DOD Public Key Infrastructure (PKI)

Status

Gilda Mckinnon

21 February 2001

(703) 681-0905

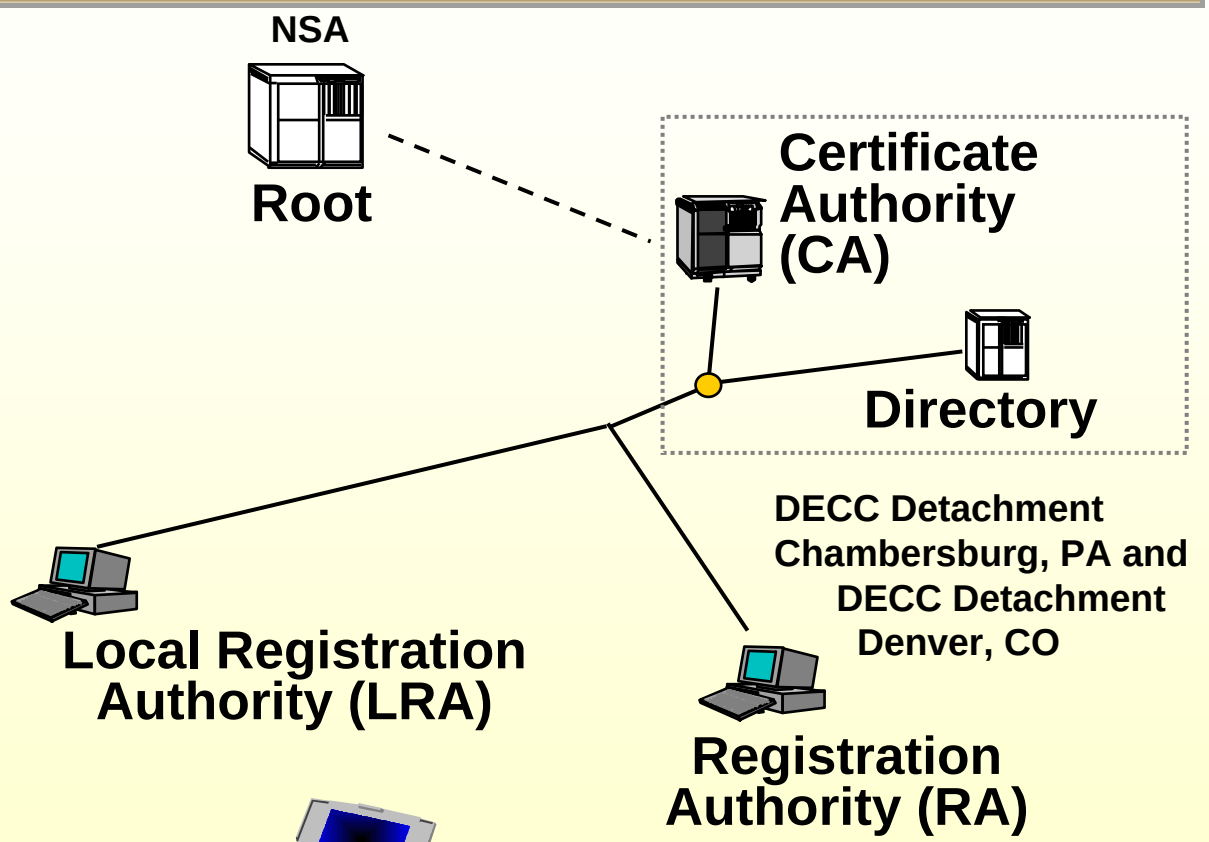
mckinnog@ncr.disa.mil

Agenda

- DOD PKI Components
- DOD PKI
  - Medium Assurance Pilot, Release 1.0
  - DOD PKI Release 2.0
  - DOD PKI Release 3.0
    - Common Access Card (CAC) Beta
- Registration Authorities/Local Registration Authorities
- Training
- Application Support
- External Certification Authorities and Interim External Certification Authorities
- Way Ahead

DOD PKI Components

- Operational on
  - NIPRNET
    - 59,438 identify
    - 37,080 e-mail
    - 4,731 servers
    - 118 RAs
    - 332 LRAs
  - SIPRNET
    - 247 identify
    - 28 e-mail
    - 86 servers
    - 9 RAs
    - 12 LRAs



