Evolution of PACS to EPACS using PIV Cards

Tony Damalas
Stanley Security

The Federal Government is moving away from a traditional PACS to an enterprise PACS architecture to leverage PIV and PIV-I credentials; "E-PACS"

Agenda

I. Traditional PACS transitioning to Enterprise PACS

   A. Traditional PACS: Fundamental Components
   B. Requirements to use PIV and PIV-I credentials in PACS
   C. Limitations of Traditional PACS for PIV and PIV-I Credentials
   D. Federal Enterprise Architecture Model extends to PACS

II. Current PACS architecture, Target PACS architecture, and the PIV and PIV-I card use with EPACS

   A. Review of traditional PACS architecture components under FIPS 201
   B. FICAM target architecture for Enterprise PACS
   C. Granting Physical Access to PIV or PIV-I Credentials

Smart Card Alliance

Part I

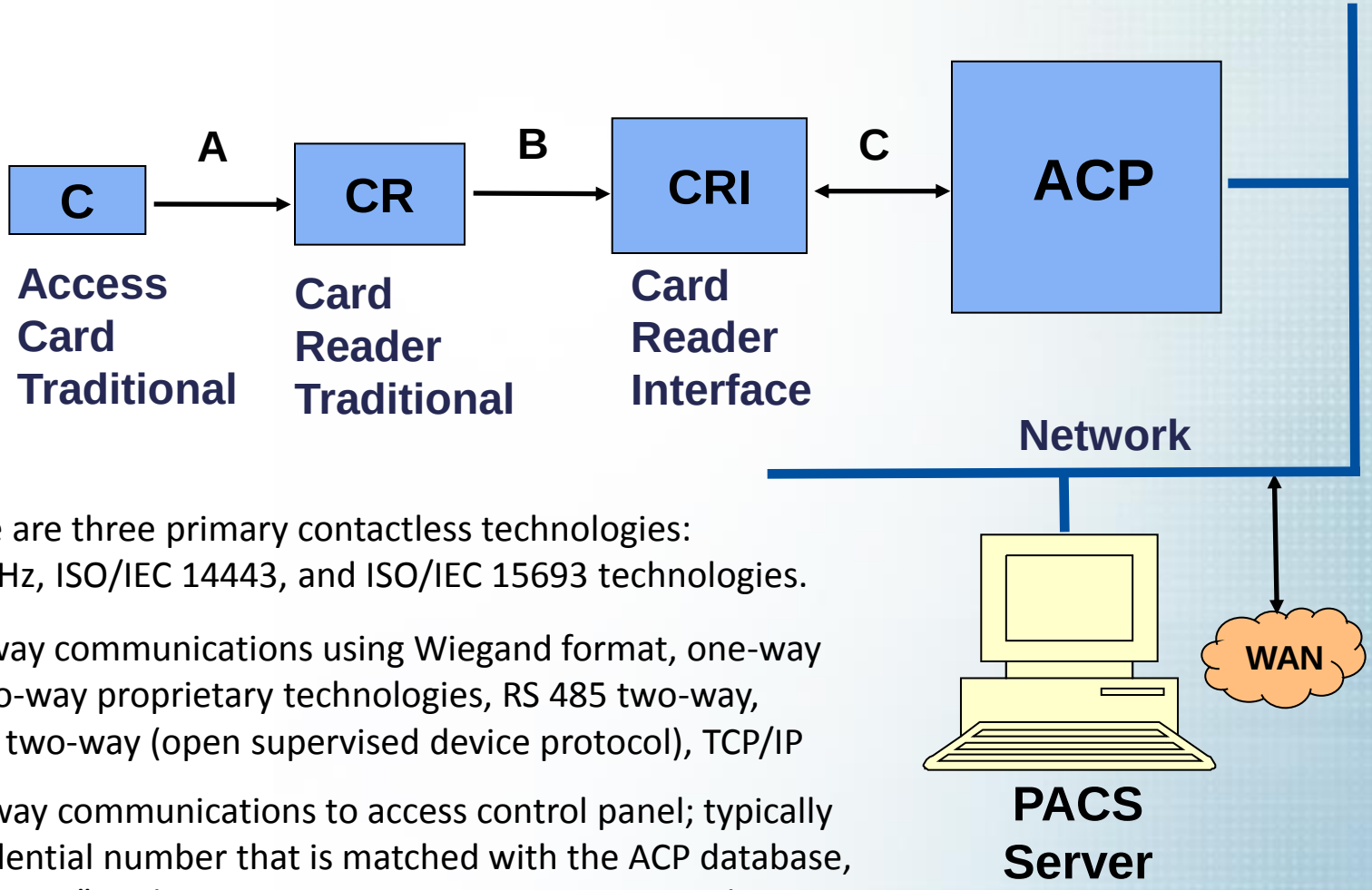
Traditional PACS

Migrates to

Enterprise PACS

Smart Card Alliance

Traditional PACS: Fundamental Components



A: There are three primary contactless technologies: 125KHz, ISO/IEC 14443, and ISO/IEC 15693 technologies.

