The Public Key Era: Why LEAF Verified and Aliro Are Stronger Together

A technical overview of the industry's shift from symmetric to public key access control, and how physical and digital credentials fit together.

FEBRUARY 2026 | LEAF COMMUNITY

EXECUTIVE SUMMARY

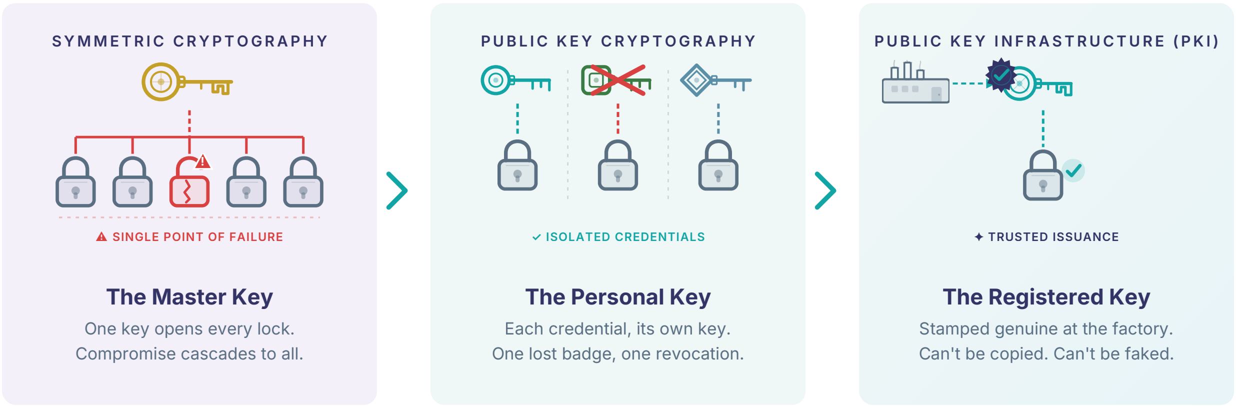
- Physical access control is transitioning from proprietary symmetric cryptography to open, public key standards, marking the most significant architectural shift in decades.
- **LEAF Verified** delivers public key security for physical credentials (cards, fobs), with cryptographic trust provisioned at the chip level through a direct NXP partnership.
- **Aliro** is the new CSA open standard for digital credential authentication on mobile devices, built on the same cryptographic foundation.
- These technologies are complementary, not competing. LEAF Verified solves the physical credential problem; Aliro solves the digital device problem. Together, they provide complete public key coverage across all form factors.

The Public Key Revolution Is Here

Physical access control is undergoing its most significant architectural shift in decades. For as long as the industry has existed, credentials and readers have relied on the same fundamental approach: symmetric cryptography, where a shared secret is distributed across every device in the system. Think of it as one master key that opens every lock. If someone copies it, every door in the building is compromised and fixing it means re-keying every lock and re-issuing every badge.

Public key cryptography changes this entirely. Each credential now holds its own unique private key that it never reveals, proving its identity through a mathematical challenge instead of a shared secret. If a badge is lost or stolen, deactivate just that one credential. No other lock or badge is affected. The key is unique, but nothing independently verifies who created it.

PKI (Public Key Infrastructure) closes that gap. A trusted authority stamps each key as genuine at the point of manufacture. Any reader can verify that stamp instantly. The credential does not just prove it holds a key; it proves the key was issued by a trusted source. It cannot be copied. It cannot be faked.



The Master Key
One key opens every lock.
Compromise cascades to all.

The Personal Key
Each credential, its own key.
One lost badge, one revocation.

The Registered Key
Stamped genuine at the factory.
Can't be copied. Can't be faked.

This progression, from shared secrets to unique keys to certified keys, is not theoretical. It is happening now. Keys no longer need to be distributed, stored, and rotated across every device. Compromised keys no longer put the entire system at risk. And because the standards are open, credentials are no longer locked to specific vendor ecosystems.

This is the same cryptographic infrastructure behind the HTTPS connections that secure every website you visit, online banking, and digital driver’s licenses, now applied to physical access control. Two developments are accelerating this transition across both cards and mobile devices. For cards, **MIFARE DUOX**, NXP’s public key IC platform, brings public key cryptography to physical credentials. For mobile devices, **Aliro**, the new open standard from the Connectivity Standards Alliance (CSA), defines how readers and other access devices communicate with mobile devices using public key authentication.

