2005 Security Industry Association: FIPS 201 Topology

Standards on Steroids: FIPS 201

Teresa Schwarzhoff, NIST

June 2005

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

Topic: Standards, Standards, Standards

- U.S. Government - FIPS
  - Homeland Security Presidential Directive 12
  - Today's focus
- U.S. National Level - ANSI
  - InterNational Committee for Information Technology Standards (INCITS)
- International – ISO
  - ISO/IEC Joint Technical Committee 1 Sub Committee 17

Common basis

- Federal, national, and international standardization work based on:
  - NIST InterAgency Report, 6887, Government Smart Card Interoperability Specification v2.1
- The Federal government’s plans for identity credentials, tokens, and management is based on open, standard-based solutions.

HSPD-12 Presidential Policy Driver

Home Security Presidential Directive 12 (HSPD-12):

"*Policy for a Common Identification Standard for Federal Employees and Contractors*"

Dated: **August 27, 2004**

http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html

FIPS 201 PIV Card topology

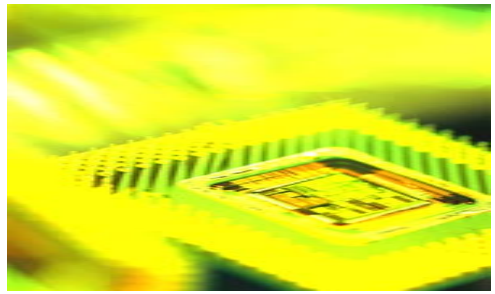
- So what does the PIV card look like?
  - General observations
  - Mandatory components
  - Optional components
  - Other features

General Observations

- Card design - balancing act
- Real estate limits
- Standard compliance
- Counterfeiting
- Interoperability – general look
- Balance security, privacy, utility, mandates

Mandatory Components: Front and Back

- Contact, contactless
- Front of PIV card
  - Color photograph
  - Name
  - Employee affiliation
  - Organizational affiliation
  - Card expiration date
- Back of card
  - Agency card serial number
  - Issuer identification



Optional Components - Front

- Agency seals
- “U.S. Government”
- Rank, grade, employee status
- Emergency responder notation
- Issue date
- 2 color coding methods for employee affiliation
- 2-dimensional portable data file bar code
- Hand written signature
- Agency specific text

Optional Components – Back

- Magnetic stripe
- Language:
  - ‘Return to’
  - Section 499 Title 18
  - Emergency responder
- Card holder physical characteristics
- Linear barcode
- Agency specific text

Other features

- One mandatory tamper resistance, anti-counterfeiting security measure required
  - additional at agency discretion
- Hole punching
  - allowed but not recommended
- Optional items
  - placed in generally the same area
- Font sizes
  - recommendations provided
- Use of areas reserved for embedded contactless module
  - two predominant locations

FIPS 201 REQUIREMENTS
PIV Electronically Stored Data

Mandatory:

- PIN (used to prove the identity of the cardholder to the card)
- Cardholder Unique Identifier (CHUID)
- PIV Authentication Data (asymmetric key pair and corresponding PKI certificate)
- Two biometric fingerprints

