



Education

Best Practices for Key Management for Secure Storage

Walt Hubis, LSI Corporation

SNIA Legal Notice

- The material contained in this tutorial is copyrighted by the SNIA.
- Member companies and individuals may use this material in presentations and literature under the following conditions:
 - ◆ Any slide or slides used must be reproduced without modification
 - ◆ The SNIA must be acknowledged as source of any material used in the body of any document containing material from these presentations.
- This presentation is a project of the SNIA Education Committee.

Best Practices for Key Management for Secure Storage

As secure storage becomes more pervasive throughout the enterprise, the focus quickly moves from implementing encrypting storage devices to establishing effective key management policies. Without the proper generation, distribution, storage, and recovery of key material, valuable data will be eventually compromised. Worse, without proper management of key information, data can be completely lost.

This session explores the current best practices for key management as described by the SNIA Security Technical Work Group (TWG). Threats to key management, protection against those threats, key management principles, key management functions, and key management issues are discussed.

Key Management Threats



➤ Confidentiality

- ◆ Key Disclosed to Unauthorized Entities
- ◆ Incomplete Destruction of Keys
- ◆ Data Accessible by Anyone
- ◆ Authentication Failure - Masquerades
- ◆ Eavesdropping
- ◆ Improper Policies and Procedures

➤ Integrity

- ◆ Modification of Keys
- ◆ Know When Key has Been Modified
- ◆ Data Accessible by None
- ◆ Denial of Service Attack

➤ Availability

- ◆ Unauthorized Deletion of Keys
- ◆ Unauthorized Modification of Keys
- ◆ Archive Failure

➤ Misuse

- ◆ Wrong Key for the Wrong Purpose
- ◆ Using Keys Outside of Key Lifetime (Cryptoperiod)
- ◆ Excessive Key Use
- ◆ Giving Keys to Unauthorized Users
- ◆ Choosing Weak Keys

Protection

➤ Protection Requirements

- ◆ Integrity Protection
- ◆ Confidentiality
- ◆ Association Protection
- ◆ Assurance of domain parameter and public key validity
- ◆ Assurance of private key possession
- ◆ Period of Protection

Protection Techniques

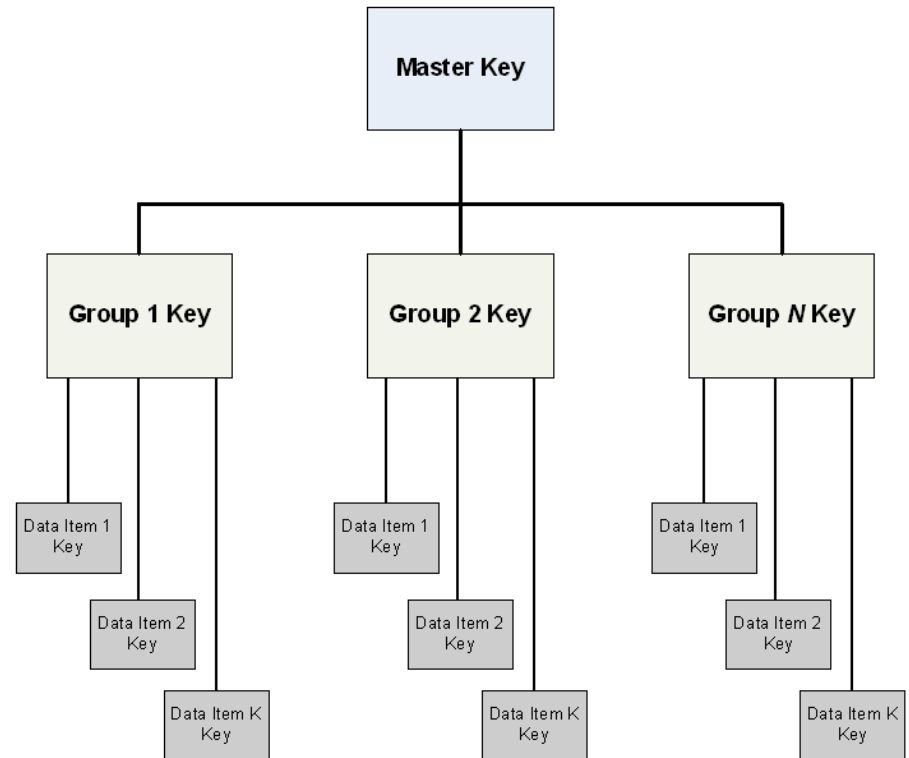
➤ Physical

- ◆ Secure Key Storage Devices
 - > Key Management Servers
- ◆ Interact with Other Cryptographic Devices
 - > Smart Cards
 - > Memory Cards
- ◆ Storage of Keys Offline
 - > Tape
 - > Optical

