SECURE TECHNOLOGY ALLIANCE

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

Educational Institute & Access Control Council Webinar Series
Session Five: Implementing the Solution

Introductions

Randy Vanderhoof, Secure Technology Alliance

Lars Suneborn, Secure Technology Alliance

Mark Dale, XTec, Inc.

Tony Damalas, Signet Technologies, Convergint Federal Solutions

SECURE TECHNOLOGY ALLIANCE

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

SECURE TECHNOLOGY ALLIANCE

Our Focus

- Access Control
- Authentication
- Healthcare
- Identity Management
- Internet of Things
- Mobile
- Payments
- Transportation

Member Benefits

- Certification
- Council Participation
- Education
- Industry Outreach
- Networking
- Technology Trends

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

SECURE TECHNOLOGY ALLIANCE

SECURE TECHNOLOGY ALLIANCE

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**

SECURE TECHNOLOGY ALLIANCE

"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*

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

Webinar Series Session Review

Session Two

Facility Characteristics & Risks

Facilities:
- Size
- Mission
- Assets
- Existing Conditions

Risks:
- Threats
- Likelihood
- Consequence

Session Three

Project Scope

- Project Context
- Government Regulation Landscape
- Developing to Agency Needs
- Gap Analysis
- Identifying Solution Providers & Products

Session Four

Procurement Strategy

- GSA, OMB & Stakeholder Responsibilities
- Standards
- Procurement vehicles
- Contract documents
- Funding
- Evaluation
- Award

Session Five

Deployment

- Planning
- Design
- Installation
- Testing
- Operations & Maintenance

SECURE TECHNOLOGY ALLIANCE

Carryover from "Session Four – Procurement Strategy" Post Contract Award Requirements

- Contract Requirements
  - Pricing/Funding
  - Schedule of Deliverables & Target Completion Date
- GSA Schedule Requirements
  - PACS Products GSA FIPS 201 APL
  - PACS System Integrators & CSEIP Certified Staff
- Technical Requirements
  - Credential Type: PIV, PIV-I, CAC, other
  - PACS Status: PIV enabling an existing PACS, or new PACS
  - Network: Stand alone; or connected to agency network/Internet
  - Integration: Identity Management System, PIV Credential Issuer System, Authoritative Data Sources
  - Locations: Entry access points, and assurance levels
- Security Requirements
  - Authorization & Accreditation (A&A), Authority to Operate (ATO)
  - Continuous Monitoring, Continuous Diagnostics & Mitigation

Implementation Life Cycle Approach

Mark Dale, XTec, Inc.

Tony Damalas, SigNet Technologies, Inc.

Planning Phase

- Establish Project Team
- Analyze Proposal and Requirements
- Define Milestones, and Deliverables
- Identify Responsibilities & Dependencies Develop Monitoring & Reporting Plan
- Plan Acquisition of Materials & Equipment
- Plan for Security & Privacy Assessment

Design Phase

- Apply Requirements Analysis
- Identify Equipment Type, Quantity & Location
- Define Connectivity Configuration
- Prepare Installation Documentation
- Identify Client Furnished Equipment
- Identify and Establish Staging and Operations Areas
- Procure Products, Materials & Equipment

Install Phase

- Install & Configure Equipment
- Develop Test Plan
- Develop Security & Privacy Assessment Documentation

Testing Phase

- Function, Partial and Integration Testing
- Final Acceptance Testing
- Information Assurance Assessment
- Authority To Operate (ATO)

O&M Phase

- Training (Operators, Administrators & Technicians
- Turnover
- Final As-Built Documentation
- Warranty
- Maintenance
- CDM

