PIV Card Enhancements and Associated Authentication Mechanisms

Hildegard Ferraiolo
Computer Security Division
Information Technology Laboratory (ITL)

NIST
National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

Topics

- Change Management Principles/Terms
- PIV Card Topology
- On-Card Credentials and Associated Authentication Mechanism
- PIV PIN updates
- PKI Related

Change Management Principles/Terms

Deprecated: Deprecated features MAY continue to be used but SHOULD be phased out in future systems since the feature will likely be removed in the next revision of the Standard.

Removed: Removed features are features that previously have been deprecated (in prior revision) and are now being removed in the current revision. Removed features SHALL NOT be used.

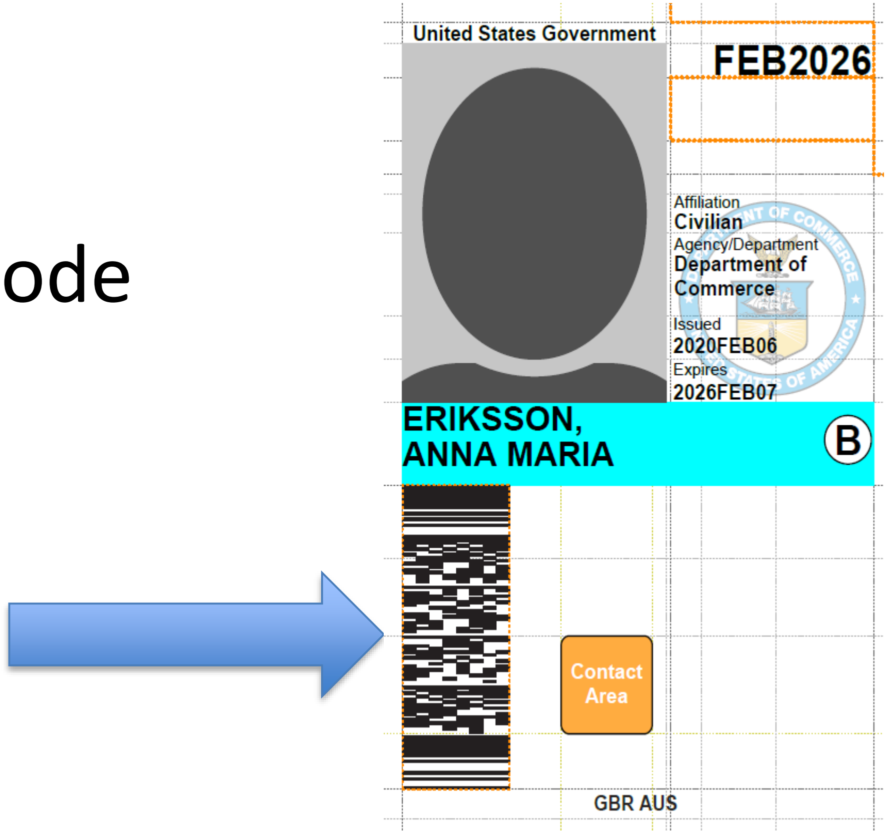
New Feature: New features are features that are added to the Standard. These features can be optional or mandatory.

Effective date: Features of this Standard that depend upon the release of new or revised NIST Special Publications, including features that are optional, deprecated, or removed, are effective upon final publication of the supporting Special Publications.

PIV Card Topology

Deprecated:

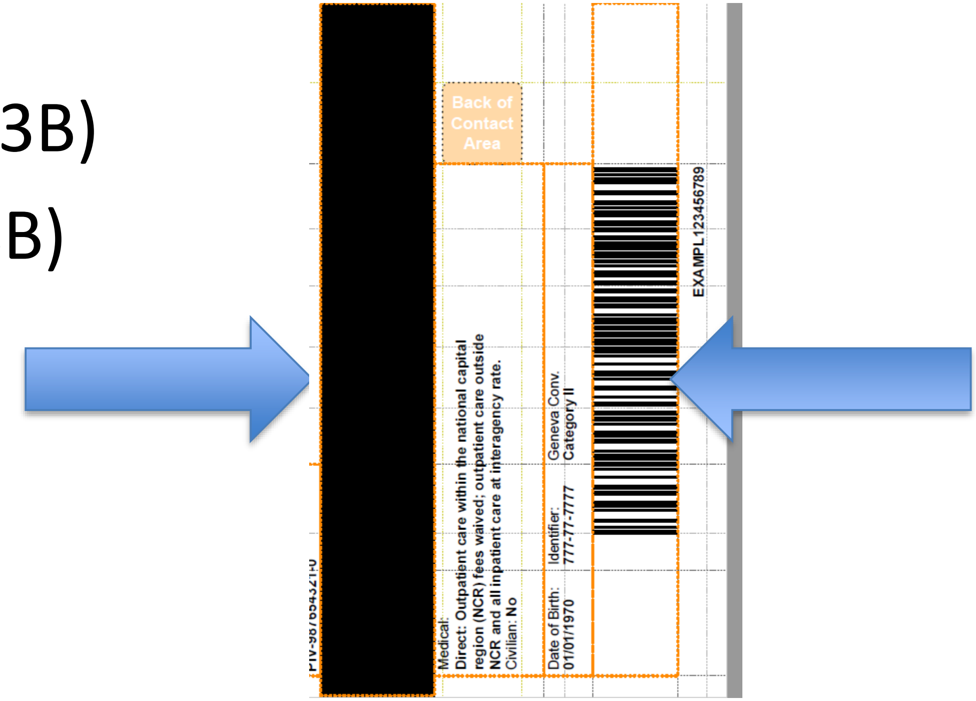
- 2-dimensional barcode (Zone 6 F)