- CA Architecture is highly centralized
- LRAs highly decentralized

24 X 7 Help Desk
1-800-582-4764
weblog@chamb.disa.mil

Medium Assurance PKI Pilot, Release 1.0

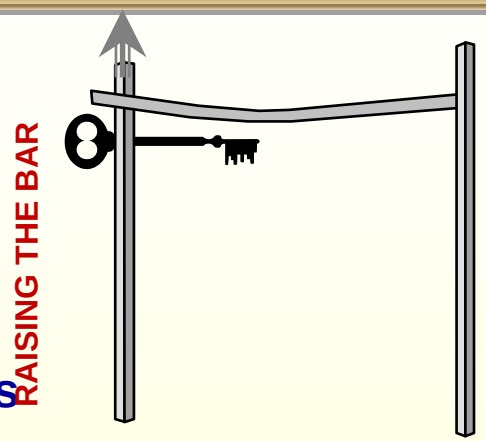
- **Operational on -**
  - **NIPRNET since April 1998**
  - **SIPRNET since September 1999**
- **NIPRNET transitioned to DOD PKI Release 2.0 - 31 December 2000**

  - Exceptions:
  - **Federal Voting Assistance Program (FVAP)**
  - **Army Recruiting Information Support System (ARISS)**

  - Release 1.0 is interoperable with DOD PKI Release 2.0

  - Release 1.0 certificates are valid until their expiration date
  - **Release 1.0 Certificate Revocation Lists still supported**
  - **RAs can still manage Release 1.0 certificates**
- **SIPRNET registration underway to support Global Combat Support System (GCCS)[reference DMS Message, Subject: DOD PKI Registration on SIPRNET to Support the GCSS Commander in Chief/Joint Task Force (CINC/JTF), 10 January 2001.]**

DOD PKI Release 2.0



- Operational July 31, 2000
- Asserts Class 3 level of assurance
- Enhancements
  - Key Escrow/Key Recovery
  - FIPS 140-1 level 2 hardware signing of certificates
  - Added Policy Object Identifiers to differentiate between HW/SW certificates
  - FIPS 140-1 level 2 smart cards for registration personnel
  - Larger capacity infrastructure
  - Improved firewall protection of the enclaves
- Training
  - RA/LRA training started in May 00
- DOD PKI RA/LRA Workstation Security Settings Document @ https://iase.disa.mil/documentlib.html#PKIDOCS

DOD PKI Certificate Policy and Certificate Practice Statement

- **Certificate Policy (CP)**
  - DOD X.509 CP version 5.2, dated 13 November 2000
    - Support DEERS/RAPIDS and CAC program
    - Permit copies of user private signature key per mission requirements
    - Support Issuance of Certificates to Foreign Nationals
- **CLASS 3 Certificate Practice Statements (CPS)**
  - Approved: Root CA CPS; CA CPS; RA & LRA Reference CPS; DIA RA & LRA CPS
  - In coordination/draft: DOD RAPIDS Workstation & VO CPS; Army RA CPS; Navy RA Reference CPS; and DISA RA CPS
- **CLASS 4 Certificate Practice Statements**
  - Approved: Fortezza/NSM Reference CPS and Marine Corp CLASS 4 CA CPS
  - In coordination: Navy, CLASS 4 CA CPS and Army, CLASS 4 CA CPS

