

UNCLASSIFIED//FOR OFFICIAL USE ONLY



NSA Key Management Experience

NIST Key Management Workshop 8 June 2009

Petrina Gillman
IA Infrastructure Development
Technical Director
National Security Agency
(301) 688-8133
pgillma@nsa.gov


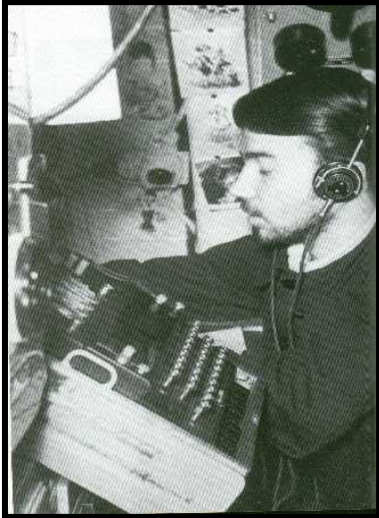
Jonathan Booth
Chief KMI Systems Engineering
National Security Agency
(301) 688 7208
jmboot3@nsa.gov

1






GERMAN ENIGMA







2

 **A RICH LEGACY** 



SIGABA **SIGSALY**

3

 **Key Management Lifecycle** 

- Key Management Lifecycle Model arising from our 50+ Years of Experience
 - Identification of crypto key needs and recipients
 - Generation
 - Distribution & Accounting/Tracking
 - Storage
 - Usage
 - Destruction
- Define in Key Management Planning document at initial product & system definition. Refine, during design, as more details defined.



4



Key Management Design Challenges

- Key Management growing in complexity
 - Cryptography providing more information assurance capabilities in highly networked systems
 - Systems must support cyberspace requirements & legacy interoperability
- Algorithms well specified but few industry standard formats for keys
 - X.509 is the exception

5



Vendor Specific Key Format Explosion

- Default has been for each vendor to define their own key format and packaging
 - Large and expensive support tail
 - Hundreds of key generation programs
 - Not just generation also ordering, distribution, accounting and destruction differences
- NSA defining standard packaging and key formats
 - Working in standards bodies to address gaps in industry standards for keys
 - Defining profiles of industry standards for use in products used in national security systems

6





NSA Crypto Key Standardization Activities




- IETF
 - Define Cryptographic Message Syntax (CMS), IETF RFC 3852, profiles for key and software packages
 - Define a standard Trust Anchor Format and Trust Anchor Management Protocol
 - Create standard asymmetric private key format
 - Create standard symmetric key format
 - Leveraging Certificate Management using CMS (CMC) for x.509 certificate management
- PKIX
 - X.509 Suite B Certificate and CRL Profile

7



Suite B Cryptographic Algorithms



Suite B Announced RSA 2005. Posted at:
http://www.nsa.gov/ia/programs/suiteb_cryptography/index/shtml

Algorithm	Bit Size	Function	Standard
ECDSA	256 / 384	Signature	FIPS 186-2
AES	128 / 256	Symmetric Encryption	FIPS 197
ECDH	256 / 384	Key Exchange	SP 800-56
SHA	256 / 384	Hashing	FIPS 180-2

- Lower key sizes are acceptable for protecting up to SECRET.
- Protecting Top Secret information requires the use of 256 bit AES keys, 384-bit prime modulus elliptic curve and SHA 384 as well as other controls on manufacture, handling and keying.
- NSA's goal with Suite B is to provide industry with a common set of cryptographic algorithms that they can use to create products that meet the needs of the widest range of US Government needs

8





The Need for Interoperability


- Many Interoperability Drivers (e.g. Katrina)
 - Wide range of customers including
 - DoD, FBI, DHS, State and Local Authorities, FEMA, Allies, Charities
 - Drives dual use devices
 - High assurance government devices that can interoperate with commercial devices
 - Commercial assurance devices that can interoperate with High Assurance Government Devices

⇒Key formats as import as algorithm for interoperability
⇒Also need to address protocols, codecs etc

9



Questions



For those viewing via webcast, please submit questions for this presentation to
kmwquestions@nist.gov

10