NSA Cryptographic Interoperability Strategy

Anne Gugel, CISSP, ISSEP

anne.gugel@jhuapl.edu

443-778-0264

05 October 2010

Keep your secrets safe with the latest security techniques

Cryptography FOR DUMMIES®

Practical directions for security methods you can use today

A Reference for the Rest of Us!®

FREE eTips at dummies.com®

Chey Cobb, CISSP
Former Sr. Tech Security Advisor, National Reconnaissance Office

The Problem – Secure Interoperability

- **Currently available, fielded technologies do not allow flexible, scalable secure interoperability**
- **Impact: War fighters, first responders, Federal, international partners lack the ability to communicate securely**

The Problem – Secure Interoperability

- **Lack support for flexible security policies**

The Problem – Secure Interoperability

- **Handling restrictions**

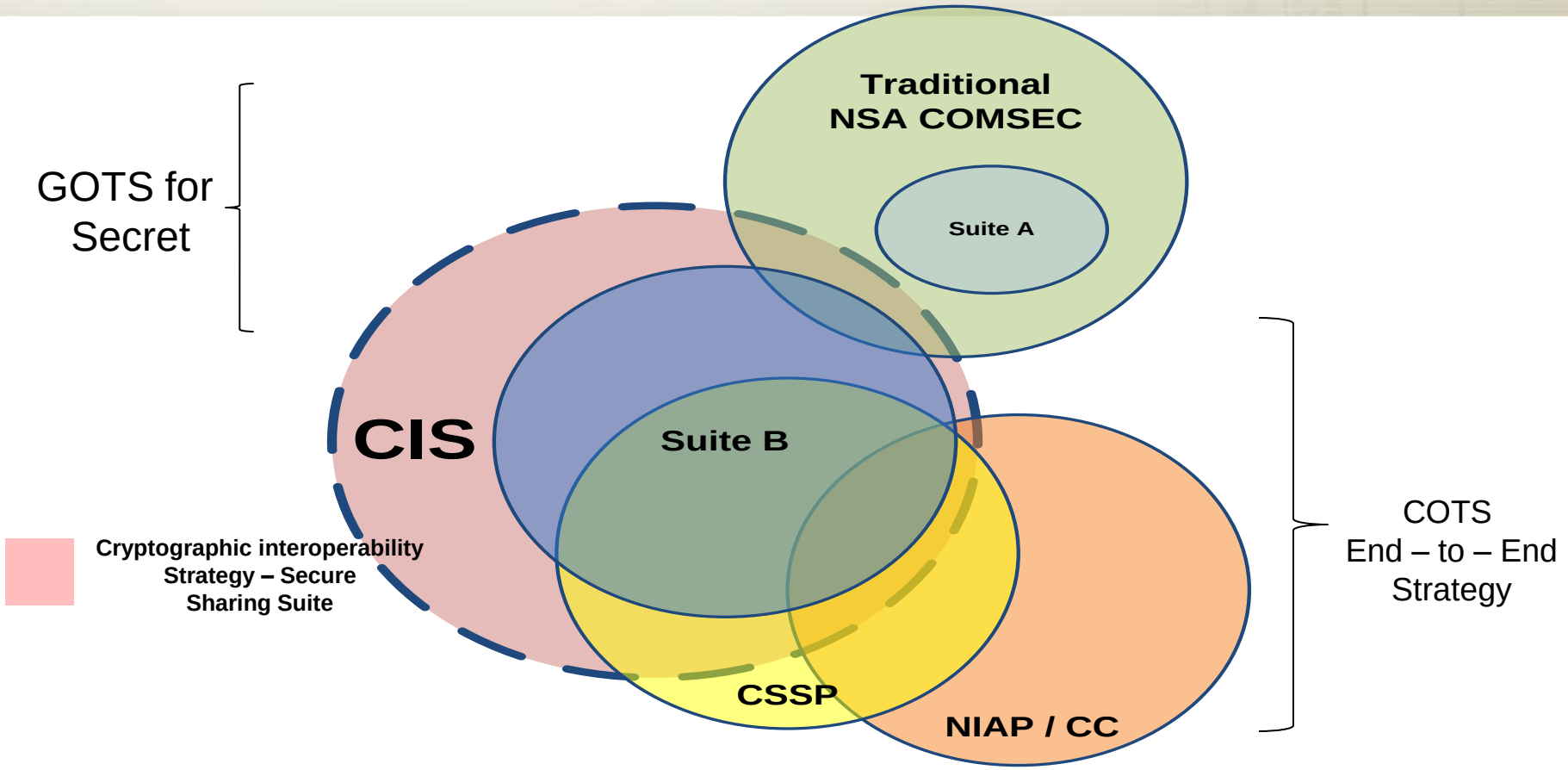
Cryptographic Suites

- Suite A – NSA developed for highly sensitive communication, critical authentication systems
- Suite B - Commercially available and published algorithms for unclassified and classified use

CIS Goal

- **Increase interoperability through supporting the Secure Sharing Suite (S3)**
  - **standards, protocols, modes that support Suite B commercially available algorithms**
- **Releasability**
- **Reduced handling requirements**

(U)Cryptographic Interoperability Strategy



CIS Strategy - Based on…

- Policy
- Standards bodies
- Key Management Infrastructure
- Product Certification
- Vendor Engagement
- International Acceptance
- Technology Demonstrations
- Product, Program Development

Suite B

- Advanced Encryption Standard (AES) with key sizes for 128 and 256 bits – symmetric encryption
- Elliptic-Curve Digital Signature Algorithm (ECDSA) – digital signatures
- Elliptic-Curve Diffie Helman (ECDH) – key agreement
- Secure Hash Algorithm (SHA-256 and SHA-384) -- message digest

Crypto Categories (CNSSI No. 4009)

- **Type 1 - Classified or controlled cryptographic item endorsed by the NSA for securing classified and sensitive U.S. Government information, when appropriately keyed.**
  - **Refers to products only; not information, keys, services, or controls.**
  - **Type 1 products contain approved NSA algorithms.**
