MSEIT ECA Certificate Instructions—Part 2

You must have completed sections 1-7 in Part 1 of the ECA Certificate Instructions before beginning section 8.

You must have received the IdenTrust certification retrieval packet before completing the following sections.

8. Required Certificate Export and Publication

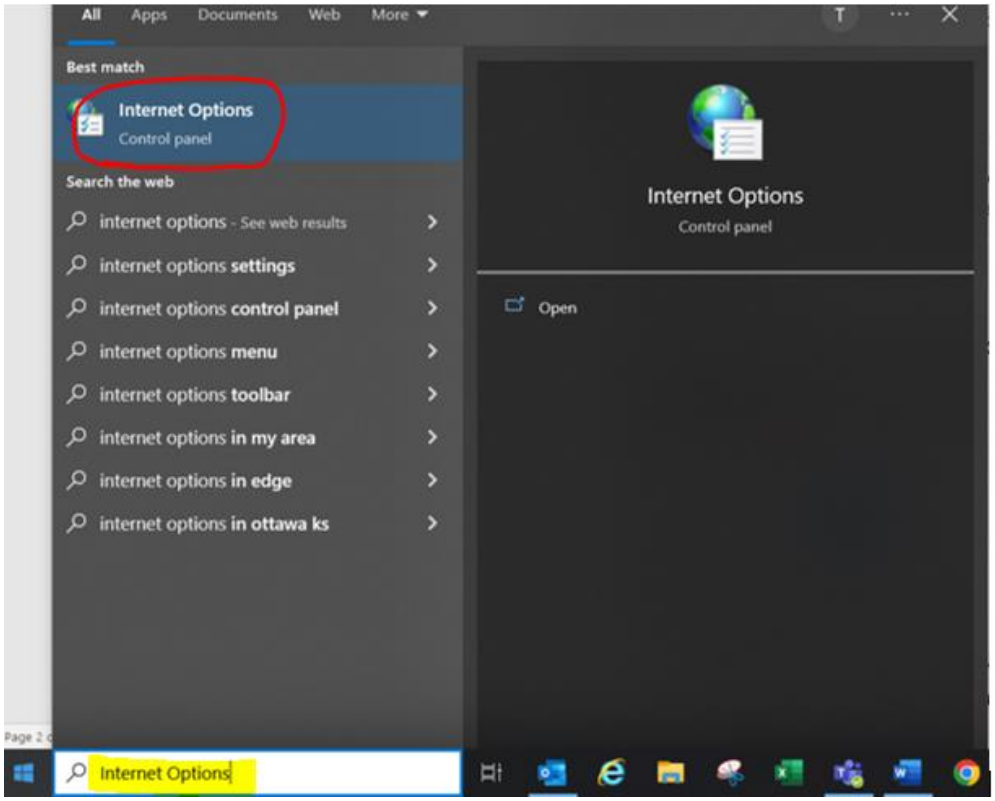
The certificate must first be exported from your computer and then sent to the eMC2 team so it can be imported into your account. After that is completed, you will be able to use it to access eMC2. Once exported, you will also need to publish the certificate to the Global Address List (GAL) in order to digitally sign and decrypt emails.

Remember that when you renew your certificate (e.g., when it expires), you must send the webmaster your updated certificate to continue to use eMC2.

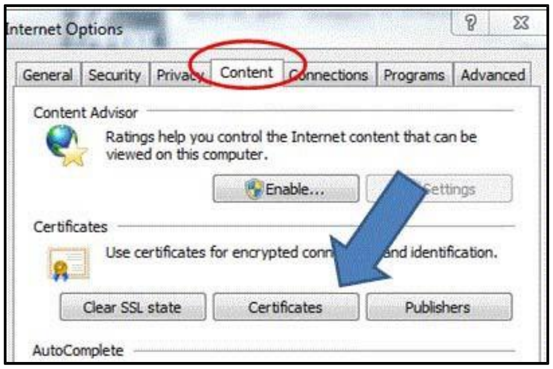
8.1 Export your Certificate for eMC2 Access

1. If you are using a DoD CAC, insert it into your card reader. You must have completed the process of making the certificates available in Windows. If you are using an IdenTrust Smart Card, ensure that you have already imported it into your Windows system.

2. In your Windows Search bar (bottom left of your computer), type **Internet Options**. Open **Internet Options Control Panel**.



3. From the Internet Options Window, navigate to **Content > Certificates**.



If you are using **Chrome** or **Edge** for your browser, perform the following steps:

a. At the top right of the browser window, click the three dots. Navigate to **Settings** > **Privacy and security** > **Security**.

b. Click **Manage Certificates**.

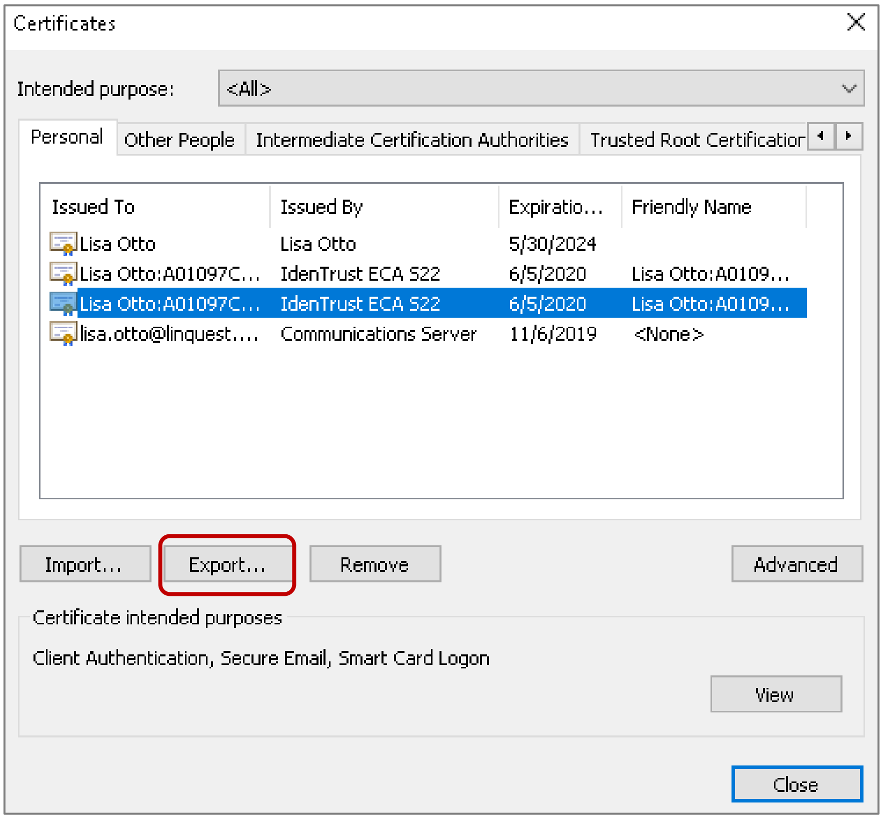
c. On the **Personal** tab, highlight your Identrust certificate with your name and valid expiration date. This is not your email certificate.

d. Click **Export**, then click **Next** until you reach the window that says Browse. Save your file to your computer and close the browser.

e. Continue to step 16 to rename the file and send to the webmaster.