Protection Techniques

➤ Organizational

- ◆ Only Single Data Items Compromised
- ◆ Threat of Master Key Disclosure
- ◆ Split Keys Can Be Used



Protection Techniques

- Non-Cryptographic Protection
 - ◆ Time Stamps
 - › Restrict Key Use to Specific Periods
 - ◆ Sequence Numbers
 - › Limit Re-Play Attacks
- Cryptographic Protection
 - ◆ Disclosure protection
 - › Key Encryption
 - › Data Integrity Checks
 - › Authentication
 - ◆ Use Protection
 - › Binding Key Information to Key

Key Management Best Practices



Important Key Properties

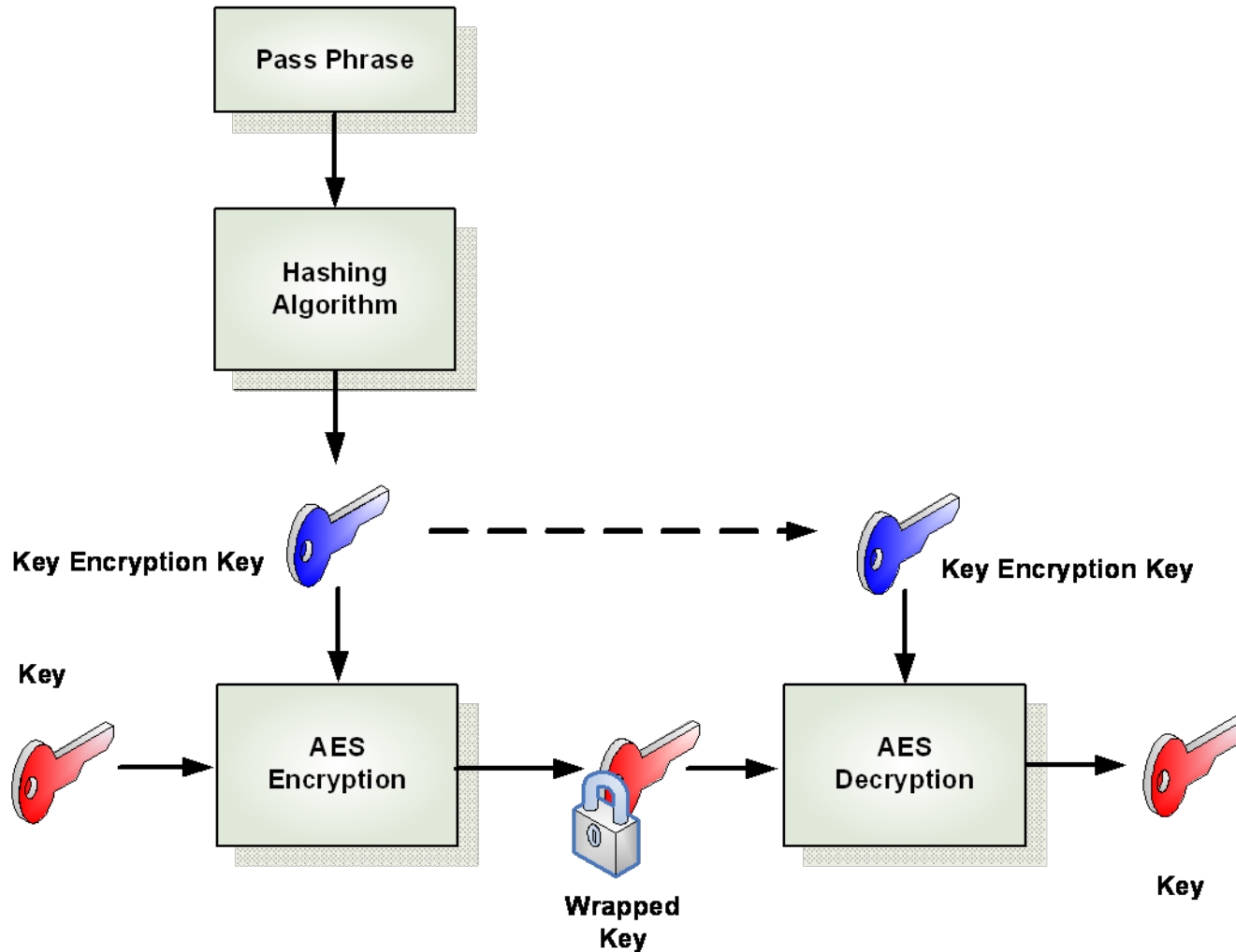
- **Use a Cryptographic Key for Only One Purpose**
 - ◆ Do Not use Key-Encrypting Keys or Wrapping Keys to Encrypt Data
 - ◆ Do Not use Data-Encrypting Keys to encrypt other keys

