PIV PACS Integration Workshop

Draft SP 800-116 Discussion

National Institute of Standards and Technology
U.S. Department of Commerce
1 May 2008

PIV PACS Integration Workshop Agenda

- Welcome
- SP 800-116 Overview
- SP 800-116 Comment Presentations
- The FIT to Reality (Q&A Session)
- What should be Standardized (Q&A Session)

Welcome to the NIST PIV PACS Integration Workshop!

- Emergency Building Exits – exit room and
  - Turn right, go to end of hall, or
  - Go straight to lobby, out main entrance, or
  - Turn left, go to end of hall, turn left & down stairs
- Cafeteria is directly across the hall
- Restrooms are half-way back to main lobby

NIST National Institute of Standards and Technology

The business at hand:

- We want you to understand what was written and why, and we want to hear your questions and comments.
- Slides presented will be made available on the NIST web site (with permission).
- The Draft SP800-116 comment period is open until 12 May; please submit all comments in writing because remarks made here do not automatically become submitted comments.
- No decisions or commitments to changes will be made during the workshop.

PIV PACS Integration Workshop Agenda

- Welcome
- SP 800-116 Overview
- SP 800-116 Comment Presentations
- The FIT to Reality (Q&A Session)
- What should be Standardized (Q&A Session)

NIST National Institute of Standards and Technology

Draft SP 800-116 Overview

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

William I. MacGregor

National Institute of Standards and Technology

U.S. Department of Commerce

1 May 2008

The HSPD-12 Criteria

"Secure and reliable forms of identification" … means identification that

(a) is issued based on sound criteria for verifying an individual employee's identity;

(b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation;

(c) can be rapidly authenticated electronically; and

(d) is issued only by providers whose reliability has been established by an official accreditation process.

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.

PIV Data Objects

Just 10 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

NIST National Institute of Standards and Technology

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.

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.

NIST National Institute of Standards and Technology

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

SP 800-116 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.

SP 800-116 Status

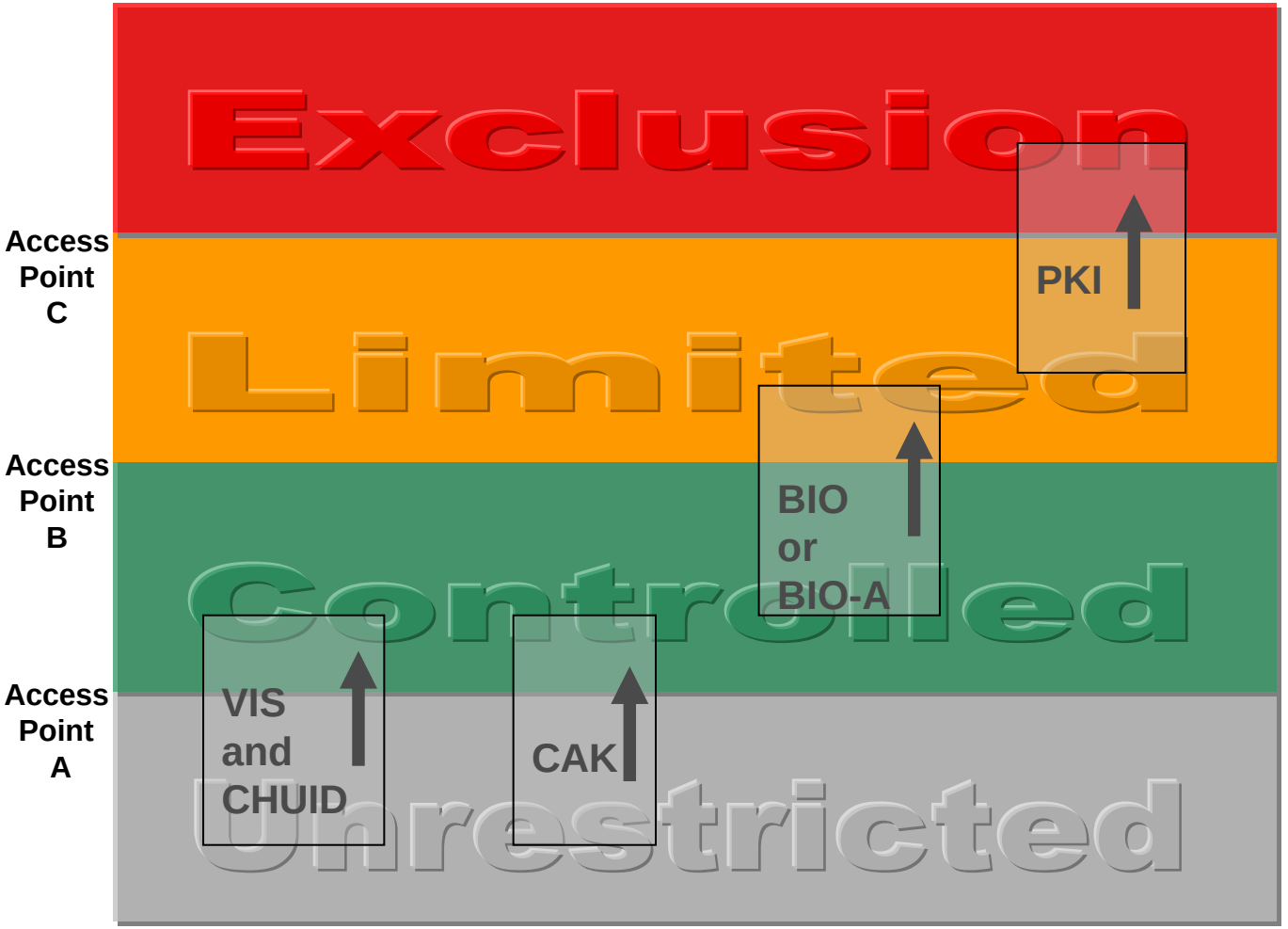
- SP800-116 will be a best practice guideline (not a normative part of FIPS 201-1).
- Draft SP800-116 public comment period closes **12 May 2008**.
- SP800-116 workshop at NIST on **1 May 2008** (*advance registration required*).
- Download Draft SP800-116, or register, at http://csrc.nist.gov/.

