Smart Card Alliance

Trust Ecosystem

Stephen P. Howard
CertiPath, Inc.

Trust Ecosystem

This session will discuss the Federal trust ecosystem and how it works to enable interoperable, high assurance identity credentials that can be used across Federal agencies.

Speaker: Steve Howard, CertiPath

Topics covered will include:

- Identity Vetting
- Trusted Framework Adoption Process for Levels of Assurance 1, 2, 3
- PIV Issuer Controls
    - NIST SP 800-79, NIST SP 800-63
- FBCA Certificate Policy
    - PKI Mapping for Cross-certification and PIV/PIV-I Certification
- FICAM
- Impact to E-PACS

Logo

Smart Card Alliance

Identity Vetting

…the cornerstone of any Trust Ecosystem

…the 101 version

A Difficult Topic

- Elements of identity vetting
- In-person proofing
- Document validation
- Biometrics
- Binding
- Proof of possession

In-Person Proofing

- As is interpreted today
  - A linked session of a Trusted Agent with the Applicant
  - Trusted Agent reviews and confirms documents from the Applicant
- But… is this ***required*** to be “face to face”?

- “Video Proofing” is a new concept being worked on today
  - Cost of deploying personnel and workstations
    - Do you have a sufficient work load that will keep this investment fully engaged?
  - Cost of training
    - Do your Trusted Agents have sufficient training to do this process?

- Consider use of remote kiosk connected to a sophisticated call center
  - Think ATM model
  - Video of session (cameras see *everything* to avoid improper actions of the applicant)
  - Document scan, fingerprint capture, facial image capture, iris capture, etc.
  - Centralize expertise and reduce wasted time of FTEs and workstations

Smart Card Alliance

Document Validation

- With over 14,000 birth certificate formats in the United States
  - How can ***anyone*** properly vet these credentials?

- The key is to have a non-confrontational session between the Trusted Agent and the Applicant
  - Scan/verify documents
  - Move through the process of enrollment
  - Defer "issuance" and allow session to end at enrollment

- Getting document exemplars
  - Very difficult
  - Limited (in general) to law enforcement
    - These are bad documents as examples allowing a trained individual to look for bad features

Biometrics

- Timing is everything
  - Make sure the Applicant, presenting documentary evidence to the Trusted Agent, is the same individual whose biometrics are captured
- Substitution of individual is not difficult

- Manage issues of §508
  - Can not capture fingerprints
    - No hands
    - Worn
  - Iris

Binding

- Linking
  - Individual
  - Identity vetting
  - Biometrics
  - Issued credential

- The issued credential enables relying parties to understand the integrity of the credential and its Level of Assurance

Proof of Possession

- How does the issued credential get used to demonstrate the correct individual is asking for access?

- LOA 1
  - Userid/Password

- LOA 4
  - Full challenge response demonstrating “holder of key” for that specific credential

Summary: Identity Vetting

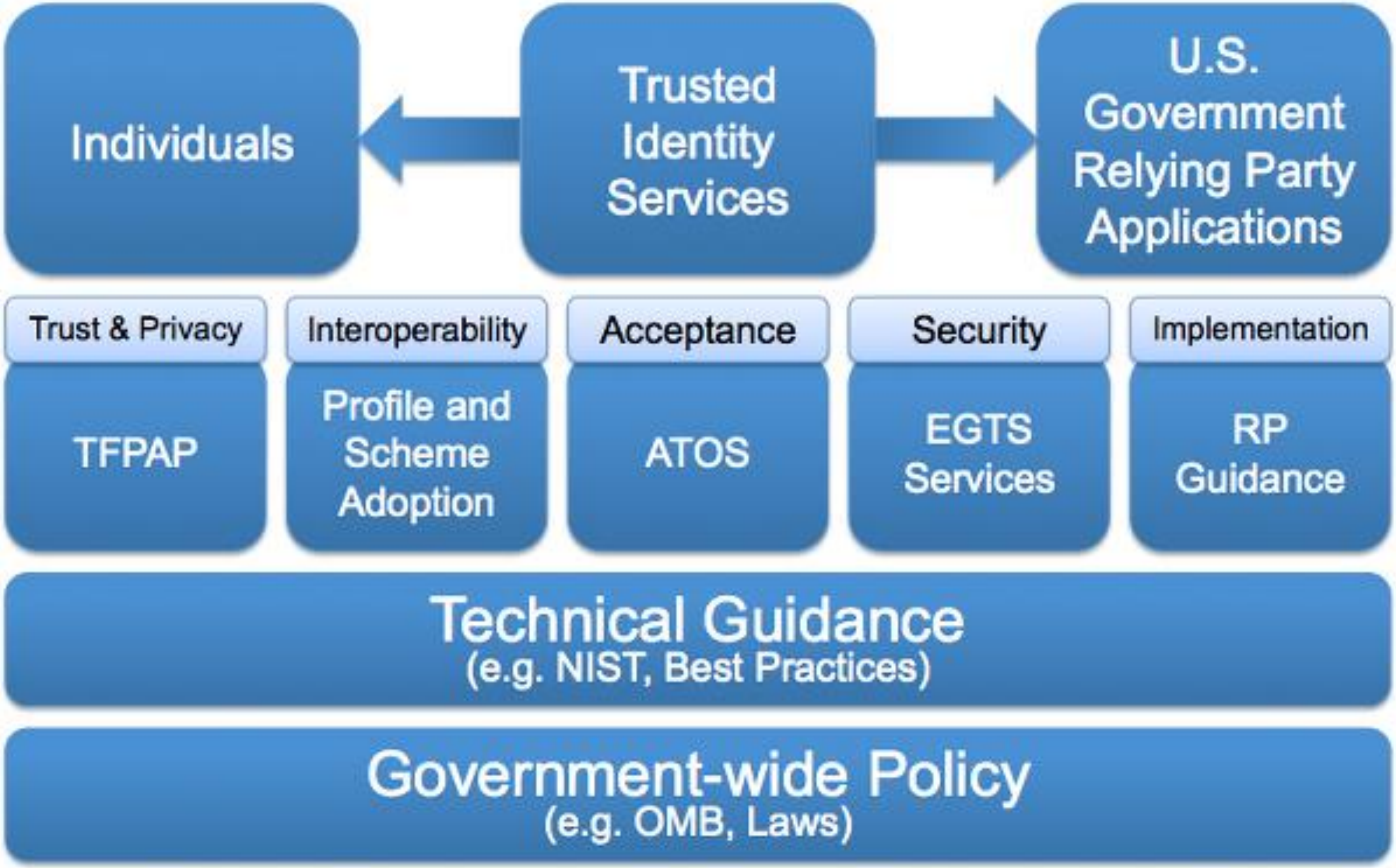
- The rules for identity vetting are determined by a chosen Trust Framework
  - Trust Framework, through TFAP, is mapped to OMB M-04-04
    - Level 1 – Little or no confidence in the asserted identity's validity
    - Level 2 – Some confidence in the asserted identity's validity
    - Level 3 – High confidence in the asserted identity's validity
    - Level 4 – Very high confidence in the asserted identity's validity
- As a relying party, you must decide what level is sufficient and/or required
- As a critical element, can the technology
- Very high confidence in the asserted identity's validity ***prove*** that you are indeed granting access to the correct individual
  - "Proof of Possession"
  - Biometrics

