Table of Contents

1. Introduction

1.1 What is Digital Signature?

You can digitally sign a document for many of the same reasons you might place a handwritten signature on a paper document. A digital signature is used to help authenticate the identity of the creator of (authenticate: The process of verifying that people and products are who and what they claim to be. For example, confirming the source and integrity of a software publisher's code by verifying the digital signature used to sign the code.) digital information — such as documents, e-mail messages, and macros — by using cryptographic algorithms.

Digital signatures are based on digital certificates. Digital certificates are verifiers of identity issued by a trusted third party, called a certification authority or CA. This works similarly to the use of standard identity documents in the non-electronic world. For example, a trusted third party such as a government entity or employer issues identity documents such as driver's licenses, passports and employee ID cards on which others rely to verify that a person is whom he/she claims to be.

1.2 What Digital Signatures Accomplish?

Digital signatures help to establish the following authentication measures:

Authenticity: The digital signature helps to assure that the signer is who he or she claims to be. This helps prevent others from pretending to be the originator of a particular document (the equivalent of forgery on a printed document).

Integrity: The digital signature helps to assure that the content has not been changed or tampered with since it was digitally signed. This helps prevent documents from being intercepted and changed without knowledge of the originator of the document.

Non-repudiation: The digital signature helps to prove to all parties the origin of the signed content. "Repudiation" refers to the act of a signer's denying any association with the signed content. This helps prove that the originator of the document is the true originator and not someone else, regardless of the claims of the signer. A signer cannot repudiate the signature on that document without repudiating his or her digital key, and thus other documents signed with that key.

1.3 Digital Signatures in the Business Environment

The following scenario illustrates how digital signing of documents can be used in a business environment:

I. An employee uses an Excel spreadsheet to create an expense report. The employee then creates three signature lines: one for herself, one for her manager and one for accounting. These lines are used to identify that the employee is the originator of the document, that no changes will take place in the document as it moves to the manager and the accounting division, and that there is proof that both the manager and accounting department have received and reviewed the document.

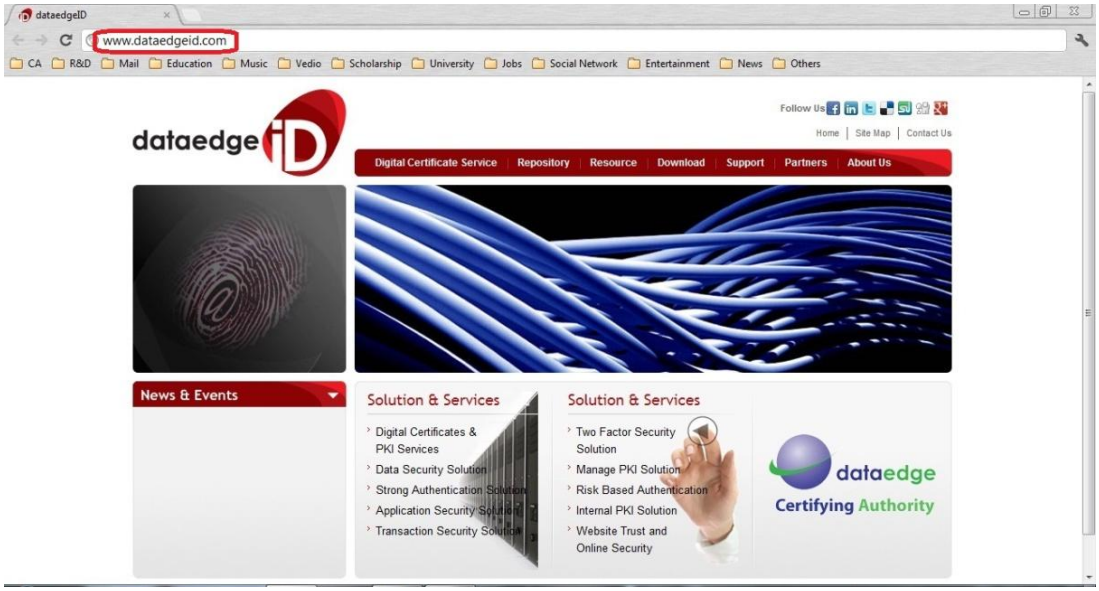
II. The manager receives the document and adds her digital signature to the document, confirming that she has reviewed and approved it. She then forwards it to the accounting department for payment. A representative in the accounting department receives the document and signs it, confirm receipt of the document.

2. How to keep your Root Certificate into Trust list?

- If you select browser to store your personal certificate while pick up from the dataedgeCA then it will come automatically to your browser. It is recommended that you should pick up your personal certificate from the same system that you used for enrollment.
- If you select eToken to store your personal certificate while pick up from dataedgeCA then it will be stored your Cryptographic eToken but when you will insert your eToken to your system, browser will automatically detect your certificate.
- To use your certificate for various purposes you need to be added your parents certificate (Root Certificate of CCA Bangladesh) to your browser trust list.

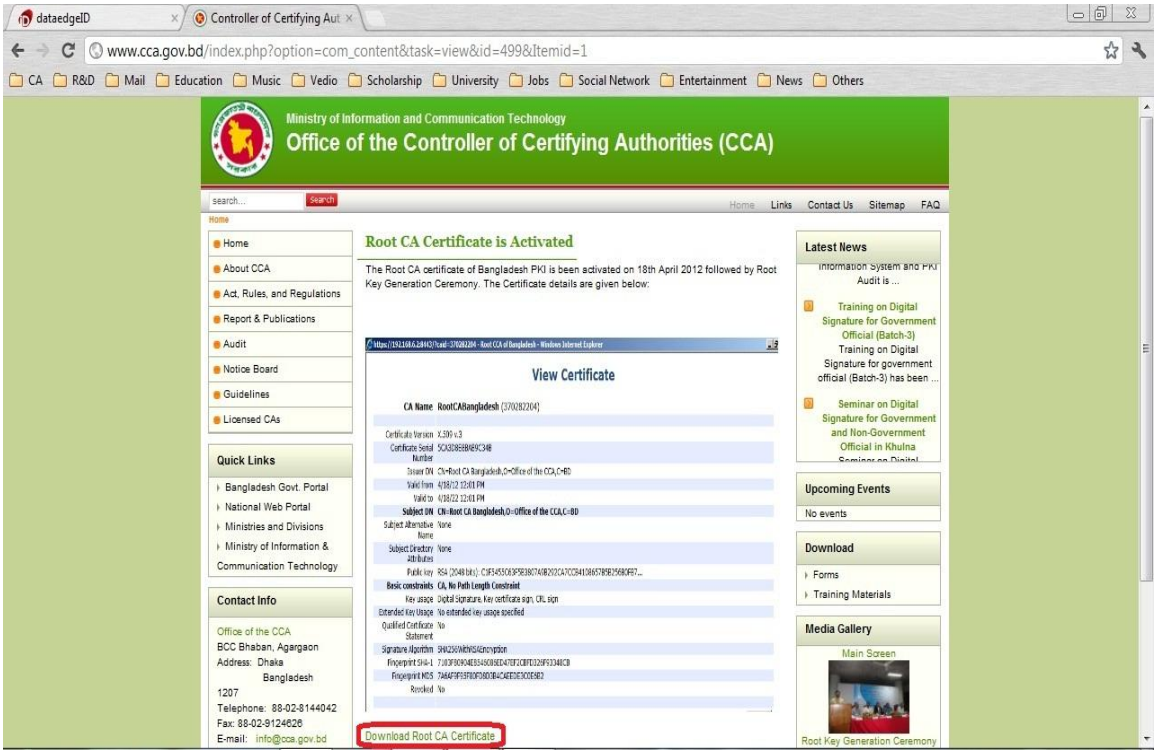
Here the steps to add the parent certificate to your browser trust list:

1. Go to www.dataedgeid.com . Here you will get the Root Certificate of CCA & dataedgeCA



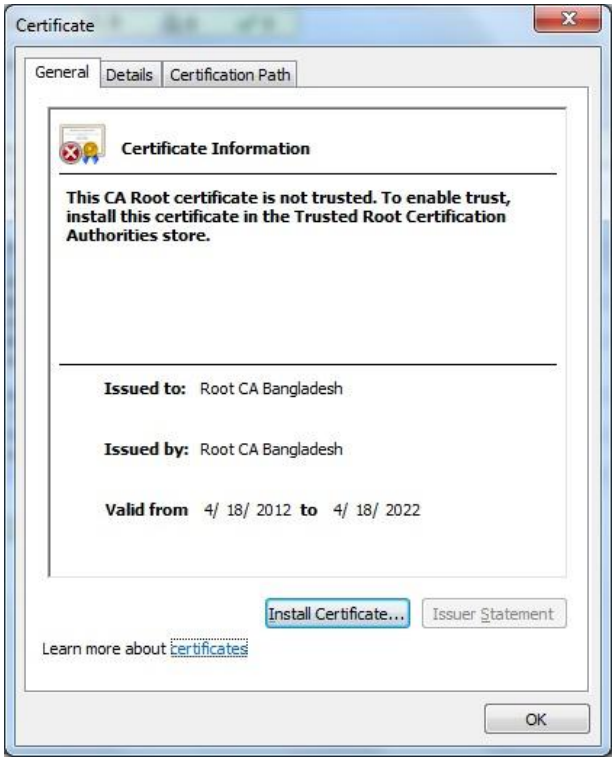
2. Click the Download options then CCA Root Certificate

3. It will redirect to www.cca.gov.bd . Click the Download Root CA Certificate



4. You can save the Certificate into your system or directly open and can add to browser

5. Click Install Certificate



6. Click the Next for further proceeding

7. Select Place all certificate in the following store and click Next

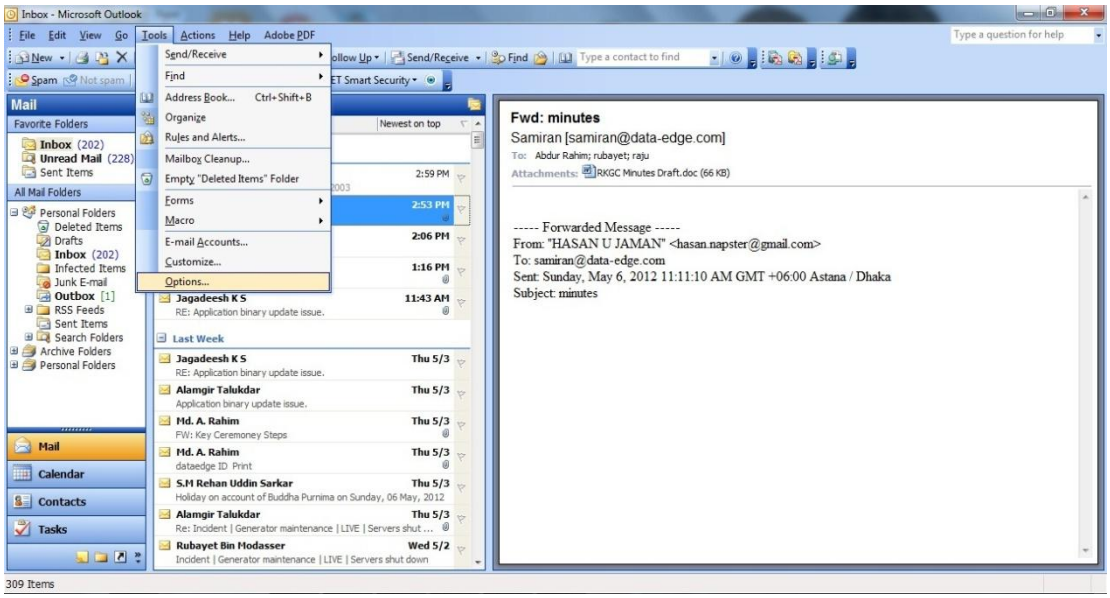
8. Select Trusted Root Certification Authorities and click ok. In next step just click Finish

9. You will get a warning massage for installing your Root certificate. Select Yes

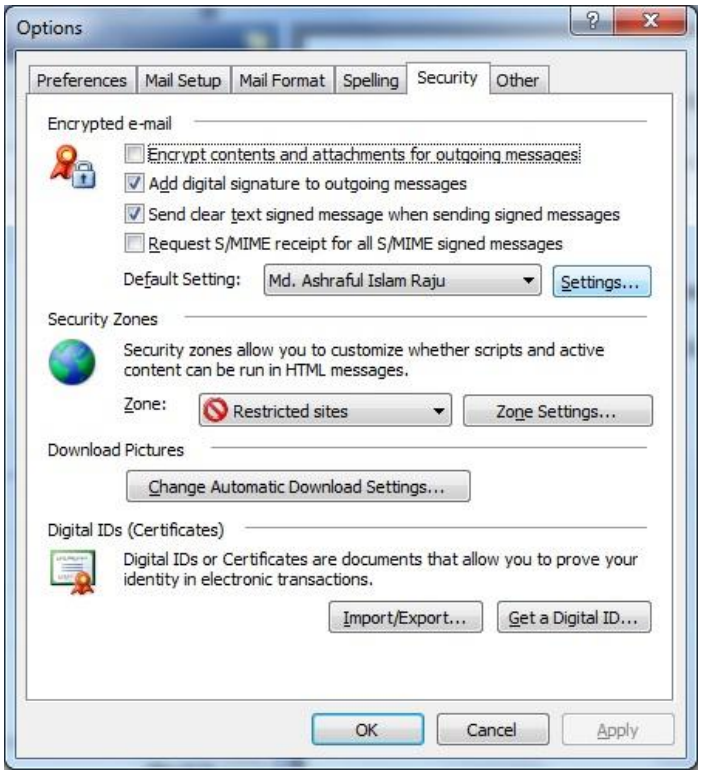
3. How to add Digital Signature with your email?

