Air Force Cryptographic Modernization Transformational Initiatives

3rd Annual Layered Assurance Workshop

Ms. Nancy Pham
CPSG/ZXE
Systems Engineering Division Chief
Air Force Cryptographic Modernization Program Office
(210) 925-2620 (DSN: 945)

4 Aug 2009

DISTRIBUTION A: Approved for public release; distribution is unlimited. (27 Jul 09).

Purpose

- Provide a high-level overview of Air Force Cryptographic Modernization Program Office’s (AF CMPO) transformational initiatives and partnerships

Agenda

- AF CMPO Overview
- Transformational Initiatives
  - Remote Operational Management of ECUs (ROME)
  - Multi-Level Security (MLS)
  - Small Unmanned Aircraft System (SUAS) Encryption
  - Dynamic Group Keying (DGK)
- Partnership/Way-Ahead

AF CMPO Overview

Mission

Enable information dominance by modernizing Air Force cryptographic implementations and sponsoring technology developments

Vision

Transparent, Net-Centric Secure Communications

AF CMPO Transformation

- **Replacing legacy algorithms and components is necessary, but replacement alone will not realize the intent of the DoD CM initiative**

- **AF CMPO vision to enable "Transparent, net-centric, secure communications" requires going beyond CJCSN 6510 to provide transformational capabilities**

- **This brief will discuss some of the AF CMPO transformational initiatives and the critical role partnerships play in realizing these capabilities**

AF CMPO Support Across GIG IA

*Supports 5 of 6 GIG IA Capability Areas**

Assured Mission Management

- Remote Operational Management of ECUs (ROME)
- Dynamic Group Keying

Highly Available Enterprise

-Dynamic Group Keying

-SWAP-Constrained Crypto

-- Smart Munitions

-- SW Crypto Prototype

-- SUAS Crypto

-High-Speed Crypto

-F-22 Crypto

Assured Information Sharing

-MLS Component Standards

-Dynamic Group Keying (DGK)

-Link 16

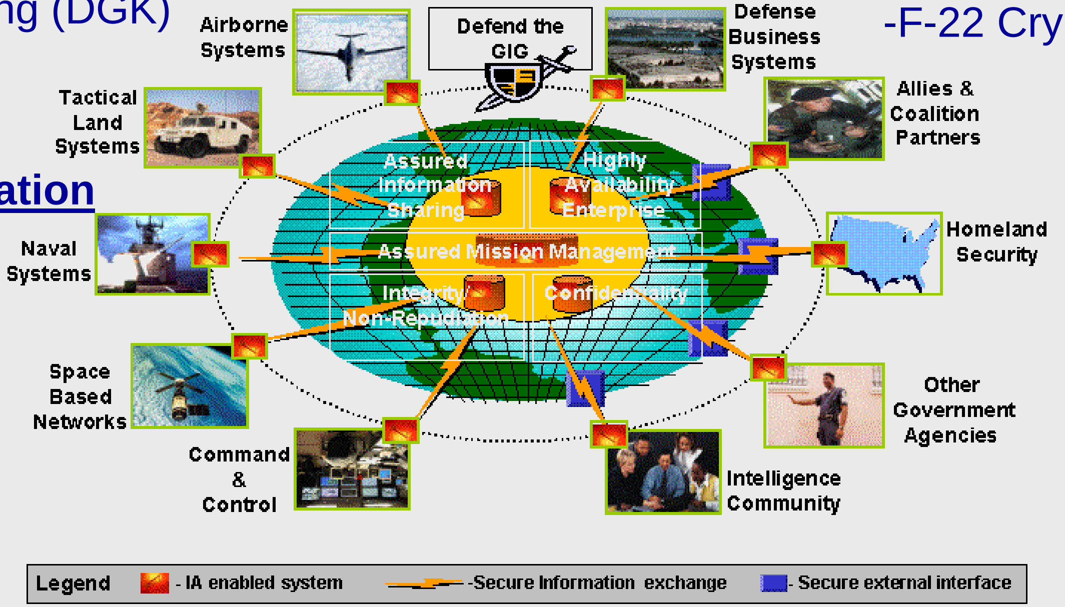
Integrity/Non-repudiation

-ROME

-Trusted Platforms

-T1D@R

Global Information Grid (GIG)
Information Assurance (IA) OV-1


Airborne Systems
Defend the GIG
Defense Business Systems
Allies & Coalition Partners
Tactical Land Systems
Assured Information Sharing
Highly Availability Enterprise
Assured Mission Management
Integrity/ Non-Repudiation
Confidentiality
Naval Systems
Homeland Security
Space Based Networks
Other Government Agencies
Command & Control
Intelligence Community
Legend
- IA enabled system
-Secure Information exchange
- Secure external interface