Publication Highlights

1. **Purpose & Scope**, ins and outs
2. **Threat Environment**, CHUID use
3. **PIV Vision**, interop goal, qualities, benefits
4. **PACS Authentication Assurance Levels**
5. **Selection of Authentication Methods**
6. **Credential & Path Validation**, trust model
7. **PACS Use Cases**, facility examples
8. **PIV Implementation Maturity Model**

PIV Authentication Mechanisms

Suggested use for nested Physical Access areas.



NIST National Institute of Standards and Technology

The “Poster” Rules

1. “VIS and CHUID” means both AMs.
2. AMs may be used lower but not higher.
3. Distinct AMs at different perimeters.
4. When “jumping” levels, use PKI+BIO(-A).
5. Within C or L, use any AM except VIS.
6. Within E, use CAK, BIO(-A), or PKI.
7. Choose based on local situation and policy.
8. At Orange or Yellow TC, use PKI+BIO(-A).

Thanks for listening!

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

SP800-116, FIPS 201 and related documents.

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

Basic Elements [of] Trust of PIV Cards.

PIV PACS Integration Workshop Agenda

- Welcome
- SP 800-116 Overview
- SP 800-116 Comment Presentations
- The FIT to Reality (Q&A Session)
- What should be Standardized (Q&A Session)

Observations and Presentations on SP 800-116

- Lars Suneborn (Hirsch Electronics)
- Roger Roehr (Smart Card Alliance) – a demo
- Tom Murphy (xTec)
- Cynthia Atkinson (Department of State)

PIV PACS Integration Workshop Agenda

- Welcome
- SP 800-116 Overview
- SP 800-116 Comment Presentations
- The FIT to Reality (Q&A Session)
- What should be Standardized (Q&A Session)

Draft SP 800-116 Overview

Does it FIT your Reality?

Magdalena C. Benitez

National Institute of Standards and Technology

U.S. Department of Commerce

1 May 2008

Does it FIT your Reality?

Is PKI considered more secure then BIO?

As defined in FIPS 201

NIST
National Institute of Standards and Technology

As defined in FIPS 201

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

Table 6-2. Authentication for Physical Access

NIST National Institute of Standards and Technology

6.2.3.1 Unattended Authentication Using PIV Biometric (BIO)

The following sequence shall be followed for unattended authentication of the PIV biometric:

1. The CHUID is read from the card.
2. The Expiration Date in the CHUID is checked to ensure the card has not expired.
3. The cardholder is prompted to submit a PIN, activating the PIV Card.
4. The PIV biometric is read from the card.

