

# United States DoD Public Key Infrastructure:

## *Deploying the PKI Token*

---

**R. Michael Green**

**Director, DoD PKI PMO**

**(410) 854-4900**

**[rmgree2@missi.ncsc.mil](mailto:rmgree2@missi.ncsc.mil)**

**Becky Harris**

**Deputy Director, DoD PKI PMO**

**(703) 882-1600**

**[Harris1B@ncr.disa.mil](mailto:Harris1B@ncr.disa.mil)**

# United States DoD Public Key Infrastructure Program



**The Goal:** To *enhance the business processes* and *improve the IA posture* of the DoD through widespread use of PK-enabled applications.

<http://iase.disa.mil> (must be from .mil or .gov domain)

<http://www.c3i.osd.mil/org/sio/ia/pki/index.html>

## DoD PKI

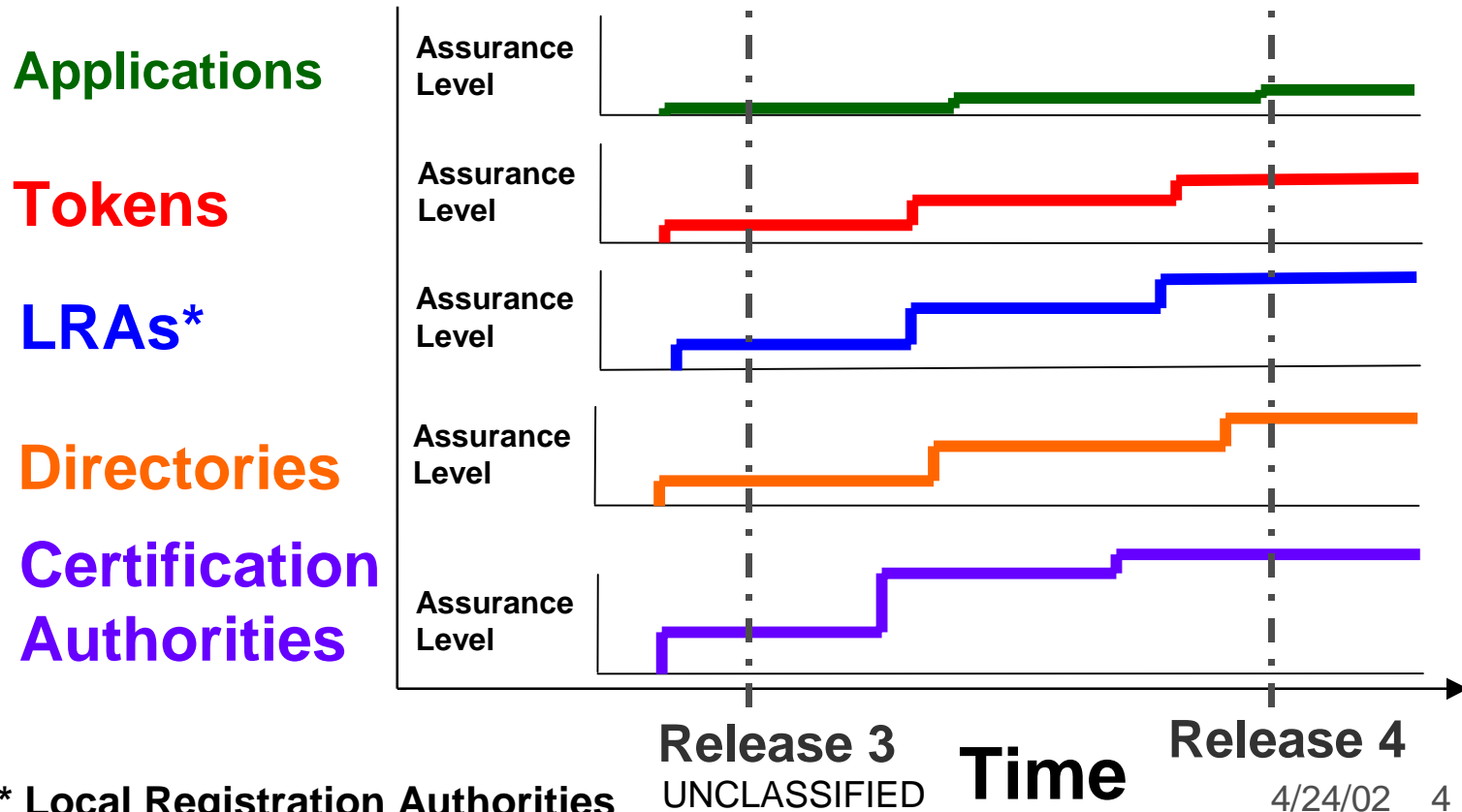
# Program Management and Policy

- **9 April 99** ASD (C3I) Memorandum  
*Assigned DoD PKI Program Management Office (PMO) Responsibility* to NSA with DISA Deputy PM
- **6 May 99** DEPSECDEF Memorandum *Defined DoD PKI Policy Objectives*
- **10 Nov 99** DEPSECDEF Memorandum  
*Established DoD Smart Card Strategy*
- **12 Aug 00** ASD (C3I) Memorandum  
**(Rewrite of 6 May DoD PKI Memo)**