- **Use Randomly Chosen Keys from the Entire Key Space**
 - ◆ Use Computer-Generated Keys Whenever Possible
 - ◆ Enforce a Broad Range of Entries in the Key Space

- **Avoid Weak Keys**
 - ◆ “00000000” or “FFFFFFF” or even “DEADBEEF”
 - ◆ Dictionary Attacks (e.g., “password”)

- **Avoid Plain Text Keys**
 - ◆ Always Encrypt Keys for Transfer
 - ◆ Prevent Observation of Plaintext Keys

Key Wrapping



Pass Phrase Strength

Password Type	Length	Example	Estimate Time
Dictionary A-Z	8	Exchange	<1 Sec
	9	Exchange A	<1 Sec
	10	Exchange Ab	<1 hr 15 min
	11	Exchange Use	<1 hr 20 min
	12	Exchange User	<1 hr 20 min
	13	Exchange UserA	<3 hrs 2 min
	14	Exchange UserAb	<3 hrs 10 min
Alpha Numeric A—Z; 0-9	8	4Exchange	<23 hrs 50 min
	9	4Exchange	<25 hrs 10 min
	10	4Exchangel	<27 hrs 30 min
	11		
	12	4Exchangel 2A	<34 hrs 50 min
	13		
	14	4Exchange2User	<39 hrs 20 min

Source: NLRB Password Cracking Information, August 20, 2001

Pass Phrase Strength

Password Type	Length	Example	Estimate Time
Alpha Numeric Plus Special Characters A—Z 0—9 !@#%&*()-_+=	8	Exch@USA	<130 hrs 10 min
	9		
	10	Exch@USA4!	<203 hrs 30 min
	11		
	12		
	13		
	14	4Exch&4U&l@pec	<223 hrs 50 min
Alpha Numeric Plus Advanced Special Characters A-Z, 0-9 !@#%&*()-_+= { } ~ ' " ? < > : ; \ , / []	8 **	Exch@t4l	<2365 hrs 10 min
	9		
	10	4Exch@(4U]	<2170 hrs 8 min*
	11		
	12		
	13 14	4Excb@~pec4U!]	<2335hrs4l min*

