LEAF Verified: Technical Architecture & Product Specifications

The industry's first turnkey public key credential, fully provisioned at the wafer level, zero downstream encoding, cryptographic trust out of the box.

MARCH 2026 | LEAF COMMUNITY

PRODUCT OVERVIEW

LEAF Verified is a finished physical access credential built entirely on modern public key infrastructure. Every credential ships fully provisioned with cryptographic trust injected at the wafer level through a direct NXP partnership. No downstream encoding. No key ceremonies.

Silicon	NXP MIFARE DUOX
Cryptography	ECC P-256 (same foundation as Aliro)
Certificate	X.509 PKI
Security Certification	Common Criteria EAL 6+
Standards	ISO 14443 Type A, ISO 7816-4 APDU
Key Storage	Hardware-based, private key never leaves the chip

Trust & Cost-Effectiveness Out of the Box

By injecting cryptographic trust into each chip during the secure production and issuance of the wafer, LEAF Verified eliminates the encoding, key management, and proprietary infrastructure that typically drive credential cost and complexity. Every credential ships with:

- **Trusted Silicon:** Secure issuance and authenticity mathematically verified through an open X.509 certificate.
- **Highly Cost-Effective:** No additional downstream encoding, no key ceremonies, and no certificate infrastructure management.
- **Tap-to-Phone (NDEF):** Seamless mobile connectivity with cryptographic validation, bridging physical credentials and smartphone workflows.
- **Unique, Federated Open ID:** Guaranteed globally unique identifiers with a strict “no replication” guarantee. Compatible with any reader.
- **Federated Unique Enterprise ID:** A guaranteed-unique identifier, uncorrelated to the Open ID, included on every credential. Independently federated and accessible only through mutual authentication for high-security zones.
- **Unrestricted Expandability:** Open memory partition ready for additional enterprise applications, with DESFire EV3 and AES256 support native to the MIFARE DUOX platform.
- **Included Cloud Services:** API services for Batch Manifest data, NDEF validation, and dynamic NFC redirects are included with every credential.

What “Open” Actually Means

LEAF Verified defines “Open” with specific, verifiable commitments:

1. **Trusted Silicon:** Secure issuance verified through publicly available X.509 certificates.
2. **Unrestricted Supply:** The LEAF Verified chip is available to all credential manufacturers.
3. **Open Specifications:** APDU commands, certificate verification procedures, and hardware integration specifications are published and freely available.
4. **Zero Complexity:** With a simple reader firmware upgrade, the credential will work natively with most access control systems, including legacy panels.
5. **True Ownership:** The credential works with any compatible reader, and additional applications can be freely added by the end-user without interference.

Feature Summary

Feature	Description
Secure Issuance	Cryptographic trust provisioned at the wafer level by NXP. No field encoding required.
Federated Unique Open ID	Guaranteed-unique 12-digit identifier. Backward-compatible with existing panels via standard reader-to-controller protocols.
Federated Unique Enterprise ID	Guaranteed-unique 12-digit identifier in a protected file, accessible only after mutual authentication. Designed for high-security zones. Included on every credential.
X.509 PKI Certificate	ECC P-256 certificate embedded in each application. Offline verification at the reader.
Wafer Pre-Encoded	Fully encoded at chip manufacture. Order, receive, deploy.
Open Memory	DESFire EV3 native to the MIFARE DUOX platform. Any EV3 application can be written to the open memory partition alongside LEAF Verified.
Tap-to-Phone (NDEF)	Unique NFC-encoded URL per credential with Secure Dynamic Messaging for replay attack prevention. Dynamically configurable via API.
Digital Credential Manifest	Complete digital inventory per order, accessible via QR code or API for bulk enrollment.

Hardware Foundation

LEAF Verified is built on NXP's MIFARE DUOX contactless IC, a Common Criteria EAL 6+ certified secure element with native ECC P-256 support.

Silicon Specifications

Parameter	Value
IC Platform	NXP MIFARE DUOX™ (View Short Datasheet)
Security Certification	Common Criteria EAL 6+
Cryptographic Engine	ECC P-256 (NIST Curve)
Key Storage	Hardware secure element, private key never extractable
Contactless Interface	ISO 14443 Type A
Command Set	ISO 7816-4 APDU
Operating Frequency	13.56 MHz

Hardware Security Guarantees

- **Unclonable by design.** The private key is permanently locked within the chip's EAL 6+ secure element and is never transmitted or remotely extractable. Every authentication requires a live cryptographic challenge, so intercepted data alone cannot produce a clone.
- **EAL 6+ certification** is the same security standard used in banking smartcards, national identity programs, and government PIV credentials.
- **No shared secrets on the reader side.** Readers hold only public keys and certificates. There are no secrets to exploit.

