



SCMS Update: The Commercial Perspective

Bill Lattin
Chief Security Architect & CMS Program Manager

experts in end-to-end embedded security



35 Years of Embedded Security

- **Green Hills Software:** (Incorporated 1982)

- Largest embedded security company in the world
- 1500+ existing embedded customers
- 37 offices worldwide
- Only RTOS to achieve Common Criteria EAL6+ certification



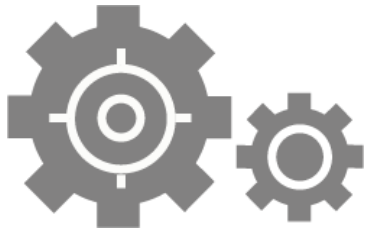
- **INTEGRITY Security Services (ISS)**

- Subsidiary of Green Hills Software
- Hardware and platform agnostic security solutions
- End-to-End Security Experts – device infrastructure
- Design and management team have 250+ years experience
- Over 1 billion devices secured with ISS solutions



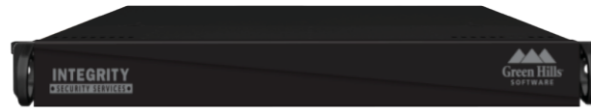
INTEGRITY Security Services

The most comprehensive and flexible standards-based solutions backed by the highest levels of government certification



ISS Embedded Security Services

- Architecture Studies & Solutions
 - NIST SP800-53; SAE J3061
- Penetration Testing
- Product/System Vulnerability Assessments
- FIPS 140-2 Certifications
- Expert Engineering Services



Device Lifecycle Management System

- Content Distribution
- Device Certificate Authority (CA)
- Software / Data Signing
- Device Enrollment
- Supply Chain Management
- Secure Device Management
- Secure Content Management
- Hosted or Standalone Deployment Models



ISS Security Toolkits

- Embedded Cryptographic Toolkits
 - Commercial & Suite B
 - Secure Protocol Stacks
 - Firewall / IDS / IPS
- INTEGRITY Control Manager
 - Secure Boot
 - Key Management
 - Data at Rest
 - Provisioning & Management

Green Hills' INTEGRITY Selected For Over 100 Flight-Critical Systems

GREEN HILLS SOFTWARE DOMINATES THE AIR



Boeing C-17



Boeing B-1B



Airbus A380



Lockheed Martin F-16



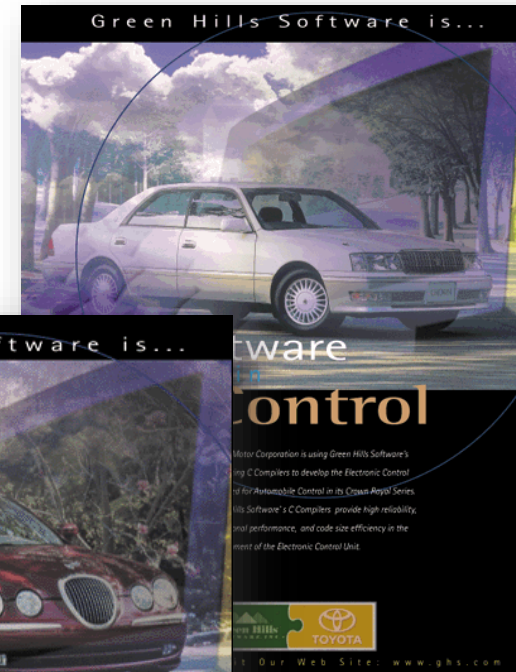
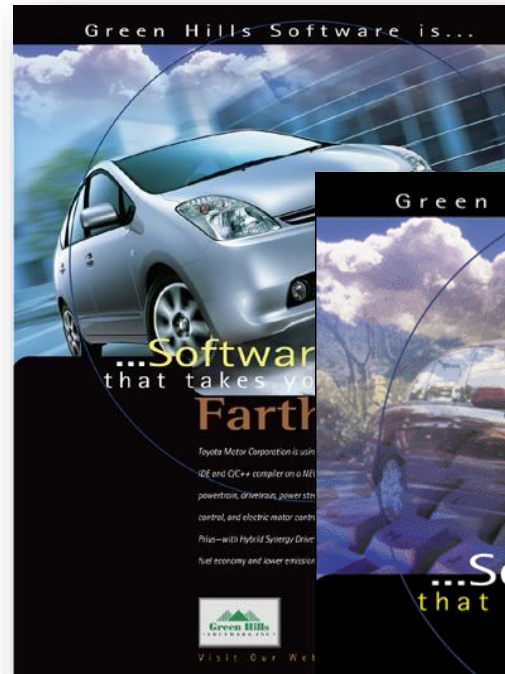
Lockheed Martin Joint Strike Fighter



