SECURE TECHNOLOGY ALLIANCE

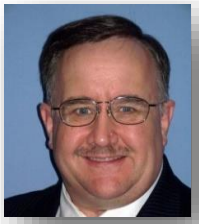
How to Plan, Procure & Deploy a PIV-Enabled PACS

Access Control Council Webinar Series

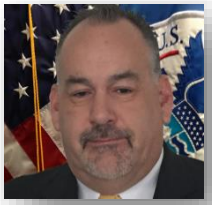
Introductions

Randy Vanderhoof, Secure Technology Alliance

Lars Suneborn, Secure Technology Alliance



Michael Kelley, Parsons Corp.



William Windsor, Department of Homeland Security

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

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

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*

Compliance Requirements

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

1) Identify and plan for the resources needed to implement information security and privacy programs;

2) Ensure that information security and privacy are addressed throughout the life cycle of each agency information system, and that security and privacy activities and costs are identified and included in IT investment capital plans and budgetary requests

3) Plan and budget to upgrade, replace, or retire any information systems for which security and privacy protections commensurate with risk cannot be effectively implemented

OMB Circular A-130, 2016

SECURE TECHNOLOGY ALLIANCE

Challenges

- *No two implementations are the same*
  - *Organization and mission*
  - *Budget and time constraints*
  - *Existing conditions*
- *Moving targets*
  - *Standards*
  - *Organization and mission*
- *Tendency to achieve full compliance all at once*
  - *NIST 800-116 PIV Implementation Maturity Model*

Series Objectives

- Present a repeatable process to plan, procure and deploy a PIV-enabled PACS
- Applicable to all organizations, facilities and budgets
- Identify key stakeholders and their roles in a successful PACS deployment
- Highlight Federal policies and regulations that impact the procurement and deployment
- Align with the processes contained in GSA Playbooks

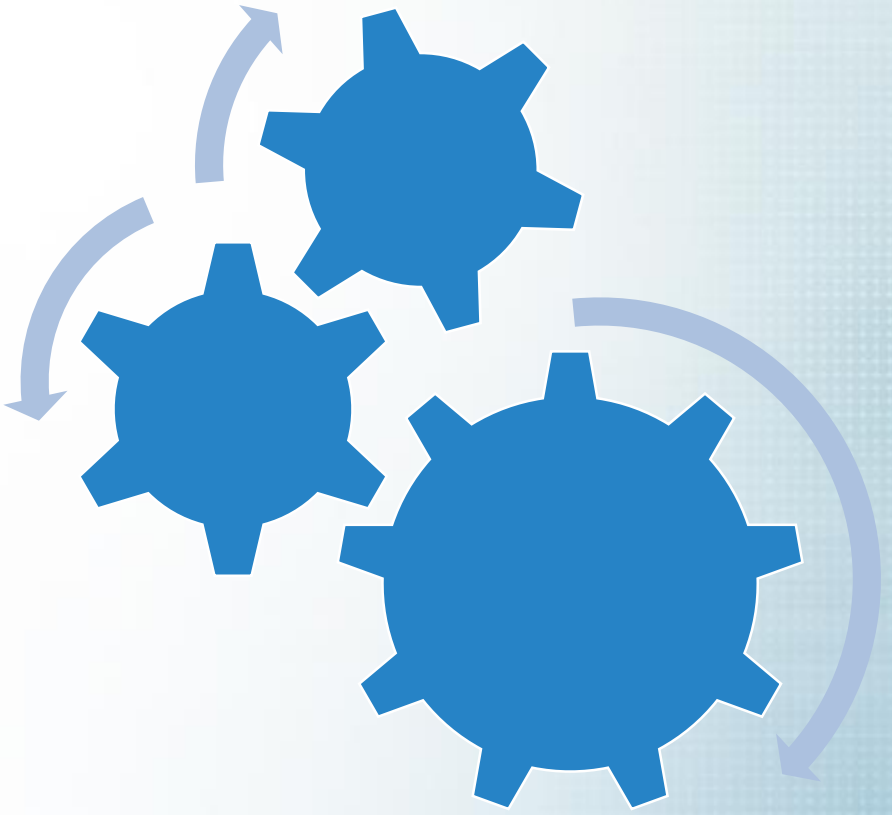
https://www.idmanagement.gov/build/#playbooks

The Process

Facility Characteristics	Risks	Scope	Procurement Strategy	Deployment
• Size • Mission • Assets • Existing Conditions • Regulatory Requirements	• Threats • Likelihood • Consequence	• Risks to be mitigated • Costs and timelines • Potential solutions • Potential providers	• Responsibilities • Standards • Procurement vehicles • Contract documents • Funding • Evaluation • Award	• Management • Design • Installation and configuration • Testing and acceptance • Training • Cutover • Close out

Stakeholders

- Acquisition
- Budget
- Customers / Tenants
- Engineering
- Executive Sponsors
- Facility Management
- Information Technology
- Legal
- Personnel
- Physical Security
- Safety



SECURE TECHNOLOGY ALLIANCE

Upcoming Sessions

- Session 2 – November 30, 2017: Facility Characterization & Risk Assessment
- Session 3 – January 11, 2018: Establishing the Project Scope
- Session 4 – February 22, 2018: Developing the Procurement Strategy
- Session 5 – March 15, 2018: Implementing the Solution
- Session 6 – April 19, 2018: Use Cases and Lessons Learned

All webinars begin at 2 p.m. ET/11 a.m. PT.

Visit the Secure Technology Alliance web site to register for a session or to watch the recording of any previous session.

SECURE TECHNOLOGY ALLIANCE

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

Michael Kelley, CSCIP/G, CSEIP, PSP, CBP

Principal ESS Technical Specialist, Parsons Corp.

michael.p.kelley@parsons.com

William Windsor, CSEIP

Department of Homeland Security

william.windsor@hq.dhs.gov

SECURE TECHNOLOGY ALLIANCE