indicio

IDEMIA PUBLIC SECURITY

A Decentralized Identity Layer for Financial Services

Interoperable Verifiable Digital Credentials for Secure, Compliant, and AI-Resistant Financial Systems

Strategic White Paper | March 2026

Table of Contents

Executive Summary

Identity fraud has become the defining security challenge for global financial services. Institutions are struggling to answer the most fundamental question in finance—*"Is this person who they claim to be?"*—using systems that were designed for a pre-AI, paper-based world. Centralized identity architectures are increasingly misaligned with modern digital finance, mobile workflows, and emerging regulatory requirements.

At the same time, financial services are undergoing a historic transformation. Stablecoins, real-time payments, and automated, programmable financial services are scaling globally, driven by always-on, web-native infrastructure. New regulatory frameworks—including the U.S. GENIUS Act, Europe's MiCA regulation, and similar regimes worldwide—explicitly require robust Know Your Customer (KYC), Customer Identification Program (CIP), and Anti-Money Laundering (AML) controls that legacy identity systems cannot reliably provide.

> *This paper presents a new identity architecture purpose-built for this environment:* ***decentralized identity using Verifiable Digital Credentials (VDCs)*** *that are cryptographically secure, privacy-preserving, interoperable, and resistant to AI-driven fraud.*

By combining **IDEMIA Public Security's identity proofing and biometric verification** with **Indicio's verifiable credential infrastructure**, financial institutions can replace vulnerable, centralized identity systems with a portable, high-assurance digital trust layer.

The result is faster onboarding, lower fraud exposure, reduced compliance costs, and a fundamentally better customer experience—delivered through a single integration that works across jurisdictions, standards, and financial ecosystems.

The Problem: Identity Infrastructure Is Failing Financial Services

1. The Identity Crisis

Identity fraud is no longer an edge case—it is a systemic risk. Financial institutions face escalating losses driven by synthetic identities, document forgery, social engineering, and AI-powered impersonation attacks. These threats exploit structural weaknesses in centralized identity systems that store sensitive personal and biometric data in large, penetrable repositories.

This crisis is amplified by the rapid adoption of generative AI, which allows attackers to scale fraud cheaply and convincingly. Deepfakes can bypass many liveness checks, forged documents can evade manual KYC reviews, and compromised credentials can be reused across institutions.

The result: higher fraud losses, slower onboarding, growing compliance costs, and declining customer trust.

2. Structural Failures of Legacy Identity Models

2.1 The Honeypot Problem

Centralized identity databases are irresistible targets. Every repository of personal data or biometrics becomes a "honeypot" that, when breached, fuels future fraud at scale. This is not a failure of implementation—it is a failure of architecture. No amount of perimeter security can eliminate the risk inherent in centralized storage.

2.2 The Limits of Multi-Factor Authentication

Multi-factor authentication (MFA) adds friction without fixing the underlying vulnerability. Passwords, SMS codes, and push notifications remain susceptible to phishing, SIM swapping, and social engineering—attacks that AI has made easier and more effective. Layering additional factors onto a centralized model yields diminishing returns.

2.3 KYC as a Paper-Thin Defense

Most KYC processes still rely on manual reviews and document inspection, making them slow, costly, and vulnerable to forged or synthetic identities. Fraud-as-a-Service platforms now offer AI-generated identity documents capable of bypassing legacy checks in minutes.

2.4 The Deepfake Threat

Biometrics were once considered the strongest form of authentication. Today, deepfakes and synthetic media undermine that assumption. Unlike passwords, compromised biometrics cannot be reset. Detecting deepfakes after the fact is an arms race that institutions cannot win.

3. A Financial System at an Inflection Point

Digital finance is scaling faster than identity infrastructure can support it. Stablecoins, real-time payments, decentralized finance, and automated treasury operations require instant, global trust. Regulatory frameworks now demand strong identity verification across these systems, yet legacy approaches cannot deliver high assurance at Internet speed.