PIV Card Topology

Deprecated:

- Magnetic Stripe (Zone 3B)
- 3-of-9 barcode (Zone 8B)


Back of Contact Area
Medical:
Direct: Outpatient care within the national capital region (NCR) fees waived; outpatient care outside NCR and all inpatient care at interagency rate.
Civilian: No
Date of Birth: 01/01/1970
Identifier: 777-77-7777
Geneva Conv. Category II
EXAMPL123456789
PIV-9876543210

National Institute of Standards and Technology
U.S. Department of Commerce

Rationale

- Barcode and magnetic stripes are old/legacy technology.
- deemed inappropriate and unsecure when used in facility access applications (as per SP 800-116R1 and per numerous PACS related IG, GAO reports –19-138, 11-751).
- End-of-life reached: in use only at a few Department and Agencies.

National Institute of Standards and Technology
U.S. Department of Commerce

On Card Credentials and Associated Authentication Mechanism

Removed:

- CHUID Authentication Mechanism
  - Rationale: It provides little to no identity assurance
  - CHUID data object itself remains on-card to enable access control privilege lookup via (FASC-N or Card UUID).

On Card Credentials and Associated Authentication Mechanism

Deprecated:

- VIS Authentication Mechanism (flash pass like)
  - Rationale: HSPD-12's directive specific to 'electronic authentication' only – not manual mechanisms

– Symmetric Card Authentication Key and associated SYM-CAK authentication mechanism

- Rationale:
  - Limited and decreased use,
  - Not suitable for interagency use-cases

On Card Credentials and Associated Authentication Mechanism

Update:

- Automated Facial Recognition
  - previously limited to issuance/re-issuance station (controlled environment) to reconnect/bind to enrollment record/PIV Card
  - Under draft FIPS 201-3 electronic facial image can now be used via the BIO/BIO-A authentication mechanism for LACS/PACS applications
    - Rationale: Technological advancements, increased accuracy
    - As a side: BIO/BIO-A is used by other on-card biometrics such as fingerprint, iris.

On Card Credentials and Associated Authentication Mechanism

New optional Feature:

- Secure messaging as an Authentication Mechanism (SM-AUTH)

  - Rationale:
    - Similar to PKI-CAK, provides an alternative to the CHUID authentication mechanism
    - Shorter time-to-market as secure messaging already implemented in card supporting OCC-AUTH
    - SP 800-73-4 to specify the details

National Institute of Standards and Technology
U.S. Department of Commerce

Expressing Authentication Mechanisms in a New Way

Express assurance level for physical and logical access in terms of PAL and AAL to align with SP800-116 and 800-63 respectively.

Physical Assurance Level (PAL)	Applicable PIV Authentication Mechanism
PAL 1	PKI-CAK, SYM-CAK
PAL 2	BIO
PAL 3	BIO-A, OCC-AUTH, PKI-AUTH

Required Authenticator Assurance Level	Local Workstation Environment	Remote/Network Environment
AAL 1	PKI-CAK	PKI-CAK
AAL 2	BIO	
AAL 3	BIO-A, OCC-AUTH	PKI-AUTH

PIV Card PIN

- The PIN SHALL be a minimum of six digits in length (existing requirement).
- The PIV Card SHALL compare the chosen PIN against a list of at least 10 commonly-chosen values (e.g., 000000, 123456) and
- require the choice of a different value if one of those is selected by the cardholder.

PKI related

Removed Section on the nomenclature "Legacy PKIs"

Reason: [COMMON] provides the requirements for department and agency CAs that might be issuing cross-certified PIV authentication certificates and card authentication certificates.

PKI related

Deprecated: The NACI indicator on the X.509 PIV Authentication Certificate

Motivation:

- Background investigative status is commonly maintained in each agency’s IDMS or personnel security system.