Smart Card Alliance

Certified System Engineer ICAM PACS Training and Certification Program

Lars R. Suneborn, CSCIP/G, CSEIP
Director, Training Programs
Smart Card Alliance
O: 1 703 794 7662
M: 1 703 904 2389
Lsuneborn@Smartcardalliance.org

191 Clarksville Road
Princeton Junction, New Jersey 08550
WWW.SMARTCARDALLIANCE.ORG

Certification Training for E-PACS

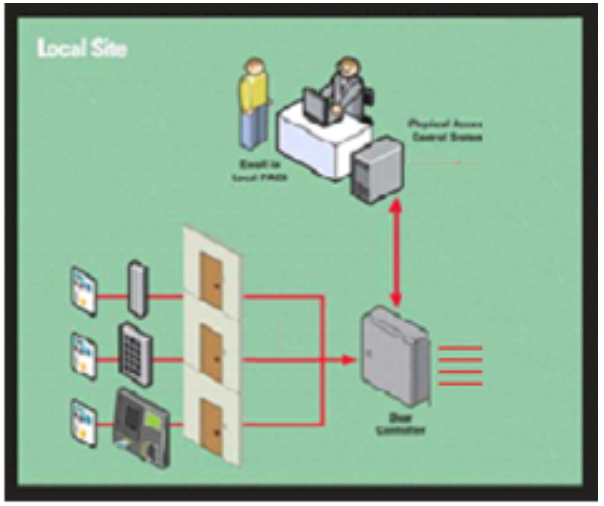
- Why this program is created
- Why agencies are requiring this certification
- Who will benefit from attending the course

