MSEIT ECA Certificate Instructions—Using the Certificate

Instructions for using a digital certificate.

1. Using the ECA Certificate

ECA certificates are used to verify that messages or information came from a specific person, and are used to encrypt messages or information for a specific recipient. These functions are performed through a process called Public Key Infrastructure (PKI). The use of “symmetric keys” (when one key is used for each communication path) becomes unmanageable with the tremendous number of potential communication paths between senders and recipients. PKI is much more efficient than symmetric keys in that an “asymmetric key pair” is associated with any specific individual.

With the PKI key pair, the two keys are mathematically related. If information is processed with one of the keys in the key pair, then only the other key of the key pair can reverse that process. Not even the original key can reverse the process. You cannot calculate what a key is by having only the other key of the key pair.

One of these two keys is called the private key. Normally, only the owner has access to the private key. The other key is called the public key. This key is freely given to everyone to verify your identity. To ensure someone does not use their public key as your public key to act as you, a trusted Certificate Authority (CA) stores and validates all of the public keys for each person.

Typical uses of PKI are with web browsers and with e-mail. For example, if a sender digitally signs his e-mail, then he uses his private key to create the digital signature. The recipients can then decode the digital signature using the sender’s public key that has been verified with the CA. If the signature decodes properly, then, in theory, it could have only come from that particular individual. You must digitally sign as the last thing before sending an e-mail, as any change to the message content after signing will invalidate the digital signature. This ensures your message was not altered after you signed it.

When a sender encrypts an e-mail, he must use the receiver’s public key to encrypt it. Only the correct recipient has the correct private key to unencrypt the message. If the message is going to multiple recipients, the sender must have the public key for each of the recipients, as the message will be encrypted by the public keys for each individual.

A similar situation occurs with webpages and browsers. The viewer’s private key is used to validate who they are to the website via the public key, and each side’s key pair is used to encrypt the traffic in both directions so that others cannot view the information.

This is a simplified overview, and the process is much more complex. However, it is sufficient to understand how you use the ECA Certificates.

This section will provide instructions on how to use your ECA certificate for the following areas:

1. Digitally Sign or Encrypt an E-mail Message
2. Sign a PDF Using Adobe Reader
3. Signing Microsoft Word Documents
4. Moving an ECA Digital Certificate to a New Computer
5. What Do I Do If I Forget My Account Password?

1.1 Digitally Sign or Encrypt an E-mail Message

> **Note**
>
> These instructions assume that the certificate is already installed into Windows (Internet Explorer) on the same computer.

Configure Outlook with a default certificate:

1. In Outlook, go to **File > Options > Trust Center**.
2. In the Encrypted E-mail section, click the **Settings** button.
3. Define the following settings:
   - Security Settings Name (this can be named anything you would like).
   - Cryptographic Format = S/MIME.
   - Check the box "Default Security Setting for this cryptographic message format".
   - Check the box "Default Security Setting for all cryptographic messages".
4. Under the Certificates and Algorithms section, click **Choose** next to the **Signing Certificate**.
5. Select the Certificate and click **OK**.
6. (Optional) Under the Certificates and Algorithms section, click **Choose** next to the **Encryption Certificate**.
7. Select the Certificate and click **OK**.
8. After both the Signing and Encryption Certificate fields have been populated, click OK to apply the settings.

1.1.1 Choosing to Sign and/or Encrypt Individual E-mails

In Outlook, before you can send an encrypted message, you must have the recipient's digital signature. Complete the following steps to add a digital signature to your address book in Outlook:

1. Open Outlook.
2. Open a digitally signed e-mail message from the sender that you want to add to your address book.
3. Right-click on the return address.
4. In the pop-up menu, select **Add to Outlook Contacts**.
5. Select **Save**. A new pop-up window appears.
6. Under **View Source**, select the **Outlook (Contacts)** link to open the Outlook contact information.
7. Select **Certificates** to view the certificates information of the Outlook contact
    a. If there is a certificate name listed, select Save and Close.
    b. If there is no certificate information listed, go to the Add Certificate to existing Outlook Contact section.

The sender's information will then be added to your address book.

For a first time external recipient, you must add the address to your contact list using the steps above. Once the address is added, these steps work for internal and external recipients, either with or without publishing to the Global Address List (GAL). In order to publish your certificate to the GAL, see the ECA Export and Publish Cert Instructions.

Within the e-mail message, to send an encrypted email, do the following. This applies when sending internal or external email.

1. In the email window, select **Options**.
2. Select **Encrypt**.
3. Compose and send the email.
4. If prompted, enter the PIN to your smartcard.

