Advanced Card Systems Ltd.
Card & Reader Technologies

ACOS5-CryptoMate Client Kit (For Windows®)

Administrator Package Manual V1.04

info@acs.com.hk
www.acs.com.hk

Table of Contents

List of Figures

List of Tables

1.0. Introduction

The ACOS5-Cryptomate Client Kit Administrator Package is a software package designed for administrators (e.g., Certificate Authorities, Registration Authorities) to prepare and maximize the use of ACOS5 cards and CryptoMate tokens for their end-users in Public Key Infrastructure (PKI) applications.

This document contains description of driver, middleware and application included in the package. To help you with managing your certificates and digital signatures, also included in this document are guides on how to use your smart cards and tokens in various third party applications such as:

- Internet Explorer®
- Mozilla® Firefox®
- Microsoft® Active Directory®
- Microsoft® Management Console
- Microsoft® Outlook®
- Mozilla® Thunderbird®
- Microsoft® Word®
- LibreOffice
- Adobe® Acrobat®
- Adobe® Reader®

This user manual will use the term **"token"** to refer to the ACOS5 smart card or CryptoMate token.

1.1. Administrator Guide

This client kit makes it easy for Administrators to manage and distribute tokens to their end-users. The ACOS5-CryptoMate Client Kit comes with two CDs, namely:

1. Administrator Package – This package is intended for Certificate Authorities, Registration Authorities and other administrator roles who will prepare the tokens to be used by their end-users.
2. User Package – This package is intended for end-users who will use their tokens with digital certificate to various PKI applications such as digital signing and encrypting.

Note: *You cannot install the Administrator Package and User Package on the same computer.*

2.0. Client Kit Specifications

To ensure optimal use of the client kit package, make sure your system is running with the following specifications:

2.1. Supported Smart Card/Token

- ACOS5-64 Cryptographic Smart Card V3.00
- CryptoMate Nano Cryptographic Token
- ACOS5-64 Cryptographic Smart Card V2.00
- CryptoMate64 Cryptographic Token

2.2. Supported Smart Card Reader

- ACR39U Smart Card Reader
- ACR38U Smart Card Reader

2.3. Supported Operating Systems

- Windows® 7 (32-bit and 64-bit)
- Windows® 8.1 (32-bit and 64-bit)
- Windows® 10 (32-bit and 64-bit)
- Windows® Server 2012 (64-bit)

2.4. Supported Third Party Applications

- Internet Explorer®
- Mozilla® Firefox®
- Microsoft® Active Directory®
- Microsoft® Management Console
- Microsoft® Outlook®
- Mozilla® Thunderbird®
- Microsoft® Word®
- LibreOffice
- Adobe® Acrobat®
- Adobe® Reader®

3.0. Client Kit Architecture

The ACS Client Kit was developed to work with **ACOS5 Card Operating System** and **ACOS5T Cryptographic USB Token** (also known as the CryptoMate Series) developed by ACS.

To use the ACOS5 and CryptoMate for PKI applications, ACS provides the CSP and PKCS #11 middleware, as well as the token management application in the ACOS5-CryptoMate Client Kit.

The client kit (Administrator Package) contains all the necessary middleware and tools for administrators to initialize tokens for their end-users. Furthermore, the Administrator Package also lets the administrators to perform various secured transactions such as digital signature, email encryption, online payments, Windows log-on, and other PKI applications.

The figure below shows the interaction of the various components of the client kit.

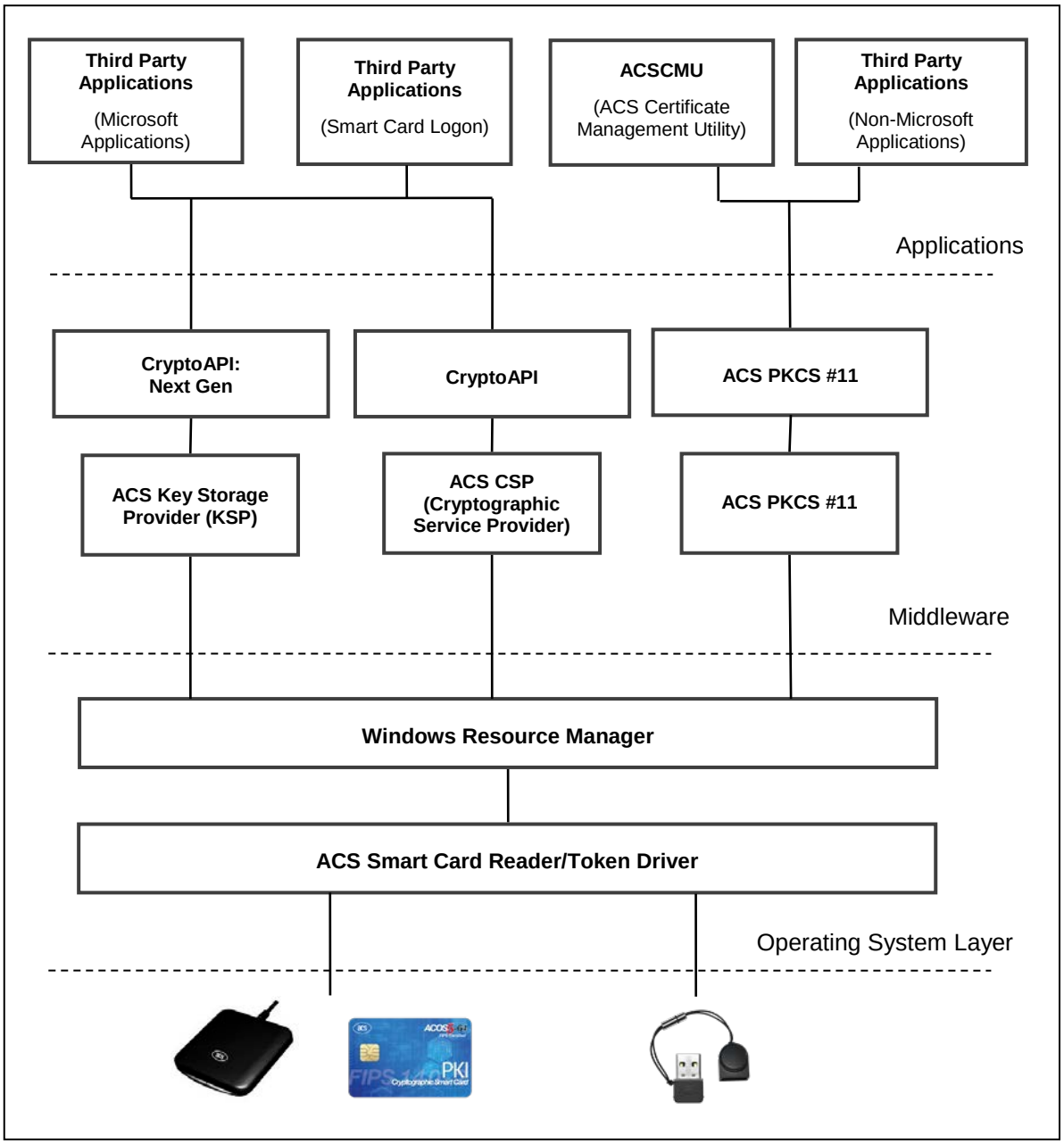


Figure 1: ACOS5-CryptoMate Client Kit Architecture

4.0. Client Kit Components

The Administrator Package installs the following components:

1. ACS Unified PC/SC Driver
2. ACS Middleware
3. ACS Certificate Management Utility

4.1. ACS Unified PC/SC Driver

The ACS Unified PC/SC Driver is a single driver installer that enables all generic ACS Smart Card Readers to run with various Windows® operating systems. It is certified by Microsoft® WHQL and allows automatic download updates when you are connected to the Internet.

4.2. ACS Middleware

Smart card technology combined with public-key security system provides an additional level of protection against hackers. All sensitive credentials and private keys are stored inside the token which helps to encrypt and protect sensitive information from security attacks.

To use the token for cryptographic applications such as PKI with your digital certificates, ACS provides the CSP and PKCS middleware components which are further discussed in the succeeding sections.

Both of these middleware components are needed to be installed in your system to allow you to use your token for various PKI applications using a Windows operating system.

4.2.1. ACS Cryptographic Service Provider (CSP)

This middleware is based from Microsoft CryptoAPI to allow your token to be instantly recognized by systems running with Windows XP.

4.2.2. ACS Key Storage Provider (KSP)

This middleware is based from Microsoft Next Generation Cryptography Middleware or CNG which was introduced for Windows Vista and later.

4.2.3. ACS PKCS #11

For cross-platform applications such as Mozilla® Firefox® and Mozilla® Thunderbird®, you need to explicitly load the PKCS in the application itself. In this case, ACS provides the PKCS #11 middleware to help you in using the token in cross-platform applications. This ensures that your application can recognize your token and perform cryptographic operation through the ACS PKCS middleware.

IMPORTANT: *To use the middleware and the application, make sure that the Microsoft Visual C++ 2008 SP1 Redistributable Package is installed in your system. You can download it from: http://www.microsoft.com/en-us/download/details.aspx?id=5582*

4.3. ACS Certificate Management Utility

The **ACS Certificate Management Utility (ACSCMU)** is an application that helps you manage the certificates and cryptographic data objects stored in your token. As an Administrator, you can use the ACSCMU to initialize and re-initialize the token in preparing it for PKI usage.

You can access this application in the Start menu:

- Advanced Card Systems Ltd
  - o ACOS5-CryptoMate Admin Client Kit
    - ACS Certificate Management Utility

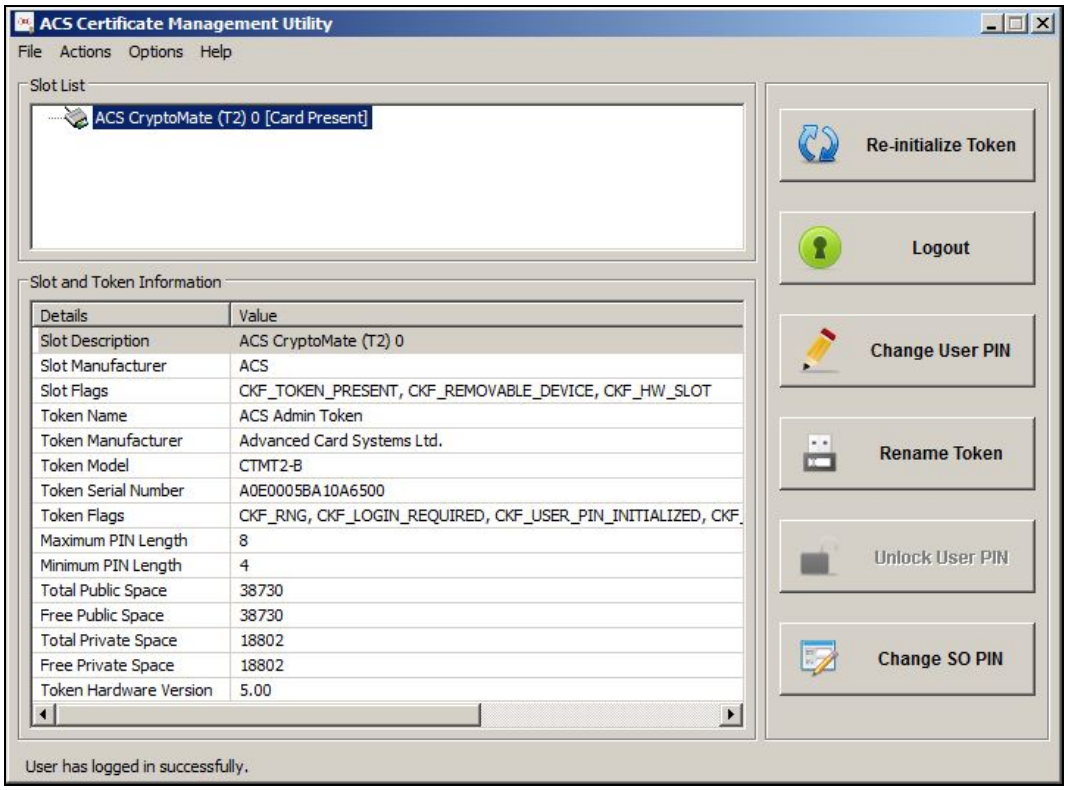


Figure 2: ACS Certificate Management Utility – User Interface

It is highly recommended that you read first the **ACSCMU Help File** provided with the tool in order to know the functionalities of this token management application.

Note: *For Windows 7 users, make sure to install the Microsoft* ***.NET Framework v4.5.1*** *to your computer to run the ACS Certificate Management Utility. Click* ***here*** *to download the installer.*

4.3.1. Administrator and User Access

The Administrator can use the ACS Certificate Management Utility (ACSCMU) to initialize and re-initialize the token in preparing it for PKI usage. For end-users, they can use the ACS Certificate Management Essentials (ACSCME) as their token management application, which is a trimmed down version of the ACSCMU.

The table below shows a comparison of functions between the token management application for Administrator and end-users.

Function	ACS Certificate Management Utility (ACSCMU)	ACS Certificate Management Essentials (ACSCME)
Initialize/Re-initialize Token	✓	×
Log in/Log out	✓	✓
Change User PIN	✓	✓
Rename Token	✓	✓
Unlock User PIN	✓	✓
Change SO PIN (or PUK)	✓	×
View Certificate	✓	✓
Import Certificate	✓	✓
Export Certificate	✓	✓
Delete Certificate	✓	×
View Data Object	✓	✓
Delete Data Object	✓	✓
Create Secret Key	✓	✓
Edit Secret Key	✓	✓
Delete Secret Key	✓	✓
Set up Token Initialization Setting	✓	×
Set up Application Setting	✓	✓
Set up Middleware Log Setting	✓	✓
View Help File	✓	✓

Table 1: Administrator and End-user Functions

5.0. Compatibility across Client Kit versions

This section discusses the compatibility across the ACOS5-CryptoMate Client Kit package releases and versions for Windows, Mac and Linux operating systems.

All components of the client kit, including ACSCMU/ACSCME tools, and CSP and KSP middleware for Windows, use the PKCS middleware that is responsible for the compatibility across client kit versions.

If a token has been initialized or used with any of the New Client Kit Packages (refer to **Table 2**), and then the user performs any of the following actions using the Old Client Kit Packages (refer to **Table 2**):

- Request, create, import or delete certificates
- Create or delete data objects
- Create or delete secret keys

These updates cannot be viewed once the token is used with the New Client Kit Packages again.

Below is a distinction of the packages:

Old Client Kit Packages	New Client Kit Packages
Client Kit for Windows v4.0.4.1 and below acospkcs11.dll v4.0.4.5 and below	**Client Kit for Windows v4.0.4.2 and later** acospkcs11.dll v4.0.4.6 and later
	Client Kit for Linux v4.0 and later libacospkcs11.so v4.0.0 and later
	Client Kit for Mac OS v4.0 and later libacos5pkcs11.dylib v4.0.0 and later

Table 2: Client Kit Package Distinctions

To ensure compatibility between package releases, use the hotfix application included in this Client Kit Package located in the same directory of ACSCMU/ACSCME.

To run the application:

1. Go to the path:

   X:\Program Files\Advanced Card Systems Ltd\ACOS5-CryptoMate Admin Client Kit\Tools

   Note: *X is the letter of your local drive.*
2. Run the *HotFix.exe* file.

Another way is to ensure that all of your end-users have installed the latest User Package first before you provide them with newly-initialized tokens using Client Kit Admin Package v4.0.4.3 and later.

6.0. Managing certificates using third party applications

This section will show you a step-by-step guide on how to manage your digital certificate with various PKI applications in different platforms.

6.1. Using certificates in Internet Explorer®

Since Internet Explorer is a Microsoft Windows application, you no longer have to manually load the middleware in the application. The ACS Cryptographic Service Provider middleware is automatically loaded in your system once you install the client kit package.

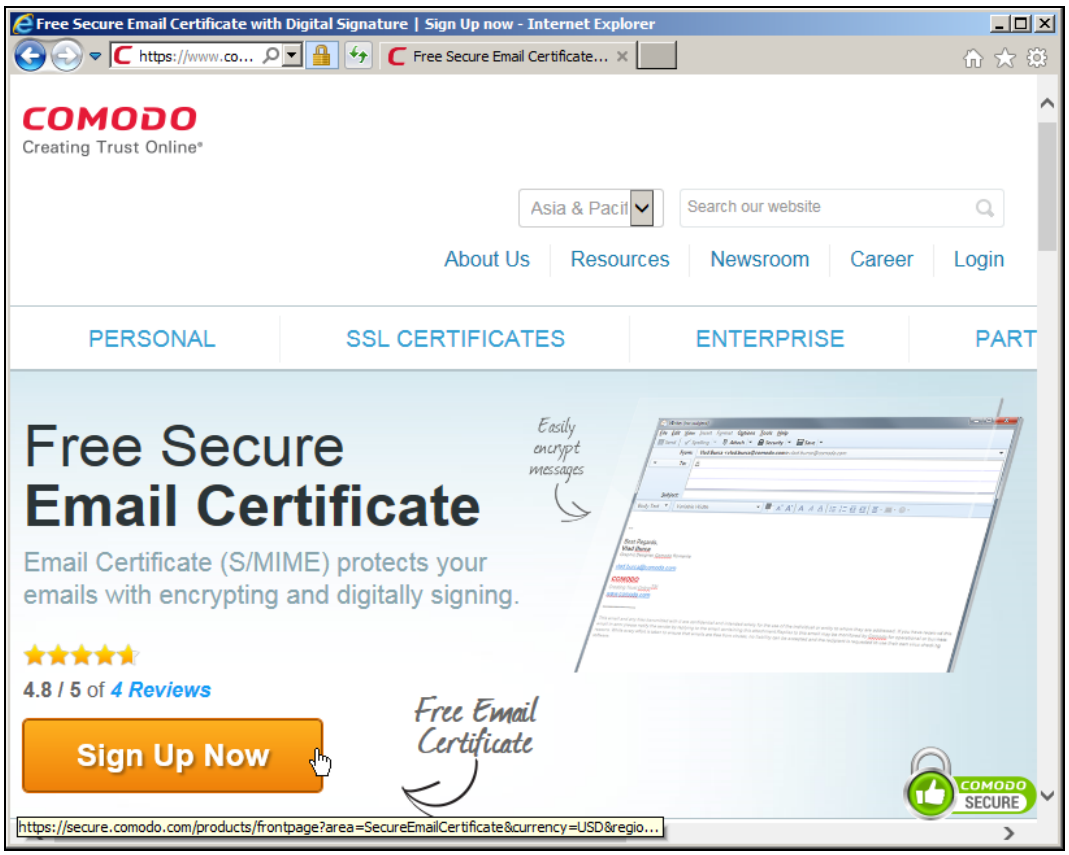
6.1.1. Requesting a certificate using Internet Explorer

Before requesting a certificate, make sure that your token has been initialized. Please refer to the Help File of ACSCMU to know how.

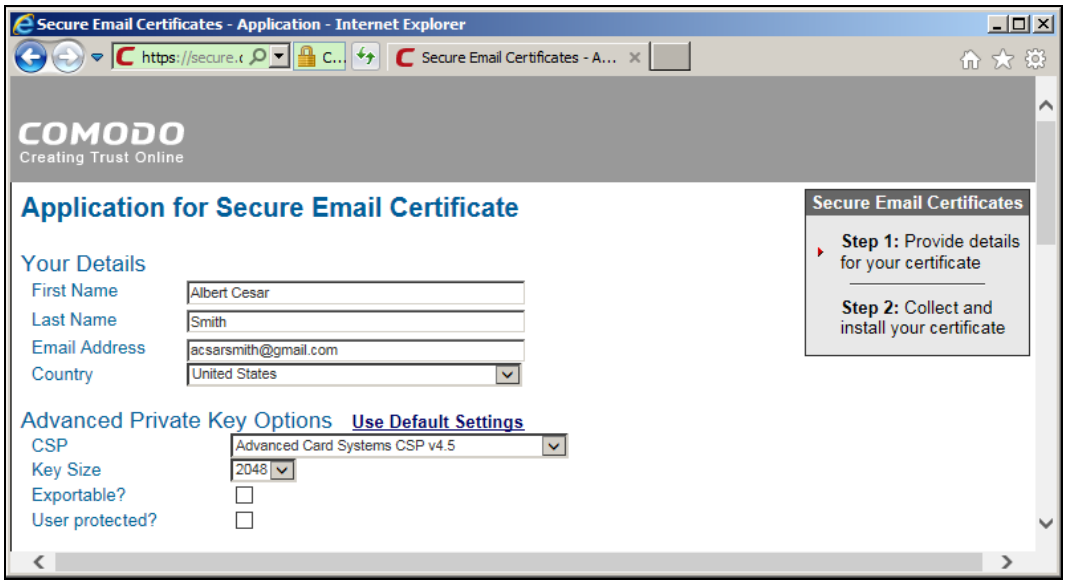
To request a certificate using Internet Explorer:

Note: *This procedure will use Comodo as the Certificate Authority.*

1. Connect your token to your computer.
2. Go to http://www.Comodo.com/home/internet-security/free-email-certificate.php and sign up for a free e-mail certificate.



3. In the **Application for Secure E-mail Certificate** page, fill up your details including **Name**, **E-mail** and **Country**.

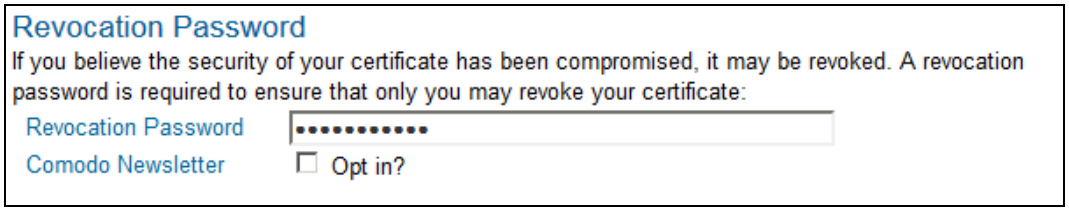


4. Under **Advanced Private Key Options**, select **Advanced Card Systems CSP vX.x** in the CSP drop-down list.

   Note: *If the Advanced Card Systems CSP is not in the list, make sure the ACOS5-CryptoMate Client Kit is properly installed.*

5. Clear the **Exportable?** check box. This adds security and prevents the private key from being exported.

6. Type in a revocation password. This allows you to revoke your digital certificate in case of loss or accidental deletion.



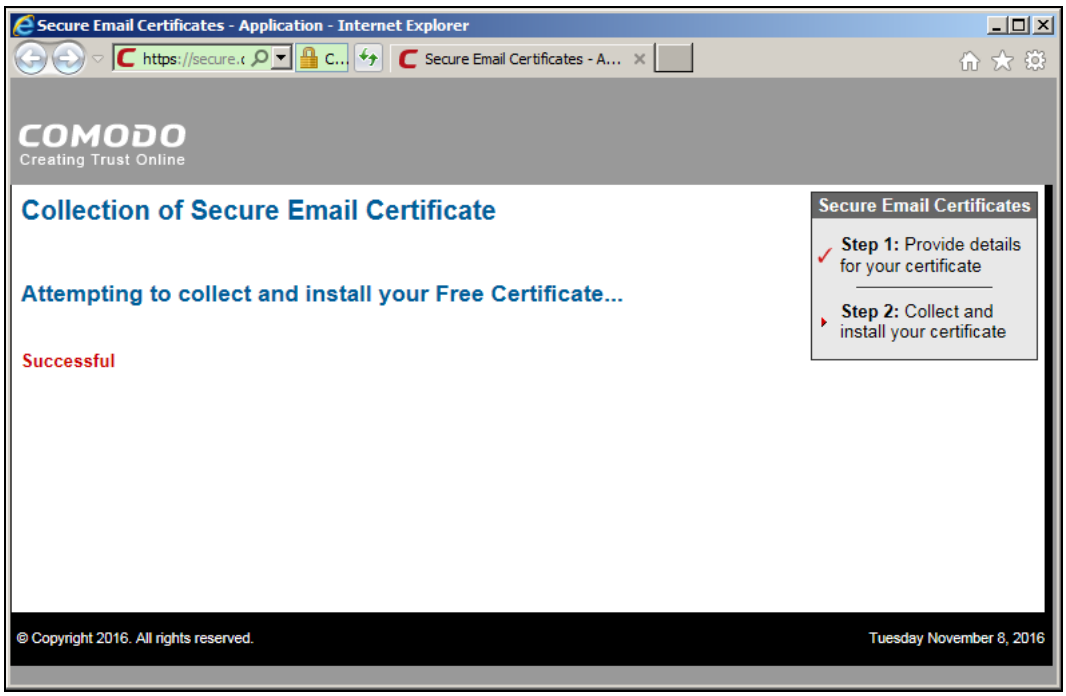
7. Accept the terms of the subscriber agreement, and then click **Next**.

8. Type in your token PIN when prompted.

9. Once the application is successful, the details on how to collect your free Secure E-mail Certificate will be sent to your e-mail.

10. In the confirmation e-mail, press the **Click & Install Comodo E-mail Certificate** button.

11. You will be directed to **Collection of Secure E-mail Certificate** page. Comodo will attempt to collect and install your Free Certificate.
12. Type in your token PIN when prompted.
13. A "**Successful**" message will appear once the certificate has been collected and installed.

