NIST Privilege Management Workshop

September 1, 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

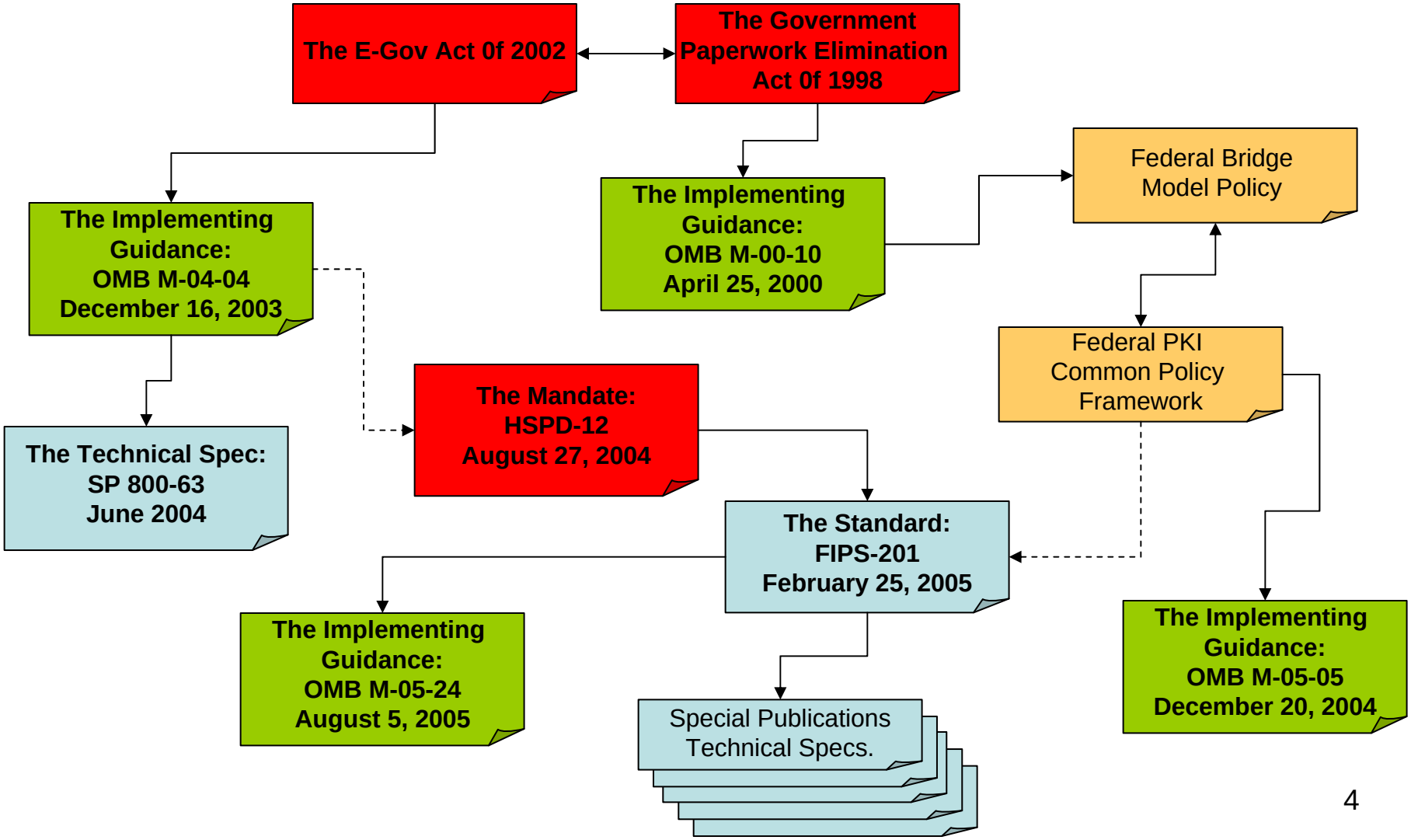
Presidents Budget for FY 2010

Extract from Section 9.
LEVERAGING THE POWER OF TECHNOLOGY TO TRANSFORM THE FEDERAL GOVERNMENT

