Key Management Evolution

Elaine Barker (NIST)

Curt Barker (Dakota Consulting)

(Presented at the NIST Crypto Reading Club on Sept. 18, 2024)

Introduction

- Definition:

  The activities involving the handling of cryptographic keys and other related key information during the entire lifecycle of the keys, including their generation, storage, establishment, entry and output, use, and destruction.

- A history of key management from Vietnam to the present

Early Key Management

Environment

- Overwhelmingly government
- Paper systems and special purpose crypto machines
- Both logic and keys classified
- Key management manual and governed by a bureaucracy

Evolution

- People were the weak link
- Computer-execution of algorithms
- Private sector use of cryptography
- Standardization outside national security community

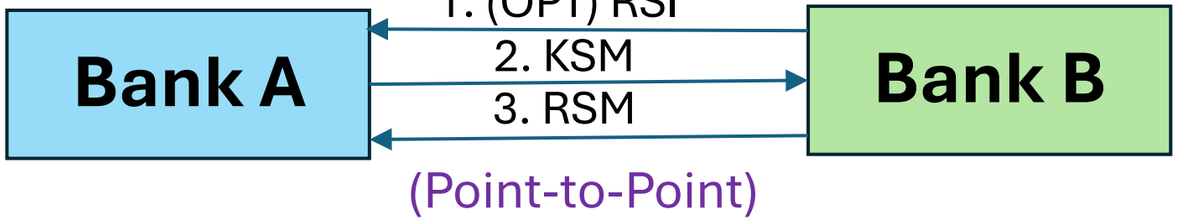
Some Historical Documentation

FIPS 46 (1977) DES
Key Notarization patent (1980)
FIPS 74 (1981) Implementing DES
ANSI X9.17 (1985) Financial Institution
Key Management (Wholesale)

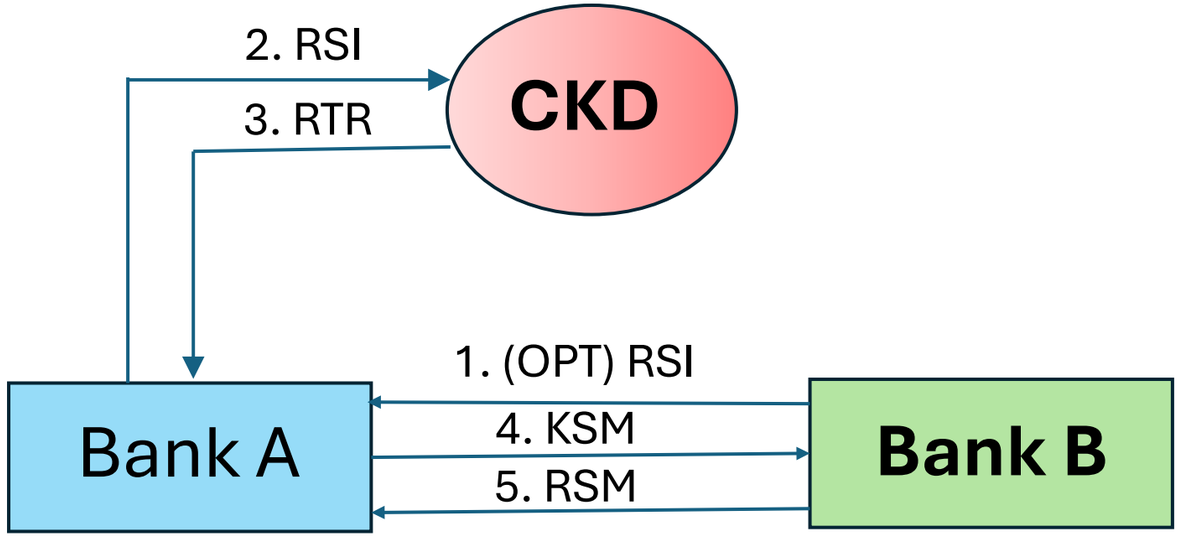
ANS X9.17 (Financial Institution Key Management (Wholesale) (X9E9 - 1985)