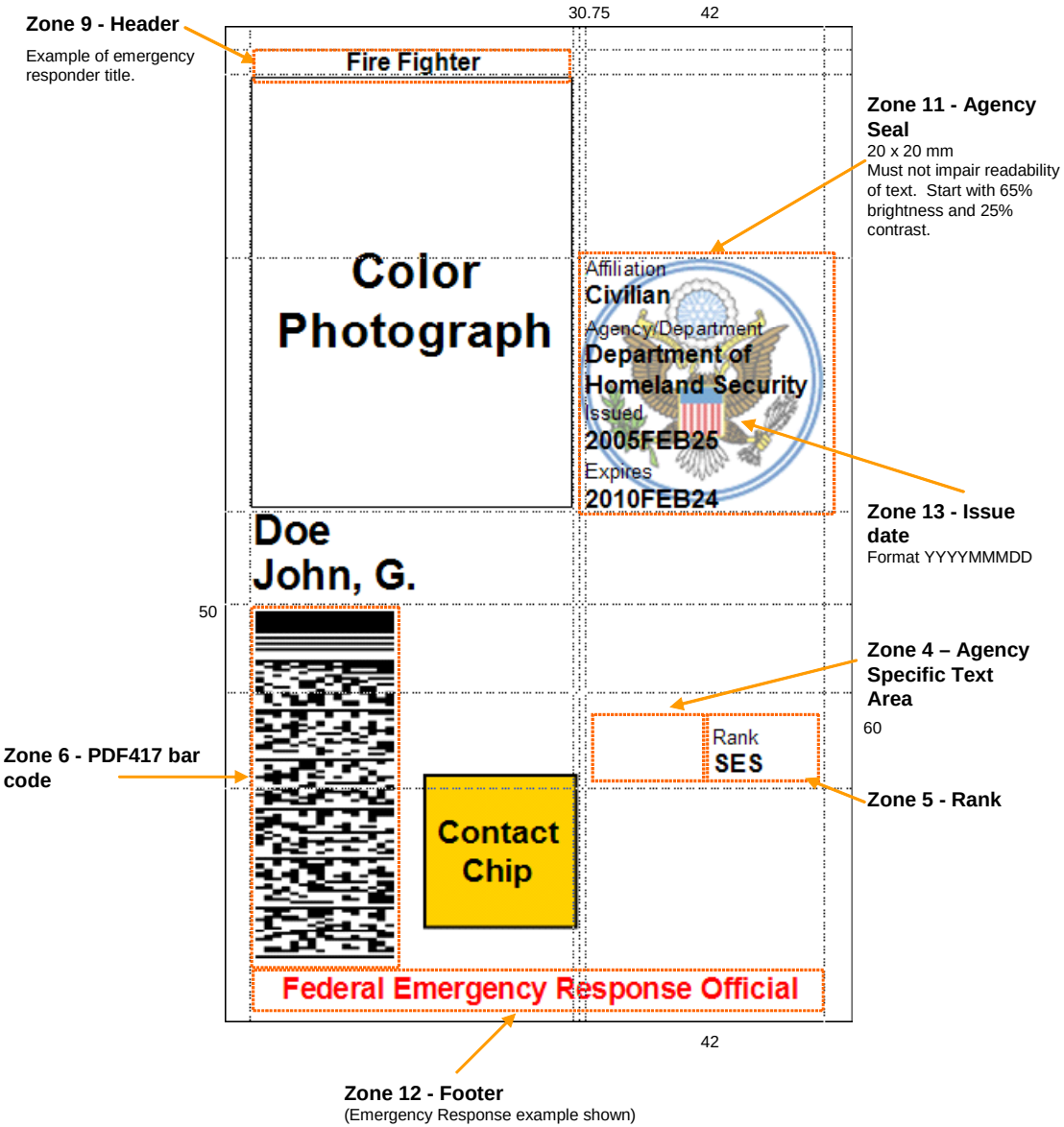
Optional:

- An asymmetric key pair and corresponding certificate for digital signatures
- An asymmetric key pair and corresponding certificate for key management
- Asymmetric or symmetric card authentication keys for supporting additional physical access applications
- Symmetric key(s) associated with the card management system

FIPS 201 REQUIREMENTS
Card Information Available for “Free Read”

- Federal Agency Smart Card Number (FASC-N)
  - Card-unique number
  - Agency-assigned number for card holder
  - Affiliation category (Employee, contractor, etc.)
  - Employer identification code
- Card Expiration Date
- Digital Signature
- Optional Information (i.e. Information not required by FIPS 201)
  - Data Universal Numbering System Number (DUNS)
  - Optional Global Unique Identifier (GUID)
  - Other optional information added at discretion of Issuing Agency

All measurements around the figure are in millimeters and are from the top-left corner.
All text is to be printed using the Arial font.
Unless otherwise specified, the recommended font size is 5pt normal weight for tags and 6pt bold for data.



Zone 9 - Header

Example of emergency responder title.

Zone 11 - Agency Seal

20 x 20 mm
Must not impair readability of text. Start with 65% brightness and 25% contrast.