3.1 How to Digitally Sign an Outlook 2003 email?

1. Open Outlook
2. From the top menu, select **Tools**, then **Options**.



3. In the **Options** window, select the **Security** tab.



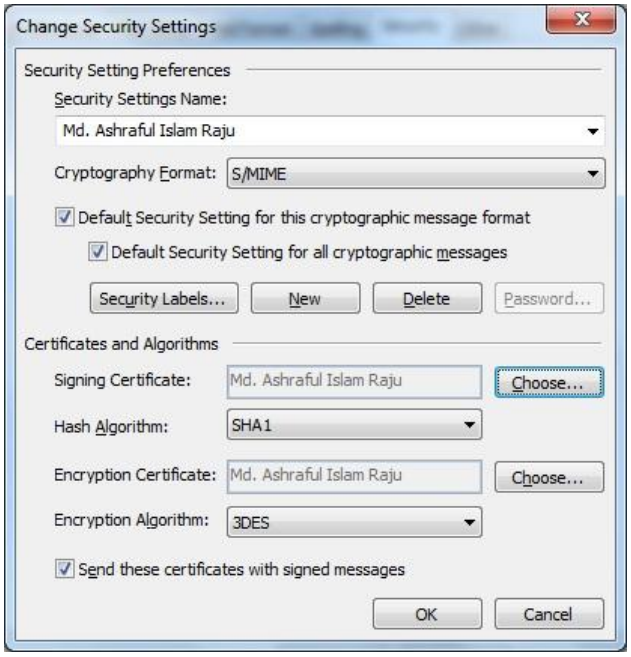
- Select **"Add ditigal signature to outgoing messages"** to automatically send digitally signed emails unless you choose not to for an individual message
- Select **"Send clear text signed message when sending signed messages"** if you always want to allow others who may be using a lesser technology with Outlook to read your message. Recipients who don't have S/MIME security will be able to read the message.
- Select **"Request S/MIME receipt for all S/MIME signed messages"** if you want to be able to verify that your digital signature is being validated by recipients and to request confirmation that the message was received unaltered, as well as notification telling you who opened the message and when it was opened.

NOTE: *It is recommended that you don't select the "Request S/MIME receipt" option unless you have a strong business need, as it doubles the number of emails in your Inbox and adds network traffic.*

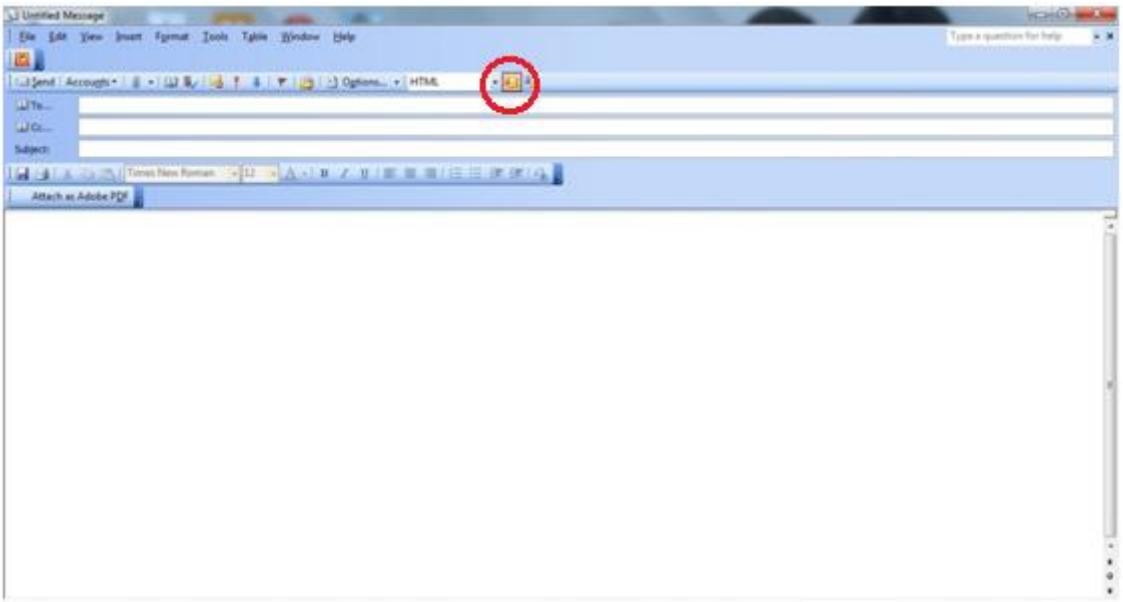
4. Select **Setting** to add a digital certificate
5. Write the security setting name

6. Choose your digital certificate for signing & encryption your email.

7. Click the **OK** button to close the **Options** window.



8. Click the **OK** button to close the Options window. When you start a new message, your toolbar will show the envelope with a small red ribbon already selected, indicating the message will be digitally signed. (You can choose not to sign an individual email by clicking the envelope icon.)
9. When you start a new message, your toolbar will show the envelope with a small red ribbon already selected, indicating the message will be digitally signed. (You can choose not to sign an individual email by clicking the envelope icon.



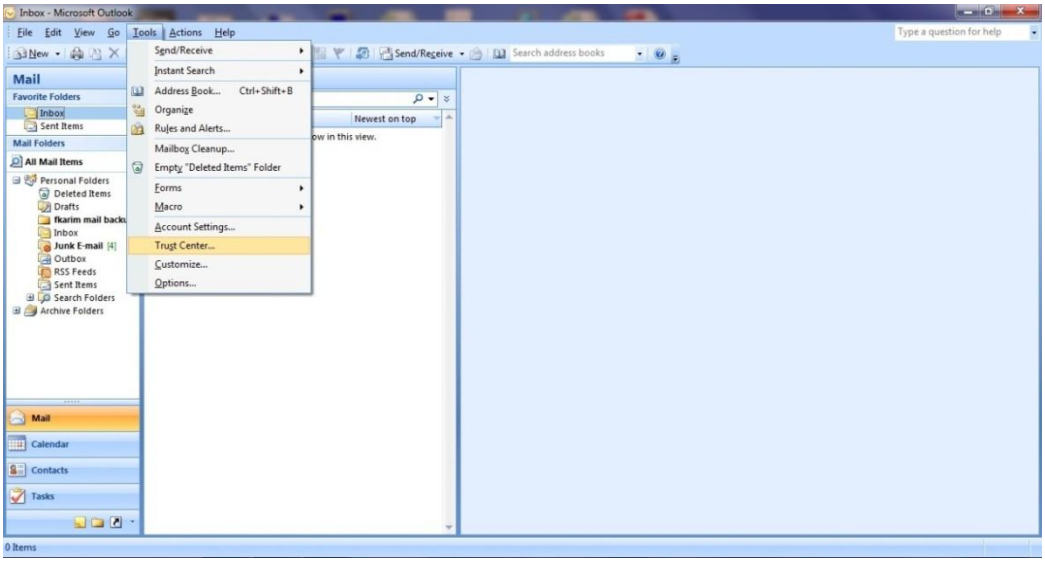
The message will appear in the recipient's Inbox with an envelope with a red ribbon on it indicating the message is digitally signed.

If this is the first time through the process, you will probably get a security warning telling you that you're about to install a certificate. Click the **Yes** button. You won't see this message again for future signed messages sent to you by anyone who used their certificate to sign the message.

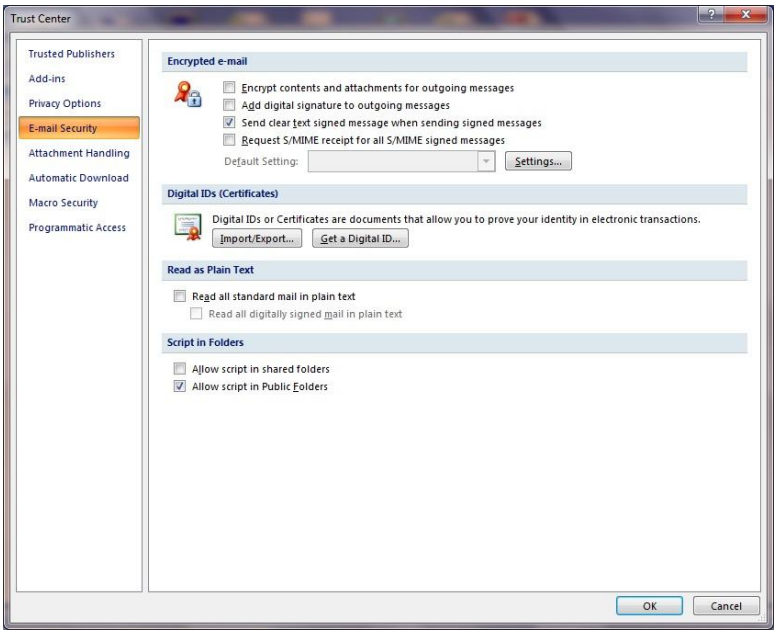
When the message opens, the red ribbon in the lower right of the header indicates the message is digitally signed.

3.2 How to Digitally Sign an Outlook 2007 email?

1. Open Outlook 2007
2. From the top menu bar, select **Tools**, then **Trust Center**.



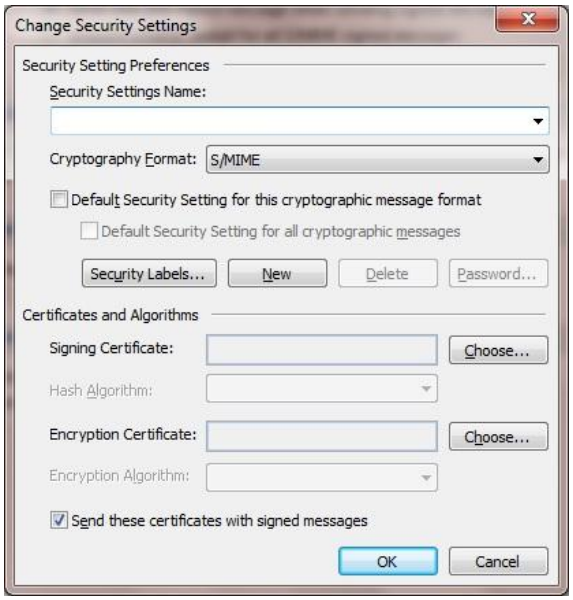
3. In the Trust Center window, select **Email Security** from the left menu.



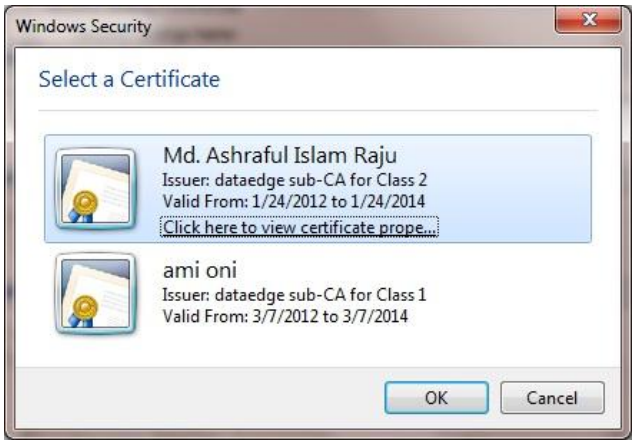
- Select **"Add digital signature to outgoing messages"** to automatically send digitally signed emails unless you choose not to for an individual message
- Select **"Send clear text signed message when sending signed messages"** if you always want to allow others who may be using a lesser technology with Outlook to read your message. Recipients who don't have S/MIME security will be able to read the message.
- Select **"Request S/MIME receipt for all S/MIME signed messages"** if you want to be able to verify that your digital signature is being validated by recipients and to request confirmation that the message was received unaltered, as well as notification telling youwho opened the message and when it was opened.