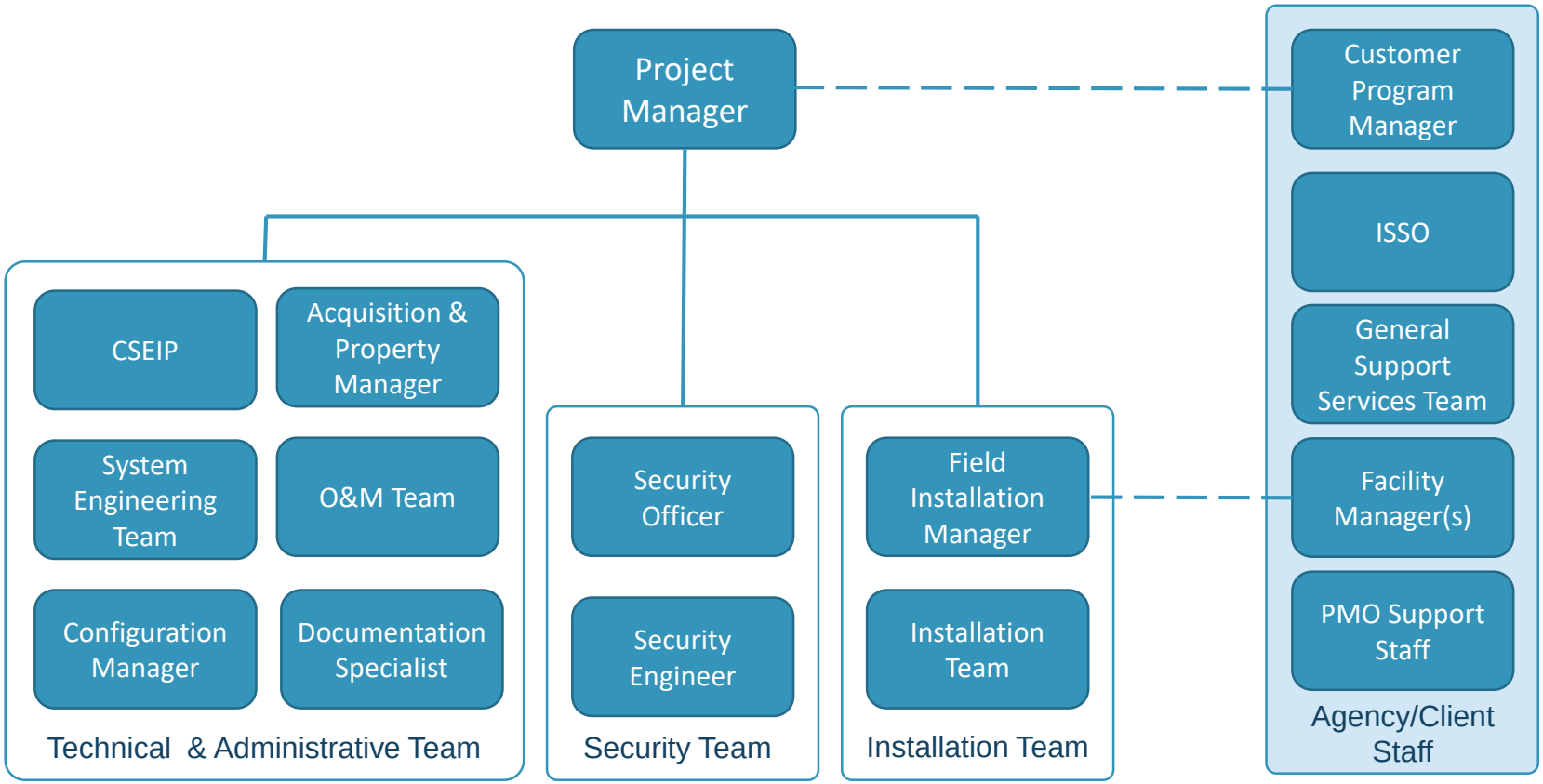
SECURE TECHNOLOGY ALLIANCE

Implementation Life Cycle Approach – Planning Phase

PLANNING PHASE

- Establish Project Team
- Analyze Proposal and Requirements
- Define Milestones, and Deliverables (Schedule)
- Identify Responsibilities & Dependencies (Internal & External)
- Develop Monitoring & Reporting Plan (Progress, Issues, Billing)
- Plan Acquisition of Materials & Equipment
- Plan for Security & Privacy Assessment, if required

Project Team



GSA Schedule 70 & 84 The primary Schedules for satisfying PACS requirements.