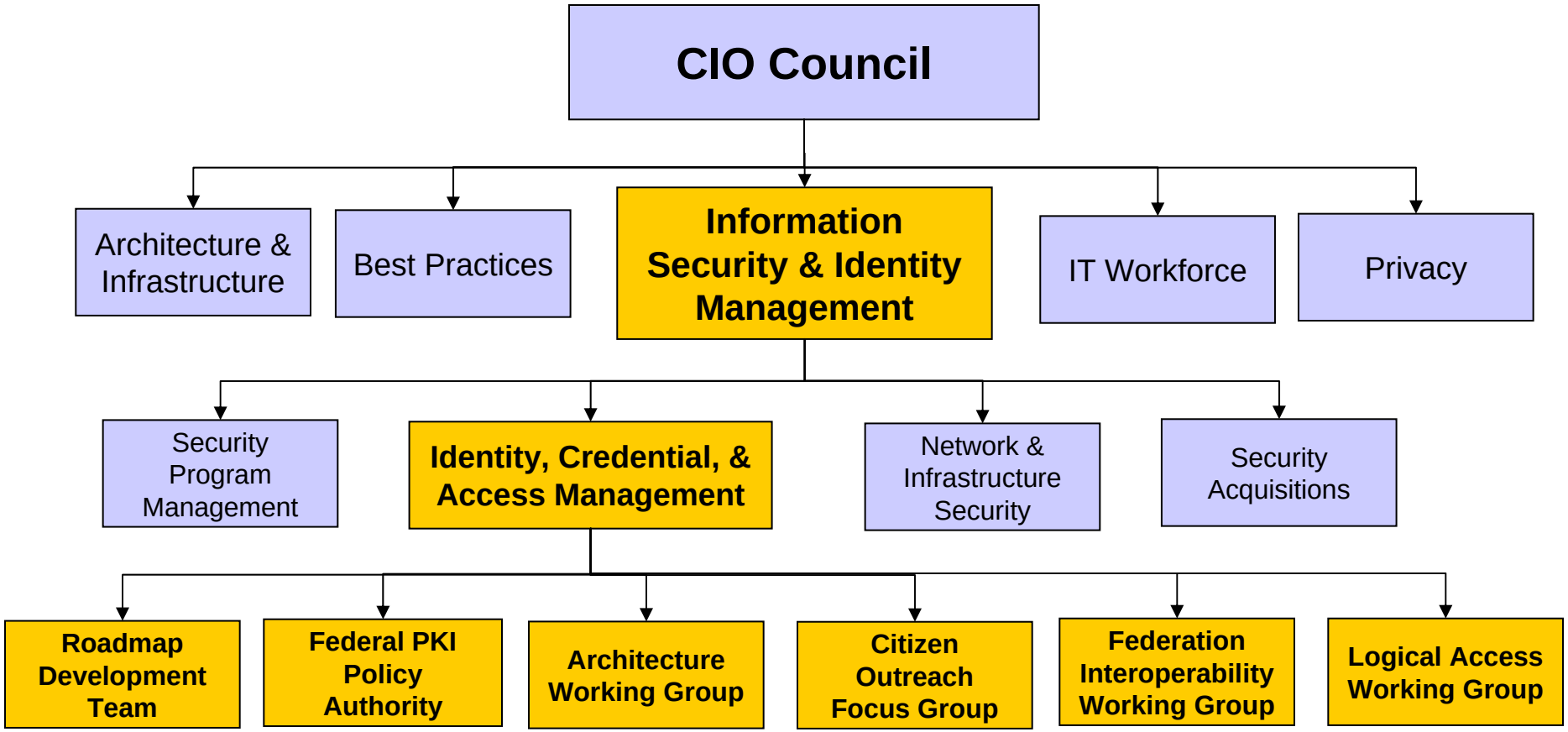
- To support this effort, the Federal Identity, Credential, and Access Management (ICAM) segment architecture provides Federal agencies with a consistent approach for managing the vetting and credentialing of individuals requiring access to Federal information systems and facilities

- 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

4 Sectors for Government Interaction

Government to Citizen

Government to Business

E-Authentication Guidance (M-04-04)

