JUNE 2011

Mapping PIVCard Certificates to a Privileged Account

MULTI-FACTOR AUTHENTICATION FOR PRIVILEGED USERS ACCESSING PIV-ENABLED SYSTEMS

Identity Management Services
Enterprise Solutions Staff
Office of the Chief Information Officer
Information Resources Management
Justice Management Division
U.S. Department of Justice

James Burke, CISSP
Technical Lead
IDMS Program Management Office

PREPARED BY eMentum

PREREQUISITES

Identity Management Services (IDMS) has written this document for Department of Justice enterprise information technology professionals who have responsibilities related to the implementation of PIVCard logon in accordance with Homeland Security Presidential Directive 12 (HSPD-12).

With regard to domain expertise, Identity Management Services assumes that readers are knowledgeable about:

- DOJ PIVCard
- HSPD-12-compliant smart cards
- public key infrastructure

APPLICABILITY TO OTHER AGENCIES

IDMS has written this document for general applicability to Federal agencies. To make use of this document, other agencies must substitute their own agency-specific terms for the following DOJ-specific terms:

DOJ TERM	AGENCY-SPECIFIC SUBSTITUTE TERM
Department of Justice	Agency name
DOJ	Agency abbreviation
DOJ PIVCard	Agency-specific term for the agency's HSPD-12 compatible smart card or the generic term "PIV card."
Support	Agency's central support organization

LEXICON	
CMS	card management system The Department's PIVCard issuer uses ActivClient as its CMS.
CSP	cryptographic service provider
DAR	data at rest
EKU	extended key usage
GFE	government-furnished equipment
HSPD-12	Homeland Security Presidential Directive 12 (2004)
IDMS	DOJ Identity Management Services
MMC	Microsoft Management Console
MSO	Managed Services Office With regard to HSPD-12 implementations, "MSO" typically refers to the General Services Administration's HSPD-12 Managed Services Office, which offers the USAccess Program.
OID	object identifier
OU	organization unit
PIN	Personal identification number (in this document, the PIVCard PIN)
PIVAUTH	PIV authentication certificate The X.509 digital certificate on the PIVCard that contains the public key issued by the CA.
PIV-I	PIV interoperable A PIV interoperable card is one that: ▪ is issued in accordance with the FIPS 201 process for enrollment and activation ▪ meets the FIPS 201 technical standards for interfacing with a PIV-enabled LACS or PACS ▪ allows Federal relying parties to trust the card across agencies In print, the term PIV-I ("PIV eye") is easily confused with PIV-1 ("PIV one"), the section of FIPS-201 that describes minimum requirements for a Federal personal identification system.
SEE	Symantec Endpoint Encryption™
SP 800-53	National Institute of Standards and Technology Special Publication 800-53: *Recommended Security Controls for Federal Information Systems and Organizations*
UPN	user principle name

CONTENTS

I. INTRODUCTION

"PIVCard logon" refers to the use of digital certificates on the PIVCard as the common means of authentication for access to departmental information systems.

The Department's policy is to enable PIVCard logon for all information systems – current and future. However, in implementing PIVCard logon, system owners must resolve a conflict between two Federal documents:

- Homeland Security Presidential Directive 12 (HSPD-12) requires that the Department issue one PIVCard to each organizational user for authentication and authorization to access departmental facilities and information systems.
- NIST Special Publication 800-53 (SP 800-53) distinguishes between organizational users and "privileged users" -- i.e., key management, network/system/database/Web administrators whom the Department has authorized to perform security-relevant functions. SP 800-53 recommends that privileged users provide additional assurances of authentication and authorization (e.g., a second PIVCard with additional digital certificates) when logging on to privileged accounts on PIV-enabled information systems.

To resolve the conflict between HSPD-12 and SP 800-53, IDMS recommends mapping the digital certificates on each privileged user's PIVCard to that user's privileged account(s) – and not issuing the privileged user a second PIVCard. Mapping will meet the "one-card" requirement of HSPD-12 and the additional assurances recommendation of SP 800-53.

In addition, mapping PIVCard certificates to privileged accounts has two ancillary benefits:

- Mapping facilitates privileged account logon for users who have temporary assignments at locations served by different domains
- Mapping facilitates the use of other trusted credentials, e.g. PIV interoperable (PIV-I)

This document details the process for mapping PIVCard digital certificates to privileged accounts on Microsoft Active Directory™.

I.A System Requirements

In complying with HSPD-12, the Department may use only those products that the General Services Administration (GSA) includes on its Approved Products List (APL). The solution described in this document applies only to systems using the following GSA-approved products:

I.A.1 SERVER

Windows Server 2008

I.A.2 WORKSTATION OPERATING SYSTEM

- Windows Vista
- Windows 7
- subsequent releases of Windows operating systems

I.A.3 CRYPTOGRAPHIC SERVICE PROVIDER

Windows Vista does not include a cryptographic service provider (CSP) and this solution requires a more robust CSP than Microsoft has provided with the Windows 7 mini-driver.

GSA has approved several middleware applications, however the Department's PIVCard issuer uses the ActivIdentity™ card management system, ActivClient™ 6.2. Therefore, IDMS used ActivClient 6.2 in designing and testing this solution.

II. MIDDLEWARE

II.A Windows Vista

To enable PIVCard logon for workstations running Windows Vista, the Department must integrate middleware.

II.B Windows 7

Windows 7 includes a mini-driver for basic PIVCard functions. However, the mini-driver does not the support the cryptographic service provisions required for this solution. IDMS recommends that the Department integrate middleware into its Windows 7 solution to provide a more robust CSP and to access the additional functions that middleware provides.

Following is a table comparing the functionality of the Windows 7 mini-driver with ActivClient:

WINDOWS 7 MINI-DRIVER		ACTIVCLIENT	
FUNCTIONALITY			**NOTES**
WINDOWS NETWORK LOGON -- standard access	✓	✓	The Department's current agreement with the middleware vendor is per-PIVCard licensed, not per-installation licensed. For example, even if a user has a government-furnished equipment (GFE) workstation, GFE laptop, and personal PC, the Department would pay for only one license because the user has only one PIVCard, which can be used to log onto all three machines. PIVCard logon does not apply for local/non-domain logon.
WINDOWS NETWORK LOGON -- privileged access (admin account)	✗	✓	With Microsoft Server 2008 domain controllers on the backend and Vista/Windows 7 on the workstation, the PIVCard digital signing certificate can be mapped to a user's privileged account. During logon, ActivClient prompts the user to choose which account to log onto (standard or privileged). However, the Windows 7 native CSP errs on privileged account access.
DAR/SEE -- laptop startup/single sign-on	✗	✓	ActivClient is required during the card registration process when using Symantec Endpoint Encryption (SEE).
PIN CHANGE	✓	✓	If a user logs on to a workstation with PIVCard+PIN, the user can change that PIN at the workstation.
PIVCARD UNLOCK AND RESET (through USAccess)	✗	✗	If a user locks a PIVCard (after six failed attempts at entering the correct PIN), the user must go to a USAccess System Activation Station to unlock the PIVCard and reset the PIN. This process cannot be done at the user's workstation.
CERTIFICATE UPDATE (through USAccess)	✗	✓	The GSA MSO uses ActivIdentity for its backend CMS so PIVCard digital certificate updates can be done only through ActivClient. (Before enabling digital certificate updates via user workstations, this functionality should be tested thoroughly.) In addition, ActivClient will be updated without delay to take advantage of new features, particularly the 128k cards that the GSA MSO will roll out in late 2011 to enable key escrow.
PIN CACHING	✗	✓	The PIN is cached for the PIVAuth certificate as long as the PIVCard is in the card reader. For subsequent authentication requests while the PIN is cached, the user will be prompted to select the PIVAuth certificate, but will not have to re-enter the PIN.
PIVCARD DIAGNOSTICS (e.g., view data, picture, CHUID, etc.)	✗	✓	ActivClient provides detailed PIVCard information that the Helpdesk can use for troubleshooting.
WEB APPLICATION AUTHENTICATION	✓	✓	
DIGITAL SIGNING: ADOBE PDF FORMAT	✓	✓	
DIGITAL SIGNING: MS OFFICE	✓	✓	
CERTIFICATE FRIENDLY NAMES SET	✗	✓	ActivClient provides this function as part of its card registration process. Certificate usage is appended at the end of the friendly name and generally not visible in the certificate selection window. However, hovering the mouse over the certificate name triggers a popup showing the full friendly name, allowing the user to choose which certificate to use. With native Windows 7, IDMS recommends creating a Windows startup script that will set the certificate friendly name for all registered certificates in the local certificate store and prepend certificate usage to the friendly name to facilitate user selection.
LOCAL CERTIFICATE STORE CLEAN-UP	✗	✓	ActivClient can be configured to remove the user's certificates from the Windows local certificate store upon card removal. This minimizes storage of older certificates that have been invalidated by a certificate update. However, if clean up is enabled, IDMS recommends using ActivClient's certificate registration process and default setting of friendly names because the customized friendly names script (described above) cannot be integrated automatically into the card registration process.

III. SECURITY CONSIDERATIONS

The Department should develop security-assurance criteria for determining which personnel will be authorized to map PIVCard certificates to privileged accounts.

Typically, if an administrator attempts to gain unauthorized access to another user's privileged account by changing the password, the user will detect and report the change immediately, triggering a domain controller audit.

However, with a user's PIVCard certificates mapped to the privileged account, unauthorized access could be transparent to the user and so not detected until a regularly scheduled domain controller audit

III.A Domain Controller Auditing

Microsoft Active Directory™ logs different types of events. The two event types that are most important for PIVCard logon are Pre-Authentication Type 15 and Type 16.

III.A.1 PRE-AUTHENTICATION TYPE 15

Pre-authentication type 15 logs the use of a certificate with the UserPrincipleName (UPN) for standard logon:

III.A.2 PRE-AUTHENTICATION TYPE 16

- Pre-authentication type 16 logs the use of a certificate without the UPN for mapping to a privileged account:

IV. MAPPING PIVCARD CERTIFICATES TO PRIVILEGED ACCOUNTS

There are many ways to get the information required to map PIVCard certificates to privileged accounts. As an example, following is a process that IDMS tested and successfully implemented for one division of the Agency:

IV.A Privileged User: E-mail Support to request mapping

- Open Microsoft Outlook.
- Click **New** to launch a new message template.
- **TO FIELD**
  Key in [***Support e-mail address***]
- **SUBJECT FIELD**
  Key in **Map certificate to [*name of your Active Directory privileged account*]**

  This is the administrative account to which you want your PIVCard digital certificate mapped. Support will verify this information before mapping.

  EXAMPLE

- **MESSAGE TAB/OPTIONS MENU**

  Click the **Sign** icon.

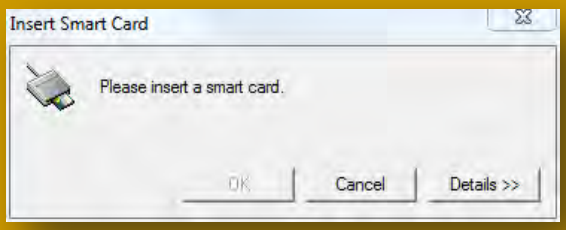
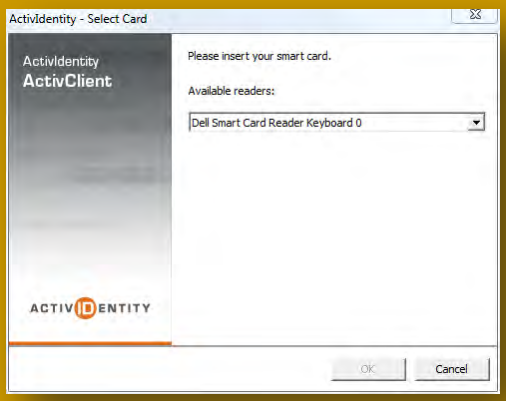
  If the Sign icon is not on your menu, see Appendix A for instructions on configuring Outlook for digital signature.

- Click **Send**.

