**HSPD-12 Logical Access Authentication and 2008 Active Directory Domains**

Microsoft Corporation

Published: February 2012

Authors: Paul Fox, Erich Karch and Adam Stasiniewicz

**Abstract**

This document demonstrates the increased flexibility of FIPS 201 PIV-II compliant smart cards with Windows Server 2008 R2 Active Directory, Windows 7 and Office 2010. Included within this document are detailed steps to configure Windows Server 2008 R2 Active Directory, Windows 7 and Office 2010 to perform traditional UPN based smart card logon, explicit smart card logon (client authentication certificate mapped to multiple accounts), explicit cross-forest smart card logon and NIST SP800-78-3 compliant S/MIME email exchanges.



The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. 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 presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, email address, logo, person, place or event is intended or should be inferred.

© 2012 Microsoft Corporation. All rights reserved.

Microsoft, Windows 7, Windows 2008 Server, Windows Vista, Windows Server 2003, Windows XP, Windows ME, and Windows 98 are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

**Contents**

[Audience 5](#_Toc322940800)

[Terminology 6](#_Toc322940801)

[Public Key Infrastructure (PKI) 6](#_Toc322940802)

[Object Identifier (OID) 6](#_Toc322940803)

[X.509 6](#_Toc322940804)

[X.509 Certificate Extensions 6](#_Toc322940805)

[X.509 Extended Key Usage (EKU) 6](#_Toc322940806)

[X.509 Subject Alternative Name (SAN) 6](#_Toc322940807)

[User Principal Name (UPN) 6](#_Toc322940808)

[Trusted Root Store 7](#_Toc322940809)

[Homeland Security Presidential Directive 12 (HSPD-12) 7](#_Toc322940810)

[Federal Information Processing Standard 201 (FIPS 201) 7](#_Toc322940811)

[Personal Identity Verification (PIV) 7](#_Toc322940812)

[Public Key Cryptography for Initial Authentication in Kerberos (RFC 4556, PKINIT) 7](#_Toc322940813)

[United States Government Configuration Baseline (USGCB) 7](#_Toc322940814)

[Secure/Multipurpose Internet Mail Extensions (S/MIME) 7](#_Toc322940815)

[altSecurityIdentities 7](#_Toc322940816)

[Windows Server 2008 Active Directory and Windows 7 Enhancements 8](#_Toc322940817)

[Kerberos PKINIT (RFC 4556) 8](#_Toc322940818)

[800-73 Smart Card Driver 8](#_Toc322940819)

[Online Certificate Status Protocol (OCSP) 8](#_Toc322940820)

[NIST Personal Identity Verification Test Card Program 9](#_Toc322940821)

[Configuring Active Directory for Smart Card Logon and S/MIME Email 10](#_Toc322940822)

[CSD.LAB 2008 Active Directory Configuration 10](#_Toc322940823)

[CSD.LAB Public Key Infrastructure 11](#_Toc322940824)

[CSD.LAB Domain Certificate Stores 12](#_Toc322940825)

[Trusted Root Certification Authorities 12](#_Toc322940826)

[NTAuth 13](#_Toc322940827)

[Intermediate Certification Authorities Store 14](#_Toc322940828)

[CSD.LAB KDC PIV Test Smart Card Certificate Validation Process 15](#_Toc322940829)

[UPN Suffixes 15](#_Toc322940830)

[altSecurityIdentities 16](#_Toc322940831)

[NIST Test PIV Card Authoritative Information Access (AIA) and CRL Distribution Point (CDP) 17](#_Toc322940832)

[KDC’s KRB\_AS\_REP 18](#_Toc322940833)

[CSD.LAB SMTP 18](#_Toc322940834)

[CSD.LAB DNS 18](#_Toc322940835)

[CSD.LAB Test Accounts 18](#_Toc322940836)

[CSD.LAB Workstation Configurations 19](#_Toc322940837)

[XP SP3 (CSD\XPSP3) 20](#_Toc322940838)

[Windows 7 (CSD\Win7-1) 20](#_Toc322940839)

[Windows 7 (CSD\Win7-2) 20](#_Toc322940840)

[Mac OS X 10.6.7 (CSD\MAC) 20](#_Toc322940841)

[Mandriva Linux 2010.2 20](#_Toc322940842)

[UPN Based Smart Card Logon Behavior 21](#_Toc322940843)

[Explicit Logon - Single Smart Card mapped to Multiple Accounts 22](#_Toc322940844)

[Explicit Mapping Workstation Logon 22](#_Toc322940845)

[Explicit Mapping and NTAuth Requirement 23](#_Toc322940846)

[Cross Forest Explicit Mapping Smart Card Logon 25](#_Toc322940847)

[S/MIME Configuration 28](#_Toc322940848)

[Example S/MIME Test Sequence 28](#_Toc322940849)

[Step 1: Digitally Signed Message 29](#_Toc322940850)

[Step 2: Validating Digitally Signed Message 30](#_Toc322940851)

[Step 3: Encrypting Message 31](#_Toc322940852)

[Step 4: Viewing/Validating Encrypted Message 31](#_Toc322940853)

[XP SP3 S/MIME Behavior 32](#_Toc322940854)

[MAC OS X S/MIME Behavior 32](#_Toc322940855)

[References 33](#_Toc322940856)

# Audience

It is assumed that the audience for this document has basic knowledge of Public Key Infrastructure and Smart Card concepts. For more information about these topics see Smart Cards (http://technet.microsoft.com/en-us/library/dd277362.aspx) and How Certificates Work (http://technet.microsoft.com/en-us/library/cc776447(WS.10).aspx).

For topics concerning the Federal PKI Common Policy Root certificate, Extended Key Usage requirements and validation of PIV client authentication certificates for smart card logon, see Deployment of the new Federal Common Policy CA Root Certificate (http://blogs.technet.com/b/pki/archive/2011/03/13/deployment-of-the-new-federal-common-policy-ca-root-certificate.aspx) and HSPD-12 Logical Access Authentication and Active Directory Domains (http://blogs.technet.com/pki/archive/2010/02/10/whitepaper-hspd-12-logical-access-authentication-and-active-directory-domains.aspx). More information about Windows XP SP3 and SHA256 support can be found in the SHA2 and Windows blog entry (http://blogs.technet.com/b/pki/archive/2010/09/30/sha2-and-windows.aspx).

# Terminology

## Public Key Infrastructure (PKI)

The laws, policies, standards, and software that regulate or manipulate certificates and public and private keys. In practice, it is a system of digital certificates, certification authorities (CAs), and other registration authorities that verify and authenticate the validity of each party involved in an electronic transaction.

## Object Identifier (OID)

(1) In the context of an object server, a 64-bit number that uniquely identifies an object.

(2) In the context of a directory service, a number identifying an object class or attribute. Object identifiers are issued by the ITU and form a hierarchy. An OID is represented as a dotted decimal string (for example, "1.2.3.4"). OIDsare used to uniquely identify certificate templates available to the certificate authority (CA). Within a certificate, OIDsare used to identify standard extensions as covered in [RFC3280] section 4.2.1.x, as well as non-standard extensions.

(3) In the Lightweight Directory Access Protocol (LDAP), a sequence of numbers in a format specified by [RFC1778]. In many LDAP directory implementations, an OIDis the standard internal representation of an attribute. In the directory model used in [MS-ADTS], the more familiar ldapDisplayName represents an attribute.

(4) In the context of Abstract Syntax Notation One (ASN.1), an object identifier, as specified in [ITUX680].

(5) A variable-length identifier from a namespace administered by the ITU. Objects, protocols, and so on that make use of ASN.1 or Basic Encoding Rules (BER), Distinguished Encoding Rules (DER), or Canonical Encoding Rules (CER) encoding format leverage identities from the ITU.

## X.509

An ITU-T standard for public key infrastructure subsequently adapted by the IETF, as specified in [RFC3280].

## X.509 Certificate Extensions

X.509 version 3 certificate fields that provides the means to associate additional attributes used in determining the validity of an identity. Each extension has an associated OID and can be marked as critical or non-critical. If an extension is marked critical, the system validating the certificate must understand the extension or else reject the certificate.

## X.509 Extended Key Usage (EKU)

Defines the intended purpose / application for which a certificate can be used. This is synonymous with the Microsoft Enhanced Key Usage [OID 2.5.29.37].

## X.509 Subject Alternative Name (SAN)

Extends a certificate’s ability to identify an entity beyond the Subject field. This field is used to map a smart cards user’s certificate to their Active Directory user object. An HSPD-12 PIV Client Authentication certificate’s Subject Alternate Name field will contain the user’s organizational user principal name [OID 2.5.29.17].

