.
- **Trust escalation:** Regulated environments increasingly require auditable, governed trust chains, not bilateral key provisioning with no external accountability. Aliro's Credential Issuer trust model cannot demonstrate to a regulator who authorized the issuer. The combined stack delivers governed trust; Aliro alone does not. This convergence is not

theoretical. NFID working group members have demonstrated a functional end-to-end implementation: government-issued digital credentials consumed at a standard access control reader, identity resolved and authorized through a PACS integration layer, and access granted on standard panel hardware — using the architectural pattern described in this brief. The demonstration will be showcased at ISC West 2026.

Conclusion

Aliro and NFID are not competing standards. They are **complementary layers of a complete access control stack**. Aliro 1.0 solves the transport problem—standardizing how a mobile device securely communicates with a reader, with a released specification defining ECDSA/ECDH P-256 mutual authentication, AES-256-GCM session encryption, compressed X.509 certificates, and an mdoc-based Access Document exchange framework. NFID addresses the credential problem—binding authority, identity, identifiers, authorization, and authentication into a verifiable presentation anchored in a decentralized, privacy-preserving framework. And the wide adoption of SIA OSDP means both can build on an established reader-to-controller infrastructure.

Without a credential layer, Aliro is a better card reader—a genuine improvement, and with the released v1.0 specification a substantial one that includes access rules, schedules, and Credential Issuer-signed documents. But these access-control-specific data elements do not constitute identity, and Aliro's Credential Issuer trust framework—while cryptographically sound—operates without a registry, without issuer qualification requirements, without purpose limitation or legal-basis transparency, and without the governance layer that regulated environments and privacy law increasingly demand. **With NFID, Aliro becomes the front end of a system that authenticates persons, not just devices**; that verifies attributes like age in a single tap; that accepts government-issued digital credentials from passports to EUDI Wallets; that eliminates centralized PII databases; that operates free of platform-dependent credentialing costs; and that converges physical and digital access under a single, holder-controlled identity.

For organizations evaluating the trajectory of access control, the question is not which standard to adopt. The answer is both—Aliro for the transport, NFID for the credential—deployed on the widely adopted OSDP infrastructure already in place across the industry. Together, they deliver the privacy, cybersecurity, assurance, trust governance, and economic benefits that neither can achieve alone.

Appendix: References

Aliro

Connectivity Standards Alliance — Aliro Overview
https://csa-iot.org/all-solutions/aliro/

CSA — Aliro Specification v1.0 (Doc 26-42802-001, Feb 18, 2026)
https://csa-iot.org/developer-resource/specifications-download-request/

CSA — Aliro Provisioning Guidance (Doc CR-31968, pending)
https://groups.csa-iot.org/wg/aliro-tsg/document/31968

Apple — HomeKey and Aliro Support
https://developer.apple.com/wallet/

NFID Foundation

NFID Foundation — Official Website
https://nfidfoundation.org/

PassiveBolt — Web3 Access Control
https://passivebolt.com/

SecurityInformed — Launch Announcement (April 2024)
https://www.securityinformed.com/news/nfid-foundation-decentralized-identity-physical-security-co-9263-ga.1712834700.html

W3C Standards

Verifiable Credentials Data Model v2.0
https://www.w3.org/TR/vc-data-model-2.0/

Decentralized Identifiers (DIDs) v1.0
https://www.w3.org/TR/did-core/

ISO / EU / AAMVA - mDL eIDAS

ISO/IEC 18013-5:2021 — mDL
https://www.iso.org/standard/69084.html

AAMVA — mDL Implementation Guidelines
https://www.aamva.org/topics/mobile-driver-license

European Commission — eIDAS 2.0 Framework
https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation

SIA OSDP

SIA — OSDP Overview
https://www.securityindustry.org/industry-standards/open-supervised-device-protocol/

IEC 60839-11-5 — OSDP International Standard
https://webstore.iec.ch/en/publication/65084

Decentralized Identity Foundations

DIF
https://identity.foundation/

Trust Over IP Foundation
https://trustoverip.org/

OpenWallet Foundation
https://openwallet.foundation/

Industry

Allegion
https://www.allegion.com/

dormakaba
https://www.dormakaba.com/

LEGIC Identsystems
https://www.legic.com/

TECH5
https://tech5.ai/

ZKTeco USA
https://www.zktecousa.com/

PDQ Manufacturing — Smart Locks
https://www.pdqlocks.com/

IDmachines
https://www.idmachines.com/

Z-bit Systems — Physical Security
https://www.z-bitsystems.com/

IBM — Cost of a Data Breach Report 2024
https://www.ibm.com/reports/data-breach