NOTE: *It is recommended that you don't select the "Request S/MIME receipt" option unless you have a strong business need, as it doubles the number of emails in your Inbox and adds network traffic.*

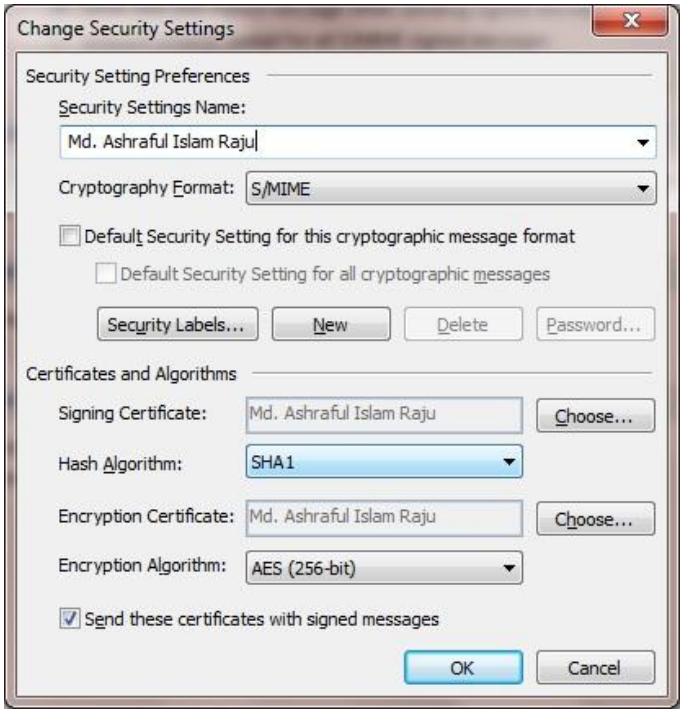
4. Select **Setting** to add a digital certificate



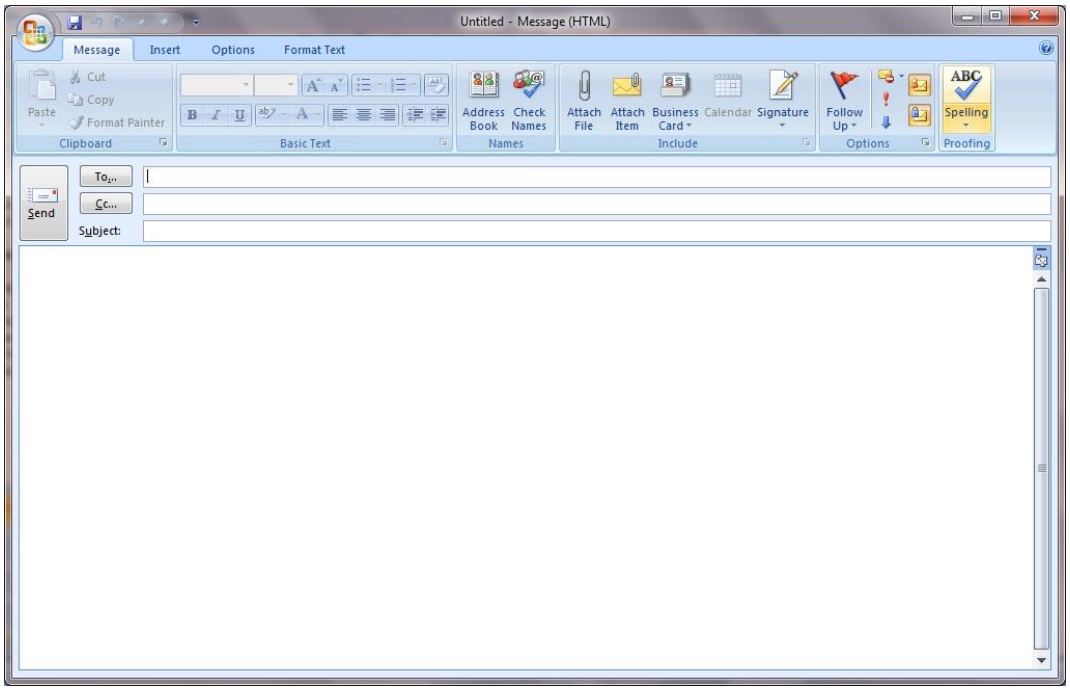
5. Write the security setting name and choose your digital certificate for signing & encryption



6. Click the **OK** button to close the **Options** window.



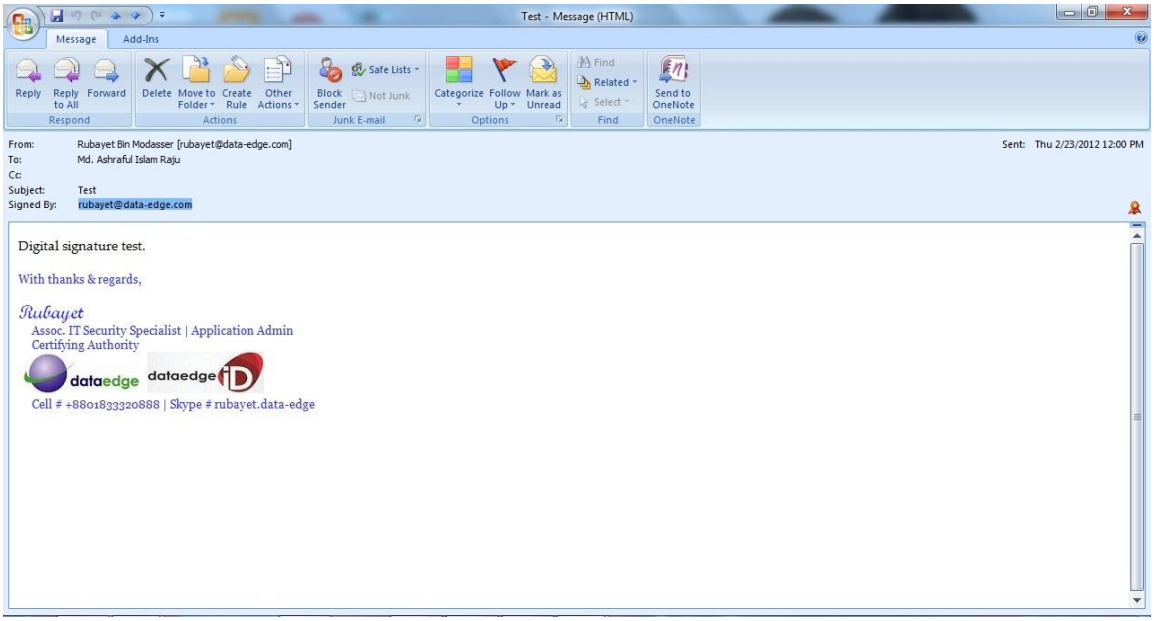
7. When you start a new message, your toolbar will show the envelope with a small red ribbon already selected, indicating the message will be digitally signed. (You can choose not to sign an individual email by clicking the envelope icon.



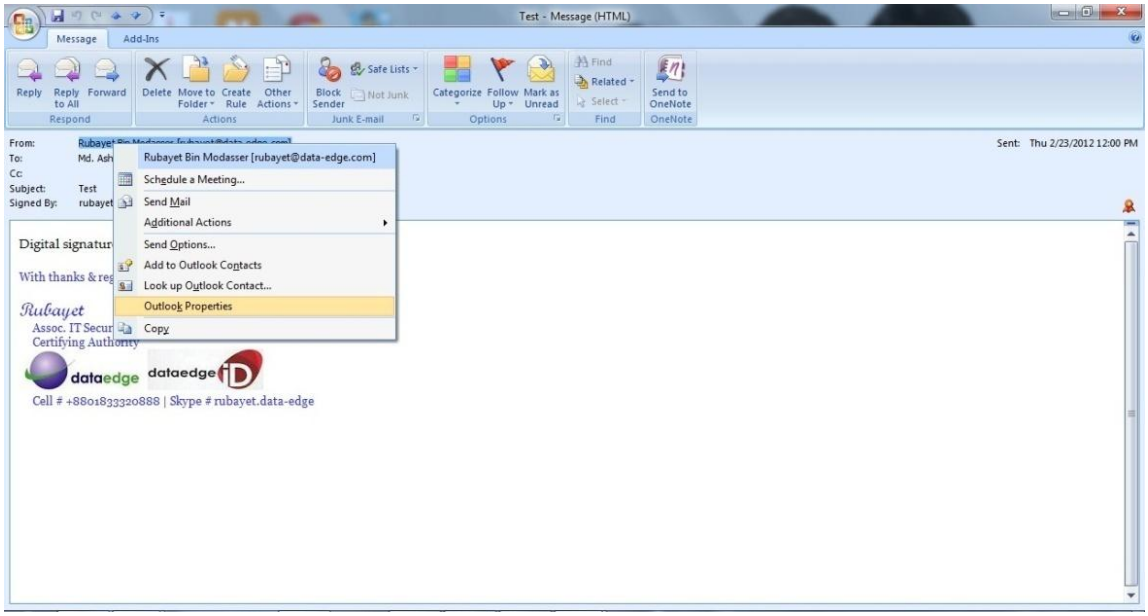
If you selected the "Request S/MIME receipt" option in step 3, you will receive a separate message with the receipt information.

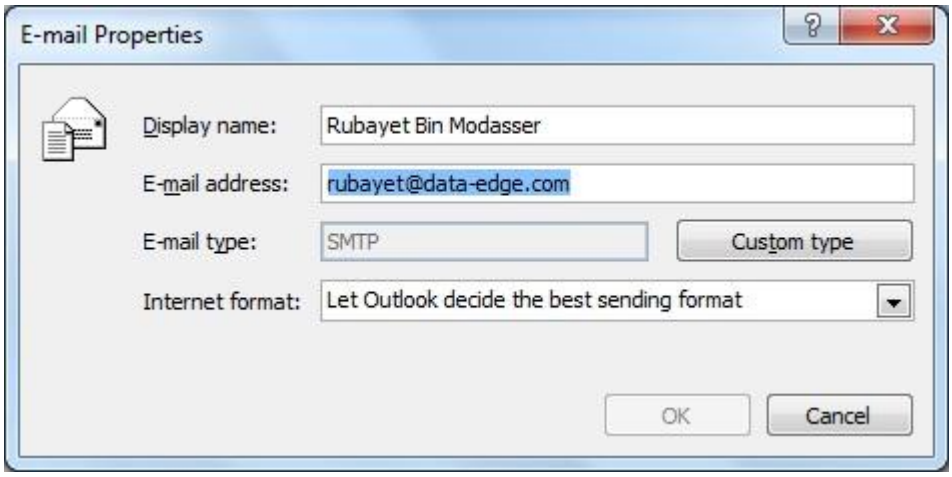
3.3 How to verify the signature is valid or not? (2003 & 2007)

1. Open the message that has been digitally signed. Outlook will show you that the email has a digital signature by showing the "Signed By" information and the red ribbon icon.



2. To verify the person who sent the email is the person who signed it, compare the "From" properties (right click the name, select Outlook Properties, then click the "Email Addresses" tab) with the email address in the "Signed By" field.



