Identity and Access Management for the Extended Enterprise

Paul Grant
Special Assistant for Identity Management and External Partnering
DoD CIO
Paul.Grant@OSD.Mil

Create an Information Advantage for our People and Mission Partners
Value Proposition is The Context

- Strong IdAM are Key to Info Sharing in Cyber Space and in Physical Access to Sensitive Locations

  - Identity Management
    - Who are you?
    - DoD Accepting eAuthentication Level 4
      (aka FBCA Med-HW and Above)

  - Access Management
    - Enforcement of Sharing Policies
    - Based up Resource Attributes

- Exploit Investments in Capabilities, Standards, Policies/Rules
  - Three Classification Fabrics
  - Extended Enterprise (ISE) (Particularly 24/7 Partners)
  - Unanticipated & Less Mature Mission Partners
Where Are We Today

**Major Identity Management Thrusts:**
- Federal Identity Credentialing Committee, FPKIPA
- DoD-DNI Joint Efforts on the Classified Fabrics
- CNSS for National Security Systems

**Major Access Management Thrusts:**
- Federal Backend Attribute Exchange (derivative of HSPD-12)
- DoD-DNI Joint Efforts on the Classified Fabrics
- IC/DoD Authorization & Attribute Services Tiger Team
  - Advancing ABAC/ICABAAD

**DoD is Member of the Federal IdAM Federation**

**External Partners are Following Our Lead With Their Investments**
Expansion of DoD Approved External PKI
Memo of July 22, 2008

The following PKIs are approved for use with DoD information systems upon successful completion of interoperability testing.

- FBCA member PKIs cross certified at Medium Hardware or High Assurance Levels
- PKI members of other PKI Bridges that are cross certified at FBCA Medium Hardware or High Assurance Levels
- PKIs that Assert the Federal PKI Common Policy Medium Hardware or High Assurance Levels
- Also, Approved Foreign, Allied, Coalition partner and other External PKIs (described in attachment to memo)
Identity Federations

**Shared Service Providers**
- VeriSign, Inc.
- Cybertrust
- Operational Research Consultants, Inc.
- The Department of the Treasury
- Entrust Managed Services
- Exostar LLC
- U.S. Government Printing Office

**Cross Certified:**
- D of Defense
- D of Justice
- Gov Printing Office
- D of State
- D of Treasury
- USPS
- Patent & Trademark Ofc
- DHS
- Versign
- Wells Fargo
- State of Illinois
- DEA CSOS
- ACES (Identrust & ORC)
- DoD ECAs

**Participants (TSCP)**
- Boeing
- Lockheed Martin
- Northrop Grumman
- Raytheon
- EADS/Airbus

**CSP:**
- Exostar, SITA, ARINC

**Certipath (Aero/Def)**

**PKI Bridges**
- Exostar LLC
- SITA
- ARINC

**Fed Bridge Status:**
http://www.cio.gov/fpkia/crosscert.htm

**SAFE (Bio/Pharma)**
- Cross Certified:
- Commercial Best Practices Level
- Interoperable & test level:
- HE Bridge dormant

**Other TSCP:**
- BAE Systems
- Rolls Royce
- Finmeccanica

**Higher Education**

**Pending:**
- MoDUK

**Participants:**
- AstraZeneca
- Bristol-Myers-Squibb
- Genzyme
- GlaxoSmithKline
- Johnson & Johnson
- Merck
- Nektar
- Organon
- Pfizer
- Procter & Gamble
- Roche
- Sanofi-Aventis

**Red:** eAuth Level 4
**Memo- July 22, 2008**

**Jasuary 2009**

**PIV Fielding Status:**
http://www.idmanagement.gov/drilldown.cfm?action=agency_hspd12_impl_rpt
Interoperability Testing of Approved External PKI
Memo July 22, 2008

- **Purpose**
  - Ensure that certificates are technically interoperable with DoD systems, and certificate revocation information can be obtained by DoD systems

- **Content**
  - Tests interoperability using Direct Trust method
  - Tests interoperability using Cross-Certification method
  - Use cases: Client Authentication to a Generic Web Site
    Digital Signing and/or Encrypting Email

- **Status**
  - DISA is scheduling qualified* Certipath member PKIs for JITC testing began at the end of September 2008
  - Developing Interoperating MOA for non-Federal external PKIs
    - Internal DoD legal requirement
    - Covers Responsibilities, Termination of interoperating, Liabilities, etc.

*PKIs from other PKI Bridges, cross certified with the FBCA at the Medium Hardware level of Assurance
JITC Interoperability Testing

Test Plan – Developed in testing between JITC and DoS

http://jitc.fhu.disa.mil/pki/pke_lab/partner_pki_testing/partner_pki_status.html

- Federal Partner Test Schedule
  - Complete – State, Treasury, Justice, Transportation, EPA, NOAA,
  - Discussions started with Others

- Other Bridge Testing (Certipath)
  - Enterprise   Sponsor                     Test Start Date
    Boeing       Army FCS            Complete
    Lockheed     Army FCS            Complete
    Northrop G   Navy SUPSHIP        Complete
    Raytheon     Army FCS            Complete
    UAL (Exostar) USAF Exec Fleet    TBD
Recent and Emerging Successes

- DoD Approved External PKI List Extended
- Joint Lessons Learned Information System
- Future Combat System Collaboration
- Security Cooperation Information Portal (Foreign Military Sales)
- Synchronized Predeployment and Operational Tracker (SPOT)
- Defense Industrial Base Critical Infrastructure Protection
Partner Expectations

Partners Can Expect

- Strong Credentialing of our Employees (Authentication)
- Access to Our Public Key Encryption Certificates
- Access to Robust Certificate Status Service
- Service Access to Attribute Service (Authorization) – Future

Expectations from Partners

- The Same as From Us for 24/7 Partners – Plus
- Binding Federation Governance Agreement(s) / Rules that Establish and Maintain Trust
- Consistency on Unanticipated & Less Mature Partners
Summary

Strong Identity and Access Management Are Key to Information Sharing and Collaboration

- We Need a Clear, Concise, Consistent, Published Course for Ourselves and Our Mission Partners.

