# HSPD-12 Logical Access Implementation and HHSIdentity

Indian Health Service

Information Management Conference

December 18, 2008

By

Ken Calabrese, HHS Chief Technology Officer

# Program Roles

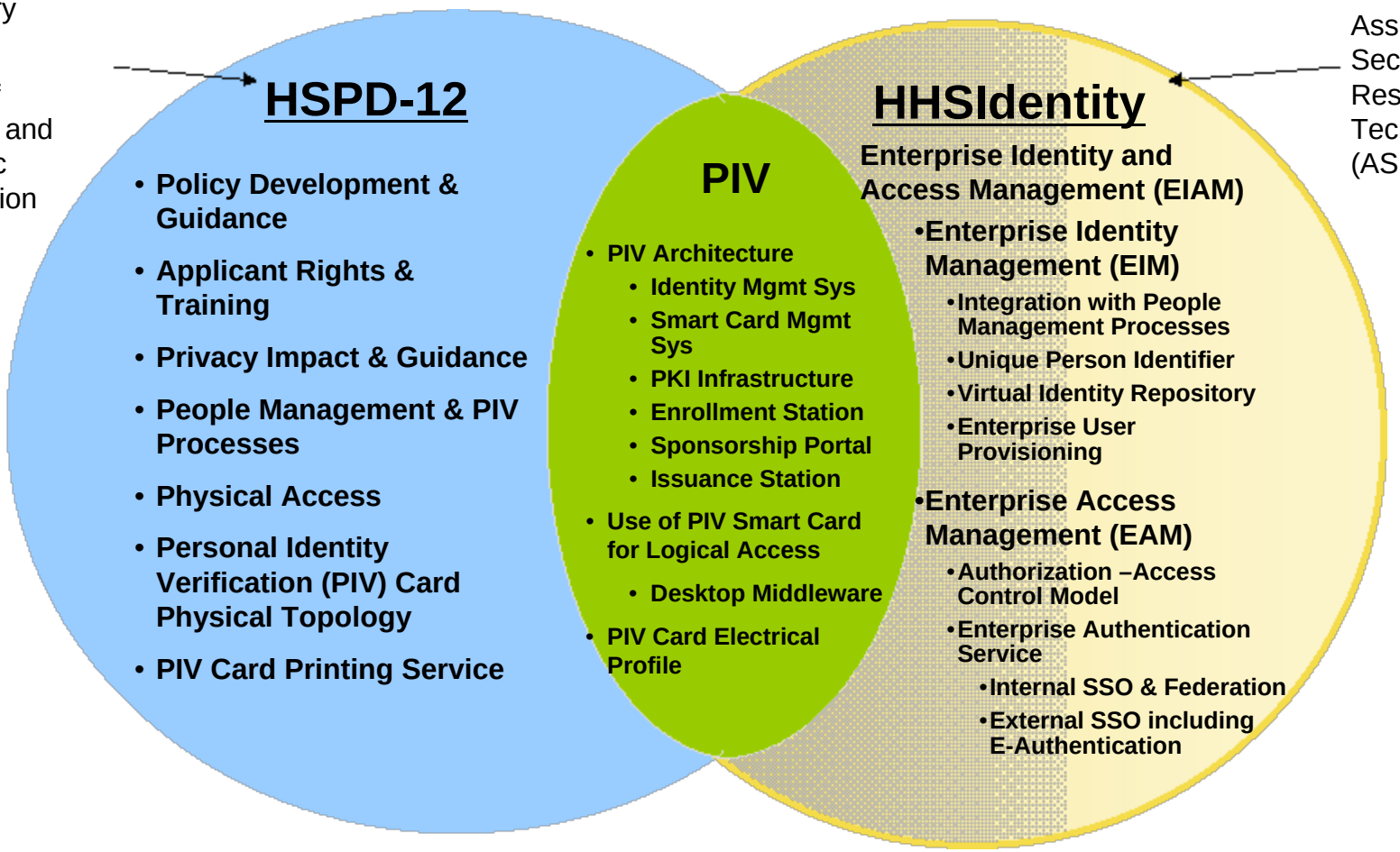
- HSPD-12 – Office of Security and Strategic Information (OSSI)
  - Reports to the Deputy Secretary of HHS
  - Departmental Policy and Program Oversight
  - Identity card issuance
    - Provide initial card stock
    - Provide initial enrollment and issuance workstations for OPDIV's
  - *Physical Access Control*
    - Sponsor perimeter access readers for OPDIV's
- HHSIdentity – Assistant Secretary of Resources and Technology (ASRT)
  - Program under HHS Chief Information Officer reporting to ASRT
  - *Access Management*
    - IT Infrastructure, Systems and Applications
    - Remote Access to Personal Identifiable Information
  - *Identity Management*
  - Issue PKI certificates for authentication, encryption, and digital signature
- Human Resources providing Personnel Security
  - Reports to Assistant Secretary for Administration and Management