4. On the **Personal** tab, highlight your Identrust certificate with your name and valid expiration date. This is **not** your email certificate. For CAC users, do **not** select the DOD E-Mail CA-XX.

5. Click **Export**.



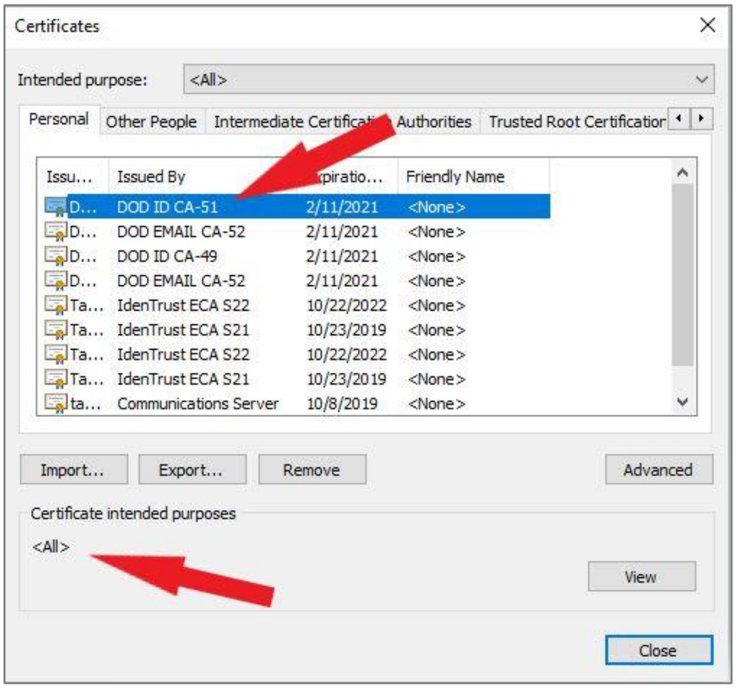
Intended purpose: <All>

Issued To	Issued By	Expiratio...	Friendly Name
Lisa Otto	Lisa Otto	5/30/2024	
Lisa Otto:A01097C...	IdenTrust ECA S22	6/5/2020	Lisa Otto:A0109...
Lisa Otto:A01097C...	IdenTrust ECA S22	6/5/2020	Lisa Otto:A0109...
lisa.otto@linquest....	Communications Server	11/6/2019	<None>

Certificate intended purposes

Client Authentication, Secure Email, Smart Card Logon

CAC cert users looks similar to this:



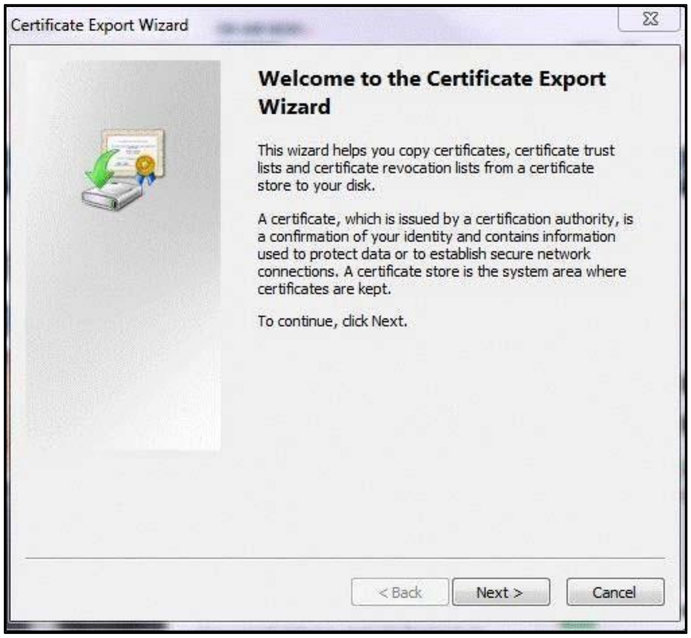
Intended purpose: <All>

Issu...	Issued By	xpiratio...	Friendly Name
D...	DOD ID CA-51	2/11/2021	<None>
D...	DOD EMAIL CA-52	2/11/2021	<None>
D...	DOD ID CA-49	2/11/2021	<None>
D...	DOD EMAIL CA-52	2/11/2021	<None>
Ta...	IdenTrust ECA S22	10/22/2022	<None>
Ta...	IdenTrust ECA S21	10/23/2019	<None>
Ta...	IdenTrust ECA S22	10/22/2022	<None>
Ta...	IdenTrust ECA S21	10/23/2019	<None>
ta...	Communications Server	10/8/2019	<None>

Certificate intended purposes

<All>

6. Click **Next**.



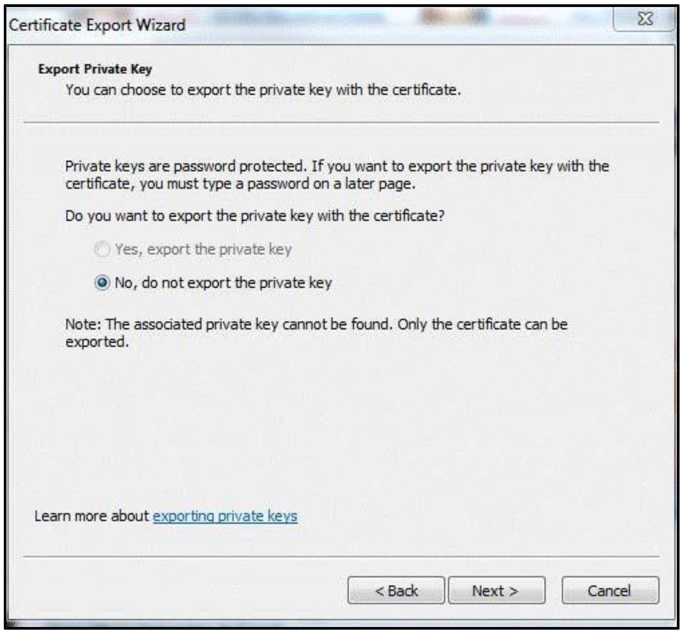
Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