B: One way communications using Wiegand format, one-way or two-way proprietary technologies, RS 485 two-way, OSDP two-way (open supervised device protocol), TCP/IP

C: Two-way communications to access control panel; typically a credential number that is matched with the ACP database, no "strong" authentication, may use proprietary authentication mechanisms, no interoperability

Smart Card Alliance

Traditional PACS: Card and reader technology

Features	14443	15693	125 kHz
Standards	ISO/IEC 14443 ISO/IEC 7810	ISO/IEC 15693 ISO/IEC 7810	None[3] (de facto)
Frequency	13.56 MHz	13.56 MHz	125 kHz
Operational range	Up to10 centimeters (~3-4 inches)	Up to 1 meter (~3.3 feet)	Up to1 meter (~3.3 feet)
Chip types supported	Memory Wired logic Microcontroller[4]	Memory Wired logic	Memory Wired logic
Encryption and authentication functions[5]	MIFARE, DES/3DES, AES, RSA[6], ECC	Supplier specific, DES/3DES	Supplier specific
Memory capacity range	64 to 64K bytes	256 and 2K bytes	8 to 256 bytes
Read/write ability	Read/write	Read/write	Read only[7]
Data transfer rate (Kb/sec)	Up to 106 (ISO) Up to 848 (available)	Up to 26.6	Up to 4
Anti-collision	Yes	Yes	Optional
Card-to-reader authentication	Challenge/Response	Challenge/Response	Password
Hybrid card capability	Yes	Yes	Yes
Contact interface support	Yes	No	No

Smart Card Alliance

Requirements to use PIV and PIV-I credentials in PACS

From HSPD 12: *Policies for a Common Identification Standard for Federal Employees and Contractors*

"it is the policy of the United States **to enhance security**, increase Government efficiency, reduce identity fraud, and protect personal privacy **by establishing a mandatory, Government-wide standard for secure and reliable forms of identification** issued by the Federal Government to its employees and contractors (including contractor employees).

Smart Card Alliance

Requirements to use PIV and PIV-I credentials in PACS

From FIPS 201-2: *Personal Identity Verification (PIV) of Federal Employees and Contractors*

This Standard is **applicable to identification** issued by Federal departments and agencies to Federal employees and contractors (including contractor employees) **for gaining physical access to Federally controlled facilities** and logical access to Federally controlled information systems

Smart Card Alliance

Requirements to use PIV and PIV-I credentials in PACS

From Office of Management and Budget: OMB M-11-11: *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12*

Every Federal agency is directed by Office of Management and Budget (OMB) Memorandum M-11-11 **to have an Enterprise Physical Access Control System (E-PACS) that meets the minimum requirements for the use of high assurance PIV credentials required in FIPS 201-2.** In addition, every Federal agency is directed to purchase E-PACS from the FIPS 201 Approved Products List (APL) to ensure a common identification standard for HSPD-12 implementation through OMB Memoranda M-06-18: *Acquisition of Products and Services for Implementation of HSPD-12*

Smart Card Alliance

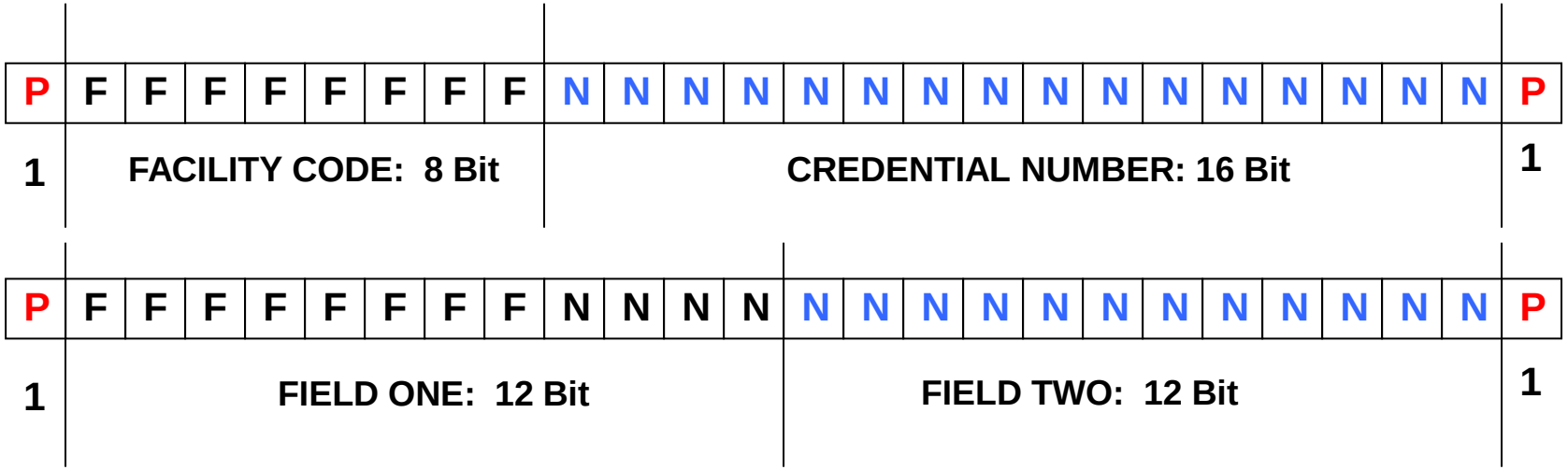
Requirements to use PIV and PIV-I credentials in PACS
Under FIPS 201

- FIPS 201 requires a smart card with both a contact and contactless interface (must be listed on APL)
- Contact specifications to conform with ISO 7816
- Contactless specification to conform with ISO 14443
- PIV Credential Data Elements: Biographic, Biometric and Digital Certificates (categories of identity data)
- Understanding PIV data elements and how they are parsed, stored, authenticated and used within ACP and host databases is key to a successful deployment and implementation of PIV-enabled PACS.
- FIPS 201 guides the PIV creation and issuance process but does not address PIV data interpretations for use

Smart Card Alliance

Requirements to use PIV and PIV-I credentials in PACS
Traditional data formats are non-compliant

Example of a Legacy Format – 26 Bit Wiegand



LEGACY DATA BIT FORMATS ARE NOT COMPLIANT BECAUSE OF SIZE AND STRUCTURE

Smart Card Alliance

Limitations of Traditional PACS for PIV and PIV-I: *Needs to read the Federal Agency Smart Credential Number*