Smart Card Alliance

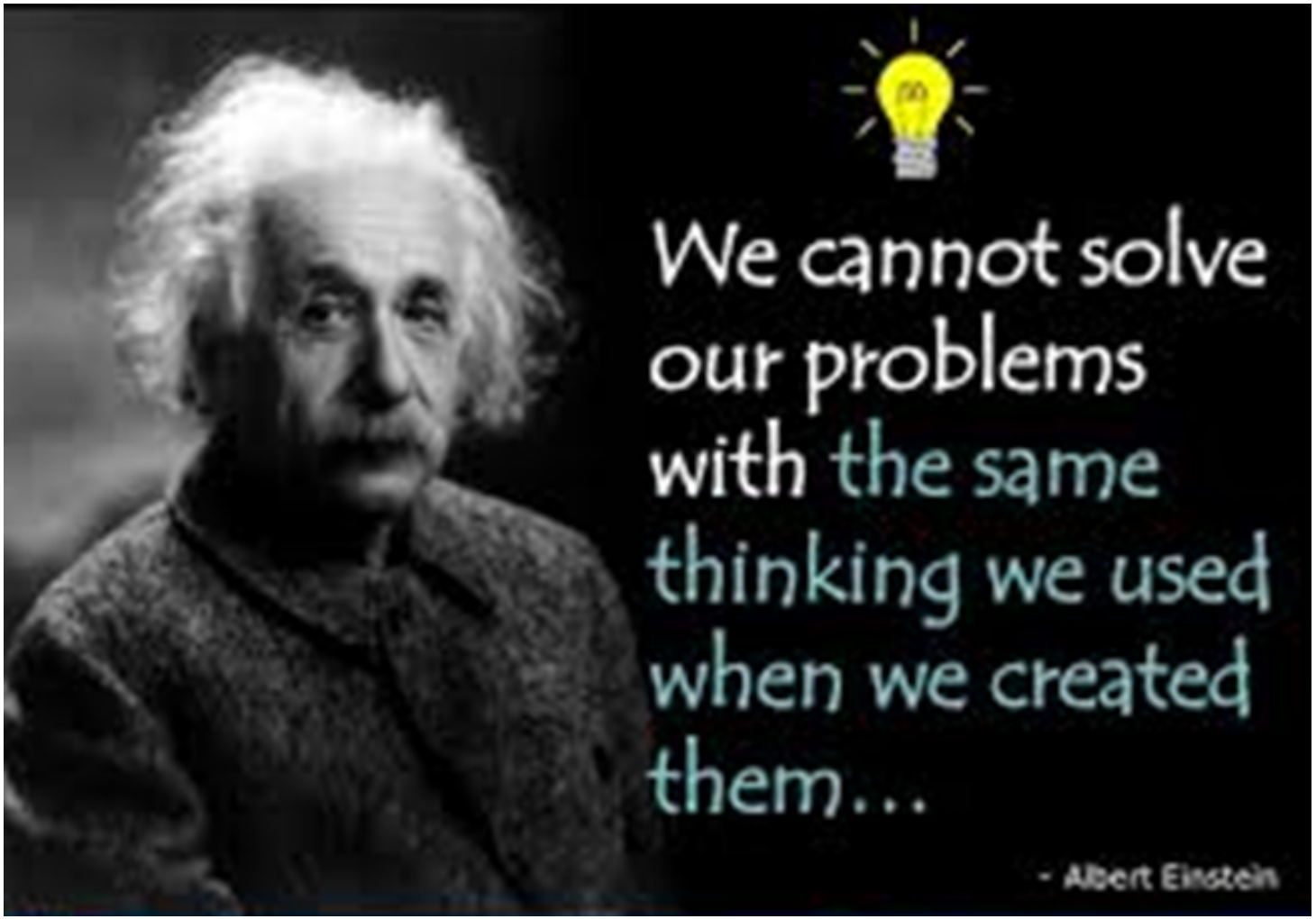
CSEIP program goal

- Enhance “Right First Time” success rate

Very different from traditional PACS: Site-centric credential



New approaches

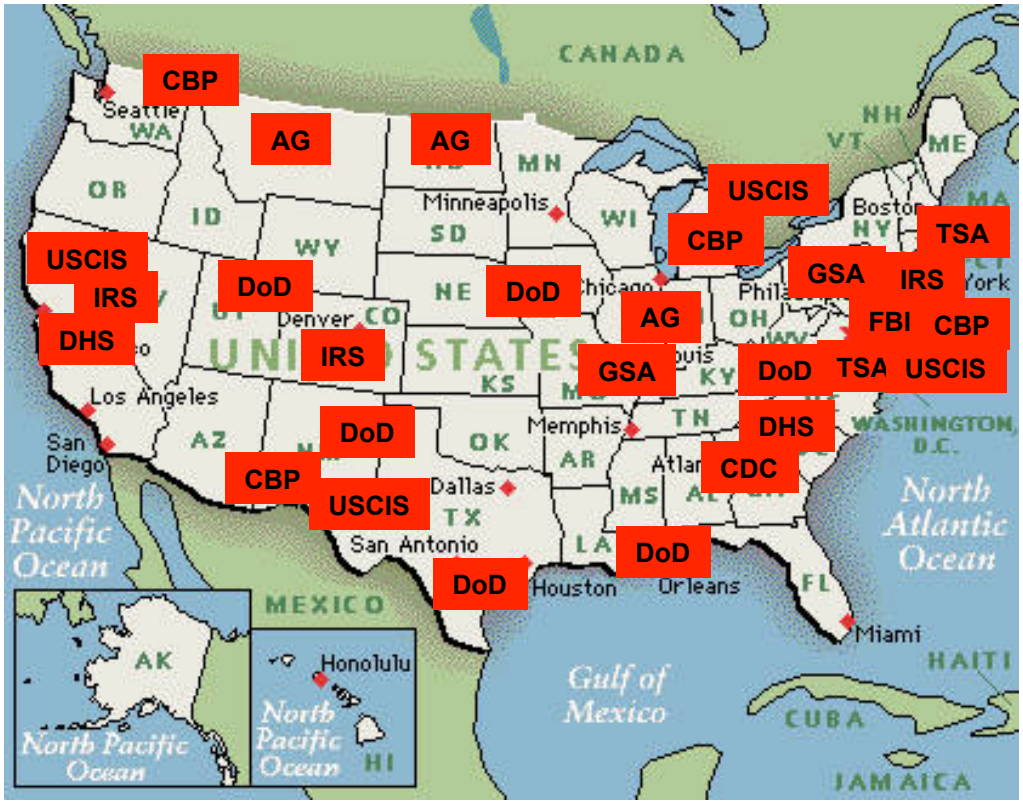


Smart Card Alliance

FICAM ePACS: Identity centric credential

Interoperability:

- Issuers
- Agencies



PACS adapt to PIV High Assurance Cards

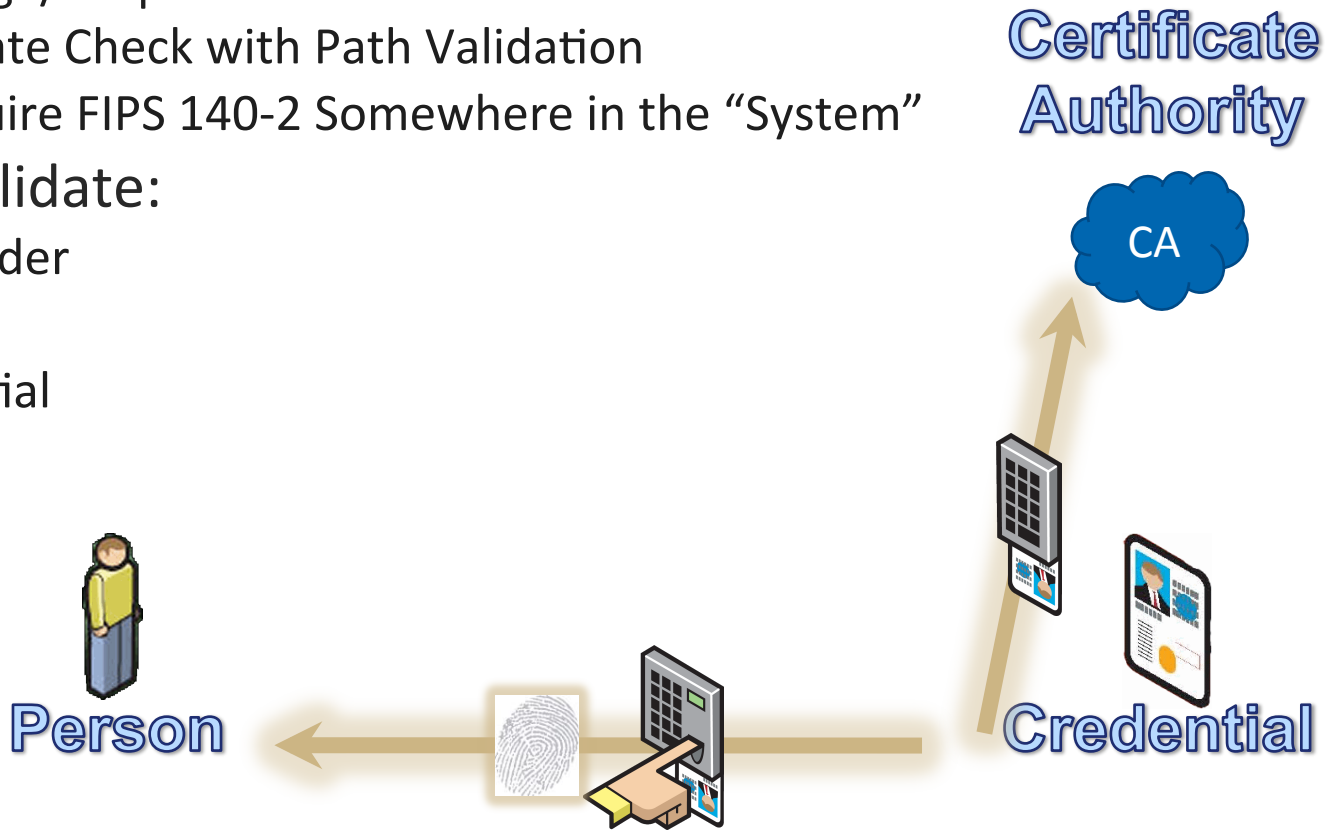
- Interoperability??
- FASC-N, UUID??
- Resistance to manipulation, cloning??
- E authentication??
- Assurance in ID??