# HSPD-12 Mission Alignment

Immediate Office of the Secretary (IOS)

Office of Security and Strategic Information (OSSI)

Assistant Secretary of Research & Technology (ASRT)




**ZONE 14: Card Expiration Date**

**ZONE 2: Card Holder's Name**

**ZONE 17: OPDIV AFFILIATION**

**ZONE 12: Federal Emergency Response Official**

**ZONE 10: HEALTH AND HUMAN SERVICES**

**ZONE 15: Affiliation Color Stripe**

**ZONE 5: Security Access Codes**

| | |
|---|---|
| A | 24 Hour Access |
| AE | 24 Hour Access – Escort Authority |
| C | C O O P |
| E | Escort Authority |
| L | Lab |
| R | Restricted Area Access |

**ZONE 4: Property Pass Codes**

| | |
|---|---|
| ANY | Any Property Type |
| AV | Audio Visual Equipment |
| CC | Computer Camera Equipment |
| CE | Computer Equipment |
| CM | Camera Equipment |
| CY | Copier Equipment |
| D | Disk/Tape/Listings |
| F | Furniture |
| L | Laptop |
| P | Packages |
| T | Telephone Equipment |

# HSPD-12 Identity "PIV" Card

- **Card Format:**
  - **Smart Chip**
    - **Picture**
    - **Card Holder Unique Identifier (CHUID) including:**
      - **Name**
      - **Agency Code**
      - **Ten digit unique identifier within agency – "HHSID"**
        - » ***Used for logical access to uniquely identify card holder***
    - ***Four Public Key Infrastructure (PKI) certificates***
  - **Electronic interfaces for Physical Access Control Systems (PACS)**
    - **Wireless "Contactless"**
      - **Antenna supporting legacy PACS systems**
        - » **Reads HID (Hughes Identification Devices) identifier**
      - **Antenna supporting new PACS standard – reads CHUID**
    - **Physical insertion "Contact" – reads all information including PKI**
  - **Magnetic strip**
  - **Barcode**

