ISS Trust Lifecycle Management (TLM) for Aerospace & Defense

ISS Trust Lifecycle Management (TLM) for Aerospace & Defense (A&D) is a comprehensive management platform to secure and monitor aerospace & defense systems. Designed to help meet the most stringent standards and provide end-to-end cybersecurity for mission-critical applications.

In today's connected battlefield, weapons systems and aerospace platforms face a range of previously unimagined cybersecurity threats. Well-financed and resourceful nation-state adversaries are mounting attacks — even in peacetime — to undermine the reliability and effectiveness of these systems.

Developers must now think beyond attacks on deployed systems and address vulnerabilities at the design and manufacturing supply chain level. The multi-tiered, multinational supply chains that deliver these complex platforms represent a soft underbelly, exposing opportunities for malware injection and the exfiltration of critical assets.

Against such skillful and determined adversaries, the Aerospace & Defense industry requires an uncompromising, end-to-end management platform capable of securing all elements of a system — across every stage of the product lifecycle.

The U.S. Department of Defense, in cooperation with the **NIST Computer Security Resource Center**, recognizes the magnitude of this risk and has instituted the Cybersecurity Maturity Model Certification (CMMC) program to raise the level of security awareness across the industry. The DoD has made clear that **future procurement decisions will depend heavily on the cybersecurity maturity** of not only prime contractors, but also every sub-contractor in the supply chain.

The ISS TLM Platform for Aerospace & Defense provides the technology foundation necessary to achieve a high level of CMMC certification, ensuring compliance while safeguarding mission-critical systems.

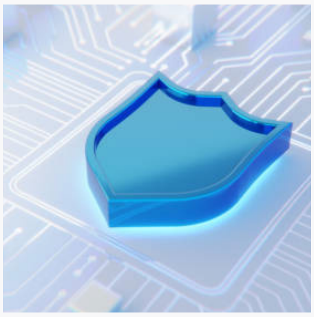
REQUIREMENTS SUPPORTED

ARINC 835, 667-1, FIPS-140, ISO 27000, CMMC, RTCA DO-326A, DO-355, DO-356, NIST SP 800-53, -171, -161, -57, -111 + More.

ISS TRUST LIFECYCLE MANAGEMENT (ISS TLM) PLATFORM FOR AEROSPACE & DEFENSE

ISS TLM for Aerospace & Defense is a comprehensive security management platform that protects and manages all elements of the system from design and development through manufacturing and deployment of operational infrastructure and the device itself.

In service ISS TLM provides secure diagnostic access and Secure Over the Air (SOTA) software updates.



Manage Your Devices from Birth to Decommissioning with the ISS DLM System

The best security teams understand that all devices are vulnerable if critical root keys are compromised due to network breach, internal attack, or error. At the same time, connected devices increasingly need to receive Over-The-Air (OTA) updates to fix vulnerabilities, improve functionality and offer new features. To address these challenges, manufacturers need to manage users, digital assets and cryptographic operations across global manufacturing supply chains.

INTEGRITY Security Services' (ISS) Device Lifecycle Management (DLM) system provides a zero-exposure, military-grade security infrastructure for locking down your entire supply chain. Built on our intuitive management portal and backed by FIPS 140-2 Level 3 assurance, DLM generates keys, certificates, and digital signatures, anywhere in your supply chain, to securely track all your users while also being able to provision, manage, and update all your critical devices.

PROVEN END-TO-END SECURITY

Most silicon manufacturers offer keys and tools to digitally sign their components but it can be insecure or create a key management problem. DLM abstracts the chip layer and provides organizations a common way to secure the devices by authenticating all chips, devices, users, and digital assets. The ISS DLM system covers the entire lifecycle and leverages a point-to-point encrypted network for true end-to-end security.

MINIMIZE RISK THROUGH THE GLOBAL SUPPLY CHAIN

In the end, security comes down to trust. It's only as strong as the weakest link and with global supply chains, it's imperative to ensure this trust covers everyone that touches your product. That's where the ISS DLM role-based access is critical to minimize risks. It assigns privileges based on roles while tracking all provisioned products so you have visibility into your entire supply chain.

