

*Implementation of the Army  
Public Key Infrastructure*

Gary A. Robison

ODISC4 Information Assurance  
Directorate

17 November 1998

# *Outline*

- **Public Key Infrastructure**
  - What it is, what it does, what it provides, and how it works.
- **Levels of Assurance**
- **Mission**
- **Registration Process**
- **Products, Services, Facilities, Policies, Procedures, Agreements, and People**
- **Interim DoD Guidance**
- **RA - LRA Roles and Requirements**
- **Army PKI Initiatives**
- **Funding**
- **Issues - Recent DoD Initiative**
- **What we are going to do**

## *What is the Public Key Infrastructure?*

- The Public Key Infrastructure is that portion of the security management infrastructure dedicated to the management of keys and certificates used by Public Key based security services.
- It is a combination of products, services, facilities, policies, procedures, agreements, and people that provides for and sustains secure interactions in open networks.

# *Levels of Assurance*

- **High - Hardware Based**
  - ***FORTEZZA* PCMCIA Card Format**
  - **DMS**
    - **Sensitive Unclassified Information**
    - **Classified Information**
  - **High Dollar Transactions**
  - **Deployed to organization message release authorities**

# *Levels of Assurance*

- **Medium - Software Based**
  - - **Standards Based**
    - **Data Encryption Standard**
    - **Digital Signature Standard (DSS)**
      - Move to add RSA
    - **FIPS 140-1 for implementation of encryption algorithms**
  - **Sensitive Unclassified Information, Routine Financial Transactions, Procurements, Medical Records**
  - **Issued on Floppy Disk**
    - *But - will move to Smart Card*

# *Our Mission*

**Integrate**

Products,  
Services,  
Facilities,  
Policies,  
Procedures,  
Agreements,  
and People