Zone 13 - Issue date

Format YYYYMMMDD

Zone 4 – Agency Specific Text Area

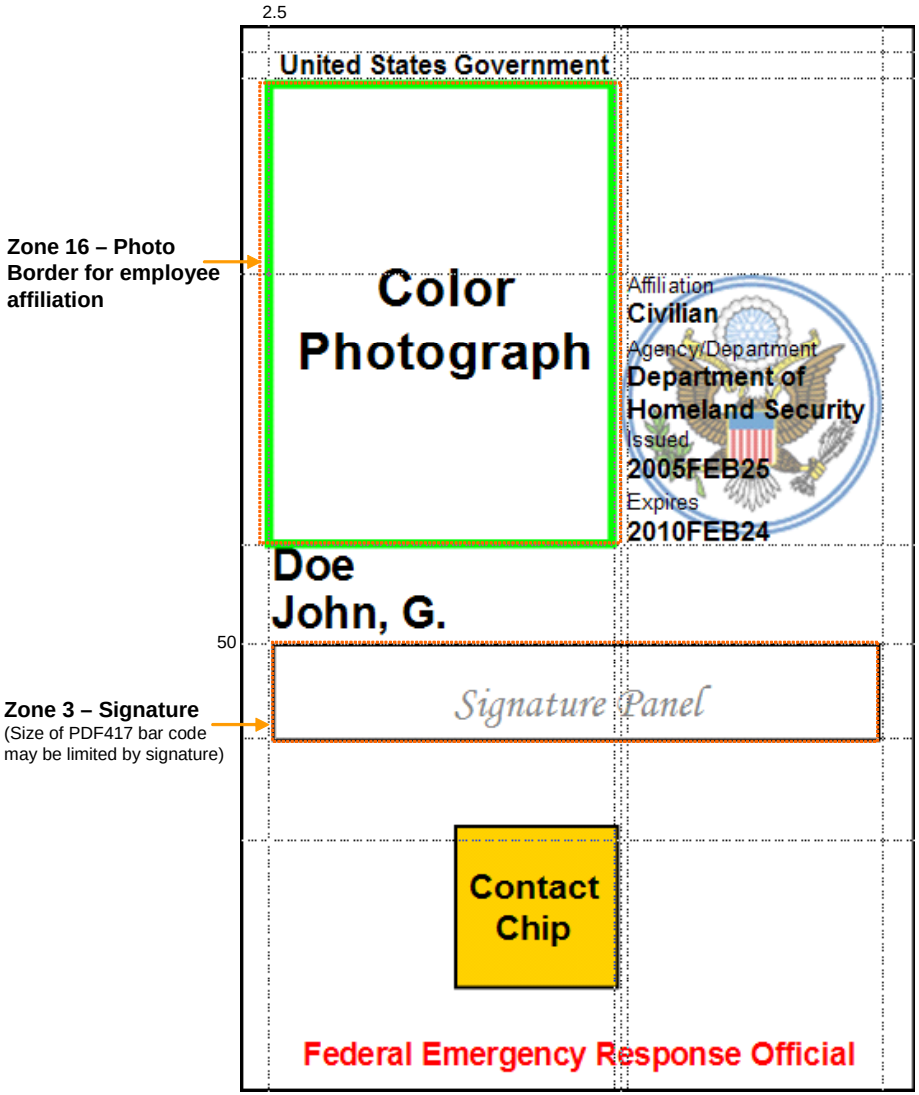
Zone 6 - PDF417 bar code

Zone 5 - Rank

Zone 12 - Footer

(Emergency Response example shown)

All measurements around the figure are in millimeters and are from the top-left corner.
All text is to be printed using the Arial font.
Unless otherwise specified, the recommended font size is 5pt normal weight for tags and 6pt bold for data.



