OmniTrust

DATA SHEET

ILM

Identity Lifecycle Management (ILM): The Control Plane for Cryptographic Trust

CHALLENGES ILM ADDRESSES:

Modern enterprises rely on cryptographic identities everywhere:

- Certificates securing networks and applications
- Keys protecting data and workloads
- Secrets enabling systems and APIs
- Signatures ensuring software and document integrity

But these identities are typically:

- Spread across PKIs, clouds, vaults, code, and devices
- Owned by different teams
- Governed inconsistently
- Invisible until something breaks

Traditional tools manage pieces of the problem. ILM governs the lifecycle of trust itself.

CONTINUOUS COMPLIANCE ENGINEERED IN:

Identity Lifecycle Management (ILM) is how organizations discover, govern, and manage cryptographic trust across certificates, keys, signatures, and secrets as a single lifecycle, rather than with disconnected tools. ILM turns cryptography from a collection of point solutions into governed infrastructure, providing a lifecycle control plane that works across existing environments to provide: visibility before outages, governance before audits, and control without lock-in.

DISCOVERY & VISIBILITY

ILM discovers cryptographic identities across the environment and makes them visible to the right stewards.

Discovery spans:

- **Network endpoints**
- **Cloud platforms**
- **Vaults and KMS**
- **Repositories and CI/CD**
- **File systems and containers**
- **Certificate Transparency logs**
- **IoT and connected systems**

CBOM Lens enhances discovery by revealing cryptography embedded in software through Cryptography Bills of Materials (CBOMs).

MANAGEMENT

Turn visibility into control as ILM manages the full lifecycle of cryptographic identities through policy-driven control. Lifecycle actions include issuance, renewal & rotation, revocation, synchronization, and migration.

Governance controls include policy & scheduling, rules & workflows, continuous monitoring, escalation & notifications, risk analysis and compliance & audit evidence.

INVENTORY

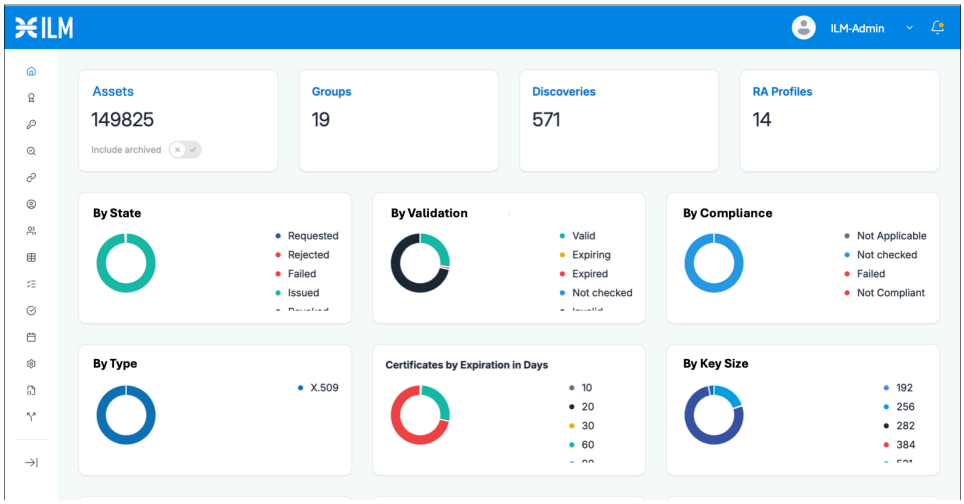
Create a system of record for trust – ILM normalizes discovered assets into a governed inventory of:

- **Certificates**
- **Cryptographic keys**
- **Secrets**
- **Digital signatures**

Each asset is enriched with: ownership, algorithms and protocols, usage context, metadata and criticality & CBOM intelligence.

AUTOMATION & ORCHESTRATION

Automation spans Discovery, Inventory, and Management. – Through automation, ILM enables organizations to automate what matters most, keep humans where oversight is required and allow security leaders to increase maturity over time. All facilitated through standards-based protocols, APIs and pre-built or custom connectors.



CLM & PKI WITHOUT LOCK-IN

PKI Consortium

ILM separates governance from implementation. Organizations can:

- **Use OmniTrust Unified PKI**
- **Bring existing PKIs, CAs, HSMs, KMS, and tools**
- **ILM provides the same lifecycle control layer either way.**

Our PKI Maturity Model helps organizations:

- **Assess where they are today**
- **Identify priority gaps**
- **Define a realistic path forward**

DEPLOYMENT OPTIONS

ILM supports cloud, hybrid, and on-premises deployments and integrates with:

- **Existing PKIs**
- **HSMs**
- **Cloud KMS**
- **Signing systems**

Organizations can deploy ILM in the way that best fits their security, regulatory, and operational requirements - without forcing architectural change.

DIGITAL CERTIFICATES

- Internal, external, cloud, and managed PKI
- Protocol-driven automation
- Multi-CA under one control plane
- Policy changes without app disruption

CRYPTOGRAPHIC KEYS

- Govern keys across HSMs, cloud KMS, software
- Inventory and usage control
- Crypto agility and algorithm migration
- Audit and PQ readiness

DIGITAL SIGNATURES & SIGNING

- Centralized signing keys
- Server-side and automated signing
- Strong authentication and control
- Standards-based validation

SECRETS

- Discover and inventory secrets
- Assign ownership and policy
- Rotate and revoke where integrated
- Monitor and audit centrally

ILM delivers the enterprise control plane for cryptographic assets - governing certificates, keys, secrets, and signing beyond CLM. Bring your own PKI or use ours while unifying trust through open connectors.

PQC READY

ABOUT OMNITRUST

OmniTrust (formerly INTEGRITY Security Services) secures the connected world — from silicon to cloud systems and AI — by delivering verifiable, enforceable trust across the entire device and software lifecycle. As the leader in Trust Lifecycle Management, OmniTrust ensures security from design and provisioning through operation, update and retirement, protecting more than 2 billion devices and 3 billion software updates per year. OmniTrust enables full-lifecycle security across the chain of trust for companies in the automotive, aerospace and defense, finance, healthcare and other safety-critical, regulated sectors.

omnitrust.com

OmniTrust