

ENABLING REPROGRAMMABLE CRYPTOGRAPHIC PRODUCTS IN SPACE

Joseph D. Bull
ACSAC 2008
December 11, 2008



The CMI Initiative

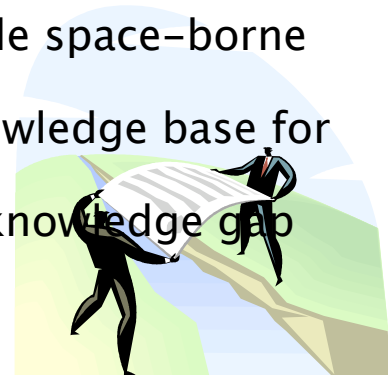
- Directed by the Department of Defense (DoD)
- Led by the National Security Agency (NSA)
- NSA's Director of the Information Assurance Directorate (IAD) Daniel G. Wolf said CMI will “transform and modernize capabilities for the 21st century ... at all echelons and points of use while exploiting new technologies and emerging technologies.”¹

Space System

- Legacy DoD communications satellites are non-programmable, point-to-point solutions that support only one static mission over their lifetime because of limitations due to major design challenges
- Those challenges stem from Size, Weight, and Power (SWAP), system availability, inaccessibility to deployed End Cryptographic Units (ECUs), and radiation effects

Impact

- The 5th CMI tenet is the most transformational—it requires reprogrammability of all cryptographic devices, which include space-borne crypto devices
- The cryptographic paradigm shift created a void in the knowledge base for space crypto
- This presentation proposes a process for addressing that knowledge gap



¹ “Leveraging Cybersecurity,” Interview with Daniel G. Wolf, Military Information Technology, Online Edition, Volume 8, Issue 1, February 9, 2004, www.military-information-technology.com/article.cfm?DocID=389

Communications Security (COMSEC)

- High Assurance Internet Protocol (IP) Encryptor (HAiPE): encrypts/decrypts classified packet traffic
- IP Security (IPSec): encrypts/decrypts sensitive packet traffic
- Circuit Encrypt and Decrypt: encrypts/decrypts all circuit traffic

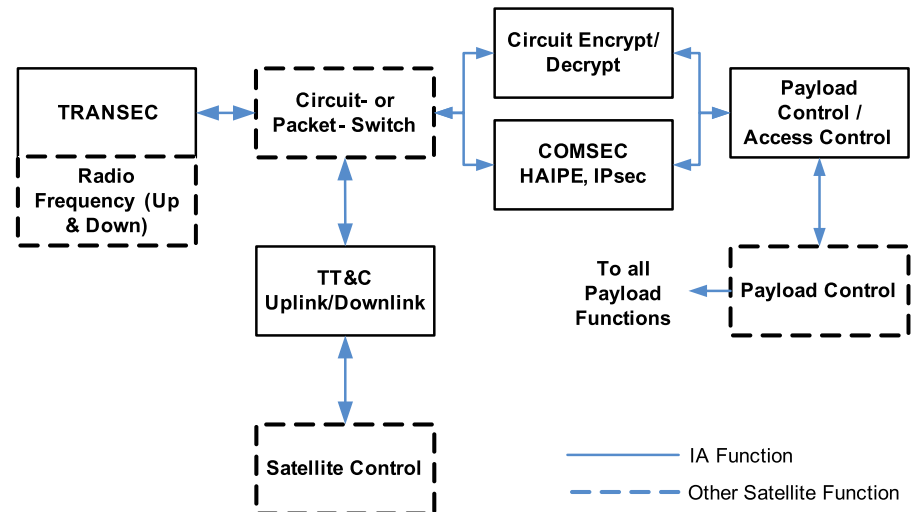
Payload and Access Control—

Authenticates and verifies the integrity of requests to be processed by the payload control

Telemetry, Tracking, and Command (TT&C)

- Uplink: decrypts, authenticates, and verifies the integrity of satellite control commands and authenticates the source
- Downlink: encrypts telemetry information and appends coding used to verify the integrity and authenticity of the commands

