BRITISH COLUMBIA

Office of the Chief Information Officer

Digital Certificate Service (DCS) - User Guide

Information Security Branch

Security Classification: **Medium Sensitivity**

Contents

Using this Guide

This Digital Certificate Service (DCS) guide provides a reference for individuals assigned a DCS ID.

DCS account creation and management is performed by individuals assigned the role of DCS Local Registration Authority, commonly referred to as DCS LRAs. DCS LRAs follow established procedures to create, modify, deactivate or reactivate accounts as well as perform other administrative functions.

DCS users should contact their LRA when additional assistance is required or check the DCS website.

User Requirements

- An approved DCS Token, such as a SafeNet 5100 or 5110 eToken
- Entrust Entelligence and SafeNet software installed on their computer
- An active DCS Account within their Ministry or Organization

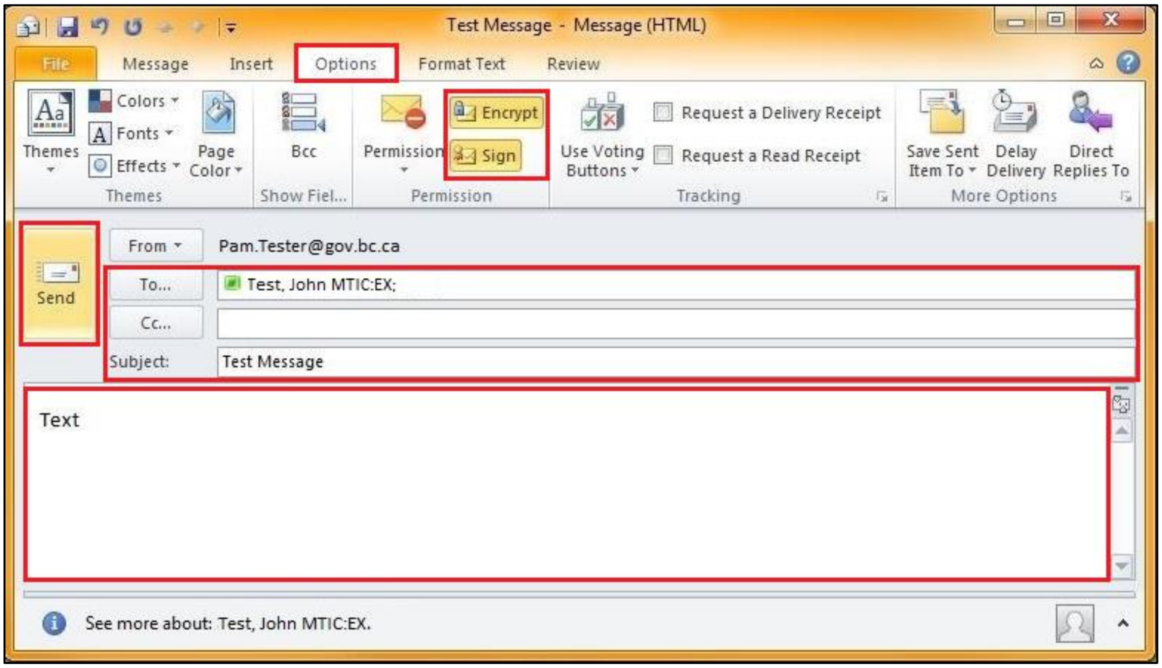
Secure E-mail Messaging

Send a Secure E-mail Message

The user completes the following steps to send a secure e-mail message:

1. Ensure the Token is inserted into a USB port.
2. From Microsoft Outlook>Home tab, in the **New** group, click **New E-mail**.

   An e-mail Message (HTML) window displays:



Test Message - Message (HTML)

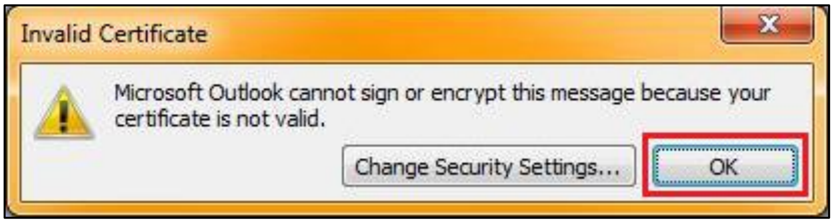
From: Pam.Tester@gov.bc.ca
To...: Test, John MTIC:EX;
Cc...:
Subject: Test Message

Text

See more about: Test, John MTIC:EX.

3. Type recipient addresses, Subject and message text.
4. Select **Options.**
5. In the Permission group, click one or both of:
   - **Encrypt** to prevent unauthorized people from reading the e-mail
   - **Sign** to digitally sign an e-mail so that other people can be sure who it came from
6. Click **Send**.

- If the Token is not inserted, the Invalid Certificate dialog box displays:

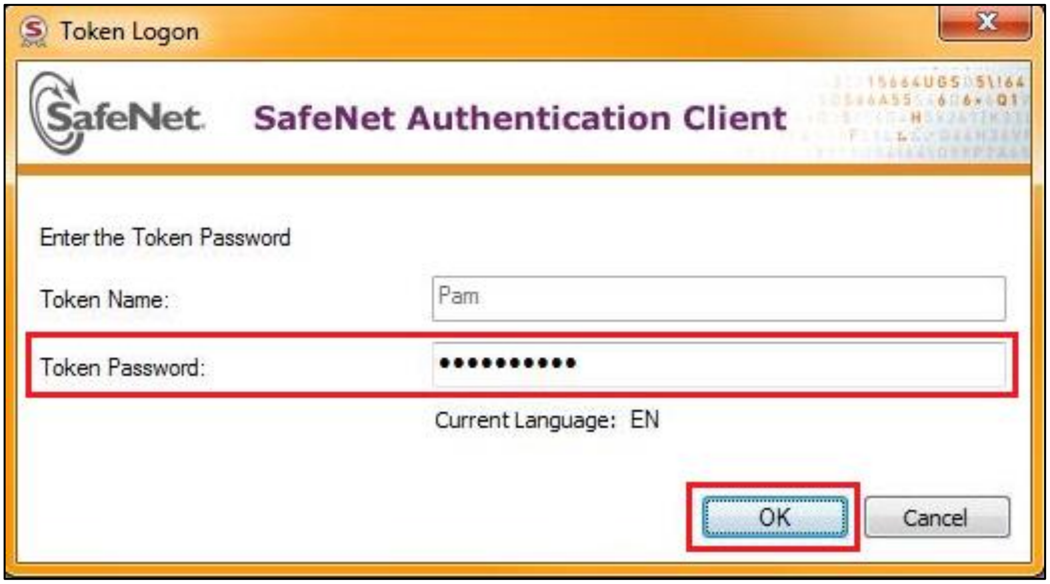


Invalid Certificate

Microsoft Outlook cannot sign or encrypt this message because your certificate is not valid.