FICAM Trust Framework Adoption Process
Levels 1 – 3
…and…
Level 4

Policy Driving TFAP – This is OLD Stuff

- **Government Paperwork Elimination Act** (P.L. 105-277), October 21, 1998
- **E-Government Act §203** (P.L. 104-347), 2001
- OMB policy Memorandum, ***Streamlining Authentication and Identity Management within the Federal Government***, July 3, 2003
  - reducing "*... the burden on the public when interacting with government by allowing citizens to use existing credentials to access government services and enabling new services that otherwise could not or would not have been available*"
- OMB policy Memorandum, ***Requirements for Accepting Externally-Issued Identity Credentials***, October 6, 2011
  - Requires agencies to enable externally-facing applications to accept third-party credentials.
- **OMB M-11-11**, February 2011
- **National Strategy for Trusted Identities in Cyberspace (NSTIC)**, April 2011
  - Federal Government to be an early adopter of services under an Identity Ecosystem by "its own participation in the Identity Ecosystem as both a subject and relying party."

TFAP in a Nutshell

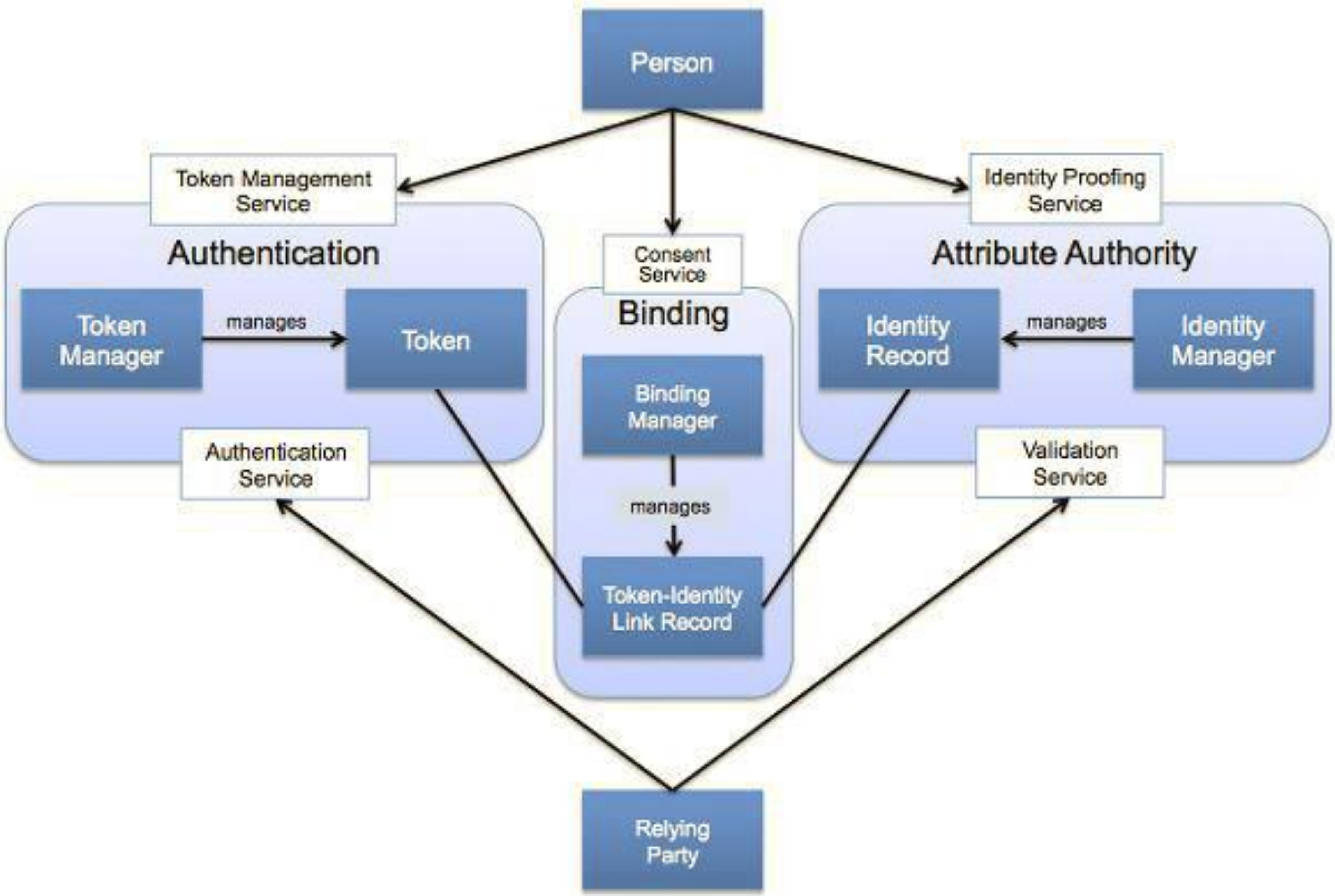


Seven Trust Criteria

1. **Registration and Issuance** – How well does the CSP register and proof the identity of the credential applicant, and issue the credential to the approved applicant?
2. **Tokens** – What is the CSP's token technology and how well does the technology intrinsically resist fraud, tampering, hacking, and other such attacks?