Confidentiality

-CJCSN 6510

-High-Speed Crypto

-Link Encryption

-T1D@R

-POET

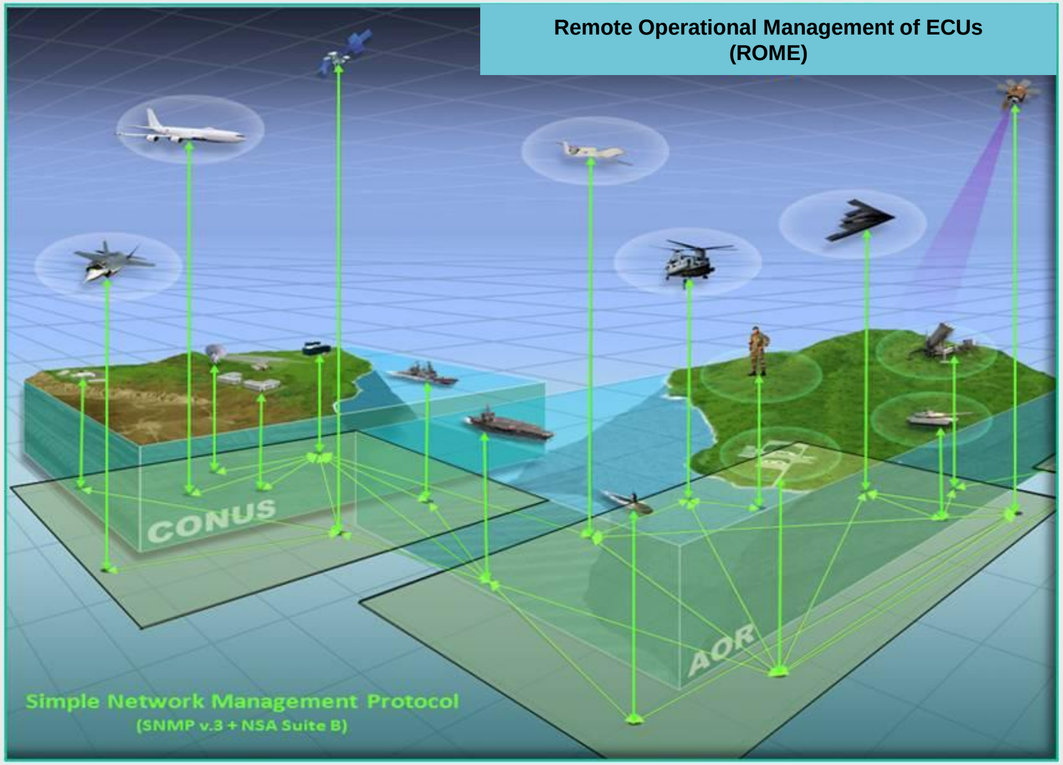
**Per ICD for Global Information Grid Infiormation Assurance (GIG IA), 6 March 2006*

Remote Operational Management of End Crypto Units (ECUs) (ROME)

ROME Background

- **Objectives:**
  - Provide standard for operational management of high assurance crypto
  - Deliver a reference implementation for secure ECU management

- **Requirements Sources:**
  - NSA Policy 3-9 for standardized ECU management
  - Crypto Mod Mission Area Initial Capabilities Document Section 5.1.3, Operational Mgt
- **Stakeholders:**
  - NSA
  - Services