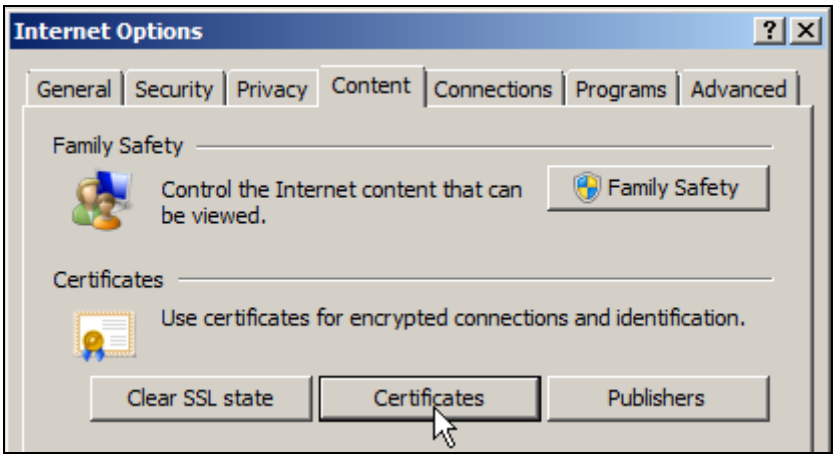


6.1.2. Viewing certificates in Internet Explorer

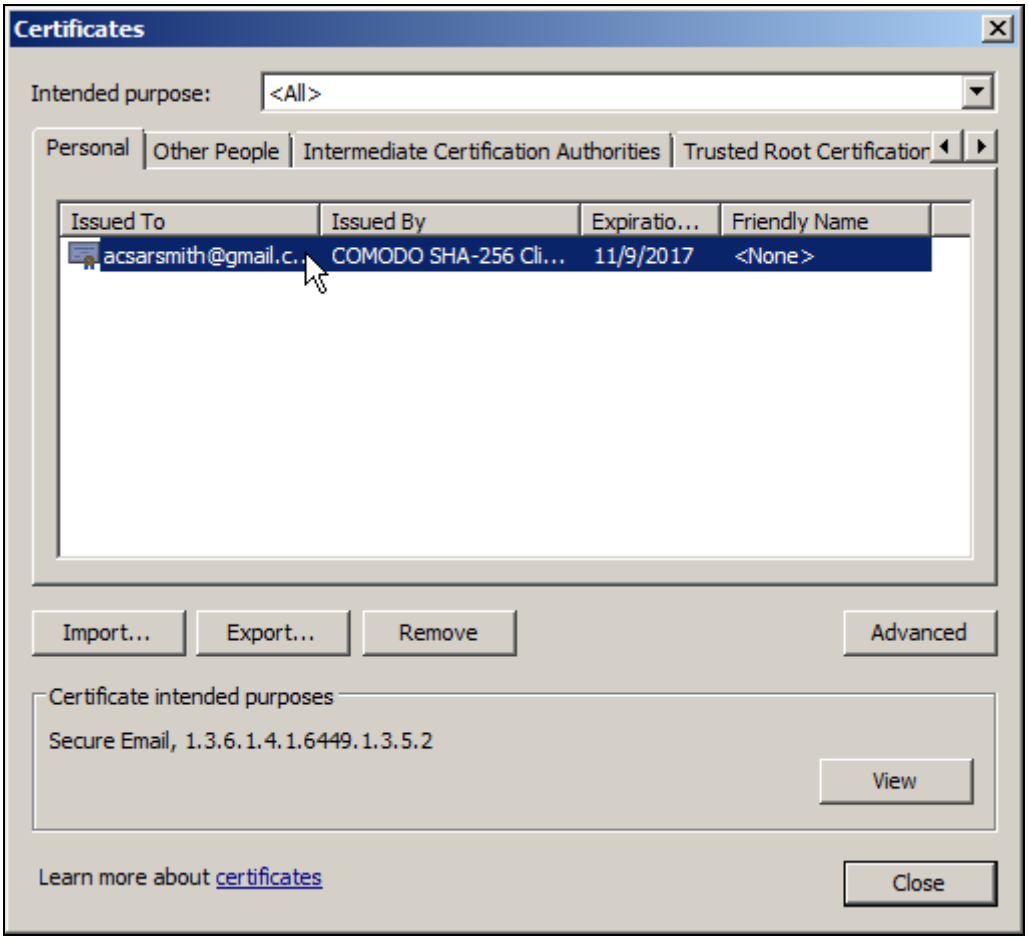
To view certificates using Internet Explorer:

Note: *Make sure that the ACS Certificate Management Utility (ACSCMU) is running in your system.*

1. In the **Tools** menu, click **Internet options**.
2. Under the **Content** tab, click **Certificates**.



3. The **Personal** tab will display the certificate(s) currently present in your system.

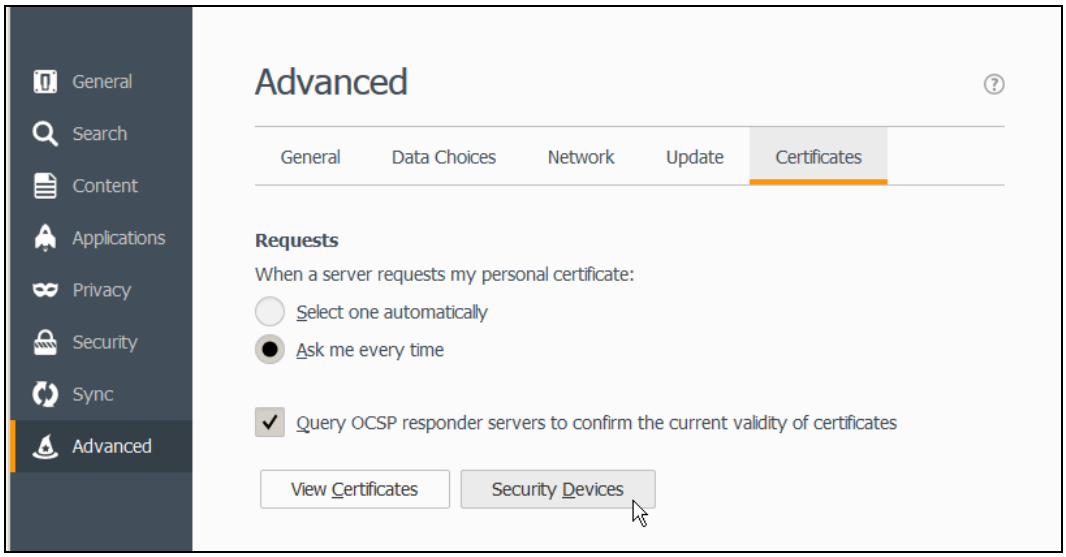


6.2. Using certificates in Mozilla® Firefox®

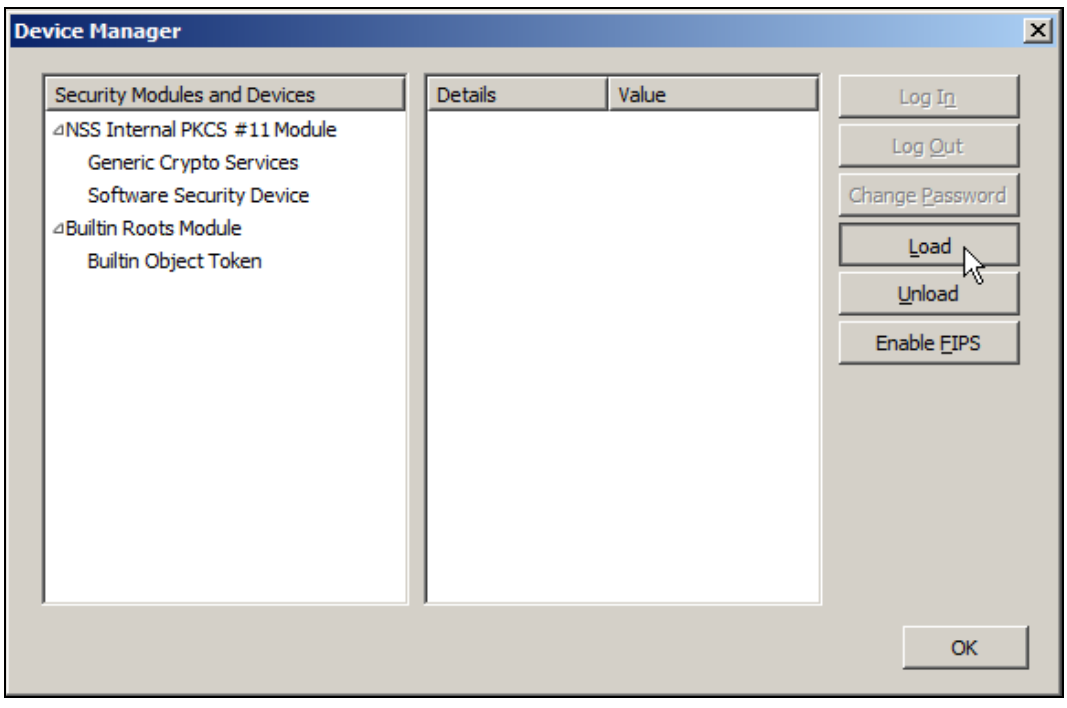
6.2.1. Loading PKCS #11 in Mozilla Firefox

To manually load the PKCS #11 in Mozilla Firefox:

1. In the **Tools** menu, click **Options**, and then click **Advanced**.
2. Under the **Certificates** tab, click **Security Devices**.

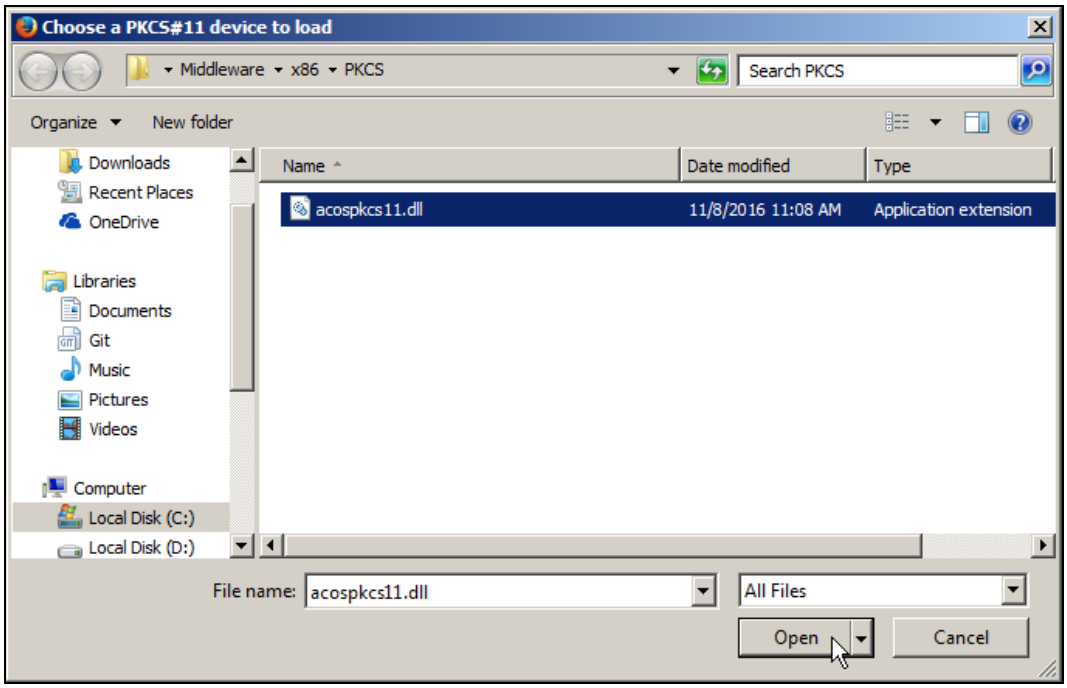


3. The Device Manager will be displayed. Click **Load**.



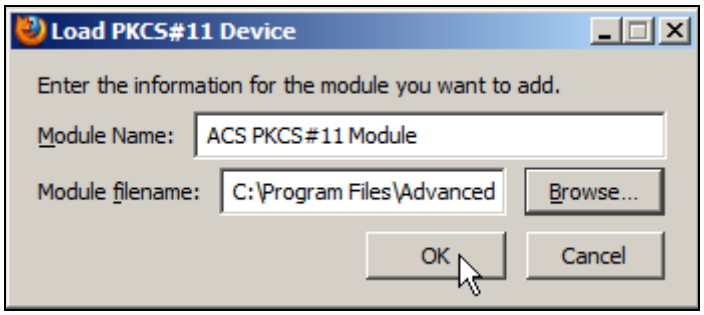
4. Type in "**ACS PKCS #11 Module**" as Module Name.

5. Locate the *acospkcs11.dll* file in the path: ***C:\Program Files\Advanced Card Systems Ltd\ACOS5-CryptoMate Admin Client Kit\Middleware\x86\PKCS***, and then click **Open**.



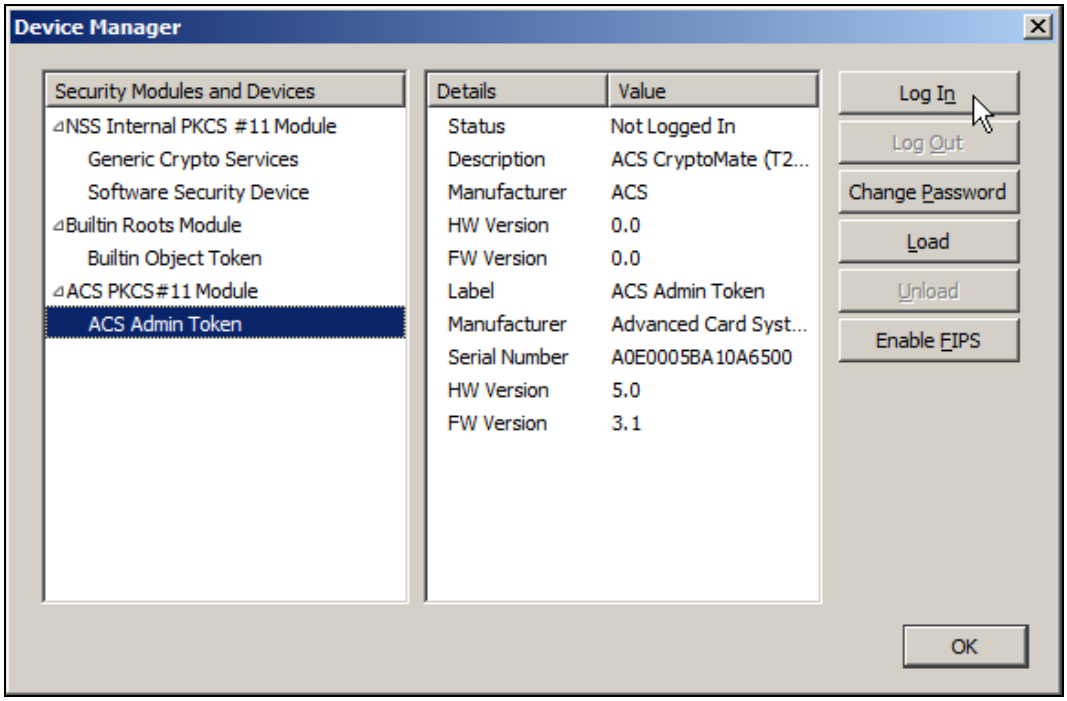
Note: *If you installed the package in another folder or path, make sure to enter the correct file path. For 64-bit platform users, please make sure to load the 64-bit .dll file in the 64-bit application and the 32-bit .dll file in the 32-bit application respectively.*

6. Once the file is located, click **OK**.



7. The Device Manager will display the **ACS PKCS #11 Module** and your token.

8. Select your token, and then click **Log in**.



9. Type in your token PIN when prompted.
10. Once logged in, your token is now ready to use with Mozilla Firefox.

6.2.2. Requesting a certificate in Mozilla Firefox

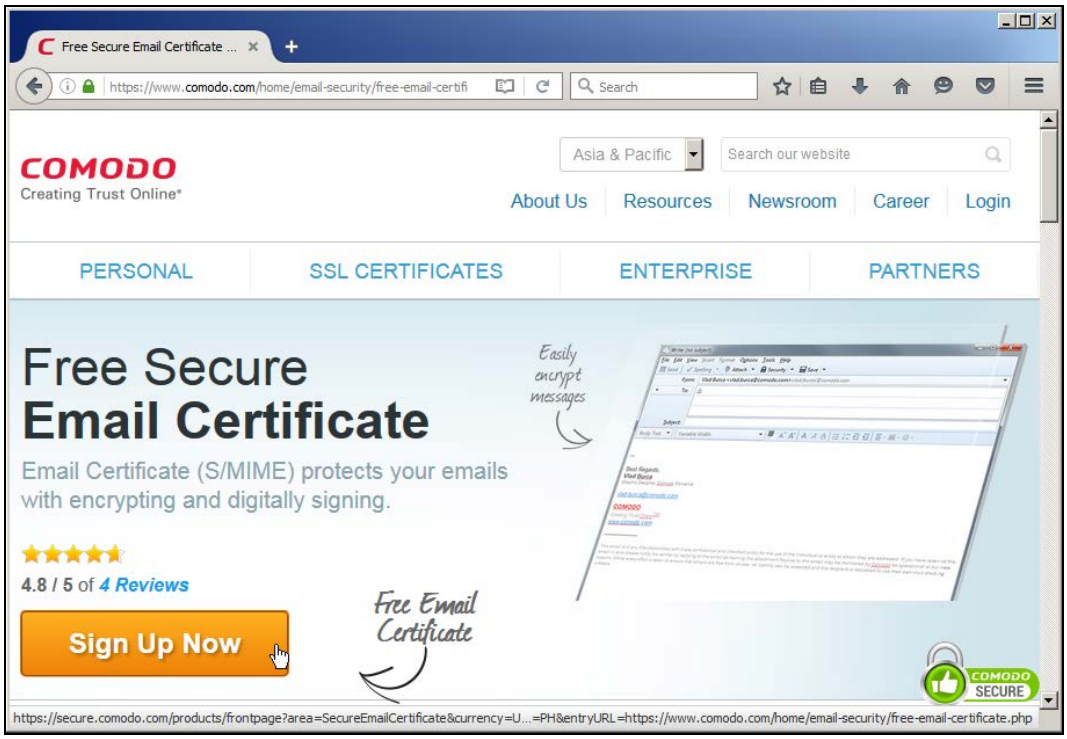
Before requesting a certificate using Mozilla Firefox, make sure that you have installed the ACS PKCS #11 Middleware for Mozilla Firefox. See **Loading PKCS #11 in Mozilla Firefox** for more details.

Make sure that your token has been initialized. Please refer to the Help file of ACSCMU to know how.

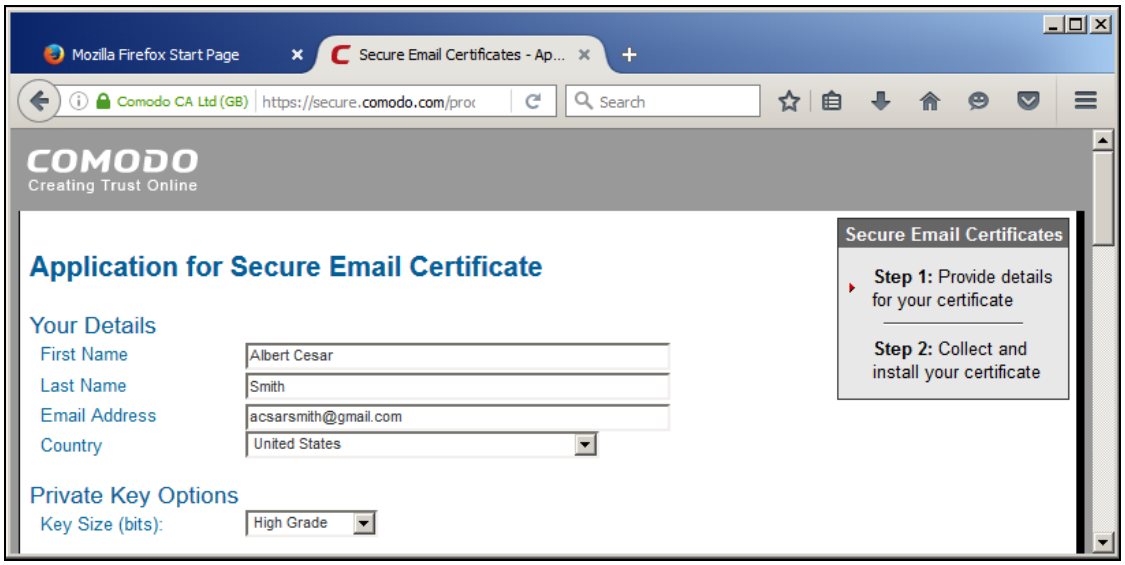
To request a certificate using Mozilla Firefox:

Note: *This procedure will use Comodo as the Certificate Authority.*

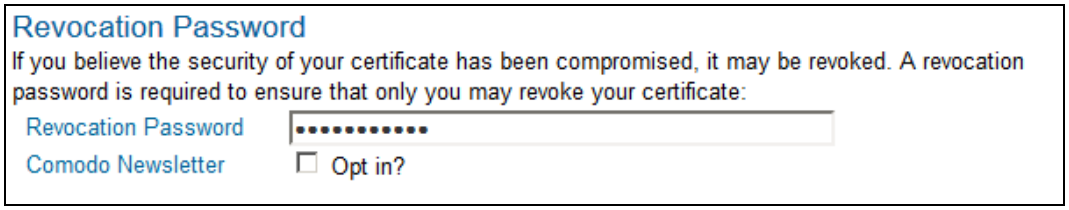
1. Connect your token to your computer.
2. Go to http://www.Comodo.com/home/internet-security/free-email-certificate.php and sign up for a free e-mail certificate.



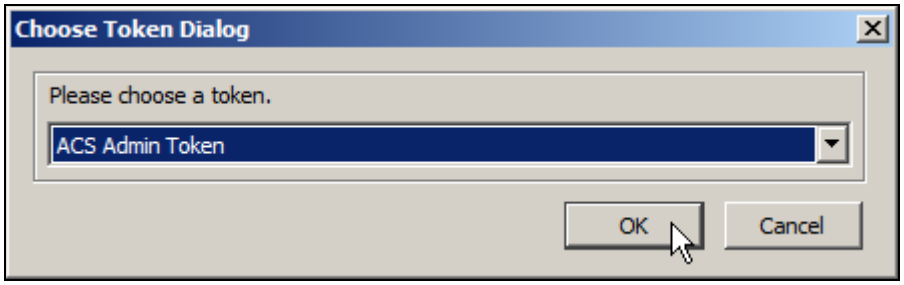
3. In the **Application for Secure Email Certificate** page, fill up your details including **Name**, **Email** and **Country**.



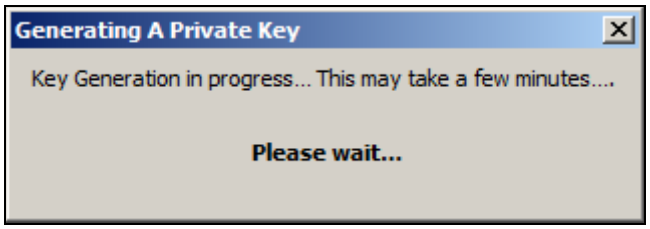
4. Under **Private Key Options**, select **High Grade** as key size.
5. Type in a revocation password. This allows you to revoke your digital certificate in case of loss or accidental deletion.



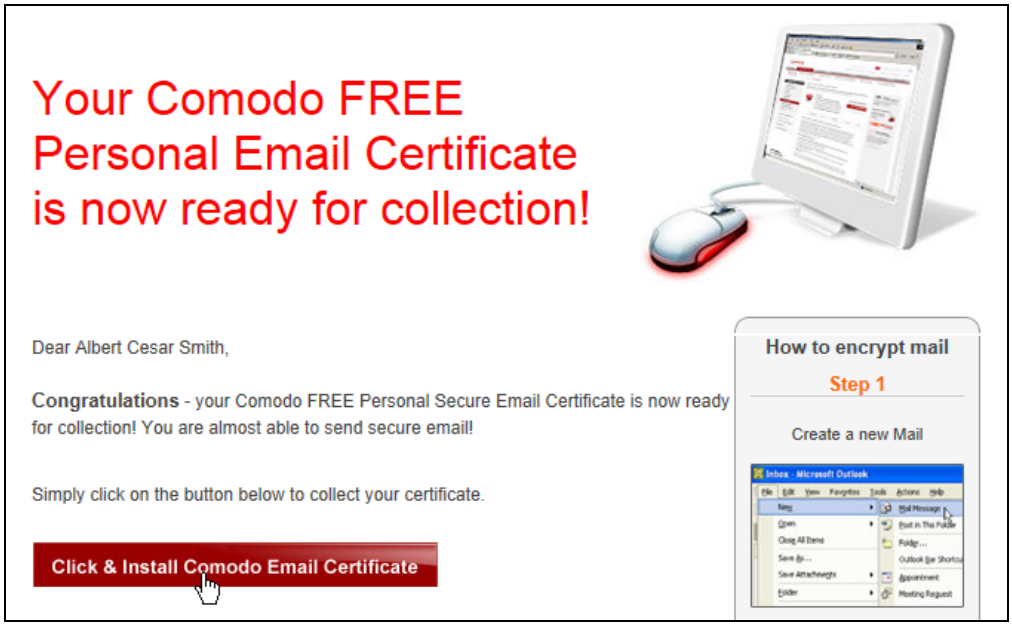
6. Accept the terms of the subscriber agreement, and then click **Next**.
7. Choose your token, and then click **OK**.



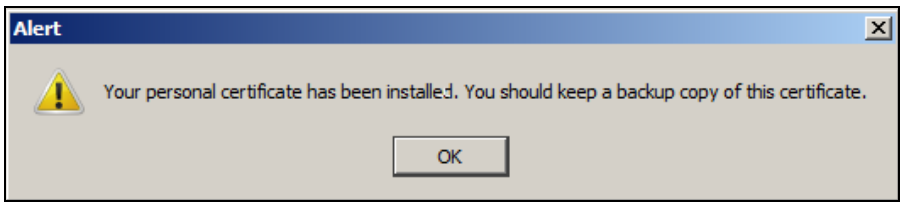
8. Wait until key generation is finished.



9. Once the application is successful, the details on how to collect your free Secure E-mail Certificate will be sent to your e-mail.
10. In the confirmation e-mail, press the **Click & Install Comodo E-mail Certificate** button.



11. You will be directed to **Collection of Secure E-mail Certificate** page. Comodo will attempt to collect and install your Free Certificate.
12. An alert will confirm that your personal certificate has been installed.

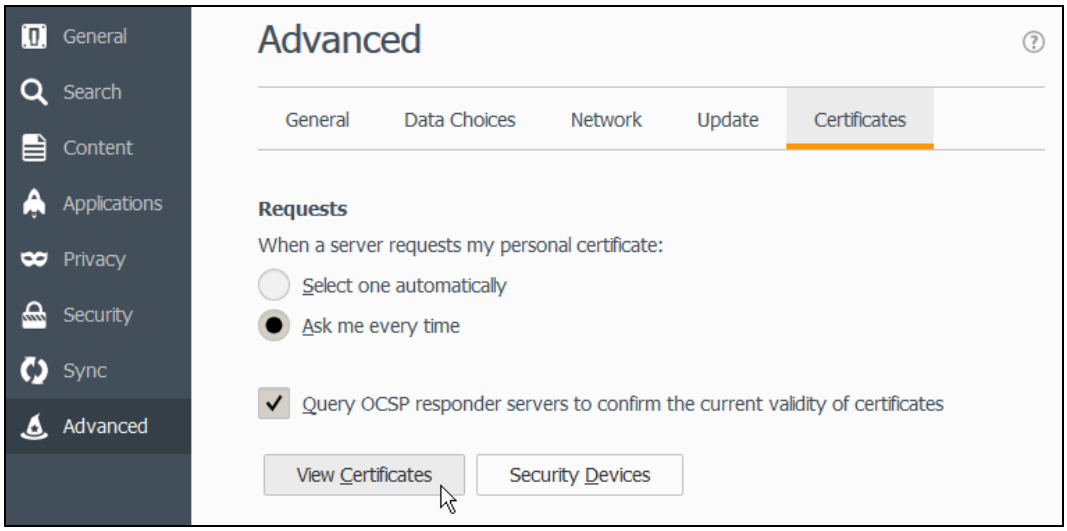


6.2.3. Viewing certificates in Mozilla Firefox

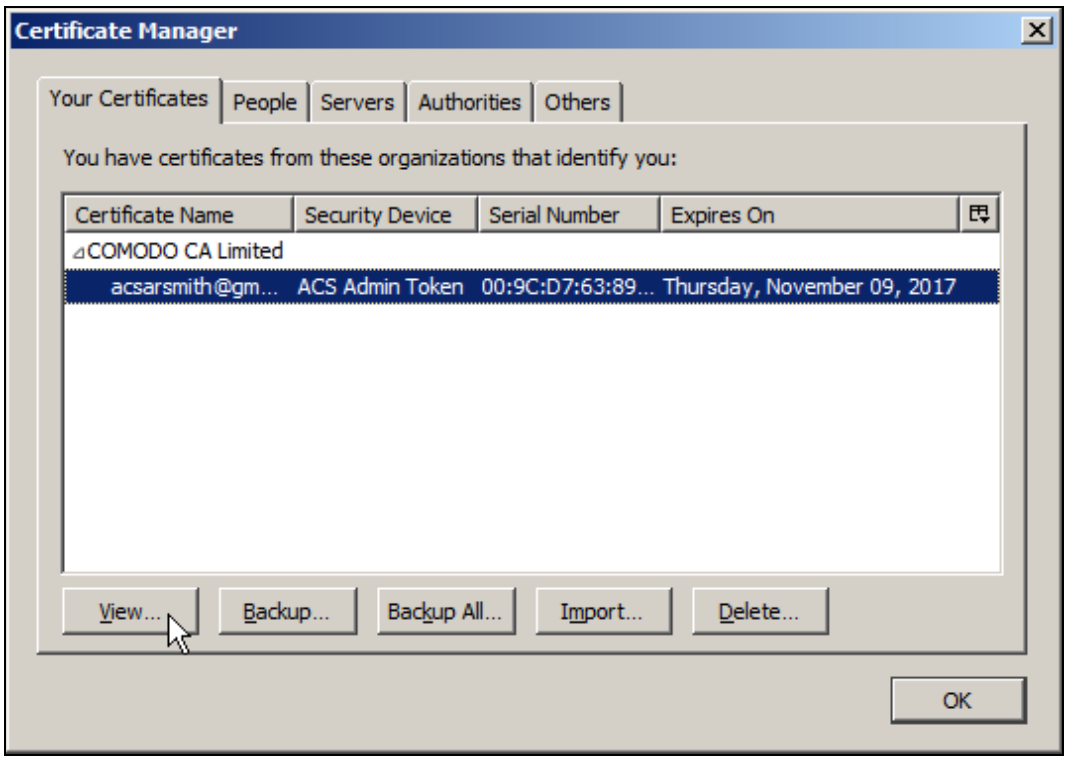
To view certificates using Mozilla Firefox:

Note: *Make sure your token is logged in to the Device Manager. See* ***Loading PKCS #11 in Mozilla Firefox*** *to know how.*

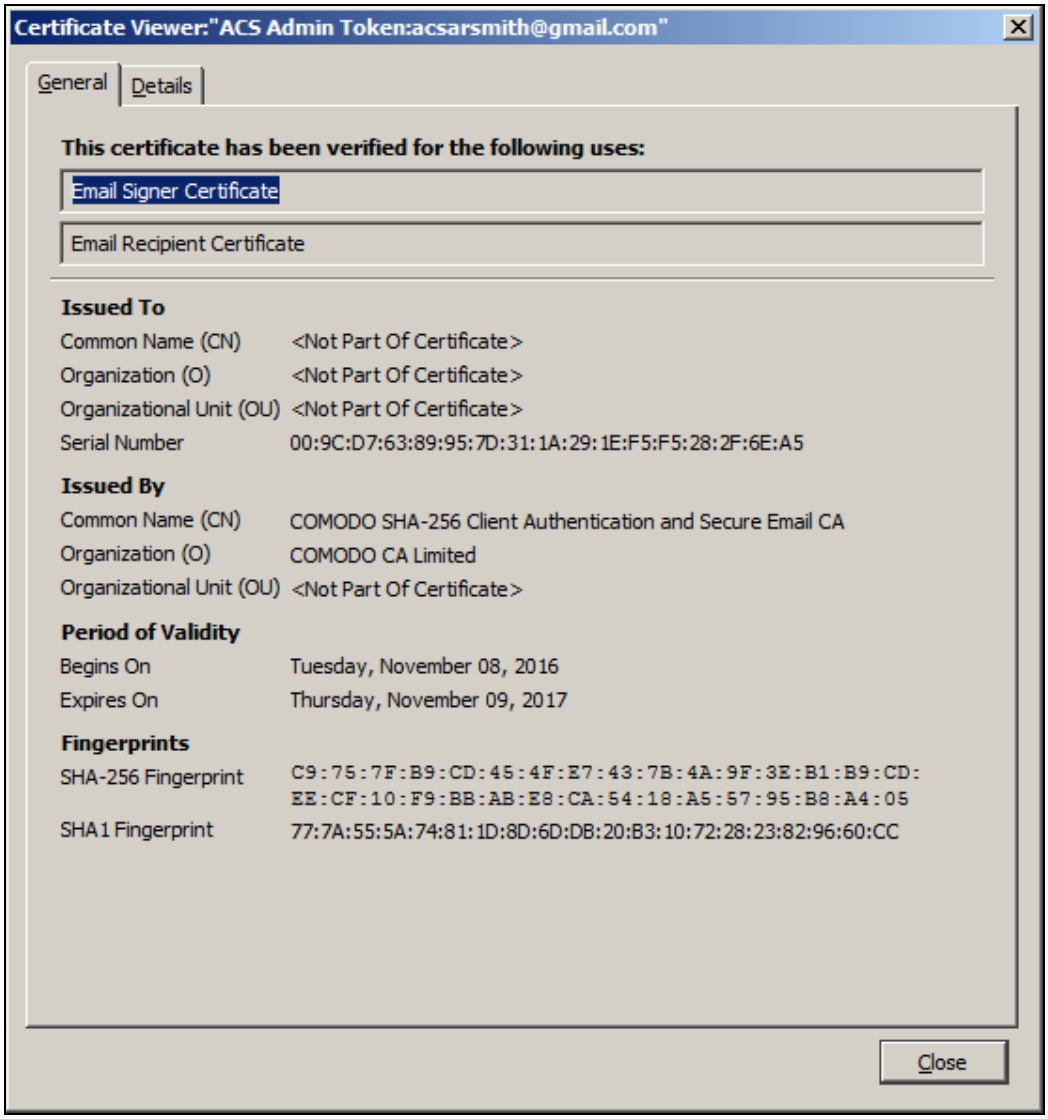
1. In the **Tools** menu, click **Options**.
2. Click **Advanced**. Under the **Certificates** tab, click **View Certificates**.