5. The signature on the biometric is verified to ensure the biometric is intact and comes from a trusted source. (Optional)

6. The cardholder is prompted to submit a live biometric sample.

7. If the biometric sample matches the biometric read from the card, the cardholder is authenticated to be the owner of the card.

8. The FASC-N in the CHUID is compared with the FASC-N in the Signed Attributes field of the external digital signature on the biometric.

9. One or more of the CHUID data elements (e.g., FASC-N, Agency Code, DUNS) are used as input to the authorization check to determine whether the cardholder should be granted access.

6.2.3.2 Attended Authentication of PIV Biometric (BIO-A)

The following sequence shall be followed for attended authentication of the PIV biometric:

1. The CHUID is read from the card.
2. The Expiration Date in the CHUID is checked to ensure that the card has not expired.
3. The cardholder is prompted to submit a PIN. The PIN entry is done in the view of an attendant.
4. The submitted PIN is used to activate the card. The PIV biometric is read from the card.
5. The signature on the biometric is verified to ensure the biometric is intact and comes from a trusted source. (Optional)
6. The cardholder is prompted to submit a live biometric sample. The biometric sample is submitted in the view of an attendant.
7. If the biometric sample matches the biometric read from the card, the cardholder is authenticated to be the owner of the card.
8. The FASC-N in the CHUID is compared with the FASC-N in the Signed Attributes field of the external digital signature on the biometric.
9. One or more of the CHUID data elements (e.g., FASC-N, Agency Code, DUNS) are used as input to the authorization check to determine whether the cardholder should be granted access.

This authentication mechanism is similar to the unattended biometric credential check; the only difference is that an attendant (e.g. security guard) supervises the use of the PIV Card and the submission of the PIN and the biometric by the cardholder.

6.2.4 Authentication Using PIV Asymmetric Cryptography (PKI)

The PIV Card carries a mandatory asymmetric authentication private key and corresponding certificate, as described in Section 4. The following steps shall be used to perform authentication using the PIV asymmetric authentication key:

1. The cardholder is prompted to submit a PIN.
2. The submitted PIN is used to activate the card.
3. The reader issues a challenge string to the card and requests an asymmetric operation in response.
4. The card responds to the previously issued challenge by signing it using the PIV authentication private key and attaching the associated certificate.
5. The response signature is verified and standards-compliant PKI path validation is conducted. The related digital certificate is checked to ensure that it is from a trusted source. The revocation status of the certificate is checked to ensure current validity.
6. The response is validated as the expected response to the issued challenge.
7. The Subject Distinguished Name (DN) and FASC-N from the authentication certificate are extracted and passed as input to the authorization function.

Some of the characteristics of the PKI-based authentication mechanism are as follows:

+ Requires the use of online certificate status checking infrastructure
+ Highly resistant to credential forgery
+ Strong resistance to use of unaltered card by non-owner since PIN is required to activate card
+ Applicable with contact-based card readers.

Does it FIT your Reality?

Should NIST consider other authentication mechanisms outside of PIV?

What are other mechanism that should be considered and included into SP 800-116?

Does it FIT your Reality?

Should we require distinct authentication mechanisms at different perimeters?*

Currently this is Rule #3 under Figure 7-1.

NIST National Institute of Standards and Technology

Does it FIT your Reality?

3. In a particular facility, the authentication mechanisms applied at enclosing perimeters of different impact levels should be distinct. For example, if PKI is applied to enter an Exclusion area, it should not be applied to enter the enclosing Limited or Controlled areas, and if BIO or BIO-A is applied to enter a Controlled area, it should not be applied to enter an enclosed Limited area

Does it FIT your Reality?

