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

March 2008

by

National Institute of Standards and Technology

Table of Contents

List of Appendices

List of Tables

List of Figures

1. Introduction

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

The PIV Card holds the identity credentials that provide 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. Three such common applications under Linux are Linux Logon, e-mail signing and encryption, and web authentication. These applications are designed to use smart cards to perform user authentication to gain higher level of assurance on a user's identity. This document provides information on how to PIV enable Linux Logon, Thunderbird e-mail client, and Firefox web browser in the Linux environment. Specifically, this document provides details of the tools and steps necessary to PIV enable these applications in the Linux environment. NIST used existing tools such as the PIV Reference Implementation, PIV Data Generator, PIV Data Loader, hex editor, certificate generator, etc. to create and store PIV data on a PIV Card. Some of these tools are discussed in this document; however, the document largely provides examples of the uses of a PIV Card once it is issued.

NIST developed the prototype solutions to guide agencies in their implementation of PIV solutions and also further the standardization work. There are many ways to implement Linux Logon, e-mail signing and encryption, and web authentication under Linux. This document shows three example of how quickly and effortlessly one can PIV-enable their applications.

1.1 Purpose and Scope

The purpose of this document is to provide detailed examples on how to enable Linux Logon, Thunderbird e-mail client, and Firefox web browser to use a PIV Card under Linux. The document provides detailed steps to configure and install tools necessary to enable these applications.

This document does not describe every application or each possible configuration parameter. Also the accompanying software is for demonstration purposes and is not meant for production use.

1.2 Audience

This document has been created for Federal government agencies responsible for PIV implementation, agencies that use the Linux Operating System, as well as IT professionals (particularly Linux system administrators and information security personnel) who may be responsible for implementing HSPD-12. 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 Linux Logon, Secure / Multipurpose Internet Mail Extensions (S/MIME), and Secure Sockets Layer (SSL) Authentication to use a PIV Card under Linux. Sections contain

walkthrough of user activities, information to support existing PIV documents, and best practice tips and troubleshooting activities.

+ Section 2 describes how to configure a Linux workstation for Linux Logon, S/MIME, and SSL Authentication using a PIV Card.
+ Section 3 describes how to log onto Linux with a PIV Card.
+ Section 4 describes how to perform S/MIME with a PIV Card.
+ Section 5 describes how to perform SSL Authentication with a PIV Card.
+ Section 6 provides troubleshooting support for performing Linux Logon, S/MIME, and SSL Authentication with a PIV Card.
+ Appendix A lists all the tools used in development 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 a list of acronyms.
+ Appendix E provides references to resources and other sources of information concerned with implementing Linux Logon, S/MIME, and SSL Authentication for Linux.

1.4 Quick Start

NIST developed the Public Key Cryptography Standards (PKCS) #11 reference implementation to provide a common interface to PIV Cards for performing application authentication under Linux. Using a few simple steps, applications can be easily configured to utilize the NIST PKCS#11 module and communicate with PIV Cards. Demonstrations were put together to show how applications can be PIV-enabled.

Note: The S/MIME and SSL authentication demonstrations described in this document utilize a Windows machine as a communications end-point to the Linux workstation (e.g., Web server). There are many other implementations of S/MIME and SSL authentication which may use a non-Windows machine as a communications end-point.

1.4.1 Linux Logon Demonstration

This demonstration shows how a PIV Card can be used to log into a Linux workstation. The event sequence for this demonstration is as follows:

1. The Linux workstation is booted up and displays the login prompt.
2. The user inserts his PIV Card into the smart card reader and enters his username.
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:

+ PIV Card loaded with a PIV Authentication key and certificate

+ A smart card reader with the necessary Linux drivers
+ Linux workstation running Fedora Core 5
+ NIST PKCS#11 installation package
+ An existing user account for the PIV card holder

1.4.2 E-mail Signing and Encryption Demonstration

This demonstration shows how Thunderbird can be configured to use the PIV credentials from a PIV Card to perform e-mail signing and encryption. The configuration consists of a Linux and Windows workstation connected via a network that is used to send signed and encrypted e-mails to one another. The event sequence for this demonstration is as follows:

1. User A launches Thunderbird on the Linux workstation.
2. User A composes an e-mail and signs it using his Digital Signature private key from his PIV Card.
3. User A sends the signed e-mail to User B.
4. User B launches Thunderbird on the Windows workstation.
5. User B receives the signed e-mail from User A.
6. Thunderbird verifies the signed e-mail has not been altered in any way.
7. User B composes an e-mail and signs it using his Digital Signature private key, which was previously imported into Thunderbird. In addition, User B encrypts the e-mail using User A's Key Management public key, which was previously exchanged and imported into Thunderbird.
8. User B sends the signed and encrypted e-mail to User A.
9. User A received the signed and encrypted e-mail from User B.
10. Thunderbird verifies the signed e-mail has not been altered in any way and decrypts the e-mail using User A's Key Management private key from his PIV Card.

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

+ PIV Card loaded with a Digital Signature and Key Management keys and certificates
+ A smart card reader with the necessary Linux drivers
+ Linux workstation:
  - Fedora Core 5
  - Thunderbird configured with User A's account
+ Windows workstation:
  - Windows XP Professional
  - Thunderbird configured with User B's account
+ NIST PKCS#11 installation package
+ Issuing CA certificate
+ OpenSSL, PIV Data Generator, and a hex editor to create a PKCS12 file for the Windows user

1.4.3 Web Authentication Demonstration

This demonstration shows how Firefox can be configured to use the PIV credentials from a PIV Card for SSL authentication. The configuration consists of a Linux workstation, a Web server, and a Windows

server connected via a network. The demonstration uses the Vistor Management System sample Web application. The Web application authenticates the PIV cardholder and based on their priviledges allows the user to add new visitors, to view the visitor list, or no access. The event sequence for this demonstration is as follows:

1. User A launches Firefox on the Linux workstation.
2. User A attempts to connect to the Visitor Management System Web site that is running on the Web server.
3. The Web server authenticates User A using his PIV Authentication certificate and grants him access to the site.
4. User A, who has administrative privileges, adds a new visitor to the visitor management database.
5. User A closes Firefox.

1. User B launches Firefox on the Linux workstation.
2. User B attempts to connect to the Visitor Management System Web site.
3. The Web server authenticates User B using his PIV Authentication certificate and grants him access to the site.
4. User B, who does NOT have administrative privileges, trys to add a new visitor to the visitor management database.
5. User B's attempt to add a new user is denied.
6. User B closes Firefox.

1. User C launches Firefox on the Linux workstation.
2. User C, who's certificate has been revoked, attempts to connect to the Visitor Management System Web site.
3. The Web server checks User C's PIV Authentication certificate and sees that his certificate has been revoked.
4. User C is denied access to the Visitor Management System Web site.
5. User C closes Firefox.

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

+ PIV Card for each user loaded with their PIV Authentication key and certificate
+ A smart card reader with the necessary Linux drivers
+ Linux workstation:
  - Fedora Core 5
  - Firefox
+ Web server:
  - Windows XP Professional
  - IIS
+ Windows server:
  - Microsoft Certificate Services
  - Windows 2003 Server
+ NIST PKCS#11 installation package
+ Issuing CA certificate

1.4.4 Tools

The following tools were used to enable PIV Card usage under Linux. Note some tools listed here are native Windows applications, such as the PIV Data Loader.

NIST PKCS#11 — NIST developed the PKCS#11 module which provides a common interface to PIV Cards for performing application authentication. The NIST PKCS#11 module was developed to interrogate the card for the certificate, PIN verification, and digital signature using the PIV card edge interface. The NIST PKCS#11 module supports Linux Logon, S/MIME, and SSL Authentication.

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.

Firefox — NIST configured the Mozilla Firefox browser to utilize the PIV Card credentials to demonstrate SSL Authentication. This represents only one possible implementation of SSL Authentication.

Thunderbird — NIST configured the Mozilla Thunderbird e-mail client to utilize the PIV Card credentials to demonstrate S/MIME. This represents only one possible implementation of S/MIME.

IIS — NIST used the Microsoft Internet Information Services (IIS) application to host a simple Web application that demonstrates SSL Authentication via communications with the Firefox browser on the Linux workstation. This represents only one possible implementation of SSL Authentication.

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 BasicCard and to read data from the BasicCard.

2. Linux Workstation Configuration

This section explains how to install and configure the PIV Middleware, NIST PKCS#11, and other components necessary to perform Linux Logon, S/MIME, and SSL Authentication under Linux. The following steps must be performed to configure the Linux workstation:

+ Install USB device library
+ Install PC/SC lite library
+ Install CCID driver
+ Install NIST PKCS#11 and Middleware package

Note:
1. Unless otherwise noted, you should be logged in as the root user on the Linux workstation before performing any steps in the following subsections.

2. It is assumed that Linux (Fedora Core 5) has already been installed on the workstation with all options, including software development packages. If the software development package has not been installed yet then the Linux installation should be updated with it before proceeding. To do so, select Applications | Add/Remove Software from the Fedora Core 5 menu. When the Package Manager is displayed, select the Development package group and click on the Development Libraries, Development Tools, GNOME Software Development, and X Software Development checkboxes. Finally, click Apply to update the Linux installation with the selected packages.

2.1 Uncompress Software Installation Package

The NIST PKCS#11 installation package includes the PIV Middleware, NIST PKCS#11 module, Pluggable Authentication Modules (PAM), PC/SC Lite, and other software components necessary to enable PIV Card usage under Linux. The following steps should be used to unpack the components and prepare for installation.

1. Create a directory named "PKCS#11" on the desktop and copy the install.tar.gz from the NIST PKCS#11 installation package to this directory.
2. Open a terminal window and navigate to the "PKCS#11" directory.
3. Execute command: `tar -xzf install.tar.gz`
4. The contents of the install.tar.gz file are unpacked to the "PKCS#11" directory.
5. Execute command: `export PKG_CONFIG_PATH=/usr/lib/pkgconfig`
6. The environment variable PKG_CONFIG_PATH is set.

2.2 Install libusb

libusb is an application library used to access USB devices on a Linux platform. Perform the following steps to install and configure libusb.

1. Open a terminal window and navigate to the "PKCS#11" directory created in section 2.1.
2. Execute command: `tar -xzvf ./libusb-0.1.12.tar.gz`
3. The contents of the libusb-0.1.12.tar.gz file are unpacked to a subdirectory named "libusb-0.1.12".
4. Execute command to change to the "libusb-0.1.12" subdirectory: `cd libusb-0.1.12`

5. Execute command to run the libusb configuration: `./configure`
6. Execute command to compile the libusb source code: `make`
7. Execute command to install the libusb module: `make install`

2.3 Install PC/SC Lite

PC/SC Lite is an API that emulates the WinSCard API used on the Windows platform to communicate with smart cards and readers. Perform the following steps to install PC/SC Lite.

1. Open a terminal window and navigate to the "PKCS#11" directory created in section 2.1.
2. Execute command: `rpm -Uh libmusclecard0-1.3.0-7.fc5.at.i386.rpm`
3. Execute command: `rpm -Uh libpcsclite1-1.3.0-7.fc5.at.i386.rpm`
4. Execute command: `rpm -Uh pcsc-lite-1.3.0-7.fc5.at.i386.rpm`
5. Execute command: `rpm -Uh pcsc-lite-devel-1.3.0-7.fc5.at.i386.rpm`
6. PC/SC Lite is installed on the Linux workstation.

2.4 Install CCID

CCID is a Linux software driver for a generic USB Chip/Smart Card Interface Devices (CCID) and Integrated Circuit Card Devices (ICCD). Perform the following steps to install and configure CCID.

1. Open a terminal window and navigate to the "PKCS#11" directory created in section 2.1.
2. Execute command: `tar -xzf ./ccid-1.1.0.tar.gz`
3. The contents of the ccid-1.1.0.tar.gz file are unpacked to a subdirectory named "ccid-1.1.0".
4. Execute command to change to the "ccid-1.1.0" subdirectory: `cd ccid-1.1.0`
5. Execute command to run the CCID configuration: `./configure`
6. Execute command to compile the CCID source code: `make`
7. Execute command to install CCID: `make install`

2.5 Configure PC/SC Lite Daemon

Once PC/SC Lite and CCID have been installed on the workstation, the PC/SC Lite daemon program should be configured to start during boot time. Perform the following steps to configure the PC/SC Lite daemon program.

1. Open a terminal window and navigate to the "PKCS#11" directory created in section 2.1.
2. Execute command to copy the daemon: `cp pcscd /etc/init.d`
3. Execute command to add the daemon to the startup configuration: `chkconfig --add pcscd`

2.6 Install NIST PKCS#11 & PIV Middleware

The NIST PKCS#11 module provides a common interface to PIV Cards for performing application authentication and uses the PIV Middleware to communicate with PIV Cards. Perform the following steps to install and configure the NIST PKCS#11 module and PIV Middleware.

1. Open a terminal window and navigate to the "PKCS#11" directory created in section 2.1.
2. Execute command to change to the "NIST_PKCS11/combined" subdirectory: `cd NIST_PKCS11/combined`
3. Execute command: `./build`
4. A single binary library file is created from the NIST PKCS#11 and PIV Middleware source code, and is located at /usr/local/lib/pkcs11.so.1. If any output results from step 3 then an error

occurred and the installation should be aborted, in which case the previous sections should be reviewed to ensure all steps have been executed correctly.

3. Linux Logon with PIV Card

Linux Logon can be easily configured to work with PIV Cards by performing the following steps:

+ Install PAM module
+ Configure Login Mapper for PAM module

This section describes these configuration steps and illustrates how to log into Linux with a PIV Card.

3.1 Install PAM Module

The PAM module is a generalized API for authentication-related services where new authentication methods can be added simply by installing new PAM modules or existing authentication policies can be modified by editing configuration files. Before installing the PAM module, the root Certificate Authority (CA) certificates that the PAM module will use for certificate validation need to be converted to base64 format (see section 6.1.1). Once this has been accomplished, perform the following steps to install the PAM module:

Note: The implementation described in this document uses the root CA certificates included with the PIV Data Generator tool. Additional/alternate root CA certificates can be used per organization requirements.

