How to Plan, Procure & Deploy a PIV-Enabled PACS

Educational Institute & Access Control Council Webinar Series
Session Three: Establish The Project Scope
Introductions

Randy Vanderhoof, Secure Technology Alliance

Lars Suneborn, Secure Technology Alliance

Michael Kelley, Parsons Corp.

Mark Steffler, Quantum Secure
Who We Are

The Secure Technology Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption and widespread application of secure solutions. We provide, in a collaborative, member-driven environment, education and information on how smart cards, embedded chip technology, and related hardware and software can be adopted across all markets in the United States.

What We Do

Bring together stakeholders to effectively collaborate on promoting secure solutions technology and addressing industry challenges

- Publish white papers, webinars, workshops, newsletters, position papers and web content
- Create conferences and events that focus on specific markets and technology
- Offer education programs, training and industry certifications
- Provide networking opportunities for professionals to share ideas and knowledge
- Produce strong industry communications through public relations, web resources and social media
Access Control Council

... focuses on **accelerating the widespread acceptance, use, and application of secure technologies** in various form factors **for physical and logical access control**. The group brings together, in an **open forum**, leading users and technologists from both the public and private sectors.

**COUNCIL RESOURCES**

**White Papers**

- Commercial Identity Verification (CIV) Credential: Leveraging FIPS 201 and the PIV Card Standards
- A Comparison of PIV, PIV-I and CIV Credentials
- Federal Identity, Credential and Access Management (FICAM) Roadmap and Implementation Guidance Summary
- FIPS 201 and Physical Access Control: An Overview of the Impact of FIPS 201 on Federal Physical Access Control Systems
- FIPS 201 PIV II Card Use with Physical Access Control Systems: Recommendations to Optimize Transaction Time and User Experience
- Guide Specification for Architects and Engineers for Smart Card-based PACS Cards and Readers for Non-government PACS
- Personal Identity Verification Interoperability (PIV-I) for Non-Federal Issuers: Trusted Identities for Citizens across States, Counties, Cities and Businesses
- PIV Card/Reader Challenges with Physical Access Control Systems: A Field Troubleshooting Guide
- Smart Cards and Biometrics
- Strong Authentication Using Smart Card Technology for Logical Access
- Supporting the PIV Application in Mobile Devices with the UICC
National Center for Advanced Payment and Identity Security
National Center for Advanced Payments and Identity Security

- National Center for Advanced Payments and Identity Security in Crystal City
- Secure Technology Alliance Educational Institute is part of the center.
- Certifications Available
  - CSCIP
  - CSCIP/Payments
  - CSCIP/G
  - CSEIP
“Physical access controls systems, which include, for example, servers, databases, workstations and network appliances in either shared or isolated networks, are considered information systems.” OMB A-130, 2016
Recap of Sessions 1 and 2

Session 1 was originally presented on 19 Oct 2017
• Webinar series introduction - How to Plan, Procure & Deploy a PIV-Enabled PACS
• Project stakeholders

Session 2 was originally presented on 30 Nov 2017
• Characterization of the facility
• Identification of risk to the facility and personnel

Both sessions can be viewed on demand at: www.securetechnologyalliance.org/
Session 3 Agenda: Developing Project Scope

• Capturing the context of the project
• Exploring the government’s regulatory landscape
• Developing a solution for your Agency’s needs
• Identifying overall solution provider qualifications
• Qualifying approved products
Identifying Government Regulatory Framework

- FIPS 201-2
- NIST SP 800 - 116
- GSA APL FIPS 201 Evaluation Program
- CDM Phase 2
- FICAM
- OMB M-11-11
- Circular A-130 Revised 2016

“Agencies shall adhere to Government-wide requirements in the deployment and use of identity credentials used by employees and contractors accessing Federal facilities.”

“Physical access controls systems, which include, for example, servers, databases, workstations and network appliances in either shared or isolated networks, are considered information systems.”

