(U) High Assurance Internet Protocol Encryptor (HAIPE®)

JCMO

December, 2010

Mike Irani
SPAWAR Systems Center Pacific
irani@spawar.navy.mil

(U) Overview

- (U) HAIPE ® Overview
- (U) HAIPE Key Management Concepts
  - EKMS and pre-KMI
  - HAIPE Interim Solutions
  - HAIPE and KMI
- (U) Current Initiatives
- (U) Products

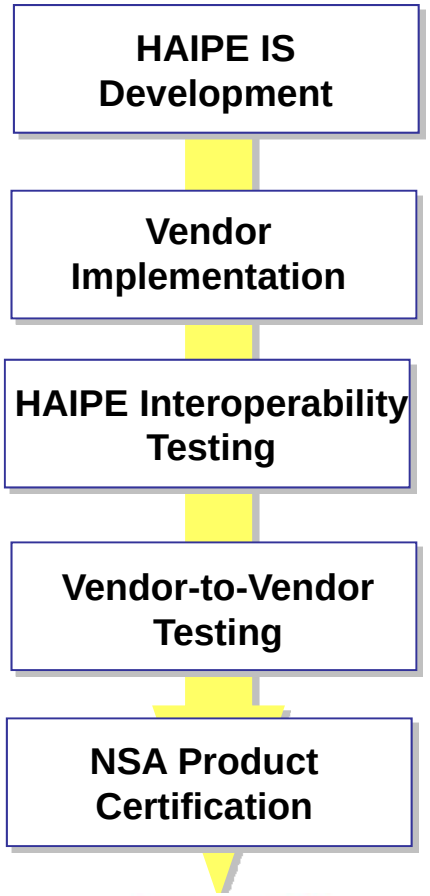
(U) The HAIPE® Program Office

- (U) The mission of the HAIPE PO is to ensure interoperability between HAIPE implementations by specifying requirements and verifying compliance through demonstration, test, analysis, and inspection
  - Development and configuration management of the HAIPE documents
  - Development, configuration management, and deployment of the HAIPE Interoperability Test Tool (HITT)
    - Embedded implementation developers must provide test harness/rig
  - Operation of the HAIPE Interoperability Test Facility
    - SPAWAR Systems Center – Pacific (San Diego, CA)

Interoperability not Interchangeability

(U) HAIPE® PO development process

- (U) Interoperability specification development based on solicited user requirements and current/near future technology trends
- (U) Vendor implementation based on market segment and user community needs
- (U) HAIPE interoperability testing ensures compliance with the HAIPE IS core and extensions
- (U) Vendor-to-vendor testing ensures interoperability across multiple vendors with similar capabilities
- (U) Product certified for the protection of National Security Sensitive information



(U)

(U) What is the HAIPE ® Product Cycle?

Key Activities	Product Cycle
– Community Buy-In – HAIPE PMO Resources – Evaluator Review	Specification
– User Demand – Funding – Evaluator Certification	Implementation
– Product Purchase & Integration – Configuration Guidance – System Accreditation	Deployment

(U) Evolution of HAIPE® Products

(U) HAIPIS 1.3.5 Compliant Products

(U) HAIPIS 1.3.5 resulted in development of primarily gateway based devices.