Credential Data Structure

Every LEAF Verified credential contains three distinct applications plus open memory, all provisioned at the wafer level.

Credential Architecture

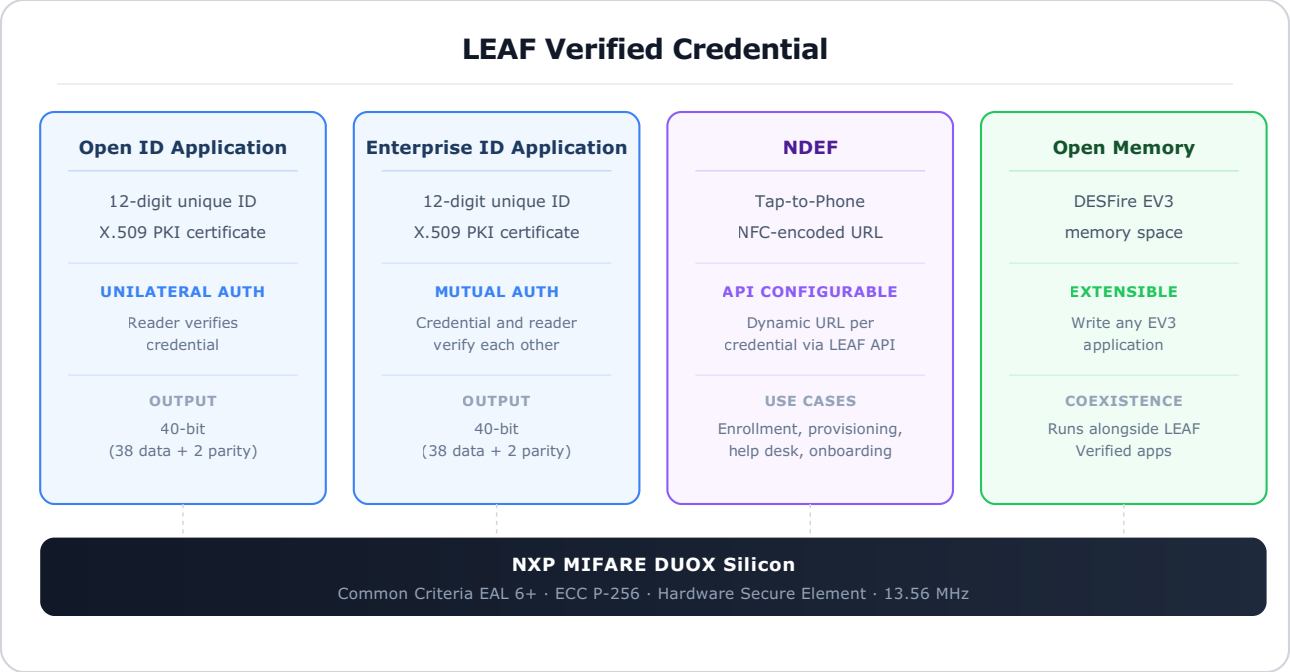

Figure 1: LEAF Verified credential application architecture

Application Details

Open ID Application

The 12-digit Open ID is a guaranteed-unique, federated identifier provisioned during wafer fabrication. It is **cryptographically bound to the credential's X.509 certificate**, not a standalone number that flows independently. The Open ID is extracted from the certificate during the authentication process.

Property	Detail
Format	12-digit numeric identifier
Uniqueness	Globally unique, assigned at wafer level
Certificate Binding	Embedded within the application's X.509 certificate
Reader Output	Standard reader-to-controller protocol (Wiegand, OSDP, MCLP, F2F, etc.)
Panel Compatibility	Works with existing access control panels, no infrastructure changes
Authentication	Reader verifies the credential's certificate using the LEAF root CA public key

The Open ID Reader Transaction

The Open ID is not a standalone number transmitted in the clear. It is structurally bound within the credential's X.509 certificate payload. During authentication, the reader does not simply ask the credential for its ID. Instead, the transaction follows this sequence:

1. **Certificate Transmission:** The reader requests and receives the credential's X.509 certificate.
2. **Trust Validation:** The reader mathematically validates the certificate's signature against the globally trusted LEAF Root CA public key.
3. **Cryptographic Challenge:** The reader issues a challenge, which the credential signs with its hardware-locked private key, proving it is the true owner of the certificate (preventing cloning).
4. **Secure Extraction:** Only upon successful validation does the reader safely parse and extract the 12-digit Open ID from the certificate's internal structure.
5. **Panel Output:** The reader passes the verified ID to the panel via the configured reader-to-controller protocol.

