

Leveraging HSPD-12 to Meet E-authentication Policy

**...and an update on
PIV Interoperability for Non-Federal Issuers**

December 2, 2008

Chris Loudon

IAB

Leveraging HSPD-12 to Meet E-Authentication Policy

□ Agenda:

- Quick E-Authentication Policy Review
- HSPD-12 Impact, Use
- Other areas to leverage
- Update on *PIV Interoperability for Non Federal Issuers*

E-Authentication Sectors for Government Interaction

Government to Citizen

Government to Business

E-Authentication (M-04-04)

Government to
Government

Internal Effectiveness
and Efficiency

HSPD-12

E-Authentication Policy Review

OMB M-04-04 E-Authentication Guidance for Federal Agencies

- ❑ *“Agencies should determine assurance levels using the following steps, (described in Section 2.3):*
 1. *Conduct a risk assessment of the e-government system.*
 2. *Map identified risks to the applicable assurance level.*
 3. *Select technology based on e-authentication technical guidance.*
 4. *Validate that the implemented system has achieved the required assurance level.*
 5. *Periodically reassess the system to determine technology refresh requirements. “*

E-Authentication Policy Review

❑ M-04-04 Risks

Potential Impact Categories for Authentication Errors	Assurance Level Impact Profiles			
	1	2	3	4
Inconvenience, distress or damage to standing or reputation	Low	Mod	Mod	High
Financial loss or agency liability	Low	Mod	Mod	High
Harm to agency programs or public interests	N/A	Low	Mod	High
Unauthorized release of sensitive information	N/A	Low	Mod	High
Personal Safety	N/A	N/A	Low	Mod High
Civil or criminal violations	N/A	Low	Mod	High

E-Authentication Policy Review

❑ SP 800-63 Technical Controls

Assurance Level

<i>Allowed Token Types</i>	1	2	3	4
Hard crypto token	√	√	√	√
One-time Password Device	√	√	√	
Soft crypto token	√	√	√	
Password & PINs	√	√		

❑ (one of 5 technical summary tables in section 9)

