



AFCEA Bethesda
4 August, 2009



Federal CIO Council
Information Security and Identity Management Committee

Identity, Credential, and Access Management

in and with

The Federal Government

Paul D. Grant
Special Assistant,
Federated IDM and External Partnering
Office of the CIO
DoD
Paul.Grant@OSD.Mil

Judith Spencer
Agency Expert - IDM
Office of Governmentwide Policy
GSA
Judith.Spencer@GSA.Gov

<http://www.IdManagement.Gov/>



ICAM Scope



- **Person and Non-Person Entities**
- **Logical Access and Physical Access**
- **All Four Segments**
 - Government to Citizen (G-C)
 - Government to Business (G-B)
 - Government to Government (G-G)
 - Internal Effectiveness and Efficiencies (IEE)
- **All Four Levels of Identity Assurance**
 - OMB M-04-04
 - Authentication Assurance Levels 1, 2, 3, 4
- **Alignment of Federal ICAM and**
 - CNSS Identity and Access Management (National Security Systems)
 - Interagency Security Committee (Physical Access Control)
 - Awareness to External Mission Partners for interoperable solutions



Presidents Budget for FY 2010

Extract from Section 9.

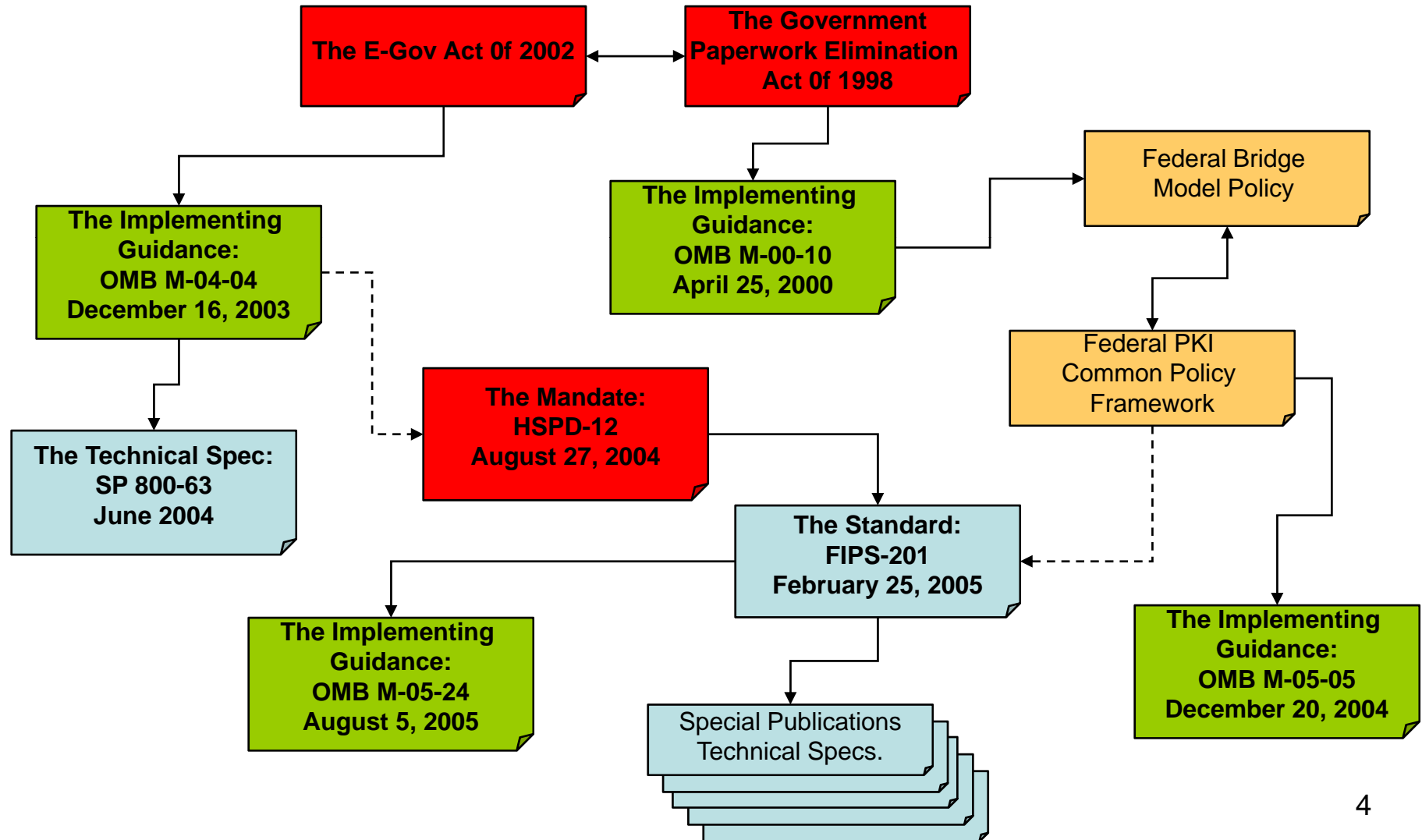
LEVERAGING THE POWER OF TECHNOLOGY TO TRANSFORM THE FEDERAL GOVERNMENT



- To support this effort, the Federal Identity, Credential, and Access Management (ICAM) segment architecture provides Federal agencies with a **consistent approach** for managing the vetting and credentialing of individuals requiring access to Federal **information systems and facilities**
- The ICAM segment architecture will serve as an important tool for providing **awareness to external mission partners** and drive the development and implementation of **interoperable solutions**.

