Personal Identity Verification (PIV) Windows Logon Reference Implementation: Best Practices and Troubleshooting

October 2009

by

National Institute of Standards and Technology

Table of Contents

List of Appendices

List of Figures

List of Tables

Executive Summary

Homeland Security Presidential Directive 12 (HSPD-12) called for a new standard to be adopted governing the use of common identity credentials for physical and logical access to Federal government locations and systems. The Personal Identity Verification (PIV) standard for Federal Employees and Contractors, Federal Information Processing Standard 201 (FIPS 201), was developed to establish government-wide identity credentials. Credentials are issued to individuals whose true identity has been verified and whose need for the credential has been established and authorized by proper authorities.

FIPS 201 describes a variety of data model components as a part of the PIV logical credentials. Such components include biometric elements in the form of fingerprint information and facial imagery and security elements such as Personal Identity Number (PIN), cryptographic keys, and certificates. FIPS 201 incorporates by reference NIST Special Publication 800-73 (SP800-73), which specifies elements related to the PIV card interface, NIST Special Publication 800-76 (SP800-76), which specifies the biometric requirements, and NIST Special Publication 800-78 (SP800-78) which specifies acceptable cryptographic algorithms and key sizes for PIV systems.

The PIV card holds the identity credentials that provides the attributes of security, authentication, trust, and privacy for the relying applications. The security and trust in the operational environment can be realized when applications are enabled to use the credentials on the PIV card. One such very common application is Windows Logon. Windows Logon application is designed to use smart cards to perform user authentication to gain higher level of assurance on user's identity. This document provides information on how to enable Windows Logon to use PIV credentials. Specifically, this document provides details of the tools and troubleshooting recommendations for implementing Windows Logon. The tools discussed in this document include Microsoft Certificate Authority, NIST Crypto Service Provider, OpenSSL, and Cygwin. NIST developed the prototype solution to guide agencies in their implementation of PIV solution. Note there are many ways to implement Windows Logon using PIV card. This document shows one possible implementation.

1. Introduction

1.1 Purpose and Scope

The purpose of this document is to provide detailed information on how to enable the Windows Logon application to use a PIV card. The document provides detailed steps to configure and install tools necessary to perform Windows Logon. This document also provides recommendations to troubleshoot issues when using the NIST PIV reference implementation. The NIST PIV reference implementation includes a Card Simulator that behaves like a real PIV card, the Middleware that interacts with the card, and the Cryptographic Service Provider (CSP) that is specifically built for Windows Logon.

1.2 Audience

This document has been created for Federal government agencies that are responsible for PIV implementation. Agencies that use Windows Operating System, as well as IT professionals (particularly Windows system administrators and information security personnel) who may be responsible for implementing HSPD-12 within home offices for their organizations can benefit from this document. This document assumes that readers have knowledge of FIPS 201 and understand the underlying technologies.

1.3 Document Structure

This document is separated into sections by topic content. Sections provide detailed description of each step required to enable Windows Logon to use a PIV card. Sections contain walkthrough of user activities, information to support existing Reference Implementation documents, best practice tips, and troubleshooting activities for enabling Windows Logon to use a PIV card.

+ Section 2 describes how to configure Windows Logon to work with a PIV card
+ Section 3 describes how to log into Windows with a PIV card
+ Section 4 provides troubleshooting support for installing the PIV Card Simulator and Middleware
+ Section 5 provides troubleshooting support for installing the NIST CSP
+ Appendix A lists all the tools used in this document and where to obtain them
+ Appendix B describes how to obtain and install Cygwin
+ Appendix C describes how to create a PIV card
+ Appendix D list all acronyms used in this document
+ Appendix E provides references to resources and other source of information concerned with implementing Windows Logon

1.4 Quick Start

NIST developed the NIST CSP to provide a common interface to PIV cards for performing cryptographic functions under Windows. The NIST CSP is not a fully functional CSP. Rather, it only implements the cryptographic functions necessary to perform Windows Logon with a PIV card (e.g., secure e-mail signing and encryption is not supported). Using a few simple steps, the Windows Logon application can be easily configured to utilize the NIST CSP and communicate with PIV cards. A demonstration was put together to show how this can be done.

1.4.1 Windows Logon Demonstration

The Windows Logon demonstration shows how a PIV card can be used to log into a Windows XP workstation. The demonstration uses the machine configuration depicted below.

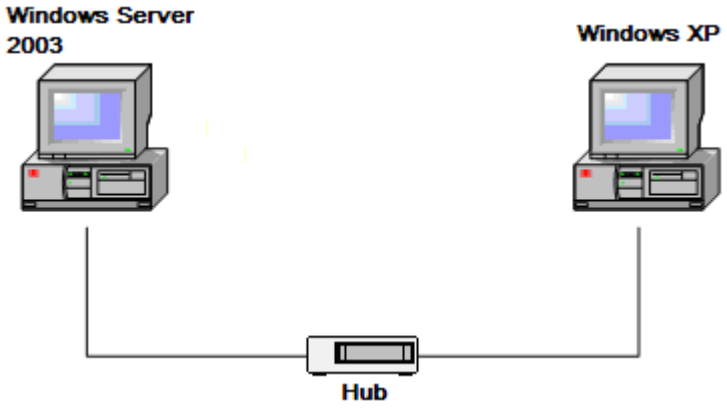

Figure 1-1. Windows Logon Machine Configuration

The event sequence for this demonstration is as follows:

1. The Windows XP workstation is booted up and displays the login prompt.
2. The user inserts his PIV card into the smart card reader.
3. The user enters the PIN for his PIV card.
4. The workstation retrieves the PIV Authentication certificate from the PIV card, validates the user's credentials, and logs him into the workstation.

The following tools, applications, and/or prerequisites are needed for this demonstration:

+ PC running Windows Server 2003 SP1 or greater
+ PC running Windows XP SP2 or greater
+ A smart card reader with the necessary Windows drivers
+ NIST CSP installation package
+ PIV card loaded with a PIV Authentication key and certificate
+ An existing user account for the PIV card holder
+ Issuing CA certificate(s)

1.4.2 Tools

The following tools were used to enable Windows Logon with a PIV card.

Microsoft CA — The MS Certificate Authority (CA) service issues certificates needed to run a public key infrastructure. These certificates enable a user to use smart card logon, send encrypted mail, sign documents, and more.

NIST CSP — NIST developed a CSP that communicates with the Microsoft application through the Crypto Application Programming Interface (CAPI) interface. The NIST CSP was developed to interrogate the card for the certificate, PIN verification, and digital signature using the PIV card edge interface. The primary intent of the NIST CSP is to support Windows Logon using a PIV Card. In this respect, the NIST CSP uses the SP 800-73-1 Client API for all communications with the PIV Card.

NIST PIV Middleware – NIST developed a reference implementation of the SP 800-73-1 Client API as defined in Section 6 of SP 800-73-1. This module creates and parses APDUs to communicate with the PIV Card.

Editors — NIST used the Hex editor (XVI32) to view and edit data in hexadecimal format. NIST also used Text Pad, an enhanced text editor, to view and edit text.

TestResMan — NIST used this utility to issue Application Programming Data Unit (APDU) to the PIV Card and to read data from the PIV Card.

2. Windows Logon Configuration

This section describes how to configure a Windows domain and workstation to enable Windows logon with a PIV card. Four major activities are involved in this process:

+ Configuration of Windows domain and policy settings
+ Establishment of trust with Certificate Authorities (CAs)
+ Configuration of user accounts
+ Installation of NIST CSP and PIV Middleware

These activities are described in the following subsections.

2.1 Windows Domain Configuration

2.1.1 Install Certificate Services

Windows Logon requires the domain controller (DC) to have a DC certificate installed. This can be accomplished by installing Certificate Services on the Windows Server 2003 machine.

1. Logon as an administrator to the Windows Sever 2003 Domain Controller.
2. From the Windows menu, click Start | Settings | Control Panel.
3. Double-click on the "Add or Remove Programs" icon.
4. Click on the "Add/Remove Windows Components" icon.
5. The Windows Components Wizard is displayed.
6. Check the "Certificates Services" checkbox.

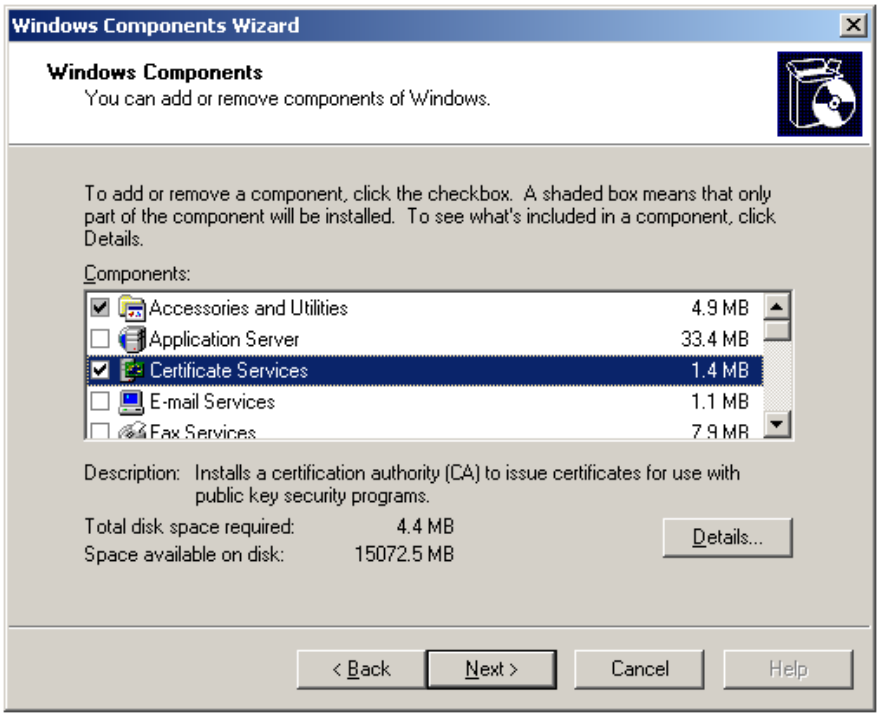

Figure 2-1. Windows Components Wizard

7. A confirmation message is displayed indicating that once Certificate Services is installed, the machine name and domain membership may not be changed. Click Yes.
8. Click Next.
9. The CA Type selection screen is displayed. Make sure "Enterprise root CA" is selected and click Next.
10. Enter the common name for the CA (e.g., "pivserver") and click Next.
11. The Certificate Database Settings screen is displayed. Click Next.
12. Installation of Certificate Services begins. During this time, you may be prompted for the Windows Server 2003 CD-ROM.
13. During installation, a message may be displayed stating that IIS is not installed and Certificate Services Web Enrollment Support will be unavailable. Click OK.
14. The Windows Components Wizard indicates that the selected components have been installed. Click Finish.
15. Reboot the Windows Server 2003 machine for the changes to take effect.

2.1.2 Configure Optional Smart Card Settings

The Windows domain security policy can be configured with optional settings that define the behavior of smart cards.

Note: After configuring the desired domain security policies on the Windows Server 2003 machine, the group policy on the Windows XP workstation has to be refreshed for the changes to take effect. This can be accomplished by logging into the Windows XP workstation as an administrator and executing the command "gpupdate /force" from a command prompt.

2.1.2.1 Set Smart Card Removal Behavior

The domain security policy can be configured to lock a workstation, logoff a user, or disconnect a user from a remote terminal session whenever the user's smart card is removed from the smart card reader. Perform the following steps to define this behavior.

1. Logon as an administrator to the Windows Sever 2003 Domain Controller.
2. From the Windows menu, click Control Panel | Administrative Tools | Domain Security Policy.
3. In the left-pane, expand the "Local Policies" item.
4. Click on the "Security Options" item to display the domain security policies.

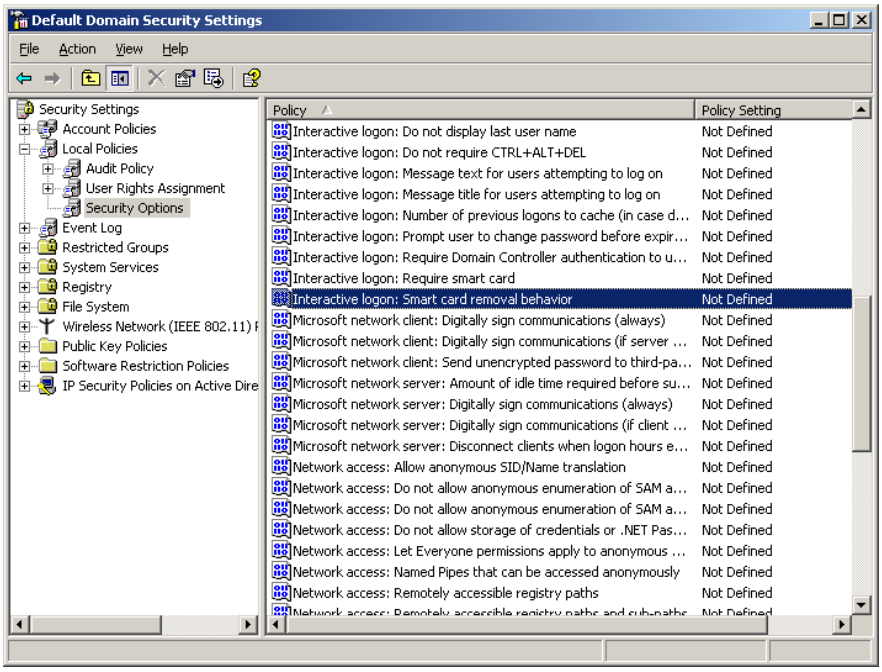

Figure 2-2. Smart Card Removal Behavior Policy

5. Double-click on the "Interactive logon: Smart card removal behavior" item to define this policy.
6. The "Interactive logon: Smart card removal behavior" property is displayed.
7. Check the "Define this policy setting" checkbox.
8. Select one of the four available choices to define the smart card removal behavior for this domain. The choices are:
    - No Action
    - Lock Workstation
    - Force Logoff
    - Disconnect if a remote Terminal Services session
9. Click OK to set the policy.

2.1.2.2 Set Smart Card Logon Requirement

The domain security policy can be configured to require a user to use a smart card to log onto a workstation (i.e., the user cannot enter a username and password to log onto a workstation). Perform the following steps to define this behavior.

Note: Care should be taken in setting this policy. If the domain security policy is configured to require smart card logon then administrators also will be unable to log onto a workstation to perform routine maintenance without the use of a smart card.

1. Logon as an administrator to the Windows Sever 2003 Domain Controller.
2. From the Windows menu, click Start | Programs | Administrative Tools | Domain Security Policy.
3. In the left-pane, expand the "Local Policies" item.
4. Click on the "Security Options" item to display the domain security policies.
5. Double-click on the "Interactive logon: Require smart card" item to define this policy.
6. The "Interactive logon: Require smart card" property is displayed.
7. Check the "Define this policy setting" checkbox.

8. Select the "Enabled" or "Disabled" choice for this policy. If set to "Enabled", make sure the Enterprise administrator has a valid smart card to log onto the domain controller. Otherwise, there is no way of using a password to log onto the domain controller except in safe mode.
9. Click OK to set the policy.

2.2 Establishment of Trust with Certificate Authorities

Smart card authentication to Active Directory (AD) requires that the following activities be performed to establish trust between the domain and the CA(s) to which an issued certificate chains:

+ Configure Domain Group Policy
+ Add CA(s) to NTAuth store in AD
+ Add Certificate Revocation List(s) (CRL) to AD

The steps described herein illustrate how to establish trust between a domain and the PIV Data Generator CAs. However, these steps can be easily adapted to any CA.

In the case of the PIV Data Generator tool, issued certificates chain to the PIV Data Generator Issuing CA (named PIV Test CA), which chains to the PIV Data Generator Root CA (named PIV Test Root). Hence, trust must be established between the domain and the PIV Data Generator Root and Issuing CAs. An example of the PIV Data Generator certificate chain is depicted below.

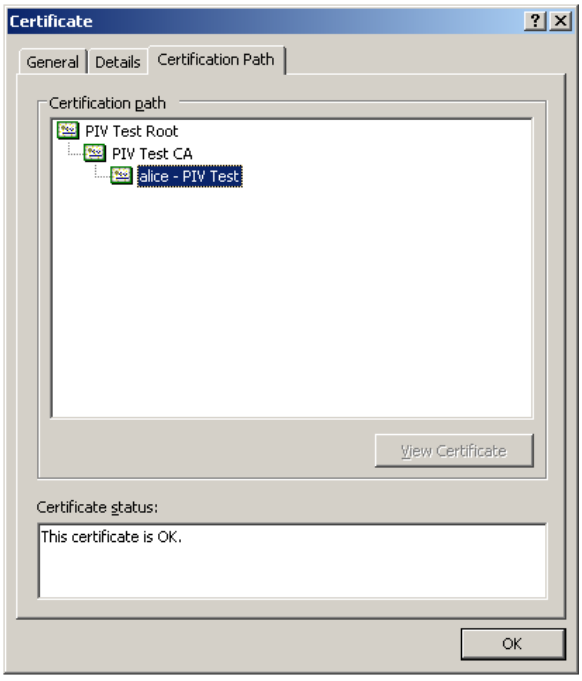

Figure 2-3. PIV Data Generator Certificate Chain

2.2.1 Configure Domain Group Policy

1. Logon as an administrator to the Windows Sever 2003 Domain Controller.
2. From the Windows menu, click Start | Programs | Administrative Tools | Active Directory Users and Computers.

3. In the left pane, right-click on the name of the domain to edit.
4. In the pop-up window, click on Properties.
5. The domain properties dialog is displayed. Click on the Group Policy tab.

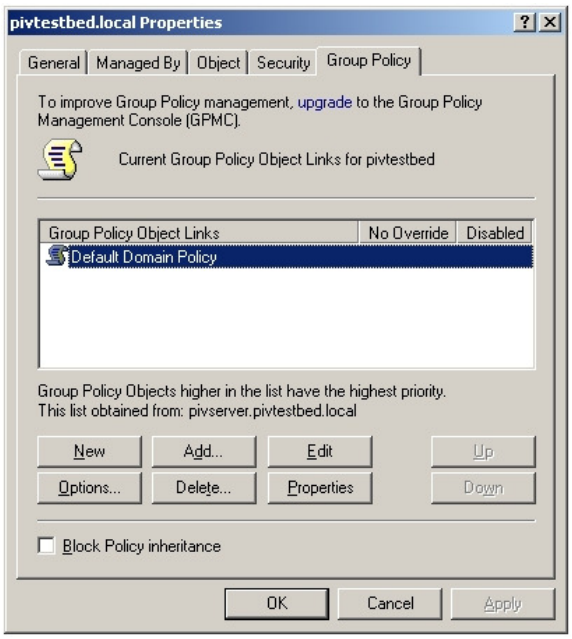

Figure 2-4. Domain Group Policy

6. Click New to create a new domain group policy and enter "PIV Policy" for the group policy name.
7. Select the newly created "PIV Policy" group policy and click Edit.
8. The Group Policy Object Editor is displayed.
9. In the left pane, expand the following items:
    - Computer Configuration
    - Windows Settings
    - Security Settings
    - Public Key Policies
10. Right-click on the Trusted Root Certification Authorities object.
11. In the pop-up window, select All Tasks | Import.
12. Follow the instructions in the wizard to import the PIV Data Generator Root CA certificate. The PIV Data Generator Root CA certificate file is named pivtestroot.cer and is located in the PIV Data Generator "extra_files" subdirectory.
13. Once the PIV Data Generator Root CA certificate has been imported, perform steps 8 – 10 again to import the PIV Data Generator Issuing CA certificate. The PIV Data Generator Issuing CA certificate file is named pivtestca.cer and is located in the PIV Data Generator "extra_files" subdirectory.