Field Name	BCD Length	Field Description of the FASC-N Data Fields Federal Smart Card Credential Number
Agency Code	4	Identifies Government Agency issuing the credential
System Code	4	Identifies the system the card is enrolled in and is unique for each site
Credential Number	6	Encoded by the issuing agency. For a given system no duplicates numbers active
CS	1	Credential Series (Series Code) (Major Sys Chg)
ICI	1	Individual Credential Issue (Credential Code) (=1)
PI	10	Person Identifier (Numeric Code used by the identity source to uniquely identify the token carrier) (e.g. DoD EDI PN ID…TWIC Credential No….NASA UUPIC)
OC	1	Organization Category (1-Fed Gov, 2-State Gov, 3-Comm Ent, 4-Foregin Gov.
OI	4	Organizational Identifier(OC=1-NIST Agency, OC=2-State Code, OC=3-Company Code, OC=4-Numeric Country Code)
POA	1	Person / Organization Association Category (1= Emp, 2=Civil, 3=Ex Staff, 4=Uniform Svc, 5=Contractor, 6=Organizational Affiliate, 7= Organizational Beneficiary)
SS	1	Start Sentinel (leading character that is read first when card is presented)
FS	1	Field Separator
ES	1	End Sentinel
LRC	1	Longitudinal Redundancy Character

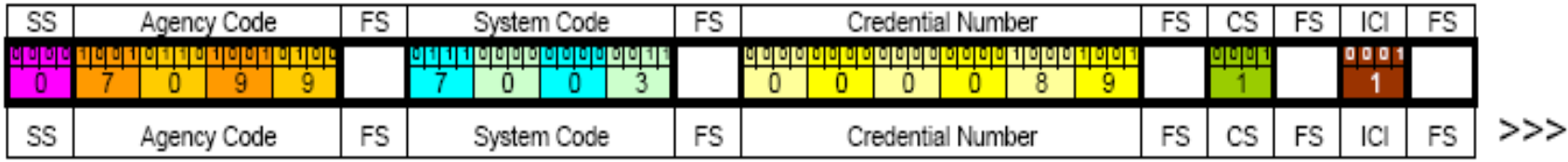
Limitations of Traditional PACS for PIV and PIV-I
Credential data size and data formats

Representation of a typical FASC-N (tag 0x30) in container 0x3000
(character parity bits omitted for readability)

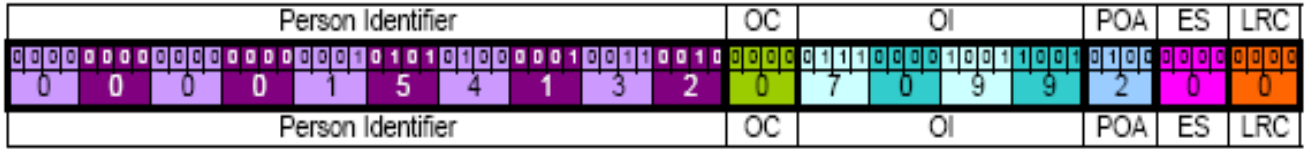
FASC-N 7099 7003 000089 1 1 0000154132 1 7099 2

FASC-N is 200 BITS (32 Digits of data plus 8 Control Digits = 40 Digits x 5 bits each)

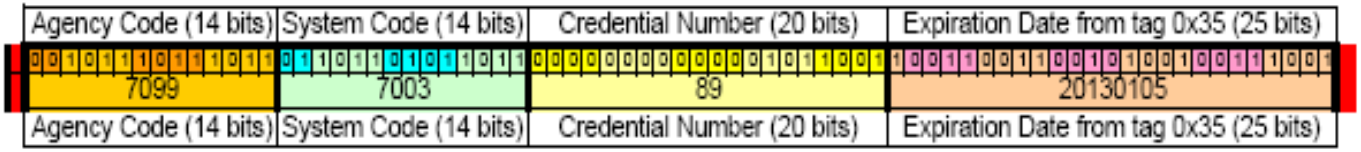
Agency card serial number: 0000086485



>>> DATA STRING ABOVE CONTINUES BELOW



Representation of same credential in GSA 75-bit Weigand format



Smart Card Alliance

Limitations of Traditional PACS for PIV and PIV-I
Automated Provisioning after authentication & validation

