Interagency Advisory Board

Meeting Agenda, February 2, 2009

1. **Opening Remarks** (*Tim Baldridge, NASA*)
2. **Mini Tutorial on NIST SP 800-116 AND PIV use in Physical Access Control Systems** *(Bill MacGregor, NIST)*
3. **Impact of Agreement Among Four PKI Bridges** *(Tim Pinegar, Protiviti Government Services (PGS) representing GSA/OGPGSA)*
4. **Microsoft's Roadmap for PIV Products: The Impact that will have on PIV Use and Interoperability** *(Vernon Lee, Microsoft)*
5. **Adobe's Roadmap for PIV Products: The impact that will have on PIV Use and Interoperability** *(John Harris, Adobe)*
6. **PAIIWG Update** (*Tim Baldridge, NASA*)
7. **Closing Remarks** (*Tim Baldridge, NASA)*

A Mini-Tutorial on Special Publication 800-116

William I. MacGregor

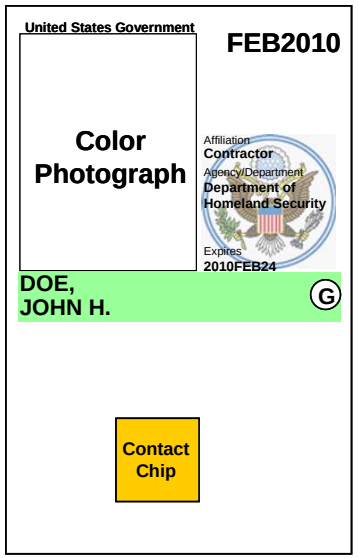
National Institute of Standards and Technology

IAB Meeting, 2 Feb 2009

Employee & Contractor

Sample PIV Cards from SP800-104

Employees



Contractors

NIST
National Institute of Standards and Technology

PIV Card Data Objects

Just 11 objects and 4 authentication methods!

MANDATORY

- **CHUID (Card Holder Unique Identifier)**
- **PIV Authentication Key and Certificate**
- **Fingerprint Template Object**
- Security Object
- Card Capability Container

OPTIONAL

- **Card Authentication Key, and Certificate**
- Key Management Key and Certificate
- Digital Signature Key and Certificate
- Facial Image Object
- Printed Information Object
- Discovery Object

HSPD-12 Status

28 Oct 2008

- 1.6 million PIV Cards issued.
- Some US agencies above 95% issuance.
- Application integration underway:
  - System logon
  - Document signing & verification
  - Secure Messaging
  - Physical Access Control Systems (PACS)

NIST Special Publication 800-116

"A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)"

- Conforms to FIPS 201-1 and SP's in effect
- Reviews current limitations & threat environment
- States the PIV-in-PACS vision and benefits
- Recommends a PACS security model and PIV integration approach
- Proposes a PIV Implementation Maturity Model (PIMM)