3. Under **Your Certificates** tab, select your certificate, and then click **View**.



4. The general properties and details of your certificate will be displayed.



6.3. Using certificates in Microsoft Management Console (MMC)

The **Microsoft Management Console (MMC)** provides system administrators and advanced users with a flexible interface through which they may access digital certificates currently present in the system. Certificates stored in a token can be automatically or manually installed in the Windows Certificate Store when a token is connected to the system. This certificate propagation service can be accessed through the **Application Settings** of **ACS Certificate Management Utility (ACSCMU)**. To know more details about this feature, see **Help File** of the ACSCMU application.

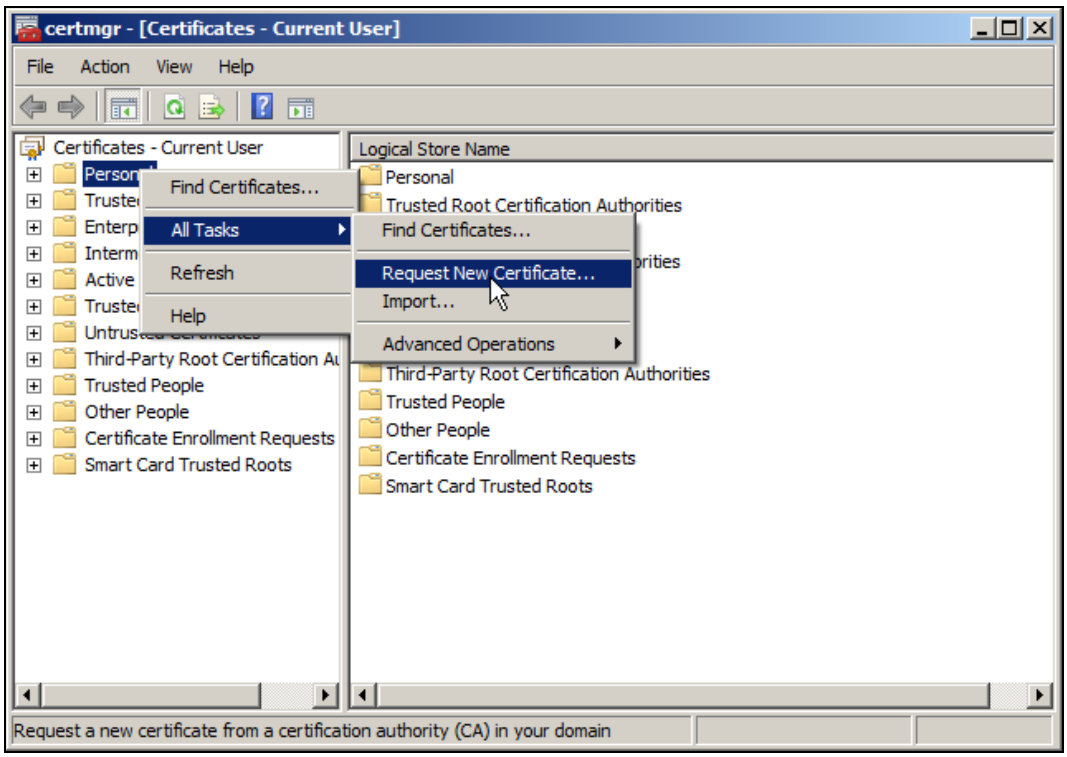
6.3.1. Requesting a certificate in Microsoft Management Console (MMC)

Requesting a certificate in MMC can only be done if you are connected to a domain server that is configured to issue digital certificates (see **Connecting to a domain**). The following procedure will show you the steps in requesting a certificate from a domain server through MMC.

To request a certificate in Microsoft Management Console (MMC):

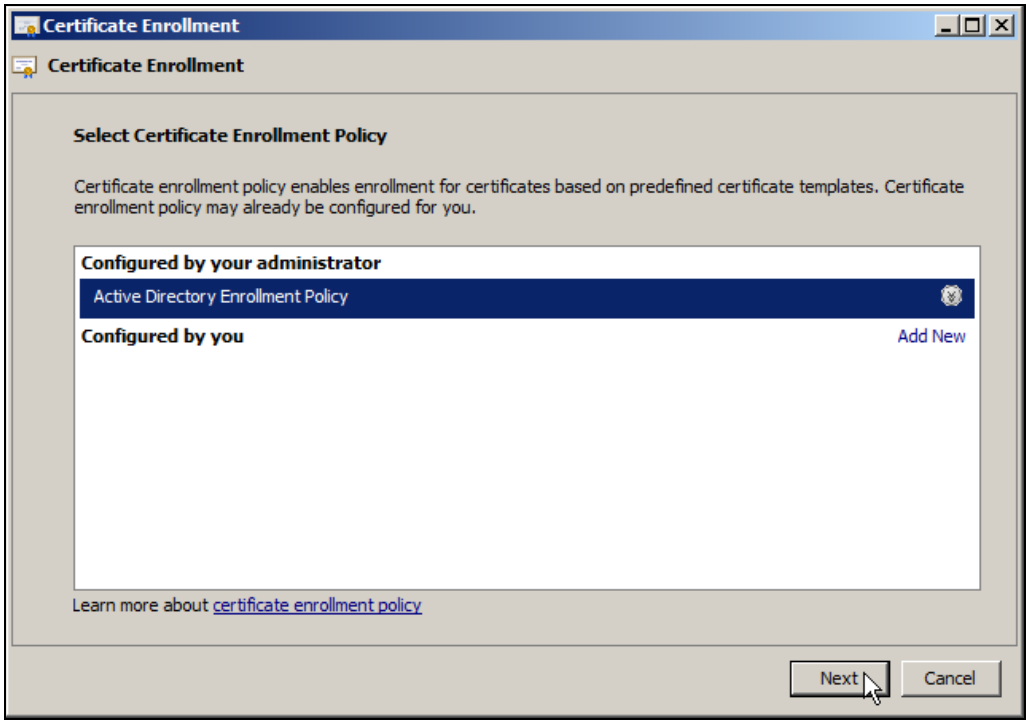
1. Type in "**certmgr.msc**" on the search text box from the **Start** menu, and then press **Enter**.

2. The MMC Console will show the certificates of the current user. Right-click on the **Personal** folder, point to **All Tasks**, and then click **Request New Certificate**.

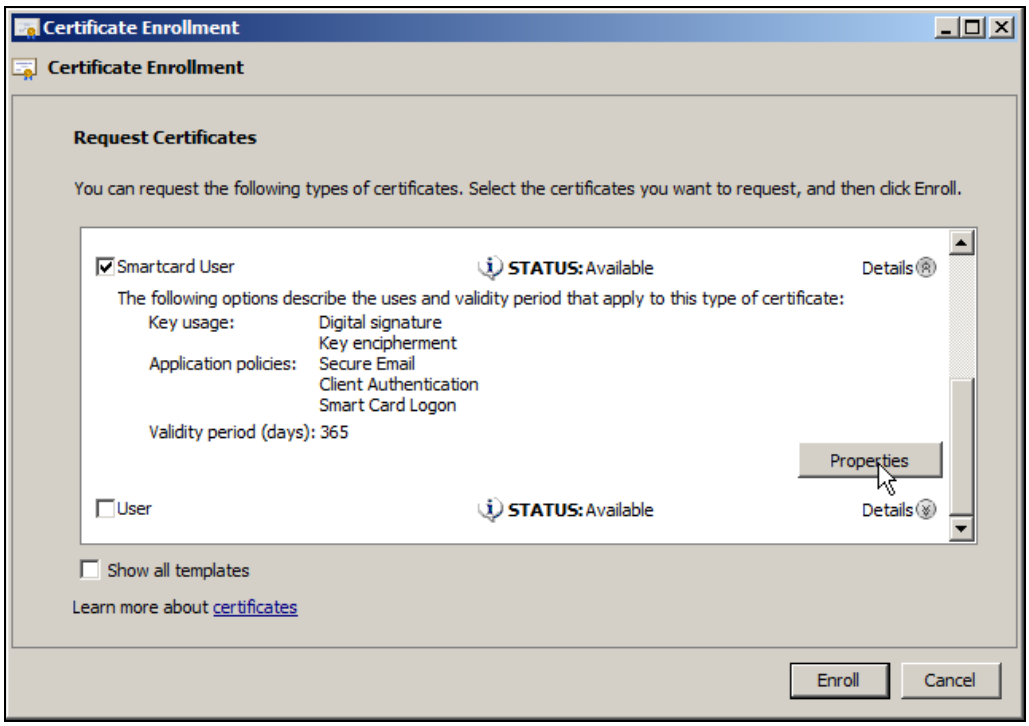


3. **Certificate Enrollment** will begin. Click **Next**.

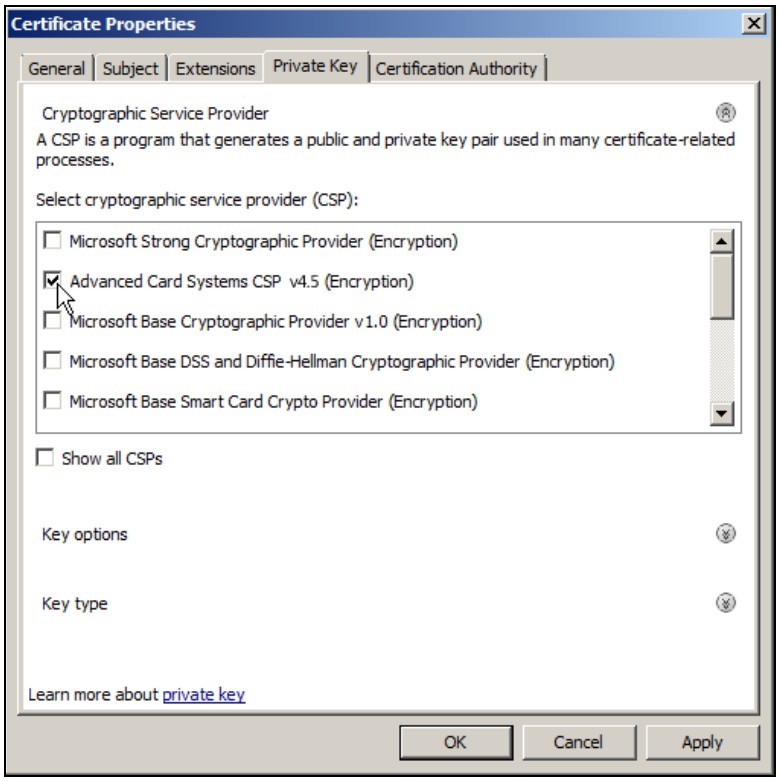
4. Select certificate enrollment policy, and then click **Next.**



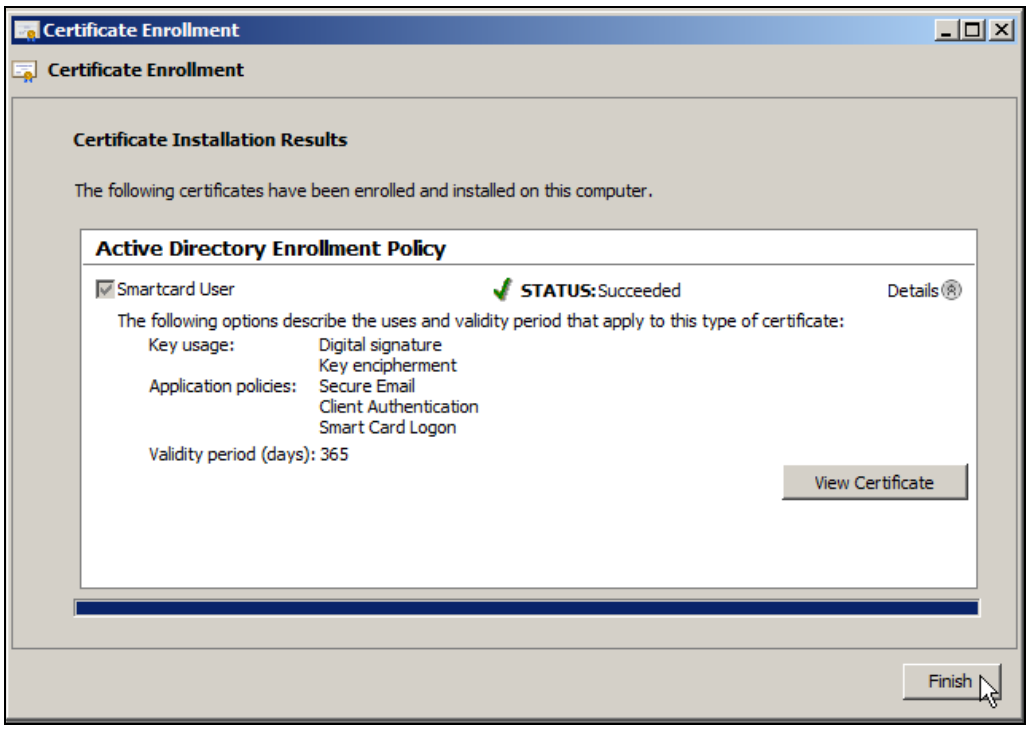
5. Scroll down and check the **Smart card User** box.
6. Click the **Details** arrow to show the description of the ce**rtificate** type, and then click **Properties**.



7. Under the **Private Key** tab, select **Advanced Card Systems CSP vX.x** in the list of Cryptographic Service Provider and make sure that this is the only CSP selected. Click **OK**.



8. Type in your token PIN when prompted.
9. Wait until the certificate request is finished.
10. Once completed, a confirmation will show that the certificate has been enrolled and installed. Click **Finish**.

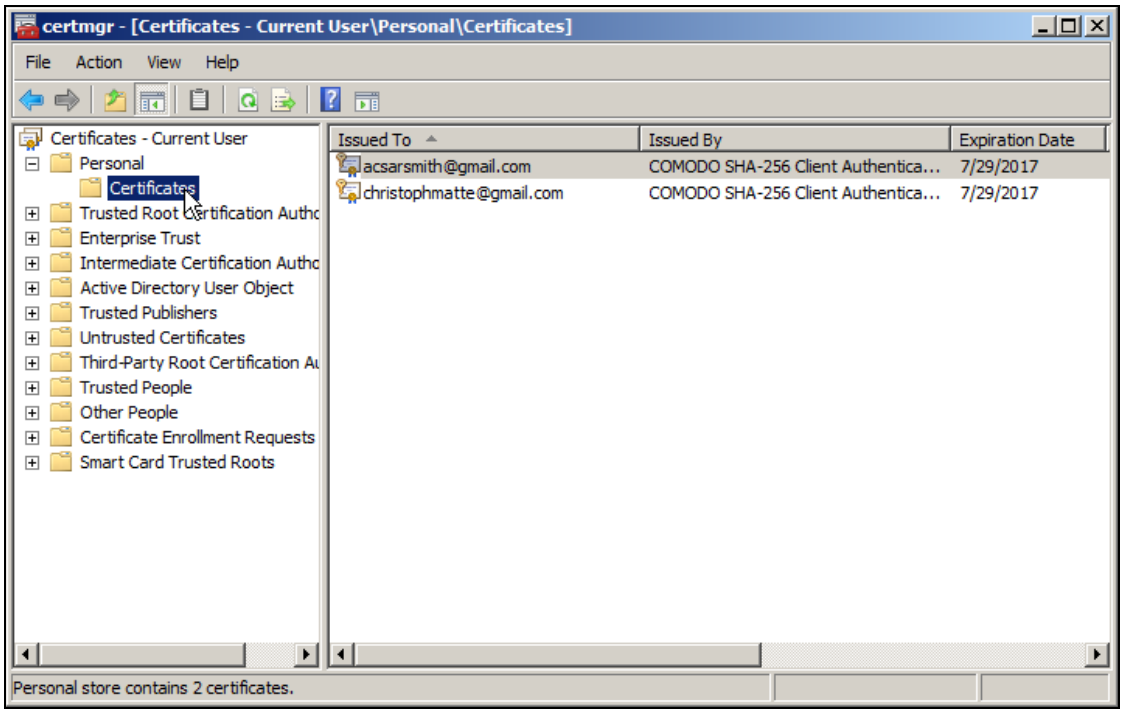


6.3.2. Viewing certificates in Microsoft Management Console (MMC)

To view certificates using MMC:

1. Click on the **Start** menu.
2. Type in "**certmgr.msc**" on the search text box and then press **Enter**.

3. The Microsoft Management Console (MMC) displays the different folders where the certificates are stored. Under the **Personal** folder, click **Certificates**.
4. The MMC displays the certificate(s) currently present in your system.



6.4. Using certificates in Microsoft® Outlook®

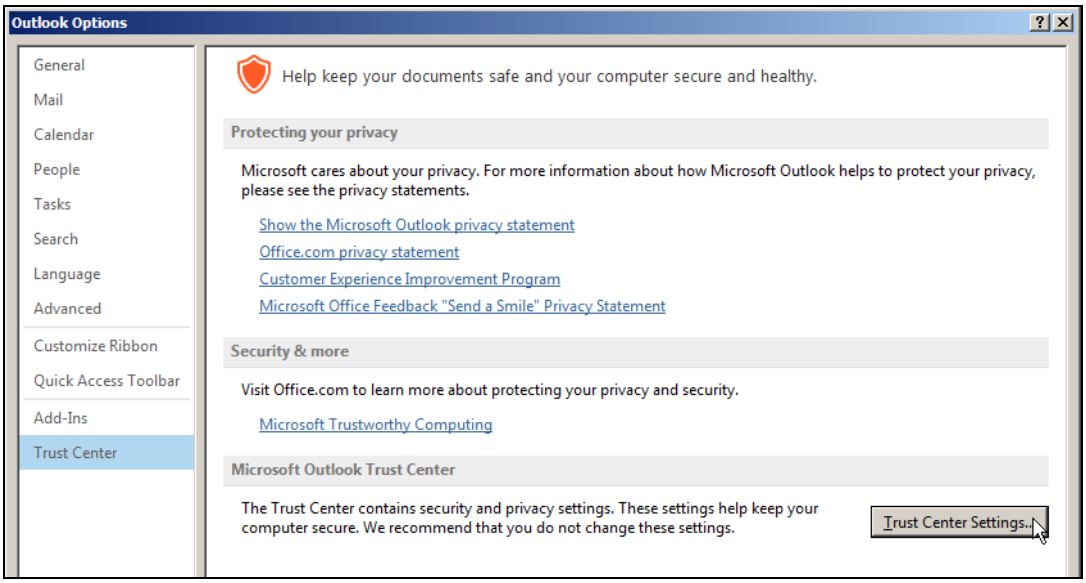
Before signing/encrypting an email, Microsoft Outlook should know which digital certificate should be used for each operation. The following procedure will help you configure your digital certificate when signing and encrypting emails.

Notes:

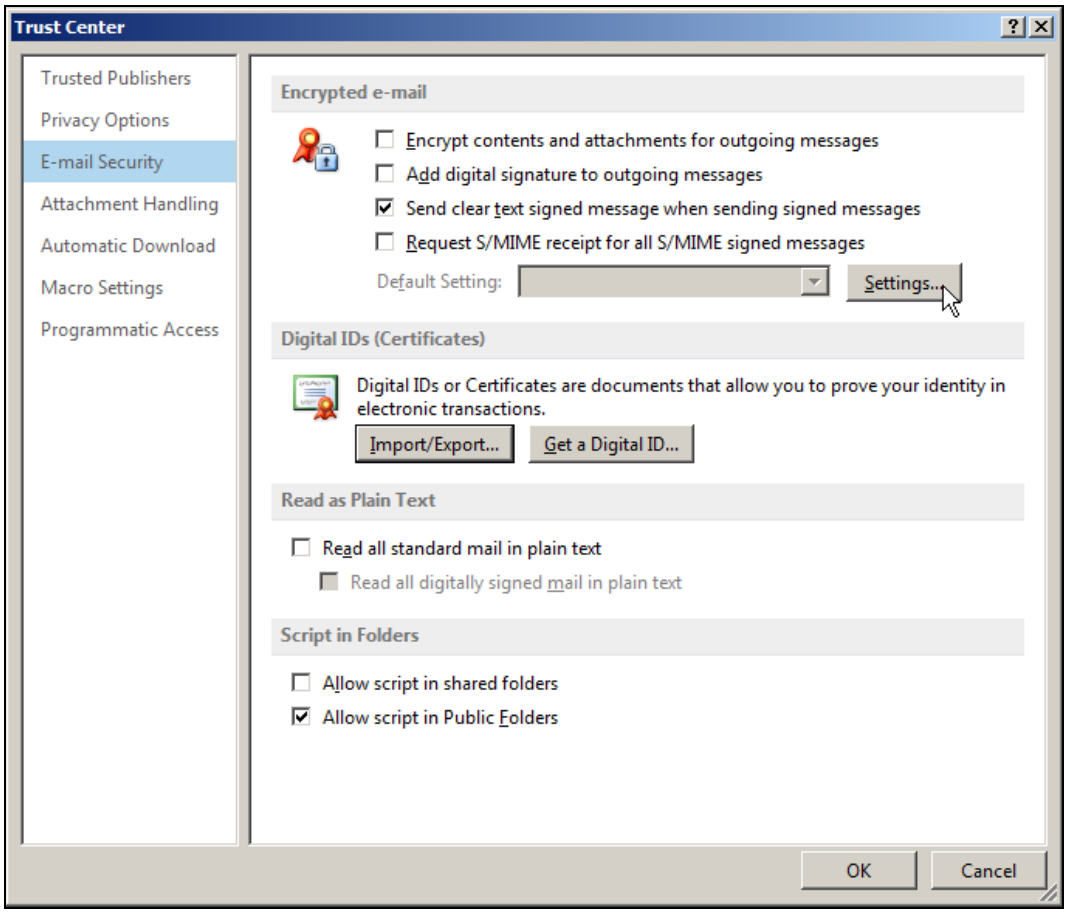
1. *The email account to be used in Microsoft Outlook SHOULD be the same email address that was used in requesting a digital certificate.*
2. *Make sure that a token with a valid certificate is connected in your system.*
3. *The certificate in the token should be installed in Windows Certificate Store. To check, see* ***Viewing certificates in Microsoft Management Console (MMC)****.*

To set up a digital certificate in Microsoft Outlook 2013:

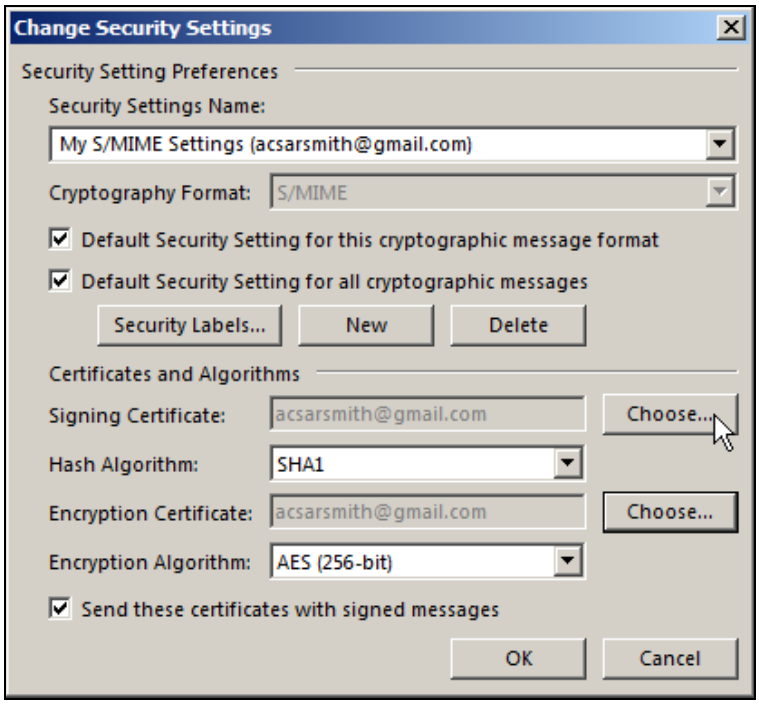
1. Go to **File | Options | Trust Center** and click **Trust Center Settings**.



2. Click **Email Security** button in the left side panel, and then click **Settings** under **Encrypted email** area.



3. The **Change Security Settings** dialog box will appear. Under **Certificates and Algorithms**, click **Choose** to specify the signing and encrypting certificates.



4. Select the certificate to be used, and then click **OK**.

   Note: *If your certificate is not in the list, close the dialog and then re-insert the token to the reader/USB slot. Wait until the reader/token stopped blinking. Repeat the previous step and see if the certificate in your token is now available in the certificate list.*

5. After specifying **Signing Certificate** and **Encryption Certificate**, click **OK**.

6. You are now ready to send/receive signed and/or encrypted emails using your ACS token in Microsoft Outlook.

6.4.1. Signing an e-mail using Microsoft Outlook

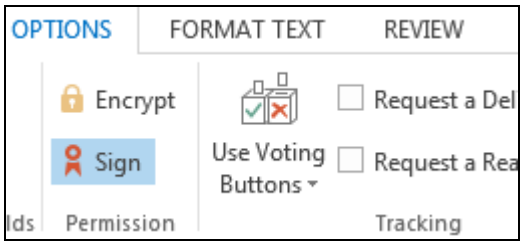
Signing emails is synonymous to putting your own signature (like a thumbprint or seal) in a letter. This ensures your recipient that the message really came from you, and that you have put your own mark on the email for the recipient to verify. This also ensures that the message has not been tampered in between the sender and the recipient.