GSA Schedule 70 & 84: FIPS 201-2 Compliant and Approved PACS Components and Services

- SIN 132-62 HSPD-12 Products & Services
- SIN 132-60 F Identity & Access Management Professional Services
- SIN 246 35 7 Physical Access Control Systems (PACS) FIPS 201 Approved PACS Products List (APL)
  https://www.idmanagement.gov/approved-products-list-pacs-products/

- SIN 246 60 5 Security System Integration, Design, Management, and Life Cycle Support
  https://www.gsaelibrary.gsa.gov/ElibMain/sinDetails.do?executeQuery=YES&scheduleNumber=84&flag=&filter=&specialItemNumber=246+60+5
  - Includes the Certified System Engineer ICAM PACS (CSEIP) - labor for installation of APL PACS Solutions. Registry of CSEIPs: https://www.securetechalliance.org/activities-cseip-registry/

Reference:

GSA Physical Access Control Systems (PACS) Customer Ordering Guide
https://www.gsa.gov/cdnstatic/Guide_to_PACS_-_REVISED_060717.pdf

SECURE TECHNOLOGY ALLIANCE

Credential Types

Common Credential Types

- PIV
- PIV-I
- CAC

Other Credentials

- Temporary Cards
- Visitor Cards
- Other variants

Basic PACS Infrastructure Characteristics

Installation Type

- PIV-Enabling Existing PACS, or
- New PIV-Enabled PACS Installation

Connectivity

- Standalone PACS, or
- Agency/Internet Network Access

Enterprise Integration

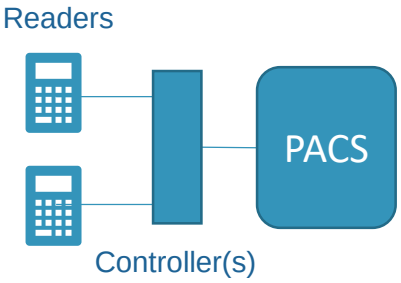
- Identity/PIV Data Provisioned, or
- No Not Provisioned

Hosting

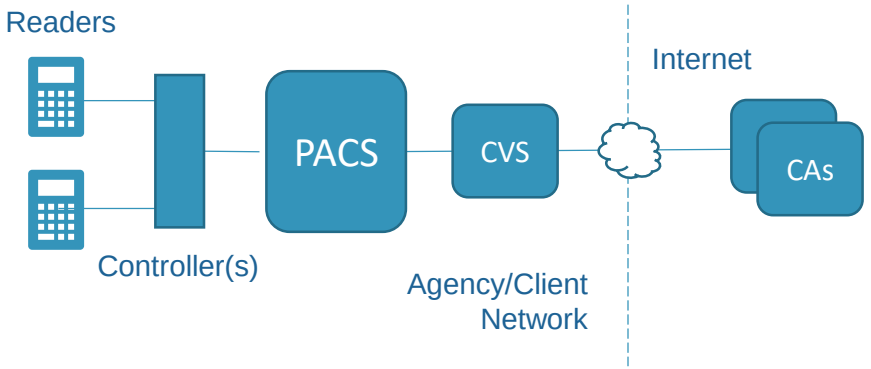
- Customer/Agency Hosted, or
- Provider Hosted (e.g., Commercial Cloud, FedRAMP Cloud)