3. **Token and Credential Management** – How well does the CSP manage and protect tokens and credentials over their full life cycle?
4. **Authentication Process –** How well does the CSP secure its authentication protocol?
5. **Assertions –** How well does the CSP secure Assertions, if used, and how much information is provided in the Assertion?
6. **Ongoing Verification –** What compensating controls does the CSP implement that provides an ongoing identity verification capability? [OPTIONAL]
7. **Privacy –** How well does the privacy policies of the CSP adhere to the Fair Information Practice Principles?

Smart Card Alliance

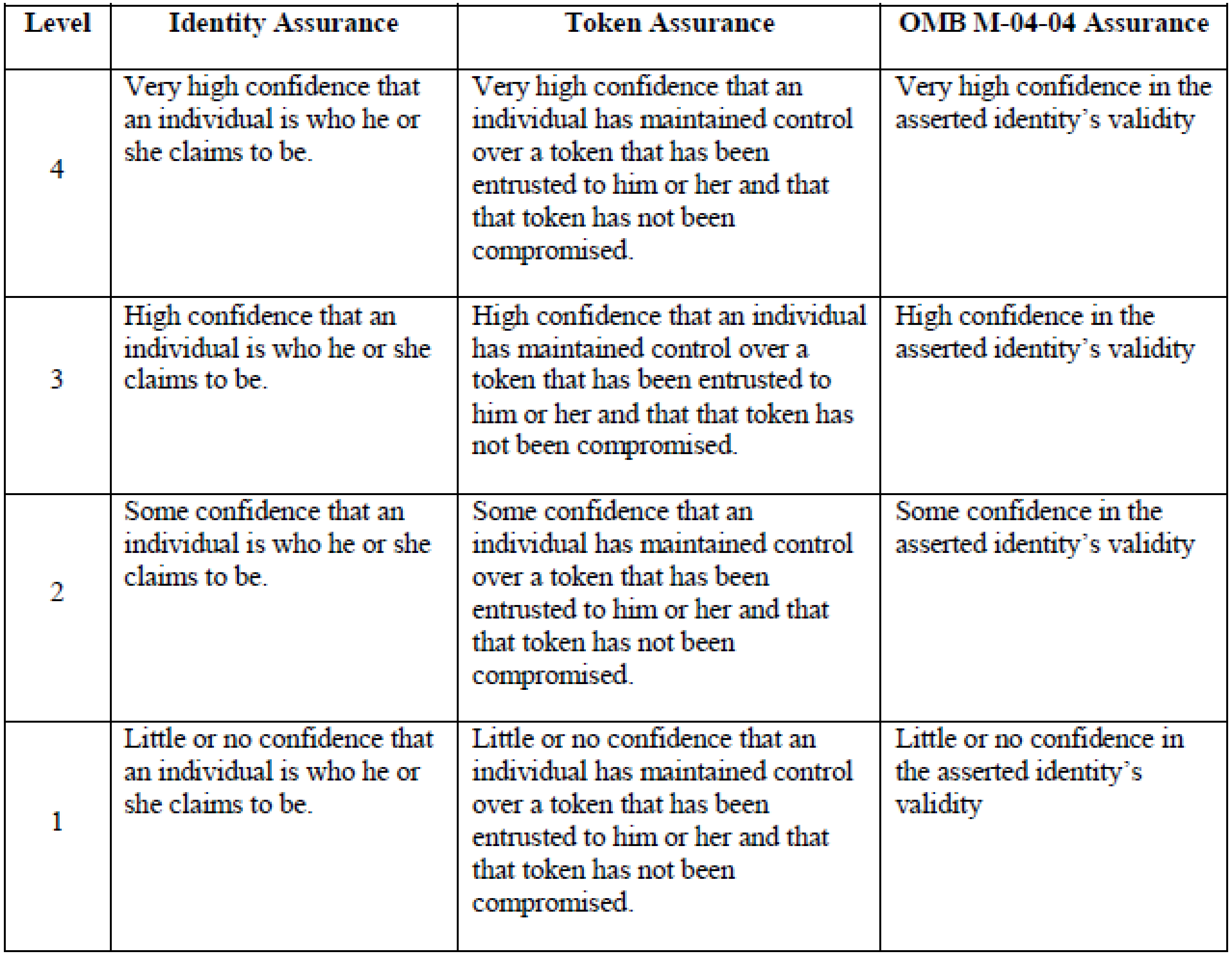
RA and CSP in SP 800-63



LOA terminology for credential assurance

- **Level of Assurance (LOA)**: Per OMB M-04-04, assurance is defined as 1) the degree of confidence in the vetting process used to establish the identity of an individual to whom the credential was issued, and 2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued.
- **Token Assurance Level (TAL)**: The degree of confidence that that an individual, organization or device has maintained control over what has been entrusted to him or her (e.g., token, identifier) and that the token has not been compromised (e.g., tampered with, corrupted, modified).
- **Identity Assurance Level (IAL)**: The degree of confidence that an individual, organization or device is who or what it claims to be.