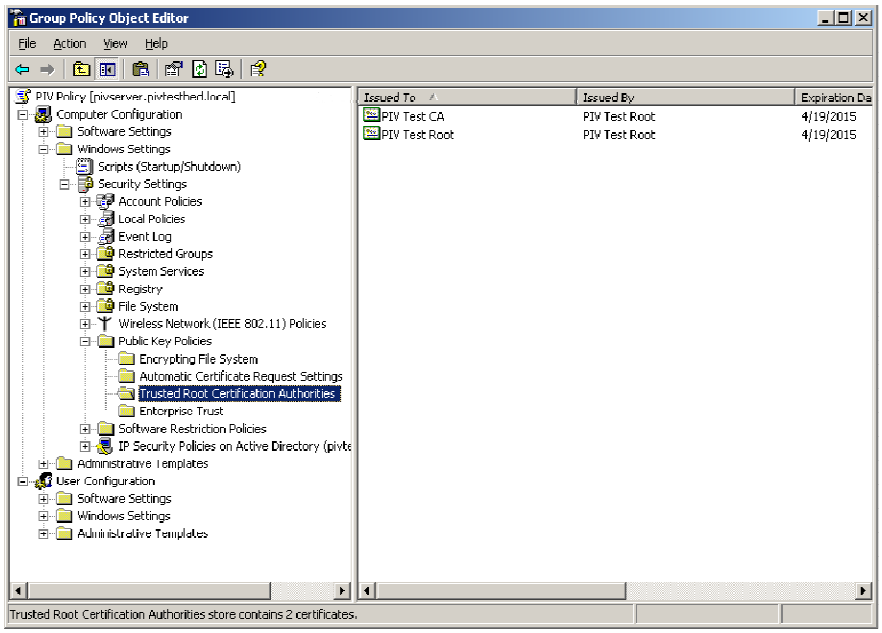

Figure 2-5. Group Policy Object Editor

14. After both PIV Data Generator CA certificates have been imported, close the Group Policy Object Editor window.
15. Click Close to close the domain properties dialog.

2.2.2 Add CA(s) to NTAuth Store in Active Directory

1. Logon as an administrator to the Windows Sever 2003 Domain Controller.
2. Open a command prompt and navigate to the PIV Data Generator "extra_files" subdirectory.
3. Enter the following command to add the PIV Data Generator Root CA to the NTAuth store:

```
certutil -dspublish -f pivtestroot.cer NTAuthCA
```

4. Enter the following command to add the PIV Data Generator Issuing CA to the NTAuth store:

```
certutil -dspublish -f pivtestca.cer NTAuthCA
```

2.2.3 Add CRL(s) to Active Directory

A CRL contains a list of certificates that have been revoked by a CA and are no longer valid. During the Windows Logon certificate validation process, Windows checks to see if a certificate has been revoked by examining the issuing CA's CRL. Hence, for Windows Logon to work with certificates issued by the PIV Data Generator tool, Windows needs to have access to the PIV Data Generator Root and Issuing CA CRLs. The CRLs can be added to Active Directory using the following procedure:

1. Logon as an administrator to the Windows Sever 2003 Domain Controller.
2. From the Windows menu, click Start | Run.
3. Type "mmc" and press Enter to launch the Microsoft Management Console (MMC). The MMC application is displayed.
4. Click File | Add/Remove Snap-in. The "Add/Remove Snap-in" dialog is displayed.
5. Click the Add button.

6. The "Add Standalone Snap-in" dialog is displayed. Select the "Certificates" snap-in and click Add.

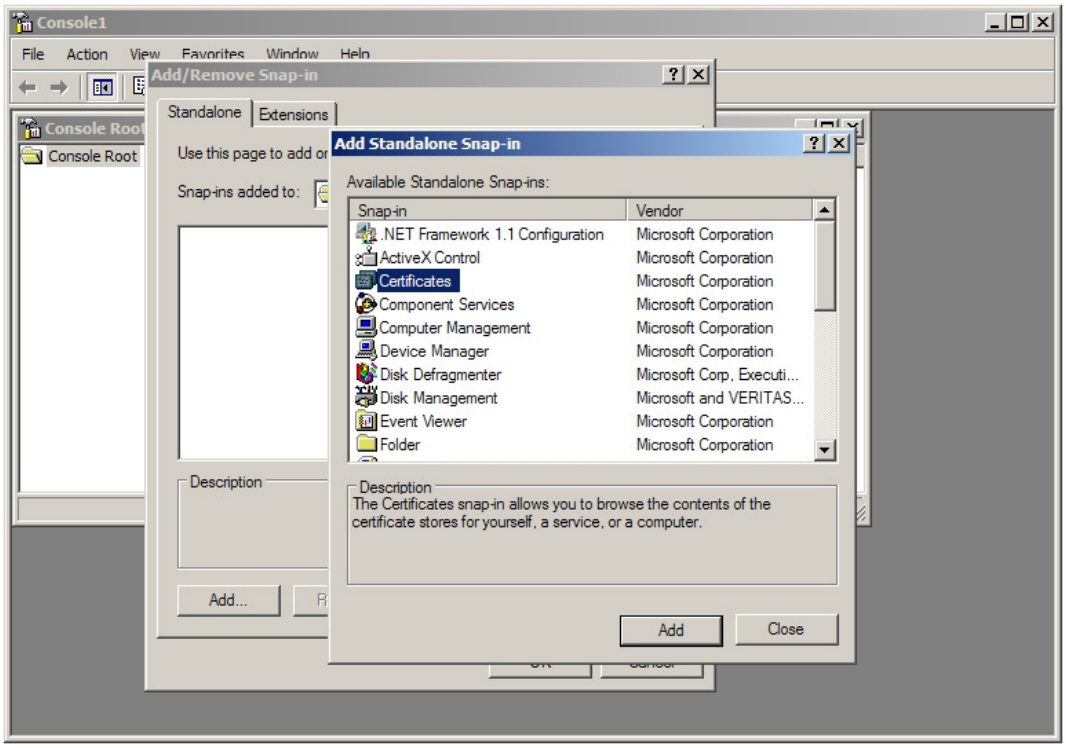

Figure 2-6. Certificates Snap-in

7. The "Certificates Snap-in" wizard is displayed.
8. Select "Computer account" and click Next.
9. Click Finish to complete the process. The Certificates snap-in has now been added to the MMC.
10. Click Close to close the "Add Standalone Snap-in" dialog.
11. Click OK to close the "Add/Remove Snap-in" dialog.
12. In the left pane of the MMC window, expand the "Certificates (Local Computer)" item.
13. Right-click the "Intermediate Certification Authorities" item.
14. In the pop-up window, select All Tasks | Import.
15. The Certificate Import Wizard is displayed. Click Next.
16. At the next screen, click Browse.
17. Browse to the PIV Data Generator "extra_files" subdirectory and make sure the "Files of Type" list box is set to "Certificate Revocation List (*.crl)".
18. Select the pivtestroot.crl file to import the PIV Data Generator Root CA CRL and click Open.
19. Click Next.
20. "Place all certificates in the following store" should be selected by default and destination certificate store should be set to "Intermediate Certification Authorities". Click Next.
21. Click Finish to complete the import process.
22. A confirmation dialog is displayed. Click OK.
23. Repeat steps 13 - 22 to import the PIV Data Generator Issuing CA CRL, which is located in the PIV Data Generator "extra_files" subdirectory and is named pivtestca.crl.

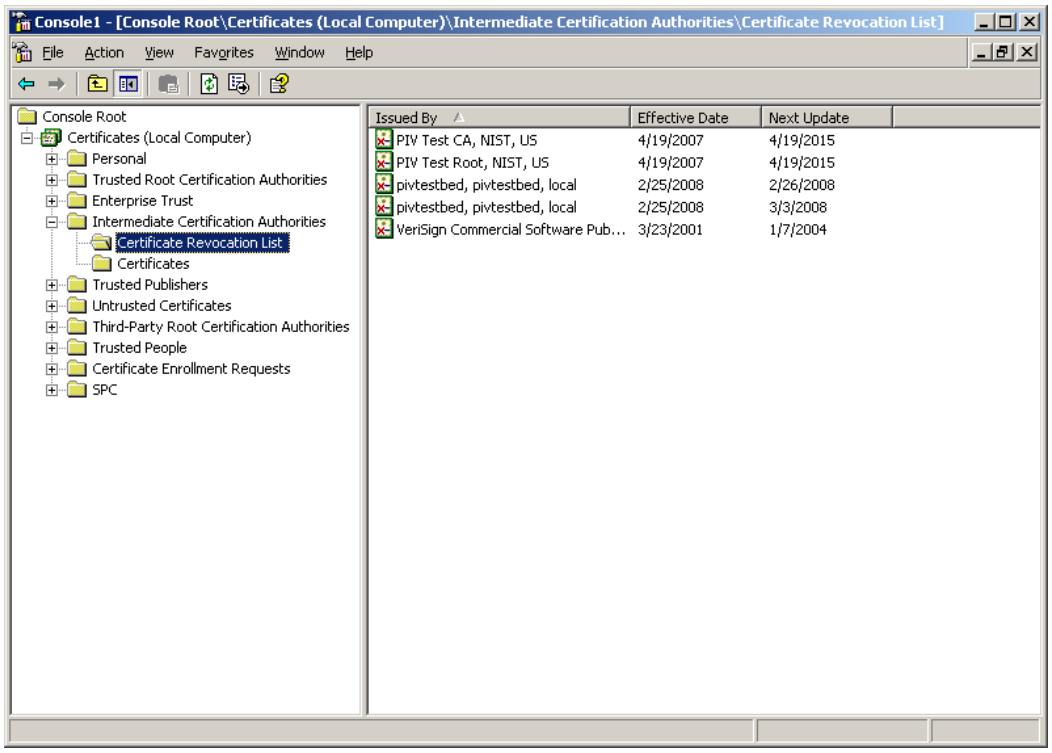

Figure 2-7. Certificates Snap-in with PIV Data Generator CRLs Imported

24. Close the MMC application.

2.2.4 Refresh Group Policy Settings

Once the domain group policy has been configured and the CA certificates and CRLs have been published, the Windows XP workstation should be updated with this information. The group policy settings for the Windows XP workstation can be updated by performing the following steps:

1. Logon as an administrator on the Windows XP workstation.
2. Open a command prompt and execute the command: `gpupdate /force`
3. A message is displayed indicating the group policy settings have been refreshed.

2.3 User Account Configuration

The following activities are performed to map a Windows user account to the PIV Authentication certificate on a PIV card:

+ Add Universal Principal Name (UPN) suffix to AD

+ Map user logon name to UPN

2.3.1 Add UPN Suffix to Active Directory

In order to map a Windows user account to the UPN specified in the PIV Authentication certificate, the UPN's suffix needs to be added to Active Directory. For example, if the UPN is alice@pivdemo.org then the following steps can be performed to add "pivdemo.org" to the list of alternative UPN suffixes in Active Directory.

1. Logon as an administrator to the Windows Sever 2003 Domain Controller.
2. From the Windows menu, click Start | Programs | Administrative Tools | Active Directory Domains and Trusts.
3. The Active Directory Domains and Trusts window is displayed.
4. Right-click on the "Active Directory Domains and Trusts" item in the tree view and select Properties from the pop-up menu.
5. The Active Directory Domains and Trusts Properties dialog displays the list of alternative UPN suffixes.
6. Enter "pivdemo.org" in the edit box and click Add.

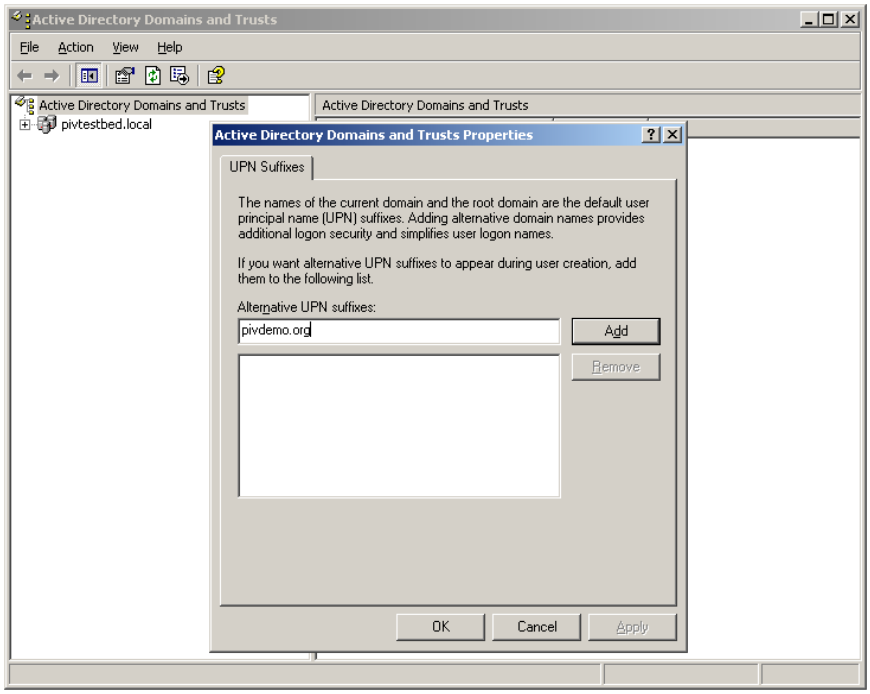

Figure 2-8. Alternative UPN Suffixes

7. The "pivdemo.org" UPN suffix is added to the list.
8. Click OK to close the Active Directory Domains and Trusts Properties dialog.
9. Close the Active Directory Domains and Trusts window.

2.3.2 Map User Logon Name to UPN

To enable Windows logon with a PIV card, the user's logon name must be associated with the UPN specified in the PIV Authentication certificate. For example, if the UPN is alice@pivdemo.org and a user account for Alice exist then the following steps can be performed to configure Alice's account:

1. Logon as an administrator to the Windows Sever 2003 Domain Controller.
2. From the Windows menu, click Start | Administrative Tools | Active Directory Users and Computers.
3. The Active Directory Users and Computers window is displayed.
4. Click on the Users folder in the tree view to display the user accounts in the domain.
5. Double-click on the "Alice" user to display Alice's user account properties.
6. Select the Account tab.
7. Enter "alice" in the "User logon name" edit box.

8. Select "@pivdemo.org" from the list of UPN suffixes.

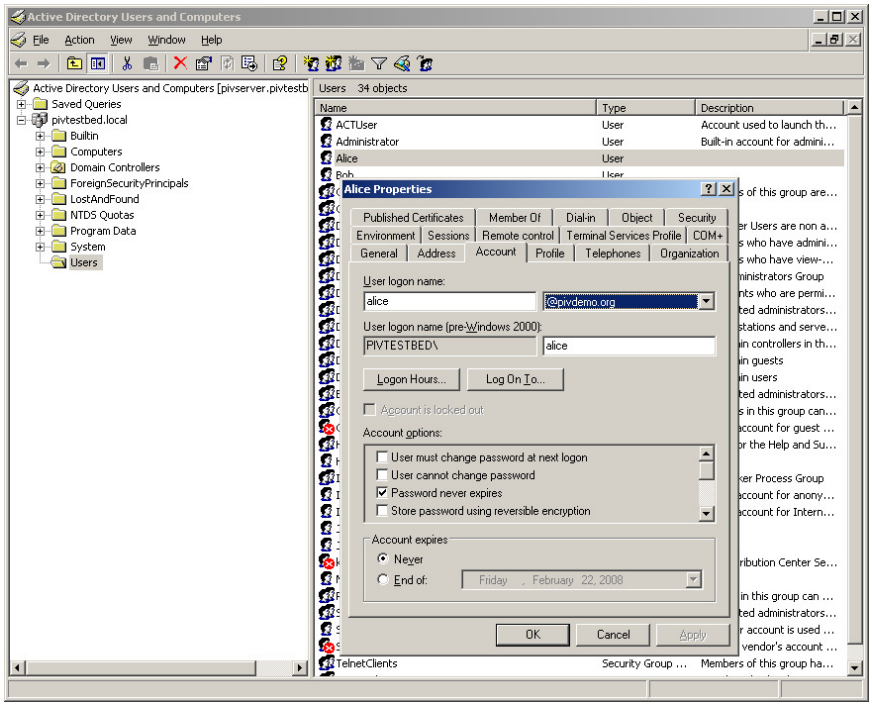

Figure 2-9. User Account Properties

9. Click OK to close Alice's user account properties.
10. Close the Active Directory Users and Computers window.

2.4 NIST CSP and PIV Middleware Installation

The NIST CSP provides an interface to the cryptographic standards and algorithms necessary to perform Windows Logon with a PIV card. The NIST CSP does not actually implement any cryptographic functions. Rather, it passes cryptographic requests either to a PIV card via the PIV Middleware or to the Microsoft CSP. The following activities must be performed to install and configure the NIST CSP and PIV Middleware for use with Windows Logon:

+ Install NIST CSP and PIV Middleware
+ Download and install third party freeware products used by NIST CSP
+ Associate NIST CSP with PIV card

2.4.1 Install NIST CSP and PIV Middleware

Perform the following steps to install the NIST CSP and PIV Middleware on the Windows XP workstation that the user will log into with their PIV card:

1. In the .\Binaries folder of the NIST CSP installation package, run the file prepcsp.bat.
2. Select option 1 "Install NIST CSP for PIV Card".
3. A message is displayed indicating installation is complete. This installs both the NIST CSP and PIV Middleware onto the system. If any warning messages appear during installation then refer to section 5.1 for troubleshooting tips on installing the NIST CSP.

4. Press any key to exit installation.

2.4.2 Download Freeware Products

NIST CSP uses Crypto++ and zlib libraries for cryptographic functions and unzip utility respectively. These libraries must be installed before NIST CSP can be used with PIV card. Refer to Section 4.3 and 4.4 for specific instructions to download and install these libraries.