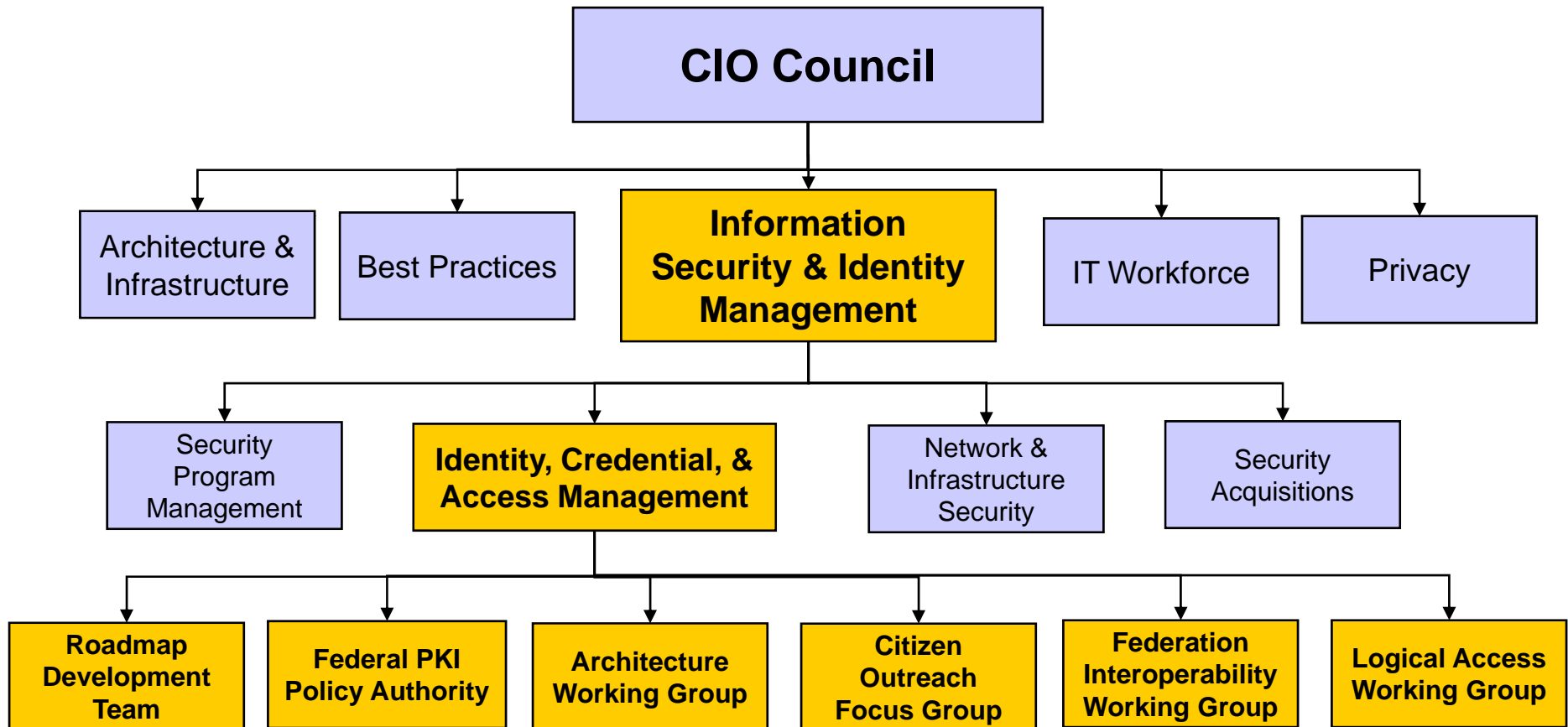


Enabling Policy and Guidance





Committee Structure





ICAM Mission



- Fostering effective **government-wide** identity and access management
- Enabling **trust** in online transactions through **common** identity and access management **policies and approaches**
- **Aligning federal agencies** around common identity and access management practices
- **Reducing the identity and access management burden** for individual agencies by fostering common interoperable approaches
- **Ensuring alignment** across all identity and access management activities that cross individual agency boundaries
- Collaborating with **external identity management** activities through **inter-federation** to enhance interoperability