## User Principal Name (UPN)

A user account name (sometimes referred to as the user logon name) and a domain name identifying the domain in which the user account is located. This is the standard usage for logging on to a Windows domain. The format is: someone@example.com (in the form of an e-mail address). In Active Directory, the UPN is the userPrincipalName attribute of the account object, as specified in [MS-ADTS]. The UPN must be unique within the forest and between forests when using a forest trust.

## Trusted Root Store

A store within the computer in which the certificates of all root CAs are held. The root keys are typically encoded within self-signed certificates, and the contents of a trust root are therefore sometimes called root certificates. In Windows, there are two types of stores. First, is the per-user/per-service store that contains certificates and trust roots that are specifically trusted by that user/service. Second, is the computer store which contains trusted roots that all processes, users, and services on the computer trust. By default, regular users (without administrative rights) have read/write access to their personal certificate store, but only have read-only rights to the computer certificate store.

## Homeland Security Presidential Directive 12 (HSPD-12)

Presidential directive signed on August 27, 2004 requiring a common identity standard for federal employees and contractors for the use of gaining physical access to controlled facilities and logical access to controlled information systems.

## Federal Information Processing Standard 201 (FIPS 201)

This standard specifies the architecture and technical requirements for a common identification standard for the HSPD-12 directive.

## Personal Identity Verification (PIV)

As defined in FIPS 201, PIV-I identifies the control objectives in vetting an applicant’s identity. PIV-II addresses the technical interoperability requirements of HSPD 12.

## Public Key Cryptography for Initial Authentication in Kerberos (RFC 4556, PKINIT)

Kerberos protocol extensions used to integrate PKI into the Kerberos authentication exchange. Microsoft Windows operating systems use the Kerberos PKINIT protocol extension to establish a secure method in the exchange of the initial Kerberos Authentication Request / Reply (KRB\_AS\_REQ / KRB\_AS\_REP).

## United States Government Configuration Baseline (USGCB)

The United States Government Configuration Baseline is an OMB mandated security configuration. USGCB settings exist for the Microsoft Windows 7, Vista and XP operating systems.

## Secure/Multipurpose Internet Mail Extensions (S/MIME)

S/MIME (Secure/Multipurpose Internet Mail Extensions) provides a consistent way to send and receive secure email. S/MIME provides cryptographic security services for electronic messaging applications authentication, message integrity and non-repudiation of origin (using digital signatures) and privacy and data security (using encryption).

## altSecurityIdentities

Active Directory attribute that contains mappings for X.509 certificates or external Kerberos user accounts to a user for the purpose of authentication.

# Windows Server 2008 Active Directory and Windows 7 Enhancements

Starting with Windows Vista significant improvements were made to Active Directory Certificate Services (ADCS), Cryptographic API (CAPI), smart card support and the Kerberos protocol. Features that increase HSPD-12 smart card capabilities include:

### Kerberos PKINIT (RFC 4556)

Microsoft’s implementation of the PKINIT standard [MS-PKCA] supports the PA-PK-AS-REQ pre-authentication message format. The most common authentication method is the Kerberos Key Distribution Center (KDC) maps the client authentication certificate’s userPrincipleName (contained within the Subject Alternate Name field) to the user account’s UPN. Active Directory 2008 supports explicit mapping to associate a certificate to user account(s) based upon certificate information stored within the user’s altSecurityIdentities attribute. The following table lists the available certificate fields to Active Directory user object’s atlSecurityIdentities mappings.

|  |  |
| --- | --- |
| **Certificate Field** | **altSecurityIdentities** |
| Subject and Issuer Name | X509:<I>*issuer*<S>*subject* |
| Subject | X509:<S>*subject* |
| Issuer and Serial Number | X509:<I>issuer<SR>*serial\_number* |
| Subject Key Identifier | X509:<SKI>*subject\_key\_identifier* |
| SHA1 hash of public key | X509:<SHA1-PUKEY> *SHA1 hash of public key* |
| RFC822 | X509:<RFC822>*email\_address* |

Table 1: altSecurityIdentities certificate mapping

### 800-73 Smart Card Driver

The Windows 7 Base Cryptographic Service Provider (CSP) includes NIST SP800-73 support allowing the use of PIV smart cards for smart card logon, digital signature and encryption without requiring additional middleware. The smart card minidriver was developed to the 800-73-2 specifications. The PIV Discovery Object (optional) and Key History (800-73-3 update) features are not supported at this time. More information can be found at Introducing Smart Card Plug and Play (http://technet.microsoft.com/en-us/library/dd560638(WS.10).aspx).

### Online Certificate Status Protocol (OCSP)

Beginning with Windows Vista, OCSP client functionality was included in the Windows operating system. By default, when Windows performs certificate validation it will first attempt to use OCSP but will fall back to standard CRL lookups if the responder is not available. The only exception to this is (by default) when Windows caches 50 time-valid OCSP responses which have the same CRL path. Once this threshold is reached, Windows will attempt to download the CRL and use that to validate certificates for the lifetime of that CRL.

In Windows Server 2008, an OCSP responder is provided to answer these requests. Windows Server 2008 OCSP responder can answer requests for certificates issued by any standards compliant CA.

# NIST Personal Identity Verification Test Card Program

The National Institute of Standards and Technology created the Personal Identity Verification Test Cards Program to facilitate PIV compliant application and middleware development. The goal of the project is to provide industry with NIST validated sample smart cards that are compliant with current and future PIV standards. Contact NIST (<http://www.nist.gov>) to purchase the set of sixteen PIV Test Cards.

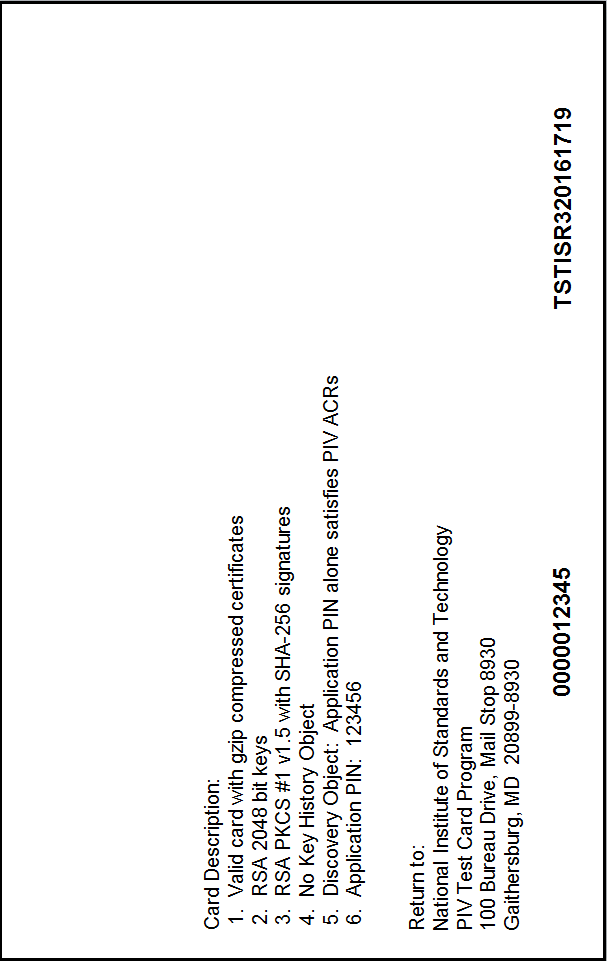
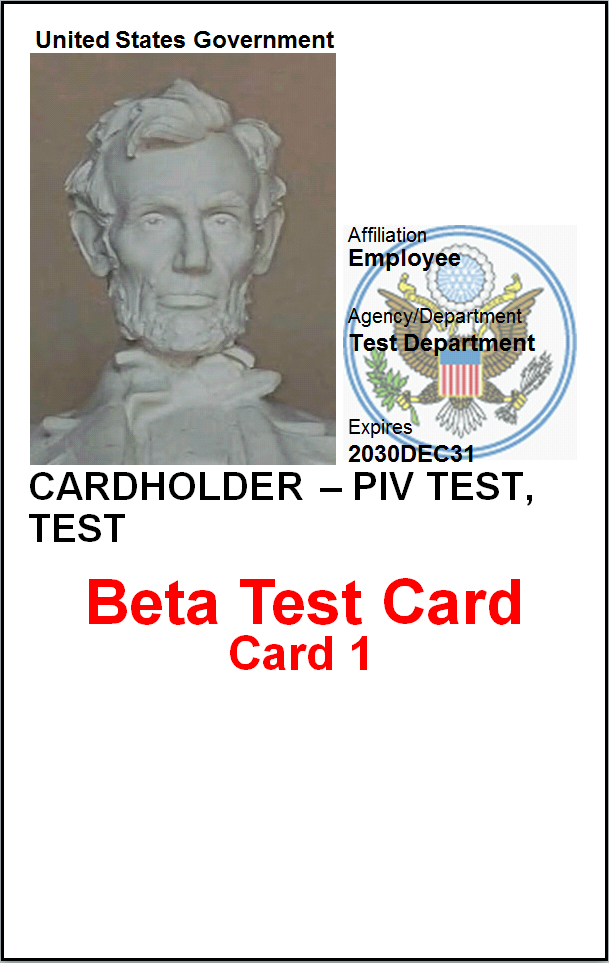


Figure 1: NIST PIV Test Card 1

The NIST PIV Test Cards are used to test the various authentication and S/MIME scenarios outlined in this document. Detailed steps on how to configure Windows Server 2008 Active Directory, Windows 7 and Office 2010 to perform the authentication and S/MIME tests and associated results are included.