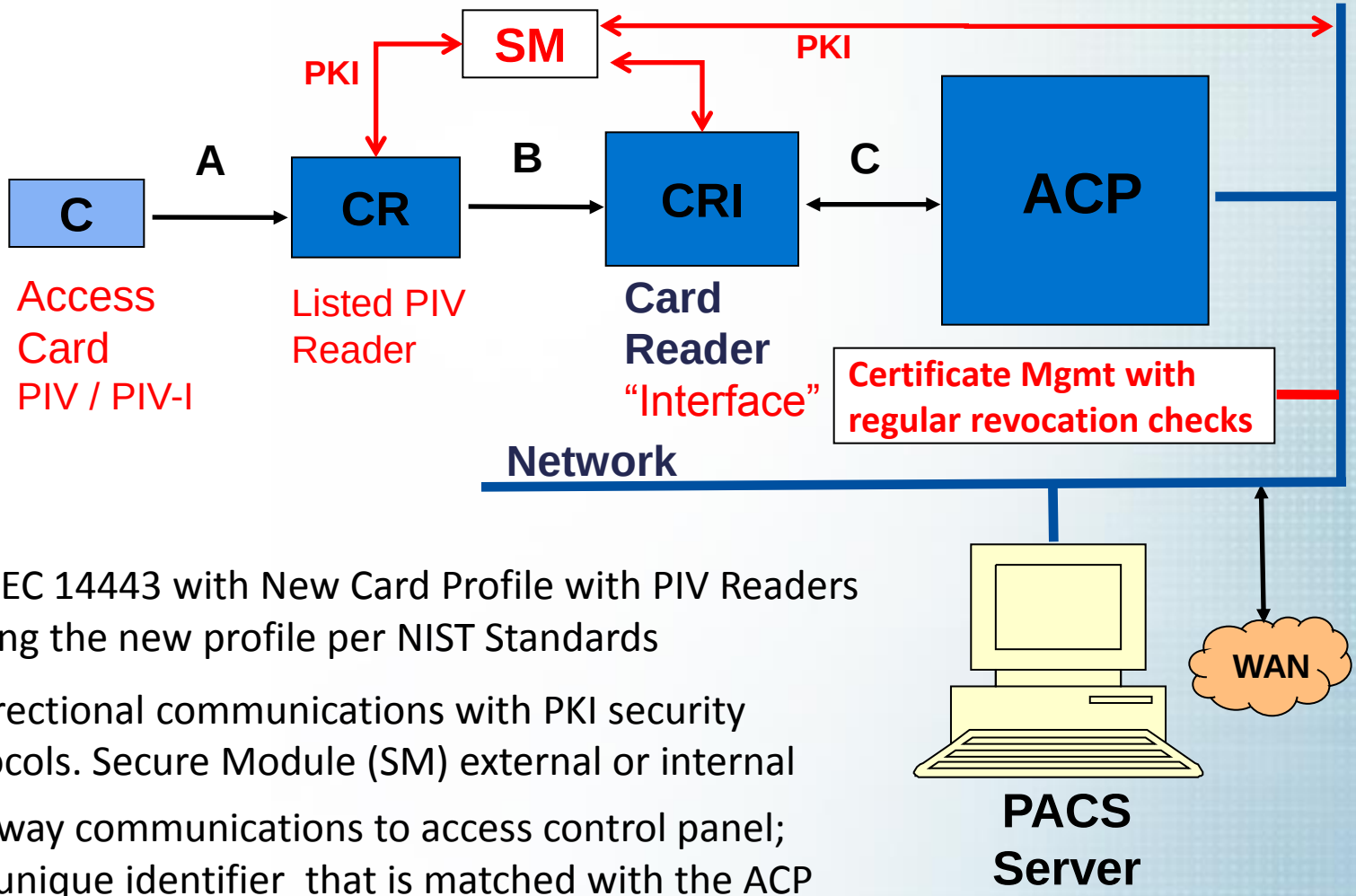
Enrolling PIV into PACS must be from Authoritative Source

TWO METHODS

- Harvest Data from Card after identity authentication and validation (PIV Card is an authoritative source)
- Mutually Authenticated Data Feed from IDMS/CMS

Smart Card Alliance

Limitations of Traditional PACS for PIV and PIV-I:
Two-Way Communications, Challenge Response, PKI



A: ISO/IEC 14443 with New Card Profile with PIV Readers reading the new profile per NIST Standards

B: Bi-directional communications with PKI security protocols. Secure Module (SM) external or internal

C: Two-way communications to access control panel; new unique identifier that is matched with the ACP database, "strong" authentication mechanisms per risk assessment (NIST SP 800-116), interoperability based on standards.

Smart Card Alliance

Limitations of Traditional PACS for PIV and PIV-I: *New Technical Controls (E-PACS Document)*

- **Technical Controls**

Technical security controls (i.e., safeguards or countermeasures) for an E-PACS are primarily implemented and executed by PACS through mechanisms contained in the hardware, software, or firmware components of the system or interconnected systems.

- **Family of Controls: *Identification and Authentication (IA)***

The security controls in the Identification and Authentication (I&A) family specify the full set of controls to completely authenticate the cardholder.

Smart Card Alliance

Limitations of Traditional PACS for PIV and PIV-I: *New Technical Controls (E-PACS Document)*

Summary of Identification and Authentication Controls

Class	Family	ID	Control
T	PIA	PIA-1	Identification and Authentication Policy Implementation
T	PIA	PIA-2	Authentication Modes
T	PIA	PIA-3	Identity Factor Authentication
T	PIA	PIA-3.1	Accepting Device (AD)
T	PIA	PIA-3.2	Validation of Trusted Origin (VTO)
T	PIA	PIA-3.3	Active Authentication (AA)
T	PIA	PIA-3.4	Protection of Authenticator (POA)
T	PIA	PIA-3.5	Revocation Check (RC)
T	PIA	PIA 3.6	Expiration Check (EC)
T	PIA	PIA-4	Signature Validation
T	PIA	PIA-5	Full Path Validation
T	PIA	PIA-6	Cross-Agency Interoperable Authentication
T	PIA	PIA-7	Card Revocation Check Mechanisms
T	PIA	PIA-8	Provisioning via Import
T	PIA	PIA-9	Provisioning via Registration
T	PIA	PIA-10	PIN Caching

Limitations of Traditional PACS for PIV and PIV-I: *Some New PACS Requirements under FIPS 201*

- Additional administrative policies
- Revocation mandates based on PIV expiration date and/or certificate status (validity)
- Enrollment of credential data more complex due to identity factors (biographic, biometric, digital) now under jurisdiction of external standards and/or systems
- New enrollment consequences introduced – multiple identities. How will the PACS handle multiple records?
- New considerations introduced for connection to federal IT Infrastructures to achieve requirements
- As an IT-based information system – ***accreditation*** is required if tied to federal IT networks

Smart Card Alliance

Limitations of Traditional PACS for PIV and PIV-I:
New PIV Authentication Mechanisms

PIV authentication mechanisms should be implemented in accordance with Table 1, and constrained by the innermost perimeters as depicted in Figure 1. (NIST SP 800-116)

Security Areas	*Number of Authentication Factors Required*
Exclusion	***3***
Limited	***2***
Controlled	***1***