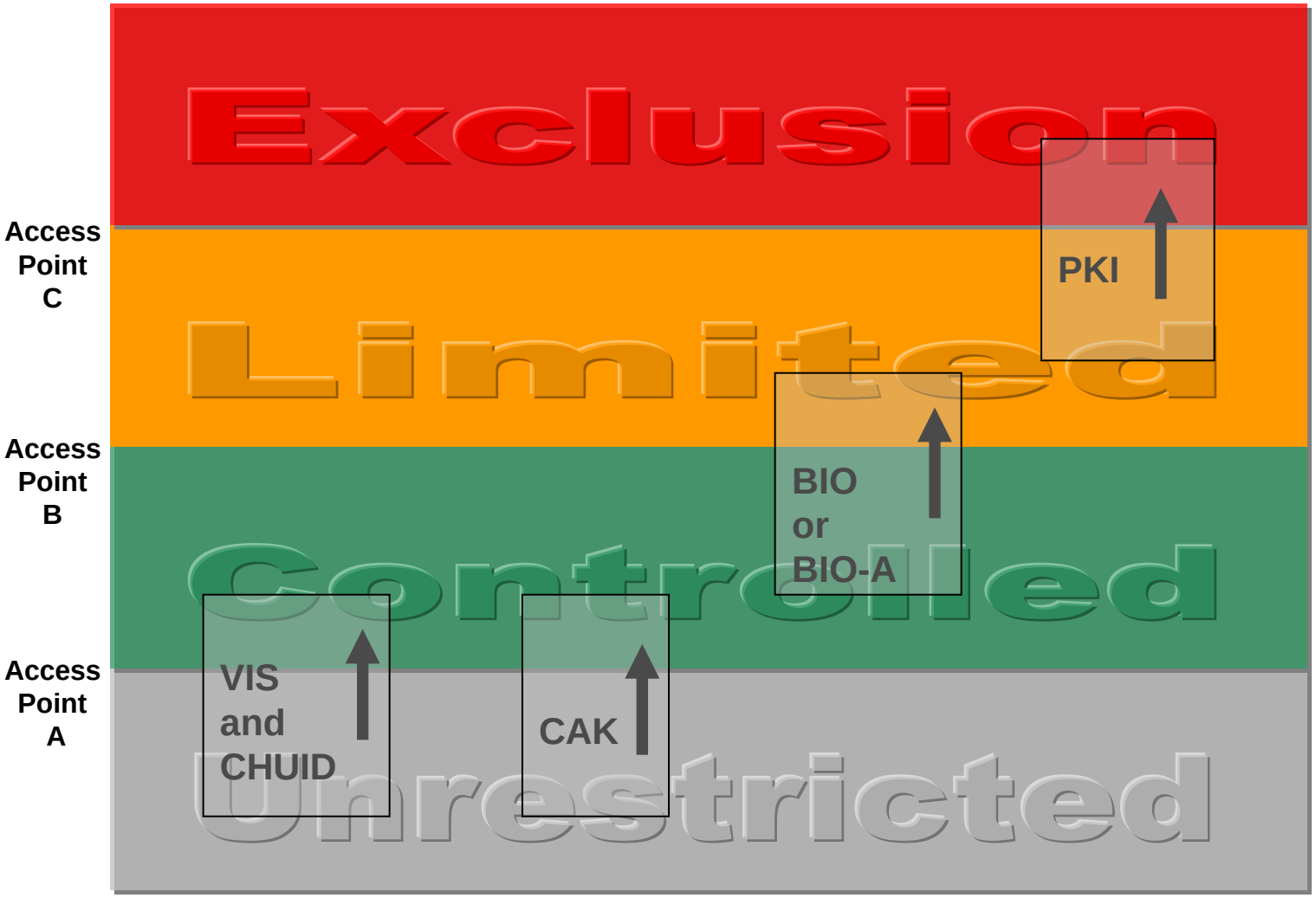


Figure 7.1

NIST National Institute of Standards and Technology

Does it FIT your Reality?

What are the various different implementations of VIS?

Is it a visual look of a picture?

Is facial comparison the industries definition of VIS?

NIST
National Institute of Standards and Technology

Does it FIT your Reality?

As defined in FIPS 201

Authentication Using PIV Visual Credentials (VIS)

Visual authentication of a PIV cardholder shall be used only to support access control to physical facilities and resources.

The PIV Card has several mandatory topographical features on the front and back that support visual identification and authentication, as follows:

Photograph
Name
Employee affiliation employment identifier
Expiration date
Agency card serial number (back of card)
Issuer identification (back of card).

The PIV Card may also bear the following optional components:

Agency name and/or department
Department or agency seal
PIV cardholder's physical characteristics
Applicant's Signature

NIST National Institute of Standards and Technology

Does it FIT your Reality?

As defined in FIPS 201

Authentication Using PIV Visual Credentials (VIS)

The series of steps that shall be applied in the visual authentication process are as follows:

The human guard at the access control entry point determines whether the PIV Card appears to be genuine and has not been altered in any way.

The guard compares the cardholder's facial features with the picture on the card to ensure that they match.