# Configuring Active Directory for Smart Card Logon and S/MIME Email

The following sections describe how to configure Windows Server 2008 R2 Active Directory Domain Services to allow smart card logon and S/MIME email exchange with the NIST PIV Test Cards. Use the following configuration guide to determine the steps required for UPN mapping, multiple account (explicit) mappings and cross-forest smart card logon.



Figure 2: Configuration Steps Based Upon Authentication Method

## CSD.LAB 2008 Active Directory Configuration

A Windows Server 2008 R2 Active Directory Domain (CSD.LAB) was created to provide a Kerberos Realm for the authentication of domain user accounts using the PIV Test Cards. An internal PKI was implemented to provide the smart card logon required domain controller certificate. Workstations with various operating systems were added to the CSD.LAB domain and all systems were routable to the Internet.



Figure 3: CSD Lab Configuration

## CSD.LAB Public Key Infrastructure

Smart card logon within Windows Active Directory domains requires the Kerberos protocol extensions used to integrate PKI into the Kerberos authentication exchange. Microsoft Windows operating systems use the Kerberos PKINIT protocol extension to establish a secure method in the exchange of the initial Kerberos Authentication Request / Reply (KRB\_AS\_REQ / KRB\_AS\_REP). The Kerberos Key Distribution Center (domain controller) encrypts the KRB\_AS\_REP message with the domain controller’s certificate issued by the csd.lab PKI issuing certification authority (issuingca-ca.csd.lab). Windows Enterprise Issuing Certification Authorities use the Kerberos Authentication certificate template to issue certificates to Windows 2008 domain controllers to facilitate the PKINIT process. The Subject Alternate Name field in the Kerberos Authentication certificate contains a DNS listing of the Active Directory Kerberos Realm. The dc1.csd.lab domain controller’s Kerberos Authentication certificate (below) was obtained from the enterprise issuing CA through the auto-enrollment protocol.

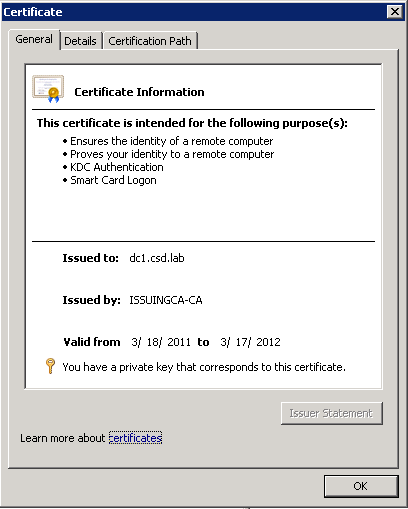
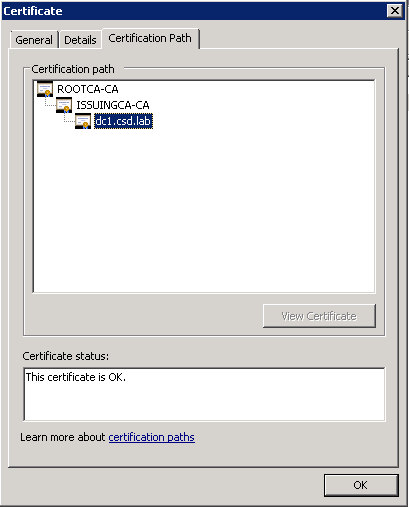
 

Figure 4: Domain Controller’s Kerberos Authentication certificate

## CSD.LAB Domain Certificate Stores

### Trusted Root Certification Authorities

The user’s authenticating workstation must trust the KDC certificate’s root trust point (rootca-ca) to successfully validate the KDC’s encrypted KRB\_AS\_REP message. The root certificate should be placed within the domain’s Trusted Root Certification Authorities store which is then distributed to all domain joined systems via group policy. Use the certutil.exe application to publish the certificate to the root store with the command ***certutil –dspublish –f rootca-ca.cer***.

The PIV Test Cards’ root certificate (Test Trust Anchor for Test PIV Cards) must be in the domain controller’s Trusted Root Certification Authorities store. It is recommended to publish this trust point to the enterprise root store which is then placed into the domain controller’s store via group policy (***certutil –dspublish –f Self-signedTrustAnchorCertificate.cer***). NIST does not publish this certificate in the subordinate issuing CA’s Authority Information Access location (<http://smime2.nist.gov/PIVTest/CACertsIssuedToTrustAnchor.p7c>). It is a common practice for relying parties to obtain root trust point certificates via a secure out-of-band mechanism. The Federal Common Policy Root CA follows this practice as well.

It should be noted that in order to publish certificates to the enterprise certificate stores the command prompt window must be in administrator mode and the account must be a member of the domain’s Enterprise Administrators group. Confirm group membership with the ***whomai /groups*** command.

Use the ***certutil –viewstore –enterprise root*** command to view the certificates in the domain’s Trusted Root Certification Authorities store.

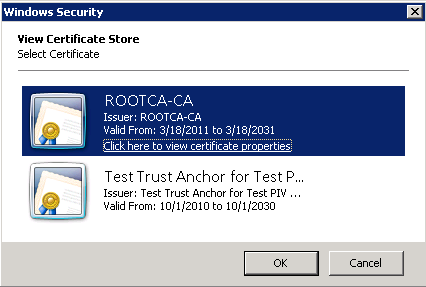


Figure 5: CSD.LAB Enterprise Trusted Root Certification Authorities Store

### NTAuth

The Active Directory NTAuth Certificate Store is used to ensure only certificates issued from a known issuing certification authority can perform smart card logon within the domain. This prevents the ability of a fraudulent user’s smart card, containing a valid userPrincipalName within the Subject Alternative Name field, issued from a non-trusted issuing CA logging onto the domain. There are other Active Directory protections involved in this scenario which are outside of the scope of this document.

Trusted issuing certification authorities must be published to the domain’s NTAuth store using the ***certutil –dspublish –f <issuing\_ca>.cer NTAuthCA*** command or using the Enterprise PKI MMC Snap-In. Windows Enterprise Certification Authorities will automatically publish their certificates to the domain’s NTAuth store at the time of installation. The PIV Test Card issuing certification authorities must be published using the following commands from an enterprise administrator account:

* ***certutil –dspublish –f ECCP256IssuingCACertificate.cer NTAuthca***
* ***certutil –dspublish –f ECCP384IssuingCACertificate.cer NTAuthca***
* ***certutil –dspublish –f RSA2048IssuingCACertificate.cer NTAuthca***
* ***certutil –dspublish –f RSA2048PIV-IIssuingCACertificate.cer NTAuthca***
* ***certutil –dspublish –f RSA3072IssuingCACertificate.cer NTAuthca***

The KDC certificate’s issuing authority certificate (issuingca-ca.csd.lab) is required in the domain’s NTAuth certificate store. The domain controller must have the domain’s NTAuth store containing the KDC’s issuing CA’s certificate and the smartcards issuing CAs’ certificates downloaded before smartcard logon can occur. From the domain controller issue the ***certutil –pulse*** command followed by ***gpupdate /force*** to force the download of the required certificates.

Use the ***certutil –viewstore –enterprise NTAuth*** command to view the certificates in the domain’s NTAuth store.

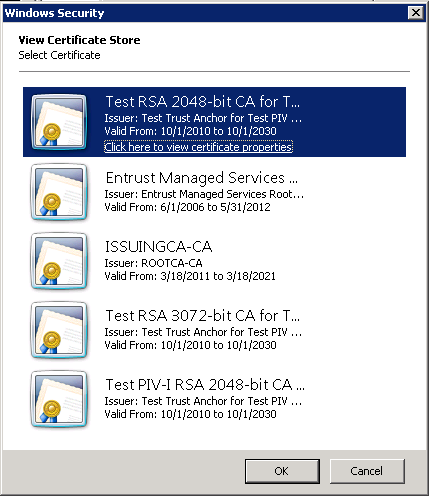


Figure 6: CSD.LAB NTAuth Store

### Intermediate Certification Authorities Store

Although not technically required, in order to improve the certificate validation process on the KDC, publish the PIV smart cards’ issuing CAs certificates to the domain’s intermediate certificate store. Issue the following command to publish the NIST PIV Test Cards’ issuing CAs’ certificates to the domain’s intermediate certificate store.