# The Challenge - It's a hard problem

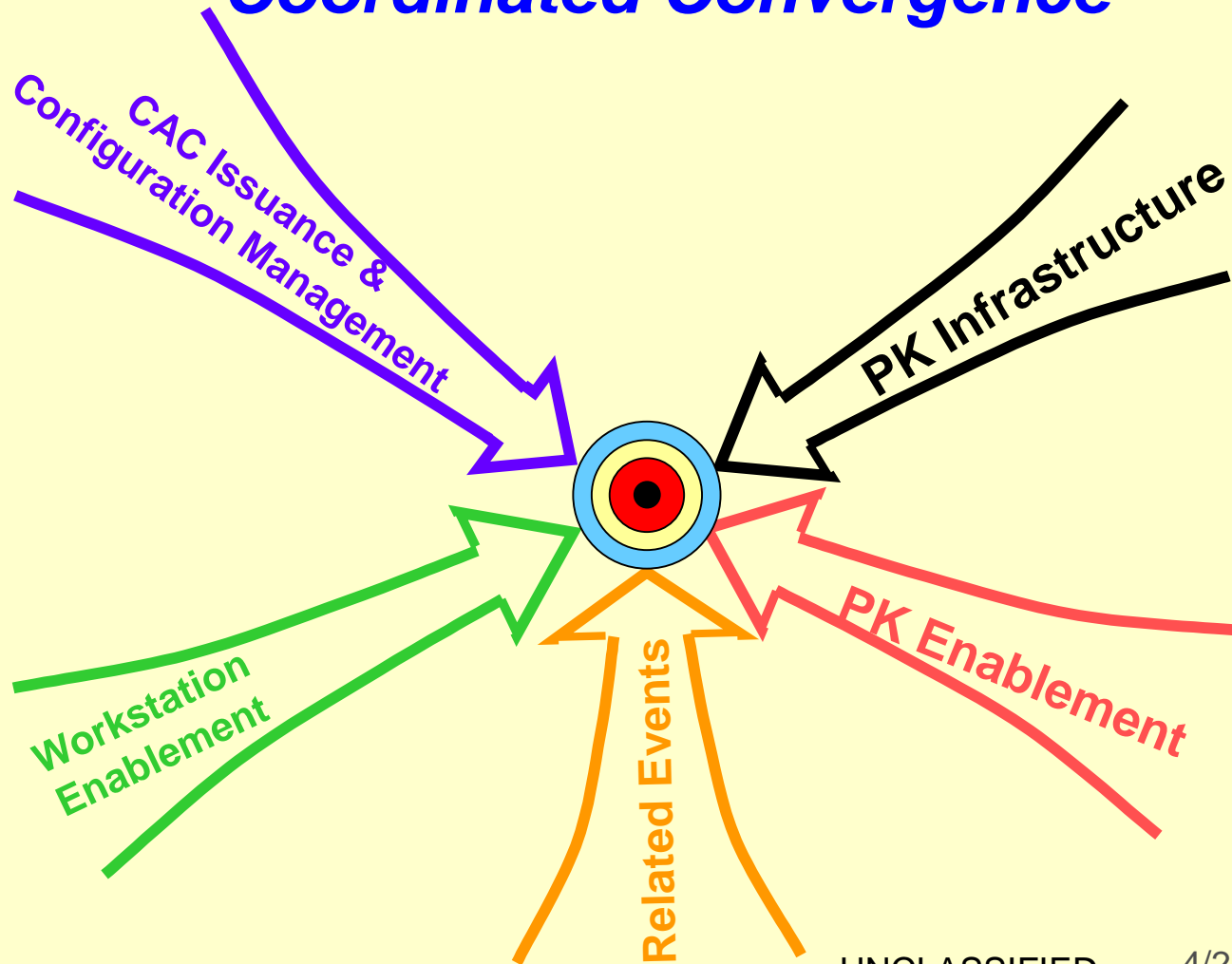
## Event Driven Security