7. Click **Next**. The option **No, do not export the private key** should be selected by default.



Export Private Key
You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

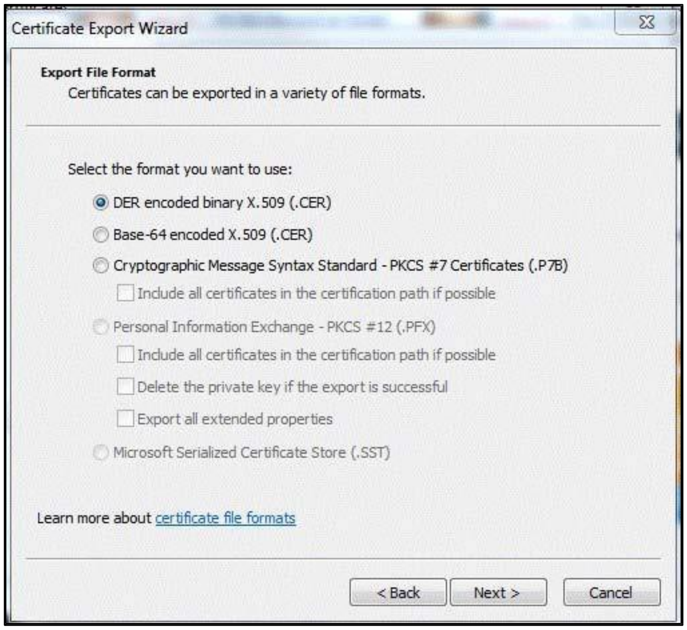
○ Yes, export the private key

● No, do not export the private key

Note: The associated private key cannot be found. Only the certificate can be exported.

Learn more about exporting private keys

8. Select the DER (.CER) format **only**, and click **Next**.



Certificate Export Wizard

Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

● DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

○ Personal Information Exchange - PKCS #12 (.PFX)

□ Include all certificates in the certification path if possible

□ Delete the private key if the export is successful

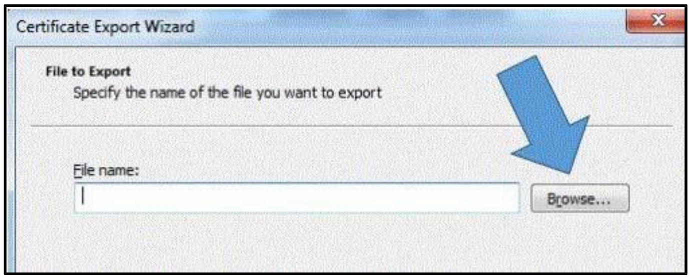
□ Export all extended properties

○ Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

9. Save file as **Firstname M Lastname.cer** into your Desktop or Documents folder by selecting the **Browse** button and navigating to the location of your choice to save the file.

   In the example below, it is being saved to a subfolder "cert" in Documents for safekeeping.

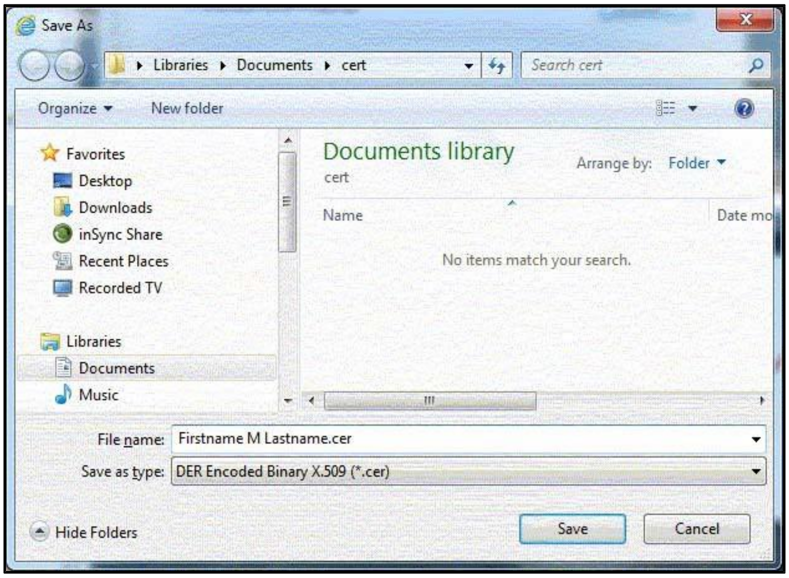


Certificate Export Wizard

File to Export

Specify the name of the file you want to export

File name:

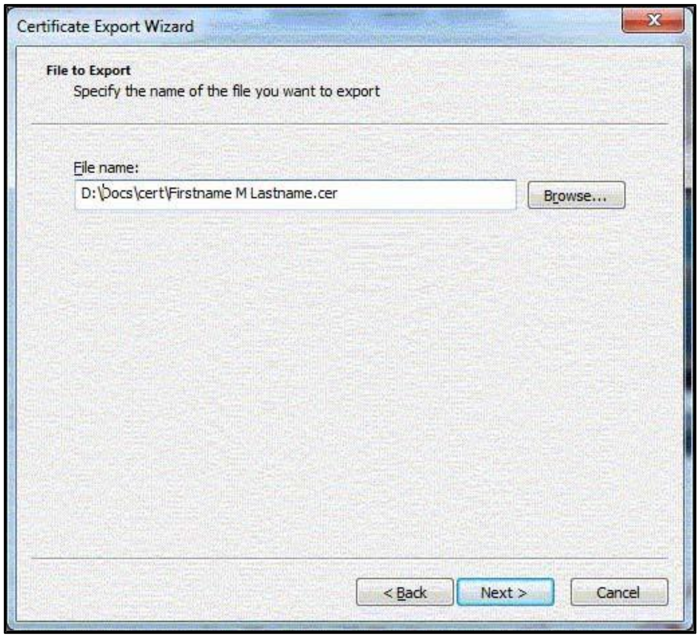


No items match your search.

File name: Firstname M Lastname.cer

Save as type: DER Encoded Binary X.509 (*.cer)

