Department of Energy
Identity, Credential, and Access Management (ICAM)

Cyber Security Training Conference

Tuesday, May 18, 2010

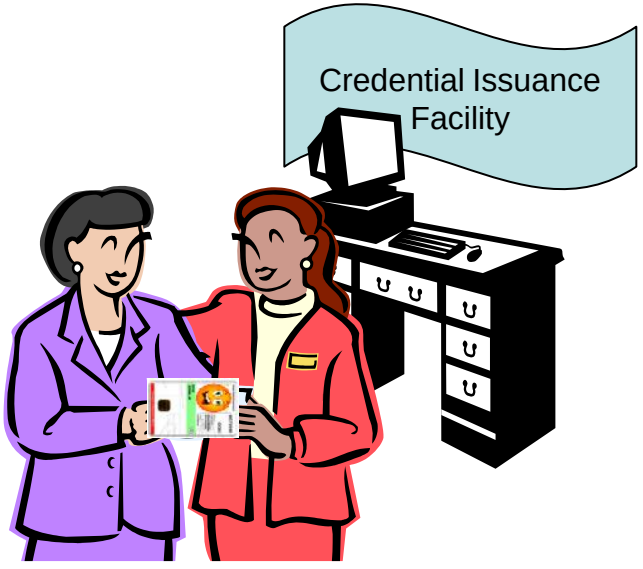
Announcement

- LACS Birds-of-a-Feather Session
  - Logistics
    - Wednesday, May 19, 2010
    - 9:30 AM – 11:30 AM EST
    - Room A708
  - Focus: LACS ONLY!
    - LACS implementation experiences, lessons, questions, challenges, etc
  - Everyone is welcome
- Science Identity Federation (Risk Management Track)
  - Logistics
    - Tuesday, May 18, 2010
    - 4:00 PM – 5:00 PM EST
    - Room A704
  - Focus
    - Ties into NSF/NIH InCommon Federation
    - Federated identity solution for Level 1 authentication