TFAP Clarification for Assurance Levels



Level	Identity Assurance	Token Assurance	OMB M-04-04 Assurance
4	Very high confidence that an individual is who he or she claims to be.	Very high confidence that an individual has maintained control over a token that has been entrusted to him or her and that that token has not been compromised.	Very high confidence in the asserted identity's validity
3	High confidence that an individual is who he or she claims to be.	High confidence that an individual has maintained control over a token that has been entrusted to him or her and that that token has not been compromised.	High confidence in the asserted identity's validity
2	Some confidence that an individual is who he or she claims to be.	Some confidence that an individual has maintained control over a token that has been entrusted to him or her and that that token has not been compromised.	Some confidence in the asserted identity's validity
1	Little or no confidence that an individual is who he or she claims to be.	Little or no confidence that an individual has maintained control over a token that has been entrusted to him or her and that that token has not been compromised.	Little or no confidence in the asserted identity's validity

Level 1

- **FICAM TFS Program DOES NOT RECOMMEND the use of Level 1 Identity Services in e-authentication transactions that require assurances of identity**
  - Decreasing the burden to individuals in having to manage multiple identity credentials
  - Explore and validate new protocols and approaches in an environment that has minimal security and privacy risk
  - Reduce, to some degree, the infrastructure and operational costs to Government in managing Level 1 credentials or services
  - Ensure that there exists a pool of identity services operating in a manner that protects the information that an applicant/individual has entrusted to it.

- The majority of high value citizen facing services require assurances of identity that range from level 2 to level 4

Level 4

- **PKI Authentication and Federation**
- PKI Credentials in a federation can be used in three use cases:
  - Presented directly to the RP and validated by the RP (Not a federation use case per se, but provided for the sake of completeness)
  - Presented to a CSP, which validates the credential and generates a bearer assertion to the RP
  - Presented to a CSP, which validates the credential and generates a holder-of-key assertion to the RP

Levels 2 & 3

- Hmmm… Why not a lot more detail here?

- This is the main body of work driven by NSTIC and TFAP
  - But these are generally new technologies and/or protocols

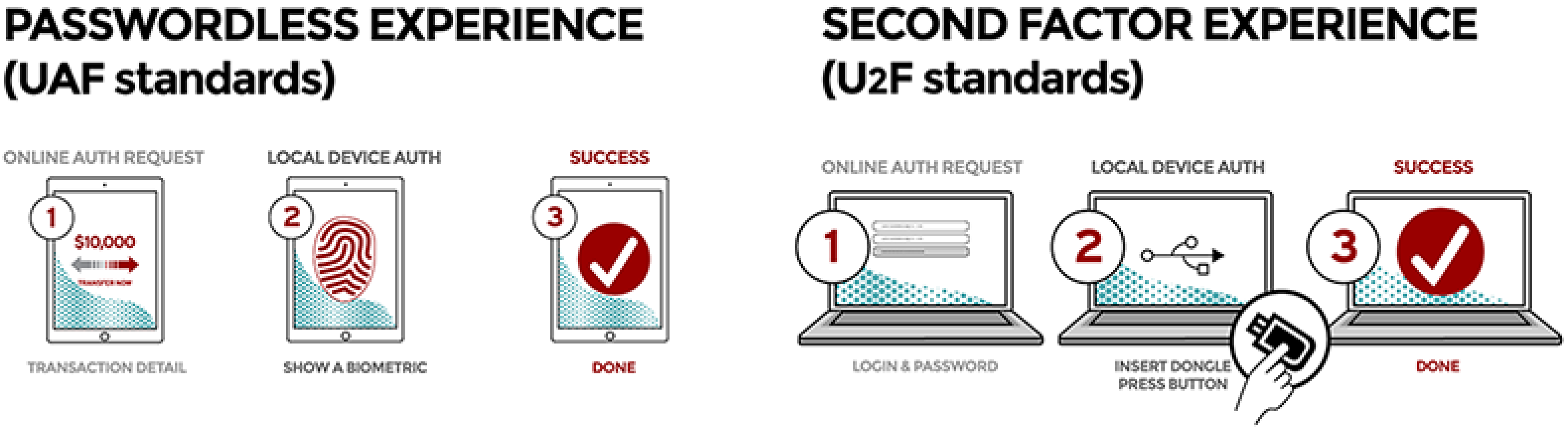
- Perfect examples of the challenge
  - External credentials: **Google's FIDO Alliance U2F** (next slide)
  - Internal credentials: **PIV Derived Credentials** on mobile phones

- Can these credentials be used for E-PACS
  - As a general concept, probably
  - More work needed
  - Very much a risk based decision

Smart Card Alliance

FIDO

- The Mission of the FIDO Alliance is to change the nature of online authentication by
  - Developing technical specifications that define an open, scalable, interoperable set of mechanisms that reduce the reliance on passwords to authenticate users.
  - Operating industry programs to help ensure successful worldwide adoption of the Specifications.
  - Submitting mature technical Specification(s) to recognized standards development organization(s) for formal standardization.