> *Without a new identity foundation, digital finance cannot scale safely or compliantly.*

The Solution: Verifiable Digital Credentials with Authenticated Biometrics

4. A New Identity Architecture

Verifiable Digital Credentials (VDCs) represent a fundamentally different approach to identity.

A VDC is a **cryptographically signed, tamper-evident container for identity data** held by the individual in a digital wallet. Credentials are issued by trusted authorities—banks, governments, or regulated institutions—and can be verified instantly, anywhere, without contacting the issuer or a centralized identity provider.

This decentralized model replaces data hoarding with cryptographic trust.

5. How Verifiable Credentials Work

- **User-controlled:** Individuals hold and control their credentials.
- **Cryptographically verifiable:** Authenticity and integrity are proven mathematically.
- **Selective disclosure:** Only the minimum required attributes are shared.
- **Portable and reusable:** Identity proofing performed once can be reused across institutions.
- **Offline-capable:** Credentials can be verified via NFC or BLE without connectivity.

6. Binding Biometrics to Verifiable Credentials

The core innovation of the **IDEMIA Public Security × Indicio** solution is the binding of **authenticated biometrics** to verifiable credentials at issuance.

6.1 Identity Proofing and Credential Issuance

Using IDEMIA Public Security's Identity Proofing Platform, institutions authenticate identity documents (passports, driver's licenses, mobile IDs), verify liveness, and match biometrics at high assurance levels (NIST IAL2/IAL3). Once verified, the individual is issued a VDC containing validated identity data and authenticated biometrics.

6.2 Structural Defense Against Deepfakes

Deepfakes can deceive cameras and humans—but they cannot forge cryptographic signatures. Verification relies on mathematical proof rather than perception. Critically, **relying parties never store biometric data**, eliminating biometric databases entirely.

> *This shifts biometric authentication from a detection problem to a cryptographic certainty.*

7. Privacy by Design and Regulatory Alignment

Verifiable credentials embed privacy as an architectural feature:

- **Data minimization:** Share only what is required.
- **Consent-driven:** Explicit user consent at every interaction.
- **No data hoarding:** No centralized storage of sensitive data.
- **Zero-knowledge proofs:** Verify claims without revealing underlying data.

This model aligns naturally with GDPR and global privacy frameworks while reducing regulatory risk and operational burden.

8. Interoperability at Global Scale

The IPS-Indicio solution supports all major identity standards through a **single integration**, including:

- ISO 18013-5 / 18013-7 (mDLs and mdocs)
- W3C Verifiable Credentials and DIDs
- EU Digital Identity (EUDI)
- ICAO Digital Travel Credentials
- ePassports

A credential issued in one jurisdiction can be verified globally—without custom integrations or API dependencies.

The Benefits: Measurable Impact for Financial Institutions

1. **Reduced Fraud and Liability**
   By eliminating centralized identity vulnerabilities and defeating deepfakes structurally, institutions dramatically reduce fraud exposure and breach risk.

2. **Faster Onboarding and Liquidity**
   KYC onboarding moves from days to minutes, accelerating account activation, capital deployment, and cross-border transactions.

3. **Lower Compliance Costs**
   With minimal data storage, simplified audits, and reduced breach exposure, compliance shifts from a cost center to a built-in capability.

4. **Operational Efficiency**
   Fewer manual reviews, fewer false positives, and identity reuse reduce operational overhead across the organization.

5. **Superior Customer Experience**
   One-time verification, seamless reuse, and user-controlled privacy create a frictionless digital experience that drives conversion and trust.

6. **Competitive Differentiation**
   Early adopters gain a durable advantage—scaling globally with lower costs, stronger security, and regulatory readiness for what comes next.

Conclusion

Legacy identity systems were designed for a paper-based world. Digital finance demands a cryptographic one.

> ***Verifiable credentials with authenticated biometrics provide the identity infrastructure modern financial services have been waiting for.*** *They defeat AI-driven fraud, allow global interoperability, transform compliance, and unlock the speed and scale required for the next generation of financial services.*

The **IDEMIA Public Security × Indicio** partnership delivers this capability today—production-ready, standards-based, and deployable as a foundational digital trust layer for the global financial system.