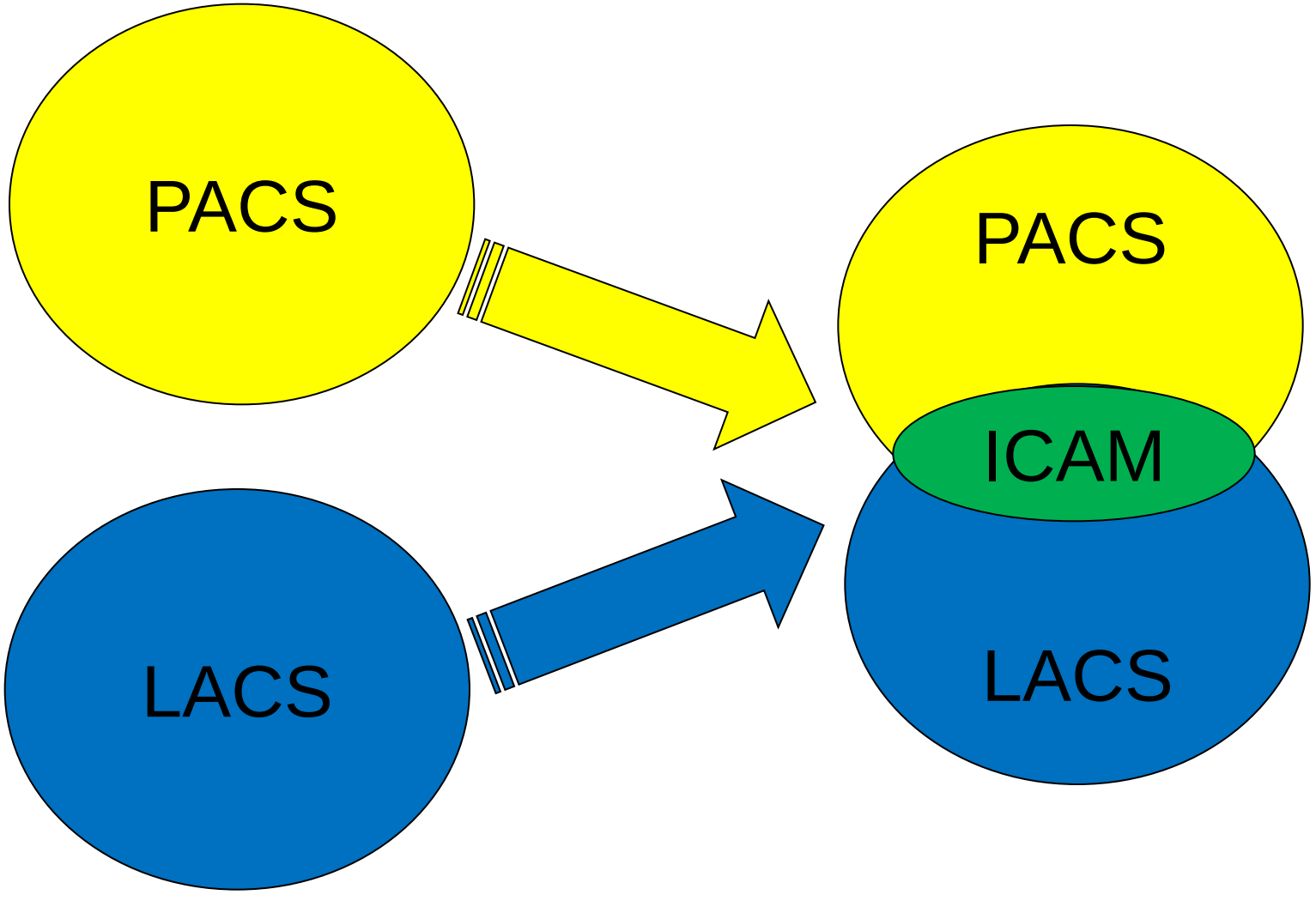
Slight Change of Focus

HSPD-12

ICAM
Identity, Credential, & Access Management



Paradigm Shift



DOE Activities

- DOE/NNSA HSPD-12/ICAM Workshop
  - March 2-4, 2010 – San Antonio, TX
  - LACS & PACS community together in one forum
- NA-1 Memo (15 March)
  - “Inconsistent approaches to physical and logical security are inefficient and costly, increasing the risks for compromise.”
  - “Successful implementation of HSPD-12 and Identity, Credential, and Access Management (ICAM) will improve the security and interoperability of the Nuclear Security Enterprise (NSE)”
- Cyber Security Governance Council Representatives
  - ICAM Governance model proposed
    - DOE ICAM Program Office
  - Meeting: 15 April 2010
  - Coordination and approval of ICAM documentation
- DOE LACS Plan
  - Draft updated per Field review
- DOE ICAM Approach
  - Consensus-based document on implementing ICAM
  - Executive Level: May 2010
  - Detailed Level: July 2010
- PACS/LACS Pilots
  - HQ and other sites
- DOE PIV Middleware Focus Group
  - DOE-wide group
  - Standard middleware for Windows Platform
  - Recommendation to Cyber Security Governance Council Representatives by 15 June