How to Plan, Procure & Deploy a PIV-Enabled PACS
PIV Authentication Mechanisms

- Defined in FIPS 201-2 Section 6.2
  - Cardholder Unique Identifier (CHUID) / Visual (VIS)
  - Card Authentication Certificate Credential (PKI-CAK)
  - Symmetric Card Authentication Key (SYM-CAK)
  - Unattended PIV Biometric (BIO)
  - Attended PIV Biometric (BIO-A)
  - On-Card Biometric Comparison (OCC-AUTH)
  - PIV Authentication Certificate (PKI-AUTH)

- Varying degrees of threat protection from SP800-116:
  - Identifier collisions
  - Terminated cards
  - Visual counterfeiting
  - Skimming
  - Sniffing
  - Electronic Cloning
  - Electronic counterfeiting
PIV Assurance Levels OMB M 04-04 E-Authentication

1. Little or no confidence
2. Some confidence
3. High confidence
4. Very high confidence

<table>
<thead>
<tr>
<th>Assurance Level</th>
<th>PIV Authentication Mechanism</th>
</tr>
</thead>
<tbody>
<tr>
<td>Little or no confidence</td>
<td>VIS, CHUID</td>
</tr>
<tr>
<td>Some confidence</td>
<td>PKI-CAK, SYM-CAK</td>
</tr>
<tr>
<td>High confidence</td>
<td>BIO</td>
</tr>
<tr>
<td>Very high confidence</td>
<td>BIO-A, OCC-AUTH, PKI-AUTH</td>
</tr>
</tbody>
</table>
## Factors of Authentication

<table>
<thead>
<tr>
<th>Authentication Mechanism</th>
<th>Have</th>
<th>Know</th>
<th>Are</th>
<th>Number of Factors</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHUID &amp; VIS</td>
<td>❖</td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>PKI-CAK</td>
<td>❖</td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>SYM-CAK</td>
<td>❖</td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>BIO</td>
<td></td>
<td>❖</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>BIO-A</td>
<td>❖</td>
<td>❖</td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>OCC-AUTH</td>
<td></td>
<td>❖</td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>PKI-AUTH</td>
<td>❖</td>
<td>❖</td>
<td>❖</td>
<td>2</td>
</tr>
<tr>
<td>PKI-AUTH &amp; BIO(-A)</td>
<td>❖</td>
<td>❖</td>
<td>❖</td>
<td>3</td>
</tr>
<tr>
<td>PKI-CAK &amp; BIO(-A)</td>
<td>❖</td>
<td>❖</td>
<td>❖</td>
<td>3</td>
</tr>
</tbody>
</table>

1 Use has been deprecated
2 If the PIN is used to satisfy the security condition for use
3 If OCC is used to satisfy the security condition for use
How to Plan, Procure & Deploy a PIV-Enabled PACS
PIV Authentication Mechanism Selection

<table>
<thead>
<tr>
<th>Risk Level</th>
<th>Number of Authentication Factors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controlled</td>
<td>1</td>
</tr>
<tr>
<td>Limited</td>
<td>2</td>
</tr>
<tr>
<td>Exclusion</td>
<td>3</td>
</tr>
</tbody>
</table>

- Other Selection Factors
  - Assurance level
  - Availability
  - Authentication speed
How to Plan, Procure & Deploy a PIV-Enabled PACS

Topology, Infrastructure, Validation System & Readers

PACS Infrastructure
- PACS Application and Server(s)
- Database and Server
- Controllers
- Workstations

PACS Validation System
- Secure Controllers
- PKI Validation Software
- PKI Registration Software
- CRLs/OCSP Responders
  - SCVP Server
  - Caching Status Proxy Server (deprecated)

PACS PIV Reader
- Number of authentication factors
- Contact or contactless interface
- User feedback
- Keypad and biometric sensors
“PACS modernization involves integrating PACS at the enterprise level, which helps an agency achieve cost savings and efficiencies while preserving local access control decisions.

