

UNCLASSIFIED//FOR OFFICIAL USE ONLY



# Department of Defense PKI Use Case/Experiences

## PKI IMPLEMENTATION WORKSHOP

Debbie Mitchell  
DoD PKI PMO  
[dmmitc3@missi.ncsc.mil](mailto:dmmitc3@missi.ncsc.mil)

UNCLASSIFIED//FOR OFFICIAL USE ONLY



# Agenda

- ~~Current Statistics~~
- Program Enhancements (Otherwise knows as lessons learned...)
- New Milestones for PK-Enabling
- FIPS 201 Challenges



DoD Public Key  
Infrastructure



# Current Statistics...

- Common Access Cards (CAC) Issued – 10 M
  - More than 90% of target population has a CAC
  - 500,000 **software certificates** being used
    - 98% of DoD web servers have certificates
- PKI Certificates issued on NIPRNet – 22M+
- PKI Certificates issued on SIPRNet - 10000
  - All Software certificates
  - NSA is currently working on enhancements to the CAC for its use on SIPRNET
- Other holders of DoD PKI Certificates
  - Intelligence Community
  - CCEB Nations (5-Eyes)
- Typical CAC issuing time with PKI Certificates
  - 12-15 minutes
  - As many as 20,000 in a day



DoD Public Key Infrastructure



# Program Enhancements

DoD Public Key  
Infrastructure



# Robust Certificate Validation Service

- **Issue:** Real-time certificate validation needed to minimize bandwidth impact
- **Field RCVS Nodes**
  - Mechanicsburg
  - San Antonio
  - EUCOM
  - PACOM
  - CONUS (2-TBD)
  - SIPRNet
- **Operational Issues**
  - CRL Size
  - Rollout of OCSP Plugins





# Non-person Entity Certificates (i.e., Device)

- **Issue:** Need to Extend PKI to support a net-centric environment by enabling recognition and authentication of those entities that operate on/within our networks.
- **Currently Developing**
  - System Requirements Spec
  - Concept of Operation (CONOP)
  - Authoritative Naming Spec
- **Develop Authoritative Naming System**
- **Develop Registration Processes & Controls**
  - Certificate Expiration Notification
  - Determine Types of Devices To Be Supported
- **Develop Device Certificate Profiles**
- **Implement Support for Certificate Request Protocols (HW & SW)**
- **Field CAs for NIPRNet and SIPRNet**
- **Continue To Evolve PKI to Support Future Devices**



# Windows Domain Controller Certificates

- **Issue**: Need to support smart card logon (with CACs) in a Microsoft Network Environment
- Develop Policy
- Design Certificate Issuance Process and Profiles
- Establish Subordinate CA for Domain Controller Certificates
- Support for SIPRNet



# Automated PKI Monitoring

- **Issue**: Need capability to remotely monitor performance of key infrastructure components
- Develop Base Monitoring Functions
- Add Monitoring of Red Hat CMS
- Add Monitoring of Auto Key Recovery
- Auto Local Registration Authority Application
- Field at JITC
- Field at Chambersburg
- Field at Denver





# Government Control of PKI Applets (aka HAPKI)

- **Issue:** Need for the DoD to acquire control of the PKI Java applets that are downloaded to the CAC for performing PKI functions
- Develop CONOP
- Develop System Requirements Specification
- Design CAC To Support Multiple Global Platform Security Domains
- Design CAC To Only Accept Government Signed Applets
- Develop Applets Under Government Control and/or Review
- Establish Mechanism To Sign Government Applets and Load CACs
- Develop CAC Proof-of-Possession for IP Issued Certificates
- Relocate PKI Sensitive Functions From CAC Infrastructure To The PKI Infrastructure



# Bulk Revocation by Components

- **Issue**: DoD Components require a capability to efficiently revoke large numbers of certificates
- Develop Prototype
- Deploy in Operational Environment
- Develop Federated Database
- Deploy in SIPRNet



# Citizenship Information

- **Issue**: DoD relying parties have a requirement for citizenship information in certificates
- Determine Owner of Citizenship Information
- Determine Source of Citizenship Information
- Determine Usage Requirements for Citizenship Information
- Design System for Hosting Citizenship Information
- Implement Citizenship Information
- Develop Training for Collecting Citizenship Information