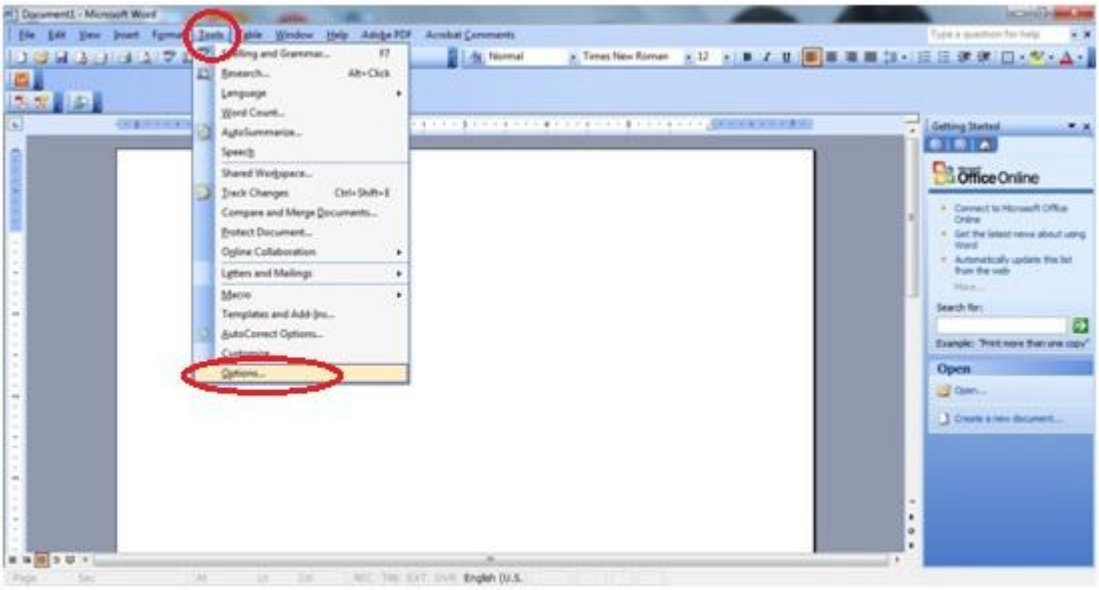


Note: *You can also click the red ribbon icon then click the Details button to look at the signature details If the Signed By information is underlined in red and the red ribbon icon has a red exclamation point, the signature is invalid. Click the red ribbon icon for more information about the signature status.*

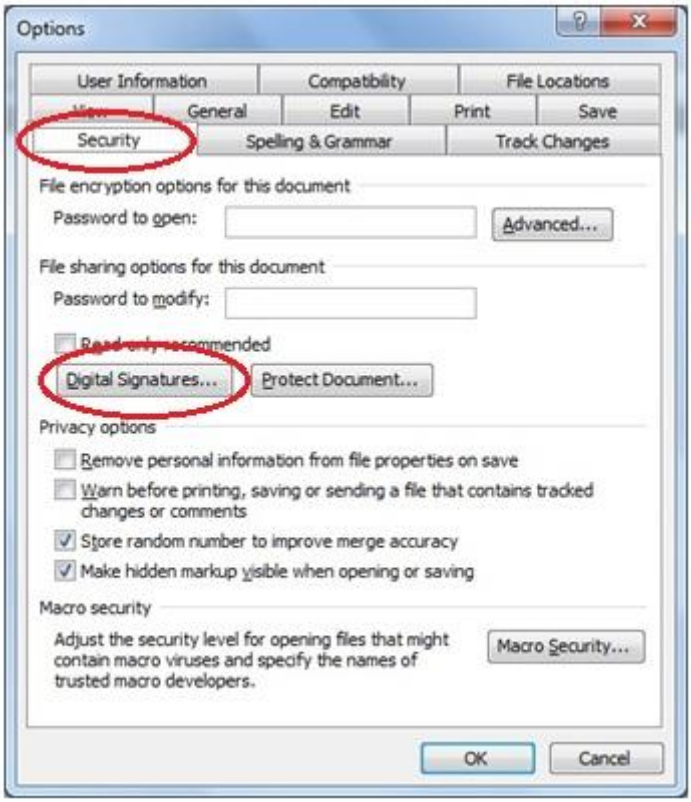
4. How to add Digital Signature into your document?

4.1 Adding Digital Signature to Microsoft Office 2003 (Word, Excel, Power Point) Document

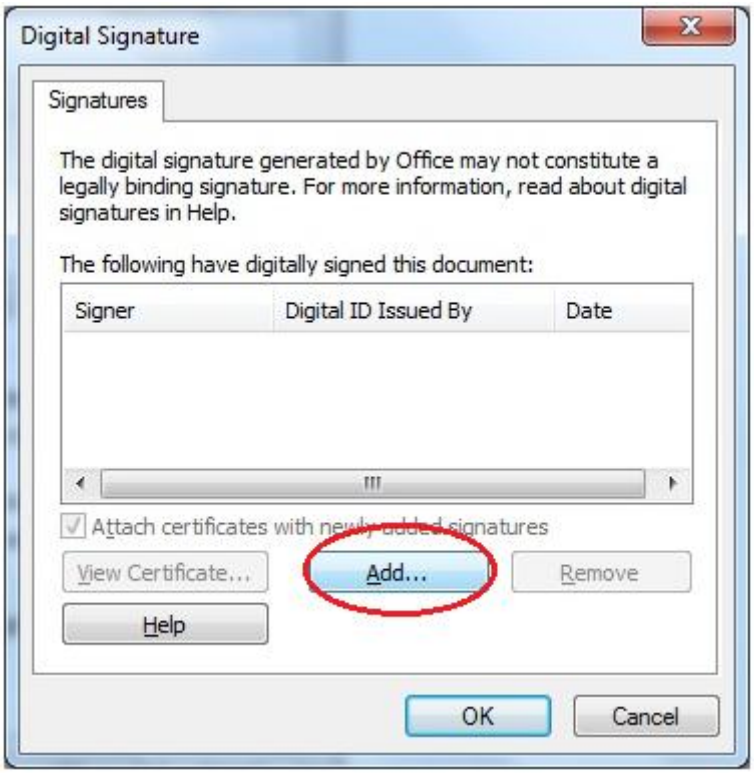
1. From the menu bar, select **Tools**, then select Options,



2. Click the "**Security" tab**, and then click the **Digital Signatures** button.



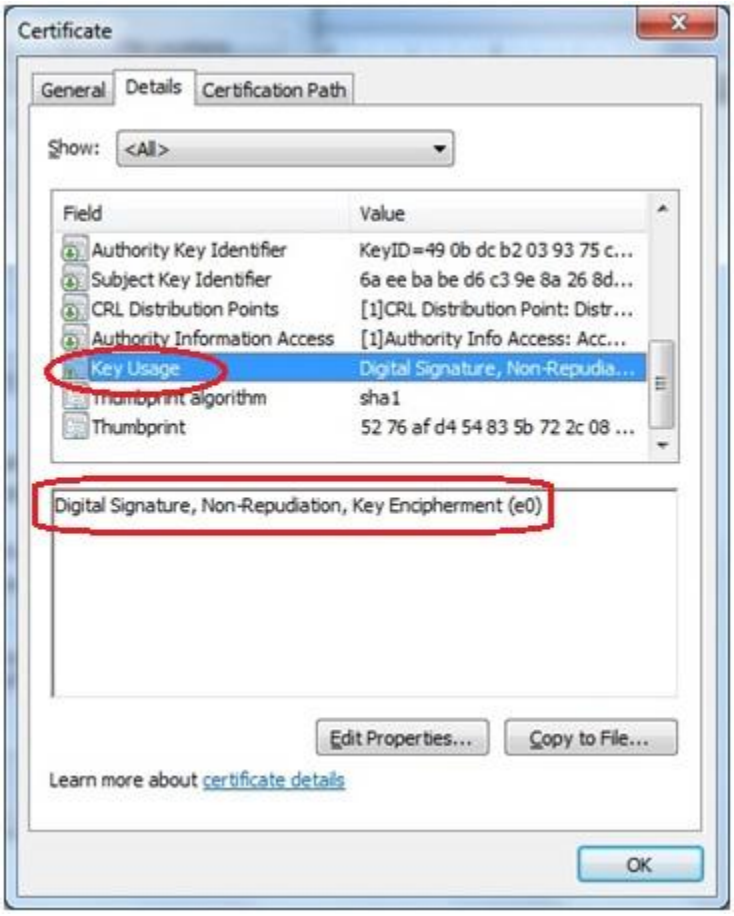
3. Click the **Add**… button.



4. Select certificate for Digital Signature by clicking the correct line. Because it is impossible to tell from this view which certificate is the one you want, go to step 5 to see how to choose the correct one.

NOTE: *If other people's certificate has used in your computer, or you have other digital certificates, you may see a long list of certificates. Only select your personal certificates.*

5. Click the **View Certificate** button, then click the "Details" tab and scroll down to the "Key Usage" field. You want the certificate that says its key usage is "Digital Signature, Non-Repudiation (c0)."



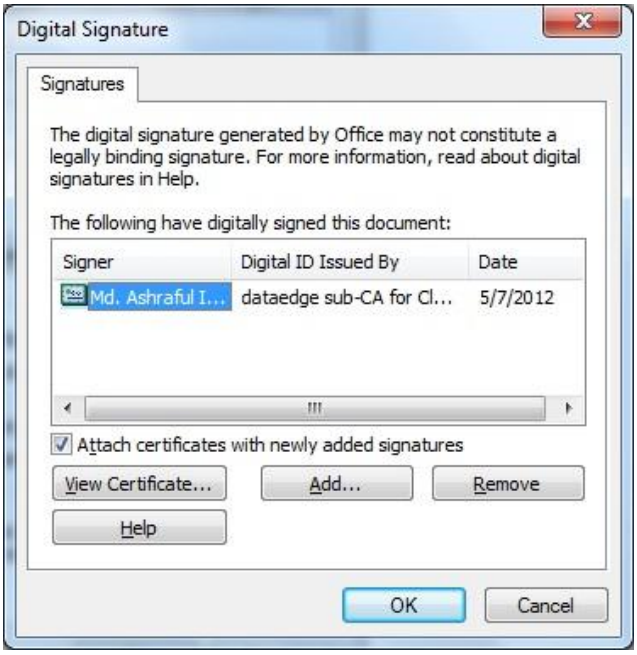
6. Click the **OK** button to close this window.

NOTE: *If you selected the wrong certificate in step 4 (e.g., the one that says only "Digital Signature" without the "Non-Repudiation (c0)" part, click the* ***OK*** *button, then go back to step 4 to select another certificate*

Back at the list of certificates, with the correct certificate highlighted, click the **OK** button.

NOTE: *If this is the first time you are using any Office 2003 application (Word, Excel, or PowerPoint) to digitally sign a document, it will take a long time – anywhere from 30 to 90 seconds – to add the certificate to the document. The next time you sign an Office 2003 document, it will go much quicker.*

7. At the Digital Signature window, click the **OK** button to close it.



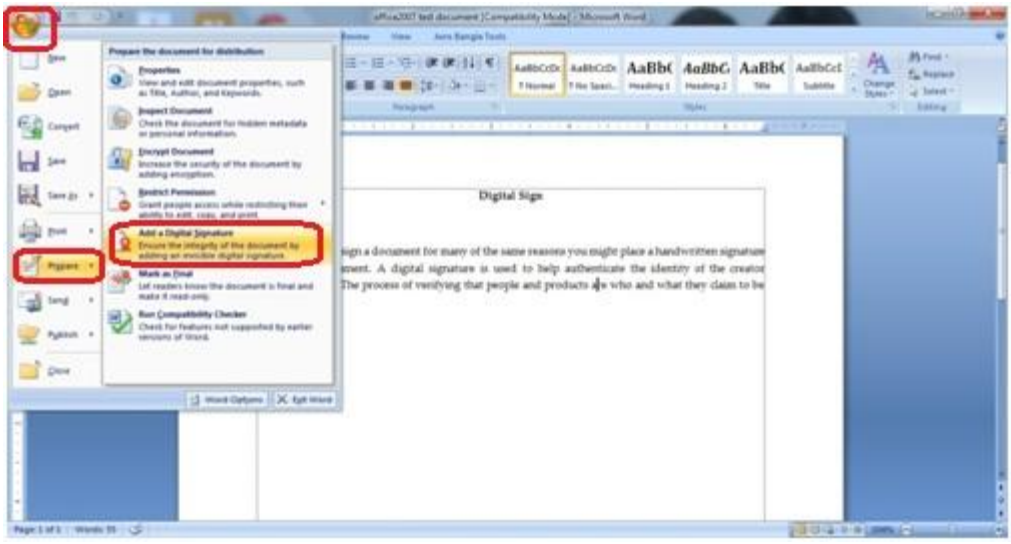
8. At the Options window, click the **OK** button to close it.

The Word file is now digitally signed by you. Close the file without making any changes (or the digital Signature will be lost).

