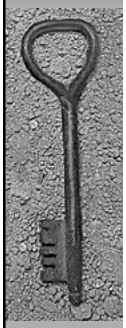
Key Management Guidelines



Key Management Guidelines

1. Introduction
2. Glossary of Terms and Acronyms
3. Cryptographic Algorithms, Keys and Other Keying Material
4. Key Management Life Cycle
5. General Key Management Guidance
6. Key Management Guidance - Selected Infrastructures
7. Key Management Guidance - Selected Applications

Appendix A: Cryptoperiods for Signing Key Pairs

Appendix X: References

Introduction

1.1 Goal/Purpose

1.2 Audience

1.3 Scope

1.4 Security Services

1.5 Content/Organization

Goal/Purpose

- Provide Key Management Background Information
- Establish Frameworks to Support Selection and Use of Cryptographic Mechanisms

Audience

- Cryptographic Module Developers
- Protocol Developers
- System or Application Owners

Scope

- Cryptographic Algorithms, Infrastructures, Protocols and Applications
- Management of Cryptographic Keys
  - Generation
  - Use
  - Destruction

Security Services

- Confidentiality
- Data Integrity
- Authentication
- Non-repudiation

Content Organization

- Glossary of Terms and Acronyms
- Cryptographic Algorithms, Keys and Other Keying Material
- Key Management Life Cycle
- General Key Management Guidance
- Guidance for Selected Infrastructures
- Guidance -for Selected Applications
- Appendices As Required

Glossary

2.1 Glossary of Terms

2.2 Acronyms

Cryptographic Algorithms, Keys and Other keying Material

3.1 Classes of Cryptographic Algorithms

3.2 Cryptographic AlgoriFunctionality

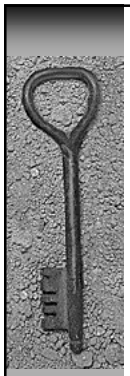
3.3 Cryptographic Keys and Other Keying Material

Classes of Cryptographic Algorithms

- Hash Algorithms
- Symmetric Key Algorithms
- Asymmetric Key Algorithms

Cryptographic Algorithm Functionality

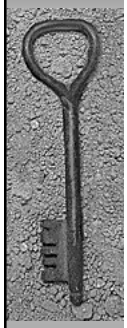
3.2.1 Hash Function
3.2.2 Encryption/Decryption Algorithms
3.2.3 Message Authentication Codes
3.2.4 Digital Signature Algorithms
3.2.5 Key Establishment Algorithms
3.2.6 Random Number Generation



Cryptographic Keys and other Keying Material

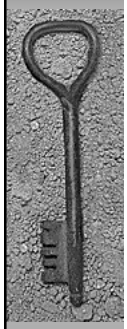
3.3.1 Classes of Keys and Protection Requirements

3.3.2 Other Keying Material and Its Protection



Key Types

Signing Keys
Signature Verification Keys
Secret Authentication Keys
Private Authentication Keys
Public Authentication Keys
Long Term Data Encryption Keys
Short Term Data Encryption Keys
Random Number Generation Keys
Key Encrypting Keys Used for Key Wrapping
Master Keys used for Key Derivation
Keys Derived From a Master Key
Key Transport Private Keys
Key Transport Public Keys
Static Key Agreement Private Keys
Static Key Agreement Public Keys
Ephemeral Key Agreement Private Keys
Ephemeral Key Agreement Public Keys
Secret Authorization Keys
Private Authorization Keys
Public Authorization Keys



Cryptographic Keys and Other Keying material

3.3.1 Classes of Keys and Protect Requirements

3.3.2 Other Keying Material and Its Protection

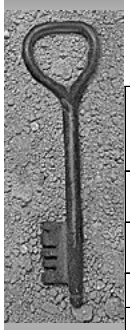


Table 1: ProtectionRequirements for Key Classes

	Confiden-tiality	Integrity	Long Term Availability	Associated with usage or application	Association with owner/other entity	Associated with other info.	Validation
Signing keys	X	X		X		Domain parameters; signature verification key	
Signature verification keys		X	X	X	X	Domain parameters; signing key	For association with private key
Secret authentication keys	X	X	X	X	X	Authenticated data	
Private authentication key	X	X		X		Public authentication key	
Public authentication key		X	X	X	X	Authenticated data; private authentication key	For association with private key
Long term data encryption keys	X	X	X	X	X	Encrypted data	
Short term data encryption keys	X	X					
RNG keys	X	X		X			
Key encrypting key used for key wrapping	X	X	X	X	X	Encrypted keys	
Master key used for key derivation	X	X	X	X	X	Derived keys	
Keys derived from a Master Key	X?	X	X?	X?	X?	Master key and protected data	