PACS Topologies

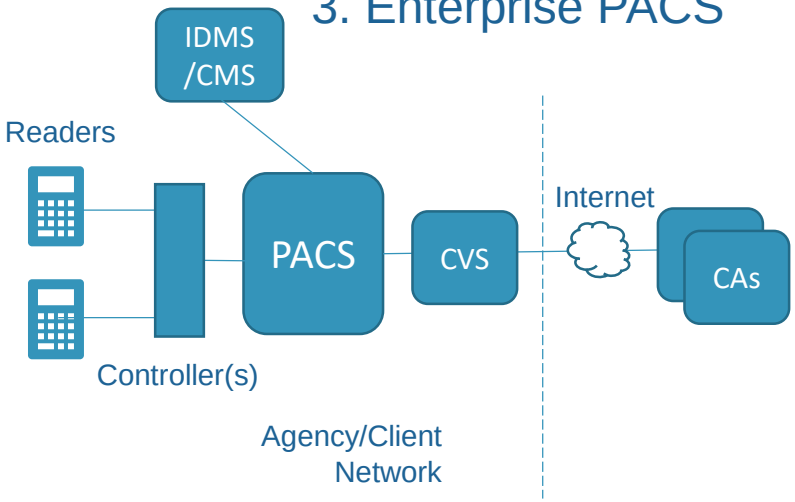
1. Stand Alone



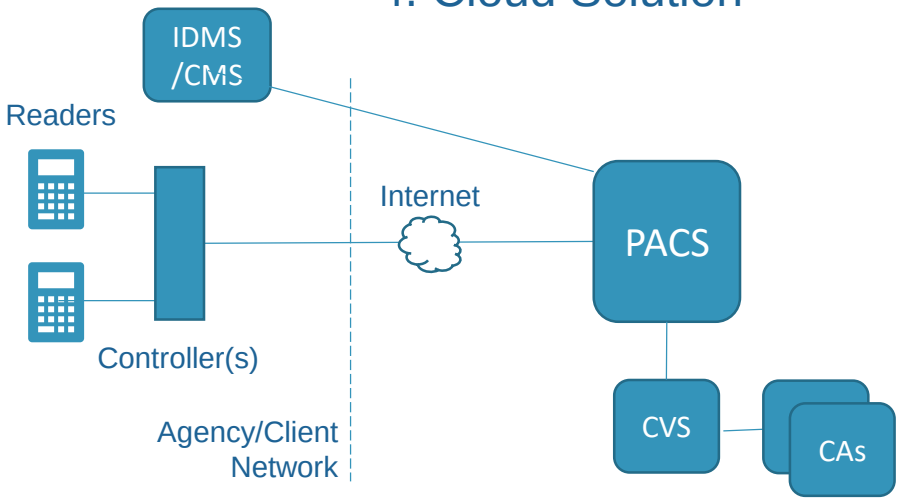
2. Networked



3. Enterprise PACS



4. Cloud Solution



SECURE TECHNOLOGY ALLIANCE

*CVS = Certificate Validation Services

*CA = Certificate Authority

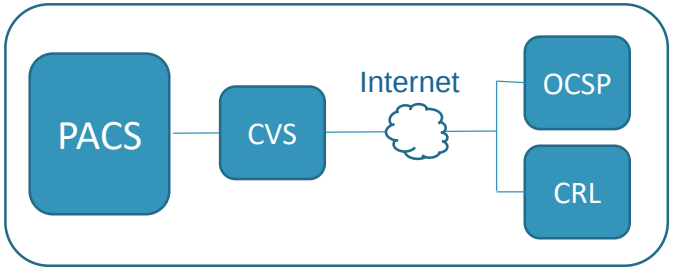
Network Connected PACS Advantages

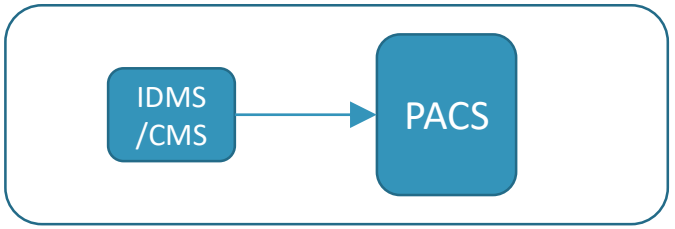
1. During authentication, PACS can **validate digital certificates** via online OCSP & CRLs provided by Certificate Authorities (CA)s; and certificate authority path validation.

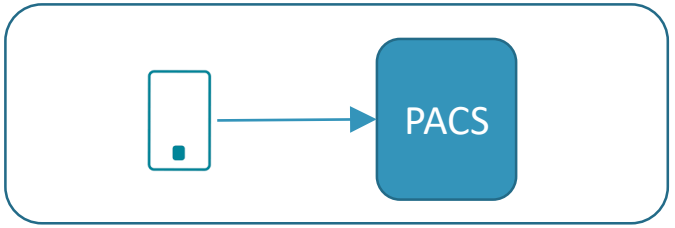
   Otherwise, best case is to load CRLs into the PACS manual (daily,) for those PACS that support offline CRL checking

2. Initial identities and/or PIV card data can be **provisioned** from an external Enterprise Identity Management System, PIV Credential Issuer, or an Authoritative Identity Data Source.