1. Open a terminal window and navigate to the "PKCS#11" directory created in section 2.1.
2. Execute command: `tar -xzf pkcs11_login-0.5.1.tar.gz`
3. The contents of the pkcs11_login-0.5.1.tar.gz file are unpacked to a subdirectory named "pkcs11_login-0.5.1".
4. Execute command to change to the "pkcs11_login-0.5.1" subdirectory: `cd pkcs11_login-0.5.1`
5. Execute command to run the PAM configuration: `./configure`
6. Execute command to compile the PAM source code: `make`
7. Execute command to install the PAM module: `make install`
8. Execute command: `mkdir -p /etc/pkcs11/cacerts`
9. The directory /etc/pkcs11/cacerts is created.
10. Copy the base64 version of the root CA certificate files that will be used for certificate validation to the /etc/pkcs11/cacerts directory. The root CA certificate files for the PIV Data Generator tool (see Appendix A) are named pivtestroot.cer and pivtestca.cer, and are located in the "extra_files" subdirectory of the tool.
11. Copy the base64 version of any other root CA certificate files that will be used for certificate validation to the /etc/pkcs11/cacerts directory.
12. Execute command to generate hash values for the root CA certificates: `./tools/make_hash_links.sh /etc/pkcs11/cacerts`
13. Execute command to go back one directory level: `cd ..`
14. Execute command to copy the PAM configuration file: `cp pam_pkcs11.conf /etc/pkcs11/`
15. Execute command to configure Linux to use the PAM module: `cp gdm /etc/pam.d/`

3.2 Configure Login Mapper

The PAM module can be configured to match the Common Name or the Universal Principal Name (UPN) extension of the PIV Authentication certificate to the login name.

Note: The PAM module initially has been configured to match the Common Name of the PIV Authentication certificate to the login name.

3.2.1 Map Common Name to Login Name

1. Open a terminal window.
2. Execute command to change to the /etc/pkcs11/ directory: `cd /etc/pkcs11/`
3. Execute command: `vim pam_pkcs11.conf`
4. The PAM configuration file is opened in the Linux vim editor.
5. Press the **I** key.
6. The vim editor is now in Input mode and the file is ready for editing.
7. Go to line 94 of the file. The line reads "use_mappers = xx;".
8. Change line 94 so that it reads "use_mappers = cn;".
9. Go to line 143 of the file. The cn mapper structure begins here and resembles the following:

```
mapper cn {
        debug = false;
        module = /usr/local/lib/pam_pkcs11/cn_mapper.so;
        ignorecase = true;
        # mapfile = file:///etc/pkcs11/cn_map;
        mapfile = "none";
}
```

10. Change the "module" value to "/usr/local/lib/pam_pkcs11/cn_mapper.so;".
11. If the PAM module should perform case insensitive matches of the Common Name then change the "ignorecase" value to "true;".
12. Press the **Esc** key.
13. The vim editor is now in Command mode.
14. Hold **Shift** and press the **Z** key twice.
15. The changes are saved to the PAM configuration file and the vim editor closes.

3.2.2 Map Universal Principal Name to Login Name

1. Open a terminal window.
2. Execute command to change to the /etc/pkcs11/ directory: `cd /etc/pkcs11/`
3. Execute command: `vim pam_pkcs11.conf`
4. The PAM configuration file is opened in the Linux vim editor.
5. Press the **I** key.
6. The vim editor is now in Input mode and the file is ready for editing.
7. Go to line 94 of the file. The line reads "use_mappers = xx;".
8. Change line 94 so that it reads "use_mappers = ms;".
9. Go to line 168 of the file. The ms mapper structure begins here and resembles the following:

```
mapper ms {
        debug = false;
        module = /usr/lib/pam_pkcs11/ms_mapper.so;
        ignorecase = false;
        ignoredomain = false;
        domain = "domain.com";
```

```
}
```

10. Change the "module" value to "/usr/local/lib/pam_pkcs11/ms_mapper.so;".
11. If the PAM module should perform case insensitive matches of the UPN then change the "ignorecase" value to "true;".
12. If the PAM module should not enforce UPN domain name checking then change the "ignoredomain" value to "true;". Otherwise, the domain name should be specified in the "domain" value. For example, if the UPN is alice@pivdemo.org then the "domain" value should be set to "pivdemo.org".
13. Press the **Esc** key.
14. The vim editor is now in Command mode.
15. Hold **Shift** and press the **Z** key twice.
16. The changes are saved to the PAM configuration file and the vim editor closes.

3.3 Attempt Linux Logon

All prerequisites for Linux logon should be satisfied prior to performing logon. The following should be true:

+ The Linux workstation (Fedora Core 5) is configured for Linux logon (see section 2).
+ The PAM module has been installed and configured with the root CA certificates that will be used for certificate validation.
+ A PIV Card is loaded with the PIV applet, PIV Authentication key pair, and PIV Authentication certificate (see Appendix C).
+ A Linux compatible smart card reader is installed.

Once the prerequisites have been met, perform the following steps to attempt Linux logon:

1. If currently logged onto the Linux workstation, log off.
2. The Linux user logon prompt is displayed.

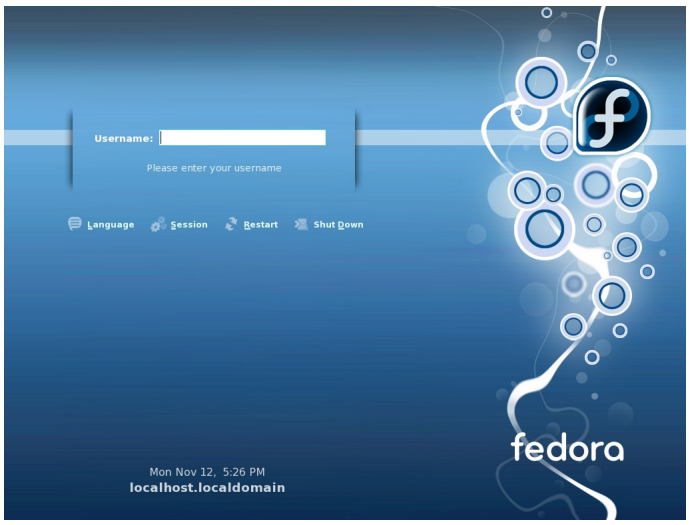

Figure 3-1. Linux Logon Prompt

3. Insert your PIV Card.
4. Enter the login username associated with the PIV Card.
5. The PIV token prompt is displayed.

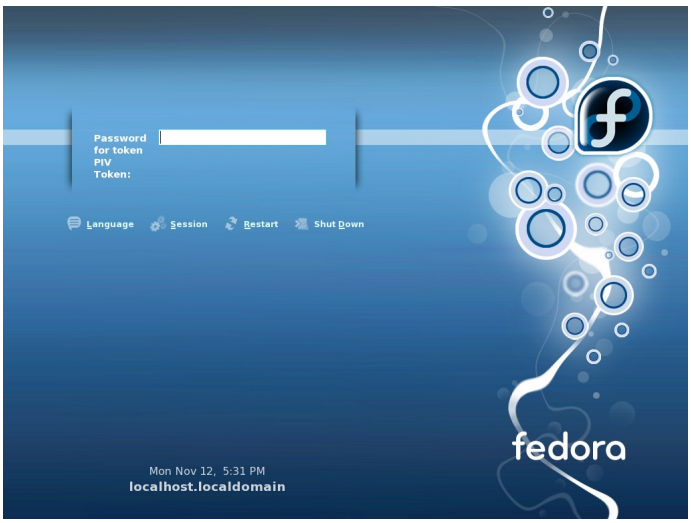

Figure 3-2. Linux Logon PIV Token Prompt

6. Enter the PIN number for the PIV Card.
7. In a few moments, you will be logged-in.

4. E-mail Signing and Encryption with PIV Card

The e-mail signing and encryption implementation described in this document utilizes the machine configuration depicted below. The configuration consists of two machines, one running Fedora Core 5 and the other running Windows XP Professional. Both machines utilize the Thunderbird e-mail client to perform e-mail signing and encryption (S/MIME). This configuration represents only one possible implementation of S/MIME using a PIV Card. Many other implementations exist.

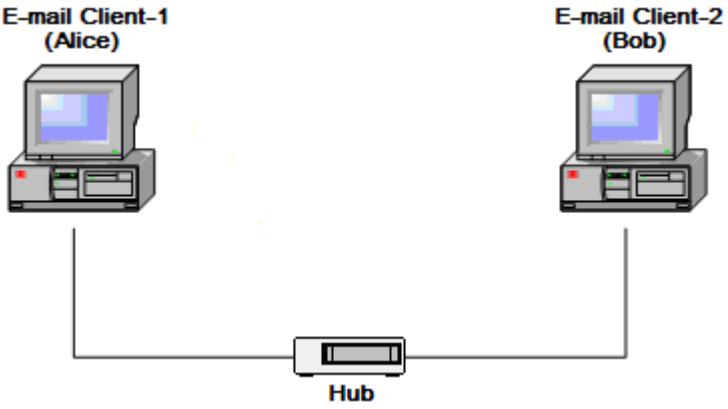

Figure 4-1. Machine Configuration for S/MIME Demonstration

The process of setting up this machine configuration involves performing the following steps:

+ Import issuing CA certificate into Linux Thunderbird
+ Configure Linux Thunderbird to use PIV credentials from a PIV Card
+ Configure other users' certificates in Linux Thunderbird
+ Import issuing CA certificate into Windows Thunderbird
+ Create PKCS12 file to hold encryption keys for Windows Thunderbird user
+ Import encryption keys from PKCS12 file into Windows Thunderbird
+ Configure other users' certificates in Windows Thunderbird

This section describes the configuration steps listed above. In addition, it describes how to use Thunderbird to perform S/MIME with the Digital Signature and Key Management keys and certificates found on a PIV Card.

Note: The latest version of Thunderbird (version 2.0.0.6 as of this publication) should be downloaded and installed before performing any steps described in this section. The latest version can be downloaded from Mozilla at http://www.mozilla.com/en-US/thunderbird/.

4.1 Configure Thunderbird for Linux

Note: The steps described in this section assume that Thunderbird has already been installed on the Linux workstation and an e-mail account has been set up. It also assumes that the user is currently

logged into the Linux workstation with their PIV Card using the steps provided in section 3.3. See section 6 for tips on troubleshooting Thunderbird installation and configuration issues that are not covered in this section.

4.1.1 Import Issuing CA Certificate into Thunderbird

1. Launch Thunderbird.
2. Select Edit | Account Settings. The account settings are displayed for the current user.
3. Select "Security" in the tree view on the left. The account security settings are displayed.
4. Click View Certificates. The Certificate Manager dialog is displayed.

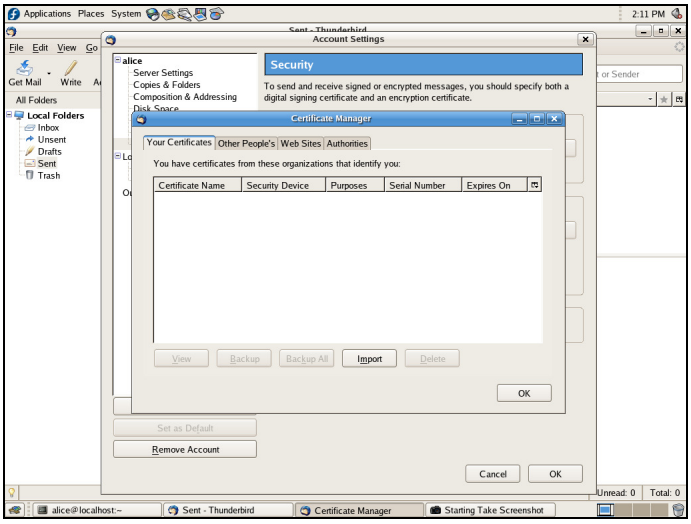

Figure 4-2. Thunderbird Certificate Manager

5. Select the "Authorities" tab.
6. Click Import. A browse dialog is displayed to select the certificate to import.
7. Navigate to the "/etc/pkcs11/cacerts" directory and select the issuing CA certificate to import. If the PIV Data Generator tool is used as the issuing CA then the issuing CA certificate filename is pivtestca.cer; however, the "etc/pkcs11/cacerts" directory contains the base64 version of this file and the filename will be whatever the user renamed it to in section 3.1.
8. Click Open.
9. The Downloading Certificate dialog is displayed.
10. Check the "Trust this CA to identify e-mail users" checkbox.
11. Click OK.
12. The issuing CA certificate is imported into Thunderbird and displayed in the "Authorities" tab (if using the PIV Data Generator as the issuing CA then it is listed under "NIST" as "PIV Test CA").
13. Click OK to close the Certificate Manager dialog.
14. Click OK to accept the new account security settings.

4.1.2 Configure Thunderbird to Use PIV Credentials

1. Launch Thunderbird.
2. Select Edit | Account Settings. The account settings are displayed for the current user.
3. Select "Security" in the tree view on the left. The account security settings are displayed.