Government to Government

Internal Effectiveness and Efficiency

HSPD-12

Identity Assurance Levels (IAL)

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

Increasing the Trusted Credential Community

- Back to Basics – M-04-04 and NIST 800-63 are still the foundational policy/technical guidance for identity management in the Federal government.
- Establish a unified architecture for Identity Management
- Expand our use of Assertion-based solutions (Levels 1 & 2)
  - Stronger industry alignment for trust and technology standards
- Federal Bridge interoperability will continue to play a role at Levels 3 & 4
- Outreach to communities of interest
  - Explore natural affinities

ICAM Roadmap and Implementation Guidance

- Segment Architecture, including tools, methodologies and transition plans, that address current ICAM needs and outlines a target future state
- ICAM priorities in sufficient detail to facilitate budgetary planning
- Guidance and best practices for agencies deploying ICAM solutions

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

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 standards-based 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.

Goals

- Utilize new Federal Identity Credential (PIV Card) for Internal government identity management and access control
  - Logical access to systems
  - Physical Access to facilities
- Define PIV-Interoperability for external communities
- Leverage Open solutions for Government interaction with the American people
  - Make it easier for American Public to access government information
  - Avoid issuance of application-specific credentials
  - Leverage Web 2.0 technologies

Governmentwide Transition Initiatives

- Augment policy and implementation guidance to agencies
  - Develop digital identity data specification
  - Develop implementation guidance for use of PIV card features
- Establish federated identity framework for the Federal Government
  - Develop attribute exchange processes for sharing identity data
  - Develop trust models for inter-organizational interoperability
- Enhance performance measurement and accountability within the ICAM initiatives
  - Establish maturity models for ICAM transition activities
- Provide government-wide services for common ICAM requirements
  - Establish criteria for inter-federation

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.

Federal Agency Initiatives

- Streamline collection and sharing of digital identity data
  - Implement digital identity data standard once developed
  - Use standardized attribute exchange processes
- Fully leverage PIV and PIV-interoperable credentials
  - Reduce or eliminate issuance or maintenance of separate identity management processes (e.g. userid/password) within Federal community
  - Adopt federated trust models exercising FedPKI capabilities
- Modernize PACS infrastructure
  - Implement SP 800-116 for building access
- Modernize LACS infrastructure
  - Enable systems for smart card log on
- Implement federated identity capability
  - Participate in inter-federated environment

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: December 2009
- Product: “Federal Identity, Credential and Access Management (FICAM) Roadmap and Implementation Guidance” document

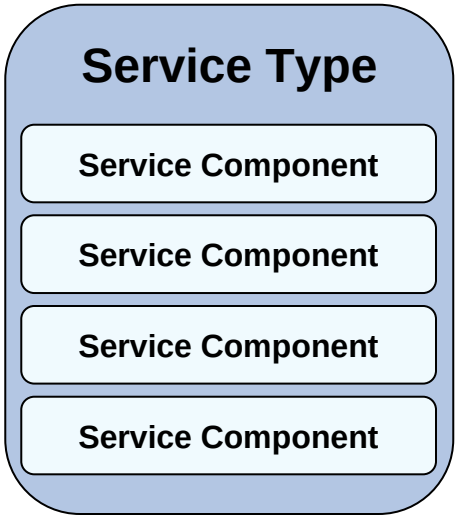
Services Framework Categorization Scheme