Table 1 Auth. Factors for Security Areas

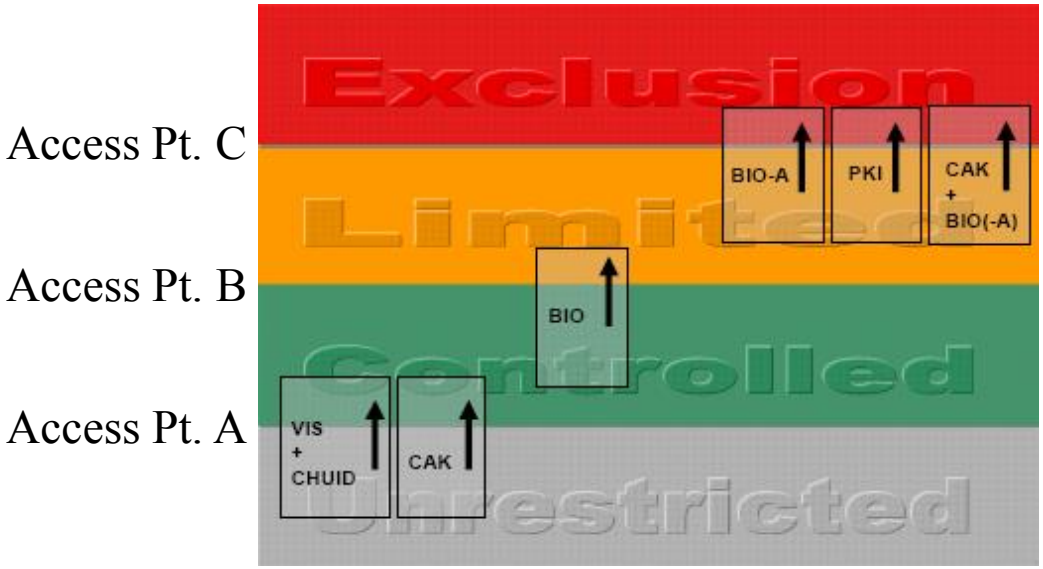
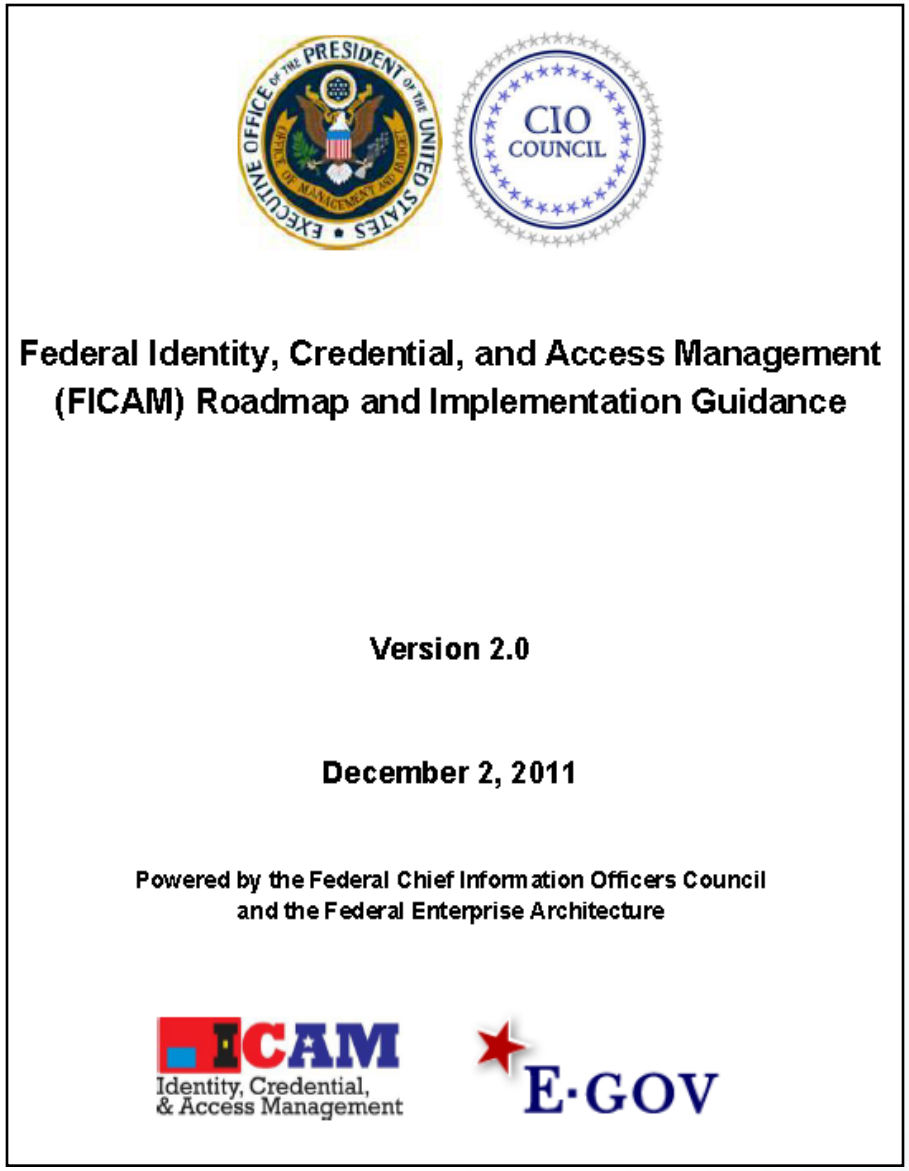


Fig. 1 Innermost Use of PIV Auth. Mechanisms

Smart Card Alliance

Federal Enterprise Architecture Model extends to PACS
The *"FICAM Roadmap and Implementation Guidance* Doc"



1.2. Purpose

The purpose of this document is to outline a common framework for ICAM within the Federal Government and to provide supporting implementation guidance for program managers, leadership, and stakeholders as they plan and execute a segment architecture for ICAM management programs. The Roadmap provides courses of action, planning considerations, and technical solution information across multiple federal programs spanning the disciplines of identity, credential, and access management

Smart Card Alliance

Federal Enterprise Architecture Model extends to PACS
The *"FICAM Roadmap and Implementation Guidance* Doc"

- The **FICAM Initiative** established the notion of an **Enterprise PACS** "from that need to leverage US Government investments in HSPD-12 compliance, FIPS 201, and PIV Card technology for physical access solutions across agency and organizational boundaries."

