Interagency Advisory Board

Meeting Agenda, February 2, 2009

1. **Opening Remarks** (*Tim Baldridge, NASA*)
2. **Mini Tutorial on NIST SP 800-116 AND PIV use in Physical Access Control Systems** *(Bill MacGregor, NIST)*
3. **Impact of Agreement Among Four PKI Bridges** *(Tim Pinegar, Protiviti Government Services (PGS) representing GSA/OGPGSA)*
4. **Microsoft's Roadmap for PIV Products: The Impact that will have on PIV Use and Interoperability** *(Vernon Lee, Microsoft)*
5. **Adobe's Roadmap for PIV Products: The impact that will have on PIV Use and Interoperability** *(John Harris, Adobe)*
6. **PAIIWG Update** (*Tim Baldridge, NASA*)
7. **Closing Remarks** (*Tim Baldridge, NASA)*

Microsoft Windows Platform and HSPD-12 PIV Smart Cards Interoperability

BUILD ON

Vernon Lee, Senior Architect

Microsoft | Services, US Federal Civilian

Microsoft | Services

Microsoft Windows Platform and HSPD-12 PIV Smart Cards Interoperability

Agenda

- Microsoft Windows smart card requirements for authentication
- Microsoft Windows smart card capabilities matrix
- Infrastructure challenges faced in interoperability scenarios
  - COOP Scenario
  - Agency Detailee Scenario
- Microsoft PIV solutions for HSPD-12
  - ILM PIVdb Identity Management for USAccess
  - ILM PIVdb Detailee Provisioning Conceptual Architecture
- Timeline for ILM PIVdb solutions and engagement model
- Q&A

Microsoft Windows Platform and HSPD-12 PIV Smart Cards Interoperability

Smart Card Authentication Requirements – Windows XP

- Microsoft Windows XP up to Service Pack 3
  - Infrastructure Requirements
    - Domain Controllers must have authentication certificates
    - Root certificate for Issuing CA(s) must be trusted
    - NTAuth inclusion of Issuing CA(s) – required for higher assurance scenarios related to auto enrollment and renewal; mitigation of rogue CA issuing duplicate credentials that are trusted for authentication
    - CRL or OCSP checking of certificate validity
    - Account for user exists in domain/forest
  - Certificate Requirements
    - CRL Distribution Point (CDP) must be populated and available
    - Key Usage = Digital Signature
    - Enhanced Key Usage = Smart Card Logon (1.3.6.1.4.1.311.20.2.2)
    - Subject Alternative Name = UPN
      - UPN = user1@example.com
    - Subject field mandatory inclusion, attribute population optional
    - Private key type = Key Exchange (AT_KEYEXCHANGE)
  - Limitations
    - One authentication certificate enumerated with an AT_KEYEXCHANGE field
    - No native OCSP support for validity checking, third party CAPI plug-in enables OCSP
    - Limited functionality related to SHA2, no ECC or other SuiteB algorithms supported

Microsoft Windows Platform and HSPD-12 PIV Smart Cards Interoperability

Smart Card Authentication Requirements – Windows Vista and Windows 7

- Microsoft Windows Vista and Windows 7
  - Infrastructure Requirements
    - Domain Controllers must have authentication certificates
    - Root certificate for Issuing CA(s) must be trusted
    - NTAuth inclusion of Issuing CA(s) – required for higher assurance scenarios related to auto enrollment and renewal; mitigation of rogue CA issuing duplicate credentials that are trusted for authentication
    - CRL or OCSP checking of certificate validity
    - Account for user exists in domain/forest
  - Certificate Requirement changes…
    - UPN in SAN supported but NOT required for authentication
    - Smart Card Logon (1.3.6.1.4.1.311.20.2.2) EKU is NOT required for SC logon, but if an EKU is present then the aforementioned must be included
    - Any certificate with Digital Signature key usage can be enabled for SC logon
    - CDP field no longer needs to be populated
    - Private Key type does not require AT_KEYEXCHANGE field
    - Not enabled by default, because some of the previous settings are considered best practices. Enabled by Group Policy or registry key changes
  - New Capabilities and Scenarios
    - X.509 Root Hints
      - Smart Card logon with a single user certificate to multiple accounts (enables user and admin account scenario)
      - Smart Card logon of multiple users to a single AD account
      - Smart Card logon across forests
    - OCSP support in PKINIT
    - Revocation Checking granular settings to disable CRL checking
    - Enhanced Terminal server SC logon support, multiple sessions, secure channel for PIN entry and cross domain logon