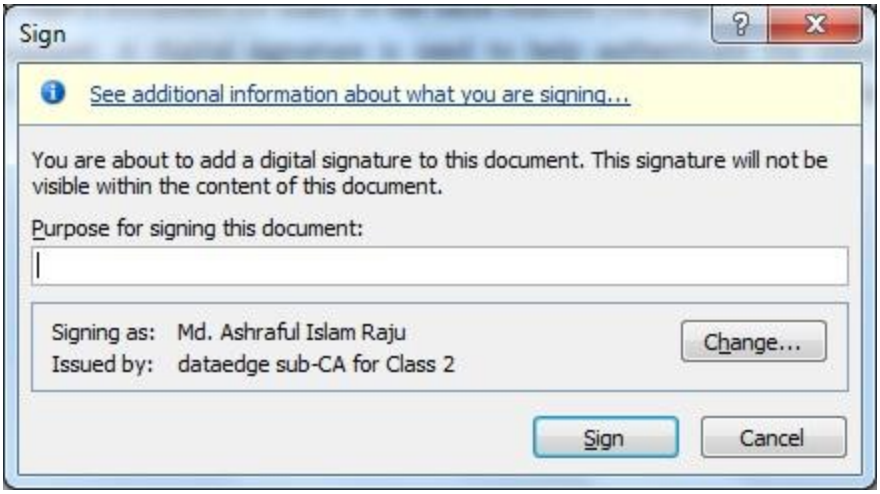
NOTE: *None of the Office 2003 applications has an indicator that the document has been digitally signed at this point. If you close the document, then reopen it again, the title bar at the top will show "signed, unverified" after the file name, and a small red certificate will show in the information bar at the bottom.*

4.2 Adding Digital Signature to Microsoft Office 2007 (Word, Excel, Power Point) Document

1. From the main menu icon, select **Prepare**, then **Add a Digital Signature**.



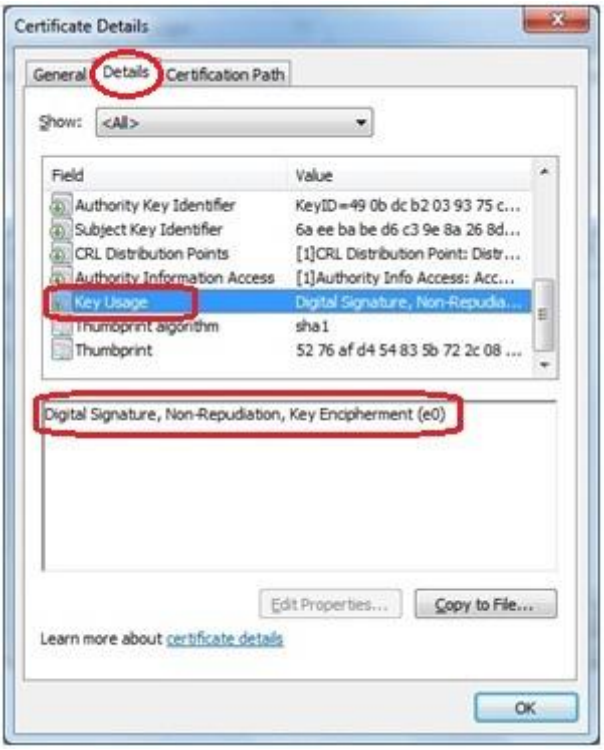
2. If this is the first time you've selected a certificate for digital signing, Microsoft offers to help you set one up. Since your browser/eToken already has certificates, click the **OK** button. (To avoid seeing this message each time, check the "Don't show this message again" option.)
3. In the ***Sign*** window, complete the optional "Purpose for signing this document" field, then click the **Change** button to confirm you have the correct Certificate selected.



4. Select the certificate you want to use by highlighting it. (The next step will help you determine which the correct certificate to select is.)

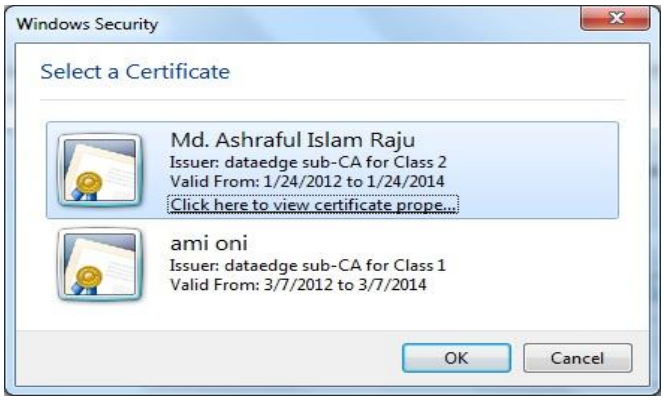
5. Click the **View Certificate** button. The *General* tab lists the information about the certificate.

6. Click the *Details* tab. Scroll down in the list of fields and values to select the "Key Usage" field. In the field below, it should say "Digital Signature, Non-Repudiation (c0)". Click the **OK** button to close the window.

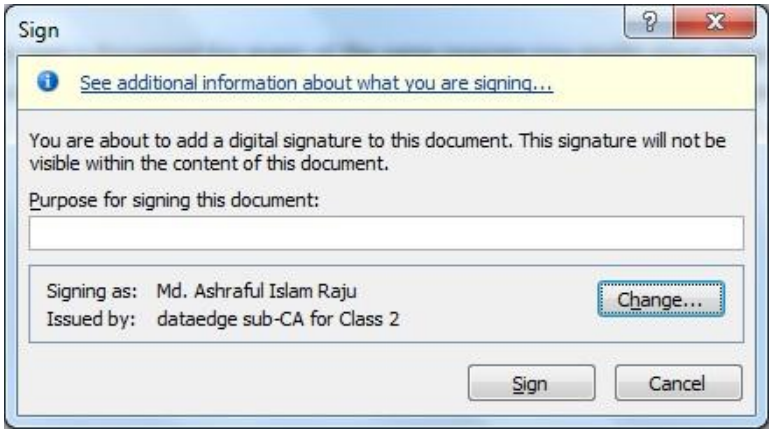


NOTE: *If the "Key Usage" field only says "Digital Signature" or something else, go back to step 5 and select one of the other certificates and use the* ***View Certificate*** *button to verify it's the one you want*

7. Back on the list of certificates, with the correct certificate highlighted, click the **OK** button.



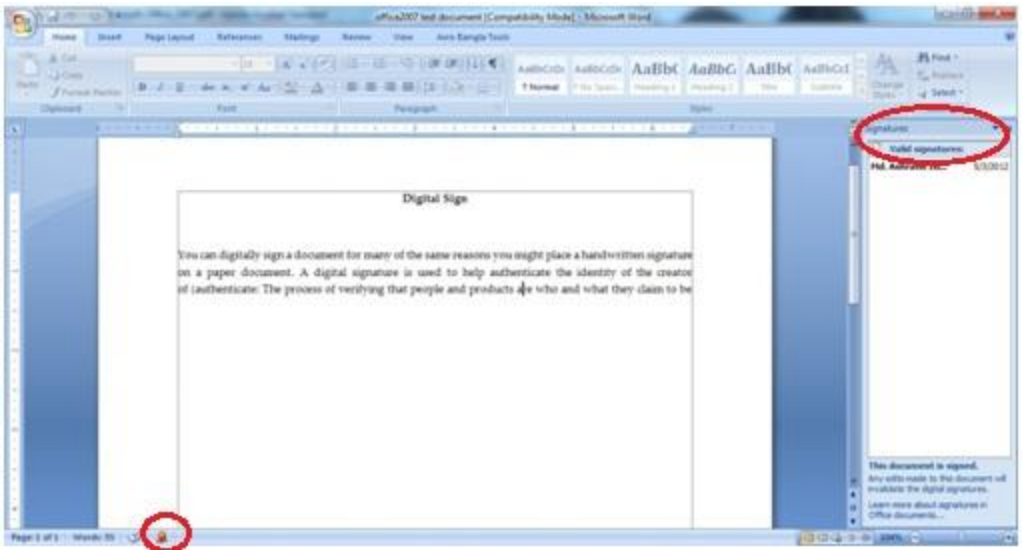
8. Back on the ***Sign*** window, Click the **Sign** button



NOTE: *After you select the certificate the first time, Office 2007 will remember this certificate choice. The next time you want to digitally sign a document, you won't have to repeat the selection process – you'll jump from step 4 to step 8 in this sequence.*

9. After the Certificate is validated, you will receive a successful signature message. Click the **OK** button.

10. Once the signature has been successfully applied, Office 2007 automatically opens a *Signatures* window on the right side of screen showing the valid signature(s).



11. The Word, Excel, or PowerPoint file is now digitally signed by you. **Close the file without making any changes** (or the digital signature will be lost).

NOTE: *More than one person can digitally sign a document, as long as the content of the document isn't changed. After the first signature is applied and the file closed, the second person can follow steps 1-12 above to apply a second signature. This can be repeated for as many signatures as are needed.*

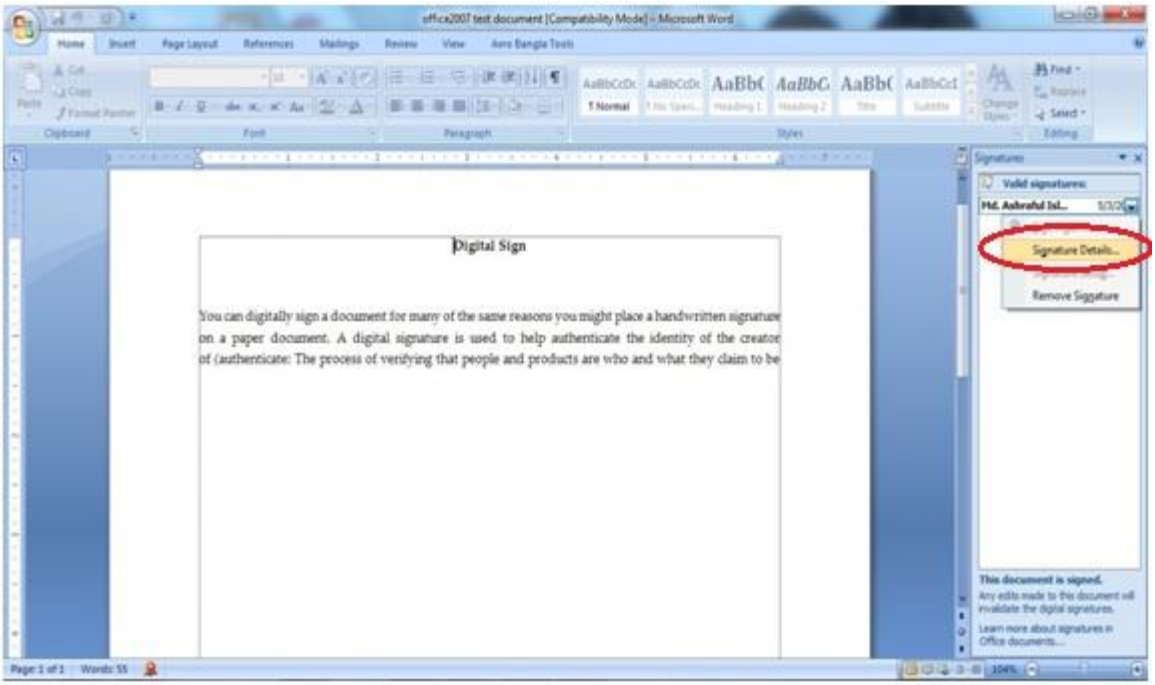
4.3 How to verify a Signature is valid in Office 2003 & 2007?

1. Open the file for which you want to verify signatures.

You can tell the document has a digital signature because in the top title bar, the name of the document has a note after that says "signed, unverified," and there is a small certificate icon in the bottom status information bar.

NOTE: *These indicators only tell you whether or not the file has a digital signature, and shows the signature as "unverified." Microsoft Office 2003 doesn't recognize the HSPD- 12 certificate authority, Entrust, so the only way to check that the signature is valid is to view the certificate.*

1. To view the digital signature(s) associated with the document, from the menu bar, select Tools, then Options, then click the Security tab, then click the **Digital Signatures** button.



2. The Digital Signature window lists the file's digital signature(s). If there is a problem with the certificate, Microsoft may show it here by showing something other than "Entrust" in the "Digital ID Issued By" field. To verify that a certificate is valid, highlight the certificate name, then click the **View Certificate** button.

3. In the "General" tab, check that the certificate is current by checking the validity date. In the "Details" tab, check that the certificate is a Digital Signature certificate, and that the issuing authority is Entrust.

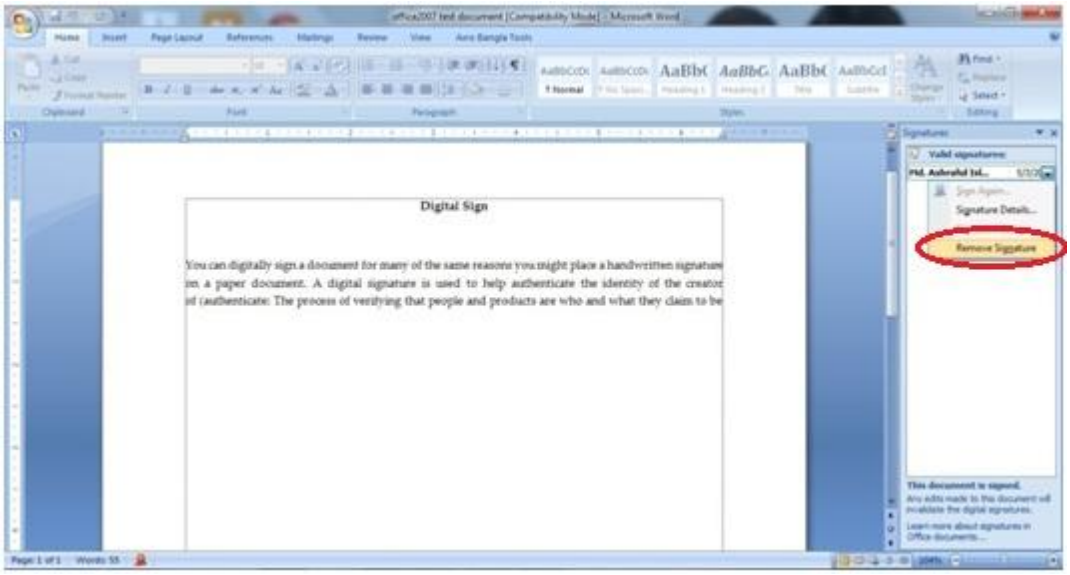
4. Click the **OK** button when you are done and close all menus. Remember, don't save the document when you close it or the digital signatures will be destroyed.