Click **OK** to close the dialog box and return to the e-mail message. Insert the Token and click **Send** again.

- If sending a secure message for the first time since inserting the Token, the Token Logon dialog box displays showing the Token Name:



Token Logon

SafeNet Authentication Client

Enter the Token Password

Token Name: Pam

Token Password: ●●●●●●●●●●

Current Language: EN

Enter the Token Password and click **OK** to close the dialog box and return to the **Home** tab.

The message will appear in the Sent folder.

7. Continue to send messages as needed without logging on again.

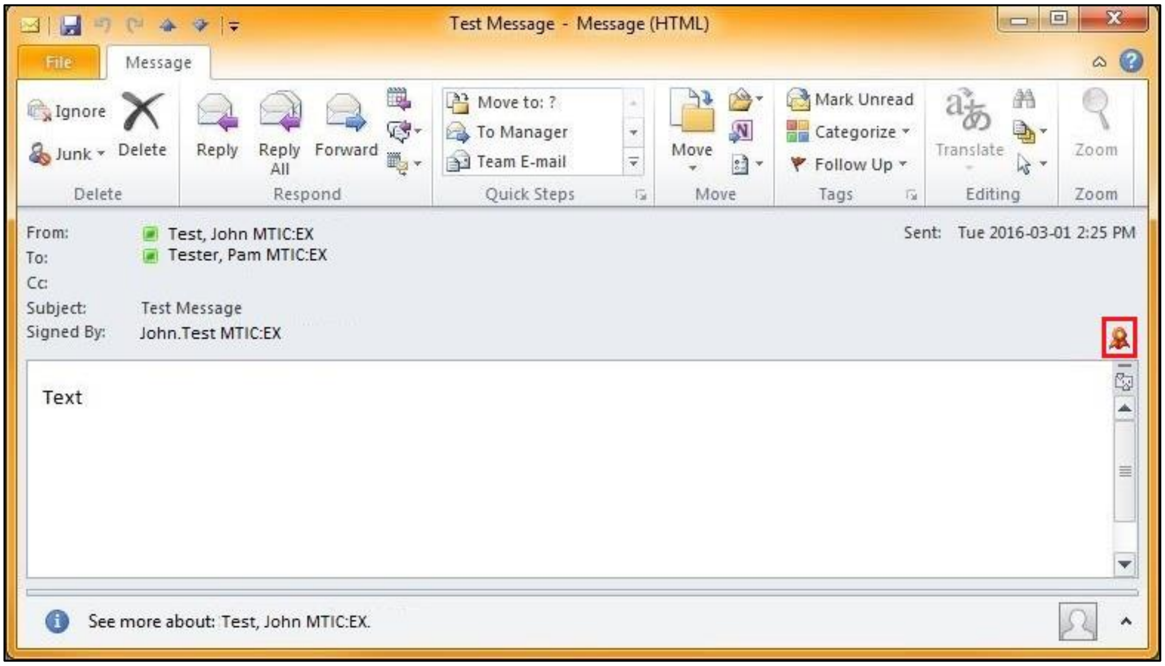
Note: After a specified period of inactivity (currently set to 12 hours), the secure session is logged off.

Receive a Secure E-mail Message (Verify a Digitally Signed E-mail)

The user completes the following steps to receive a secure e-mail message (Token is not required):

1. From the Microsoft Outlook tabs, select **Home** (selected by default).
2. In the left navigation, select **Inbox** (selected by default).
3. In the message list, double-click the e-mail to be verified.

   The e-mail Message (HTML) window displays with an icon indicating that the e-mail is digitally signed:



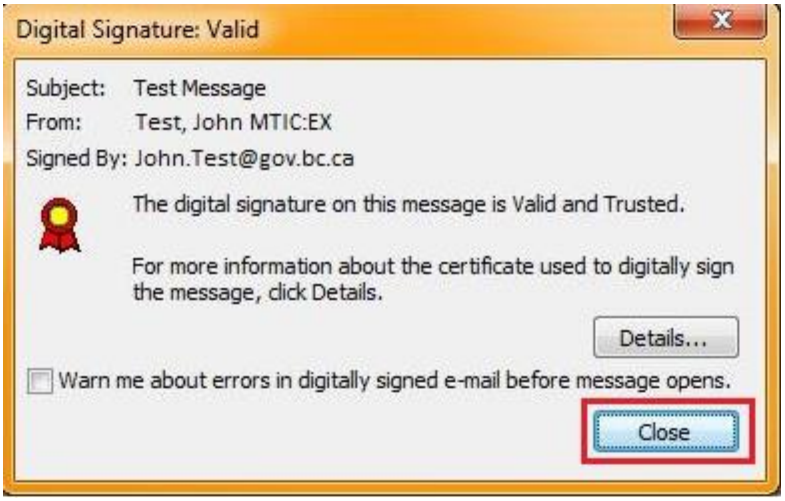
From: Test, John MTIC:EX
To: Tester, Pam MTIC:EX
Cc:
Subject: Test Message
Signed By: John.Test MTIC:EX
Sent: Tue 2016-03-01 2:25 PM

Text

See more about: Test, John MTIC:EX.

4. Click the **Digital signature is trusted** icon.

The Digital Signature: Valid window displays:



Digital Signature: Valid

Subject: Test Message
From: Test, John MTIC:EX
Signed By: John.Test@gov.bc.ca

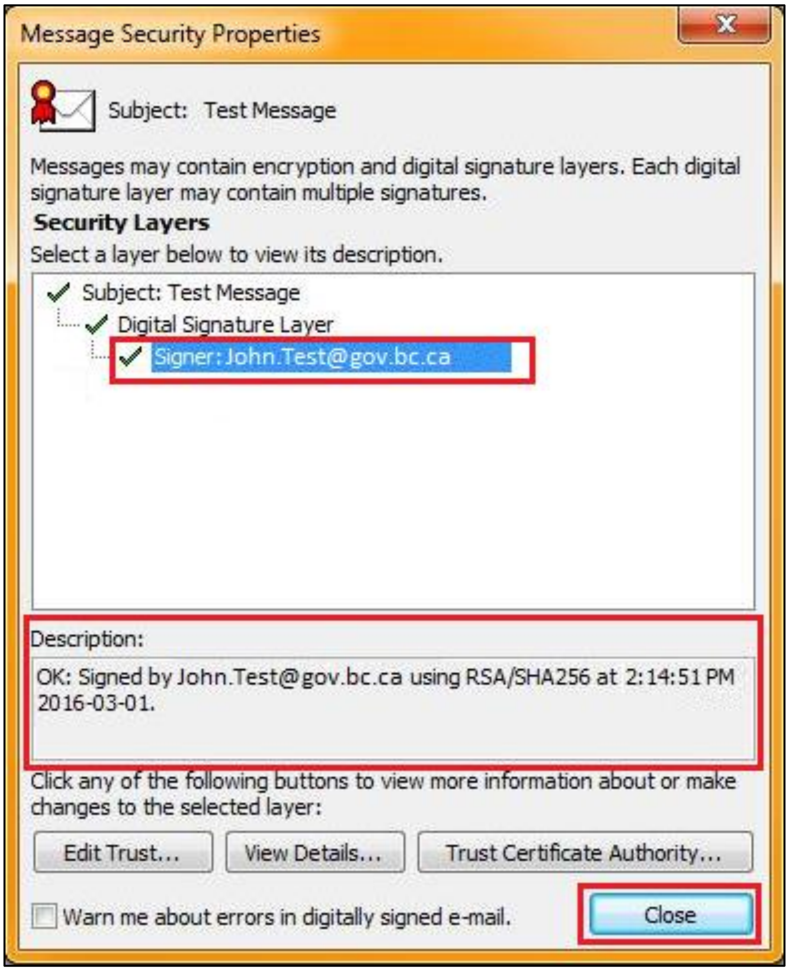
The digital signature on this message is Valid and Trusted.