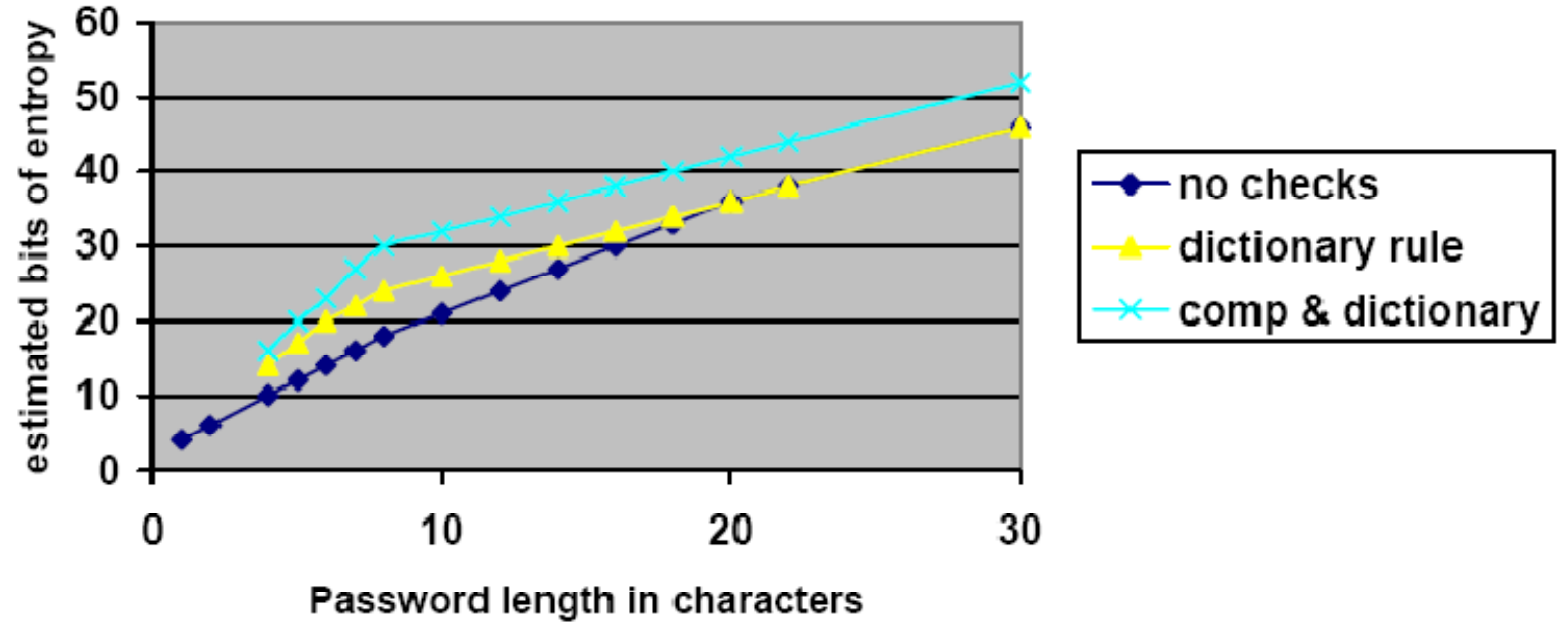
Source: NLRB Password Cracking Information, August 20, 2001

Pass Phrase Strength

Length Char.	User Chosen			Randomly Chosen		
	94 Character Alphabet			10 char. alphabet		94 char alphabet
	No Checks	Dictionary Rule	Dict. & Comp. Rule			
1	4	-	-	3	3.3	6.6
2	6	-	-	5	6.7	13.2
3	8	-	-	7	10.0	19.8
4	10	14	16	9	13.3	26.3
5	12	17	20	10	16.7	32.9
6	14	20	23	11	20.0	39.5
7	16	22	27	12	23.3	46.1
8	18	24	30	13	26.6	52.7
10	21	26	32	15	33.3	65.9
12	24	28	34	17	40.0	79.0
14	27	30	36	19	46.6	92.2
16	30	32	38	21	53.3	105.4
18	33	34	40	23	59.9	118.5
20	36	36	42	25	66.6	131.7
22	38	38	44	27	73.3	144.7
24	40	40	46	29	79.9	158.0
30	46	46	52	35	99.9	197.2
40	56	56	62	45	133.2	263.4

Source: NIST Special Publication 800-63 Version 1.0.2 Electronic Authentication Guideline