For deployments using ECC-capable readers, the full transaction above is executed. Readers without ECC capability can still read the 12-digit Open ID directly.

Enterprise ID Application

The Enterprise ID brings high-assurance security to restricted zones (server rooms, executive suites, data centers). Designed for zero-trust environments, it provides **mutual authentication**, where both the credential and the reader cryptographically verify each other before any data is exchanged. The Enterprise ID application is included on every credential, with a guaranteed-unique 12-digit identifier provisioned at the wafer level.

- **Mutual Cryptographic Trust:** During authentication, both sides exchange X.509 certificates and derive shared session keys via ECDH.
- **Zero Accessibility Without Auth:** The Enterprise ID is safely locked in a protected file. The reader can only retrieve it by issuing an authenticated, MAC-protected read command through this encrypted session channel. Without completing mutual authentication, the session keys do not exist, and the file cannot be read.

Property	Detail
Format	12-digit numeric identifier
Uniqueness	Globally unique, assigned at wafer level
Storage	Protected file on credential; accessible only through authenticated secure channel
Reader Output	Standard reader-to-controller protocol (Wiegand, OSDP, MCLP, F2F, etc.)
Authentication Model	Mutual (bidirectional): credential verifies reader, reader verifies credential

Property	Detail
ID Accessibility	Requires completed mutual auth; reader must issue MAC'd read command using ECDH-derived session keys
Reader Requirement	Reader must hold a provisioned certificate
Deployment	Ships on every credential, activated per-door based on reader configuration
Use Cases	Server rooms, executive suites, data centers, restricted zones

> **Dual-Application Deployment:** Both applications ship on every credential. The reader at each door determines which application runs. No changes to the credential are needed.

Open Memory (DESFire EV3)

Unrestricted memory space is provided beyond the core LEAF Verified applications. The MIFARE DUOX platform natively supports **DESFire EV3**, allowing any EV3 application to be written to the open memory partition alongside LEAF Verified. The credential is configured to allow new application creation without Km authentication.

NDEF Application (Tap-to-Phone & Replay Prevention)

Every credential contains an NFC-encoded URL. Tapping the credential to an NFC-enabled smartphone triggers a secure LEAF API workflow, bridging physical security with mobile workflows.

Replay Attack Prevention (Secure Dynamic Messaging)

Standard static URLs can be easily copied and shared. To prevent bad actors from copying a credential's URL and reusing it off-site (a replay attack), LEAF Verified utilizes Secure Dynamic Messaging (SDM):

- **Dynamic Generation:** With every physical tap, the credential's silicon generates a unique, one-time URL.
- **Cryptographic Proof:** This URL appends two vital pieces of data: an **incrementing tap counter** and a unique **Cryptographic Message Authentication Code (CMAC)** generated by the chip's internal keys.
- **Cloud Validation:** The smartphone browser routes this dynamic URL to the LEAF Validation API. The API cryptographically verifies the CMAC and checks the tap counter.
- **Active Rejection:** Because the CMAC changes on every tap and the counter must strictly increment, if a malicious actor copies the URL and attempts to open it later, the LEAF API will instantly reject it as a stale replay attack.

Signed Redirect Process:

Once the LEAF API validates the tap as an authentic physical presentation, it issues an HTTP 302 redirect to the credential's configured destination. The redirect URL includes a **signed JWT token** as a query parameter:

```
https://partner-portal.com/enroll?token={ES256_SIGNED_JWT}
```

This token is signed by LEAF Verified using ES256 (ECDSA P-256) and contains the credential's `open_id` and `printed_id`. The receiving server verifies the token's signature against LEAF's public JWKS endpoint, confirming three things:

1. **Authenticity:** The redirect genuinely originated from LEAF Verified, not a phishing or spoofing attempt.
2. **Integrity:** The credential identifiers in the token have not been tampered with in transit.
3. **Freshness:** The token expires in 60 seconds, preventing reuse of intercepted redirects.