For more information about the certificate used to digitally sign the message, click Details.

□ Warn me about errors in digitally signed e-mail before message opens.

5. Click **Details** to see details of the certificate used to sign the message.

The Message Security Properties window displays:



Message Security Properties

Subject: Test Message

Messages may contain encryption and digital signature layers. Each digital signature layer may contain multiple signatures.

Security Layers

Select a layer below to view its description.

✓ Subject: Test Message
✓ Digital Signature Layer
✓ Signer: John.Test@gov.bc.ca

Description:

OK: Signed by John.Test@gov.bc.ca using RSA/SHA256 at 2:14:51 PM 2016-03-01.

Click any of the following buttons to view more information about or make changes to the selected layer:

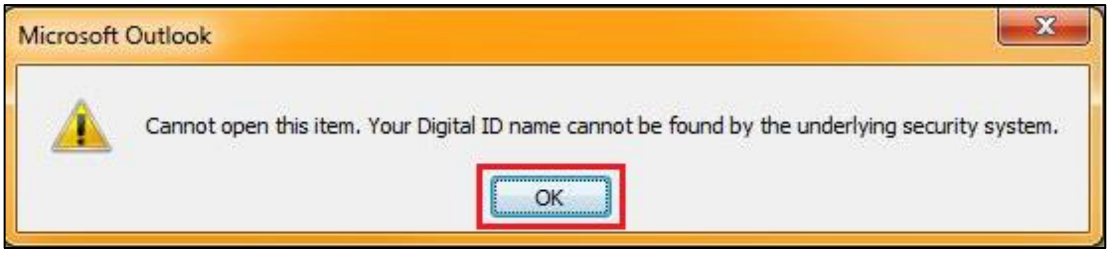
Edit Trust...
View Details...
Trust Certificate Authority...
□ Warn me about errors in digitally signed e-mail.
Close

6. From the Digital Signature Layer, select **Signer** to see the signature details.
7. Click **Close** to close the dialog and return to the e-mail.

Receive a Secure E-mail message (Decrypt an E-mail)

The user completes the following steps to decrypt an e-mail:

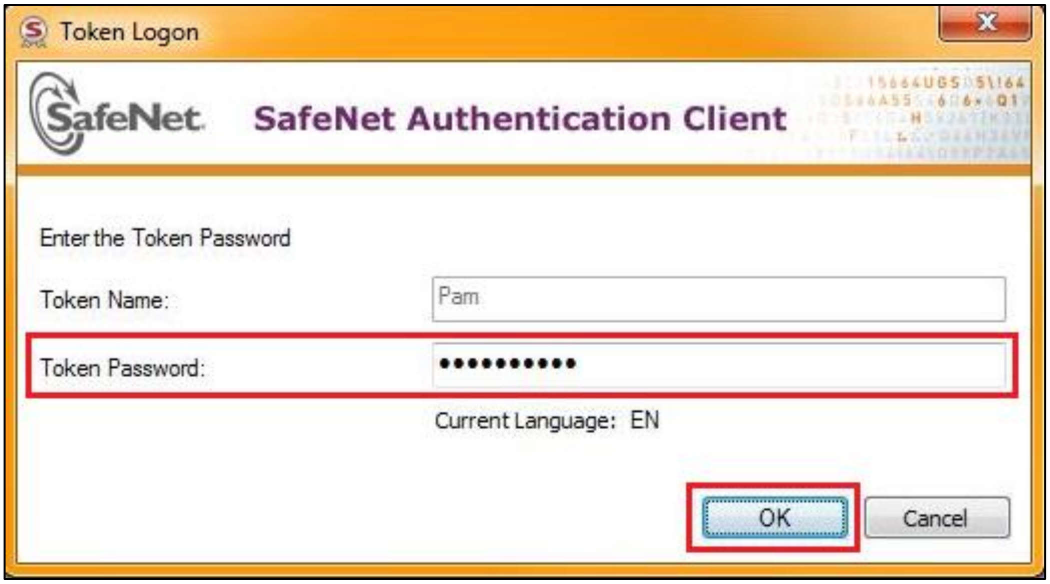
1. Ensure the Token is inserted into a USB port.
2. From the Microsoft Outlook tabs, select **Home** (selected by default).
3. In the left navigation, select **Inbox** (selected by default).
4. In the message list, double-click the e-mail to be decrypted.
   - If the Token is not inserted, a Microsoft information message appears:


Microsoft Outlook

Cannot open this item. Your Digital ID name cannot be found by the underlying security system.

Click **OK** to close the dialog box and return to the message list. Insert Token in a USB port.

   - If decrypting a secure message for the first time since inserting the Token, the Token Logon dialog box displays showing the Token Name:


Token Logon

SafeNet Authentication Client

Enter the Token Password

Token Name: Pam

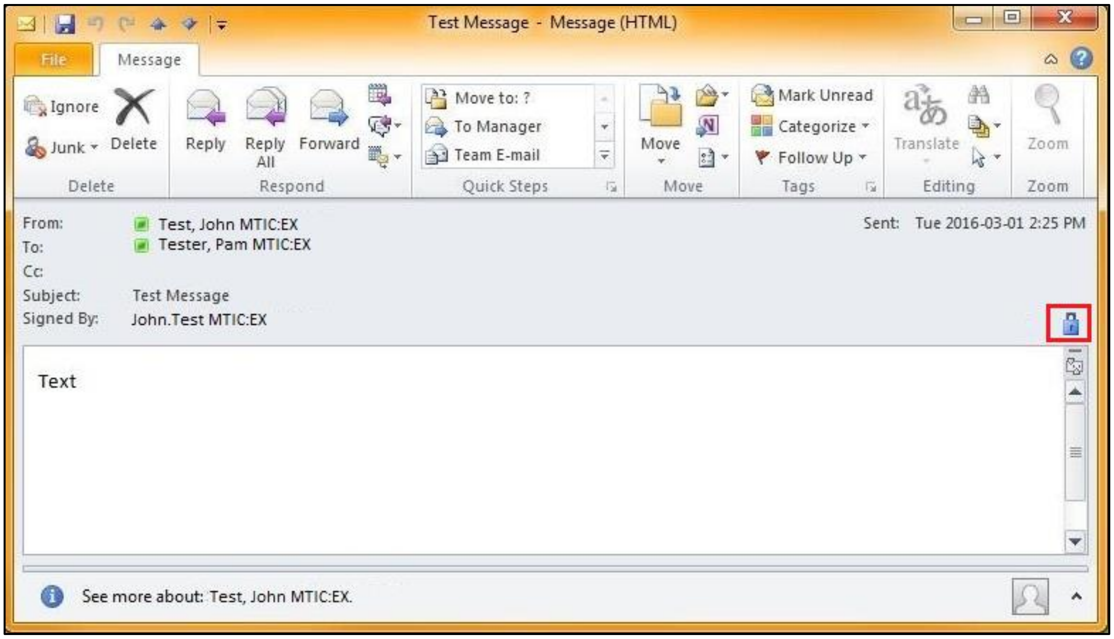
Token Password: ••••••••••

Current Language: EN

Enter the Token Password and click **OK** to close the dialog box and return to the **Home** tab.

In the message list, double-click the e-mail to be decrypted.

The e-mail Message (HTML) window displays with an icon indicating that the e-mail is encrypted:



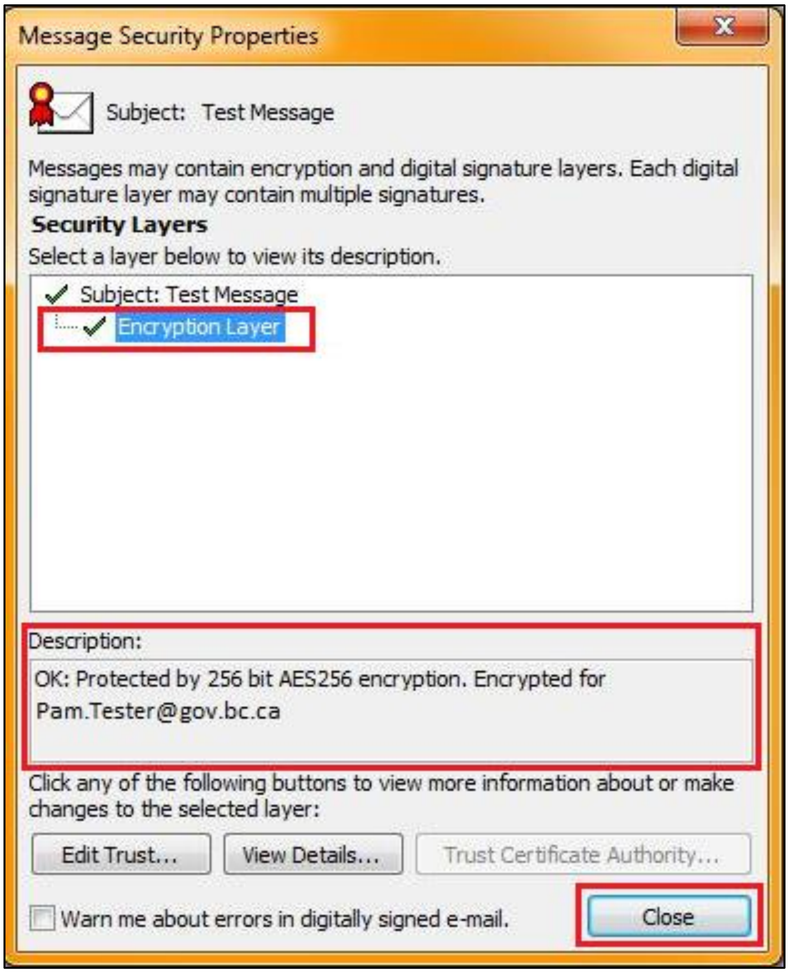
From: Test, John MTIC:EX
To: Tester, Pam MTIC:EX
Cc:
Subject: Test Message
Signed By: John.Test MTIC:EX
Sent: Tue 2016-03-01 2:25 PM

Text

See more about: Test, John MTIC:EX.

5. Click the icon.

The Message Security Properties window displays:



Message Security Properties

Subject: Test Message

Messages may contain encryption and digital signature layers. Each digital signature layer may contain multiple signatures.

Security Layers

Select a layer below to view its description.

✓ Subject: Test Message
✓ Encryption Layer

Description:

OK: Protected by 256 bit AES256 encryption. Encrypted for Pam.Tester@gov.bc.ca

Click any of the following buttons to view more information about or make changes to the selected layer:

Edit Trust...
View Details...
Trust Certificate Authority...
☐ Warn me about errors in digitally signed e-mail.
Close

6. Select **Encryption Layer** to see the Encryption Layer details.
7. Click **Close** to close the window and return to the e-mail.

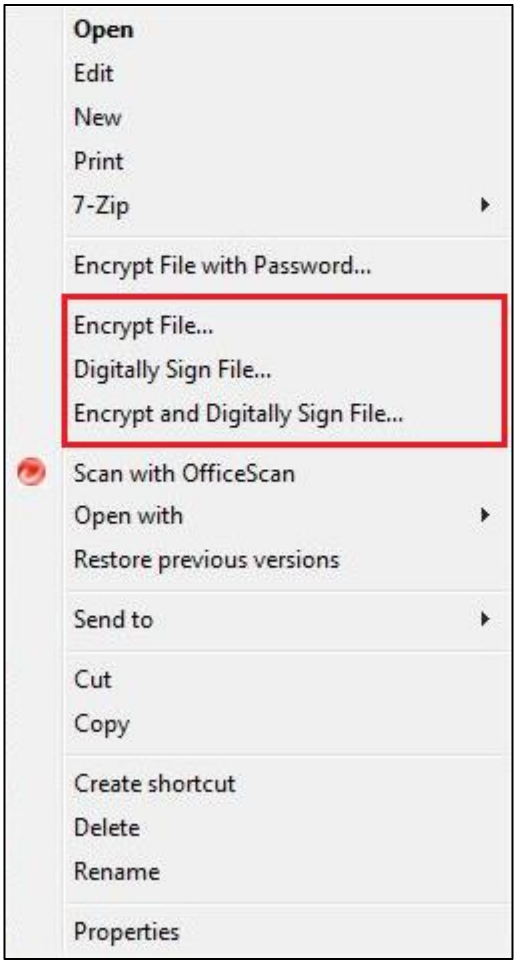
Secure Files in a Folder

Encrypt and Digitally Sign File(s)

The user completes the following steps to encrypt and digitally sign file(s) in a folder:

1. Ensure the Token is inserted into a USB port.
2. Navigate to the folder containing the file(s) to be secured.
3. Select the file(s) and right-click (multiple files may be selected at the same time).