As excitement builds around both, a natural question has emerged: are these technologies competing for the same space?

They are not. LEAF Verified (the physical credential product built on MIFARE DUOX) and Aliro serve the same use case: secure access. But they do so through fundamentally different form factors, each with its own architectural constraints. One is built for physical credentials, cards and fobs that are passive, carry no battery or network connection, and ship fully provisioned from the factory, ready to authenticate out of the box. The other is built for digital credentials on connected devices, where both the device and the reader authenticate each other through mutual certificate exchange. The shift happening in access control is not a format war between competing standards. It is the entire industry moving from symmetric to public key cryptography, across both physical and digital credentials simultaneously.

> “The question is not which one wins. It is how they work together.”

Understanding the Layers: Chip, Credential, and Community

Much of the current industry discussion fails to clearly differentiate between three distinct things: a chip, a credential product, and a community. Separating them is essential to understanding the landscape clearly.

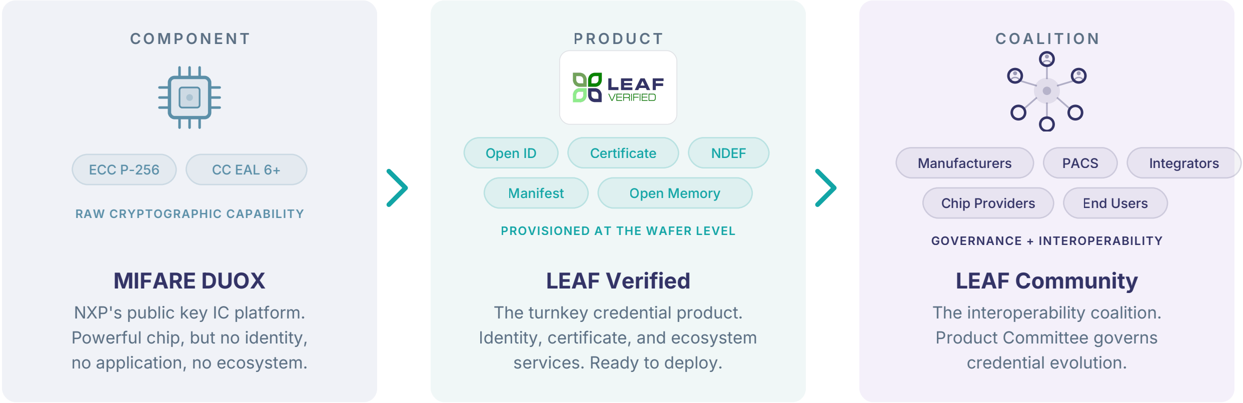
MIFARE DUOX: The Chip

MIFARE DUOX is NXP's contactless IC technology. It is the first MIFARE product to support public key cryptography, specifically elliptic curve cryptography (ECC) with ECDSA and ECDH on the NIST P-256 curve, certified at Common Criteria EAL 6+.

A blank DUOX chip is a component. It has powerful cryptographic capability, but on its own, it has no application, no identity, and no ecosystem to plug into. Anyone can purchase DUOX wafers from NXP's distribution network. What you build on them is what creates value.

> "A blank DUOX chip is to a finished credential what raw silicon is to a configured smartphone. The material matters, but it is not the final product."

The diagram below illustrates these three distinct layers: a chip, a credential product, and a coalition, each serving a fundamentally different role in the access control value chain.


COMPONENT
ECC P-256
CC EAL 6+
RAW CRYPTOGRAPHIC CAPABILITY
MIFARE DUOX
NXP's public key IC platform. Powerful chip, but no identity, no application, no ecosystem.
PRODUCT
LEAF VERIFIED
Open ID
Certificate
NDEF
Manifest
Open Memory
PROVISIONED AT THE WAFER LEVEL
LEAF Verified
The turnkey credential product. Identity, certificate, and ecosystem services. Ready to deploy.
COALITION
Manufacturers
PACS
Integrators
Chip Providers
End Users
GOVERNANCE + INTEROPERABILITY
LEAF Community
The interoperability coalition. Product Committee governs credential evolution.