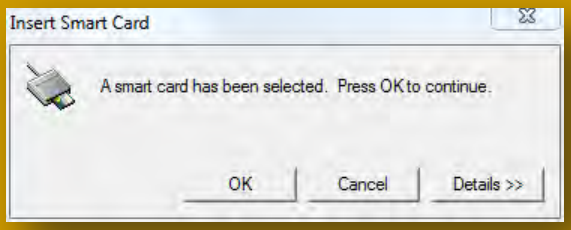
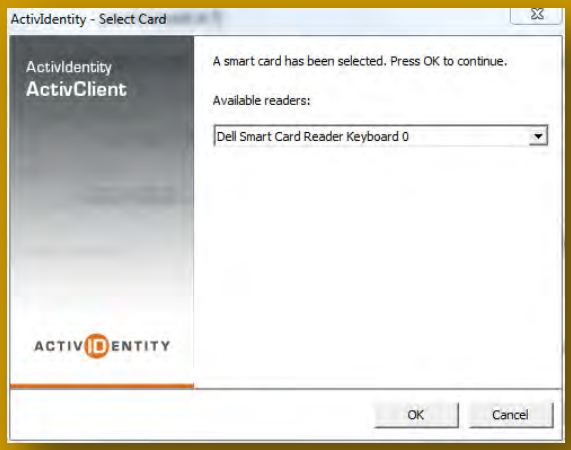
IV.B Standard Configuration/ActivClient

The Department is deploying ActivClient™ software to increase workstation security. The examples in this section show both the standard Windows configuration and the configuration with ActivClient installed.

- If your PIVCard is not already in the card reader, the system prompts you to insert it:

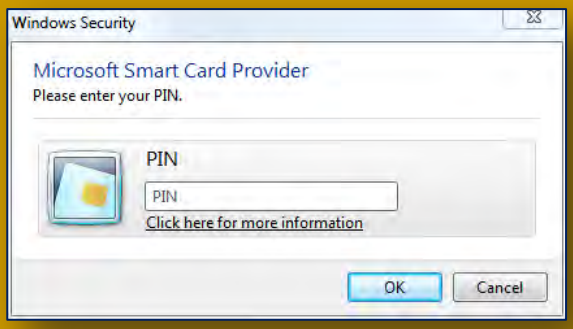
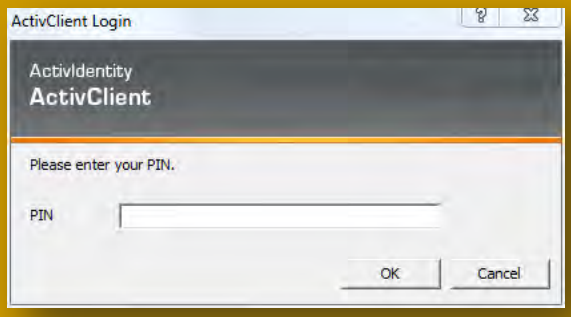
STANDARD CONFIGURATION	WITH ACTIVCLIENT INSTALLED
	

- Insert your PIVCard in the card reader.
- Once the system has read your PIVCard, it prompts you to click **OK** to continue.

STANDARD CONFIGURATION	WITH ACTIVCLIENT INSTALLED
	

- Click **OK**.

The system prompts you to enter your PIN.

STANDARD CONFIGURATION	WITH ACTIVCLIENT INSTALLED
	

- **PIN**
  Key in the personal identification number (PIN) for the PIVCard.
  (Users who forget their PINS must follow their agency's policies and processes for PIN reset before continuing.)
- Click **OK** to send the e-mail to Support.

IV.C Support: Export the Privileged User's Digital Certificate

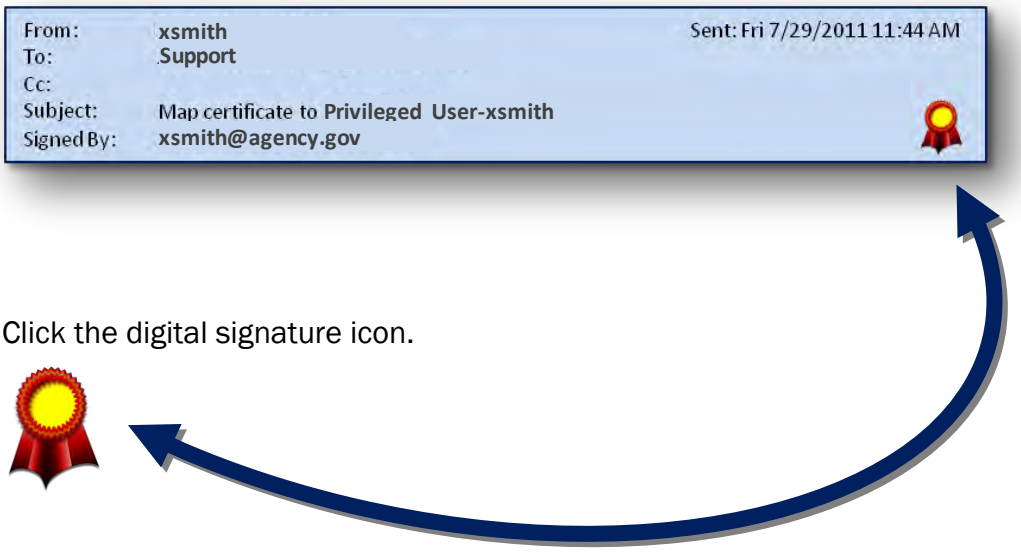
- Open Outlook.

DIGITALLY SIGNED MESSAGES APPEAR WITH THE DIGITAL SIGNATURE ICON NEXT TO THEM:	NON-DIGITALLY SIGNED MESSAGES APPEAR WITH THE REGULAR ENVELOPE ICON:
	

- Open the digitally signed e-mail from the privileged user requesting mapping.

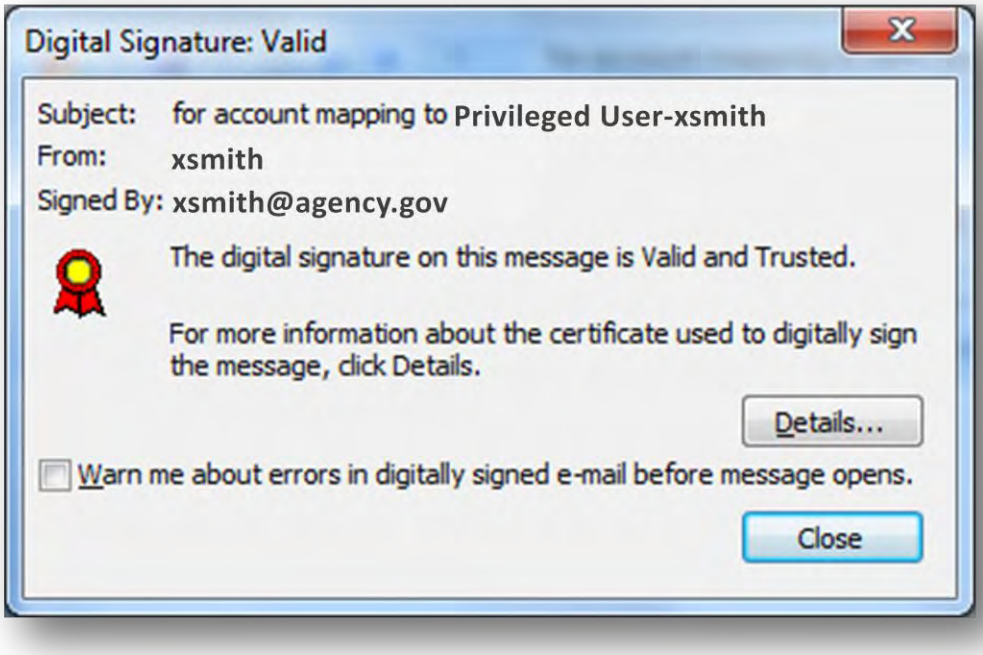
  If ActivClient displays an Auto Contacts message, click ***No****.*

  On the right side of the address panel, just below the timestamp, the system displays the digital signature icon:

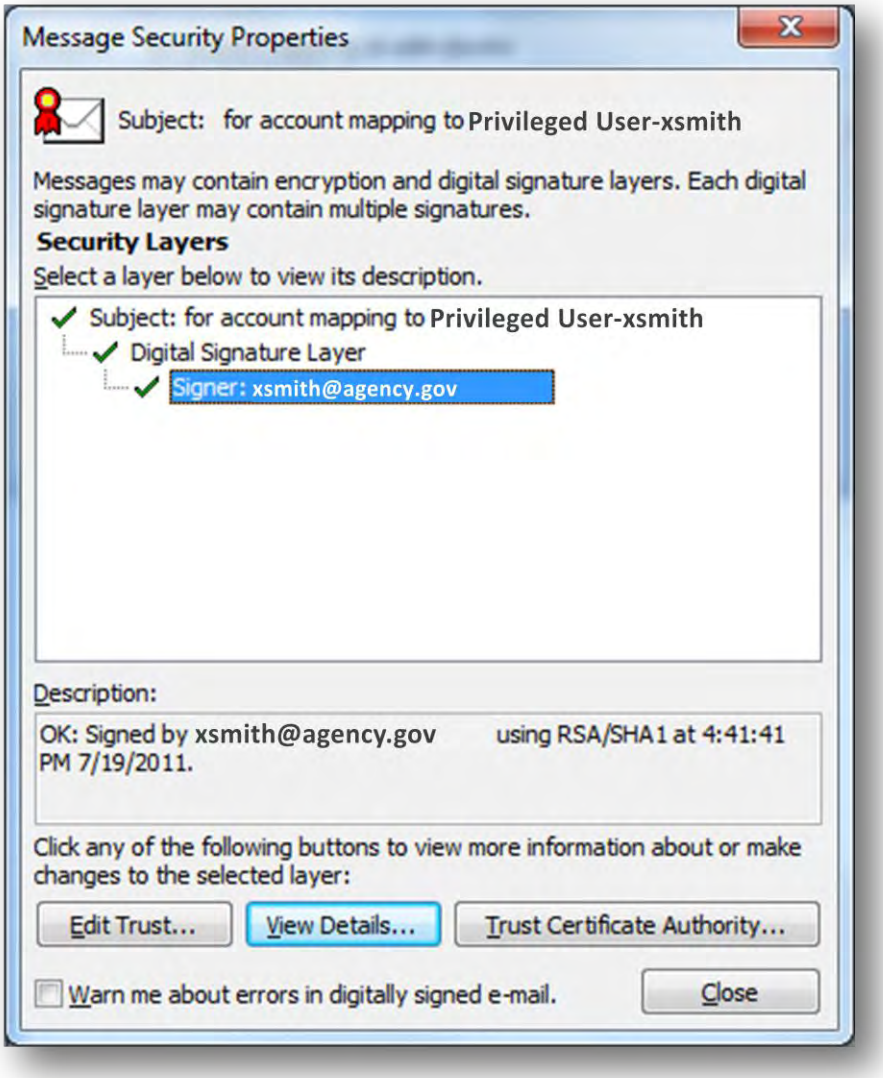


- Click the digital signature icon.