Threat Environment

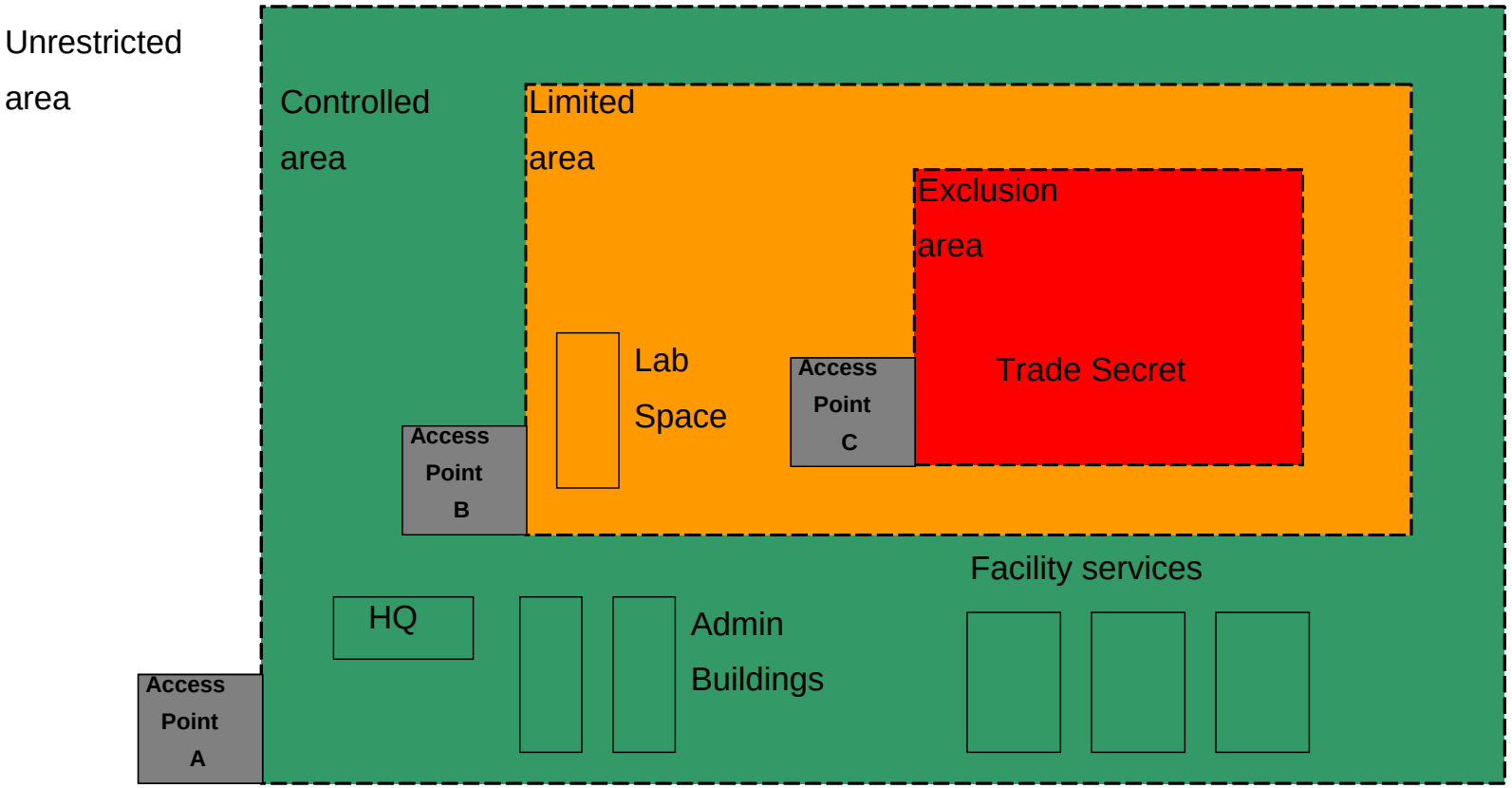
- Threats Considered:
  - Identifier Collisions
  - Terminated PIV Cards
  - Visual Counterfeiting
  - Skimming
  - Sniffing
  - Social Engineering
  - Electronic Cloning
  - Electronic Counterfeiting
- Main Conclusions:
  - The CHUID mechanism is weaker than other PIV authentication mechanisms.
  - PKI path validation is necessary for complete trust.