LEAF Verified: The Credential Product

LEAF Verified is what happens when a DUOX chip is securely provisioned through a direct partnership between NXP and LEAF.

The distinction starts at the very beginning of the supply chain. Every LEAF Verified credential is provisioned at the wafer level, before it ever reaches a credential manufacturer. Cryptographic trust is established at the source, not added after the fact. This secure provisioning pipeline is the foundation that everything else builds on. While any organization can purchase blank DUOX chips, replicating the full stack (wafer-level PKI provisioning, federated identity issuance, enrollment tooling, and multi-vendor interoperability) requires deep infrastructure and supply chain partnerships that take years to build.

At its core, LEAF Verified delivers **card authenticity**: cryptographic proof that a credential is genuine, issued through a trusted supply chain. Like any access credential, a LEAF Verified card must still be enrolled into the access control system before it grants access at a door. But unlike traditional credentials, its security model is based on public key cryptography, and that authenticity is guaranteed from the point of chip manufacture, well before the credential is assembled into its final card or fob form factor. Every LEAF Verified credential ships with:

- **A Guaranteed Unique Open ID**: a federated, 12-digit identifier securely programmed at the wafer level. This is not a self-assigned number. It is guaranteed unique across the entire LEAF Verified ecosystem and serves as the credential's identity across any compatible reader or system. The 12-digit format was chosen deliberately to enable broad compatibility with existing access control infrastructure, including legacy systems that cannot support full or hashed public keys, and panels with limited memory for large credential databases. This allows organizations to bring modern public key security to the door without having to rip-and-replace their backend legacy panels and software that rely on standard Wiegand or limited-bit formats.

> "The 12-digit Open ID format was chosen deliberately to enable broad compatibility with existing access control infrastructure, including legacy systems."

- **A LEAF Certificate**: enabling any compatible reader to cryptographically verify the credential's authenticity. This goes beyond verifying that a public key and private key pair match. It verifies that the presented badge is an authentic LEAF Verified credential, issued through the trusted provisioning pipeline.

These are the foundation: the core security and identity that every LEAF Verified credential carries.

Physical Credential that Adds Value

Beyond this core, the LEAF Verified platform includes additional capabilities that customers can choose to leverage based on their needs:

- **Digital Credential Manifest**: every order of LEAF Verified credentials can include a digital footprint accessible via QR code or API. Rather than manually entering card numbers (a labor-intensive process and a common source of enrollment errors), access control systems can securely bulk-import credential data through the LEAF API. What traditionally takes days of manual data entry becomes a single scan.
- **NDEF (Tap-to-Phone)**: NDEF (NFC Data Exchange Format) is a standard data structure for NFC communication that allows a passive credential to transmit information, such as a URL, to any NFC-enabled smartphone with a simple tap. Each LEAF Verified credential includes a unique NDEF-encoded URL that can be dynamically redirected via API. This enables software providers to build custom workflows: self-service enrollment, mobile wallet provisioning, help desk routing, and more.
- **Open Memory**: LEAF Verified credentials include DESFire-compatible memory beyond the core credential applications, allowing any existing or new DESFire applications to be encoded alongside LEAF Verified. Because the architecture is open, future community-driven applications and data structures can be seamlessly layered onto the card as the ecosystem evolves.

What you deploy today is the foundation. The LEAF Community's Product Committee defines the direction of standard product releases and updates, ensuring the credential platform evolves through industry collaboration, not just individual customization. What the platform becomes tomorrow is shaped by both the community's governance and your own requirements.

> **Key Distinction:** Buying blank DUOX chips and building your own solution is possible, but it requires custom encoding, a self-built PKI infrastructure, enrollment tooling, API development, and ongoing management, all before a single credential reaches a door. LEAF Verified provides all of this as a turnkey product, backed by a provisioning pipeline that starts at the chip level and extends through a coalition of industry partners.

LEAF Community: The Interoperability Coalition

The LEAF Community is not another name for LEAF Verified. It is a coalition of organizations across the access control value chain (reader manufacturers, physical access control software (PACS) providers, credential manufacturers, chip and module providers, integrators, and end users) who have committed to driving interoperability across the industry.