Transmission Security (TRANSEC)—
Protects against detection, jamming, and physical layer denial of service

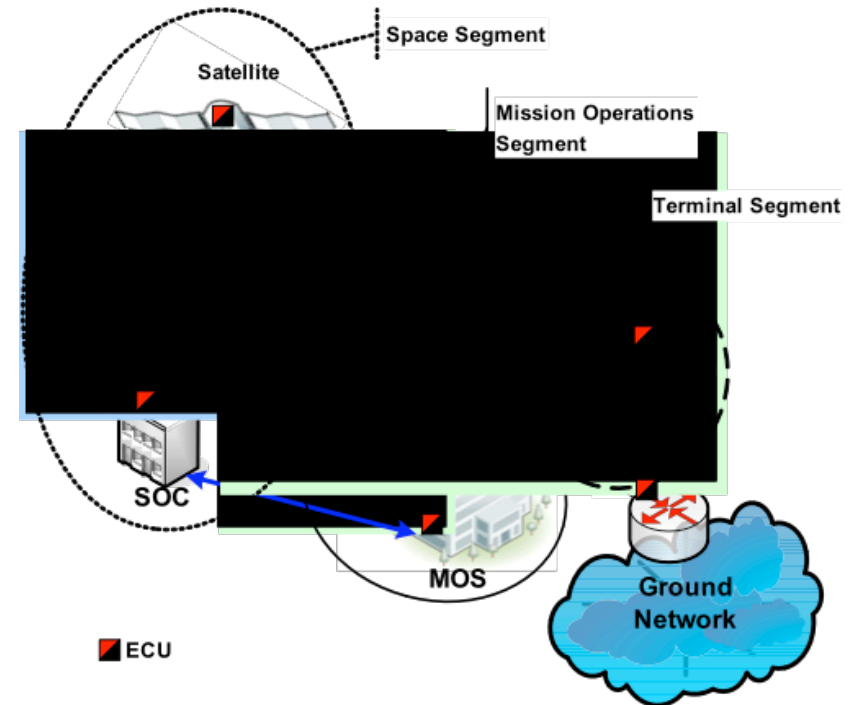


Use Cases

Use cases “allow [a] description of sequences of events that, taken together, lead to a system doing something useful.”¹

System Nodes

- End Cryptographic Unit (ECU): Product that utilizes cryptographic algorithms in support of security services
- Mission Operations Segment (MOS): Entity responsible for the mission of the satellite (payload portion of the satellite)
- Sustainment Factory (SF): Contractor that performs sustainment activities after the system is operational
- Space Segment (SS): System segment responsible for the satellite operation (bus portion of the satellite); includes the satellites and systems operation center (SOC)
- Terminal Segment (TS): System segment responsible for the terminals that connect to the Space Segment for communication with other users on the system



¹ Kurt Bittner and Ian Spence, Use Case Modeling, 1st Edition, Boston: Addison-Wesley Professional, 2002, pp. 2-3.

Use cases “allow [a] description of sequences of events that, taken together, lead to a system doing something useful.”¹

Message Types

- Algorithm Data File (ADF): Data package delivered to an ECU that contains the Cryptographic Algorithm Code (CAC) and the Cryptographic Algorithm Support Software (CASS)
- Accreditation Letter: Letter authorized by the DAA that states that the system can become operational
- Cryptographic Algorithm Specifications (CAS): The mathematical representation of the algorithm that can be translated into software for use in an ECU
- Cryptographic Algorithm Support Software: The supporting software for the implementation of the algorithm; this software is needed to allow the hardware to interface with the other management functions of the ECU

- Cryptographic Algorithm Code: The code that implements the cryptographic algorithm specifications
- Key Specifications: The details of the key that will be utilized with a given cryptographic algorithm
- Receipt: A message generated by the ECU to verify certain events to external components and systems

Actors

- Designated Approval Authority (DAA): Official with the authority to formally assume responsibility for operating a system at an acceptable level of risk
- National Security Agency: The supplier of key material and algorithms to all DoD programs utilizing Type 1 ECUs and the Type 1 ECU Certifier

¹ Kurt Bittner and Ian Spence, Use Case Modeling, 1st Edition, Boston: Addison-Wesley Professional, 2002, pp. 2-3.