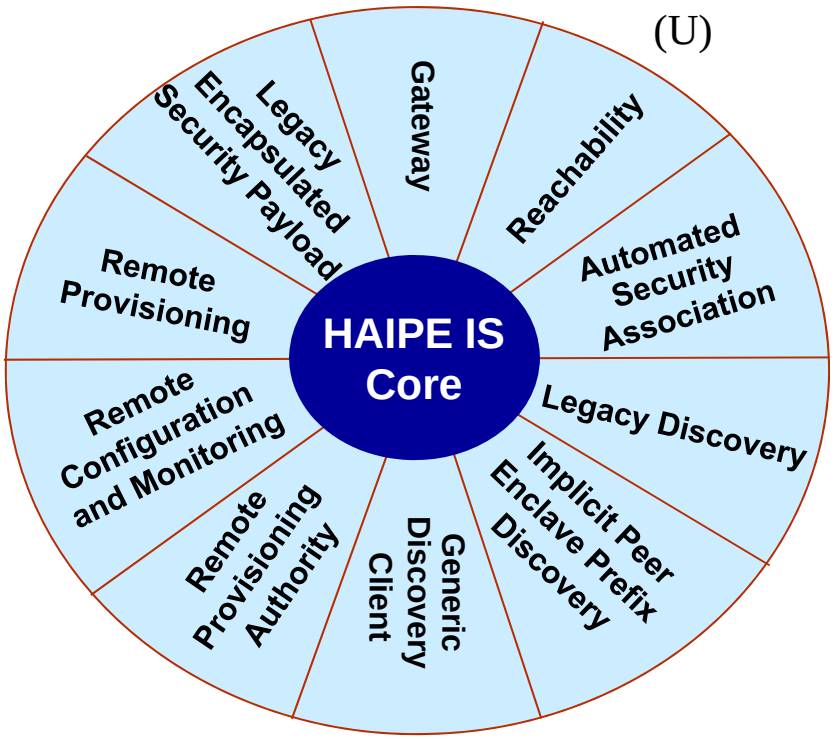
(U) HAIPE IS 3.X Compliant Products

(U) HAIPE IS 3.X is modular to enable development of a wide variety of devices

- Network Gateway
- Host/Embedded application

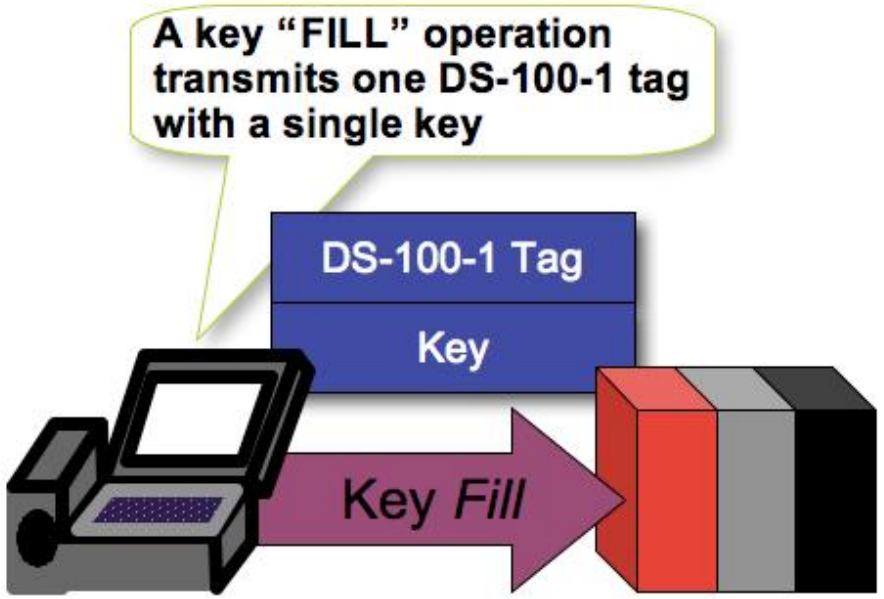
(U) HAIPE® IS Hierarchy

- (U//FOUO) The HAIPE Interoperability Specification is a set of documents that contains all HAIPE feature interoperability requirements (The HAIPE IS is not a product specification)
  - Core features (mandatory for all implementations)
  - Extension features (mandatory for some implementations)
  - Multiple cryptographic suites
    - Suite A (U.S., second party)
    - Suite B (high risk of compromise, third party, and commercial)
    - Legacy (backwards compatibility)



(U) Current HAIPE® Key Products

- (U//FOUO) Suite A
  - EFF vector (EFF exchange)
    - In 5 DePAC (US, Coalition, CCEB, NATO, NATO Nations)
    - CKL
  - PPK
- (U//FOUO) Suite B
  - EFF vector (MQV exchange)
    - In 5 DePAC (US, Coalition, CCEB, NATO, NATO Nations)
    - CKL
  - APPK
- (U//FOUO) Device Keys
  - S^2 (change software signature)
  - P^3 (change DePAC)
  - Q^2 (future change APPK trust anchor)