10. Click **Save**. It should look similar to this.

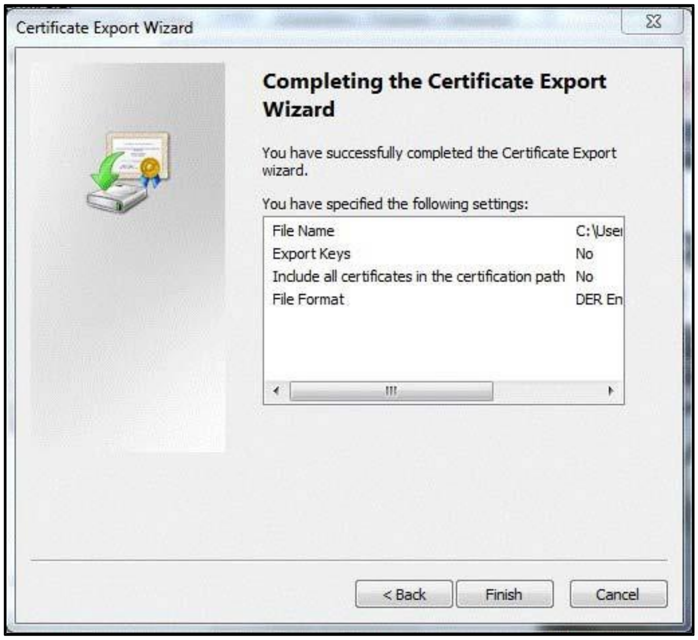


Specify the name of the file you want to export

File name: D:\Docs\cert\Firstname M Lastname.cer

11. Click **Next**.

12. Click **Finish**; you should see a pop-up telling you that the export was successful.

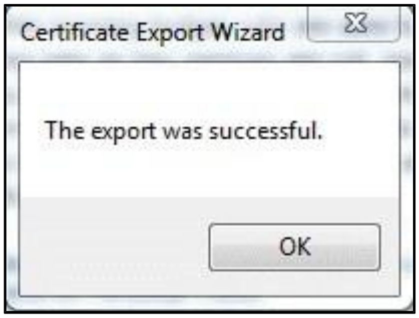


Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

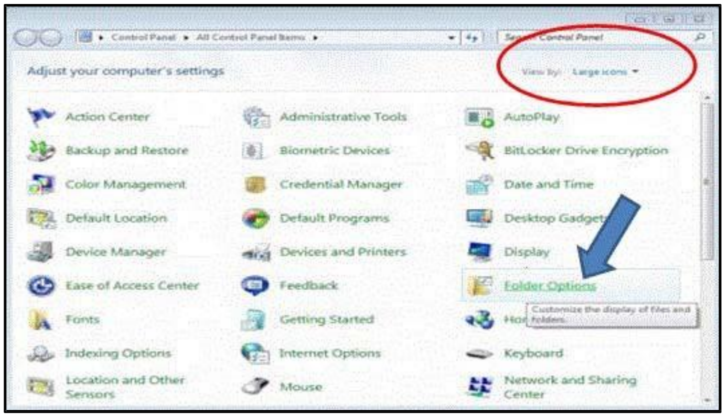
File Name	C:\Use
Export Keys	No
Include all certificates in the certification path	No
File Format	DER En



The export was successful.

13. Due to the .cer extension name, it is necessary to have proper view settings on your computer in order to see the file in the following steps. To verify the setting, open the Control Panel from your Start Menu and click **Folder Options**.

> **Note**
>
> If Folder Options is not available, change your “view by” settings to **View by Large Icons** at the top right of the Control Panel.



Control Panel ▸ All Control Panel Items ▸

Search Control Panel

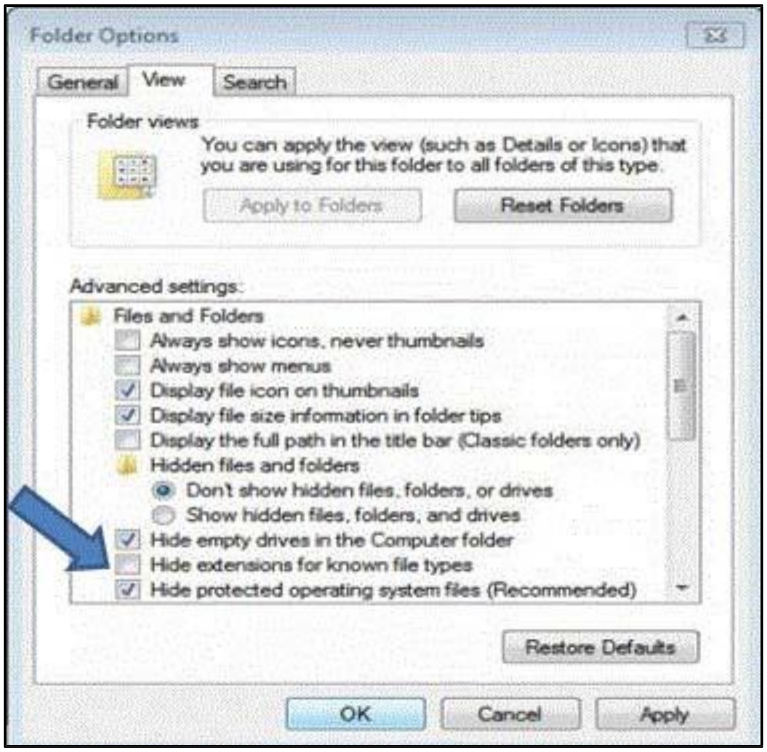
Adjust your computer's settings

View by: Large icons ▾

Action Center
Backup and Restore
Color Management
Default Location
Device Manager
Ease of Access Center
Fonts
Indexing Options
Location and Other Sensors
Administrative Tools
Biometric Devices
Credential Manager
Default Programs
Devices and Printers
Feedback
Getting Started
Internet Options
Mouse
AutoPlay
BitLocker Drive Encryption
Date and Time
Desktop Gadgets
Display
Folder Options
HomeGroup
Keyboard
Network and Sharing Center

Customize the display of files and folders.

14. Select the **View** tab in the Folder Options window. Then, deselect **Hide extensions for known file types**.



Folder Options

General | View | Search

Folder views

You can apply the view (such as Details or Icons) that you are using for this folder to all folders of this type.

Apply to Folders | Reset Folders

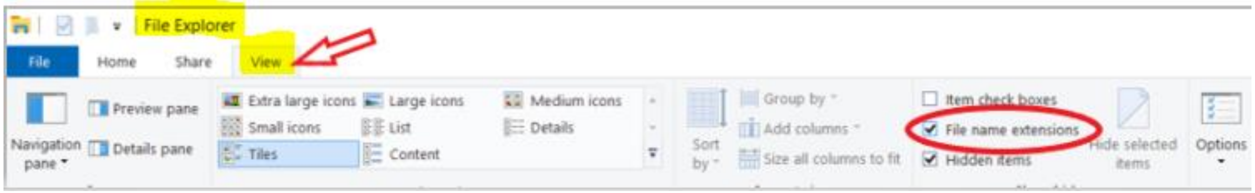
Advanced settings:

Files and Folders
☐ Always show icons, never thumbnails
☐ Always show menus
☑ Display file icon on thumbnails
☑ Display file size information in folder tips
☐ Display the full path in the title bar (Classic folders only)
Hidden files and folders
● Don't show hidden files, folders, or drives
○ Show hidden files, folders, and drives
☑ Hide empty drives in the Computer folder
☐ Hide extensions for known file types
☑ Hide protected operating system files (Recommended)

Restore Defaults

OK | Cancel | Apply

You can also open Windows File Explorer > **View** to see file extensions. Add a check mark to **File name extension**.