Modernized PACS leverage user identity and credential data from authoritative sources and are supported by enterprise resource, privilege, and policy management processes.”

-- CIO Council, *FICAM Roadmap PACS Brochure*
FICAM Insists that Logical and Physical Access Control Follow the Same Paradigm

Implementation of Enterprise PACS
PACS modernization involves integrating PACS at the enterprise level, which helps an agency achieve cost savings and efficiencies while preserving local access control decisions. Modernized PACS leverage user identity and credential data from authoritative sources and are supported by enterprise resource, privilege, and policy management processes. PACS modernization also includes use of the PIV card in order to gain physical access to a federally controlled facility, in accordance with HSPD-12.

Identity Management
PACS user accounts are provisioned from authoritative sources as part of the overall identity lifecycle management process.

Credential Management
PIV, PIV-I, or other accepted credentials. Modernized PACS are designed to electronically validate and interoperate with employee and visitor credentials.

Physical Access Control Systems
PACS can be used to control both routine employee and visitor access to federal campuses, facilities, and controlled interior areas.

Resource Management
- Facilities
- Data
- Systems
- Applications

Privilege Management
- Roles
- Entitlements

Policy Management
- Rules
- Transaction Context

Benefits of PACS Modernization
The design characteristics of a modernized PACS solution offer agencies a wide variety of benefits and increased efficiencies, as described below.

- Increases security and privacy at your facility (Uses stronger technology to validate cardholders, Electronic verification provides reliable information to assist the guard force in making access decisions)
- Reduces costs and increases efficiency (Agency-wide approach eliminates redundant processes and investments, Enterprise integration enables reduced manual efforts)
- Promotes trust and interoperability (Supports acceptance of PIV, PIV-I, and other trusted external credentials, User privileges can be shared across agency locations and with trusted external sites)
- Improves overall support for ICAM implementation (Feeds user information from agency-wide identity sources, Enables sharing of access control leg information with security monitoring tools, Shares data (as needed and permissible) with credentialing system)

Implementation of Enterprise LACS
LACS modernization involves integrating an agency’s IT resources at the enterprise level, to control access in a streamlined and consistent manner. A modernized LACS standardizes on use of the PIV credential as the common means of validating the identity of a user and granting access to networks and information systems, in accordance with federal policies.

Identification Management
User accounts are provisioned from authoritative sources as part of the overall identity lifecycle management process.

Credential Management
PIV card, PIN, Biometric

Logical Access Control Systems
A LACS uses authentication of a user’s identity to make an authorization decision to grant or deny the user access to one or more computer system resources.

Resource Management
- Data
- Systems
- Applications

Privilege Management
- Roles
- Entitlements

Policy Management
- Rules
- Transaction Context

Benefits of LACS Modernization
A modernized LACS solution offers agencies a wide variety of benefits and increased efficiencies, as described.

- Improved Security. Provides high assurance of user identity and strong authentication for users accessing agency resources. Securely authenticates remote users while leveraging existing infrastructure.
- Reduced Administrative Burden and Cost. Requires less effort on the part of resource owners and administrators to manage user accounts and access privileges, resulting in lower life-cycle costs.
- Increased Compliance. Enables detection and remediation of conflicting access privileges within and across resources (e.g., segregation of duties).
- Increased Customer Satisfaction and Convenience. Provides consumers ease of use with the ability to access multiple applications using a single credential.
- Support for Encryption/Digital Signature Services. Supports additional security functionality to encrypt and digitally sign data using the PIV card.