   Otherwise, PIV cards must be registered locally into the PACS





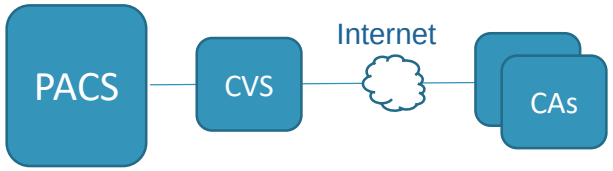


SECURE TECHNOLOGY ALLIANCE

Interoperability Planning

- Is the PACS to accept PIV/PIV-I credentials from outside agencies or qualified business entities?

- If so,
  - Provisioning of external PIV cards from external sources (e.g., IDMS/CMS) may not be feasible; i.e., cards would be registered manually into the PACS
  - Certificate Validation Services (CVS) my have to access multiple Certificate Authorities to validate digital certificates



PIV Enabling an Existing PACS

- Will need to add/replace PIV-card readers at access points
- Will need to install PACS software that can authenticate PIV cards
- May have to:
  - Replace wiring 
  - Replace control panels 
  - Replace PACS Head-End equipment (e.g., server or desktop) 

Updating an Existing PIV-Enabled PACS

- Before CHUID authentication was deprecated in FIPS 201-2 (2013), many PIV-Enabled PACS were deployed using it.

- Updating an existing PIV-enabled PACS may include upgrading readers to perform PKI-CAK authentication instead of CHUID authentication..

Accreditation & Authorization Planning

- For Agency-hosted PACS, an **Accreditation & Authorization** (A&A) must be performed. This process includes:

  a. FIPS-199 Categorizing as a **Low, Moderate or High Impact System**
  b. Applying applicable NIST SP 800-53 **Security Controls**
  c. Delivering **A&A Documentation** well in advance of Test Phase
     e.g., SSP, FIPS-199, eAuth, PIA, PTA, BIA, IRP, CP, CMP, …
  d. Scheduling Independent **Security Control Assessment(s)**
  e. Obtaining an **Authority to Operate** (ATO), or Interim ATO.
  f. Perform regular **Continuous Monitoring** activities following ATO

- **FedRAMP** PACS Cloud Service Offerings have already been ATO'd through the FedRAMP A&A Process

- **Non-FedRAMP** PACS Cloud Service Offerings may have an existing ATO that can be leveraged

Implementation Life Cycle Approach – Design Phase

DESIGN PHASE

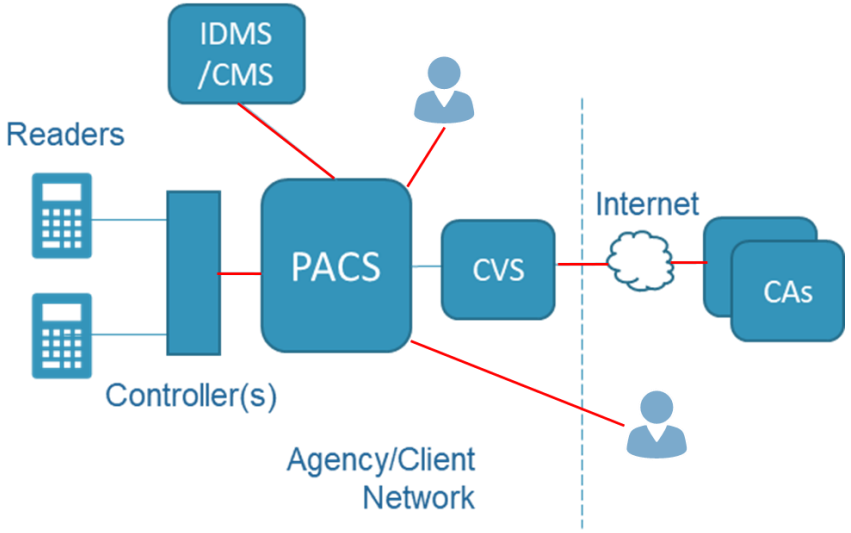
- Apply Requirements Analysis
- *Identify Equipment Type, Quantity & Location*
- *Define Connectivity Configuration*
- *Prepare Installation Documentation*
- Identify Client Furnished Equipment
- Identify and Establish Staging and Operations Areas
- Procure Products, Equipment, and Materials