Co-Chairs: Paul D. Grant, DOD & Judith Spencer, GSA



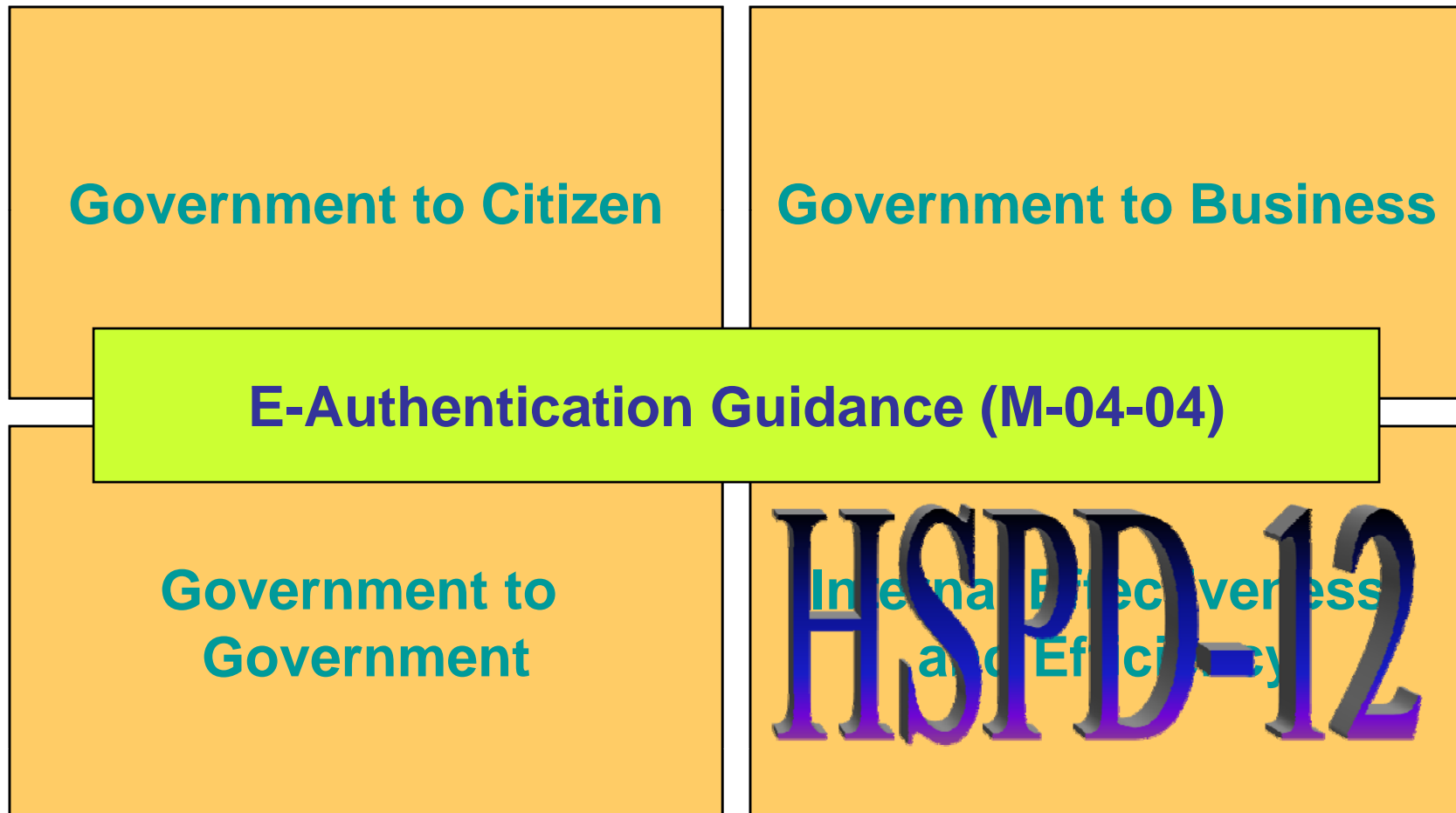
Working Groups



- **Federal PKI Policy Authority** – administers the policies of Federal PKI
- **Roadmap Development Team** – Review team for the development and content of the ICAM Roadmap and Implementation Guidance (including Segment Architecture)
- **Architecture Working Group** – develop the new ICAM technical architecture
- **Citizen Outreach Focus Group** – to make recommendation concerning solution sets for government-to-citizen interaction (including G-G and G-B)
- **Federation Interoperability Working Group** – determine business drivers and terms of engagement for inter-organizational trust.
- **Logical Access Working Group** - developing guidance/best practices to assist agencies in implementing log on/ authentication capabilities using PIV cards.



4 Sectors for Government Interaction





Identity Assurance Levels (AL)



**M-04-04:E-Authentication Guidance for
Federal Agencies
OMB Guidance establishes 4 authentication
assurance levels**

Level 1	Level 2	Level 3	Level 4
Little or no confidence in asserted identity	Some confidence in asserted identity	High confidence in asserted identity	Very high confidence in asserted identity
Self-assertion minimum standards	On-line instant qualification, out-of- band follow-up	On-line out-of-band verification for qualification Cryptographic Solution	In person proofing Record a biometric Cryptographic solution Hardware Token



ICAM Roadmap and Implementation Project Overview



- **Scope includes:**
 - **Federal Segment ICAM Architecture of the FEA**
 - » including tools
 - » methodologies
 - » transition plans
 - » that address current ICAM needs
 - » outlines a target future state
 - **ICAM priorities in sufficient detail to facilitate budgetary planning**
 - **Guidance and best practices for agencies deploying ICAM solutions**
 - **2 Phases - This Year**

- **Goal: To produce and maintain the:**
“Federal Identity, Credential and Access Management (FICAM) Roadmap and Implementation Guidance” document.