2.4.3 Associate NIST CSP with PIV Card

After the NIST CSP has been installed, the Windows XP workstation has to be configured to utilize the NIST CSP whenever a PIV card is inserted into the smart card reader. Windows associates smart cards with CSPs by the smart cards' Answer To Reset (ATR) byte string. Hence, the smart card's ATR must be mapped to the NIST CSP. Typically, each smart card has a unique ATR, but certain values of the ATR are usually shared. Smart cards from the same manufacturer will usually have some similar values.

2.4.3.1 Determine PIV Card's ATR

2.4.3.1.1 Determine ATR of a PIV Card

The ATR of a PIV card can be determined by using the TestResMan tool (see Appendix A) to establish a connection with the card and retrieving its ATR.

1. Launch TestResMan.
2. Click Select Reader. A list of available smart card readers is displayed.
3. Select the smart card reader the card is inserted in and click OK.
4. Click Card Connect. Share mode and protocol types are displayed.
5. Click OK to accept the default values and connect to the card.
6. If a connection was successfully established with the card then no error messages should be displayed in the bottom left corner of the TestResMan dialog.
7. Click Card State.
8. The ATR is displayed in the Output as a string of hex characters.
9. Copy the ATR (TestResMan does not allow the Output's contents to be copied to the clipboard so it will have to be typed manually).
10. Click Card Disconnect.
11. Select 'Leave Card' and click OK. The card is now disconnected.
12. Click Close to close TestResMan.

2.4.3.1.2 Determine ATR of PIV Card Simulator

The ATR of the PIV Card Simulator is set to 3B 90 96 40 0A. Hence, no additional steps are required to determine its ATR.

2.4.3.2 Associate ATR with NIST CSP

Windows stores ATR and CSP information in the Registry. Perform the following steps to associate an ATR with the NIST CSP.

1. From the Windows menu, click Start | Run, type "regedit" and press enter.

2. Browse to:
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards
3. Right-click on SmartCards and select New | Key from the pop-up menu.
4. Enter a name for the card (e.g. PivCard).
5. Right-click on the newly created key and select New | Binary Value from the pop-up menu.
6. Name this new Binary Value: **ATR**.
7. Double-click ATR to edit it and enter the ATR from section 2.4.2.1.
8. Click OK to save.
9. Add another Binary Value called: **ATRMask**.
10. Enter FF for the number of bytes in the **ATR** above. For example, if the ATR is 17 bytes then enter: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF.
11. The last value that needs to be added is a string. This string specifies what CSP to load when Windows encounters a smart card with the specified ATR.
12. Right-click on your key and select New | String Value.
    Name: **Crypto Provider**
    Value: **NIST-ESI CSP**

3. Windows Logon with PIV Card

This section describes the Windows Logon process using a PIV Card or PIV Card Simulator. All prerequisites for smart card logon should be satisfied. In particular, the following should be true:

+ Windows XP Workstation is joined to a Windows Server 2003 domain running Microsoft CA.
+ Trust has been established between the domain and the root CA to which the issuing CA chains.
+ Windows XP and Server 2003 are configured for smart card logon.
+ The PIV card is loaded with the PIV applet, PIV Authentication key pair, and PIV Authentication certificate.
+ The NIST CSP and PIV middleware is installed on Windows XP workstation and associated with the PIV card.
+ A Windows compatible smart card reader is installed.

3.1 Windows Logon with a PIV Card

Perform the following steps to attempt Windows Logon using a PIV card:

1. If currently logged onto the Windows XP workstation, log off.

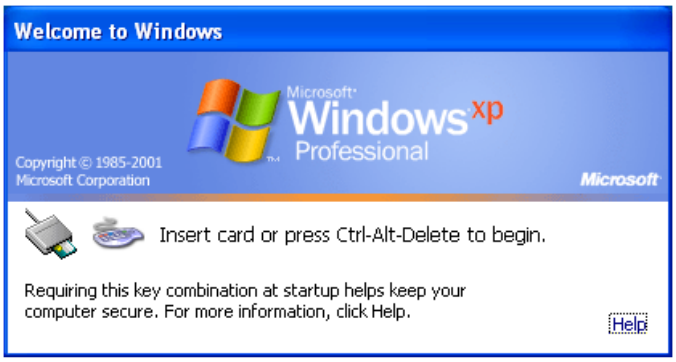

Figure 3-1. Windows Smart Card Logon Prompt

2. Insert your card.
3. The PIN prompt is displayed. Enter the PIN number for the PIV card and click OK.

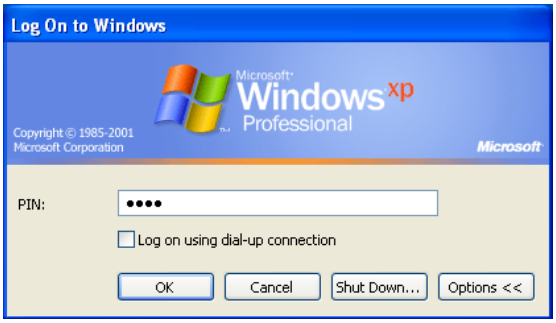

Figure 3-2. Windows Smart Card Logon PIN Prompt

4. In few moments you will be logged-in.

Note: The first time you attempt smart card logon, the Windows XP workstation must be connected to the Windows Server 2003 Domain Controller. Once you have successfully logged onto the workstation, you can perform subsequent smart card logons disconnected from the Domain Controller.

3.2 Windows Logon with PIV Card Simulator

In order to perform Windows Logon with a smart card, a smart card reader must be installed on the system. Hence, Windows Logon with the PIV Card Simulator requires the use of the NIST Virtual Smart Card Reader (VSCR) too. The PIV Card Simulator emulates a PIV card application while the NIST VSCR emulates a physical smart card reader. Perform the following steps to Logon with the PIV Card Simulator:

On the Windows Server 2003 Domain Controller:

1. Logon as an administrator to the Windows Sever 2003 Domain Controller.
2. Launch Windows Explorer and navigate to the directory that contains the PIV Card Simulator executable.
3. Double-click on the "pivd_local_server.bat" batch file to run the PIV Card Simulator. The batch file runs the pivd.exe executable in a continuous loop using the "piv.fs" file system created in section C.3.3.3 as input until the user stops the batch script by entering Ctrl-C.

Note: The PIV Card Simulator should not be running from the Windows XP workstation that will be used to perform Windows Logon since the application must be running while the user is not logged into the workstation. In this configuration, the NIST VSCR (running on the Windows XP workstation) will communicate with the PIV Card Simulator (running on the Windows Server 2003 machine) via the TLP-224 protocol to perform Windows Logon.

On the Windows XP workstation:

1. Logon as an administrator to the Windows XP workstation.
2. Install and configure the NIST VSCR to connect to the PIV Card Simulator. When configuring the NIST VSCR, make sure the "Automatically insert card when service starts" option is not checked. Refer to the *Virtual Smart Card Reader User Guide* for instructions on doing this (see Appendix E, [6]).
3. Open the "%SystemRoot%\system32\VSCR Event Script.ini" file in a text editor.
4. Change the value of "EventCount" to "1".
5. Set the time to insert a virtual smart card into the NIST VSCR. An example appears below.

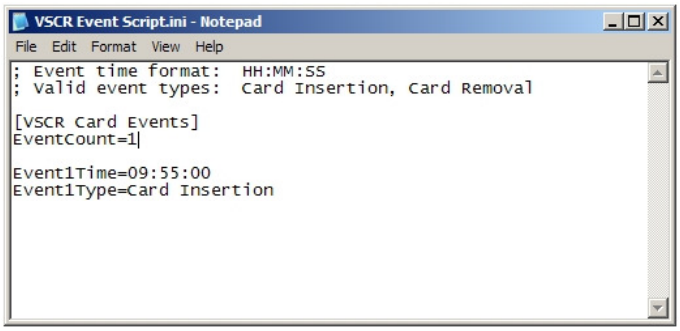

Figure 3-3. Sample NIST VSCR Event Script

6. Save the file.
7. From the Windows menu, select Start | Programs | Administrative Tools | Services.
8. Right-click on the 'PIV Virtual Smart Card Reader' service and select Start. The service is started.
9. Close the Services window.
10. Log off of the Windows XP workstation.
11. At the time specified in step 5, a virtual smart card will be inserted into the NIST VSCR.
12. The PIN prompt is displayed. Enter the PIN number for the PIV Card Simulator and click OK.
13. In few moments you will be logged-in.

4. Troubleshooting PIV Card Simulator and Middleware Compilation and Building

The *PIV Card Simulator User's Guide* (see Appendix E, [3]) briefly describes how to compile, install and use the SP 800-73-1 PIV Card Simulator. These sections cover how to handle some issues you may encounter, including prerequisites and additional configurations. Some of this material can be found on the PIV Project Question & Answer Website (see Appendix E, [4]).

4.1 PIV Card Simulator Installation [reference]

The sixth instruction of the "Recompile and Building" section of the *PIV Card Simulator User's Guide* indicates to open the PIV project in Visual Studio .NET. The PIV Card Simulator and installation instructions can be obtained from the http://csrc.nist.gov/piv-program webpage under the "SP 800-73 Reference Implementation" download package.

4.2 Java Card Development Kit 2.2.1 Installation

The PIV Card Simulator relies on the Java Card Development Kit 2.2.1, which is available from Sun at http://java.sun.com/products/javacard/dev_kit.html. The installation guide for the Java Card development kit references several prerequisites required that are not mentioned in the *PIV Card Simulator User's Guide* (See Appendix A, Tools for information on where to download these packages):

+ Java 2 Standard Edition Software Developer's Kit (SDK)
    - Run the binary downloaded to install.

Note: All these instructions apply to the Windows platform.

1. Unzip the JavaCard development kit into a directory of your choice, such as c:\nist.
   Root of the JCDK installation: C:\nist\java_card_kit-2_2_1
2. Set several environment variables (Load Control Panel | System | Advanced tab | Environment Variables):
    a. New system variable: JC_HOME
       Set this to the location where you extracted the JCDK, e.g. c:\nist\java_card_kit-2_2_1
    b. New system variable: JAVA_HOME
       Set this to the location where the JDK is installed, e.g. C:\Progra~1\Java\jdk1.5.0_07
       Note: The JCDK tools (e.g. apdutool, capdump) have trouble dealing with spaces in the JAVA_HOME variable. Use the Windows 95 naming compatibility syntax if your JDK is installed in \Program Files ("Program Files" becomes "Progra~1")
    c. Append the following to the PATH system variable to enable running the tools from the command line:
       ;%JC_HOME%\bin;%JAVA_HOME%\bin

Installation is complete. You can verify the JCDK was installed correctly by launching a command prompt and executing "cref". You should see the following.

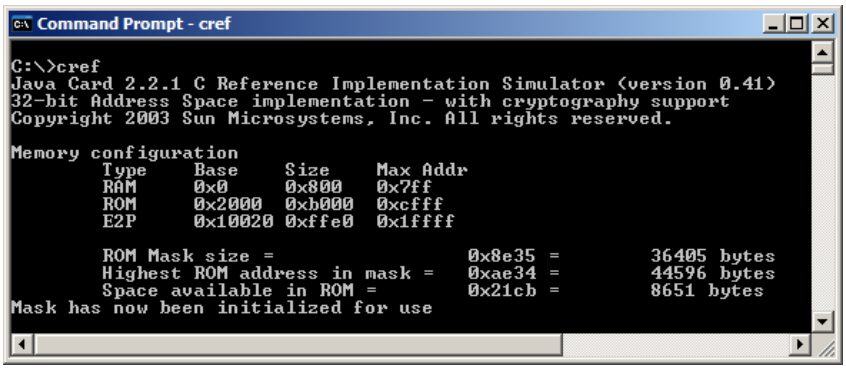

Figure 4-1. Java Card SDK tool, cref

4.3 Crypto++ Library Installation

The Crypto++ Library package contains the cryptographic algorithms needed for compiling the PIV Card Simulator. The fourth instruction of the "Recompile and Building" section of the *PIV Card Simulator User's Guide* indicates to "Download the crypto++ package and extract the zip file into %PIV_HOME%\cryptopp".

The next step indicates to compile the cryptlib libraries and copy the resulting files into %PIV_HOME%\lib\.

To compile the Crypto++ Library with Microsoft Visual Studio .NET 2003:[1]

1. Open the cryptlib.dsp project in %PIV_HOME%\cryptopp.
2. Convert project.
3. Open the project properties (right click cryptlib in the solution explorer), and navigate to C/C++ | Code Generation.
4. With the Debug configuration selected, change the "Runtime Library" value to Multi-threaded Debug DLL.
5. Change the configuration to Release and change the "Runtime Library" value to Multi-threaded DLL.
6. Navigate inside project properties to Librarian | General.
7. With the configuration set to Debug, change the value of "Output File" to "$(PIV_HOME)/lib/$(ProjectName)D.lib".
8. Click OK.
9. With the Debug configuration selected, select Build | Build Solution from the menu bar at the top of the Visual Studio window, saving the solution as requested, and wait several minutes for cryptlibD.lib to compile.
10. With the Release configuration selected, select Build | Build Solution from the menu bar at the top of the Visual Studio window and wait several minutes for cryptlib.lib to compile.

At this point, the two static libraries should be compiled and in the appropriate library folder for the PIV Card Simulator to successfully compile in the Debug or Release configuration.

[1] Much of the following is taken from the Personal Identity Verification Information Site – Frequently Asked Questions – Topic SP 800-73 - Question 219 - http://piv.nist.gov/pivqa/faq.php?qid=219.

4.4 zlib Library Installation

SP 800-73 provides an option to store certificate data in a gzip compressed format. Since this utility is an option, some PIV Cards may have compressed certificate data. The NIST CSP allows the read of compressed and uncompress format. The NIST CSP uses freeware zlib library package to uncompress the certificate read from the PIV Card. The zlib library package does not come in NIST CSP distribution but can be obtained from the http://www.zlib.net web site.

To install the zlib library, the user must download the compiled DLL package and unzip it to a directory. Next, the user should perform the following:

1. Create a directory named "zlib" under the %PIV_HOME%\Source\dev\ directory and unzip the contents of the ZLib package to this directory.

2. Copy the zlib1.dll file from the ZLib package to the %PIV_HOME%\Binaries directory of the NIST CSP package.

4.5 PIV Middleware Installation [reference]

The NIST CSP installation package includes a pre-built PIV Middleware. It is only necessary to rebuild the PIV Middleware if changes are made to the source code.

The fourth instruction of the "Build / Recompile" section of the *PIV Middleware User's Guide* indicates to open the PIV Middleware Reference project in Visual Studio .NET. The PIV Middleware and installation instructions can be obtained from the http://csrc.nist.gov/piv-program webpage under the "SP 800-73 Reference Implementation".

To compile the Release or TLP224_Release configurations, perform the following change to remedy the "'/O2' and '/RTC1' command-line options are incompatible" error message:

1. Right-click the PIV project and select Properties.
2. Check to make sure "Release" is selected in the Configuration drop-down.
3. Select C/C++ | Code Generation.
4. Set "Basic Runtime Checks" to "Default".
5. Click OK.
6. Recompile a Release configuration.

One other issue to note is that when switching between building the TLP224 and non-TLP224 configurations, you should clean the solution before building. This is recommended because the PIVTLP224.dll used by pivTest.exe in both the TLP224 and non-TLP224 version will not get rebuilt for a new configuration if it already exists.

4.6 PIV Middleware Sample Application Usage

The PIV Middleware pivTest.exe application is rather straightforward to use but there are a few prerequisites to note.

TLPCLIB.dll is included in the PIV Middleware package. It is located in %PIVMW_HOME%\bin. This DLL is required to run the pivTest.exe Middleware test application in TLP224 mode. By default, it is not included in the %PIVMW_HOME%\build\bin directory, and therefore pivTest.exe is not able to execute

in TLP224 mode. To fix this, copy the TLPCLIB.dll from %PIVMW_HOME%\bin to %PIVMW_HOME%\build\bin.

5. Troubleshooting Cryptographic Service Provider and Windows Logon

Section 2 describes how to install and configure the NIST CSP for Windows Logon. Section 3 describes the prerequisites and usage of a PIV card for Windows Logon.

This section addresses some issues that may be encountered, additional prerequisites, signature debugging, and interpretation of log files.

5.1 NIST CSP Installation Error

The following message may appear during installation of the NIST CSP:

The process cannot access the file because it is being used by another process.

0 file(s) copied

This message appears if one or more files from the NIST CSP installation package is already installed on the workstation and it is currently being used by another process. To fix this problem, reboot the workstation, log on as an administrator, and run the NIST CSP installation package again. After doing this, you may get the following messages:

1 files(s) copied.

1 files(s) copied.

The process cannot access the file because it is being used by another process.

0 file(s) copied

This indicates that the NIST CSP and PIV Middleware DLLs were copied successfully but the msvcr71.dll could not be copied because it is currently in use. The PIV Middleware utilizes the msvcr71.dll DLL and is provided as part of the NIST CSP installation package in case that DLL is currently not installed on the target machine. Since this message indicates the msvcr71.dll file already resides on the target machine, it can be safely disregarded.

5.2 Card NOT Properly Associated with NIST CSP

The following error message may appear after inserting the PIV card into the smart card reader at the logon prompt:

The card supplied requires drivers that are not present on this system. Please try another card.

This error appears if the NIST CSP has not been installed correctly and/or the PIV card's ATR has not been associated with the NIST CSP. Make sure the NIST CSP has been installed on the machine using the steps described in section 2.4.1. In addition, make sure the ATR of the PIV card has been associated with the NIST CSP as described in section 2.4.2.

5.3 Untrusted Certificate Authority

The following error message may appear after entering the PIN for the PIV card at the logon prompt:

The system cannot log you on due to the following error:

An untrusted certificate authority was detected while processing the smartcard certificate used for authentication. Please contact your system administrator.

Please try again or consult your system administrator.

This error occurs if the CA certificates could not be located in the domain group policy. This error can be resolved by forcing the workstation to update its group policy settings. To do this, logon as an administrator on the Windows XP workstation and run the command "gpupdate /force" at a command prompt.

5.4 Invalid Credentials

The following error message may appear after entering the PIN for the PIV card at the logon prompt:

The system could not log you on. Your credentials could not be verified.

This error can occur for a number of reasons, including a mismatch between the UPN and user logon name or an out-of-date domain group policy. First, extract the PIV Authentication certificate from the PIV card using the PIV Data Loader tool (see Appendix A). Examine the certificate's UPN (specified as "Principal Name" in the Subject Alternative Name extension) and make sure it matches the user logon name specified in section 2.3.2. In addition, logon as an administrator on the Windows XP workstation and run the command "gpupdate /force" at a command prompt to refresh the group policy settings.