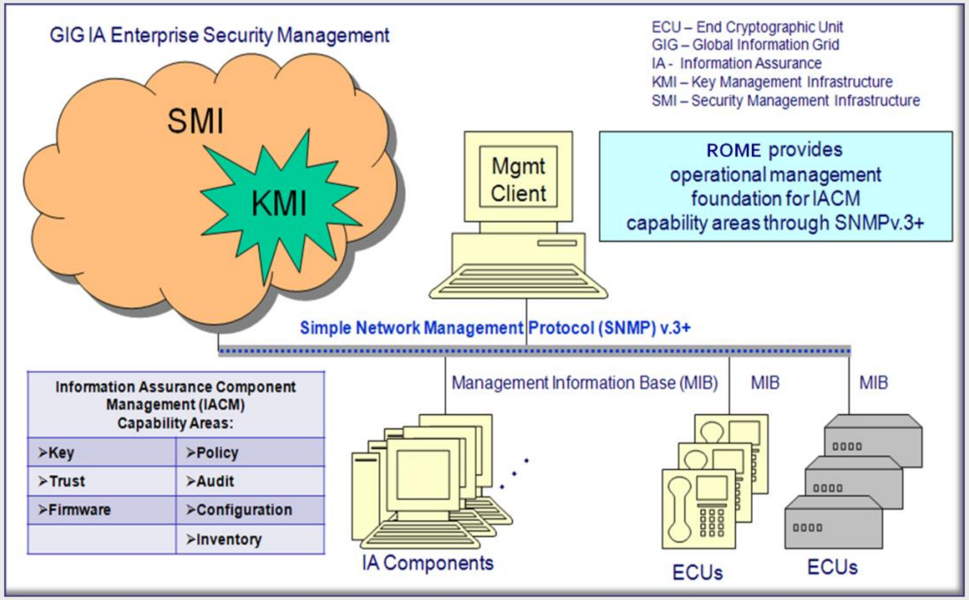


Remote Operational Management of ECUs (ROME)

"Securing the Global Information Grid"

ROME Progress

- 2006: Proof-of-concept implementation
  - Enhanced security in the Simple Network Management Protocol version 3
  - Highlighted gap in Information Assurance Component Management (IACM) standards
- 2007: Prototype implementation
  - Conducted in partnership with NSA/I5
  - Internet-Draft document delivered
- 2008: Concept Synchronization
  - Synchronizing ROME with KMI Over The Network Keying (OTNK) effort
  - Sponsoring ROME standard within Internet Engineering Task Force: Datagram Transport Layer Security (DTLS) Transport Model (TM) for Simple Network Management Protocol version 3 (SNMPv3)


GIG IA Enterprise Security Management
SMI
KMI
Mgmt Client
Simple Network Management Protocol (SNMP) v.3+
Management Information Base (MIB)
MIB
MIB
IA Components
ECUs
ECUs

ECU – End Cryptographic Unit
GIG – Global Information Grid
IA - Information Assurance
KMI – Key Management Infrastructure
SMI – Security Management Infrastructure

ROME provides operational management foundation for IACM capability areas through SNMPv.3+

Information Assurance Component Management (IACM) Capability Areas:	
➢Key	➢Policy
➢Trust	➢Audit
➢Firmware	➢Configuration
	➢Inventory

ROME Way Ahead

- **2009: Technology Maturation**
  - Continue DTLS TM maturation through Internet Engineering Task Force (IETF) Request for Comments process
  - Initiate standardization of Management Information Base (MIB) for operational management of Type 1 ECUs

- **2010: Reference Implementation**
  - Instantiate DTLS TM based reference implementation
    - Demonstrate security enhanced protocol
    - Demonstrate use of a standardized ECU MIB with modernized IP-addressable ECU
    - Demonstrate secure remote management of a modernized ECU through a Graphical User Interface (GUI)

Multi-Level Security (MLS)

MLS Background

> "Future military applications require the ability to process information with different classifications and handling caveats. Cryptographic devices must support user applications that can process and protect information with different classifications."
>
> MA ICD - CRYPTOGRAPHIC MODERNIZATION 14 Aug 04

Objective:

- Advance standards and technologies of high assurance MLS/Multiple Independent Levels of Security (MILS) solutions for insertion into mission critical systems and network infrastructure

Supports AF CM Common Standards Thrust

MLS Progress

- Identified specific user requirements via engagement with stakeholders
  - Desktops
  - Embedded Weapon Systems
  - Toolsets