Zone 16 – Photo Border for employee affiliation

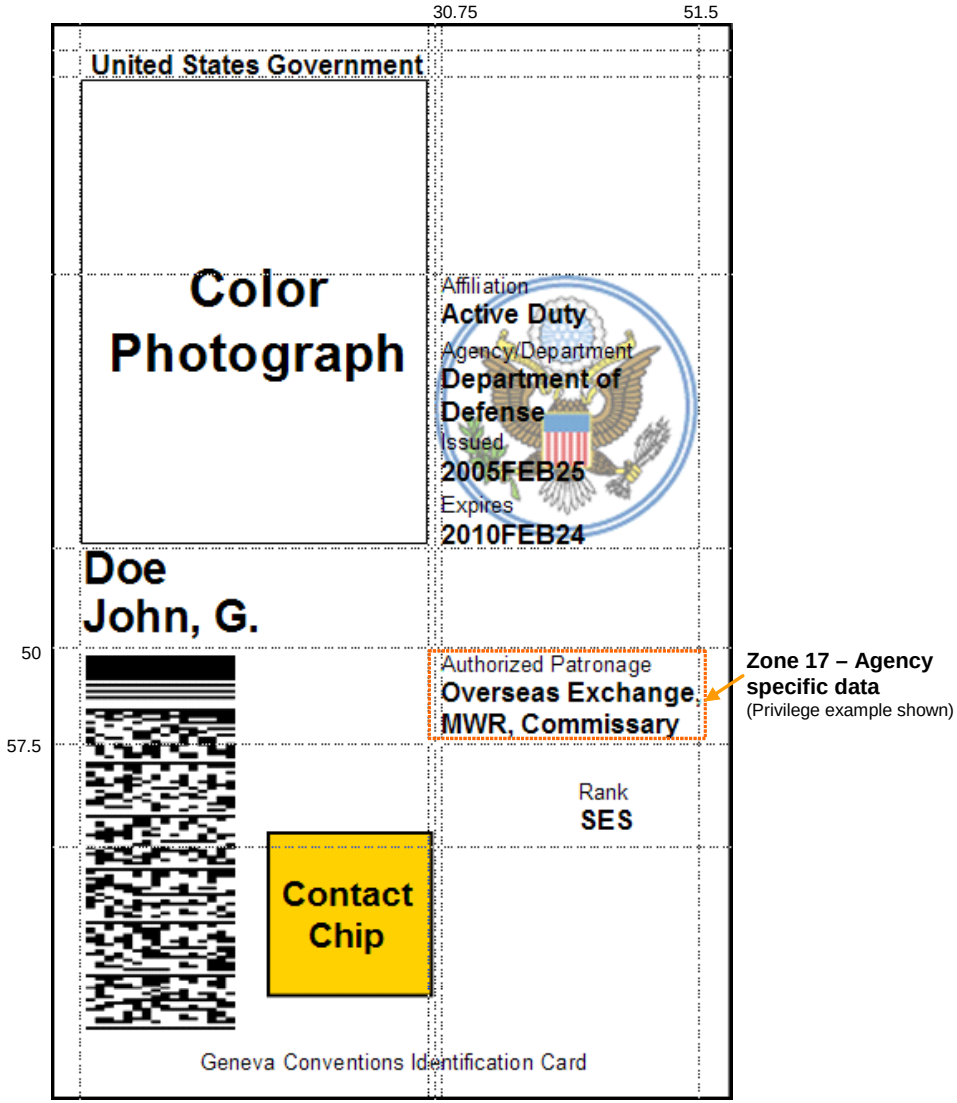
Zone 3 – Signature
(Size of PDF417 bar code may be limited by signature)

All measurements around the figure are in millimeters and are from the top-left corner.
All text is to be printed using the Arial font.
Unless otherwise specified, the recommended font size is 5pt normal weight for tags and 6pt bold for data.