Table 6-2. Authentication for Physical Access

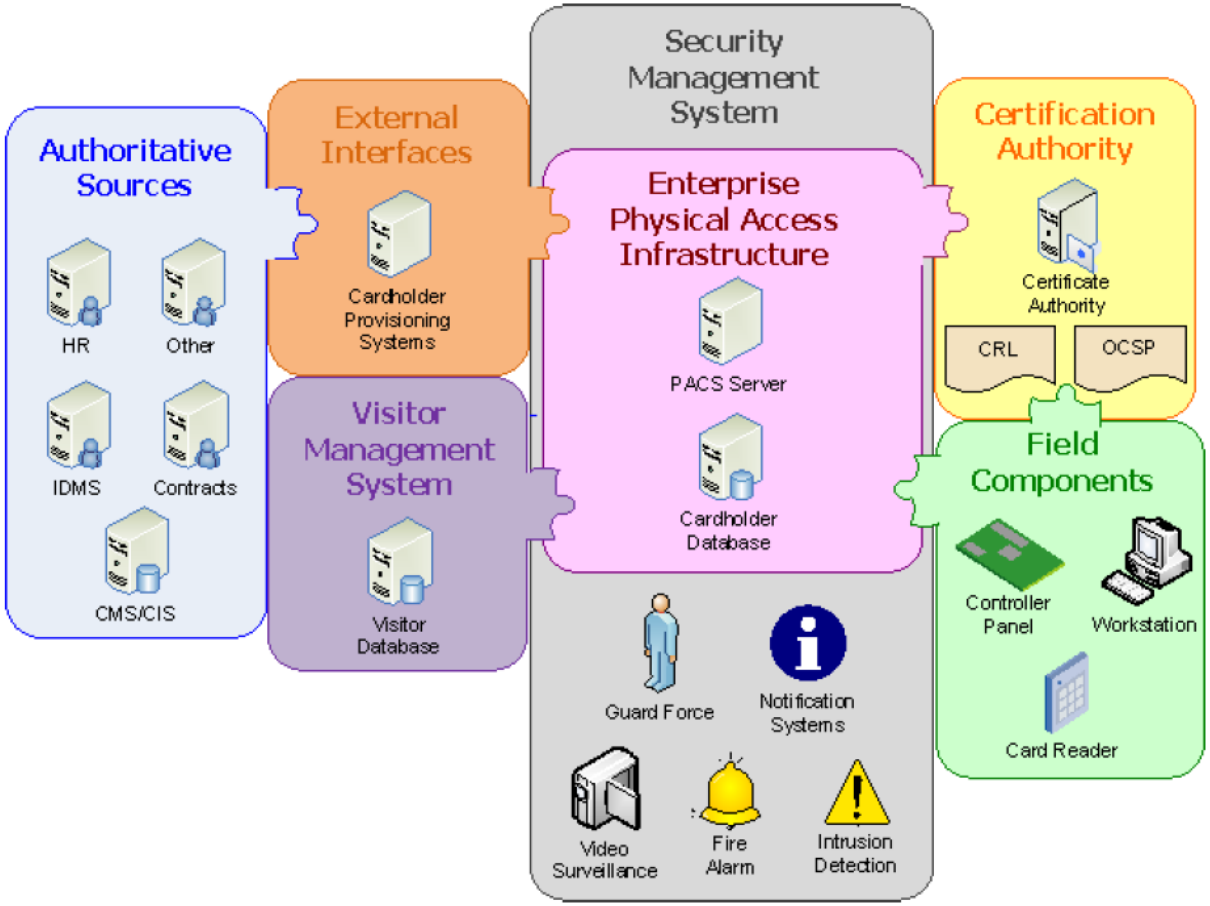
PIV Assurance Level Required by Application/Resource	Applicable PIV Authentication Mechanism
SOME confidence	VIS, CHUID
HIGH confidence	BIO
VERY HIGH confidence	BIO-A, PKI

PACS – Adapting to FICAM view of Trust

- GSA APL Require new PACS processes:
  - Signature Checking of Signer
  - Challenge/Response to Card
  - Certificate Check with Path Validation
  - All Require FIPS 140-2 Somewhere in the “System”
- Must Validate:
  - Cardholder
  - Card
  - Credential