File Explorer

File | Home | Share | View

Navigation pane ▾ | Preview pane | Details pane

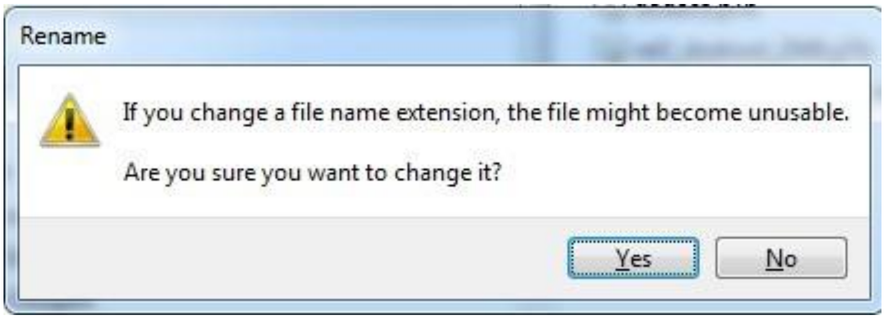
Extra large icons | Large icons | Medium icons | Small icons | List | Details | Tiles | Content

Sort by ▾ | Group by ▾ | Add columns ▾ | Size all columns to fit

☐ Item check boxes
☑ File name extensions
☑ Hidden items

Hide selected items | Options ▾

15. Click **OK** to save the changes.
16. Navigate to the file that was saved in the previous step and rename the file. Change the .CER to **.TXT**. This is necessary because some e-mail systems deem this as a malicious file and will block it. You may get the following warning box; if so, click **Yes**.



Rename

If you change a file name extension, the file might become unusable.

Are you sure you want to change it?

17. E-mail the file to webmaster@linquest.com for processing.

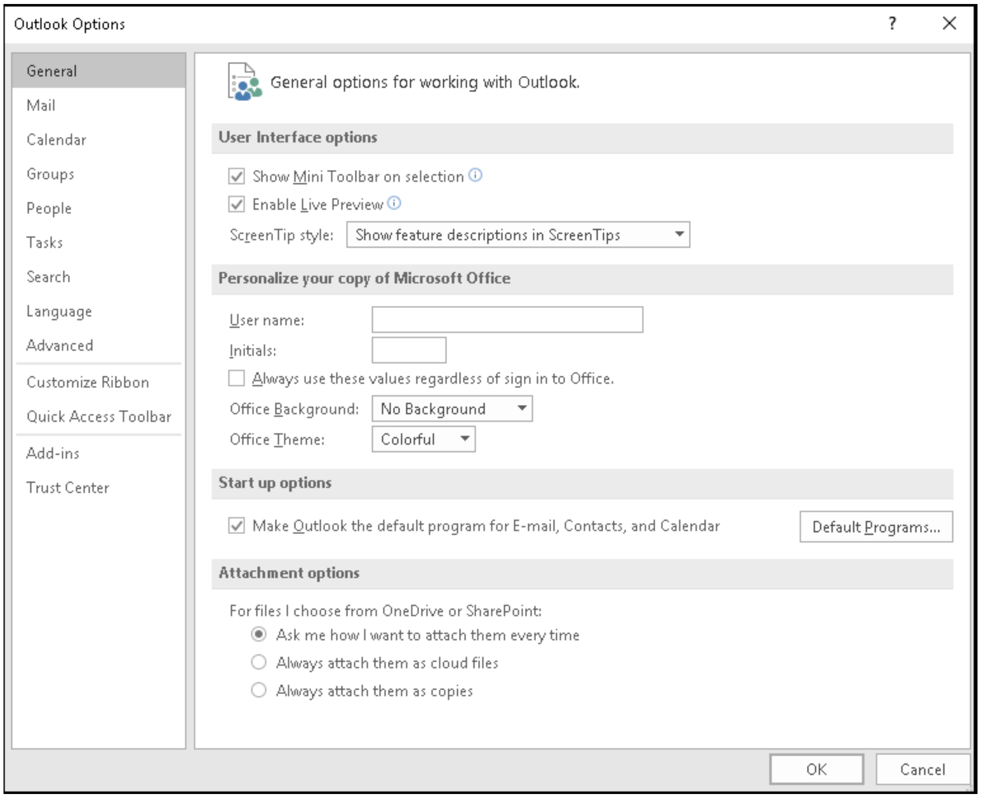
8.2 Publish Certificates to the Global Address List (GAL)

Once you have exported the certificate, you must upload this certificate to the GAL in Outlook in order to digitally sign and decrypt emails sent to you. If you have multiple Outlook accounts, you will not have the option to publish to GAL.

> **Warning**
>
> If for any reason you have updated the ECA certificate, and previously had your ECA certificate loaded in the GAL, then you need to contact IT to remove the old ECA certificate before loading the new one.

Follow the steps below:

1. In Outlook, go to **File > Options**.



General options for working with Outlook.

User Interface options

☑ Show Mini Toolbar on selection

☑ Enable Live Preview

ScreenTip style: Show feature descriptions in ScreenTips

Personalize your copy of Microsoft Office

User name:

Initials:

□ Always use these values regardless of sign in to Office.

Office Background: No Background

Office Theme: Colorful

Start up options

☑ Make Outlook the default program for E-mail, Contacts, and Calendar

Attachment options

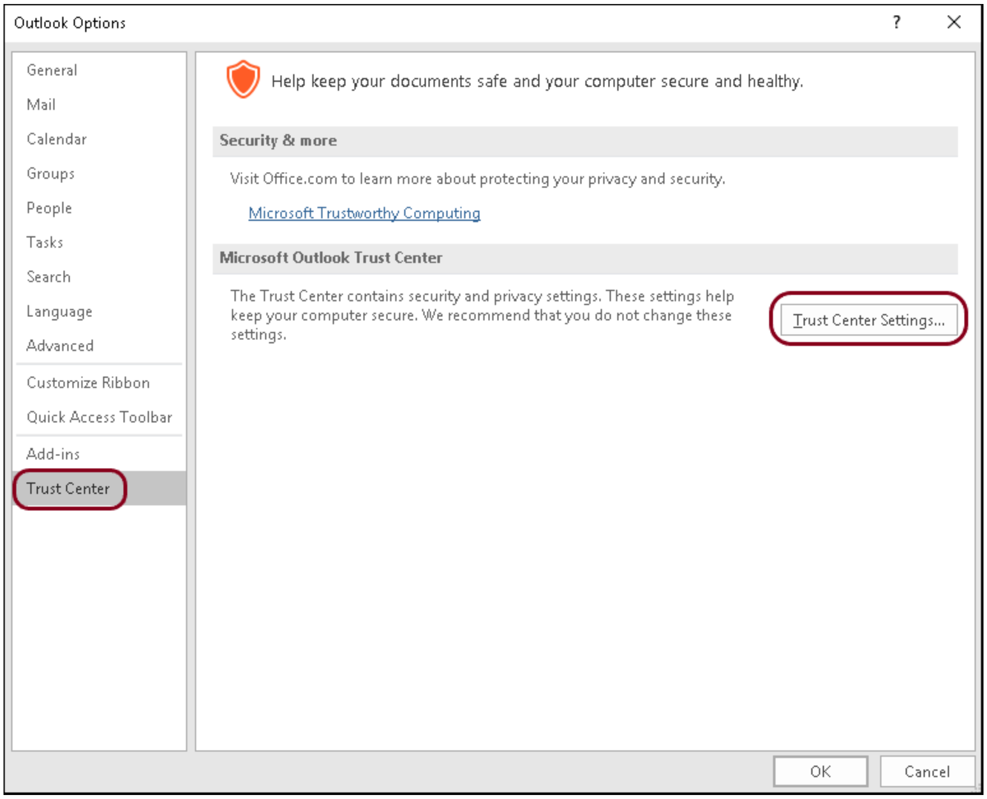
For files I choose from OneDrive or SharePoint:

● Ask me how I want to attach them every time

○ Always attach them as cloud files

○ Always attach them as copies

2. Click **Trust Center > Trust Center Settings**.



Help keep your documents safe and your computer secure and healthy.