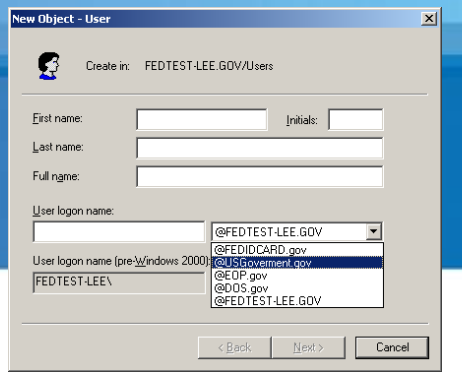
Microsoft Windows Platform and HSPD-12 PIV Smart Cards Interoperability

Smart Card Capabilities Matrix

	Windows XP SP2	Windows XP SP3	Windows Vista	Windows 7	Windows Server 2003	Windows Server 2008	Windows Server 2008 R2
SC Logon **without** UPN	NO	NO	**YES**	**YES**	NO	**YES**	**YES**
NTAuth published CA(s)	YES	YES	**YES**	**YES**	YES	**YES**	**YES**
AD account object	YES	YES	**YES**	**YES**	YES	**YES**	**YES**
Trusted root CA(s)	YES	YES	**YES**	**YES**	YES	**YES**	**YES**
x.509 Root hints	NO	NO	**YES**	**YES**	NO	**YES**	**YES**
OCSP PKINIT and client (native)	NO*	NO*	**YES**	**YES**	NO*	**YES**	**YES**
1 user to multiple accounts	NO	NO	**YES**	**YES**	NO	**YES**	**YES**
PIV native support	NO*	NO*	**NO***	**YES**	NO*	**NO***	**YES**
ECC and SuiteB	NO	NO	**YES**	**YES**	NO	**YES**	**YES**
SHA2 support	NO	LIMITED	**YES**	**YES**	LIMITED	**YES**	**YES**

* Requires 3rd party client or middleware

Microsoft Windows Platform and HSPD-12 PIV Smart Cards Interoperability



Interoperability Challenges

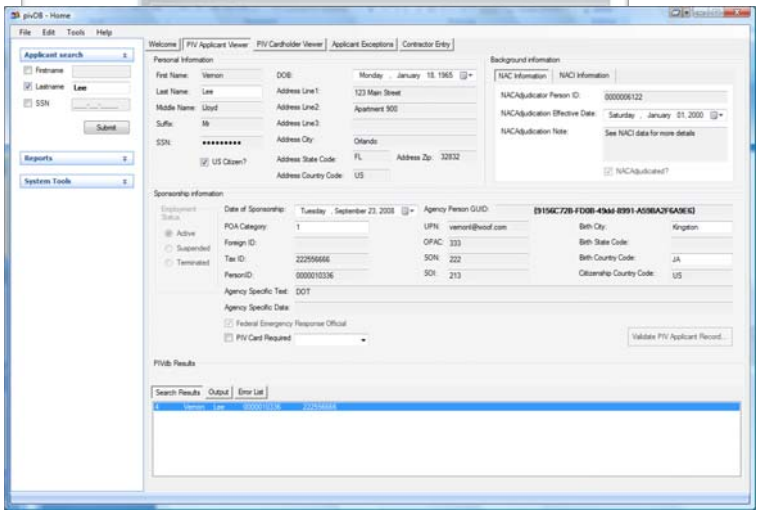
- In an Interop Scenario for COOP or in the case of a Detailee, UPN is a manageable issue. Why? There is no account for the user, therefore, one would need to be created, and any UPN could be assigned to the account, as long as the UPN suffix is enabled in AD.
  - For FEDIDCARD.GOV we would just have to provide guidance for the department/agency to add the suffix to their AD schema.
  - In the case that an agency is NOT using USAccess and have deployed their own PIV Card Issuance system, i.e. DOS, NASA, DOT/FAA, EOP and others. The UPNs will vary and be rooted in the agency suffix, i.e. EOP.GOV. Therefore, for each of these the agency UPN suffices would need to be added to their AD schema.
- In addition to the UPN suffix, accounts would need to be created and the UPN field changed to match the UPN in the PIVAuth certificate for the specific user.
- Detailees could have their accounts de-provisioned at the end of the loan period using the same account provisioning tools.
- COOP presents some additional challenges, related to account creation, i.e.
  - What forest domain will the account be created in?
  - What department/agency owns the forest/domain and cares for it?
  - Does the forest/domain and account have a TTL requirement beyond the period of the COOP instance?