Phase 1

The Federal ICAM Segment Architecture



The Federal ICAM Segment Architecture was developed as Phase 1 of the FICAM Roadmap and Implementation Guidance

- **Complied with Federal Segment Architecture Methodology (FSAM)**
- **Draft Completed Review Period on 15 July, 2009**
- **Adjudication of Comments Underway**
- **Phase I ends with Public Release of the FICAM Roadmap in August**

Federal ICAM Segment Architecture Purpose:

The purpose of the Federal Identity, Credential, and Access Management (ICAM) segment architecture is to provide federal agencies with a consolidated approach for implementing government-wide ICAM initiatives. The use of enterprise architecture techniques helped ensure alignment, clarity, and interoperability across agency ICAM initiatives and enable agencies to eliminate redundancies by identifying shared ICAM services across the Federal Government.



Phase 2 Implementation Guidance



- **Phase 2 includes the development of ICAM best practices and implementation guidance. This work is the extension of the Phase 1, and will include sections on:**
 - **Identity Proofing and Background Investigations**
 - **Physical Access**
 - **Logical Access**
 - **Role of PKI**
 - **Use of Digital Signatures**
 - **Federation and Information Sharing**
 - **Other Credential Types and Interoperability**
 - **Acquisition Guidance**
- **Estimated Completion: September 2009**
- **Product: “Federal Identity, Credential and Access Management (FICAM) Roadmap and Implementation Guidance” document**



Services Framework Categorization Scheme

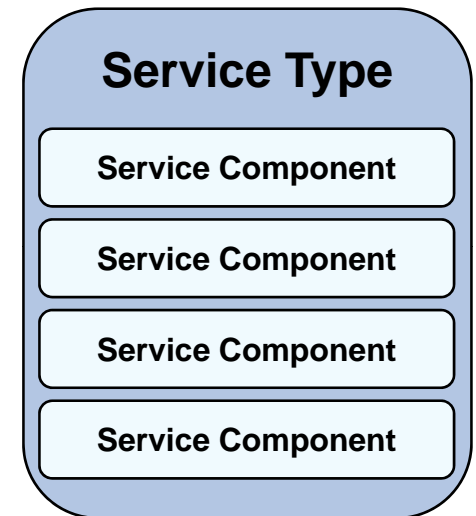


Service Type

- Provides a layer of categorization that defines the context of a specific set of service components