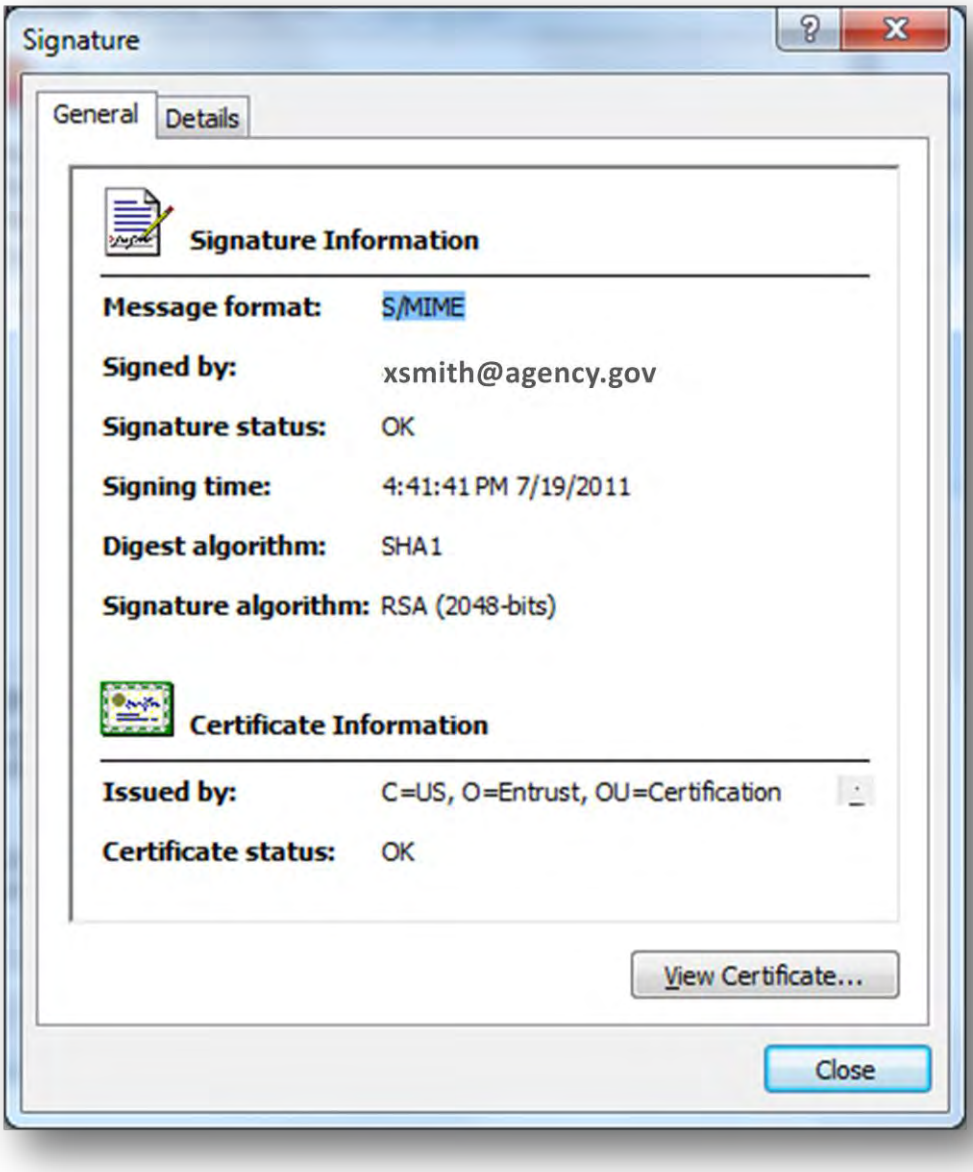
- **DIGITAL SIGNATURE: VALID**
  Click **Details...**



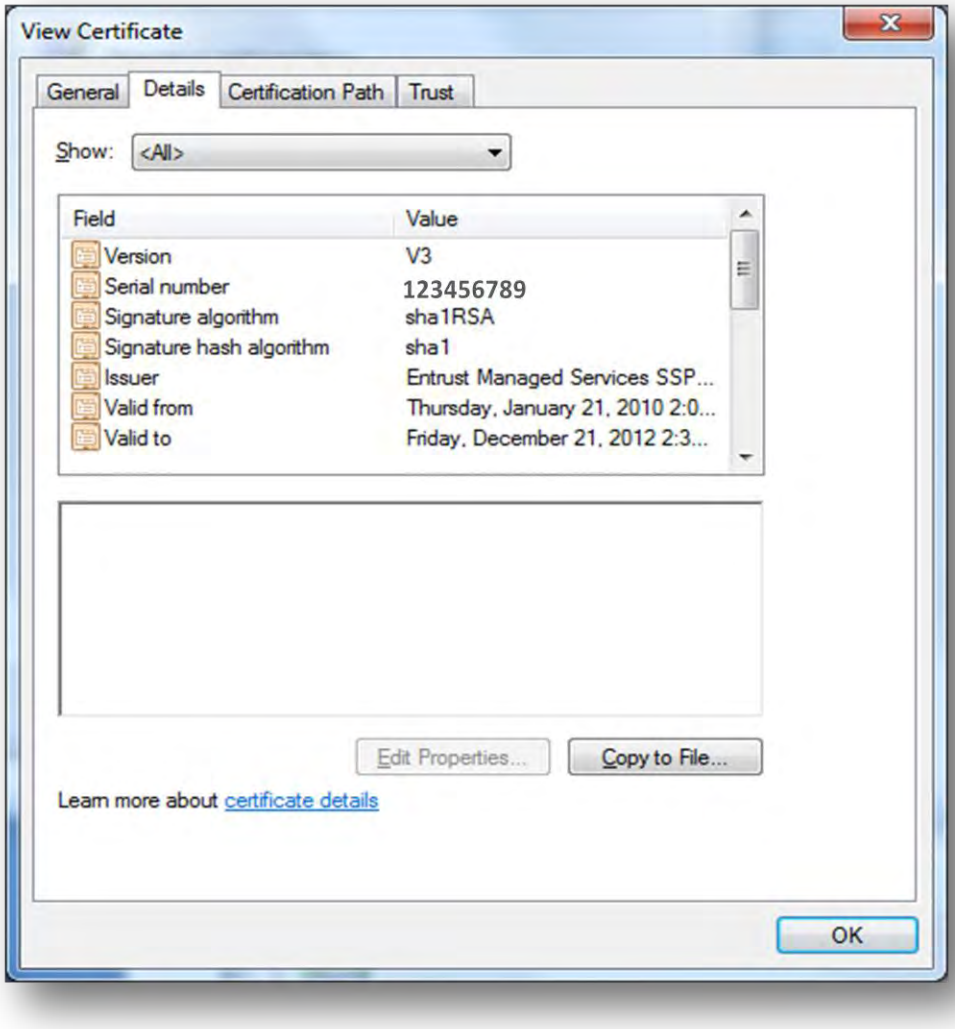
- **MESSAGE SECURITY PROPERTIES/SECURITY LAYERS**
  Click to highlight the security layer that begins with **Signer:**
  - Click **View Details…**



- **SIGNATURE/GENERAL TAB**
  Click **View Certificate**.



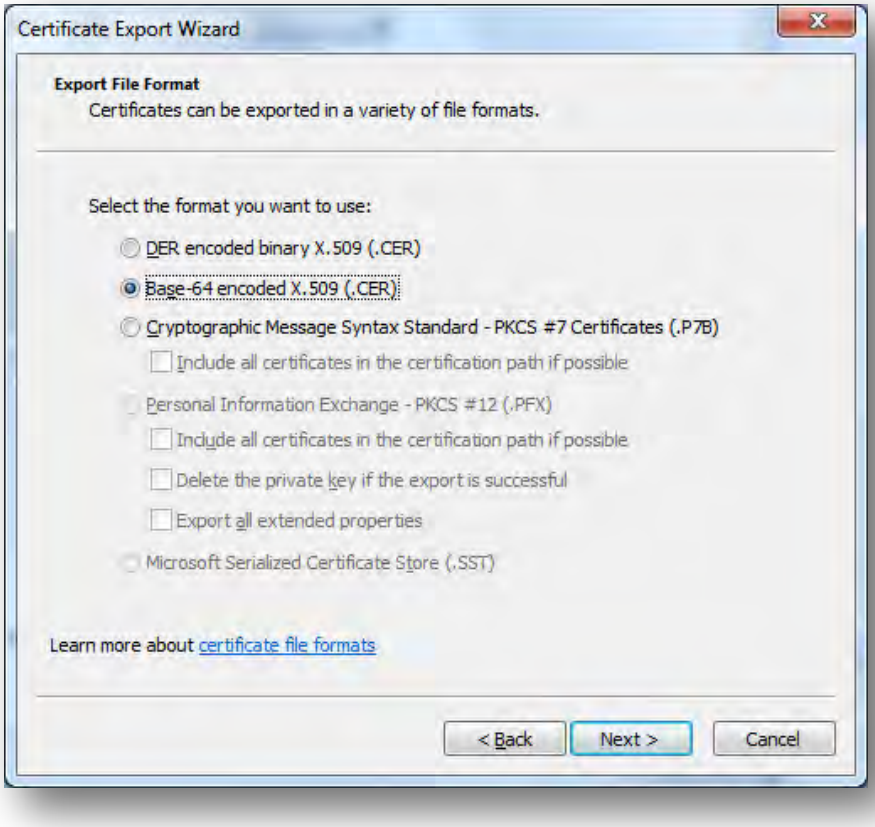
- **VIEW CERTIFICATE**
  Click the **Details** tab.
- **DETAILS TAB**
  Click **Copy to File** to launch the Certificate Export Wizard.



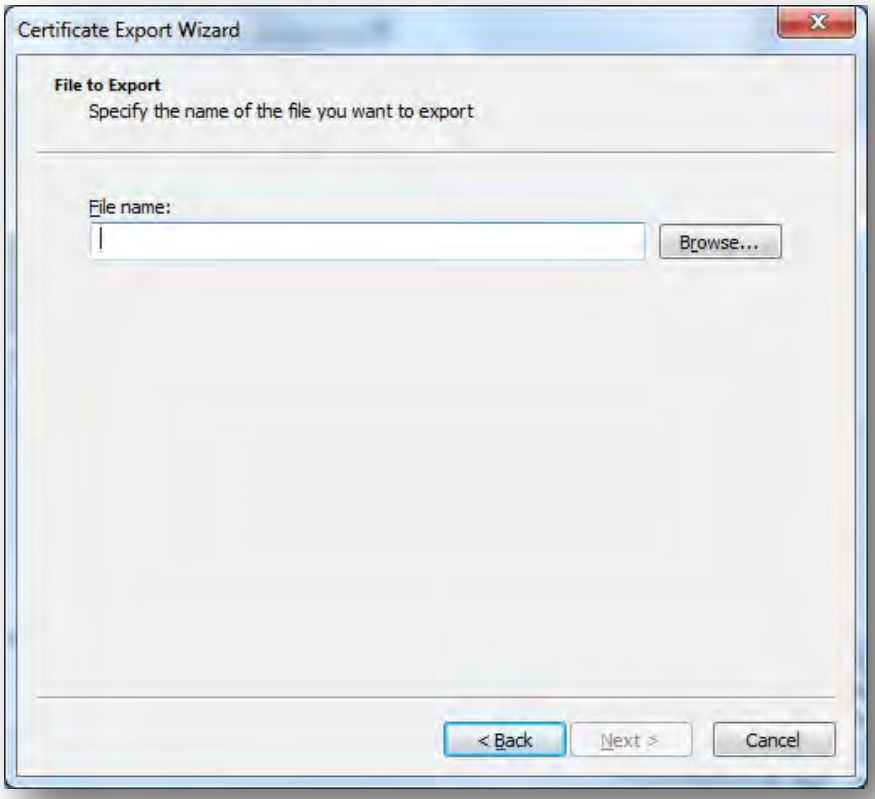
- **CERTIFICATE EXPORT WIZARD**

  Click **Next**.

- **CERTIFICATE EXPORT WIZARD/EXPORT FILE FORMAT/ SELECT THE FORMAT YOU WANT TO USE**
  Click **Base-64 encoded X.509 (.CER)**.
  - Click **Next**.



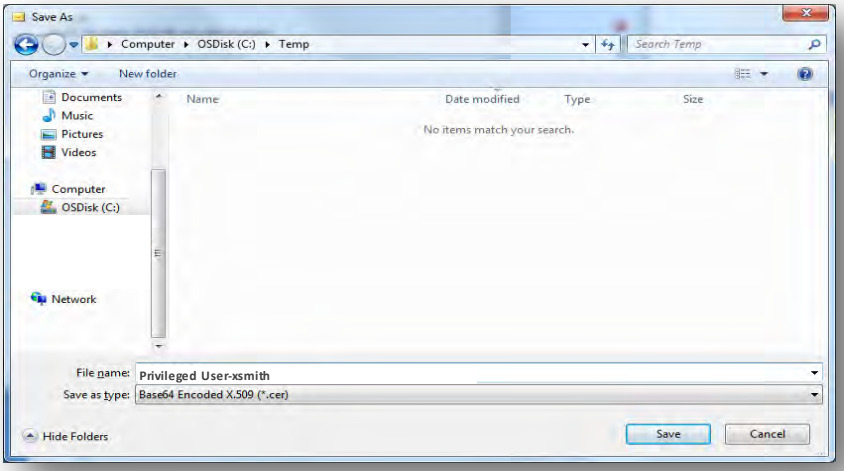
- **CERTIFICATE EXPORT WIZARD/FILE TO EXPORT/FILE NAME**
  Click **Browse**.



- Navigate to **c:\temp**
- **SAVE AS/FILE NAME**
  Name the certificate.