Facility Access Points & Risk Levels, and Equipment Type, Quantity & Location

Risk Level	Number of Authentication Factors	Example Authentication Mechanism
Controlled	1	PKI-CAK
Limited	2	PKI-AUTH
Exclusion	3	PKI-AUTH+BIO

Connectivity Configuration

Critical Network Connections
- User Workstations
- IDMS/CMS to PACS
- PACS to Controllers
- PACS/CVS to CAs



Identify Network Issues
- Are there any Virtual Private Network(s) (VPNs) requirements?
- Does the client network support PACS system network transaction loads? Examples:
  - Reader-to-PACS Head-End Traffic
  - Head-End to External Services; e.g., Certificate Authorities

Installation Documentation

- Riser Diagrams (per site)
- Reader and Controller Installation & Configuration
- Network Configurations Settings
- Installation Training Materials
- Etc.

Implementation Life Cycle Approach – Installation Phase

INSTALLATION PHASE

- Install & Configure Equipment
- Develop Test Plan
- Develop Security & Privacy Assessment Documentation

IMPLEMENTATION OF SOLUTION

A. Establish Certified PACS Validation System

1. Network connectivity with IT policy compliance
   a. Identity Validation requires external network
   b. Card Authentication requires internal network

2. Validation of PIV Certificates at time of registration
   a. Required prior to provisioning PACS
   b. Harvest Credential or Authoritative Source provisioning

3. Configure recurring validation checks

4. Validation protocol: OCSP or CRL Checks

IMPLEMENTATION OF SOLUTION

B. Define locations and areas where high assurance of identity authentication will be required. Use appropriate authentication mechanism for each. This is typically guided by organization's policy and final design.

Risk Level	Number of Authentication Factors	Example Authentication Mechanism
Controlled	1	PKI-CAK
Limited	2	PKI-AUTH
Exclusion	3	PKI-AUTH+BIO

IMPLEMENTATION OF SOLUTION

C. Access Levels and Privilege Management

1. Some PACS allow access levels to be assigned at time of credential registration. Plan the method of assignment before provisioning/registration.
2. Have the access level assignments for each cardholder ready or it will require revisiting the cardholder record to add privileges later.
3. If not available at time of registration, establish a minimum set of access levels approved by the client.

IMPLEMENTATION OF SOLUTION

D. PACS Registration Mechanisms (Provisioning)

1. Individual card harvesting and PACS provisioning
   a. Credential holder authenticates and validates as part of the process; or, certs cached for bulk validation prior to operational use. Validation requires external network.
   b. Mapping of credential data to PACS pre-configured so PACS database populated properly.

2. Automated PACS provisioning - Integration
   a. Requires IT integration with authoritative data source
   b. Confirm whether credential validation will be performed prior to provisioning or after – who performs validation?

IMPLEMENTATION OF SOLUTION

E. Perform Registration / Enrollment of Credentials

1. Establish per contract who is to perform credential registration process (partial or all). Partial includes operator training to complete.
2. Verify there are no card harvesting issues that could impact project timetable such as improperly formatted cards or validation system connectivity.
3. Test all anticipated card types. Not all PIV cards are created equal! (they are suppose to be)
4. Continue with field equipment installation.

IMPLEMENTATION OF SOLUTION

F. Test and Verify Authentication Mechanisms, Access Privilege Assignments and Performance

1. Test one factor, two factor and three factor authentication mechanisms.
2. Verify access grants occur in accordance with access level assignments and privilege levels.
3. Confirm transaction time from card read to access grant is acceptable. Design phase should have addressed component interoperability. In the field we now add the cabling infrastructure.