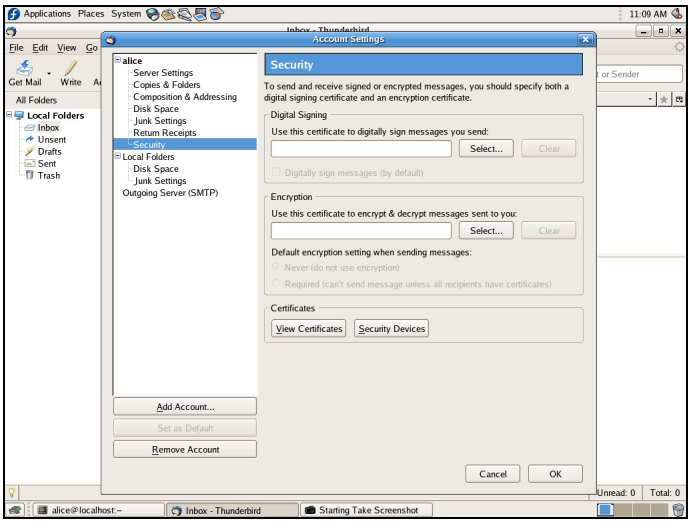

Figure 4-3. Thunderbird Account Security Settings

Configure PKCS#11 library

4. Click Security Devices. The "Device Manager" dialog is displayed.

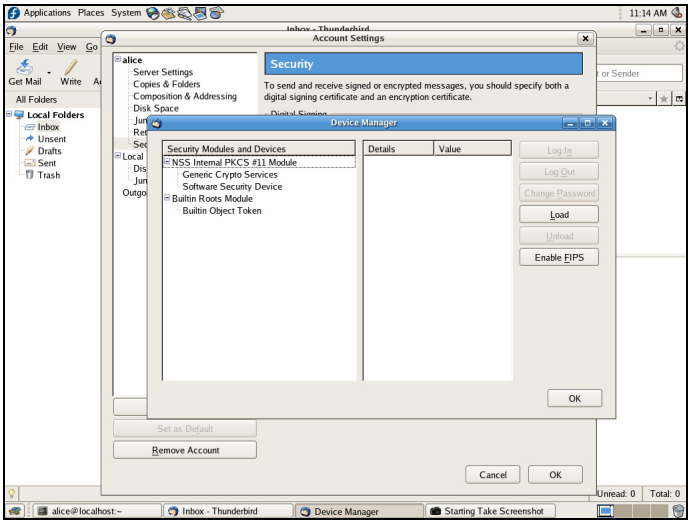

Figure 4-4. Thunderbird Device Manager

5. Click Load. The "Load PKCS#11 Device" dialog is displayed.
6. Enter "NIST PKCS#11" for the module name.
7. Enter "/usr/local/lib/pkcs11.so.1" for the module filename.
8. Click OK.
9. You will be asked to confirm the installation of the NIST PKCS#11 module in Thunderbird. Click OK.
10. A message is displayed indicating the NIST PKCS#11 module has been installed. Click OK.
11. The Device Manager displays the NIST PKCS#11 module in the list of installed security modules.

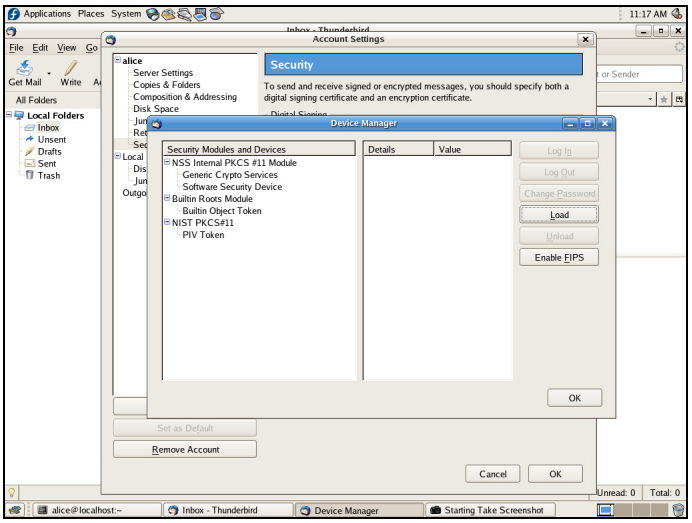

Figure 4-5. Thunderbird Device Manager with NIST PKCS#11 Installed

12. Click OK to close the Device Manager.
13. The account security settings is displayed again.

Configure e-mail digital signing

14. Click Select under "Digital Signing".
15. The PIV Token prompt is displayed. Enter the PIN for your PIV Card and click OK.
16. The Select Certificate dialog is displayed.
17. Select the X.509 Certificate for Digital Signature.

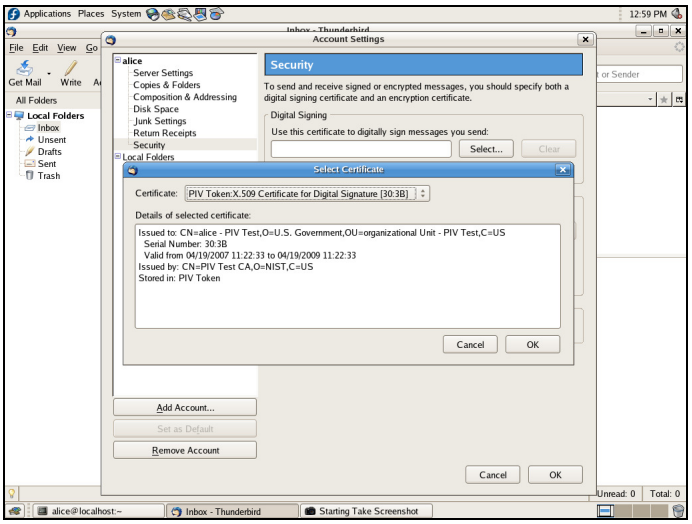

Figure 4-6. Thunderbird Select Certificate Window

18. Click OK.
19. A message is displayed asking if you want to use the same certificate to encrypt and decrypt messages sent to you. Click Cancel.

Configure e-mail encryption

20. The account security settings is displayed again. Click Select under "Encryption".
21. The Select Certificate dialog is displayed.
22. Select the X.509 Certificate for Key Management.
23. Click OK.
24. A message is displayed asking if you want to use the same certificate to digitally sign messages. Click Cancel.
25. Click OK to accept the new account security settings.

4.1.3 Configure Other Users' Certificates

In order to send encrypted e-mails to other users, their Key Management certificate needs to be imported into Thunderbird.

1. Launch Thunderbird.
2. Select Edit | Account Settings. The account settings are displayed for the current user.
3. Select "Security" in the tree view on the left. The account security settings are displayed.
4. Click View Certificates. The Certificate Manager dialog is displayed.
5. Select the "Other People's" tab.
6. Click Import. A browse dialog is displayed to select the certificate to import.
7. Select the Key Management certificate of the user to import.
8. Click Open.
9. The certificate is imported and listed in the Certificate Manager dialog.
10. Click OK to close the Certificate Manager dialog.
11. Click OK to accept the new account security settings.

4.2 Configure Thunderbird for Windows

Under Windows, the NIST Cryptographic Service Provider (CSP) provides cryptographic functions for a PIV Card similar to the NIST PKCS#11 module under Linux. However, the NIST CSP does not provide cryptographic functions to perform S/MIME. Hence, Thunderbird cannot be configured to use the NIST CSP to retrieve the Digital Signature and Key Management certificates necessary to perform S/MIME. This is a limitation of the NIST CSP and not of PIV Cards or the PIV standard – solution providers can develop their own PIV cryptographic module to support S/MIME. For those who wish to recreate the S/MIME configuration described above, the following subsections provide steps on configuring Thunderbird to perform S/MIME under Windows without using a PIV Card.

Note: The steps described in this section assume that Thunderbird has already been installed on the Windows XP workstation and an e-mail account has been set up. It also assumes that the user is currently logged into the Windows XP workstation.

4.2.1 Import Issuing CA Certificate into Thunderbird

1. Launch Thunderbird.
2. Select Tools | Account Settings. The account settings are displayed for the current user.
3. Select "Security" in the tree view on the left. The account security settings are displayed.
4. Click View Certificates. The Certificate Manager dialog is displayed.
5. Select the "Authorities" tab.
6. Click Import. A browse dialog is displayed to select the certificate to import.

7. Navigate to the directory that contains the issuing CA certificate to import and select the certificate (if the PIV Data Generator tool is used as the issuing CA then navigate to the "extra_files" subdirectory of the PIV Data Generator tool and select the "pivtestca.cer" file).
8. Click Open.
9. The Downloading Certificate dialog is displayed.
10. Check the "Trust this CA to identify email users" checkbox.
11. Click OK.
12. The issuing CA certificate is imported into Thunderbird and displayed in the "Authorities" tab (if using the PIV Data Generator as the issuing CA then it is listed under "NIST" as "PIV Test CA").
13. Click OK to close the Certificate Manager dialog.
14. Click OK to accept the new account security settings.

4.2.2 Create PKCS12 Files

A PKCS12 file stores both a private key and the accompanying public key certificate. In the absence of a PIV Card, it can be used to import a public/private key pair into Thunderbird. PKCS12 files need to be created for the Digital Signature and Key Management keys of the Windows user who will be receiving e-mails from the Linux user.

4.2.2.1 Create PKCS12 File for Digital Signature Key

1. Generate an RSA key pair for the Digital Signature key using the steps provided in section C.1.2.1.
2. Rename the resulting RSA key pair file digitalsig_key.pem.
3. Create a Digital Signature certificate using the RSA key pair generated in step 1 and the procedure described in section C.2. The resulting certificate should not contain certificate tag information pre-pended by the PIV Data Generator tool (refer to section C.2.3 on how to remove this information from the certificate).
4. Rename the resulting Digital Signature certificate file digitalsig.cer.
5. Copy the digitalsig_key.pem and digitalsig.cer files to the Cygwin user home directory. If Cygwin is installed in C:\Cygwin then the Cygwin user home directory is C:\Cygwin\home\[username].
6. Launch Cygwin.
7. Execute command: `openssl x509 -inform DER -in digitalsig.cer -outform PEM -out digitalsig_pem.cer`
8. A new file is created, digitalsig_pem.cer, that contains the base64 encoding of the digitalsig.cer file.
9. Execute command (replacing **[friendly name]** with the name of the person associated with the certificate): `openssl pkcs12 -export -in digitalsig_pem.cer -inkey digitalsig_key.pem -name "[friendly name]" -out digitalsig.p12`
10. You are prompted to enter a password that will be used to secure the PKCS12 file. Enter a password.
11. You are prompted to reenter the password. Reenter the password.
12. A new file is created, digitalsig.p12, that contains the private key and public key certificate for the Digital Signature key.

4.2.2.2 Create PKCS12 File for Key Management Key

1. Generate an RSA key pair for the Key Management key using the steps provided in section C.1.2.1.
2. Rename the resulting RSA key pair file keymanage_key.pem.

3. Create a Key Management certificate using the RSA key pair generated in step 1 and the procedure described in section C.2. The resulting certificate should not contain certificate tag information pre-pended by the PIV Data Generator tool (refer to section C.2.3 on how to remove this information from the certificate).
4. Rename the resulting Key Management certificate file keymanage.cer.
5. Copy the keymanage_key.pem and keymanage.cer files to the Cygwin user home directory. If Cygwin is installed in C:\Cygwin then the Cygwin user home directory is C:\Cygwin\home\[username].
6. Launch Cygwin.
7. Execute command: `openssl x509 -inform DER -in keymanage.cer -outform PEM -out keymanage_pem.cer`
8. A new file is created, keymanage_pem.cer, that contains the base64 encoding of the keymanage.cer file.
9. Execute command (replacing **[friendly name]** with the name of the person associated with the certificate): `openssl pkcs12 -export -in keymanage_pem.cer -inkey keymanage_key.pem -name "[friendly name]" -out keymanage.p12`
10. You are prompted to enter a password that will be used to secure the PKCS12 file. Enter a password.
11. You are prompted to reenter the password. Reenter the password.
12. A new file is created, keymanage.p12, that contains the private key and public key certificate for the Key Management key.

4.2.3 Import Digital Signature and Key Management Keys into Thunderbird

1. Launch Thunderbird.
2. Select Tools | Account Settings. The account settings are displayed for the current user.
3. Select "Security" in the tree view on the left. The account security settings are displayed.
4. Click View Certificates. The Certificate Manager dialog is displayed.
5. From the "Your Certificates" tab, click Import. A browse dialog is displayed to select the certificate to import.
6. Select the digitalsig.p12 file created in section 4.2.2.1.
7. Click Open.
8. If the Thunderbird master password is not set then you are prompted to enter a password to set it to. Enter a password and click OK.
9. If the Thunderbird master password has previously been set then you are prompted to enter it. Enter the master password and click OK.
10. You are prompted to enter the password for the PKCS12 file.
11. Enter the PKCS12 file password and click OK.
12. A message is displayed indicating the file was imported successfully.
13. Click OK. The certificate is listed in the Certificate Manager dialog.
14. Repeat steps 5 – 13 for the Key Management PKCS12 file created in section 4.2.2.2.
15. Click OK to close the Certificate Manager dialog.
16. Click OK to accept the new account security settings.

4.2.4 Configure Thunderbird to Use Digital Signature and Key Management Keys

1. Launch Thunderbird.
2. Select Tools | Account Settings. The account settings are displayed for the current user.
3. Select "Security" in the tree view on the left. The account security settings are displayed.

Configure e-mail digital signing

4. Click Select under "Digital Signing".
5. The Select Certificate dialog is displayed.
6. Select the X.509 Certificate for Digital Signature.
7. Click OK.
8. A message is displayed asking if you want to use the same certificate to encrypt messages. Click Cancel.

Configure e-mail encryption

9. The account security settings is displayed again. Click Select under "Encryption".
10. The Select Certificate dialog is displayed.
11. Select the X.509 Certificate for Key Management.
12. Click OK.
13. A message is displayed asking if you want to use the same certificate to digitally sign messages.
14. Click Cancel.
15. Click OK to accept the new Security Settings.

4.2.5 Configure Other Users' Certificates

In order to send encrypted e-mails to other users, their Key Management certificate needs to be imported into Thunderbird.

1. Launch Thunderbird.
2. Select Tools | Account Settings. The account settings are displayed for the current user.
3. Select "Security" in the tree view on the left. The account security settings are displayed.
4. Click View Certificates. The Certificate Manager dialog is displayed.
5. Select the "Other People's" tab.
6. Click Import. A browse dialog is displayed to select the certificate to import.
7. Select the Key Management certificate of the user to import.
8. Click Open.
9. The certificate is imported and listed in the Certificate Manager dialog.
10. Click OK to close the Certificate Manager dialog.
11. Click OK to accept the new account security settings.

4.3 Send/Received Signed E-mail

To digitally sign an e-mail using the user's Digital Signature key:

1. Launch Thunderbird.
2. Compose a message to a user in Linux.
3. Select Options | Security | Digitally Sign This Message.
4. A  icon appears in the lower right corner of the e-mail indicating the e-mail will be digitally signed before being sent.
5. Click Send.
6. The e-mail is digitally signed using the user's Digital Signature key and sent to the intended recipient.