- Supporting research and development efforts to further the technology state of MLS/MILS solutions
  - Sponsoring AFRL (Composability Toolset and Protection Profile)
    - Partnering with Industry
  - Investigating CENTCOM One Box One Wire (OB-1) JCTD effort

MLS Way Ahead

- Minimize risks and determine appropriate set of technologies to integrate into full MLS/MILS systems development
  - Toolsets
    - Developing MLS toolsets
    - Investigating MLS data labeling/transfer study
  - Desktops
    - Formulating OB-1 JCTD Technical Manager Risk Reduction Effort
  - Embedded Weapon Systems

Leverage existing MLS/MILS research to satisfy AF / Joint requirements for operational networks

Small Unmanned Aircraft Systems (SUAS) Encryption

SUAS Encryption Status

- ♦ **Partnered with Army's Natick Labs to prototype a software based crypto solution (not Type I) for Raven B's Digital Data Link (DDL)**

<u>Platform Name</u>: Raven B (RQ-11B)
<u>Platform Weight</u>: 4.5 Pounds

SUAS Encryption Status (cont.)

- **Partnering with 670th AESS to develop a secure Digital Data Link for AFSOC's Battlefield Air Targeting Micro Air Vehicle (BATMAV)**

Platform Name: BATMAV (WASP)
Platform Weight: 1 Pound

SUAS Encryption Way Ahead

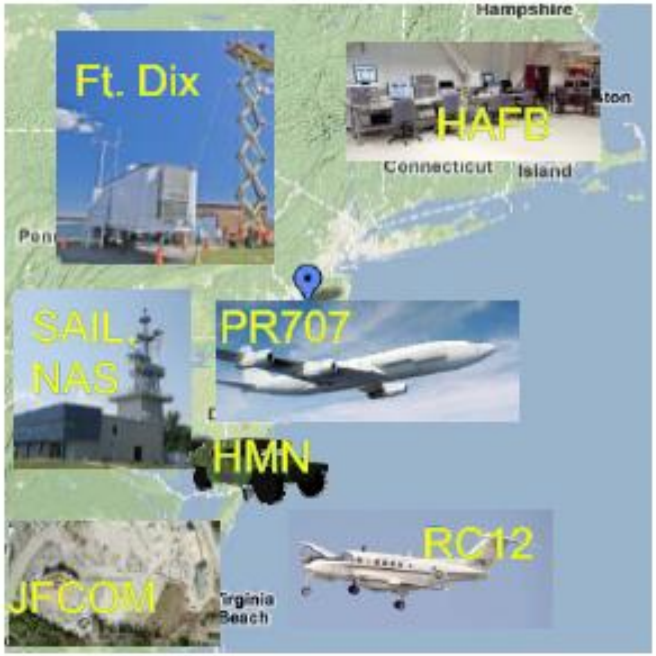
- Continue to work with AF CM Lead Command in supporting 670th AESS by working towards integrating an NSA-approved crypto solution within the DDL for development of future SUAS platforms

Dynamic Group Keying (DGK)

DGK Background

- AF CMPO has been working with MIT Lincoln Lab’s Information Systems Technology Group to realize a secure dynamic group keying capability
- DGK is currently being investigated for air/ground chat applications and SUAS video distribution
- DGK will draft a potential standard for general use

DGK utilized in Capstone II Exercise (Sept 2008)



34 hours	4 rooms	23-31 users	10.5K msgs	~2500 gr.ch.

"GROK chat was very intuitive and easy to use. The chat session was always reliable and available."
Capt. Derek Dwyer
630 ELSS, ESC (TD)

"GROK chat provided secure communications and was a vast improvement over previous chat platforms utilized on the Boeing 707."
Mr. James Carroll
950 ELSG, ESC (TD)

Successful demonstration of on-the-fly keying of dynamic groups in airborne networks

DGK applied to SUAS

Small Unmanned Aerial System

High-priority for DoD

- Secure video bcast
- Dynamic groups of remote video terminals

DGK Focus

- Usability and low comm. overhead
- Support for both passive and active video terminals
- General, extensible DGK solution

Summary

Summary

- AF CMPO is taking a phased approach to implementing DoD's CM initiative

- While replacement of legacy crypto has dominated the first phase of the initiative, AF CMPO is now focusing more on developing transformational cryptographic capabilities