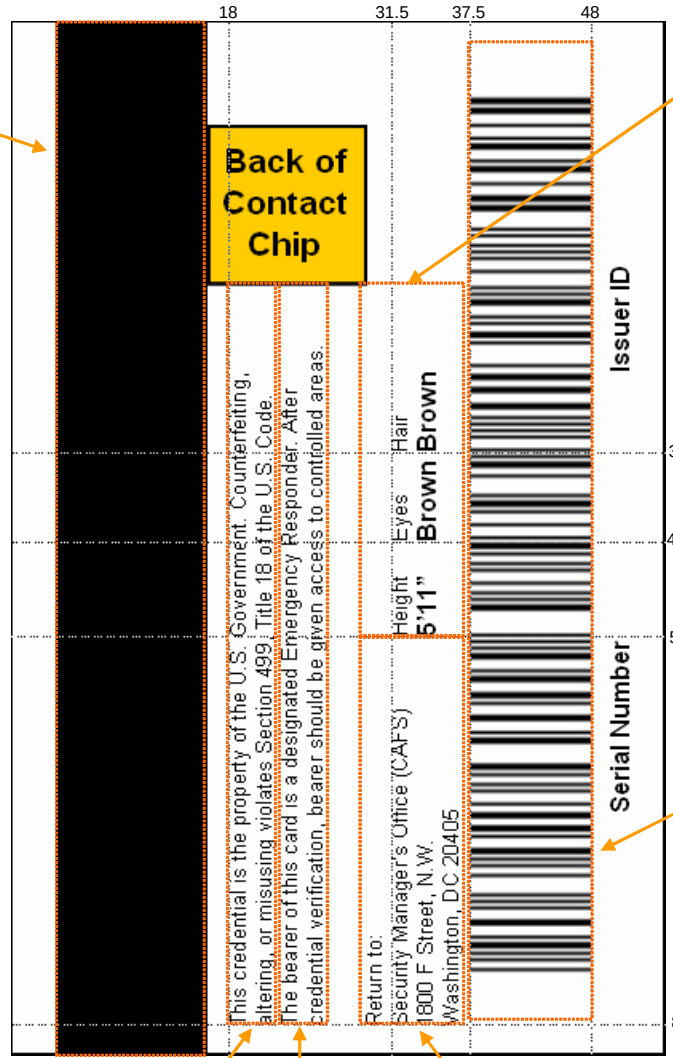
Zone 15 – Color-coding for employee affiliation

Zone 12 – Footer
The bottom of the card is preferred, but this area may be used if printing is not permitted at the bottom. (Emergency Response example shown.)

All measurements around the figure are in millimeters and are from the top-left corner.
All text is to be printed using the Arial font.
Unless otherwise specified, the recommended font size is 5pt normal weight for tags and 6pt bold for data.



All measurements are in millimeters and are from the top-left corner.
All text is to be printed using the Arial font.
Unless otherwise specified, the recommended font size is 5pt normal weight for tags and 6pt bold for data.



Zone 3 – Magnetic Stripe
ISO 7811-6 standard

Zone 5 – Physical characteristics
Limit use of abbreviations. Use English units.

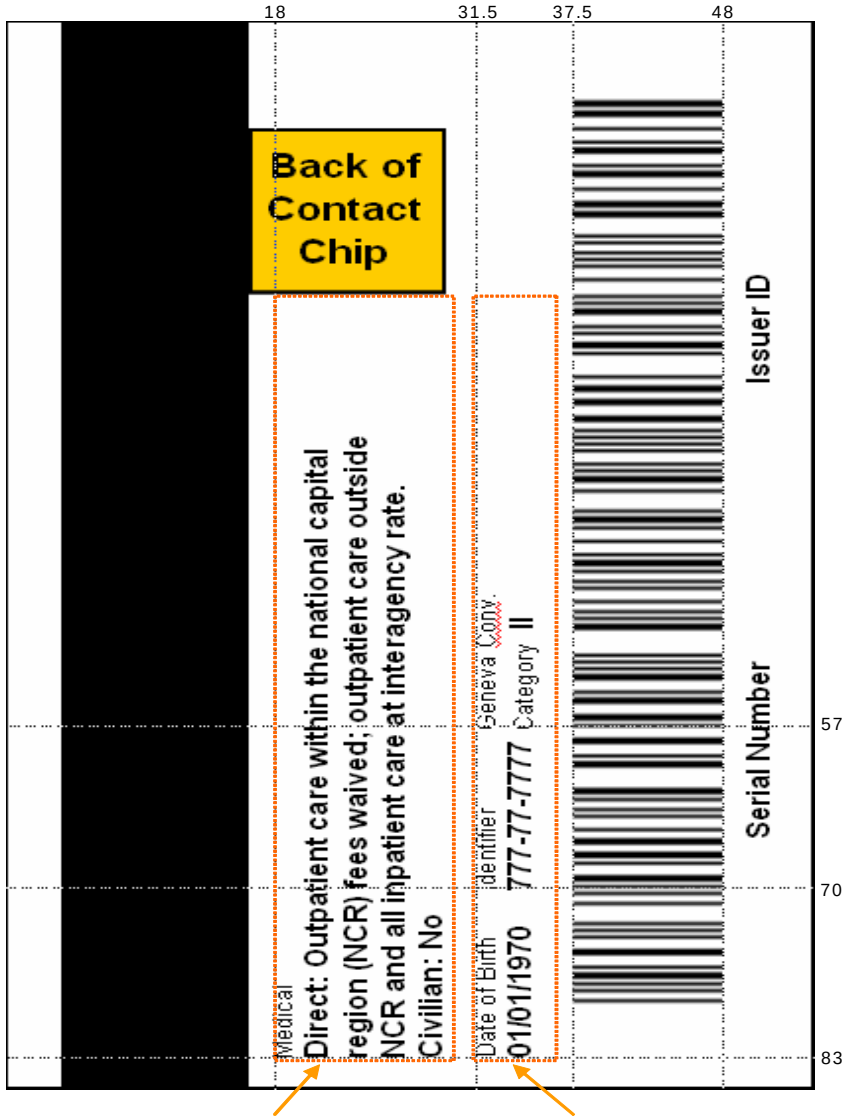
Zone 8 – 3 of 9 bar code
May use optional printing areas for ends of bar code. Must be positioned as shown for slot-reader compatibility.