Description

Purpose: Development of a new algorithm for space-borne ECUs post-launch. This development would occur after the NSA and DAA determine that a need exists for a new algorithm, regardless of the motivation for the change.

Pre-Conditions

- DAA decided to modify a cryptographic algorithm.
- A cryptographic algorithm already existed.
- ECU memory and processing capacity were available.
- A Recertification Plan existed.
- Host and ECU specifications were available.
- A representative ECU was available.

Post-Conditions

- Key Management Plan (KMP) is updated.
- Key Specifications are updated.

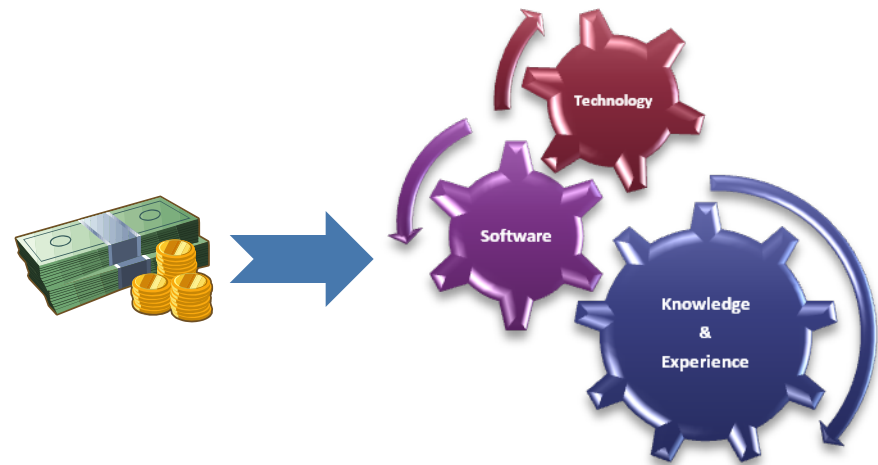


Issues Identified

Recertification of Space ECUs



Maintaining Ground Infrastructure



Description

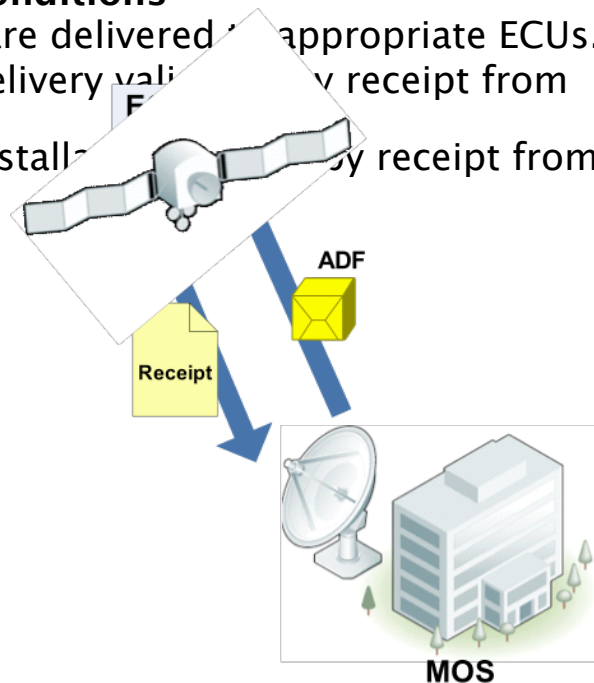
Purpose: Distribution of an ADF by the distribution agent to an ECU. For the satellites: in-band via the mission data link or out-of-band via the TT&C link. For the Terminal Segment: in-band via the mission link or, when necessary, by physical access. The ADFs can be sent in parallel to the various segments.