PIV Benefits

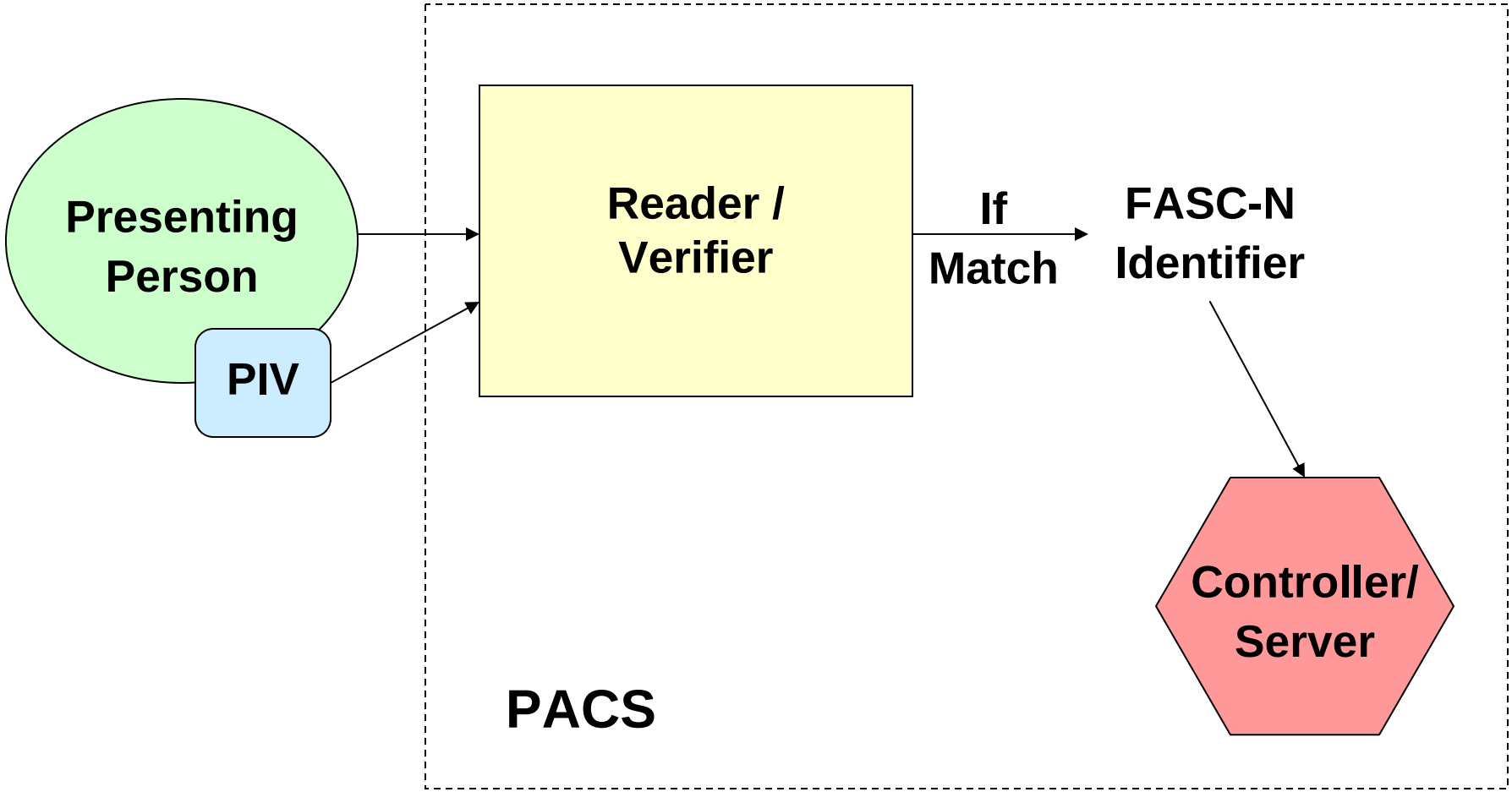
The *PIV System* is an identity infrastructure for Federal employees and contractors.

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

A PACS Model
Unrestricted, Controlled, Limited, Exclusion



Authentication



The FASC-N Identifier

- Federal Agency Smart Credential Number (FASC-N) is the primary PIV identifier

- FIPS 201-1 requires a 14 decimal digit subset to be unique over all PIV Cards:

(Agency Code, System Code, Credential Number)

4 digits 4 digits 6 digits

PIV Authentication Mechanisms
Characteristics

Method	Type	Use of PKI	Assurance Level
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 Public Key Infrastructure (PKI) trust.
- If PKI credential and path validation are not done, authentication assurance is reduced.
- Credential and path validation **must** be done with the PKI and CAK mechanisms.
- Credential and path validation **should** be done with *all* PIV authentication mechanisms.

How to select mechanisms at access points?