### Robustness Growth

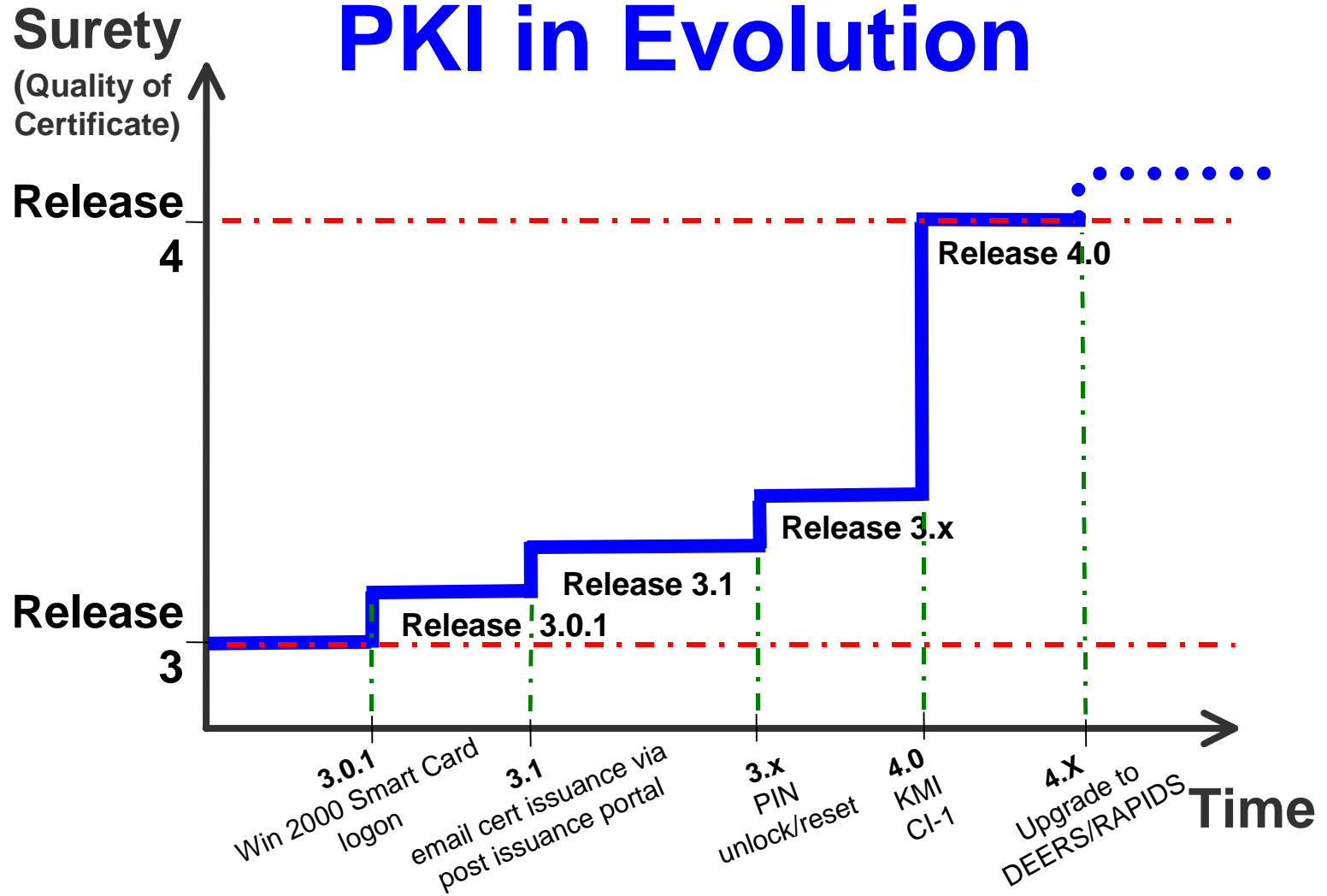


\* Local Registration Authorities