Service Type

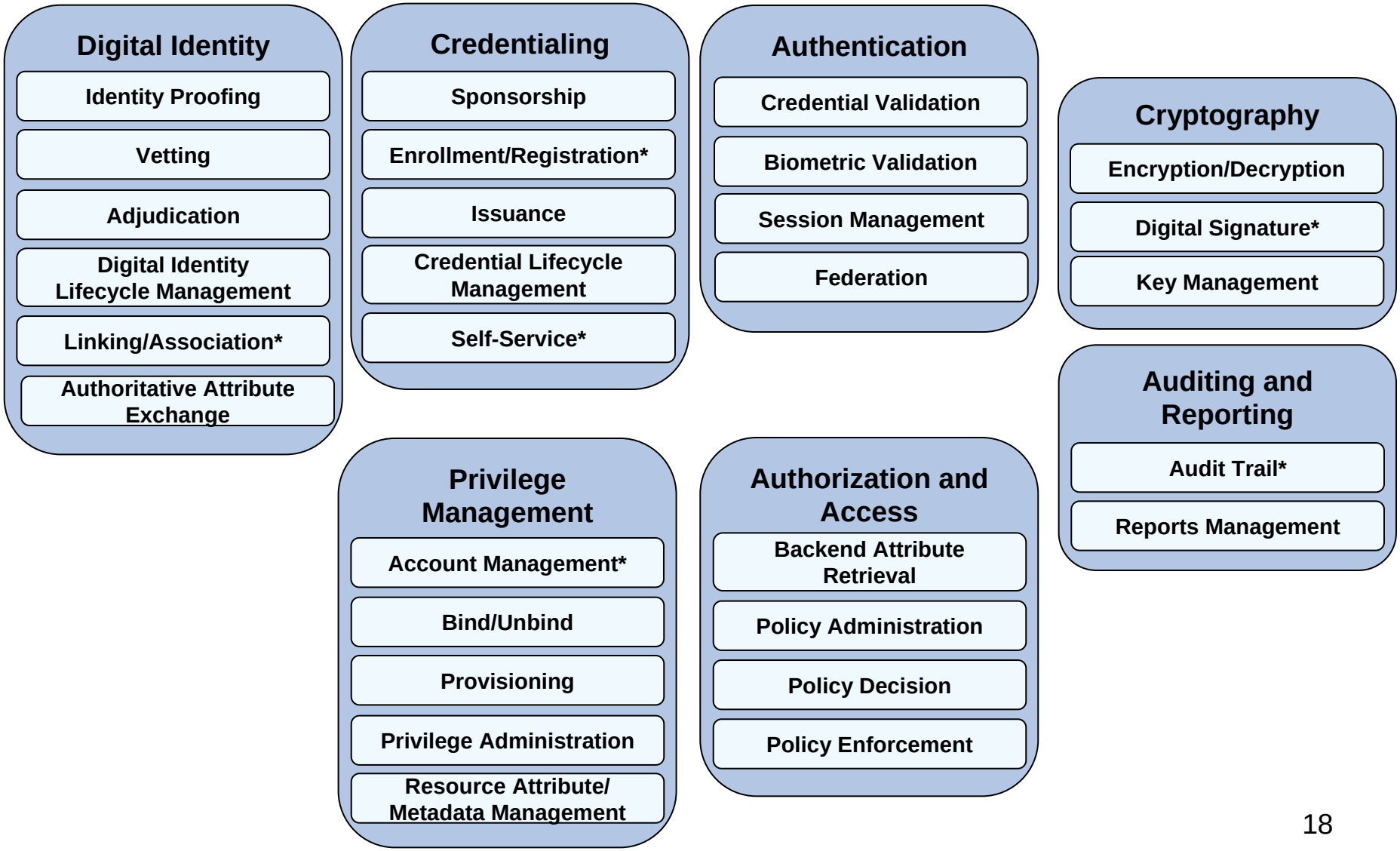
Provides a layer of categorization that defines the context of a specific set of service components