# Architecture Improvements

- Design and Implement Improvements To The Overall Architecture of The DoD PKI
- Architecture Improvements include:
  - Second Source Certification Authorities
    - Second Source Certification Authorities implement CA software from a second vendor to remove the dependency that the DoD currently has on a single vendor to support the DoD PKI
  - Automated Load Balancing for Issuance Portals (IP) and LRAs
    - Automated Load Balancing provides a load balancer between the CAs and the LRAs and CAC Issuance. By implementing a load balancing capability, LRA workstations and IPs could all be configured to access the load balancer, which would automatically route the request to an available CA



# Other Slated Enhancements

- Trust Relationships with External PKIs
- Group/role certificates
- Distribution of the DoD Root CA certificate to all subscribers and relying parties in a trusted manor
- Improvements of compliance audits
- Enhance archival process of DoD PKI objects
- Access to encrypted data
- Trusted Timestamp



# New Milestones for PK-Enabling

DoD Public Key  
Infrastructure



# Past PK-Enabling Guidance

- August 12, 2000
  - Updated DoD policies for development and implementation of a Department-wide PKI
  - Aligned PKI activities and milestones with those of the DoD CAC program
- May 17, 2001
  - Provided specific guidelines for the Public Key Enabling of Applications, Web Servers, and Networks for DoD
- May 21, 2002
  - Mandated CAC as primary token platform for PKI certificates
  - Adjusted milestone dates of two earlier memorandum





*THE FORCE IS WITH  
US*





# New Milestones Set for PK-Enabling Within the DoD Community

- The DRIVING FORCE:
  - JOINT TASK FORCE - GLOBAL NETWORK OPERATIONS (JTF-GNO) - Responsible for operation and defense of the Global Information Grid (GIG) framework for DoD
  
- JTF-GNO Actions:
  - Issued a WARNING ORDER (WARNORD)
  - Issued a COMMUNICATIONS TASKING ORDER (CTO)
    - Directed compliance with specified tasks
    - Provided dates for compliance, options for waivers, and percentages for completion within tasks by various deadlines



# All DoD Components Directed To:

- Provide **lessons learned** from CAC/PKI implementation efforts
- Complete **PKI training** for all System Admins
- Implement **SCL** to the NIPRNet
- Develop an initial plan for **email encryption** and **digital signature** using DoD PKI
- Allow only **certificate-based client authentication** to private DoD web-servers using certificates issued by the DoD PKI
- **Verify** CAC readers, middleware, and ensure CAC users' required information and certificates are correct



*FIPS 201*  
*CHALLENGES!*



# Comparison of CAC and PIV Certificate Usage

## CAC User Certificates

- Identity
  - Web client authentication
  - Document Signing
- Digital Signature
  - Email signatures
  - Smartcard Login
- Encryption
  - Encrypted email

## PIV User Certificates

- PIV Authentication
  - Web client authentication
  - Smartcard Login
- Digital Signature
  - Email signatures
  - Document Signing
- Key Management
  - Email encryption
- Card Authentication
  - Physical access control
- Card Management
  - Personalization
  - Post Issuance



DoD Public Key  
Infrastructure



# Alignment with Common Policy

- **Requirement**: January 1, 2008 - Legacy PKIs cross certified with the Federal Bridge have to assert common policy oids in certs
  - Aug 2005 - Established team to look at differences between DoD Certificate Policy and Federal Common Policy
  - Sep 2005 - Briefed Federal Bridge Policy Authority
  - Oct 2005 - Briefed Federal Certificate Policy Working Group
- Even though we are compliant with the Federal Bridge policy we aren't compliant with the Federal Common Policy
- There are some **Significant** care-about
- We're working with Judy Spencer and the federal community to harmonize policies and try to come to some mutual agreement for a way forward.
- Federal entities operating legacy PKIs need to perform a similar analysis



# Other PIV Challenges

- Certificate Profiles – changes to our existing ones
  - Issuer Signature Algorithm
    - Phased approach for changes
  - CRL Distribution Point
  - Subject Public Key Information
  - AIA
- Need additional certificate profile – Card Issuer Certificate
- Foreign National Identity Proofing
  - Within the US
  - OCONUS
  - Ties into our Citizenship initiative