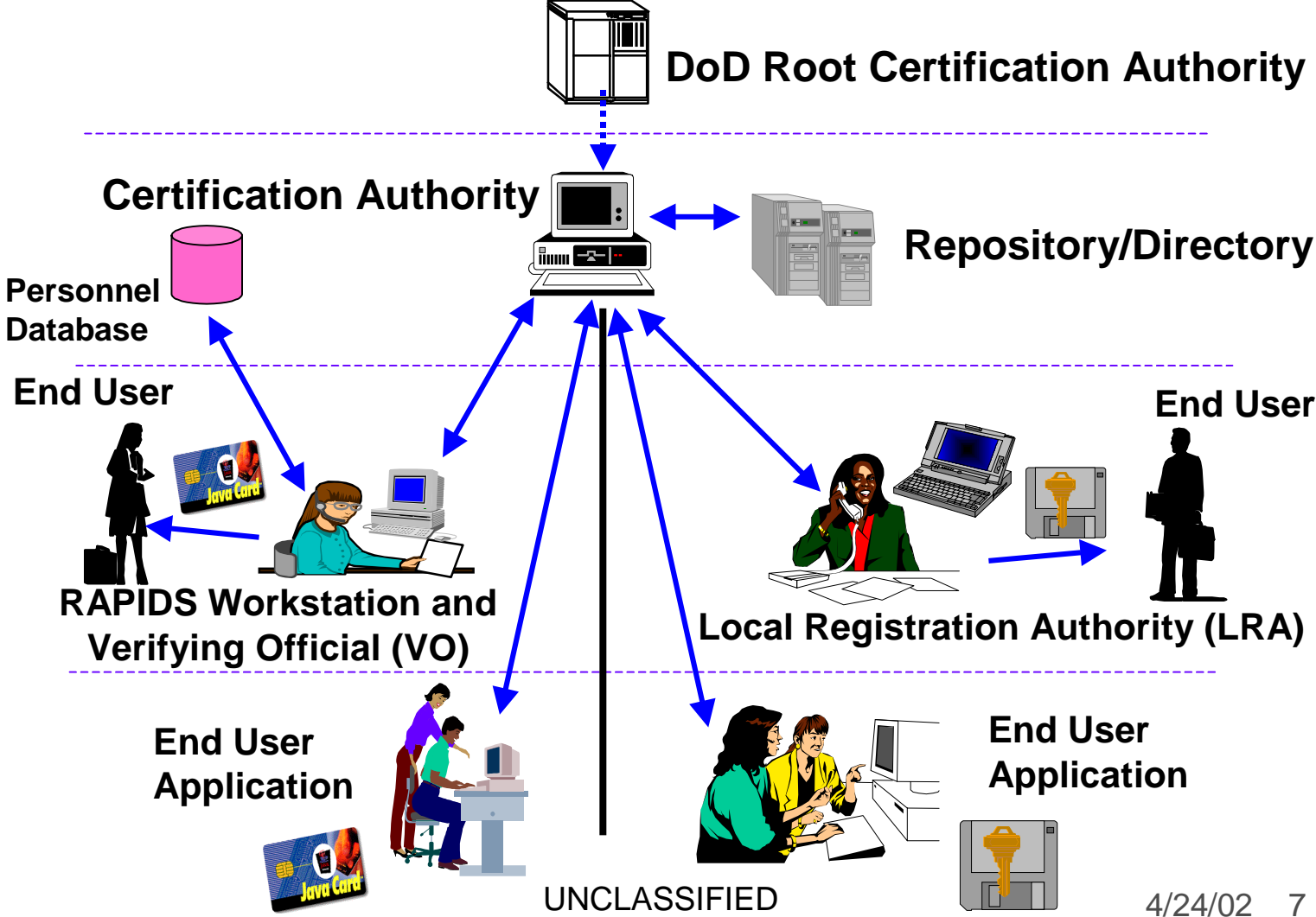
# DoD Public Key Capability Requires *Coordinated Convergence*



