JITC Interoperability Certification of Public Key Enabled (PKE) Applications

Ms. Cammie Webster
JITC PKI Action Officer
(520) 538 5485
webstercc@fhu.disamil
19 June 2002
Agenda

• DOD PKE Overview
• Testing Overview
• Testing Process
• Findings
• Lessons Learned
• Applications
• Summary
• Applications must be enabled to take advantage of PKI services
• Applications are a key aspect to trust
• DOD’s approach to applications
  – Establish a set of requirements
  – Leverage on commercial applications
  – Require interoperability testing
  – Provide DOD entities with a list of approved commercial applications
Testing Overview

• Testing Scope
  – Certificate Processing
  – CRL Processing
  – Certificate Path Processing
  – Storing Trust Points
  – Communication Protocols
  – Importing/Exporting Keys and Certificates
Testing Overview

- **Testing Benefits**
  - Ensures enabling process was done correctly and vendor claims are true
  - Maintains the integrity of the infrastructure
  - Ensures interoperability with the infrastructure
Testing Overview

• Goals
  – Determine the extent that the application complies with DOD requirements
  – Determine application’s ability to properly use and process certificates issued by the DOD PKI
  – Confirm accuracy of methods used to communicate with the DOD PKI
Testing Process

1. Application PMO contacts JITC
2. Application Assessment Worksheet Completed by PMO
3. Evaluation Process
4. Interoperability Testing Conducted
5. Testing Completed
6. Test Report Written
7. Interoperability Certification Letter Issued
8. Results Published
Findings

• No path processing performed
  – Validation of unauthorized certificates

• Certificate presented as valid without presence of CRL
  – Allows use of revoked certificates

• Critical sections of User Manual Incomplete
  • Operators unable to follow to complete transactions
Findings

• Incorrect handling of deltaCRLIndicator
  – Validate certificates when only checking a partial CRL

• Incorrect processing of path development (certificates and CRLs)
  – Potential for a valid DOD certificate to sign certificates for unauthorized users or to sign CRLs with false revocation
Lessons Learned

- Many are unfamiliar with DOD PKE requirements
- Most applications fall short on path processing
- Assessment period is often the most time consuming
- Software changes are likely
Applications

Lexign - ProSigner
(ELock - Assured Office)
Silanis - Approvelt
PKWare – PKZip
Microsoft – Office XP
Gradkell Systems - DBSign
Pure Edge – US Air Force custom app
Information Security Corp - Secret Agent
Ilumin – Digital Handshake Server
Envinsible - Envinsible Ink
Applications are a crucial aspect of trust, don’t assume they are doing their job correctly!

Testing ensures applications maintain the trust a PKI provides.
Questions?

Ms. Cammie Webster
(520) 538-5485
E-mail: websterc@fhu.disa.mil

JITC PKI Web Site:
http://jitc.fhu.disa.mil/pki