# PKI Certificates

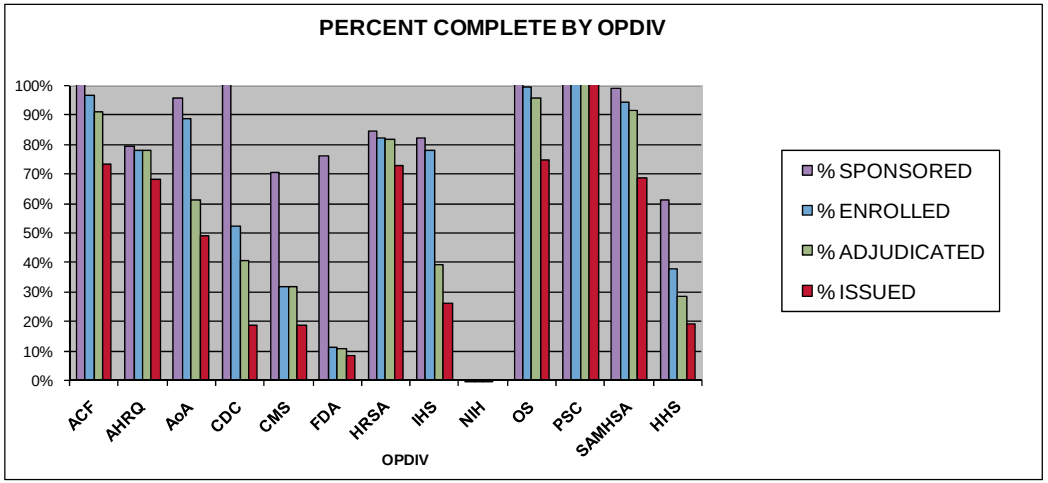
- Certificates are electronic identifiers
  - Issued by a Certificate Authority (CA)
    - CA's abide by strict rules for identity proofing, issuance and revocation
    - PKI is an International, Government, and industry standard
    - Certificate Authorities are certified by "Policy Authorities"
      - Federal PKI Policy Authority establishes Federal PKI governance
    - Policy authorities agree to trust certificates issued by other CA's
      - Federal Bridge governs certificates Federal Government accepts
  - Can be "soft" or "hard" certificates
    - Hard certificates are issued to a device and cannot be transferred
      - *Basis for "two factor authentication" for remote access to PII*
      - Very high level of assurance (level 4) since "bound" to device
        - » Requires physical possession of the single device to which issued
      - Requires software "middleware" on desktop to interface to device
    - Soft certificates are media independent and can be transferred
      - *Windows certificate store*
      - CD's and USB drives
      - High level of assurance (level 3) because not bound to a device

# PKI Certificates on HSPD-12 Identity Card

- HSPD-12 identify card contains four certificates
  - Card authenticity – validates the identity card is genuine
  - *Authentication – used to authenticate (log in) to logical systems (LACS)*
  - *Encryption – used to encrypt files and electronic mail messages*
  - *Digital Signature – used to digitally sign documents and electronic mail*
- HHSIdentity Program also issues:
  - “soft” certificates
  - TLS (server) certificates to allow servers to communicate securely

# Card Issuance Status as of Dec 3, 2008

| Totals by OpDiv | | | | | | | | | | | Total HHS Population | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| OPDIV | Sponsored | Enrolled | | # Need SMTP/UPN | # Adj. Pend | Adjudicated | Issued | | Issued: Federal | Issued: Contractors | Federal | Contractors / Organizational Affiliates | Total |
| | | Total | Bi-Weekly Trend | | | | Total | Bi-Weekly Trend | | | | | |
| ACF | 2,132 | 2009 | 15 | 45 | 91 | 1,873 | 1,511 | 36 | 1,036 | 475 | 1,311 | 746 | 2,057 |
| AHRQ | 433 | 427 | 1 | 1 | 2 | 424 | 372 | - | 281 | 91 | 350 | 195 | 545 |
| AoA | 113 | 106 | 1 | 3 | 31 | 72 | 58 | 2 | 54 | 4 | 104 | 14 | 118 |
| CDC | 19,988 | 9696 | ***268*** | 8 | 2,411 | 7,273 | 3,343 | ***375*** | 1,625 | 1,718 | 9,927 | 8,037 | 17,964 |
| CMS | 4,632 | 2246 | ***151*** | 10 | 142 | 2,094 | 1,216 | ***98*** | 1,206 | 10 | 4,106 | 2,452 | 6,558 |
| FDA | 11,883 | 1832 | 40 | 23 | 113 | 1,696 | 1,311 | 21 | 1,237 | 74 | 10,284 | 5,300 | 15,584 |
| HRSA | 1,667 | 1632 | 5 | 9 | 13 | 1,610 | 1,435 | 15 | 1,258 | 177 | 1,253 | 716 | 1,969 |
| IHS | 13,197 | 12,620 | 31 | 220 | 6,119 | 6,271 | 4,181 | ***183*** | 4,158 | 23 | 15,448 | 616 | 16,064 |
| NIH | 32 | 32 | 1 | 2 | 29 | 1 | - | - | - | - | 16,907 | 16,957 | 33,864 |
| OS | 5,740 | 5,610 | ***57*** | 163 | 126 | 5,321 | 4,162 | 85 | 3,419 | 743 | 4,584 | 987 | 5,571 |
| PSC | 2,373 | 2151 | 29 | 74 | 30 | 2,047 | 1,708 | 22 | 704 | 1,004 | 717 | 764 | 1,481 |
| SAMHSA | 721 | 691 | 1 | 6 | 19 | 666 | 501 | 11 | 449 | 52 | 528 | 200 | 728 |
| **TOTALS** | **62,911** | **39,052** | **600** | **564** | **9,126** | **29,348** | **19,798** | **848** | **15,427** | **4,371** | **65,519** | **36,984** | **102,503** |