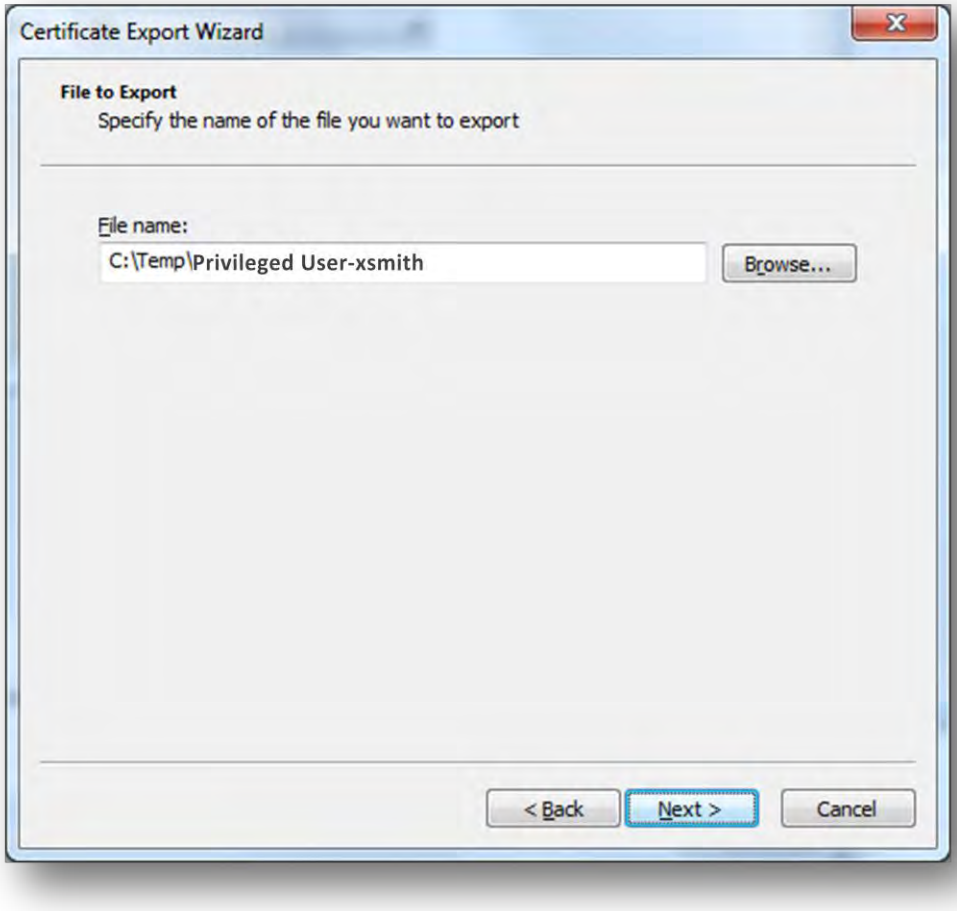
  For easy reference, name the certificate for the privileged account to which you are mapping it.

- Click **Save**.


Save As
Computer ▸ OSDisk (C:) ▸ Temp
Search Temp
Organize
New folder
Documents
Music
Pictures
Videos
Computer
OSDisk (C:)
Network
Name
Date modified
Type
Size
No items match your search.
File name: Privileged User-xsmith
Save as type: Base64 Encoded X.509 (*.cer)
Hide Folders
Save
Cancel

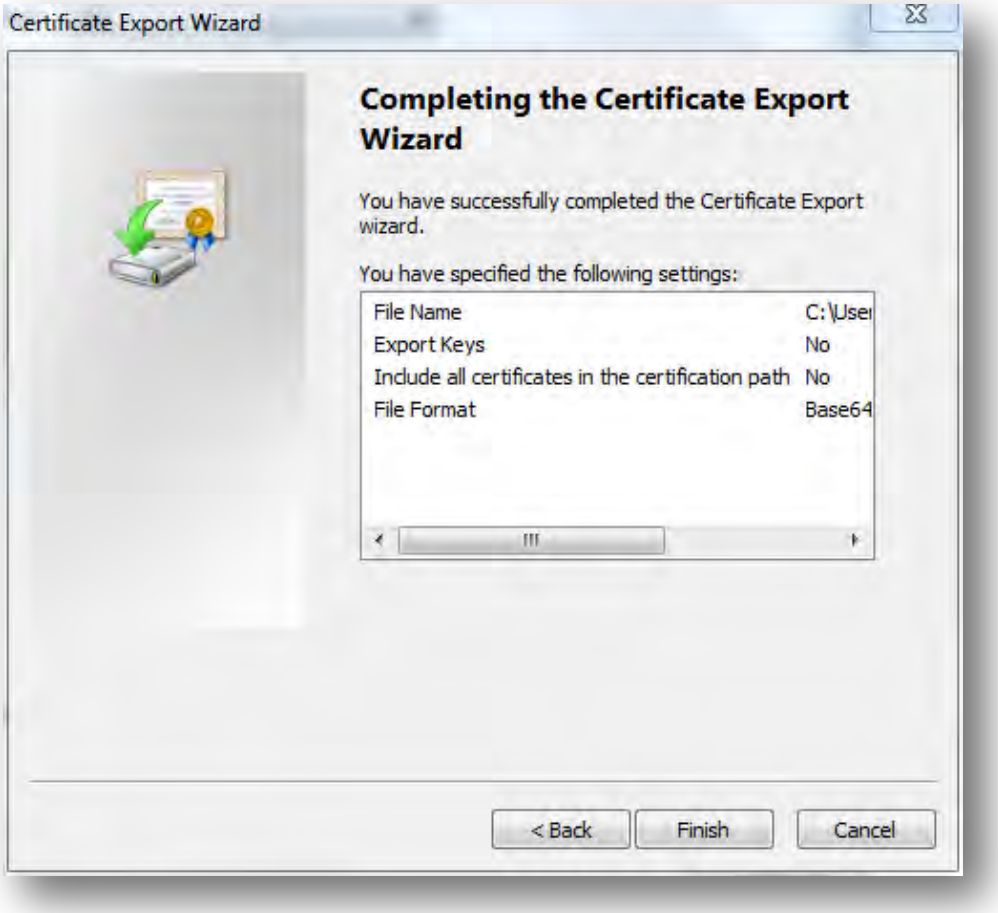
- **CERTIFICATE EXPORT WIZARD/FILE TO EXPORT/FILE NAME**

  Click **Next**.

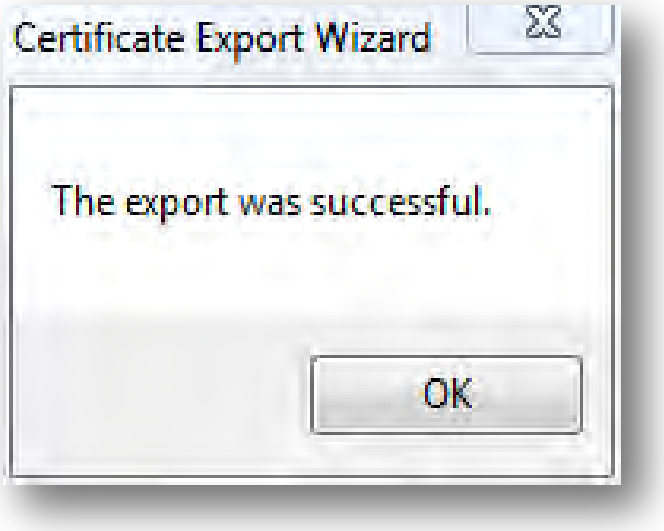


- **CERTIFICATE EXPORT WIZARD/ COMPLETING THE CERTIFICATE EXPORT WIZARD**

  Click **Finish**.

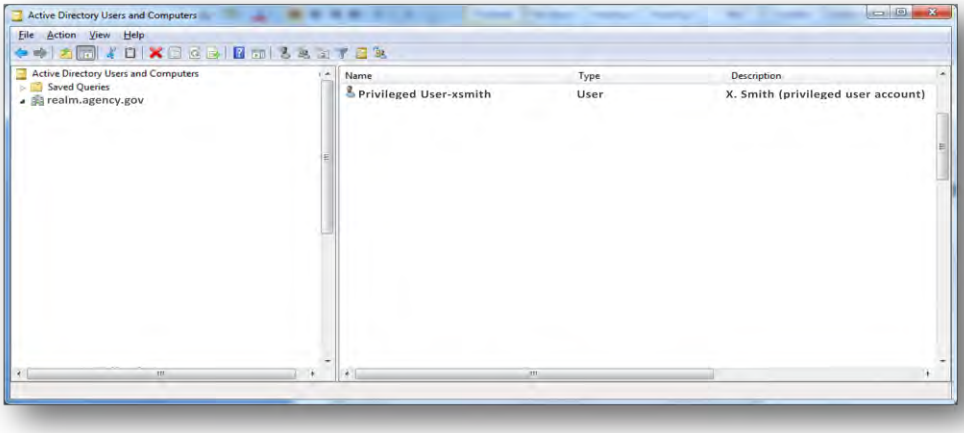


- **CERTIFICATE EXPORT WIZARD/THE EXPORT WAS SUCCESSFUL**
  Click **OK**.

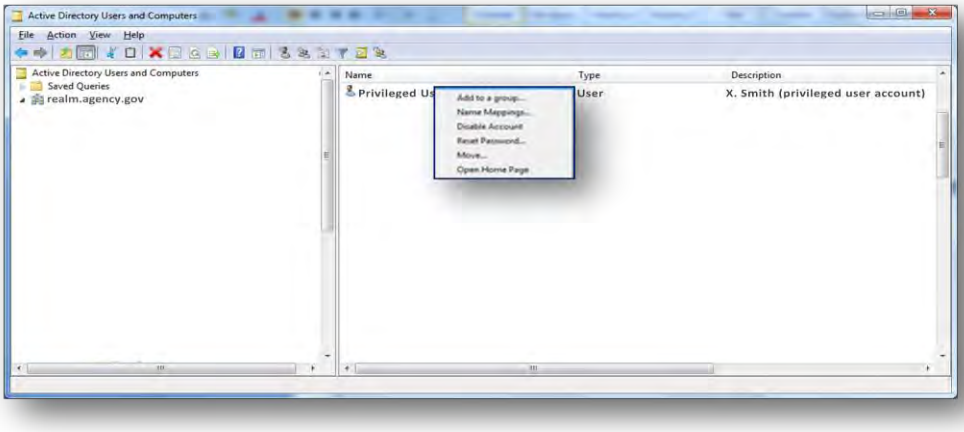


IV.D Support:
Map the PIVCard Digital Certificate to the Privileged Account

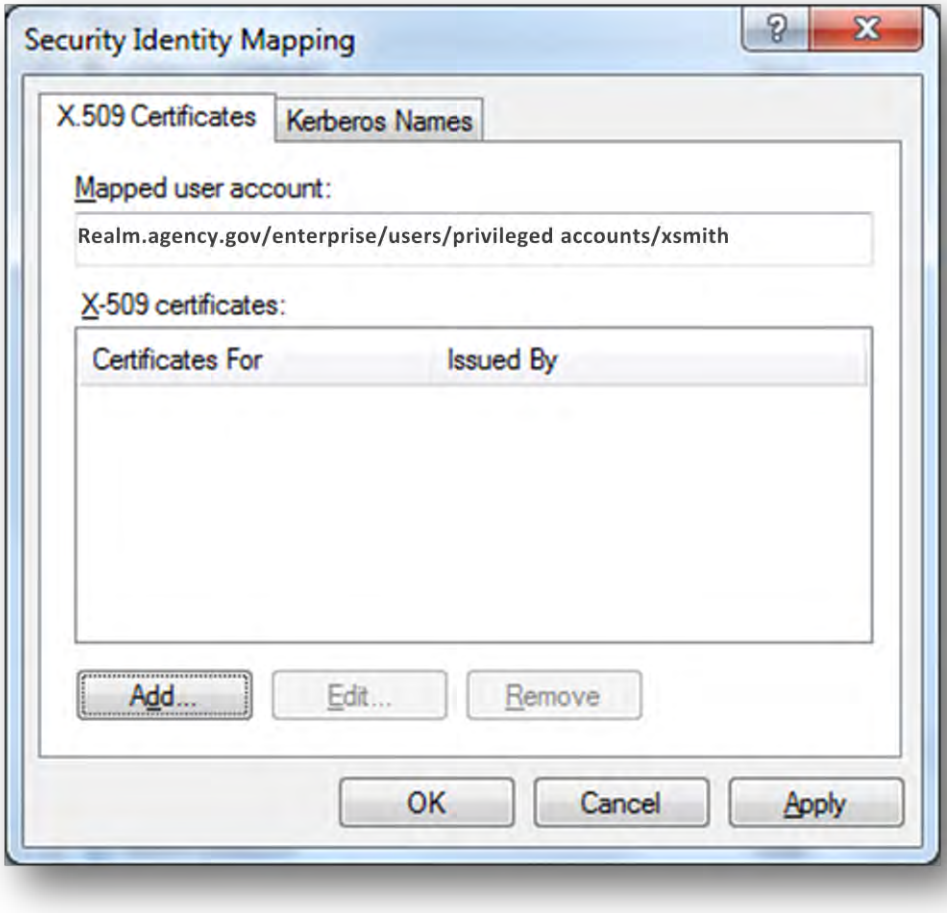
- Open **Active Directory Users and Computers**.
- **ACTIVE DIRECTORY USERS AND COMPUTERS**
  Click the **View** tab.
- **VIEW TAB**
  Turn on **Advanced Features**.
- **ACTIVE DIRECTORY USERS AND COMPUTERS**
  Find the user name to which the digital certificate should be mapped.