Sikorsky S-92 (2002 Collier Trophy winner)

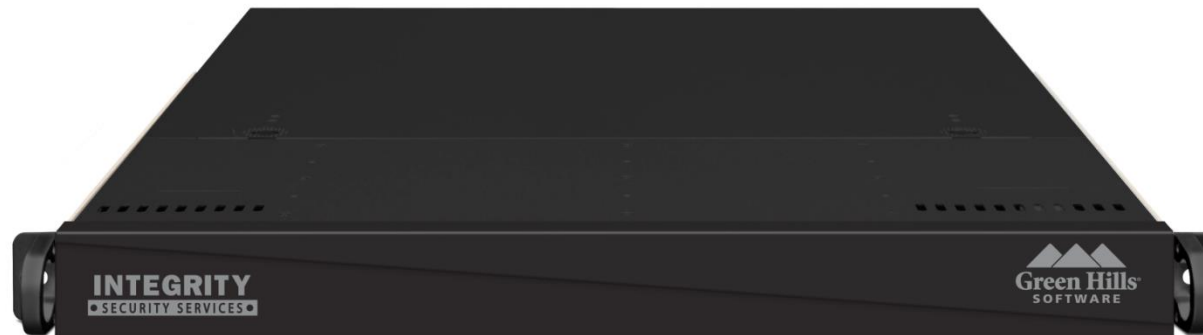
Strategic Supplier to Auto OEMs Since 1990

- ❑ Telematics & Infotainment Security & Content Management Solutions
- ❑ ECU Security Solutions
- ❑ Embedded PKI
- ❑ Code Signing
- ❑ Key Injection
 - HDCP, DTCP
 - SHE
- ❑ Secure OTA Update
- ❑ Feature Control
- ❑ Secure Diagnostics
- ❑ Secure Post Sale Vehicle Servicing
- ❑ V2X/C2X Credentials



ISS Security Infrastructure Solution - Device Lifecycle Management System

- ❑ 5th generation secure database application and security services platform that provides secure sensitive digital asset lifecycle management from manufacturing through aftermarket operation
 - Device Lifecycle Management System is a hardened platform using FIPS 140-2 L3 certified Hardware Security Modules (HSMs)
 - All cryptographic keys properly generated, managed and protected against misuse/compromise/theft/loss
 - Provides trusted and reliable operation in untrusted insecure environments
 - Provides access to keys for the target product lifetime (20 - 30 years)



ISS and V2X

- ❑ ISS has been involved with SCMS and V2X since 2014
- ❑ We provide both on-premise and hosted CMS solutions today for OEMs, Tier-1s, & Roadside Infrastructure Providers
 - ISS built the first on-premise CMS solution that is currently in production
 - Supports V2X & C2X certificates today
 - Maintains compliance with evolving standards
 - Hosted CMS Service announced December 2016
 - Currently serving certs for both V2V and V2I markets
 - Test branch providing certs to this PlugFest
- ❑ V2X Root CA
 - ISS raised the V2X Root CA in February 2016
 - Offline root CA serving both V2V and V2I SCMS applications for the industry today
 - Root raising was witnessed by CAMP, GM, US DOT & KPMG
 - WebTrust 2.0 certification in 2017

ISS and V2X – cont'd

- ❑ ISS contracted by CAMP to develop Proof of Concept SCMS
 - PoC SCMS development completed in August 2016
 - Will enter operational phase in September 2017
 - Will serve Connected Vehicle Pilot, Smart Cities, and additional programs
 - US DOT funded lifetime of approximately 5 years