* ***certutil –dspublish –f ECCP256IssuingCACertificate.cer subCA***
* ***certutil –dspublish –f ECCP384IssuingCACertificate.cer subCA***
* ***certutil –dspublish –f RSA2048IssuingCACertificate.cer subCA***
* ***certutil –dspublish –f RSA2048PIV-IIssuingCACertificate.cer subCA***
* ***certutil –dspublish –f RSA3072IssuingCACertificate.cer subCA***

## CSD.LAB KDC PIV Test Smart Card Certificate Validation Process

The Kerberos Key Distribution Center (i.e. domain controller) receives the user’s client authentication certificate via the KRB\_AS\_REQ packet and performs the user account mapping and certificate validation.

### UPN Suffixes

The domain controller will find the user’s account based upon the userPrincipalName in the certificate’s Subject Alternative Name field. The PIV Test Cards contain UPN values of <user>@upn.example.net and <user>@upn.example.com. Perform the following steps to add the upn.example.net and upn.example.com to the CSD.LAB’s alternative UPN suffixes:

* Launch Active Directory Domain and Trusts snap-in
* Right click on the top level Active Directory Domains and Trusts
* Select Properties
* In UPN Suffixes tab add “upn.example.net” and “upn.example.com” domain suffixes

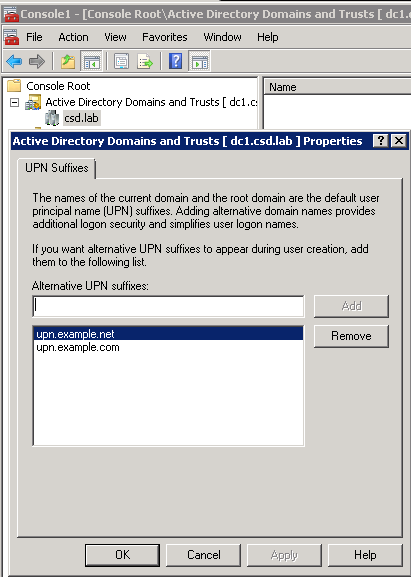


Figure 7: CSD.LAB UPN Suffixes

When creating user accounts the UPN value is implicitly created. For example when csd\testcard16 account is created the UPN value will automatically be set to [testcard16@csd.lab](mailto:testcard16@csd.lab). To change the UPN value select Properties on the user account and go to the Account tab. Set the “user logon name” to the user name in the certificate’s UPN (pivtestcardholder) and select the UPN suffix (upn.example.com) from the right hand drop down menu. The “user logon name (pre-Windows 2000)” can remain as testcard16.

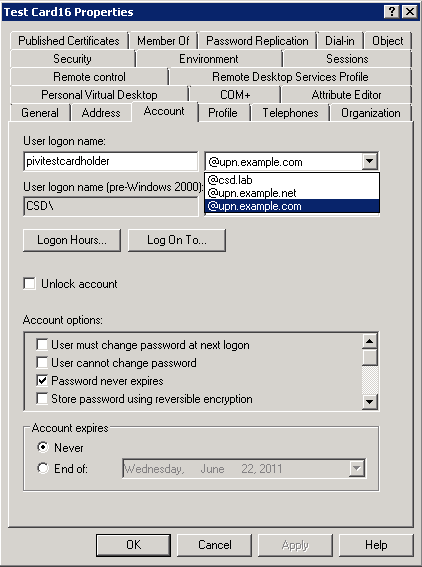


Figure 8: Test Cardholder XVI (csd\testcard16) UPN mapping

### altSecurityIdentities

For the PIV Test Cards that do not contain UPN values (e.g. Test Card2, Test Cardholder Jr. (affiliate)) within the Subject Alternative Name field, Active Directory 2008 allows alternative account mappings using the altSecurityIdentities user attribute. This attribute contains the user’s certificate information that is used by the Kerberos Authentication Service to identify the associated Active Directory user account. Active Directory Users and Computers snap-in’s Name Mappings task (enable Advanced Features view) populates the user account’s altSecurityIdentities attribute with the client authentication certificate’s information. For example to map Test Card2’s client authentication certificate to the CSD\testcard2 account perform the following steps:

* Obtain Test Cardholder Jr. (affiliate) client authentication certificate
* Start Active Directory Users and Computers (ADUC) MMC snap-in
* Enable Advanced Features within the ADUC View menu
* Find CSD\testcard2 account
* Right click on CSD\testcard2 account
* Select Name Mappings
* In X.509 tab select Add
* Open the Test Cardholder Jr. (affiliate) client authentication certificate

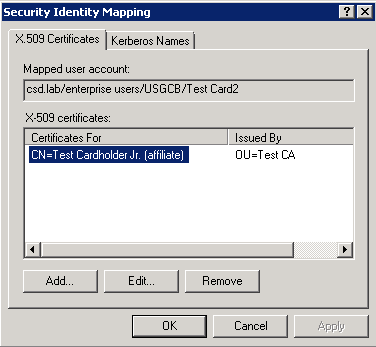


Figure 9: CSD\testcard2 User Name Mapping

The default mapping method used by Active Directory Users and Computers MMC snap-in is

Subject and Issuer (X509:<I>issuer<S>subject). To change the altSecurityIdentities mapping method use the “Attribute Editor” feature within the user properties. Refer to HowTo: Map a user to a certificate via all the methods available in the altSecurityIdentities attribute for more information (http://blogs.msdn.com/b/spatdsg/archive/2010/06/18/howto-map-a-user-to-a-certificate-via-all-the-methods-available-in-the-altsecurityidentities-attribute.aspx).

### NIST Test PIV Card Authoritative Information Access (AIA) and CRL Distribution Point (CDP)

The KDC will perform the user’s client authentication certificate chaining and validation process. Therefore the domain controller must have the client authentication certificate’s root trust point certificate (Test Trust Anchor for Test PIV Cards) in its Trusted Root Certification Authorities store. Publishing the root trust certificate to the domain’s trusted root store as described in [Trusted Root Certification Authorities section](#_Trusted_Root_Certification) will fulfill this requirement.

The KDC must be able to route to the NIST Test PIV Cards’ AIA and CDPs:

* AIA: <http://smime2.nist.gov/PIVTest>
* AIA: ldap://smime2.nist.gov
* CDP: <http://smime2.nist.gov/PIVTest>
* CDP: ldap://smime2.nist.gov

The Test PIV Card certificates contain an OCSP entry within the Authority Information Access field (<http://seclab7.ncsl.nist.gov>). Windows Vista and higher operating systems have an OCSP client built into the operating system. To trouble shoot the certificate validation process, enable the CAPI2 eventlog on a Windows Vista or higher operating system

* Start Event Viewer MMC (eventvwr.msc)
* Application and Services \ Microsoft \ Windows \ CAPI2
* Right click and select “enable”

To test a domain controller’s ability to chain and validate a NIST PIV Test Smart Card copy the client authentication certificate to the domain controller and issue the command ***certutil –verify –urlfetch <piv\_test\_client\_authentication\_cert>.crt***. The domain controller will build the certificate’s chain of trust and check for validity in real time. To test the smart card logon application policy (1.3.6.1.4.1.311.20.2.2) for the chain of trust issue the command ***certutil –verify –urlfetch <piv\_test\_client\_authentication\_cert>.crt 1.3.6.1.4.1.311.20.2.2***

### KDC’s KRB\_AS\_REP

When a user account is found and the client authentication certificate is validated, the KDC returns to the authenticating workstation a Ticket Granting Ticket that is encrypted with the domain’s krbtgt account password and then encrypted with the Kerberos Authentication certificate’s associated private key. The authenticating workstation decrypts the EncryptedContent of the KRB\_AS\_REP packet and validates the KDC’s certificate. The workstation’s Trusted Root Certification Authorities store must contain the root trust point of the domain controller Kerberos Authentication certificate (rootca-ca). The root trust point was published to domain’s Trusted Root Certification Authorities store and distributed via group policy.

## CSD.LAB SMTP

The Mandriva 2010.2 Linux workstation served as the SMTP and Cyrus POP3 server for S/MIME tests.

## CSD.LAB DNS

In addition to the CSD.LAB DNS zone a primary zone was created for example.com to route mail to the @mail.example.com addresses to the Mandriva Linux SMTP server.