# HHSIdentity Business Need

- **Universal access to core set of identity attributes**
  - **Key attributes with extensive use across broad range of systems**
  - **Updated by the true authoritative sources**
  - **Timely, consistent and accurate**
- **Secure access to sensitive data and personal identifiable information (PII)**
  - **Two-factor authentication for privileged access**
  - **Audit files identifying system access**
- **Improved efficiency**
  - **Lower overall cost through elimination of redundancy**
  - **Improved efficiency through direct access to authoritative information**
  - **Reduced administrative overhead through elimination of duplicative manual processes**
  - **Reduced/Single Sign-On (SSO) improves user productivity and experience**
    - **Significant reduction in help desk calls**
- **Enhanced security**
  - **Universal, real-time revocation of physical and logical access rights for terminated staff**
  - **Robust and consistent identity vetting**
  - **Reduced number of user credentials**
- **HSPD-12, OMB M-06-16, and OMB M-04-04 compliance**
  - **Supports HIPAA compliance**
  - **Supports Privacy Act compliance**

# HHSIdentity Benefits

- Significantly enhances security for access to computer systems and data
  - Provides Department-wide solution for secure remote access
- Reduces the number of accounts and passwords required to access systems
- Leverages HSPD-12 PIV card for single sign-on
- Provide robust identity auditing capabilities
- Provide a standardized and automatable process that enables business process and application owners to control access to applications and services
  - Automate the removal or disablement of the HHS-wide identity and associated attributes from applications when a user relationship to HHS terminates
- Reduce support costs by reducing the number of accounts and passwords a user must manage