Zone 7 – Section 499, Title 18 language
5pt Arial Normal

Zone 6 – Emergency Responder details
5pt Arial Normal

Zone 4 – Return Address
5pt Arial Normal

All measurements are in millimeters and are from the top-left corner.
All text is to be printed using the Arial font.
Unless otherwise specified, the recommended font size is 5pt normal weight for tags and 6pt bold for data.



Zone 9 – Agency specific text
Used instead of zones 6 & 7 (Medical example shown)

Zone 10 – Agency specific text
Used instead of zones 4 & 5 (DOB, ID, Geneva example shown)

Topology summary

- Minimal mandatory set (visual and electronic)
- General placement of optional visual elements
- Agency flexibility
- Security features
- Support passive technologies; migration to more secure identity verification

Challenges

- Existing investments
- Security and Privacy – two sides of the same coin
- Maintaining aggressive timelines
- Striking the right balance between Federal, national, international initiatives

The best standard is one in which everyone is equally unhappy….

Thank you.

Questions….

Contact Information:

Teresa Schwarzhoff

U.S. Department of Commerce, NIST

schwarzhoff@nist.gov

301.975.5727

Additional Slides

Further Guidance

- Supporting Publications
  - SP 800-73 – *Interfaces for Personal Identity Verification* (card interface commands and responses)
  - SP 800-76 – *Biometric Data Specification for Personal Identity Verification**
  - SP 800-78 – *Recommendation for Cryptographic Algorithms and Key Sizes*
  - SP 800-79 – *Issuing Organization Accreditation Guideline*
- NIST PIV Website (http://csrc.nist.gov/piv-project/)
  - Draft Documents
  - Frequently Asked Questions (FAQs)
  - Comments Received in Original Format
- Additional Guidance
  - OMB Guidance (Policy) {http://www.whitehouse.gov/omb/inforeg/hspd-12_guidance_040105.pdf}
  - FICC Guidance (Implementation – *Identity Management Handbook*) {http://www.cio.gov/ficc/documents/FedIdentityMgmtHandbook.pdf}
  - NIST Guidance on Certification and Accreditation

* Pending

Current Fiscal Year 2005 FIPS 201 Schedule

Scheduled Deliveries

Homeland Security Presidential Directive Signed	August 27, 2004
DoC Promulgation of FIPS 201	February 25, 2005
[GSA Federal Identity Management Handbook v0.2	March 8, 2005]
NIST SP 800-73, Interfaces for Personal Identity Verification	April 8, 2005
NIST SP 800-78, Crypto Algorithms for Personal Identity Verification	April 8, 2005
NIST SP 800-76, Biometric Data Specification for Personal Identity Verification	June 17, 2005*
Draft SP 800-79, PIV Card Issuing Organization Accreditation Guidelines	June 17, 2005
Publish FIPS 201 Reference Implementation	June 25, 2005
[FIPS 201 Implementation Plans Due to OMB	June 27, 2005]
NIST Workshop	June 27-28,2005
Draft SP 800-79 Comments Due	July 15, 2005
Final SP 800-79, PIV Card Issuing Organization Accreditation Guidelines	July 25, 2005