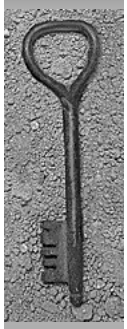


Table 1: ProtectionRequirements for Key Classes

	Confiden-tiality	Integrity	Long Term Availability	Associated with usage or application	Association with owner/other entity	Associated with other info.	Validation
Key transport private keys	X	X		X?		Encrypted keys; key transport public key	
Key transport public keys		X	X		X	Key transport private key	X
Static key agreement private keys	X	X	X	X?		Domain parameters; static key agreement public key	
Static key agreement public keys		X	X	X?	X	Domain parameters; static key agreement private key	X
Ephemeral key agreement private keys	X	X					
Ephemeral key agreement public keys		X					X
Secret authorization key	X	X		X	X		
Private authorization key	X	X		X		Public authorization key	
Public authorization key		X		X	X	Private authorization key	

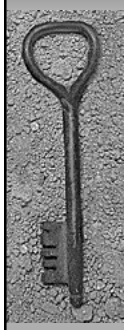
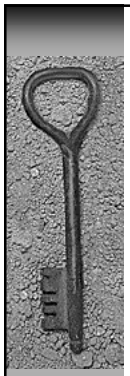


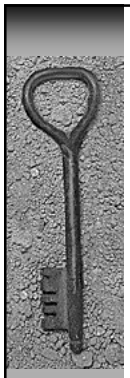
Table 1: ProtectionRequirements for Key Classes

	Confiden-tiality	Integrity	Long Term Availability	Associated with usage or application	Association with owner/other entity	Associated with other info.	Validation
Domain parameters		X	X?	X		Private and public keys	X
Initialization vectors	?	X	X			Protected data	
Shared secrets	X	X	?	X	X	?	
Seeds	X?			X?		Generated data?	
Intermediate results	X			X		Process data	



Key Management Lifecycle

4.1 User Registration
4.2 System and User Initialization
4.3 Keying Material Installation
4.4 Key Establishment
4.5 Key Registration
4.6 Operational Use
4.7 Storage of Keying Material
4.8 Key Update
4.9 Key Recovery
4.10 Key De-registration and Destruction
4.11 Key Revocation



Key Establishment

4.4.1 Generation and Distribution of Public/Private Key Pairs
- **Static Public Keys**
- **Ephimeral Public Keys**
- **Centrally Generated Private Keys**

4.4.2 Generation and Distribution of Symmetric Keys
- **Key Generation**
- **Key Distribution**
- **Key Agreement**

4.4.3 Generation and Distribution of Other Keying Material
- **Domain Parameters**
- **Initialization Vectors**
- **Shared Secrets**
- **Seeds**
- **Intermediate Results**

Key Management Lifecycle

4.1 User Registration
4.2 System and User Initialization
4.3 Keying Material Installation
4.4 Key Establishment
4.5 Key Registration
4.6 Operational Use
4.7 Storage of Keying Material
4.8 Key Update
4.9 Key Recovery
4.10 Key De-registration and Destruction
4.11 Key Revocation

Storage of Keying Material

4.7.1 General Protection Methods
- **Confidentiality**
- **Integrity**
- **Association With Usage or Application**
- **Association With the Other Entity**
- **Long Term Availability**
- **Association With Other Information**

4.7.2 Operational Storage
4.7.3 Backup Storage
4.7.4 Key Archive Storage

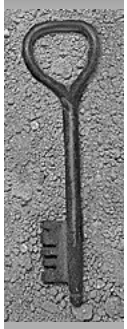


Table 2: Backup of Keying Material by Material Type

Type of Key	Backup?
Signing keys	No; non-repudiation would be in question.[However, it may be warranted in some cases - a CA's signing key, for example]
Signature verification keys	OK; its presence in a public-key certificate that is available elsewhere may be sufficient.
Secret authentication keys	OK
Private authentication key	OK, if required by an application.
Public authentication key	OK; its presence in a public-key certificate that is available elsewhere may be sufficient.
Long term data encryption keys	OK
Short term data encryption keys	May not be necessary
RNG keys	Not necessary and may not be desirable, depending on the application.
Key encrypting key used for key wrapping	OK
Master key used for key derivation	OK, unless a new master key can easily be generated and distributed.
Keys derived from a Master Key	Depends on the use of the derived key, but backup may not be needed if the master key is backed up.

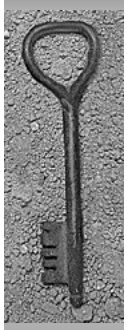


Table 2: Backup of Keying Material by Material Type

Type of Key	Backup?
Key transport private keys	OK
Key transport public keys	OK; presence in a public-key certificate available elsewhere may be sufficient.
Static key agreement private keys	No, unless needed for reconstruction during key recovery?
Static key agreement public keys	OK; its presence in a public-key certificate that is available elsewhere may be sufficient.
Ephemeral key agreement private keys	No
Ephemeral key agreement public keys	No, unless needed for reconstruction during key recovery?
Secret authorization key	OK
Private authorization key	OK
Public authorization key	OK; its presence in a public-key certificate that is available elsewhere may be sufficient.
Domain parameters	OK
Initialization vectors	OK, if necessary
Shared secrets	No, unless needed for reconstruction during key recovery?
Seeds	No, unless required for the validation of domain parameters
Intermediate results	No