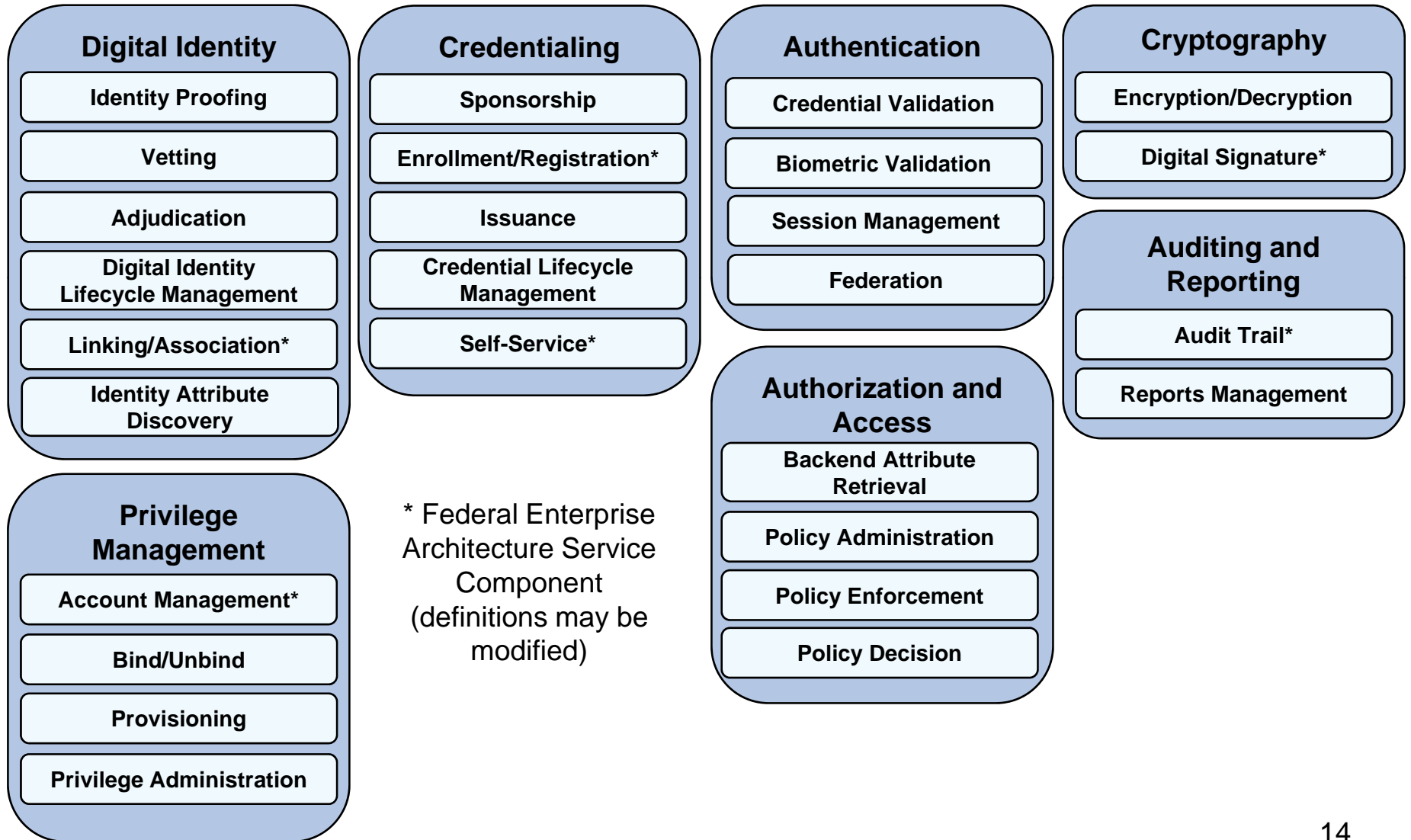
Service Component

- A self contained business process or service with predetermined and well-defined functionality that may be exposed through a well-defined and documented business or technology interface





Services Framework





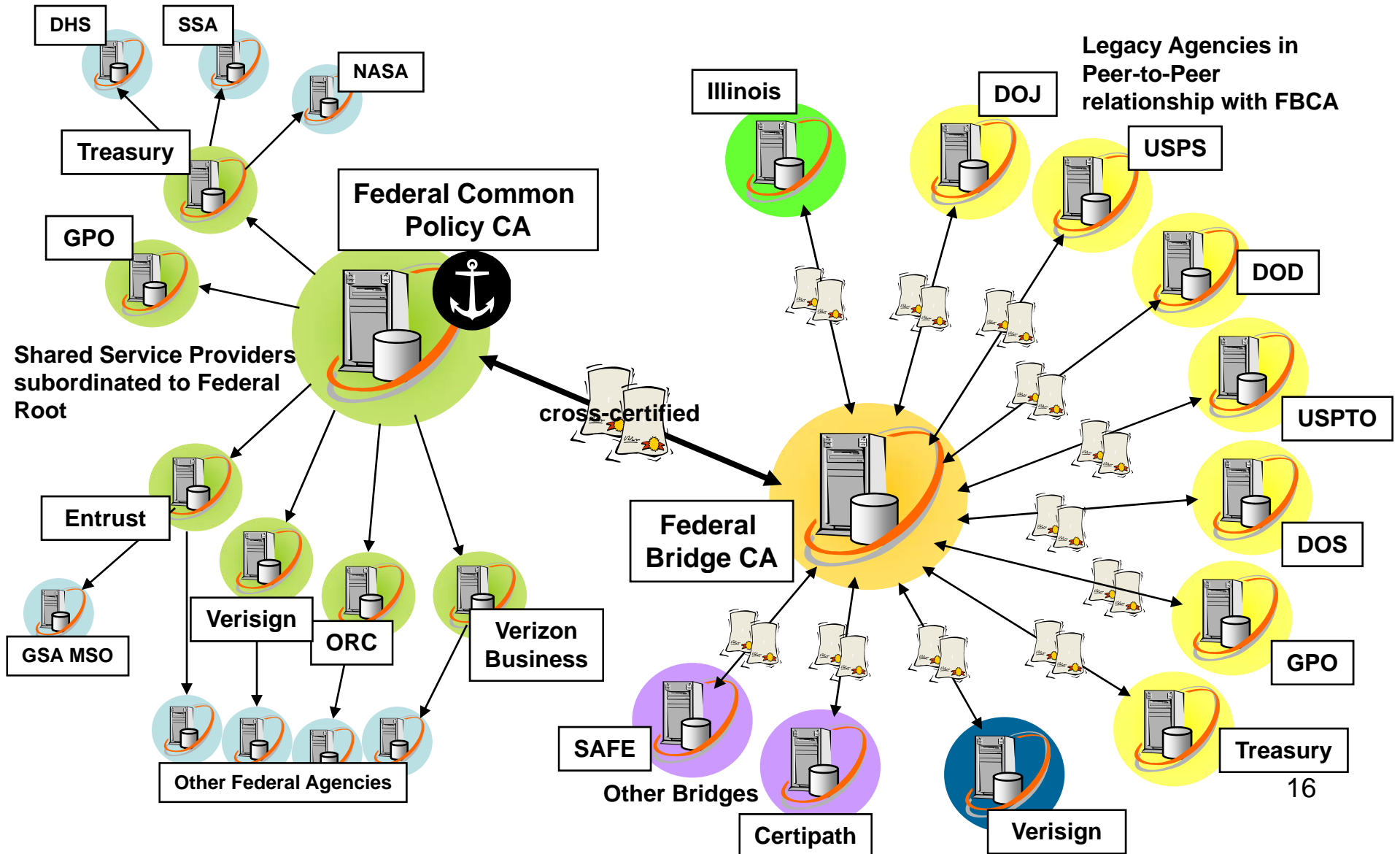
The Journey Continues



- **Published Personal Identity Verification Interoperable Cards for Non-Federal Issuers (PIV-I for NFI) in May 2009**
- **Published Initial Guidance for Validating Credentials of Non-Federal Issuers**
- **Federal ICAM Roadmap & Implementation Guidance**
 - Is the Federal ICAM Segment Architecture
 - Phase I nearing Completion for Version 1
 - Publish in Mid-August to Public
 - Phase 2 in Progress for Version 2 with Implementation Guidance by End of September
- **Promote activities of Citizen Outreach Focus Group**
 - Produce Solution Recommendation for the CIO Council (6 month effort – Draft in Mid-July)
- **Continue Outreach Activities**
 - Kantara (Liberty Alliance Partnership)
 - Higgins Project
 - Transglobal Secure Collaboration Program
 - Educause (post-secondary education)
 - AFEI Identity Protection and Privilege Management Forum