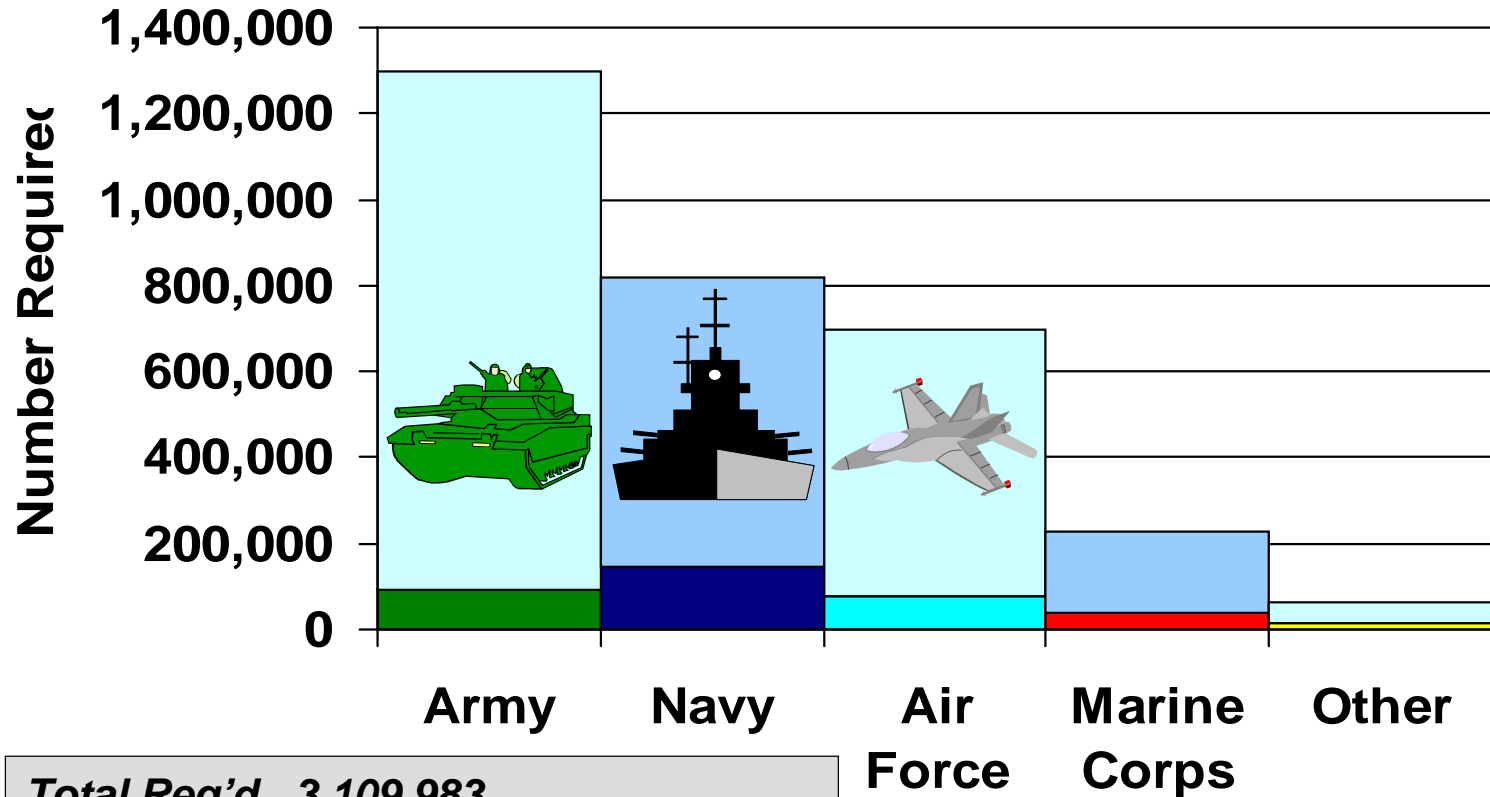
# PKI in Evolution



# DoD PKI Registration Scenarios



# # People Requiring Certs and # People Issued Certs



**Total Req'd 3,109,983**  
**Total Issued 558,659 (14 April 02)**

UNCLASSIFIED

# Current Status

- **DoD PKI Release 3 Operational - October 01**
- **Key Management Infrastructure Capability Increment-1 (KMI CI-1) awarded Nov 01; will provide Release 4.**
- **Established PKI Interoperability Testing capability**
- **Reviewing and approving DoD PKI Certificate Practice Statements**

# Preparing for the Future

- **Collected Tactical PKI User requirements**
- **Working with NIST & Smart Card Senior Coordinating Group to define process to add applets to FIPS 140 certified cards while maintaining FIPS 140 certification**
- **Updating the DoD PKI Certificate Policy (CP)**
- **Finalizing the DoD Key Recovery Policy**
- **Developed high-level approach to PK-Enabled applications**