Digitally signing an e-mail ensures the recipient that the e-mail has been sent from a specific e-mail address and the message has not been altered. Encrypting e-mails will prevent anyone but the intended recipient from viewing the message with the corresponding certificate.

Video instructions:

https://www.identrust.com/certificates/eca/set_up_outlook_sign_encrypt_video.html
https://www.identrust.com/certificates/eca/add_sign_encrypt_icons_video.html
https://www.identrust.com/certificates/eca/request_public_keys_video.html

1.1.2 Adding Certificate to an Existing Outlook Contact

> **Note**
>
> During the upgrade to GCC, many certificates were stripped from existing Outlook Contacts.

If you do not have the contact's certificate exported to a file, see Exporting a Contact's Certificate.

1. In an email from the contact, right-click the contact email address/name and select **Open Contact Card**.
2. Under **View Source**, select the **Outlook (Contacts)** link to open the Outlook contact information.
3. Select **Certificates** to view the certificates information of the Outlook contact.
4. Select the **Import…** button.
5. Select the contact's **.CER** file. The contact certificate name appears.
6. Click **Save & Close**.

1.1.3 Exporting a Contact's Certificate (to Later Import into Outlook Contacts)

1. In a signed email from the contact, click the **signed email** icon.
2. Select the **Details** button in the popup window.
3. Select **Signer: name@company.com** bottom layer in the new popup window.
4. Select the **View Details** button.
5. Select the **View Certificate** button in the new popup window.

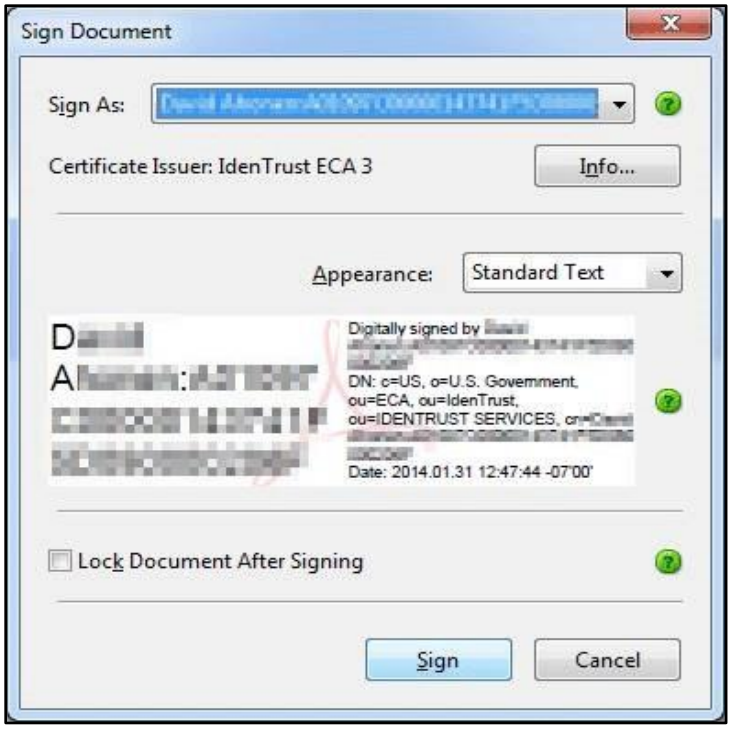
6. Select the **Details** tab.
7. Select the **Copy to File**… button.
8. Follow the steps in the **Certificate Export Wizard** window (the default format of "DER encoded binary X.509 (.CER)" is fine).
9. Close all the popup windows.