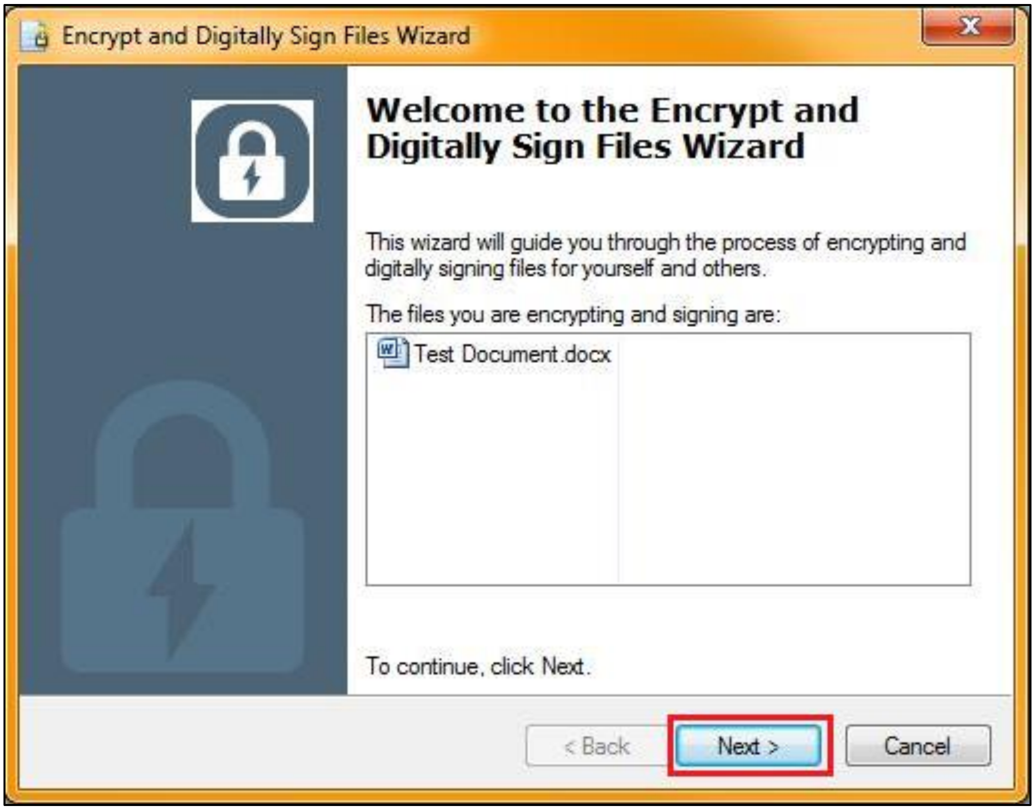
   A menu displays:



4. Select one of the following options:
   - Encrypt File… to prevent unauthorized people from reading the file
   - Digitally Sign File… to digitally sign a file so that other people can be sure who it came from

- Encrypt and Digitally Sign File… to prevent unauthorized people from reading the file and digitally sign the file so that other people can be sure who it came from

An Encrypt Files Wizard specific to the selected option opens, and the Welcome page lists the selected file(s):



Welcome to the Encrypt and Digitally Sign Files Wizard

This wizard will guide you through the process of encrypting and digitally signing files for yourself and others.

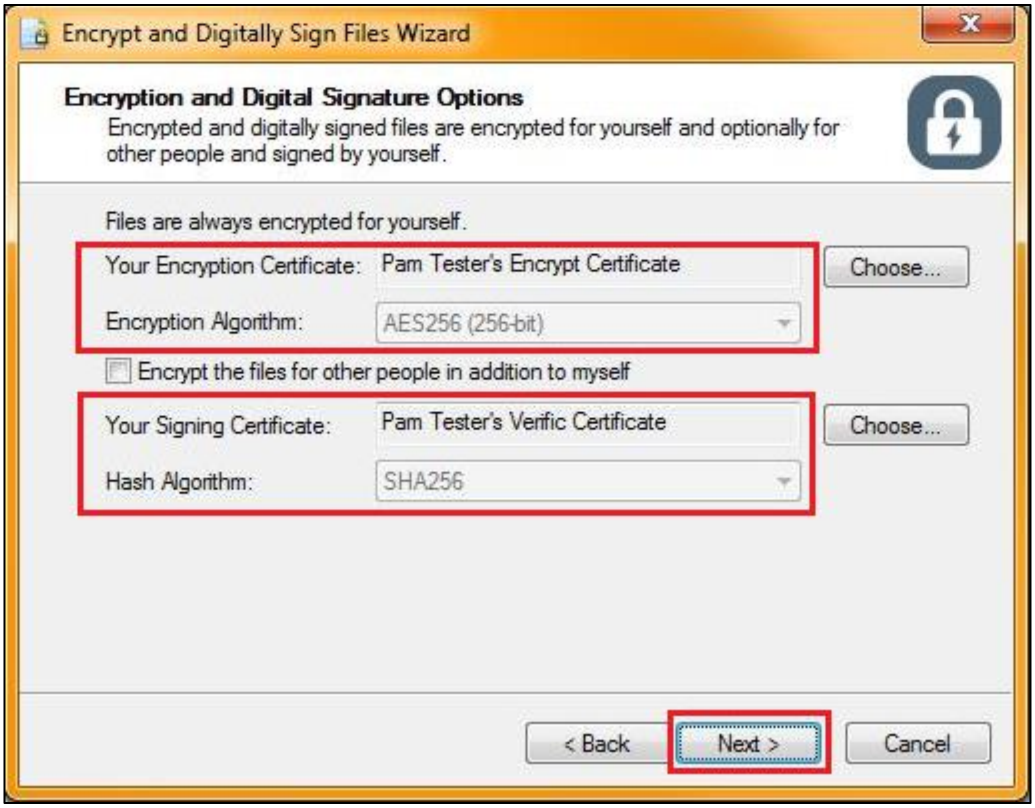
The files you are encrypting and signing are:

Test Document.docx

To continue, click Next.

5. Click **Next**.

The Encryption and Digital and Signature Options page displays showing the Encryption Certificate and/or Signing Certificates:


Encrypt and Digitally Sign Files Wizard

Encryption and Digital Signature Options

Encrypted and digitally signed files are encrypted for yourself and optionally for other people and signed by yourself.

Files are always encrypted for yourself.