# Future PKI Activities

- DoD Policy Rewrite/Milestone Review
- **SIPRNET Plan**
- MS Logon Agreement - Release 3.0.1
- **Code Signing - Release 3.1**
- Private Web Server Certs/Client Side Authentication
- **Biometrics**

# Other Activities

- **Directories, Directories, Directories**
- **DoD PKI and Allied Interoperability**
- **DoD PKI “versus” Federal and IC**
- **Vetting and piloting tactical and SIPRNET requirements**

# DoD PK-Enabled Applications

- **PKI provides the underlying foundation for security services, but PK-enabled applications are required in order to implement them**
- **We Must Depend on Industry to Maintain the Apps**
- **Evaluated Applications that can process our Certificates with little User Involvement**

# DoD PK-Enabled Applications

- **PK-Enabled Services/Applications:**
  - **Medium Grade Services (MGS) - secure, interoperable e-mail**
  - **Secure Web Services**
  - **DoD-specific applications (e.g. Defense Travel System, Wide Area Work Flow)**

# DoD PKI and KMI Token Protection Profile

- Used **Smart Card Security Users Group Smart Card Protection Profile** as baseline document
- Information Assurance Technical Framework Forum Protection Profiles:  
[http://www.iaf.net/protection\\_profiles/index.cfm](http://www.iaf.net/protection_profiles/index.cfm)
- Previous draft was released for public comment  
October 00 - Feb 01
- **Tokens meeting this protection profile:**
  - required by **mid-late 2003**

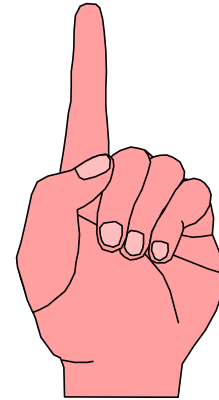
# Token PP FIPS 140 Requirements

- FIPS 140-2 **Level 2** for Subscribers \*
- FIPS 140-2 **Level 3** for Registration Authorities

\* If the DoD Common Access Card issuing infrastructure is not capable of issuing two different levels of cards, then all CACs will be required to meet FIPS 140-2 Level 3.

# Biometrics, DMDC and CAC

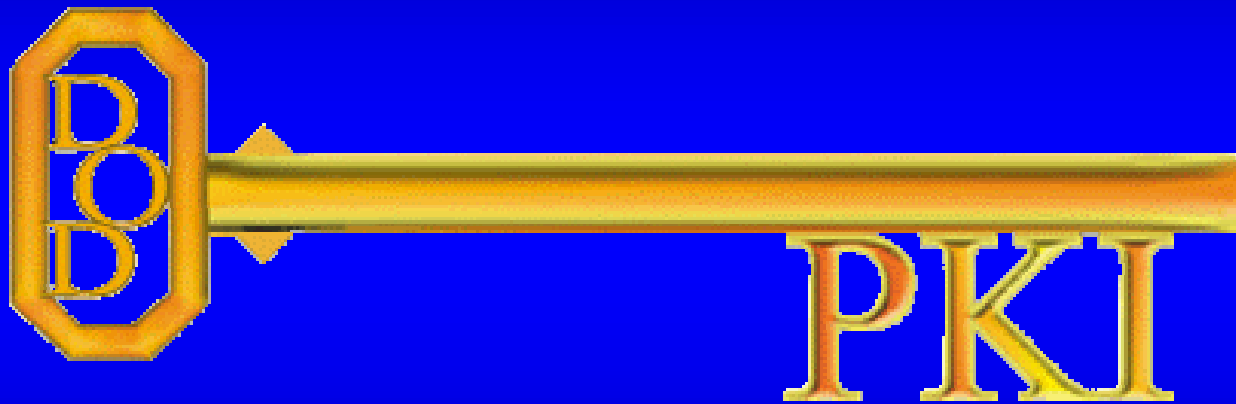
- DMDC has been collecting and storing fingerprints (template & minutia) when issuing cards.
- Biometric data is not stored on the CAC
- In the event of a forgotten PIN, biometric (fingerprint) can be provided by user at a RAPIDS workstation for authentication and to unlock her CAC



# Adding Biometrics to PKI & CAC

- Pilots under way now
- Discrete points where biometrics can be added:
  - CAC task order/purchase\*
  - middleware upgrades\*
  - DMDC/RAPIDS/DEERS upgrades\*
- \* Probably need all three of these before fully incorporating biometrics
- May impact CAC FIPS 140 certification





UNCLASSIFIED

3/13/02 19