- ❑ ISS CMS and CAMP PoC SCMS are both certified under the ISS V2X Root CA and are interoperable

CAMP & ISS SCMSes Compared

❑ CAMP QA SCMS

- Available mid to end of May 2017
- Will supply test certificates only for experimental purposes

❑ CAMP PoC SCMS

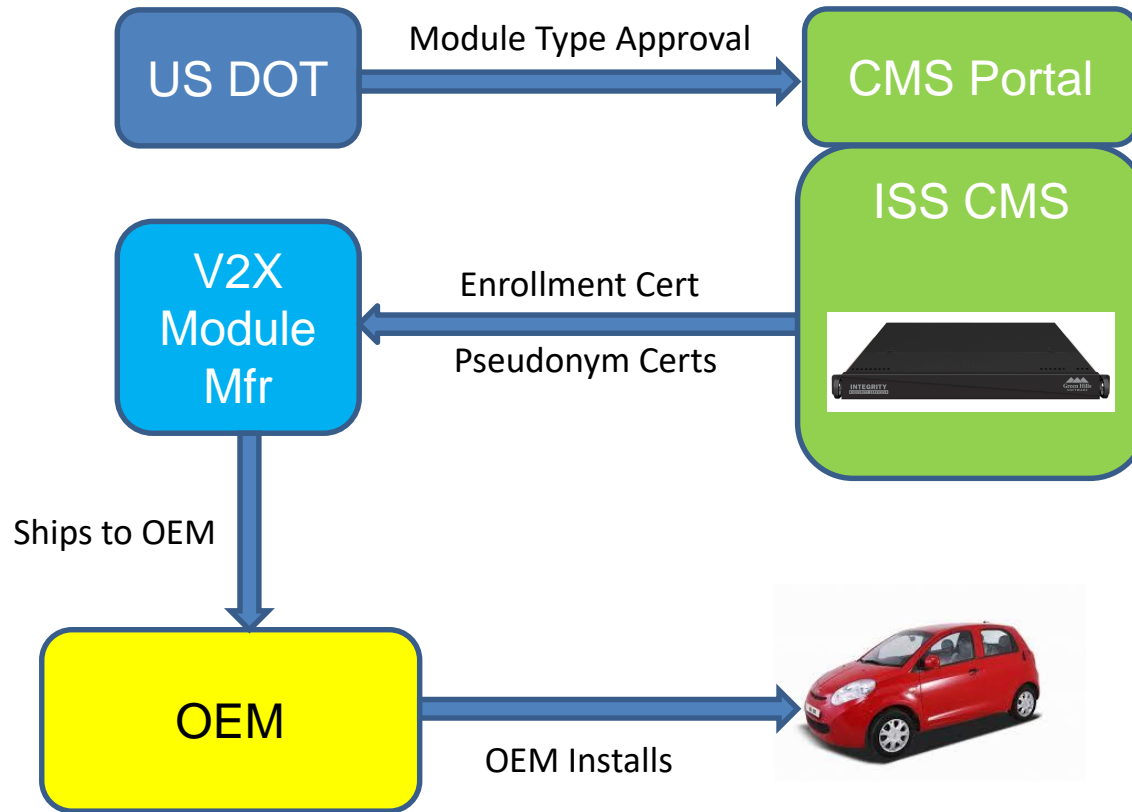
- No FIPS 140-2 Level 3 HSMs or operating policies & procedures
- Operational in September 2017
- Will supply certificates for CV Pilot & Smart Cites
- 5 year expected lifetime as funded by US DOT

❑ ISS CMS

- Commercial system available now
 - Uses FIPS 140-2 L3 HSMs; has operating policies and procedures
 - Redundant design for 24x7 operation
- Independently audited to ISO 27001
- Provides variety of initial provisioning methods for high volume manufacturing
- Will supply certificates for CV Pilot & Smart Cites
- Built to scale to serve the US national market with certificate top-offs for the life of the vehicle
- For OBU and RSU that will be operational beyond the 5 year CAMP window, ISS CMS provides a long-term option