Your Encryption Certificate: Pam Tester's Encrypt Certificate

Encryption Algorithm: AES256 (256-bit)

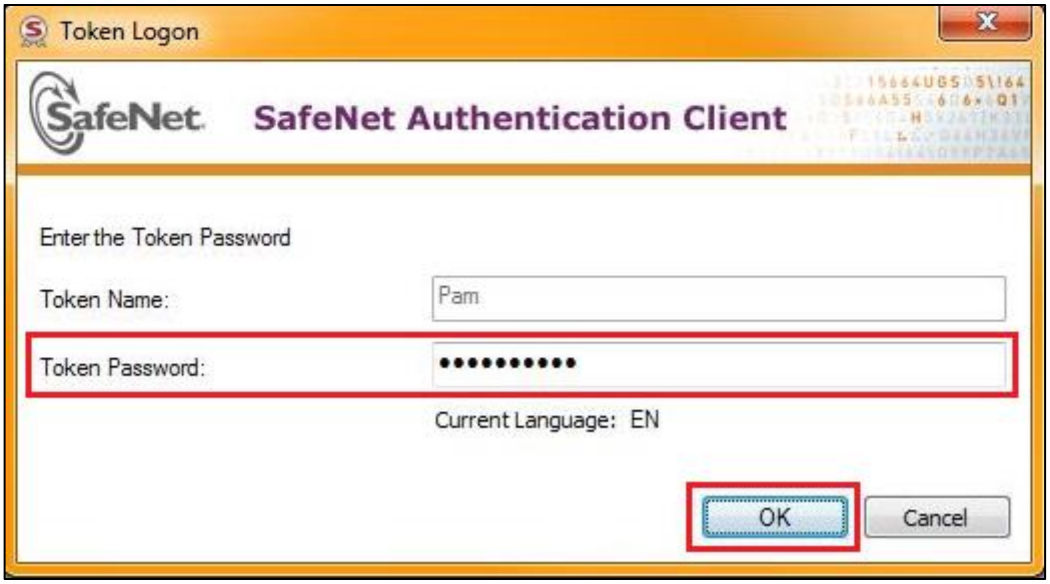
□ Encrypt the files for other people in addition to myself

Your Signing Certificate: Pam Tester's Verific Certificate

Hash Algorithm: SHA256

6. Click **Next**.
   - If the Token is not inserted, select **Cancel**, insert the Token and return to Step 3 to start the wizard again.

- ○ If securing a file for the first time since inserting the Token, the Token Logon dialog box displays showing the Token Name:



Enter the Token Password

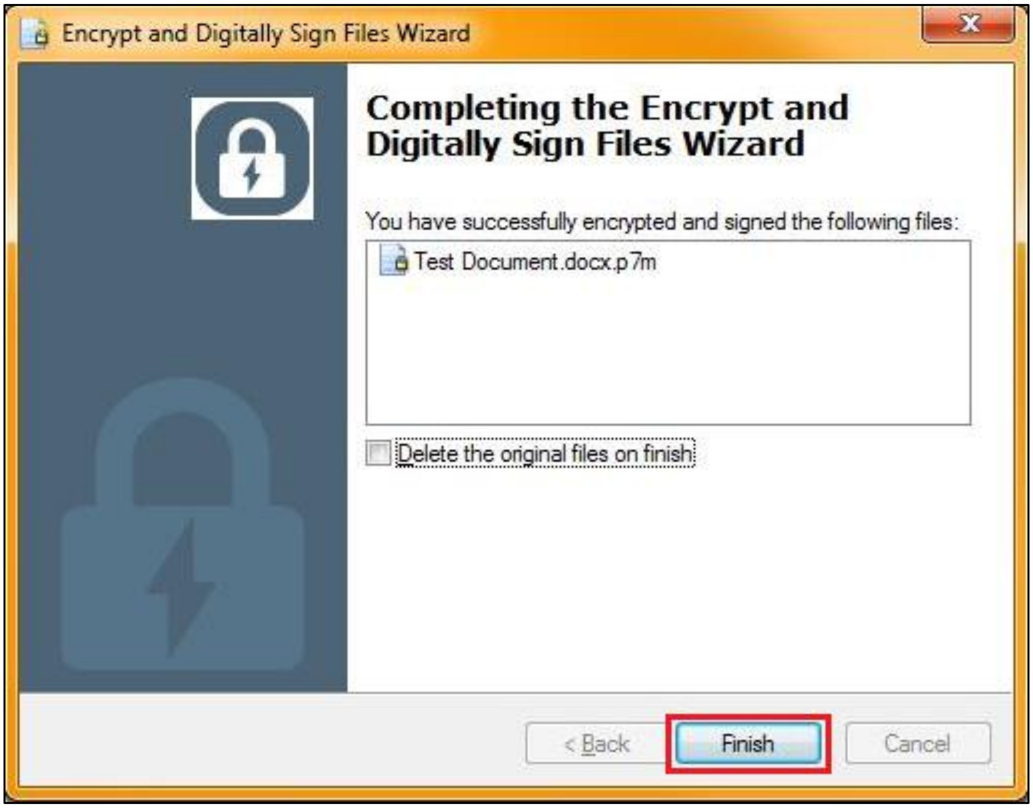
Token Name: Pam

Token Password: ●●●●●●●●●●●

Current Language: EN

Enter the Token Password and click **OK**.

The Completing the Wizard page displays with a success message and lists the secured file(s).
Note: The files have a .p7m extension indicating that they are secure.



Encrypt and Digitally Sign Files Wizard

Completing the Encrypt and Digitally Sign Files Wizard

You have successfully encrypted and signed the following files:

Test Document.docx.p7m

□ Delete the original files on finish

7. If shown, select the option: Delete the original files on finish, as needed.
8. Click **Finish** to exit the wizard.
   - A lock icon 🔒 appears on the secure file(s).
   - The original file(s) are deleted only where specified in the previous step.

9. Continue to encrypt and digitally sign files as needed without logging on again.

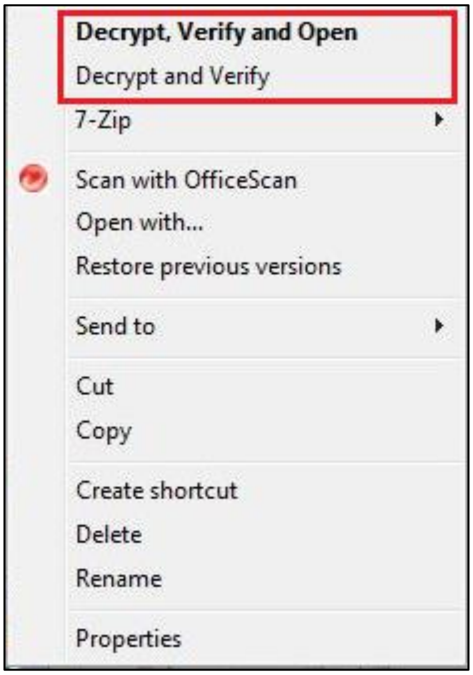
   Note: After a specified period of inactivity (currently set to 12 hours), the secure session is logged off.