DLM
DEVICE
LIFECYCLE
MANAGEMENT

HIGHLIGHTS

- → Protect users and digital assets throughout the supply chain
- → Offers hosted and on-premise options
- → High availability for uninterrupted production across remote sites
- → FIPS 140-2 Level 3 tamper resistant appliances for untrusted sites
- → DLM securely provisions over 2 billion devices worldwide in over 500 remote sites
- → DLM secures all safety critical IOT supply chains

APPLICATIONS

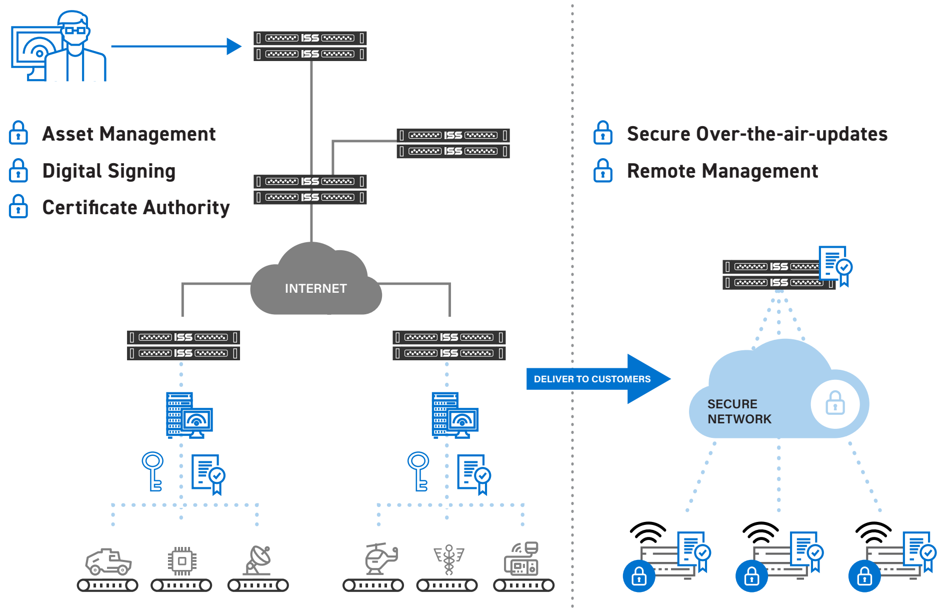
- → Secure injection of keys for parts identity
- → Authenticate and track user actions across supply chain
- → Develop and test secure devices with certificates and digital signing services
- → Protect historically unsecure manufacturing sites with FIPS-Certified appliances
- → Over-the-air updates and remote management across the full lifecycle
- → Defend against unauthorized use and counterfeiting
- → Manage all digital assets across unsecure supply chains

LOWER TOTAL COST OF OWNERSHIP

Every manufacturer uses different chips and has multiple, even hundreds of SKUs making product inventory and bill of materials management a costly nightmare. The ISS DLM abstracts the certificates and keys for signing different code into a common interface, which saves developers a lot of time. You can even personalize each SKU at the final DLM step and make them software-defined parts which results in even lower TCO.

ISS INTEGRITY® SECURITY SERVICES

Key Components of the ISS DLM System



The ISS DLM System includes all hardware, software, and services to securely share trusted digital assets across global supply chains.

It is built on an encrypted network for controlled end-point access to assets and cryptographic operations.

Our DLM system is a complete end-to-end security solution to protect devices and their critical assets across all lifecycle phases and includes three key components:

DLM TRUST

Certificates, issued by a trusted PKI that can digitally sign software and data is the core mechanism to detect tampered software, spoofing attacks and other risks. It can also generate x.509v3 and custom certificates to identify manufacturers, integrators, and end users while supporting several signing algorithms and hardware profiles.

DLM UPDATE

When delivering OTA updates, a defense-in-depth approach for the distribution of software upgrades and digital assets in the field is critical. DLM Update is standards-based Open Mobile Alliance Device Management (OMA-DM) software that is integrated with your enterprise IT system. This allows developers to securely send software updates that fix vulnerabilities, when discovered, while continuously improving product features.

DLM SCM

You need to securely inject unique keys, certificates, and data into devices during manufacturing. DLM SCM enables the distribution of keys and collects device information across distributed environments and suppliers. Critical assets are protected within our encrypted network until individually metered into each device. Once a device goes into use, DLM can update, authenticate, manage, and decommission devices and users at any point in time.