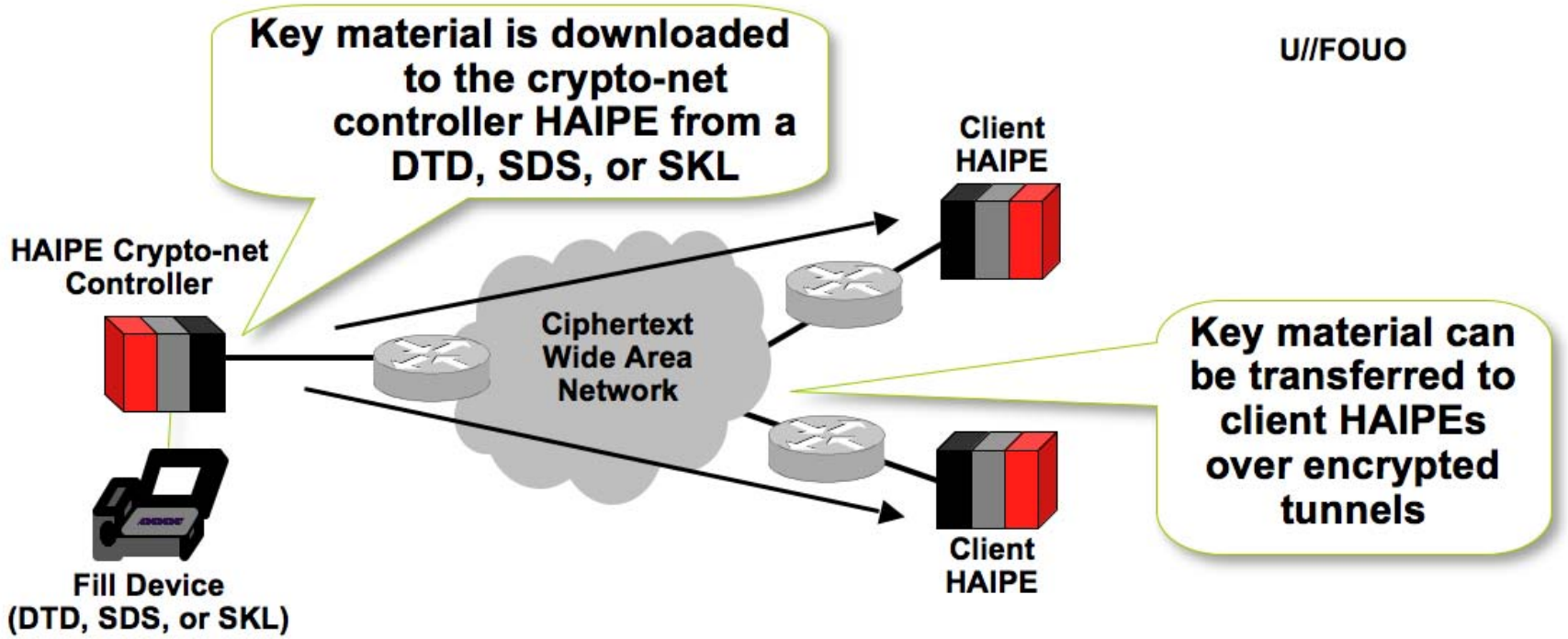


(U) HAIPE® Key Products Delivery Today

- (U//FOUO) EFF, PPK, APPK, P^3 and Q^2
  - Fax or call order
  - Central Facility (CF) generated to Message Server (MS)
  - Call for LMD to MS (or STE transfer to Data Transfer Device (DTD))
  - LMD decrypts Bulk Encrypted Transaction (BET)
  - LMD transfer to DTD
  - DTD file HAIPE
- (U//FOUO) PPK
  - Generated at Key Processor (KP)
  - LMD transfer to DTD
  - DTD to HAIPE

Note:
1. PPK, APPK, P^3, Q^2 generated at Fort Meade transferred to CF to MS
2. S^2 generated a Fort Meade and delivered on physical media only
3. PPK can be generated at KP or Fort Meade
4. APPK, S^2, P^3 and Q^2 must be called into Fort Meade
5. HAIPE IS 3.1 allows key to be loaded at one HAIPE and transferred to another HAIPE for consumption

(U) HAIPE®-to-HAIPE Key Transfer (HAIPE 3.1)



(U) H2HKT Modes

- (U) Key material can be transferred using in-band and out-of-band modes
  - In-band supports the delivery of symmetric key material only
  - Out-of-band supports symmetric and asymmetric
- (U) Authentication and dePAC operations are performed at the client