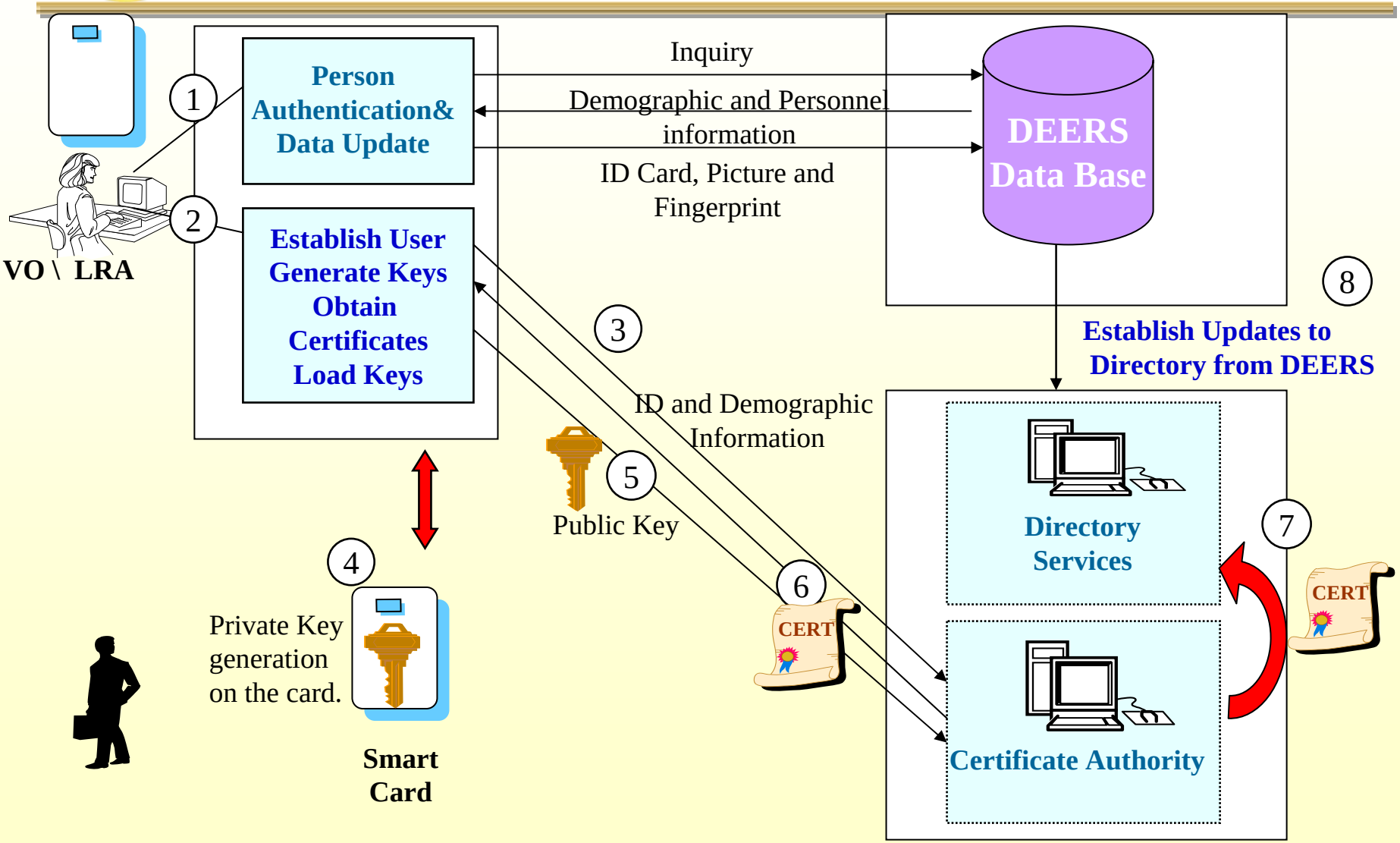
DOD CP & CPS are reviewed, analyzed, & approved by the DOD PKI CPMWG

DOD PKI Release 3.0 Enhancements

- **Establishes connection to Defense Enrollment Eligibility Reporting System (DEERS), which provides the PKI Unique Identification Number.**
- **Enables Real-time Automated Personnel Identification System (RAPIDS) Verification Officers (VOs) to issue PKI certificates on Common Access Card (CAC)**
- **Schedule:**
  - **CAC BETA** **1st QTR FY01**
  - **System Security Assessment** **2nd QTR FY01**
  - **Release 3.0** **3rd QTR FY01**

Common Access Card (CAC) BETA

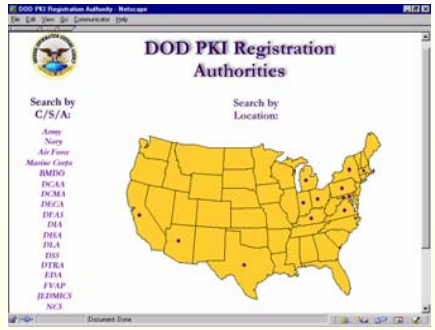
ID Certificate Issuance



Registration Authorities and Local Registration Authorities

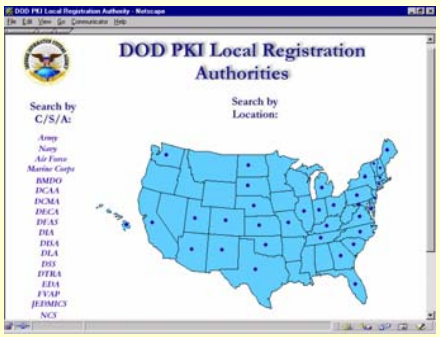
- **Registration Authorities (RA)**
  - **List of RAs can be found at**

https://iase.disa.mil/PKI/RA/ra.html



- **Local Registration Authorities (LRA)**
  - **List of LRAs can be found at**

https://iase.disa.mil/PKI/RA/lra.html



RA/LRA Training

- **Planned Training Dates**
  - **26 - 30 March**
  - **23 – 27 April**
  - **21 – 25 May**
  - **25 – 29 June**
- **An additional 16 hours of LRA training at Defense Security Service Academy (DSSA) each quarter**
- **Three (3) one week on-site training sessions are planned for C/S/As**
- **Attendees must coordinate registration for RA/LRA class with their respective C/S/A PKI representative**

https://iase.disa.mil/PKI/PKITrain.html

Application Support

- **Requirement Documentation:**
  - **DOD Class 3 Public Key Infrastructure Interface Specification, Version 1.2, dated August 10, 2000, draft**
  - **DOD CLASS 3 PKI Public Key-Enabling of Applications, dated September 29, 2000**
  - **DOD CLASS 3 PKI Public Key-Enabled Application Requirements V1.0, dated July 13, 2000**