Pass Phrase Strength

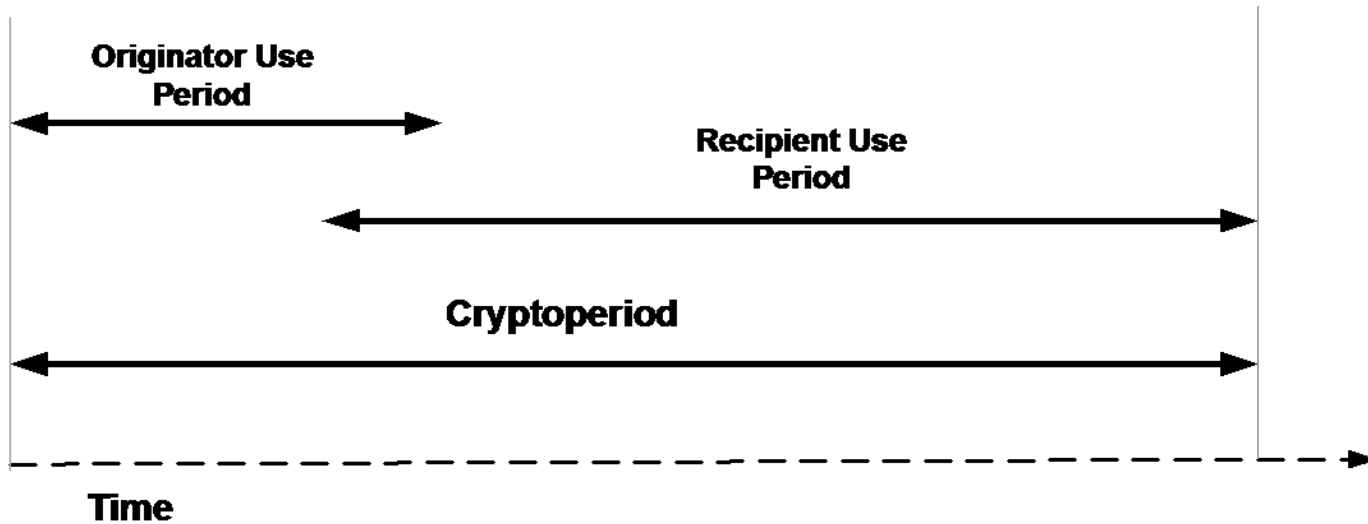


Source: NIST Special Publication 800-63 Version 1.0.2 Electronic Authentication Guideline

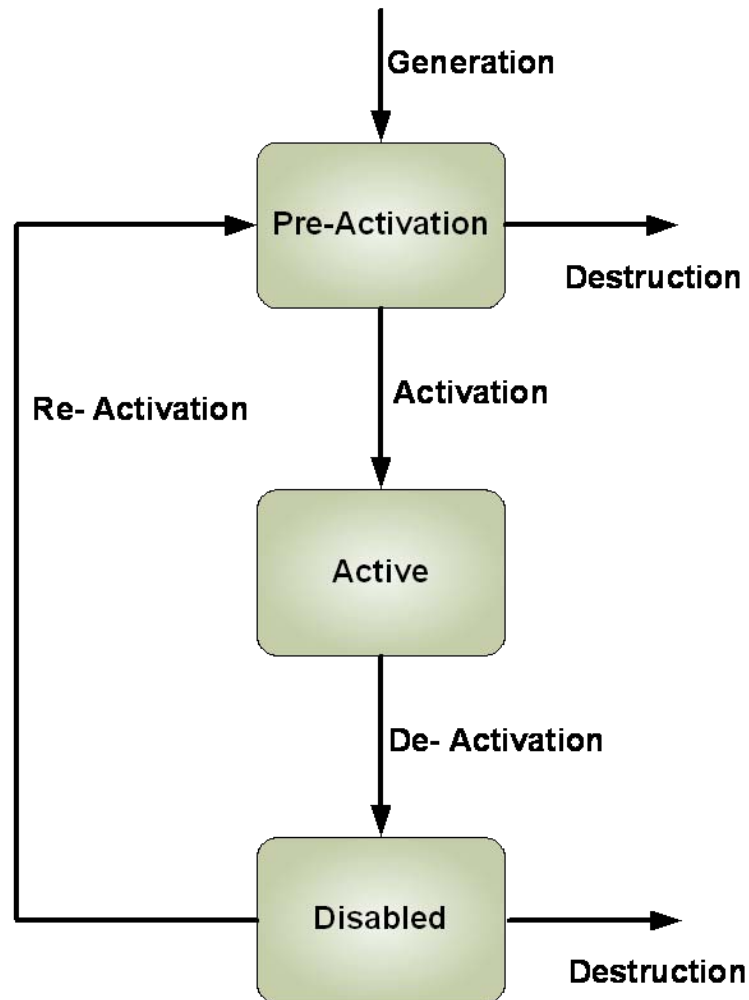
Key Management Safety

- **Automate Key Management Whenever Possible**
 - ◆ Authentication
 - ◆ Key Generation
- **Observe and Enforce Cryptoperiod**
 - ◆ Also, Limit Keys to Maximum Amount of Data
- **Limit Keys with Long Lifetime**
 - ◆ Archived Keys Only
- **Separate Key Functions**
 - ◆ Don't Mix Key Encryption and Data Encryption Keys