- **Enterprise PACS** allows Federal government personnel and their contractors **to authenticate their identities** as visitors to other agencies' facilities using secure, PKI-enabled Federal PIV Card standards.

- **This is done using cards (e.g., PIV Cards, PIV-I Cards) already issued by their own organizations**, which are subjected to fine-grained authorization decisions made by the agency or organization they are visiting, and by leveraging many aspects of existing PACS infrastructure.

Smart Card Alliance

Federal Enterprise Architecture Model extends to PACS
Chapter 10: Initiative 7: Modernize PACS Infrastructure.

- **FICAM Chapter 10: Discusses the activities associated with planning, designing, and implementing a PACS that meets relevant policy and technology requirements**
- **Physical Access Technical Implementation**
  - **Automated Provisioning to PACS**
    - Integrated Provisioning Capability
    - Vendor Interfaces
    - Batch Processes
  - **Common Physical Access Scenarios**
    - Authentication mechanisms associated with PIV/PIV-I
    - Use of PKI based authentication mechanisms
    - Biometric based authentication mechanisms
    - Multi-factor authentication

Smart Card Alliance

Federal Enterprise Architecture Model extends to PACS
Chapter 10: Initiative 7: Modernize PACS Infrastructure.

Initiative 7: Modernize PACS Infrastructure:

- ❑ **An agency-level ICAM implementation initiative**
- ❑ **Includes upgrading PACS for PIV cardholders**
- ❑ **ICAM PACS defined:**

➢*an automated system that manages the passage of people or assets through an opening(s) in a secure perimeter(s) based on successful authentication and associated authorization rules.*

Smart Card Alliance

Federal Enterprise Architecture Model extends to PACS
Chapter 10: Initiative 7: Modernize PACS Infrastructure.

Initiative 7: Modernize PACS Infrastructure continued:

- **The target state calls for a modernized PACS, which includes the following characteristics:**

  a) Electronically authenticates PIV cards and accepts multi-factor authentication as defined in NIST SP 800-116

  b) Supports an agency-wide approach to managing physical access services that links individual PACS via an enterprise level network wherever possible and appropriate, while maintaining local control over authorization decisions;

  c) Interfaces with authoritative Identity Providers and data source(s) to supply user attributes and credential information for automated provisioning and de-provisioning;

  d) Incorporates technologies that support secure, automated processes for requesting and provisioning visitor access.

Smart Card Alliance

Federal Enterprise Architecture Model extends to PACS
Federal Information Security Management Act

Federal Information Security Management Act (FISMA)

- This act requires each federal agency to develop, document, and implement an agency-wide program to provide information security for IT systems.

- As covered under FISMA, PACS implementers must meet all requirements associated with the RMF as defined in SP 800-3 and implement the appropriate security controls outlined in SP 800-53.

Smart Card Alliance

Federal Enterprise Architecture Model extends to PACS
Risk Management Framework per NIST SP 800-53

The RMF addresses the security concerns of organizations related to the design, development, implementation, operation, and disposal of information systems and the environments in which those systems operate. The RMF consists of the following six steps:

Step 1: *Categorize the system based on a FIPS 199 impact assessment*

Step 2: *Select an initial set of baseline security controls for the system*

Step 3: *Implement the security controls and document the design, development, and implementation details for the controls;*

Step 4: *Assess the security controls*

Step 5: *Authorize system operation based on a determination of risk*

Step 6: *Monitor the security controls in the information system*

Smart Card Alliance

Federal Enterprise Architecture Model extends to PACS
Adds E-PACS specific overlay to RMF / NIST SP 800-53

- As an information system, E-PACS is subject to the NIST Risk Management Framework to ensure that it is correctly protected.
- E-PACS augments the controls defined in [NIST SP 800-53] for how the E-PACS itself should be protected by providing an additional set of security controls specific to E-PACS services.
- This type of supplemental controls specific to a particular community or system type is allowed per [NIST SP 800-53] and is called an overlay. The supplemental controls should be considered the overlay for E-PACS to ensure that appropriate security measures are in place and that the E-PACS provides adequate protection.

