IDs & Keys in the 21st Century

William I. MacGregor

NIST PIV Coordinator

<william.macgregor@nist.gov>

National Institute of Standards and Technology

US Department of Commerce

Presented

Rome, Italy, 18 Nov 2008

Please Note

The presentation material, written and spoken, expresses the opinions of the presenter, and does not necessarily express an official position of the United States Government.

Increasing Threats Reported

One Sinowal Trojan + One Gang = Hundreds of Thousands of Compromised Accounts

*by **RSA FraudAction Research Lab** on 10/31/2008 12:00:00 AM*

Topics: E-Security | Online Fraud, Fraudsters

The RSA FraudAction Research Lab would like to share its startling findings based on its tracking and research of the Sinowal Trojan, also known as Torpig and Mebroot. Our findings based on the data we have collected on this Trojan over the course of almost three years – including information regarding its design and its infrastructure – indicate that this may be one of the most pervasive and advanced pieces of crimeware ever created by fraudsters.

We recently discovered that, dating back as early as February 2006, the Sinowal Trojan has compromised and stolen login credentials from approximately 300,000 online bank accounts as well as a similar number of credit and debit cards. Other information such as email, and FTP accounts from numerous websites, have also been compromised and stolen.

The Roadmap

1. Information Technology Drivers
2. Basic Concepts of IDs and Keys
3. Case Study: The US Federal PIV Card
4. Lessons Learned
5. Areas to Watch

Information Technology Drivers

Empowerment

Give the citizen, customer, member an active role.

Participation

Develop the broadest participation.

Anytime, Anywhere Access

Allow transactions at the convenience of the user.

Enterprise Efficiency

Reduce the cost of enterprise operations.

Service Integration

Improve services through useful connections.

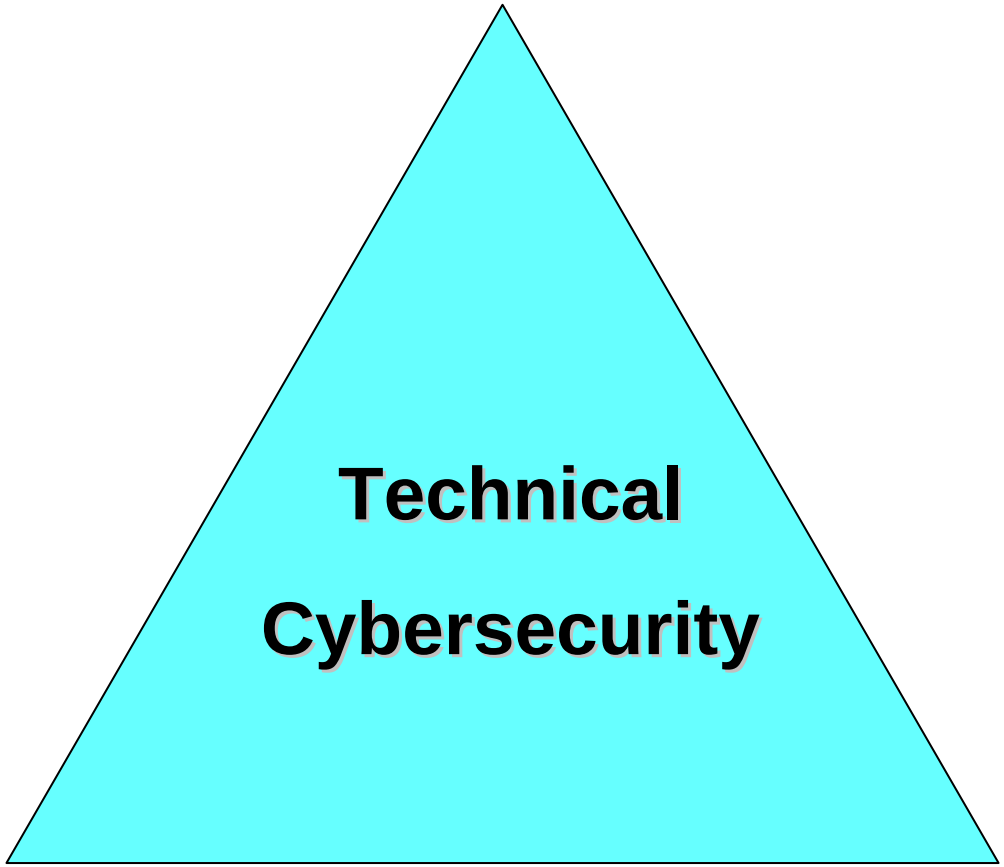
Identity & Access Control

IT systems will only provide the benefits we seek if they are trustworthy.

IT systems manage the identities of people to control access to information and transactions.

Do you trust your IT systems to give you access to your information, and allow others access only as you authorize?