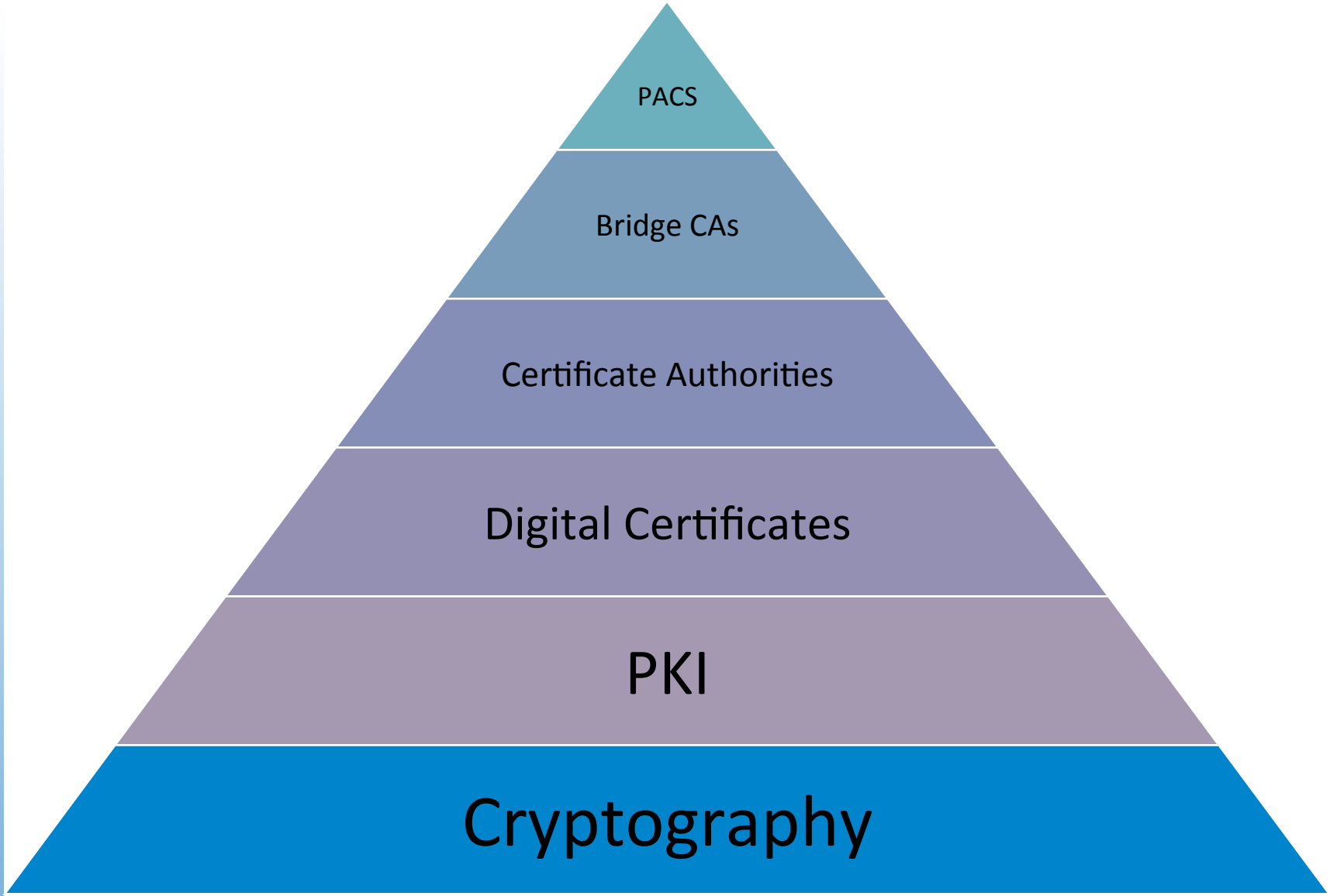
FICAM Roadmap Overview of PACS within the Overall Infrastructure