5.5 NIST VSCR Fails to Initiate Card Insertion Event

When utilizing the NIST VSCR and PIV Card Simulator with Windows Logon, a card insertion event may fail to fire, which prevents the PIN prompt from being displayed. If 30 seconds have passed since the time that the NIST VSCR was configured to "insert" a card and the PIN prompt is not displayed then log into the workstation and examine the Windows Application event log. The following errors may appear in the event log:

Associated Event Viewer entry on *Workstation* (in the Application group):

Description

Couldn't connect to socket in initialize_socket client!

This error indicates that a socket connection could not be established between the NIST VSCR service and the PIV Card Simulator.

Associated Event Viewer entry on *Workstation* (in the Application group):

Description

Failed to connect to the TLP server.

This error indicates that a TLP-224 connection could not be established with the PIV Card Simulator.

Associated Event Viewer entry on *Workstation* (in the Application group):

Description

Card could not be inserted into reader. Failed to establish connection with card simulator.

This error indicates that the NIST VSCR could not "insert" a card because a connection was not established with the PIV Card Simulator.

Resolution

These errors indicate that the PIV Card Simulator is not running and/or the NIST VSCR service has not been configured to connect to the PIV Card Simulator correctly.

Refer to the *Virtual Smart Card Reader User Guide* for instructions on configuring the NIST VSCR service to connect to the PIV Card Simulator (see Appendix E, [6]). Also, when configuring the NIST VSCR service, make sure the "Automatically insert card when service starts" option is not checked.

5.6 General Cryptography Problems

When getting a new card to work with the NIST CSP, one of the most common errors encountered is that the PIV card or PIV Card Simulator is not handling cryptographic functions properly. The usual cause of this problem is due to the header, footer, and padding of the data before and after signing. One error message that can occur after inserting the card and entering the PIN is:

The system could not log you on. An error occurred trying to use this smart card. You can find further details in the event log. Please report this error to the system administrator.

Associated Event Viewer entry on *Workstation* (in the Application group):

Description

An error occurred while signing a message using the inserted smart card: Invalid algorithm specified.

For more information, see Help and Support Center at http://go.microsoft.com/fwlink/events.asp.

Data

0000: 80090008

The 80090008 error indicates that an invalid algorithm was specified.

Associated Event Viewer entry on *Domain Controller* (in the Application group):

Description

An error occurred while verifying a signed message using the inserted smart card: Invalid Signature.

For more information, see Help and Support Center at http://go.microsoft.com/fwlink/events.asp.

Data

0000: 80090006

The 80090006 error indicates that an invalid signature was processed.

Resolution

These errors typically indicate that the bytes in the header of the reply from the PIV card or PIV Card Simulator are incorrect.

Confirm that the correct private and public keys are correctly formatted and loaded into the proper containers on the card. Also, make sure that the PIV card / PIV Card Simulator is passing general authenticate APDU's in the correct format for the NIST CSP.

The NIST CSP expects bytes to be in the following format:

```
Signing Request APDU sent to card (141 bytes):

00 87 06 9A 88          136 bytes to follow

7C                      data objects in the dynamic authentication template
81 85                   133 bytes to follow

81                      challenge request
81 80                   128 bytes to follow

<128 challenge bytes>

82                      response request
00                      0 bytes to follow


Signing Complete, APDU received from card (2 bytes):

61 86                   Successful Execution, 134 bytes to receive

Get Response, APDU sent to card

00 C0 00 00 86

Signed data returned (134 bytes):

7C                      data objects in the dynamic authentication template
84                      authentication code, hash-code of one or more data
                        fields and a witness object
```

```
82                      response

81                      witness
00                      0 bytes to follow

80                      128 bytes to follow

<128 response bytes>

Status Word returned (2 bytes):

90 00

** Signing Complete **
```

Once the PIV card or PIV Card Simulator is configured to send and receive APDUs in the aforementioned format, the NIST CSP's cryptographic calls will work properly.

5.7 Invalid PIN

Initial testing has shown that the PIN for the NIST CSP must be 4 digits. This has not yet been tested exhaustively. If there are issues with PIN validation, set the PIN to 4 digits and re-attempt.

Appendix A—Tools

Appendix A lists all the tools used in this document, their general purpose and where they can be obtained.

Table A-1. Tools

Tool Name	Purpose	How to Obtain
Java Card development kit 2.2.1	Prerequisite for the SP 800-73 Reference Implementation software	Online: http://java.sun.com/products/javacard/dev_kit.html Check the "Still Available for download" section
Java 2 Standard Edition Software Developer's Kit	Prerequisite for the Java Card development kit 2.2.1	Online: http://java.sun.com/javase/downloads/index.jsp
Crypto++ Library 5.2.1	Prerequisite for the SP 800-73 Reference Implementation software	Online: http://www.eskimo.com/~weidai/cryptlib.html#download
zLib Library 1.2.3	Prerequisite for the use of NIST CSP	Online: http://www.zlib.net
BasicCard Kit V5.22	BasicCard applet compilation and loading	Online: http://www.basiccard.com/index.html?instkit.htm Click "BasicCard Kit Setup Package"
Cygwin and OpenSSL	Key pair generation, certificate request creation, key and certificate examination, signature verification	Online: http://cygwin.com Click "Install or update now!" and follow Appendix B for an installation walkthrough.
PIV Data Generator tool	PIV data element generation	Online: http://csrc.nist.gov/groups/SNS/piv/index.html Click "PIV Data Generator and PIV Data Loader" under the downloadable PIV software section and follow the instructions to download. Extract the zip and view the Readme.txt file for additional requirements and instructions on running the tool.
PIV Data Loader tool	PIV data loader	Online: http://csrc.nist.gov/groups/SNS/piv/index.html Click "PIV Data Generator and PIV Data Loader" under the downloadable PIV software section and follow the instructions to download. Extract the zip and view the Readme.txt file for additional requirements and instructions on running the tool.

Tool Name	Purpose	How to Obtain
Bouncy Castle Crypto API	Prerequisite for the PIV Data Generator tool. Provides a lightweight cryptographic API in Java.	Online: http://www.bouncycastle.org/latest_releases.html Click "bcprov-jdkxxx" and "bcmail-jdkxxx", where "xxx" refers to the JDK and Bouncy Castle Crypto API version being used (e.g., "bcprov-jdk15-132.jar")
XVI32 2.51	Hex editor	Online: http://www.chmaas.handshake.de/delphi/freeware/xvi32/xvi32.htm Click "Download" and then "here" to retrieve the XVI32 zip file. Extract the zip and run XVI32.exe.
TestResMan 1.42.00.01	PC/SC APDU Utility	Online: http://www.scmmicro.com/support/pcs_product_drivers.html Click "Utilities" under the download type, read and accept the EULA, click Next, click "TestResMan V1.xx". Extract the zip and run the TestResMan.exe file to launch TestResMan.
TextPad 4.7.3	Enhanced text editor	Online: http://textpad.com/download/ Download and run installation file, txpeng473.exe.
Microsoft certutil Version 402.203.0: 0x80070057 (WIN32: 87)	Command-line Windows certificate and smart card utility	Online: http://www.microsoft.com/downloads/details.aspx?FamilyID=c16ae515-c8f4-47ef-a1e4-a8dcbacff8e3&DisplayLang=en Download and install the Windows Server 2003 Administration Tools Pack. Open a command prompt and type "certutil –scinfo"
Windows Calculator	Useful for converting numbers from Base 10 (decimal) to Base 16 (hexadecimal).	Included with Windows. (Start | Programs | Accessories | Calculator)
Registry Editor	Windows Registry Editor, need to manually add/change/delete registry keys	Included with Windows. (Start | Run | regedt32)

Appendix B—Cygwin

Appendix B describes how to install Cygwin, "a Linux-like environment for Windows."

1. Run setup.exe after downloading it from http://www.cygwin.com/.
2. Click "Next".
3. Keep "Install from Internet" selected and click "Next".
4. Keep defaults for install location (e.g. c:\cygwin), users and text file type and click "Next".
5. Keep default for local package directory (e.g. c:\cygwin\packages) and click "Next".
6. Keep "Direct connection" selected and click "Next".
7. Choose a mirror and click "Next".
8. Package list is downloaded and the Select Packages screen is shown.
9. Expand the "Net" group, scroll down to "openssl: the OpenSSL runtime environment" and click the "Skip" label until the latest version is shown (currently 0.9.8a-1).
10. Click "Next" – All base and OpenSSL packages and dependences are downloaded and installed.
11. Keep the boxes checked if you would like to place a cygwin shortcut on the Desktop and in the Start Menu. Click "Finish".
12. A dialog box indicates that Cygwin Setup is complete. Click "OK" and double-click the Cygwin shortcut on the desktop to launch Cygwin.
13. Type "openssl version" and press enter to test your OpenSSL installation. You should see something similar to the following:

```
$ openssl version
OpenSSL 0.9.8a 11 Oct 2005
```

Appendix C—How to Create a PIV Card

Appendix C describes how to create a PIV card that can be used with Windows Logon. The general steps for creating a PIV card using the NIST tools referenced in this document are:

+ Generate RSA key pairs
+ Generate X.509 certificates from RSA key pairs
+ Load X.509 certificates onto PIV card

Instructions are provided for generating and loading only X.509 certificates onto a PIV card, since these data objects are necessary for Windows Logon. Windows Logon is not dependent on other mandatory PIV data objects, such as the CHUID and Card Capability Container. Hence, instructions have been omitted for generating and loading these other data objects for brevity. Readers who wish to generate and load all mandatory data objects onto a PIV card should consult the documentation for the PIV Data Generator and PIV Data Loader.

C.1 Generate RSA Key Pairs

The first step in creating a PIV card is to generate RSA 1024-bit key pairs, which are later used with the PIV Data Generator tool to create X.509 certificates for a PIV card.

C.1.1 Generate RSA Key Pair with Real PIV Card

Real PIV cards provide the cryptographic functions necessary to support RSA key pair generation on the card. An RSA key pair can be generated by sending a GENERATE ASYMMETRIC KEY PAIR command to the card (see SP 800-73-1). The PIV Data Loader tool is used to send this command to a real PIV card.

1. Launch PIV Data Loader.
2. Select Tools | Options.
3. Enter the 0x9B key and Global PIN associated with the PIV card (refer to the PIV card vendor's documentation if this is not known).
4. Click Save.
5. Select the card reader that the PIV card is inserted into from the dropdown list.
6. Click Connect. The controls in the Asymmetric Key Pair group box are enabled.
7. To generate the PIV Authentication key pair, select 'PIV Authentication Key' as the key name.
8. Select 'RSA 1024' as the cryptographic algorithm.
9. Enter "pivauth_public_key.dat" in the 'Output Location' field.

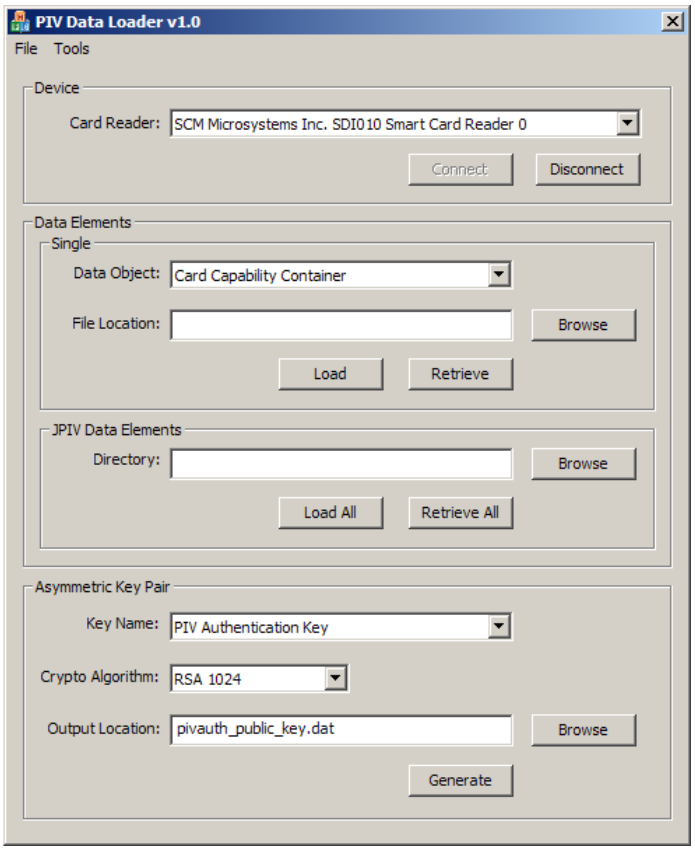

Figure C-1. Generating RSA Key Pairs with PIV Data Loader

10. Click Generate.
11. Once the PIV Authentication key pair has been generated, a status dialog will be displayed. Click OK.
12. To generate the Digital Signature key pair, select 'Digital Signature Key' as the key name.
13. Enter "digitalsig_public_key.dat" in the 'Output Location' field.
14. Click Generate.
15. Once the Digital Signature key pair has been generated, a status dialog will be displayed. Click OK.
16. To generate the Key Management key pair, select 'Key Management Key' as the key name.
17. Enter "keymanage_public_key.dat" in the 'Output Location' field.
18. Click Generate.
19. Once the Key Management key pair has been generated, a status dialog will be displayed. Click OK.
20. To generate the Card Authentication key pair, select 'Card Authentication Key' as the key name.
21. Enter "cardauth_public_key.dat" in the 'Output Location' field.
22. Click Generate.
23. Once the Card Authentication key pair has been generated, a status dialog will be displayed. Click OK.
24. Click Disconnect to disconnect from the PIV card.
25. Select File | Exit to close the PIV Data Loader tool.

Files are created in the PIV Data Loader directory which contain the public keys of the generated RSA key pairs.

C.1.2 Generate RSA Key Pair for BasicCard or Card Simulator

OpenSSL can be used to generate an RSA 1024-bit key pair that is loaded onto a BasicCard or PIV Card Simulator. Unlike a real PIV card, the BasicCard and PIV Card Simulator can only store the RSA 1024-bit key pair of the PIV Authentication key. Hence, RSA key pairs for the Digital Signature, Key Management, and Card Authentication keys will not be created.

Note that Cygwin must be installed in order to access the OpenSSL application. Refer to Appendix B for information on how to install Cygwin.

C.1.2.1 Create a RSA 1024-bit key pair with OpenSSL

1. Launch cygwin.
2. Execute command: `openssl genrsa –out private_key.pem 1024`
   e.g.

```
$ openssl genrsa –out private_key.pem 1024
Generating RSA private key, 1024 bit long modulus
..............................++++++
.....................................................................++++++
e is 65537 (0x10001)
```

Private_key.pem contains both the public and private keys. It is not password protected; therefore, ensure the file is safe.

C.1.2.2 Extract a Public Key from the Private Key

1. Launch cygwin.
2. Execute command: `openssl rsa –pubout –in private_key.pem –out public_key.pem`
   e.g.

```
$ openssl rsa –pubout –in private_key.pem –out public_key.pem
writing RSA key
```

A new file is created, public_key.pem, with *only* the public key.

Note: It is not necessary to extract the public key using this command to create the public key to be put on the card since the public key components (modulus & exponent) are included in the private key and are viewable using the command in section C.1.2.3.

C.1.2.3 View the Public and Private Key

1. Launch cygwin.
2. Execute command: `openssl rsa –text –in private_key.pem`

All parts of private_key.pem are printed to the screen. This includes the modulus (also referred to as public key and n), public exponent (also referred to as e and exponent; default value is 0x010001), private exponent, and primes used to create keys (prime1, also called p, and prime2, also called q), as well as a few other variables used to perform RSA operations faster and the Base64 PEM encoded version of the key.

C.2 Generate X.509 Certificates

After RSA 1024-bit key pairs have been generated, the next step in creating a PIV card is to generate X.509 certificates that are PIV-compliant using the PIV Data Generator tool. The following subsections provide steps involved in creating X.509 certificates.

C.2.1 Extract Public Key

If using a BasicCard or PIV Card Simulator, the public key from the RSA key pair generated in section C.1.2.1 must be extracted and formatted to be compatible with the PIV Data Generator tool (real PIV card users who generated RSA key pairs using the PIV Data Loader tool can skip this step and proceed to section C.2.2). The public key can be extracted using the following steps.

1. Launch cygwin.
2. Execute command: "openssl rsa –text –in private_key.pem"
   In the output of this command, copy the text in the "modulus:" section:
   ```
   modulus:
    00:c8:9b:c3:4e:e4:9d:50:37:16:7b:96:b7:a0:1b:
    42:e9:bf:a8:e1:1c:a1:8e:ff:17:35:fe:22:5a:2a:
    10:2d:9c:aa:e1:14:ee:3b:ab:3c:b5:9e:db:1a:2c:
    6b:45:61:1c:15:e6:90:e1:2e:22:be:a6:db:c7:44:
    21:a3:47:22:35:8a:99:2e:20:bb:b8:68:bd:6f:77:
    4c:29:72:f0:14:9c:42:77:b9:66:af:e3:9b:05:1a:
    37:fd:87:36:be:7f:a0:e1:c7:94:f2:22:57:3a:94:
    16:7c:5c:f8:5e:84:ac:0d:5d:be:02:23:57:7c:f2:
    f4:a4:27:2d:3a:14:c4:88:7f
   ```
3. Paste the hex string text (everything after "modulus:", beginning with "00:c8:" and ending with "88:7f") into an editor of your choice, such as TextPad (see Appendix A).
4. If your modulus contains a leading "00", delete it.
5. Remove all spaces, line breaks and colons so that all you have remaining is one large hex string (representing exactly 128 bytes. It will contain 256 characters – each byte is represented by 2 characters):
   ```
   c89bc34ee49d5037167b96b7a01b42e9bfa8e11ca18eff1735fe225a2a102d9caae114e
   e3bab3cb59edb1a2c6b45611c15e690e12e22bea6dbc74421a34722358a992e20bbb868
   bd6f774c2972f0149c4277b966afe39b051a37fd8736be7fa0e1c794f222573a94167c5
   cf85e84ac0d5dbe0223577cf2f4a4272d3a14c4887f
   ```
6. Now, add the PIV Data Generator tool public key header and footer to this string. Before the first digit insert: "7f49818981818100" and after the last digit add: "8203010001".
   a. 7f49 is the data objects tag
   b. 8189 is the length of the public key information that follows (decimal value of 0x89 = 137 bytes for modulus and exponent)
   c. 81 is the modulus tag
   d. 8181 is the length of the modulus that follows plus a 1-byte padding char (decimal value of 0x81 = 129 bytes)
   e. 00 is a padding char set to zero since integers in ASN.1 are encoded in two's complement
   f. 82 is the exponent tag
   g. 03 is the length of the exponent that follows
   h. 010001 is the value of the exponent
   i. The final version of the public key above:
      ```
      7f49818981818100c89bc34ee49d5037167b96b7a01b42e9bfa8e11ca18eff173
      5fe225a2a102d9caae114ee3bab3cb59edb1a2c6b45611c15e690e12e22bea6db
      c74421a34722358a992e20bbb868bd6f774c2972f0149c4277b966afe39b051a3
      ```

```
7fd8736be7fa0e1c794f222573a94167c5cf85e84ac0d5dbe0223577cf2f4a427
2d3a14c4887f8203010001
```

C.2.2 Create X.509 Certificates with the PIV Data Generator Tool

1. Launch the PIV Data Generator tool.
2. Navigate to the "Crypto Provider" tab and complete all fields. For the "Keystore Path" field, enter the full path to the "jks_keystore" file located in the "extra_files" subdirectory of the PIV Data Generator tool. All remaining fields should be set to the values specified in the "example input.txt" file of the PIV Data Generator tool directory. See example below.
3. Click Load Certs to load the key store. See example below.