IMPLEMENTATION OF SOLUTION

G. Continue with field equipment installation

1. Complete the installation of all access control panels, verify network connectivity and configuration and provisioning of reader PKI licenses and certificates.
2. Verify correct PIV authentication mechanisms are functioning properly. One, Two and Three Factor.
3. Verify design loading of FICAM readers to controller is in accordance with manufacturer's recommendation and the performance is not degraded. (GSA APL does not test loading factor).

Implementation Life Cycle Approach – Testing Phase

TESTING & ASSESSMENT PHASE

- Function, Partial and Integration Testing
- Final Acceptance Testing
- Information Assurance Assessment
- Authority To Operate (ATO)

TESTING & COMPLETION

A. Functional Testing

1. During initial installation – Cards, Authentication, Network
2. Partial functional testing – Access, Workflow & Systems Integration functions (Video, Alarm Monitoring, Reporting)
3. Complete functional testing (Full System)
4. Information assurance testing – ATO compliance

B. Acceptance Testing

1. Partial acceptance testing (per approved phases)
2. Final acceptance testing (individual systems or all systems)
3. Information Assurance – documentation and support for ATO.

C. Punch List Corrections – Created during inspections

Implementation Life Cycle Approach – O&M Phase

OPERATIONS & MAINTENANCE PHASE

- Training
  (Operators, Administrators & Technicians)
- Turnover
- Final As-Built Documentation
- Warranty
- Maintenance
- Continuous Diagnostics and Mitigation (CDM)

SECURE TECHNOLOGY ALLIANCE

TRAINING

A. Operator Training

1. Identify individuals who will perform day-to-day operational duties and provide training for those functions as required. Hands on training preferred.
2. Prepare training document with screen shots from actual system for reference.

B. Administrator Training

1. Identify primary and secondary administrators and prepare training syllabus to address applicable functions as determined by prior review.

TRAINING

C. Technical Training

1. Routine maintenance – Identity those elements of the system that are to be regularly inspected and checked to maintain expected level of performance to include power failure conditions and battery life.
2. First level technical support – What is to be performed by the customer and to what level
3. Second level technical support – procedures for executing service calls
4. Third Level technical support – procedures that would allow for third party access or remote diagnostics