1.2 Signing a PDF using Adobe Reader

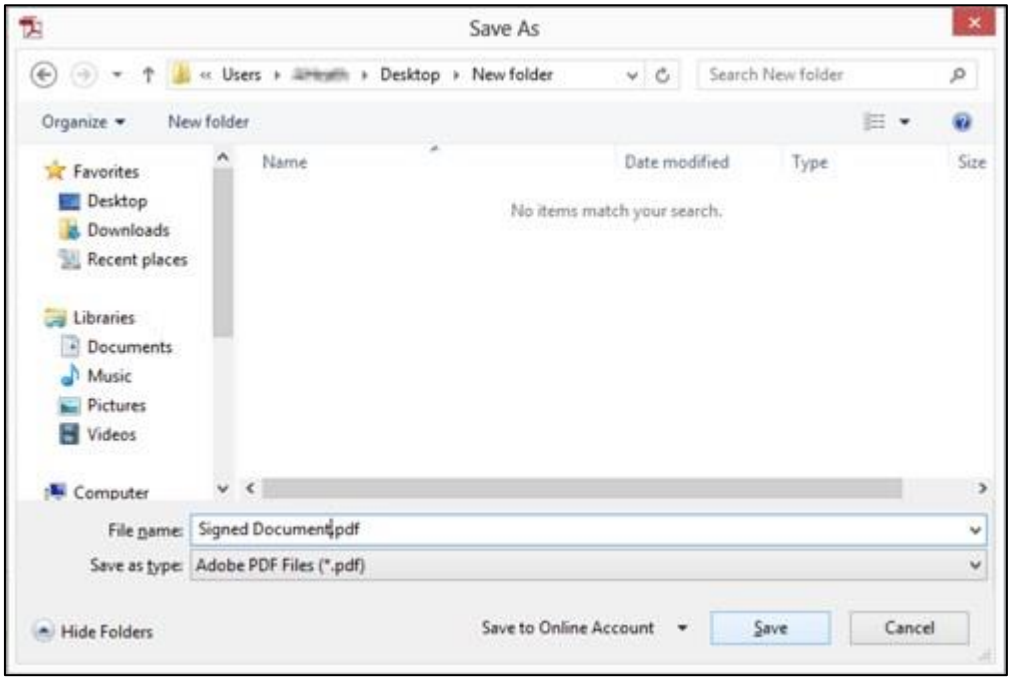
Most PDFs that you will receive will come pre-made with a signature box similar to the one shown below.

1. Once you have filled out the document, click inside the signature box.

2. This will open "Sign Documents" window. Here, you will be able to select the Certificate you wish to use to sign your document. If you have more than one certificate, you will be able to select the correct certificate by clicking on the "Sign As" dropdown box.

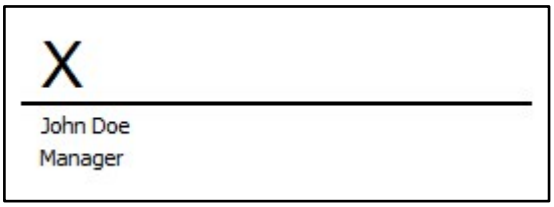


3. Once the appropriate certificate is selected, click **Sign**. The “Save As” dialogue box will appear. Select the location you would like to save the signed PDF to and click **Save**.



1.3 Signing Microsoft Word Documents

1. When you receive a Word document that requires a signature, first complete the form as required, then locate the signature box (as shown below).



2. To sign, double-click the signature line. This will open the **Sign** window.

3. Type your name on the line marked by the X.

4. Next, confirm that the correct certificate is selected. If the wrong certificate is selected, click **Change** and chose from a list of your certificates. Click **Sign**.

1.4 Moving an ECA Digital Certificate to a New Computer

Your IdenTrust certificate is composed of two separate files: an encryption certificate and a signing certificate. Make sure when moving your certificate that you make an operational copy of both files.

If your certificate is housed on a smart card or token, please install the SafeNet software onto the new computer, reboot it, and insert the smart card or token. Your certificate will then be ready for use on the new machine. If you would like to test the certificate, refer to section 10.2.3 Test Your Certificates for instructions.

1.4.1 Importing your ECA Browser-based Certificates to the New Computer

1. Locate the backup file previously saved/exported.
2. Double-click the file. The **Certificate Import Wizard** will open. Click **Next** twice.
3. Type in the password that was chosen when exporting the certificate. The check boxes on this screen are optional, but it is recommended to check them. Here is the description of each:
    - Mark the Private Key as Exportable: If this is not chosen, then you can never export this certificate from this computer in the future.
    - Enable Strong Private Key Protection.
    - Include all extended properties.
4. Click **Next**.
5. Select **Automatically select the certificate store based on the type of Certificate** and **Next**.

6. If **Enable Strong**... was chosen, then the **Importing a new private exchange key** window will open. By default, it is set to medium security. If you choose to use high security, click the **Set Security Level** button, and follow the instructions there.
7. The **Importing a new private exchange key** window will open. Click **OK**.
8. The **import was successful** will appear. Click **OK**.

1.4.2 Testing your Certificates

Enter www.identrust.com/test into your browser to test your certificates.

1.5 What Do I Do If I Forget My Account Password?

If you have forgotten your password, and know your account number, you can request automated password assistance by following these simple steps.

1. Enter www.IdenTrust.com into your browser.
2. Click the **Certificate Management Center**.
3. Click the orange login prompt on the left-hand side of the screen.
4. When the Choose a digital certificate window appears, click **Cancel**.
5. Enter your account number and click the **I forgot my password** link.
6. You will receive an e-mail with instructions on how to reset your password.

> **Note**
>
> IdenTrust does not have access to any passwords, and therefore does not have the ability to reset them for you. If you forget your password, and you are unable to reset your password through the instructions above, you will need to apply for and repurchase a new digital certificate.