*Immediately*

23 November, 1998

7#

# Using internal resources

23 November, 1998

8#

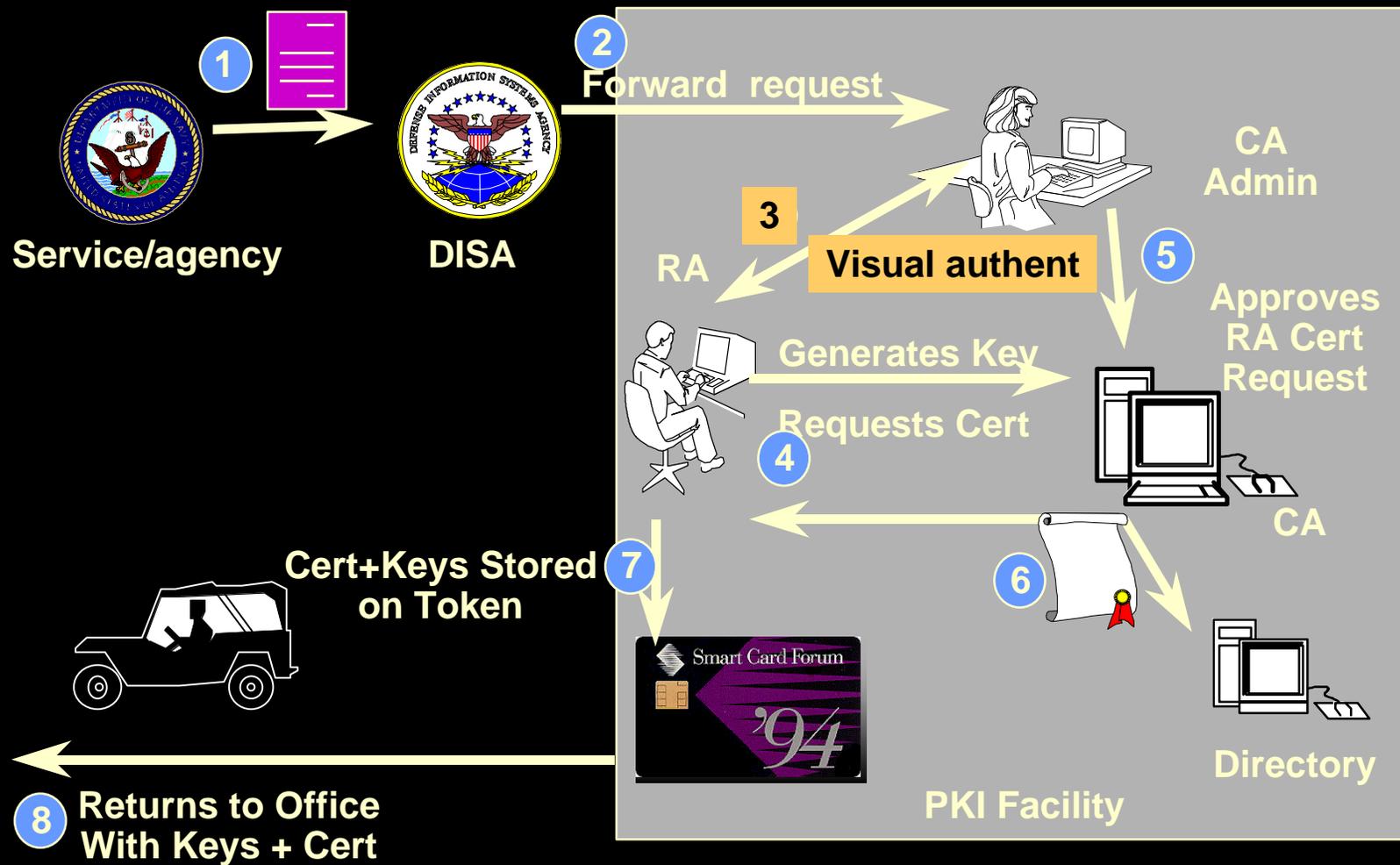
Wild

# BRITAIN'S OUTDOOR HOUSE

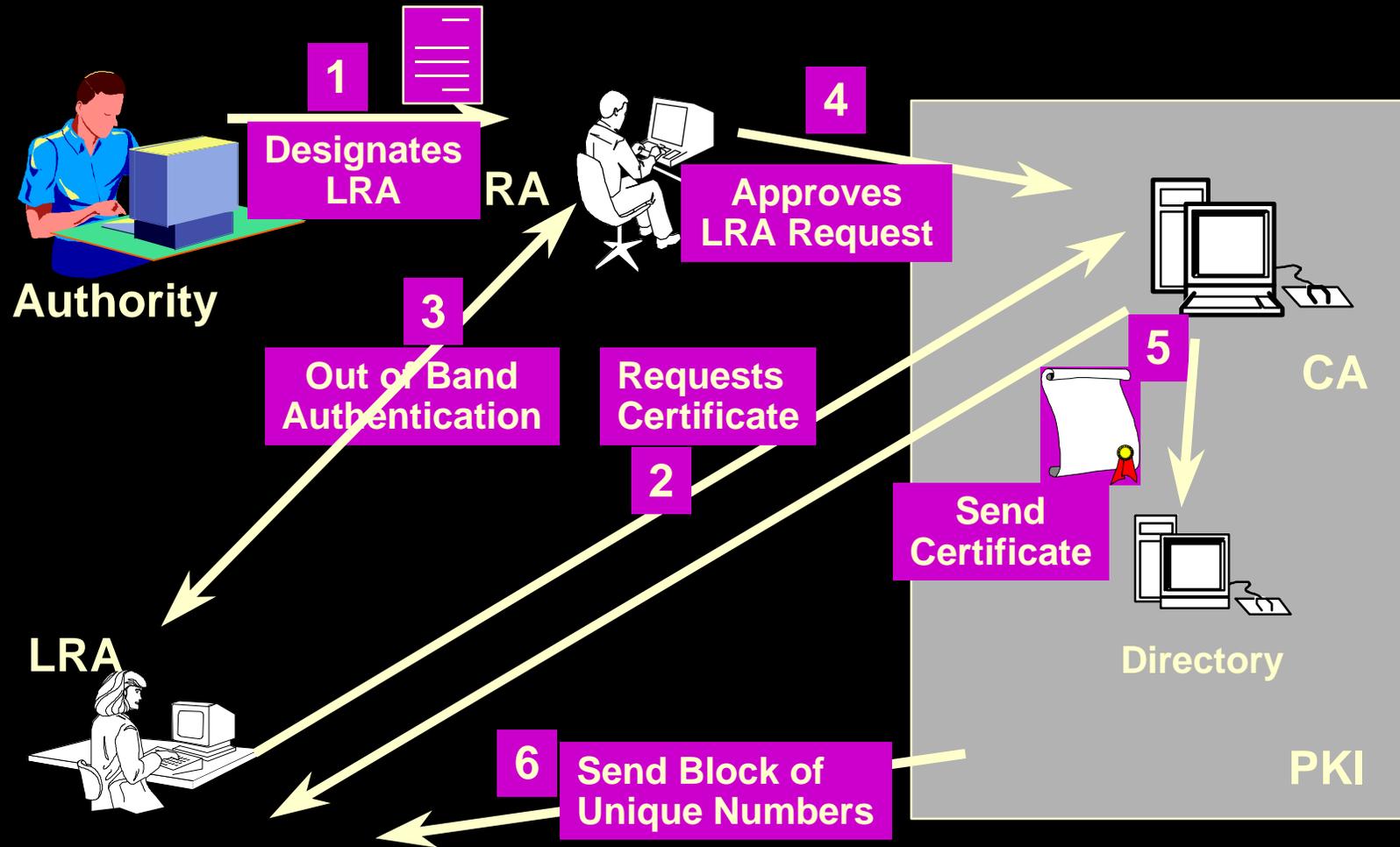
23 November, 1998

9#

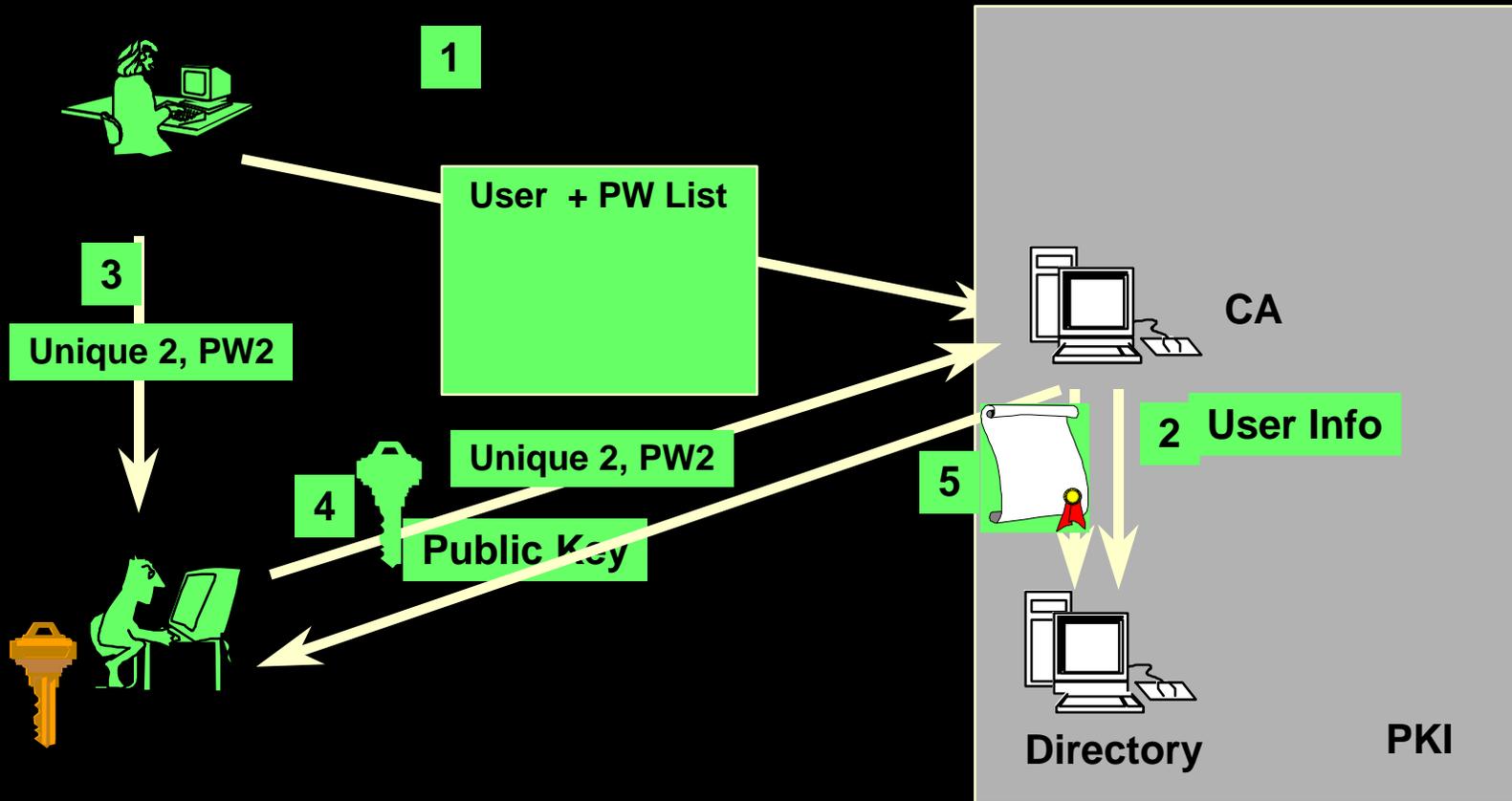
# RA Registration



# LRA Registration



# End User Registration



# *Products*

- Netscape
  - enterprise license across DoD
  - Free -- go to DISA and download
- Microsoft
  - Internet Explorer -- but not yet FIPS 140-1 compliant -- price unknown
- Lotus
  - ??

# *Services*

- DoD
  - NSA Root Certificate Authority
  - DISA Certificate Authorities and Directories
    - Chambersburg
    - Denver
- Commercial Market Place
  - Verisign

## *Facilities*

- Installations will be required to provide a securable, accessible location to house the Local Registration Authority (LRA) workstation
  - Personnel will travel to the LRA's place of business to be registered
