Interagency Advisory Board

Meeting Agenda, Wednesday, February 27, 2013

1. **Opening Remarks**

2. **Discussion on Revisions Contained in Draft SP 800-63-2** *(Bill Burr, NIST)*

3. **The Objectives and Status of Modern Physical Access Working Group (MPAWG)** *(Will Morrison and J'son Tyson, MPAWG Co-Chair)*

4. **Overview of PACS Specification from the Security Industry Association (SIA) to Include All PIV Functionality** *(Rob Zivney, Chair of the SIA PIV Working Group and Vice Chair of the Standards Committee)*

5. **Closing Remarks**

Federal CIO Council
Information Security and Identity Management Committee

IDManagement.gov

Expectation of PIV use with Physical Access Systems

J'son Tyson & Will Morrison
Co-Chair,
ICAMSC Modernized Physical Access Working Group (MPAWG)

February 27, 2013

Agenda

- MPAWG Overview
- Evolution of PIV & PACS
- FASC-N, CHUID, CAK, PKI
- Challenge Factors (1,2,3)
- PACS-Enabled Authentication Mechanisms
- PACS in EPACS Requirements

MPAWG Overview

Working Group Description:	Facilitates the implementation and use of the technology and processes related to a modernized PACS.
Functions:	• Coordinate with the Interagency Security Committee (ISC) to harmonize policy and guidance related to PACS • Create guidance on enabling and configuring PACS to accept PIV and PIV-I credentials • Coordinate with industry and PACS product vendors on behalf of the ICAMSC to ensure alignment with ICAM guidance and requirements
Membership Profile:	• Minimum of one standing member who is a member of the ISC • Representatives designated by their agency for physical security implementation/development • Experience writing/reviewing technical physical access guidance • Understanding of PIV-enablement for PACS (or a desire to understand) • Federal Employee or Contractor sponsored by agency

MPAWG Docket

Item Name	Item Description	Status
Enterprise PACS Guidance (PIV in EPACS)	Guidance on establishing Enterprise PACS	From AWG's 2011 docket
Selecting PIV Authentication Mechanisms for PACS	Guidance to bridge the ISC facility risk assessment process and ICAM guidance for using PIV in PACS	Recommended from ICAMSC Governance Review
PACS Implementation Metrics	A set of metrics to track and capture PACS implementations across agencies to be submitted as part of annual FISMA metric reporting.	Recommended from ICAMSC
PACS Policy and Guidance Gap Analysis	An analysis of the gaps between PACS policy and guidance.	Recommended from ICAMSC Governance Review
GSA Schedule Analysis	An analysis of where there are inconsistencies across the PACS products on the schedules and contradictions with the APL	Recommended from ICAMSC Governance Review
Mandatory PIV Usage Guidance	Technical guidance on how to implement a mandatory PIV “usage”	Recommended from ICAMSC Governance Review

Basics of HSPD-12

- Enhance security
- Increase Government efficiency
- Reduce identity fraud
- Government-wide standard for secure and reliable forms of identification

Brief Evolution of PIV for PACS

- August 2004, HSPD-12 Signed
- February 2005, FIPS 201 Published
- March 2006, FIPS 201-1 Published
- November 2008, NIST SP 800-116 Published
- November 2009, FICAM Roadmap Guidance (v1) Published
- February 2011, OMB Memo M-11-11 Promulgated
- December 2011, FICAM Roadmap Guidance (v2) Published (*Chapter 10, Modernized PACS*)
- ANTICIPATED, 2013: ICAMSC PIV in EPACS Guidance Released (*Update to Federated PACS Guidance Doc dtd 6-2011*)
- ANTICIPATED, 2013: FIPS 201-2 Published

FASC-N, CHUID, CAK, PKI

ICAM Identity, Credential, & Access Management

Federal Agency Smart Credential Number (FASC-N):

A fixed length (75 Bit) data object; **The primary identified on the PIV Card for physical access control**

FASC-N Identifier: A subset of the FASC-N, it is a unique identifier.

"*For full interoperability of a PACS it must at a minimum be able to distinguish fourteen digits (i.e., a combination of an Agency Code, System Code, and Credential Number) when matching FASC-N based credentials to enrolled card holders*."

Cardholder Unique Identifier (CHUID):

An authentication mechanism that is implemented by transmission of the data object from the PIV Card to the PACS

Card Authentication Key (CAK) ['keyk']:

Defined in NIST SP 800-73; An authentication mechanism that is implemented by a key challenge/response protocol

Source: NIST SP 800-116

❖ Public Key Infrastructure (PKI):

Defined in X.509 Certification Policy for the Federal Bridge Certification Authority (FBCA); A set of policies, processes, server platforms, software, and workstations used for administering certificates and public/private key pairs, **including the ability to issue, maintain, and revoke public key certificates**.