This allows partners to securely route authenticated taps to self-service enrollment flows, mobile wallet provisioning, help-desk routing, and custom onboarding workflows.

Certificate Architecture

The X.509 PKI certificate is embedded within the Open Application and the Enterprise Application, serving as the cryptographic trust foundation for each authentication path.

Property	Detail
Standard	X.509
Algorithm	ECC P-256 (NIST Curve)
Verification	Any reader holding the LEAF root CA public key can verify authenticity
Backend Required	No. Verification is offline, at the reader

During authentication, the reader selects the application, reads the certificate, verifies it against the LEAF root CA, and issues a challenge-response to prove the credential possesses the corresponding private key. The certificate guarantees that every identifier on the credential was issued through the trusted LEAF provisioning pipeline and has not been tampered with.

Data Flow Architecture

Upstream: Secure Issuance (Production)

Trust is injected at the earliest possible point in the manufacturing process: the silicon wafer itself.

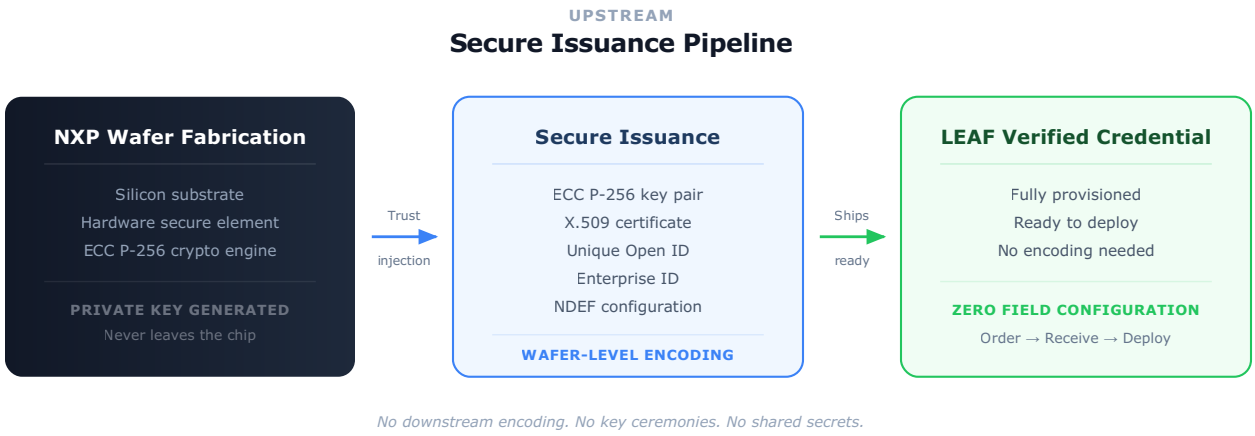

Figure 2: Secure issuance pipeline, trust injected at wafer fabrication

At the point of wafer fabrication, each credential receives:

- A unique ECC P-256 key pair (private key hardware-locked)
- A signed X.509 certificate embedded in each application
- A globally unique 12-digit Open ID
- A globally unique 12-digit Enterprise ID
- A pre-configured NDEF application

> No downstream encoding is required. The credential ships from the manufacturer fully functional.

Downstream: Authentication at the Door

Every LEAF Verified credential supports three distinct paths. For reader-based authentication, the reader at each door determines which path runs. The credential itself does not change. For mobile workflows, the NDEF path provides cryptographically validated tap-to-phone connectivity.

Path 1: Open Application (Unilateral PKI)

For the majority of doors: lobbies, stairwells, parking structures, common areas.

