Post-Quantum Identity and Access for Regulated Institutions: ACM's Multi-Tenant, White-Label IAM with ML-DSA-Signed Federation Tokens

ACM Global Tech

Abstract

ACM Global Tech licenses an end-to-end, post-quantum, regulatory-compliant banking and digital-securities stack. This white paper describes the identity and access management (IAM) layer of that stack: a multi-tenant, white-label identity service in which every institution is an isolated tenant, social and enterprise federation is built in, and the authentication and federation tokens that downstream services trust are signed with NIST-standardized post-quantum signatures. The design derives from the Hanzo multi-tenant IAM platform [1], from the post-quantum migration that replaces classical token and certificate signatures with ML-DSA (FIPS 204) under a hybrid transition strategy [2], and from the investor-onboarding integration that links IAM identities to KYC/AML verification and an on-chain compliance registry [3]. As a member of the Web3 Alliance (W3A, w3a.foundation), ACM licenses this intellectual property and partners to resell and co-build the white-label stack for regulated institutions, built on Lux (blockchain, post-quantum cryptography, and FHE), Hanzo (AI and data), and Zen (LLMs).

1 The Problem: Identity Must Outlive Its Cryptography

For a regulated institution, identity is not a convenience layer; it is the control surface on which every other obligation rests. The same identity system that authenticates a user also encodes which broker-dealer (BD), alternative trading system (ATS), or transfer-agent (TA) role that user holds, and it gates every downstream action a regulator may later audit. A compromised identity system therefore compromises the entire compliance posture, which makes correctness and isolation non-negotiable [1].

Two structural problems compound this. First, multi-tenancy: a white-label platform serves many institutions, and each institution's identities, policies, and federation trust must be isolated so that one tenant can neither see nor affect another. Second, cryptographic longevity. Authentication tokens are short-lived, but the audit records, signed attestations, and certificate chains that anchor a regulated workflow can be retained for years to decades, and the classical signature schemes that secure today's tokens—Ed25519 and ECDSA—are vulnerable to a cryptographically relevant quantum computer (CRQC), whose arrival is conservatively estimated within a horizon shorter than typical financial-data retention requirements [2]. A "harvest now, forge later" adversary can record signed tokens and certificates today and forge against them once such hardware exists. An identity layer for regulated banking must therefore be *tenant-isolated* and *quantum-resistant in its signatures* at the same time.

2 ACM's Approach

ACM packages a licensable, white-label IAM offering that composes a proven multi-tenant identity service with a post-quantum signing path, and links the resulting identities to the regulated-onboarding workflow that BD/ATS/TA operations require.

Multi-tenant, white-label identity.
Each institution is an isolated tenant. Identity is modeled as the triple (user, organization, roles), and the organization identifier travels inside every issued token as an `owner` claim so that downstream services scope all data access to the tenant without re-consulting the identity service [1]. Access control uses a Casbin policy engine with a per-organization policy store, so each tenant's authorization rules—including the role hierarchies needed to model BD, ATS, and TA separations—are evaluated in isolation [1].

Standards-aligned issuance and federation.
The service implements OAuth 2.0, OpenID Connect (OIDC), SAML 2.0, LDAP, and WebAuthn from a single binary, with OIDC discovery served at the standard `/.well-known/openid-configuration` endpoint and a JWKS endpoint that publishes current and previous public keys for zero-downtime key rotation [1]. Federation spans both social identity providers (the source platform ships connectors for more than forty) and enterprise directories via SCIM 2.0 provisioning and SAML SSO, so an institution can onboard users from its existing Okta or Azure AD directory and deprovision them automatically [1].

Post-quantum token and certificate signatures.
The signing algorithm for tokens and certificates migrates from Ed25519 to ML-DSA-65 (FIPS 204, NIST Security Level 3) under a hybrid, dual-signature strategy: during the transition a token carries both signatures and a verifier accepts either, so the scheme stays valid as long as either assumption holds; issuance then moves to ML-DSA only, and classical verification is finally removed [2]. Long-lived root certificates use SLH-DSA (FIPS 205), whose security rests only on hash-function resistance, as a conservative backup at the root of the trust chain [2]. The certificate chain structure—root, organization, leaf—is preserved across the migration; only the signature algorithm changes, with cross-signed certificates bridging old and new roots during the hybrid period [2].

ACM's role is commercial and integrative. As a member of the Web3 Alliance (W3A, w3a.foundation), ACM licenses this intellectual property and partners to resell and co-build the white-label IAM for regulated institutions. The stack is built on Lux (blockchain, post-quantum cryptography, and FHE), Hanzo (AI and data), and Zen (LLMs).

3 Identity for Regulated Roles and Onboarding

The IAM layer is the place where a regulated workflow begins, and where the identity that later authorizes a trade is first bound to a verified person and a compliance status.