- Purpose: Manual and automated management of keying material
- Key management facility protection:
  - Facility requirements
  - Key entry
  - Transportation and storage
  - Equipment operational integrity
  - Destruction
  - Accountability
  - Archiving
- Protocol specification

ASC X9.17 ENVIRONMENTS

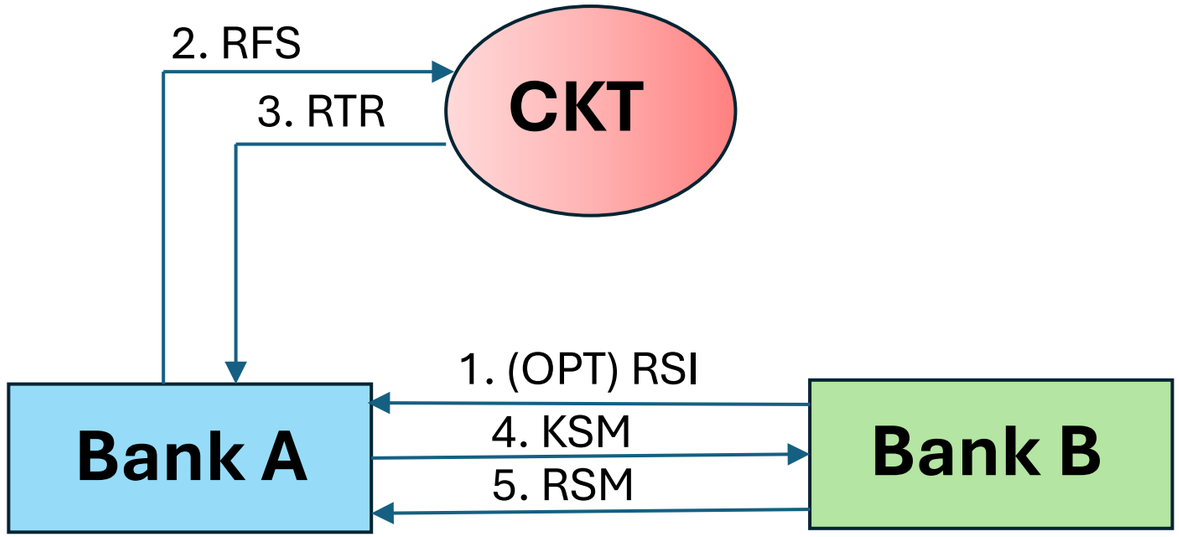


(Point-to-Point)



(Key-Distribution Center)

(Key-Translation Center)



RSI: Request (no key included)
RFS: Request (includes key(s))
RTR: Response to request (includes key(s))
KSM: Key service msg. (includes key(s))
RSM: Response to KSM (no key included)

More Details

- Based on DEA; first use of 2-key TDEA
  - KK: one DEA key
  - *KK: two DEA keys – a key pair
  - KD: a data key (either for encryption or authentication)
- Initial keys MUST be manually distributed
- Message security features:
  - Message counters (CT)
  - Key offset
  - Key notarization
  - Message Authentication (a MAC on most messages)

Key Offset: XOR a (*)KK with a counter

- $KK_O = (KK \oplus CT)$
- $*KK_O = (KK_{left} \oplus CT) \,||\, (KK_{right} \oplus CT)$

KK: 56-bits of key and 8 parity bits
CT: 56 bits of counter and 8 zero bits

Key Notarization: XOR a (*)KK with 16-character IDs

From: Bank A: AAAAAAAAaaaaaaaa
To: Bank B:BBBBBBBBbbbbbbbb

Notarize a KK:

KKR = KK ⊕ AAAAAAAA
NS_1 = eKKR(bbbbbbbb)

KKL = KK ⊕ BBBBBBBB
NS_2 = eKKL(aaaaaaaa)

NS = (leftmost 32 bits of NS_1) || (rightmost 32 bits of NS_2)

Notarization key (KN) = KK ⊕ NS

Key Notarization (continued)

