

Interagency Advisory Board

Meeting Agenda, Wednesday, December 7, 2011

1. **Opening Remarks** (*Mr. Tim Baldrige, IAB Chair*)
2. **FIPS 201-2 Goes Mobile** (*Bill MacGregor, NIST*)
3. **Logon to Google Apps Using NASA Issued PIV** (*Tim Baldrige, NASA, IAB Chair*)
4. **Implementing PKE for JPAS** (*Maxwell Funk and Autumn Crawford-Grijalva, DoD*)
5. **Provisioning PACS using the GAMS** (*Bill Lin, GSA*)
6. **Closing Remarks** (*Mr. Tim Baldrige, IAB Chair*)

Implementing Public Key Enablement for the Joint Personnel Adjudication System (JPAS)

Presented By: Maxwell Funk & Autumn Grijalva



Serving Those Who Serve Our Country



DMDC's Mission

DMDC is the DoD enterprise human resource information source, providing secure services and solutions to support the Department's mission.

Strategic Goals

1. Promote DMDC's core values in everything we do
 - a. Do the right things – do things right
 - b. People Focused
 - c. Extraordinary results through customer service
 - d. Agile, quick, creative, and responsive
 - e. Respect privacy/secure information sharing
 - f. Success through teamwork
2. Be the leader in joint information sharing and decision support on DoD human resource issues
3. Be the central source to identify, authenticate, authorize and provide information on personnel during and after their affiliation with DoD
4. Be the one, central access point for information and assistance on DoD entitlements, benefits and medical readiness for uniformed service members, veterans & their families
5. Expand Electronic Government, in the broadest sense, across the DoD and its partners



JPAS General Information

- Serves as a master repository that performs comprehensive personnel security management of all DOD employees, military personnel, civilians and DOD contractors

- **Composed of two sub-systems:** Joint Adjudication Management System (JAMS) and Joint Clearance and Access Verification System (JCAVS)

- **JPAS Stats** - On average JPAS has approx.
 - 60,000 active users with differing access-levels
 - 2 million transactions a day
 - 750 concurrent users at any given time
 - Peak hours almost 3,000 concurrent users
 - Total number of hits 30 million hits (3 servers each with approx. 10 million hits) with an average of 1.1 second response time
 - JPAS Support Team consists of 63 HP/ES employees
 - JPAS Call Center *(under DSS) has approx. 50% of its calls are JPAS related*



PK-Enabling Initiative

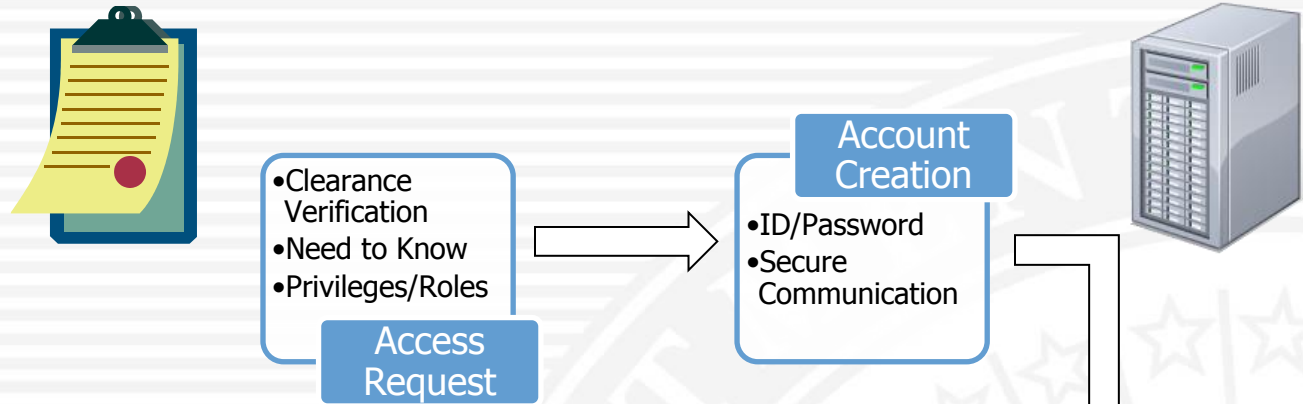
- **Phase I (Completed in January 2011):**
 - JPAS was CAC-Enabled as of January 15, 2011
 - Coordination between DSS, DMDC, USDI, and F5
 - Able to use Username/Password and CAC for JPAS application login