Security & more

Visit Office.com to learn more about protecting your privacy and security.

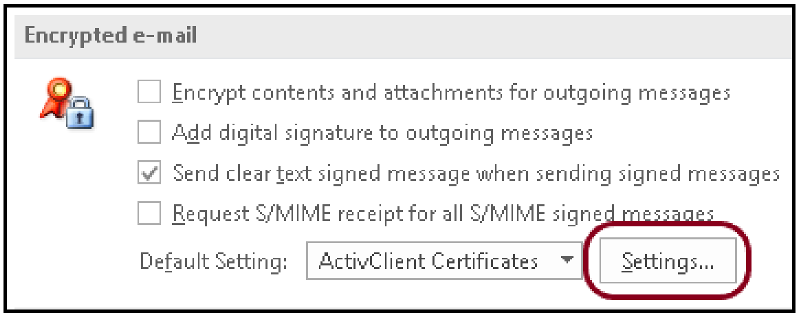
Microsoft Trustworthy Computing

Microsoft Outlook Trust Center

The Trust Center contains security and privacy settings. These settings help keep your computer secure. We recommend that you do not change these settings.

3. Click **Email Security**. In the Encrypted e-mail section, you must verify the Default Setting is correct. If you recently installed a new certificate, Outlook should default to the new cert. If you have previously had a certificate linked and have since updated it, you need to verify that you are linking to the updated cert. To do that, complete the following:

   a. Next to the Default Settings droplist, click the **Settings** button.



Encrypted e-mail

□ Encrypt contents and attachments for outgoing messages

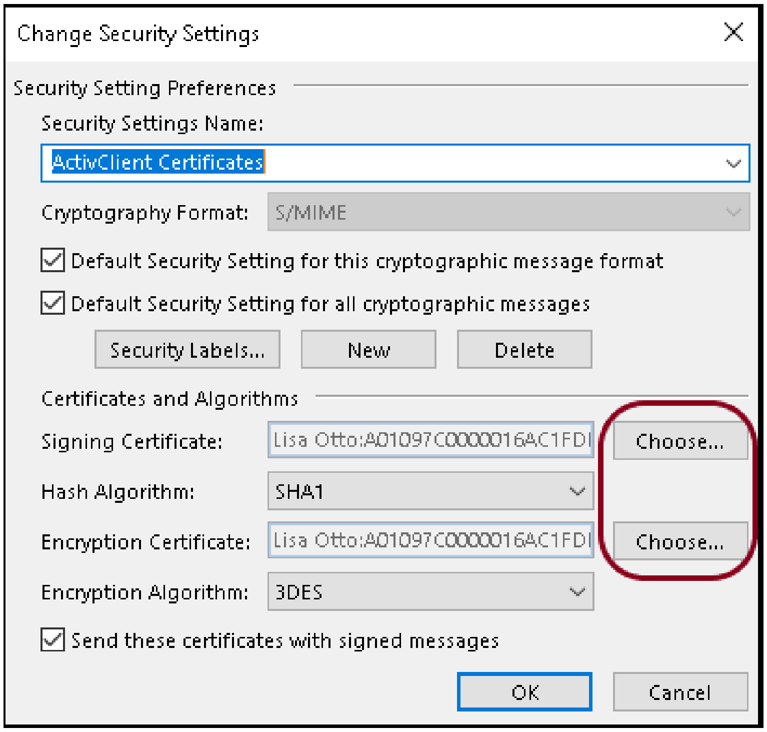
□ Add digital signature to outgoing messages

☑ Send clear text signed message when sending signed messages

□ Request S/MIME receipt for all S/MIME signed messages

Default Setting: ActivClient Certificates

   b. You will need to verify the updated certificate for both the Signing Certificate and the Encryption Certificate. Click the **Choose** button.



Change Security Settings

Security Setting Preferences

Security Settings Name: ActivClient Certificates

Cryptography Format: S/MIME

☑ Default Security Setting for this cryptographic message format

☑ Default Security Setting for all cryptographic messages

Certificates and Algorithms

Signing Certificate: Lisa Otto:A01097C0000016AC1FDI

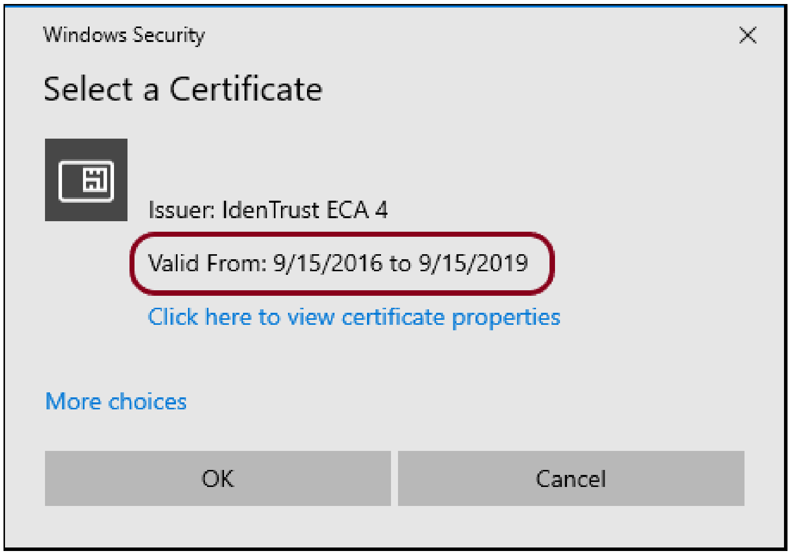
Hash Algorithm: SHA1

Encryption Certificate: Lisa Otto:A01097C0000016AC1FDI

Encryption Algorithm: 3DES

☑ Send these certificates with signed messages

c. You will see the certificate currently associated. This example shows an outdated cert linked to Outlook.