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



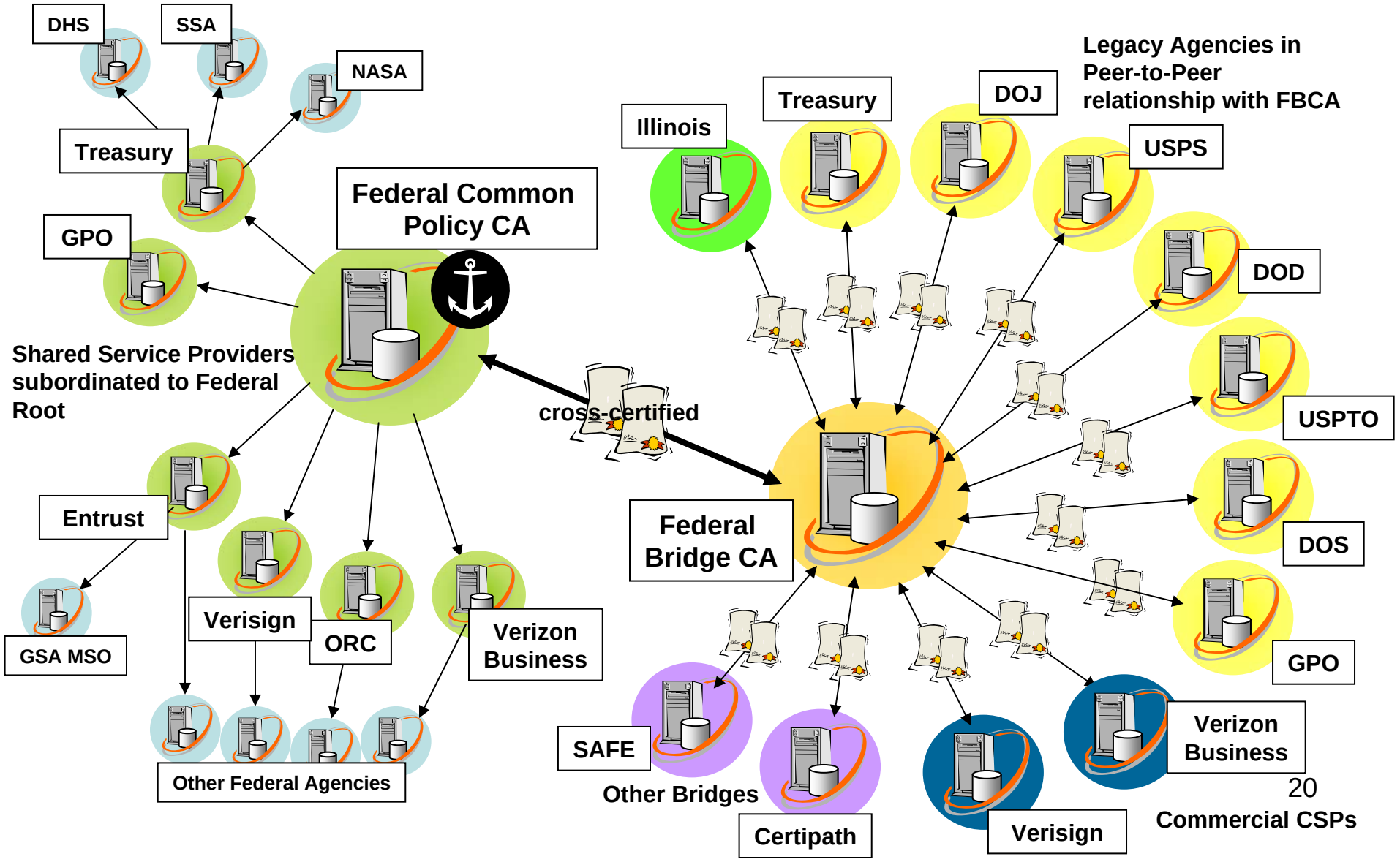
Services Framework



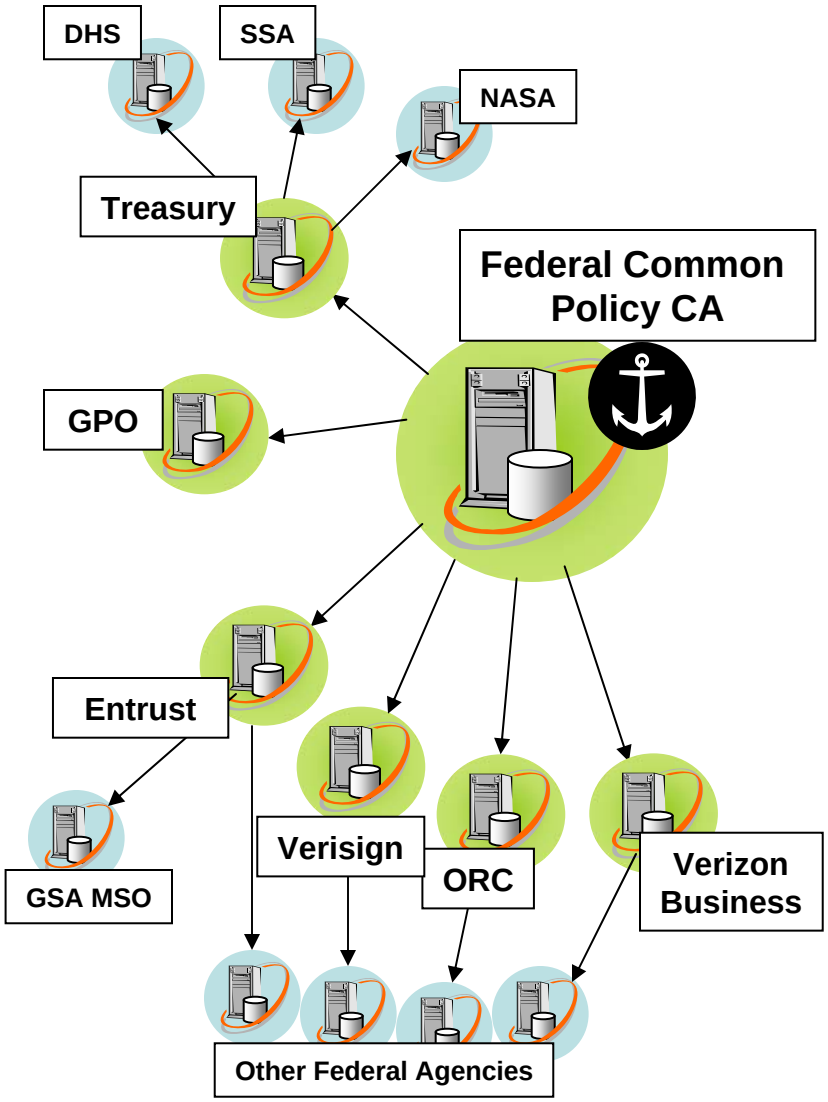
The Journey Continues

- 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
- Promote activities of Citizen Outreach Focus Group
  - Produce Solution Recommendation for the CIO Council (6 month effort – Draft in End of August)
- Continue Outreach Activities
  - Kantara (Liberty Alliance Partnership)
  - Higgins Project
  - OpenID Foundation
  - Transglobal Secure Collaboration Program (Aero/Defense)
  - Secure Access for Everyone (Bio/Pharma)
  - Educause (post-secondary education)
  - AFEI Identity Protection and Privilege Management Forum