## CSD.LAB Test Accounts

The following test accounts were created for each smart card tested:

|  |  |  |  |
| --- | --- | --- | --- |
| **displayName** | **sAMAccountName** | **userPrincipalName** | **altSecurityIdentities** |
| Test Card1 | testcard1 | [32015465737401@upn.example.com](mailto:32015465737401@upn.example.com) | X509:<I>C=US,O=Test Certificates 2010,OU=Test CA,CN=Test RSA 2048-bit CA for Test PIV Cards<S>C=US,O=Test Government,OU=Test Department,OU=Test Agency,CN=Test Cardholder |
| Test Card2 | testcard2 | [testcard2@csd.lab](mailto:testcard2@csd.lab) | X509:<I>C=US,O=Test Certificates 2010,OU=Test CA,CN=Test RSA 3072-bit CA for Test PIV Cards<S>C=US,O=Test Government,OU=Test Department,OU=Test Agency,CN=Test Cardholder Jr. (affiliate) |
| Test Card3 | testcard3 | [testcard3@csd.lab](mailto:testcard3@csd.lab) | X509:<I>C=US,O=Test Certificates 2010,OU=Test CA,CN=Test RSA 2048-bit CA for Test PIV Cards<S>C=US,O=Test Government,OU=Test Department,OU=Test Agency,SERIALNUMBER=D650185855E56DC8127985A1645B906E7880C08286501843FC |
| Test Card4 | testcard4 | [32011152472674@upn.example.com](mailto:32011152472674@upn.example.com) | X509:<I>C=US,O=Test Certificates 2010,OU=Test CA,CN=Test ECC P-256 CA for Test PIV Cards<S>C=US,O=Test Government,OU=Test Department,OU=Test Agency,CN=Test E. Cardholder IV |
| Test Card5 | testcard5 | [testcard5@csd.lab](mailto:testcard5@csd.lab) | X509:<I>C=US,O=Test Certificates 2010,OU=Test CA,CN=Test ECC P-384 CA for Test PIV Cards<S>C=US,O=Test Government,OU=Test Department,OU=Test Agency,CN=Test E. Cardholder V |
| Test Card6 | testcard6 | [testcard6@csd.lab](mailto:testcard6@csd.lab) | X509:<I>C=US,O=Test Certificates 2010,OU=Test CA,CN=Test RSA 2048-bit CA for Test PIV Cards<S>C=US,O=Test Government,OU=Test Department,OU=Test Agency,SERIALNUMBER=D65018582214EC29D721CDA1685899207990B49086501857E4 |
| Test Card7 | testcard7 | [testcardholder7@upn.example.net](mailto:testcardholder7@upn.example.net) | X509:<I>C=US,O=Test Certificates 2010,OU=Test CA,CN=Test RSA 2048-bit CA for Test PIV Cards<S>C=US,O=Test Government,OU=Test Department,OU=Test Agency,CN=Test Cardholder VII |
| Test Card8 | testcard8 | [32017525816451@upn.example.com](mailto:32017525816451@upn.example.com) | X509:<I>C=US,O=Test Certificates 2010,OU=Test CA,CN=Test RSA 2048-bit CA for Test PIV Cards<S>C=US,O=Test Government,OU=Test Department,OU=Test Agency,CN=Test Cardholder VIII |
| Test Card9 | testcard9 | [32012243747282@upn.example.com](mailto:32012243747282@upn.example.com) | X509:<I>C=US,O=Test Certificates 2010,OU=Test CA,CN=Test RSA 2048-bit CA for Test PIV Cards<S>C=US,O=Test Government,OU=Test Department,OU=Test Agency,CN=Test Cardholder IX (affiliate) |
| Test Card10 | testcard10 | [testcard10@csd.lab](mailto:testcard10@csd.lab) | X509:<I>C=US,O=Test Certificates 2010,OU=Test CA,CN=Test RSA 2048-bit CA for Test PIV Cards<S>C=US,O=Test Government,OU=Test Department,OU=Test Agency,CN=Test Cardholder X |
| Test Card11 | testcard11 | [testcard11@csd.lab](mailto:testcard11@csd.lab) | X509:<I>C=US,O=Test Certificates 2010,OU=Test CA,CN=Test RSA 2048-bit CA for Test PIV Cards<S>C=US,O=Test Government,OU=Test Department,OU=Test Agency,CN=Test Cardholder |
| Test Card 12 | testcard12 | [32014001354205@upn.example.com](mailto:32014001354205@upn.example.com) | X509:<I>C=US,O=Test Certificates 2010,OU=Test CA,CN=Test RSA 2048-bit CA for Test PIV Cards<S>C=US,O=Test Government,OU=Test Department,OU=Test Agency,CN=Test Cardholder XII |
| Test Card13 | testcard13 | [testcard13@upn.example.com](mailto:testcard13@upn.example.com) | X509:<I>C=US,O=Test Certificates 2010,OU=Test CA,CN=Test RSA 2048-bit CA for Test PIV Cards<S>C=US,O=Test Government,OU=Test Department,OU=Test Agency,CN=Test Cardholder XIII |
| Test Card14 | testcard14 | [32016091935084@upn.example.com](mailto:32016091935084@upn.example.com) | X509:<I>C=US,O=Test Certificates 2010,OU=Test CA,CN=Test RSA 2048-bit CA for Test PIV Cards<S>C=US,O=Test Government,OU=Test Department,OU=Test Agency,CN=Test Cardholder XIV |
| Test Card15 | testcard15 | [testcard15@csd.lab](mailto:testcard15@csd.lab) | X509:<I>C=US,O=Test Certificates 2010,OU=Test CA,CN=Test ECC P-256 CA for Test PIV Cards<S>C=US,O=Test Government,OU=Test Department,OU=Test Agency,CN=Test E. Cardholder XV |
| Test Card16 | testcard16 | [pivitestcardholder@upn.example.com](mailto:pivitestcardholder@upn.example.com) | X509:<I>C=US,O=Test Certificates 2010,OU=Test CA,CN=Test PIV-I RSA 2048-bit CA for Test PIV Cards<S>C=US,O=Test Government,OU=Test Department,OU=Test Agency,CN=Test Cardholder XVI |

Table 2: Test Card csd.lab Active Directory accounts

## CSD.LAB Workstation Configurations

The United States Government Configuration Baseline was applied to all user and workstation accounts via domain group policies. One policy deviation was made. To ensure all authentication attempts occurred on the domain controller, all workstations’ cached credentials setting were set to “0.” Modify the USGCB Windows 7 and XP Computer Settings GPOs’ Computer Configuration \ Policies \ Windows Settings \ Security Settings \ Local Policies \ Security Options : Interactive logon = 0. All systems were completely patched.

### XP SP3 (CSD\XPSP3)

* Windows XP Professional edition
* Outlook 2010
* ActivIdentity Client (PIV smart card middleware)

### Windows 7 (CSD\Win7-1)

* Windows 7 Professional edition
* Outlook 2007

### Windows 7 (CSD\Win7-2)

* Windows 7 Professional edition
* Outlook 2010

The following domain level group policy settings were applied to the Win7-2 workstation:

|  |  |  |
| --- | --- | --- |
| **Policy** | **Path** | **Reason** |
| Allow user name hint : Enabled | Computer Configuration \ Policies \ Administrative Templates \ Windows Components \ Smart Card | Send Kerberos pre-authentication data to allow for altSecurityIdentities name mappings for client authentication certificates that do not contain UPN values within the Subject Alternate Name field |
| Allow certificates with no extended key usage certificate attribute : Enabled | Computer Configuration \ Policies \ Administrative Templates \ Windows Components \ Smart Card | Allow smart card logon with client authentication certificates that do not contain the Smart Card Logon (1.3.6.1.4.1.311.20.2.2) OID in the Enhanced Key Usage field |
| Allow ECC certificates to be used for logon and authentication | Computer Configuration \ Policies \ Administrative Templates \ Windows Components \ Smart Card | Allows elliptic curve cryptography certificates on the smart card to be used for domain logon (note: not supported at this time) |

Table 3: Win7-2 additional group policy settings

### Mac OS X 10.6.7 (CSD\MAC)

The MAC OS X client was used only during the S/MIME testing using Microsoft Office 2011.

### Mandriva Linux 2010.2

The Mandriva Linux workstation was configured as the mail.example.com SMTP and POP3 server. The Thunderbird email client was used.