- **ACTIVE DIRECTORY USERS AND COMPUTERS**
  Right click on the user name.
- From the drop-down, select **Name Mappings...**



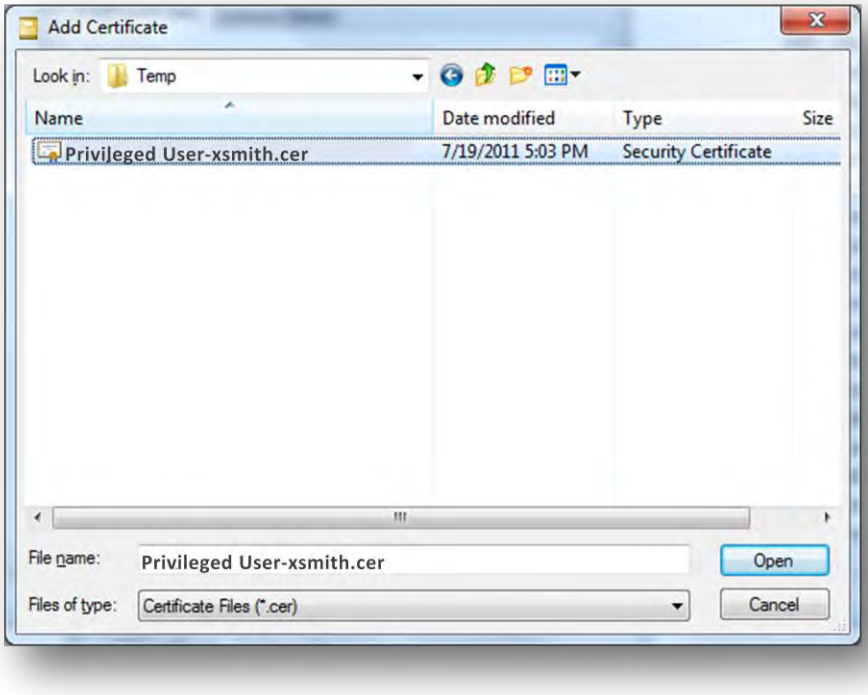
- **SECURITY IDENTITY MAPPING/X.509 CERTIFICATES TAB**
  Click **Add**.



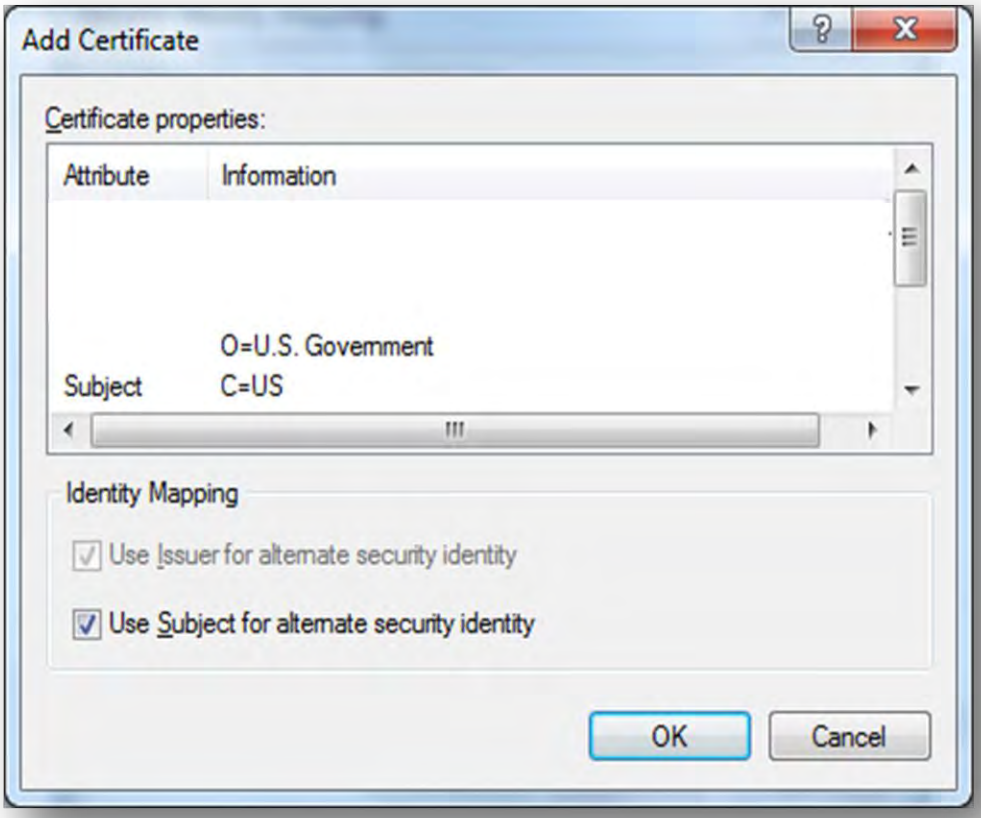
- **ADD CERTIFICATE**

  Browse to the administrator's digital certificate saved earlier.

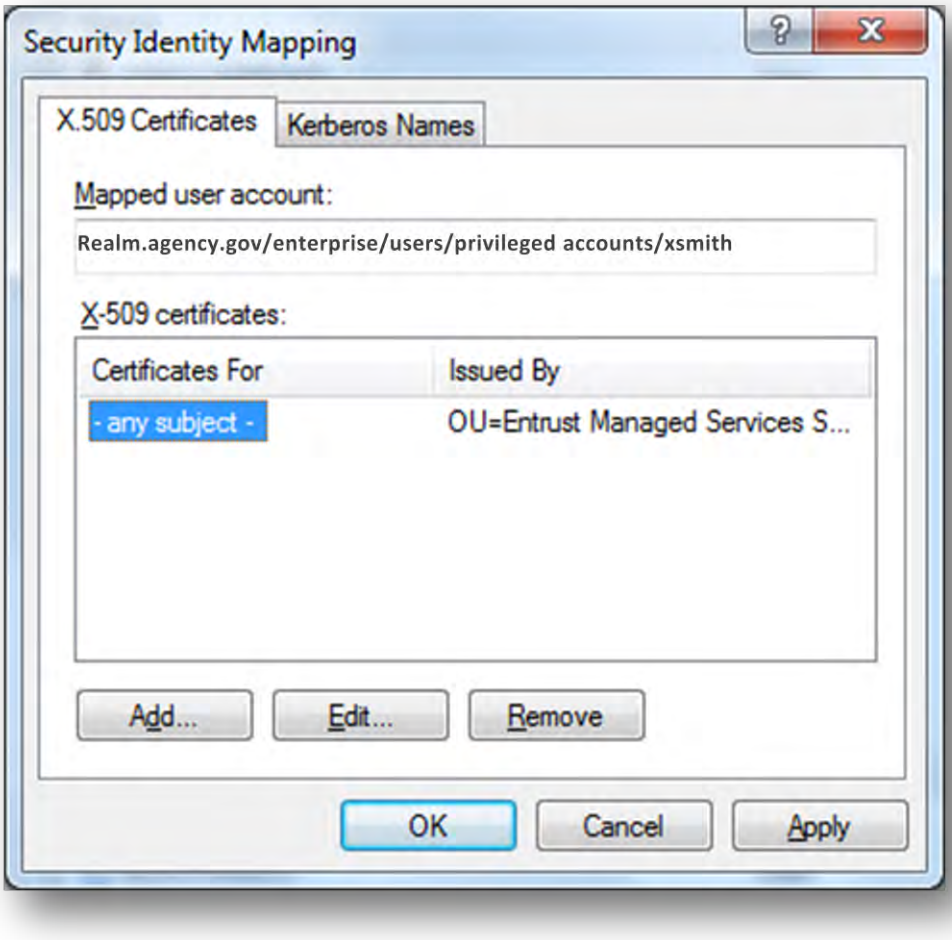
  - Click **Open**.



- **ADD CERTIFICATE/CERTIFICATE PROPERTIES/IDENTITY MAPPING**
  Leave both boxes checked.
  - Click **OK**.



- **SECURITY IDENTITY MAPPING/X.509 CERTIFICATES TAB**
  Click **OK**.



Using a PIVCard, the privileged account holder may now log onto a privileged account from a machine running Windows Vista, Windows 7, or Windows Server 2008.

NOTE: When a privilege user has their PIVCard Re-Keyed or a new PIVCard issued, remapping is not required unless there is a change in the "Distinguished Name" e.g. user changes components.

V. CONFIGURING THE WORKSTATION

This section includes configurations that were tested at the workstation level and then applied at a Microsoft Active Directory Organization Unit (OU) level to all workstations within that OU.

V.A Required Policies

For this solution to work, there are three policies that must be applied to the workstation.

There are a number of ways to apply the policies. In the example below, IDMS used Microsoft Management Console (MMC).

V.A.1 ALLOW CERTIFICATES WITH NO EXTENDED KEY USAGE CERTIFICATE ATTRIBUTE

In Windows operating systems before Vista, smart card certificates used for logon required an enhanced key usage (EKU) extension with a smart card logon object identifier (OID).

With this policy setting enabled, certificates with the following attributes can be used to log on with a PIVCard:

- certificates with no EKU
- certificates with an All Purpose EKU
- certificates with a Client Authentication EKU

V.A.2 ALLOW SIGNATURE KEYS VALID FOR LOGON

With this policy setting enabled, the logon screen will list all available PIVCard certificates that have a signature key.

V.A.3 ALLOW USER NAME HINT

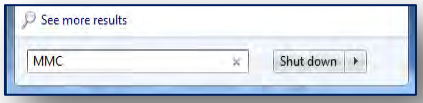
With this policy setting enabled, the system will display an optional field during logon and elevation allowing the user to enter user name or username+domain to associate the user with a PIVCard certificate.

V.B Accessing Policy Settings

There are a number of ways to access the policy settings. In the example below, IDMS used Microsoft Management Console (MMC).

- Click the **Start** icon.

- In the search field, key in **MMC**.



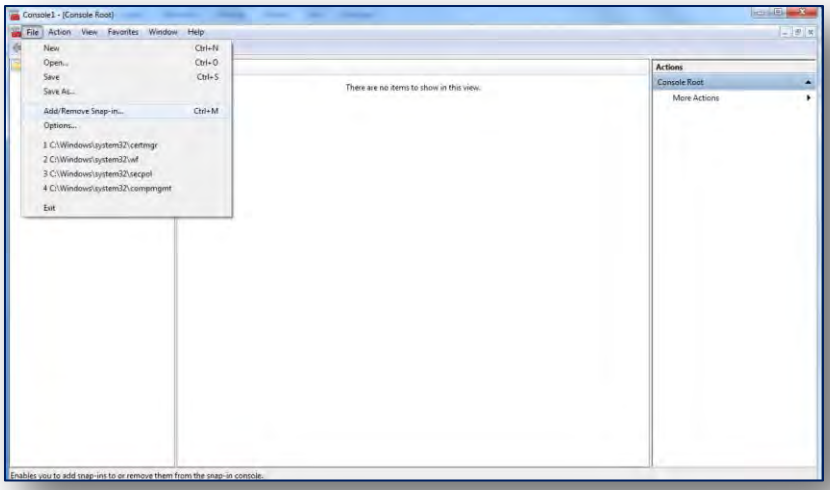
- **Enter**

  Microsoft Management Console opens with an empty console (or administrative tool). The empty console has no management functionality until you add snap-ins.