Federal PKI Trust Framework



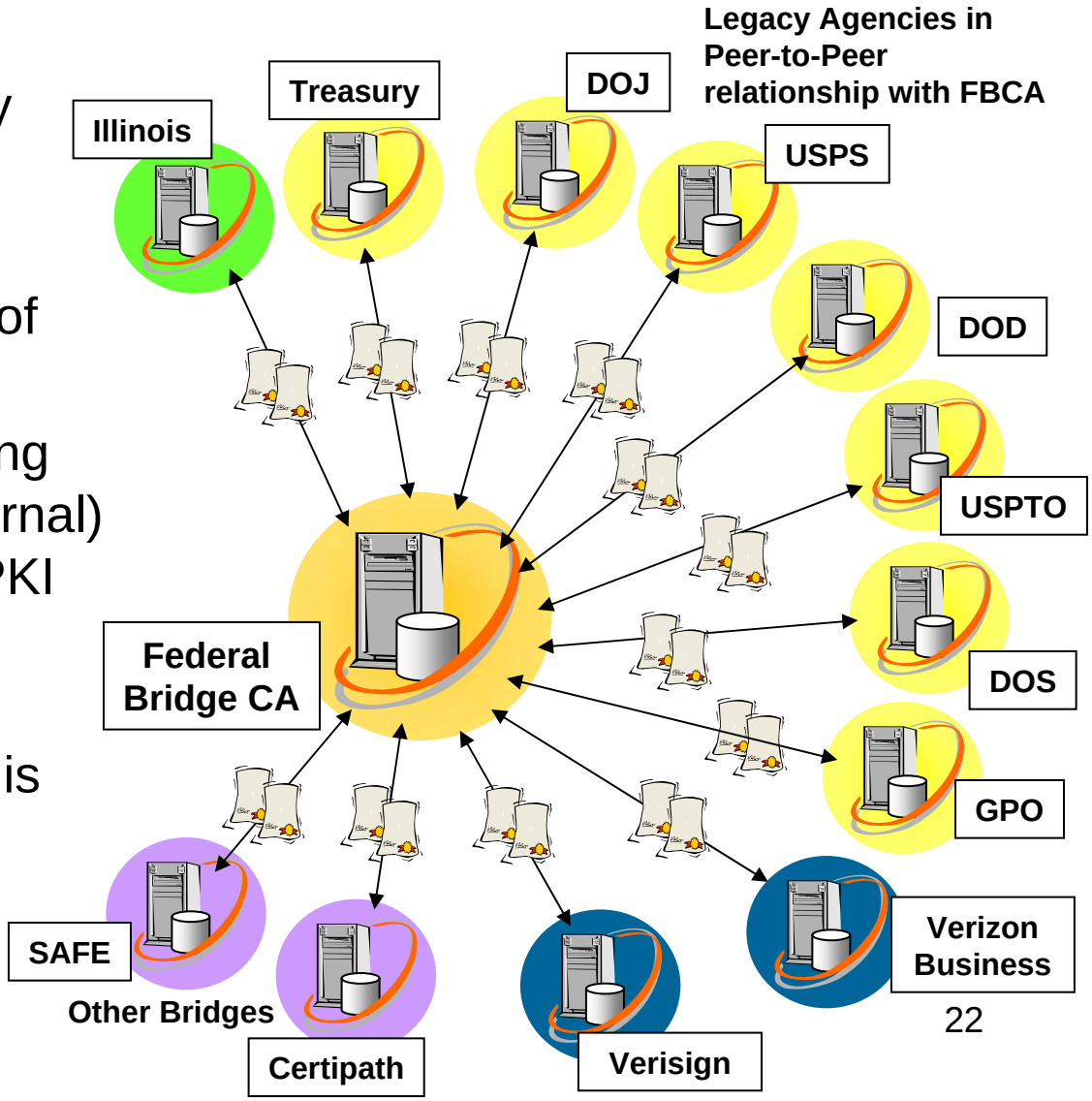
Federal Common Policy Root



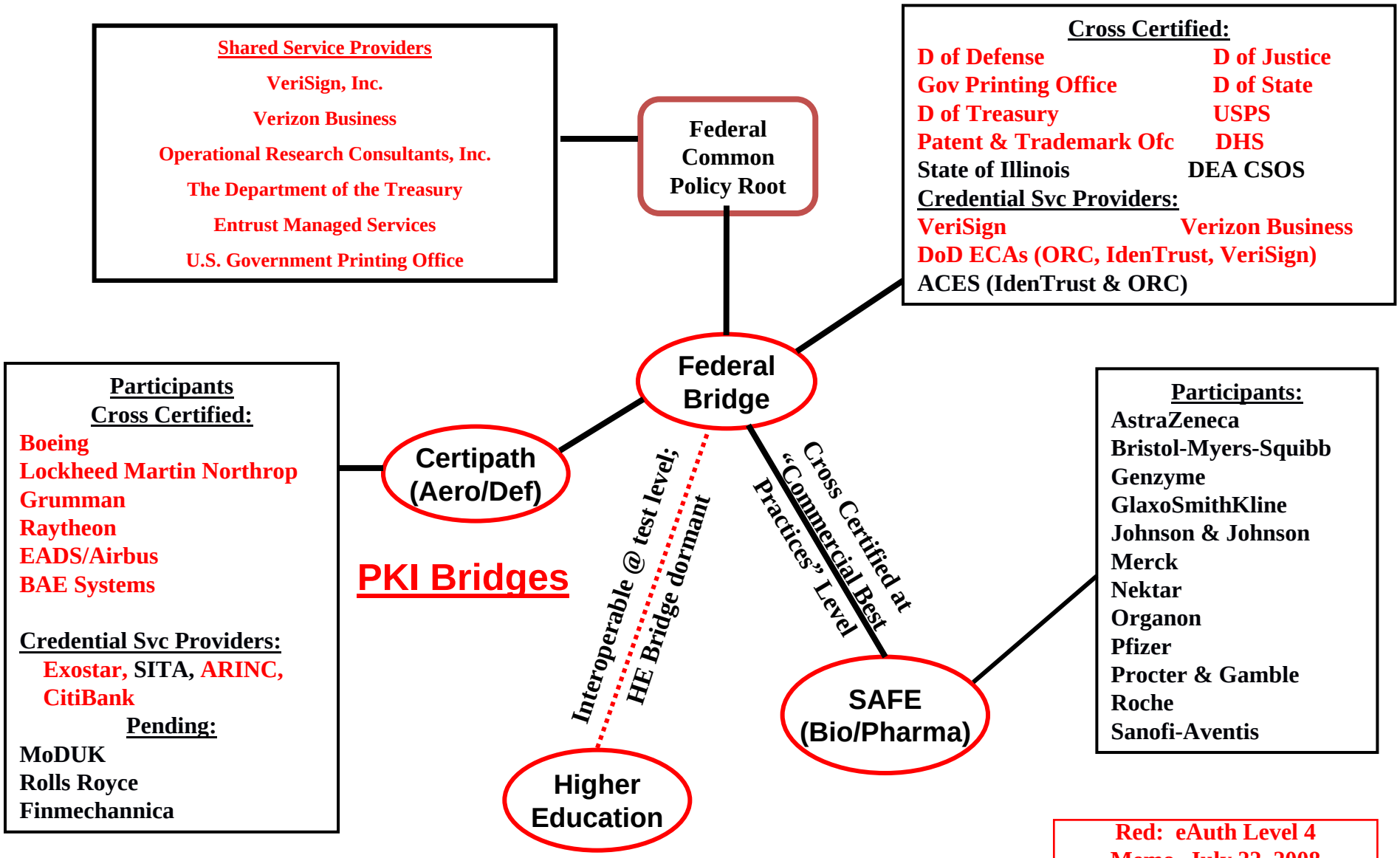
- Federal Root CA
- Per M-05-05 – Agencies should acquire PKI credentials from PKI service Providers
- Per FIPS-201 – PIV Authentication certificates must conform to the Federal Common Policy
- Common Policy Root is in the Microsoft Store, negotiations under way to include in other major browser stores.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



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

PIV Fielding Status: http://www.idmanagement.gov/drilldown.cfm?action=agency_hspd12_impl_rpt

May 2009

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.

Available at: http://www.IdManagement.Gov

Initial Guidance for Validating Credentials of Non-Federal Issuers

- Leverage Industry credentials for Government use
- Make Government more transparent to the Public
- Make it easier for American Public to access government information
- Avoid issuance of application-specific credentials
- Leverage Web 2.0 technologies
- Demonstrate feasibility with application(s) assessed at Assurance Level 1
- Support applications at higher assurance levels as appropriate

Approach

- Adopt technologies in use by industry (Scheme Adoption) . . .
- Adopt industry Trust Models (Trust Framework Adoption) . . .
- . . . While ensuring the principles of M-04-04 and SP 800-63 are observed and . . .
- . . . In a manner that promotes individual privacy protections

Scheme Adoption

Federal ICAM Identity Scheme Adoption Process, July 8, 2009.

- Scheme – specific type of authentication token and associated protocols (e.g. user ID & password; PKI; SAML assertion)
- Adoption requires reviewing technical processes of an identified "scheme" and developing a "Profile" for use with government.
- The Federal Profile defines MUSTs, SHOULDs, SHOULD nots, etc. for identity providers and relying parties
- Does not change the existing technical standard

Trust Framework Adoption

Federal ICAM Trust Framework Provider Adoption Process for Levels of Assurance 1, 2, and Non-PKI 3, July 8, 2009

- Trust Framework Provider – organization engaged in the assessment of identity providers to determine assurance level(s) inherent the identity credentials offered and conformance to Federal Scheme Profile
- Establishes the ground-rules for industry 'self-certification'
- Federal community will recognize 'assessor' organizations through "Trust Framework Adoption"
- Considers requirements of NIST SP 800-63
- Identity Providers approved via this process will be placed on a 'certified identity provider' list

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, Credible
  - 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 (= AAL-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