- **Role separation for BD/ATS/TA.** Because authorization is expressed as per-organization Casbin policy over hierarchical roles, the distinct duties of a broker-dealer, an alternative trading system operator, and a transfer agent can be encoded as separate roles within a tenant and enforced uniformly at every protected endpoint [1]. The same policy isolation that separates tenants also separates roles within a tenant.

- **Investor onboarding and KYC/AML linkage.** The onboarding flow documented in the source integration creates an IAM identity with an OIDC subject identifier, assigns the investor to the institution's organization with an appropriate role, and carries the organization in the token's `owner` claim; a third-party verification provider then performs identity-document verification, liveness detection, OFAC/sanctions and PEP screening, and accredited-investor checks, returning a signed attestation that updates the investor's IAM profile with KYC status, accreditation status and expiry, and jurisdiction, and that is written to an on-chain compliance registry whitelist [3]. Ongoing monitoring—daily sanctions re-screening, adverse-media monitoring, and accreditation re-verification—keeps that identity-bound compliance status current [3].
- **Durable, standards-aligned credentials.** Because issuance follows OIDC and JWT with a published JWKS, and because the signing algorithm is a NIST post-quantum standard, the credentials an institution relies on are both interoperable with standard tooling and designed to remain non-repudiable as the cryptographic threat landscape evolves [1, 2].

Real-time AI/ML for AML. ACM operates a real-time AI/ML engine for anti-money-laundering and transaction monitoring. It complements the KYC/AML onboarding and continuous sanctions and adverse-media screening documented in the cited integration [3], extending identity-bound compliance from onboarding into live, ongoing transaction surveillance.

4 Cryptographic and Architectural Foundation

The platform's technical guarantees trace directly to research in the Hanzo and Lux ecosystems:

- **Multi-tenant identity service.** *Hanzo IAM: Multi-Tenant Identity and Access Management* [1] specifies the single-binary identity provider supporting OAuth 2.0, OIDC, SAML 2.0, LDAP, and WebAuthn; the (user, organization, roles) identity model with the org-scoping `owner` claim; Casbin RBAC with per-organization policy isolation; SCIM 2.0 provisioning against enterprise directories; and JWKS-based key rotation. It is the basis for the multi-tenant, white-label and federation properties claimed here.
- **Post-quantum signature migration.** *Hanzo Post-Quantum Cryptography: Migration Path for AI Infrastructure* [2] specifies the migration of IAM JWT tokens and service certificates from Ed25519 to ML-DSA-65 (FIPS 204), the hybrid dual-signature transition in which a verifier accepts either signature, the use of SLH-DSA (FIPS 205) for long-lived root certificates, and the threat model that motivates migration ahead of a CRQC. It is the basis for every post-quantum claim in this paper.
- **Onboarding and compliance linkage.** The investor-onboarding section of *Hanzo Platform Integration with Digital Securities* [3] documents how an IAM identity is created, bound to an organization and role, verified through KYC/AML, recorded with accreditation and jurisdiction, written to an on-chain compliance registry, and continuously monitored. It is the basis for the regulated-onboarding and KYC/AML-linkage claims.

5 Outcomes

The intended outcomes of ACM's post-quantum IAM offering, as supported by the cited research, are:

1. **Tenant isolation by construction.** Per-organization policy stores and an org-scoped token claim mean one institution's identities and authorization rules are evaluated in isolation from every other tenant's [1].

2. **Quantum-resistant authentication.** Federation and authentication tokens, and the certificate chains beneath them, are signed under NIST post-quantum algorithms (ML-DSA, with SLH-DSA at the root), so their validity is designed to survive the arrival of a quantum adversary [2].

3. **Non-disruptive migration.** The hybrid dual-signature path lets classical and post-quantum verification coexist during transition—a token is accepted if either signature verifies—so institutions migrate without a flag-day cutover [2].

4. **Standards-aligned, role-aware identity for regulated workflows.** OIDC/JWT issuance, SCIM and SAML federation, and per-tenant role hierarchies give regulated institutions interoperable credentials and the BD/ATS/TA role separation their obligations require, with identities bound to KYC/AML status at onboarding [1, 3].

References

[1] Z. Kelling. *Hanzo IAM: Multi-Tenant Identity and Access Management with 40+ Social Providers*. Hanzo Industries. Source: `hanzo:hanzo-iam-platform.tex`.

[2] Z. Kelling. *Hanzo Post-Quantum Cryptography: Migration Path for AI Infrastructure*. Hanzo Industries Inc. Source: `hanzo:hanzo-pq-crypto/hanzo-pq-crypto.tex`.

[3] Z. Kelling. *Hanzo Platform Integration with Digital Securities*. Hanzo Industries Inc. Source: `hanzo:hanzo-digital-securities-integration/hanzo-digital-securities-integration.tex`.