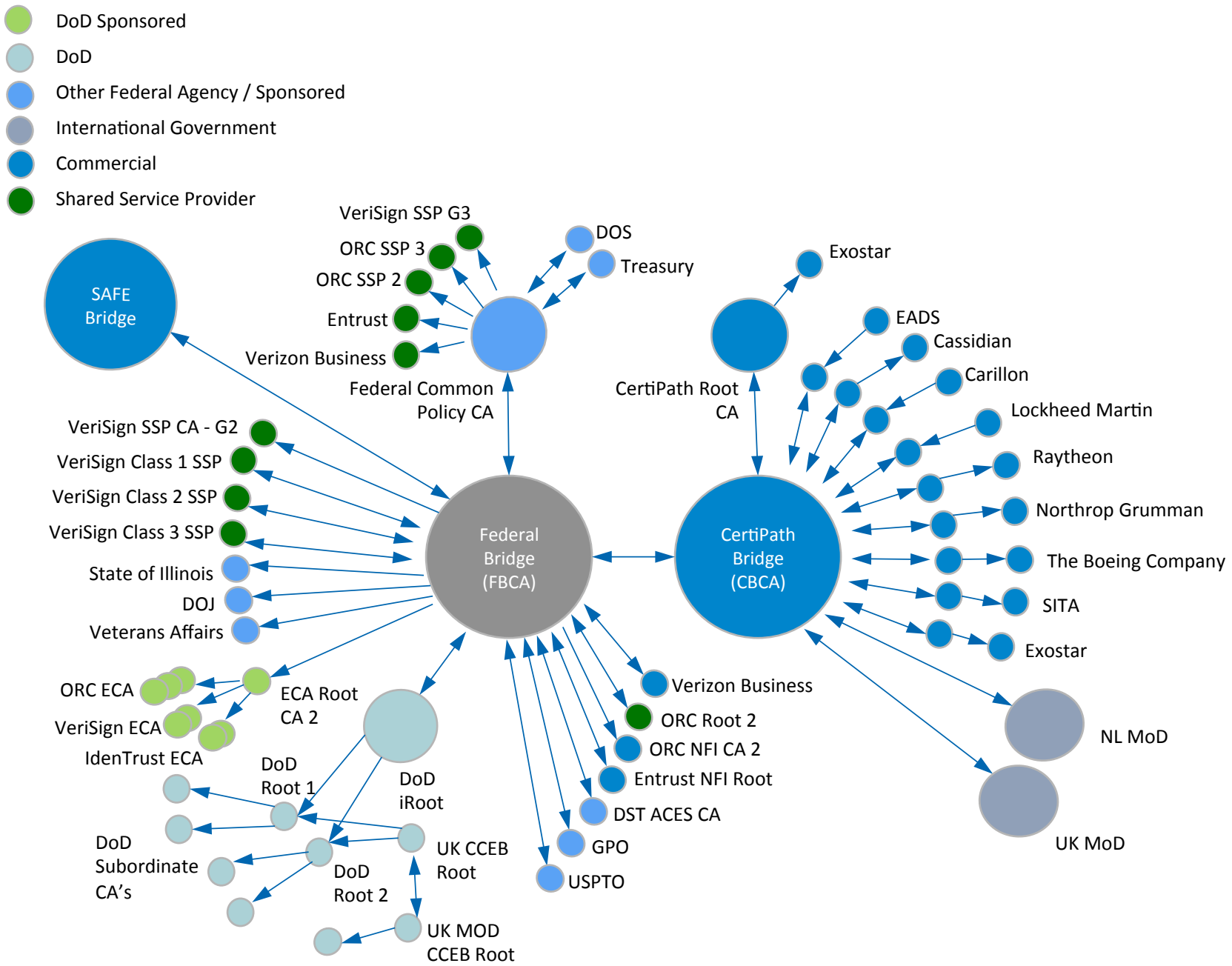
Impact of High assurance credential on PACS