When a digitally signed e-mail is received that contains a valid digital signature, the  icon appears in the e-mail. Clicking on the icon will display a dialog with information about the signing certificate.

Note:
1. These instructions apply to both the Linux and Windows versions of Thunderbird.
2. An e-mail can be signed and encrypted at the same time. See section 4.4 for instructions on encrypting an e-mail.

4.4 Send/Receive Encrypted E-mail

To encrypt an e-mail using the Key Management key of the intended recipient:

1. Launch Thunderbird.
2. Compose a message to a user.
3. Select Options | Security | Encrypt This Message.
4. A  icon appears in the lower right corner of the e-mail indicating the e-mail will be encrypted before being sent.
5. Click Send.
6. The e-mail is encrypted and sent to the intended recipient using their Key Management key.

When an encrypted e-mail is received, it is decrypted using the Key Management key of the user and the  icon appears in the e-mail. Clicking on the icon will display a dialog indicating that the message is encrypted.

Note:
1. These instructions apply to both the Linux and Windows versions of Thunderbird.
2. An e-mail can be signed and encrypted at the same time. See section 4.3 for instructions on signing an e-mail.

5. SSL Authentication with PIV Card

The SSL Authentication implementation described in this document utilizes the machine configuration depicted below. The configuration consists of a client machine, Web server, and Windows 2003 Server. The client machine is running Fedora Core 5 and has Firefox installed on it. The Web server machine is running Windows XP Professional and has IIS installed on it. In addition, the Web server is hosting the Visitor Management System sample Web application provided with the NIST PKCS#11 installation package. The Windows 2003 Server machine has Microsoft Certificate Services installed on it. This configuration represents only one possible implementation of SSL Authentication using a PIV Card. Many other implementations exist.

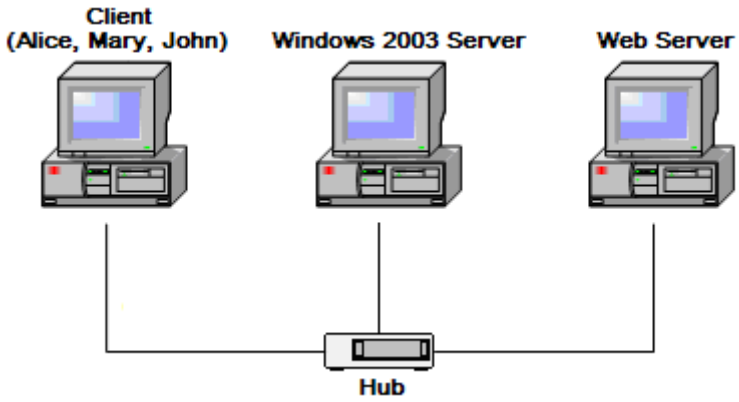

Figure 5-1. Machine Configuration for SSL Demonstration

The process of setting up this machine configuration involves performing the following steps:

+ Add Visitor Management System to IIS
+ Obtain and import Web Server certificate into IIS
+ Configure SSL and administrative privileges for Visitor Management System
+ Add CRL distribution point to IIS
+ Import issuing CA certificate into Firefox
+ Configure Firefox to use PIV credentials from a PIV Card

This section describes the configuration steps listed above (it is assumed that IIS and Firefox are already installed on the machines). In addition, it describes how to use Firefox to perform SSL authentication with the Visitor Management System sample Web application using the PIV Authentication certificate.

5.1 Configure Web Server

The following subsections provide steps on configuring IIS under Windows to recreate the configuration described above.

Note: Unless otherwise noted, the steps described in the following subsections assume the user is currently logged into the Windows XP workstation with administrator privileges.

5.1.1 Add Visitor Management System to IIS

The NIST PKCS#11 installation package includes the Visitor Management System Web application, a sample application that is used to demonstrate SSL authentication with a PIV Card. The Visitor Management System is a front-end to a visitor management database that allows users to add visitors to the database. The application supports two types of users:

+ Normal users – Normal users can access the Visitor Management System and view the visitors in the visitor management database

+ Administrators – Administrators can perform all functions that normal users can perform. Administrators also can add new visitors to the visitor management database.

The Visitor Management System relies on SSL authentication and a user's PIV Authentication certificate to verify the user's identity and allow access to the site. Upon access to the Visitor Management System, a list of visitors currently in the visitor management database is displayed to the user. In addition, the Visitor Management System provides a mechanism for users who have been designated as administrators to add new visitors to the database. Perform the following steps to add the Visitor Management System to IIS.

1. Copy the "piv" directory from the NIST PKCS#11 installation package to the C: drive. The "piv" directory is located at ".\Sample Web-Application\piv".
2. Launch IIS.
3. Expand the "local computer" item in the tree view.
4. Expand the "Web Sites" folder in the tree view.
5. Right-click on the "Default Web Site" item in the tree view.
6. In the pop-up menu, select New | Virtual Directory.
7. The Virtual Directory Creation Wizard is displayed. Click Next.
8. Enter "piv" for the virtual directory alias and click Next.
9. Enter "c:\piv" for the directory path to the virtual directory and click Next.
10. The Access Permissions dialog is displayed. Ensure the "Read" and "Run Scripts (such as ASP)" checkboxes are checked and click Next.
11. Click Finish.
12. The "piv" virtual directory appears in IIS.

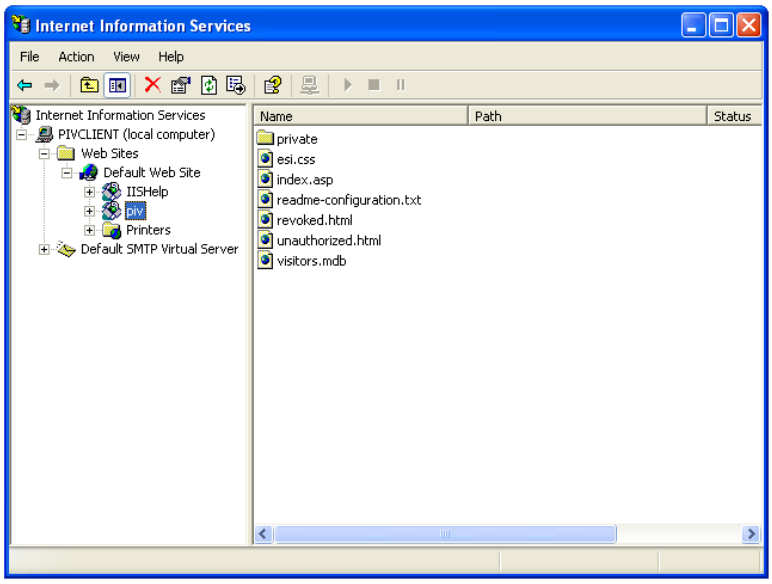

Figure 5-2. Visitor Management System Virtual Directory in IIS

13. Right-click on the "piv" item in the tree view.
14. In the popup menu, select Properties.
15. The "piv" virtual directory properties are displayed.

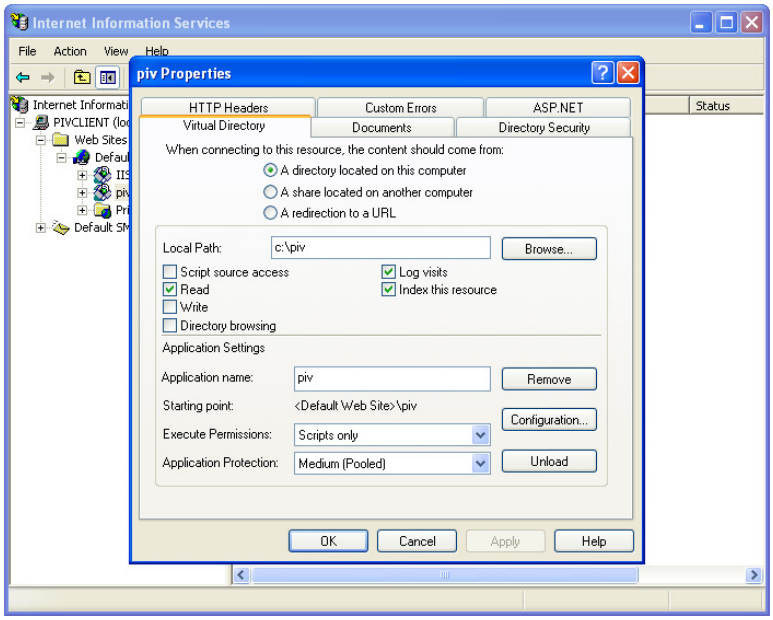

Figure 5-3. Visitor Management System Properties in IIS

16. Select the "Custom Errors" tab.
17. Select the "401;3" HTTP error and click Edit Properties.
18. The Error Mapping Properties dialog is displayed.
19. Change the value of the "File" field to "c:\piv\unauthorized.html".
20. Click OK.
21. The "Custom Errors" tab is redisplayed.
22. Select the "403;13" HTTP error and click Edit Properties.

23. The Error Mapping Properties dialog is displayed.
24. Change the value of the "File" field to "c:\piv\revoked.html".
25. Click OK.
26. The "Custom Errors" tab is redisplayed.
27. Click OK.
28. Close IIS.

5.1.2 Configure Secure Communication for Visitor Management System

5.1.2.1 Generate Web Server Certificate Request

In order to enable secure communication on the Web server, a Web server certificate needs to be installed in IIS. Perform the following steps to generate a Web server certificate request, which can be submitted to a Certificate Authority to obtain a Web server certificate.

1. Launch IIS.
2. Expand the "local computer" item in the tree view.
3. Expand the "Web Sites" folder in the tree view.
4. Right-click on the "Default Web Site" item in the tree view.
5. Select Properties from the pop-up menu.
6. The Web site properties are displayed. Select the "Directory Security" tab.
7. Click Server Certificate.
8. The Web Server Certificate Wizard is displayed.

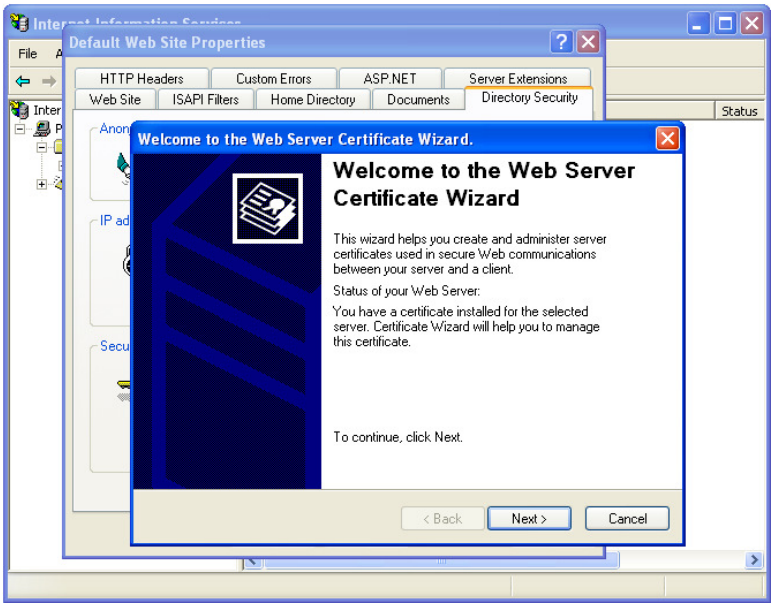

Figure 5-4. IIS Web Server Certificate Wizard

9. Click Next.
10. Select "Create a new certificate" and click Next.
11. Select "Prepare the request now, but send it later" and click Next.
12. The Name and Security Settings dialog is displayed.
13. Enter "pivdemo" for the certificate name.
14. Select "1024" for the encryption bit length.
15. Click Next.

16. Enter a name for your organization and organizational unit and click Next.
17. Enter "pivclient" for the common name and click Next.
18. Enter your country, state, and city, and click Next.
19. Enter "c:\certreq.txt" for the filename and click Next.
20. A summary of the selected options is displayed. Click Next.
21. Click Finish.
22. The Web Server certificate request is saved to c:\certreq.txt.
23. Click OK to close the Web site properties dialog.
24. Close IIS.

5.1.2.2 Obtain Web Server Certificate

After a Web Server certificate request has been generated, the request must be submitted to a Certificate Authority to obtain the Web Server certificate. In this implementation, a Windows Server 2003 machine has been configured with Microsoft Certificate Services and will be used to issue the Web Server certificate.

1. Log into the Windows Server 2003 machine using an account with administrative privileges.
2. Launch Internet Explorer.
3. Enter http://localhost/certsrv in the address window.
4. Microsoft Certificate Services is displayed.

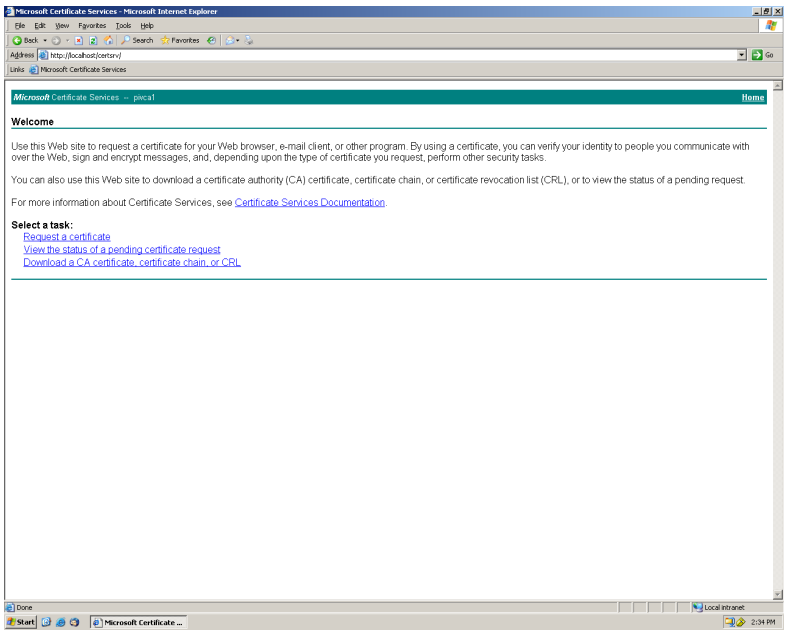

Figure 5-5. Microsoft Certificate Services

5. Click the "Request a certificate" link.
6. Click the "advanced certificate request" link.
7. Click the "Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file" link.
8. Copy the contents of the certreq.txt file created in section 5.1.2.1 and paste it in the "Saved Request" box.
9. Select "Web Server" for the Certificate Template field.