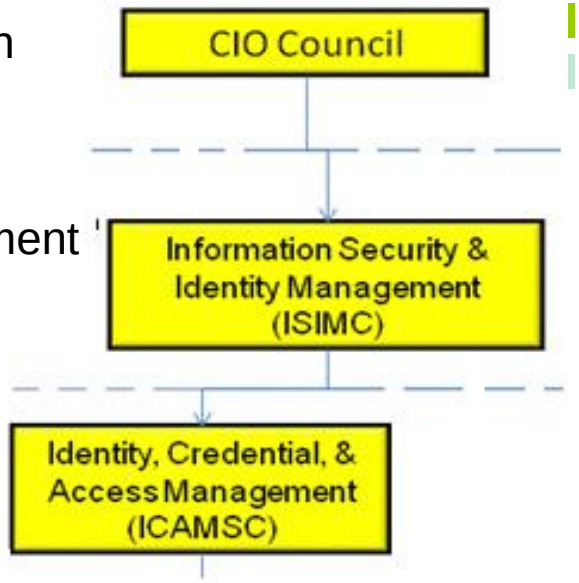
Office of the
Chief Information Officer

Identity, Credential, and Access Management (ICAM)

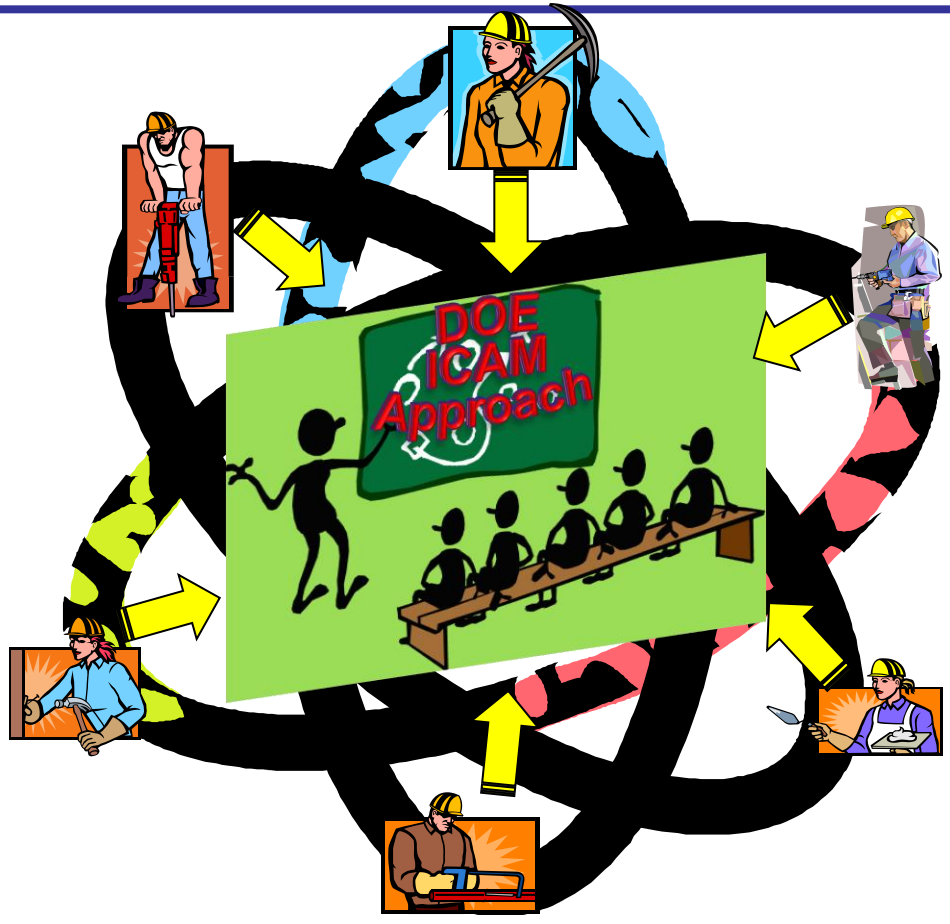
- What is ICAM? It is the intersection of:
  - Identity Management:
    - A combination of technology, rules and procedures for assigning attributes to a digital identity, associating the digital identity to an individual, and managing the digital identity throughout its life cycle.
  - Credential Management:
    - The management of the lifecycle of a credential, which is “an object that authoritatively binds an identity to a token possessed and controlled by a person.” (sp 800-63)
  - Access Management:
    - The management and control of how individuals are granted logical access to an IT network, system or application and physical access to physical locations such as a building, parking lot, garage, or office.
- Why ICAM?
  - Holistic approach for government-wide identity, credential and access management initiatives that support access to federal IT systems and facilities
  - Prevent unauthorized access to federal IT systems and facilities
  - Authoritative enterprise view of identity that can enable application and mission-specific uses