# UPN Based Smart Card Logon Behavior

The following table contains the results of UPN based smart card logon tests. Several NIST PIV Test Cards contain faults that will cause logon failures. For example testcard10’s certificate is revoked. All smart card logons were performed from the physical Windows workstations (XPSP3, Win7-1 & Win7-2) with USB attached smart card readers. The reason for the resulting logon behavior is provided.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Smart Card** | **XPSP3** | **Win7-1** | **Win7-2** | **Pin** | **Reason** |
| testcard1 | Success | Success | Success | 123456 | SHA256 supported |
| testcard2 | Fail | Fail | Success | 123456 | No EKU or UPN in client authentication certificate, requires Smart Card group policies to allow no EKU logon and send Kerberos pre-authentication data for altSecurityIdentities mappings |
| testcard3 | Fail | Fail | Success | 90909090 | Discovery Object is not implemented by 800-73 mini driver therefore PIV Card Application PIN is used. No smart card OID in the EKU and UPN in client authentication certificate, requires Smart Card group policies to allow no EKU logon and send Kerberos pre-authentication data for altSecurityIdentities mappings |
| testcard4 | Fail | Fail | Fail | n/a | Elliptic curve cryptography smart card certificates cannot be read by the 800-73 mini driver at this time |
| testcard5 | Fail | Fail | Fail | n/a | Elliptic curve cryptography smart card certificates cannot be read by the 800-73 mini driver at this time |
| testcard6 | Fail | Fail | Success | 123456 | No EKU or UPN in client authentication certificate, requires Smart Card group policies to allow no EKU logon and send Kerberos pre-authentication data for altSecurityIdentities mappings |
| testcard7 | Success | Success | Success | 90909090 | Discovery Object is not implemented by 800-73 mini driver therefore PIV Card Application PIN is used |
| testcard8 | Fail | Fail | Success | 123456 | No smart card OID in the EKU client authentication certificate, requires Smart Card group policies to allow no EKU logon |
| testcard9 | Fail | Fail | Fail | 123456 | Client authentication certificate expired |
| testcard10 | Fail | Fail | Fail | 123456 | Client authentication certificate was revoked |
| testcard11 | Fail | Fail | Fail | 123456 | Client authentication certificate was modified after issuance |
| testcard12 | Success | Success | Success | 123456 | SHA256 supported |
| testcard13 | Fail | Fail | Fail | 123456 | Client authentication certificate expired |
| testcard14 | Success | Success | Success | 123456 | SHA256 supported |
| testcard15 | Fail | Fail | Fail | n/a | Elliptic curve cryptography smart card certificates cannot be read by the 800-73 mini driver at this time |
| testcard16 | Success | Success | Success | 123456 | SHA256 supported |

Table 4: PIV Test Card smart card logon behavior

# Explicit Logon - Single Smart Card mapped to Multiple Accounts

A significant feature of the Windows 7 and Active Directory 2008 is the ability to map a single certificate to multiple accounts within the domain. For example, a user is able to log on to a standard user account and also is able to log on to a second administrative account with the same smart card client authentication certificate. The mapping is done using the user account’s altSecurityIdentities attribute mapping to the certificate properties as outlined in table 1. Since each user account has a unique account name, enable the X509Hints group policy setting to provide the user with a logon field to supply the name of the account to authenticate to. Windows Server 2008 domain controllers have the ability to ignore the client authentication certificate’s UPN value. To ignore a certificate’s UPN value in the Subject Alternate Name extension the KDC must have the following registry entry:

|  |  |  |  |
| --- | --- | --- | --- |
| **Registry Path** | **Key** | **Type** | **Value** |
| HKey\_Local\_Machine\System\CurrentControlSet\Services\KDC | UseSubjectAltName | DWORD | 0 |

Table 5: KDC registry entry to ignore certificate UPN value

To allow explicit smart card logon with certificates that contain an UPN value in the Subject Alternate Name field the KDCs must be instructed to ignore the certificate’s UPN value. Only certificates without UPN values can be used to map to multiple accounts if the UseSubjectAltName registry setting is not set on the KDC. NIST PIV Test Cards without UPN values are Test Card2, Test Card3 and Test Card6. Refer to How to disable the Subject Alternate Name for UPN mapping article (http://technet.microsoft.com/en-us/library/ff520074(WS.10).aspx).

## Explicit Mapping Workstation Logon

The following tests were performed on the Win7-2 workstation, user name hint group policy applied, to demonstrate multiple account mapping smart card logon. Test Card1 was used in the following tests since it is similar to FIPS 201 PIV-II compliant smart cards available today. Test Card1 contains an UPN value within the SAN therefore the domain controller’s registry was modified to ignore UPN mapping. The accounts used were CSD\testcard1 and CSD\testcard1\_admin.

|  |  |  |  |
| --- | --- | --- | --- |
| **AD Account** | **Subject Alternate Name** | **AD userPrincipalName** | **AD altSecurityIdentities** |
| testcard1 | Other Name:  Principal Name=32015465737401@upn.example.com  Other Name:  2.16.840.1.101.3.6.6=04 19 d6 50 18 58 28 9d 6d ca cc 93 25 a1 68 59 a4 69 27 c9 d4 5c 86 50 18 43 e2 | [32015465737401@upn.example.com](mailto:32015465737401@upn.example.com) | X509:<I>C=US,O=Test Certificates 2010,OU=Test CA,CN=Test RSA 2048-bit CA for Test PIV Cards<S>C=US,O=Test Government,OU=Test Department,OU=Test Agency,CN=Test Cardholder |
| testcard1\_admin | Other Name:  Principal Name=32015465737401@upn.example.com  Other Name:  2.16.840.1.101.3.6.6=04 19 d6 50 18 58 28 9d 6d ca cc 93 25 a1 68 59 a4 69 27 c9 d4 5c 86 50 18 43 e2 | Testcard1\_admin@csd.lab | X509:<I>C=US,O=Test Certificates 2010,OU=Test CA,CN=Test RSA 2048-bit CA for Test PIV Cards<S>C=US,O=Test Government,OU=Test Department,OU=Test Agency,CN=Test Cardholder |

Table 6: Explicit Mapping Account Configuration

In the following tests the value in the X509Hint field was supplied in the username hint field on the Windows Logon screen. The results of the explicit logon for testcard1 are as follows:

|  |  |  |  |
| --- | --- | --- | --- |
| Smart Card | Pin | X509Hint | Result |
| testcard1 | 123456 | Testcard1 | Authenticated to the csd\testcard1 account |
| testcard1 | 123456 | Testcard1\_admin | Authenticated to the csd\testcard1\_admin account |
| testcard1 | 123456 | <not supplied> | Authenticated to the csd\testcard1 account (fallback to UPN based mapping) |

Table 7: Explicit Mapping Logon Results

Explicit mapping can be performed with the Remote Desktop Protocol (RDP).

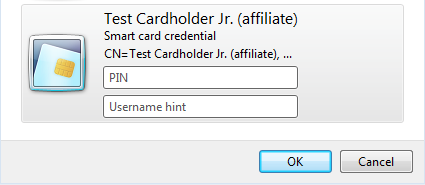


Figure 10: RDP X509Hint logon

## Explicit Mapping and NTAuth Requirement

The Active Directory NTAuth Certificate Store is used to ensure only certificates issued from a known issuing certification authority can perform smart card logon within the domain. Certain explicit mapping methods do not check the NTAuth store for the user certificate’s issuing CA certificate. They are:

* Subject and Issuer
* Subject Key Identifier
* Public Key SHA1 Hash
* Issuer, Subject & Serial Number

Explicit mapping methods that require the user certificate’s issuing CA certificate in the NTAuth store are:

* Subject
* RFC822

To remove an issuing CA from the enterprise NTAuth certificate store issue the command ***certutil –viewdelstore –enterprise NTAuth***, select the certificate then select OK. The pkiview.msc snap-in can also be used to remove certificates from the enterprise stores. Ensure the certificate is removed from the KDC by issuing the ***certutil –pulse*** and ***gpupdate /force*** commands.

The following test was performed on the Win7-2 workstation, user name hint group policy applied, using the Test Card2 smart card since it does not contain an UPN value within the Subject Alternate Name field. The Test RSA 3072-bit CA for Test PIV Cards issuing CA’s certificate was removed from the enterprise NTAuth Certificate Store. In the following tests the value in the X509Hint field was supplied in the username hint field on the Windows Logon screen.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Smart Card** | **Pin** | **X509Hint** | **altSecID** | **Result** |
| Testcard2 | 123456 | Testcard2 | X509:<S>C=US,O=Test Government,OU=Test Department,OU=Test Agency,CN=Test Cardholder Jr. (affiliate) | Failed. “The system could not log you on. An untrusted certificate authority was detected while processing the smart card certificate used for authentication.” |
| Testcard2\_admin | 123456 | Testcard2\_admin | X509:<I>C=US,O=Test Certificates 2010,OU=Test CA,CN=Test RSA 3072-bit CA for Test PIV Cards<S>C=US,O=Test Government,OU=Test Department,OU=Test Agency,CN=Test Cardholder Jr. (affiliate) | Authenticated to the CSD\testcard2\_admin account |

Table 8: NTAuth Requirement for Explicit Mapping Logon

# Cross Forest Explicit Mapping Smart Card Logon

Explicit mapping smart card logon can occur across Active Directory forest trusts. For the following tests two domains were created (F.Internal and G.Internal) and a two way forest trust was established. The domains were configured as outlined in the Figure 2: Configuration Steps Based upon Authentication Method diagram. The internal PKI root certificates for the F and G domains’ KDC certificates were added to the enterprise root certificate stores in both domains. Both domains’ KDCs were configured not to perform UPN based account mapping (HKey\_Local\_Machine\System\CurrentControlSet\Services\KDC\UseSubjectAltName = 0). The same [group policies](#_Windows_7_(CSDWin7-2)) applied to CSD\Win7-2 workstation were applied to the F\Win7-2 computer account. Test Card1 (contains UPN value) and Test Card2 (does not contain UPN value) were used in the following tests.