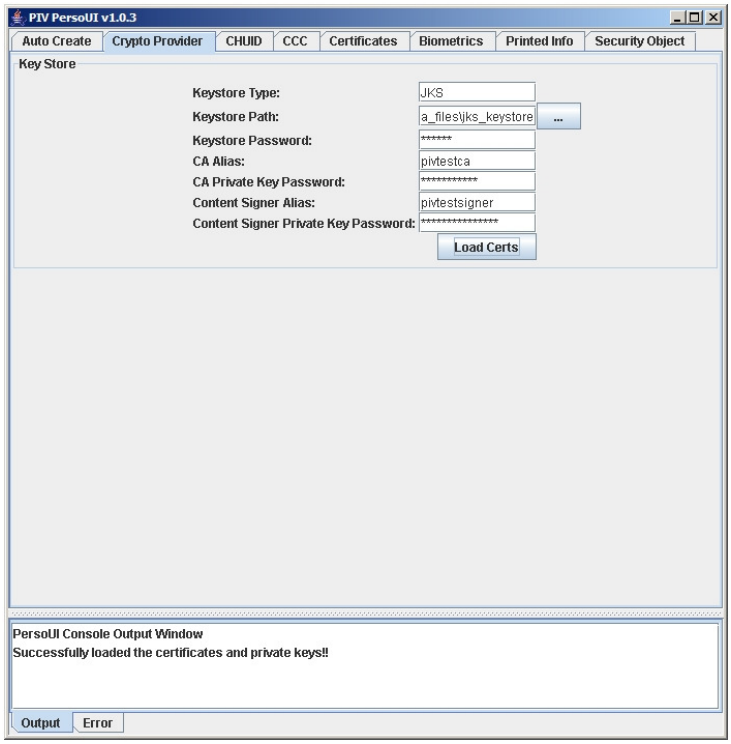

Figure C-2. PIV Data Generator Crypto Provider Tab

4. Navigate to the "CHUID" tab and complete all FASC-N fields. Sample values can be found in the "example input.txt" file of the PIV Data Generator tool directory.
5. Click Generate in the FASC-N group box to generate the FASC-N. See example below.

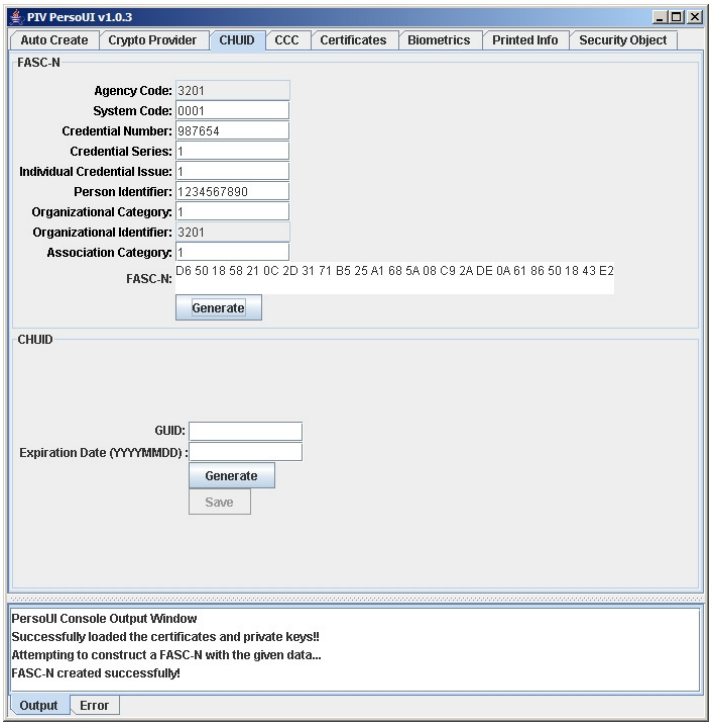

Figure C-3. PIV Data Generator CHUID Tab – FASC-N Fields

6. Complete all CHUID fields on the "CHUID" tab. Sample values can be found in the "example input.txt" file of the PIV Data Generator tool directory.
7. Click Generate in the CHUID group box to generate the CHUID. See example below.

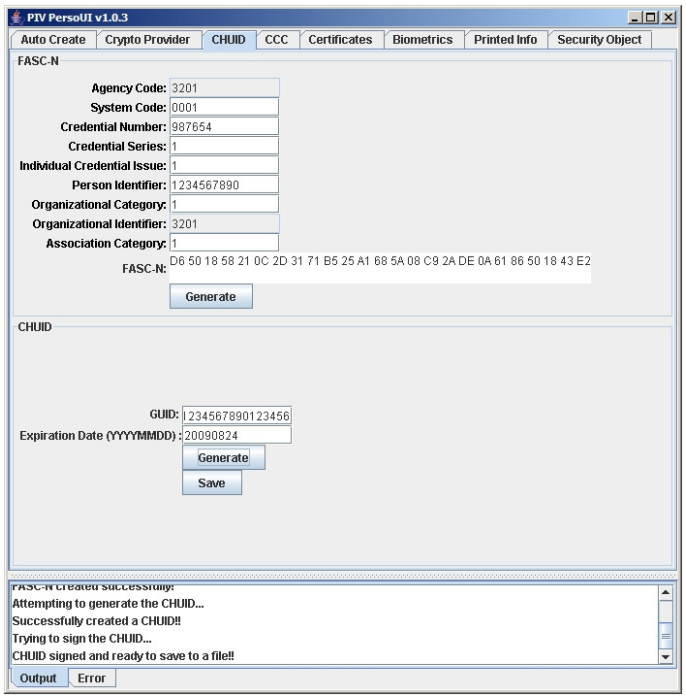

Figure C-4. PIV Data Generator CHUID Tab – CHUID Fields

8. Navigate to the "Certificates" tab and select "PIV Auth Cert" for the certificate type.
9. Enter the public key for the certificate.
    a. If using a real PIV card, select "Get public key from file" and enter the file path to the pivauth_public_key.dat file created in section C.1.1.
    b. If using a BasicCard, select "Get public key from text", copy the 282 characters (141 bytes) representing the public key from step 6 of section C.2.1 to the clipboard, and paste the clipboard contents to the "Public key:" edit box by placing the cursor in the edit box and pressing Ctrl-V.
10. Enter "http://localhost/crl/ca.crl" for the "CRL http URI" field.
11. Complete all remaining fields on the "Certificates" tab. Sample values can be found in the "example input.txt" file of the PIV Data Generator tool directory. Ensure the "UPN" field is set to the name of the user account to associate with the certificate.
12. Click Generate to generate the PIV Authentication certificate. See example below.

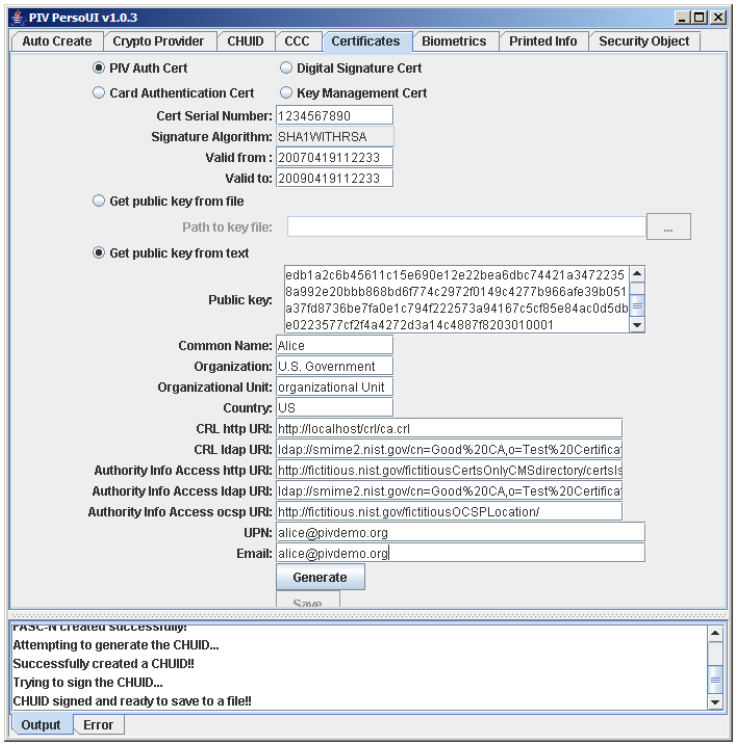

Figure C-5. PIV Data Generator Certificates Tab

13. After generating the PIV Authentication certificate, the Save button should be enabled. Click Save to save the certificate to a file.
14. A Save dialog is displayed. Browse to a directory and enter "pivauth.cer" for the filename to save the certificate to.
15. Click Save to save the certificate to the specified file.
16. On the "Certificates" tab, select "Digital Signature Cert" for the certificate type.
17. Enter the public key for the certificate.
    a. If using a real PIV card, select "Get public key from file" and enter the file path to the digitalsig_public_key.dat file created in section C.1.1.
    b. If using a BasicCard, this step can be skipped since the BasicCard only supports storage of the RSA key pair for the PIV Authentication key and hence, the certificate will use the same public key specified in step 9.
18. Click Generate to generate the Digital Signature certificate.

19. After generating the Digital Signature certificate, the Save button should be enabled. Click Save to save the certificate to a file.
20. A Save dialog is displayed. Browse to a directory and enter "digitalsig.cer" for the filename to save the certificate to.
21. Click Save to save the certificate to the specified file.
22. On the "Certificates" tab, select "Key Management Cert" for the certificate type.
23. Enter the public key for the certificate.
    a. If using a real PIV card, select "Get public key from file" and enter the file path to the keymanage_public_key.dat file created in section C.1.1.
    b. If using a BasicCard, this step can be skipped since the BasicCard only supports storage of the RSA key pair for the PIV Authentication key and hence, the certificate will use the same public key specified in step 9.
24. Click Generate to generate the Key Management certificate.
25. After generating the Key Management certificate, the Save button should be enabled. Click Save to save the certificate to a file.
26. A Save dialog is displayed. Browse to a directory and enter "keymanage.cer" for the filename to save the certificate to.
27. Click Save to save the certificate to the specified file.
28. On the "Certificates" tab, select "Card Authentication Cert" for the certificate type.
29. Enter the public key for the certificate.
    a. If using a real PIV card, select "Get public key from file" and enter the file path to the cardauth_public_key.dat file created in section C.1.1.
    b. If using a BasicCard, this step can be skipped since the BasicCard only supports storage of the RSA key pair for the PIV Authentication key and hence, the certificate will use the same public key specified in step 9.
30. Click Generate to generate the Card Authentication certificate.
31. After generating the Card Authentication certificate, the Save button should be enabled. Click Save to save the certificate to a file.
32. A Save dialog is displayed. Browse to a directory and enter "cardauth.cer" for the filename to save the certificate to.
33. Click Save to save the certificate to the specified file.

C.2.3 Examine the X.509 Certificates with OpenSSL

The PIV Data Generator tool pre-pends certificate tag information to generated certificates that are incompatible with OpenSSL. In order to view certificates in OpenSSL, a temporary copy of the certificates should be created and the extra tag information must be removed from the temporary copy. The following steps describe this process:

1. Load XVI32 (see Appendix A).
2. Copy the pivauth.cer file created in section C.2.2 and rename it pivauth_temp.cer.
3. Open the pivauth_temp.cer file that was just created by selecting File | Open.
4. Select the first four bytes of the pivauth_temp.cer file by holding shift and pressing the right arrow key three times.
5. Delete the first four bytes from the pivauth_temp.cer file by selecting Edit | Block delete (they are specific to PIV and are not compatible with OpenSSL).
6. Save the changes to the pivauth_temp.cer file by selecting File | Save.
7. Close the file by selecting File | Close.
8. Repeat steps 2 – 7 for the digitalsig.cer, keymanage.cer, and cardauth.cer files created in section C.2.2, renaming the copied files digitalsig_temp.cer, keymanage_temp.cer, and cardauth_temp.cer respectively.

9. Close XVI32.

Once the extra tag information has been removed from the certificates, they can be viewed using the following steps:

1. Launch cygwin.
2. Execute command: `openssl x509 -text -inform DER -in [cert filename]`
3. The certificate file is examined and attributes displayed. See example below.

```
$ openssl x509 -text -inform DER -in pivauth_temp.cer
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1234567890 (0x499602d2)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, O=NIST, CN=PIV Test CA
        Validity
            Not Before: Apr 19 15:22:33 2007 GMT
            Not After : Apr 19 15:22:33 2009 GMT
        Subject: C=US, OU=NIST Computer Security Division - PIV Test, O=U.S.
Government, CN=John G.
Doe - PIV Test
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:c8:9b:c3:4e:e4:9d:50:37:16:7b:96:b7:a0:1b:
                    42:e9:bf:a8:e1:1c:a1:8e:ff:17:35:fe:22:5a:2a:
                    10:2d:9c:aa:e1:14:ee:3b:ab:3c:b5:9e:db:1a:2c:
                    6b:45:61:1c:15:e6:90:e1:2e:22:be:a6:db:c7:44:
                    21:a3:47:22:35:8a:99:2e:20:bb:b8:68:bd:6f:77:
                    4c:29:72:f0:14:9c:42:77:b9:66:af:e3:9b:05:1a:
                    37:fd:87:36:be:7f:a0:e1:c7:94:f2:22:57:3a:94:
                    16:7c:5c:f8:5e:84:ac:0d:5d:be:02:23:57:7c:f2:
                    f4:a4:27:2d:3a:14:c4:88:7f
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:

keyid:EB:DA:19:D2:08:42:8D:F4:DE:25:87:69:C9:BB:AB:0C:D3:96:30:01

            X509v3 Subject Key Identifier:
                A5:80:ED:7C:B5:52:25:26:55:65:09:58:3B:4A:07:F2:59:25:BD:99
            X509v3 Key Usage: critical
                Digital Signature
            X509v3 Extended Key Usage:
                TLS Web Client Authentication, Microsoft Smartcardlogin,
2.5.29.37.0
            X509v3 Certificate Policies:
                Policy: 2.16.840.1.101.3.2.1.3.13

            X509v3 CRL Distribution Points:

URI:http://fictitious.nist.gov/fictitiousCRLdirectory/fictitiousCRL1.crl
```

```
URI:ldap://smime2.nist.gov/cn=Good%20CA,o=Test%20Certificates,c=US?certificat
eRevoca
tionList

            Authority Information Access:
                OCSP - URI:http://fictitious.nist.gov/fictitiousOCSPLocation/
                CA Issuers -
URI:http://fictitious.nist.gov/fictitiousCertsOnlyCMSdirectory/certsIss
uedToGoodCA.p7c
                CA Issuers -
URI:ldap://smime2.nist.gov/cn=Good%20CA,o=Test%20Certificates,c=US?cACe
rtificate,crossCertificatePair

            X509v3 Subject Alternative Name:
                othername:<unsupported>, othername:<unsupported>
            2.16.840.1.101.3.6.9.1:
                ...
    Signature Algorithm: sha1WithRSAEncryption
        25:6b:07:de:51:65:3b:af:17:0f:2b:09:a9:4c:64:36:3c:b0:
        0c:d2:91:44:ff:79:b8:db:8a:5f:74:1d:3a:19:19:2b:29:ed:
        9d:2f:b0:7a:b3:10:f1:ce:90:dd:ff:88:60:08:18:c3:d7:4b:
        38:55:4a:03:7f:5d:70:b6:1f:0f:70:80:d9:4c:4f:a9:97:dc:
        d0:8e:6b:c6:00:57:ae:15:0b:90:fc:d5:8b:1c:6f:f6:34:5f:
        8a:b0:a9:29:ea:24:7c:b4:9b:9e:1d:22:8e:aa:36:4e:03:5b:
        03:42:5f:63:8b:36:f2:63:6f:33:2c:9c:9a:b6:7e:2e:9c:d7:
        2b:c5:24:f5:14:06:07:03:45:f2:5a:4b:b2:38:91:03:82:b3:
        b0:58:89:2b:4d:92:ff:92:63:ee:4d:01:4b:05:48:a1:c7:57:
        2b:b2:b2:2a:95:20:1c:c3:9c:6b:cf:24:43:4d:9f:49:ab:c5:
        88:30:85:9b:3d:45:55:46:67:c7:fd:ea:4c:b4:7c:eb:62:8c:
        66:7c:13:d1:47:8c:81:9f:bc:80:33:3b:6b:bc:b4:34:b6:f4:
        54:75:88:73:ea:0b:2d:95:4b:0a:a0:06:fd:c8:a2:2a:d0:09:
        96:1f:57:e8:67:79:00:a8:c8:f7:77:d2:98:14:2e:a0:3b:c9:
        cc:8c:28:4d
-----BEGIN CERTIFICATE-----
MIIFhzCCBG+gAwIBAgIESZYC0jANBgkqhkiG9w0BAQUFADAyMQswCQYDVQQGEwJV
UzENMAsGA1UEChMETklTVDEUMBIGA1UEAxMLUElWIFRlc3QgQ0EwHhcNMDcwNDE5
MTUyMjMzWhcNMDkwNDE5MTUyMjMzWjB9MQswCQYDVQQGEwJVUzEzMDEGA1UECxMq
TklTVCBDb21wdXRlciBTZWN1cml0eSBEaXZpc2lvbiAtIFBJViBUZXN0MRgwFgYD
VQQKEw9VLlMuIEdvdmVybm1lbnQxHzAdBgNVBAMTFkpvaG4gRy4gRG9lIC0gUElW
IFRlc3QwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMibw07knVA3FnuWt6Ab
Qum/qOEcoY7/FzX+IloqEC2cquEU7jurPLWe2xosa0VhHBXmkOEuIr6m28dEIaNH
IjWKmS4gu7hovW93TCly8BScQne5Zq/jmwUaN/2HNr5/oOHHlPIiVzqUFnxc+F6E
rA1dvgIjV3zy9KQnLToUxIh/AgMBAAGjggLcMIIC2DAfBgNVHSMEGDAWgBTr2hnS
CEKN9N4lh2nJu6sM05YwATAdBgNVHQ4EFgQUpYDtfLVSJSZVZQlYO0oH8lklvZkw
DgYDVR0PAQH/BAQDAgeAMCUGA1UdJQQeMBwGCCsGAQUFBwMCBgorBgEEAYI3FAIC
BgRVHSUAMBcGA1UdIAQQMA4wDAYKYIZIAWUDAgEDDTCBtAYDVR0fBIGsMIGpMIGm
oIGjoIGghkRodHRwOi8vZmljdGl0aW91cy5uaXN0Lmdvdi9maWN0aXRpb3VzQ1JM
ZGlyZWN0b3J5L2ZpY3RpdGlvdXNDUkwxLmNybIZYbGRhcDovL3NtaW1lMi5uaXN0
Lmdvdi9jbj1Hb29kJTIwQ0Esbz1UZXN0JTIwQ2VydGlmaWNhdGVzLGM9VVM/Y2Vy
dGlmaWNhdGVSZXZvY2F0aW9uTGlzdDCCASEGCCsGAQUFBwEBBIIBEzCCAQ8wPgYI
KwYBBQUHMAGGMmh0dHA6Ly9maWN0aXRpb3VzLm5pc3QuZ292L2ZpY3RpdGlvdXNP
Q1NQTG9jYXRpb24vMF4GCCsGAQUFBzAChlJodHRwOi8vZmljdGl0aW91cy5uaXN0
Lmdvdi9maWN0aXRpb3VzQ2VydHNPbmx5Q01TZGlyZWN0b3J5L2NlcnRzSXNzdWVk
VG9Hb29kQ0EucDdjMG0GCCsGAQUFBzAChmFsZGFwOi8vc21pbWUyLm5pc3QuZ292
L2NuPUdvb2QlMjBDQSxvPVRlc3QlMjBDZXJ0aWZpY2F0ZXMsYz1VUz9jQUNlcnRp
ZmljYXRlLGNyb3NzQ2VydGlmaWNhdGVQYWlyMFgGA1UdEQRRME+gJwYIYIZIAWUD
```

```
BgagGwQZ1lAYWCEMLTFxtSWhaFoIySreCmGGUBhD4qAkBgorBgEEAYI3FAIDoBYM
FGpvaG5fZG9lQHBpdmRlbW8ub3JnMBAGCWCGSAFlAwYJAQQDAQEAMA0GCSqGSIb3
DQEBBQUAA4IBAQAlawfeUWU7rxcPKwmpTGQ2PLAM0pFE/3m424pfdB06GRkrKe2d
L7B6sxDxzpDd/4hgCBjD10s4VUoDf11wth8PcIDZTE+pl9zQjmvGAFeuFQuQ/NWL
HG/2NF+KsKkp6iR8tJueHSKOqjZOA1sDQl9jizbyY28zLJyatn4unNcrxST1FAYH
A0XyWkuyOJEDgrOwWIkrTZL/kmPuTQFLBUihx1crsrIqlSAcw5xrzyRDTZ9Jq8WI
MIWbPUVVRmfH/epMtHzrYoxmfBPRR4yBn7yAMztrvLQ0tvRUdYhz6gstlUsKoAb9
yKIq0AmWH1foZ3kAqMj3d9KYFC6gO8nMjChN
-----END CERTIFICATE-----
```

