GMU C4I Center—AFCEA Symposium

Session 4
Identity Management

May 23, 2012

The Goal

Enabling Solutions for Identity Assurance and Critical Infrastructure Protection

How do we protect our Identity Assurance goals and critical infrastructure resources, balanced with ease of use? ---Let's start by:

- ***Providing easy and secure access for those who belong (both public and private users)***
- ***Simplifying identification verification and authorizations of visitors and network users by using federated solutions***

Identity assurance (IA) and Identity management (IM) programs for contractors and suppliers must use certified and accredited solutions and:

- ***Incorporate strong vetting for those that require network or installation and facility access and authorizations***
- ***Follow established and emerging DoD, Federal & Commercial guidelines and consensus built standards on interoperability and secure information sharing***

Access decisions must become automated, reliable & trusted.

Network Operators/Installation and Facility Owners/ Security Managers and Application Owners are ultimately responsible, so lets help to:

- ***Improve decision making capability***
- ***Make it more secure, smarter and cost efficient with available IM and IA tools and solutions***

OMB Memo 11-11
Meeting FICAM Objectives

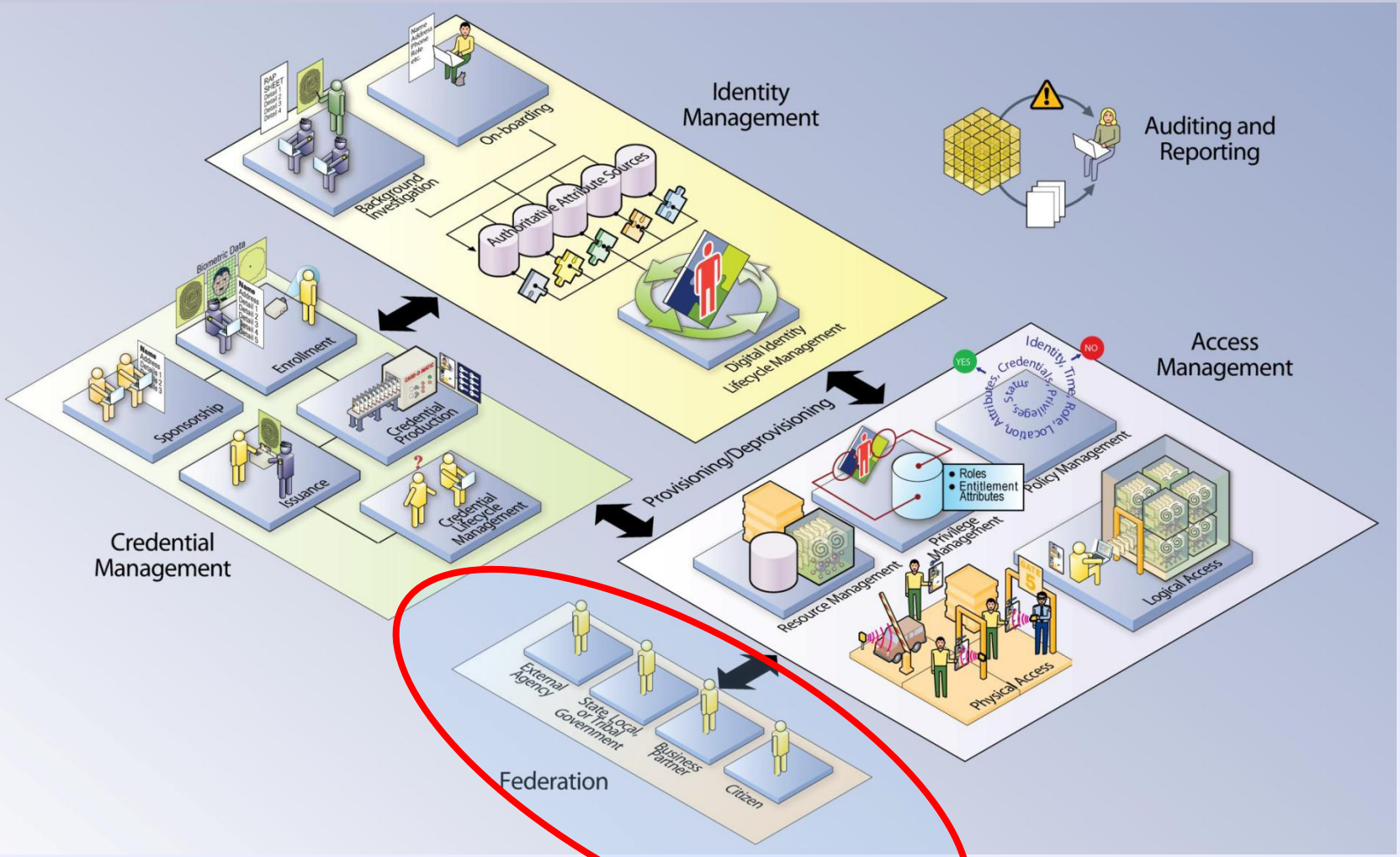


Figure 1: ICAM Conceptual Diagram

FICAM Targets

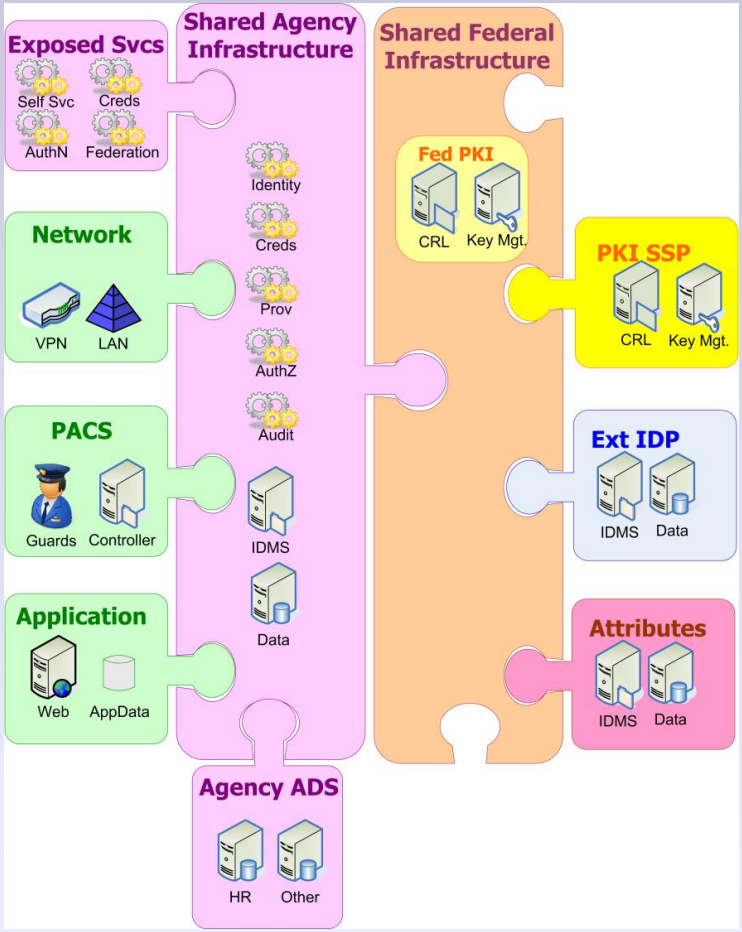


Figure 11: Federal Enterprise Target Conceptual Diagram

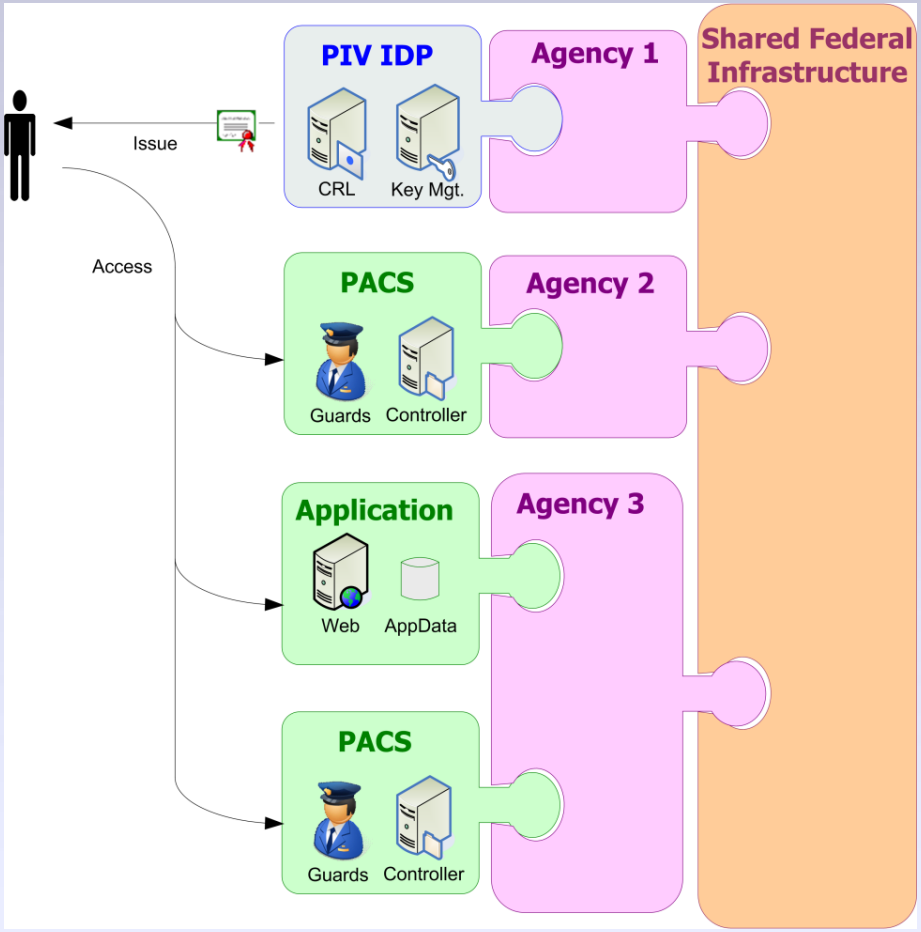


Figure 12: Federal Enterprise Target Conceptual Diagram: Cross-Agency Access

The Problem Defined

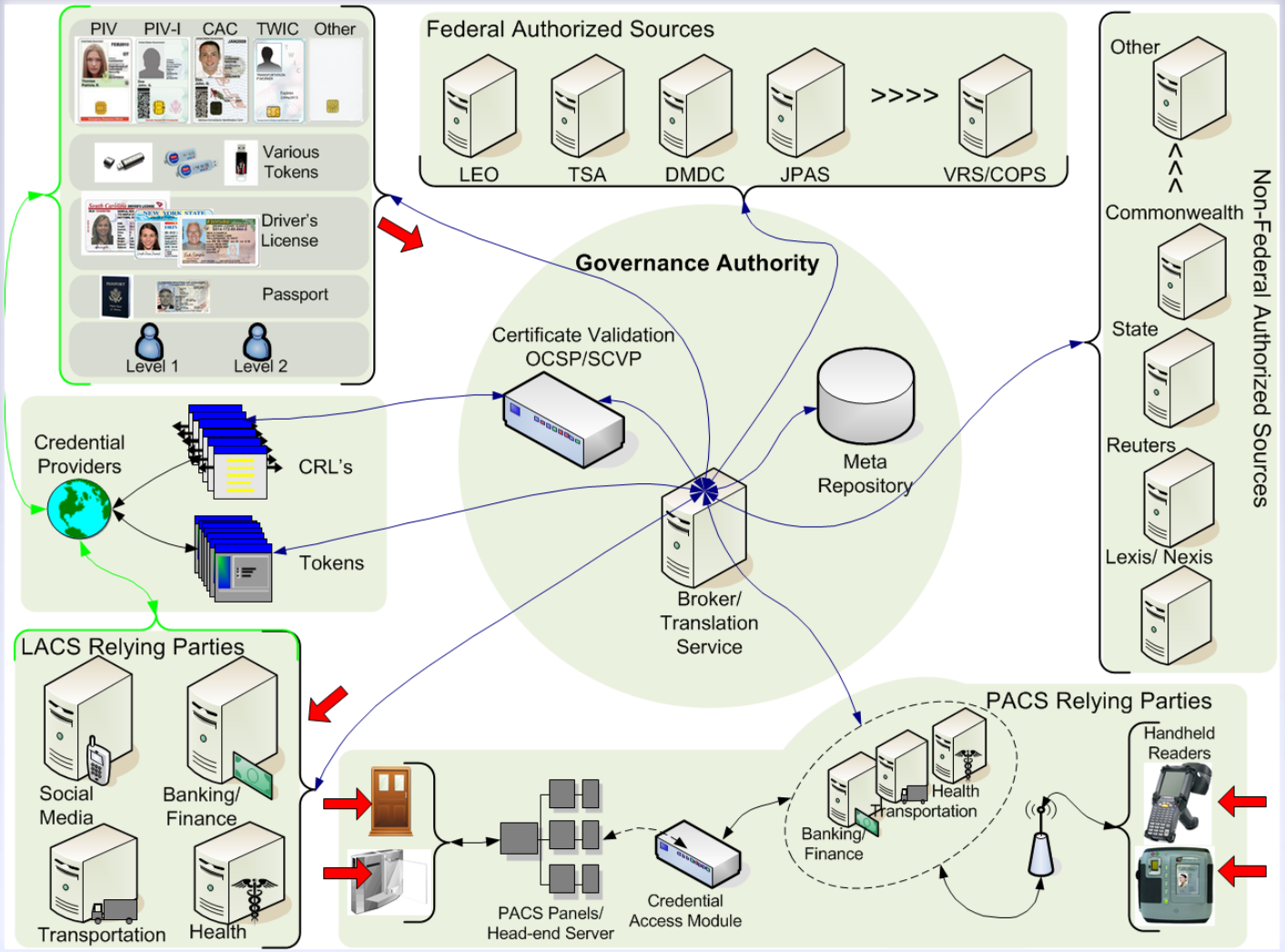
- ***Identity Assurance is a critical foundational element of information sharing and access decisions***
- ***Federal, State, Local Governments and their commercial partners have minimal/no interoperable and integrated means of trusting identity credentials issued externally.***
- ***Results:***
  - Less efficient, less effective information sharing/authentication
  - Increased costs
    - Redundant credential issuance, background check, identity management operations
  - Limited situational/resource awareness in all response and operational scenarios including cloud and mobile environments
    - Inefficient deployment of resources & lack of training/education
    - Confusion on what is acceptable solution

The Federated Identity Ecosystem Solution

Consists of an identity framework and network leveraging a common trust model, issuance, governance, revocation, and operational policies:

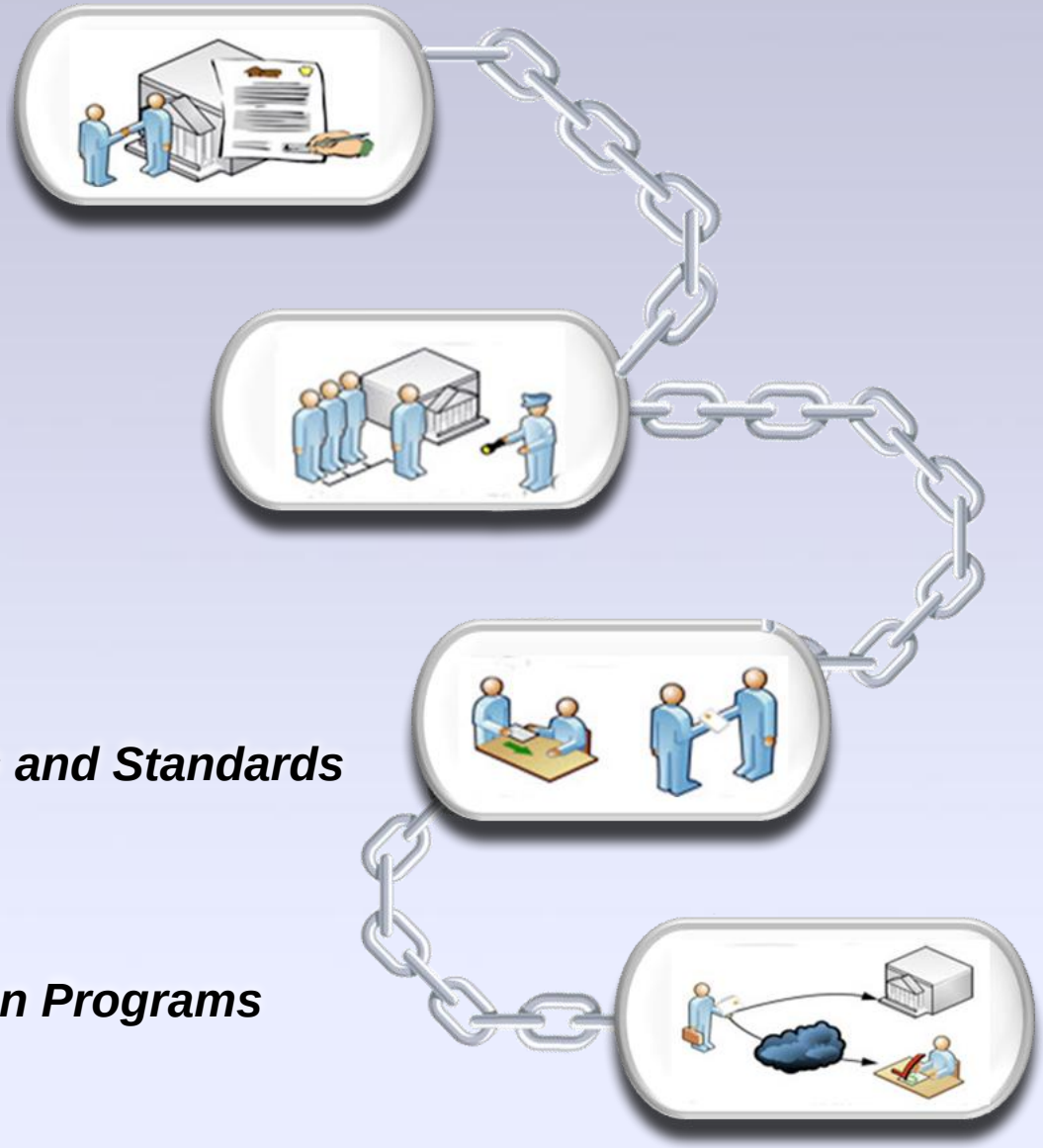
- ***Solves problems raised across disparate organizations (both government and commercial/private) by providing a strong, biometrically enabled identity credential that can be validated at any logical/physical access point***
- ***Allows a decision maker or trusted application (in either public or private environment) to make a locally-specific privilege and/or authorized ACCESS decision confident that:***
  - the identity of the person can be electronically verified
  - the organization the person represents was properly vetted
  - the individual possesses attributes he or she claims to posses
  - the organization and the individual have a legal relationship to do business with the government or commercial organization; and,
  - that the individual has been issued a credential, in person-- and has undergone a background vetting process consistent with DoD, Federal, State, Local Agency or commercially defined criteria.

Trusted Federated Ecosystem



What Sustains the Ecosystem ?

- *Defined Trust Model*
- *Legal foundation*
- *Operating Rules*
- *Security Guidelines*
- *Policy Standards*
- *Privacy Act compliance*
- *Technical Architecture Specs and Standards*
- *Implementation Guidelines*
- *Certification and Accreditation Programs*



Value Proposition and ROI

- *Easy business decision for CIO and Security officer---"identity as a service"*
- *Leverages existing organizational infrastructures*
- *It's operational TODAY for both LACS and PACS*
- *Achieves enterprise-wide capability and best practices*
- *Provides security and privacy of staff, systems, and facilities*
- *Provides method for data assurance in compliance with latest identity authentication processes*
- *Complies with FAR contract requirements*
- *Supports the FICAM Roadmap and Implementation Guidance*
- *Demonstrates leadership in a large and developing market on a matter that is of major national importance*