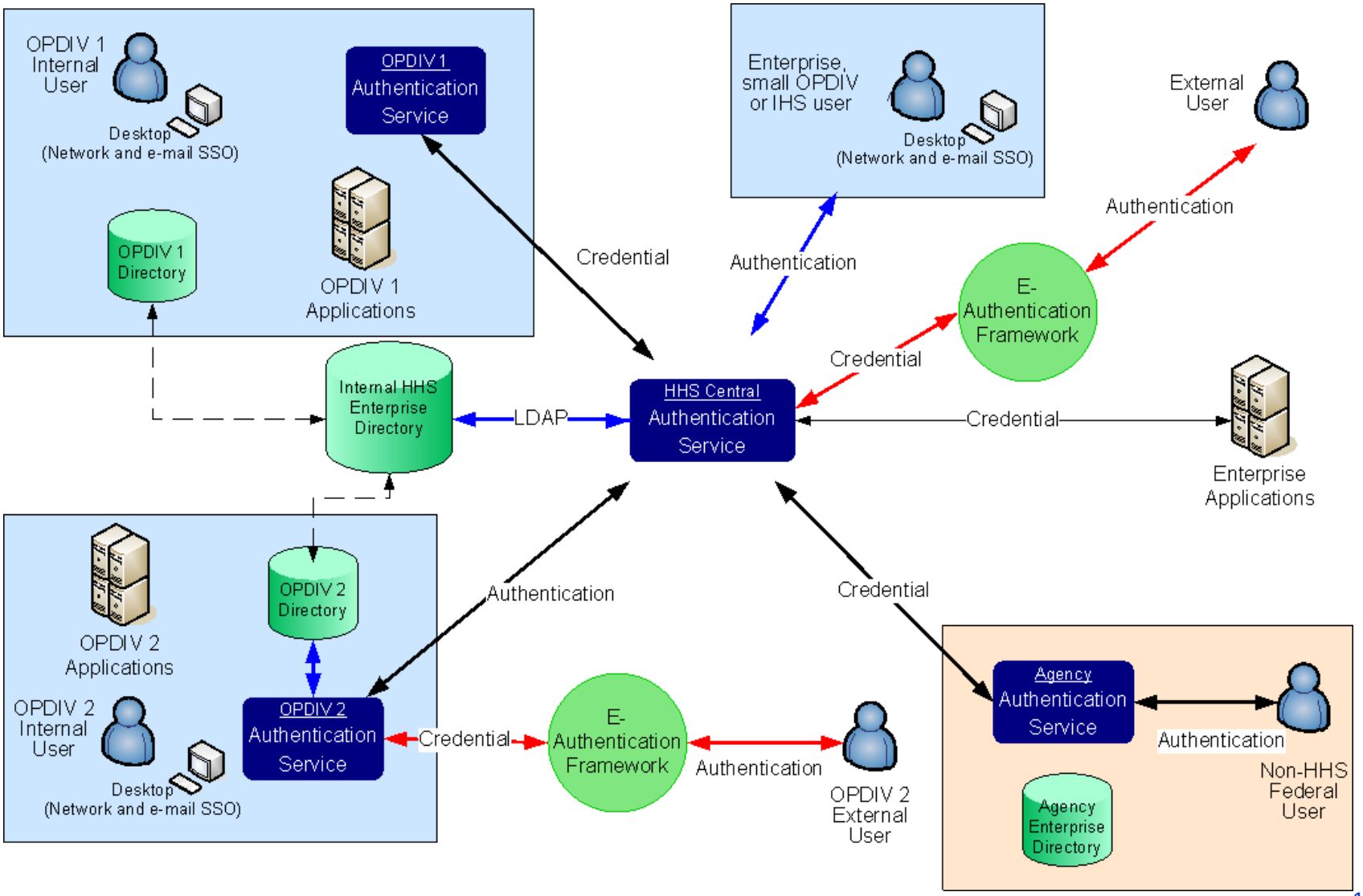
# HHSIdentity Program Overview

- Program Goals:
  - Implement Enterprise Identity and Access Management (EIAM) Services
    - Provide secure *access* to information systems and data
    - Provide repository of core *identity* attributes
- Program Vision:
  - The HHSIdentity Program will institute a *federated* IAM model:
    - Leverages large OPDIVs single sign-on investments
  - Establishes the Enterprise Identity and Access Management Service for:
    - OS and Small OPDIV's
    - Enterprise Systems
    - Indian Health Service
  - Establish the Enterprise Access Management Service
  - Establish *virtual repository* containing the core set of identity attributes

# HHSIdentity Work Streams

- Enterprise Access Management Workstream
  - Provides multi-level access to systems and data
  - Implements Single/Reduced Signon
- Enterprise Identity Management Workstream
  - Virtual Identity Manager
    - Provides repository for the core set of commonly used identity attributes
    - Attributes are either:
      - Physically contained in repository
      - Mapped to source attributes
        - » Reduces size of central information hub
        - » Reduces issues related to data synchronization
  - Serves as “proxy” for authoritative sources
    - Authoritative source pushed information to repository