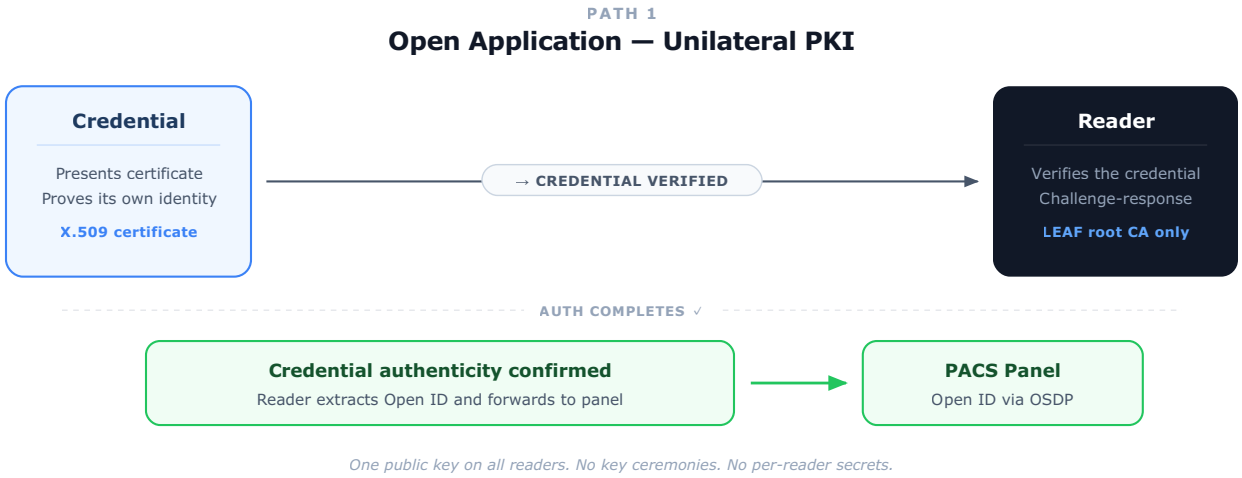

Figure 3: Open Application authentication flow (unilateral PKI)

Path 2: Enterprise Application (Mutual Authentication)

For high-security zones: server rooms, executive suites, data centers, restricted areas.

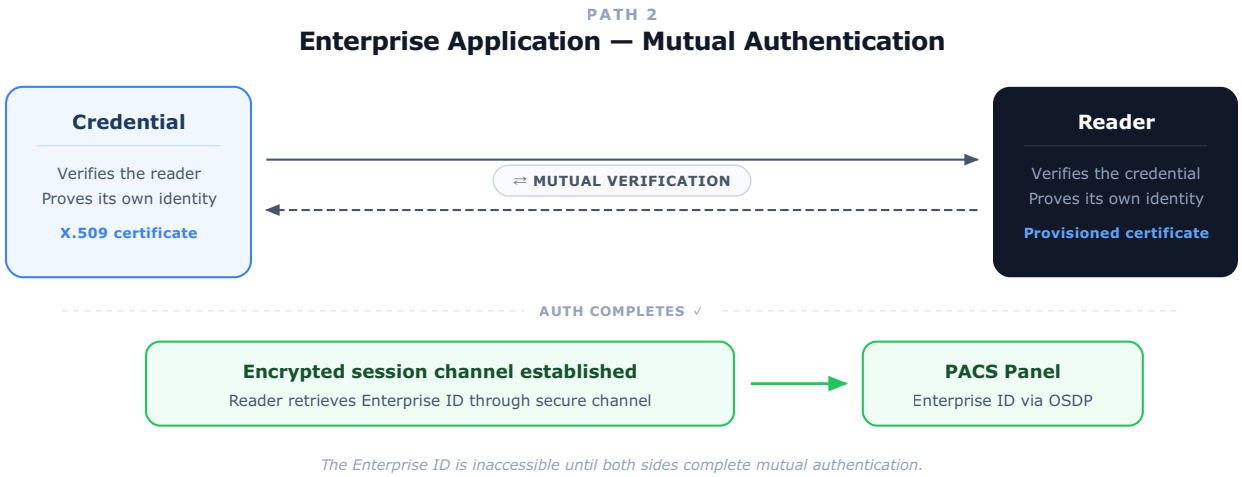

Figure 4: Enterprise Application authentication flow (mutual authentication)

Path 3: NDEF Tap-to-Phone (Dynamic Mobile Validation)

For self-service mobile workflows, external system validation, and secure redirects using standard smartphones.