Notes:

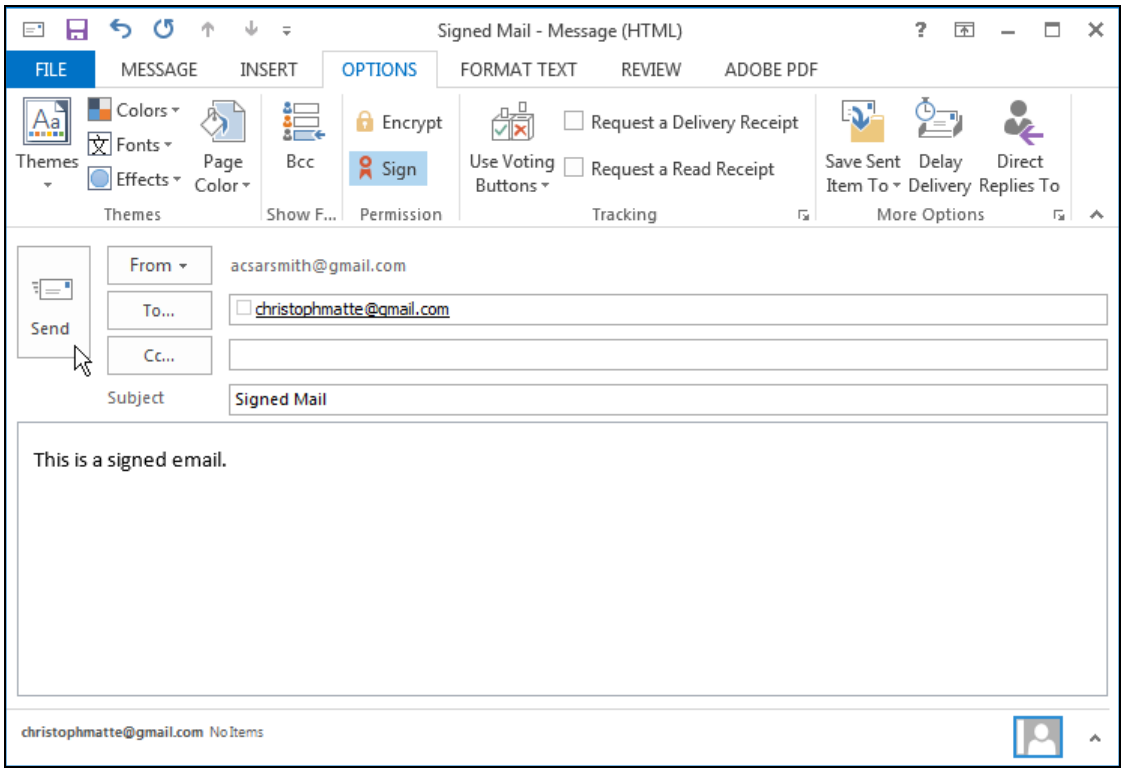
1. *Make sure that a token with a valid certificate is connected in your system.*
2. *The certificate in the token should be installed in Windows Certificate Store. To check, see* ***Viewing certificates in Microsoft Management Console (MMC)****.*

To sign an email in Microsoft Outlook 2013:

1. Create a new mail message as usual.
2. Before sending, click the **Sign** button in the **Options** tab.

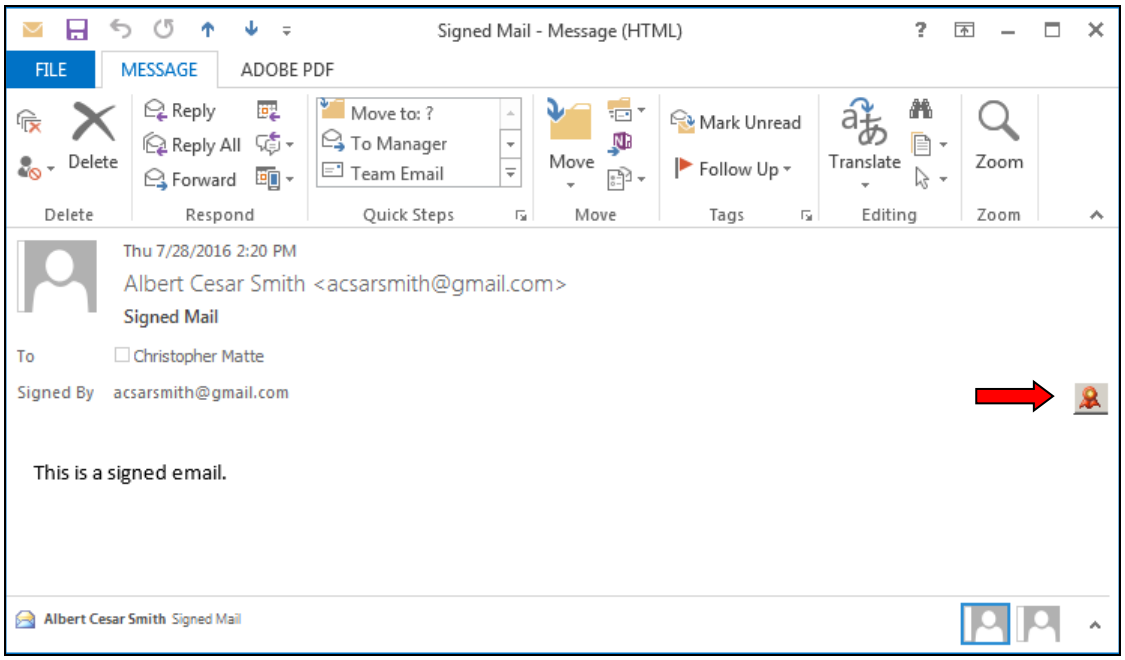


3. Click **Send**.

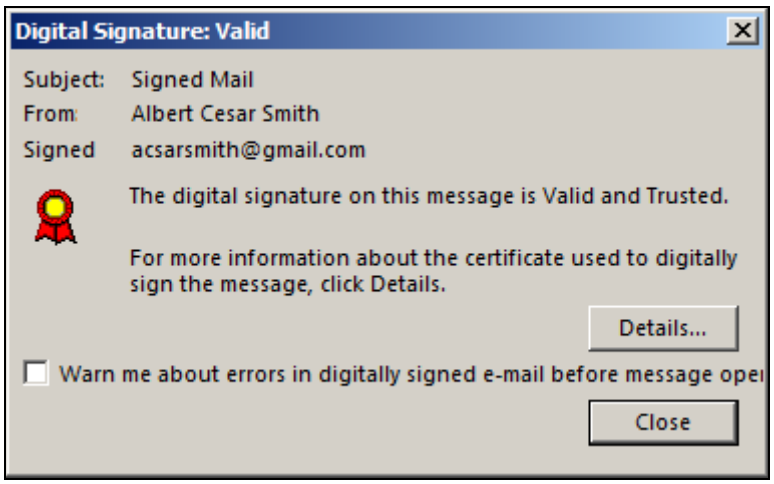


4. Type in your token PIN when prompted.

5. A small red ribbon icon is attached to the message indicating that the email was signed, and the digital signature is trusted.



6. Click the red ribbon icon to view the details of the digital signature.



6.4.2. Encrypting an e-mail using Microsoft Outlook

Encrypting an email adds another security feature that prevents a third party entity to see the actual content of the email. It also protects sending of mail messages through an unsecured medium (e.g., a compromised wireless network).

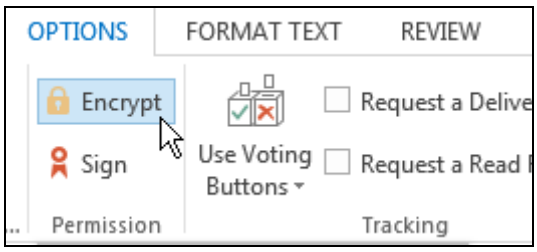
On the other hand, if you received a signed email, you can also reply to that email and have it encrypted.

Notes:

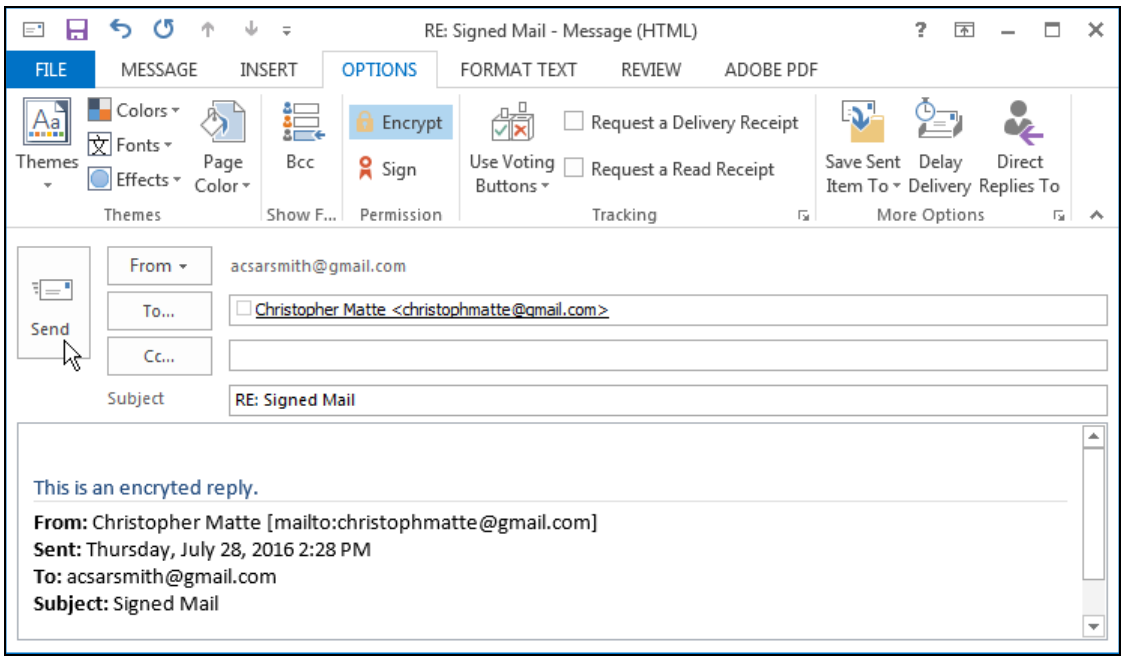
1. *Make sure that a token with a valid certificate is connected in your system.*
2. *The certificate in the token should be installed in Windows Certificate Store. To check, see* ***Viewing certificates in Microsoft Management Console (MMC)****.*

To encrypt an email using Microsoft Outlook 2013:

1. When you receive a signed email and you want to reply with an encrypted email, click **Reply** button under the **Message** tab.
2. Compose your reply message as usual, and then click **Encrypt** in the **Options** ribbon.

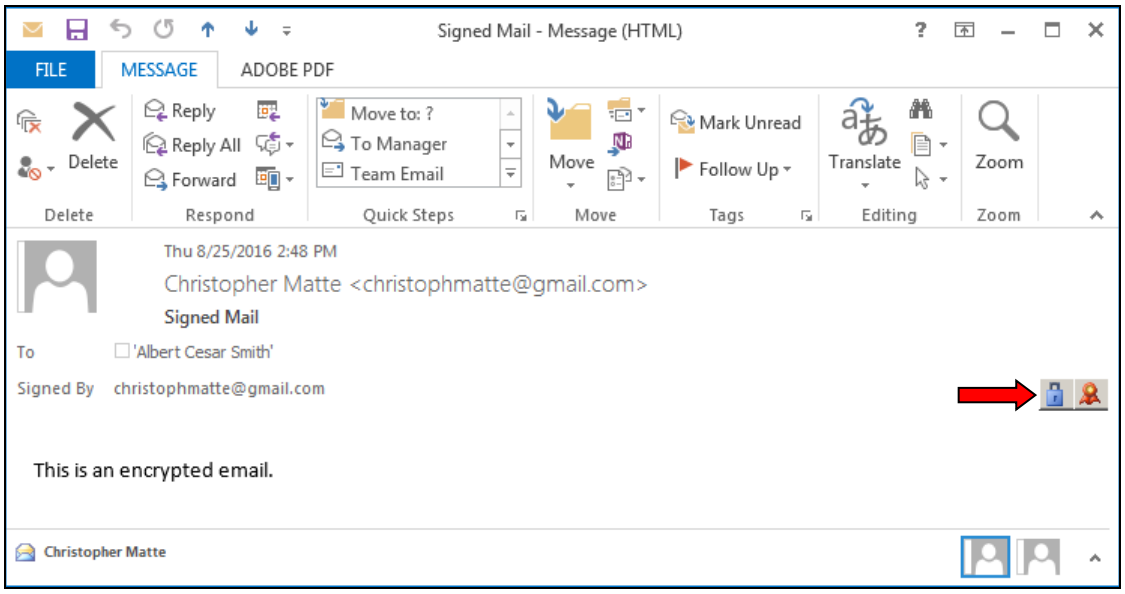


3. Click **Send**.

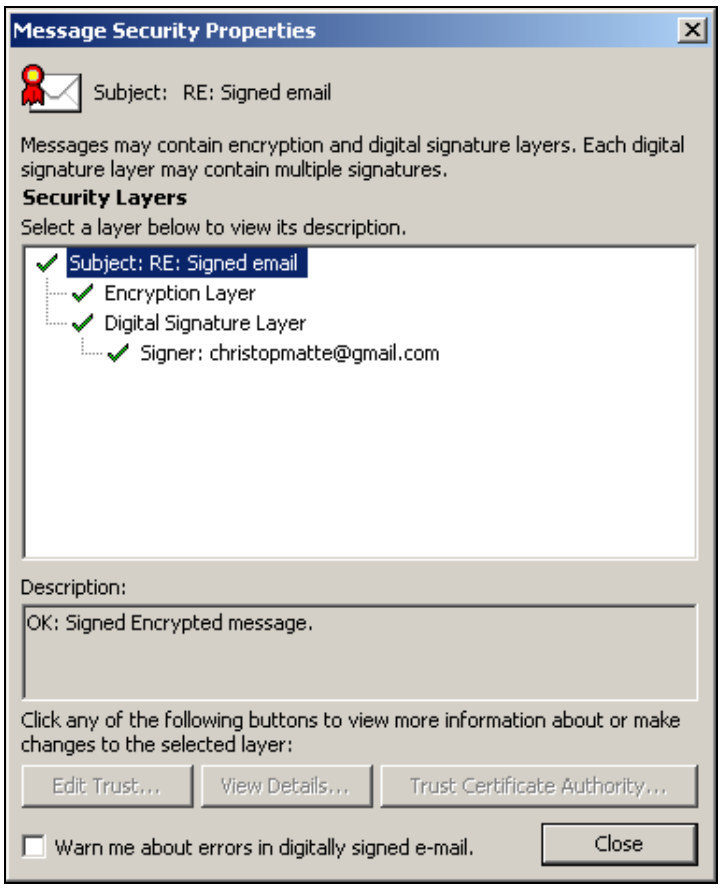


4. Type in your token PIN when prompted.

5. If you are the recipient of an encrypted email, a small blue padlock is attached to the mail message icon indicating that it is encrypted.



6. Click the blue padlock icon to view the details of the encrypted mail message.



6.5. Using certificates in Mozilla® Thunderbird®

Similar to Microsoft Outlook, you can send and receive signed/encrypted emails using your token in Mozilla Thunderbird.

The **ACS PKCS Middleware** also allows a user to send/receive signed and/or encrypted emails using the token.

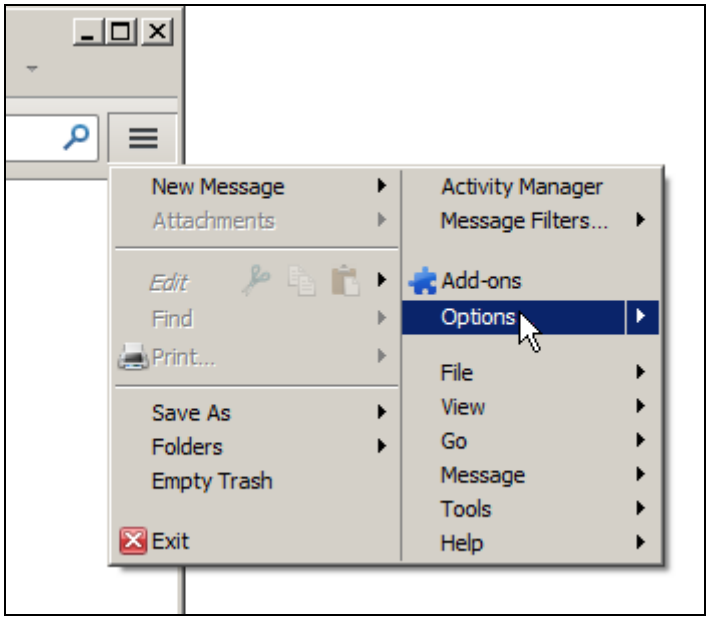
Note: *Before using a token in Mozilla Thunderbird, make sure that you have requested a certificate from a Certificate Authority. This certificate will be used for encryption and signing email.*

6.5.1. Loading PKCS #11 in Mozilla Thunderbird

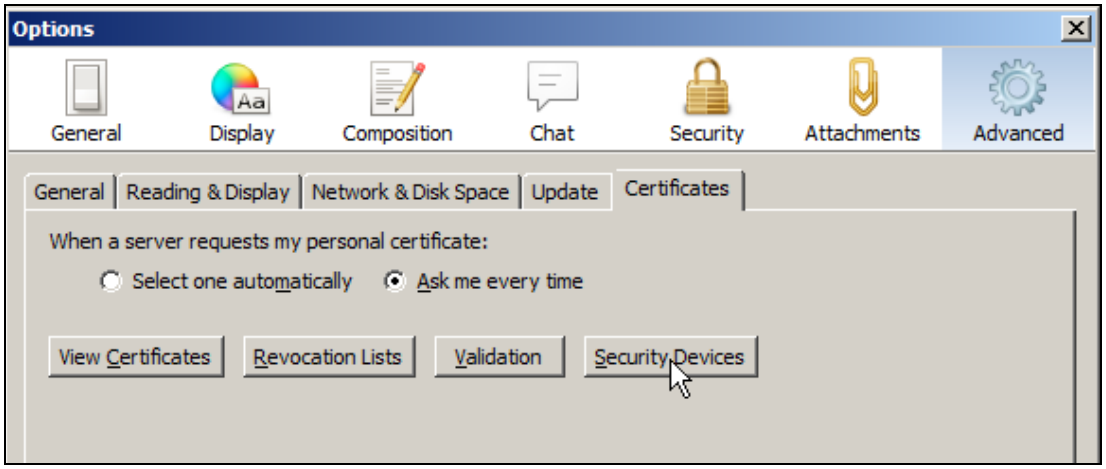
To start using your token in Mozilla Thunderbird, make sure that you have loaded the ACS PKCS #11 Module in the application.

To load ACS PKCS #11 in Mozilla Thunderbird:

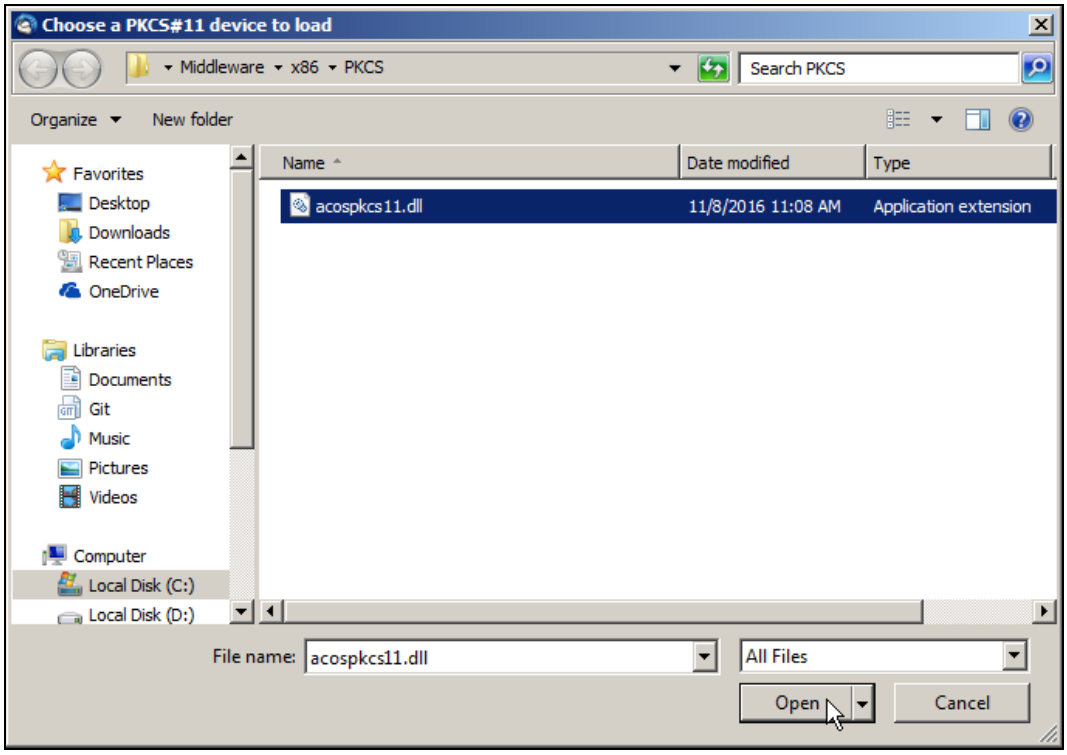
1. Click the **Menu** button  on the top right corner of the application, and then click **Options**.



2. Click **Advanced**.
3. Under the **Certificates** tab, click **Security Devices**.

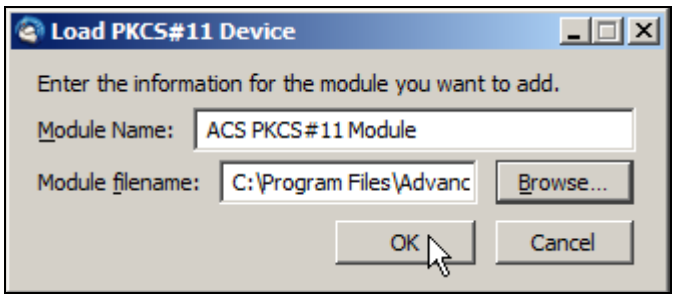


4. The Device Manager will be displayed. Click **Load**.
5. Type in "**ACS PKCS #11 Module**" as Module Name.
6. Locate the *acospkcs11.dll* file in the path: ***C:\Program Files\Advanced Card Systems Ltd\ACOS5-CryptoMate Admin Client Kit\Middleware\x86\PKCS***, and then click **Open**.



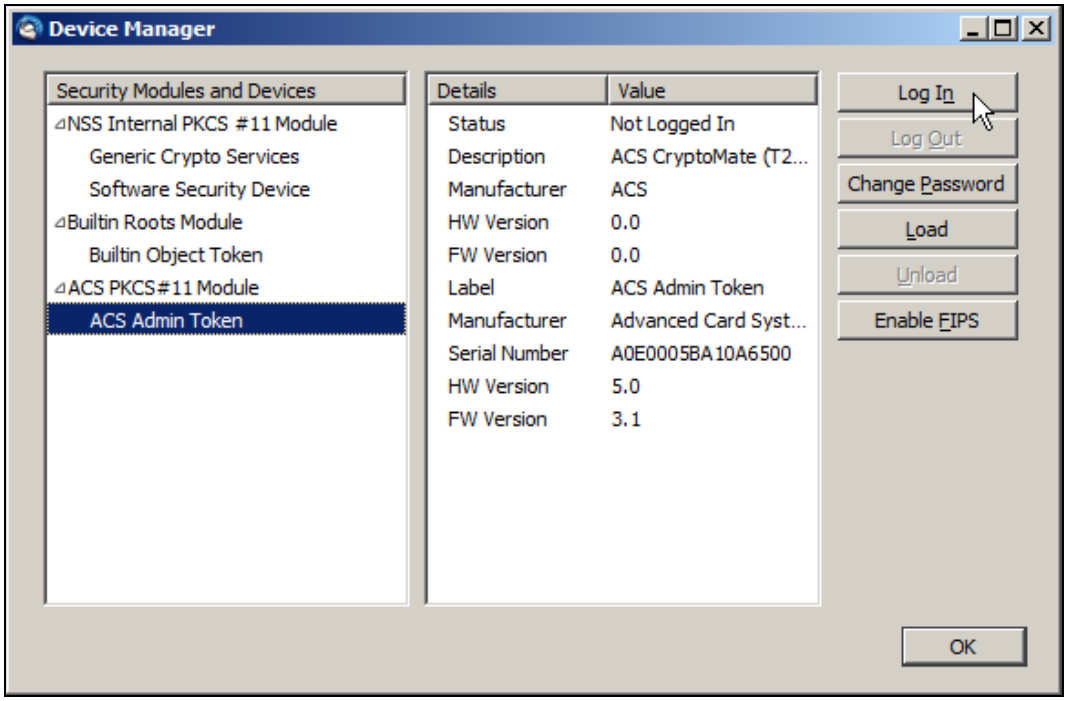
Note: *If you installed the package in another folder or path, make sure to enter the correct file path. For 64-bit platform users, please make sure to load the 64-bit .dll file in the 64-bit application and the 32-bit .dll file in the 32-bit application respectively.*

7. Once the file is located, click **OK**.



8. The Device Manager will display the **ACS PKCS #11 Module** together with your token.

9. Select your token, and then click **Log in**.



10. Type in your token PIN when prompted.
11. Once logged in, you are now ready to send/receive signed and/or encrypted e-mails using your ACS token with Mozilla Thunderbird.

6.5.2. Configuring your digital certificate in Mozilla Thunderbird

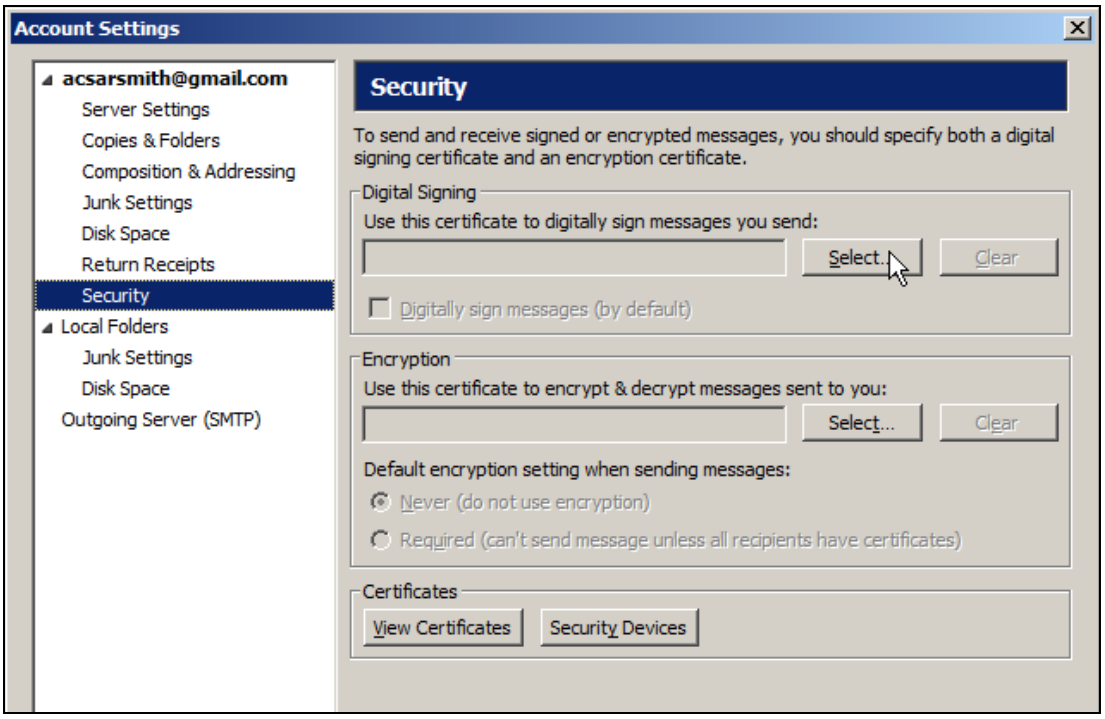
Before signing/encrypting an email, Mozilla Thunderbird should know which digital certificate should be used for each operation. The following procedure will help you configure your digital certificate for signing and encrypting emails.

Notes:

1. *The email account to be used in Mozilla Thunderbird SHOULD be the same email address used when the digital certificate was requested.*
2. *Make sure that the token with a valid certificate is connected in your system, and that you have loaded the ACS PKCS #11 Middleware for Mozilla Thunderbird.*

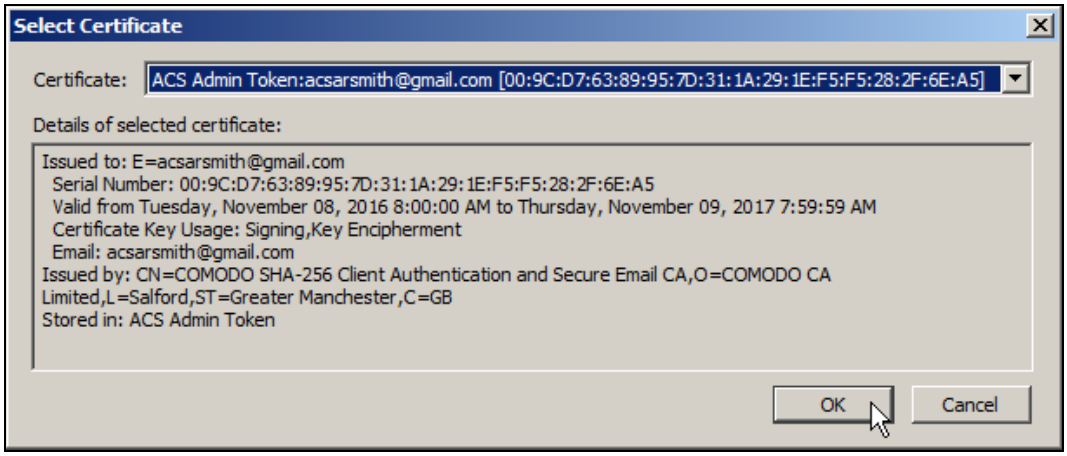
To set up a digital certificate using Mozilla Thunderbird:

1. Click the **Menu** button  , point to **Options**, and then click **Account Settings**.
2. In the **Account Settings** window, click **Security** in the left side of the panel.
3. Under Digital Signing, click **Select**.



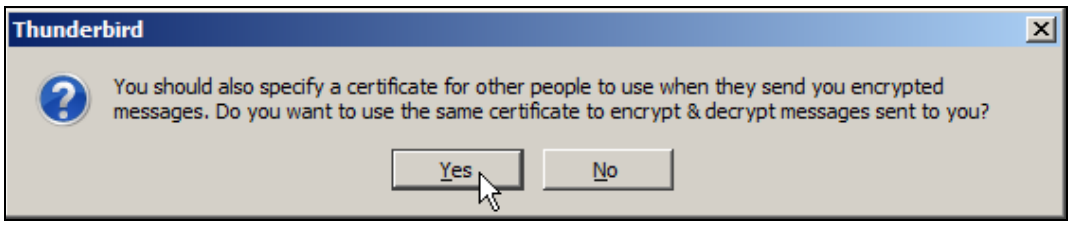
4. Type in your token PIN when prompted.

5. Select the certificate to be used in the drop-down list, and then click **OK**.



Note: *The "Stored in" property indicates which token the selected certificate is stored in. This value SHOULD be the same label with the token being used.*

6. A dialog box appears and asks if you want to use the same certificate in encrypting and decrypting messages sent to you. Click **Yes**, otherwise, click **No** and select a different certificate.