4.4 How to remove Digital Signature from Office 2003 & 2007 document?

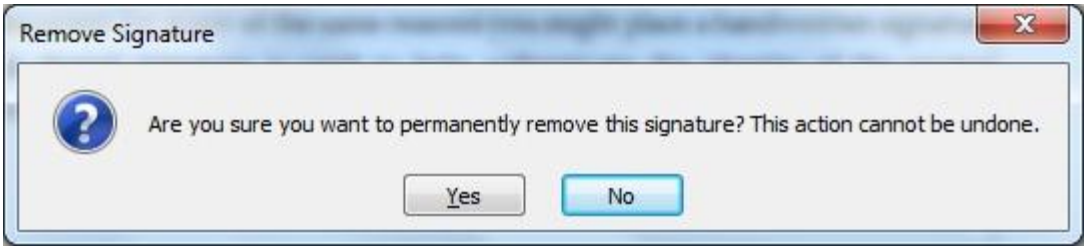
If you want to remove all digital signatures from a document, the simplest way is to make a minor change to the document (e.g., add a space), then save the document. When Word warns you that all signatures will be lost, click the **Yes** button to continue the save operation.

If you want to remove one or more digital signatures from the document without changing the document contents, follow these steps:

1. From the menu bar, select Tools, then Options, then click the "Security" tab, and then click the **Digital Signatures** button.



2. At the Digital Signature window, highlight the signature to be removed, and then click the **Remove** button.

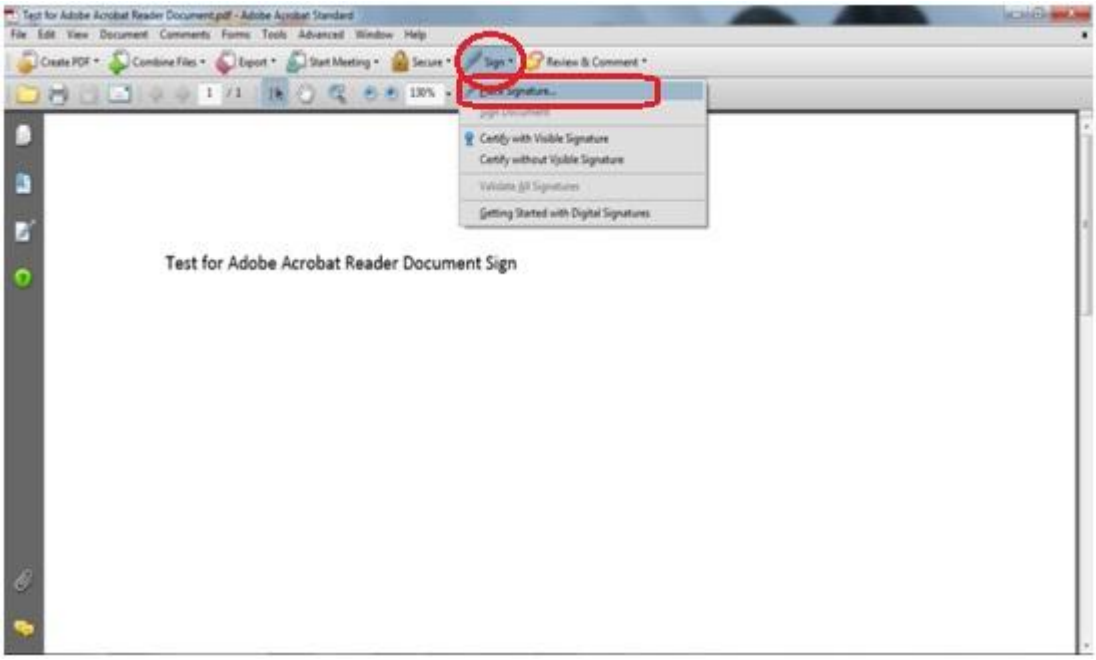


3. At the Options window, click the **OK** button to close it.

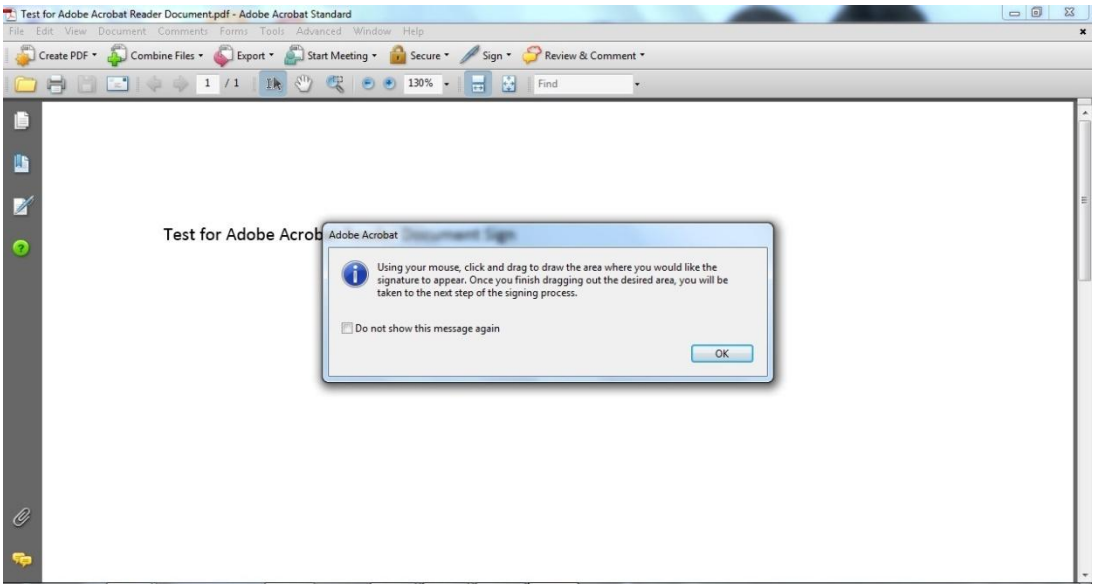
That digital signature has now been removed from the Word document.

4.5 Adding a Digital Signature to Adobe Acrobat Reader document

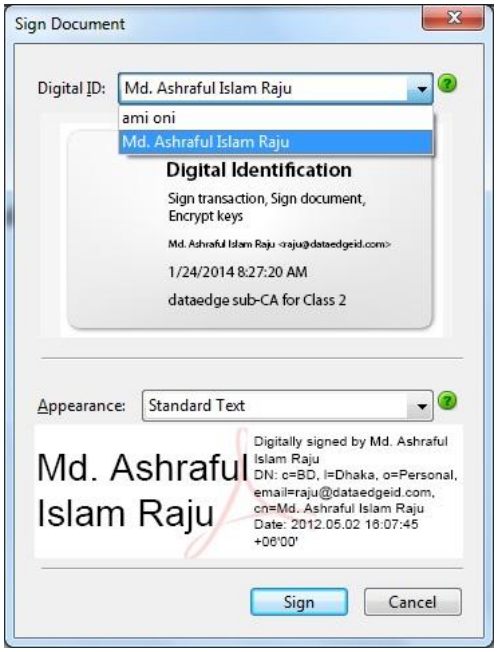
1. Please confirm that your Digital Certificate is in your browser or please insert your eToken into USB port where your Digital Certificate is stored.
2. Open Adobe Acrobat. Either create a new document or open an existing document you want to sign.
3. From the top menu, select Sign, then Place Signature.



4. Adobe will instruct you to draw an area on the screen where you want to place the signature. Click the OK button, and then with your mouse, draw a box for the signature. You can seethe size of the signature, but it's easier to read if you make it as large as possible. You can place the signature anywhere in your document as well, but the recommended locations are at the beginning or the end of the document.



5. After you have created the signature box, a "Sign Document" window appears. From the Digital ID drop list, select the certificate for Digital Signature.

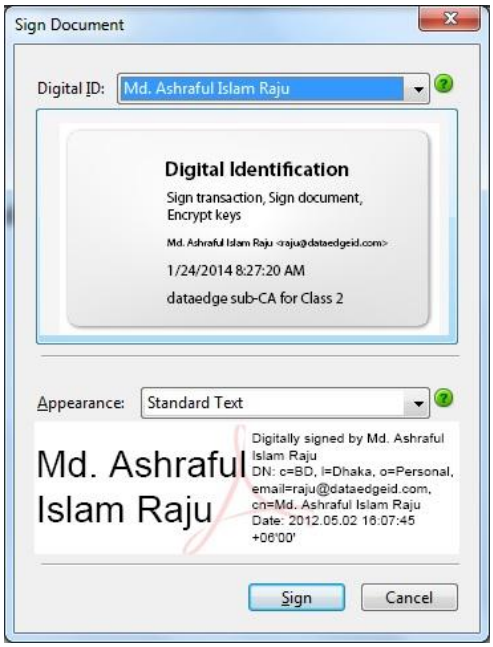


NOTES:

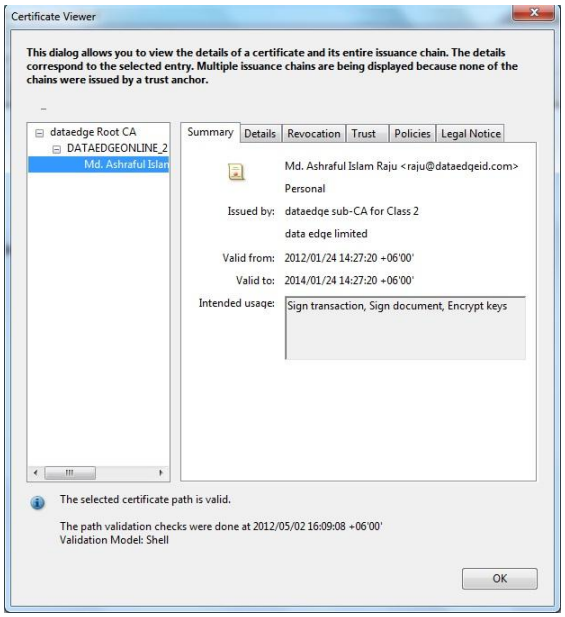
- *If other people's certificate has used your computer, you may see their certificates offered in this list. Only select your personal certificates.*
- *If you don't see your certificate keys listed at all, first check that your card is in the reader and wait a minute or two for Acrobat to find it. If your keys still aren't listed, your agency may need to implement the Adobe Technical Modification for Digital Signature.*

6. Because the "Digital ID" drop list isn't very helpful in describing the certificates, you'll need to view the certificate to confirm it is the correct certificate to use for signing.

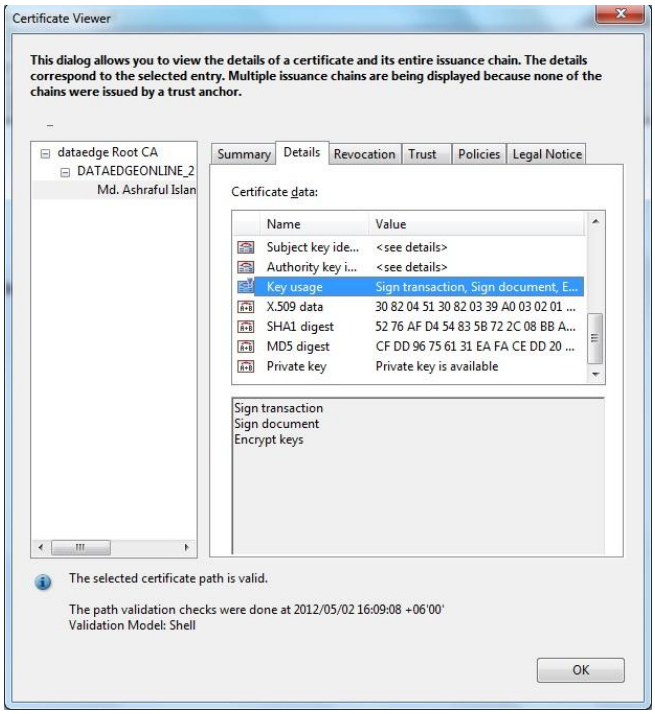
7. Select one of the two lines with your name, then double click the large rectangle that says "Digital Identification." For most certificates, the correct one will be one with your name.