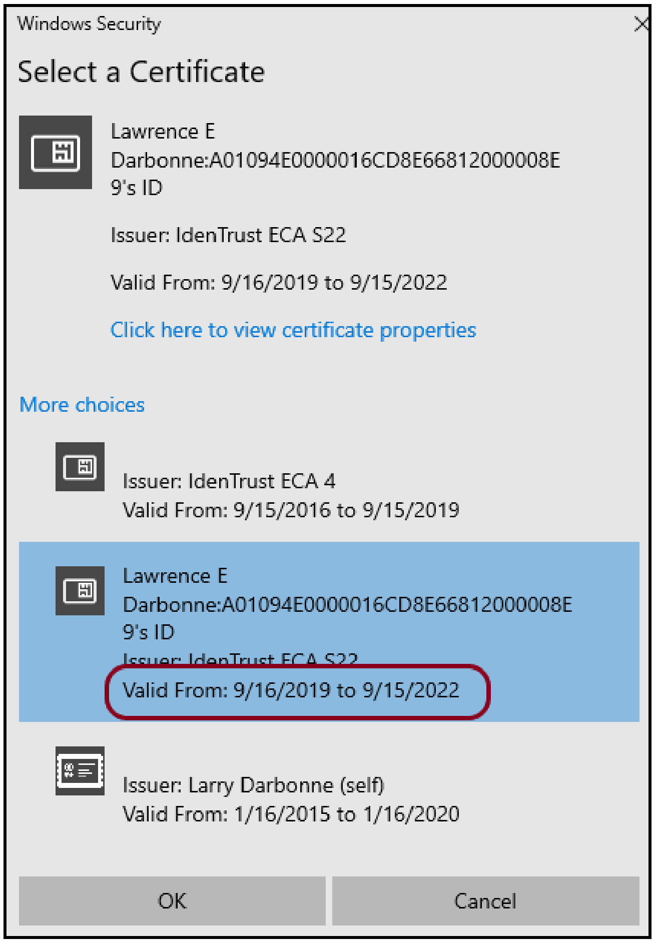
Windows Security

Select a Certificate

Issuer: IdenTrust ECA 4

Valid From: 9/15/2016 to 9/15/2019

d. If the cert is outdated, click **More choices**. You will see a list of certificates to choose from. Select the certificate with the updated dates.



Windows Security

Select a Certificate

Lawrence E Darbonne:A01094E0000016CD8E66812000008E 9's ID

Issuer: IdenTrust ECA S22

Valid From: 9/16/2019 to 9/15/2022

Click here to view certificate properties

More choices

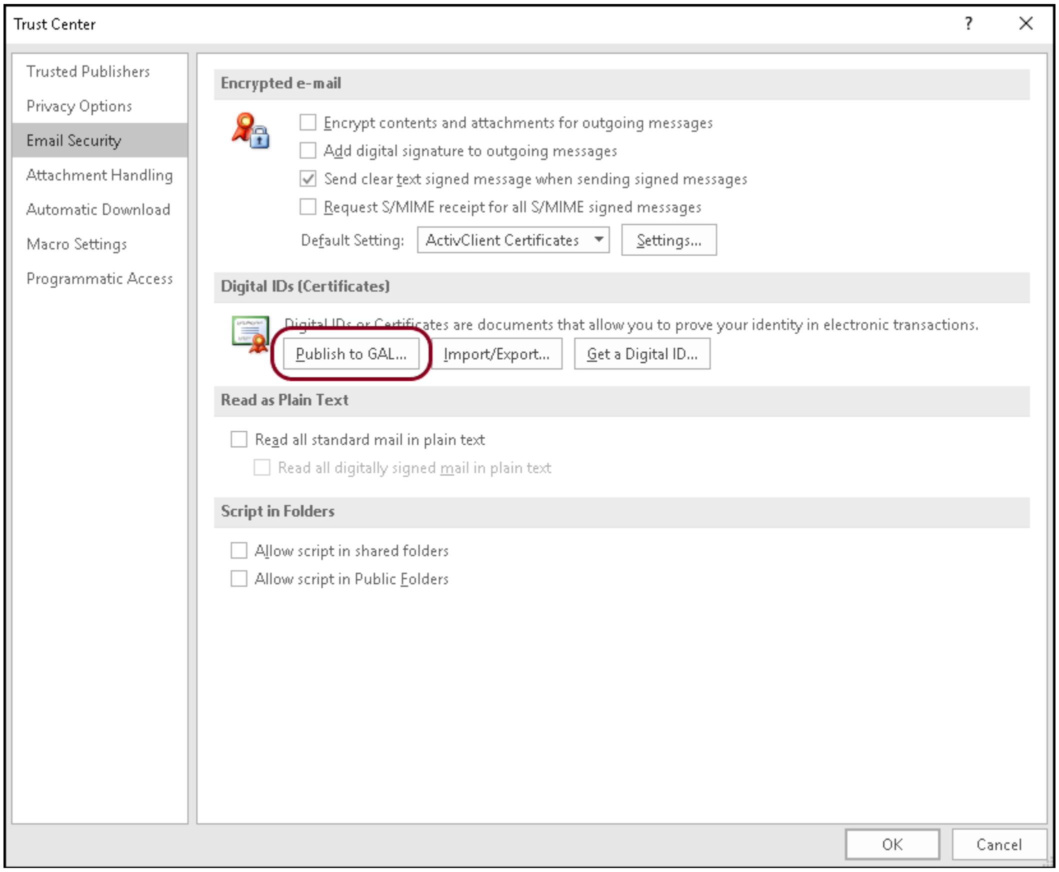
Issuer: IdenTrust ECA 4
Valid From: 9/15/2016 to 9/15/2019

Lawrence E Darbonne:A01094E0000016CD8E66812000008E 9's ID
Issuer: IdenTrust ECA S22
Valid From: 9/16/2019 to 9/15/2022

Issuer: Larry Darbonne (self)
Valid From: 1/16/2015 to 1/16/2020

e. Click **OK**. Remember to select the updated certificates for both the Signing and Encryption options. Once both options have been updated/verified, you can proceed to the next step.

4. Under Digital IDs (Certificates), click **Publish to GAL…**



Encrypted e-mail

□ Encrypt contents and attachments for outgoing messages
□ Add digital signature to outgoing messages
☑ Send clear text signed message when sending signed messages
□ Request S/MIME receipt for all S/MIME signed messages

Default Setting: ActivClient Certificates

Digital IDs (Certificates)

Digital IDs or Certificates are documents that allow you to prove your identity in electronic transactions.

Read as Plain Text

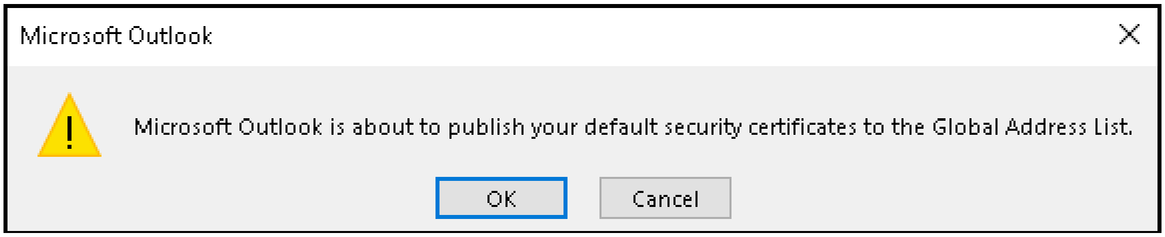
□ Read all standard mail in plain text
□ Read all digitally signed mail in plain text

Script in Folders

□ Allow script in shared folders
□ Allow script in Public Folders

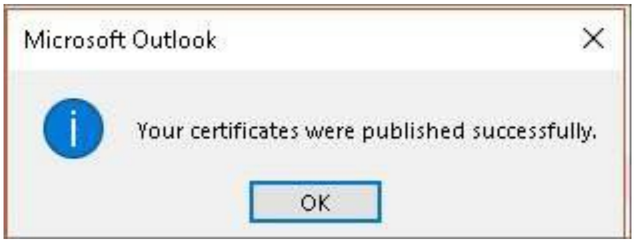
For subcontractors using a newly issued LinQuest laptop, you may need to click the **Import/Export** button and import your new certificate to Outlook before you can publish to GAL. For questions or concerns, contact IT Support for assistance in completing the task.