How Will This Affect E-PACS

- Level 1 is most likely “out of the question”
- Level 4 credentials are supported
  - PIV/PIV-I credentials
  - As tested and certified by the FIPS 201 Evaluation Program APL

- How will Levels 2-3 apply?
  - Unclear to me (yes, this is a real cop-out)
  - First to operational use will be from DoD using PIV Derived PKI credentials on mobile smartphones

Smart Card Alliance

PIV Issuer Controls…

…NIST SP 800-79

Relying Party Controls…

…NIST SP 800-63

PIV Issuer Controls

- NIST SP 800-79-1, *Guidelines for the Accreditation of Personal Identity Verification Card Issuers*, June, 2008

- Being a PIV issuer is a highly regulated activity
- Union of two documents
  - FIPS 201-2
    - Requirements for a credential to represent employer/employee relationship
  - Federal Common Policy
    - Over 400 controls
    - Binary: yes/no

- SP 800-79-1 focuses on making sure everything is done correctly
  - PCI Roles and Responsibilities
  - Preparing for a PCI's Assessment
  - Accreditation Decisions (with risk involved)
  - PCI Controls

Relying Party Controls

- NIST SP 800-63-2, *Electronic Authentication Guideline*, August 2013
- Core document defining
  - Multi-factor authentication
  - Tokens and token threats
  - Token and Credential Management
    - Threats and mitigation strategies
    - Assurance levels

- Over 111 pages long
  - What controls apply to my application (E-PACS)?
  - This is a risk based decision by the relying party

FBCA Certificate Policy
PKI Mapping for Cross-certification…

…PIV/PIV-I Certification

Mapping… You Really Don't Want to Know
…No One Gets to Meet the Wizard, No Way, No how!

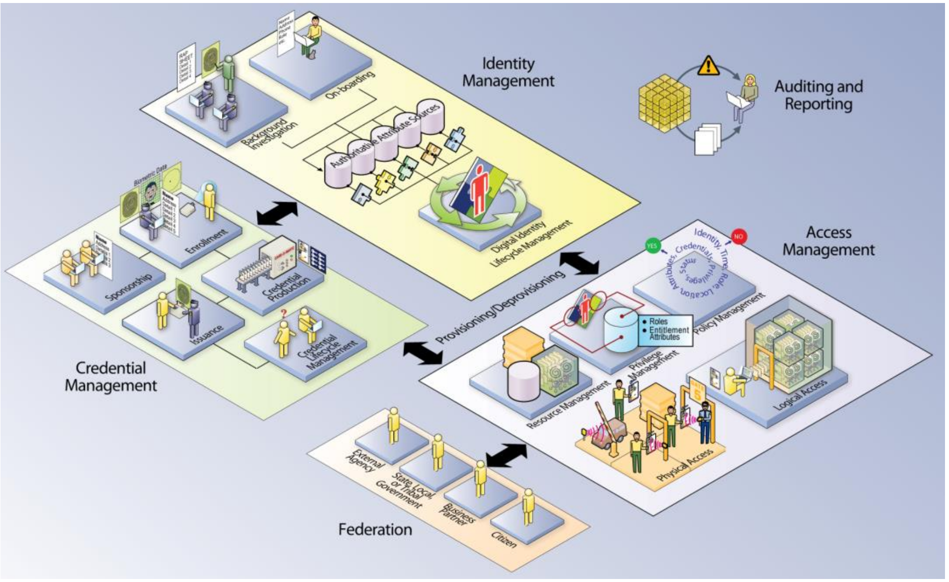
CertiPath CP Section	Entity CP Section	CertiPath CP Section Title	CP Mapping Verdict
3.2.2	3.2.2	Authentication of Organization Identity	Complies
§ 4 of the Entity CP was examined in addition to 3.2.2 to ensure that the PMA and/or the OA verify the organization authority of cross certified CAs.			
3.2.3	3.2.3; 3.2.3.1;	Authentication of Individual Identity	Equivalent
3.2.3.1	3.2.3.2	Authentication of Component Identities	Equivalent
3.2.3.2	none	Human Subscriber Re-Authentication	Complies
Absence of this section in the Entity CP is acceptable. This means that the Entity does not plan to use the re-authentication option; it will use initial identity proofing approach.			
3.2.3.3	3.2.3.3	Initial Identity Proofing Via Antecedent Relationship	Equivalent
3.2.3.4	3.2.3.4	Authentication of Human Subscribers for Role Certificates	Equivalent
3.2.4	3.2.4	Non-verified Subscriber Information	Identical
3.2.5	3.2.5	Validation of Authority	Complies
§ 4 was reviewed to ensure that it contains appropriate requirements.			
3.2.6	3.2.6	Criteria for Interoperation	Comparable

