ISS INTEGRITY® SECURITY SERVICES

DATA SHEET

TLM

Trust Lifecycle Management – A Unified Approach to Connected Trust

TRUST IS A CONTINUUM

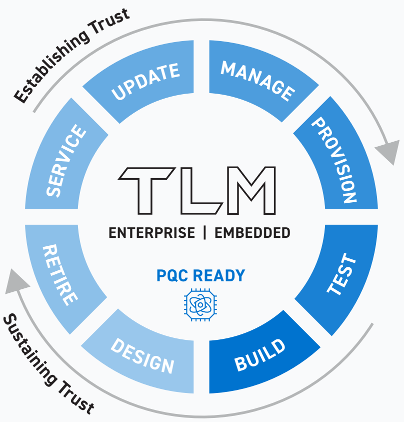
Every connected asset must be born trusted, live trusted, and retire trusted. From devices and embedded controllers to cloud workloads, users, applications, and AI agents, trust cannot be stitched together from disconnected tools. It must be orchestrated holistically.

THE CHALLENGE: FRAGMENTED TRUST

Organizations use multiple isolated tools for PKI, signing, provisioning, cloud identity, secrets, and device management - each solving part of the problem but none enforcing trust across the 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 ungoverned**
- **An AI agent's output cannot be relied upon without continuous identity, signature, and data lineage assurance**

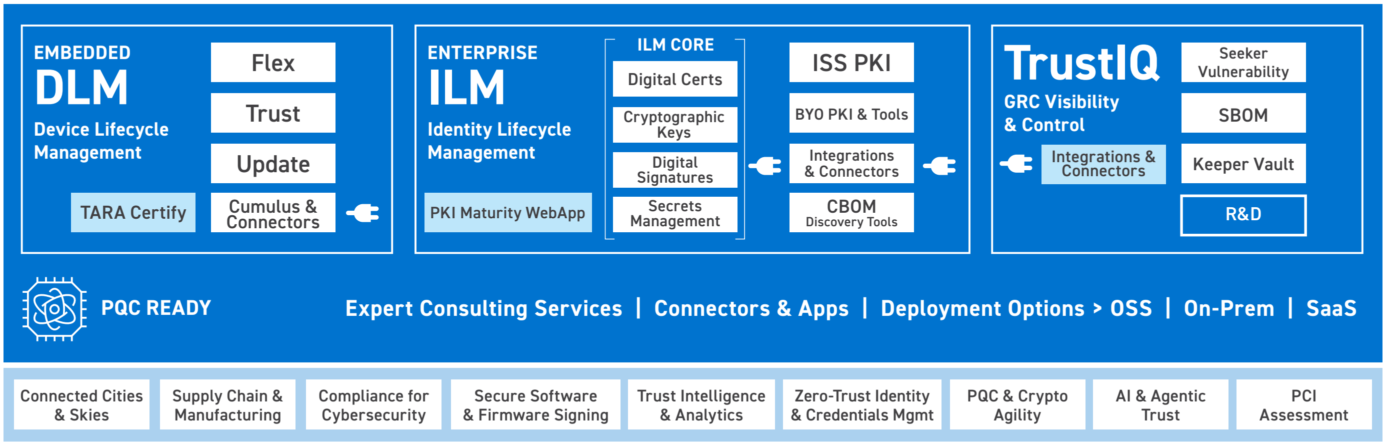
Trust must be continuous, contextual, and connected - regardless of tools or vendors.



The ISS TLM platform provides the unified foundation to establish, govern, update, and retire trust across physical and digital domains

A UNIFIED PLATFORM

The ISS Trust Lifecycle Management (TLM) unified platform merges device trust, identity and cryptographic lifecycle management, with trust intelligence as one continuous framework. Our clients establish and maintain trust across embedded systems, cloud applications, enterprise infrastructure, and AI-powered services – enabling consistent security, compliance, and lifecycle governance.



CONTINUOUS COMPLIANCE ENGINEERED IN:

FDA APPROVED · Webtrust · PCI · CISA · NIST CSF · ISO 27001 · U.S. CYBER TRUST MARK

Key Features of the ISS TLM Platform

TRUST IQ

Visibility and control over the trust map of your cryptographic assets across devices, systems, and workloads. **Seeker** discovers certificates, keys, secrets, and algorithms, while **CBOM** maps provenance and relationships. **DLM Cumulus** aggregates telemetry into posture dashboards, enabling crypto risk management, compliance validation, and lifecycle governance.

PKI, IDENTITY & SECRETS

ISS Identity Lifecycle Management (ILM) extends traditional certificate lifecycle management (CLM) into full lifecycle management for certificates, keys, signatures, and secrets. **PKI** and **certificates** support issuance and renewal across hybrid environments, while **keys**, **signatures**, and **IDs** unify identity control for users, devices, and agents. Secrets integrates password, token, and API credential handling for secure, policy-driven authentication everywhere.

SIGNING SERVICES

Ensures integrity, authenticity, and compliance for firmware, software, and enterprise code. **Software signing** and **firmware signing** deliver cryptographic assurance for binaries and images, while **OTA** updates enforce verified code execution in production and fielded devices. Hardware security module (**HSM**) and Cloud key management system (**KMS**) integrations anchor key custody across hybrid deployments.

VAULT SERVICES

Provides resilient protection and lifecycle governance for cryptographic material. **Keeper Vault** secures secrets and keys in an open, standards-based vault architecture. **Key Rotation and Renewal** enforce hygiene policies, while **Secret Federation** connects multi-cloud and DevOps environments. **Lifecycle Hooks** automate provisioning, archival, and revocation to maintain security from creation through decommissioning.

START ANYWHERE, BUILD CONTINUITY EVERYWHERE

The TLM platform lets organizations begin wherever trust is most critical and expand as their needs grow:

- **Simple certificate management use cases**
- **Deployment of secure firmware signing and device lifecycle management (DLM) for connected fleets**
- **Extend into enterprise PKI orchestration and credential lifecycle management — certs, keys, signatures, secrets**
- **Add crypto discovery, posture management, and continuous monitoring**

With open connectors and flexible deployment (cloud/SaaS, on-prem, or hybrid), TLM adapts to your environment, unifying fragmented trust operations into a single, resilient continuum.

Azure

awsmarketplace

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

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

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

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

THE MOST EXPERIENCED PROVIDER OF EMBEDDED SECURITY PLATFORMS

INTEGRITY Security Services LLC (ISS) provides best-in-class embedded security products and infrastructure solutions for protecting smart connected devices from cyberattacks. With end-to-end solutions ranging from software toolkits to large-scale public key infrastructure and device lifecycle management, ISS secures over 2 billion devices across automotive, aerospace and defense, financial, medical and other industries. Trusted by some of the largest Fortune 100 companies, ISS signs and manages more than 3 billion software images per year and continues to lead the industry in security innovations.

www.securedbyintegrity.com

ISS INTEGRITY® SECURITY SERVICES