# Authentication Architecture



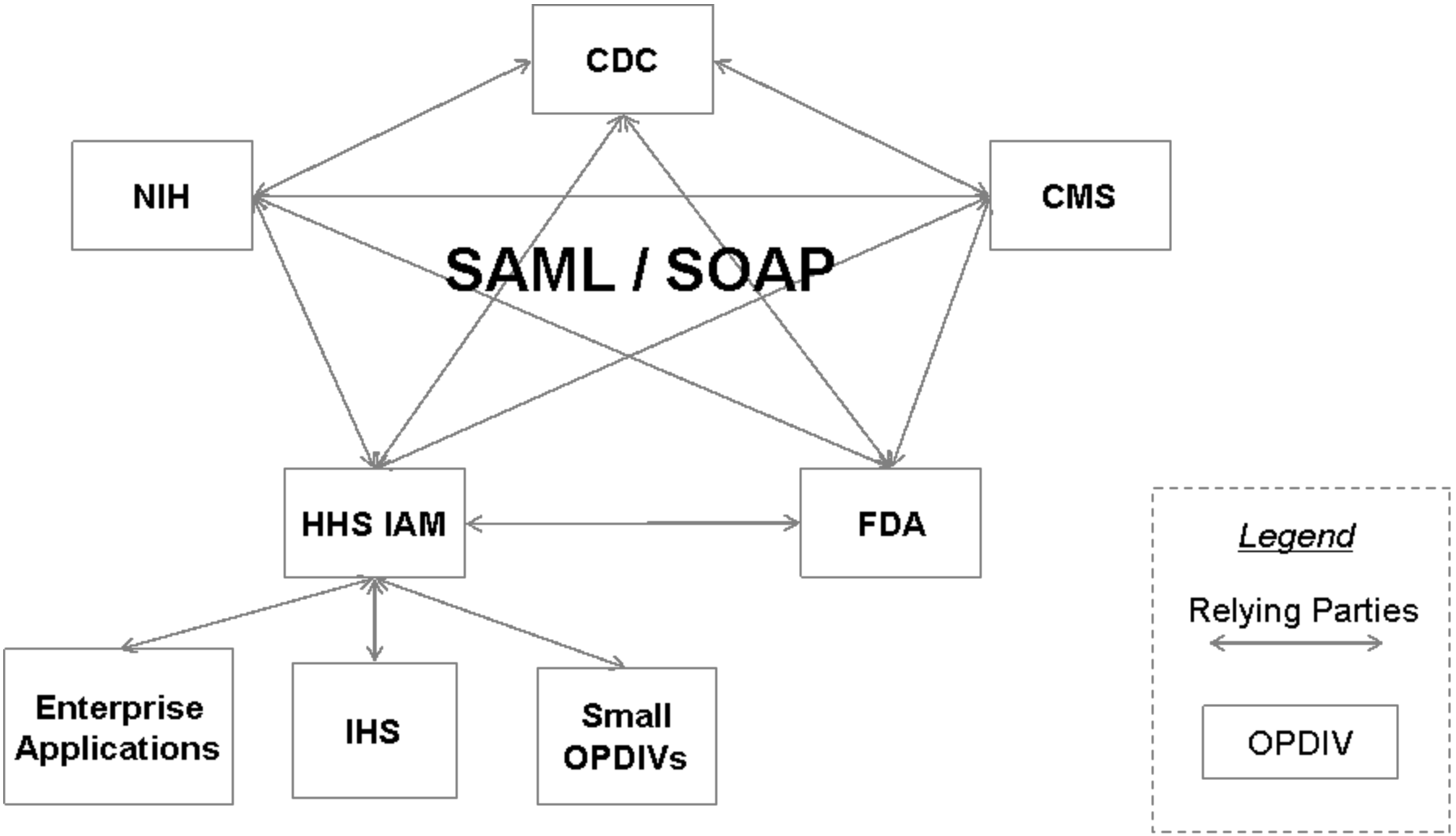
# Enterprise Access Management

- **Provides authentication services for web-based systems**
  - **Provides authentication as well as complete auditing services**
- **User authenticates to web-based authentication service**
  - **Level 2 credential: USERID/password**
  - **Level 3 credential: Soft certificate**
  - **Level 4 credential: PIV card**
    - **Provides two factor authentication for remote access to PII data**
  - **Application determines the required minimum assurance level**
- **Initial systems integrated into Enterprise Authentication Service**
  - **EHRP and EWITS: Jan 2009**
  - **Requires Level 4 (PIV card) for privileged access by administrators**
    - **Requires loading of middleware on desktop**
  - **Allows USERID or higher credential for routine user access**
  - **Does not require use of PIV card for network authentication**
  - **User authenticates once and may gain access to either application**

# Enterprise Identity Management

- Identity Management Database (IDMS)
  - Serves as precursor of the virtual identity manager
  - Contains attributes required to support HSPD-12 card issuance
  - All attributes are physically stored in IDMS
  - Initial applications and demonstration of capability
    - Integration of OS Lenel PACS with IDMS
    - Real time updates pushed from IDMS to Lenel system
    - Production scheduled for Jan 2009
  - Integration with electronic mail system CY 2009
  - Contains full life cycle of identity attributes
    - Sponsorship to revocation