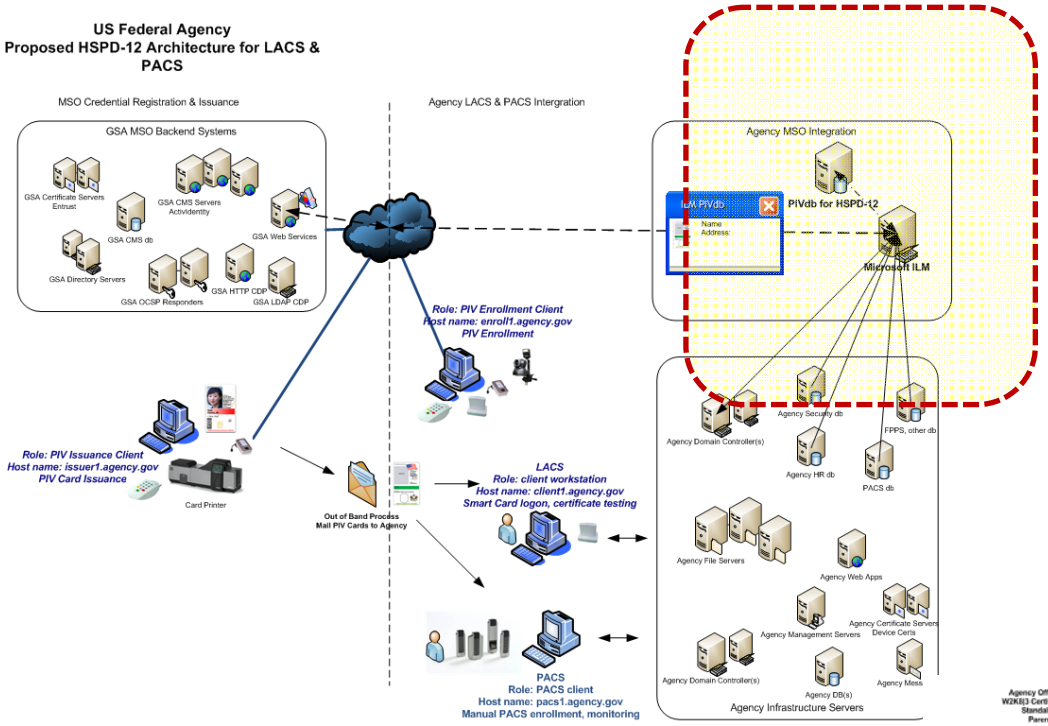
Microsoft Windows Platform and HSPD-12 PIV Smart Cards Interoperability

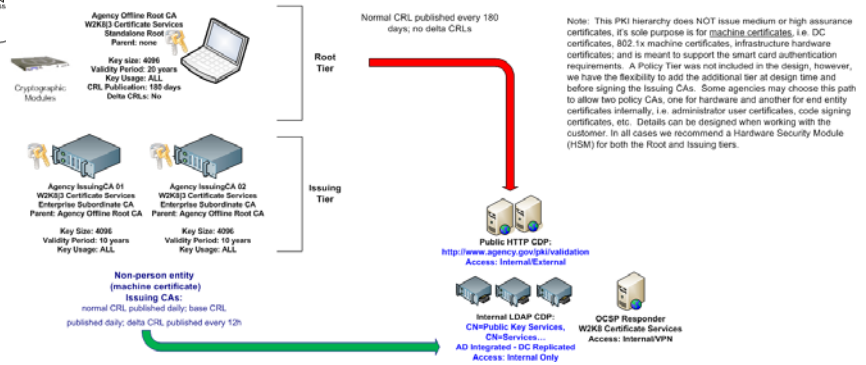
Microsoft ILM PIV solutions for HSPD-12

- What Microsoft products, technology or solutions are available or will be offered for HSPD-12?
  - Currently Microsoft has the following products and technologies that can play a role in HSPD-12 implementations…
    - Microsoft Windows Server Certificate Services
      - x.509 Certificate issuance for HSPD-12 PIV – NIST approved CA for use by SSPs to issue certificates chained to the Federal Common.
      - Internal PKI hierarchy for domain controller certificates, capable of auto enrollment and renewal of certificates, reducing operational overhead of requesting, installing and maintaining DC certificates
    - Microsoft Windows Server Domain Services: directory services, authentication, PKINIT for smart card logon, NTAuth, user accounts, etc.
    - Microsoft Identity Lifecycle Manager: directory and attribute synchronization, account provisioning, de-provisioning, etc.
    - Microsoft Windows clients operating systems (Windows XP, Windows Vista and Windows 7) – smart card authentication, OCSP/CRL validation
  - Proposed ILM PIVdb solutions for HSPD-12
    - Directory synchronization for USAccess sponsorship and PIV card issuance (In Development)
    - Detailee account provisioning solution for PIV Cardholders (Conceptual)
    - COOP account provisioning solution for PIV Cardholders (Conceptual)