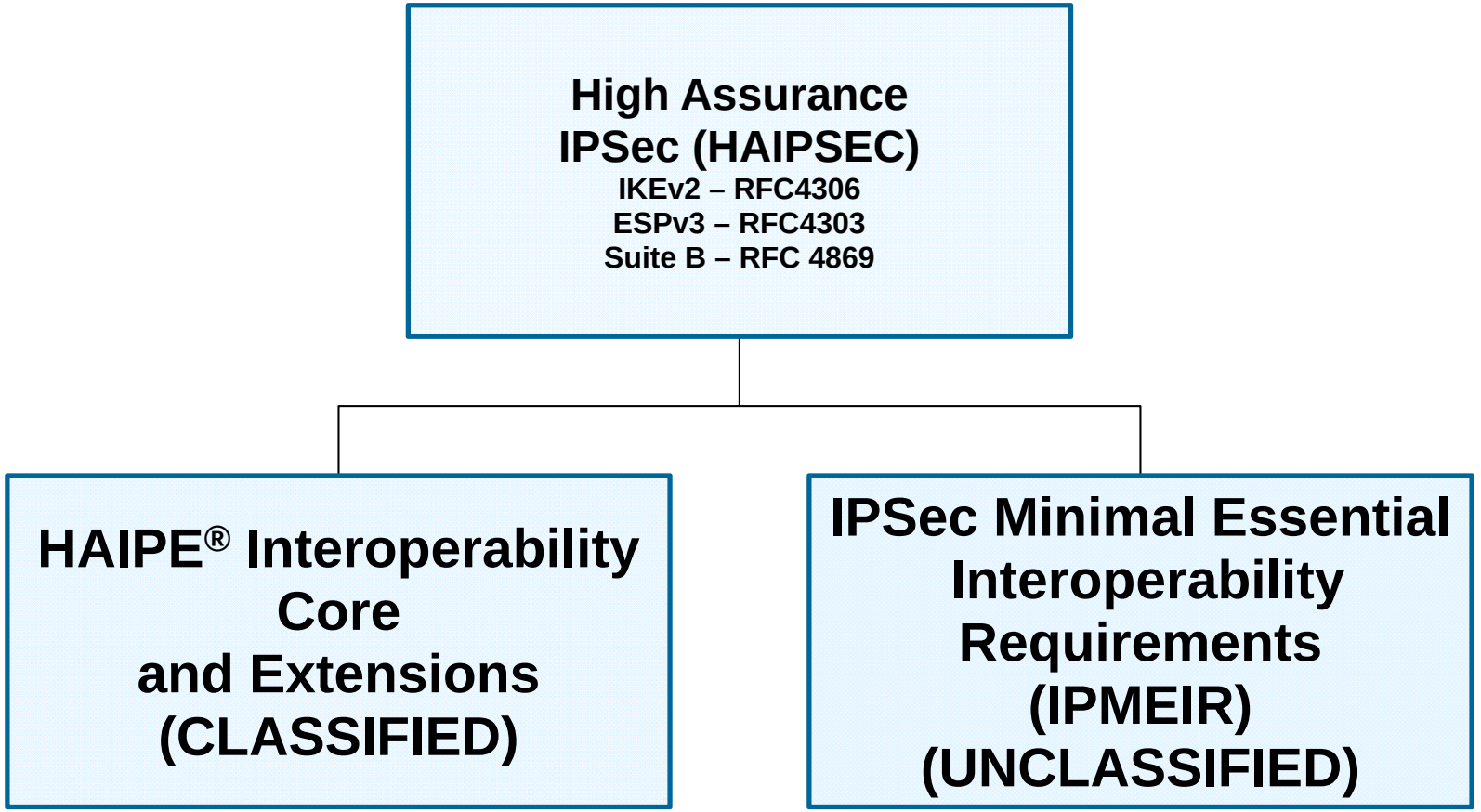
(U) HAIPE ® and KMI

- (U) HAIPEs are expected to be a major consumer of KMI products.
- (U) HAIPE 4.1 extension adds requirement for KMI/OTNK
  - KMI 3301 describes HAIPE extension for OTNK
- (U) Additional work needed in determining delivery options for those device not able to connect to PDE.
  - Disconnected nodes
  - KMI Aware, non-PDE enabled.