Decrypt and Verify Digitally Secured File(s)

The user completes the following steps to decrypt, verify and open file(s) secured (encrypted, digitally signed or both) using the DCS service:

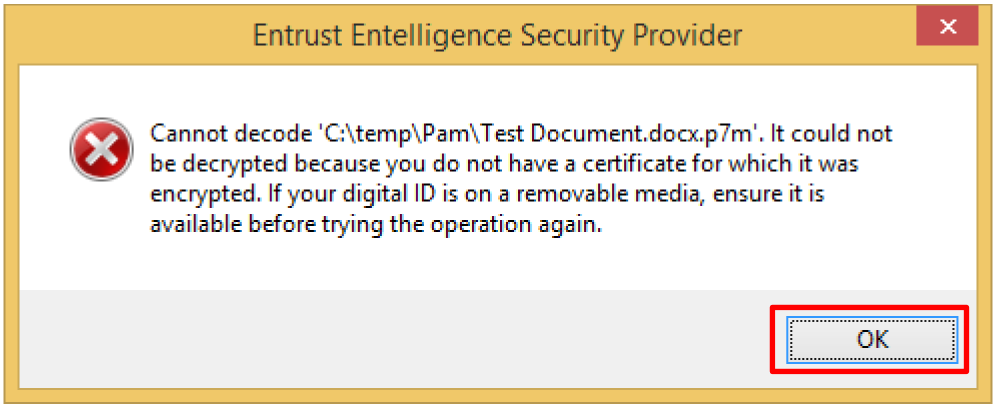
1. Insert Token.
2. Navigate to the folder containing the file(s).
3. Select the file(s) and right-click (one or more files may be selected at the same time).

   A menu displays:



4. Select one of the following options:
   - Decrypt, Verify and Open…
   - Decrypt and Verify…

- If the Token is not inserted, the Entrust Entelligence Security Provider dialog box appears, requesting confirmation to replace the file:

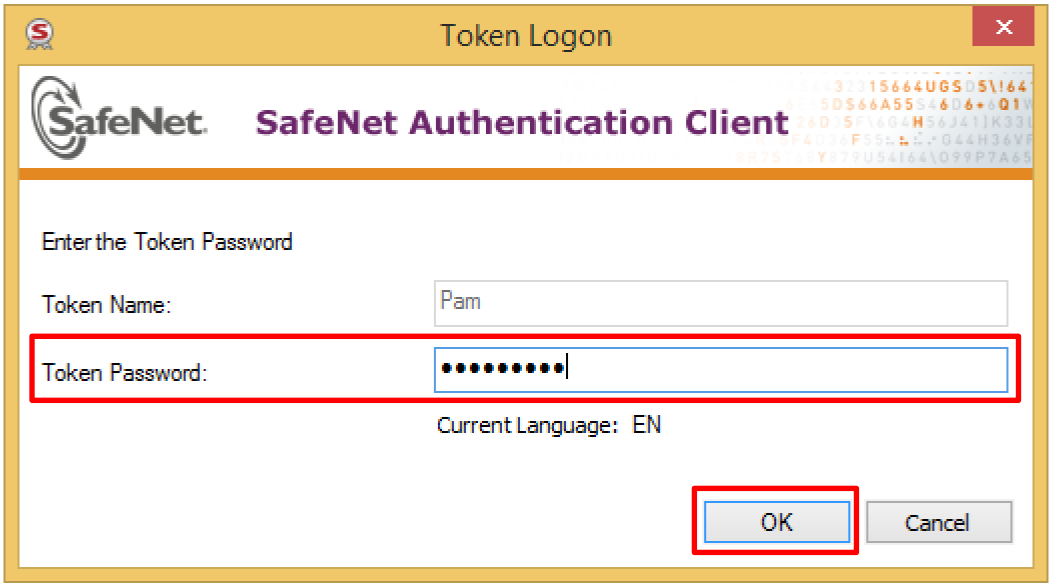


Entrust Entelligence Security Provider

Cannot decode 'C:\temp\Pam\Test Document.docx.p7m'. It could not be decrypted because you do not have a certificate for which it was encrypted. If your digital ID is on a removable media, ensure it is available before trying the operation again.

Select **OK** to close the dialog. Insert the Token and try again.

- If the Token Logon dialog box displays showing the Token Name:



Token Logon

SafeNet Authentication Client

Enter the Token Password

Token Name: Pam

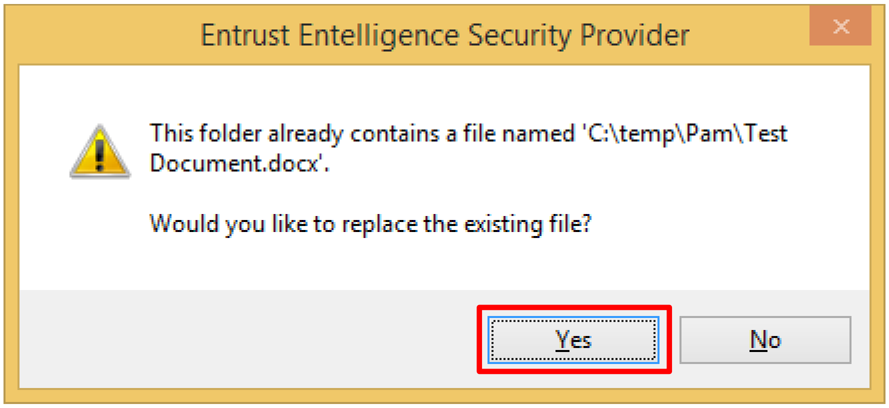
Token Password: ●●●●●●●●●

Current Language: EN

Enter the Token Password and click **OK**.

Note: A file that is only digitally signed will not require password authentication.

- ○ If the Entrust Entelligence Security Provider dialog box displays requesting confirmation to replace the file:


Entrust Entelligence Security Provider

This folder already contains a file named 'C:\temp\Pam\Test Document.docx'.

Would you like to replace the existing file?