# HHS IAM Federation Concept



# Federation

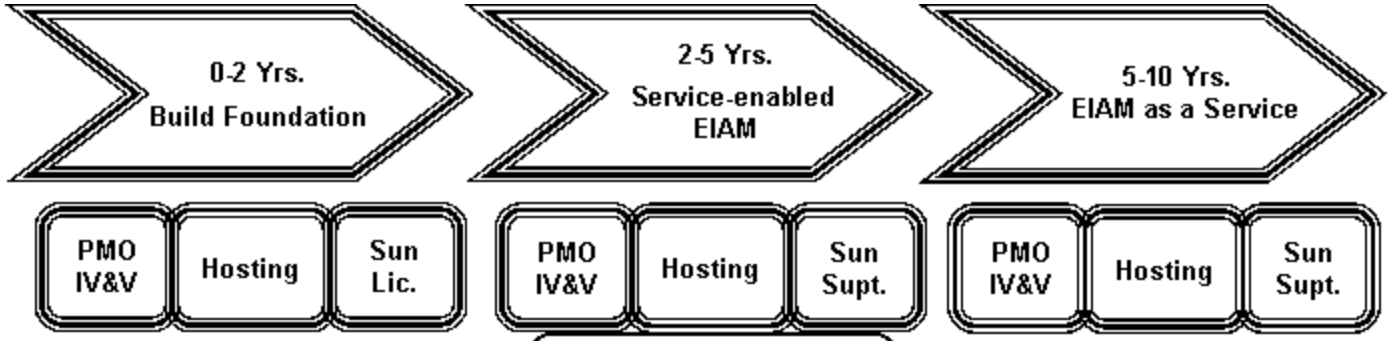
- **HHSIdentity built on Federated Architecture**
  - **Credentials passed between OPDIV home services and External Services**
    - **Utilize standard protocols: SAML, SOAP, SPML, etc.**
    - **User Authenticates to home authentication service**
      - **Provides single signon to internal applications**
    - **Credential passed by home authentication service to external service**
      - **Extends single signon to external applications**
      - **Includes systems supported by other OPDIV's or agencies**
      - **Includes external line of business systems**
        - » **eOPF; GovTrip; MyPay; ITAS; etc.**
  - **Federation with NIH and CDC in CY 2009**
  - **Implementation with external application subject to funding and support**
  - **Federation also support access by external users HHS systems**
    - **Other Agencies, Industry, Education, and Public**

# PIV Card vs Other Technologies

- PIV is a one stop technology:
  - CHUID contains unique identifier to identity user
    - Negates need for USERID's known by user
  - Card provides two factor authentication for remote access
  - Card provides certificate for digital signature
  - Card provides certificate for encryption
  - User must only remember the eight digit PIN
  - Leverages investment mandated for HSPD-12
- Use of PIV requires loading middleware to workstation
  - Major consideration for systems used for remote access
  - Major challenge for non-Government systems

# Enterprise Identity & Access Management Future State

U.S. Department of Health and Human Services




**Small OPDIVs, IHS and Enterprise Applications**

**Large OPDIVs***

**Provides Capabilities to Both Groups**

- Central Authentication PIV and uid/password
- Federated Single Sign On (SSO) with Internal Partners
- Custom Registration and User Linking
- Self Service Password Mgmt.
- Identity Reporting

- Enterprise SSO with other applications
- High Value Application Provisioning
- Delegated Administration
- Enterprise Role Mgmt Implementation
- Self Service and User Linking through EIM
- Centralized Identity and Access Administration
- Compliance Reporting and Auditing

- EIM as a Service
- Comprehensive Automated Provisioning Workflow
- LACS, PACS and NAC Integration
- External Federation E-Authentication
- Role Based Authorization

* Provided through Federation and Service-based Interfaces

# Questions and Contact

- Questions?
- Contact
  - Ken Calabrese
  - HHS Chief Technology Officer
  - 202-205-4287
  - E-Mail Ken.Calabrese@HHS.GOV