ICAM Governance

- Federal ICAM Subcommittee (ICAMSC)
  - Consolidated HSPD-12, Federal PKI and E-Authentication initiatives
  - Foster effective government-wide identity and access management
  - Ensure alignment across all identity and access management activities that cross agency boundaries
- Federal ICAM Roadmap
  - www.idmanagement.gov
  - Released November 2009 by ICAMSC
  - ICAM Segment Architecture
    - As is:
      - application/system specific, stove-piped implementation of establishing and managing identity and credentials for access
    - Target:
      - enterprise digital identity established and managed by authoritative systems, which can be leveraged within the organization and across agencies for physical and logical access
  - 81 Milestones
    - 42 Milestones for Agencies
    - FY10, 11, & 12
- Tracking
  - ICAM Template
  - Annual FISMA Report



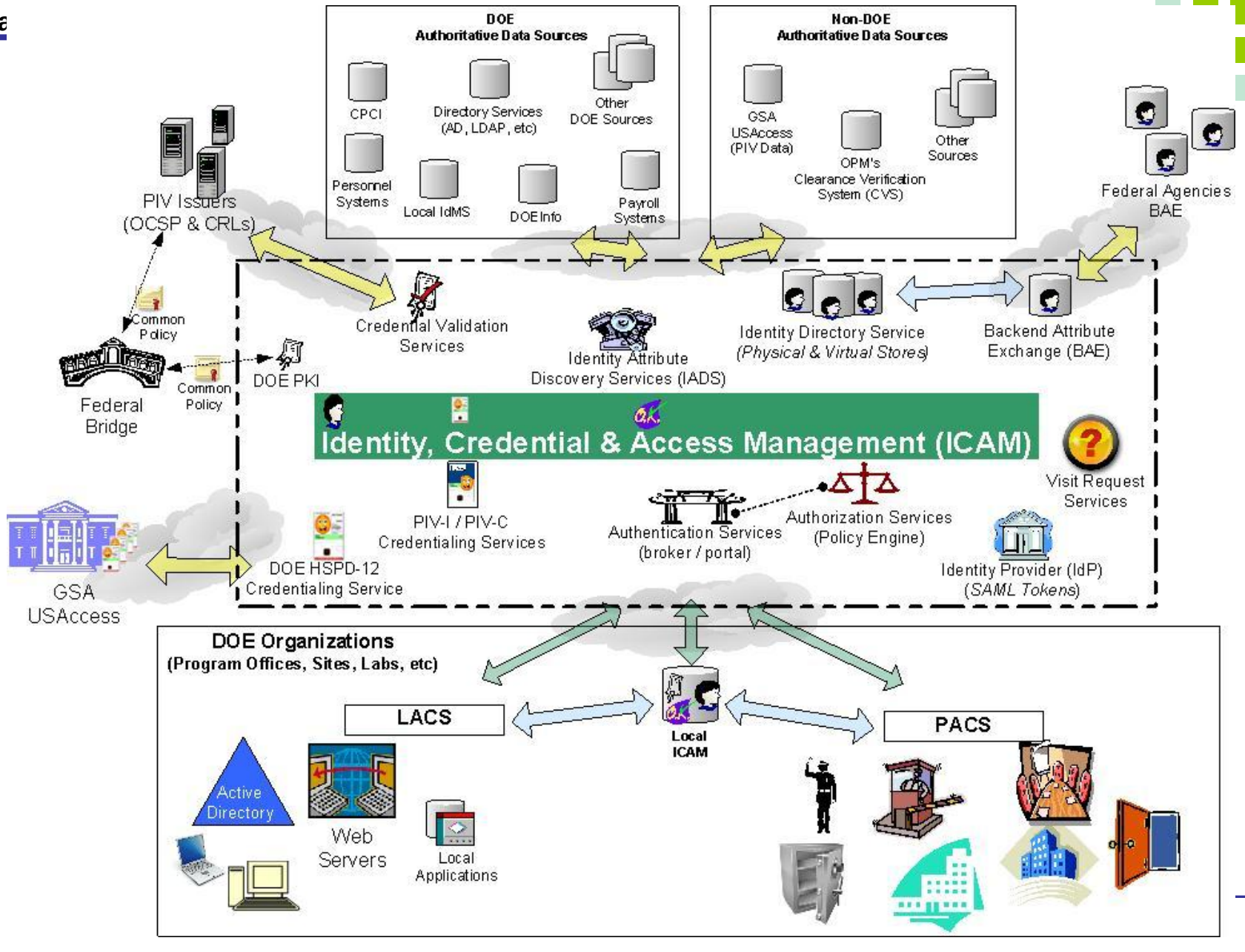
Department Approach



- ICAM Roadmap Milestones
  - (PACS, 7.2) Adopt an agency-wide approach to managing physical access that links individual PACS via a federated network wherever possible. (6/30/2010)
  - (LACS, 8.1) Adopt an agency-wide approach to managing logical access that links individual applications to a common access management infrastructure wherever possible. (12/31/2009)