- Migration to compliance
- SCA PACS Migration paper
- Implementation

Foundations for APL Approved PACS



Smart Card Alliance



PKI Policy Mapping Uses Transitive Trust

- My certificate's policy OID
  - 1.3.6.1.4.1.1.16304.3.6.2.20
- My trust anchor's certificate policy OID
  - 2.16.840.1.101.3.2.1.3.18

- Can I find a path of certificates where
  - A = B = C = D such that
  - 1.3.6.1.4.1.1.16304.3.6.2.20 = B = C = … = 2.16.840.1.101.3.2.1.3.18?

Smart Card Alliance

Threats/Countermeasures

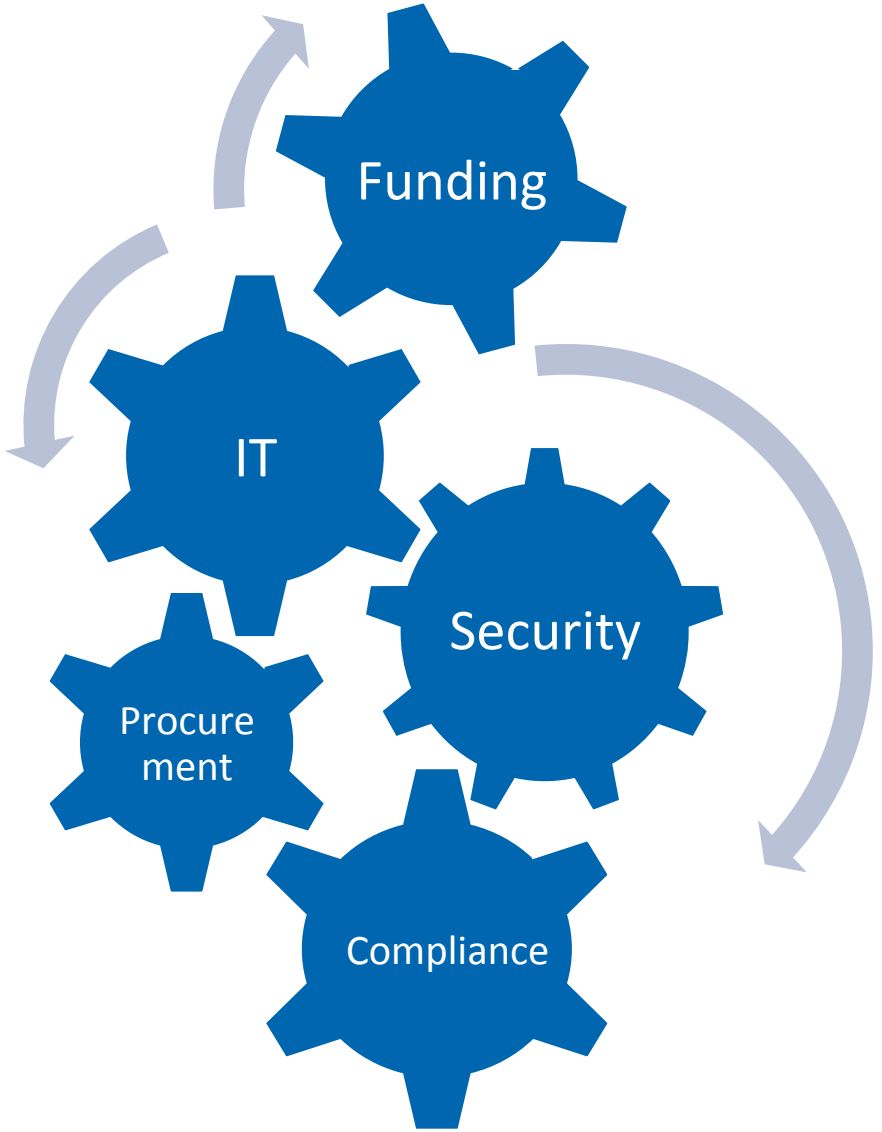
	Secures against cards that are						
Auth Modes ↓	Revoked	Counterfeit or Altered	Copied or Cloned	Lost or Stolen	Shared	Auth Factors	SP 800-116 Security Area
Chip Serial #						None	Uncontrolled
FASC-N/UUID	✓					None	Uncontrolled
CHUID+VIS	✓	✓				1	Controlled
PKI-CAK	✓	✓	✓			1	Controlled
PKI-AUTH	✓	✓	✓	✓		2	Limited
PKI-AUTH+BIO	✓	✓	✓	✓	✓	3	Exclusion