7. Once the certificate has been selected for digital signing and encryption, click **OK**.
8. Your ACS token is now ready to use in signing/encrypting e-mails with Mozilla Thunderbird.

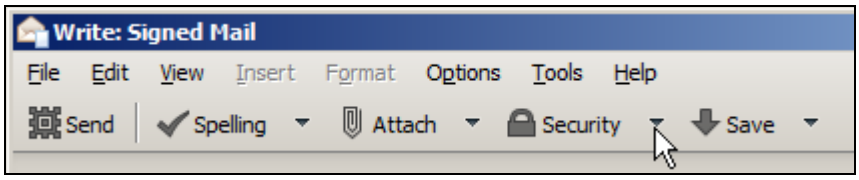
6.5.3. Signing an e-mail in Mozilla Thunderbird

Signing emails is synonymous to putting one's own signature (like a thumbprint or a seal) in a letter. This ensures the recipient that the message came from you and that you have put your own mark on the email for the recipient to verify. This also ensures that the message has not been tampered in between the sender and the recipient.

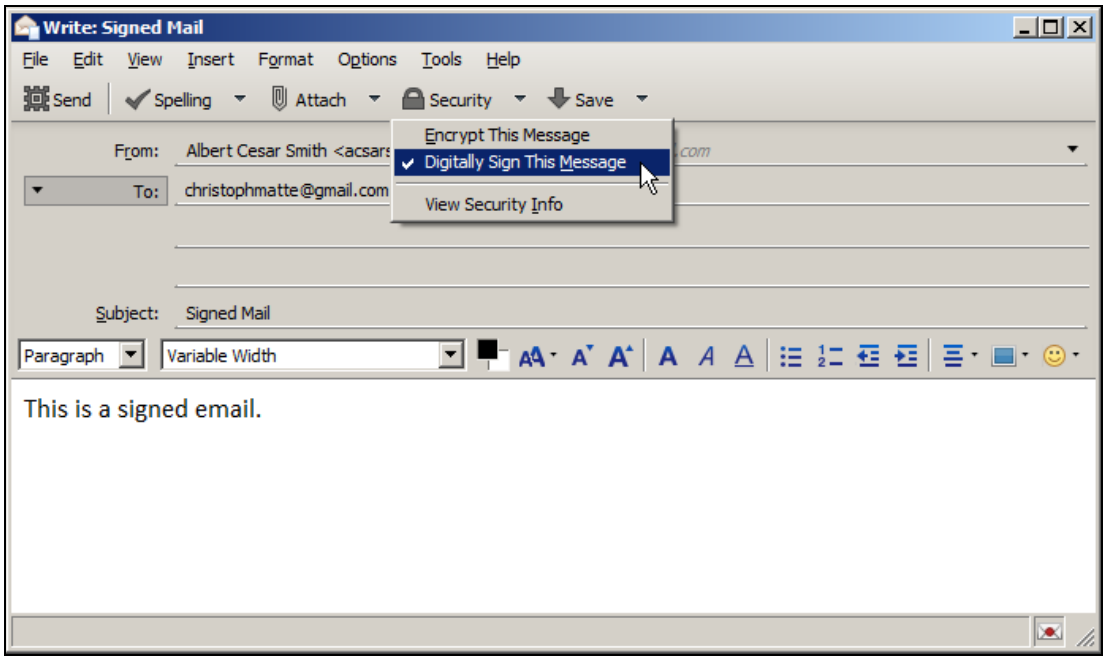
Note: *Make sure that a token with a valid certificate is connected in your system.*

To sign an email using Mozilla Thunderbird:

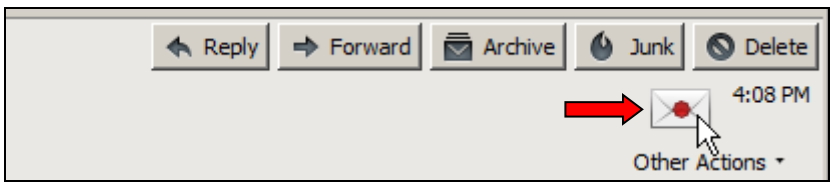
1. Create a new mail message as usual.
2. Before sending, click the arrow beside **Security** in the Composition Toolbar.



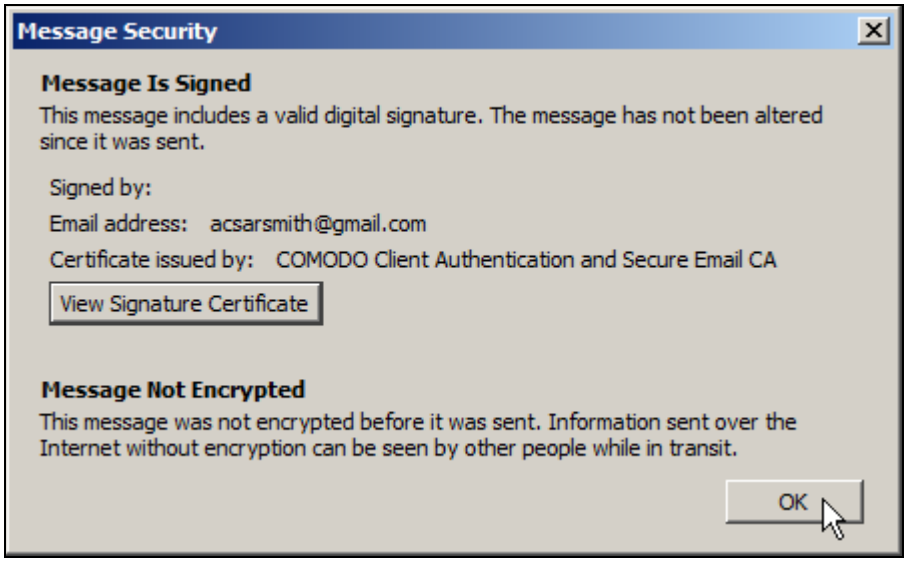
3. Click **Digitally Sign This Message**.



4. Click **Send**.
5. Type in your token PIN when prompted.
6. Once sent, a signed email will indicate a white envelope with a red seal.



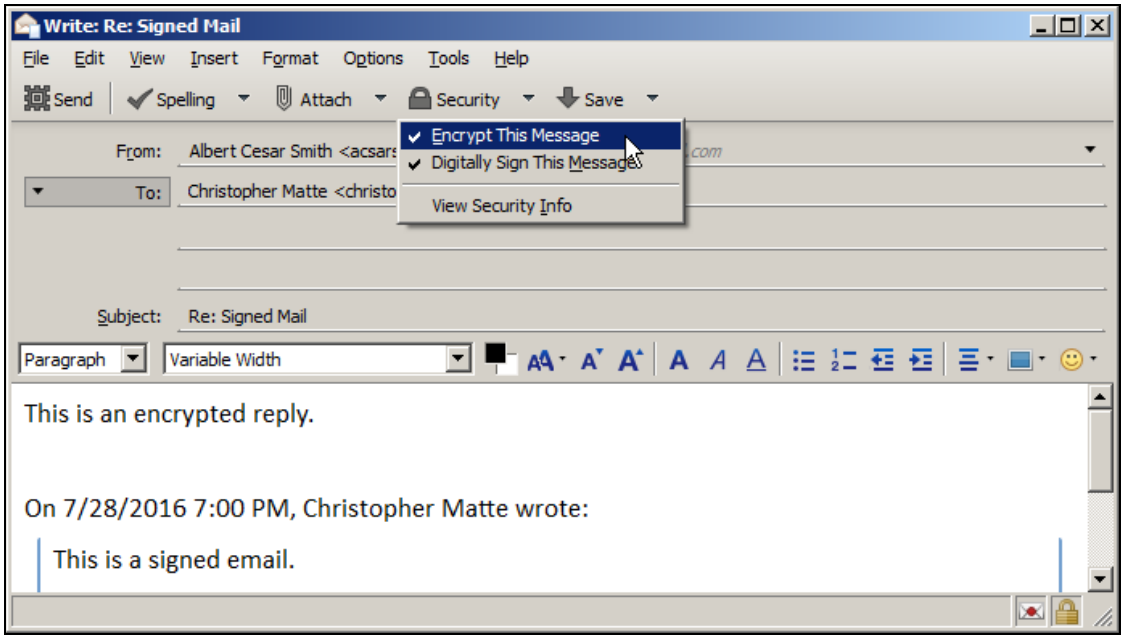
7. Click the envelope to view the details of the signed email.



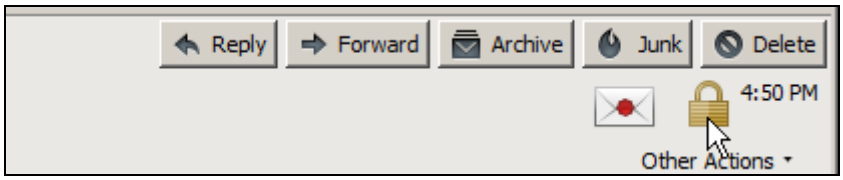
6.5.4. Encrypting an e-mail in Mozilla Thunderbird

To encrypt an email using Mozilla Thunderbird:

1. When you receive a signed email and you want to reply with an encrypted email, click on the **Reply** button.
2. Compose your reply as usual. Before sending, click the arrow beside **Security** in the Composition Toolbar.
3. Click both **Encrypt This Message** and **Digitally Sign This Message**.



4. Click **Send**.
5. Type in your email password when prompted.
6. Once sent, an encrypted email will indicate a padlock right beside the envelope with the red seal.



7. Click the padlock icon to view the details of the encrypted and signed email.

6.6. Using certificates in Microsoft Word

Using digital certificates and signatures assure that the file you are about to use comes from a reliable source, and that it has not been tampered with.

Using Microsoft Word and ACS CSP Middleware, you can sign documents by using certificates stored in your token.

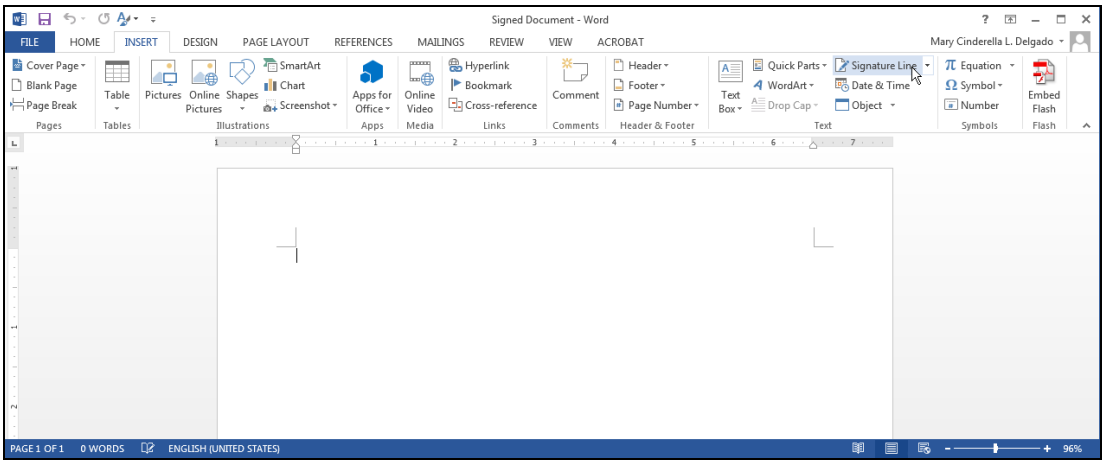
6.6.1. Signing a document using Microsoft Word

Notes:

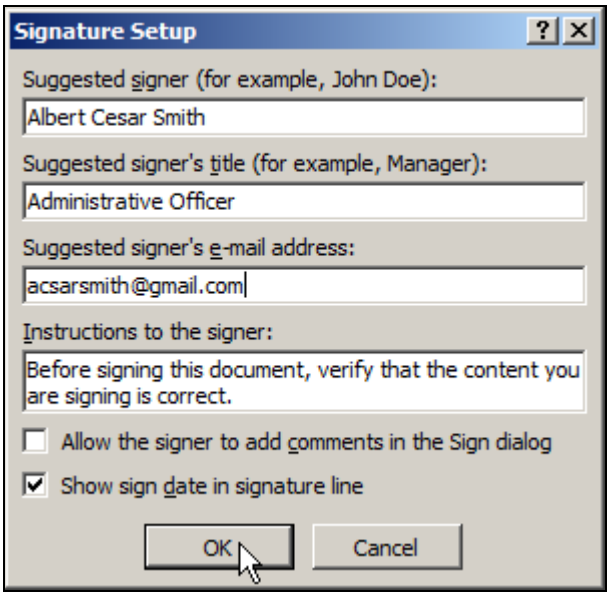
1. *Make sure that a token with a valid certificate is connected in your system.*
2. *The certificate in the token should be installed in Windows Certificate Store. To check, see* ***Viewing certificates in Microsoft Management Console (MMC)****.*

To sign a document using Microsoft Word 2013:

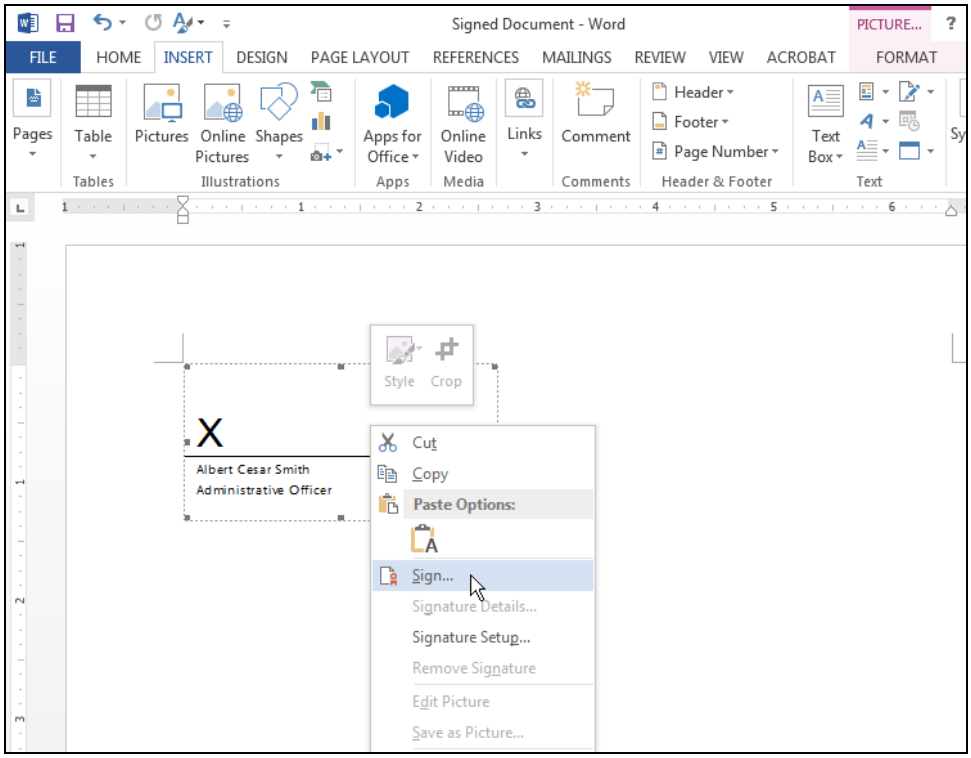
1. Under the **Insert** tab, click **Signature Line** in the **Text** ribbon.



2. Fill up the **Signature Setup** dialog box with your details, and then click **OK**.



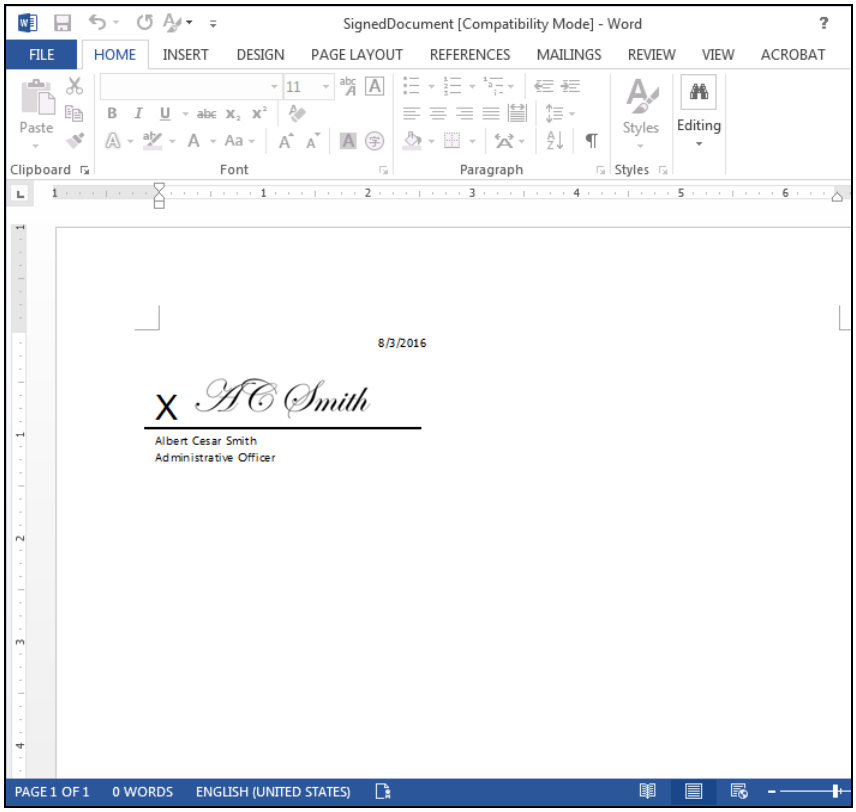
3. The signature is inserted in the document. Right-click on the signature, and then click **Sign**.



4. The **Sign** dialog box will appear. You can type your name in the field or insert an image to the signature.
5. Click **Change** to select the certificate you want to use.

6. Once the certificate has been selected, click **Sign**.

7. Type in your token PIN when prompted.
8. The document is now signed.



Note: *Any modification in the document will make the digital signature invalid.*

6.7. Using certificates in LibreOffice

LibreOffice is a free open source office suite that includes a word processor, spreadsheet, presentation tool, drawing package and database. With LibreOffice, you can sign documents to ensure authenticity and security using your digital certificate.

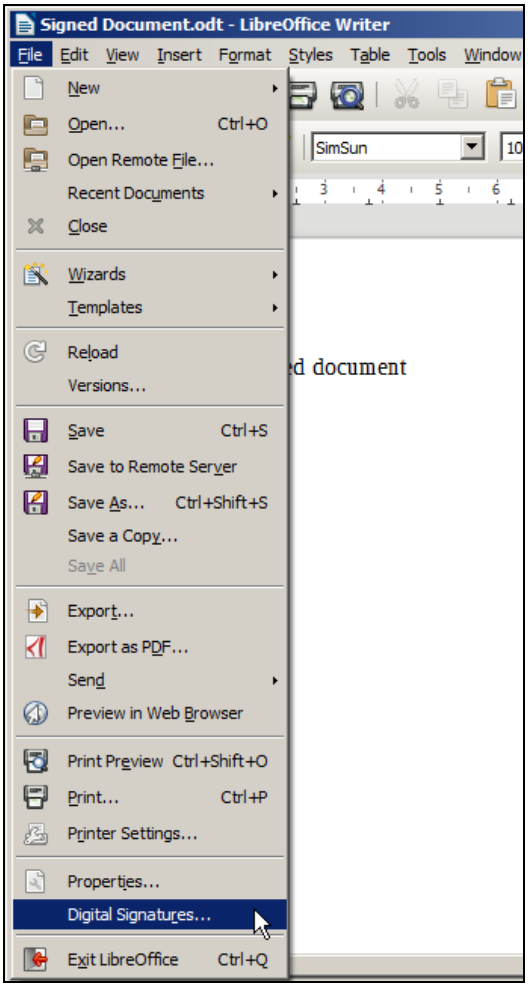
Note: *Make sure you have loaded the PKCS #11 in Mozilla Thunderbird to proceed with signing a document in LibreOffice. See* ***Loading PKCS #11 in Mozilla Thunderbird****.*

6.7.1. Signing a document in LibreOffice

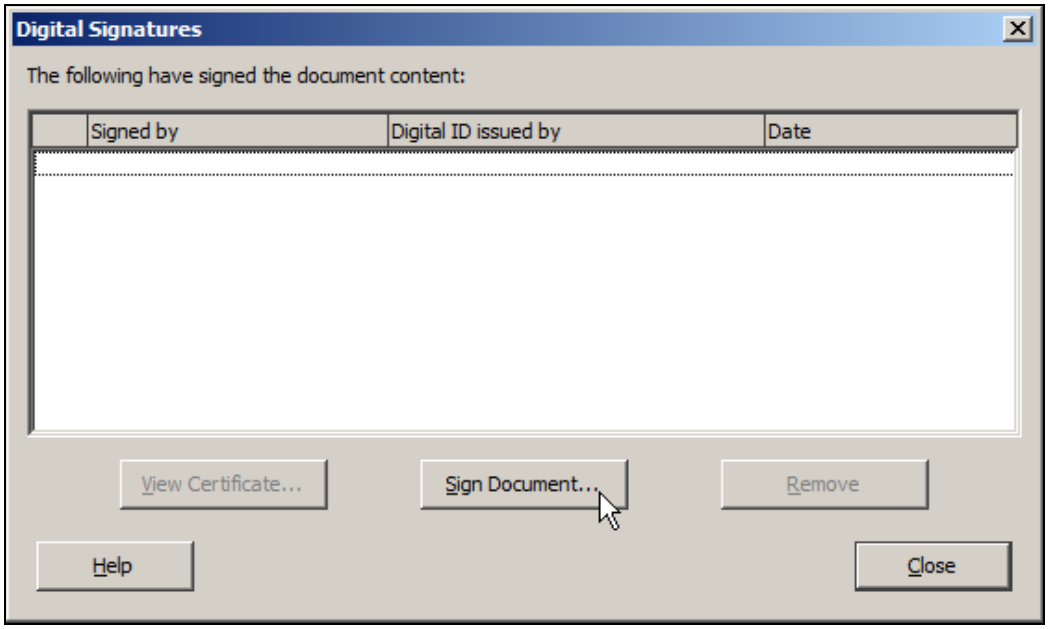
To sign a document in LibreOffice:

Note: *This procedure uses LibreOffice Writer.*

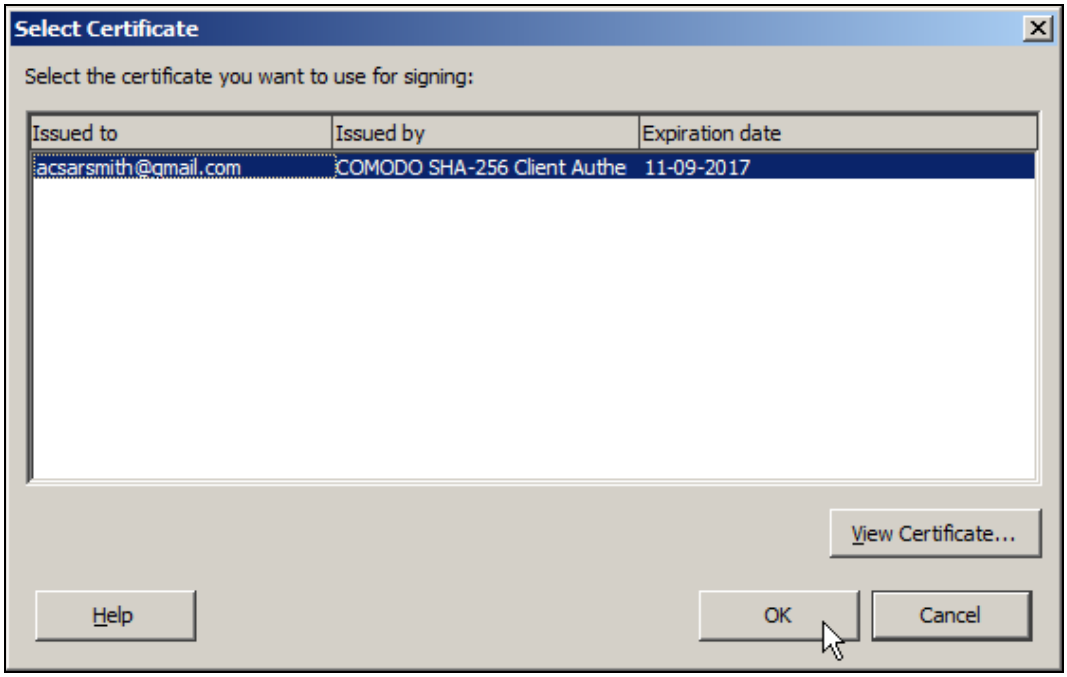
1. Make sure that your document has been saved.
2. In the **File** menu, click **Digital Signatures**.



3. The **Digital Signatures** window will appear. Click **Sign Document** to select your certificate.

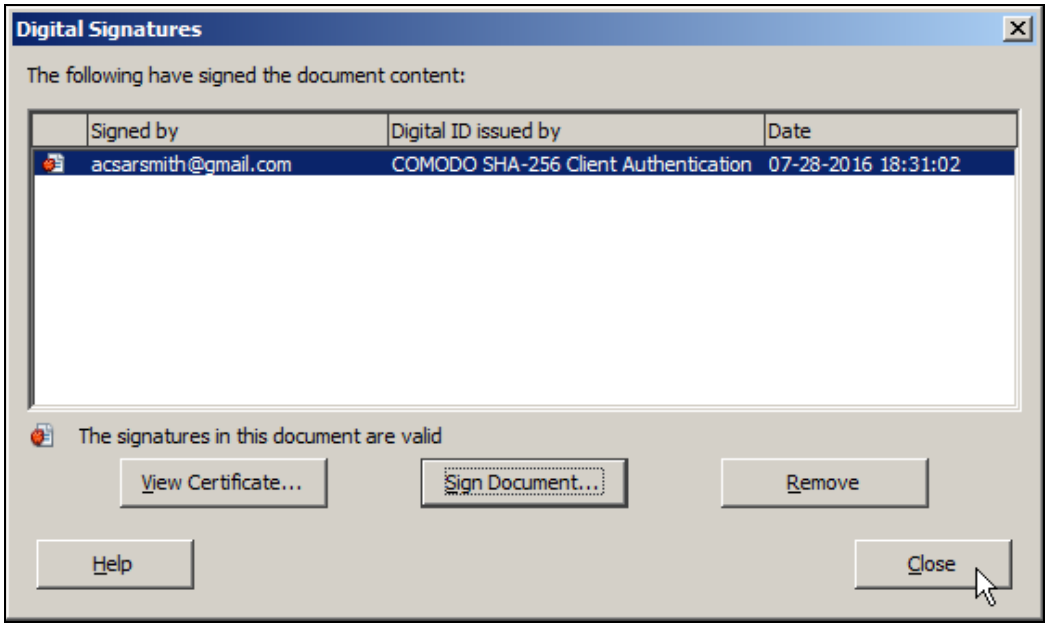


4. Select your certificate, and then click **OK**.

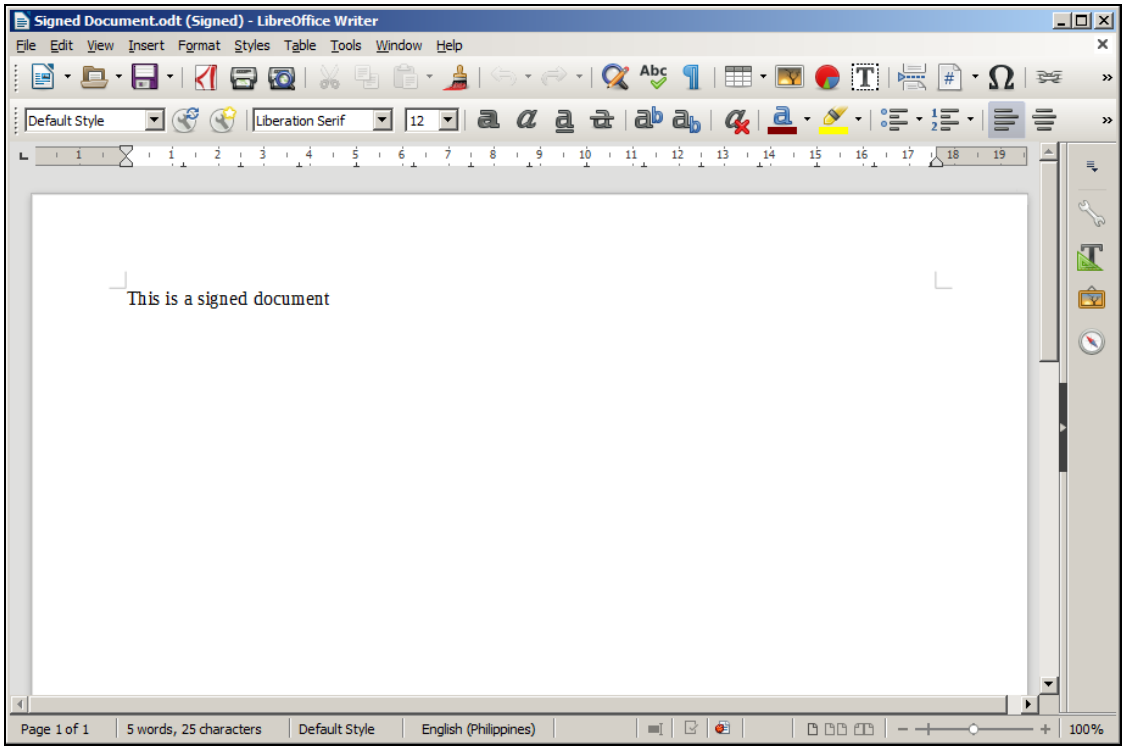


5. Type in your token password when prompted.

6. Digital Signatures window will show that your certificate is valid. Click **Close**.



7. Once the document has been signed, you will see the word *"(Signed)"* beside the filename on the top bar, and an indicator appears on the status bar.