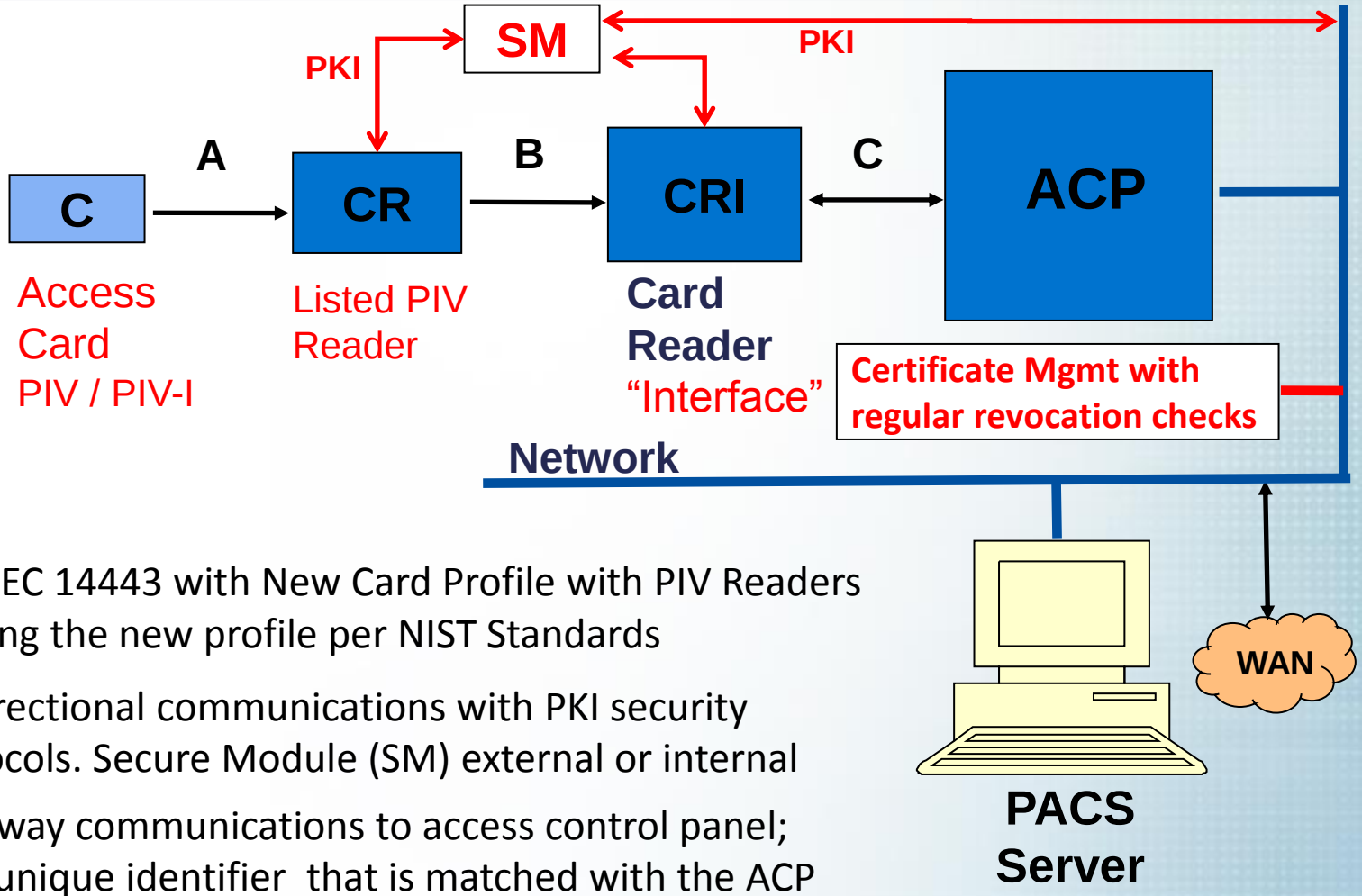
Smart Card Alliance

Part II

Current PACS architecture, Target Enterprise PACS architecture, and the PIV and PIV-I card use with EPACS