Notes:
1. The Public Key in the certificate is identical to the Public Key generated in section C.1.
2. The Subject Alternative Name, which contains the user's UPN – needed for Smart Card Logon, is not displayed by OpenSSL. It will be shown in the next section.

C.2.4 Examine the Smart Card Logon Certificate with Windows

The PIV Data Generator tool pre-pends certificate tag information to generated certificates that are incompatible with Windows. In order to view a certificate in Windows, a temporary copy of the certificate should be created and the extra tag information must be removed from the temporary copy. See section C.2.3 for instructions on doing this. Once the extra tag information has been removed, the following steps can be performed to view the certificate in Windows:

1. Log into a Windows Server or XP Workstation on the domain that trusts the CA that issued the X.509 certificate. See section 2.2 on how to configure a domain to trust the issuing CA – in this case, the PIV Data Generator tool.
2. Copy a certificate file created in section C.2.3 to the desktop.
3. Double-click the certificate file to launch Windows Certificate Viewer. See screenshots below.

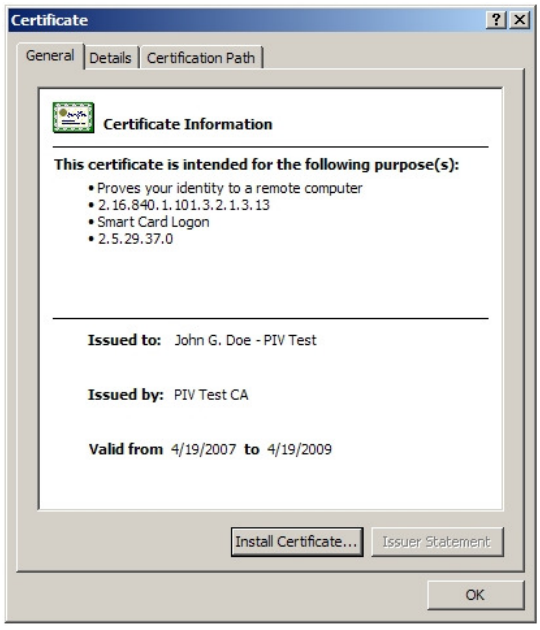

Figure C-6. X.509 Certificate – General

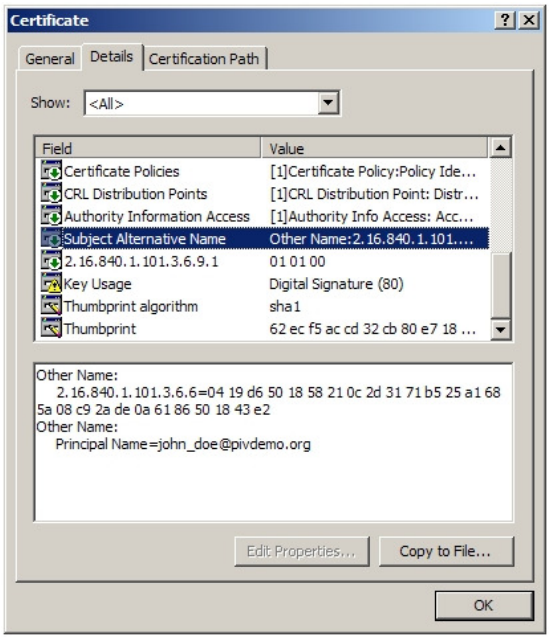

Figure C-7. X.509 Certificate – Details – Subj. Alt. Name

Notes:
1. The Public Key in the certificate is identical to the Public Key generated in section C.1.
2. The Subject Alternative Name, which contains the user's UPN – needed for Smart Card Logon, is shown in Figure C-7. General naming convention is username@domain.com

C.3 Load X.509 Certificates

Once X.509 certificates have been generated, the final step in creating a PIV card is to load the certificates onto the card.

C.3.1 Load a Real PIV Card

Section C.1.1 was used to generate RSA key pairs on a real PIV card. In order to finish configuring the card, the certificates created in section C.2.2 need to be loaded onto the PIV card. Data elements are loaded onto a PIV card using the PUT DATA command (see SP 800-73-1). The PIV Data Loader tool can be used to send this command to a real PIV card.

1. Launch PIV Data Loader.
2. Select Tools | Options.
3. Enter the 0x9B key and Global PIN associated with the PIV card (refer to the PIV card vendor's documentation if this is not known).
4. Click Save.
5. Select the card reader that the PIV card is inserted into from the dropdown list.
6. Click Connect. The controls in the Data Elements group box are enabled.
7. Select 'X.509 Certificate for PIV Authentication' as the data object.
8. Enter the file path to the pivauth.cer file created in section C.2.2 in the 'File Location' field.

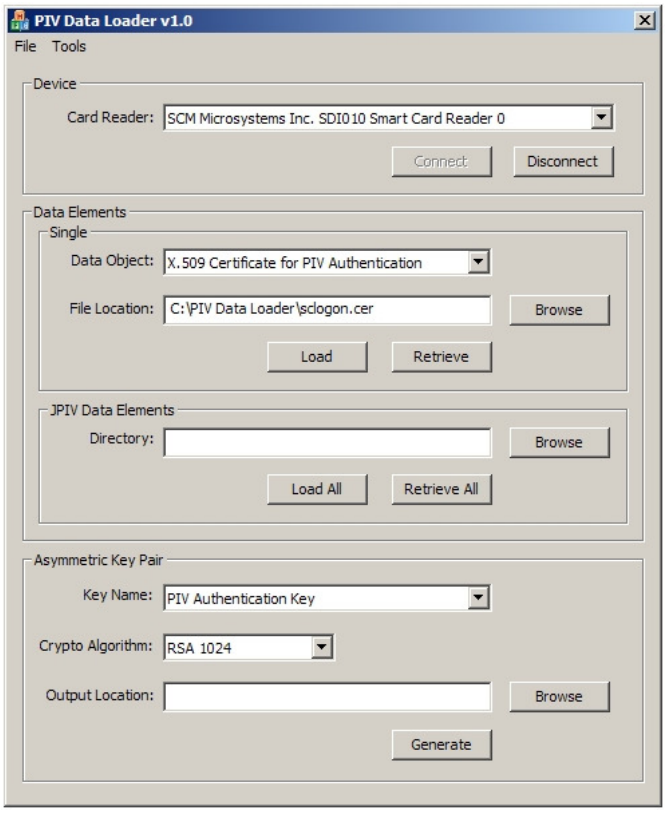

Figure C-8. Load Certificate Using PIV Data Loader

9. Click Load.
10. Once the PIV Authentication certificate has been loaded onto the PIV card, a status dialog will be displayed. Click OK.
11. Select 'X.509 Certificate for Digital Signature' as the data object.
12. Enter the file path to the digitalsig.cer file created in section C.2.2 in the 'File Location' field.
13. Click Load.
14. Once the Digital Signature certificate has been loaded onto the PIV card, a status dialog will be displayed. Click OK.
15. Select 'X.509 Certificate for Key Management' as the data object.
16. Enter the file path to the keymanage.cer file created in section C.2.2 in the 'File Location' field.
17. Click Load.
18. Once the Key Management certificate has been loaded onto the PIV card, a status dialog will be displayed. Click OK.
19. Select 'X.509 Certificate for Card Authentication' as the data object.
20. Enter the file path to the cardauth.cer file created in section C.2.2 in the 'File Location' field.
21. Click Load.
22. Once the Card Authentication certificate has been loaded onto the PIV card, a status dialog will be displayed. Click OK.
23. Click Disconnect to disconnect from the PIV card.
24. Select File | Exit to close the PIV Data Loader tool.

C.3.2 Load a BasicCard

C.3.2.1 BasicCard Overview

BasicCard is a programmable smart card available from ZeitControl Cardsystems GmbH, based in Germany. This card comes with its own OS and as the name implies supports the BASIC programming language for its applets.

NIST has developed a BasicCard that implements the PIV interfaces as described in NIST SP 800-73-1. A development BasicCard can be purchased online through ZeitControl at http://www.basiccard.com/.

The card version used in this document is "BasicCard ZC 4.5D Rev F". This version of the card contains the RSA 1024-bit key and algorithm support as well as DES and Triple-DES.

C.3.2.2 Install PIV BasicCard Reference Implementation

Download and extract the PIVCard.zip package from the NIST website onto the C:\NIST\BasicCard\PivCard directory. The NIST BasicCard reference implementation can be found at http://csrc.nist.gov/groups/SNS/piv/download.html under the item "Example PIV Card Code Package" in the "Downloadable PIV Software" section. For this walkthrough, this will be the base directory.

C.3.2.3 Setup BasicCard PIV Project

The BasicCard Integrated Development Environment (IDE), including a BasicCard compiler and applet loader is also available (at no charge) online at http://www.basiccard.com/index.html?instkit.htm. For first time users, download the BasicCardKit.zip file by clicking on the "BasicCard Kit Setup Package". The version used for this guide is V5.22 dated March 21, 2005.

Download and install the BasicCardKit.zip package. The program will be installed in the C:\BasicCardPro\ directory. For this walkthrough, this will be the base directory.

After downloading and installing the BasicCard IDE from the website above, launch the ZeitControl Professional IDE from the BasicCard Pro group in Start Menu > Programs.

Figure C-9. ZeitControl Professional IDE

1. Select Project | New from the IDE menu.
2. Select the BasicCard Programs tab and click Add.
3. Browse to the directory where you extracted (e.g., C:\NIST\BasicCard\PivCard in section C.3.2.2) the PIV BasicCard source files, select PivCard.BAS and click Open.
4. The BasicCard Program Options dialog is displayed. Apply the following configuration settings:
    a. Card Type: Professional: Select ZC45D_F.zcf from the BasicCardPro installation directory's subfolder "Pro" (e.g. C:\BasicCardPro\Pro\ZC45D_F.zcf)
    b. Card State: TEST
    c. Source file: Already selected – Absolute path to PivCard.BAS file (e.g. C:\NIST\BasicCard\PivCard\PivCard.BAS)

d. Include paths: Add the following directories, several depend on your BasicCardPro installation directory, and the last one depends on where you extracted the PIV BasicCard source files:
c:\BasicCardPro\inc;c:\BasicCardPro\lib;c:\BasicCardPro\pro;c:\BasicCardPro\tools;c:\BasicCardPro\lib\curves;C:\NIST\BasicCard\PivCard
e. Output files: Select "Image" (Debug already selected)
f. P-Code Stack Size: Check the box and enter "80"

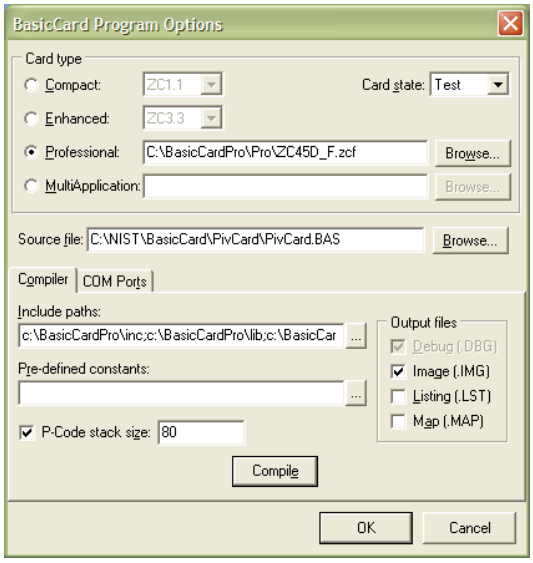

Figure C-10. BasicCard Program Options

5. Click Compile.

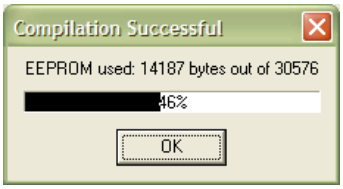

Figure C-11. BasicCard Compilation Successful

6. Click OK and save the BasicCard Program in the same directory as the source files (file: PivCard.zcc).
7. Click OK on the Project Options dialog box and save the ZeitControl Project in the same directory as the source files (file: PivCard.zcp).
8. Close the ZeitControl Professional IDE.

The BasicCard source is compiled and the image is ready to be loaded onto a BasicCard. The next step is to load the PIV Authentication key pair and certificate into this BasicCard project and recompile. In addition, the Digital Signature, Key Management, and Card Authentication certificates will be loaded as well (the BasicCard does not support loading of the key pair for these keys).

C.3.2.4 Extract PIV Authentication Key Pair

PIV Authentication Public Key Extraction

1. Extract the public key from the key pair generated in section C.1.2.1:
    a. Launch cygwin.
    b. Execute command: "openssl rsa -text -in private_key.pem"
    In the output of this command, copy the text in the "modulus:" section:
    ```
    modulus:
        00:c8:9b:c3:4e:e4:9d:50:37:16:7b:96:b7:a0:1b:
        42:e9:bf:a8:e1:1c:a1:8e:ff:17:35:fe:22:5a:2a:
        10:2d:9c:aa:e1:14:ee:3b:ab:3c:b5:9e:db:1a:2c:
        6b:45:61:1c:15:e6:90:e1:2e:22:be:a6:db:c7:44:
        21:a3:47:22:35:8a:99:2e:20:bb:b8:68:bd:6f:77:
        4c:29:72:f0:14:9c:42:77:b9:66:af:e3:9b:05:1a:
        37:fd:87:36:be:7f:a0:e1:c7:94:f2:22:57:3a:94:
        16:7c:5c:f8:5e:84:ac:0d:5d:be:02:23:57:7c:f2:
        f4:a4:27:2d:3a:14:c4:88:7f
    ```
2. Paste the hex string text (everything after "modulus:", beginning with "00:c8:" and ending with "88:7f") into an editor of your choice, such as TextPad (see Appendix A).
3. If your modulus contains a leading "00", delete it. (This works in OpenSSL, but not on the BasicCard)
4. Remove all spaces, line breaks and colons so that all you have remaining is one large hex string (representing exactly 128 bytes. It will contain 256 characters – each byte is represented by 2 characters):
    ```
    c89bc34ee49d5037167b96b7a01b42e9bfa8e11ca18eff1735fe225a2a102d9caae114e
    e3bab3cb59edb1a2c6b45611c15e690e12e22bea6dbc74421a34722358a992e20bbb868
    bd6f774c2972f0149c4277b966afe39b051a37fd8736be7fa0e1c794f222573a94167c5
    cf85e84ac0d5dbe0223577cf2f4a4272d3a14c4887f
    ```
5. Now, add the BasicCard header and footer to this string. Before the first digit insert: "0583" and after the last digit add: "010001".
    a. 05 is the tag indicating this is a key
    b. 83 is the length of the data that follows (decimal value of 0x83: 131 bytes = 128 byte modulus + 3 byte exponent)
    c. 010001 is the value of the exponent
    d. The final version of the key above:
    ```
    0583c89bc34ee49d5037167b96b7a01b42e9bfa8e11ca18eff1735fe225a2a102
    d9caae114ee3bab3cb59edb1a2c6b45611c15e690e12e22bea6dbc74421a34722
    358a992e20bbb868bd6f774c2972f0149c4277b966afe39b051a37fd8736be7fa
    0e1c794f222573a94167c5cf85e84ac0d5dbe0223577cf2f4a4272d3a14c4887f
    010001
    ```
6. Copy these 266 characters (133 bytes) to the clipboard and load XVI32 (see Appendix A).
7. Create a new file in XVI32 by selecting File | New
8. Paste the hex string on the clipboard into the new file: Edit | Clipboard | Paste from hex string
9. Click the last byte (01) and confirm the value of "Adr. hex:" in the lower left of the XVI32 window equals "84". Since the first box equals 00, the total length of the Public Key is 0x85 or 133 bytes.