  - In some situations the LRA may be required to travel

# *Policies*

- Interim DoD Guidance
  - ASD C3I memorandum
- Army Guidance
  - being developed in parallel with DoD

## *Interim Guidance for the Department of Defense Public Key Infrastructure*

- ASD C3I will coordinate
  - DoD X.509 Certificate Policy
  - DoD Certificate Practice Statement
  - DoD Public Key Infrastructure Roadmap
- Until these documents are fully coordinated, and a DoD PKI Strategy has been developed
  - no new certificate infrastructures will be created.
  - On going pilots may be continued, but costs should be minimized
  - risk management decision must be reviewed

## *Interim Guidance for the Department of Defense Public Key Infrastructure- cont'd*

- Additional applications wishing to use the current medium assurance pilot infrastructure, must
  - conduct a risk assessment
- DISA and NSA will provide guidance on conduct of the Risk assessment
- DoD PKI Senior Steering Committee will grant approval
- Pilots are required to report lessons learned

## *Interim Guidance for the Department of Defense Public Key Infrastructure- cont'd*

- Goal for publication of DoD PKI Strategy
  - DoD X.509 Certificate Policy
  - DoD Certificate Practice Statement
  - DoD Public Key Infrastructure Roadmap

**15 January 1999**

# *Procedures*

- Drafts available on Army PKI Web Site

# *Agreements*

- External Certificate Authorities
  - Pending

# People

•Active Army:	482,847	31 March 1997
•Civilians:	279,259	June 1997
•National Guard:	367,973*	30 June 1997
•Army Reserve:	211,876*	30 June 1997
<b>Total</b>	<b>1,341,955</b>	
•Army Dependents:	780,967	<b>Total DoD: 2,224,978</b>
•Army Retirees:	451,757	<b>Total DoD: 1,444,088</b>
•Medical Program:	1,231,724	<b>Total DoD: 3,669,066</b>

