

IAB Agenda

- **Opening Remarks** (*Tim Baldrige, NASA*)
- **Credentialing Interoperability in DHS Programs** (*Tom Lockwood, DHS*)
- **Backend Attribute Exchange** (*Chris Loudon*)
- **Results of Winter Blast Exercise** (*Craig Wilson, DHS/FEMA*)
- **Status of NASA HSPD-12 Implementation** (*Tim Baldrige, NASA*)
- **TWIC Update** (*Maurine Fanguy, TWIC PM*)
- **SP 800-116 Strategy for use of PIV Credentials in PACS** (*Bill Macgregor, NIST*)
- **Closing Remarks** (*Tim Baldrige, NASA*)

SP800-116

**A Recommendation for the use of
PIV Credentials in PACS**

William I. MacGregor

National Institute of Standards and Technology

U.S. Department of Commerce

26 March 2008

SP800-116 Goals

- Best practice guidelines for the use of PIV with Physical Access Control Systems.
- Fulfill the interoperability and security objectives of HSPD-12.
- Place no unnecessary restrictions on PACS policy, procedures, or architectures.

PIV Benefits

The *PIV System* is an identity infrastructure for Federal employees and contractors.

- Enhanced identity assurance at three levels.
- Rapid electronic verification.
- Resistance to forgery, cloning, and transfer.
- Credential status services.
- Integrated provisioning (over time).
- One credential for multiple applications.

PIV Limitations

The *PIV System* is an identity infrastructure for Federal employees and contractors.

- Subjects other than Federal employees and contractors are out-of-scope.
- Authorization is out-of-scope.
- The electronic authentication methods rely on a PKI trust model (Federal Bridge).
- PIV defines a few, general-purpose authentication methods.

Authentication Mechanisms

FIPS 201 Table 6-2 for Physical Access

PIV Assurance Level Required by Application/Resource	Applicable PIV Authentication Mechanism
SOME confidence	VIS, CHUID, CAK*
HIGH confidence	BIO
VERY HIGH confidence	BIO-A, PKI

* CAK is defined in FIPS 201, but optional.

Characteristics

<u>Method</u>	<u>Type</u>	<u>Use of PKI</u>	<u>Assurance Level</u>
CHUID	Data Token	Optional Sig. Verification	SOME
CAK (Optional)	Challenge/ Response	Certificate Validity	SOME
BIO	Fingerprint Biometric	Optional Sig. Verification	HIGH
BIO-A (Attended)	Fingerprint Biometric	Optional Sig. Verification	VERY HIGH
PKI	Challenge/ Response	Certificate Validity	VERY HIGH