- Performing signature checks and private key challenges at enrollment is not sufficient to achieve these levels of assurance. They must be done at the time-of-access.
- Revocation checking for FASC-N and CHUID modes must be done using the PIV authentication certificate.

Smart Card Alliance

New demand environment

- Increased number of stakeholders
- Coordination



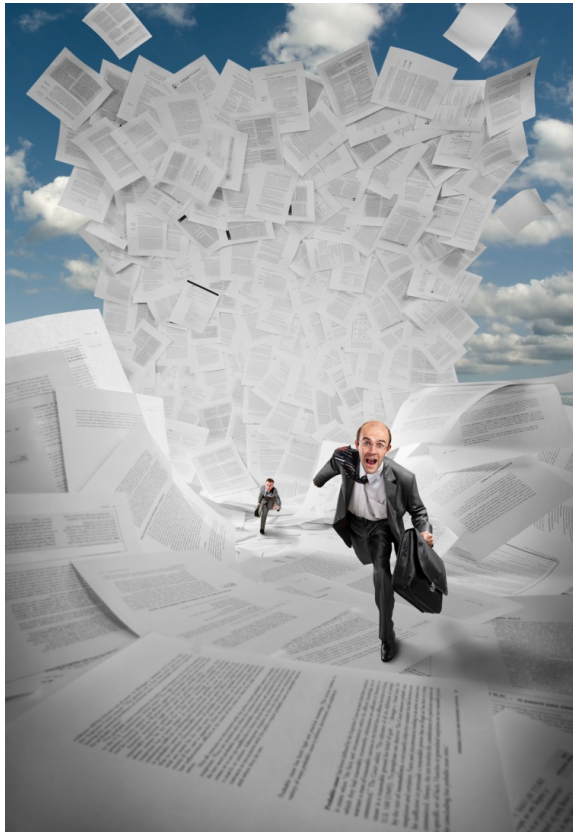
Smart Card Alliance

Communication

- New vocabulary, terminology

Requirements avalanche

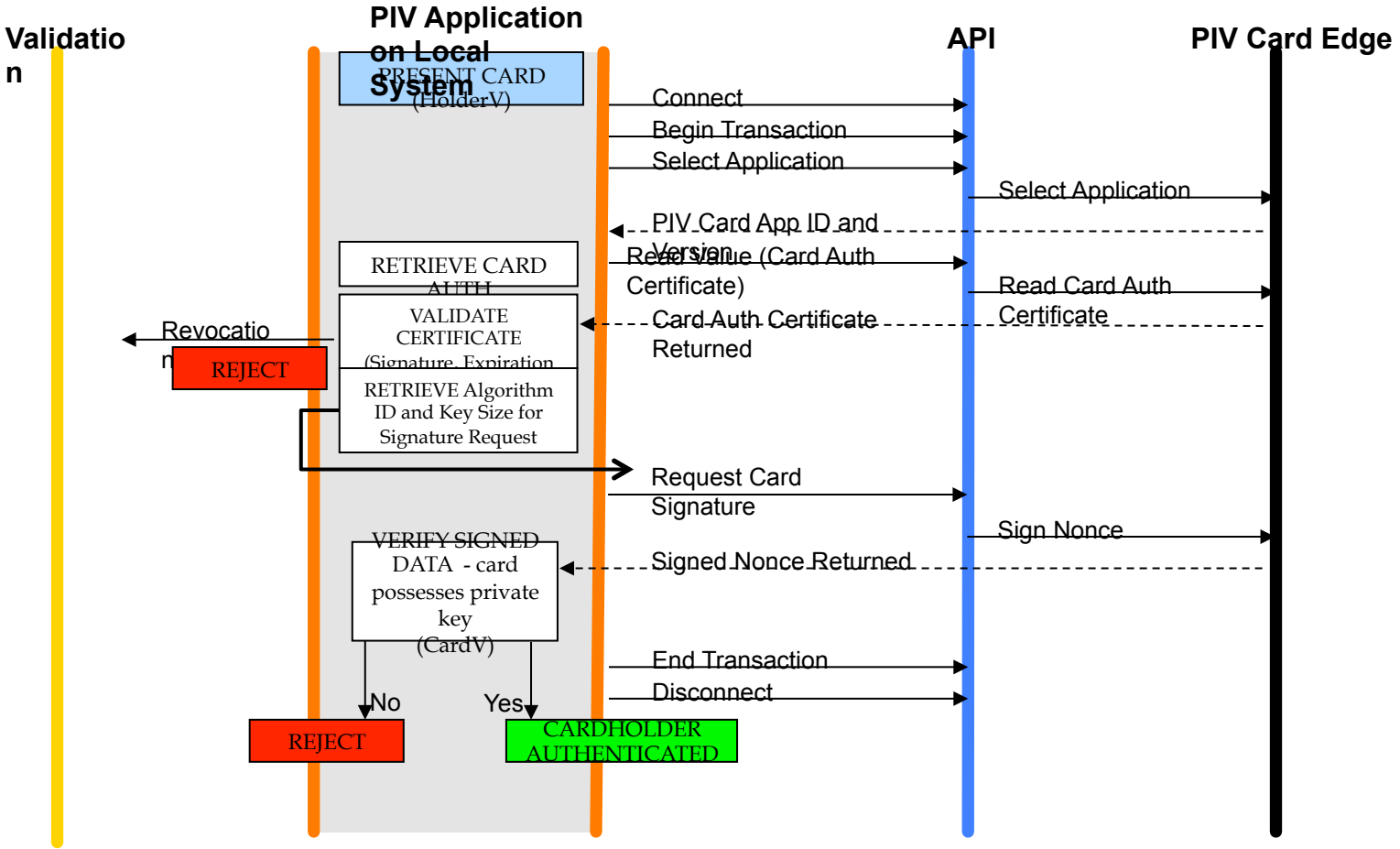
- What are the rules
  - FIPS 201-2
  - SP 800 Documents
  - OMB M 06 -18
  - PIV in E-PACS
  - FRTC
  - ADA 508
- Agency
  - FISMA, C&A
  - Authentication
  - Authorization, Provisioning
- Local considerations



Smart Card Alliance

Enhance understanding of operation

- Authentication using CAK



Agenda

- Objectives
- Foundations of GSA APL Approved PACS
  - Major system differences to support Public Key Infrastructure (PKI)
  - Biometrics
  - High Assurance Credentials
  - FICAM PIV in E-PACS
- Hands On Lab Day 2
  - PKI configuration for APL Approved PACS
  - Hands-on
- Day three
  - Exam

Smart Card Alliance

Summary

- Get it "Right the first time"
- New thinking
- Avoid costly post installation changes
- Enhance communications
  - Common language, terminology

Smart Card Alliance

Lars R. Suneborn, CSCIP/G, CSEIP
Director, Training Programs
Smart Card Alliance
O: 1 703 794 7662
M: 1 703 904 2389
Lsuneborn@Smartcardalliance.org

Certified System Engineer ICAM PACS - Integrator Training