\*does not include inactive reserve

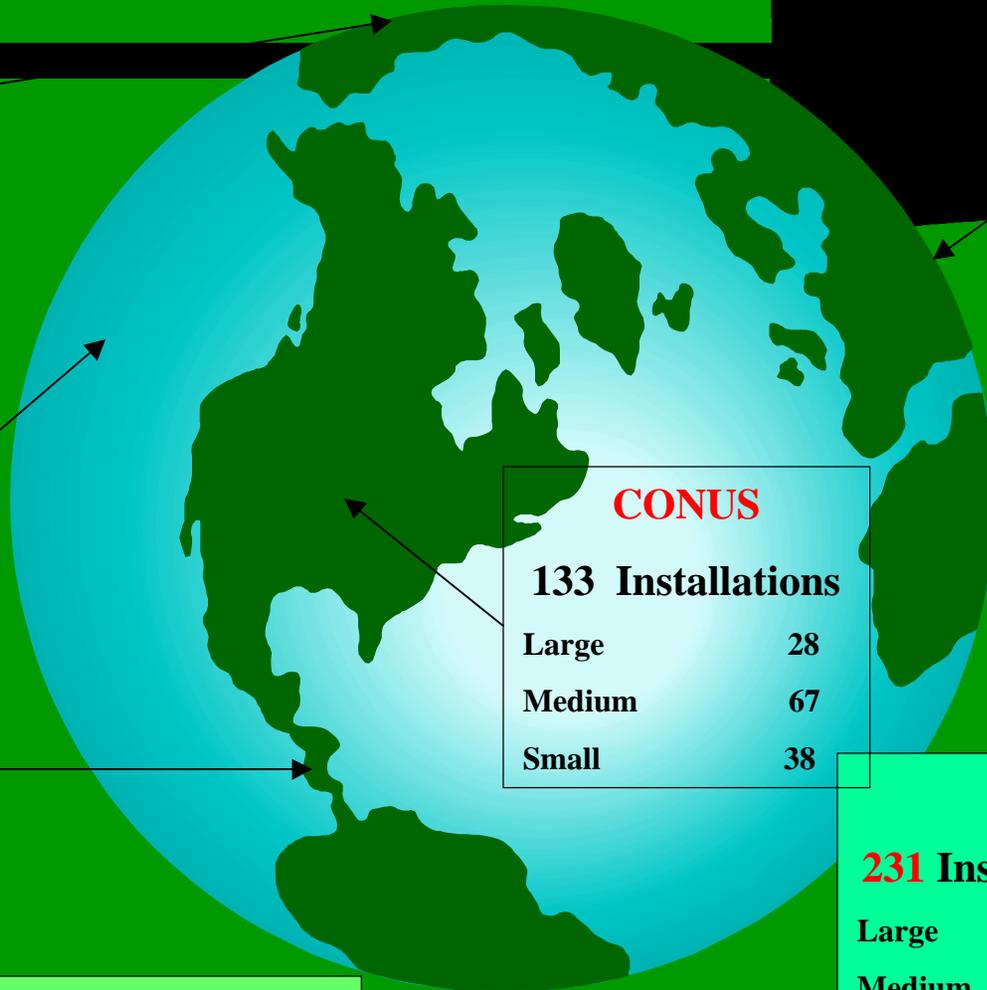
# Army Personnel on Installations

Korea	
<b>23 Communities</b>	
Large	2
Medium	19
Small	2

Pacific	
<b>16 Installations</b>	
Large	1
Medium	11
Small	4

Southern	
<b>4 Communities</b>	
Large	1
Medium	3

**5400 Guard/Reserve locations**



Europe	
<b>55 Communities</b>	
Large	6
Medium	32
Small	17

CONUS	
<b>133 Installations</b>	
Large	28
Medium	67
Small	38

TOTALS		
<b>231 Installations/Communities</b>		
Large	( 5,501 - 47,375)	38
Medium	(101 - 5,500)	132
Small	( 0 - 100)	61

# *Roles of RA and LRA*



- Registration Authority (RA)
  - One per MACOM
  - Approves, registers, oversees LRAs
  - Performs user and LRA Certificate Revocation
- Local Registration Authority (LRA)
  - Collocated with and knowledgeable about users
  - Verifies user identity
  - Pre-approves certificates
  - Provides PKI information to users
  - Passes revocation info to RAs

## *Estimated number of LRA's Required to Sustain User Registration*

• <b>Active Army + Civilians</b>	<b>Total</b>
– <b>Large Installations</b>	<b>44</b>
– <b>Medium Installations</b>	<b>132</b>
– <b>Small Installations</b>	<b>60</b>
• <b>National Guard (1 per TAG)</b>	<b>54</b>
• <b>Army Reserve (1 per RSC/ARCOM)</b>	<b>50</b>
<b>Total</b>	<b>340</b>

