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 Algorithm Functionality

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

<table>
<thead>
<tr>
<th>Signing Keys</th>
<th>Keys Derived From a Master Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature Verification Keys</td>
<td>Key Transport Private Keys</td>
</tr>
<tr>
<td>Secret Authentication Keys</td>
<td>Key Transport Public Keys</td>
</tr>
<tr>
<td>Private Authentication Keys</td>
<td>Static Key Agreement Private Keys</td>
</tr>
<tr>
<td>Public Authentication Keys</td>
<td>Static Key Agreement Public Keys</td>
</tr>
<tr>
<td>Long Term Data Encryption Keys</td>
<td>Ephemeral Key Agreement Private Keys</td>
</tr>
<tr>
<td>Short Term Data Encryption Keys</td>
<td>Ephemeral Key Agreement Public Keys</td>
</tr>
<tr>
<td>Random Number Generation Keys</td>
<td>Secret Authorization Keys</td>
</tr>
<tr>
<td>Key Encrypting Keys Used for Key Wrapping</td>
<td>Private Authorization Keys</td>
</tr>
<tr>
<td>Master Keys used for Key Derivation</td>
<td>Public Authorization Keys</td>
</tr>
</tbody>
</table>
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: Protection Requirements for Key Classes

<table>
<thead>
<tr>
<th>Key Class</th>
<th>Confidentiality</th>
<th>Integrity</th>
<th>Long Term Availability</th>
<th>Associated with usage or application</th>
<th>Association with owner/other entity</th>
<th>Associated with other info.</th>
<th>Validation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signing keys</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Signature verification keys</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secret authentication keys</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Private authentication key</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Public authentication key</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Long term data encryption keys</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Short term data encryption keys</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RNG keys</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Key encrypting key used for key wrapping</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Master key used for key derivation</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Keys derived from a Master Key</td>
<td>X?</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>Master key and protected data</td>
</tr>
</tbody>
</table>
### Table 1: Protection Requirements for Key Classes

<table>
<thead>
<tr>
<th></th>
<th>Confidentiality</th>
<th>Integrity</th>
<th>Long Term Availability</th>
<th>Associated with usage or application</th>
<th>Association with owner/other entity</th>
<th>Associated with other info</th>
<th>Validation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key transport private keys</td>
<td>X</td>
<td>X</td>
<td>X?</td>
<td>X</td>
<td>Key transport public keys</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Key transport public keys</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Key transport private key</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Static key agreement private keys</td>
<td>X</td>
<td>X</td>
<td>X?</td>
<td>X?</td>
<td>Domain parameters; static key agreement public keys</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Static key agreement public keys</td>
<td>X</td>
<td>X</td>
<td>X?</td>
<td>X?</td>
<td>Domain parameters; static key agreement public keys</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Ephemeral key agreement private keys</td>
<td>X</td>
<td>X</td>
<td>X?</td>
<td>X?</td>
<td>Domain parameters; static key agreement public keys</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Ephemeral key agreement public keys</td>
<td>X</td>
<td>X</td>
<td>X?</td>
<td>X?</td>
<td>Domain parameters; static key agreement public keys</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Secret authorization key</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Private authorization key</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Public authorization key</td>
<td></td>
</tr>
<tr>
<td>Public authorization key</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Private authorization key</td>
<td></td>
</tr>
</tbody>
</table>

### Table 1: Protection Requirements for Key Classes

<table>
<thead>
<tr>
<th></th>
<th>Confidentiality</th>
<th>Integrity</th>
<th>Long Term Availability</th>
<th>Associated with usage or application</th>
<th>Association with owner/other entity</th>
<th>Associated with other info</th>
<th>Validation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain parameters keys</td>
<td>X</td>
<td>X</td>
<td>X?</td>
<td>X</td>
<td>Private and public keys</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Initialization vectors</td>
<td>X</td>
<td>X</td>
<td>X?</td>
<td>X</td>
<td>Protected data</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Shared secrets</td>
<td>X</td>
<td>X</td>
<td>X?</td>
<td>X</td>
<td>Generated data</td>
<td>X?</td>
<td></td>
</tr>
<tr>
<td>Intermediate results</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td>Process data</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>
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

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

### Table 2: Backup of Keying Material by Material Type

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

<table>
<thead>
<tr>
<th>Bits of security</th>
<th>Symmetric key alg.</th>
<th>Hash alg.</th>
<th>DSA, D-H, MQV</th>
<th>RSA</th>
<th>Elliptic Curves</th>
</tr>
</thead>
</table>
| 80               | SHA-1              | L = 1024
N = 160        | k = 1024          | f = 160 |
| 112              | TDES               | L = 2048
N = 224        | k = 2048          | f = 224 |
| 128              | AES-128            | L = 3072
N = 256        | k = 3072          | f = 256 |
| 192              | AES-192            | L = 7680
N = 384        | k = 7680          | f = 384 |
| 256              | AES-256            | 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

<table>
<thead>
<tr>
<th>Years</th>
<th>Symmetric key alg. (Encryption &amp; MAC)</th>
<th>Hash Alg.</th>
<th>HMAC</th>
<th>DSA, D-H, MQV</th>
<th>RSA</th>
<th>Elliptic Curves</th>
</tr>
</thead>
<tbody>
<tr>
<td>Present - 2015</td>
<td>TDES</td>
<td>SHA-1</td>
<td>SHA-1 (≥80 bit key)</td>
<td>Min.: $L = 1024$, $N = 160$</td>
<td>Min.: $f = 1024$</td>
<td>Min.: $f = 160$</td>
</tr>
<tr>
<td></td>
<td>AES-128</td>
<td>SHA-256</td>
<td>SHA-256 (≥128 bit key)</td>
<td>Min.: $L = 1024$, $N = 160$</td>
<td>Min.: $f = 1024$</td>
<td>Min.: $f = 160$</td>
</tr>
<tr>
<td></td>
<td>AES-192</td>
<td>SHA-384</td>
<td>SHA-384 (≥192 bit key)</td>
<td>Min.: $L = 2048$, $N = 224$</td>
<td>Min.: $f = 2048$</td>
<td>Min.: $f = 224$</td>
</tr>
<tr>
<td></td>
<td>AES-256</td>
<td>SHA-512</td>
<td>SHA-512 (≥256 bit key)</td>
<td>Min.: $L = 2048$, $N = 224$</td>
<td>Min.: $f = 2048$</td>
<td>Min.: $f = 224$</td>
</tr>
</tbody>
</table>

2016 and beyond | TDES                                  | SHA-256   | SHA-256 (≥128 bit key) | Min.: $L = 2048$, $N = 224$ | Min.: $f = 2048$ | Min.: $f = 224$ |
|              | AES-128                                | SHA-384   | SHA-384 (≥192 bit key) | Min.: $L = 2048$, $N = 224$ | Min.: $f = 2048$ | Min.: $f = 224$ |
|              | AES-192                                | SHA-512   | SHA-512 (≥256 bit key) | Min.: $L = 2048$, $N = 224$ | Min.: $f = 2048$ | 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