➤ Cryptoperiod

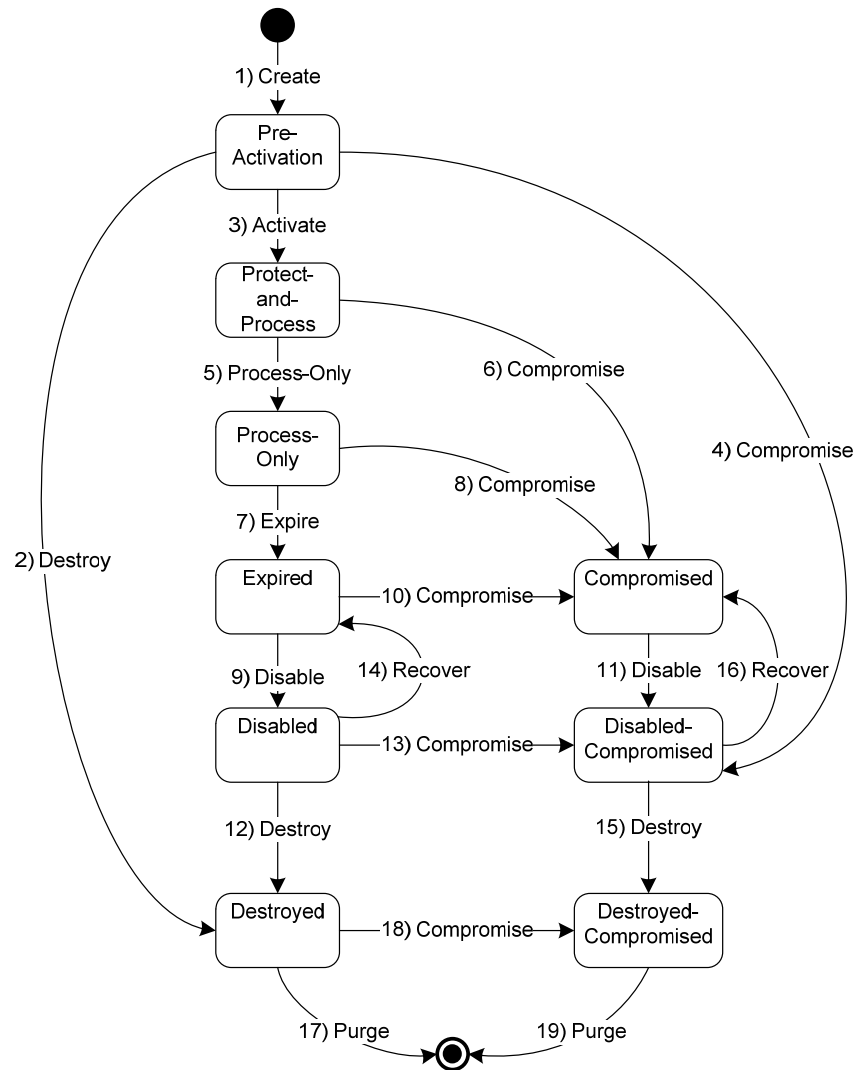


➤ Generic



Key Lifecycle

➤ Actual



Source: IEEE P1619.3

Key Management Safety

➤ Document Objectives

- ◆ Authorization Objectives
- ◆ Protection Objectives
- ◆ Key Management Services Objectives
- ◆ Key Material Destruction

➤ Enforce Strict Access Controls

- ◆ Limit User Capabilities
- ◆ Segregate Duties
 - > Audit
 - > User
 - > Management

Establish Keys Securely

➤ Symmetric Keys

- ◆ Use an Approved Random Number Generator
- ◆ Use an Approved Key Update Procedure
- ◆ Use an Approved Key Derivation Function from a Master Key
- ◆ Don't Concatenate Split Keys to Generate Keys