The guard checks the expiration date on the card to ensure that the card has not expired.

The guard compares the cardholder's physical characteristic descriptions to those of the cardholder. (Optional)

The guard collects the cardholder's signature and compares it with the signature on the card. (Optional)

One or more of the other data elements on the card (e.g., name, employee affiliation employment identifier, agency card serial number, issuer identification, agency name) are used to determine whether the cardholder should be granted access.

Some of the characteristics of the visual authentication mechanism are as follows:

Human inspection of card, which is not amenable for rapid or high volume access control

Resistant to use of unaltered card by non-owner of card

Low resistance to tampering and forgery

Applicable in environments with and without card readers.

NIST National Institute of Standards and Technology

Does it FIT your Reality?

Are there any vendors that have implemented CAK?

And if they have implemented CAK, do they need to upgrade to PKI?

Does it FIT your Reality?

General Comments

PACS is in a controlled environment and devices are monitored 24/7. The environment requires fast transaction times (higher throughput) and accurate results.

Your experience or comment?

NIST National Institute of Standards and Technology

Does it FIT your Reality?

Authorization and authentication are required to gain access. What is the new maintenance process?

Does it FIT your Reality?

Do we perform a strong authentication once, so that subsequently we can depend on the CHUID read?

Does it FIT your Reality?

Have we covered all the facility / applicable scenarios?

Does it FIT your Reality?

Open Comments

NIST
National Institute of Standards and Technology

PIV PACS Integration Workshop Agenda

- Welcome
- SP 800-116 Overview
- SP 800-116 Comment Presentations
- The FIT to Reality (Q&A Session)
- What should be Standardized (Q&A Session)

Draft SP 800-116 Overview

New Business?

Magdalena C. Benitez

National Institute of Standards and Technology

U.S. Department of Commerce

1 May 2008

What needs to be Standardized?

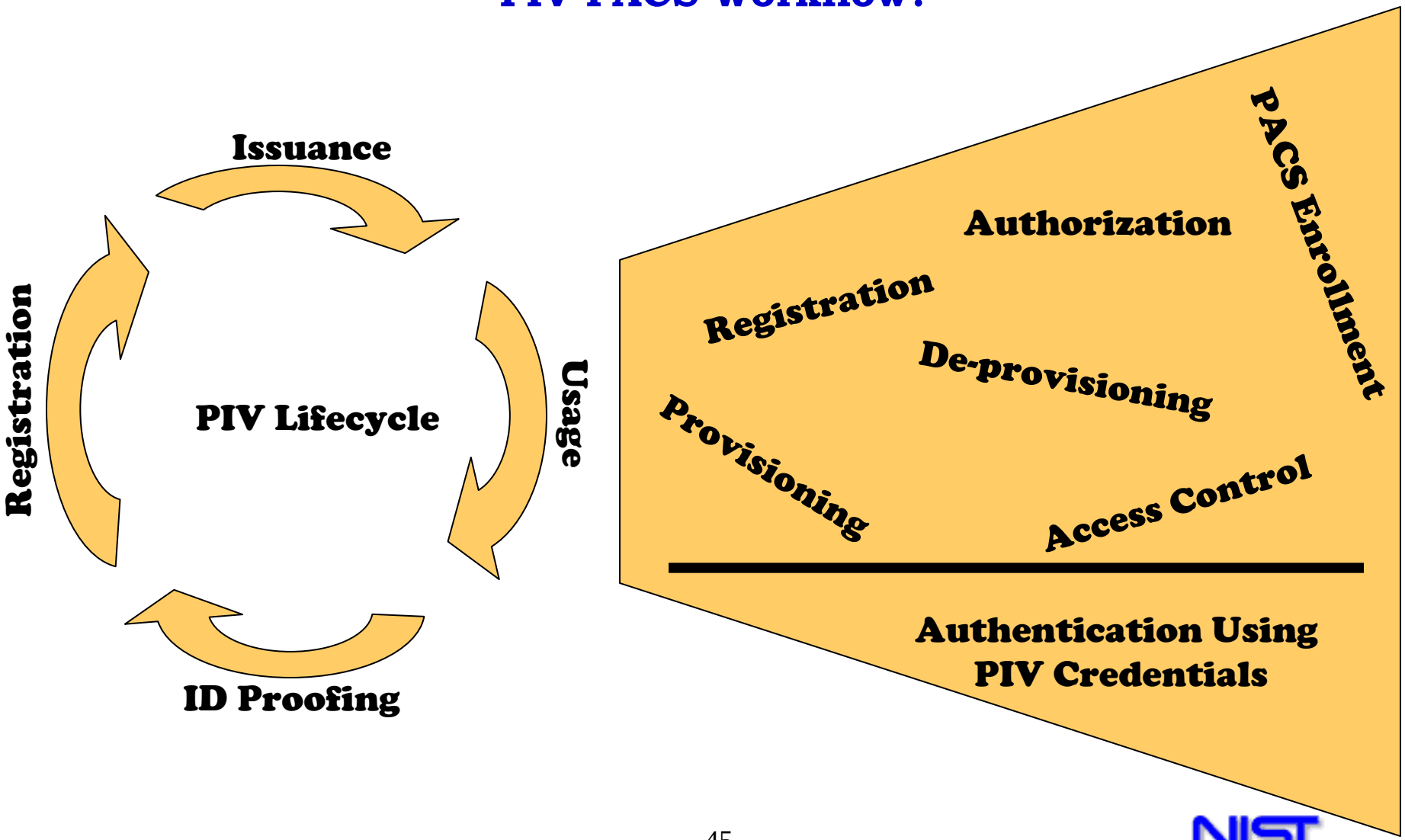
How does PACS registration and enrollment work in the new environment?