10. Click Submit.
11. The certificate is issued.
12. Select "DER encoded" and click the "Download certificate" link.
13. The File Download dialog is displayed.
14. Click Save.
15. The Save As dialog is displayed.
16. Enter "pivwebserver.cer" for the filename and save the certificate to it.
17. Close Internet Explorer.

5.1.2.3 Install Web Server Certificate

1. Copy the pivwebserver.cer file created in section 5.1.2.2 to the Web server machine (i.e., the Windows XP workstation).
2. Launch IIS.
3. Expand the "local computer" item in the tree view.
4. Expand the "Web Sites" folder in the tree view.
5. Right-click on the "Default Web Site" item in the tree view.
6. Select Properties from the pop-up menu.
7. The Web site properties are displayed. Select the "Directory Security" tab.
8. Click Server Certificate.
9. The Web Server Certificate Wizard is displayed. Click Next.
10. Select "Process the pending request and install the certificate" and click Next.
11. Enter the file path to the pivwebserver.cer file and click Next.
12. The certificate details are displayed. Click Next.
13. Click Finish.
14. The Web server certificate is installed in IIS.
15. Click OK to close the Web site properties dialog.
16. Close IIS.

5.1.2.4 Configure Integrated Windows Authentication

Integrated Windows authentication provides a secure form of user authentication. Perform the following steps to enable Integrated Windows Authentication in IIS.

1. Launch IIS.
2. Expand the "local computer" item in the tree view.
3. Expand the "Web Sites" folder in the tree view.
4. Right-click on the "Default Web Site" item in the tree view.
5. Select Properties from the pop-up menu.
6. The Web site properties are displayed. Select the "Directory Security" tab.
7. Click Edit in the "Anonymous access and authentication control" group box.
8. The Authentication Methods dialog is displayed.
9. Check the "Integrated Windows Authentication" checkbox.
10. Click OK.
11. The "Directory Security" tab is redisplayed.
12. Click OK to close the Web site properties dialog.
13. Close IIS.

5.1.2.5 Enable SSL Authentication

1. Launch IIS.

2. Expand the "local computer" item in the tree view.
3. Expand the "Web Sites" folder in the tree view.
4. Expand the "Default Web Site" item in the tree view.
5. Right-click on the "piv" item in the tree view (the "piv" item was created in section 5.1.1).
6. Select Properties from the pop-up menu.
7. The Web site properties are displayed. Select the "Directory Security" tab.
8. Click Edit in the "Secure communications" group box.
9. The Secure Communications dialog is displayed.
10. Check the "Require secure channel (SSL)" checkbox.
11. Check the "Require 128-bit encryption" checkbox.
12. Select "Require client certificates" in the "Client certificates" group box.
13. Check the "Enable client certificate mapping" checkbox.
14. Click Edit.
15. The Account Mappings dialog is displayed.
16. Select the "1-to-1" tab.
17. Click Add.
18. Select the PIV authentication certificate of a user who will be granted administrative access to the Visitor Management System Web site and click Open. The user's PIV authentication certificate can be retrieved from their PIV Card using the PIV Data Loader tool (see Appendix A) – be sure the extra tags prepended to the certificate are removed as described in Appendix C.2.3.
19. The Map to Account dialog is displayed.
20. Click Browse.
21. The Select User dialog is displayed.
22. Enter "Administrator" in the object name box and click OK.
23. The Map to Account dialog is redisplayed with the full name of the Administrator account entered in the Account field.
24. Enter the password associated with the Administrator account and click OK.
25. The Confirm Password dialog is displayed. Reenter the password and click OK.
26. The new mapping is displayed.

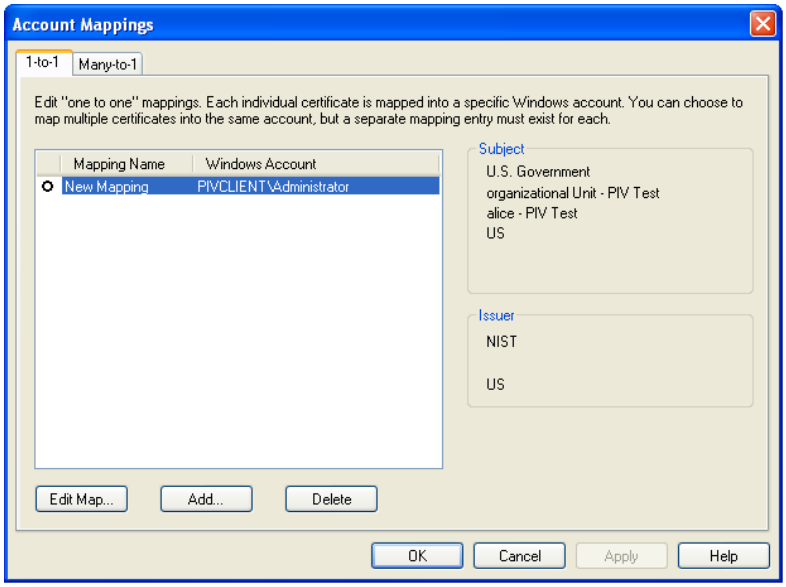

Figure 5-6. IIS Account Mappings

27. Repeat steps 17 – 26 for each additional user who will be granted administrative access to the Visitor Management System Web site.
28. Click OK.
29. The Secure Communications dialog is redisplayed.
30. Click OK.
31. The Web site properties are redisplayed.
32. Click OK to close the Web site properties dialog.
33. Close IIS.

Note: Be sure the administrator password entered in step 24 is correct. IIS does not validate the password – it only confirms that the password was reentered correctly (in step 25). If an invalid password is entered then certificate mapping will not work correctly. See section 6.3 for troubleshooting tips on detecting an invalid certificate mapping.

5.1.3 Set Access Privileges for Visitor Management System

The Visitor Management System supports two types of users: ordinary users and administrators. Ordinary users can view the list of visitors currently in the Visitor Management System. Administrators, on the other hand, can view the list of visitors currently in the system as well as add new visitors to it. Access privileges for the Visitor Management System are controlled by NTFS file permissions for the site's directories. Perform the following steps to set access privileges for the Visitor Management System.

1. Launch Windows Explorer.
2. Navigate to the c:\piv directory.
3. Right-click on the directory and select Sharing and Security from the pop-up menu.
4. Select the "Security" tab.
5. A list of users and groups with access to the directory is displayed.
6. Ensure that the local Users account is listed. If it is then click Cancel and proceed to step 13.
7. To add the local Users account to this list, click Add.
8. The Select Users and Groups dialog is displayed.
9. Enter "Users" in the edit box and click OK.
10. The access permission for the directory is redisplayed.
11. In the list of permission for the local Users account, ensure that ONLY the Read & Execute, List Folder Contents, and Read permission checkboxes are checked.
12. Click OK to accept the changes.
13. Navigate to the c:\piv\private directory.
14. Right-click on the directory and select Sharing and Security from the pop-up menu.
15. Select the "Security" tab.
16. A list of users and groups with access to the directory is displayed.
17. Click Advanced.
18. Uncheck the "Inherit from parent the permission entries that apply to child objects. Include these with entries explicitly defined here" checkbox.
19. A dialog is displayed asking you to confirm your choice. Click Copy.
20. The "Permissions" tab displays all user/group permissions for this directory. Remove all users and groups from this list except the following users/groups: Administrator, Administrators, CREATOR OWNER, and SYSTEM. A user or group can be removed from this list by selecting the entry and clicking Remove.
21. Click OK to return to the "Security" tab.
22. Click OK to accept the security settings.

5.1.4 Add CRL Distribution Point to IIS

A Certificate Revocation List (CRL) contains a list of certificates, identified by serial number, that have been revoked and are no longer valid. In order for the Web server to verify that a user's PIV Authentication certificate is still valid when the user accesses the Visitor Management System Web site, it needs to access the CRL located at the CRL distribution point specified in the user's PIV Authentication certificate. The steps below describe how to add a CRL distribution point to IIS.

Note:

1. These steps should only be followed if the CRL distribution point refers to a location that is to be hosted on the local Web server. If the CRL distribution point refers to a remote location then these steps should be skipped. However, the reader should ensure that the remote CRL distribution point is accessible by the Web server.

2. The implementation described herein utilizes CRL checking to verify certificate status. Although other methods exist to perform certificate validation, such as Online Certificate Status Protocol (OCSP),their usage is beyond the scope of this document.

1. View the PIV Authentication certificate in Windows (see section C.2.4) and record the CRL distribution point (specified in the "CRL Distribution Points" certificate extension).
2. Note the CRL directory and filename specified in the CRL distribution point. For example, if the CRL distribution point is http://localhost/crl/ca.crl then the CRL directory is "crl" and the CRL filename is "ca.crl" (i.e., http://[computer_name]/[crl_directory]/[crl_filename]).
3. Recreate the directory structure of the specified CRL directory name on the C: drive. In this example, the directory "crl" would be created on the C: drive.
4. Copy the issuing CA's CRL file to the directory created in step 3. If the PIV Data Generator was used to issue the PIV Authentication certificate then the CRL file can be found in the "extra_files" subdirectory of the PIV Data Generator tool and is named pivtestca.crl.
5. Rename the CRL file to the CRL filename specified in step 2. In this example, the pivtestca.crl file would be copied to the c:\crl directory and renamed ca.crl.
6. Launch IIS.
7. Expand the "local computer" item in the tree view.
8. Expand the "Web Sites" folder in the tree view.
9. Right-click on the "Default Web Site" item in the tree view.
10. In the pop-up menu, select New | Virtual Directory.
11. The Virtual Directory Creation Wizard is displayed. Click Next.
12. Enter the CRL directory name for the virtual directory alias and click Next (in this example, the virtual directory alias is "crl").
13. Enter the path to the CRL virtual directory and click Next (in this example, the virtual directory path is "c:\crl".
14. The Access Permissions dialog is displayed. Ensure the "Read" and "Run Scripts (such as ASP)" checkboxes are checked and click Next.
15. Click Finish.
16. The CRL distribution point is added to IIS.

5.2 Configure Firefox

5.2.1 Import Issuing CA Certificate into Firefox

1. Launch Firefox.
2. Select Edit | Preferences. The Firefox preferences are displayed for the current user.

3. Select the "Advanced" icon in the toolbar.
4. Select the "Security" tab in the advanced preferences. The security preferences are displayed.
5. Click View Certificates. The "Certificate Manager" dialog is displayed.
6. Select the "Authorities" tab.
7. Click Import. A browse dialog is displayed to select the certificate to import.
8. Navigate to the "/etc/pkcs11/cacerts" directory and select the issuing CA certificate to import. If the PIV Data Generator tool is used as the issuing CA then the issuing CA certificate filename is pivtestca.cer; however, the "etc/pkcs11/cacerts" directory contains the base64 version of this file and the filename will be whatever the user renamed it to in section 3.1.
9. Click Open.
10. The Downloading Certificate dialog is displayed.
11. Check the "Trust this CA to identify web sites" checkbox.
12. Click OK.
13. The issuing CA certificate is imported into Firefox and displayed in the "Authorities" tab (if using the PIV Data Generator as the issuing CA then it is listed under "NIST" as "PIV Test CA").
14. Click OK to close the Certificate Manager dialog.
15. The security preferences are displayed again. Click Close.

5.2.2 Configure Firefox to Use PIV Credentials

1. Make sure your PIV Card is inserted in the smart card reader.
2. Launch Firefox.
3. Select Edit | Preferences. The Firefox preferences are displayed.
4. Select the "Advanced" icon in the toolbar.
5. Select the "Security" tab in the advanced preferences. The security preferences are displayed.
6. Click Security Devices. The "Device Manager" dialog is displayed.

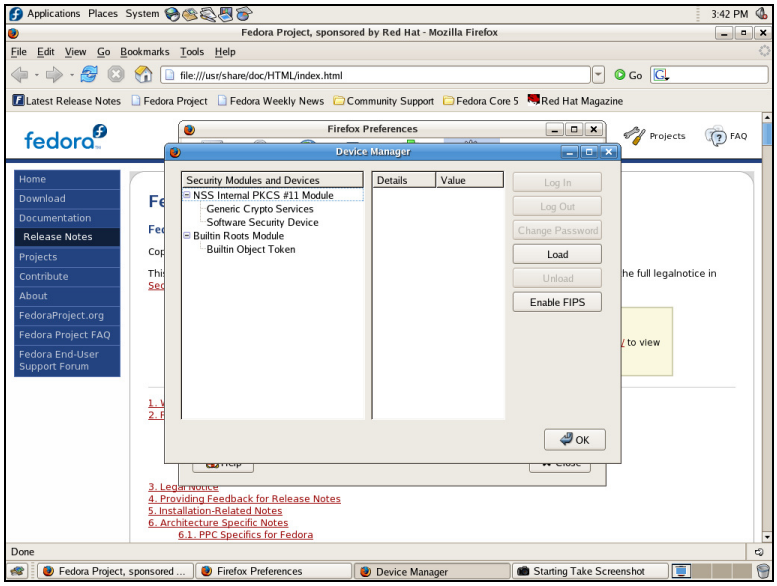

Figure 5-7. Firefox Device Manager

7. Click Load. The "Load PKCS#11 Device" dialog is displayed.
8. Enter "NIST PKCS#11" for the module name.
9. Enter "/usr/local/lib/pkcs11.so.1" for the module filename.
10. Click OK.

11. You will be asked to confirm the installation of the NIST PKCS#11 module in Firefox. Click OK.
12. A message is displayed indicating the NIST PKCS#11 module has been installed. Click OK.
13. The Device Manager displays the NIST PKCS#11 module in the list of installed security modules.