TURNOVER

A. Contract Completion

B. Final System Documentation

C. Final Assignment Correspondence

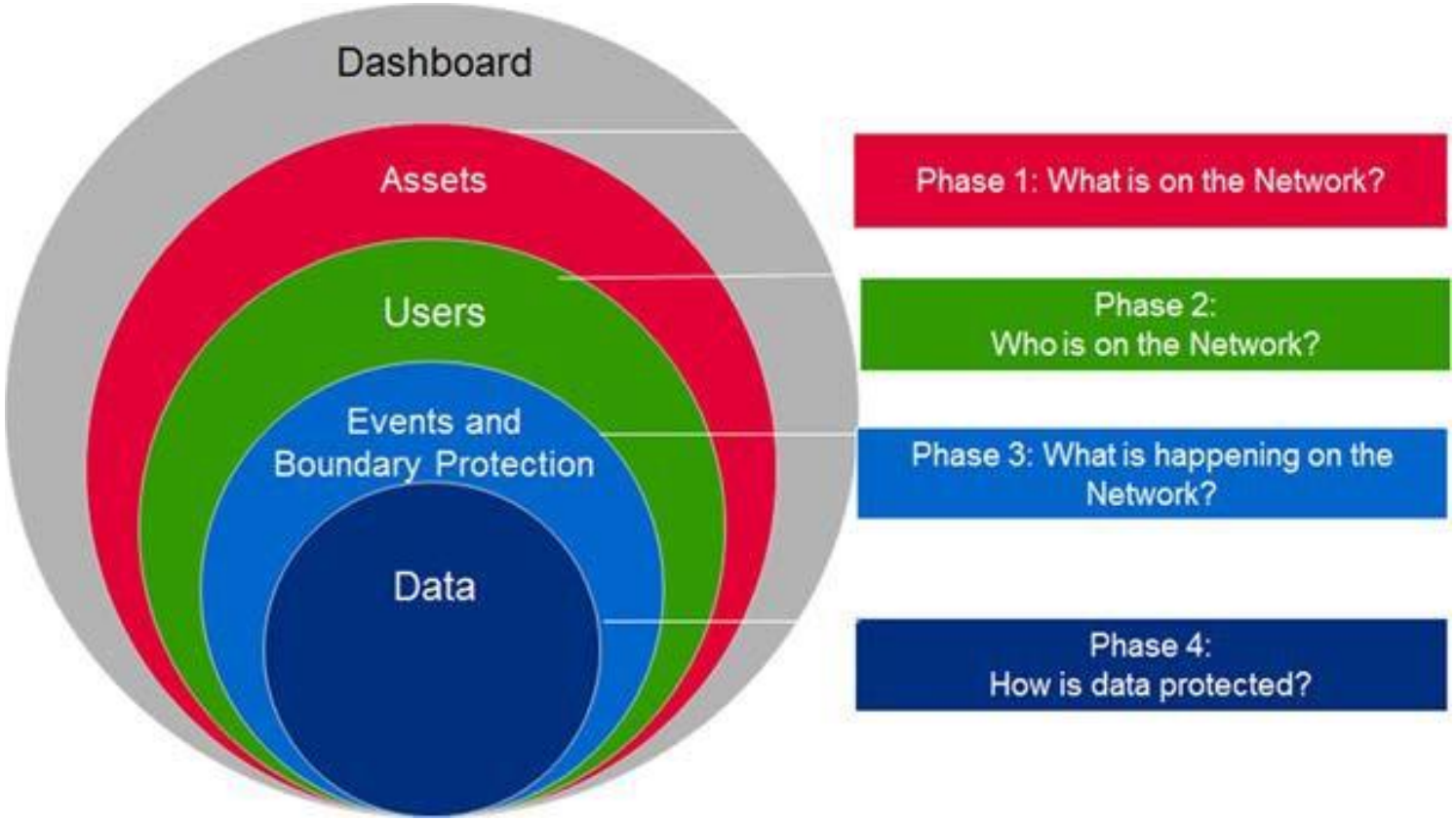
D. Lifecycle Management

Coming to a PACS near you…

Continuous Diagnostics and Mitigation (CDM) Technical Capabilities Volume Two Requirements Catalog

Version 1.0
July 18, 2017

Phases of CDM



SECURE TECHNOLOGY ALLIANCE

Manage Boundary Protections (BOUND), or "How is the network protected?"

- BOUND is categorized into three security capabilities:
- BOUND-F to Manage Network Filters and Boundary Controls
- BOUND-E to Monitor and Manage Cryptographic Mechanisms Controls
- BOUND-P to Monitor and Manage Physical Access Controls

II - 4.1.3.1 BOUND-P Operational Requirements

BOUND OR-3-1: Shall integrate with IP-addressable PACS components to support all CDM capabilities.

https://www.gsa.gov/cdnstatic/CDM_Tech_Cap_Vol_Two_Req_Catalog_v1.0_2017-07-18.pdf

Upcoming Sessions

Stakeholders	Session 1 10/19/2017	Session 2 11/30/2017	Session 3 1/11/2018	Session 4 2/22/2018	Session 5 3/15/2018	Session 6 4/19/2018
Acquisition	♦		♦	♦		♦
Budget	♦		♦	♦		♦
Customers / Tenants	♦	♦	♦		♦	♦
Engineering	♦				♦	♦
Executive Sponsors	♦	♦	♦	♦	♦	♦
Facility Management	♦	♦	♦		♦	♦
Information Technology	♦		♦		♦	♦
Legal	♦	♦		♦		♦
Personnel	♦		♦		♦	♦
Physical Security	♦	♦	♦	♦	♦	♦
Safety	♦	♦			♦	♦

SECURE TECHNOLOGY ALLIANCE

Resources and Contacts

http://www.securetechalliance.org

Lars Suneborn, CSCIP/G, CSEIP

Director, Training Programs, Secure Technology Alliance

lsuneborn@securetechalliance.org

Mark Dale,

Senior Systems Engineer, XTec, Inc.

mdale@xtec.com

Tony Damalas,

VP ICAM Professional Services, Signet Technologies Convergint Federal Solutions

Tony.Damalas@signetinc.com