➤ Limit Distribution of Data Encryption Keys

- ◆ No Gratuitous Distribution
- ◆ Limit to Backups
- ◆ Limit to Authorized Entities

➤ Protect Keys

- ◆ Wrap Keys Before Distribution
- ◆ Use Appropriate Physical Security

Operational Use

➤ **Secure Devices and Processes**

- ◆ Insure that Installation does not Result in Key Leakage
- ◆ Insure that Device or Process Meets Key Best Practices

➤ **Secure Key Storage**

- ◆ Cryptographic Security (e.g., Wrapping)
- ◆ Physical Security

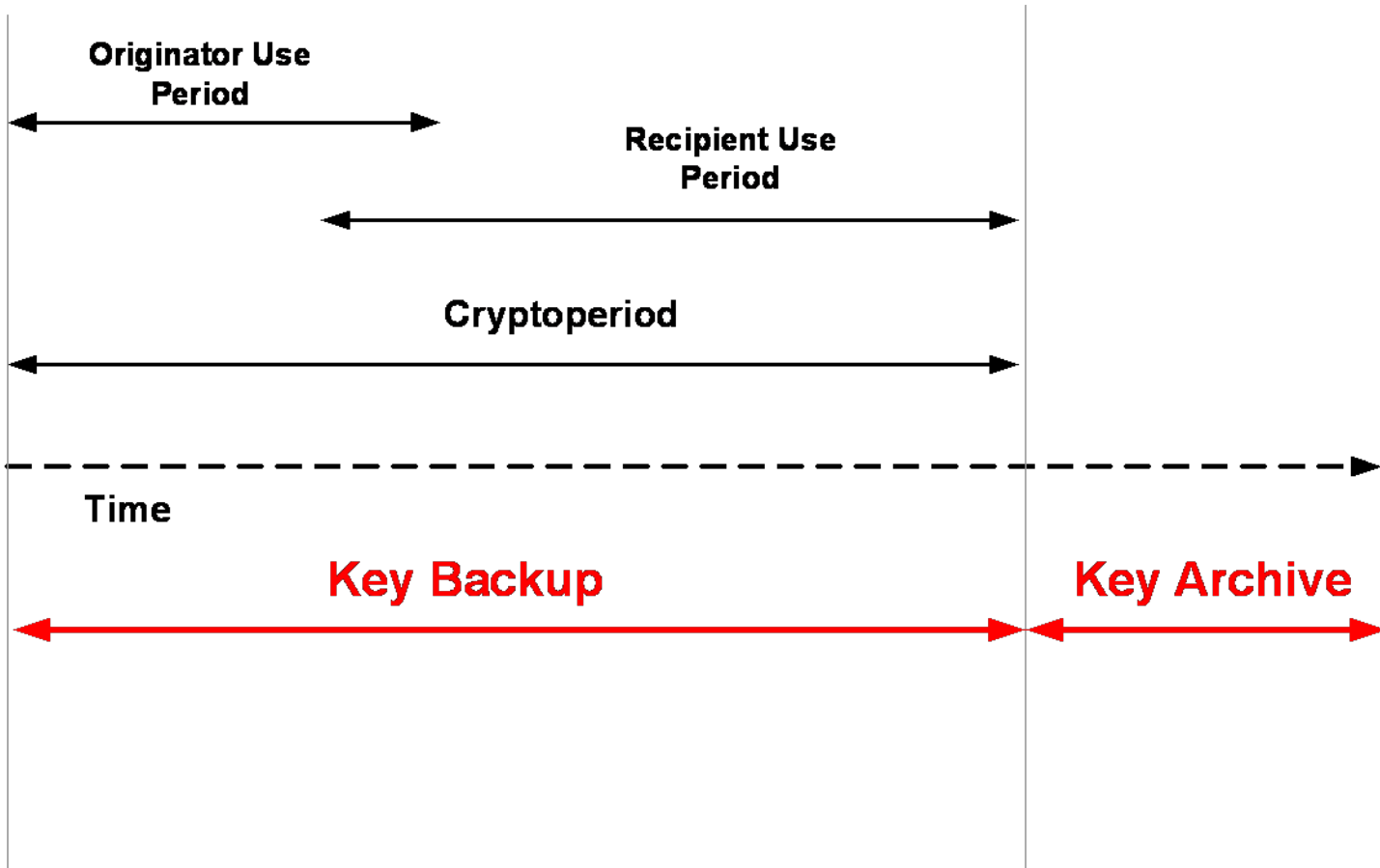
➤ **Integrity**

- ◆ Employ Methods to Detect Modifications
- ◆ Ability to Restore Key Material when Unauthorized Modifications Occur