PIV Trust Model

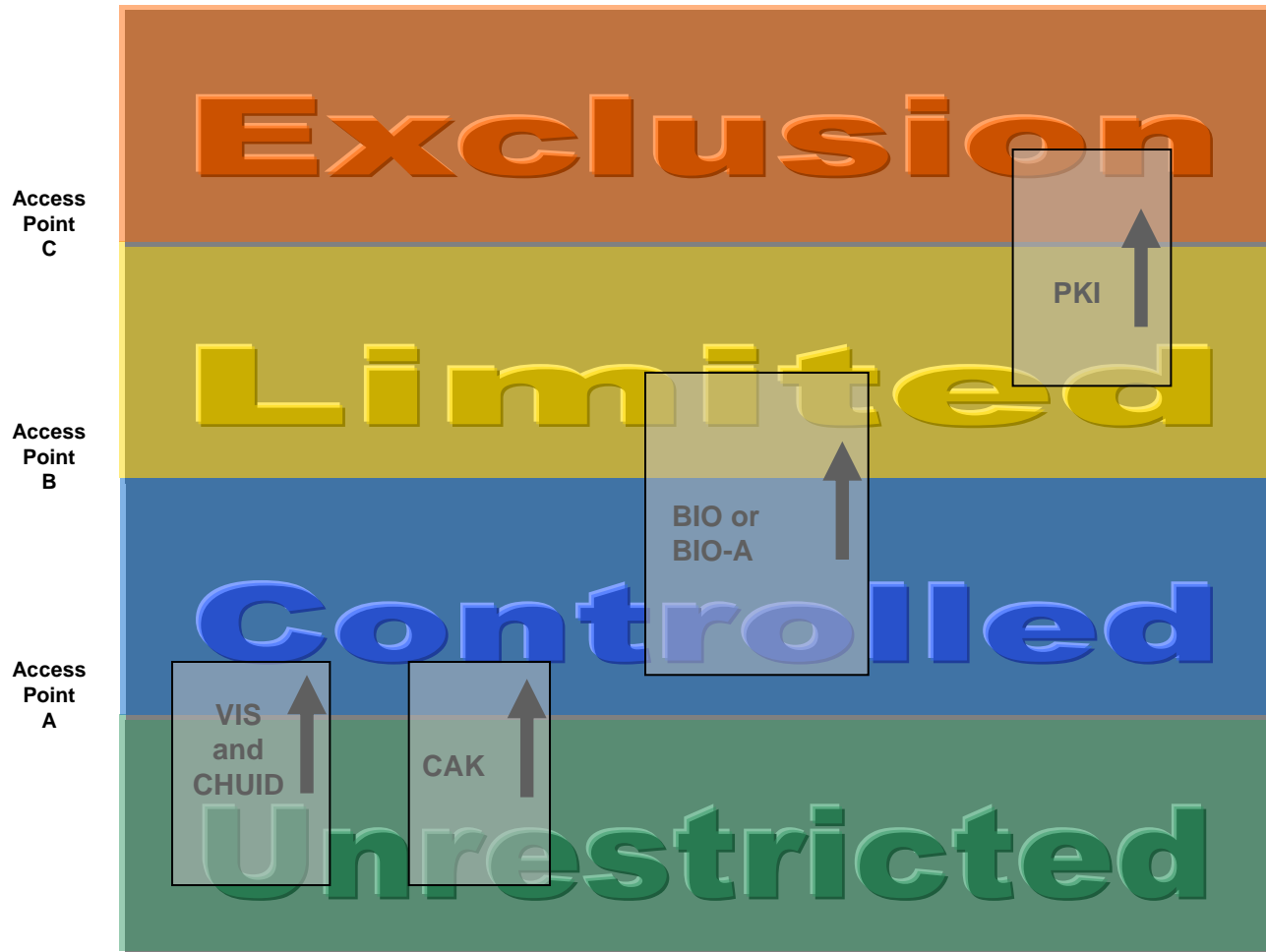
- *All* of the PIV electronic authentication mechanisms rely on PKI trust.
- If PKI credential and path validation are not done, authentication assurance is reduced.
- Credential and path validation should be done with *all* PIV authentication mechanisms.

Planning for PACS

- Issue cards with asymmetric CAK if possible
- Develop a prioritization of controlled access areas
 - Unrestricted, Controlled, Limited, Exclusion...
 - ...or any equivalent 2-, 3-, or 4-tiered model
- Formulate policy for changing Threat Conditions
- Select authentication mechanisms for access control points
 - Consider PIV + legacy multi-technology readers
 - Consider multi-mechanism readers
 - Implement all algorithms required by SP800-78-1

PIV Authentication Mechanisms

Suggested use for nested Physical Access areas.



SP800-116 Status

- NSIT authors are making adjustments based on reviewer comments.
- SP800-73-2 in public comment until 18 Apr 2008.
- -116 public comment target is 31 Mar 2008.
- Comment period duration about 45 days.
- Workshop schedule at NIST on 1 May 2008 (*advance registration required*).

Green Lights

10. Plan & monitor the shared identity infrastructure
9. Develop & coordinate a PIV termination process
8. For PACS, rely on CAK, VIS+CAK, BIO, BIO-A, PKI
7. For visitors, paper for short-term, smart cards for long-term
6. PIV-enable application classes: Windows SSO, web services
5. PIV-enable anchor applications: PACS, logon, secure web, WDE
4. (Agency Code, System Code, Credential Number) identifiers
3. See SP800-73-2 for good news on Global PIN
2. Credential and path validation on every transaction
1. Put out the welcome mat: **“PIV Accepted Here!”**

Thanks for listening!

William I. MacGregor
NIST PIV Coordinator
301 975 8721

william.macgregor@nist.gov

<http://csrc.nist.gov/piv-program/>

FIPS 201 and related documents.

<http://www.cio.gov/ficc/documents/BasicElementsTrustPIVcards103107.pdf>

Basic Elements [of] Trust of PIV Cards.