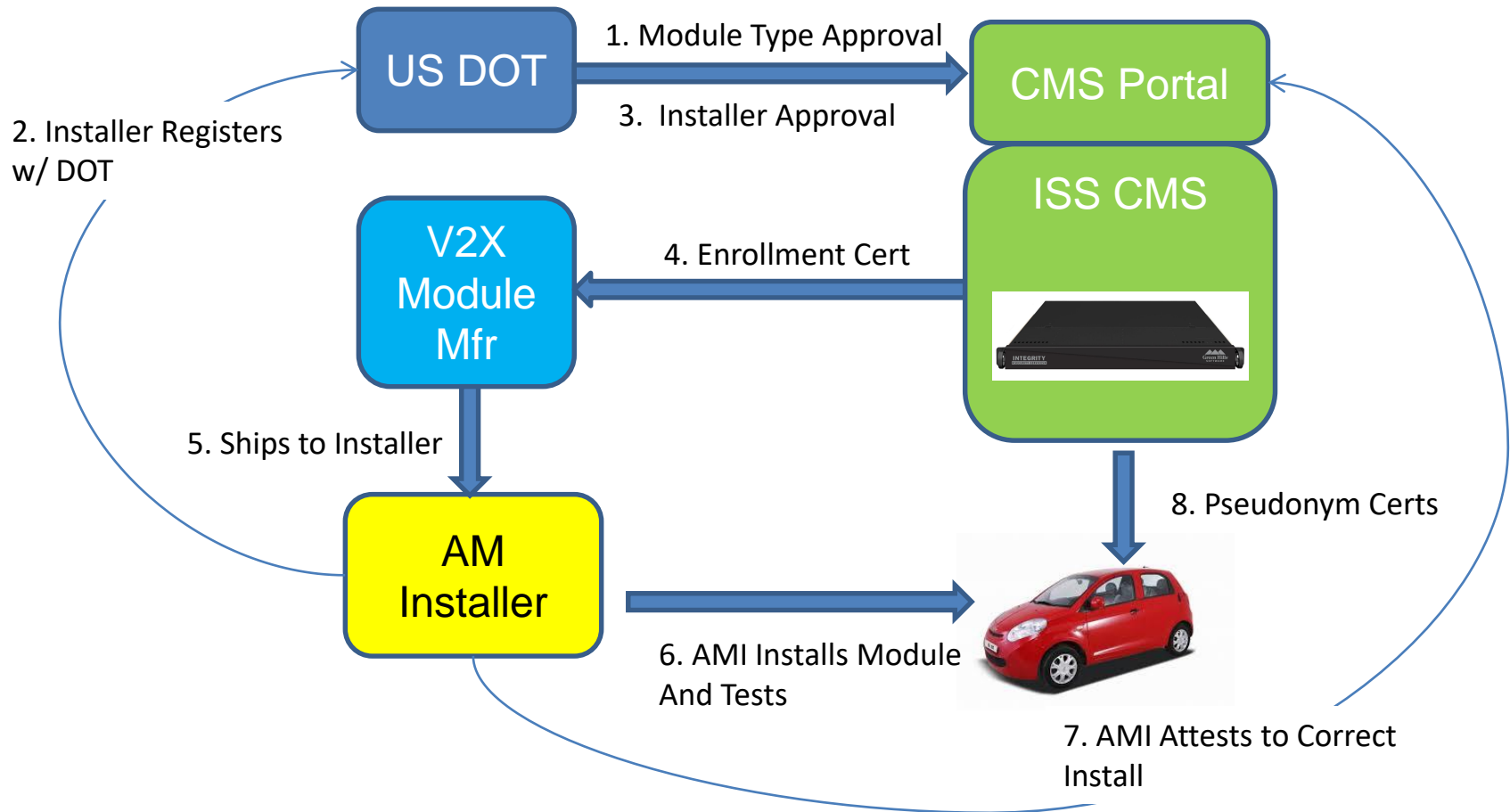
ISS CMS – Process Automation

❑ OEM Install of V2X Module



ISS CMS – Process Automation

❑ Aftermarket Install of V2X Module



Thanks!

Bill Lattin
Chief Security Architect &
CMS Program Manager
INTEGRITY Security Services

Dan Fynaardt
CMS Dev Team Lead
INTEGRITY Security Services