Figure11: Cross Forest Explicit Mapping Configuration

The user attributes of the F and G domain user accounts are as follows.

|  |  |  |
| --- | --- | --- |
| **AD Account** | **AD userPrincipalName** | **AD altSecurityIdentities** |
| F\testcard1 | [32015465737401@upn.example.com](mailto:32015465737401@upn.example.com) | X509:<I>C=US,O=Test Certificates 2010,OU=Test CA,CN=Test RSA 2048-bit CA for Test PIV Cards<S>C=US,O=Test Government,OU=Test Department,OU=Test Agency,CN=Test Cardholder |
| F\testcard1\_admin | Testcard1\_admin@f.internal | X509:<I>C=US,O=Test Certificates 2010,OU=Test CA,CN=Test RSA 2048-bit CA for Test PIV Cards<S>C=US,O=Test Government,OU=Test Department,OU=Test Agency,CN=Test Cardholder |
| F\testcard2 | [Testcard2@f.internal](mailto:Testcard2@f.internal) | X509:<I>C=US,O=Test Certificates 2010,OU=Test CA,CN=Test RSA 3072-bit CA for Test PIV Cards<S>C=US,O=Test Government,OU=Test Department,OU=Test Agency,CN=Test Cardholder Jr. (affiliate) |
| F\testcard2\_admin | [Testcard2\_admin@f.internal](mailto:Testcard2_admin@f.internal) | X509:<I>C=US,O=Test Certificates 2010,OU=Test CA,CN=Test RSA 3072-bit CA for Test PIV Cards<S>C=US,O=Test Government,OU=Test Department,OU=Test Agency,CN=Test Cardholder Jr. (affiliate) |
| G\g-testcard1 | [g-testcard1@g.internal](mailto:g-testcard1@g.internal) | X509:<I>C=US,O=Test Certificates 2010,OU=Test CA,CN=Test RSA 2048-bit CA for Test PIV Cards<S>C=US,O=Test Government,OU=Test Department,OU=Test Agency,CN=Test Cardholder |
| G\g-testcard1\_priv | [g-testcard1\_priv@g.internal](mailto:g-testcard1_priv@g.internal) | X509:<I>C=US,O=Test Certificates 2010,OU=Test CA,CN=Test RSA 2048-bit CA for Test PIV Cards<S>C=US,O=Test Government,OU=Test Department,OU=Test Agency,CN=Test Cardholder |
| G\g-testcard2 | [g-testcard2@g.internal](mailto:g-testcard2@g.internal) | X509:<I>C=US,O=Test Certificates 2010,OU=Test CA,CN=Test RSA 3072-bit CA for Test PIV Cards<S>C=US,O=Test Government,OU=Test Department,OU=Test Agency,CN=Test Cardholder Jr. (affiliate) |
| G\g-testcard2\_priv | g-testcard2\_priv@g.internal | X509:<I>C=US,O=Test Certificates 2010,OU=Test CA,CN=Test RSA 3072-bit CA for Test PIV Cards<S>C=US,O=Test Government,OU=Test Department,OU=Test Agency,CN=Test Cardholder Jr. (affiliate) |

Table 9: Cross Forest Explicit Mapping Account Settings

In the following tests the value in the X509Hint field was supplied in the username hint field on the Windows Logon screen. The results of the cross-forest explicit mapping authentication tests are as follows.

|  |  |  |  |
| --- | --- | --- | --- |
| **Smart Card** | **Pin** | **X509Hint** | **Result** |
| testcard1 | 123456 | f\testcard1 | Authenticated to the f\testcard1 account |
| testcard1 | 123456 | f\testcard1\_admin | Authenticated to the f\testcard1\_admin account |
| testcard1 | 123456 | <not supplied> | Authenticated to the f\testcard1 account (fallback to UPN based mapping) |
| testcard1 | 123456 | g\g-testcard1 | Authenticated to the g\g-testcard1 account |
| testcard1 | 123456 | g\g-testcard1\_priv | Authenticated to the g\g-testcard1\_priv account |
| testcard2 | 123456 | f\testcard2 | Authenticated to the f\testcard2 account |
| testcard2 | 123456 | f\testcard2\_admin | Authenticated to the f\testcard2\_admin account |
| testcard2 | 123456 | <not supplied> | Authenticated to the f\testcard2\_admin account (KDC selects the first account found) |
| testcard2 | 123456 | g\g-testcard2 | Authenticated to the g\g-testcard2 account |
| testcard2 | 123456 | g\g-testcard2\_priv | Authenticated to the g\g-testcard2\_priv account |

Table 10: Cross Forest Explicit Mapping Smart Card Logon Results

# S/MIME Configuration

The National Institute of Standards and Technology Personal Identity Verification Test Cards include digital signature and key management (encryption) certificates. There are too many digital signature and encryption test scenarios due to the number of test cards, workstation/email clients and algorithm combinations. Therefore this section will describe how to configure Microsoft Outlook 2010 to send digitally signed and encrypted S/MIME messages and demonstrate a NIST SP800-78-3compliant S/MIME email exchange.

The Outlook 2010 hotfix KB2475877 (http://support.microsoft.com/kb/2475877) was installed to ensure that the minimum encryption algorithm used was 3DES. Elliptic curve cryptography digital signature and key management certificates (i.e. Test Card4, Test Card5 and Test Card15) cannot be loaded into Outlook’s Security Center Signing and Encryption certificate fields. This is a known issue and is being addressed.

## Example S/MIME Test Sequence



Figure 12: PIV Test Card S/MIME test

Test Card1 account sends email from Win7-2 workstation to Test Card12 using the Outlook clients on the XPSP3, Win7-1 and MAC OS X clients and the Thunderbird client on the Linux based system. The email exchange steps are as follows:

1. Test Card1 sends digitally signed SHA256 email message to the Test Card12 account (includes Key Management certificate in the email)
2. Test Card12 validates Test Card1’s digital signature on XP SP3, Win7-1, MAC OS X and Mandriva 2010.2 workstations
3. Test Card12 replies back with an encrypted AES128 email message to Test Card1 on all workstations
4. Test Card1 decrypts and validates the digital signature of Test Card12’s messages on the Win7-2 workstation.

### Step 1: Digitally Signed Message

The Outlook signature/encryption settings are configured in File \ Options \ Trust Center \ Trust Center Settings \ E-mail Security \ Encrypted e-mail, Default Settings \ Settings

* Signing Certificate: Digital Signature certificate, select Hash Algorithm SHA256
* Encryption Certificate: Key Management certificate, select Encryption Algorithm AES(128-bit)

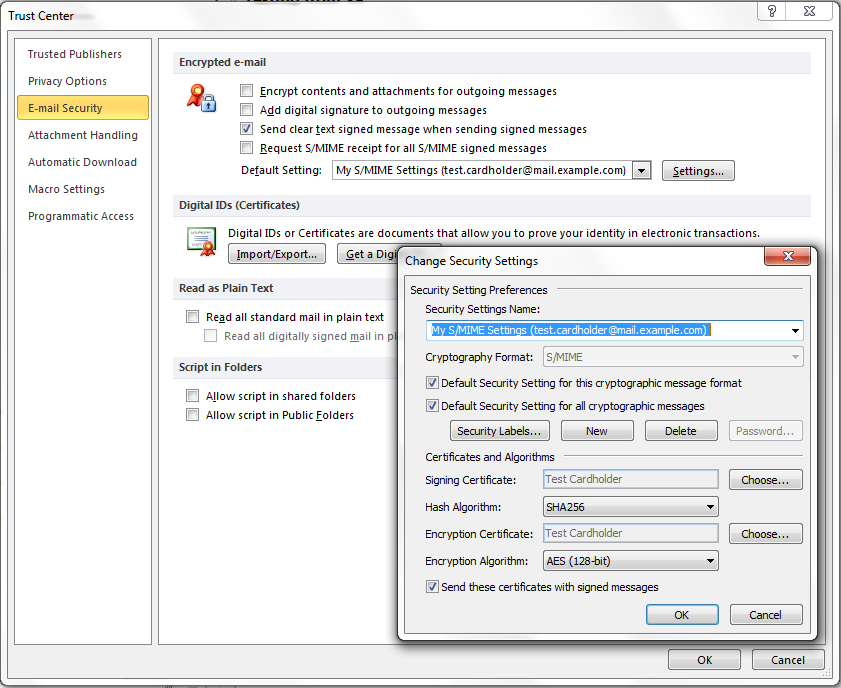


Figure 13: Test Card1 Outlook Security Settings.