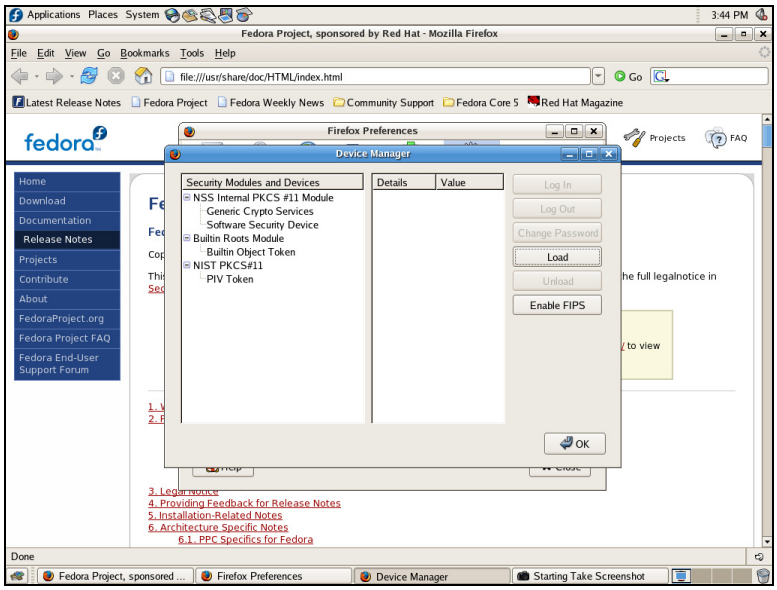

Figure 5-8. Firefox Device Manager with NIST PKCS#11 Installed

14. Click OK to close the Device Manager.
15. The security preferences are displayed again. Click Close.

5.3 Visitor Management System Use Cases

The following Visitor Management System use cases are described in this document:

+ Access Visitor Management System – This use case demonstrates how both normal users and administrators can access the Visitor Management System and view the list of visitors in the visitor management database.

+ Verify Access Permissions – This use case is used to verify that administrators can successfully add new visitors to the visitor management database. It also is used to verify that normal users can access the Visitor Management System and view the list of visitors currently in the database, but they cannot add new visitors to the database.

+ Certificate Revocation Checking – This use case is used to verify that the Visitor Management System is performing CRL checking correctly and that users whose PIV Authentication certificate has been revoked cannot gain access to the system.

5.3.1 Access Visitor Management System

1. Log into the Linux workstation with your PIV Card (see section 3.2).
2. Launch Firefox.

3. Enter "https://[*web server*]/piv/index.asp" in the address window to access the Visitor Management System Web site, where *web server* is the IP address of the Web server (e.g., https://192.168.0.11/piv/index.asp).
4. The first time the site is accessed, a message is displayed indicating the Web server's certificate is not from a trusted site.

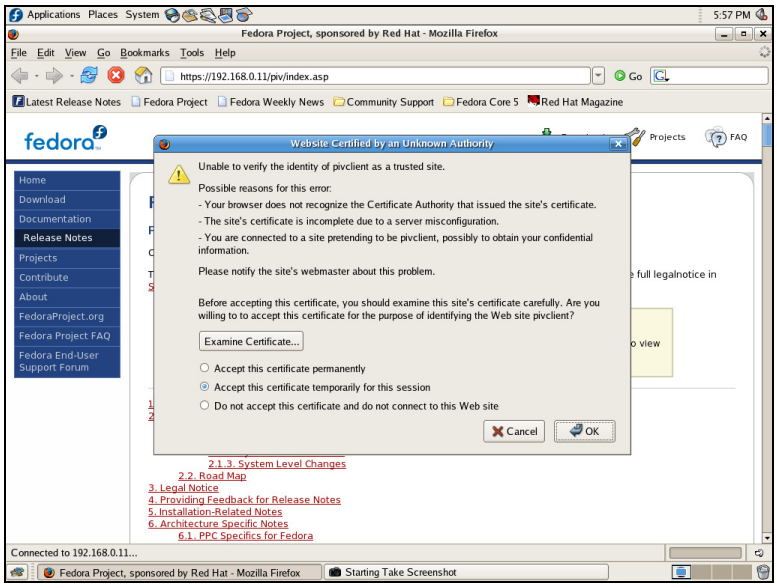

Figure 5-9. Untrusted Web Site Prompt

5. Select "Accept this certificate permanently" and click OK.
6. A message is displayed asking you to confirm the certificate belongs to the Web server.
7. Click OK.
8. You are prompted to enter the PIN for the PIV Card.
9. Enter the PIV Card PIN number and click OK.
10. The Visitor Management System main page is displayed.

5.3.2 Verify Access Permissions to Visitor Management System

Section 5.1 describes how to configure IIS to map PIV Authentication certificates to user accounts so that certain users are granted administrative access to the Visitor Management System Web site. Perform the following to verify account permissions.

5.3.2.1 Verify Administrative Access is Granted

1. Log into the Linux workstation using a PIV Card that is associated with an account that has been granted administrative access to the Visitor Management System Web site.
2. Access the Visitor Management System Web site as described in section 5.3.1.
3. Click Add Visitor to the List.
4. The Add Visitor page is displayed.
5. Enter the name of the visitor to add.
6. Select the valid start date for this visitor.
7. Select the valid end date for this visitor.
8. Click Add Visitor to the List.
9. A confirmation page is displayed indicating the visitor has been added to the system.

10. Click View Visitor List.
11. The Visitor Management System main page is displayed with the newly added visitor.

5.3.2.2 Verify Administrative Access is Restricted

1. Log into the Linux workstation with a PIV Card that is associated with an account that has NOT been granted administrative access to the Visitor Management System Web site.
2. Access the Visitor Management System Web site as described in section 5.3.1.
3. Click Add Visitor to the List.
4. A prompt is displayed to enter the username and password of an account that has been granted administrative access to the Visitor Management System Web site.
5. Click Cancel.
6. A page is displayed indicating you are not authorized to perform this action.
7. Click Go Back.
8. The Visitor Management System main page is displayed.

5.3.3 Check for Revoked Certificates

The Visitor Management System Web site utilizes CRL checking to determine whether a user's PIV Authentication certificate has been revoked. For demonstration purposes, the implementation described herein references the CRL packaged with the PIV Data Generator tool, which has been configured to revoke certificates having a serial number of 9. The following steps can be performed to verify that certificate revocation status is being checked for the Visitor Management System Web site.

1. Load a PIV Authentication certificate onto a PIV Card where the certificate's serial number is set to 9 (see Appendix C for instructions on creating and loading a PIV Authentication certificate onto a PIV Card).
2. Log into the Linux workstation with the PIV Card.
3. Access the Visitor Management System Web site as described in section 5.3.1.
4. A page is displayed indicating your certificate has been revoked.

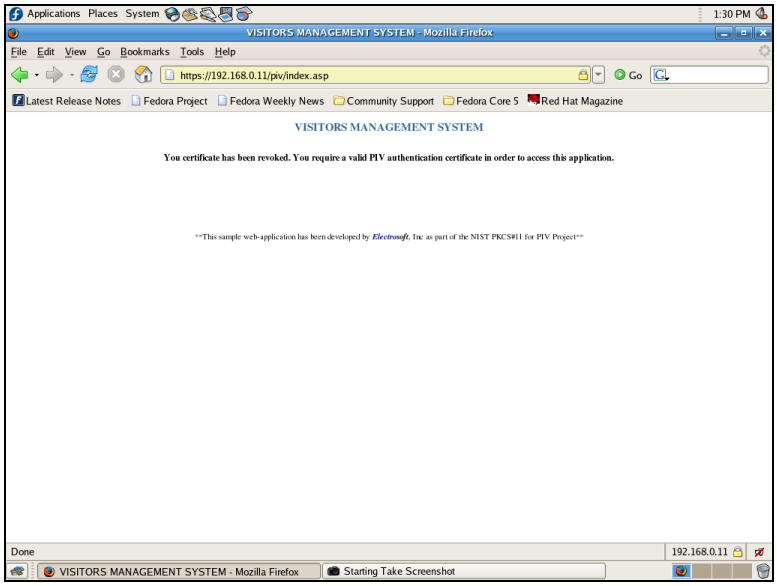

Figure 5-10. Revoked Certificate Page

5. Close Firefox.

6. Troubleshooting Tips

This section covers how to handle some issues you may encounter when attempting Linux Logon, S/MIME, or SSL Authentication using a PIV Card.

6.1 Troubleshooting Linux Logon

6.1.1 Invalid Root CA Certificate Format

When installing the PAM module for Linux Logon, the root CA certificates that will be used for certificate validation need to be in base64 format. Perform the following steps to convert a certificate from DER to base64 format:

1. Copy a root CA certificate file to the Cygwin user home directory. If Cygwin is installed in C:\Cygwin then the Cygwin user home directory is C:\Cygwin\home\[username].
2. Launch Cygwin.
3. Execute command: `openssl x509 -inform DER -in [DER root CA filename] -outform PEM -out [base64 root CA filename]`

   Ex: `openssl x509 -inform DER -in pivtestca.cer -outform PEM -out pivtestca_pem.cer`

4. A new certificate file is created in the Cygwin user home directory with the specified output filename that contains the base64 encoding of the input certificate file.

6.1.2 Login Failed Due to Invalid Username or Password

When attempting to log onto the Linux workstation using a PIV Card, the following error may be displayed:

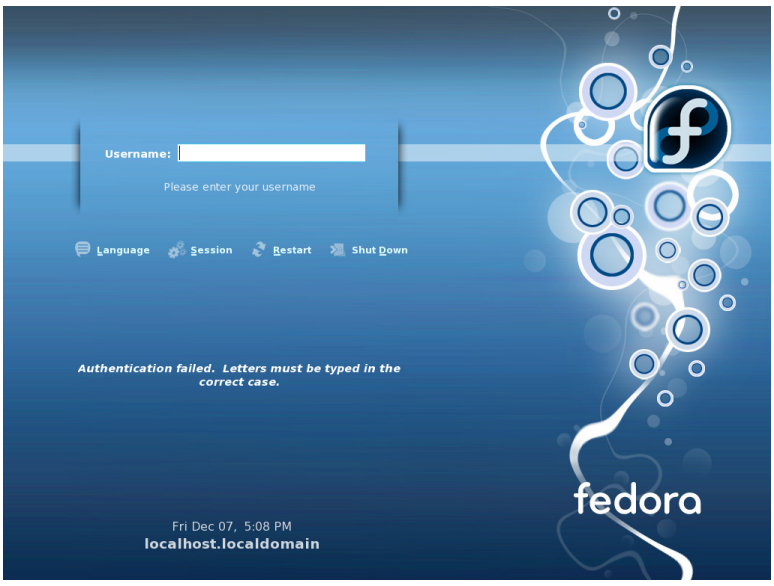

Figure 6-1. Linux Login Failure Due to Invalid Username or Password

This error is due to an invalid username and/or PIN number that was entered for the PIV Card. Make sure the username and/or PIN number associated with the PIV Card is entered correctly. Note that the username must be entered in the correct case.

6.1.3 Login Failed Due to Missing User Account

When attempting to log onto the Linux workstation using a PIV Card, the following error may be displayed:

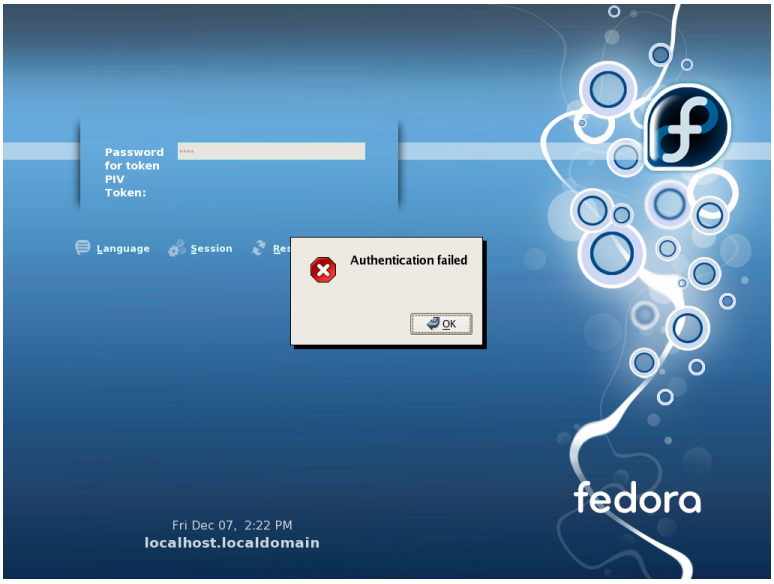

Figure 6-2. Linux Login Failure Due to Missing User Account

This error occurs when a username is entered but the corresponding user account does not exist. Perform the following steps to add a new user account:

1. Remove the PIV Card from the reader.
2. Login as the 'root' user.
3. Select System | Administration | Users and Groups from the Fedora Core 5 menu.
4. The User Manager is displayed.
5. Select the "Users" tab.
6. Click Add User in the toolbar.
7. Enter the username for the account. The username should match the Common Name or UPN extension in the PIV Authentication certificate of the PIV Card.
8. Enter the remaining account information and click OK.
9. The newly created account is displayed in the User Manager window.

6.2 Troubleshooting S/MIME

6.2.1 NIST PKCS#11 Module Cannot Be Loaded in Thunderbird

If after attempting to load the NIST PKCS#11 module in Thunderbird, it still does not appear in the Device Manager list then examine the list of security modules that are currently installed. There should be an installed security module named "NSS Internal PKCS #11 Module". If no security modules are listed then Thunderbird may have been installed using the "Add/Remove Software" feature of Fedora,

which causes an older version to be installed. Remove Thunderbird from the workstation using the "Add/Remove Software" feature, and download and install the latest version.

6.2.2 Library Dependencies for Thunderbird Not Installed

When running Thunderbird for the first time under Fedora Core 5, the following error may be encountered:

> **Error while loading shared libraries: libstdc++.so.5: cannot open shared object file: No such file or directory**

By default, Fedora Core 5 is not installed with legacy shared libraries necessary for Thunderbird to run. The required libraries can be installed by performing the following steps:

1. Ensure the Linux workstation is connected to the Internet.
2. Login as the 'root' user.
3. Select Applications | Add/Remove Software from the Fedora Core 5 menu.
4. In a few moments, the Package Manager is displayed.

