SECURE TECHNOLOGY ALLIANCE

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

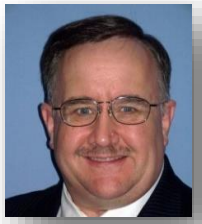
Access Control Council Webinar Series

Session Six: Lessons Learned

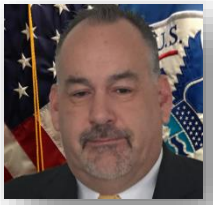
Introductions

Lars Suneborn, Secure Technology Alliance

Michael Kelley, Parsons Corp.



William Windsor, Department of Homeland Security



Tony Damalas, Signet Convergint Federal Solutions

Mark Steffler, Quantum Secure

Stafford Mahfouz, Software House

Daryl Hendricks, General Services Administration

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/Government**
  - **CSEIP**

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

Webinar Series Session Review

All reference documents are on the last slides

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

Session Six

Lessons Learned

- Policies
- Operation & Implementation
- Procurement

SECURE TECHNOLOGY ALLIANCE

Policies

Operation
&
Implementation

Procurement

Summary

- Achieving compliance is being completed by use of an increasing number of COTS equipment that have passed strict conformance testing by GSA EV Program Test Laboratories
- Use Services delivered by a growing number of Certified System Integrators
- Requires cooperation between IT, Security, Facilities and Procurement

SECURE TECHNOLOGY ALLIANCE

SECURE TECHNOLOGY ALLIANCE

Q&A

(Reference documents & links on last slides)

Resources and Contacts

http://www.securetechalliance.org

- Lars Suneborn, CSCIP/G, CSEIP, Secure Technology Alliance, lsuneborn@securetechalliance.org
- Tony Damalas, Technologies Convergint Federal Solutions, Tony.Damalas@signetinc.com
- Daryl Hendricks, General Services Administration, daryl.hendricks@gsa.gov
- Michael Kelley, Parsons Corp., michael.p.kelley@parsons.com
- Stafford Mahfouz, Software House, stafford.mahfouz@jci.com
- Mark Steffler, Quantum Secure, msteffler@quantumsecure.com
- William Windsor, Department of Homeland Security, william.windsor@hq.dhs.gov

SECURE TECHNOLOGY ALLIANCE

References

"Managing Information as a Strategic Resource", OMB Circular No. A-130
https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf

"Digital Identity Guidelines", NIST Special Publication 800-63-3
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

"A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)", NIST Special Publication 800-116
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-116.pdf

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

"The Risk Management Process for Federal Facilities: An Interagency Committee Standard"
https://hsin.dhs.gov/Pages/home.aspx

ASIS International Risk Assessment Standard ANSI/ASIS/RIMS RA.1-2015
https://www.asisonline.org/Standards-Guidelines/Standards/Pages/default.aspx

"Continued Implementation of Homeland Security Presidential Directive (HSPD) 12– Policy for a Common Identification Standard for Federal Employees and Contractors", OMB Memorandum M-11-11
https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2011/m11-11.pdf

SECURE TECHNOLOGY ALLIANCE

References

"Personal Identity Verification (PIV) of Federal Employees and Contractors", FIPS 201-2
https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.201-2.pdf

"E-Authentication Guidance for Federal Agencies", OMB Memorandum M-04-04
https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2004/m04-04.pdf

"Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors"
https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2005/m05-24.pdf

FIPS 201 Evaluation Program Approved Products List
https://www.idmanagement.gov/approved-products-list-pacs-products/

“Strengthening the Cybersecurity of Federal Agencies through Improved Identity, Credential, and Access Management”, draft OMB Memorandum M-18-XX
https://policy.cio.gov/identity-draft/

"Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities", IC Tech Spec for ICD/ICS 705
https://www.dni.gov/files/NCSC/documents/Regulations/Technical-Specifications-SCIF-Construction.pdf

SECURE TECHNOLOGY ALLIANCE