This is not aspirational. Device manufacturers already support LEAF Verified in production today. Readers capable of verifying LEAF Verified credentials are available now, and open-source integration documentation is available to enable any device manufacturer to add support.

At the center of the LEAF Community is the **Product Committee**, the governance body that defines and evolves the LEAF credential platform over time. While LEAF Verified is the current focus, the Product Committee's scope extends to any specification built on the platform. The committee can introduce new applications, add use cases leveraging the credential's open memory, define new specification layers, and adapt standards as the industry's needs change. This governance structure is what ensures the LEAF platform is not a frozen-in-time product but a living ecosystem that improves through industry collaboration.

What Is Aliro, and What It Isn't

Aliro is an open standard developed by the Connectivity Standards Alliance (CSA), the same organization behind Matter, Zigbee, and Thread. It defines a secure, interoperable communication protocol between access control readers and user devices such as smartphones and smartwatches.

Like LEAF Verified, Aliro is built on public key cryptography, specifically ECC on the P-256 curve. When a user presents their device to a reader, the Aliro protocol enables mutual authentication: the reader proves its identity to the device, and the device proves its identity to the reader. No shared secrets are exchanged.

Aliro supports multiple transport protocols. NFC is mandatory for all conformant readers, with BLE and UWB available as optional transports for hands-free and secure-ranging use cases.

A defining characteristic of Aliro is that it is hardware-agnostic. The protocol can be implemented on secure elements from multiple vendors as well as through Host Card Emulation (HCE) on devices that lack dedicated secure hardware. This cross-platform support is one of Aliro's key strengths for the mobile ecosystem, where device diversity is enormous.

What Aliro Does, and What It Leaves to the Ecosystem

Understanding Aliro's scope is as important as understanding its capabilities. Aliro defines far more than just a communication protocol; it specifies the authentication exchange, the artifacts transmitted between reader and device, and a certificate-based trust model. Together, these elements provide the core infrastructure for secure, interoperable digital credential authentication.

On Aliro's Certificate Model: Aliro's certificate model is lightweight by design. Loading a certificate is a single, standardized operation, the same type of operation that powers every secure browser connection. This is not the complex, heavyweight PKI infrastructure associated with systems like PIV. Aliro's approach is deliberately simple, portable, and well understood.

That said, deploying Aliro-based access in practice does require implementation beyond what the specification defines. The specification does not cover:

- How credentials are provisioned to user devices
- How readers communicate with backend access control systems
- Credential lifecycle management
- Physical credential identity or issuance
- The credential identifier or "card number" presented to the access control system for authorization decisions

> "Aliro defines how to securely deliver a package from device to reader: the transport, the handshake, the trust verification. But what is inside the package, the credential identifier that the access control system ultimately uses to grant or deny access at the door, is outside the specification's scope."

Aliro answers the question "how does a reader authenticate a mobile device?" with a comprehensive, well-architected standard. LEAF Verified answers a different question: "how do I get an authentic physical credential into the field today?"

Both require enrolling the credential into the access control system; that step is universal. Where they differ is in what else is needed. For LEAF Verified, the credential ships ready to use; the remaining requirement is that readers and access devices support the credential format, a one-time device manufacturer integration. For Aliro, deploying the standard also involves setting up certificate infrastructure for readers and building credential provisioning flows. These are lightweight operations individually, but they represent additional implementation work beyond enrollment alone.

They solve different problems. One delivers card authenticity for physical credentials; the other defines how digital devices authenticate to readers. Both are essential.

Why Aliro Excels on Mobile, and Why Physical Is a Different Problem

Aliro was designed around a fundamental assumption: the device on the other side of the reader is smart and connected.

This assumption is what makes Aliro powerful for mobile. Smartphones can remember previous interactions with a reader, making repeat visits fast and seamless without repeating the full authentication process. Phones receive provisioning updates and credential revocations remotely. They manage reader group associations dynamically. They have user interfaces for consent flows and step-up authentication. The Aliro protocol leverages all of these capabilities to deliver a seamless mobile access experience. Even here, however, it is important to remember that Aliro defines the secure transport, not the credential payload itself. What identifier flows through that channel to the access control system remains an implementation decision for the deploying organization.