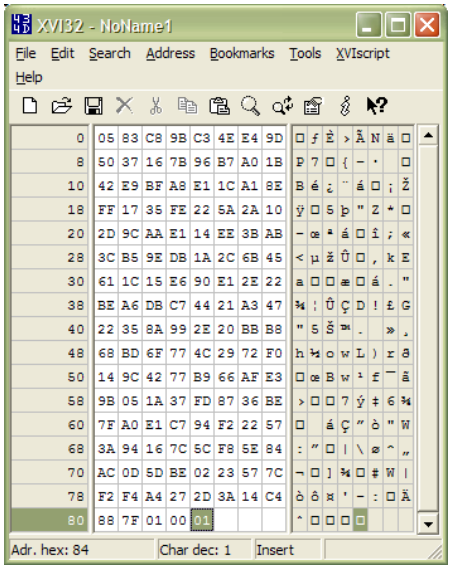

Figure C-12. XVI32: BasicCard Public Key

10. Select File | Save and place this file in the subdirectory of your BasicCard code named "KeyFiles". The file should be titled "PublicKey.bin" – you can overwrite the current PublicKey.bin file in the KeyFiles directory.

Note: The keys must be placed in this directory and named exactly as indicated for the BasicCard code to compile the keys properly.

PIV Authentication Private Key Extraction

1. Extract the private key from the key pair generated in section C.1.2.1:
   a. Launch cygwin.
   b. Execute command: "openssl rsa -text -in private_key.pem"
   In the output of this command, copy the text in the "prime1:" and "prime2:" sections:

```
prime1:
    00:f4:45:71:94:38:27:0e:67:cb:a6:1c:43:16:e3:
    fc:c1:f5:01:4a:c8:9c:ba:06:8d:93:9e:dc:b7:55:
    35:8b:0f:0b:01:f9:0d:98:4c:9a:11:1b:6e:69:04:
    c7:ec:5c:3a:46:0e:ed:21:75:02:ac:f3:8f:37:11:
    43:55:53:75:47
prime2:
    00:d2:3d:9e:de:94:ba:4f:6c:04:a5:b8:9d:4a:90:
    50:69:55:f2:75:f2:13:2d:1c:fc:1e:4e:fe:2e:a4:
    58:6f:37:b0:5d:73:92:20:3d:b7:c5:ed:cd:d2:e5:
    e8:22:f9:e9:7d:53:65:18:6f:37:46:b4:e6:e9:f0:
    db:c3:77:cf:09
```

2. Paste the hex strings (everything except "prime1:" and "prime2:") into an editor of your choice, such as TextPad (see Appendix A).
3. If either of your primes contains a leading "00", delete it from each. (This works in OpenSSL, but not on the BasicCard)
4. Remove all spaces, line breaks and colons so that all you have remaining is one large hex string (representing exactly 128 bytes. It will contain 256 characters – each byte is represented by 2 characters):

```
f445719438270e67cba61c4316e3fcc1f5014ac89cba068d939edcb755358b0f0b01f90
```

```
d984c9a111b6e6904c7ec5c3a460eed217502acf38f37114355537547d23d9ede94ba4f
6c04a5b89d4a90506955f275f2132d1cfc1e4efe2ea4586f37b05d7392203db7c5edcdd
2e5e822f9e97d5365186f3746b4e6e9f0dbc377cf09
```

5. Now, add the BasicCard header and footer to this string. Before the first digit insert: "05850000" and after the last digit add: "010001".
    a. 05 is the tag indicating this is a key
    b. 85 is the length of the data that follows (decimal value of 0x85: 133 bytes = 2 byte header (0x00, 0x00) + 64 byte prime1 + 64 byte prime2 + 3 byte exponent)
    c. 00 00 are the two extra bytes used for padding
    d. 01 00 01 is the value of the exponent
    e. The final version of the key above:

```
05850000f445719438270e67cba61c4316e3fcc1f5014ac89cba068d939edcb75
5358b0f0b01f90d984c9a111b6e6904c7ec5c3a460eed217502acf38f37114355
537547d23d9ede94ba4f6c04a5b89d4a90506955f275f2132d1cfc1e4efe2ea45
86f37b05d7392203db7c5edcdd2e5e822f9e97d5365186f3746b4e6e9f0dbc377
cf09010001
```

6. Copy these 270 characters (135 bytes) to the clipboard and load XVI32 (see Appendix A).
7. Create a new file in XVI32 by selecting File | New
8. Paste the hex string on the clipboard into the new file: Edit | Clipboard | Paste from hex string
9. Click the last byte (01) and confirm the value of "Adr. hex:" in the lower left of the XVI32 window equals "86". Since the first box equals 00, the total length of the Private Key is 0x87 or 135 bytes.

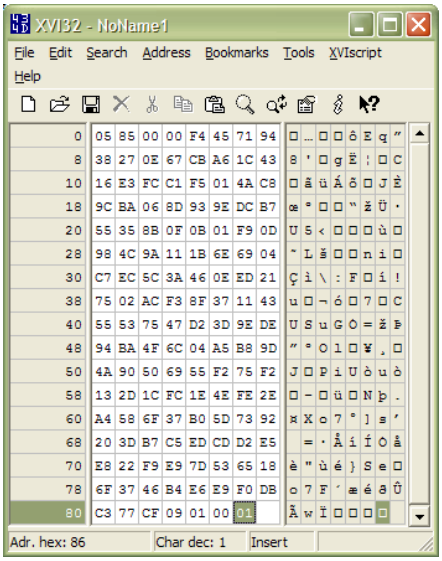

Figure C-13. XVI32: BasicCard Private Key

10. Select File | Save and place this file in the subdirectory of your BasicCard code named "KeyFiles". The file should be titled "PrivateKey.bin" – you can overwrite the current PrivateKey.bin file in the KeyFiles directory.

Note: The keys must be placed in this directory and named exactly as indicated for the BasicCard code to compile the keys properly.

C.3.2.5 Copy Certificates to BasicCard Project

1. Delete the "authcert", "sigcert", "keycert", and "cardcert" files located in the "SampleData" subdirectory of your BasicCard project.
2. Copy the certificate files created in section C.2.2 into the "SampleData" subdirectory of your BasicCard project and rename the files "authcert", "sigcert", "keycert", and "cardcert" accordingly. Note "authcert" corresponds to the PIV Authentication certificate, "sigcert" corresponds to the Digital Signature certificate, "keycert" corresponds to the Key Management certificate, and "cardcert" corresponds to the Card Authentication certificate.

Notes:

1. The certificates must be placed in this directory and named exactly as indicated for the BasicCard code to compile the certificates properly.

2. Although the certificates generated by the PIV Data Generator tool contain pre-pended certificate tag information that is incompatible with Windows Logon, the PIV Middleware and NIST CSP are able to handle the extra tag information so that the certificates can be used with Windows Logon. Hence, the extra tag information does not have to be removed from the certificates prior to loading on the BasicCard.

C.3.2.6 Compile BasicCard Code and Load BasicCard

Now all the custom key pair and certificate files have been placed in the appropriate locations to be compiled into a BasicCard image. Once this data is compiled, the image is loaded onto a BasicCard.

1. Launch ZeitControl Professional IDE.
2. Open the project created in section C.3.2.2: Project | Open, select PivCard.zcp and click Open.
3. Press F10 or select Project | Compile All to compile the BasicCard with the new key pair and X.509 certificates.

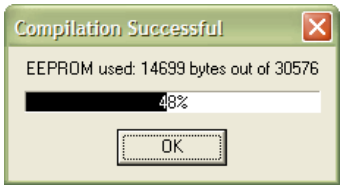

Figure C-14. BasicCard Compilation with new key pair and certificates Successful

Now this compiled image needs to be loaded onto a real BasicCard.

4. Press F2 or select Project | Start to load the compiled BasicCard program (PivCard.zcc).

   Note: If you receive an error dialog stating "compiler options have changed. Please re-compile." Click OK. Click OK again on the BasicCard Program Options Screen. You may not see the exact same screenshot below with source code. Continue with instruction #5.

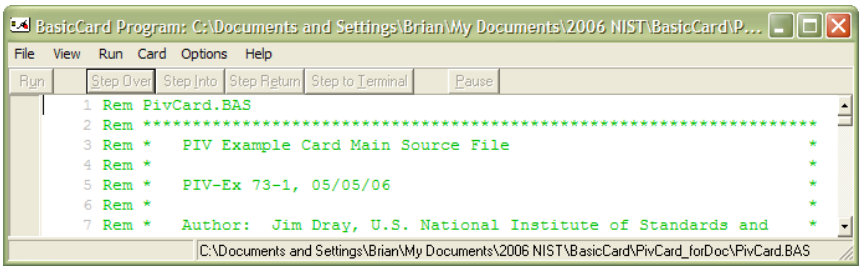

Figure C-15. BasicCard Program

5. Select Card | Download to Real Card
6. Confirm the following settings:
   a. The Image file should already be selected (PivCard.DBG)
   b. COM port should be the port on which your smart card reader is connected. If you have a USB or PCMCIA PC/SC reader, you will see virtual COM ports beginning with COM100.
   c. Card state: Test
   d. Multiple cards is not checked

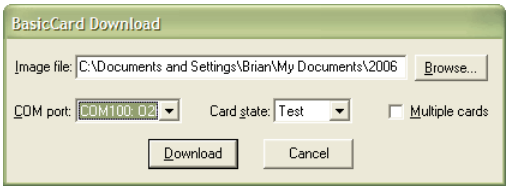

Figure C-16. BasicCard Download configuration dialog

7. Insert your BasicCard into the smart card reader and click Download.

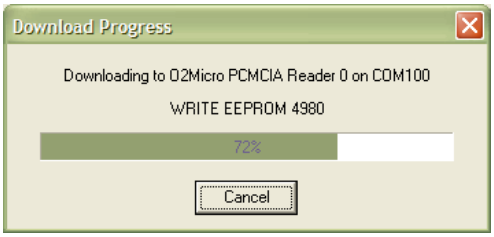

Figure C-17. BasicCard Download Progress dialog

8. In less than 30 seconds the card should be initialized and the BasicCard Download dialog box will be displayed again. Click Done.
9. Close the BasicCard Program file and click Yes to Save Changes.
10. Close the ZeitControl Professional IDE.

Your BasicCard is now loaded with the PIV applets and latest key pair and X.509 certificates.

C.3.3 Load the PIV Card Simulator

The PIV Card Simulator can be configured with a user-selected PIV Authentication key pair and certificate. In addition, although the PIV Card Simulator does not store the key pair for the Digital

Signature, Key Management, and Card Authentication keys, the certificate for those keys be loaded as well.

C.3.3.1 Extract PIV Authentication Key Pair

PIV Authentication Public Key Extraction

1. Extract the public key from the key pair generated in section C.1.2.1:
    a. Launch cygwin.
    b. Execute command: "openssl rsa -text -in private_key.pem"
    In the output of this command, copy the text in the "modulus:" section:

```
modulus:
    00:c8:9b:c3:4e:e4:9d:50:37:16:7b:96:b7:a0:1b:
    42:e9:bf:a8:e1:1c:a1:8e:ff:17:35:fe:22:5a:2a:
    10:2d:9c:aa:e1:14:ee:3b:ab:3c:b5:9e:db:1a:2c:
    6b:45:61:1c:15:e6:90:e1:2e:22:be:a6:db:c7:44:
    21:a3:47:22:35:8a:99:2e:20:bb:b8:68:bd:6f:77:
    4c:29:72:f0:14:9c:42:77:b9:66:af:e3:9b:05:1a:
    37:fd:87:36:be:7f:a0:e1:c7:94:f2:22:57:3a:94:
    16:7c:5c:f8:5e:84:ac:0d:5d:be:02:23:57:7c:f2:
    f4:a4:27:2d:3a:14:c4:88:7f
```

2. Paste the hex string text (everything after "modulus:", beginning with "00:c8:" and ending with "88:7f") into an editor of your choice, such as TextPad (see Appendix A).
3. If your modulus contains a leading "00", delete it. (This works in OpenSSL, but not with the PIV Card Simulator).
4. Replace all colons with commas and add "0x" to the beginning of each byte value. The final version of the hex string is:

```
0xc8,0x9b,0xc3,0x4e,0xe4,0x9d,0x50,0x37,0x16,0x7b,0x96,0xb7,0xa0,0x1b,
0x42,0xe9,0xbf,0xa8,0xe1,0x1c,0xa1,0x8e,0xff,0x17,0x35,0xfe,0x22,0x5a,0x2a,
0x10,0x2d,0x9c,0xaa,0xe1,0x14,0xee,0x3b,0xab,0x3c,0xb5,0x9e,0xdb,0x1a,0x2c,
0x6b,0x45,0x61,0x1c,0x15,0xe6,0x90,0xe1,0x2e,0x22,0xbe,0xa6,0xdb,0xc7,0x44,
0x21,0xa3,0x47,0x22,0x35,0x8a,0x99,0x2e,0x20,0xbb,0xb8,0x68,0xbd,0x6f,0x77,
0x4c,0x29,0x72,0xf0,0x14,0x9c,0x42,0x77,0xb9,0x66,0xaf,0xe3,0x9b,0x05,0x1a,
0x37,0xfd,0x87,0x36,0xbe,0x7f,0xa0,0xe1,0xc7,0x94,0xf2,0x22,0x57,0x3a,0x94,
0x16,0x7c,0x5c,0xf8,0x5e,0x84,0xac,0x0d,0x5d,0xbe,0x02,0x23,0x57,0x7c,0xf2,
0xf4,0xa4,0x27,0x2d,0x3a,0x14,0xc4,0x88,0x7f
```

PIV Authentication Private Key Extraction

1. Extract the private key from the key pair generated in section C.1.2.1:
    a. Launch cygwin.
    b. Execute command: "openssl rsa -text -in private_key.pem"
    In the output of this command, copy the text in the "privateExponent:" section:

```
privateExponent:
      f4:45:71:94:38:27:0e:67:cb:a6:1c:43:16:e3:fc:
      c1:f5:01:4a:c8:9c:ba:06:8d:93:9e:dc:b7:55:35:
      8b:0f:0b:01:f9:0d:98:4c:9a:11:1b:6e:69:04:c7:
      ec:5c:3a:46:0e:ed:21:75:02:ac:f3:8f:37:11:43:
      55:53:75:47:d2:3d:9e:de:94:ba:4f:6c:04:a5:b8:
      9d:4a:90:50:69:55:f2:75:f2:13:2d:1c:fc:1e:4e:
      fe:2e:a4:58:6f:37:b0:5d:73:92:20:3d:b7:c5:ed:
      cd:d2:e5:e8:22:f9:e9:7d:53:65:18:6f:37:46:b4:
      e6:e9:f0:db:c3:77:cf:09
```

2. Paste the hex string text (everything after "privateExponent:", beginning with "f4:45" and ending with "cf:09") into an editor of your choice, such as TextPad (see Appendix A).
3. Replace all colons with commas and add "0x" to the beginning of each byte value. The final version of the hex string is:

```
0xf4,0x45,0x71,0x94,0x38,0x27,0x0e,0x67,0xcb,0xa6,0x1c,0x43,0x16,0xe3,0xfc,
0xc1,0xf5,0x01,0x4a,0xc8,0x9c,0xba,0x06,0x8d,0x93,0x9e,0xdc,0xb7,0x55,0x35,
0x8b,0x0f,0x0b,0x01,0xf9,0x0d,0x98,0x4c,0x9a,0x11,0x1b,0x6e,0x69,0x04,0xc7,
0xec,0x5c,0x3a,0x46,0x0e,0xed,0x21,0x75,0x02,0xac,0xf3,0x8f,0x37,0x11,0x43,
0x55,0x53,0x75,0x47,0xd2,0x3d,0x9e,0xde,0x94,0xba,0x4f,0x6c,0x04,0xa5,0xb8,
0x9d,0x4a,0x90,0x50,0x69,0x55,0xf2,0x75,0xf2,0x13,0x2d,0x1c,0xfc,0x1e,0x4e,
0xfe,0x2e,0xa4,0x58,0x6f,0x37,0xb0,0x5d,0x73,0x92,0x20,0x3d,0xb7,0xc5,0xed,
0xcd,0xd2,0xe5,0xe8,0x22,0xf9,0xe9,0x7d,0x53,0x65,0x18,0x6f,0x37,0x46,0xb4,
0xe6,0xe9,0xf0,0xdb,0xc3,0x77,0xcf,0x09
```