**Note: Bases on 22,000 certificates /LRA/year (1 certificate / 5 min)**

**Retirees and Dependents NOT included**

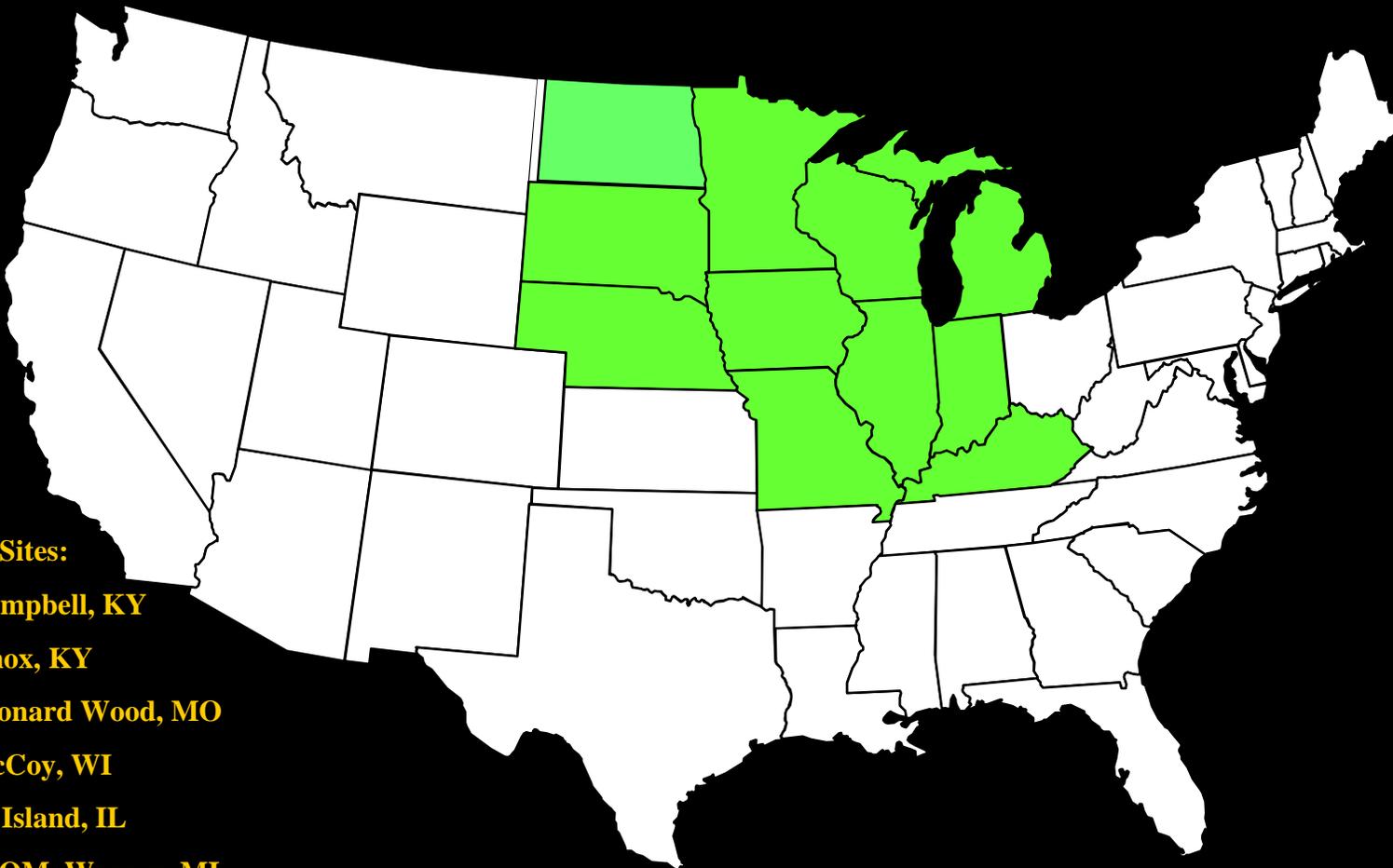
## *RA and LRA Requirements*

- Primary and Alternate must be appointed
- Minimum of Secret clearance based on a Single Scope Background Investigation.
- Must complete training before beginning to work