6.8. Using certificates in Adobe® Acrobat® Pro

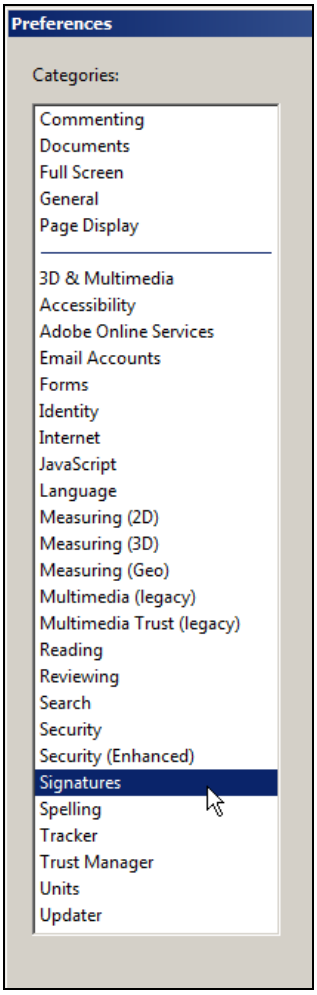
Using the Adobe® Acrobat® Pro and ACS Middleware, you can sign and encrypt PDF files using the certificates stored in your token. The following sections will show you the steps in using a digital certificate in Adobe Acrobat Pro application.

6.8.1. Loading PKCS #11 in Adobe Acrobat Pro

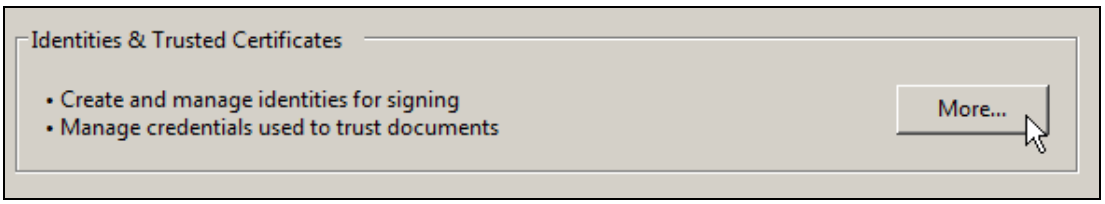
To start using you token in Adobe Acrobat Pro, make sure that you have loaded the ACS PKCS #11 Module in the application.

To load the ACS PKCS Module in Adobe Acrobat XI Pro:

1. From the **Edit** menu, point to **Preferences**, and then click **Signatures**.

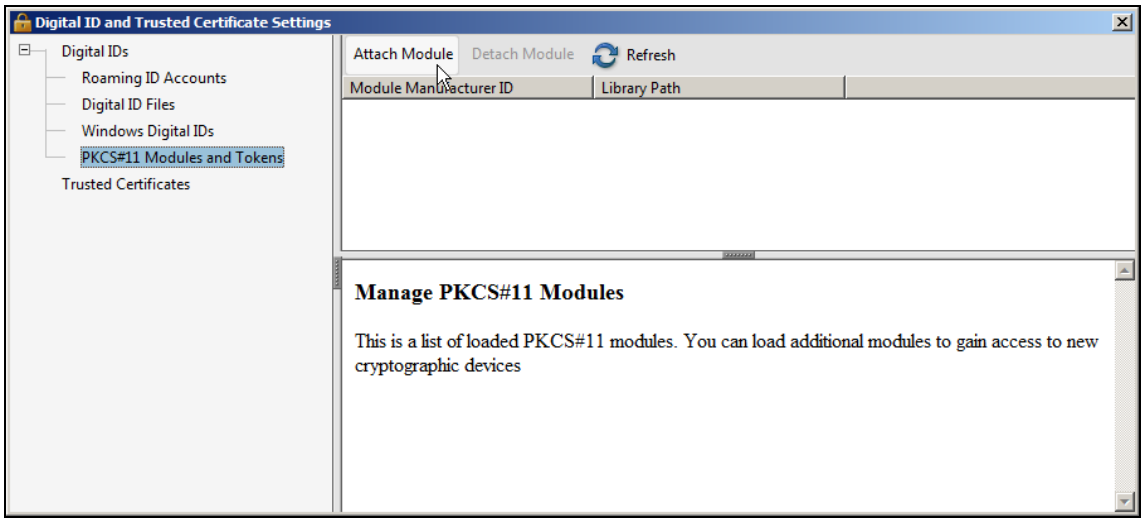


2. Under **Identities & Trusted Certificates**, click **More**.

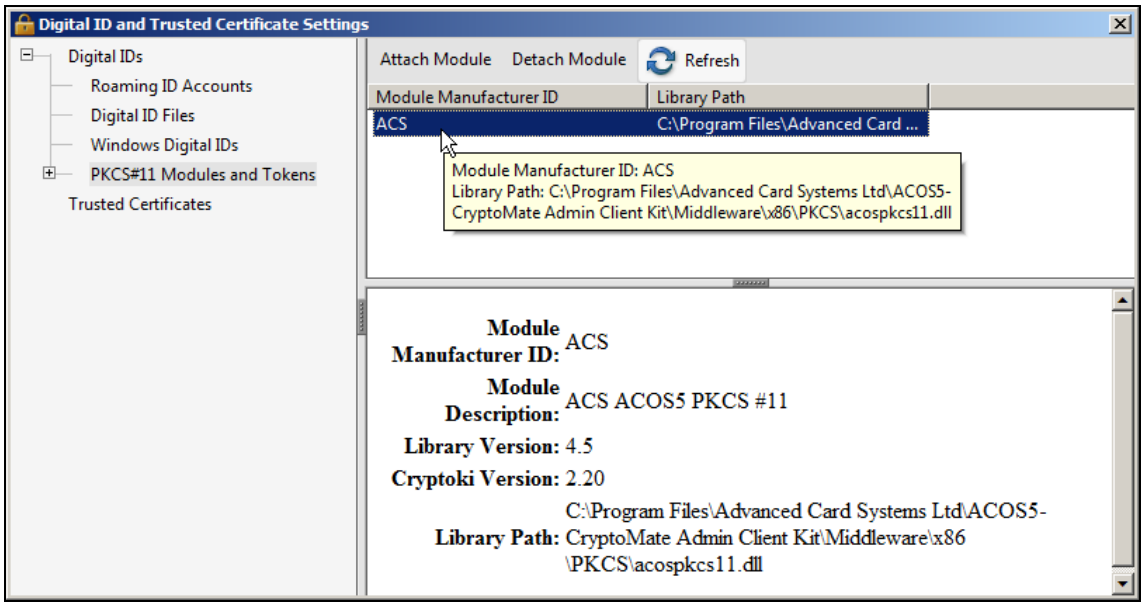


3. The Security Settings window will appear. Click **Digital IDs**, and then select PKCS#11 Modules and Token.

4. Click **Attach Module**.



5. Locate the *acospkcs11.dll* file in the path: ***C:\Program Files\Advanced Card Systems Ltd\ACOS5-CryptoMate Admin Client Kit\Middleware\x86\PKCS***, and then click **Open**.
6. The ACS PKCS#11 Module should now be visible in the **Security Settings** panel.

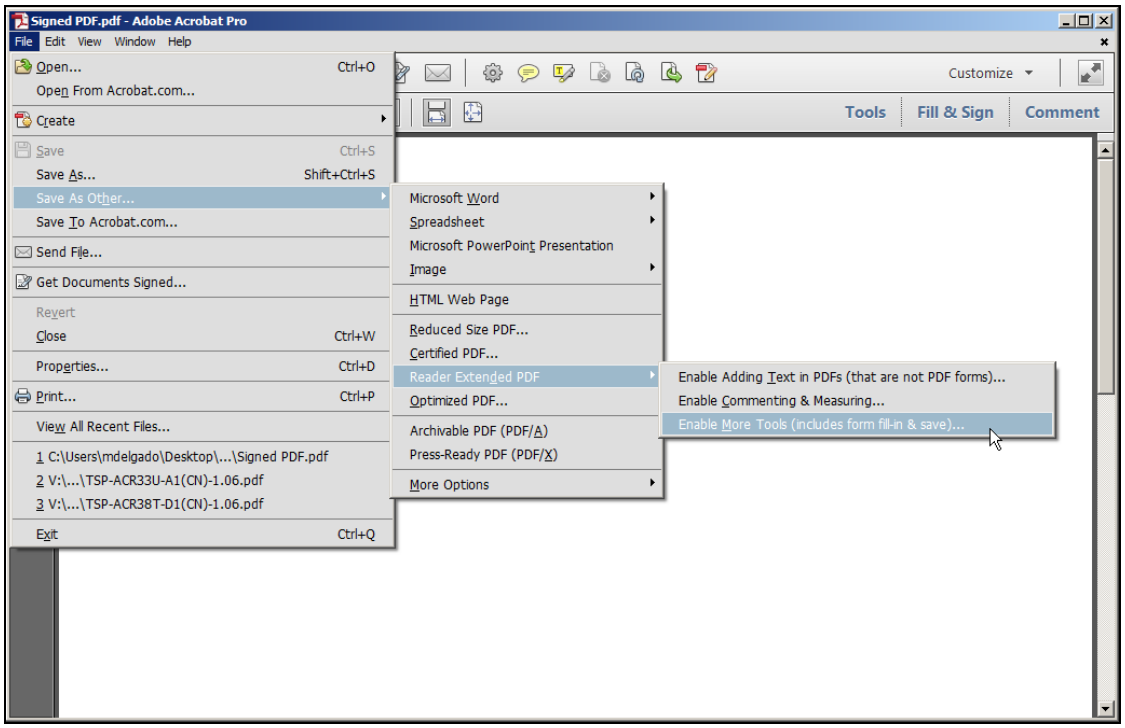


6.8.2. Enabling digital signing for other PDF users

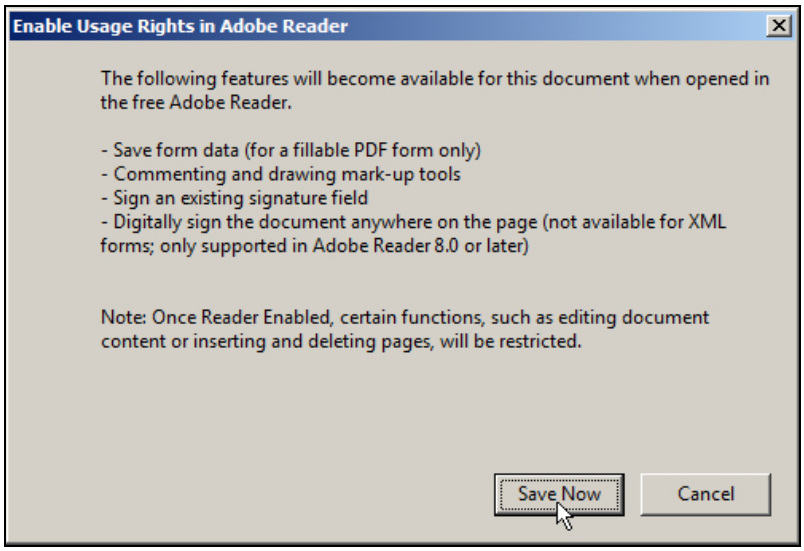
To allow other intended users of a PDF document to digitally sign a document, the Author must first prepare the PDF document with the Reader Extended features. To do this, **you need to have the Adobe Acrobat Pro installed in your system**.

To enable Reader Extended features:

1. Open the PDF document to be signed.
2. In the **File** menu, click **Save As Other**, point to **Reader Extended PDF**, and then click **Enable More Tools (includes form fill-in & save)…**.



3. The **Enable Usage Rights** window appears. Click **Save Now**.



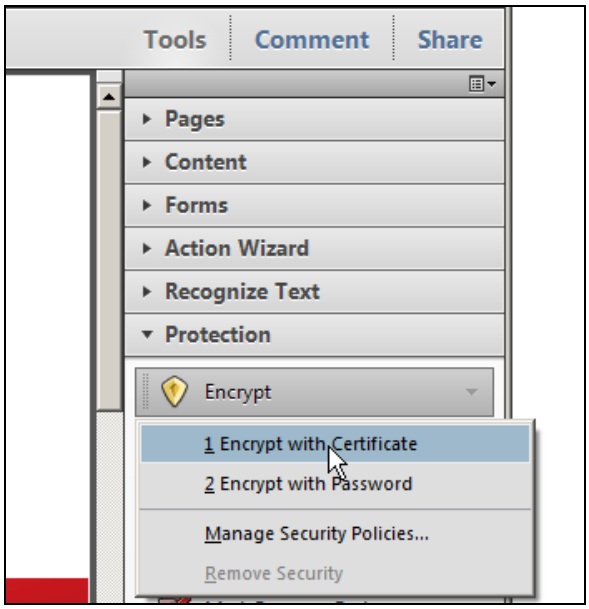
4. Save the document.
5. You can now affix your digital signature. For recipients of documents that need digital signature but are using the free Adobe PDF Reader, see **Using certificates in Adobe® Reader®**.

6.8.3. Encrypting a PDF document

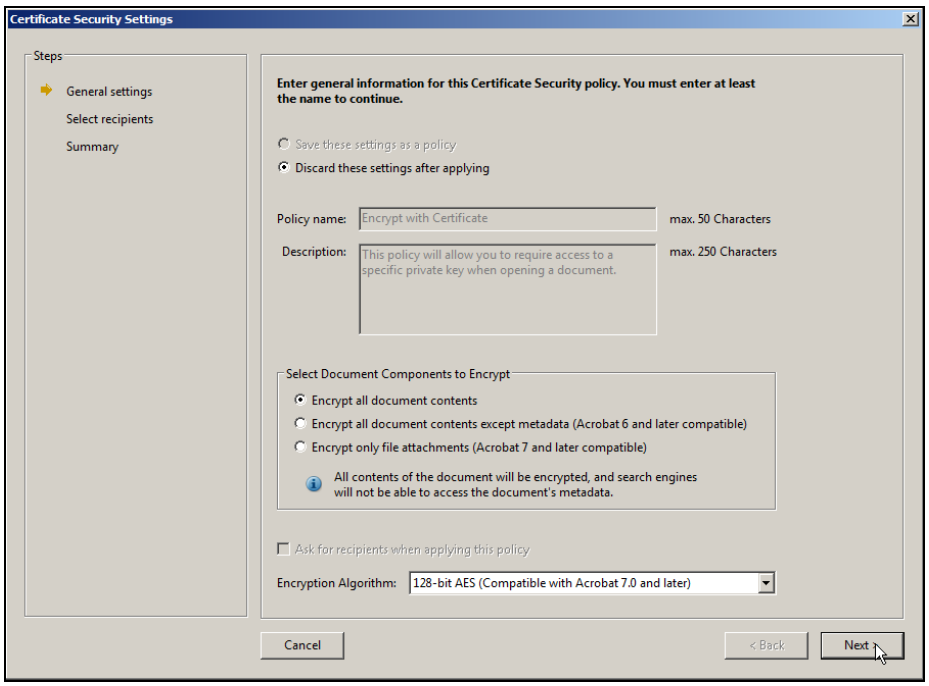
Encrypting a PDF document ensures that only the intended readers can decrypt and read the contents of the document.

To encrypt a PDF document:

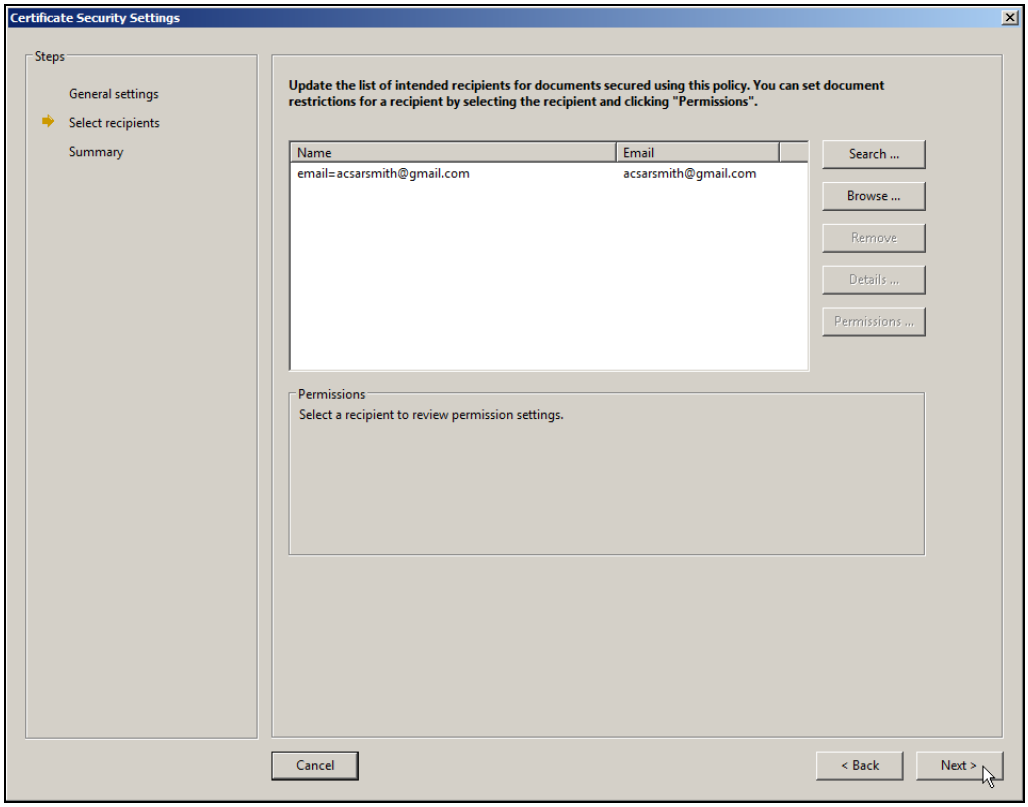
1. Make sure that the document is enabled with Reader Extended features (see **Enabling digital signing for other PDF users**).
2. Once you have your PDF document ready, click on **Tools**. Under **Protection**, click **Encrypt**, and then select **Encrypt with Certificate**.



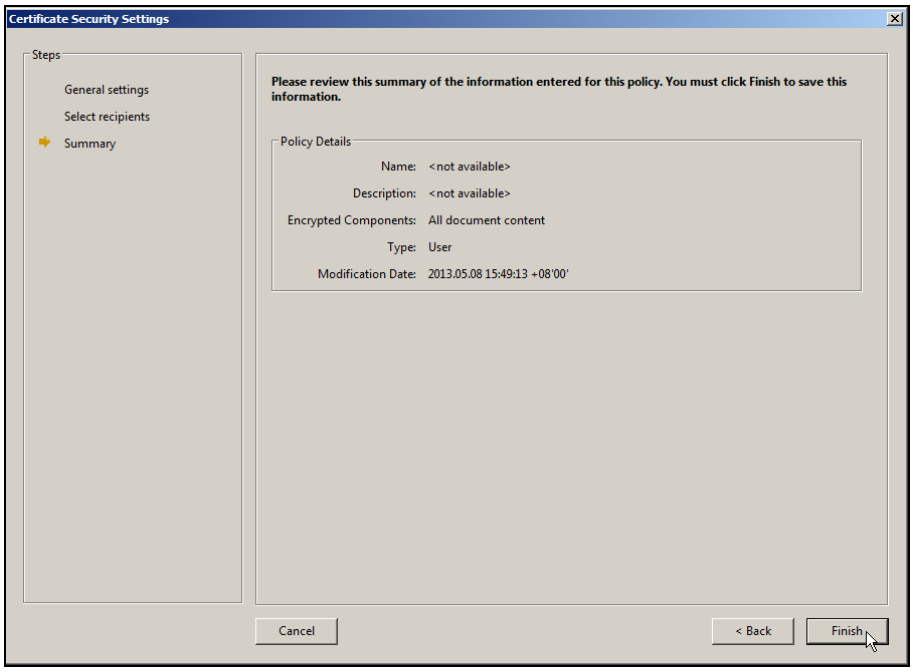
3. The **Certificate Security Settings** will appear. Select document components to encrypt, and then click **Next**.



4. Add the intended readers of the encrypted PDF file. This is the most important part of encrypting a document. If you do not add any recipients in the list, then you will be the only one who can decrypt and read the encrypted file properly. To add recipients of your document, you should first have a copy of the certificate file (*.cer) of your recipient's digital certificate. Click **Browse** to add recipient(s) and their corresponding certificate(s), and then click **Next**.



5. After finalizing the list of recipients, review the summarized policy details of the encrypted document. Click **Finish**.



6. To finalize the encryption, save the document. Notice the word *"(SECURED)"* will appear on the top bar of the document beside the filename.

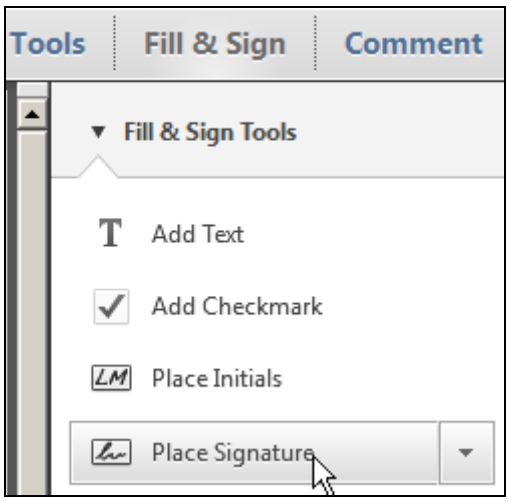
6.8.4. Signing a PDF document

Signing a PDF document ensures that the document had not been tampered since the digital signature has been added. This security feature is particularly important when sending documents through emails.

Note: *Make sure that the token with a valid certificate is connected to your system and that you have loaded the ACS PKCS #11 Middleware for Adobe Acrobat Pro (see* ***Loading PKCS #11 in Adobe Acrobat Pro****).*

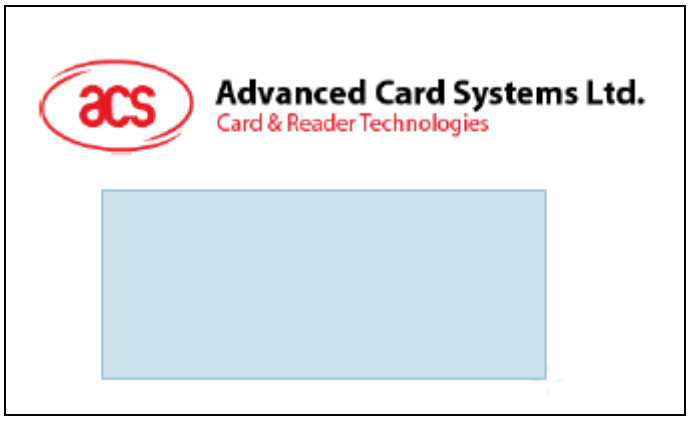
To digitally sign a PDF document:

1. Open the PDF document to be signed.
2. In the top right corner of the toolbar, click **Fill & Sign** and select **Place Signature**.

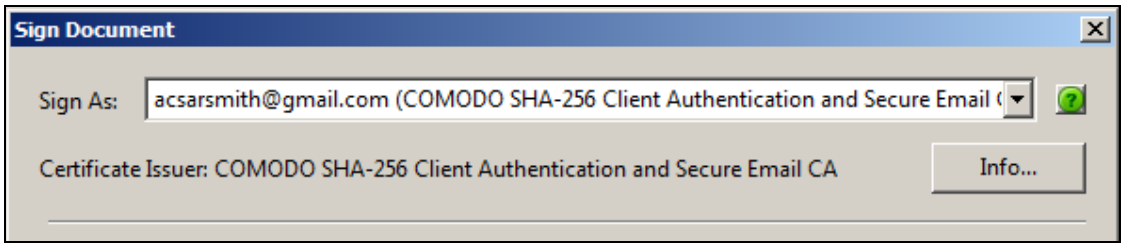


3. Adobe Acrobat prompts on how to create a signature field. Click **Drag New Signature Rectangle**.

4. Click and drag out the field's area in the location where the digital signature should appear in the document.

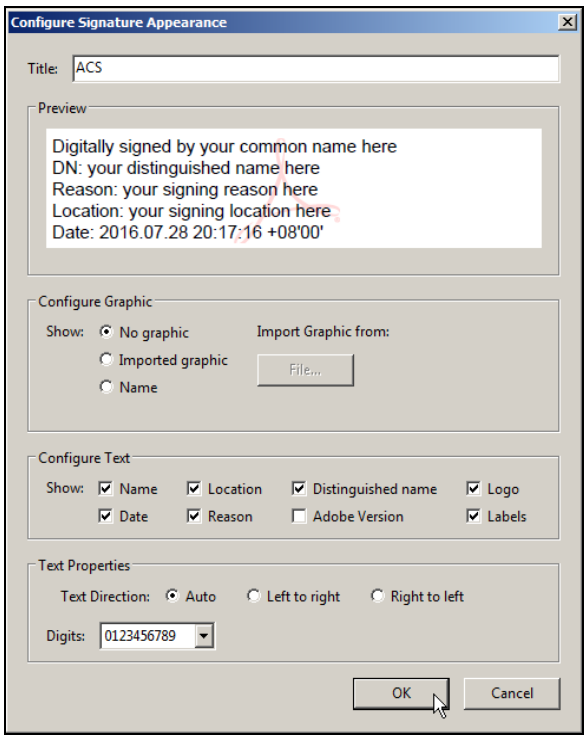


5. The **Certify Document** window will appear. Select the certificate to be used from the **Sign As** drop-down list.

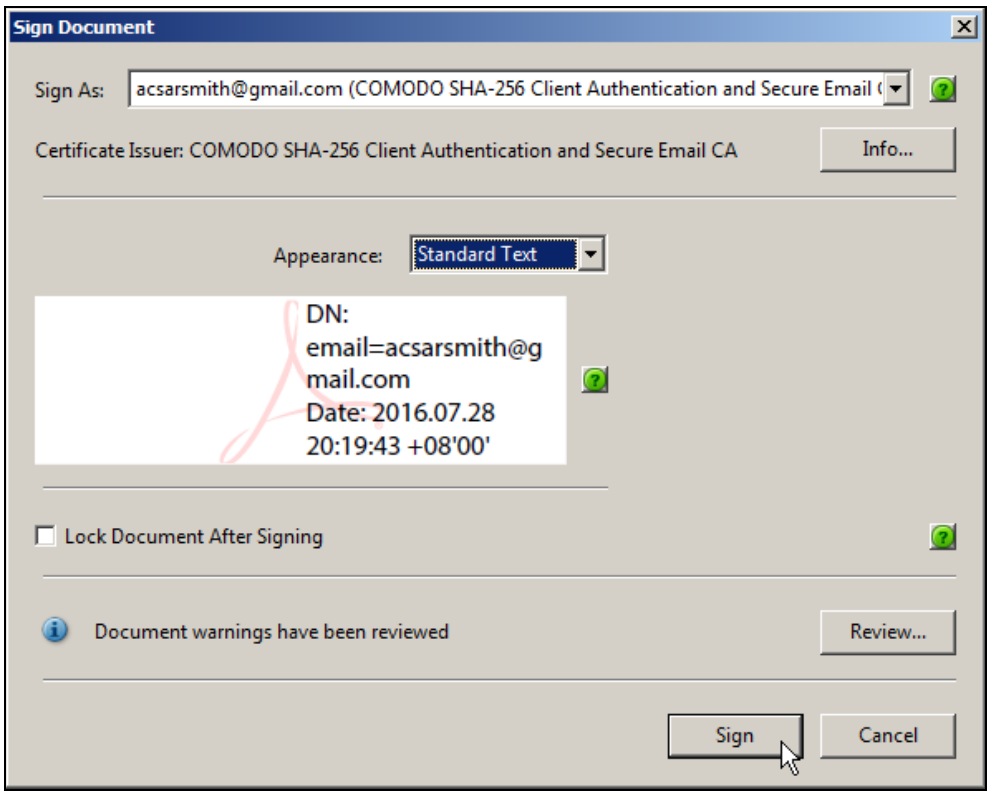


Note: *If you cannot see your digital certificate, try re-inserting the token.*

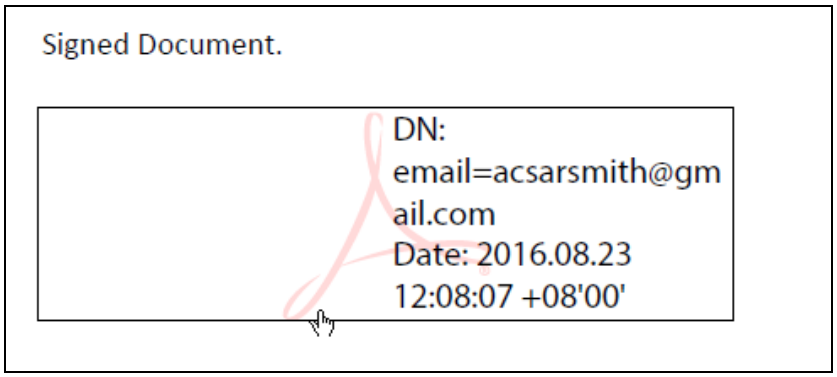
6. You can customize the appearance of your digital signature by clicking on the **Appearance** drop-down listing, and selecting **New Appearance**.
7. Configure the properties of your digital signature as preferred. Click **OK**.