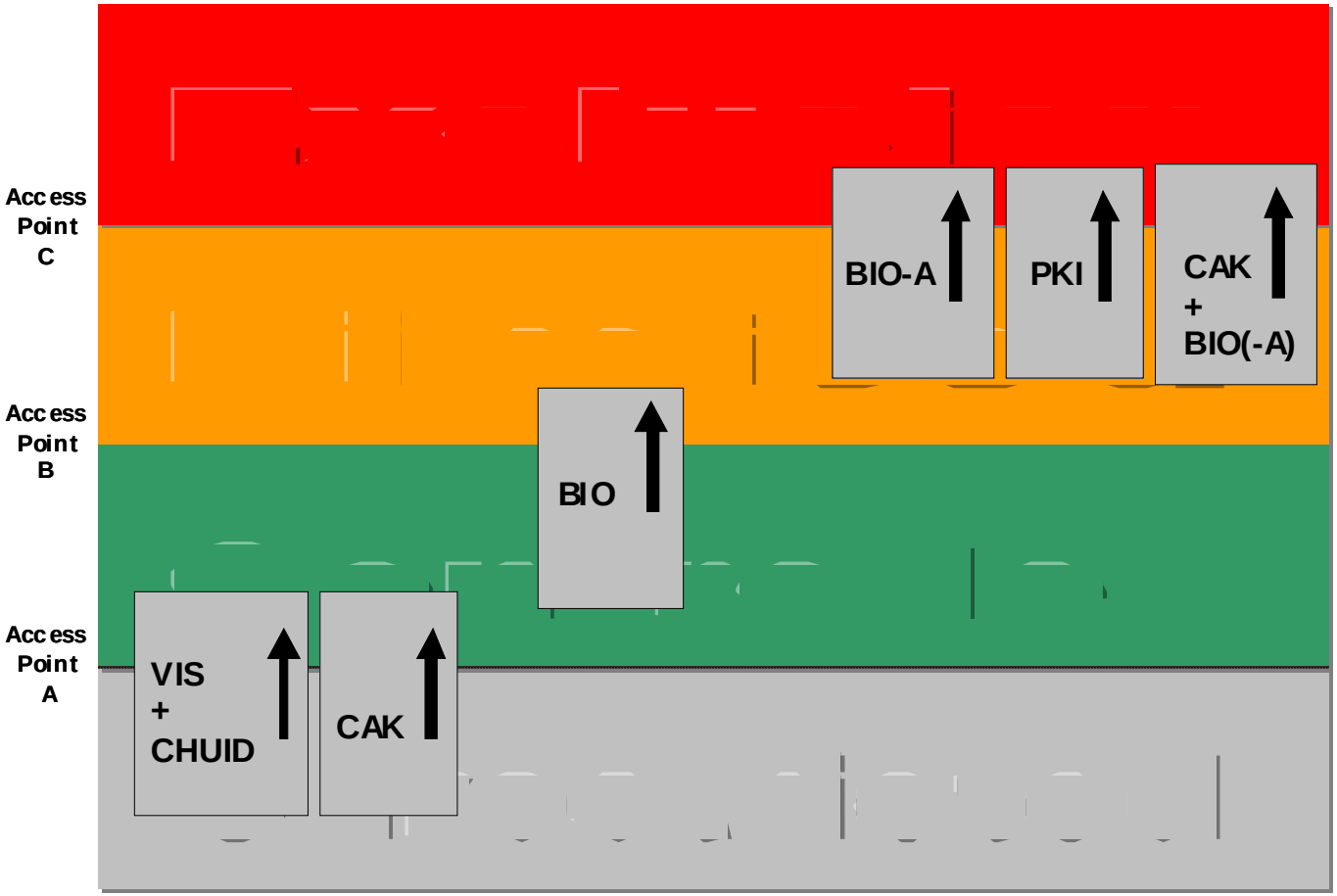
To enter <left column> area, factors in <right column> are required…

Security Areas	Authentication Factors Required
Controlled	1
Limited	2
Exclusion	3

Converting Mechanisms to Factors

PIV Authentication Mechanism	Have	Know	Are	Authentication Factors (HKA Vector)	Interface
CAK + BIO (-A)	x	x	x	3	Contact
BIO-A	x		x	2	Contact
PKI	x	x		2	Contact
BIO			x	1	Contact
CAK	x			1	Contact/ Contactless
CHUID + VIS	x			1	Contact/ Contactless

…and, the mechanisms must be used at or below the perimeter shown.