FICAM…

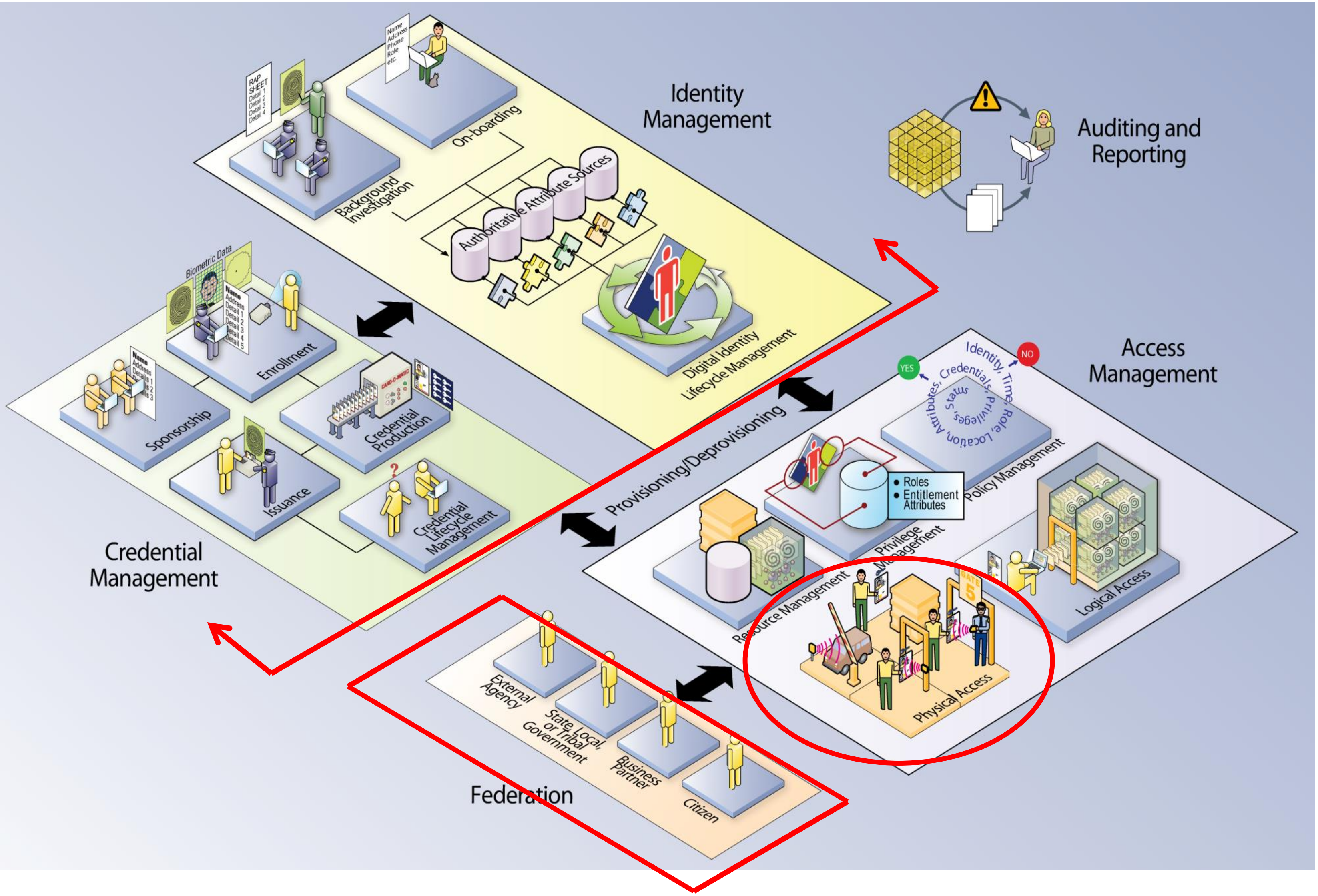
…two slides say it all

What is ICAM? (and ICAM Roadmap)

- ICAM represents the intersection of digital identities, credentials, and access control into one comprehensive approach
- Key ICAM Service Areas Include:
  - Digital Identity
  - Credentialing
  - Privilege Management
  - Authentication
  - Authorization & Access
  - Cryptography
  - Auditing and Reporting