    @ https://iase.disa.mil/documentlib.html#PKIDOCS
- **DOD PKI Testbed**
  - **Mirrors DOD PKI operational environment**
  - **Resides at the DISA Joint Interoperability Test Command (JITC)**
  - **Additional information at http://jitc.fhu.disa.mil**
- **Working with Defense Information Assurance Program on process for PK-enabling of applications**

External Certificate Authority (ECA) & Interim External Certificate Authority (IECA)

- An ECA is an entity authorized to issue certificates interoperable with the DOD PKI to non-DOD personnel
- What is an IECA?
  - Entity authorized to issue certificates interoperable with the DOD PKI to non-DOD personnel, for a period of one year
- Why an *Interim* ECA?
  - Need to work out best practices, understand technical and process issues, and understand and resolve legal concerns before finalizing ECA approach and processes.
- IECA Help Desk and Website
  - E-mail: pkieca@ncr.disa.mil
  - Phone: (703) 681-0287
  - http://www.disa.mil/infosec/pkieca

IECA Status Update

- **IECA Pilot extended one more year (until September 2001)**
  - **Operational Research Consultants (ORC)**
  - **Digital Signature Trust (DST)**
  - **VeriSign**
  - **General Dynamics**
- **DOD contributed to four programs/organizations for the purchase of IECA certificates**
  - **Medium Grade Services (MGS)**
  - **Joint Electronic Commerce Program Office (JECPO)**
  - **Defense Technical Information Center (DTIC)**
  - **Military Traffic Management Command (MTMC)**
- **Currently testing IECA Server Certificates**
- **Planning to transition IECAs to meet Release 3.0 requirements.**

The Way Ahead

- **Provide support to Common Access Card (CAC) Beta and Release 3.0**
- **Expand use of PKI on the SIPRNET**
- **Continue development of application enabling guidance and enabling templates**
- **Continue incremental releases of DOD PKI to improve product, service, and availability**
- **Envision seamless transition to Target**

Continue Satisfying The Warfighter Requirements!

Backup Slides

DOD PKI Working Groups

- **DOD PKI Certificate Policy Management Working Group:**
  - **co-chair - NSA - Gary Dahlquist gndahlq@missi.ncsc.mil**
  - **co-chair - DOD GC - Shauna Russell - russels@osdgc.osd.mil**
- **DOD PKI Business Working Group (BWG):**
  - **co-chair - NSA - Debra Grempler - DAGremp@missi.ncsc.mil**
  - **co-chair - DISA - Gilda McKinnon - McKinnog@ncr.disa.mil**
- **DOD PKI Technical Working Group (TWG):**
  - **co-chair - DISA - Adam Britt - britta@ncr.disa.mil**
  - **co-chair - NSA - Dave Fillingham dwfilli@missi.ncsc.mil**

Using the DOD PKI
An Example

The *I Assure* Advantage

http://www.disa.mil/D4/diioss/iachar.html

Key Points:

- **Contract supports up to TS / SCI security requirements**
- **7 year multi-award contract**
- **All tasks MUST BE competed, no follow-on work from previous contracts**

Most of the work awarded under this contract will be professional services, however,

…. ***the contract is structured to permit purchase of a full range of Information Assurance (IA) solutions, including the hardware, software and enabling products necessary to implement these solutions.***

The Math

9 Large Businesses
plus 2 Small Businesses
plus DISA
equals 1 Great Team

ARTEL INCORPORATED

CSC

SRA Software Research Associates, Inc.

VERIDIAN Trusted Solutions For Mission Critical Systems

PRAGMATICS, INC. "technical gateways to a practical tomorrow"

Carnegie Mellon Software Engineering Institute CMM Level 2+ Externally Certified

Litton TASC

Wang Government Services, Inc. A Getronics Company

ACS Defense, Inc.

LOGICON A Northrop Grumman Company

SAIC An Employee-Owned Company

EDS

Solutions-based: Contractors can tailor services and products for each task order proposal; Complements Enterprise Software Initiative: I Assure vendors can provide integration services for ESI products

Task Areas:

- **Policy, planning, process, program and project management support**
- **Standards, Architecture, Engineering and Integration support**
- **Solution Fielding / Implementation and operations**
- **Education, training, and awareness; certification and accreditation; and IA support**

DISA 'I ASSURE' - Employed the DOD PKI in the Paperless "Pre-Award" of Contract Process