From: Bank A: AAAAAAAAaaaaaaaaa

To: Bank B:BBBBBBBBbbbbbbbbb

Notarize a *KK: $KK_{left} \,||\, KK_{right}$

$KKR = KK_{right} \oplus AAAAAAAA$

$NS_1 = eKKR(bbbbbbbb) \oplus CT$

$KKL = KK_{left} \oplus BBBBBBBB$

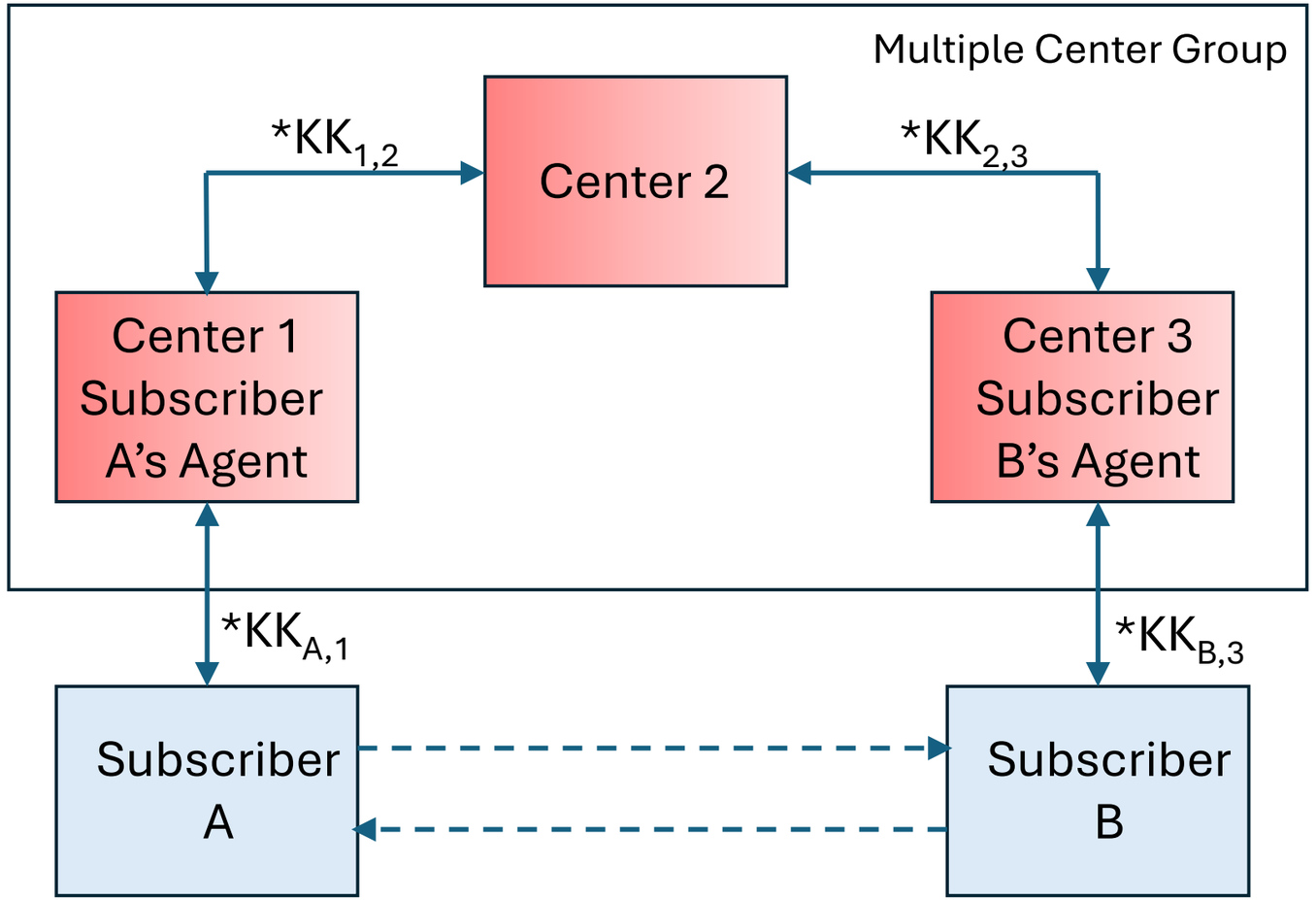
$NS_2 = eKKL(aaaaaaaa) \oplus CT$

Notarization key (*KN) = $(KK_{left} \oplus NS_1) \,||\, (KK_{right} \oplus NS_2)$

FIPS 171: Key Management Using ANSI X9.17 (1992)

- Discusses the use of 27 of the options in X9.17 for the Federal Government, e.g.,
  - Use NIST-approved algorithms
  - All keys **shall** be uniquely named
  - Use key pairs (*KKs), not KKs
  - IVs **shall** be encrypted
  - Etc.

