OmniTrust

DATA SHEET

TLM

Trust Lifecycle Management – A Unified Approach to Connected Trust

TRUST IS A CONTINUUM

Every connected system must be born trusted, operate trusted, and retire trusted. From silicon and embedded controllers to cloud services, users, applications, and autonomous AI agents, trust cannot rely on isolated tools. It must be enforced continuously across identities, cryptography, software, devices, and data. OmniTrust enables organizations to establish, govern, and maintain trust across the entire lifecycle – from manufacturing and deployment to operation, update, and retirement.

THE CHALLENGE: FRAGMENTED TRUST

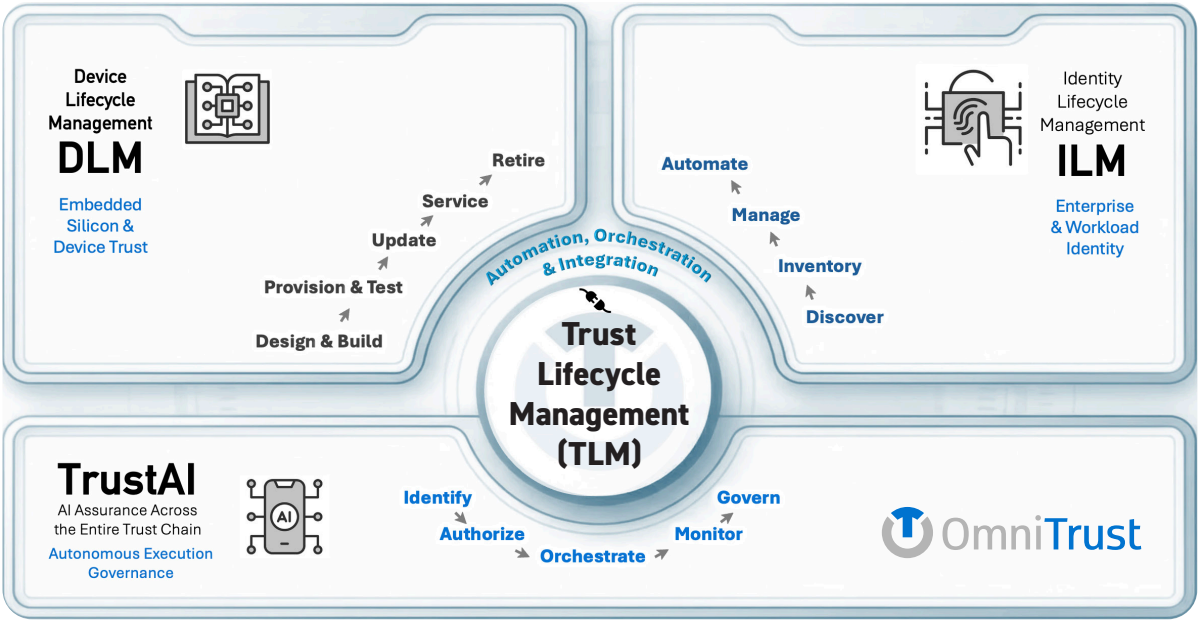
Organizations rely on multiple disconnected tools for PKI, secrets, signing, provisioning, and identity. Each solves part of the problem, but none govern trust across the full lifecycle.

- **A signed image is meaningless if the signer, device, or provenance cannot be verified.**
- **A device cannot be trusted if its firmware, identity, or keys are unknown or unmanaged.**
- **AI agents cannot be trusted without identity, signing authority, and data lineage control.**

Trust must be continuous, enforceable, and governed across devices, enterprise systems, and autonomous environments.

A UNIFIED PLATFORM

The OmniTrust Trust Lifecycle Management (TLM) platform unifies device trust, enterprise cryptographic governance, and AI system trust into one lifecycle framework. Organizations can establish and enforce trust across embedded systems, cloud infrastructure, enterprise applications, and autonomous agents. By governing identities, cryptography, signing, and device integrity across the lifecycle, OmniTrust delivers continuous security, compliance readiness, and operational resilience.