Office of the
Chief Informa

DOE ICAM Approach



High-level ICAM Approach Targets

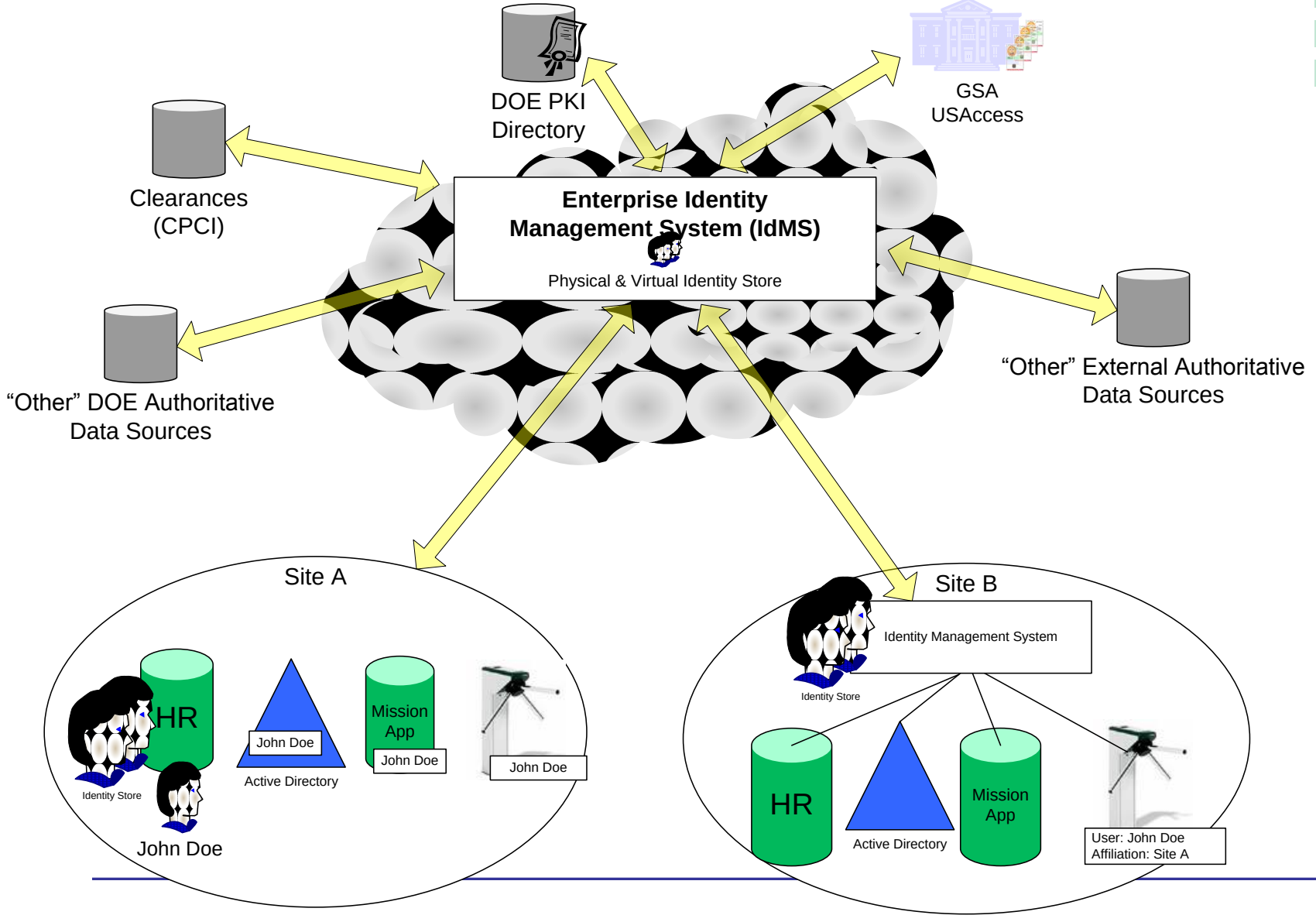
- Short term (FY10/11)
  - Domain Logon (feds and contractors)
    - Readers ($15) and Middleware ($10)
  - HSPD-12 Repository
    - CFO initiative (30 Sep)
  - PACS using HSPD-12 credential
    - Interoperability proof
- Mid term (FY11/12)
  - Identity Management System
    - CFO initiative
  - Enterprise authentication service
    - HQ Applications
  - PACS/LACS using IdMS for data
  - Credential Validation Services
    - OCSP and CRLs
  - Credential Issuance Service
    - HSPD-12 and PIV-I
- Long term (FY12/13)
  - Enterprise ICAM
  - Local ICAM
  - Automated Workflows
  - LACS/PACS for field

ICAM Key Services & Elements

- Identity Directory Services
  - DOE HSPD-12 Credential Repository
- Credential Validation Services
- PKI
- Authentication & Authorization Services
  - Identity Provider (IdP)
- Privilege Management