- **MICROSOFT MANAGEMENT CONSOLE**
  Click **File**

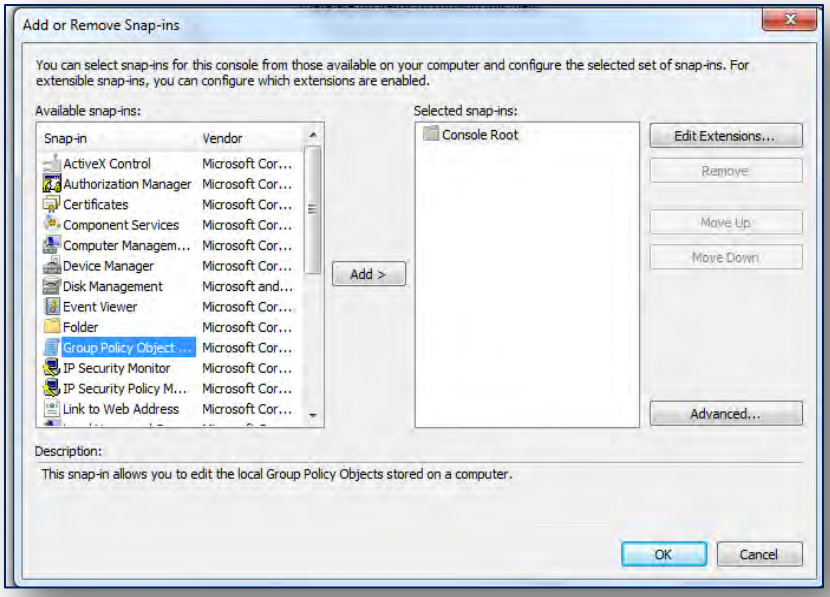
- **FILE**

  Click **Add/Remove Snap In**

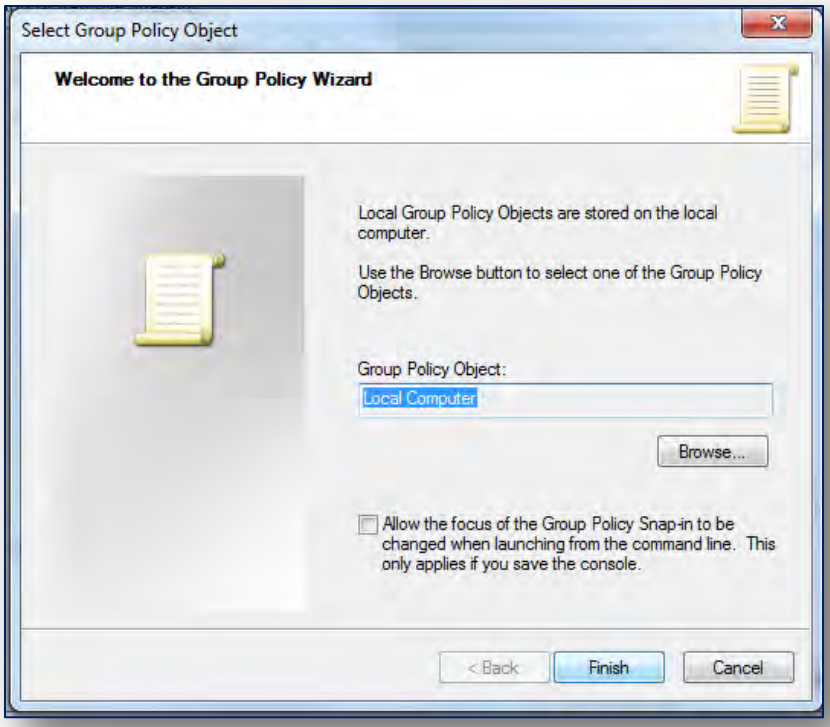


- **AVAILABLE SNAP-INS**

  Click **Group Policy Object Editor**



- Click **Add** to launch the Group Policy Wizard

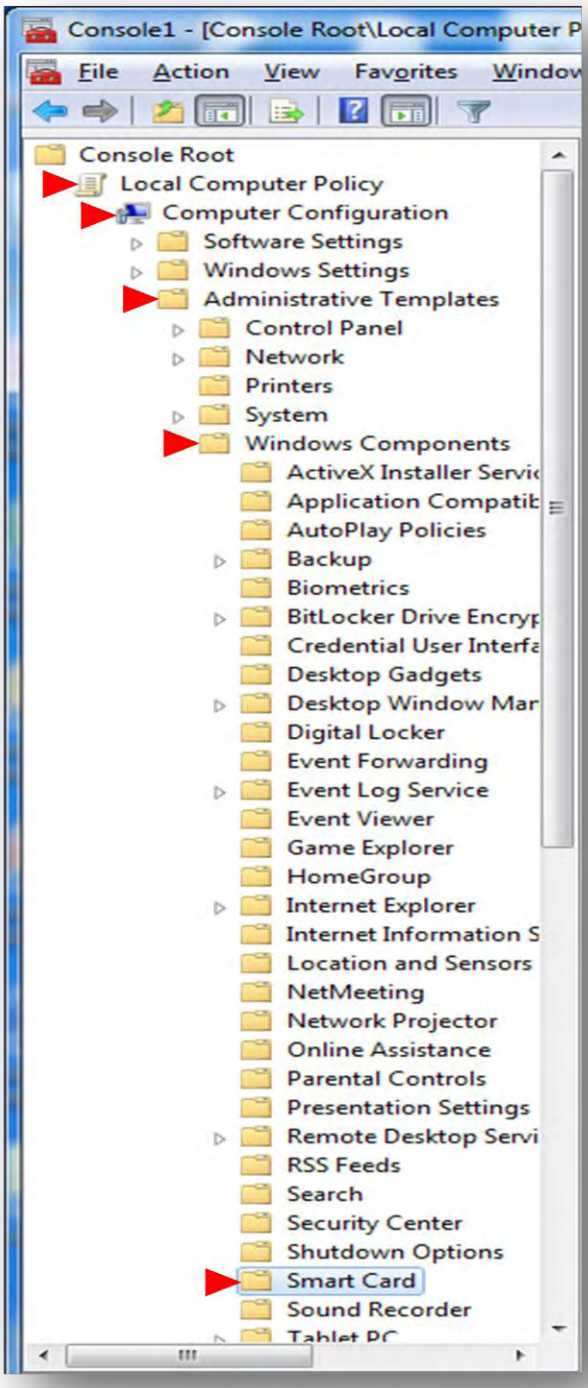


- **SELECT GROUP POLICY OBJECT**
  Leave the Group Policy Object field set to **Local Computer**.
- Click **Finish**
- Click **OK**

- **CONSOLE/CONSOLE ROOT**

Click the triangle to the left of “Local Computer Policy” to expand the selection.

- Click the triangle to the left of “Computer Configuration” to expand the selection.
- Click the triangle to the left of “Administrative Templates” to expand the selection.
- Click the triangle to the left of “Windows Components” to expand the selection.
- Click **Smart Card**



V.C Enable Policy Settings

V.C.1 ALLOW CERTIFICATES WITH NO EXTENDED KEY USAGE CERTIFICATE ATTRIBUTE

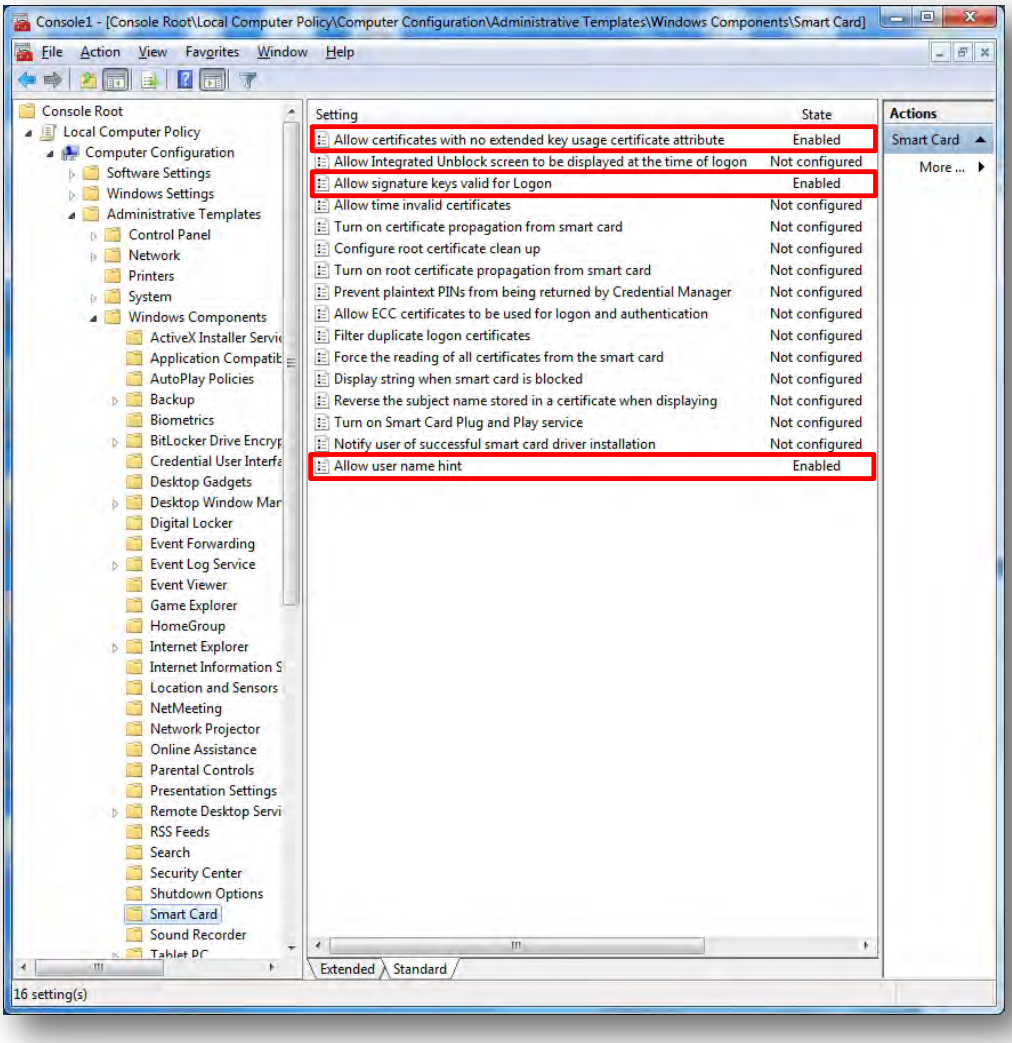
- Highlight **Allow Certificates with no extended key usage certificate attribute**.
- Click Edit **policy setting**. .
- Click **Enabled**.
- Click **OK**.

V.C.2 ALLOW SIGNATURE KEYS VALID FOR LOGON

- Highlight **Allow signature keys valid for logon**.
- Click Edit **policy setting**.
- Click **Enabled**.
- Click **OK**.