Application Security



Identity Management

Network & Platform Security

Definitions

1. Digital Identity
2. Identifier
3. Authenticator
4. Authentication
5. Authentication Mechanism
6. Security Association

Step 1

A ***digital identity*** is:

(identifier, -- or identifiers
authenticators, -- e.g., password, token, biometric
attributes) -- e.g., authorizations

Example:

((name: Joe Smith, account: 1234567890123456),
pin: "7924",
expires: 31 Dec 2008)

Step 2

An ***identifier*** is a designator or name for a single person in a well-defined community of people.

NB: identifiers could also identify things and devices, but not in this talk!

Step 3

An ***authenticator*** is information that can be used to decide, with some level of confidence, if a ***presenting person*** is the person identified by this digital identity.

Step 4

Authentication is a process involving a presenting person, a ***verifier***, and a ***relying party***. The verifier that tells the relying party either

<identifier>	-- if success, or
“unknown”	-- if failure

Step 5

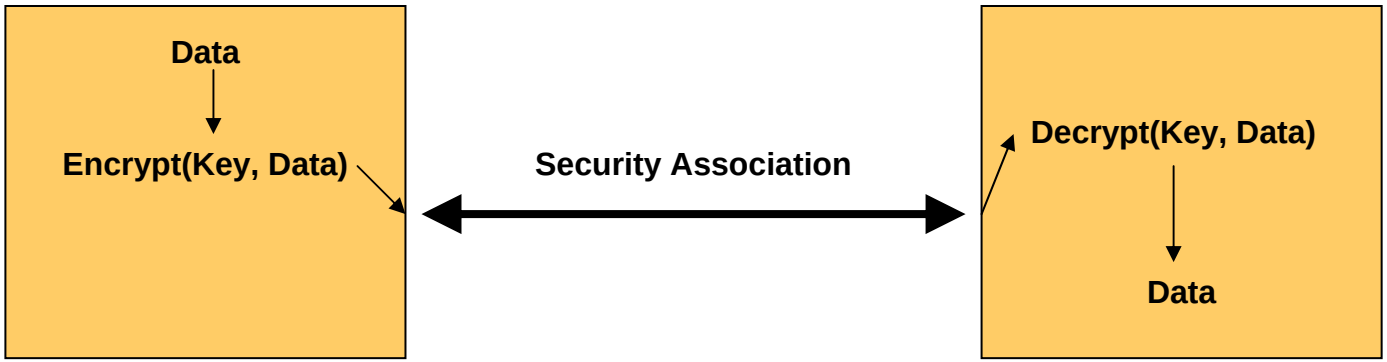
An ***authentication mechanism*** is a method of authenticating a person to an IT system, using the authenticators and identifiers in a digital identity.

Types of authentication mechanisms are

- Something you know -- passwords, PINs
- Something you have -- token, mobile, laptop
- Something you are -- biometrics

Step 6

A ***security association*** (SA) is a trust relationship between two IT system components. An SA is present if they share the same cryptographic key (or two related keys).



Bank ATM Example

Magstripe

ATM

Bank

Encrypted

Communications

PIN + Data Block

PIN Verifier → **Account Identifier**

Person

PIN Authenticator

Card Authenticator

NIST National Institute of Standards and Technology

It all fits together!

A **presenting person** gives proof of **authenticators** to a **verifier**…

…the verifier decides if authentication succeeds, and then provides the *identifier(s*) to a **relying party**…

…the relying party may be remote, and trusts the authentication because of a **security association** with the verifier.

Case Study:

The U.S. Federal Standard:

Personal Identity Verification (PIV)

Homeland Security Presidential Directive 12

27 Aug 2004

"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.

A New Federal Standard

HSPD-12 required a new US Federal standard:

Federal Information Processing Standard 201, "Personal Identity Verification"