➤ **Backup and Archive**

- ◆ Backup Keys During the Key's Cryptoperiod
- ◆ Archive Keys after the Cryptoperiod has Expired – *As Needed.*

Key Backup and Archive



Operational Use

➤ Change Keys

- ◆ When a Compromise is Detected
- ◆ When the Key's Cryptoperiod Nears Expiration
- ◆ When the Key's Data Limit Approaches

➤ Destroy Keys

- ◆ Remove Keys from Backups when Not Needed for Operational Use
- ◆ Destroy Keys When No Longer needed for Backup or Archive

Other Issues

➤ Import and Export Controls

- ◆ Understand and Obey Government Import and Export Regulations

➤ Plan for Problems

- ◆ Have a Recovery Plan in Place for a Key Compromise Event

➤ Plan for Disaster

- ◆ Have a Recovery Plan in Place for Catastrophic Events
- ◆ Consider an Escrow Plan to Protect Mission Critical Information
- ◆ *Archives May Need to Last for a Very Long Time*

Archive Security

➤ Active Archive

- ◆ Contains *Some* Data Subject to Retention Policies
- ◆ Retention Policies Driven by Governmental Compliance Requirements

➤ Long Term Archive

- ◆ Data Life Exceeds the Life Span of Formats and Storage Mechanisms
- ◆ Preserve Data Long Periods of Time
- ◆ Wills, Land Records, Medical Data, Criminal Case Files, etc.

Active Archive Security

➤ Active Archive Security

- ◆ Ensure Read-Only Enforcement is Adequate
- ◆ Ensure Data Privacy
 - > Access Controls
 - > Encryption
- ◆ Provide Appropriate Index and Search Capabilities
- ◆ Prepare for a Disaster
- ◆ Enforce Role and Access Policies

➤ Governance and Compliance

- ◆ Data Retention Requirements
- ◆ Data Disposition Requirements
- ◆ Preserve Evidentiary Nature of the Data
 - > Rigorous Authenticity Checks
 - > Chain of Custody (Audits)

Long-Term Archive

➤ Policies

- ◆ Establish Type of Data to be Accepted
- ◆ Determine Preservation Period
- ◆ Define Archived Data Object Maintenance Policy
- ◆ Establish Authorization Policy
- ◆ Specify the Preservation Activities
- ◆ Define a Cryptographic Maintenance Policy

➤ Security

- ◆ Access Control Mechanisms Must be Appropriate to the Lifespan
- ◆ Perform Periodic Data Conversions and Revalidations
- ◆ Address Long-Term Non-Repudiation of Digitally Signed Data

For More Information

- NIST Special Publication 800-57: Recommendation for Key Management (http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf)
- ISO/IEC 11770 Parts 1-3: Information technology - Security techniques - Key management
- FIPS 140-2: SECURITY REQUIREMENTS MODULES (<http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>)
- Trusted Computing Group (<https://www.trustedcomputinggroup.org/home>)
- IEEE P1619.3: Security in Storage Workgroup (SISWG) Key Management Subcommittee (<http://siswg.net/>)
- OASIS Enterprise Key Management Infrastructure (EKMI) Technical Committee (http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ekmi)
- IETF: Provisioning of Symmetric Keys (KEYPROV) (<http://www.ietf.org/html.charters/keyprov-charter.html>)

- Please send any questions or comments on this presentation to SNIA:
tracksecurity@snia.org

**Many thanks to the following individuals
for their contributions to this tutorial.**

SNIA Education Committee

**Larry Hofer CISSP
Eric Hibbard CISSP
Mark Nossokoff**

**Blair Semple
SNIA SSIF
SNIA Security TWG**