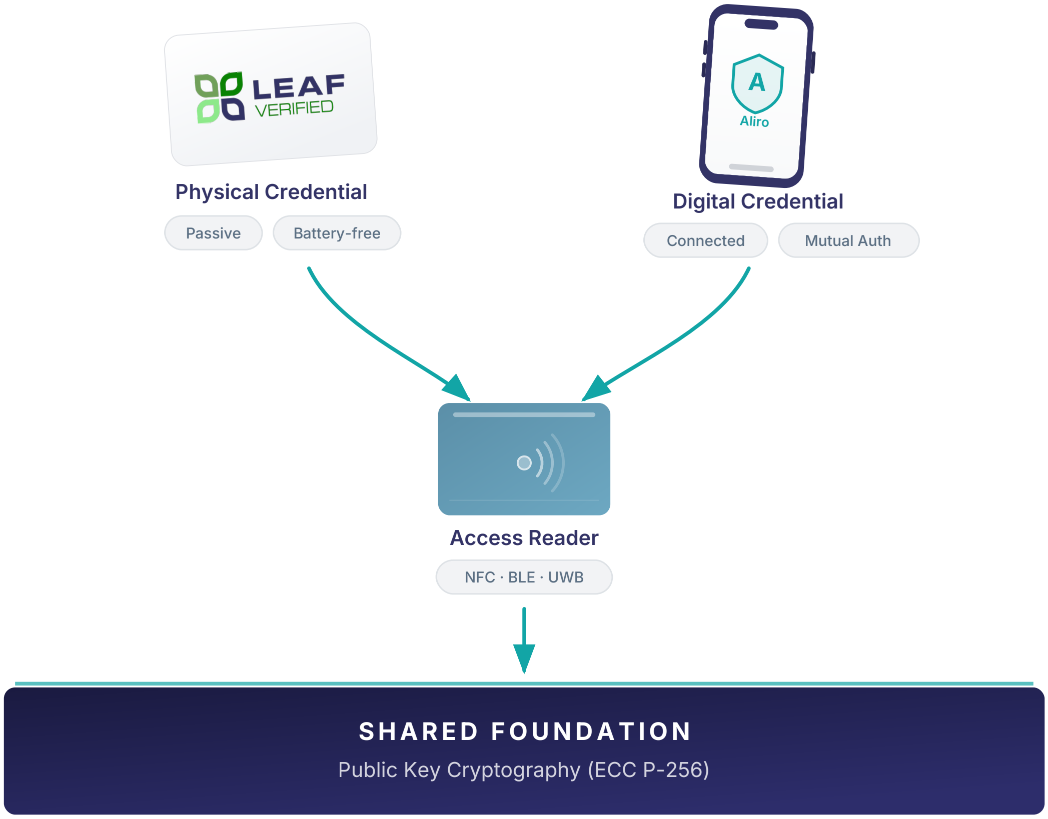
A physical card operates under fundamentally different constraints. It is passive, carries no battery, and has no network connection. It cannot receive over-the-air updates or dynamically manage which reader groups it belongs to the way a connected device can. That said, a card with writable memory is not entirely stateless. Offline locks can write data to the card, and when the card is next presented at a connected controller, that data is relayed back to the system, enabling meaningful offline workflows. This is precisely the kind of capability that the Product Committee can formalize through purpose-built DESFire applications on the card's open memory. But it is a fundamentally different architecture from the always-connected, mutual-authentication model that Aliro is designed around.

> "A card can carry similar data structures, but Aliro's real power comes from what connected devices enable: real-time provisioning, dynamic state, and mutual trust. Physical credential security is a different problem, and it deserves a purpose-built solution."

This is not a limitation of Aliro; it is a reflection of what Aliro was designed to optimize for. Physical credentials operate under different constraints, and LEAF Verified was purpose-built for exactly those constraints: delivering public key cryptographic security on passive physical media, at scale, ready to authenticate from the moment a credential leaves the factory.

Better Together: The Complementary Model

LEAF Verified and Aliro are not competing for the same space. They solve different problems, for different form factors, optimized for different deployment realities, and they share the same cryptographic foundation.