Pre-Conditions

- DAA authorizes the distribution of new ADFs.
- ADFs are prepared for distribution.
- System is operational.

Post-Conditions

- ADFs are delivered to appropriate ECUs.
- ADF delivery validated by receipt from ECU.
- ADF installation validated by receipt from ECU.



Issues Identified

Distribution Agent

- Entity with authority to distribute the ADF to the system ECUs
- Determined by scope of ECUs affected
- Provides direct insight into system impacts

ADF Transition Risk

- Actions
 - Minimize steps in transition process
 - Install ADF upon receipt
- Benefits
 - Reduces time to transition
 - Reduces potential for performance degradation

Description

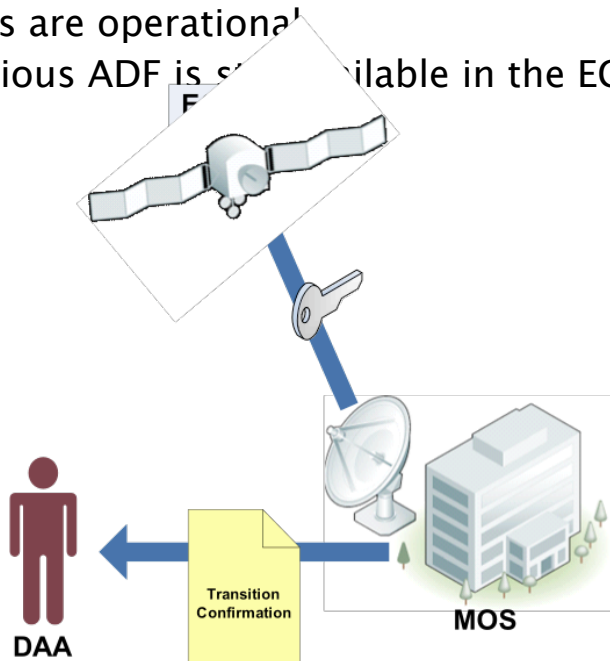
Purpose: Transition between the current ADF in operation and the new ADF uploaded and installed during the distribution use case

Pre-Conditions

- ADFs have been properly installed in the system ECUs.
- An ADF Transition Strategy exists.
- The DAA issues a directive to proceed with the transition.

Post-Conditions

- ADFs are operational
- Previous ADF is still available in the ECU.



Issues Identified

Transition Trigger Mechanism

- Mechanism is separate message OR Key tagged with algorithm name
- Goal is to reduce steps and complexity

ADF Rollback

- Enables the ECU to revert back to a last known good state
- Leverages emergency re-key function
- Creates potential need to limit number of ADF transitions within a period to reduce margin required for ECU

Threshold of ECUs before Transition

- Determined by system DAA
- Identifies specific ECUs in addition to the minimum number of ECUs required to be prepared for transition prior to the transition's occurrence
- Ensures that the system remains operational in support of the warfighter

Requirements Development

Requirements Were Derived From The Three Use Cases (Development, Distribution, Transition)

Requirements Categories

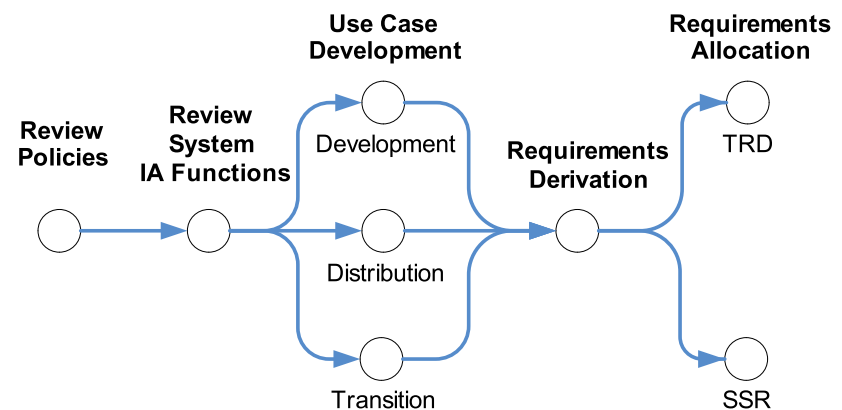
- Algorithm integrity specifications: Integrity mechanisms for ADF receipt and ADF retrieval from storage
- Storage specifications: The verification and validation required when the ADF is pulled from memory and the encryption required during storage (assured hardware backup)
- Margin: Memory and processing capability in excess of what is required for supporting the initial set of cryptographic algorithms and security functions for the mission
- Process functions: Steps required for receipt, installation, and transition between ADFs, in addition to supporting requirements
- ECU management: Requirements identifying the management functions that the ECU would support, including