Should there be one workflow diagram?

NIST National Institute of Standards and Technology

What needs to be Standardized?

PIV PACS Workflow?



NIST
National Institute of
Standards and Technology

What needs to be Standardized?

SP 800-116 does not address time-based access control changes.

ex. The authentication mechanisms may be different depending on working hours.

NIST
National Institute of Standards and Technology

What needs to be Standardized?

Do we need additional guidance in use and storage of PIV Card data?

Should the PACS store everything it reads from the card?

What are the benefits and issues of this approach?

What needs to be Standardized?

Specifically what guidance should NIST provide related to 508 compliance?

http://www.section508.gov/index.cfm?FuseAction=content&ID=12#Purpose

What needs to be Standardized?

508-Subpart A -- General
§ 1194.1 Purpose.
The purpose of this part is to implement section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d). Section 508 requires that when Federal agencies develop, procure, maintain, or use electronic and information technology, Federal employees with disabilities have access to and use of information and data that is comparable to the access and use by Federal employees who are not individuals with disabilities, unless an undue burden would be imposed on the agency. Section 508 also requires that individuals with disabilities, who are members of the public seeking information or services from a Federal agency, have access to and use of information and data that is comparable to that provided to the public who are not individuals with disabilities, unless an undue burden would be imposed on the agency.

What needs to be Standardized?

508 -§ 1194.2 Application.

(a) Products covered by this part shall comply with all applicable provisions of this part. When developing, procuring, maintaining, or using electronic and information technology, each agency shall ensure that the products comply with the applicable provisions of this part, unless an undue burden would be imposed on the agency.

(1) When compliance with the provisions of this part imposes an undue burden, agencies shall provide individuals with disabilities with the information and data involved by an alternative means of access that allows the individual to use the information and data.

(2) When procuring a product, if an agency determines that compliance with any provision of this part imposes an undue burden, the documentation by the agency supporting the procurement shall explain why, and to what extent, compliance with each such provision creates an undue burden.

(b) When procuring a product, each agency shall procure products which comply with the provisions in this part when such products are available in the commercial marketplace or when such products are developed in response to a Government solicitation. Agencies cannot claim a product as a whole is not commercially available because no product in the marketplace meets all the standards. If products are commercially available that meet some but not all of the standards, the agency must procure the product that best meets the standards.

(c) Except as provided by §1194.3(b), this part applies to electronic and information technology developed, procured, maintained, or used by agencies directly or used by a contractor under a contract with an agency which requires the use of such product, or requires the use, to a significant extent, of such product in the performance of a service or the furnishing of a product.

What needs to be Standardized?

There are many card standards that one reader might use … PIV, TWIC, ACIS, CACI, CAC2, FRAC, Legacy prox, etc.

Can this be simplified?

What needs to be Standardized?

Should this document provide testable requirements / specifications?

NIST
National Institute of Standards and Technology

What needs to be Standardized?

Open Comments

NIST
National Institute of Standards and Technology

What needs to be Standardized?

Thank you