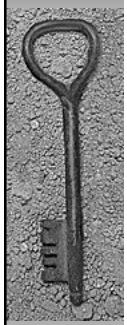
Storage of Keying Material

4.7.1 General Protection Methods
- **Confidentiality**
- **Integrity**
- **Association With Usage or Application**
- **Association With the Other Entity**
- **Long Term Availability**
- **Association With Other Information**

4.7.2 Operational Storage

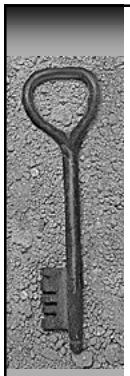
4.7.3 Backup Storage

4.7.4 Key Archive Storage



Key Management Lifecycle

4.1 User Registration
4.2 System and User Initialization
4.3 Keying Material Installation
4.4 Key Establishment
4.5 Key Registration
4.6 Operational Use
4.7 Storage of Keying Material
4.8 Key Update
4.9 Key Recovery
4.10 Key De-registration and Destruction
4.11 Key Revocation

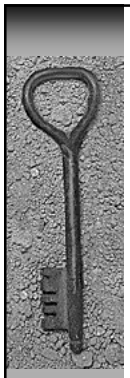


General Key Management Guidance

5.1 Key Management Policy

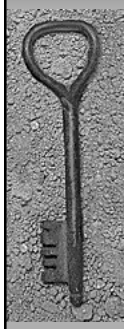
5.2 Guidance for Cryptographic Algorithm and Key Size Selection

5.3 Key Establishment Schemes



Key Management Policy

5.1.1 Key Management Practices Statement
5.1.2 Key Usage
5.1.3 Cryptoperiods
5.1.4 Domain Parameter Validation and Public Key Validation
5.1.5 Compromise of Keys and Other Keying Material
5.1.6 Accountability
5.1.7 Audit
5.1.8 Key Recovery
Considerations
Policy



Guidance for Cryptographic Algorithm and Key Size Selection

5.2.1 Equivalent Algorithm Strength

5.2.2 Defining Appropriate Algorithm Strengths

5.2.3 Transitioning to New Algorithms and Key Sizes

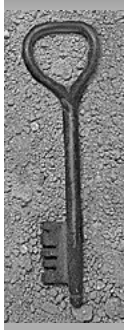
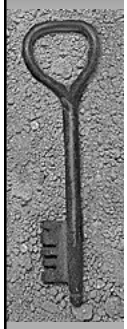


Table 3: Equivalent Algorithm Strengths

Bits of security	Symmetric key algs.	Hash algs.	DSA, D-H, MQV	RSA	Elliptic Curves
80		SHA-1	$L = 1024$ $N = 160$	$k = 1024$	$f = 160$
112	TDES		$L = 2048$ $N = 224$	$k = 2048$	$f = 224$
128	AES-128	SHA-256	$L = 3072$ $N = 256$	$k = 3072$	$f = 256$
192	AES-192	SHA-384	$L = 7680$ $N = 384$	$k = 7680$	$f = 384$
256	AES-256	SHA-512	$L = 15360$ $N = 512$	$k = 15360$	$f = 512$



Guidance for Cryptographic Algorithm and Key Size Selection

5.2.1 Equivalent Algorithm Strength

5.2.2 Defining Appropriate Algorithm Strengths

5.2.3 Transitioning to New Algorithms and Key Sizes

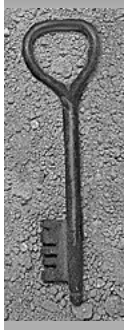


Table 4: Recommended Algorithms and Minimum Key Sizes

Years	Symmetric key algs. (Encryption & MAC)	Hash Alg.	HMAC	DSA, D-H, MQV	RSA	Elliptic Curves
Present - 2015	TDES AES-128 AES-192 AES-256	SHA-1 SHA-256 SHA-384 SHA-512	SHA-1 (≥80 bit key) SHA-256 (≥128 bit key) SHA-384 (≥192 bit key) SHA-512 (≥256 bit key)	Min.: L = 1024; N =160	Min.: k=1024	Min.: f=160
2016 and beyond	TDES AES-128 AES-192 AES-256	SHA-256 SHA-384 SHA-512	SHA-256 (≥128 bit key) SHA-384 (≥192 bit key) SHA-512 (≥256 bit key)	Min.: L = 2048 N = 224	Min.: k=2048	Min.: f=224

Guidance for Cryptographic Algorithm and Key Size Selection

5.2.1 Equivalent Algorithm Strength

5.2.2 Defining Appropriate Algorithm Strengths

5.2.3 Transitioning to New Algorithms and Key Sizes

General Key Management Guidance

5.1 Key Management Policy

5.2 Guidance for Cryptographic Algorithm and Key Size Selection

5.3 Key Establishment Schemes

Key Management Guidance Selected Infrastructures

6.1 Public Key Infrastructure

6.2 Kerberos

Key Management Guidance Selected Protocols

7.1 S/MIME

7.2 TLS/SSL

- **7.2.1 Version**
- **7.2.2 Cipher Suite Selection**
- **7.2.3 Public Key Certificates for TLS**

Key Management Guidance Selected Applications

8.1 Encrypted File Storage

8.2 ???

Appendix A

Cryptoperiods for Signing Key Pairs

Appendix X

References