- Delivery: Requirements identifying the approved process for delivery of the ADFs to the distribution agent

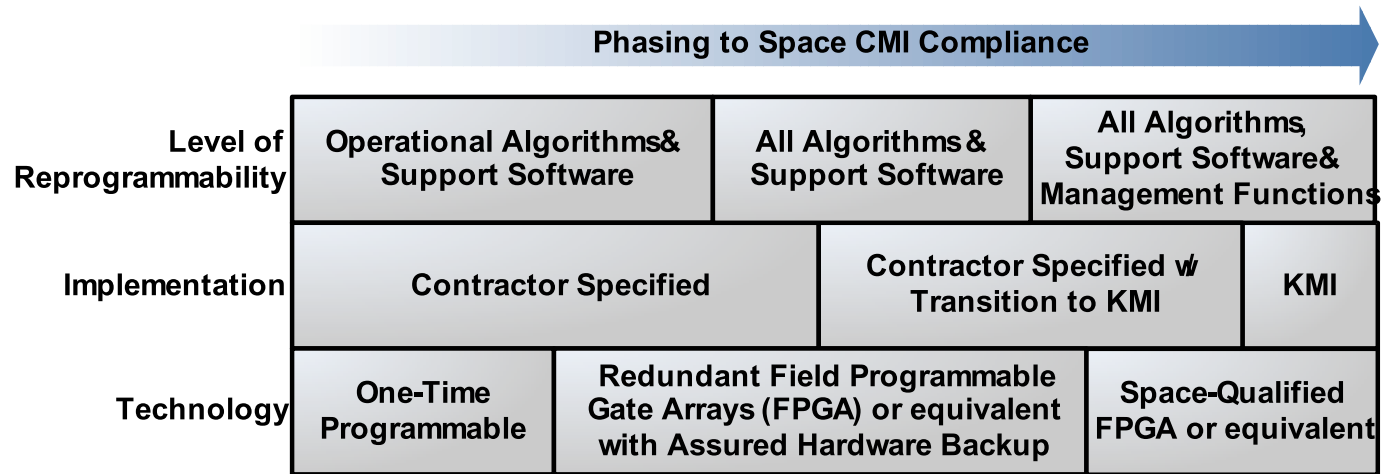
Requirements Placement

- Technical Requirements Document (TRD)
- System Security Requirements (SSR) document

Requirements Development Process



Phasing in the Transition



Enabling the Transition

- **Development of policies & guidance supporting Cryptographic Modernization**
 - Enable use of emerging technologies
 - Define minimum level of programmability
 - Guidance and baseline for application of CMI to space cryptographic products
- **Convergence towards standards & protocols**
 - Creation of standards & protocols removing reliance on proprietary implementations
- **Investment in enabling technologies**
 - Space environment necessitates specific technology

Steps to Success

- Understanding reprogrammability and its application to space crypto
- Reviewing policies and publicly available best practices
- Phasing in of Technology, the enabler for CMI compliance
- Enable the transition through policies, standards & protocols, and investments in enabling technologies

A CMI-compliant satellite system that supports the Warfighter of the future is possible!

Joseph D. Bull
Booz|Allen|Hamilton
(410) 684-6216
bull_joseph@bah.com