ANSI X9.28 (Financial Institution Multiple Center Key Management (Wholesale) (1990)



Other Early Key Management Activity

- GCHQ Public Key Cryptography Investigation (Early 1970s)
- Diffie-Hellman-Merkle Key Exchange (1976)
- RSA (1978)
- 1970s Work on Electronic Permuters and Over-the Air Rekeying (OTAR)
- Secure Data Network System (NSA - 1986)
  - NBS NISTIR 90-4262 & 4259
- ITU-T X.509 Public Key Certificate Formats (1989)
- NIST SP 800-2 (1991) Public Key Cryptography

SP 800-21: Guideline for Implementing Cryptography in the Federal Government (1999 and 2005; now withdrawn)

- Purpose: To provide guidance to Federal agencies on how to select cryptographic controls for protecting Sensitive Unclassified information.
- Included a small section on key management
  - Compromise
  - Split knowledge and dual control
  - Centrally stored keys and system software
  - Key recovery
  - Archiving.
  - Key lifetimes

SP 800-57

- Background/History
  - Begun in 2001 to provide key mgmt. guidance to everyone
  - Initial development team for Part 1:
    - Curt Barker, Elaine Barker, and Miles Smid (NIST, formerly NSA)
    - Bill Burr and Tim Polk (NIST PKI)
    - Lydia Zieglar (NSA)

- Part 1: General (2005, 2006, 2007, 2012, 2016, 2020)
- Part 2: Best Practices for Key Management Organizations (2005, 2019)
- Part 3: Application-specific Key Management Guidance (2009, 2012, 2015)

SP 800-57, Part 1: General

- Written to expand on SP 800-21.
  - Focuses on issues involving the management of cryptographic keys

- Security Services:
  - Confidentiality
  - Data Integrity
  - Authentication
  - Authorization
  - Non-repudiation

- Cryptographic Algorithms
  - Hash functions
  - Symmetric-key algorithms for encryption and decryption
  - Message Authentication Codes
  - Digital Signature Algorithms
  - Key-establishment schemes
  - Key confirmation
  - Key-establishment protocols
  - Random number generation

SP 800-57, Part 1 (continued)

- General Key Management Guidance
  - Key Types and how they are used
  - Other related information
  - Key usage (e.g., single-purpose preferred)
    - Using the same key for multiple processes could weaken security
    - Limits the damage if a key is compromised

SP 800-57, Part 1 (continued)

- Cryptoperiod (time span during which a key can be used)
  - Limits the amount of data that can be compromised
  - Limits the time for computationally intensive attacks
  - Risk factors to be considered
  - Consequence factors measured by information sensitivity, etc.
  - Other factors to consider
  - Recommended cryptoperiods:

    Table 1 provides recommended/suggested cryptoperiods for each key type

SP 800-57, Part 1 (continued)

- Guidance for Algorithm and Key Size Selection
  - Defines security strength: 80, 112, 128, 192, and 256 bits
  - Table of key strengths for the approved algorithms
  - Table of algorithm and key-size time frames
  - Guidance on using different algorithms and key sizes together
  - Transitioning to new algorithms and key sizes

SP 800-57, Part 1 (continued)

- Key States
  - Pre-activation state
  - Active state
  - De-activated state
  - Destroyed state
  - Compromised state
  - Destroyed compromised state
- Key Management Phases and Functions
  - Pre-operational phase
  - Operational phase
  - Post-operational phase
  - Destroyed phase

SP 800-57, Part 1 (continued)

- Compromise of keys and other keying material
  - What can happen if a key is compromised
  - Protective measures
- Assurances
  - Integrity
  - Domain parameters validity
  - Public key validity
  - Private key possession
- Accountability, Audit, and Survivability