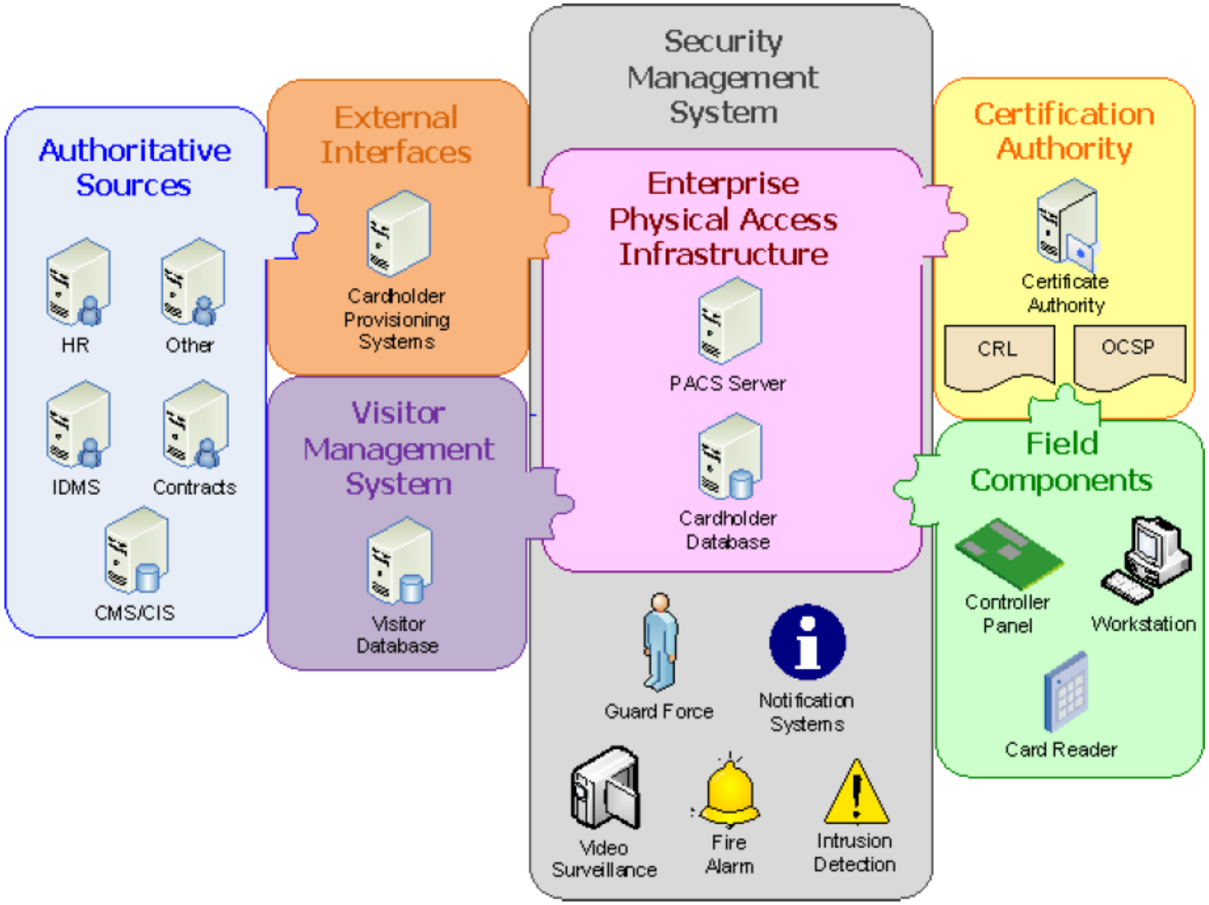
ICAM Foundational Architecture


Identity Management
Name Address Phone Role etc.
On-boarding
RAP SHEET Detail 1 Detail 2 Detail 3 Detail 4
Background Investigation
Authoritative Attribute Sources
Digital Identity Lifecycle Management
Auditing and Reporting
Credential Management
Biometric Data
Name Address Detail 1 Detail 2 Detail 3 Detail 4 Detail 5
Enrollment
Name Address Detail 1 Detail 2 Detail 3
Sponsorship
CARD-O-MATIC
Credential Production
Issuance
Credential Lifecycle Management
Provisioning/Deprovisioning
Access Management
YES
NO
Identity, Time, Role, Location, Attributes, Credentials, Status, Privileges
Policy Management
Roles
Entitlement
Attributes
Privilege Management
Resource Management
Logical Access
GATE 5
Physical Access
Federation
External Agency
State, Local, or Tribal Government
Business Partner
Citizen