- Mission Partners are Fielding Strong Identity & Managed Credentials (PKI) as well as Identity Federations

- Progress Continues in IdAM Expansion toward Consistent Dynamic Policy-Based Sharing
Backup
Credential Service Providers (at eAuth-4) for External Partners (non-Federal)

- CSPs on Fed Bridge at eAuth-4
  - http://www.cio.gov/fpkia/crosscert.htm
  - Verisign
  - Wells Fargo

- CSPs on Other Bridges at eAuth-4 (Certipath only today)
  - Exostar
  - ARINC
Status, Fabric by Fabric

- **TS/SCI Fabric**
  - Environment: Homogeneous
  - Lead is DNI/CIO
  - PKI: IC PKI available for authentication by US
  - Federation: Among IC Certificate Authorities (CAs) and Commonwealth CAs
  - Notes: Enterprise services for central identity management, Enterprise attribute, authentication, and authorization services

- **Secret Fabric**
  - Environment: More diverse
  - Lead: CNSS (DoD CIO Chairs)
  - PKI: Minimal, CNSS PKI WG Recommendations for SAB. DoD implementing in FY09
  - Federation: Commensurate with CNSS Authority (DoD CIO Chairs)
  - Notes: No centralized Identity Mgmt, Therefore immature IdAM environment at this time

- **Unclassified Fabric**
  - Environment: Extremely Diverse, Complex Environment
  - Lead: No Single Lead; Must Cooperate & Federate (DoD & Exec Branch are Heavies)
  - PKI: 24/7 Partners Adopting eAuthentication Level 4
  - Federation: Federal Identity & Access Management Federation is Central
  - Notes: Multiple enclave-specific IdAM services, Most Partners Not Yet Mature
Key Conceptual Threads in DoD Net-Centric Information Sharing

- **Extended Enterprise**
  - All Internal and External Participants Required for Mission Success
  - Facilitates Collaborative and Coordinated Decision Making
  - Shared Situational Awareness and Improved Knowledge

- **Federation**
  - Autonomous Organizations Operating Under a Common Rule Set for a Common Purpose
  - Legally Binding Framework Policies, Standards and Protections to Establish and Maintain Trust

- **Information Mobility**
  - Dynamic Availability of Information.
  - Enhanced or Impeded by Culture, Policy, Governance, Economics and Resources and Technology and Infrastructure

- **Trust / Trustworthiness**
  - Cornerstone of Information Sharing is Trust in Partner Enterprises
  - Trusting Policies, Procedures, Systems, Networks, and Data

**Threads permeate all Information Sharing Activities**
IdAM Collaboration

- DoD / IC
  - DoD/IC PKI Tiger Team
    - Coordinate and align on hardware authentication solution
    - Develop comprehensive PKI solution for our mission partners
  - DoD/IC Authorization and Attribute Services Tiger Team (AATT)
    - Co-Chairs: NSA and DOD/CIO
    - Advance Dynamic Policy-Based Sharing Capabilities
  - Cover Tiger Team
    - Provide recommendations on the use and protection of identities

- Federal (Created by OMB and Federal CIO Council)
  - Federal Identity Credentialing Committee
  - Federal PKI Policy Authority
  - HSPD-12 Executive Steering Committee
  - eAuthentication Executive Steering Committee
Identity and Access Management

Unclassified Sharing

- **Internally**
  - Operations - Mission & Business
    - Strong Id Proofing & Vetting (eAuth Level-4 & CAC/PIV)
    - Static ACL and limited ABAC (internally)
  - Non-CAC/PIV Holders (e.g., Family Accounts)
    - eAuth Level 2 or Level 3 Credentials
    - Limited functionality – Bounded privileges

- **External Partners**
  - 24/7 Partners - eAuth Level 4 and static ACL
  - Unanticipated & Less Mature Partners
    - Situational Dependency
    - Under Development for controlled functionality / privileges

- **Partner Expectations**
  - Strong Credentialing of Employees (Authentication)
  - Access to Public Key Encryption Certificates
  - Access to Robust Certificate Status Service
  - Service Access to Attribute Service (Authorization) – Future
  - Binding Federation Governance Agreement(s) / Rules(s) that Establish and Maintain Trust
  - Consistency on Unanticipated & Less Mature Partners

**A Responsibility to Provide**
Dynamic Attribute-Based Access Management is Policy Compliant Information Sharing

Interface #1: Identity Management
- Identity Management
- Credential Management
- Attribute Management
- Audit Management

Interface #2
- Digital Policy Management
- Configuration Management
- Metadata Management

Policy Enforcement Point (PEP)
Policy Decision Point (PDP)
Policy Store

Environmental Factors (e.g., DEFCON, INFOCON, Etc.)

Crypto Key Mgt

Authenticate

Resource

Interface #2