

DoD  
Public Key-Enabling (PK-E)  
of Applications

1st Annual PKI Research  
Workshop  
NIST  
4/25/02

# Overview

- PK-E distinct from PKI
- Definition of “PK-E”
- Interoperability with DoD PKI
- “Security Goodness”
- Protection Profile, Technical Instruction, Proof of Concept (POC)

# PK-E Distinct from PKI

- PK Infrastructure - CAs and RAs and LRAs, Revocation Information Repositories, Certificate Policies, Certification Practice Statements, etc, etc
- PK-Enabling - builds or modifies applications to use the security services supported by the PKI

# Definition of PK-E

- An application is PK-Enabled if it
  - Can accept and process a DoD PKI X.509 digital certificate in order to use one or more of the security services supported by the DoD PKI (confidentiality, authenticity, integrity, non-repudiation)
  - Contains an interface to the Common Access Card (CAC) or other DoD approved hard token
  - Collects, stores and maintains any data required to support digital signature and data encryption
  - Maintains accurate time to a sufficient degree of precision

# Interoperability with DoD PKI

- Determined by the Joint Interoperability Test Command (JITC) by means of “DoD PKI Interoperability Master Test Plan”.

# “Security Goodness”

- Application could pass JITC functional test for “interoperability” with DoD PKI but still be deficient in “security”
- National Security Telecommunications and Information Systems Security Policy (NSTISSP), Number 11- requires U.S. Govn. IT systems to be evaluated and validated by Common Criteria after 1 July 2002

# Protection Profile (PP)

- Public Key-Enabled Protection Profile – generic, system level PP, for PK-Enabled applications
  - In draft, soon to be presented for NIAP evaluation

# PK-E Technical Instruction

- One-stop document (theory, policy, technical, procurement) for an application owner/manager (contract to be awarded in 5/02)

# PK-E TI Proof of Concept

- Contractor who wrote TI uses it to PK-E an application selected by USMC (part of TI contract to be awarded in 5/02)

# Further Study

- How much is all this going to cost?
- Role of PKI/PK-E in a tactical environment (some of the standard assumptions don't apply)
- Can an application be “partially PK-Enabled”?

# PK-Enabled ?