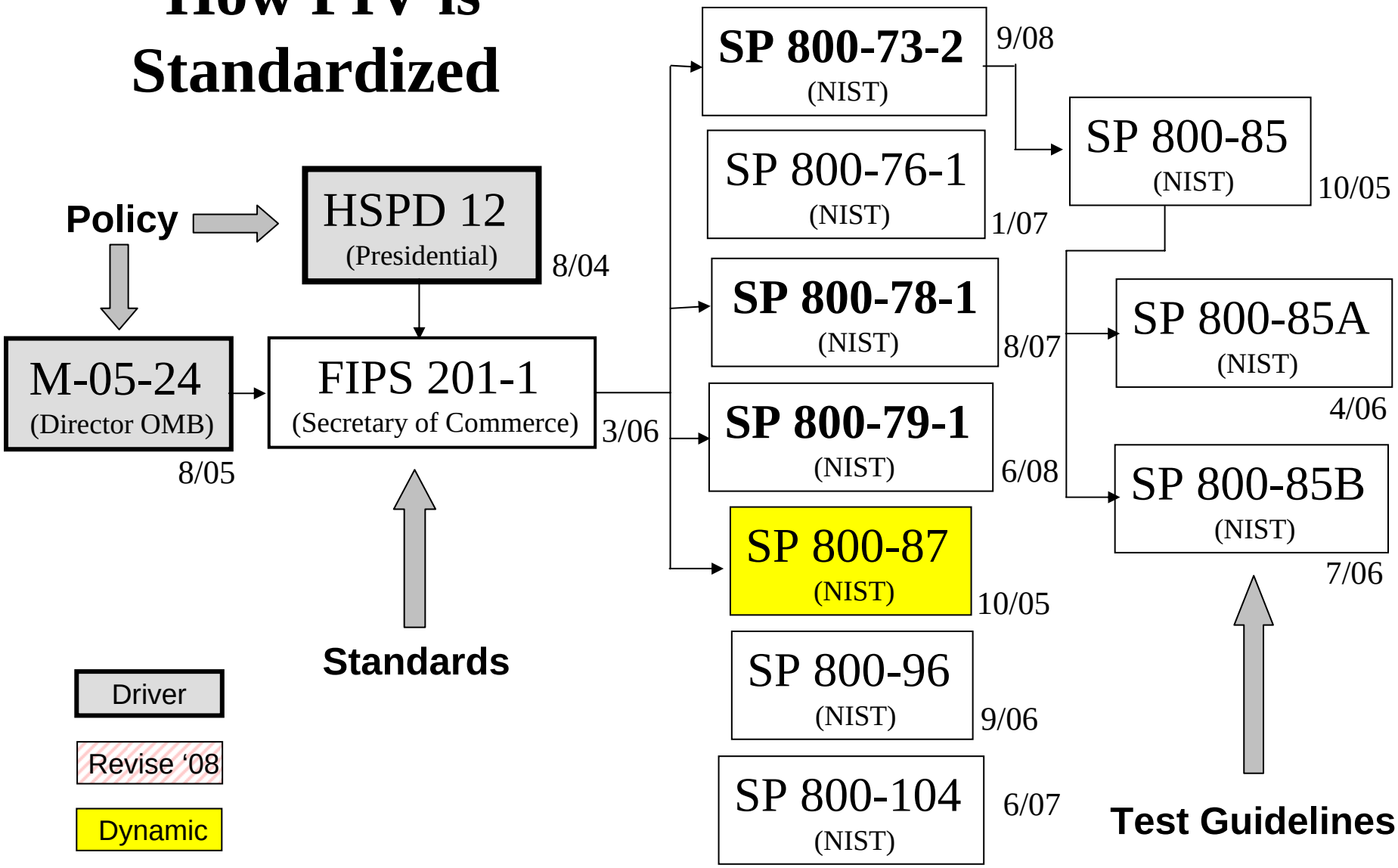
Referred to as FIPS 201 or PIV

Establishes

– Process requirements for credential lifecycle

– Technical specs for the multi-technology "PIV Card"

How PIV is Standardized



National Institute of Standards and Technology

HSPD-12 Status

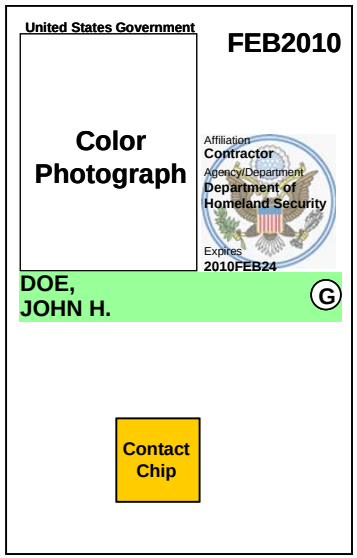
28 Oct 2008

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

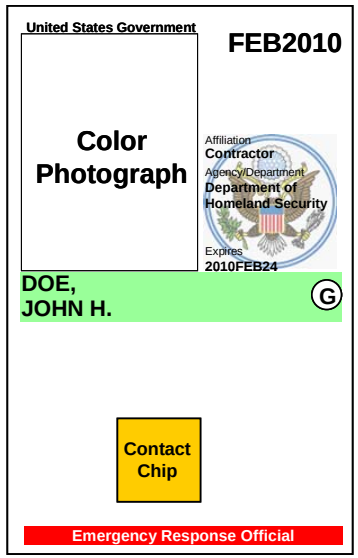
Employee & Contractor

Sample PIV Cards from SP800-104

Employees



Contractors



NIST National Institute of Standards and Technology

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.