  - **Available to U.S. Government users, their contractors, and federally sponsored non-U.S. Government activities subject to export restrictions in accordance with International Traffic in Arms Regulation.**
    - **Certification process consist of Functional Security, Tamper Resistance, Emissions Security (EMSEC/TEMPEST) Testing and formal analysis of cryptographic security Devices.**
- **Type 2 - Unclassified cryptographic equipment, assembly, or component, endorsed by the NSA, for use in national security systems as defined in Title 40 U.S.C. Section 1452.**

Crypto Categories

- **Type 3: NIAP/FIPS evaluated Cryptography**
  - **Encryption algorithm that has been adopted as a Federal Information Processing Standard (FIPS) for use with Sensitive, But Unclassified (SBU) information on non-national security systems.**
- **Type 4: Best Commercial Practices**
  - **Encryption algorithm has been registered with NIST but is not a Federal Information Processing Standard (FIPS).**
  - **"*Type 4 algorithms may not be used to protect classified information*".**

Infrastructure Activities

- **Suite B Base Certificate and CRL Profile**
  - **To be proposed as an IEFT standard**
  - **X.509 Certificates for TLS v1.2, IKE v1 and v2, S/MIME, CMS and SSH**
- **Key Management Infrastructure (KMI)**
- **DOD Public Key Infrastructure (PKI)**
  - **elliptic curve certificates projected 2012**
- **Commercial PKI for SECRET and Below**
  - **DHS to pilot**

Commercial COMSEC Evaluation Program (CCEP)

- **Relationship between NSA and industry in which NSA provides the COMSEC expertise (i.e., standards, algorithms, evaluations, and guidance)**
  - **Industry provides design, development, and production capabilities to produce a type 1 or type 2 product. Products may include modules, subsystems, equipment, systems, and ancillary devices.**

GOTS for SECRET

- **Intellectual Property Rights – Patented Elliptic Curve techologies**

- **NSA licensed the rights to 26 elliptic curve technology patents held by Certicom, Inc. NSA may provide a sub-license to vendors to build products or components using the patented technologies to protect national security information.**

