Outline

• Objectives
• Progression of technical capabilities
• Current enterprise
• Future vision
Functional Objectives and Description

• COTS-based architecture
• Support of multiple applications and vendors through open systems, standards-based approach
• FIPS-compliant crypto modules
• Services include digital signature/non-repudiation, authentication, key escrow and recovery of confidentiality (decryption) keys
Milestones

- August 1998: Medium Assurance Pilot introduced with two certificates (signing, email)
- July 2000: Release 2 delivers CA signing in h/w, functional separation of email certs, and key escrow and recovery of decryption keys
- October 2001: Release 3 delivers operational issuance to the DoD Common Access Card (CAC)
Current DoD CLASS 3 PKI
Release 3 Integrated Process

1. **Person Authentication & Data Update**
   - **Establish User**
   - **Generate Keys**
   - **Obtain Certificates**
   - **Load Keys**

2. **DEERS Data Base**
   - Inquiry
   - Demographic and Personnel information
   - ID Card, Picture and Fingerprint

3. **Private Key generation on the card.**
   - **User’s Smart Card (CAC)**

4. **Certificate Requests and decryption keys for escrow**

5. **Certificate Authority**
   - **Directory Services**

6. **CERT**

---

**V.O.**
Future Vision

- DoD Mobile Code signing implementation
- Support for Microsoft Win2K Smart Card logon
- Browser-based key recovery and card “maintenance”
- Revocation information improvements
  - Testing and deployment of On-line Certificate Status Protocol (OCSP) service
  - Testing http reference in CRL Distr. Point
  - Testing Delta CRL implementation
- Focus on enabling applications to use PKI