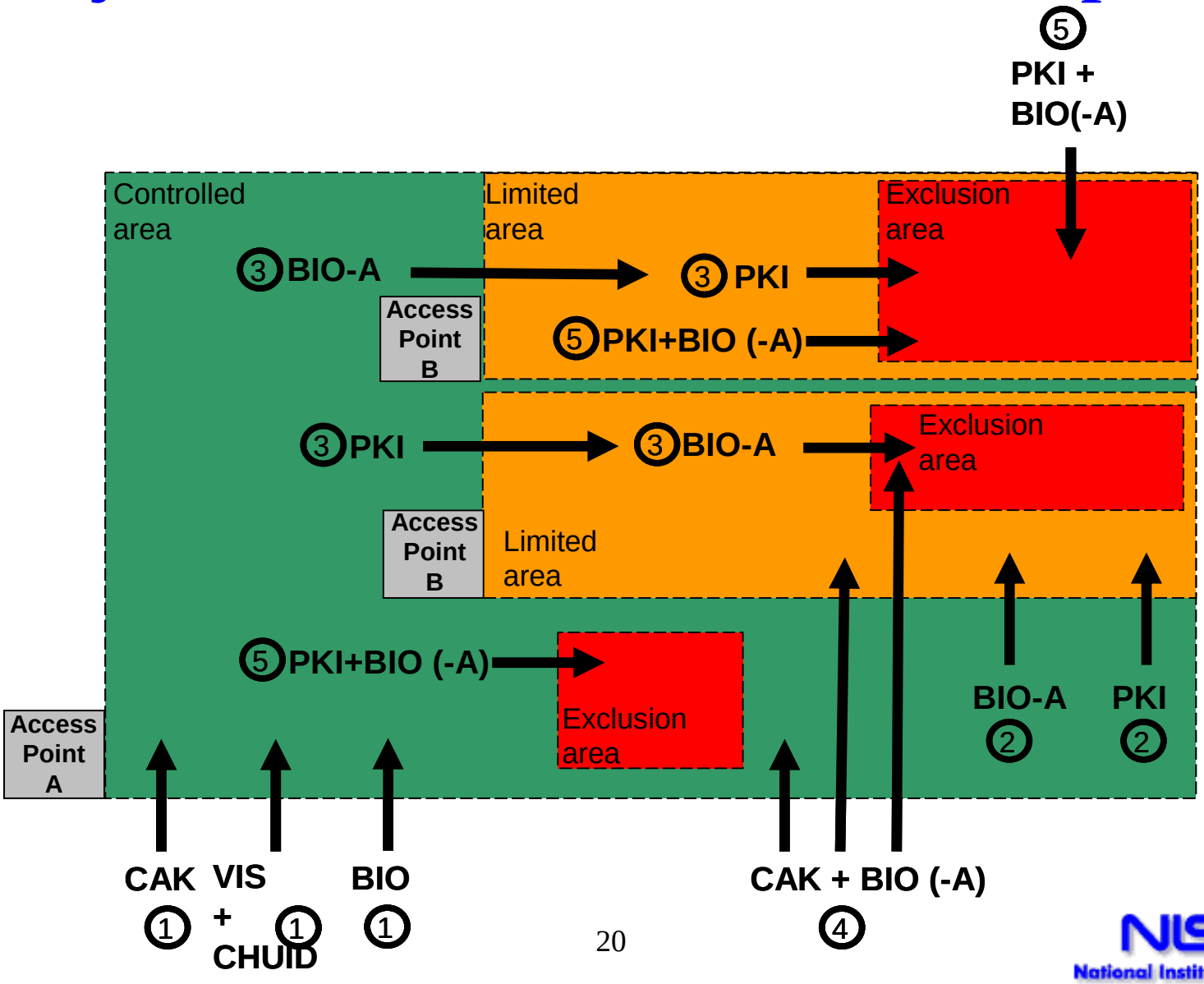


Key Concepts

Illustrated on next slide

1. Access to Controlled Area (most common case.
2. Two factor authentication to Limited Area.
3. Authentication-in-Context.
4. Three factor authentication to Exclusion Area.
5. A single perimeter may separate areas with a difference of more than one impact level.

Physical Access Control Examples



NIST National Institute of Standards and Technology

PIV Implementation Maturity Model (PIMM)

1. PIV Cards accepted on ad hoc basis
2. PIV Cards accepted at the main entrance
3. Only PIV Cards accepted for Exclusion
4. Only PIV Cards accepted for Limited
5. Only PIV Cards accepted for Controlled

Note: levels are cumulative; “only” applies to PIV-eligible persons.

Lessons Learned

- Practical, effective high assurance ID systems are within reach today.
- Multi-factor authentication (two or three factors) are needed for HIGH confidence.
- Good approaches use cryptography to protect all transactions, and authentication-in-context.
- Key management remains a challenging aspect of system architecture and design.
- Public Key Infrastructure (PKI) is well understood, Symmetric Key Infrastructure less so.

Thanks for listening!

William I. MacGregor
NIST PIV Coordinator
(301) 975-8721
william.macgregor@nist.gov

http://csrc.nist.gov