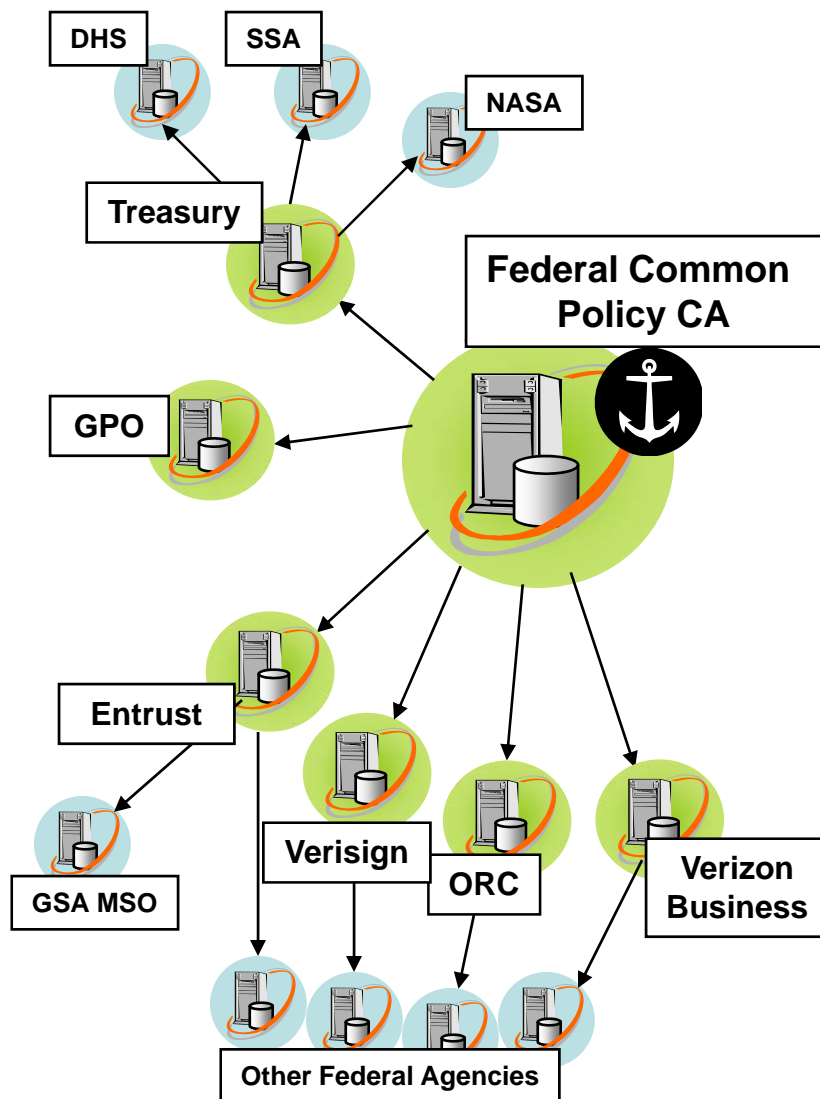


Federal PKI Trust Framework





Federal Common Policy Root



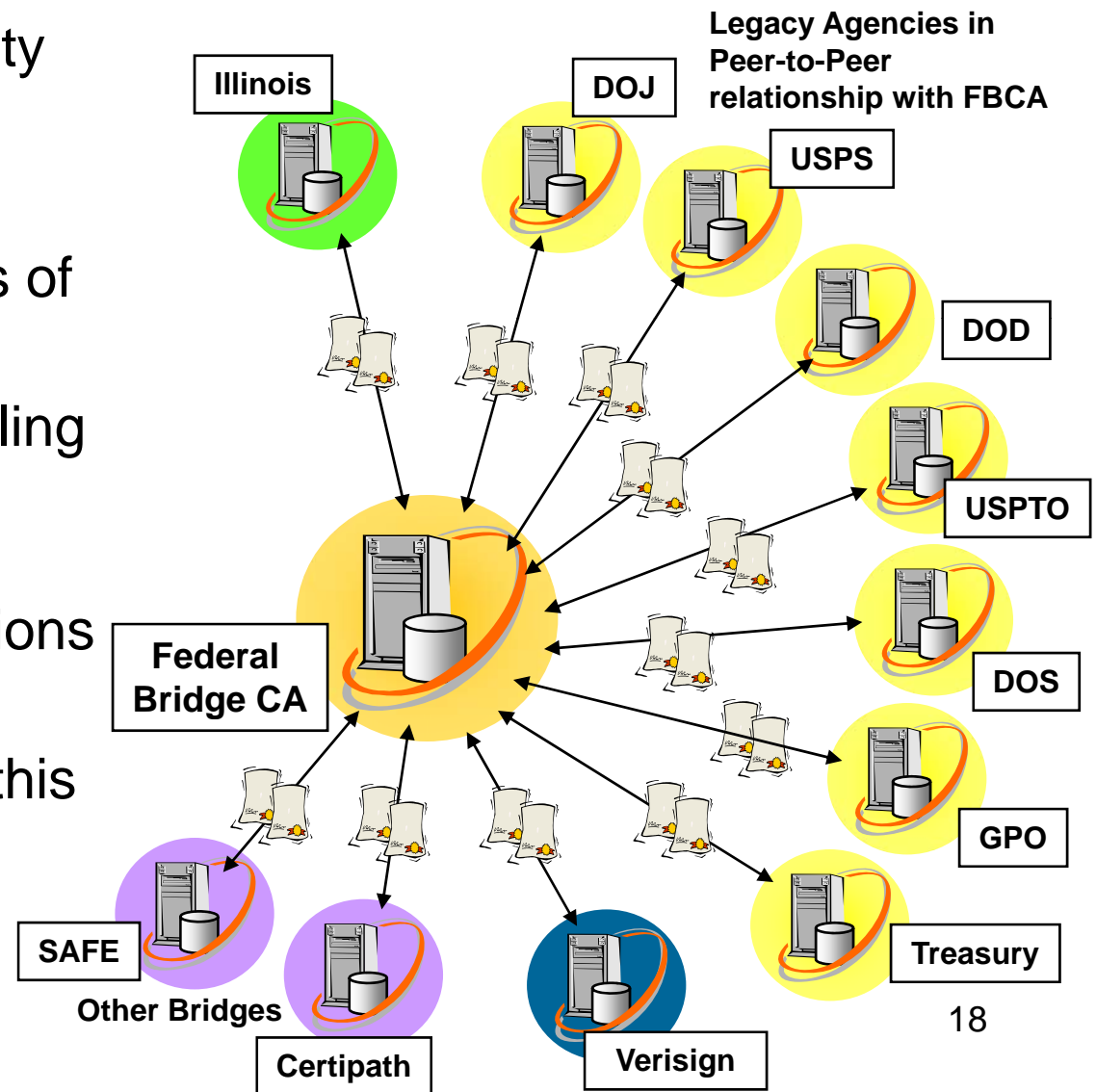
- Federal Root CA
- Per M-05-05 – Agencies should acquire PKI credentials from PKI service Providers
- Per FIPS-201 – PIV Authentication certificates must conform to the Federal Common Policy
- Common Policy Root is in the Microsoft Store, negotiations under way to include in other major browser stores.
- Working with Adobe to include in Adobe White List



