Implementation and Operations Guidelines for an
Enterprise Key Management Infrastructure (EKMI)

Table of Contents

1. Introduction
   1.1. Background
       1.1.1. What is key-management?
       1.1.2. Why key-management?
   1.2. What is an EKMI?
   1.3. Components of an EKMI
       1.3.1. PKI
           1.3.1.1. What is a PKI?
           1.3.1.2. Why PKI?
       1.3.2. SKMS
           1.3.2.1. What is an SKMS?
           1.3.2.2. Why SKMS?

2. PKI
   2.1. Applications
   2.2. Architecture
   2.3. Policy Considerations
   2.4. Best Practice Policies for PKI
   2.5. Security Considerations
   2.6. Technology
       2.6.1. Certification Authority
       2.6.2. Registration Authority
       2.6.3. Hardware Security Module(s)
       2.6.4. Publishing Directory
       2.6.5. Certificate Validation
   2.7. Standards and Protocols
   2.8. Operations

3. SKMS
   3.1. Applications
   3.2. Architecture
   3.3. Policy Considerations
3.4. Best Practice Policies for SKMS
3.5. Security Considerations
3.6. Technology
   3.6.1. Symmetric Key Services Server
   3.6.2. Symmetric Key Client Library
   3.6.3. Hardware Security Module(s)
3.7. Standards and Protocols
3.8. Operations

4. The future of EKMI
   4.1. Short-term
   4.2. Long-term

5. EKMI Resources
   5.1. PKI Resources
   5.2. SKMS Resources

6. Appendices