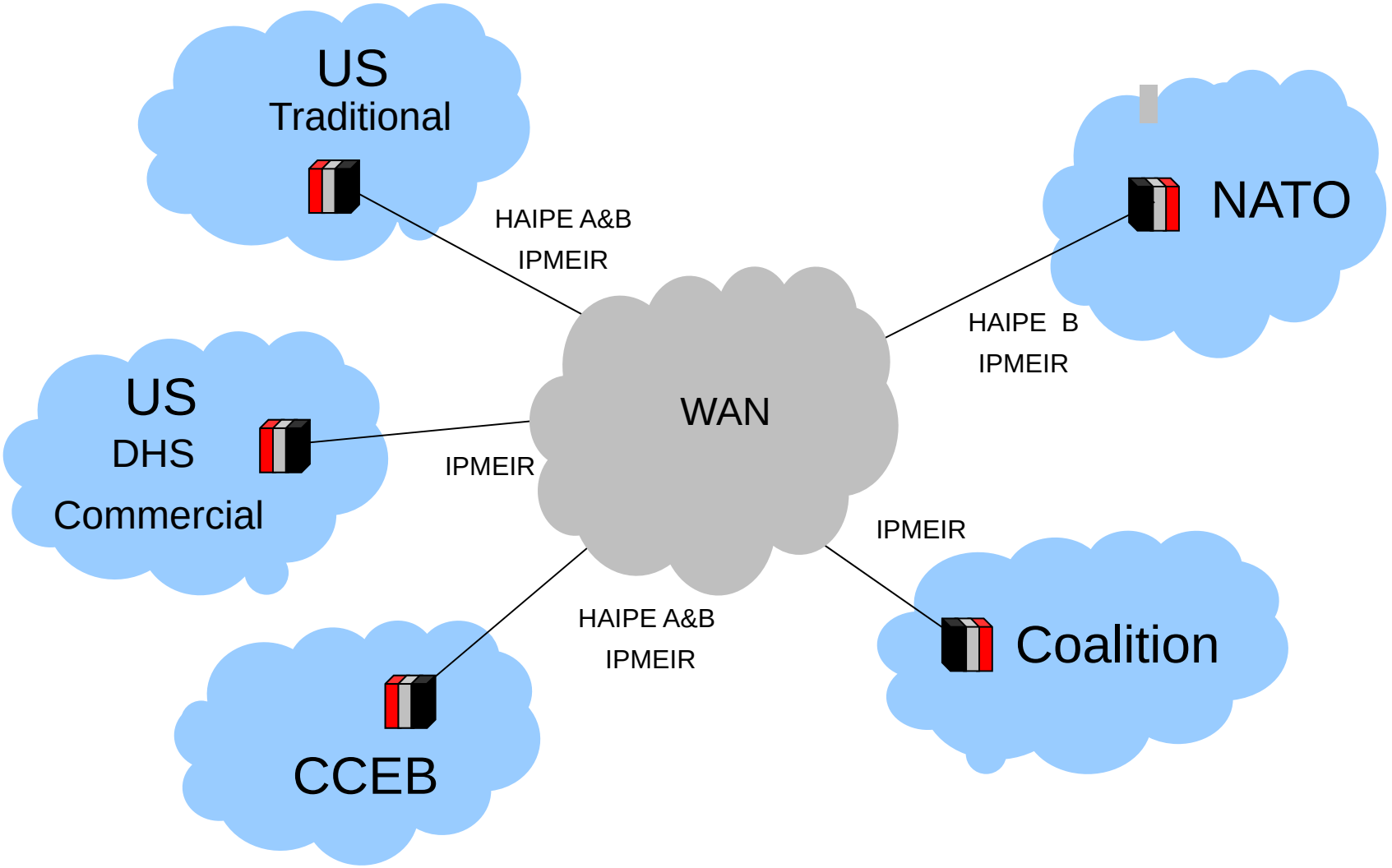
(U) Current Developments

- (U) HAIPE ® version 4.1.0
  - Added IKEv2, ECDH
  - Added Dynamic Multicast Group Creation
- (U) Participating in Corporate Initiatives
  - GOTS Secret and Below
  - Cryptographic High Valued Product (CHVP)
  - IPMEIR
    - Interoperability with CIS Suite B
- (U) Over 140,000 products fielded over 10 years
- (U) User input still influencing feature evolution

(U) HAIPsec


High Assurance IPSec (HAIPSEC)
IKEv2 – RFC4306
ESPv3 – RFC4303
Suite B – RFC 4869
HAIPE® Interoperability Core and Extensions (CLASSIFIED)
IPSec Minimal Essential Interoperability Requirements (IPMEIR) (UNCLASSIFIED)