❖ PKI-PIV Authentication Key (PKI-AUTH) or (PAK):

Defined in FIPS 201-2; A PIV authentication mechanism that is implemented by an asymmetric key challenge/response protocol using the PIV authentication key of the PIV card and a contact reader.

Change?

Federal Information Processing Standards Publication 201-2 (FIPS 201-2)

Anticipated:

- ✓ Nexus for updating NIST SP 800-116
- ✓ Deprecates use of CHUID as an authentication mechanism (low)
- ✓ CAK becomes mandatory
- ✓ Impose use of PKI-AUTH (PAK) or CAK for token authentication

Challenge Factors

HAVE

e.g., PIV or PIV-I Card (Challenge/Response)

KNOW

e.g., PIN (either to unlock card or PACS verification)

ARE

e.g., Biometrics (fingerprint, et cetera)

Challenge Factors

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

Source: NIST SP 800-116

PACS-enabled Authentication Mechanisms

ICAM Identity, Credential, & Access Management

Factors	PACS-enabled Authentication Mechanism	Max Confidence	CL?	Int?	Factors
No Factor	PIN to PIV/PIV-I[30] (without cryptography)	No Confidence	CL	✓	
	CHUID (FASC-N, UUID)	No Confidence	CL	✓	
One Factor	CHUID+VIS	Little or No Confidence	CL	✓	Have
	BIO	Some Confidence	-	✓	Are
	CAK	Some Confidence	CL		Have
	CHUID[31] + PIN to PACS	Some Confidence	CL	✓	Know
	CHUID + BIO to PACS	Some Confidence	CL	✓	Are

CL? = Authentication Mode is available on the contactless interface
INT? = Authentication Mode is interoperable across cards from other PIV issuers

PACS-enabled Authentication Mechanisms

ICAM Identity, Credential, & Access Management

Factors	PACS-enabled Authentication Mechanism	Max Confidence	CL?	INT?	Factors
Two Factor	CAK + PIN to PACS	High Confidence	CL		Have + Know
	CAK + BIO to PACS	High Confidence	CL		Are + Have
	PKI-Auth (PAK)	High Confidence	-	✓	Know + Have
Three Factor	PKI-Auth (PAK) + BIO	Very High Confidence	-	✓	Know + Are + Have
	PKI-Auth (PAK) + BIO to PACS	Very High Confidence	-	✓	Know + Are + Have
	CAK + BIO	Very High Confidence	-		Know + Are + Have
	CAK + BIO to PACS + PIN to PACS	Very High Confidence	CL	✓	Know + Are + Have
	BIO-A	Very High Confidence			Know + Are + Have

CL? = Authentication Mode is available on the contactless interface
INT? = Authentication Mode is interoperable across cards from other PIV issuers

PIV in EPACS

PACS will need to:

- Provision or register the PIV Authentication Key (PKI-AUTH / PAK) or Card Authentication Cert (CAK)

OR

- Provision or register a PKI credential derived from PAK/CAK

AND

- Electronically validate PKI certificate
- Validate/Challenge the private key of registered PIV/PKI certificate

Align → Collaborate → Enable

Challenge Factors

PIV Authentication Mechanism	Have	Know	Are	Authentication Factors[19]	Interface
PKI-Auth + BIO-A	Smartcard with crypto key (High Assurance Factor)	PIN with crypto proof (Medium Assurance Factor)	Observed Fingerprint (Medium Assurance Factor)	3	Contact
PKI-Auth + BIO	Smartcard with crypto key (High Assurance Factor)	PIN with crypto proof (Medium Assurance Factor)	Fingerprint (Low Assurance Factor)	3	Contact
CAK[20] + BIO-A	Smartcard with crypto key (High Assurance Factor)	PIN with indirect verification assumption (Low Assurance Factor)	Observed Fingerprint (Medium Assurance Factor)	3	Contact
CAK[20] + BIO	Smartcard with crypto key (High Assurance Factor)	PIN with indirect verification assumption (Low Assurance Factor)	Fingerprint (Low Assurance Factor)	3	Contact
PKI-Auth	Smartcard with crypto key (High Assurance Factor)	PIN with crypto proof (Medium Assurance Factor)		2	Contact
BIO			Fingerprint (Low Assurance Factor)	1	Contact
CAK[20]	Smartcard with crypto key (High Assurance Factor)			1	Contact/Contactless
CHUID + VIS	Printed Security feature on the Smartcard (Low Assurance Factor)			1	Contact/Contactless

- Grayed areas do not appear in NIST SP 800-116
- ✓ Low assurance factors indicate no cryptographic verification
- ✓ The CAK may be a symmetric or asymmetric key