Key Management Guidelines

Selected Infrastructures

Tim Polk, NIST

Status

- This section is currently empty
Classes of Infrastructures

- Three identified so far
  - Public Key Infrastructure
  - Kerberos
  - DNSSec
- Others?

Scope

- Key management requirements for
  - Infrastructure components
  - Infrastructure “relying parties”
- Should be an infrastructure-specific interpretation of the guidelines in section 5
Example: PKI

- Infrastructure components
  - CA
  - RA
  - Repository
  - Status Servers
- Infrastructure users
  - Certificate subject
  - Relying Party

Classes of keys Handled by RA/CA

- 3 Classes by “owners”
  - CIMS personnel keys
  - Component keys
  - Certificate subject private keys
Classes of keys Handled by RA/CA, Cont’d

♦ 7 classes of keys by utility
  – Certificate and Status Signing Keys
  – Integrity or Approval Authentication Keys
  – General Authentication Keys
  – Long Term Private Key Protection Keys
  – Long Term Confidentiality Keys
  – Short Term Private Key Protection Keys
  – Short Term Confidentiality Keys

Repositories

♦ Trusted repositories?
♦ Access Control?
Certificate Subjects/Relying Parties
- Their own public and private keys
- Trusted public keys
- Untrusted public keys for other certificate subjects
- May handle authorization codes, other infrastructure-supplied key materials

Goal
- Establish key management requirements for all the different types of keys
  - Selecting algorithms and key lengths
  - Key protection requirements
    - Generation, storage, import/export (e.g., POP)
    - Cryptoperiods and CRLs
Sources

- Source for infrastructure: CIMC
- Source for user components: ?

Completion

- Repeat this process for each infrastructure