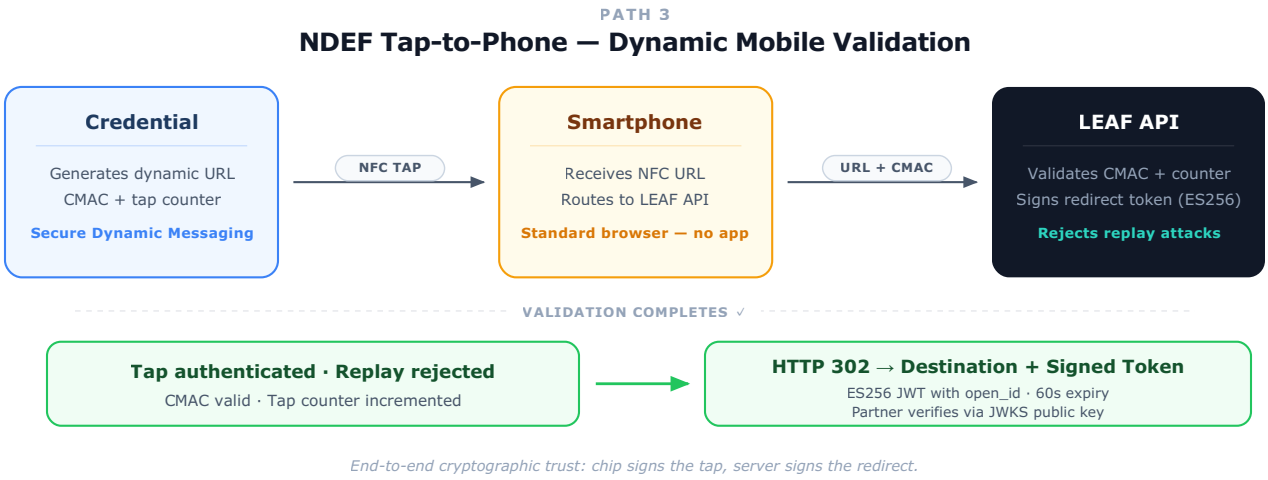

Figure 5: NDEF tap-to-phone data flow with signed redirect

Graduated Security Model

Both applications ship on every credential. The security level is determined by the reader, not the card.

	Open Application	Enterprise Application
Authentication	Unilateral: reader verifies credential	Mutual: credential and reader verify each other
Reader Requirements	LEAF root CA public key only	Provisioned reader certificate
Key Management	Zero	Per-reader certificate provisioning
Reader Output	Standard protocol (Wiegand, OSDP, MCLP, F2F, etc.)	Standard protocol (Wiegand, OSDP, MCLP, F2F, etc.)
Typical Doors	Lobbies, parking, stairwells, common areas	Server rooms, executive suites, restricted zones
Deployment Effort	Mount reader, load one public key, done	Mount reader, provision reader certificate

Digital Credential Manifest

Every LEAF Verified order includes access to a digital credential manifest: a complete inventory of every credential in the order. The manifest can be accessed via a QR code on the pack or directly through the LEAF API.

Capability	Detail
Access	QR code on pack (optional) or LEAF API
Data Per Credential	Printed ID, 12-digit Open ID
Export	CSV download for bulk import
Enrollment Time	Under 60 seconds for an entire pack
API Access	RESTful API with JWT authentication

Reader Output Format

After authentication, the reader outputs the credential's identifier to the access control panel. LEAF recommends the 40-bit reader output (38 data bits + 2 parity bits) for Wiegand and OSDP readers, to ensure functionality on the vast majority of legacy access systems.

Property	Detail
Format	40-bit (38 data bits + 2 parity bits)
Transport	Any standard reader-to-controller protocol (Wiegand, OSDP, MCLP, F2F, etc.)
ID Field	38 bits (supports up to 12-digit identifiers)
Parity	Bit 0: even parity over bits 1–19. Bit 39: odd parity over bits 20–38.
Compatibility	Drop-in replacement for existing deployments

This format is identical for both Open ID and Enterprise ID output. The authentication path differs (depending on the reader configuration); the output format does not.

Integration & Device Support

Integration Surface	Detail
Standards	ISO 14443 Type A, ISO 7816-4 APDU, X.509 PKI

Integration Surface	Detail
Crypto Stack	ECC P-256, shared foundation with Aliro. Implement once, support both.
Reader-Side Requirements	No proprietary secure elements. No licensing fees.
Device Onboarding	Open-source guide
Platform Integration	One integration covers all LEAF Verified credentials regardless of tier or branding
Manifest API	Bulk enrollment via QR code or RESTful API with JWT authentication
Tap-to-Phone Configuration	Per-credential NFC redirect URLs configurable via API

LEAF COMMUNITY

Build on LEAF Verified

Access open integration documentation, connect with the LEAF Community Product Committee, and deploy the industry's first turnkey public key credential today.

Visit leaf-community.com →