GOTS for SECRET

- GOTS for Secret evaluation process
  - Allows vendors with Type 1 certified products that use Suite B cryptography to protect data up to SECRET
    - Revised set of NSA security and testing requirements
  - Supports development new products to meet the revised standards
  - Minimized certification deliverables
  - Decreased time to market
  - With no classified algorithms, or technologies, reduced handling requirements
    - Not considered a Controlled COMSEC Item (CCI)

COTS for SECRET

- **Commercial Solutions Partnership Program (CSPP)**
  - **Composed solution of multiple COTS products providing confidentiality for classified information.**
    - **Streamlined NIAP**
      - **Requires NIAP and FIPS approved products**
      - **Standard Protection Profiles**
    - **Additional NSA review of COTS products as required**
  - **NSA publishes solution architecture specifications**
    - **Wireless LAN, VPN, disk encryptor, etc**
  - **User develops solution implementation from architecture**
  - **NSA approves solution implementation**

Standards

- Leveraging IETF, NIST standards
  - IPsec using IKEv2 – RFC 4869
  - IPsec Profile for IPv6– NIST Pub 500-267
  - TLS – RFC 5430
  - S/MIME – RFC 5008
  - SSH – AES Galois Counter Mode for Secure Shell Transport Layer Protocol

- Published Guidance documents for vendors implementing ECDH and ECDSA
  - Suite B Implementers' Guide to FIPS 186-3 (ECDSA)
  - includes the Suite B elliptic curve domain parameters, along with example data for the ECDSA signature algorithm and auxiliary functions that are necessary for ECDSA implementations to be in compliance with FIPS 186-3 and Suite B
  - Suite B Implementers' Guide to NIST SP 800-56A

Guidance

- Published Guidance documents for vendors implementing ECDH and ECDSA
  - Suite B Implementers' Guide to FIPS 186-3 (ECDSA)
    - includes domain parameters and example data for the ECDSA signature algorithm and auxiliary functions to be in compliance with FIPS 186-3 and Suite B
  - Suite B Implementers' Guide to NIST SP 800-56A
    - Details on key-agreement schemes from NIST SP 800-56A: Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography
      - Includes elliptic curve and domain parameters, key generation methods, ECDH primitives, key derivation and other functions for compliant implementation

Policy Updates

- **Revised CNSSP-15**
  - Acquisition Policy with mandates in 2015
  - Signed by CNSS March 2010
  - Guidance on use of Suite B and commercial standards
    - SHA 256 and AES 128 for protection of classified information up to SECRET.
    - SHA 384, AES 256 for protection of classified information up to TOP SECRET.
    - Requires NSA approval
- New Handling instructions for Secure Sharing Suite products

Strategy Benefits

- "Quick to Market" Secure Solution sets for broad set of data

- Commercial standards, algorithms reduces handling instructions
- Evolving key management infrastructure(s) to potentially support
  - Federal, DoD, IC, domestic and international partner interoperability

Strategy Benefits

- "Enhanced secure information sharing





Resources

- **NIST SP 800-56A: "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"**
- **NSA IAD CIS Strategy**
  - **www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml**
- **NSTISSP 11 Fact Sheet**
  - ***www.niap-ccevs.org/nstissp_11_revised_factsheet.pdf***
- **CNSSP 15**
- **FIPS PUBs 197 (AES), 180-3 (SHA), 186-3 (ECDSA)**
- ***Suite B Implementer's Guide to FIPS 186-3***
  - ***www.nsa.gov/ia/_files/ecdsa.pdf***

Resources

- **FIPS 140-2**
  - ***csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf***
- **FIPS 140-2 Validated Products List**
  - **http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm**
- **Common Criteria Validated Products List**
  - **http://www.niap-ccevs.org/vpl/**
- **NIST Special Publication 800-59 Guideline for Identifying an Information System as a National Security System**
- **Vendor websites**