- **Phase II (Completed in August 2011):**
 - Successfully testing PK-Enablement with Pilot Group
 - July 14-28, 2011
 - 18 Companies/Agencies/Departments with over 50 users
 - Type of Participants: 3 Govt, 9 Sm/Med; 6 Large
 - Coordination between DSS, DMDC, USDI, DHRA, DoD CIO, & Industry
 - Able to use Username/Password, CAC, PIV or PKI (ECA) for JPAS login

- **Phase III (Scheduled for Jan 21, 2012):**
 - Eliminating Username/Password login capability
 - Ability to use CAC, PIV and/or PKI (ECA) for JPAS login

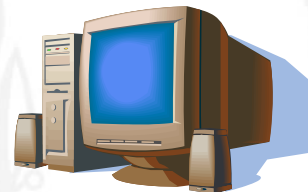
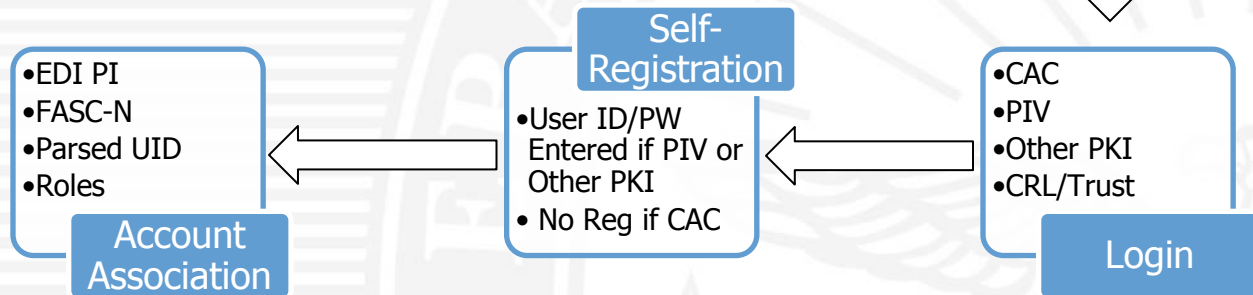


