ISS INTEGRITY® SECURITY SERVICES

DATA SHEET

DLM

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

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
- Supports post-quantum cryptographic algorithms

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

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.

The ISS Device Lifecyle Management (DLM) system provides a zero-exposure, enterprise 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 IoT devices.

PROVEN END-TO-END SECURITY

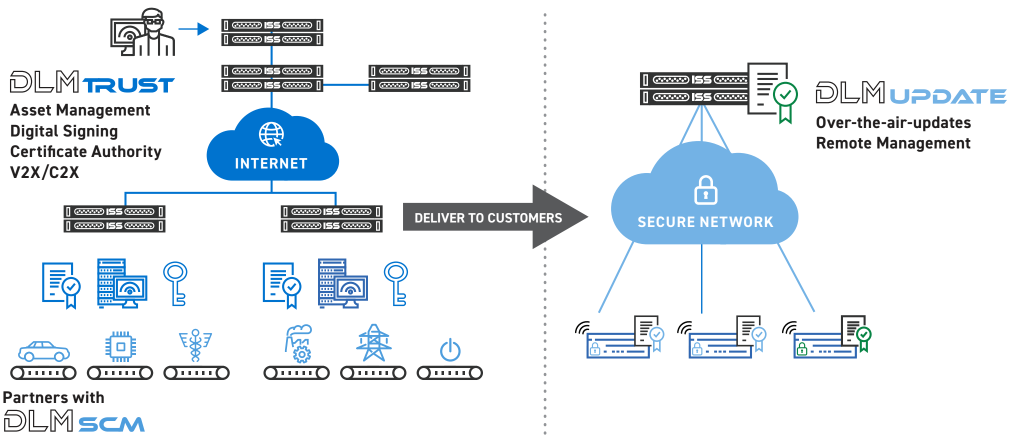
Most chip companies offer keys and tools to digitally sign their components but it can be insecure or create a key management problem. DLM abstracts the chip layer and provides OEMs a common way to secure the IoT devices by authenticating all chips, devices, users, and digital assets. The ISS DLM system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

MINIMIZE RISK THROUGH 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.

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.



The components of the ISS DLM system work to protect digital assets across all lifecycle phases.

Key Features 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. DLM Trust is the first and only root certificate authority and provider of production V2X and C2X digital certificates. 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, and Admin Interfaces

ENCLOSURE

- Form Factor: 1U rack mountable
- 1U Dimensions: 17.2"W × 19.85"D × 1.7"H
- Power Supplies: AC Input: 100–240V, 50–60 Hz, autosensing
- Rated Input Current: 6.0A @100, 3.0A 240Vac, 50-60Hz
- Power Supply Connector Style: C-14

REGULATORY COMPLIANCE

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

OPERATING ENVIRONMENT

- Temperature—Operating: 10–35°c (50–95°f)
- Temperature—Non-Operating: -40–70°c (-40–158°f)
- Humidity—Operating: 20–90% non-condensing
- Humidity—Non-Operating: 50–90% non-condensing

HIGH AVAILABILITY

- Shipped in high availability configurations
- Redundant pairs may be physically separated for disaster recovery purposes
- Sensitive keys may be securely stored offline and offsite - Offline CA appliance available
- Interfaces to corporate NAS for backup via standard corporate processes
- M of N key splitting to Smart Cards enables full recovery and duplication

KEY MANAGEMENT SERVICES

- Signing: FIPS 186-3 compliant, RSA PKCS 1 v1.5 & PSS using 2048, 3072 & 4096 bit keys & ECDSA with 256, 384 and 512. SHA-1, SHA-256, SHA-384, SHA-512 hashing
- Keys may be securely imported or internally generated
- X.509v3 and proprietary certificate formats are supported
- Certificate revocation supported using CRL and OCSP
- Keys can be metered by product type and location; remote appliances only store limited quantities of keys
- Supports post-quantum cryptographic algorithms: ML-DSA, ML-KEM, LMS, SLH-DSA

DLM CONTROLLER (DC)

- Hosted or on-premise configuration options
- Manages DLM appliances and controls available services
- Web-based user interface for system configuration and key generation
- Local database can interface with external databases such as Oracle
- Aggregates backups and archived data from all appliances

USER ACCESS CONTROL

- Admin, Security Officer, and Developer operating roles
- Password or two-factor mechanism login
- Federate with corporate access control services

24X7 SUPPORT AND MAINTENANCE

- INTEGRITY Security Services offers the essential service level agreements to support global, high-volume device production. Expert in-house support staff operates our critical severity response hot line and works closely with escalation engineers in North America, Europe, and the Asia Pacific region.

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