Key Target State Metrics
1 digital identity per user
100% of employees and contractors have PIV credentials
100% of applications are accessible to employees and contractors using PIV cards
100% of externally-facing applications are enabled to accept third-party credentials
100% of applications are integrated with an automated provisioning workflow

Both Physical and Logical Access Controls are held to the Same Standard
FICAM Enterprise PACS Modernization

Source: CIO Council FICAM Roadmap Modernized PACS Brochure - 2011
FICAM Directed Enterprise PACS Modernization: Figure 108

1. Connection to Authoritative Data Sources
   - HR
   - Other
   - IDMS
   - Contracts
   - CMS/CIS

2. Connection to Physical Access Control Systems
   - Cardholder Provisioning Systems
   - Visitor Database

3. Connection to Internet to Validate PIV Cards
   - Certification Authority
   - CRL
   - OCSP
   - Controller Panel
   - Workstation
   - Card Reader
   - Video Surveillance
   - Fire Alarm
   - Intrusion Detection

4. FICAM EPACS Applications
   - Privilege/Access Mgmt
   - Rules/Workflow Engine
   - Visitor Management
   - Reporting

How to Plan, Procure & Deploy a PIV-Enabled PACS
Self-service Portal

Process and Policy Automation Privilege/Access Mgmt

Connections to Physical Access Control Systems

Audit Portal

Email Notification

FICAM EPACS Privilege Management Process Flow

How to Plan, Procure & Deploy a PIV-Enabled PACS
Risks Mitigated by Applying EPACS Best Practices

1. Only assured identities sourced from an agency authoritative source are provisioned into PACS.

2. Only valid PIV cards are provisioned into PACS.

3. PIV cards that become invalid (expired, placed on CRL, etc.) are immediately terminated for access into all PACS simultaneously.

4. Any identity terminated in the authoritative source causes immediate termination of any access privileges in all PACS simultaneously.

5. Any elevated (privileged) access is immediately revoked when a qualifying identity attribute ceases to be in compliance.

6. Ability to perform audit at any time across all PACS simultaneously

7. 100% PII protection by removing PII from PACS endpoints
Physical identity and access management (PIAM) technologies provide authentication, authorization and provisioning services in order to efficiently streamline the lifecycle of a physical identity within a global organization.

PIAM ensures the right physical IDs – i.e., employees, visitors, contractors, vendors are properly authenticated and have the right access to the right areas, for the right reasons for a specified duration of time.

“Physical identity and access management (PIAM) deployments are increasing due to technology and product development, compliance mandates, a greater desire to manage alternative user populations such as on-premises visitors and contractors, and a sharp emphasis on timely and secure access”

1Gartner Research; Physical Identity and Access Management; Feb 2012
Gap Analysis
Gap Analysis

- New installation, replacement or upgrade
  - Compatibility
  - Physical and logical transition strategies

- Reader, panel and card holder locations and quantities
  - Software licenses
  - Storage requirements

- Infrastructure requirements
  - Bi-directional reader communication
  - Network communication
  - System availability
  - External system integration
  - Environmental factors
Complete Project Scope

- Addressed and accepted risks
- Cost and schedule estimates
- Roles and responsibilities
  - Self perform vs. contract
  - Well defined
  - Commitment
- System specification
- Alternatives
  - Prioritize areas that deliver greatest risk reduction
  - PIV Implementation Maturity Model (PIMM)
  - Self-perform vs. contract
- Executive sponsor acceptance
Identify Solutions Providers & Products
Identifying Overall Solutions Providers

- Capability to support full scope of project
- Ability to partner with experts in certain areas of implementation
- Experience & skill set
  - VAR relationship with manufacturers
  - Prior history for similar deployments
  - System design (architecture)
  - Project management
  - Communication
- Certifications required
  - Certified System Engineers ICAM PACS
  - CISSP or other information assurance
Qualifying Hardware and Software Products

"A. Requirement to use federally approved products and services – To ensure government-wide interoperability, all departments and agencies must acquire products and services that are approved to be compliant with the Standard and included on the approved products list.