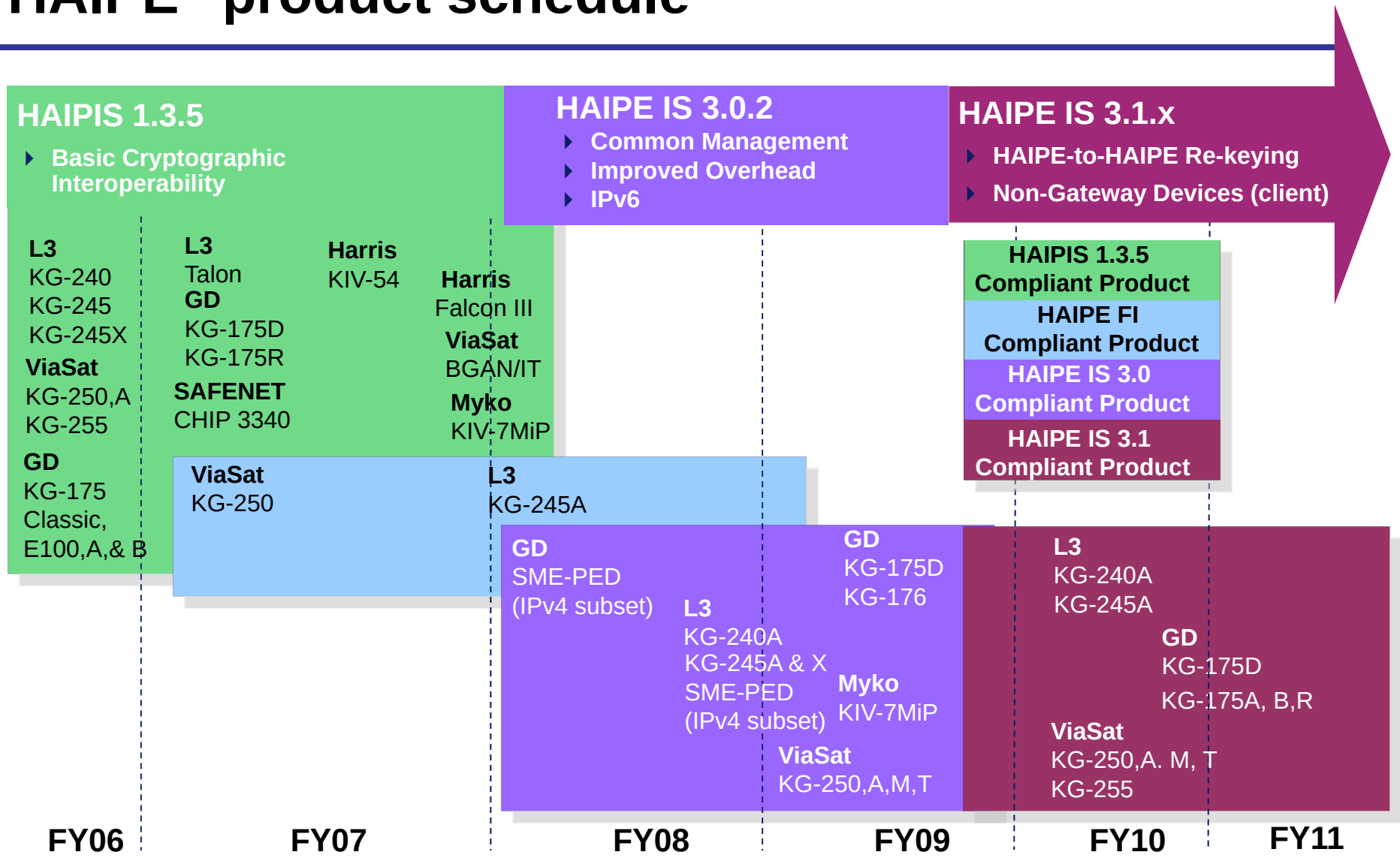
(U) Interoperability Model



(U) Challenges

- (U) Keying Infrastructures Alignment
- (U) Interoperability Testing
- (U) Beyond the US

(U) HAIPE® product schedule



(U) Questions?

December, 2010

Mike Irani
SPAWAR Systems Center Pacific
irani@spawar.navy.mil