8. In the Certificate Viewer window, open items in the left-side menu until you get to the lowest level. Click to highlight your name.

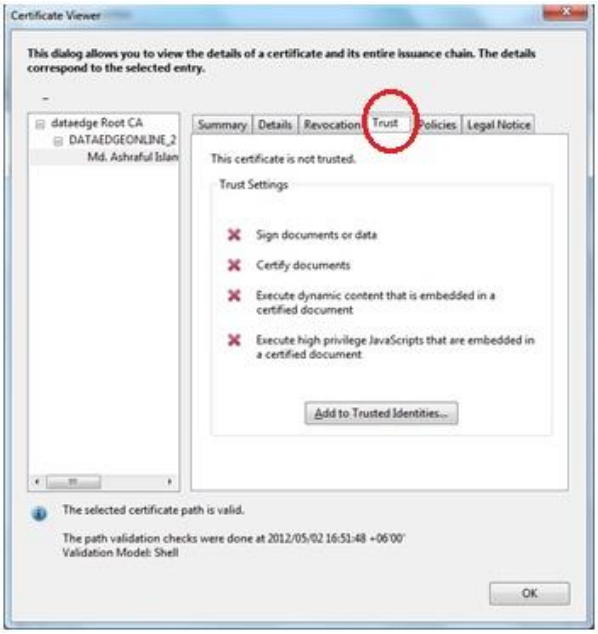


9. Click the "Details" tab, then in the right-hand window, scroll down to the "Key usage field."

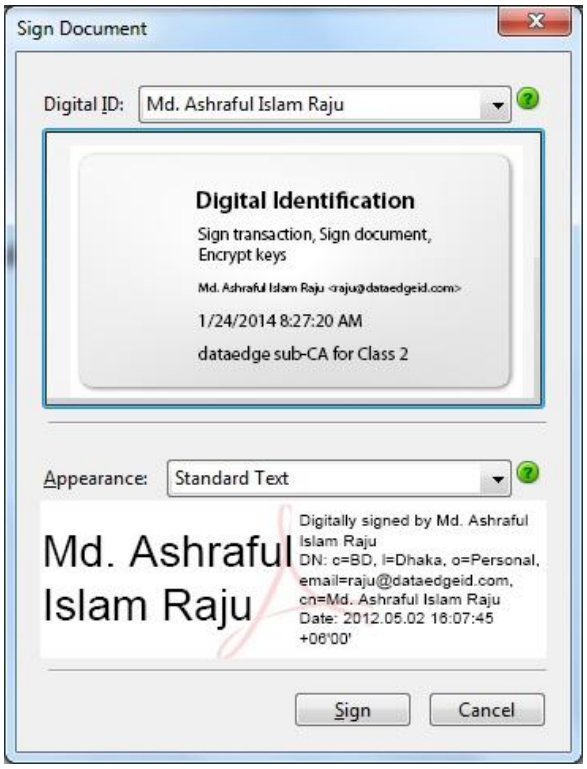


You want the certificate that says "Sign transaction, Sign document" in the Key usage value column. Click the OK button to close the window.

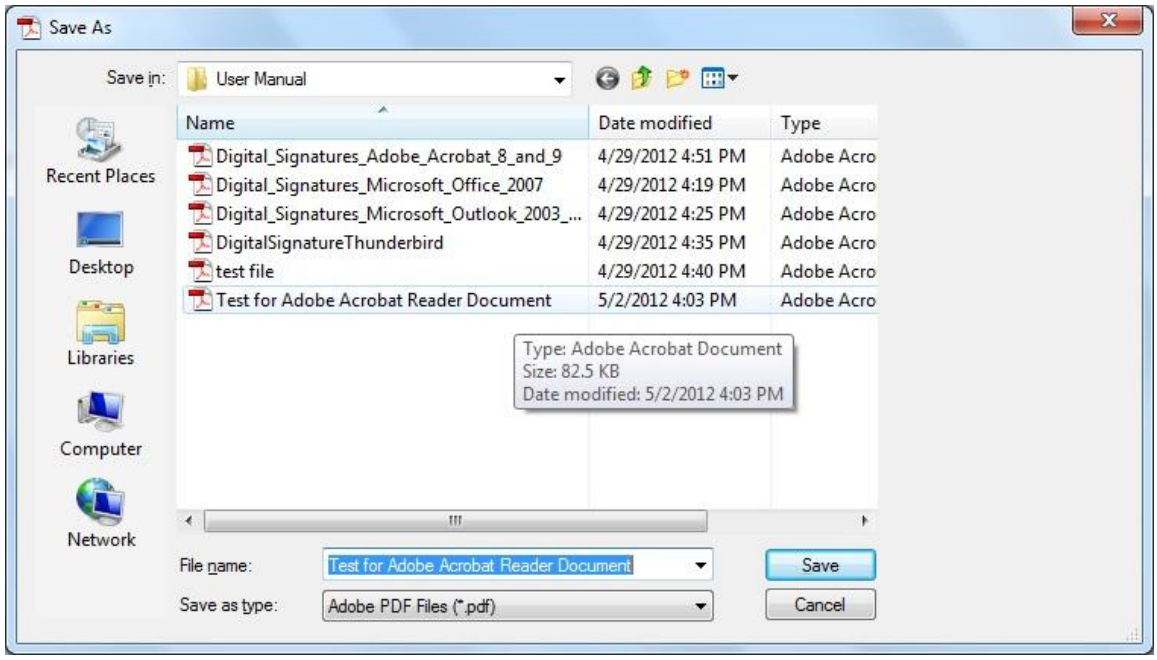
To view the trust level at this point, click the "Trust" tab. It will show there is no trust established yet, wh ich is Adobe's way of saying the document isn't signed yet. Click the OK button to close the window.



10. The Sign Document window now shows the correct certificate selected in the bottom area . Click the Sign button



11. When Acrobat prompts you, save the file. If you are working with an existing document, you may want to save it with a new name to distinguish it from the unsigned version of the document

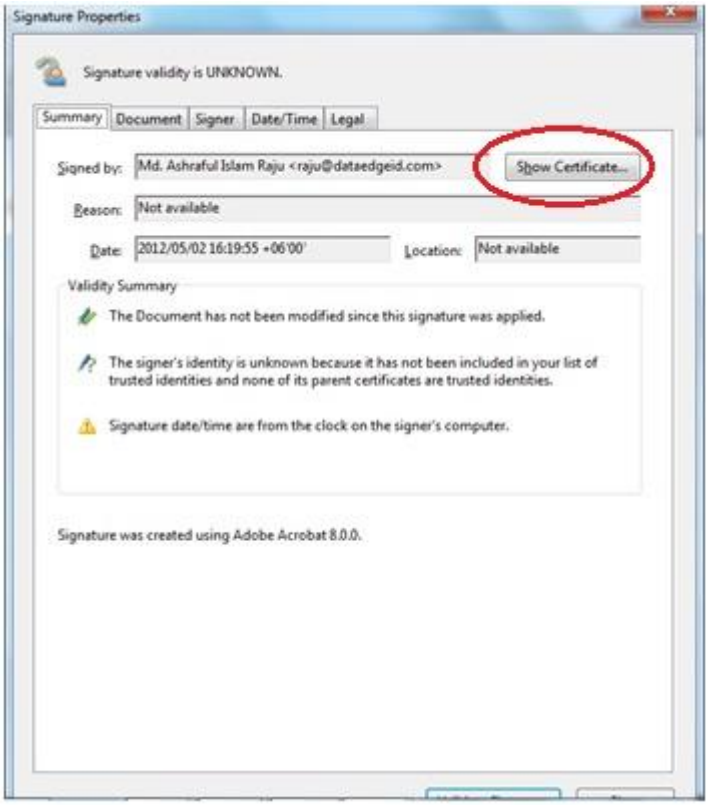


12. Your document is now signed, and you will see the digital signature representation on the document where you placed it. If the signature has a green pencil icon over the name, the signature has a valid trust. If the digital signature block has a question mark over the name, it means the signature still needs to be validated with the trust from the certificates.

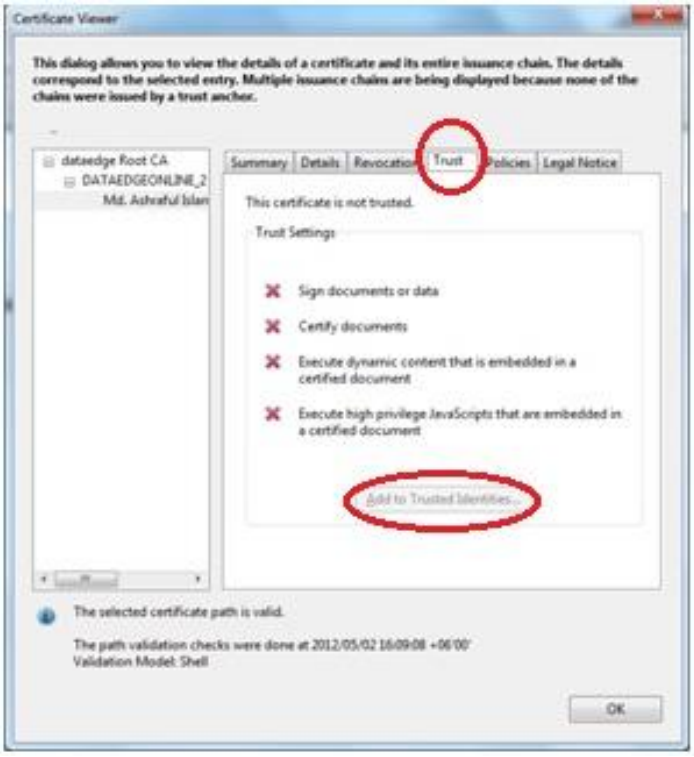
If your signature shows a question mark icon, you must to validate it through Adobe by following steps 13-17. You will only need to do this once; thereafter, you can skip to step 18.

13. Double-click the digital signature in your document to open the **Signature Properties** window,

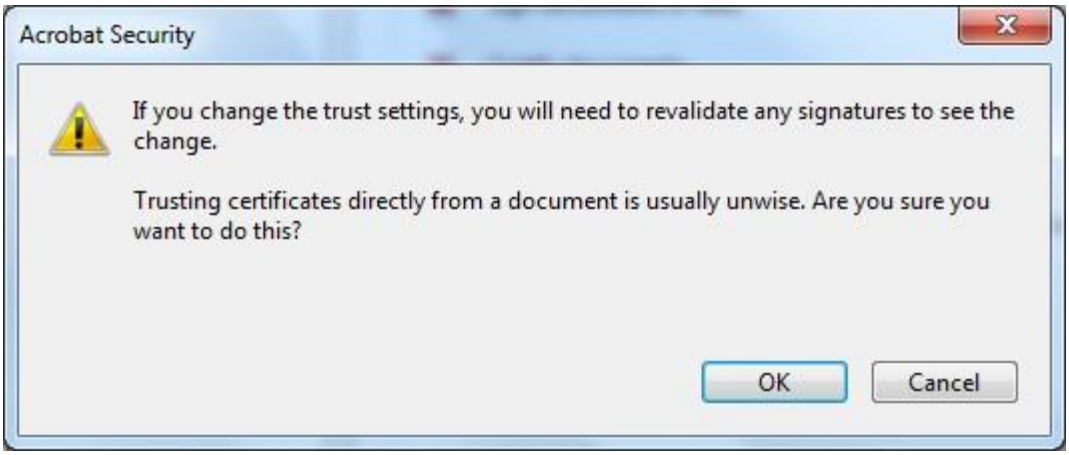
14. Click the Show Certificate button



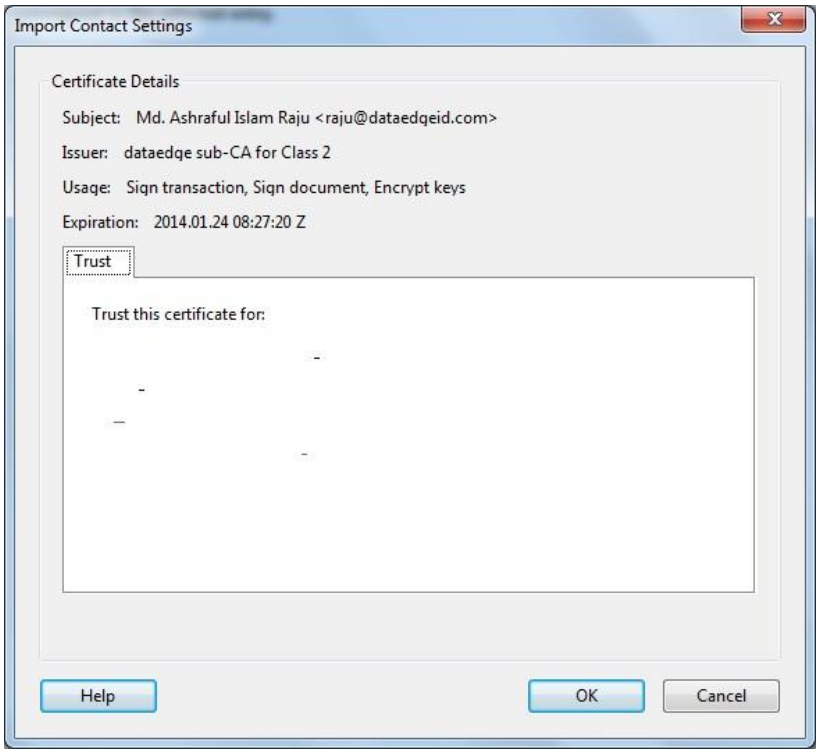
15. Click the Trust tab, then click the hierarchy in the left window to find the certificate with your name. Click the Add to Trusted Identities button.