PACS Components Defined by GSA FIPS 201 Evaluation Program

<table>
<thead>
<tr>
<th>Product</th>
<th>Approving Governance</th>
<th>Implementation</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>PACS Card Readers</td>
<td>GSA APL</td>
<td>Hardware and firmware</td>
<td>Contact PIV readers Contactless PIV Readers (with or without biometrics)</td>
</tr>
<tr>
<td>PACS Validation System</td>
<td>GSA APL</td>
<td>Hardware and/or software</td>
<td>PACS Panels and/or servers</td>
</tr>
<tr>
<td>PACS Infrastructure</td>
<td>GSA APL</td>
<td>Software</td>
<td>PACS Headend Server</td>
</tr>
</tbody>
</table>

https://www.idmanagement.gov/approved-products-list-pacs-products/

Enterprise PACS Software

<table>
<thead>
<tr>
<th>Product</th>
<th>Approving Governance</th>
<th>Implementation</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise PACS Software/Visitor Management</td>
<td>GSA/DHS CDM APL Phase 2 for BOUND-P (GSA Schedule 70, SIN 132-44 designation)</td>
<td>Software</td>
<td>SP800-116 has enumerated requirements and the FICAM Roadmap delineates “Solution Characteristics” for three relevant categories: PACS, Automated Provisioning and Visitor Management</td>
</tr>
</tbody>
</table>

Upcoming Sessions

<table>
<thead>
<tr>
<th>Stakeholders</th>
<th>Session 1 10/19/2017</th>
<th>Session 2 11/30/2017</th>
<th>Session 3 1/11/2018</th>
<th>Session 4 2/22/2018</th>
<th>Session 5 3/15/2018</th>
<th>Session 6 4/19/2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acquisition</td>
<td>◆</td>
<td></td>
<td>◆</td>
<td>◆</td>
<td>◆</td>
<td>◆</td>
</tr>
<tr>
<td>Budget</td>
<td>◆</td>
<td></td>
<td>◆</td>
<td>◆</td>
<td>◆</td>
<td>◆</td>
</tr>
<tr>
<td>Customers / Tenants</td>
<td>◆</td>
<td>◆</td>
<td>◆</td>
<td>◆</td>
<td>◆</td>
<td>◆</td>
</tr>
<tr>
<td>Engineering</td>
<td>◆</td>
<td></td>
<td>◆</td>
<td>◆</td>
<td>◆</td>
<td>◆</td>
</tr>
<tr>
<td>Executive Sponsors</td>
<td>◆</td>
<td>◆</td>
<td>◆</td>
<td>◆</td>
<td>◆</td>
<td>◆</td>
</tr>
<tr>
<td>Facility Management</td>
<td>◆</td>
<td>◆</td>
<td>◆</td>
<td>◆</td>
<td>◆</td>
<td>◆</td>
</tr>
<tr>
<td>Information Technology</td>
<td>◆</td>
<td></td>
<td>◆</td>
<td>◆</td>
<td>◆</td>
<td>◆</td>
</tr>
<tr>
<td>Legal</td>
<td>◆</td>
<td>◆</td>
<td></td>
<td>◆</td>
<td></td>
<td>◆</td>
</tr>
<tr>
<td>Personnel</td>
<td>◆</td>
<td></td>
<td>◆</td>
<td></td>
<td>◆</td>
<td>◆</td>
</tr>
<tr>
<td>Physical Security</td>
<td>◆</td>
<td>◆</td>
<td>◆</td>
<td>◆</td>
<td>◆</td>
<td>◆</td>
</tr>
<tr>
<td>Safety</td>
<td>◆</td>
<td>◆</td>
<td></td>
<td></td>
<td>◆</td>
<td>◆</td>
</tr>
</tbody>
</table>
Q & A
Resources and Contacts

http://www.securetechalliance.org

Lars R. Suneborn, CSCIP/G, CSEIP
Director, Training Programs, Secure Technology Alliance
lsuneborn@securetechalliance.org

Michael Kelley, CSCIP/G, CSEIP, PSP, CBP
Principal ESS Technical Specialist, Parsons Corp.
michael.p.kelley@parsons.com

Mark Steffler
VP Government Practice, Quantum Secure/HID
msteffler@quantumsecure.com