JPAS Access



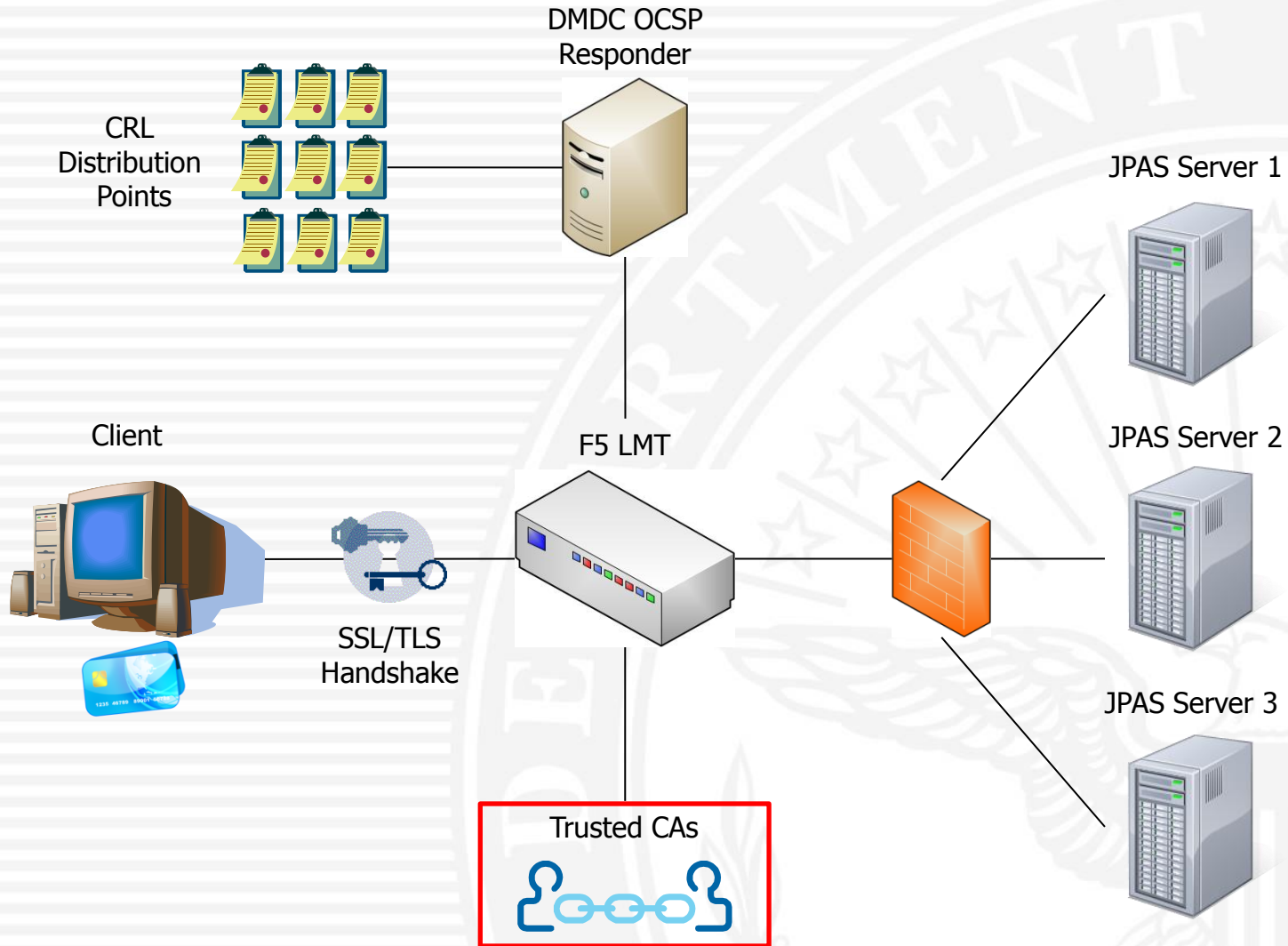
Authorization

Authentication





How do we Authenticate?





PKI and Certificate Specifics

- **Direct Trust Model was selected for this implementation which was dependent upon:**
 - DoD Approved PKI Providers – manually updated on a periodic basis via the DISA IASE website:
 - <http://iase.disa.mil/pki-pke/interoperability/index.html>
 - DoD Approved Policy OIDs for medium token and hardware devices – necessary for uniquely identifying certain entities
- **Unique Identifier Parsing**
 - DoD Credentials – Policy OID of 2.16.840.1.101.2.1.11.9, UID is EDIPI
 - Federally Issued Credentials – Policy OID of 2.16.840.1.101.3.2.1.3.13, UID is FASC-N
 - “Other” DoD Approved Credentials – All non CAC/PIV policy OIDs, UID is parsed from Subject Distinguished Name, Subject Alternate Name, Issuer Distinguished Name and Credential Serial Number



PK-Enabling Lessons Learned

1. The direct trust model has increased the level of effort and implementation time related to application maintenance and configuration to include credential revocation... Independently mirroring approved lists
2. Minimal guidance on identifying and parsing unique identifiers from user credentials especially from external approved PKIs (not CAC or PIV) for the purpose of account association... Custom Scripts
3. Clearly defined policies need to be communicated when implementing change... Populations and CAC usage
4. Properly documented policies, user system configuration and PKI education needs to be available especially for the non-technical folks... Step-by-Step FAQs



QUESTIONS???



FAQs available @ <https://www.dmdc.osd.mil/psawebdocs/docPage.jsp?p=JPAS>