Smart Card Alliance

Review of PACS architecture components under FIPS 201

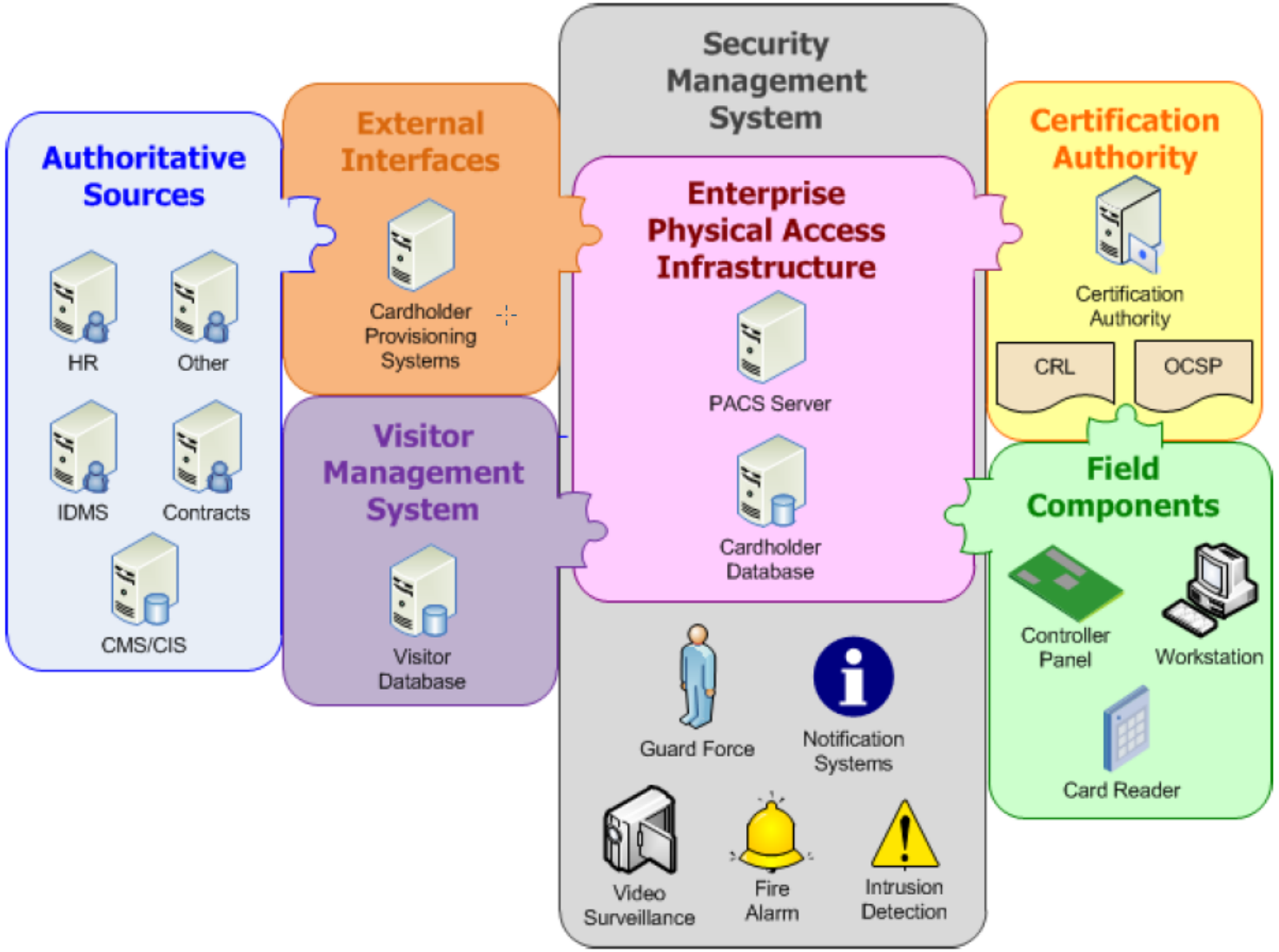


A: ISO/IEC 14443 with New Card Profile with PIV Readers reading the new profile per NIST Standards

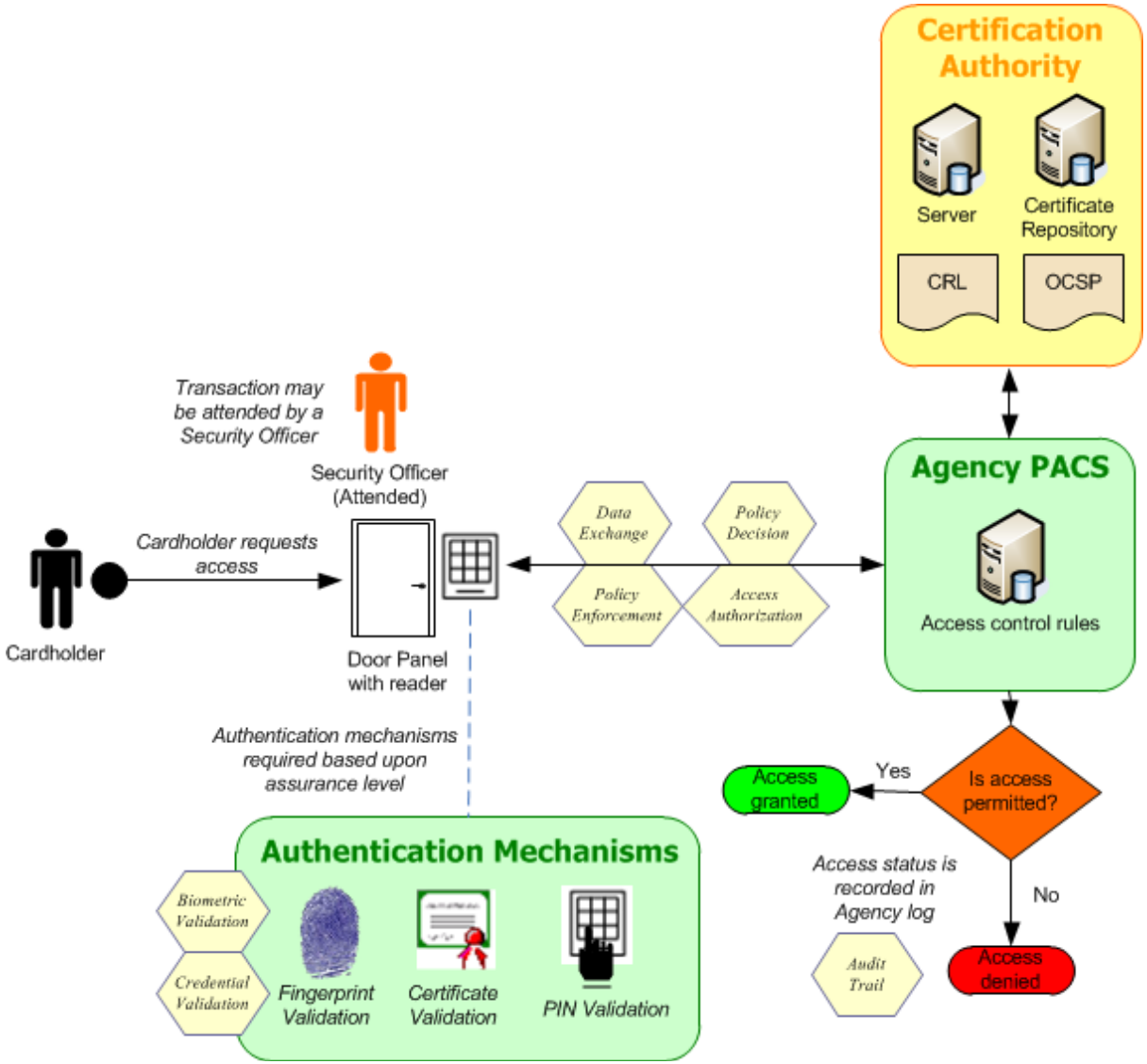
B: Bi-directional communications with PKI security protocols. Secure Module (SM) external or internal

C: Two-way communications to access control panel; new unique identifier that is matched with the ACP database, "strong" authentication mechanisms per risk assessment (NIST SP 800-116), interoperability based on standards.

FICAM target architecture for Enterprise PACS



Granting Physical Access to PIV or PIV-I Credentials



Smart Card Alliance

Tony Damalas
Principal Solutions Architect
Stanley Security
757-679-4243
tony.damalas@sbdinc.com

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