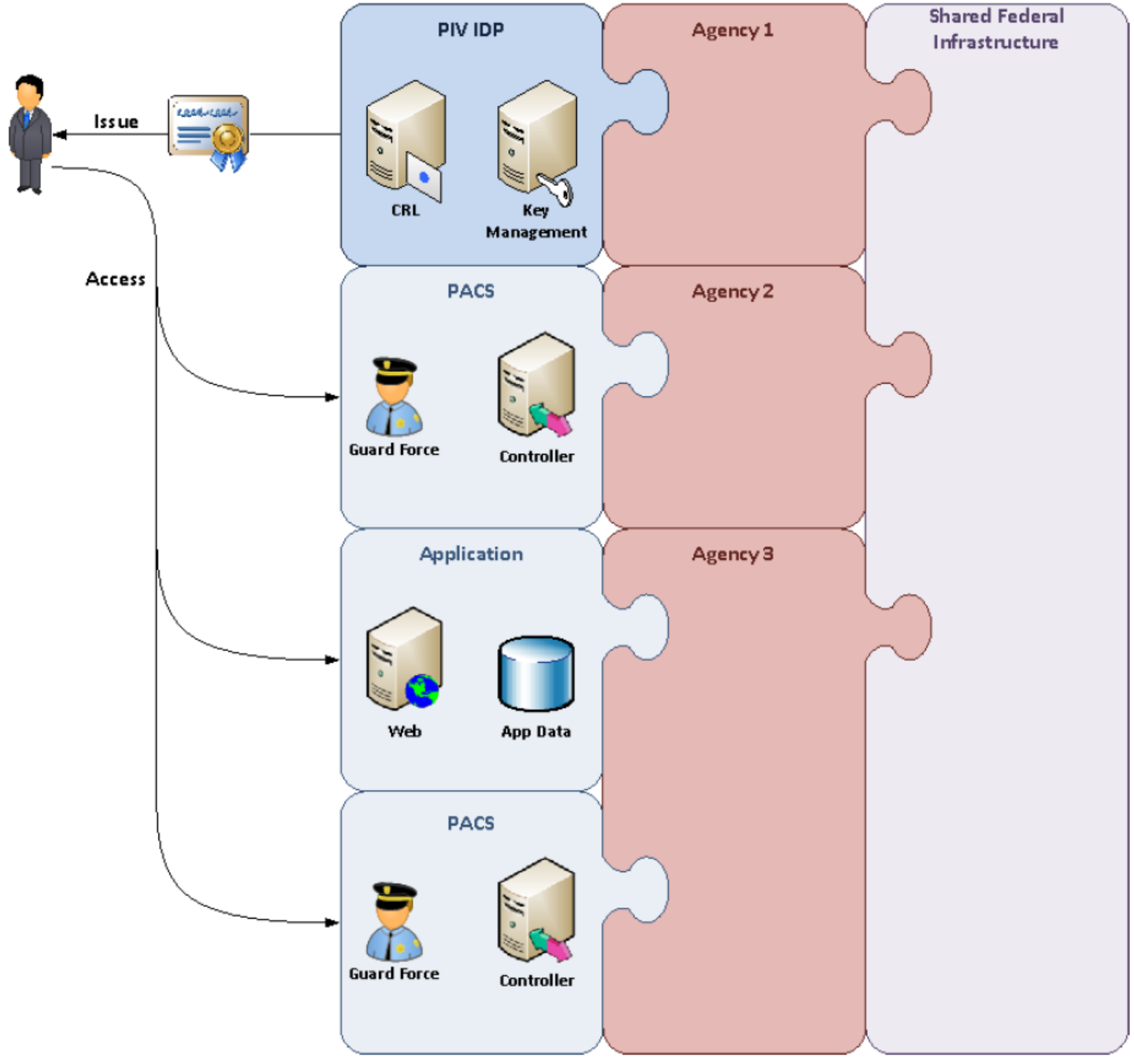
PACS/LACS Convergence…

…Concepts and Maturity Model

FICAM Roadmap Overview of PACS within the Overall Infrastructure



FICAM Roadmap Federal Enterprise Target Conceptual Diagram



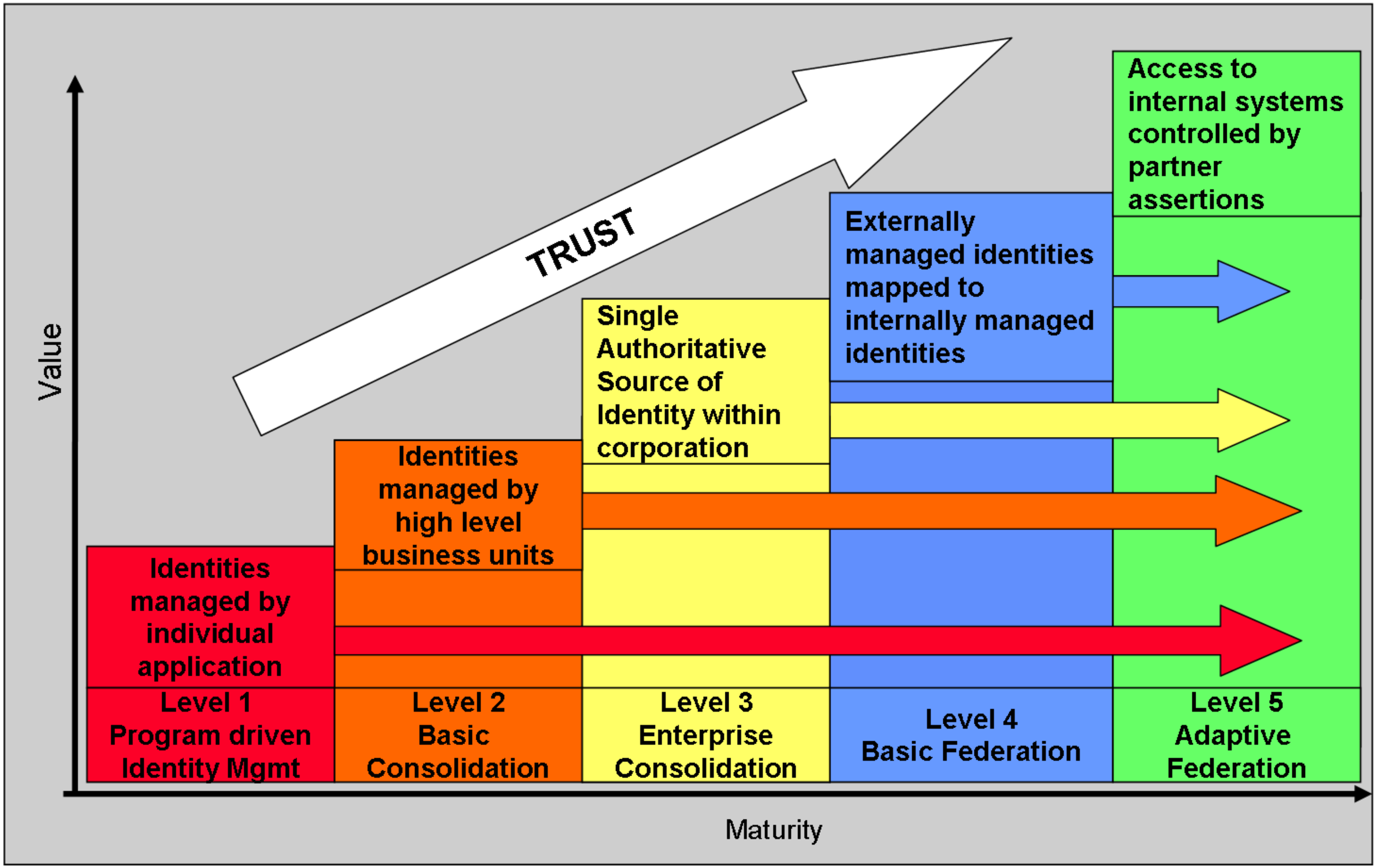
PACS and LACS are the Same Thing!

- Share 75% of the same words
- Share 100% of the same objectives
- At would seem to be able to share at least as much

- Access control for resource granting in any situation
  - Having an identity token that represents identity alone, not attributes
    - Hallmark of PIV/PIV-I
- Access control decision points can stand in front of ***ANY*** resource
  - Policy Decision Points
  - Policy Enforcement Points
- XACML is reasonably successful for LACS
  - Why not PACS?

- Ultimately, access is access
  - Common tools simplify the infrastructure , operations and maintenance

Maturity Model – a 2010 Draft



Value
TRUST
Access to internal systems controlled by partner assertions
Externally managed identities mapped to internally managed identities
Single Authoritative Source of Identity within corporation
Identities managed by high level business units
Identities managed by individual application
Level 1
Program driven Identity Mgmt
Level 2
Basic Consolidation
Level 3
Enterprise Consolidation
Level 4
Basic Federation
Level 5
Adaptive Federation
Maturity

Created by Jeff Nigriny, CertiPath, Inc.

Summary

Access is Access

- FICAM is all about
  - Identity ONCE
    - One person
    - One identity vetting event
    - One capture of biometrics
    - One binding of individual to credential
  - Use identity and credential EVERYWHERE
    - Proof of possession

- Re-use is the key
  - Policy Decision Points
  - Policy Enforcement Points

- Merging Trust Frameworks into E-PACS
  - LACS/PACS convergence in the next generation
  - The cornerstone of long term success
  - Enhanced situational awareness
  - Enhanced security, control, safety of facilities and personnel