8. Once you have customized your digital signature, click **Sign**.



9. Specify the location where the signed document will be saved, and then click **Save**.
10. Type in your token PIN when prompted.
11. The watermark is added permanently in the document. It indicates who signed the document.



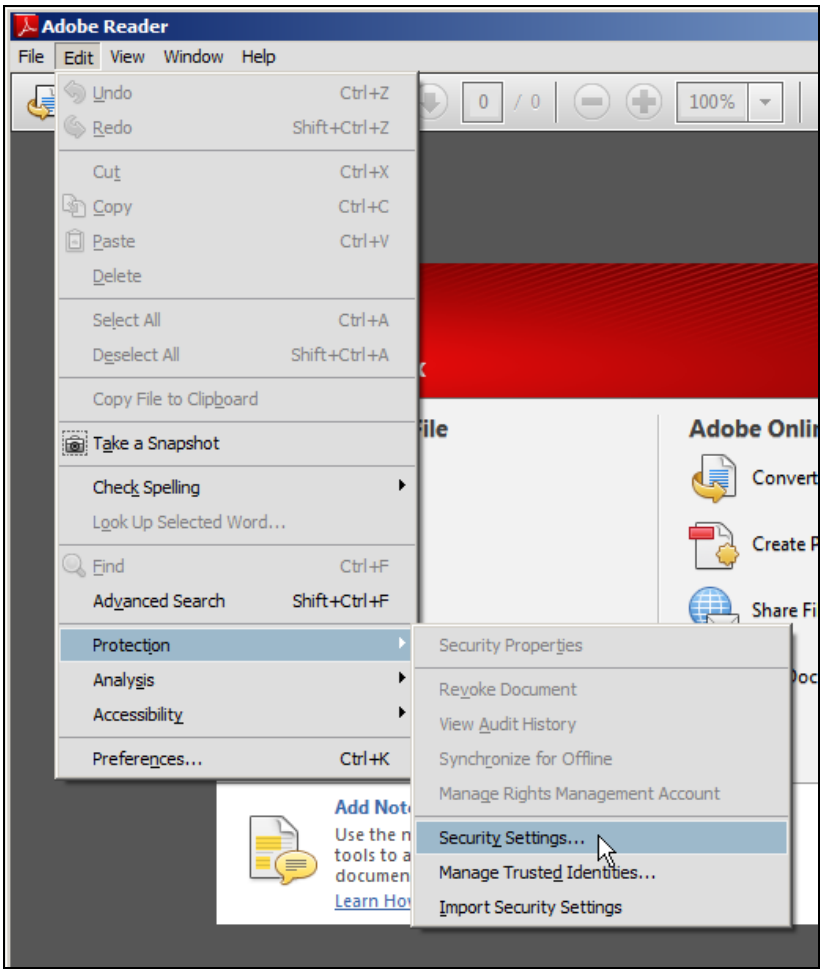
6.9. Using certificates in Adobe® Reader®

6.9.1. Loading PKCS #11 in Adobe Reader

Before you can use digital signatures in your Adobe Reader, the PDF document you are going to sign should have been saved with the Reader Extended functionality using Adobe Acrobat Pro (see **Enabling digital signing for other PDF users**).

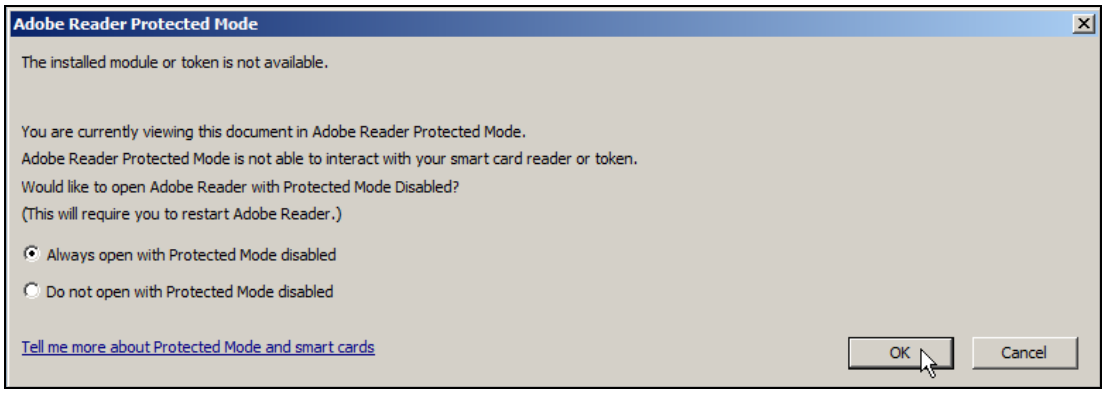
To load the ACS PKCS Module using Adobe Reader X:

1. Under the **Edit** menu, point to **Protection**, and then click **Security Settings**.

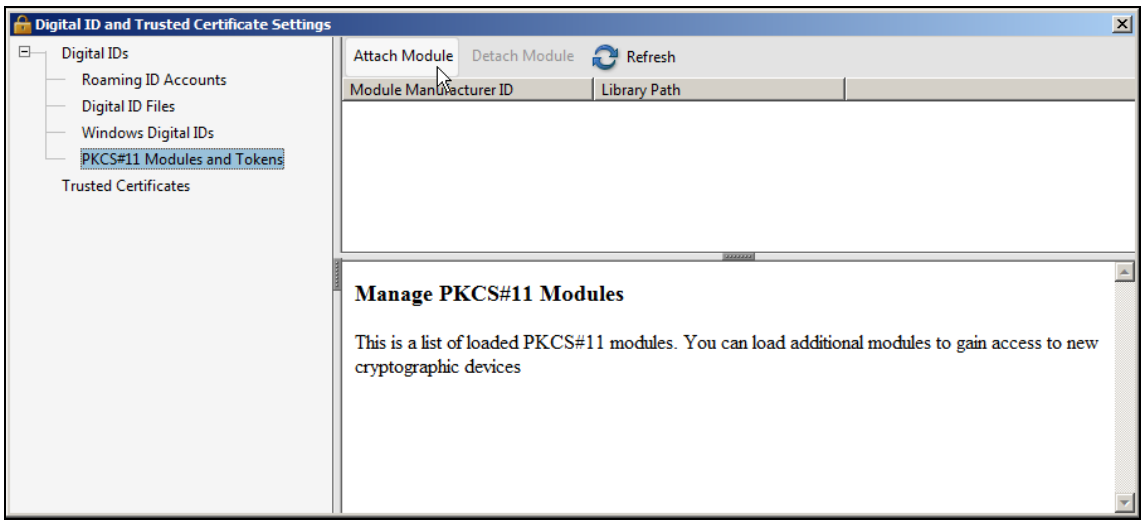


2. The Security Settings window will appear. Click **Digital IDs**, and then select PKCS#11 Modules and Token.

3. When prompted with Adobe Reader Protected Mode window, select **Always open with Protected Mode disabled** and then click **OK**. This will require you to restart Adobe Reader.

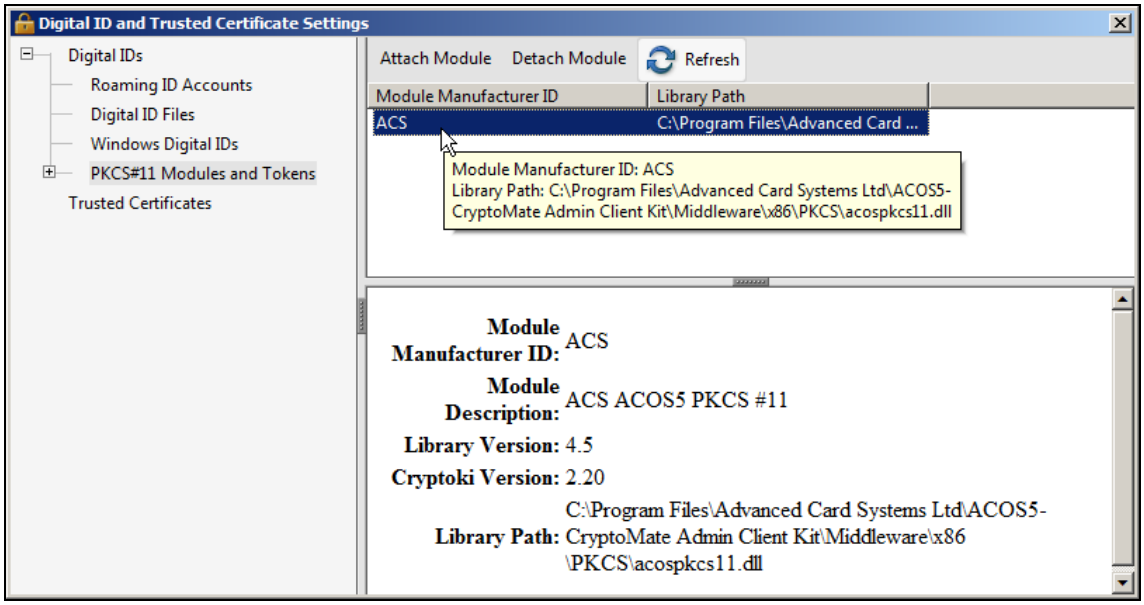


4. Once you have restarted Adobe Reader, repeat steps 1 to 2.
5. Click **Attach Module**.



6. Locate the *acospkcs11.dll* file in the path: ***C:\Program Files\Advanced Card Systems Ltd\ACOS5-CryptoMate Admin Client Kit\Middleware\x86\PKCS***, and then click **Open**.

7. The PKCS #11 Module information should now be visible in the **Security Settings** panel.



8. You are now ready to use your ACS token in Adobe Reader.

6.9.2. Signing a PDF document

Before you can digitally sign a PDF document using the Adobe Reader, the document should have the Reader Extended feature. The Reader Extended feature is enabled by saving the document in Adobe Acrobat Pro (see **Enabling digital signing for other PDF users**).

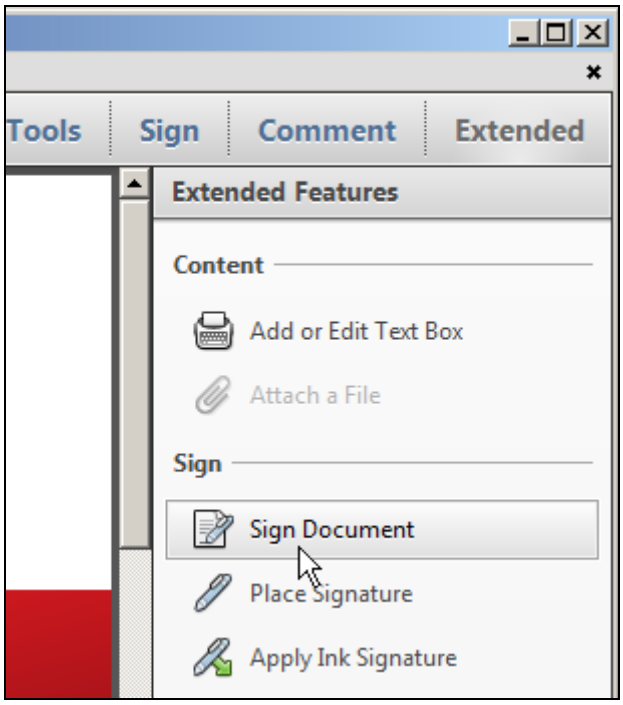
When a document is saved with the Reader Extended feature, the Adobe Reader displays the **Extended** tab in the toolbar.

Figure 3: Adobe Reader Extended Tab

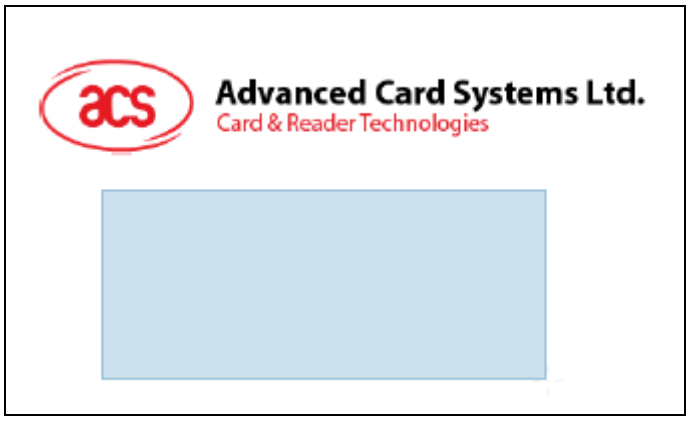
Note: *Make sure that the token with a valid certificate is connected in your system and that you have loaded the ACS PKCS #11 Middleware for Adobe Acrobat Pro (see **Loading PKCS #11 in Adobe Acrobat Pro**).*

To sign a PDF document using Adobe Reader X, follow the steps below:

1. Open the PDF document to be signed.
2. Under the **Extended** tab, click **Sign Document**.



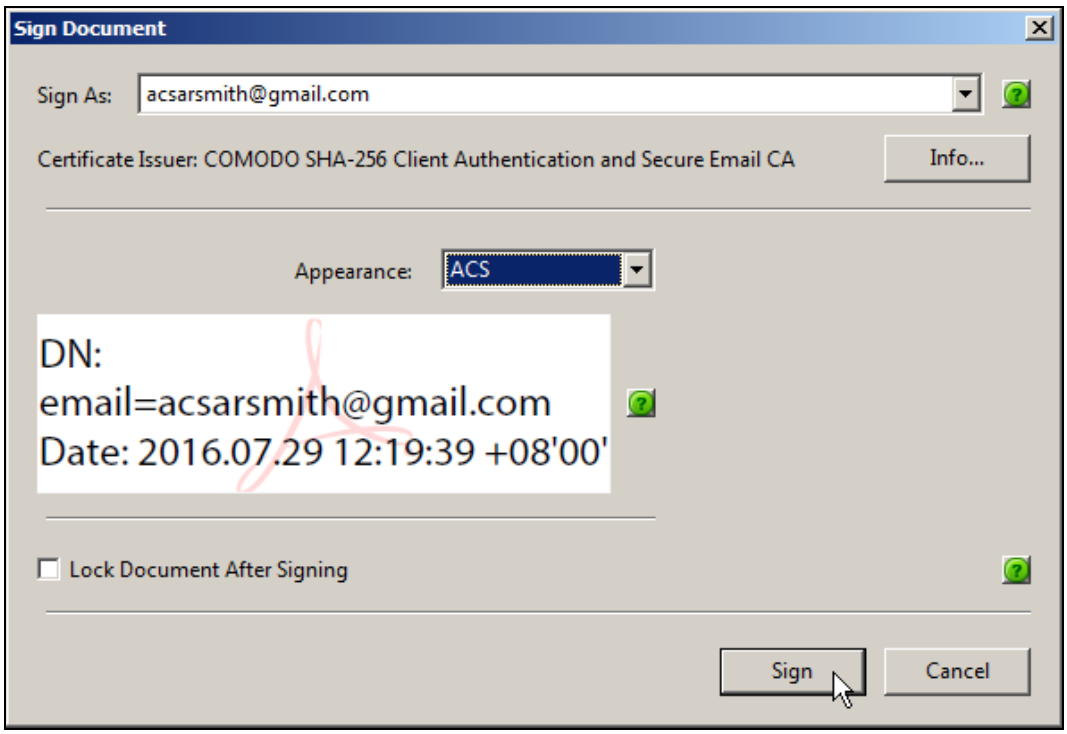
3. Click and drag out the field's area in the location where the digital signature should appear in the document.



4. The **Sign Document** window will appear. Select the certificate to be used from the **Sign As** drop-down list.

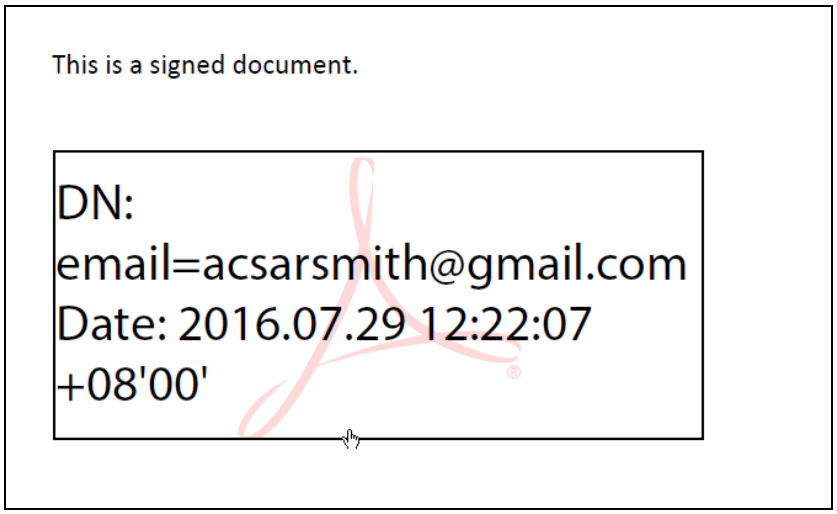
   Note: *If you cannot see your digital certificate, try re-inserting the token.*

5. To configure the appearance of your digital signature, click the **Appearance** drop-down list.
6. Once you have selected and configured your digital certificate, click **Sign**.



7. Specify the location where the signed document will be saved, and then click **Save**.

8. Wait until the process is finished. Once the document has been successfully saved, the signed PDF document will be shown together with the digital signature.



6.10. Using certificates in Windows® Logon

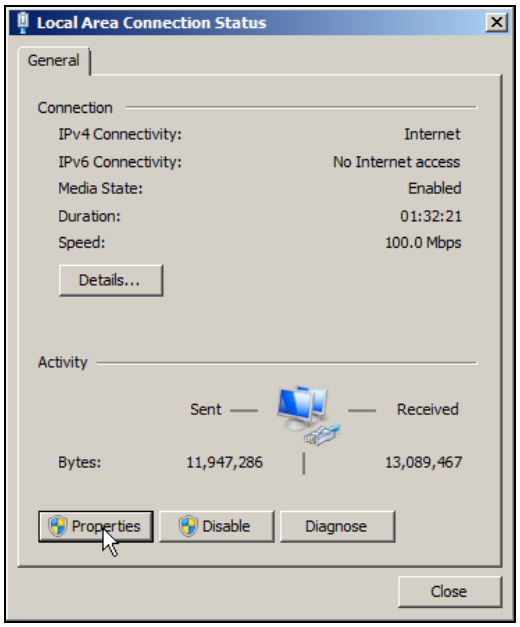
Before using your token for domain logon, you should first configure your connection to a particular domain (e.g., your company domain). This domain server must be configured to issue digital certificates.

The next sections will show the steps in logging in to a domain using a certificate in a token.

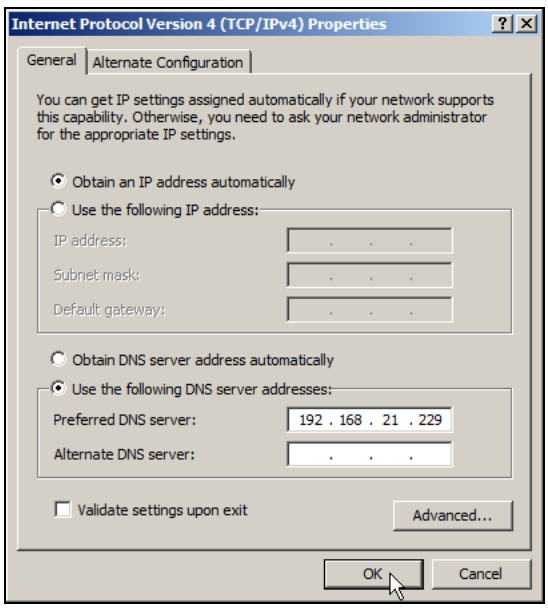
6.10.1. Connecting to a domain

To configure your computer to connect to a domain logon:

1. Go to your **Local Area Connection**, and then click **Properties**.

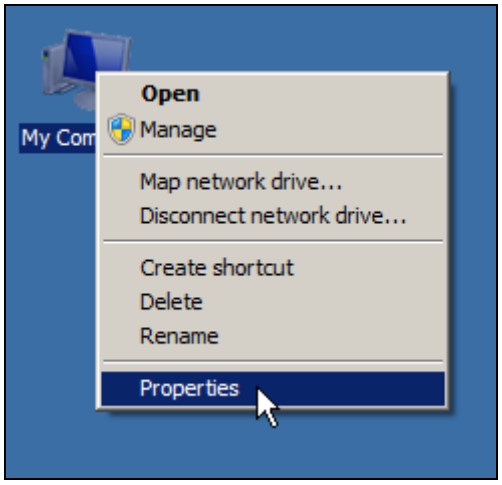


2. In the list of connections, select **Internet Protocol TCP/IP**, and then click **Properties**.
3. In the **General** tab, select **Use the following DNS server addresses**. Type in the IP address of your DNS server, and then click **OK**.

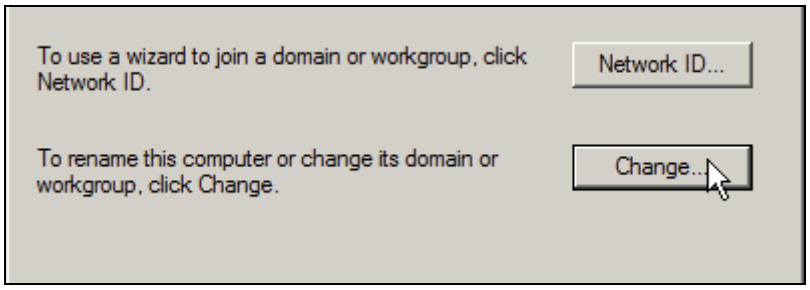


Note: *To know the IP address of your DNS server, contact your Network Administrator.*

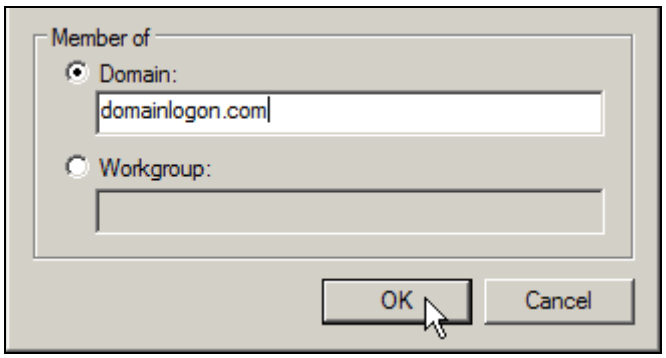
4. Once you have configured your DNS server, right-click on **My Computer**, and then click **Properties**.



5. The **System** window will appear. Under the **Computer name, domain, and workgroup settings**, click **Change settings**.
6. Under the **Computer Name** tab, click **Change**.



7. Under **Member of**, select **Domain**, and then type in the domain name of your DNS server.



Note: *To know the domain name of your DNS server, contact your Network Administrator.*

8. Type in the username and password of the domain when prompted.
9. Once successful, your computer will perform a restart.

6.10.2. Logging in to Windows using a token

1. Once you have successfully joined a domain, you will notice a difference in your Welcome screen.
2. Connect your token.

   Note: *Make sure that it has a certificate stored in it that has been requested from MMC/Active Directory.*
3. Click the smart card reader icon in the Welcome screen.
4. Type in your token PIN to log in.

6.11. Using certificates in Windows® WIFI EAP-TLS

The Extensible Authentication Protocol Transport Layer Security (EAP-TLS) is a protocol for wireless networks used when connecting a computer to the Internet. EAP-TLS authentication method is enabled for Windows® operating systems to support multiple authentication mechanisms, such as token cards, smart cards, certificates, one-time passwords, and public key encryption authentication.

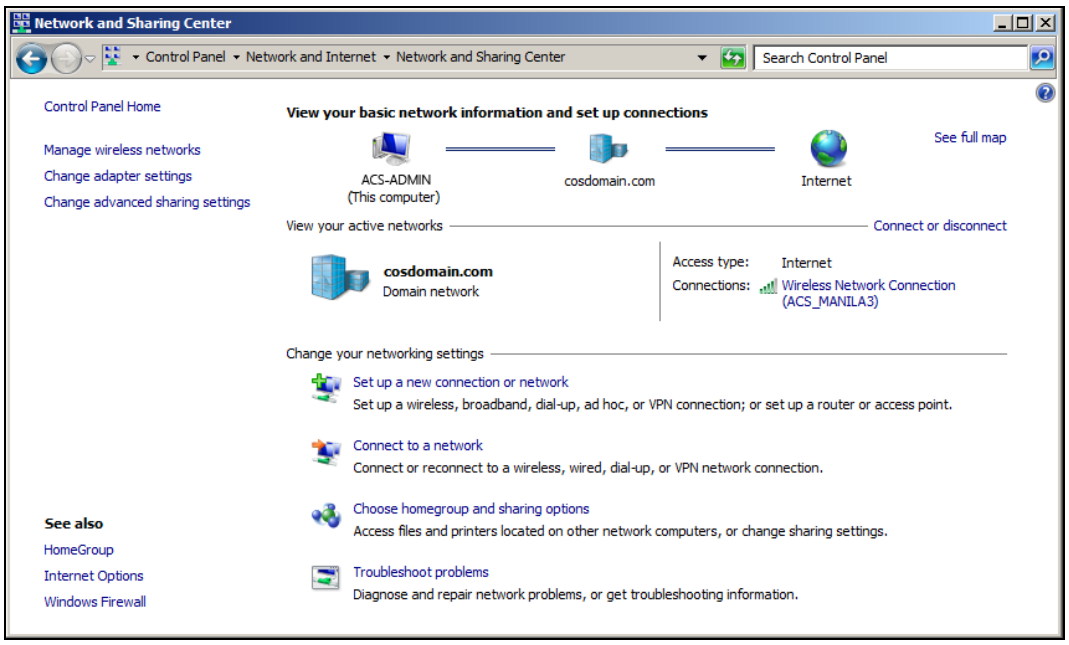
Notes:

1. *Make sure that a token with a valid certificate is connected in your system (see **Connecting to a domain**).*
2. *Contact your network administrator for the Wireless Access Point (WAP) with smart card security.*

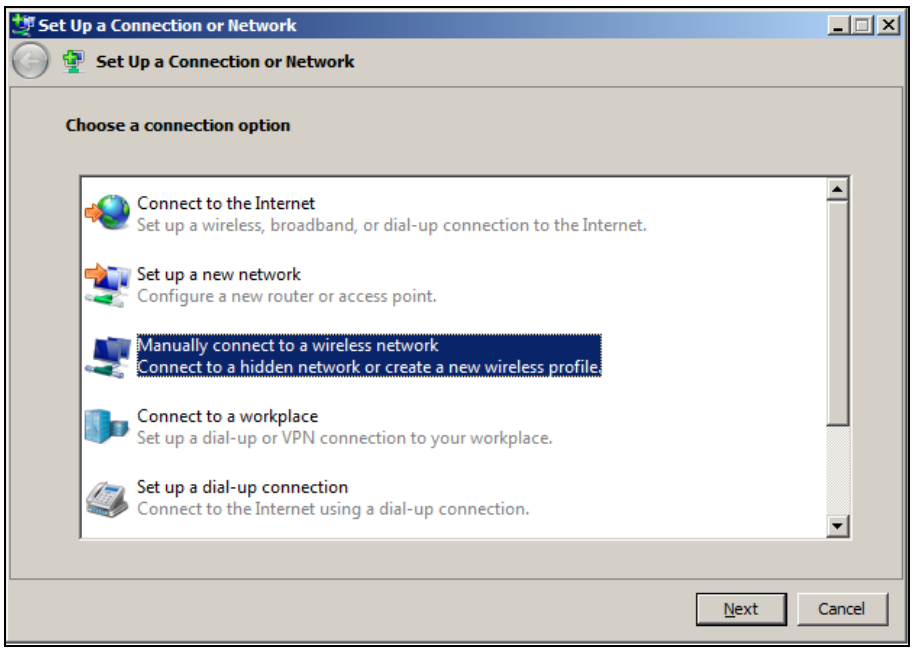
6.11.1. Setting a Wireless Access Point

To configure smart card–enabled WAP:

1. Click the **Start** menu.
2. Go to **Control Panel** | **Network and Internet** | **Network and Sharing Center**.
3. Select **Setup a new connection or network**.