**Note:** Select the “Send these certificates with signed messages” to ensure the sender’s Key Management certificate is available to the recipient for email encryption.

To digitally sign the email message select the Options \ Permission \ Sign.

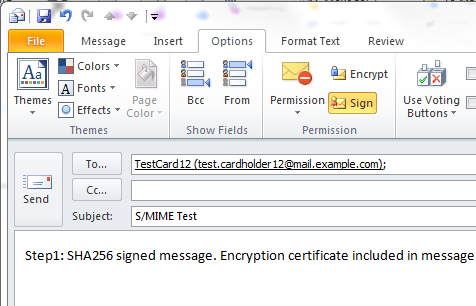


Figure 14: Test Card 1 digitally signed email message

### Step 2: Validating Digitally Signed Message

Test Card1’s digitally signed message will have a red ribbon in the right hand side of the message header. Double click on the ribbon to confirm the message’s integrity.

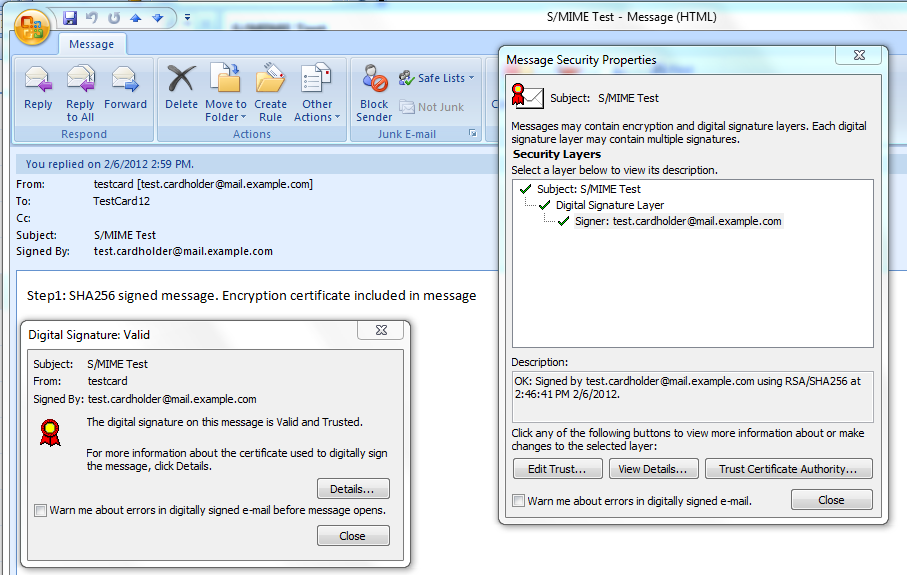


Figure 15: Test Card12 Win7-1 Outlook 2007 validation of step1 message

The following table contains the results of Test Card12’s validation of Test Card1’s SHA256 digitally signed email message on the respective workstation.

|  |  |  |
| --- | --- | --- |
| **Message** | **Valid Digital Signature** | **Reason** |
| From Test Card1 on XP SP3 | Fail | XP cannot validate SHA256 signed message |
| From Test Card1 on Win7-1 | Success | SHA256 signed message |
| From Test Card1 on MAC OS X | Success | SHA256 signed message |
| From Test Card1 on Mandriva 2010.2 | Success | SHA256 signed message |

Table 11: Step2 Message Digital Signature Validation

### Step 3: Encrypting Message

Test Card1’s digitally signed message contains its encryption certificate, which includes the public key, within the message. When Test Card12 replies to the message, with encryption, Test Card1’s key management certificate/public key is used to encrypt the message. A user’s key management certificate can be stored within the Outlook contact for Test Card1 and/or the Exchange Global Address Book (GAL) to allow S/MIME encryption without the initial exchange of certificates (Step1).

### Step 4: Viewing/Validating Encrypted Message

To confirm Test Card1 validation of Test Card12’s encrypted email, double click on the blue safe icon. In Outlook 2010 if the contents can be decrypted they will be rendered in the reading pane. In Outlook 2007 the message contents will not be legible within the Outlook reading pane and the message must be opened to decrypt the message.

Click on the safe and ribbon icons for validation of the message’s encryption and non-repudiation.

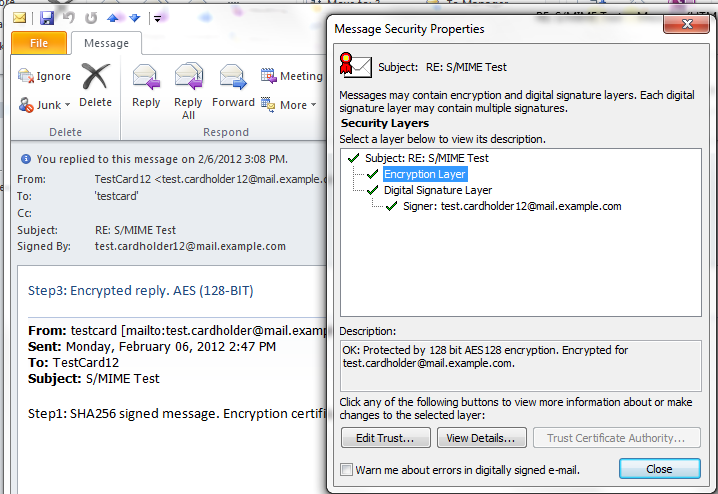


Figure16: Encryption and Digital Signature validation

The following table contains the results of Test Card1’s validation of Test Card12’s encrypted email messages from the respective workstations.

|  |  |  |
| --- | --- | --- |
| **Message** | **Decrypted** | **Valid Digital Signature** |
| From Test Card12 on XP SP3 | Fail | Fail |
| From Test Card12 on Win7-1 | Success, AES (128-bit) | Success, SHA256 |
| From Test Card12 on MAC OS X | Success, 3DES (168-bit) | Fail (SHA1 only support) |
| From Test Card12 on Mandriva 2010.2 | Success, 3DES (168-bit) | reply was not digitally signed |

Table 12: Step4 Message Encryption

### XP SP3 S/MIME Behavior

Test Card12 on XP SP3 was unable to validate, sign or encrypt any of the messages in the test S/MIME exchange. To perform a similar test for XP SP3 set Test Card1’s E-mail Security settings (on Win7-2) to Hash Algorithm SHA1 (not NIST SP800-78-3compliant) and Encryption Algorithm 3DES. The XP SP3 Outlook 2010 client will be able to validate Step1’s digital signature and encrypt a reply.

### MAC OS X S/MIME Behavior

Test Card12 on MAC OS X was able to validate the signed SHA256 message. OS X Outlook 2011 and Apple Mail are able to validate a SHA256 hash but are unable to generate a SHA256 hash.

# References

1. National Institute of Standards and Technology (NIST) Personal Identity Verification (PIV) Test Cards, <http://www.nist.gov>
2. HSPD-12 – Homeland Security Presidential Directive 12, <http://www.dhs.gov/xabout/laws/gc_1217616624097.shtm>
3. FIPS 201-2 – Federal Information Processing Standard 201-2 (Draft), <http://csrc.nist.gov/publications/drafts/fips201-2/Draft_NIST-FIPS-201-2.pdf>
4. RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, <http://tools.ietf.org/html/rfc5280>
5. How the Kerberos Version 5 Authentication Protocol Works,<http://technet.microsoft.com/en-us/library/cc772815.aspx>
6. RFC 4556 - Public Key Cryptography for Initial Authentication in Kerberos (PKINIT), <http://www.ietf.org/rfc/rfc4556.txt>
7. [MS-ADTS]: Active Directory Technical Specification, <http://msdn.microsoft.com/en-us/library/cc223122(v=PROT.10).aspx>
8. [MS-PKCA]: Public Key Cryptography for Initial Authentication (PKINIT) in Kerberos Protocol Specification,<http://msdn.microsoft.com/en-us/library/cc238455(v=prot.13).aspx>
9. Windows Vista Smart Card Infrastructure, <http://www.microsoft.com/downloads/details.aspx?FamilyID=ac201438-3317-44d3-9638-07625fe397b9&displaylang=en>
10. Understanding S/MIME, <http://technet.microsoft.com/en-us/library/aa995740(EXCHG.65).aspx>
11. Smart Cards, <http://technet.microsoft.com/en-us/library/dd277362.aspx>
12. How Certificates Work, <http://technet.microsoft.com/en-us/library/cc776447(WS.10).aspx>
13. United States Government Configuration Baseline, <http://usgcb.nist.gov/>
14. How Certificate Revocation Works, <http://technet.microsoft.com/library/ee619754.aspx>