TECHNICAL SPECIFICATIONS

Network Interfaces
3×1Gbps Inter-Appliance, Application, Admin

Enclosure
1U rack mount (17.2"W × 19.85"D × 1.7"H)
Power: 100–240V, 50–60Hz autosensing
Current: 6.0A @100V, 3.0A @240V
Connector: C-14

Regulatory Compliance
Emissions: FCC Part 15B Class A, EN 55022, EN 61000-3-2/-3-3, CISPR 22
Immunity: EN 55024/CISPR 24 (EN 61000-4-2/-3/-4/-5/-6/-8/-11)
Safety: CSA/EN/IEC/UL 60950-1, UL/CSA Listed (USA/Canada), CE (Europe)

Operating Environment
Temp: 10–35°C (op), -40–70°C (non-op)
Humidity: 20–90% (op), 50–90% (non-op), non-condensing

High Availability
Shipped HA; redundant pairs for DR
Offline CA appliance for secure key storage
Corporate NAS backup integration
Smart Card key-splitting for recovery

Key Management
FIPS 186-3; RSA 1024–3072, ECDSA 256–512, SHA-1/256/384/512
Keys importable/generated; X.509v3 + proprietary formats
Revocation via CRL & OCSP
Keys metered by type/location; limited remote storage

DLM Controller (DC)
Hosted/on-premise options
Manages appliances, key generation, services
Web UI; Postgres DB integrates with Oracle
Aggregates backups/archives

User Access Control
Roles: Admin, Security Officer, Developer
Password or 2FA login; federated access

24×7 Support & Maintenance
Global SLAs for high-volume production
In-house expert response team; escalation support in NA, EU, Asia-Pacific

FLEXHSM and FLEXARMOR

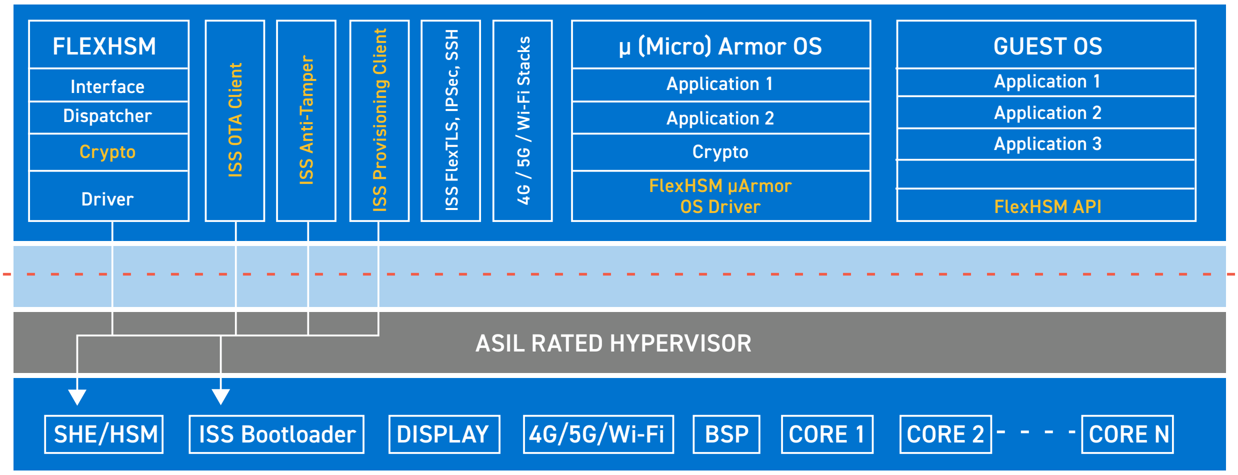
FlexHSM or FlexArmor have a war chest of embedded software and IP Blocks to lock down any embedded device. The Flex Products have been deployed to the most popular embedded CPUs or FPGAs in use today. The Flex products have been seamlessly integrated with DLM infrastructure. Flex products anchor the embedded end of ISS's end-to-end security.

FLEXHSM

FLEXARMOR

FLEXHSM & FLEXARMOR ON ANY DEVICE AND ANY OS

- Device independent API
- Reduce development and training cost
- Transparent use of hardware security features
- Complete suite of crypto algorithms
- Complete suite of security protocols
- FIPS 140-2 certified
- Security separation
- Secure memory controller
- True random number generator
- Post Quantum Crypto algorithm IP
- Secure boot for FPGAs
- Tamper detection
- Side channel prevention



ISS CONSULTING & PROFESSIONAL SERVICES

INTEGRITY Security Services is your partner for embedded security development. Committed to best practice security design, ISS collaborates with your teams to provide the best solutions for your product and business goals. Our consulting services include;

- **Security assessments**
- **End-to-end security architecture design addressing device and infrastructure security across all lifecycle phases**
- **White/Black box testing and reverse engineering**
- **Support for security certification including FIPS-140, ISO 27000, CMMC, RTCA DO-326A, DO-355, DO-356, SP 800-xx and others.**