C.3.3.2 Extract Certificate Data

1. Launch XVI32 (see Appendix A).
2. Select File | Open.
3. Browse to the pivauth.cer certificate file created in section C.2.2 and open it.
4. Click on the first byte in the file and select Edit | Block mark.
5. Click on the last byte in the file and select Edit | Block mark. All of the bytes in the file should change to red to indicate they have been selected.
6. Select Edit | Clipboard | Copy as hex string.
7. Open a text editor and paste the contents of the clipboard to it.
8. Insert "0x" before the first character in the hex string.
9. Replace all occurrences of blank spaces in the hex string with ",0x". The final version of the hex string is:

```
0x70,0x82,0x05,0x8B,0x30,0x82,0x05,0x87,0x30,0x82,0x04,0x6F,0xA0,0x03,0x02,0x01,
0x02,0x02,0x04,0x49,0x96,0x02,0xD2,0x30,0x0D,0x06,0x09,0x2A,0x86,0x48,0x86,0xF7,
0x0D,0x01,0x01,0x05,0x05,0x00,0x30,0x32,0x31,0x0B,0x30,0x09,0x06,0x03,0x55,0x04,
0x06,0x13,0x02,0x55,0x53,0x31,0x0D,0x30,0x0B,0x06,0x03,0x55,0x04,0x0A,0x13,0x04,
0x4E,0x49,0x53,0x54,0x31,0x14,0x30,0x12,0x06,0x03,0x55,0x04,0x03,0x13,0x0B,0x50,
0x49,0x56,0x20,0x54,0x65,0x73,0x74,0x20,0x43,0x41,0x30,0x1E,0x17,0x0D,0x30,0x37,
0x30,0x34,0x31,0x39,0x31,0x35,0x32,0x32,0x33,0x33,0x5A,0x17,0x0D,0x30,0x39,0x30,
0x34,0x31,0x39,0x31,0x35,0x32,0x32,0x33,0x33,0x5A,0x30,0x7D,0x31,0x0B,0x30,0x09,
0x06,0x03,0x55,0x04,0x06,0x13,0x02,0x55,0x53,0x31,0x33,0x30,0x31,0x06,0x03,0x55,
0x04,0x0B,0x13,0x2A,0x4E,0x49,0x53,0x54,0x20,0x43,0x6F,0x6D,0x70,0x75,0x74,0x65,
0x72,0x20,0x53,0x65,0x63,0x75,0x72,0x69,0x74,0x79,0x20,0x44,0x69,0x76,0x69,0x73,
0x69,0x6F,0x6E,0x20,0x2D,0x20,0x50,0x49,0x56,0x20,0x54,0x65,0x73,0x74,0x31,0x18,
0x30,0x16,0x06,0x03,0x55,0x04,0x0A,0x13,0x0F,0x55,0x2E,0x53,0x2E,0x20,0x47,0x6F,
0x76,0x65,0x72,0x6E,0x6D,0x65,0x6E,0x74,0x31,0x1F,0x30,0x1D,0x06,0x03,0x55,0x04,
0x03,0x13,0x16,0x4A,0x6F,0x68,0x6E,0x20,0x47,0x2E,0x20,0x44,0x6F,0x65,0x20,0x2D,
0x20,0x50,0x49,0x56,0x20,0x54,0x65,0x73,0x74,0x30,0x81,0x9F,0x30,0x0D,0x06,0x09,
0x2A,0x86,0x48,0x86,0xF7,0x0D,0x01,0x01,0x01,0x05,0x00,0x03,0x81,0x8D,0x00,0x30,
0x81,0x89,0x02,0x81,0x81,0x00,0xC8,0x9B,0xC3,0x4E,0xE4,0x9D,0x50,0x37,0x16,0x7B,
0x96,0xB7,0xA0,0x1B,0x42,0xE9,0xBF,0xA8,0xE1,0x1C,0xA1,0x8E,0xFF,0x17,0x35,0xFE,
0x22,0x5A,0x2A,0x10,0x2D,0x9C,0xAA,0xE1,0x14,0xEE,0x3B,0xAB,0x3C,0xB5,0x9E,0xDB,
0x1A,0x2C,0x6B,0x45,0x61,0x1C,0x15,0xE6,0x90,0xE1,0x2E,0x22,0xBE,0xA6,0xDB,0xC7,
0x44,0x21,0xA3,0x47,0x22,0x35,0x8A,0x99,0x2E,0x20,0xBB,0xB8,0x68,0xBD,0x6F,0x77,
0x4C,0x29,0x72,0xF0,0x14,0x9C,0x42,0x77,0xB9,0x66,0xAF,0xE3,0x9B,0x05,0x1A,0x37,
0xFD,0x87,0x36,0xBE,0x7F,0xA0,0xE1,0xC7,0x94,0xF2,0x22,0x57,0x3A,0x94,0x16,0x7C,
0x5C,0xF8,0x5E,0x84,0xAC,0x0D,0x5D,0xBE,0x02,0x23,0x57,0x7C,0xF2,0xF4,0xA4,0x27,
0x2D,0x3A,0x14,0xC4,0x88,0x7F,0x02,0x03,0x01,0x00,0x01,0xA3,0x82,0x02,0xDC,0x30,
0x82,0x02,0xD8,0x30,0x1F,0x06,0x03,0x55,0x1D,0x23,0x04,0x18,0x30,0x16,0x80,0x14,
0xEB,0xDA,0x19,0xD2,0x08,0x42,0x8D,0xF4,0xDE,0x25,0x87,0x69,0xC9,0xBB,0xAB,0x0C,
0xD3,0x96,0x30,0x01,0x30,0x1D,0x06,0x03,0x55,0x1D,0x0E,0x04,0x16,0x04,0x14,0xA5,
```

```
0x80,0xED,0x7C,0xB5,0x52,0x25,0x26,0x55,0x65,0x09,0x58,0x3B,0x4A,0x07,0xF2,0x59,
0x25,0xBD,0x99,0x30,0x0E,0x06,0x03,0x55,0x1D,0x0F,0x01,0x01,0xFF,0x04,0x04,0x03,
0x02,0x07,0x80,0x30,0x25,0x06,0x03,0x55,0x1D,0x25,0x04,0x1E,0x30,0x1C,0x06,0x08,
0x2B,0x06,0x01,0x05,0x05,0x07,0x03,0x02,0x06,0x0A,0x2B,0x06,0x01,0x04,0x01,0x82,
0x37,0x14,0x02,0x02,0x06,0x04,0x55,0x1D,0x25,0x00,0x30,0x17,0x06,0x03,0x55,0x1D,
0x20,0x04,0x10,0x30,0x0E,0x30,0x0C,0x06,0x0A,0x60,0x86,0x48,0x01,0x65,0x03,0x02,
0x01,0x03,0x0D,0x30,0x81,0xB4,0x06,0x03,0x55,0x1D,0x1F,0x04,0x81,0xAC,0x30,0x81,
0xA9,0x30,0x81,0xA6,0xA0,0x81,0xA3,0xA0,0x81,0xA0,0x86,0x44,0x68,0x74,0x74,0x70,
0x3A,0x2F,0x2F,0x66,0x69,0x63,0x74,0x69,0x74,0x69,0x6F,0x75,0x73,0x2E,0x6E,0x69,
0x73,0x74,0x2E,0x67,0x6F,0x76,0x2F,0x66,0x69,0x63,0x74,0x69,0x74,0x69,0x6F,0x75,
0x73,0x43,0x52,0x4C,0x64,0x69,0x72,0x65,0x63,0x74,0x6F,0x72,0x79,0x2F,0x66,0x69,
0x63,0x74,0x69,0x74,0x69,0x6F,0x75,0x73,0x43,0x52,0x4C,0x31,0x2E,0x63,0x72,0x6C,
0x86,0x58,0x6C,0x64,0x61,0x70,0x3A,0x2F,0x2F,0x73,0x6D,0x69,0x6D,0x65,0x32,0x2E,
0x6E,0x69,0x73,0x74,0x2E,0x67,0x6F,0x76,0x2F,0x63,0x6E,0x3D,0x47,0x6F,0x6F,0x64,
0x25,0x32,0x30,0x43,0x41,0x2C,0x6F,0x3D,0x54,0x65,0x73,0x74,0x25,0x32,0x30,0x43,
0x65,0x72,0x74,0x69,0x66,0x69,0x63,0x61,0x74,0x65,0x73,0x2C,0x63,0x3D,0x55,0x53,
0x3F,0x63,0x65,0x72,0x74,0x69,0x66,0x69,0x63,0x61,0x74,0x65,0x52,0x65,0x76,0x6F,
0x63,0x61,0x74,0x69,0x6F,0x6E,0x4C,0x69,0x73,0x74,0x30,0x82,0x01,0x21,0x06,0x08,
0x2B,0x06,0x01,0x05,0x05,0x07,0x01,0x01,0x04,0x82,0x01,0x13,0x30,0x82,0x01,0x0F,
0x30,0x3E,0x06,0x08,0x2B,0x06,0x01,0x05,0x05,0x07,0x30,0x01,0x86,0x32,0x68,0x74,
0x74,0x70,0x3A,0x2F,0x2F,0x66,0x69,0x63,0x74,0x69,0x74,0x69,0x6F,0x75,0x73,0x2E,
0x6E,0x69,0x73,0x74,0x2E,0x67,0x6F,0x76,0x2F,0x66,0x69,0x63,0x74,0x69,0x74,0x69,
0x6F,0x75,0x73,0x4F,0x43,0x53,0x50,0x4C,0x6F,0x63,0x61,0x74,0x69,0x6F,0x6E,0x2F,
0x30,0x5E,0x06,0x08,0x2B,0x06,0x01,0x05,0x05,0x07,0x30,0x02,0x86,0x52,0x68,0x74,
0x74,0x70,0x3A,0x2F,0x2F,0x66,0x69,0x63,0x74,0x69,0x74,0x69,0x6F,0x75,0x73,0x2E,
0x6E,0x69,0x73,0x74,0x2E,0x67,0x6F,0x76,0x2F,0x66,0x69,0x63,0x74,0x69,0x74,0x69,
0x6F,0x75,0x73,0x43,0x65,0x72,0x74,0x73,0x4F,0x6E,0x6C,0x79,0x43,0x4D,0x53,0x64,
0x69,0x72,0x65,0x63,0x74,0x6F,0x72,0x79,0x2F,0x63,0x65,0x72,0x74,0x73,0x49,0x73,
0x73,0x75,0x65,0x64,0x54,0x6F,0x47,0x6F,0x6F,0x64,0x43,0x41,0x2E,0x70,0x37,0x63,
0x30,0x6D,0x06,0x08,0x2B,0x06,0x01,0x05,0x05,0x07,0x30,0x02,0x86,0x61,0x6C,0x64,
0x61,0x70,0x3A,0x2F,0x2F,0x73,0x6D,0x69,0x6D,0x65,0x32,0x2E,0x6E,0x69,0x73,0x74,
0x2E,0x67,0x6F,0x76,0x2F,0x63,0x6E,0x3D,0x47,0x6F,0x6F,0x64,0x25,0x32,0x30,0x43,
0x41,0x2C,0x6F,0x3D,0x54,0x65,0x73,0x74,0x25,0x32,0x30,0x43,0x65,0x72,0x74,0x69,
0x66,0x69,0x63,0x61,0x74,0x65,0x73,0x2C,0x63,0x3D,0x55,0x53,0x3F,0x63,0x41,0x43,
0x65,0x72,0x74,0x69,0x66,0x69,0x63,0x61,0x74,0x65,0x2C,0x63,0x72,0x6F,0x73,0x73,
0x43,0x65,0x72,0x74,0x69,0x66,0x69,0x63,0x61,0x74,0x65,0x50,0x61,0x69,0x72,0x30,
0x58,0x06,0x03,0x55,0x1D,0x11,0x04,0x51,0x30,0x4F,0xA0,0x27,0x06,0x08,0x60,0x86,
0x48,0x01,0x65,0x03,0x06,0x06,0xA0,0x1B,0x04,0x19,0xD6,0x50,0x18,0x58,0x21,0x0C,
0x2D,0x31,0x71,0xB5,0x25,0xA1,0x68,0x5A,0x08,0xC9,0x2A,0xDE,0x0A,0x61,0x86,0x50,
0x18,0x43,0xE2,0xA0,0x24,0x06,0x0A,0x2B,0x06,0x01,0x04,0x01,0x82,0x37,0x14,0x02,
0x03,0xA0,0x16,0x0C,0x14,0x6A,0x6F,0x68,0x6E,0x5F,0x64,0x6F,0x65,0x40,0x70,0x69,
0x76,0x64,0x65,0x6D,0x6F,0x2E,0x6F,0x72,0x67,0x30,0x10,0x06,0x09,0x60,0x86,0x48,
0x01,0x65,0x03,0x06,0x09,0x01,0x04,0x03,0x01,0x01,0x00,0x30,0x0D,0x06,0x09,0x2A,
0x86,0x48,0x86,0xF7,0x0D,0x01,0x01,0x05,0x05,0x00,0x03,0x82,0x01,0x01,0x00,0x25,
0x6B,0x07,0xDE,0x51,0x65,0x3B,0xAF,0x17,0x0F,0x2B,0x09,0xA9,0x4C,0x64,0x36,0x3C,
0xB0,0x0C,0xD2,0x91,0x44,0xFF,0x79,0xB8,0xDB,0x8A,0x5F,0x74,0x1D,0x3A,0x19,0x19,
0x2B,0x29,0xED,0x9D,0x2F,0xB0,0x7A,0xB3,0x10,0xF1,0xCE,0x90,0xDD,0xFF,0x88,0x60,
0x08,0x18,0xC3,0xD7,0x4B,0x38,0x55,0x4A,0x03,0x7F,0x5D,0x70,0xB6,0x1F,0x0F,0x70,
0x80,0xD9,0x4C,0x4F,0xA9,0x97,0xDC,0xD0,0x8E,0x6B,0xC6,0x00,0x57,0xAE,0x15,0x0B,
0x90,0xFC,0xD5,0x8B,0x1C,0x6F,0xF6,0x34,0x5F,0x8A,0xB0,0xA9,0x29,0xEA,0x24,0x7C,
0xB4,0x9B,0x9E,0x1D,0x22,0x8E,0xAA,0x36,0x4E,0x03,0x5B,0x03,0x42,0x5F,0x63,0x8B,
0x36,0xF2,0x63,0x6F,0x33,0x2C,0x9C,0x9A,0xB6,0x7E,0x2E,0x9C,0xD7,0x2B,0xC5,0x24,
0xF5,0x14,0x06,0x07,0x03,0x45,0xF2,0x5A,0x4B,0xB2,0x38,0x91,0x03,0x82,0xB3,0xB0,
0x58,0x89,0x2B,0x4D,0x92,0xFF,0x92,0x63,0xEE,0x4D,0x01,0x4B,0x05,0x48,0xA1,0xC7,
0x57,0x2B,0xB2,0xB2,0x2A,0x95,0x20,0x1C,0xC3,0x9C,0x6B,0xCF,0x24,0x43,0x4D,0x9F,
0x49,0xAB,0xC5,0x88,0x30,0x85,0x9B,0x3D,0x45,0x55,0x46,0x67,0xC7,0xFD,0xEA,0x4C,
0xB4,0x7C,0xEB,0x62,0x8C,0x66,0x7C,0x13,0xD1,0x47,0x8C,0x81,0x9F,0xBC,0x80,0x33,
0x3B,0x6B,0xBC,0xB4,0x34,0xB6,0xF4,0x54,0x75,0x88,0x73,0xEA,0x0B,0x2D,0x95,0x4B,
0x0A,0xA0,0x06,0xFD,0xC8,0xA2,0x2A,0xD0,0x09,0x96,0x1F,0x57,0xE8,0x67,0x79,0x00,
0xA8,0xC8,0xF7,0x77,0xD2,0x98,0x14,0x2E,0xA0,0x3B,0xC9,0xCC,0x8C,0x28,0x4D,0x71,
0x01,0x00,0xFE,0x00
```

10. Repeat steps 2 – 9 for the digitalsig.cer, keymanage.cer, and cardauth.cer certificate files created in section C.2.2.

C.3.3.3 Compile PIV Card Simulator Project with Key Pair and Certificates

1. Open the PIV project in Visual Studio .NET (see the sixth instruction of the "Recompile and Building" section of the *PIV Card Simulator User's Guide*).
2. Open the %PIV_HOME%\RefImp\File_Manager\File_System_Initial_Configuration.inc file.
3. Copy the PIV Authentication public key hex string from section C.3.3.1 to the clipboard.
4. Overwrite the value of the_default_RSA_key_n variable in the File_System_Initial_Configuration.inc file with the new PIV Authentication public key by pasting the contents of the clipboard over it.
5. Copy the PIV Authentication private key hex string from section C.3.3.1 to the clipboard.
6. Overwrite the value of the_default_RSA_key_d variable in the File_System_Initial_Configuration.inc file with the new private exponent by pasting the contents of the clipboard over it.
7. Copy the certificate hex string of the pivauth.cer file from section C.3.3.2 to the clipboard.
8. Overwrite the value of PIV_X509_DATA in the File_System_Initial_Configuration.inc file with the new certificate data by pasting the contents of the clipboard over it. PIV_X509_DATA represents the X.509 Certificate for PIV Authentication (BER-TLV Tag '5FC105') data.
9. Copy the certificate hex string of the digitalsig.cer file from section C.3.3.2 to the clipboard.
10. Overwrite the value of SIGNING_X509_DATA in the File_System_Initial_Configuration.inc file with the new certificate data by pasting the contents of the clipboard over it. SIGNING_X509_DATA represents the X.509 Certificate for Digital Signature (BER-TLV Tag '5FC10A') data.
11. Copy the certificate hex string of the keymanage.cer file from section C.3.3.2 to the clipboard.
12. Overwrite the value of KEY_MANAGEMENT_X509_DATA in the File_System_Initial_Configuration.inc file with the new certificate data by pasting the contents of the clipboard over it. KEY_MANAGEMENT_X509_DATA represents the X.509 Certificate for Key Management (BER-TLV Tag '5FC10B') data.
13. Copy the certificate hex string of the cardauth.cer file from section C.3.3.2 to the clipboard.
14. Overwrite the value of CARD_X509_DATA in the File_System_Initial_Configuration.inc file with the new certificate data by pasting the contents of the clipboard over it. CARD_X509_DATA represents the X.509 Certificate for Card Authentication (BER-TLV Tag '5FC101') data.
15. Select File | Save All to save the changes.
16. Select Build | Rebuild Solution to rebuild the PIV solution in Visual Studio .NET. A new pivd.exe executable will be built in %PIV_HOME%\bin\.
17. Copy the DLLs in the %PIV_HOME%\build\bin\ directory to the %PIV_HOME%\bin\ directory. These files are needed by the pivd.exe executable to run.
18. Open a command prompt and navigate to the %PIV_HOME%\bin\ directory.
19. Execute the following command at the command prompt to create a PIV card configuration file: "pivd –o piv.fs –s 256000".
20. Send LOAD and INSTALL commands to the Card Simulator to load the PIV Card Application (PCA) onto the PIV Reference Implementation platform, as instructed in the "Creating, Saving and Restoring the PIV Card Simulator" section of the *PIV Card Simulator User's Guide.*
21. After the `powerdown` command is sent to the Card Simulator, the current configuration will be written to the piv.fs file.
22. Execute the following command at a command prompt to run the Card Simulator with the user-selected key pair and certificates: "pivd –i piv.fs –s 256000"

Appendix D—Acronyms

The following acronyms and abbreviations are used throughout this document:

AD	Active Directory
APDU	Application Programming Data Unit
API	Application Programming Interface
ATR	Answer-to-Reset
CA	Certificate Authority
CAPI	Crypto Application Programming Interface
CHUID	Cardholder Unique Identifier
CRL	Certificate Revocation List
CSP	Cryptographic Service Provider
DLL	Dynamic Link Library
FASC-N	Federal Agency Smart Credential Number
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
HSPD	Homeland Security Presidential Directive
IDE	Integrated Development Environment
ITL	Information Technology Laboratory
JCDK	Java Card Development Kit
MMC	Microsoft Management Console
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency Report
OMB	Office of Management and Budget
PC/SC	Personal Computer/Smart Card
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
RSA	Rivest Shamir Adleman
SDK	Software Development Kit
SP	Special Publication
TLS	Transport Layer Security
UPN	Universal Principal Name
VSCR	Virtual Smart Card Reader

Appendix E—References

[1] Electrosoft, Inc., *MS Cryptographic Service Provider – Design, Build and Installation Procedures*, Prepared for: NIST, Version 1.1 (draft), January 9, 2005

[2] Electrosoft, Inc., *Windows Logon using the PIV card*, Version 0.3 (draft), July 26, 2005

[3] NIST, *PIV Card Simulator User's Guide*, Version 1.2, May 4, 2007 (included with the SP 800-73 Reference Implementation package – available at http://csrc.nist.gov/piv-program/)

[4] NIST, *PIV Project – Question and Answer Website*, Last modified April 17, 2006 - http://piv.nist.gov/pivqa/

[5] Microsoft Corporation, *The Smart Card Cryptographic Service Provider Cookbook*, October 2002. http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnscard/html/smartcardcspcook.asp

[6] NIST, *Virtual Smart Card Reader User Guide*, November 21, 2006 (included with the SP 800-73 Reference Implementation package – available at http://csrc.nist.gov/piv-program/)