Other FY 2005 Activities

- FIPS 201/FIPS 140-2 Derived Test Requirements
- FIPS 201 Conformance Test Suite
- FIPS 201 Compliance Test Facility Accreditation Guideline
- FIPS 201 Test Implementation Guidelines
- FIPS 201 Pre-Issuance Specification
- [Standard Common Software Platform – Facilitation of FIPS 140-2 Validation]
- [FIPS 201 Component and System Developer's Handbooks]
- Training Documentation [Testing, Developer, Issuer, User]

* Dependent on Homeland Security Council Action

Topic: Standards, Standards, Standards

- U.S. Government - FIPS
  - Homeland Security Presidential Directive 12
- U.S. National Level - ANSI
  - InterNational Committee for Information Technology Standards (INCITS)
- International – ISO
  - ISO/IEC Joint Technical Committee 1 Sub Committee 17

Activity at the national level

- ANSI INCITS B10 Technical Committee, Identification Cards and Related Devices

  http://www.incits.org/tc_home/b10.htm
- B10 scope
  - Identification cards, ICC cards, optical, machine readable documents, mag stripe…
- B10.9 – Task Group on smart card interoperability
  - International: US initiated work, ISO SC 17 Work Group 4 Task Force 9
  - National: Approved to work on national smart card interoperability standard (Aug ’04)
    - Ballot based on GSC-ISv2.1 plus NIST reference implementation
    - Work impacted by HSPD-12

B10.9 Membership

- ActivCard
- Assa Abloy
- Axalto
- BearingPoint*
- Colorado Plastic Card
- Cubic
- DataCard
- US Dept of Commerce
- US Dept of Defense
  - DISA, Navy, DMDC
- Exponent, Inc
- Fall Hill Associates
- Gemplus
- GlobalPlatform*
- IdentityAlliance
- Litronic
- MagTek
- MasterCard International
- Mobile-Mind
- Oberthur
- SAFLINK
- SIA*
- SAIC
- Sharp
- Sony
- Texas Instruments
- Unisys
- Verifone

* Observer

B10.9 next steps

- Current status
  - New ballot underway for national standard
  - Challenge: avoid divergence, avoid duplication
  - September national meeting – determine way forward

- Get involved, get a voice at the table

  http://www.incits.org (membership information)

  http://www.incits.org/tc_home/b10.htm

Topic: Standards, Standards, Standards

- U.S. Government - FIPS
  - Homeland Security Presidential Directive 12
- U.S. National Level - ANSI
  - InterNational Committee for Information Technology Standards (INCITS)
- International – ISO
  - ISO/IEC Joint Technical Committee 1 Sub Committee 17

New proposed suite of international standards

- **ISO/IEC JTC 1 SC 17/WG 4 TF9** (yes, this a real title)
  - Sub Committee 17 Work Group 4 Task Force 9
  - ANSI secretariat
  - Chaired by NIST

  http://www.iso.org/jtc1/sc17/wg4/tf9

TF9 scope

Standardization of a set of structured programming interfaces for interactions between integrated circuit cards and external applications to include generic services for multi-sector use

ISO/IEC 24727 multi-part standard

- ***ISO/IEC WD 24727, Integrated circuit cards programming interfaces***
  - Builds upon ISO/IEC 7816
  - Focuses on services and interfaces
  - Card type neutral
  - Contact and contactless agnostic
  - Includes identification, authentication, and signature services

ISO/IEC WD 24727 summary and status

- Part 1 Project Editor: Gerald Smith, Sharp, smithg@sharpsec.com
  - Overarching framework, common 24727 terminology and approach
  - Status: 2nd Committee Draft ballot this summer
- Part 2 Project Editor: Scott Guthery, Mobile-Mind, sguthery@mobile-mind.com
  - Describes common card interface
  - Builds upon ISO/IEC 7816 series, “fine-tuning”
  - Status: Under CD ballot, closes August 19, 2005
- Part 3 Project Editor: Michael Neumann, Axalto, mneumann@axalto.com
  - New territory for smart card standards: API, middleware
  - Set of services: connection, discovery, retrieval, identity, cryptographic
  - Status: Anticipate CD candidate in Oct 2005

TF9 website: http://www.iso.org/jtc1/sc17/wg4/tf9