# *People Issue*

- Where should the LRA be located at the installation?
  - Security
  - DOIM
  - Personnel
  - Financial

# *Defense Travel Region 6*



**Army Sites:**

- Ft Campbell, KY
  - Ft Knox, KY
  - Ft Leonard Wood, MO
  - Ft McCoy, WI
  - Rock Island, IL
  - TACOM, Warren, MI
  - Detroit Arsenal, MI
- 23 November, 1998

# *Army PKI Initiatives*

- America's Army On-line - GOMO
- Army Knowledge Office for PEO & Acquisition Community Management Information Storage, Retrieval, Dissemination & Security - PEO C3S
- Army Single Face to Industry (ASFI) - Paperless Contracting Office, SARDA
- Defense Travel System (DTS) - DOD
- Electronic Transportation Acquisition (ETA) - MTMC
- Enterprise Wide Email, Itranet & WebServer - CECOM
- Forensic Toxicology Drug Test Laboratory (FTDTL) - MEDCOM
- Global Combat Support System - Army (GCSS-A) - PEO STAMIS
- Joint Computer-Aided Acquisition and Logistic Support (JCALS) - PEO STAMIS
- Military History Institute (MHI) Digital Library (AKA MHI Electronic Document Archival Management System) - TRADOC
- Project Manager Night Vision/Reconnaissance, Surveillance, and Target Acquisition (PM NV/RSTA) Budget Planning, Execution and Reporting System (BPERS) - PEO STAMIS
- Reserve Component Automation System (RCAS) - NGB
- The Defense Civilian Personnel Data System (DCPDS) Modernization Program, DCPDS Personnel Process Improvement (PPI), Army Civilian Personnel Community - PEO STAMIS
- DoD Paperless Contracting - Electronic Document Access (EDA), Wide Area Workflow Pilot (WAWF) - DOD

# *Funding*

- Requirements have been identified, but .....

PKI is *unresourced* at this time.

# *Issues*

- Digital signature
  - Key(s) will not be archived
- Privacy
  - Key(s) must be archived
  - Key recovery on large scale untried

# *Issues*

- Issuing certificates to contractors
- Issuing certificates to foreign nationals
  - Department of Army employees
  - Foreign contractors

# *Recent briefing to DoD Senior Leadership*

- History and statistics reminds us that the largest security risk is from insider attack
- Certifying each user must be our starting point for enterprise security
- DISA and NSA are providing a solution for PKI
- Full scale implementation can begin

# *Recent briefing to DoD Senior Leadership*

- Recommendation
  - Implement medium grade PKI certificates on common access cards (building and computer) using biometric verification.....
  - within the next 26 months.

# *Implications*

- “on common access cards (building and computer) using biometric verification.”
  - building access card will require photo
  - need a smart card (card with chip) to store the PKI certificate keys
  - will need to capture the biometric data during the registration process
- Essentially doubles the registration time
  - from 5 minutes to 10+ minutes

# *Implications*

- Will require more equipment at LRA site
  - Digital camera
  - Biometric capture (fingerprint) equipment
  - Data base
  - Smart Card reader/programmer
- Will require smart cards for everyone
- Will require smart card and biometric readers at each workstation

# *Cost Estimate*

- \$234 Million across POM
  - \$69 Million in FY99
  - \$95 Million in FY00

## *What we are going to do*

- Listen to your concerns
- Capture your ideas
- Develop an action item list
- Assign personnel to work the issues
- Regardless of the current funding status,

**WE WILL MOVE AHEAD**

Break

23 November, 1998

39#

# *POC*

- Gary A. Robison
- (703) 604-7573 or DSN 664-7573
- Robisga@hqda.army.mil

# COMPARISON

CCSLA

**AKMS**



Tier 1 Facility

**DMS**



Policy Creation Authority

DISA

**PKI**



Certificate Authority

COMSEC Custodians



Key Processor  
Local Management Device

761 + Spares



Data Transfer Device

170,140

Security



Certificate Authority Workstation

214



Organizational Registration Authority Workstation

??

Personnel



Registration Authority

20+



Local Registration Authority

340



23 November, 1998

89,210

1,300,000+

41#