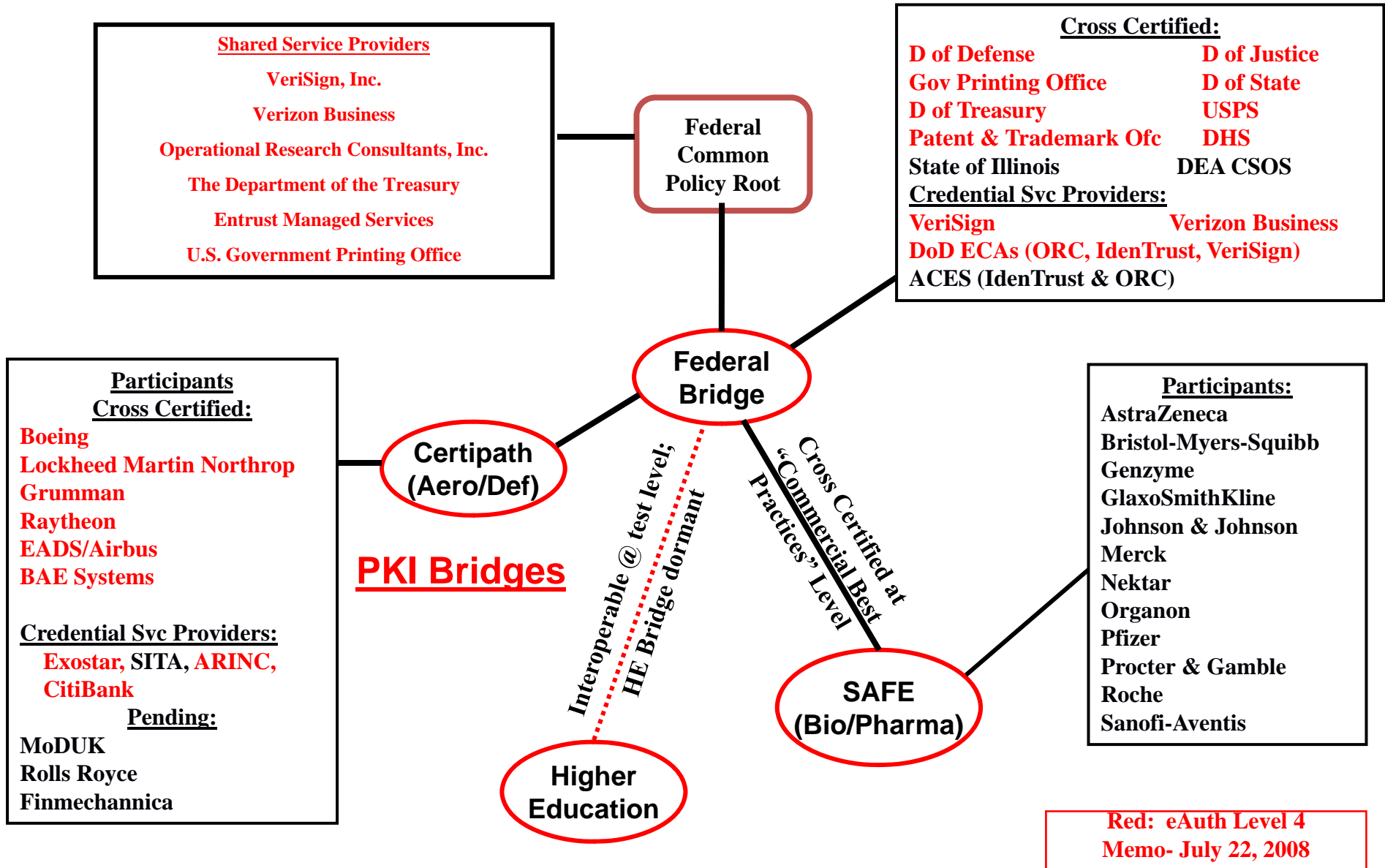
Federal Bridge CA



- Peer-to-Peer interoperability mechanism for PKI
- Acts as a trust facilitator
- Operates at multiple layers of assurance
- Chief mechanism for enabling trust between industry (external) PKI and Federal (internal) PKI implementations
- Undergoing upgrade and redesign to be completed this year



Identity Federations (PKI Based)





Personal Identity Verification (PIV) Cards for Non-Federal Issuers



Basis for PIV Card Trust

- **Well-defined standards**
- **A compliance regimen that ensures parties adhere to the well-defined standards**
- **Relying Party verification that allows relying parties to verify compliance when trusting and**
- **Secure components inherent to the PIV Card**

Situation

- **PIV Cards, by definition, are issued only to/by the Federal Government**
- **Organizations external to the U.S. Federal government have expressed a desire to establish identity credentials that are interoperable with the Federal PIV card.**
- **They want a card that is:**
 - **Technically compatible / interoperable with the PIV system**
 - **Capable of Trust in the Federal environment**



Published PIV Interoperability for Non-Federal Issuers (NFI) Guidance (May 2009)



• **PIV Interoperable Card** – an identity card that meets the PIV technical specifications to work with PIV infrastructure elements such as card readers, and is issued in a manner that allows Federal government relying parties to trust the card at AAL-4.

• **PIV Compatible Card** – an identity card that meets the PIV technical specifications so that PIV infrastructure elements such as card readers are capable of working with the card, but the card itself has not been issued in a manner that assures it is trustworthy by Federal government relying parties.



Credential Service Providers at AAL-4 for External Partners (non-Federal)



- **Credential Service Providers cross-certified with the FBCA at Medium Hardware**
 - VeriSign
 - Verizon
 - Exostar via Certipath Bridge
- **CSPs Pending Addition to List Above:**
 - DoD ECAs (ORC, VeriSign, IdenTrust) via DoD PKI Root
 - CitiBank via Certipath Bridge

Status is available at:

http://www.idmanagement.gov/drilldown.cfm?action=external_ssp

Federal Bridge: <http://www.cio.gov/fpkia/crosscert.htm>

Certipath Bridge: <http://www.certipath.com/pki-ts.htm>



Using Open Solutions for Extending Government outreach to the Public



- **Federal ICAM Identity Scheme Adoption Process, July 8, 2009.** This document defines a process whereby the government can assess the efficacy of specific subsets of identity management standards (i.e., schemes) for federal purposes...interoperability will be achieved at a known level of assurance comparable to one of the four Office of Management and Budget (OMB) Levels of Assurance.
- **Federal ICAM Trust Framework Provider Adoption Process for Levels of Assurance 1, 2, and Non-PKI 3, July 8, 2009** – Trust Frameworks that are comparable to federal standards are *adopted* through this process, which include requirements for trust framework provider (TFP) and TFP member identity providers.



Summary & Conclusions



- **Strong Identity and Access Management Are Foundational to Secure Information Sharing and Collaboration**
- **Shared Guidance is Improving: Much Room for More Improvement**
 - **Clear, Concise, Consistent, Published**
 - **For Ourselves and Our Mission Partners**
- **Federal Identity, Credential, and Access Management (ICAM) is providing this consistent approach (with your help)**
- **Mission Partners are Fielding Strong Identity Credentials (PKI) as well as Creating Federations for Sharing & Collaboration**
- **Progress Depends on Public-Private Partnering**
 - **Domestically and**
 - **Internationally**



Backup



Key Conceptual Threads for Secure Information Sharing and Collaboration

Source: DoD Information Sharing Strategic Plan

- **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 Assured Information Sharing activities



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 (= EAAL-4)**
- **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)**

Dynamic Attribute-Based Access Management is Policy Compliant Sharing & Collaboration