5. You will see a message that Microsoft Outlook is about to publish your default security certificates. Click **OK**. This process can take a few minutes to complete.



Microsoft Outlook is about to publish your default security certificates to the Global Address List.

6. Once the certificates are published, a success message appears.



Microsoft Outlook

Your certificates were published successfully.

7. Once done, you can then set your certificate to send your public key and “sign” (add digital signature to outgoing messages option) each email by default. Signing essentially sends the public portion of your ECA certificate so that users may send you an encrypted email.

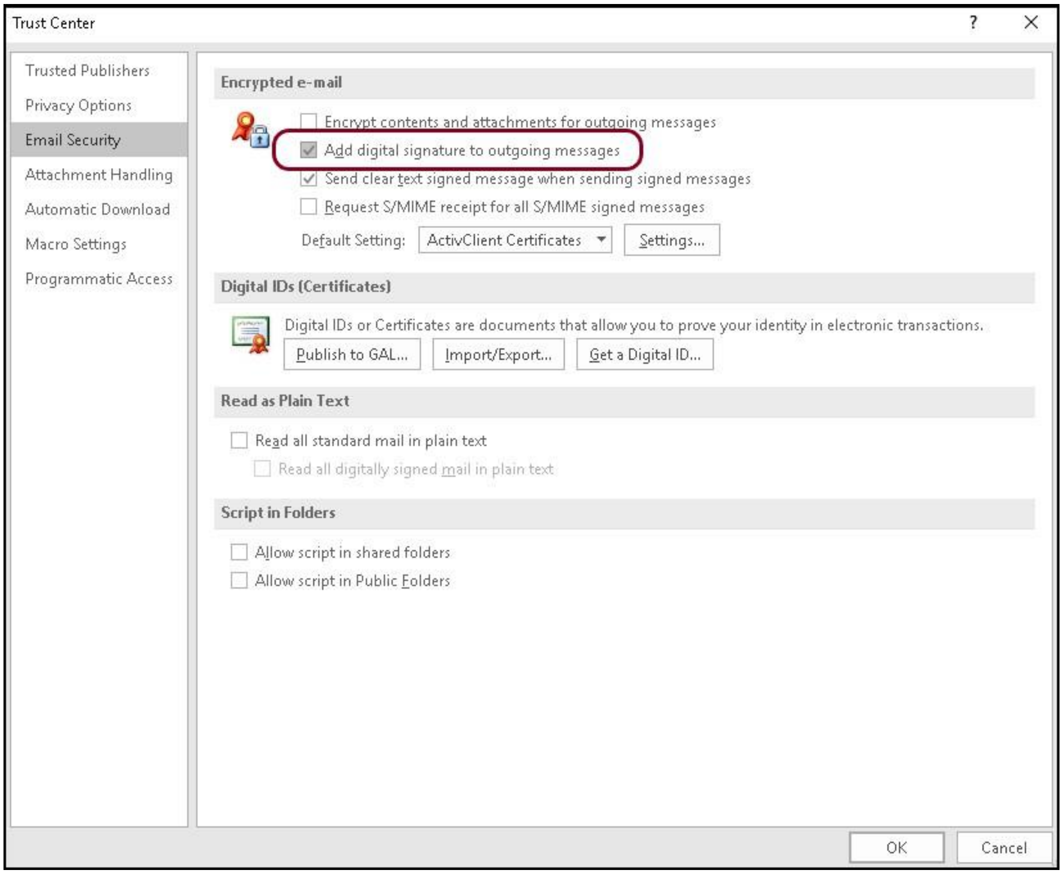
> **Note**
>
> If you have difficulty with this step, contact IT Support for assistance in completing the task.

8. You can choose to sign all emails by default, or select to sign each email individually. To set the email to sign by default, do the following:

    a. In Outlook, click **File > Options**.

    b. Click **Trust Center > Trust Center Settings.**

    c. Click **Email Security**. Under Encrypted e-mail, select the **Add digital signature to outgoing messages** checkbox.



Trust Center

Encrypted e-mail

☐ Encrypt contents and attachments for outgoing messages

☑ Add digital signature to outgoing messages

☑ Send clear text signed message when sending signed messages

☐ Request S/MIME receipt for all S/MIME signed messages

Default Setting: ActivClient Certificates

Digital IDs (Certificates)

Digital IDs or Certificates are documents that allow you to prove your identity in electronic transactions.

Read as Plain Text

☐ Read all standard mail in plain text

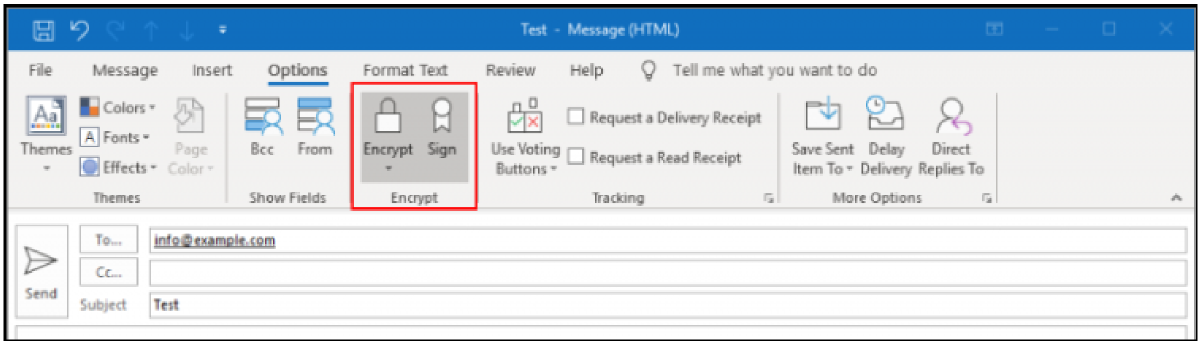
☐ Read all digitally signed mail in plain text

Script in Folders

☐ Allow script in shared folders

☐ Allow script in Public Folders

To individually sign emails, from the Outlook message, click **Options > Sign**.



☐ Request a Delivery Receipt

☐ Request a Read Receipt

To... info@example.com

Subject Test