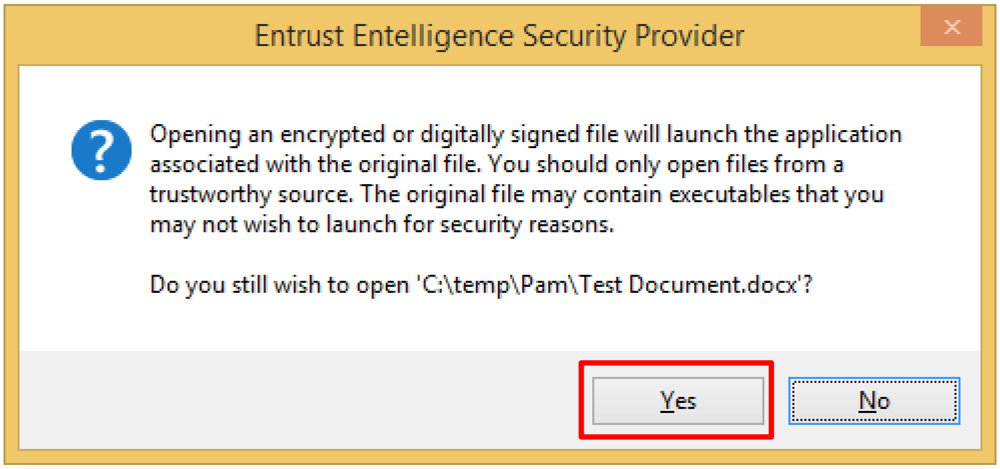
Click Yes.

A decrypted version of the file is created.

This ends the Decrypt and Verify process.

Note: The remaining steps apply if the option to Decrypt, Verify and Open digitally secured file(s) (in Step 4) was chosen.

5. The Entrust Entelligence Security Provider dialog box displays requesting confirmation to open the file:


Entrust Entelligence Security Provider

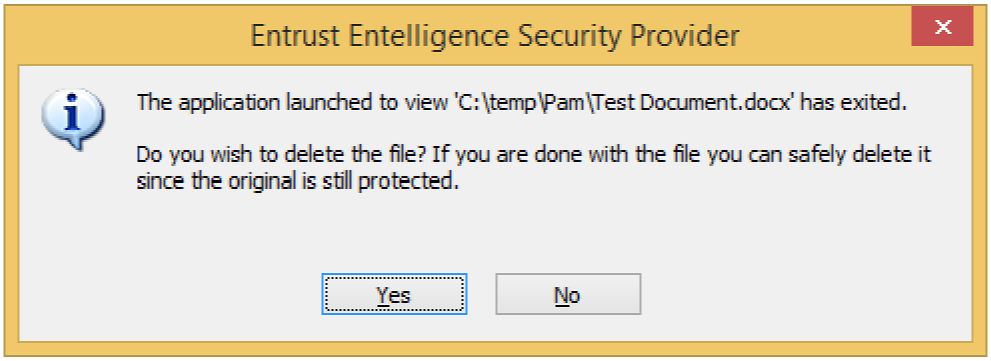
Opening an encrypted or digitally signed file will launch the application associated with the original file. You should only open files from a trustworthy source. The original file may contain executables that you may not wish to launch for security reasons.

Do you still wish to open 'C:\temp\Pam\Test Document.docx'?

6. Click **Yes**.

   The file opens.

7. When closing the file (i.e. when no longer needing to use the file) the Entrust Entelligence Security Provider dialog box displays requesting confirmation to delete (and securely erase) the decrypted version of the file:



The application launched to view 'C:\temp\Pam\Test Document.docx' has exited.

Do you wish to delete the file? If you are done with the file you can safely delete it since the original is still protected.

Note: only the decrypted version of the file is deleted, not the secured (encrypted/digitally signed) version of the file.

8. Either:
   - ○ Click **Yes** to close the dialog box and delete (and securely erase) the decrypted version of the file.

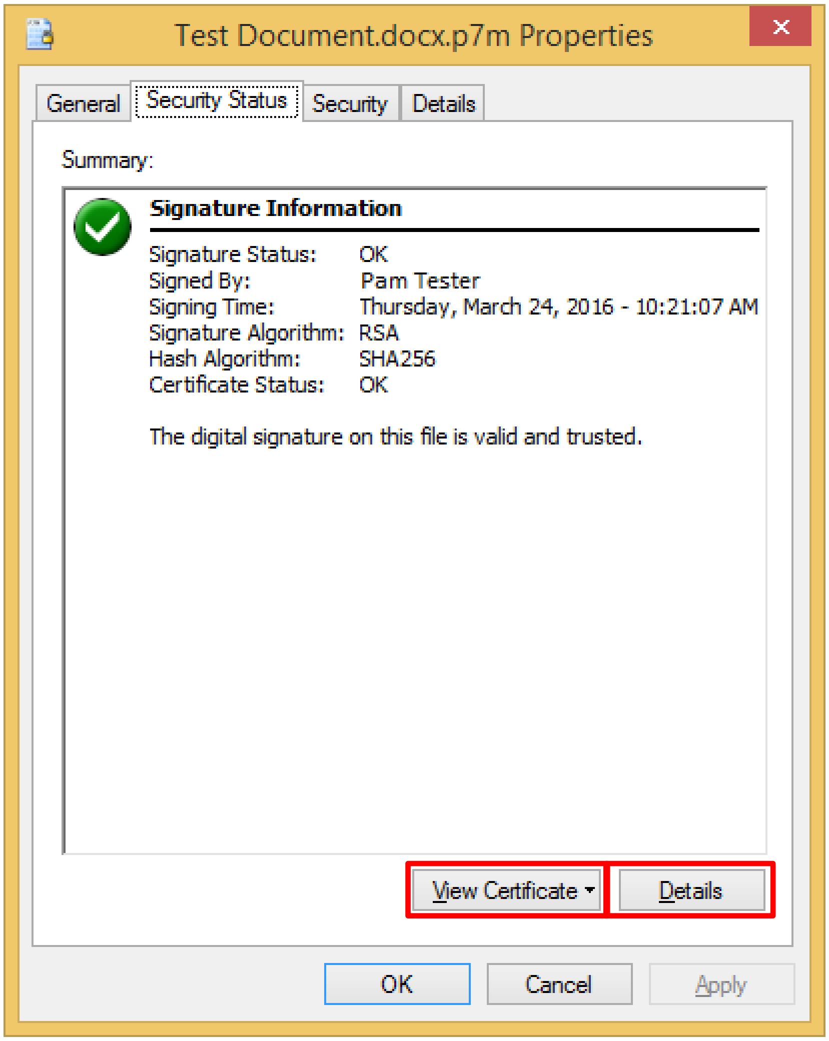
     Note: to see that the decrypted version of a file is deleted from a folder you may need to refresh right-click the folder and select Refresh.

   - ○ Click **No** to close the dialog box and keep both the decrypted version and the secured version of the file.

Manual check of a digital signature

The user completes the following steps to see details of the individual who digitally signed a file:

1. Open the Properties of the digitally-signed file (right-click the file and select Properties).
2. Select the Security Status tab to view Signature Information.



Signature Information

Signature Status: OK
Signed By: Pam Tester
Signing Time: Thursday, March 24, 2016 - 10:21:07 AM
Signature Algorithm: RSA
Hash Algorithm: SHA256
Certificate Status: OK

The digital signature on this file is valid and trusted.

3. Click **View Certificate** or **Details** to see additional information contained in the digital certificate that was used in digitally signing the file.