Office of the
Chief Information Officer

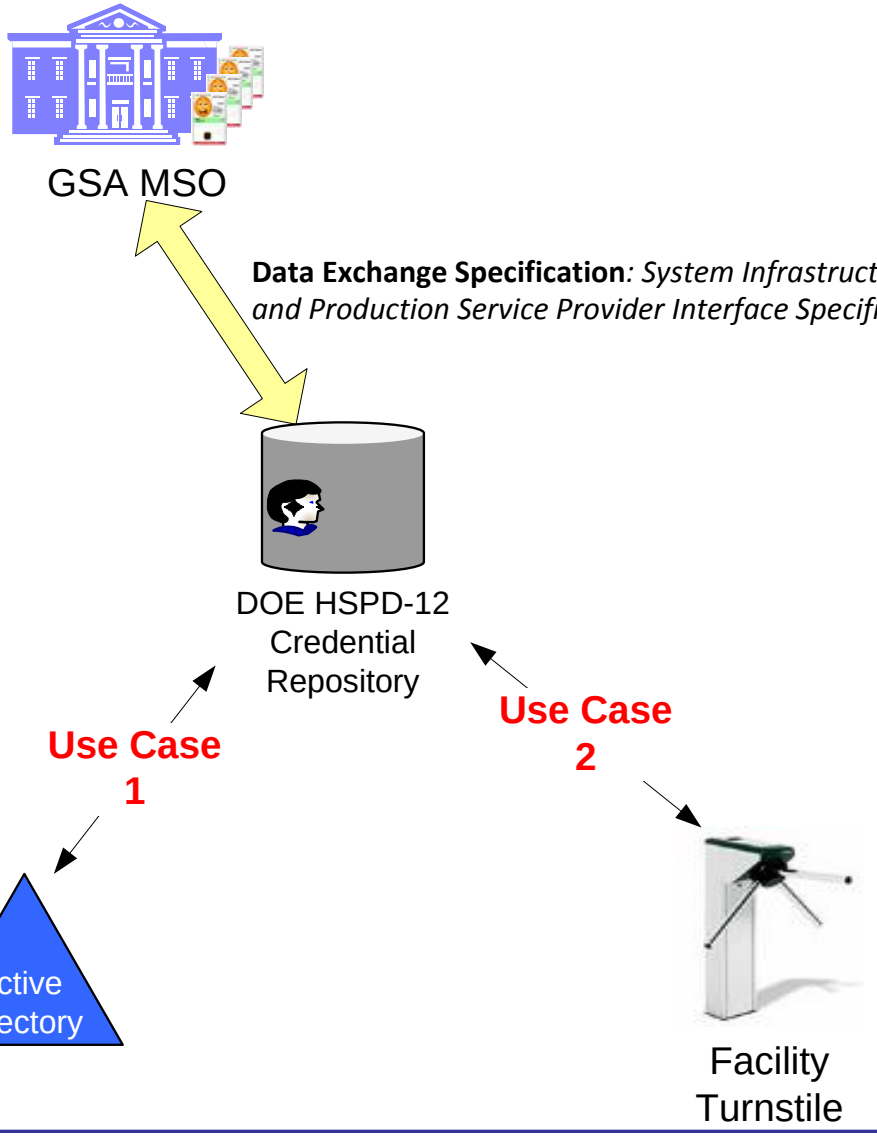
Identity Management System



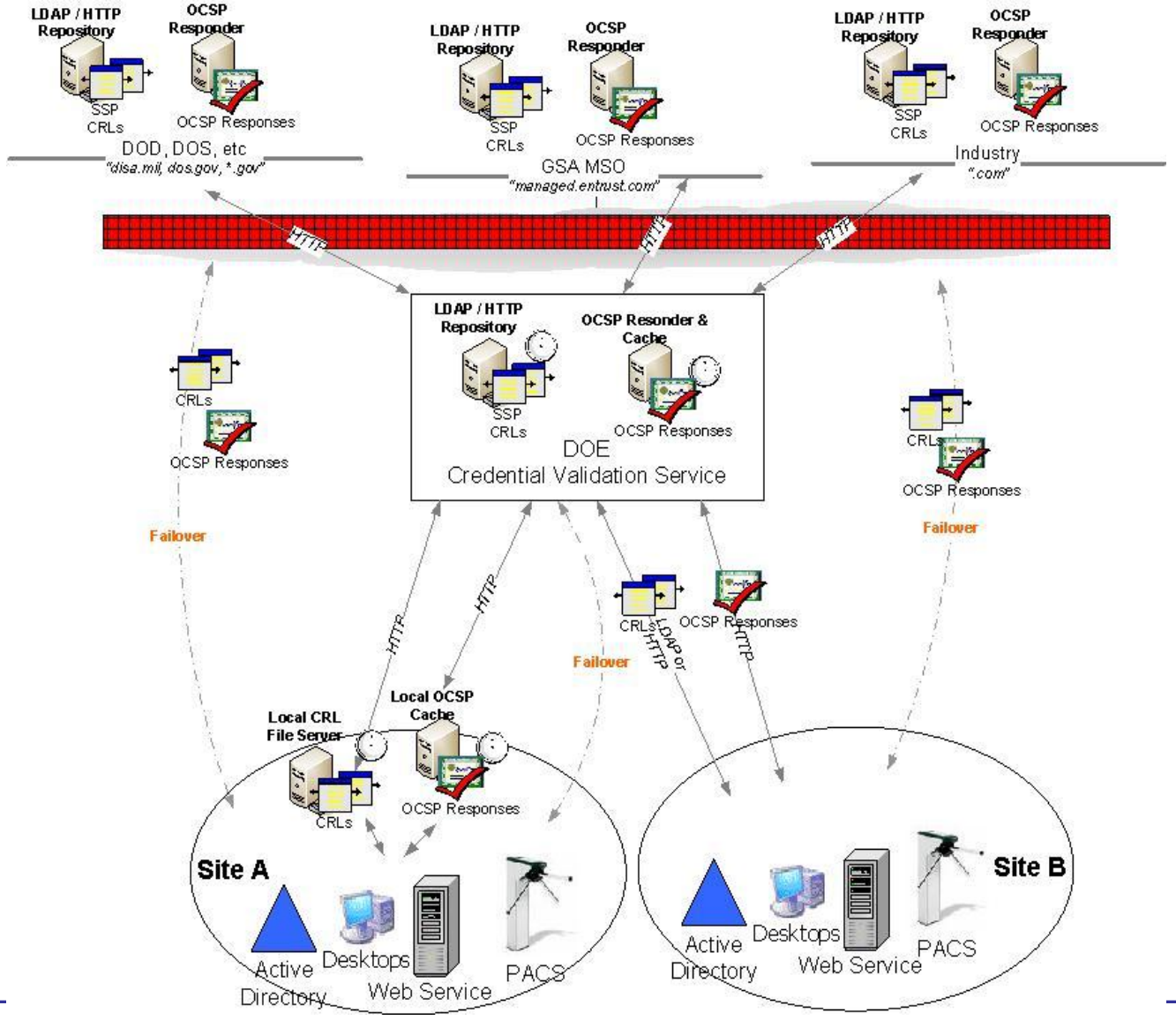
Office of the
Chief Information Officer

HSPD-12 Credential Repository

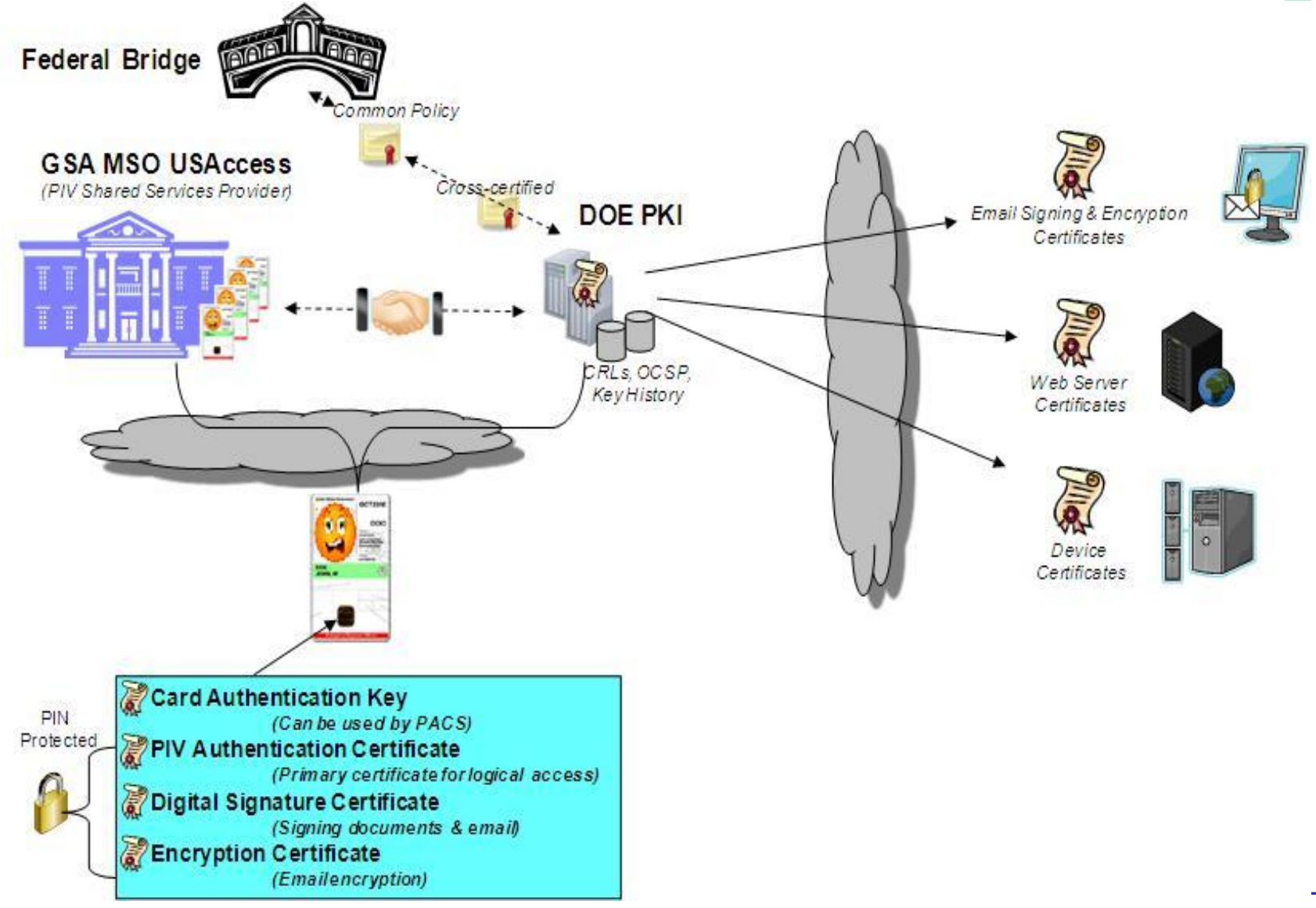
CF-40 Initiative In-Progress



Credential Validation

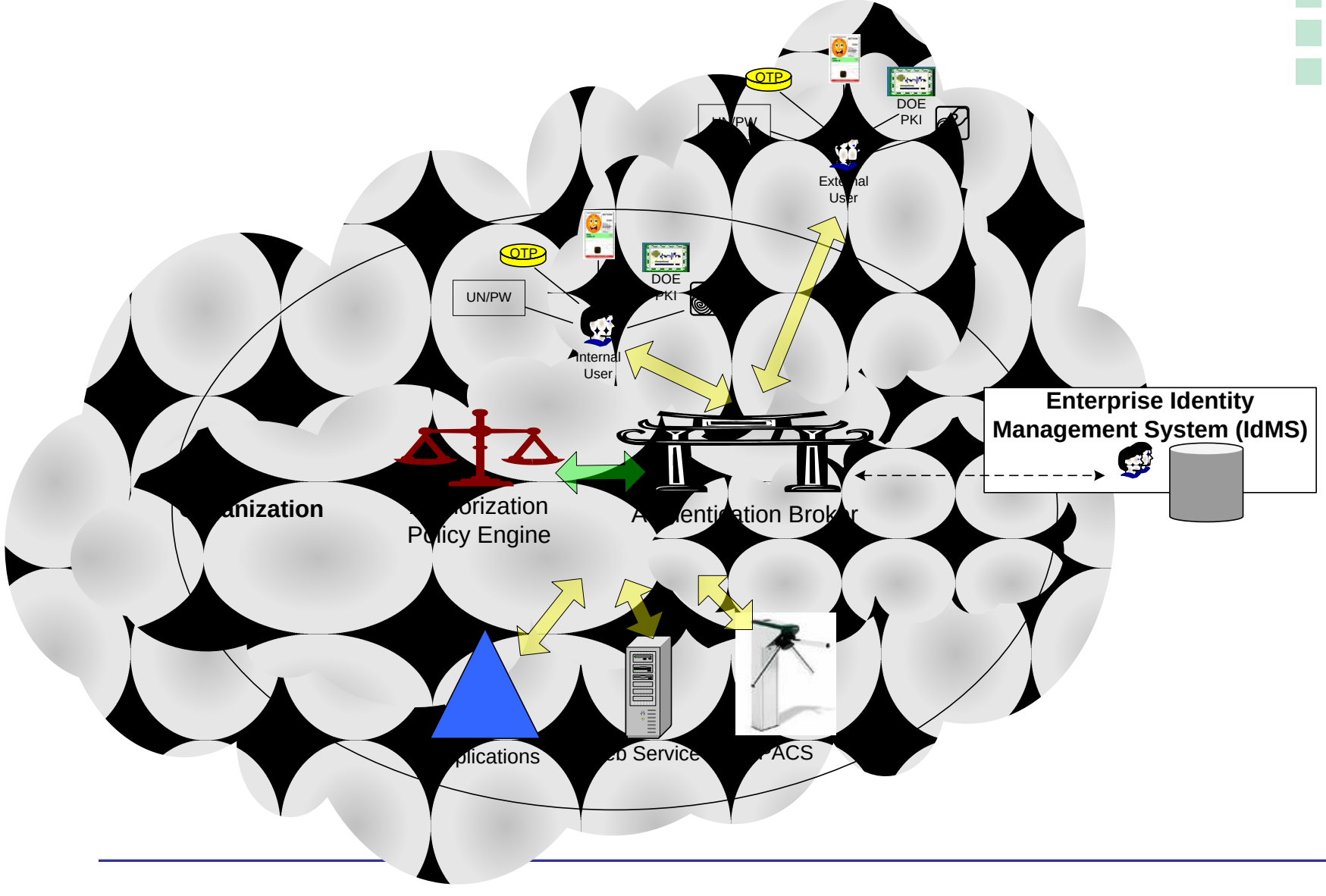


PKI


Federal Bridge
Common Policy
GSA MSO USAccess
(PIV Shared Services Provider)
Cross-certified
DOE PKI
CRLs, OCSP,
Key History
Email Signing & Encryption
Certificates
Web Server
Certificates
Device
Certificates
PIN
Protected
Card Authentication Key
(Can be used by PACS)
PIV Authentication Certificate
(Primary certificate for logical access)
Digital Signature Certificate
(Signing documents & email)
Encryption Certificate
(Emailencryption)