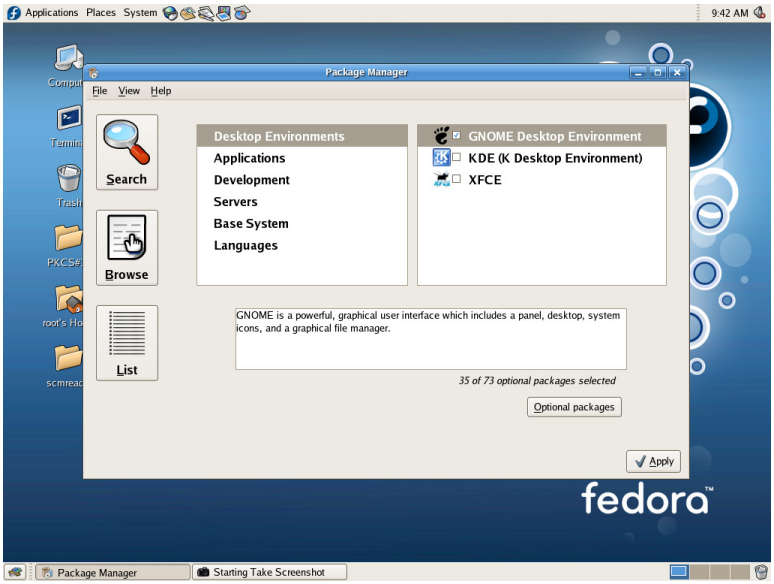

Figure 6-3. Fedora Package Manager

5. Select the Development package group.
6. Check the Legacy Software Development package checkbox.
7. Click Apply.
8. The Package Selections dialog is displayed.
9. Click Continue.
10. In a few moments, the selected package is installed.
11. Click OK.

6.2.3 Failure to Encrypt E-mail

When attempting to send an encrypted e-mail using Thunderbird, the following error may be encountered:

Sending of message failed. You specified encryption for this message, but the application failed to find an encryption certificate for [recipient].

The Key Management certificate for the intended recipient must be imported into Thunderbird before an encrypted e-mail can be sent to that person. Follow the procedure in section 4.1.3 to import this certificate.

6.3 Troubleshooting SSL Authentication

6.3.1 Access Failed Due to Missing Certificate

When attempting to access the Visitor Management System using Firefox, the following error may be encountered:

The page requires a client certificate

This error occurs when Firefox cannot retrieve the PIV Authentication certificate from the PIV Card to perform SSL client authentication. Make sure Firefox has been configured to use the NIST PKCS#11 module (see section 5.2) and the PIV Card is securely inserted into the smart card reader. If the PIV Card is inserted in the smart card reader then Firefox has lost communication with the PIV Card. Restart Firefox and if still unsuccessful, restart the Linux workstation.

6.3.2 Invalid Certificate Mapping in IIS

When accessing the Visitor Management System with an account that has administrative privileges, you may be prompted to enter a username and password. This is an indication that the administrator password entered in section 5.1.2.5 to map the user's certificate to the administrator account is invalid. To verify this, perform the following steps on the Windows XP workstation where the Visitor Management System is hosted:

1. From the Windows Control Panel, select Administrative Tools | Event Viewer.
2. Select System from the tree view on the left.
3. Look for any errors that appear in the System Event Log. If an invalid password was entered in section 5.1.2.5 then an error similar to the following will appear in the log:

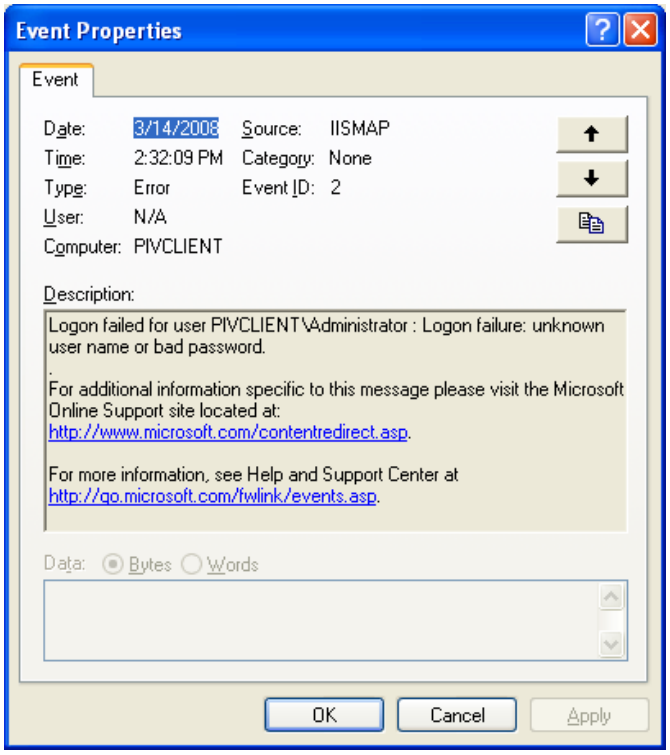

Figure 6-4. Invalid Certificate Mapping in IIS

To resolve this error, delete the certificate mapping in IIS and perform the steps described in section 5.1.2.5 to recreate the certificate mapping, ensuring that the correct administrator password is entered.

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
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 Loader tool	Loads PIV data elements onto a PIV Card	Online: http://csrc.nist.gov/groups/SNS/piv/download.html Click "PIV Data Generator and PIV Data Loader" 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 Generator tool	PIV data element generation	Online: http://csrc.nist.gov/groups/SNS/piv/download.html Click "PIV Data Generator and PIV Data Loader" and follow the instructions to download. Extract the zip and view the Readme.txt file for additional requirements and instructions on running the tool.
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.

Tool Name	Purpose	How to Obtain
TestResMan 1.42.00.01	PC/SC APDU Utility	Online: http://www.scmmicro.com/support/pcs_downloads.php?lang=en Click "Utilities" from the list of available downloads. Accept the EULA and click Next. Click "TestResMan V1.xx" to download the file. Extract the zip and run TestResMan.exe 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)
Mozilla Firefox	Web browser	Online: http://www.mozilla.com/en-US/firefox/all.html Download and extract the latest version.
Mozilla Thunderbird	E-mail client	Online: http://www.mozilla.com/en-US/thunderbird/all.html Download and extract the latest version.

Appendix B—Cygwin

Appendix B describes how to install the 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 bog 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 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 Linux Logon, e-mail signing and encryption, and web authentication under Linux. 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 Linux Logon, e-mail signing and encryption, and web authentication. These applications are not dependent on other mandatory PIV data objects, such as the CHUID and Card Capability Container. Hence, instructions are not provided to generate and load 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 Pairs 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.

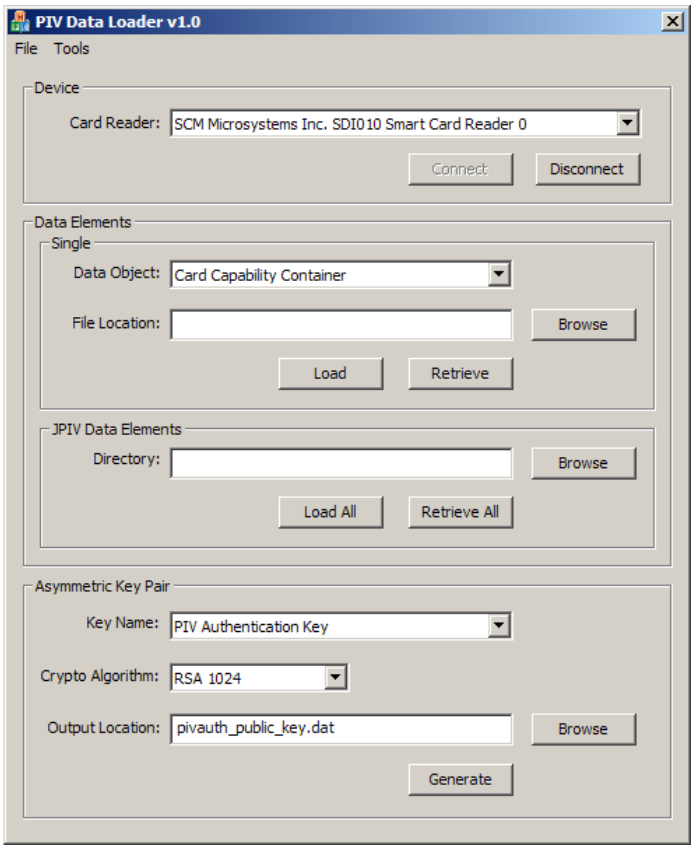

Figure C-1. Generating RSA Key Pairs with PIV Data Loader

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

OpenSSL can be used to generate an RSA 1024-bit key pair that is loaded onto a BasicCard. Unlike a real PIV Card, the BasicCard 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, 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.

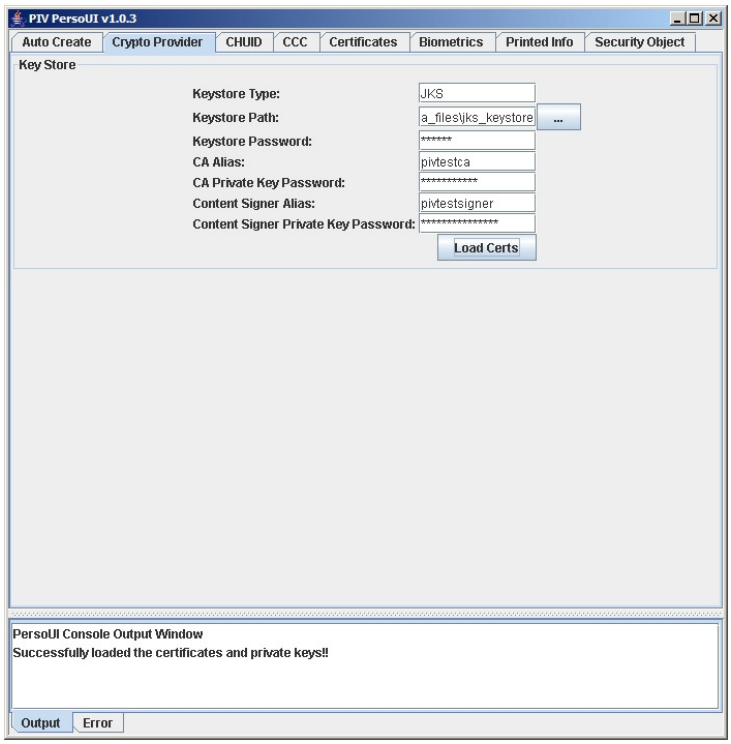

Figure C-2. PIV Data Generator Crypto Provider Tab

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.

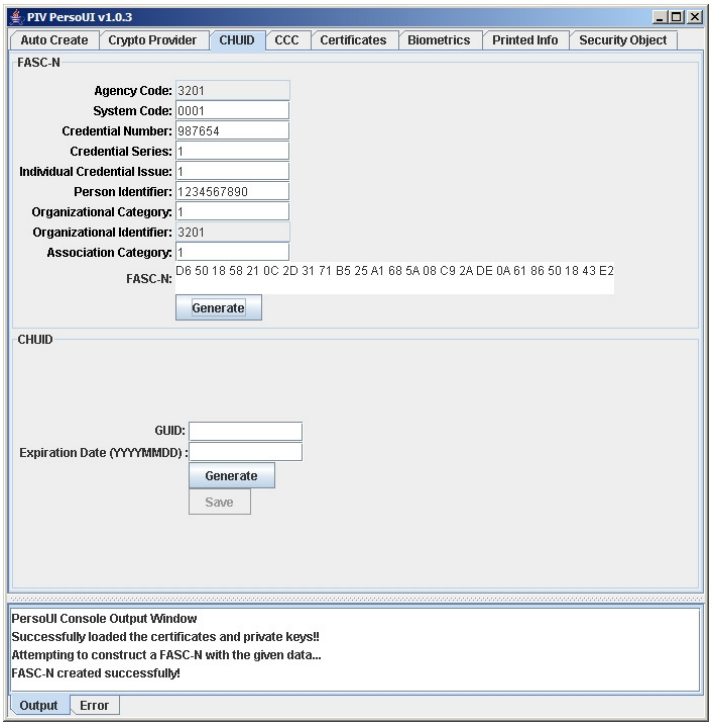

Figure C-3. PIV Data Generator CHUID Tab – FASC-N Fields

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.

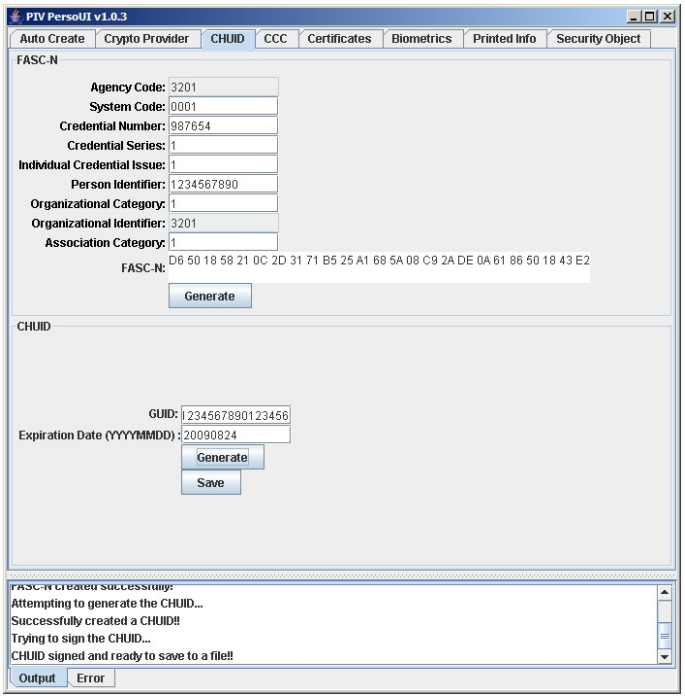

Figure C-4. PIV Data Generator CHUID Tab – CHUID Fields

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.