V.C.3 ALLOW USER NAME HINT

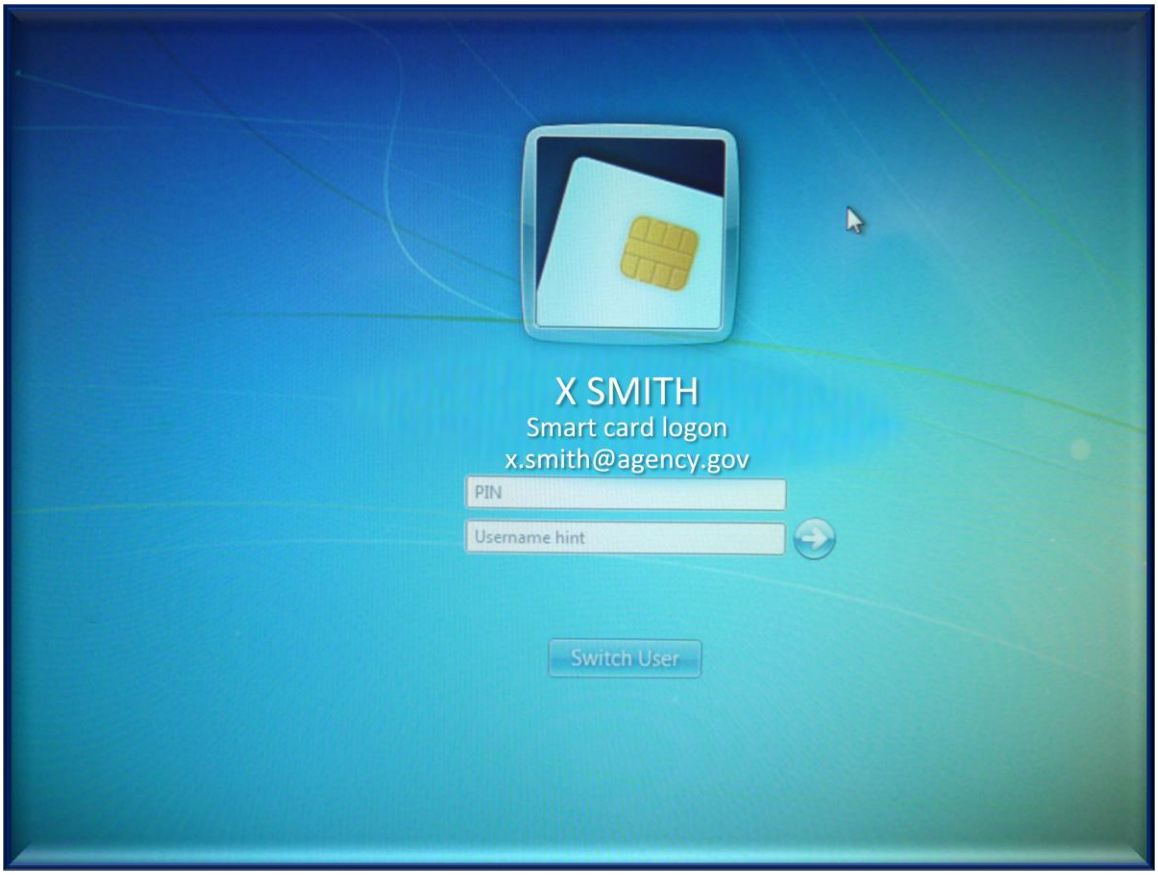
- Highlight **Allow user name hint**.
- Click Edit **policy setting**.
- Click **Enabled**.
- Click **OK**.


Console1 - [Console Root\Local Computer Policy\Computer Configuration\Administrative Templates\Windows Components\Smart Card]
File Action View Favorites Window Help
Console Root
Local Computer Policy
Computer Configuration
Software Settings
Windows Settings
Administrative Templates
Control Panel
Network
Printers
System
Windows Components
ActiveX Installer Servic
Application Compatibi
AutoPlay Policies
Backup
Biometrics
BitLocker Drive Encryp
Credential User Interfa
Desktop Gadgets
Desktop Window Mar
Digital Locker
Event Forwarding
Event Log Service
Event Viewer
Game Explorer
HomeGroup
Internet Explorer
Internet Information S
Location and Sensors
NetMeeting
Network Projector
Online Assistance
Parental Controls
Presentation Settings
Remote Desktop Servi
RSS Feeds
Search
Security Center
Shutdown Options
Smart Card
Sound Recorder
Tablet PC
Setting
State
Allow certificates with no extended key usage certificate attribute
Enabled
Allow Integrated Unblock screen to be displayed at the time of logon
Not configured
Allow signature keys valid for Logon
Enabled
Allow time invalid certificates
Not configured
Turn on certificate propagation from smart card
Not configured
Configure root certificate clean up
Not configured
Turn on root certificate propagation from smart card
Not configured
Prevent plaintext PINs from being returned by Credential Manager
Not configured
Allow ECC certificates to be used for logon and authentication
Not configured
Filter duplicate logon certificates
Not configured
Force the reading of all certificates from the smart card
Not configured
Display string when smart card is blocked
Not configured
Reverse the subject name stored in a certificate when displaying
Not configured
Turn on Smart Card Plug and Play service
Not configured
Notify user of successful smart card driver installation
Not configured
Allow user name hint
Enabled
Extended
Standard
16 setting(s)
Actions
Smart Card
More ...

VI. LOGGING ON

- Insert the PIVCard in the card reader.

  Microsoft Windows automatically identifies the certificate with the OID and presents that certificate for authentication.



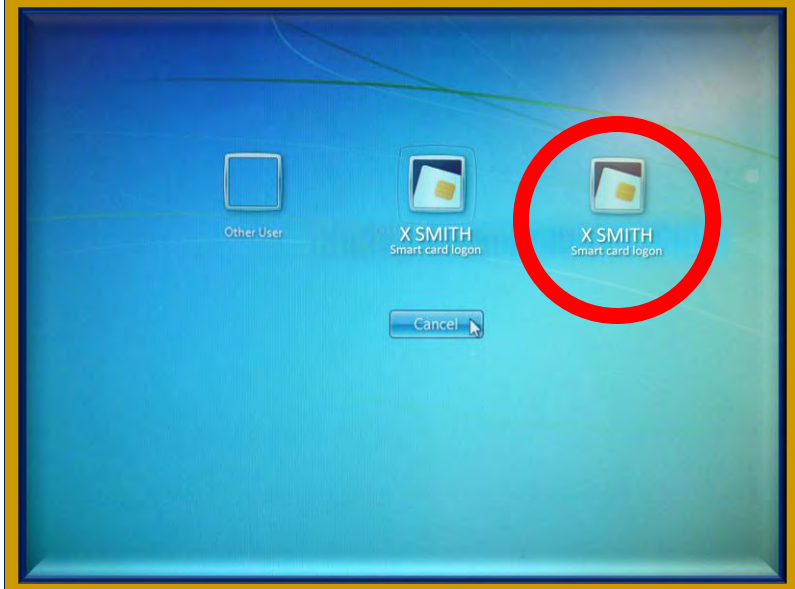
- Click **Switch User**.

At this point, the logon screen differs between workstations with ActivClient 6.2 and those with ActivClient 7 (beta) installed:

ACTIVCLIENT 6.2

The certificate with the transparent box around it is the PIV Authentication Certificate.

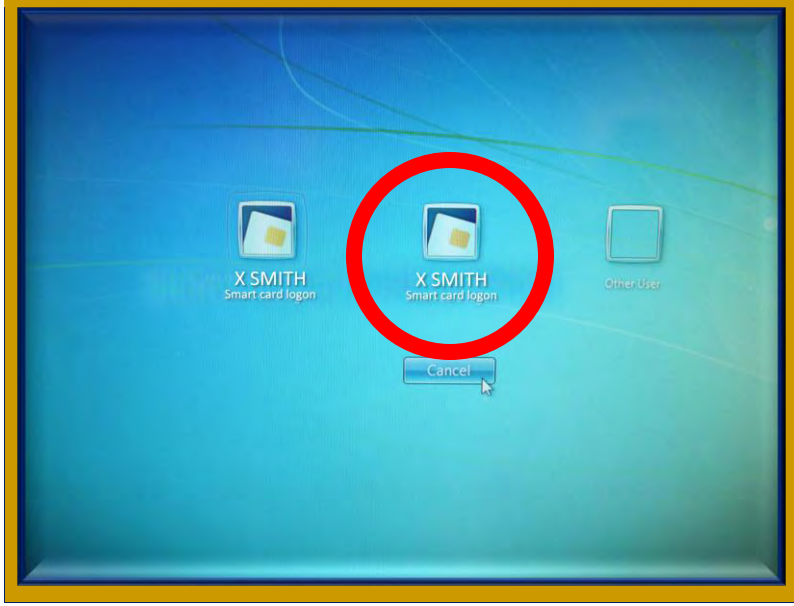
The certificate on the right is the PIV digital signing certificate. Select this certificate for mapping.



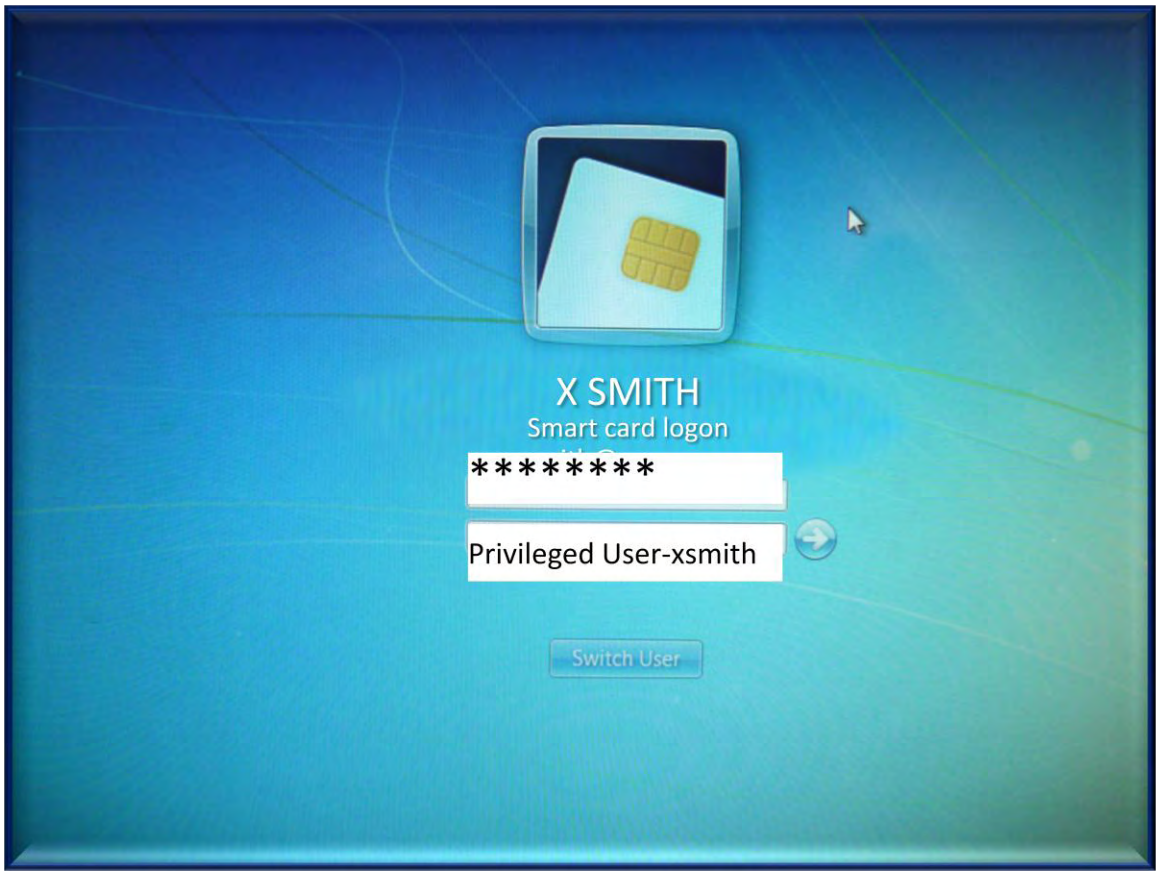
ACTIVCLIENT 7 (BETA)

The certificate with the transparent box around it is the PIV authentication certificate.

The certificate in the middle is the PIV digital signing certificate. Select this certificate for mapping.



- Key in the PIN
- Key in the account as follows…
  - IF ACCOUNT IS WITHIN THE SAME DOMAIN AS THE COMPUTER: **username**
  - IF ACCOUNT IS ON A DIFFERENT DOMAIN THAN THE COMPUTER: **domain\username**

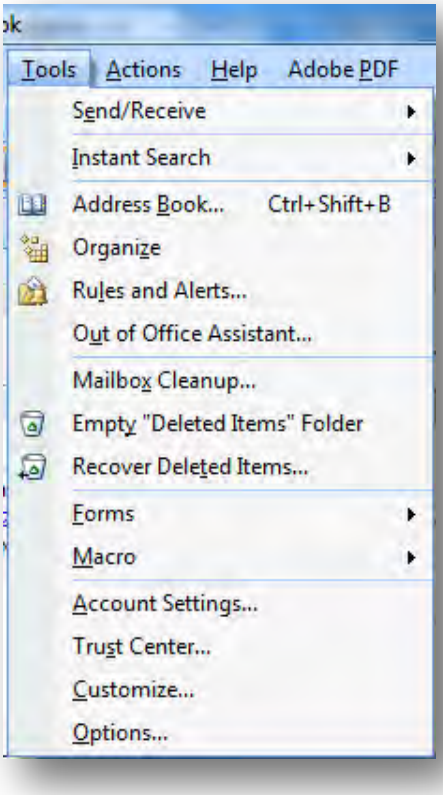


If the user's digital certificate is mapped to only one account and that account is within the same domain as the computer, then the "Hint" field is not required.