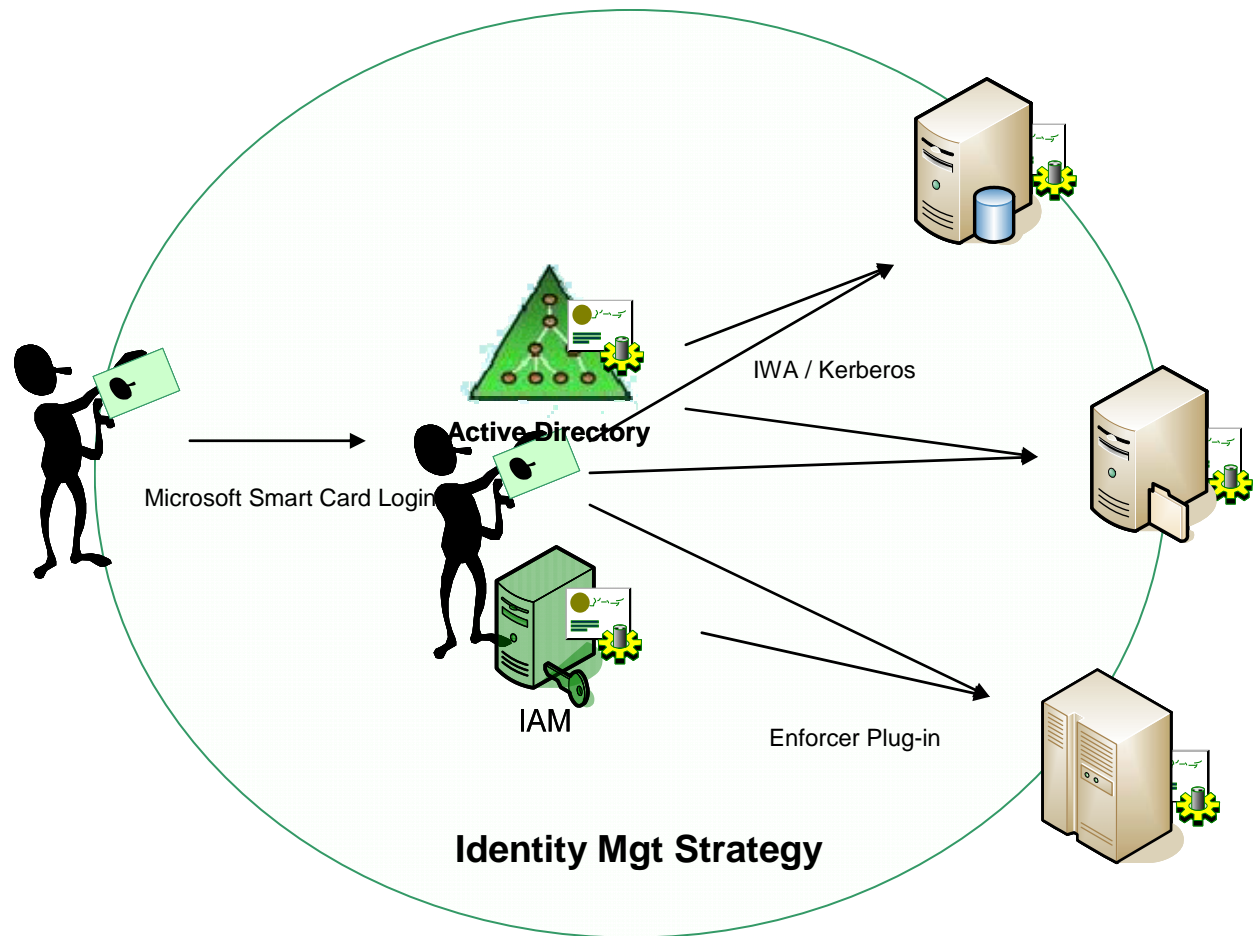
HSPD-12 Impact / Use

- ❑ PIV Cards meet Assurance Level 4
 - Suitable for systems with any risk

- PIV Enable internal applications to meet E-Authentication Policies

HSPD-12 Impact / Use

- ❑ PIV Enable every application?



Leveraging HSPD-12 to Meet E-Authentication Policy

□ Agenda:

- ✓ Quick E-Authentication Policy Review
- ✓ HSPD-12 Impact, Use
- Other areas to leverage
- Update on *PIV Interoperability for Non Federal Issuers*

OMB M-05-24

- ❑ *“Agencies must require the use of the identity credential for system access. Prioritize this requirement based on risk, using your authentication risk assessments required by previous OMB guidance and the categorization required by FIPS 199”*

OMB M-07-16

- *“While this framework identifies a number of steps to greatly reduce the risks related to a data breach of personally identifiable information, it is important to emphasize that a few simple and cost-effective steps may well deliver the greatest benefit, such as:*
 - *reducing the volume of collected and retained information to the minimum necessary;*
 - *limiting access to only those individuals who must have such access; and*
 - *using encryption, strong authentication procedures, and other security controls to make information unusable by unauthorized individuals. ”*

OMB M-06-16

- *“In addition to using the NIST checklist, I am recommending all departments and agencies take the following actions:*
 1. *Encrypt all data on mobile computers/devices which carry agency data unless the data is determined to be non-sensitive, in writing, by your Deputy Secretary or an individual he/she may designate in writing;*
 2. *Allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access; “*

And More...

- ❑ Digital Signature (GPEA)
- ❑ Encrypted Documents
- ❑ Signed / Encrypted email
- ❑ F/ERO designation, Emergency Response
- ❑ Records Management
- ❑ VPN / Remote Access
- ❑ Laptop Disk Encryption
- ❑ etc

Leveraging HSPD-12 to Meet E-Authentication Policy

□ Agenda:

- ✓ Quick E-Authentication Policy Review
- ✓ HSPD-12 Impact, Use
- ✓ Other areas to leverage
- Update on *PIV Interoperability for Non Federal Issuers*

Definitions

PIV Card

- an identity card that is fully conformant with federal PIV standards (i.e., Federal Information Processing Standard (FIPS) 201 and related documentation). Only cards issued by federal entities can be fully conformant. Federal standards ensure the PIV cards are interoperable with and trusted by all federal relying parties.

PIV Interoperable Card

- an identity card that meets the technical standards to work with PIV infrastructure elements such as card readers, and is issued in a manner that allows federal relying parties to trust the cards.

PIV Compatible Card

- an identity card that meets the technical specifications so that PIV infrastructure elements such as card readers are capable of working with the cards, but the card itself has not been issued in a manner that assures it is trustworthy by federal relying parties.

Definitions

	GSA APL 800-85b Tested	Medium Hardware Equivalent Auth Cert	PIV Auth Cert
PIV Compatible	✓		
PIV Interoperable	✓	✓	
PIV Card	✓	✓	✓

Tidbits: Trust

- ❑ PIV Interoperable Cards must include an Authentication Credential that chains to Federal Bridge Medium Hardware Assurance via cross-certification.
 - Issuance of a MEDIUM HARDWARE PKI credential requires the same level of identity proofing designated for E-Authentication Assurance Level 4
 - <http://www.cio.gov/fpkipa/>

Next Steps

- ❑ PAIIWG addressing identifier namespace (Next Gen FASC-N)
- ❑ Incorporating Government Comments now
- ❑ New version released to public before the end of the calendar year

➤ Questions