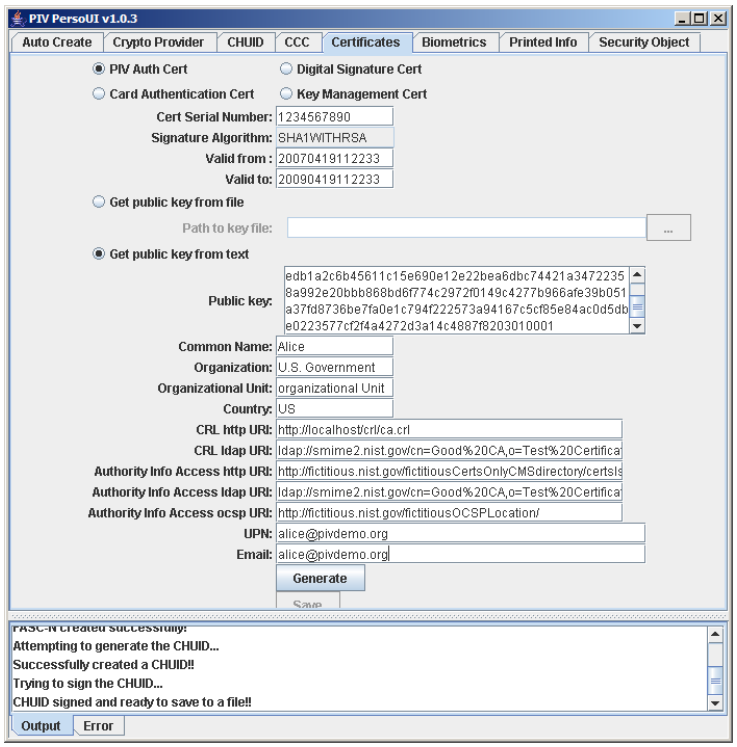

Figure C-5. PIV Data Generator Certificates Tab

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 an X.509 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 5.2 of the *PIV Windows Logon Reference Implementation: Best Practices and Troubleshooting* guide 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.

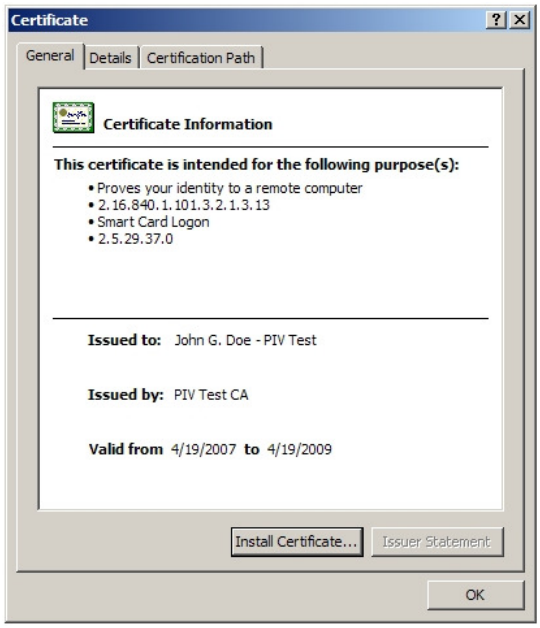

Figure C-6. X.509 Certificate – General

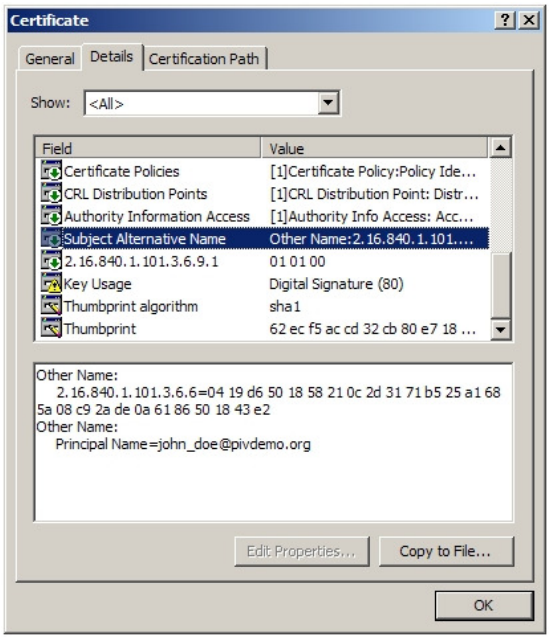

Figure C-7. X.509 Certificate – Details – Subj. Alt. Name

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.

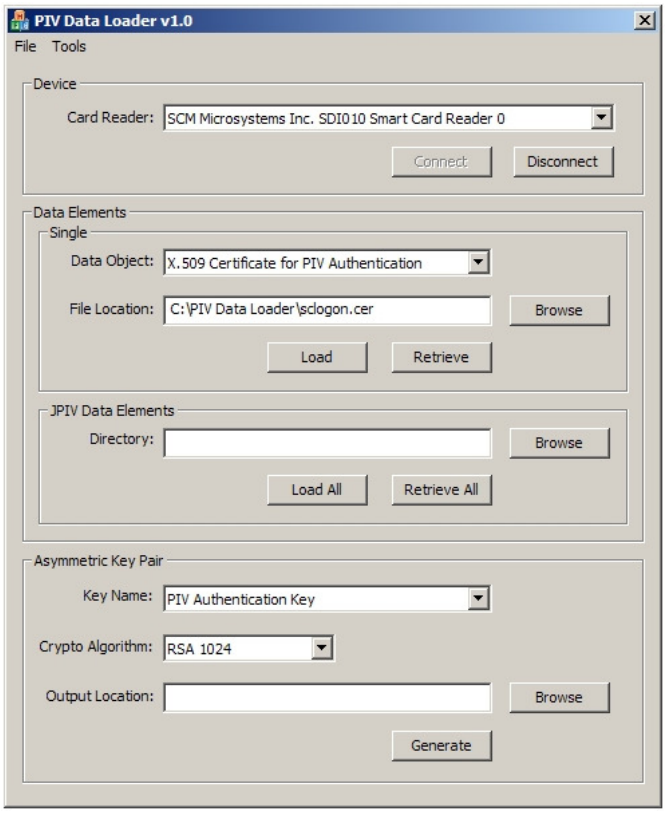

Figure C-8. Load Certificate Using PIV Data Loader

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.

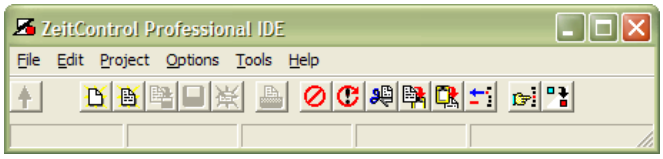

Figure C-9. ZeitControl Professional IDE

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"

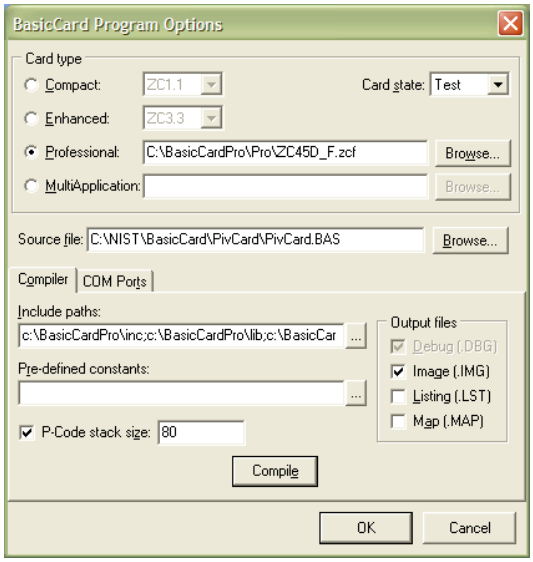

Figure C-10. BasicCard Program Options

5. Click Compile.

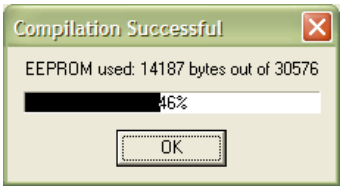

Figure C-11. BasicCard Compilation Successful

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 correct key pairs and certificates into this BasicCard project and recompile.

C.3.2.4 Extract Key Pairs

Public Key Extraction

1. To extract the public key from the key pair generated with OpenSSL, use the command specified in section C.1.2.3:
   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.

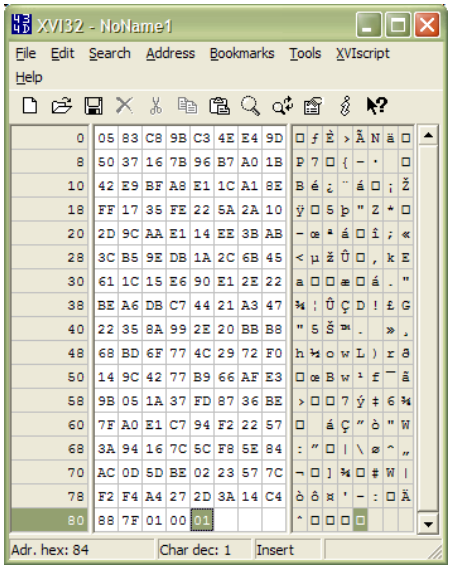

Figure C-12. XVI32: BasicCard Public Key

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.

Private Key Extraction

1. To extract the private key from the key pair generated with OpenSSL, use the command specified in section C.1.2.3:
   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.

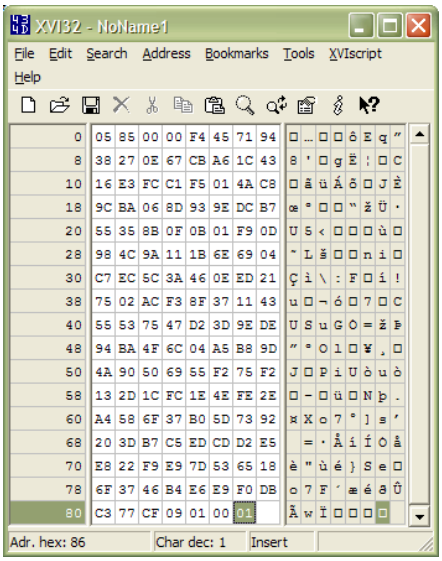

Figure C-13. XVI32: BasicCard Private Key

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 certificate properly.

2. Although the certificates generated by the PIV Data Generator tool contain pre-pended certificate tag information that is incompatible with Linux, the PIV Middleware and NIST PKCS#11 are able to handle the extra tag information so that the certificates can be used with Linux Logon, S/MIME, and SSL Authentication. 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.

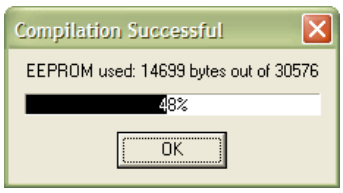

Figure C-14. BasicCard Compilation with new key pair and certificates Successful

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.

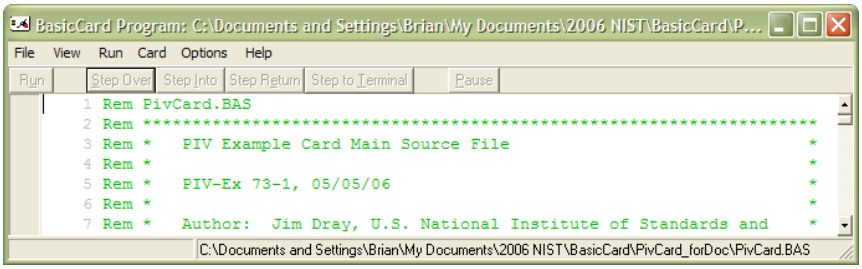

Figure C-15. BasicCard Program

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

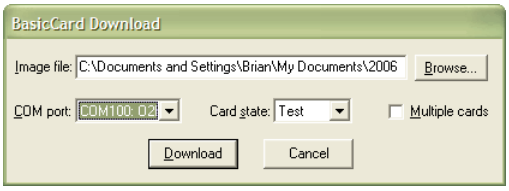

Figure C-16. BasicCard Download configuration dialog

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

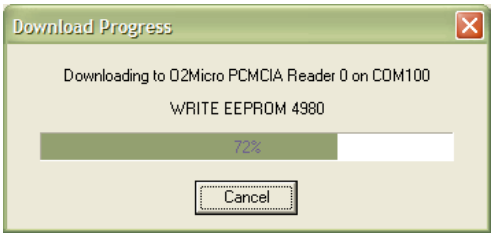

Figure C-17. BasicCard Download Progress dialog

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.

Appendix D—Acronyms

The following acronyms and abbreviations are used throughout this document:

APDU	Application Programming Data Unit
API	Application Programming Interface
CA	Certificate Authority
CHUID	Cardholder Unique Identifier
CRL	Certificate Revocation List
CSP	Cryptographic Service Provider
DER	Distinguished Encoding Rules
DES	Data Encryption Standard
DLL	Dynamic Link Library
FASC-N	Federal Agency Smart Credential Number
FIPS	Federal Information Processing Standards
HSPD	Homeland Security Presidential Directive
IDE	Integrated Development Environment
IIS	Internet Information Services
ITL	Information Technology Laboratory
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency Report
OCSP	Online Certificate Status Protocol
OS	Operating System
PAM	Pluggable Authentication Modules
PC/SC	Personal Computer/Smart Card
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
RSA	Rivest Shamir Adleman
S/MIME	Secure / Multipurpose Internet Mail Extensions
SP	Special Publication
SSL	Secure Sockets Layer
TLS	Transport Layer Security
UPN	Universal Principal Name
USB	Universal Serial Bus

Appendix E—References

[1] Electrosoft, Inc., PKCS11 Interface for Personal Identity Verification Cards: Design, Build and Installation Procedure, Prepared for: NIST, Version 1.0 (draft), January 12, 2007

[2] Electrosoft, Inc., PKCS#11 for PIV: Machine Configurations and Demonstration Scenarios, Version 1.0 (draft), January 12, 2007

[3] Electrosoft, Inc., PKCS#11 for Personal Identity Verification (PIV): Demonstration Scenarios, December 29, 2006

[4] NIST, *PIV Windows Logon Reference Implementation: Best Practices and Troubleshooting*, June 22, 2007 (included with the SP 800-73 Reference Implementation package – available at http://csrc.nist.gov/piv-program/)