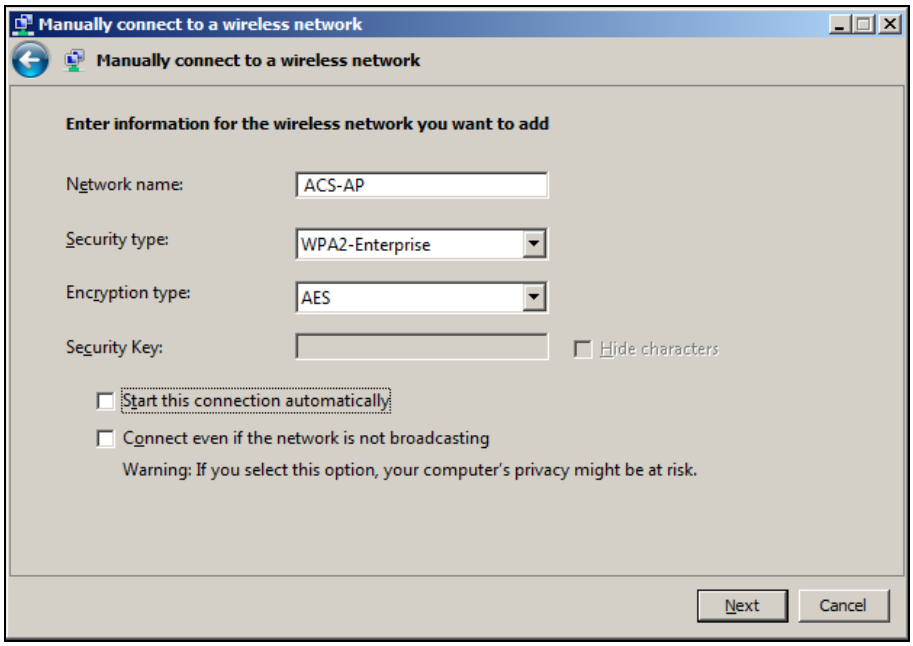


4. Choose **Manually connect to a wireless network**, and then click **Next**.



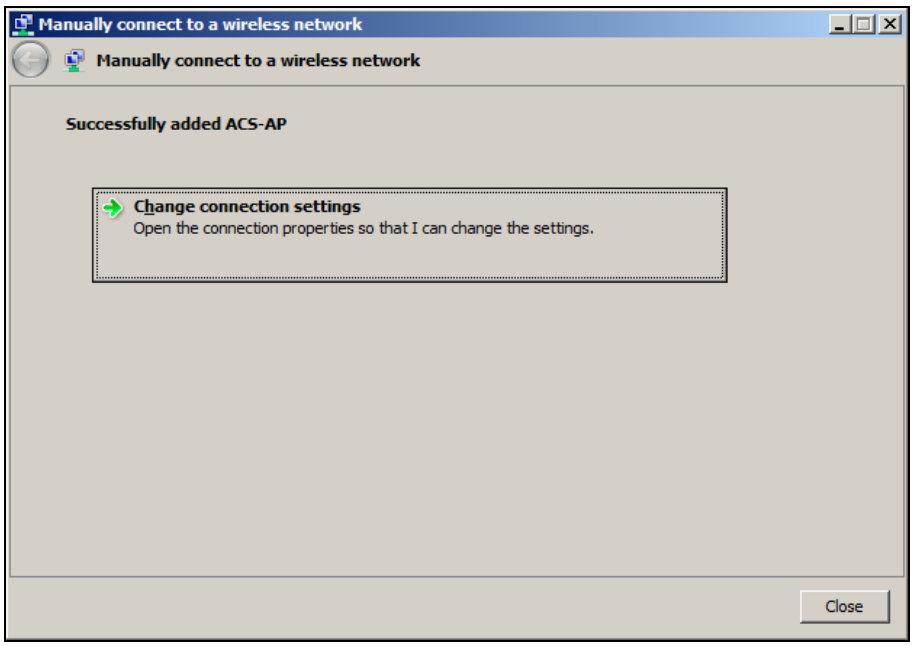
5. Wireless network settings will appear. Type in the following details for each configuration:

   Note: *Contact your network administrator for the specified settings for this configuration.*

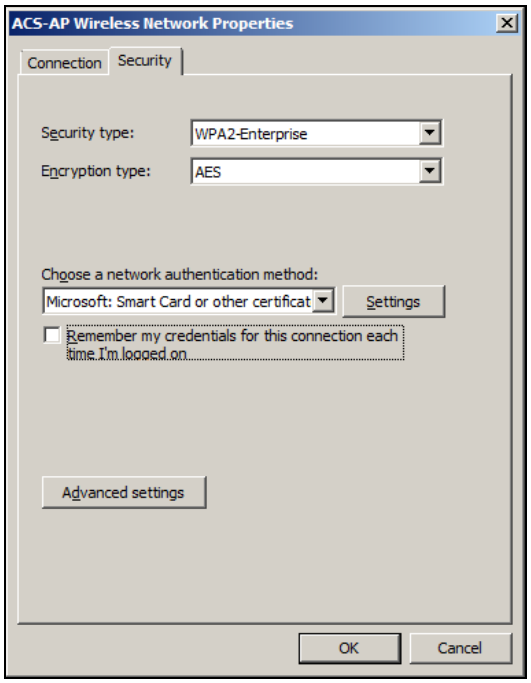


6. Click **Next**.

7. A prompt will show for the successfully added access point. Click **Change connection settings**.



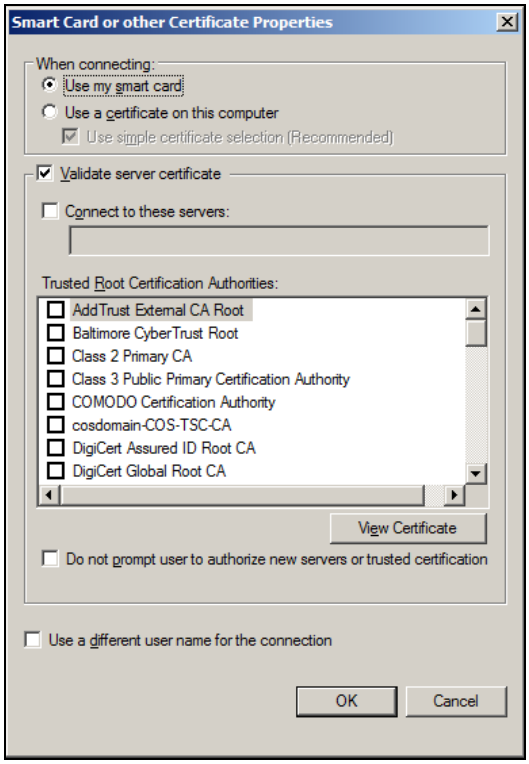
8. Your WAP network properties will appear. Go to **Security** tab.
9. Under **Choose a network authentication method**, select **Microsoft: Smart Card or other certificate**.



Note: *Clear the* ***Remember my credentials for this connection each time I'm logged on*** *option for security.*

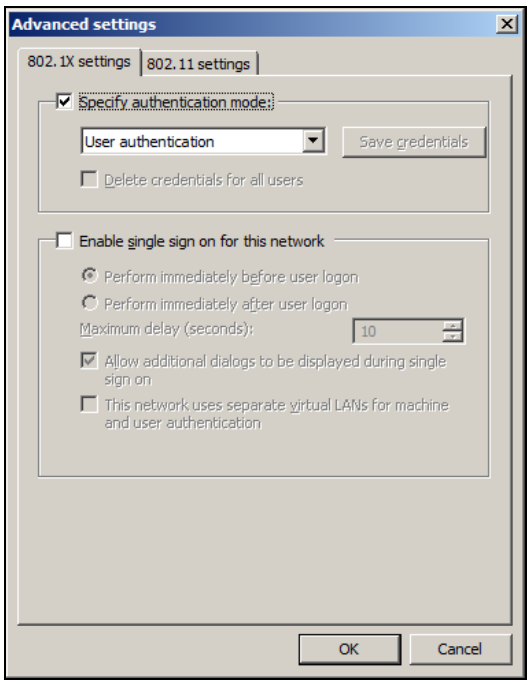
10. Click **Settings**.

11. **Smart Card or other Certificate Properties** will appear. Select the option **Use my smart card**, and then click **OK**.

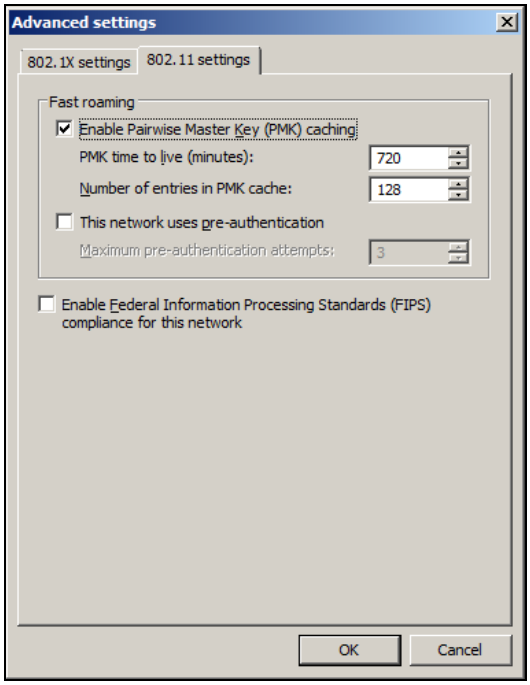


12. Click **Advanced Settings**.

13. Under **802.1X settings** tab, select **Specify authentication mode**, and then choose **User Authentication** in the drop-down list.



14. Under **802.11 settings** tab, select **Enable Pairwise Master Key (PMK) caching**.



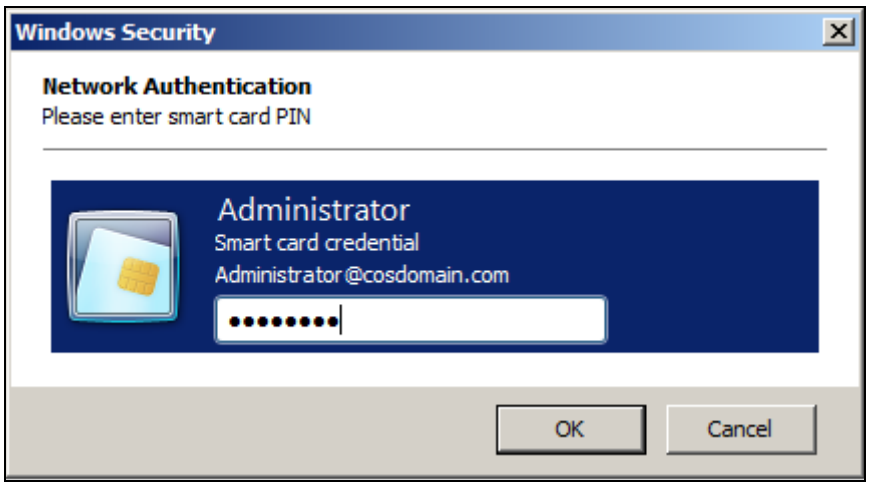
15. Click **OK** to save configuration.

6.11.2. Connecting to a WAP using a token

1. Run the **ACSCMU** application.
2. Connect your token and log in.

   Note: *Make sure that it has a certificate stored in it that has been requested from MMC/Active Directory.*
3. On the task bar, open **Wireless Network Connection** and select the access point.

4. Click **Connect**.
5. Type in your token PIN, and then click **OK**.



6.12. Certificate Chains

6.12.1. Certificate chains in Mozilla Firefox/Thunderbird

Mozilla Firefox/Thunderbird has its own certificate repository where certificate and certificate chains are located. When viewing a certificate in the Certificate Manager, sometimes the error message "**Could not verify this certificate for unknown reasons**" is displayed. Below is a sample of the error message:

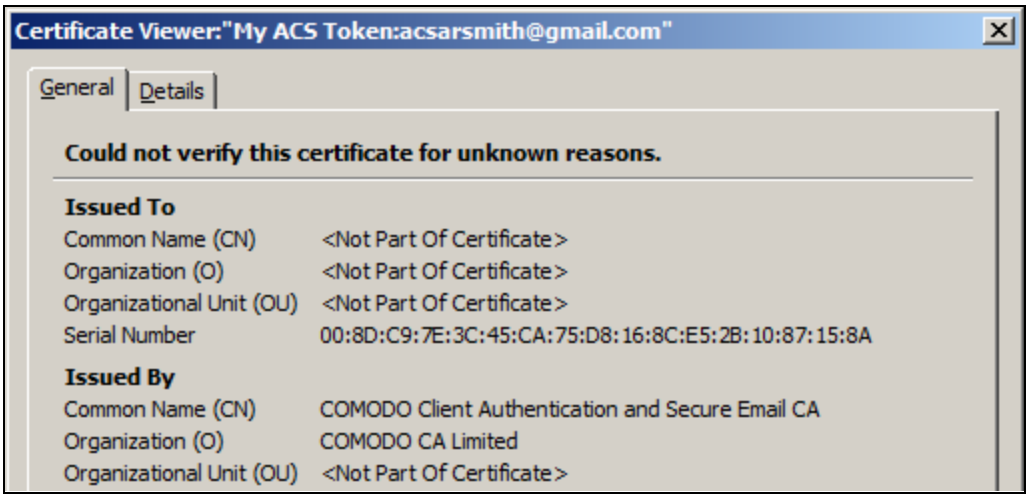
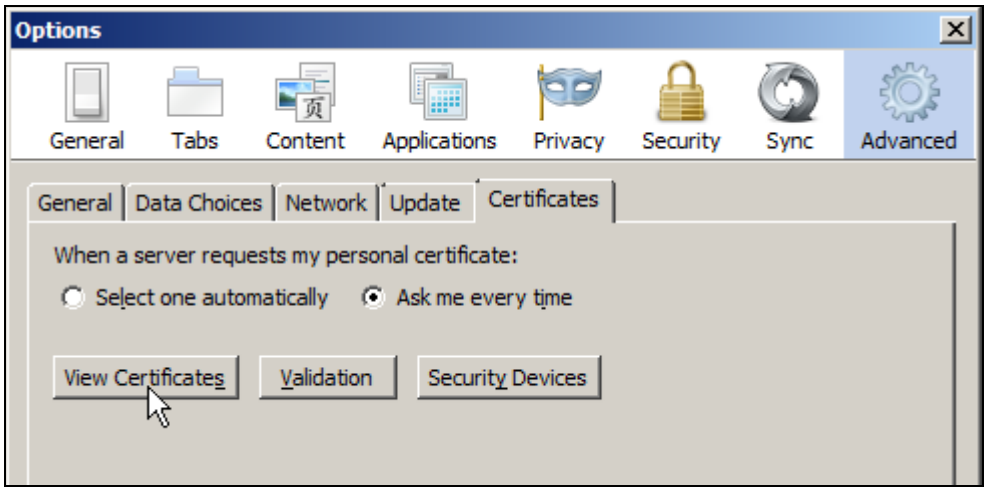


Figure 4: Unverified Certificate Error Message

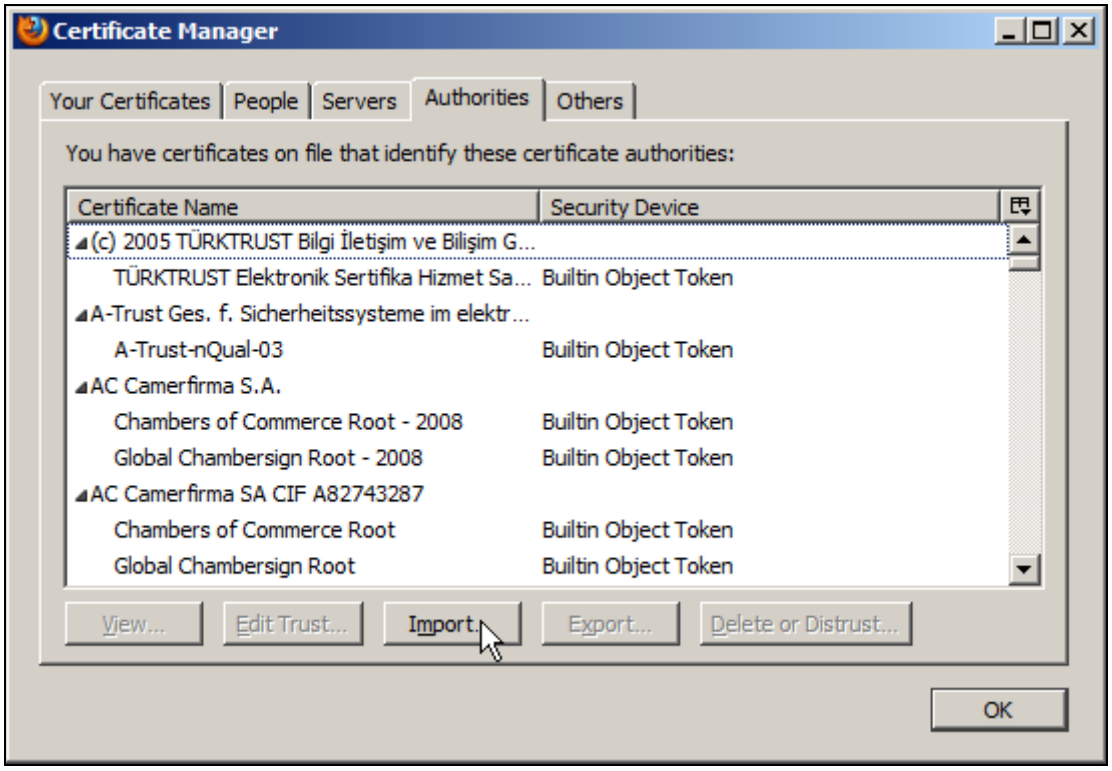
To fix this problem, you need to manually install the missing certificate file (*.cer) to Mozilla Firefox/Thunderbird.

To manually install a certificate to Mozilla Firefox:

1. In the **Tools** menu, click **Options**.
2. Click **Advanced**. Under the **Certificates** tab, click **View Certificates**.



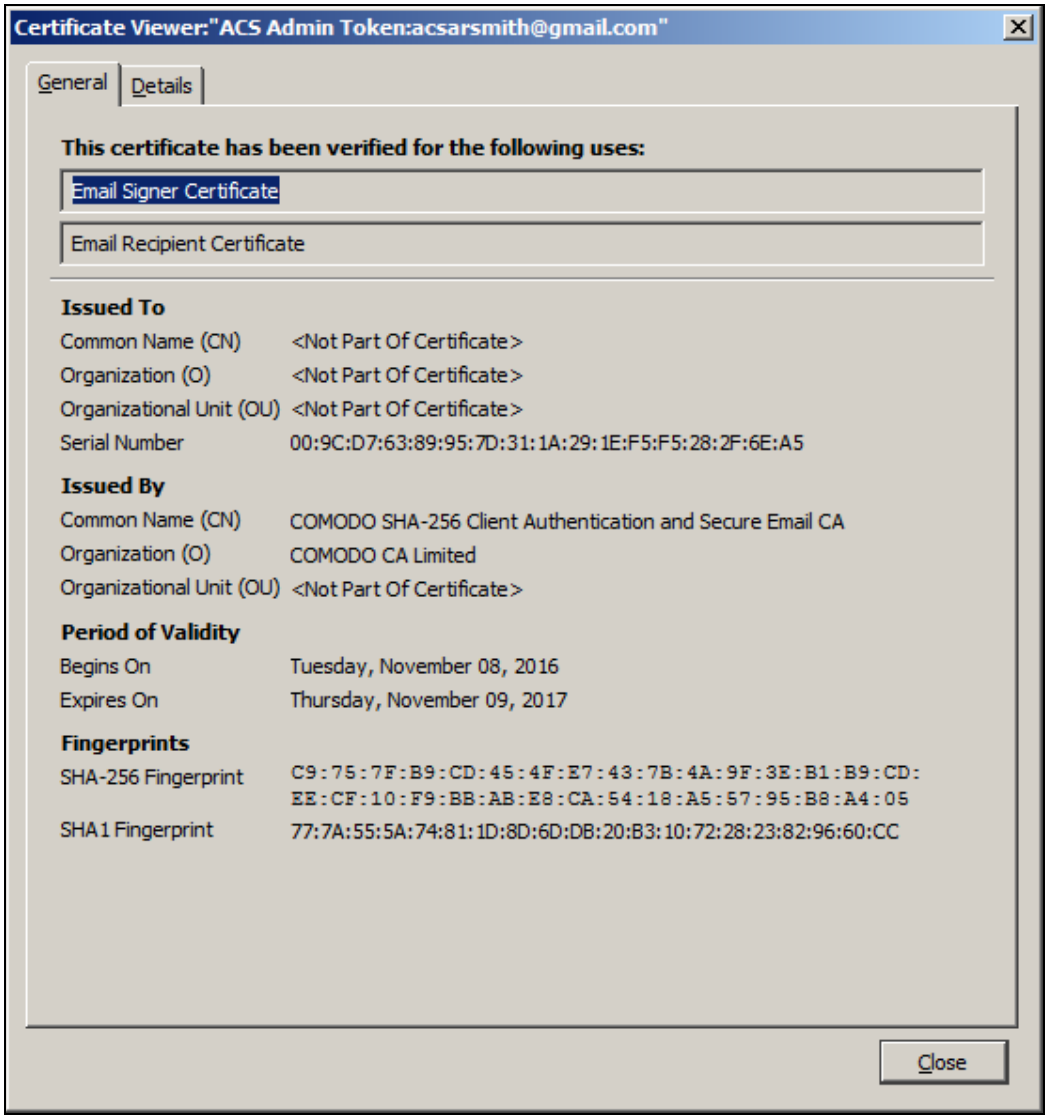
3. The Certificate Manager will open. Under the **Authorities** tab, click **Import**.



4. Locate and select the missing certificate file (*.cer), and then click **Open**.
5. You will be asked for the Trust settings of the newly-loaded certificate file. Check all the options for Trust purposes, and then click **OK**.

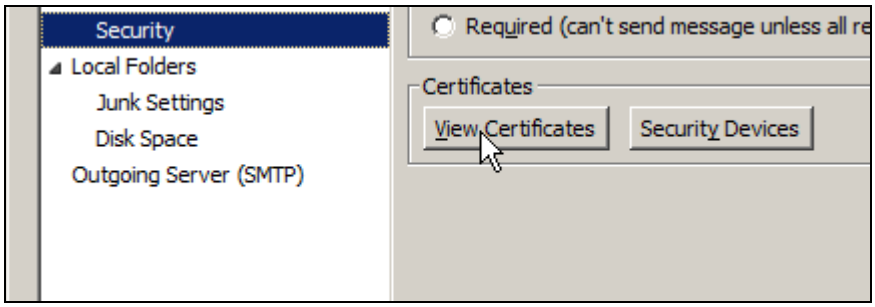
6. Go to **Your Certificates** tab, and then click **View**.

7. Under the **General** tab, it should show that the certificate has been verified for use.

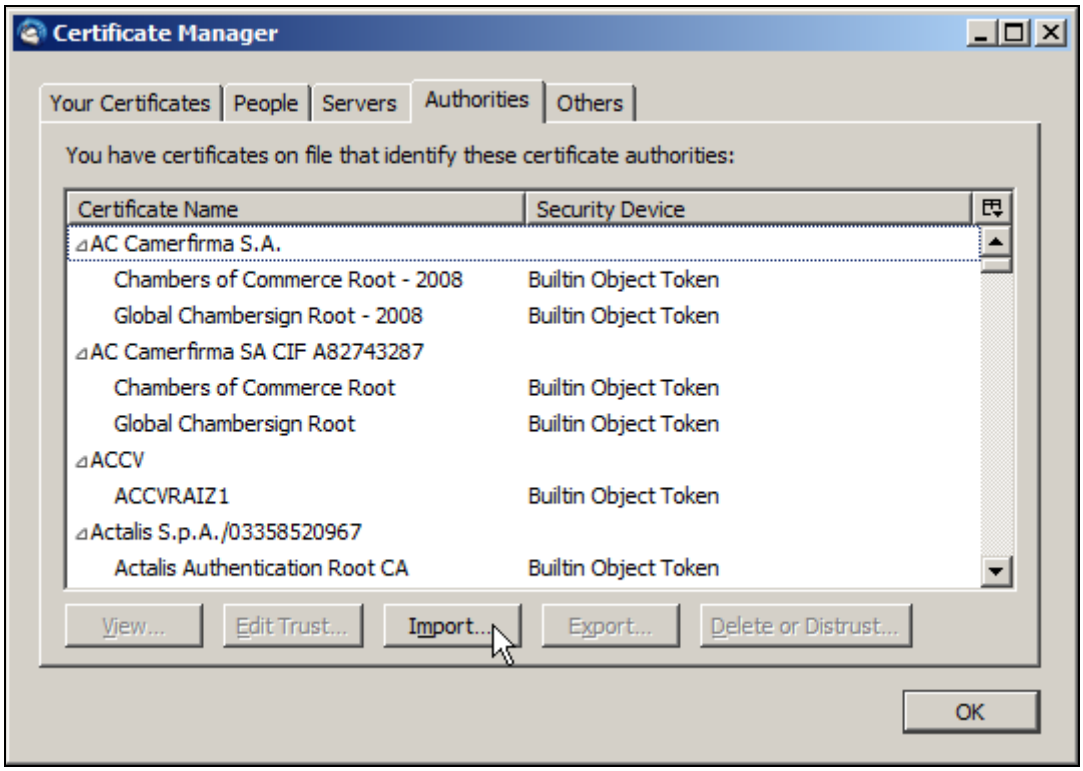


To manually install a certificate to Mozilla Thunderbird:

1. Click the **Menu** button , point to **Options**, and then click **Account Settings**.
2. In the **Account Settings** window, click **Security** in the left side of the panel.
3. Under Certificates, click **View Certificates**.



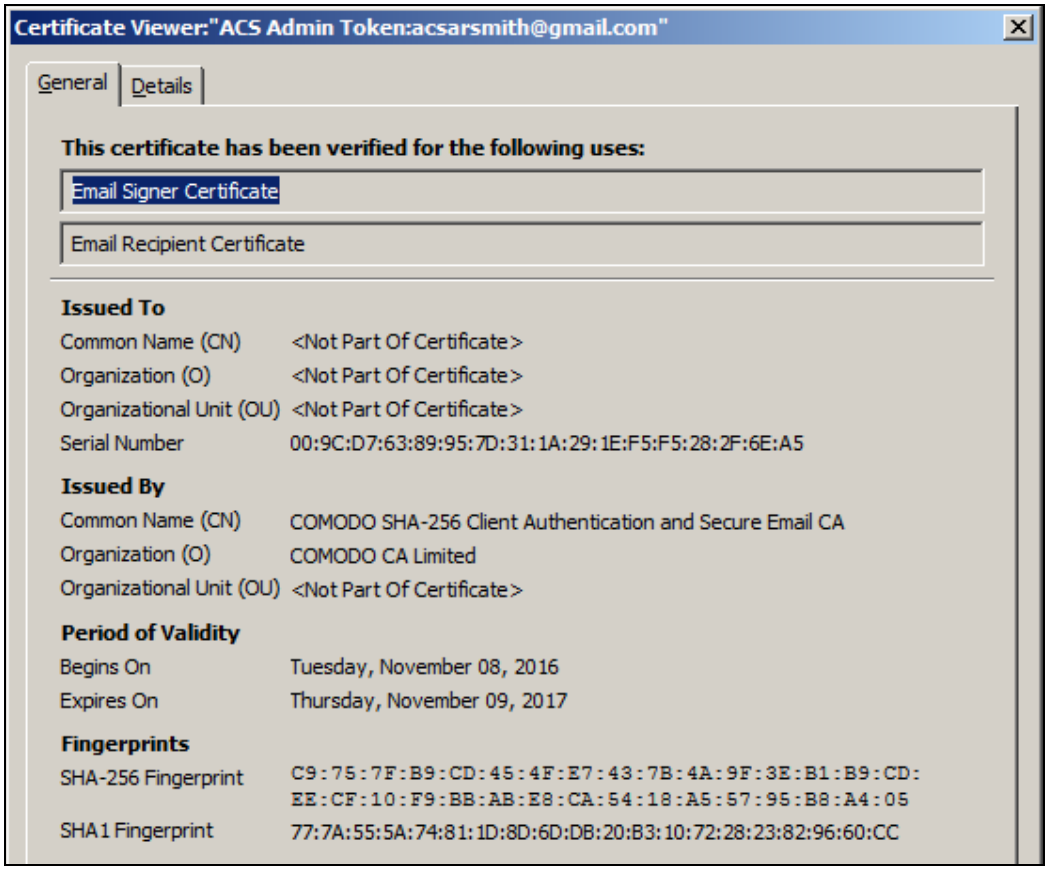
4. The Certificate Manager will open. Under **Authorities** tab, click **Import**.



5. Locate and select the missing certificate file (*.cer), and then click **Open**.

6. You will be asked for the Trust settings of the newly-loaded certificate file. Check all the options for Trust purposes, and then click **OK**.

7. Go to **Your Certificates** tab, and then click **View**.
8. Under the **General** tab, it should show that the certificate has been verified for use.



7.0. Troubleshooting Guide

7.1. Upgrading from earlier versions

To properly install the ACOS5-CryptoMate Client Kit, all the registry settings must first be cleared from your computer. To do this:

1. Uninstall any previous versions of the package from your computer.
   a. Go to **Control Panel**, and then click **Programs and Features**.
   b. Select the previous version of the client kit, and then click **Uninstall**.

7.2. Allowing PKCS logs to be recorded

This setup permits the ACS middleware to access your system to record your PKCS logs. To do this:

1. For Windows® 7 and Windows® 8 users, set your **User Account Control (UAC)** to **Very Low**.
   a. Go to **Control Panel**, and then click **User Accounts**.
   b. Click **Change User Account Control settings**.
   c. Set the notification control to **Never notify**, and then click **OK**.
2. Restart your computer for the changes to take effect.