SP 800-57, Part 1 Revisions

- Revisions 1-5
  - Updated references and material that was updated in other referenced documents, defined/redefined/removed terms, clarifications
  - Added SHA-3, EdDSA, and KMAC
  - Non-approval of 2-key TDEA and SHA-1 (for digital signatures)
  - Transitioned to the 112-bit security strength
- Plans for Revision 6
  - Add the PQC keys and publications and PQC security categories
  - Disallow 3-key TDEA and DSA
  - Deprecate SHA-1 and 224-bit SHAs
  - Reference 131A for algorithm transition details rather than including in Part 1

SP 800-57, Part 2: Best Practices for Key Management Organizations

Security management focus

Provides guidance on security policy and planning requirements

- Identifies the concepts, functions and elements common to effective systems for the management of symmetric and asymmetric keys
- Identifies the security planning requirements and documentation necessary for effective institutional key management
- Describes Key Management Specification requirements
- Describes cryptographic Key Management Policy documentation for organizations that use cryptography
- Describes Key Management Practice Statement requirements
- Provides examples of key management infrastructures
- Includes supplemental materials for security plans
- Checklists for product development

SP 800-57, Part 3: Application-Specific Key Management Guidance (2009 and 2015)

- Purpose: To address the key management issues associated with currently available cryptographic mechanisms.
- Originally included sections on PKI, IPsec, TLS and SSL, S/MIME, Kerberos, OTAR, DNSSEC, and EFS
- For each topic:
  - Description
  - Security and compliance issues,
  - Procurement guidance
  - Recommendations for system installers/administrators
  - User guidance
- Revision 1:
  - TLS moved to SP 800-52
  - Added Secure Shell (SSH)

SP 800-131A: Transitioning the Use of Cryptographic Algorithms and Key Lengths (2011, 2015, 2019)

- Security strength discussion
- Status: Acceptable, Deprecated, Disallowed, Legacy Use
- Uses discussed
  - Block Cipher Encryption/Decryption
  - Digital Signature
  - Random Bit Generation
  - Key Agreement, key transport, and key encapsulation
  - Key Wrapping
  - Derived Keys
  - Hash Functions and XOFs
  - Message Authentication Codes (MACs)

SP 800-130: A Framework for Designing Cryptographic Key Management Systems (2013)

- Purpose: To provide topics to be considered and the documentation requirements to be addressed when designing a Cryptographic Key Management System.
- Topics:
  - Security policies
  - Roles and responsibilities
  - Cryptographic keys and metadata
  - Interoperability and transitioning
  - Security controls
  - Testing and system assurances
  - Disaster recovery

SP 800-152: A Profile for U.S. Federal Cryptographic Key Management Systems (CKMS) (2015)

- Purpose: To provide specific requirements, based on the topics in SP 800-130
- "Requirement" categories:
  - Profile requirements (PR) – using "**shall**"
  - Profile augmentations (PA) – using "**should**"
  - Profile features (PF) – using "**could**"
- Examples:

  PR6.21: A Federal CKMS **shall** support and use NIST-approved methods for key generation.

  PF6.3: A Federal CKMS **could** notify the owner of a public-key certificate that the certificate is about to expire.

Other Publications Mentioning Aspects of Key Management

Current publications:

- FIPS 186 (Now FIPS 186-5)
- FIPS 203 (key encapsulation)
- FIPS 204 (ML-DSA)
- FIPS 205 (SLH-DSA)
- SP 800-38F (key wrapping)
- SP 800-52 (TLS guidelines)
- SP 800-56 A, B, & C
- SP 800-131A (transitions)
- SP 800-132 (key derivation)
- SP 800-133 (key generation)
- SP 800-135 (key derivation)
- SP 800-175B
- SP 800-208 (stateful hash signatures)

Historical Publications

- SP 800-32 (PKI – Withdrawn)
- SP 500-54 (key notarization 1979)
- NIST IR 4262 (SDNS key mgt 1990)
- NIST IR 4983 (open system interconnection key mgt. (1992)
- NIST IR 6977 (QKD vulnerabilities)
- NIST IR 7551 (symmetric key injection)
- NIST IR 7956 (key mgt. in cloud services)
- NIST IR 7676 (PIV key history)