PQC | EU CRA | DORA | NIS2 | NIST CSF 2.0 | NIST SP 800-53 | NIST SP 800-57 | NIST SP 800-218 (SSDF) | Executive Order 14028 | CISA | PCI DSS 4.0
SOC 2 | ISO 27001:2022 | ISO 27400 (IoT Security) | GDPR | eIDAS 2.0 | NYDFS 23 NYCRR 500 | UK PSTI Act | SEC Cyber | SBOM / NTIA

Key Features of the OmniTrust TLM Platform

TRUST AI

TrustAI extends lifecycle trust governance to autonomous systems and AI agents operating across APIs, cloud platforms, and connected systems. It establishes identity, authority, and policy enforcement for models, agents, and automated services. Discovery capabilities including Seek and CBOM Lens provide visibility into certificates, keys, secrets, algorithms, and component provenance, helping organizations understand and govern cryptographic risk across their environments.

SIGNING SERVICES

OmniTrust provides cryptographically enforced signing services for firmware, software, and enterprise workflows. Centralized signing authorities, HSM-protected key custody, and policy-driven workflows ensure code and artifacts can only execute when verified. Signing services integrate with OT PKI or existing enterprise CAs, enabling secure software pipelines, OTA updates, and verifiable software provenance across development and production environments.

IDENTITY, PKI & CRYPTOGRAPHIC GOVERNANCE

Identity Lifecycle Management (ILM) extends beyond traditional Certificate Lifecycle Management (CLM). While CLM focuses on certificates, ILM governs the lifecycle of certificates, keys, secrets, tokens, and digital signatures across hybrid environments. Organizations can deploy OmniTrust PKI (OT PKI) for integrated issuance, automation, and governance — or connect existing certificate authorities through open connectors. This flexible model eliminates vendor lock-in, allowing organizations to operate existing PKI environments or migrate to OT PKI over time.

SECRETS & KEY GOVERNANCE

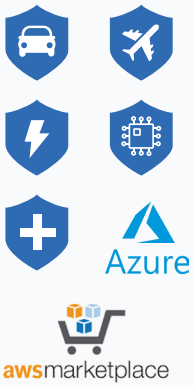
OmniTrust secures and governs secrets, keys, and tokens across enterprise, cloud, and DevOps environments. Keep provides centralized protection and lifecycle management for sensitive credentials with policy-driven access control. Automated rotation, issuance, and revocation enforce strong cryptographic hygiene while integrating with existing vaults and infrastructure services across hybrid environments.

START ANYWHERE, BUILD CONTINUITY EVERYWHERE

The TLM platform allows organizations to begin wherever trust is most critical and expand as requirements evolve.

- **Start with certificate lifecycle management (CLM) use cases**
- **Extend to ILM governance for certificates, keys, secrets, signatures, and tokens**
- **Deploy secure firmware signing and device lifecycle management for connected systems**
- **Add discovery with Seek and CBOM Lens and governance for AI and autonomous systems**

With open connectors and flexible deployment (SaaS, on-prem, or hybrid), OmniTrust integrates with existing PKI or OT PKI while unifying fragmented trust operations into a single lifecycle platform.



Consulting: Expert engineering and advisory services to design, deploy, and optimize trust architectures across embedded, enterprise, and cloud ecosystems. Accelerates adoption and compliance

API Integration: Standards-based APIs for orchestrating trust workflows across enterprise systems, pipelines, and manufacturing environments. Enables automation without re-architecting infrastructure

BYOT (Bring Your Own Tools): Integrate your existing PKI, vault, discovery, analytics, or DevOps tools directly into the TLM framework through open connectors and APIs. Zero-lock-in flexibility

Deployment Options: Flexible delivery models including on-prem, managed service, SaaS, or hybrid. Available via AWS and Azure Marketplace for global scalability and cloud agility

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