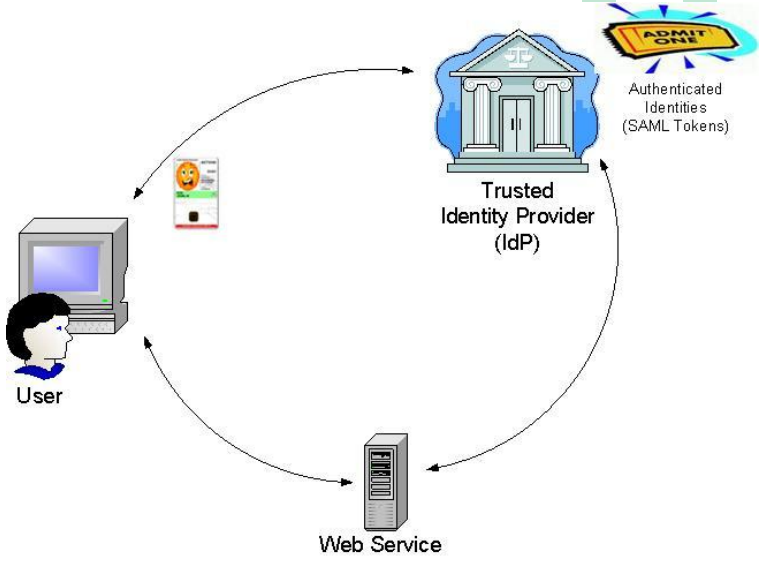
Office of the
Chief Information Officer

Authentication & Authorization

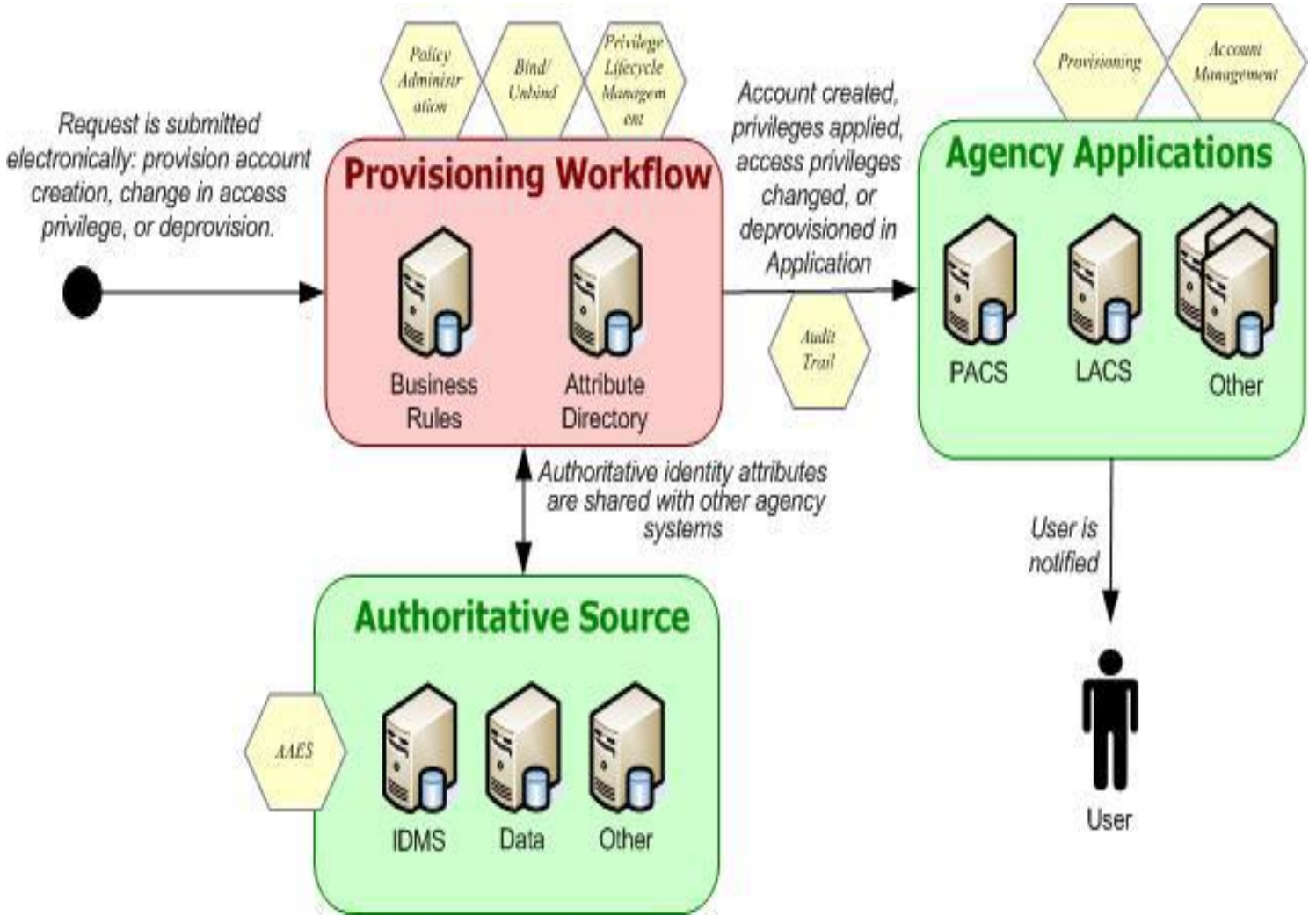


Identity Provider (IdP) "Generalized Concept"

- The IdP authenticates the user and creates a SAML Token
  - The IdP is configured with the types of authentication credentials to accept to include, OpenID, CardSpace, UN/PW, HSPD-12 credentials, and others.
- The SAML Token is provided to the user and the web service provider
  - The SAML token provides identity information about the user as well as what type of credential the user authenticated (a.k.a. Level of Assurance per M-04-04)
- The web service provider consumes the SAML Token and makes an authorization decision
  - Web service provider may provide different levels of privileges based on the level of assurance of authentication conveyed in the SAML token
- The user provides the same SAML Token (unless it has expired) to access other web service providers that recognize (or "Trust") the IdP.



Privilege Management



Office of the
Chief Information Officer

ICAM Success Story… NASA

- Population: 20,000 Feds | 55,000 Contractors | 25,000 Others
- Provide Central Authentication and Authorization (A&A) Service
  - PIV-enable the A&A service
  - Applications integrate with the A&A service, not directly to PIV
- A&A Service supports credentials at all levels of assurance
  - Applications can use mixed sets of credentials according to system needs and users' capabilities
  - Users get Single Sign-on benefit
- Status
  - Smart Card Logon: 81%
  - NASA Account Management System (NAMS) Integration: 70%
  - Authentication Integration: 21% (complete Sep 2011)
- Benefits today
  - Smartcard login to the desktop, then get to over 300 applications without re-logging in
  - Any NASA worker can visit any NASA Center and get pre-authorized access to any building/room
  - Ensure on a person-by-person basis that those who need IT security training have taken it
  - Provide "Basic Level of Entitlement" access to IT systems based on Identity attributes
  - Initiate "Close Account" processes on 70% of our IT assets when someone leaves
- Benefits tomorrow
  - Establish a non-PIV smartcard for use by temporary workers and others
    - Allows us to lock IT systems down to smartcard-only
  - Assign a Level of Risk to each Access role in our IT systems
    - Automatic comparison of Level of Risk of the Asset to Level of Confidence in a person
    - Allows early access to low-risk systems, while protecting our higher-risk systems
  - Link training requirements to each Access role
    - Automatic check against our training system to ensure proper training for the role has been completed

What's next

- DOE ICAM Approach
  - Department collaboration
- Garner support for enterprise services to facilitate local implementations
- Collaboration
  - DOE PACS Wiki: https://spaces.kcp.com/display/doepacs
  - DOE LACS Wiki: https://spaces.kcp.com/display/doelacs
  - DOE LACS ListServ: doelacs@vm1.hqadmin.doe.gov

- LACS Birds-of-a-Feather Session
  - Logistics:
    - Wednesday, May 19, 2010
    - 9:30 AM – 11:30 AM EST
    - Room A708
- Science Identity Federation (Risk Management Track)
  - Logistics
    - Tuesday, May 18, 2010
    - 4:00 PM – 5:00 PM EST
    - Room A704
  - Focus
    - Ties into NSF/NIH InCommon Federation
    - Federated identity solution for Level 1 authentication