Microsoft ILM PIVdb to USAccess for HSPD-12







Microsoft ILM PIVdb Detailee and COOP Conceptual Process

Detailee:

1.Agency has deployed ILM for AD account provisioning; various UPN suffices have been added to their AD instance

2.Security Office has ILM PIVdb UI installed with a smart card reader installed

3.Detailee inserts PIV card, and PINS to verify ownership

4.ILM PIVdb detailee function reads card and extracts PIVAuth certificate and CHUID

5.ILM PIVdb detailee function gets issuing CA certificate from chain and verifies or adds to NTAuth

6.Attributes and fields from certificate read and saved to Detailee table, additional detailee data added by security personnel

7.Security personnel clicks on create account which calls ILM functions to synchronize data into metaverse from the detailee table

8.AD connector runs and provisions account based on established account creation rules, sets expiration date of account

9.PACS connector runs and synchronizes CHUID data with PACS or vice versa, PACS pulls data from PIVdb database

10.User can now use their PIV card for logon or physical access

11.At expiration of detailee period ILM AD connetor disables or deletes the user account and the PACS system disables the user's access

COOP:

1.Similar to Detailee, however, if the forest that is being used for COOP does not exist, then the creation and setup of ILM precedes the steps.

2.A previous assessment of the civilian agencies can e used to determine what UPN suffices will need to be added to the COOP directory.

3.If COOP is an extension of an agency's directory at a COOP site, then the detailee steps may work in the same manner.

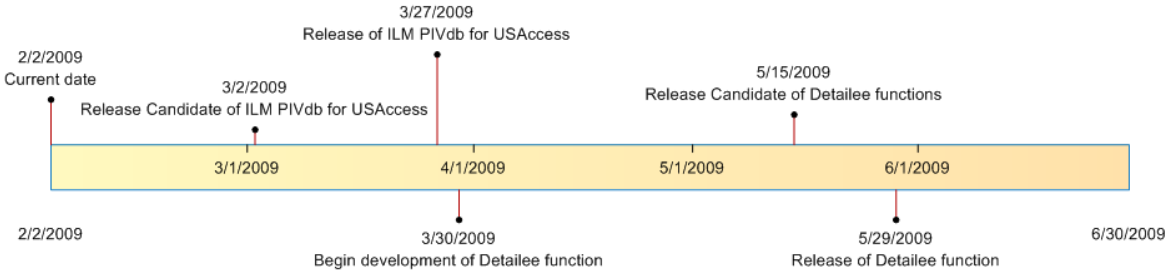
4.For future interop scenarios, a single government namespace may help with UPN suffix. For example if all government employees and contractors had a unique ID that was globally unique, then you could create Agency.USGovernment.gov as the common namespace for the suffix. This could even be extended to include SLG, i.e. agency.florida.state.USGovernment.gov for interop in a first responder scenario. MUST be unique ID to prevent collisions, however, we could combine this with x.509 root hints to resolve ambiguous UPNs

These are conceptual idea, detailed testing and design has not been done to address the issues that may arise. Working with the government on a CRADA type project we could bring Microsoft | Services and the product groups to complete the design and architecture.

Microsoft Windows Platform and HSPD-12 PIV Smart Cards Interoperability

Solution Timeline and Engagement Model

- Solutions are NOT products from the Microsoft product groups, they are typically developed in conjunction with the product groups by Microsoft | Services.
  - Due to the differences in departments and agencies related to authoritative sources of attributes, the solution is delivered as a Microsoft | Services engagement to address the unique ILM management agent development to connect to sources. In addition the solution includes planning and designing for an internal PKI hierarchy to handle infrastructure certificate requirements of smart card logon.
  - Services engagements of this type are scoped to deliver a limited production pilot for up to 1000 users, with a duration of approximately six (6) months.
- Proposed availability of the common reusable components and services are as follows:



Microsoft®

Your potential. Our passion.™

© 2008 Microsoft Corporation. All rights reserved. Microsoft, Windows, Windows Vista and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries.
The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation.
MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.