	LEAF Verified	Aliro
What it is	Physical credential product with secure issuance and ecosystem services	Open standard for digital credential authentication
Primary medium	Physical cards, fobs	Smartphones, smartwatches, digital wallets
Optimized for	Turnkey physical credential deployment at scale	Digital credential authentication across diverse device ecosystems
Cryptographic basis	Public Key, ECC P-256	Public Key, ECC P-256

	LEAF Verified	Aliro
Key management	Certificate-based, zero symmetric keys	Certificate-based mutual authentication
Power & connectivity	Passive, battery-less, offline-capable out-of-the-box	Active, connected smart endpoints

The Shared Foundation

Both LEAF Verified and Aliro authenticate using the same elliptic curve cryptography. This is not a coincidence. It reflects broad industry consensus on the right cryptographic foundation for the next generation of access control.

> **For Reader Manufacturers:** The cryptographic algorithms required to support LEAF Verified are the same algorithms required to support Aliro. Supporting both does not mean implementing two different security architectures. It means implementing one.

To support this, LEAF Verified integration documentation for device manufacturers is open-source and publicly available, making it straightforward for any reader manufacturer to add support for LEAF Verified credentials. No LEAF Community membership is required.

Why Organizations Will Deploy Both

The reality of enterprise access control is that no single form factor serves every use case. Physical badges remain essential for everyday reliability: they work without batteries, without network connectivity, and without requiring employees to carry personal devices. Mobile credentials offer flexibility, convenience, and capabilities that physical media cannot match, including dynamic provisioning, remote revocation, and integration with device-native security features.

A modern access control deployment will use both. LEAF Verified addresses the physical credential requirement that Aliro's specification explicitly does not cover. Aliro addresses the mobile and digital credential requirement with a purpose-built protocol. Together, they provide complete coverage across form factors, on the same public key cryptographic foundation, using the same underlying standards (ISO 14443, ISO 7816-4), and supported by the same reader infrastructure.

The real transition happening in access control is not physical versus digital. It is the shift from proprietary symmetric keys to open, public key security, and LEAF Verified and Aliro are the two pillars of that transition. One serves physical. One serves digital. Both are built on public key encryption. And they are stronger together.

> “The real transition happening in access control is not physical versus digital. It is proprietary symmetric keys versus open public key cryptography.”

Common Questions

“LEAF Verified uses only NXP chips. Isn’t that vendor lock-in?”

Every credential product is built on a specific chip, just as every Aliro implementation runs on a specific vendor’s secure element. The relevant measure is system-level interoperability: any reader that supports the open LEAF Verified protocol can verify any LEAF Verified credential, regardless of who manufactured the card. The LEAF Community exists to ensure exactly that.

“Can’t I just buy blank MIFARE DUOX chips and encode them myself?”

You can purchase blank DUOX wafers from NXP’s distribution network, but a blank chip is a component with no identity, no certificate, and no ecosystem. Building a comparable solution from scratch requires custom PKI, encoding pipelines, enrollment tooling, and API development, all before a single credential reaches a door. LEAF Verified delivers all of this as a turnkey product, provisioned at the wafer level and backed by a multi-vendor interoperability coalition.

“Should I wait for Aliro before making credential decisions?”

No. LEAF Verified is available now and addresses the physical credential use case that Aliro’s specification does not cover. Deploying LEAF Verified today means deploying on the same public key foundation Aliro is built on. Your physical credentials are future-aligned from day one.

Looking Ahead

The access control industry’s transition from symmetric to public key cryptography is well underway. LEAF Verified and Aliro represent the leading edge of that transition: one for physical credentials, one for digital, both built on the same open cryptographic foundation.

Reader manufacturers, PACS, and credential manufacturers interested in supporting LEAF Verified can engage with the LEAF Community and access integration documentation today. The ecosystem is live, manufacturers are already in production, and the Product Committee is actively shaping what comes next. The future of physical access is open, interoperable, and built on public key cryptography. LEAF Verified and Aliro are two essential pillars of that future.

LEAF COMMUNITY

Ready to Build on Public Key?

Join the coalition of reader manufacturers, PACS providers, credential manufacturers, integrators, and end users already supporting LEAF Verified.

Access open integration documentation, connect with the Product Committee, and deploy the future of physical access control today.

Visit leaf-community.com →