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 Card 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

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

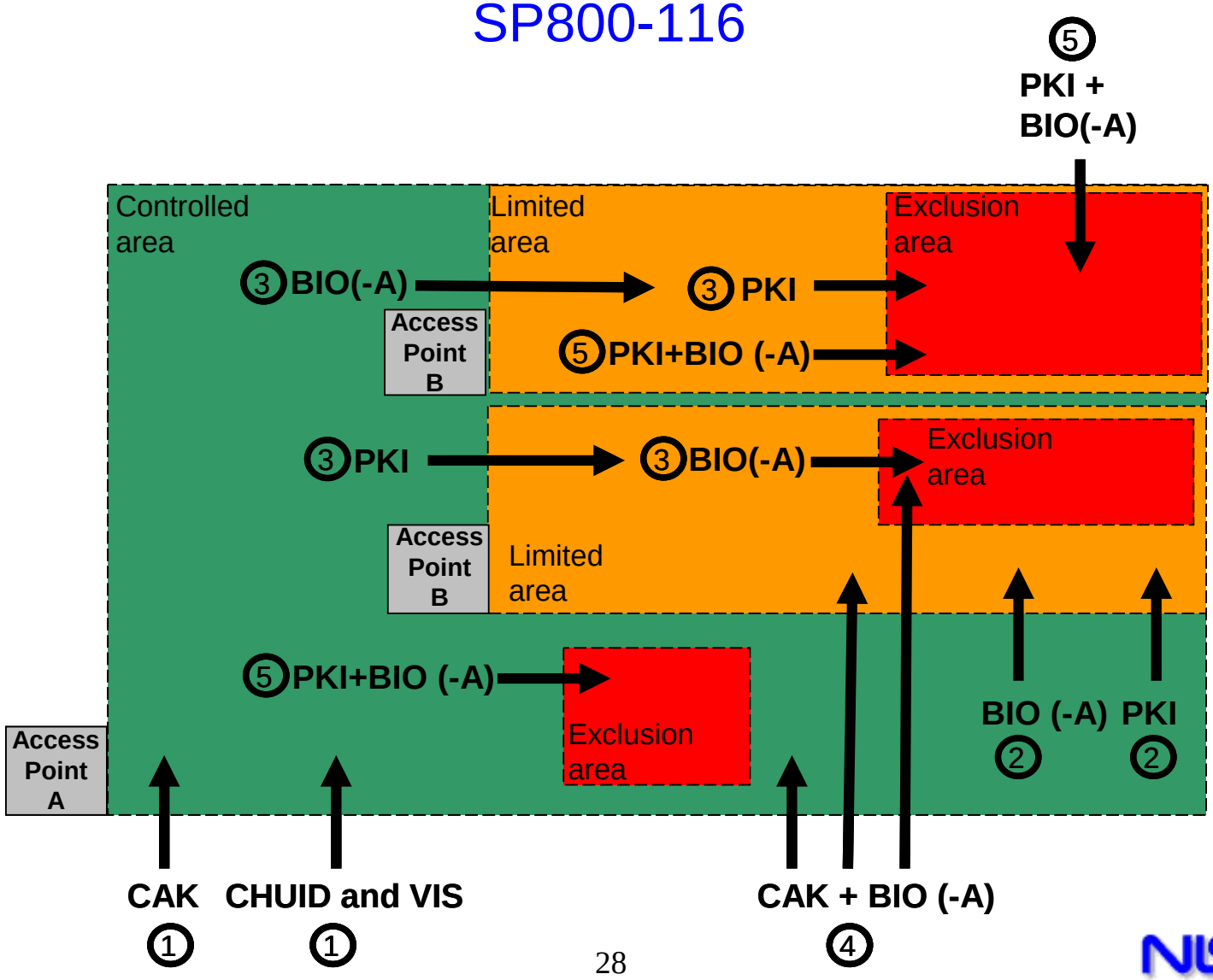
* CAK is defined in FIPS 201, but optional.

Characteristics

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

Physical Access Control Examples

SP800-116



NIST National Institute of Standards and Technology

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 should be done with *all* PIV authentication mechanisms.

Lessons Learned

- Practical, effective high assurance ID systems are within reach today.
- Multi-factor authentication (three or more mechanisms) is needed for high assurance.
- Good approaches use cryptography to protect all communication paths.
- Key management remains a challenging aspect of system architecture and design.

Areas to Watch

- What are the best ways to integrate new applications?
  - Middleware? CAPI/CNG? CardSpace?
- How can USG accept different ID types?
  - ISO/IEC 24727? Federation systems?
- How do we add new authentication mechanisms?
  - Iris, Match-On-Card fingerprint, voice?
- What will a Next Generation ID be like?
  - Smart card? Mobile phone? Server-based?

Thanks for listening!

http://csrc.nist.gov/

FIPS 201-1 Change Notice 1, and related documents, including SP 800-116

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

Basic Elements [of] Trust of PIV Cards.