For either certificate -- PIV authentication or PIV digital signature – if incorrect information is entered into the "Hint" field, the system will deny logon.

VII. APPENDIX A: CONFIGURING OUTLOOK FOR DIGITAL SIGNATURE

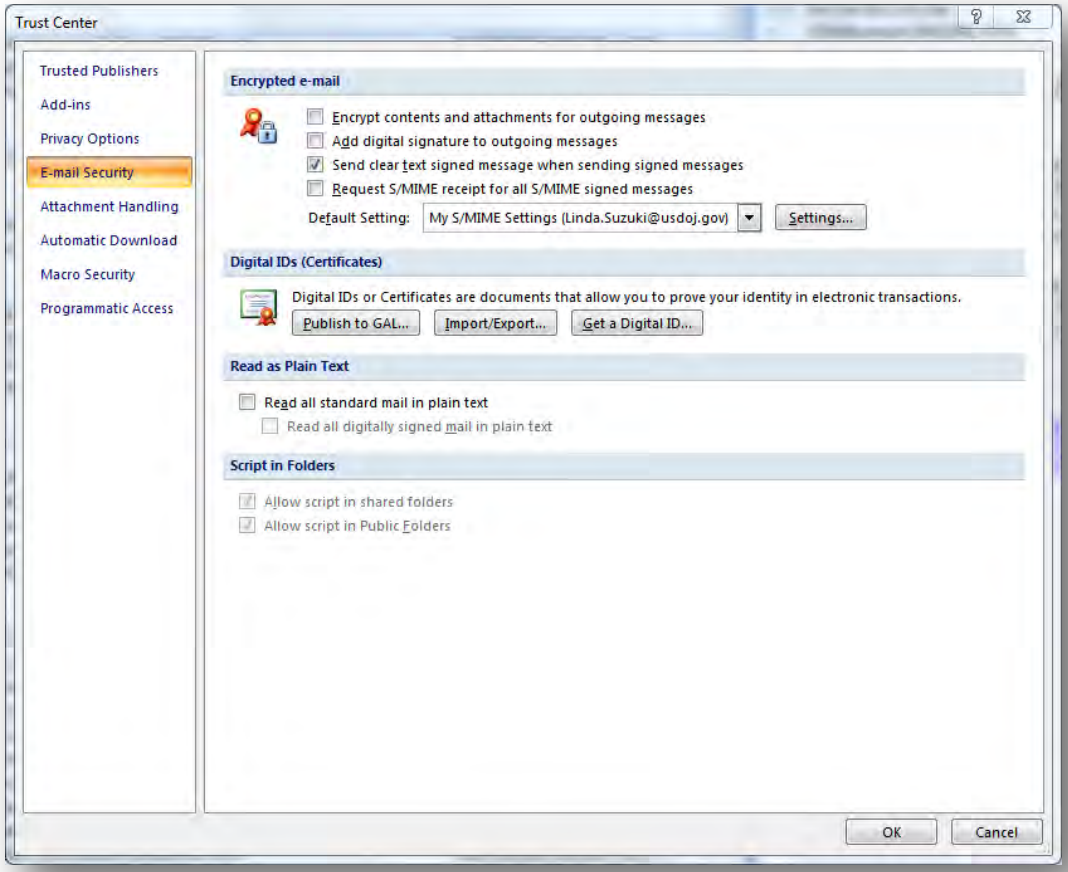
- Open Outlook.
- **MENU**
  Click **Tools**.



- **TOOLS**
  Click **Trust Center...**

- **TRUST CENTER**
  Click **E-Mail Security**.

Although Outlook displays an E-Mail Security option for "Encrypted E-mail," this is not a recommended encryption solution.

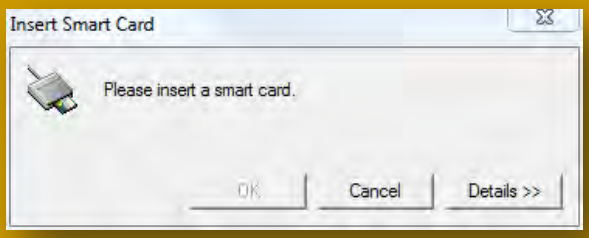
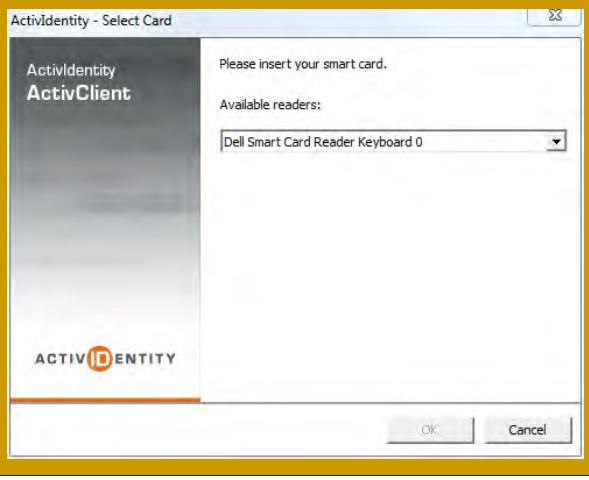


- **E-MAIL SECURITY/ENCRYPTED E-MAIL**
  If not checked already, check the box to select **Send clear text signed message when sending message**.

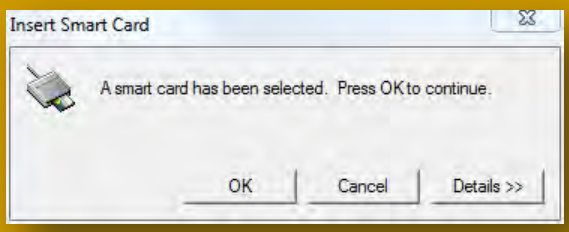
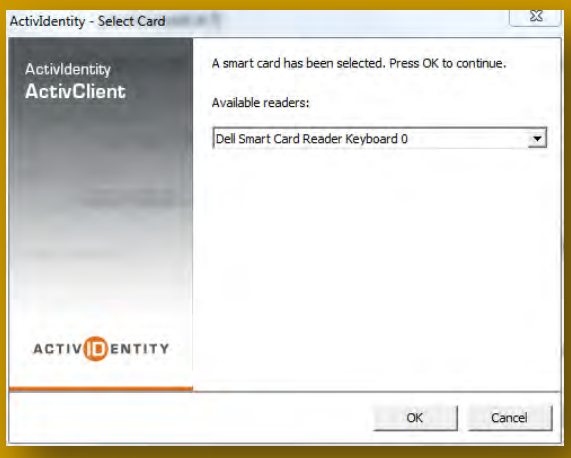
- **E-MAIL SECURITY/ENCRYPTED E-MAIL**
  Click **Settings**.

The Department is deploying ActivClient™ software to increase workstation security. The examples in this section show both the standard Windows configuration and the configuration with ActivClient installed.

- If your PIVCard is not already in the card reader, the system prompts you to insert it:

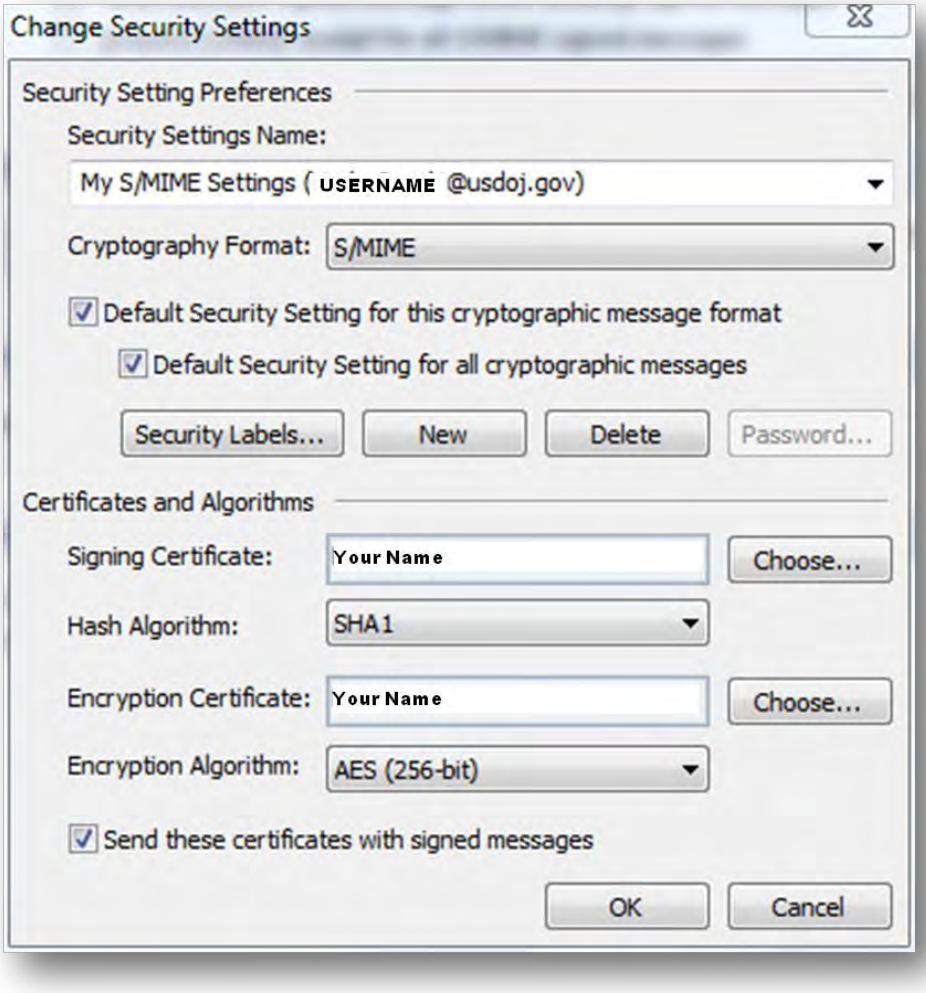
STANDARD CONFIGURATION	WITH ACTIVCLIENT INSTALLED
	

- Once the system has read the PIVCard, it will prompt you to click **OK** to continue.

STANDARD CONFIGURATION	WITH ACTIVCLIENT INSTALLED
	

- Click **OK**.

- **CHANGE SECURITY SETTINGS**
  The Security Settings auto-populate from the PIVCard.



- Click **OK**.
- Click **OK**.

You have now configured Outlook for digital signature.

VIII. AUTHOR

James Burke is an expert in identity, credential, and access management with extensive experience developing technology strategy and architecture for access control systems.

At the U.S. Department of Justice, Mr. Burke provides technical leadership for Identity Management Services as senior consultant on Federal policies for e-authentication, PKI, and personal identity verification.

James Burke, CISSP, MCSE

Technical Lead
Identity Management Services
Enterprise Solutions Staff
Office of the Chief Information Officer
Information Resources Management
Justice Management Division
U.S. Department of Justice

202-305-4370
james.burke@usdoj.gov
Two Constitution Square
145 “N” Street, NE
Washington, DC 20002

IDENTITY MANAGEMENT SERVICES

Identity Management Services (IDMS) develops and implements the Department's strategy for defining identity, managing identity, granting identity-based access to logical and physical assets, and enabling role-based delivery of information. The return on the Department's investment in identity management is increased security for DOJ's people, information systems, and facilities – and increased efficiency as we leverage digital identity to manage workflows.

IDMS accomplishes its mission by:

- providing leadership in advancing a forward-looking and comprehensive approach to identity management at the Federal, Departmental, and Component levels
- synergizing the strengths of DOJ's human resources, information security, personnel security, and physical security in verifying, managing, and leveraging identity
- supporting DOJ Components in implementing identity management

PRIORITIES

Executive mandates, Federal regulations, the Department's mission, and best practices for identity management drive the programmatic priorities for IDMS. Current priorities include:

- Federal Identity, Credential, and Access Management
  Identity Management Services implements the ICAM roadmap at DOJ.
- Identity Management Infrastructure
  Identity Management Services facilitates the integration of people, policies, processes, systems, and tools to build DOJ's identity management infrastructure.
- Homeland Security Presidential Directive 12
  Identity Management Services ensures DOJ's compliance with HSPD-12.
- Workflow
  Identity Management Services leverages digital identity to enhance customer service, eliminate redundancies, and increase protection of personally identifiable information by piloting PIVCard-based workflow initiatives.