16. Adobe warns you about trusting certificates. Since you are trusted the certificates click the OK button.



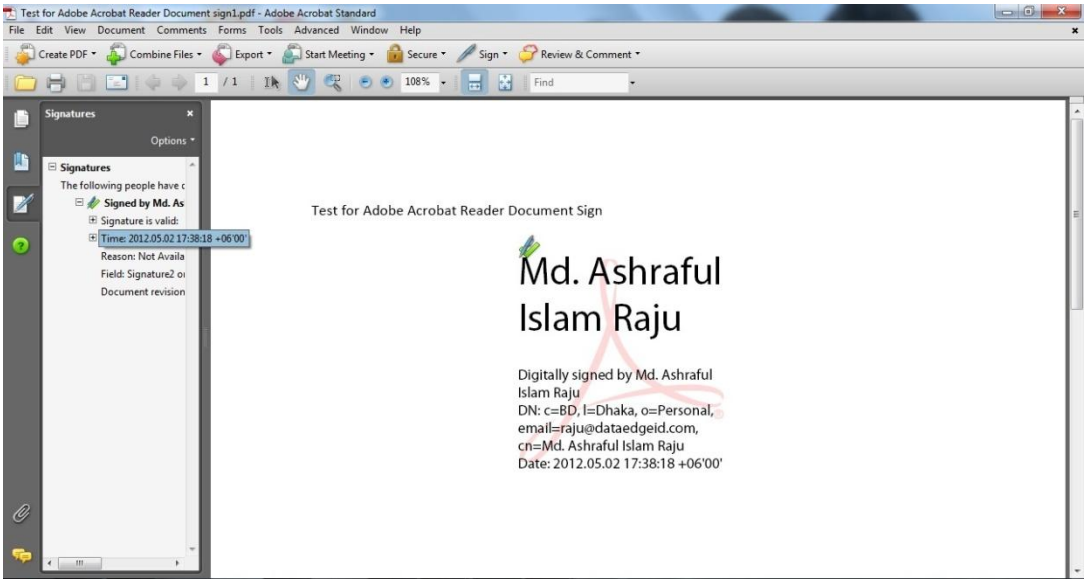
17. In the Import Contact Settings window, make sure the "Signatures and as a trusted root" option s checked, then click the OK button.



18. Your document is now digitally signed. Close it without making any changes.

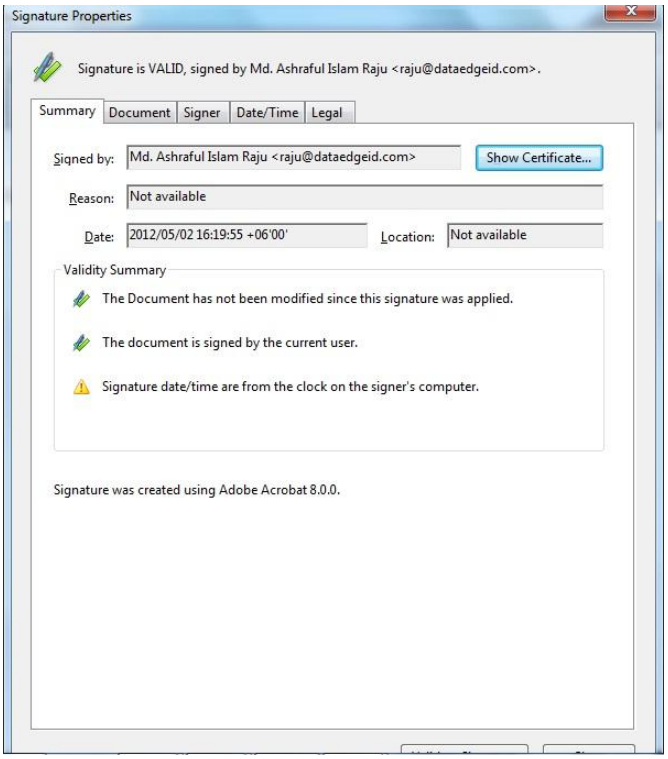
4.6 How to Verify a Digital Signature by Acrobat Reader?

1. Open the file for which you want to verify signatures.
2. You can tell the document has a digital signature because Acrobat automatically displays the Signatures panel. (If Acrobat doesn't automatically open the Signatures panel, click the Signature icon on the left-side toolbar.) The Signatures panel shows the list of the document's digital signatures and the date each was added.

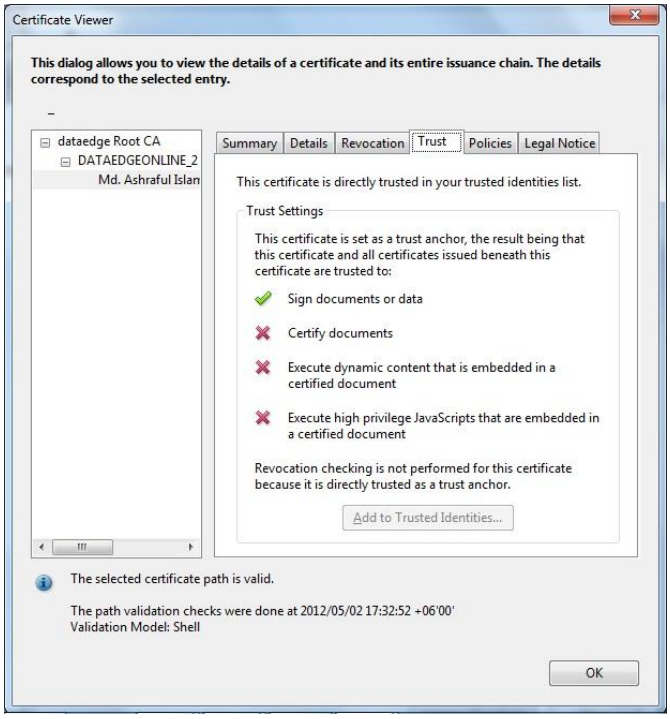


3. A graphic or text also shows where the signature was placed. You can right-click the signature block itself and select "Show Signature Properties" to see details about the signature. Click the **Signature Properties** button.

4. The Signature Properties window shows the name and when the document was signed. If you want to look at the specific certificate details, click the **Show Certificate** button.

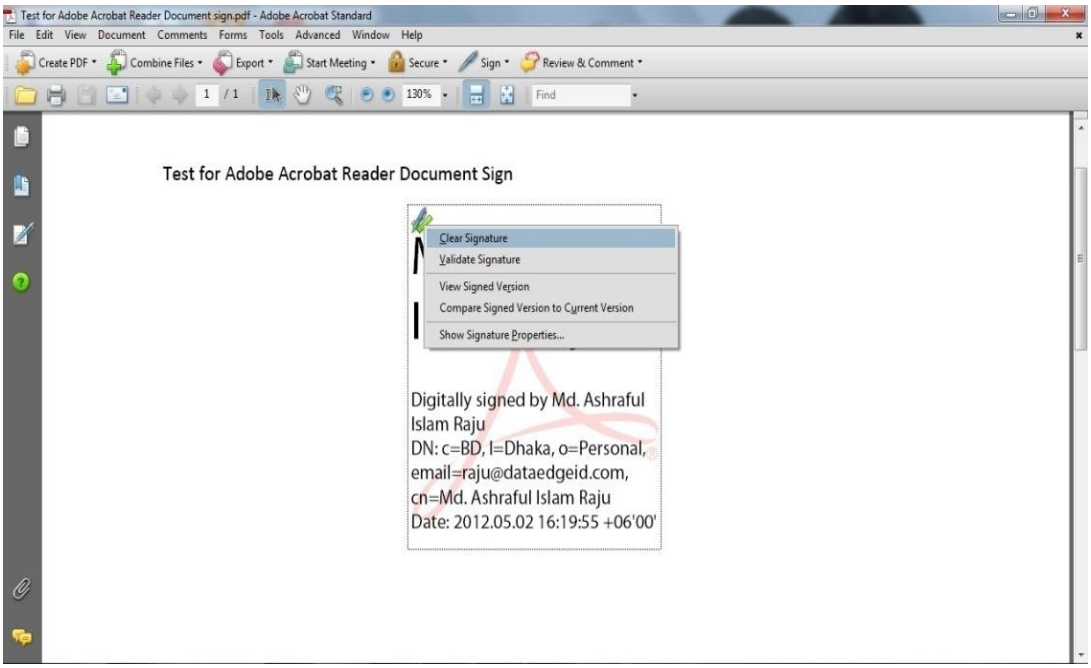


5. The Certificate Viewer window shows all the details of the certificate, including the issuance chain, whether or not the certificate is trusted, etc. Click the **OK** button to close the window, then the **Close** button to close the Signature Properties window.

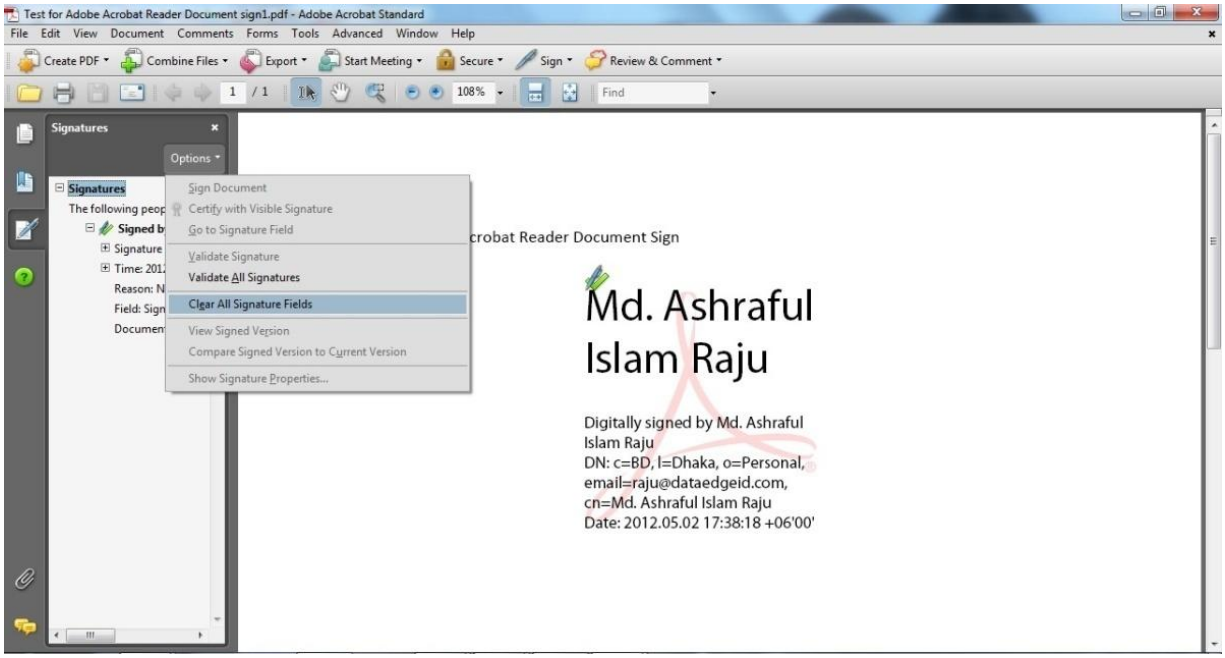


4.7 How to Remove a Digital Signature by Acrobat Reader?

1. Open the file from which you want to remove a digital signature.
2. Find the signature block of the signature you want to remove, and right-click to open the context menu. Select the Clear Signature option to remove this signature.



3. If you want to remove all the signatures at once, open the Signatures panel (click the Signature icon in the left-side toolbar). Click the Options tab in the Signatures panel, then select the "Clear All Signature Fields" option.



4. Acrobat will warn you that you can't undo this action and ask you to confirm you want to remove the signatures. Click the OK button.

5. Click OK to finish