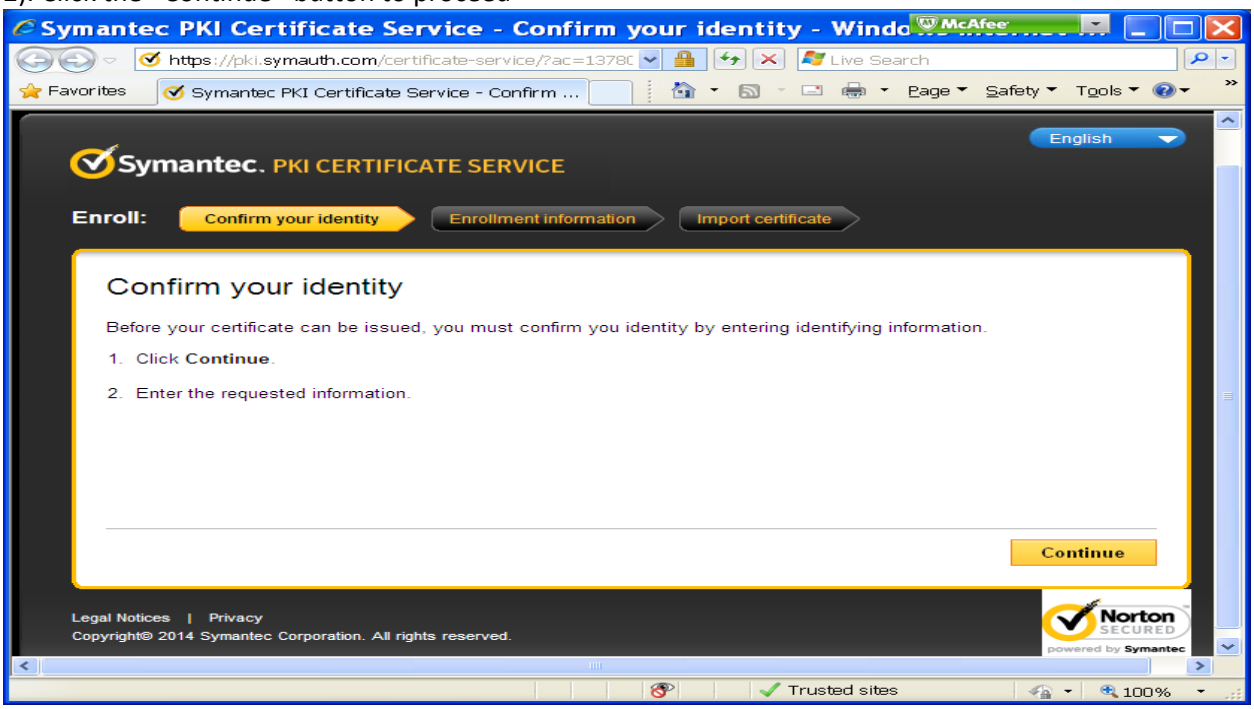
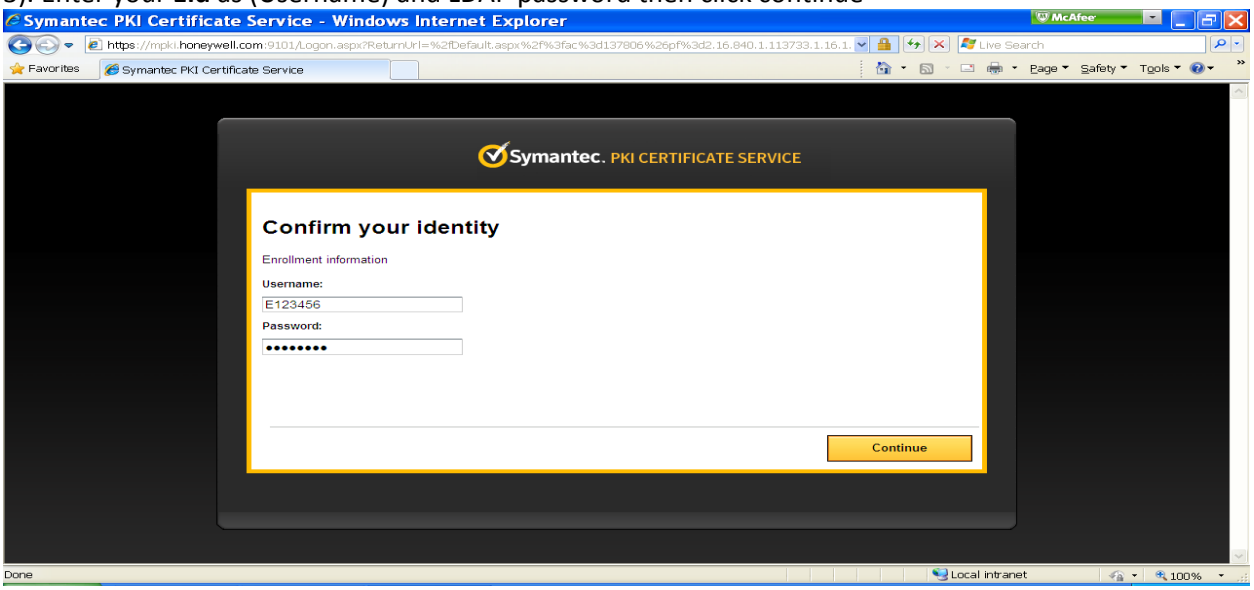
Please ensure you have completed all steps in this document including the Outlook Email configuration steps for successful email encryption and signing services to function properly.

To obtain your PKI 2 Hon Public Identity certificate for use with Secure Email / email encryption.
1). Click on the link below to begin:
Hon Public Identity

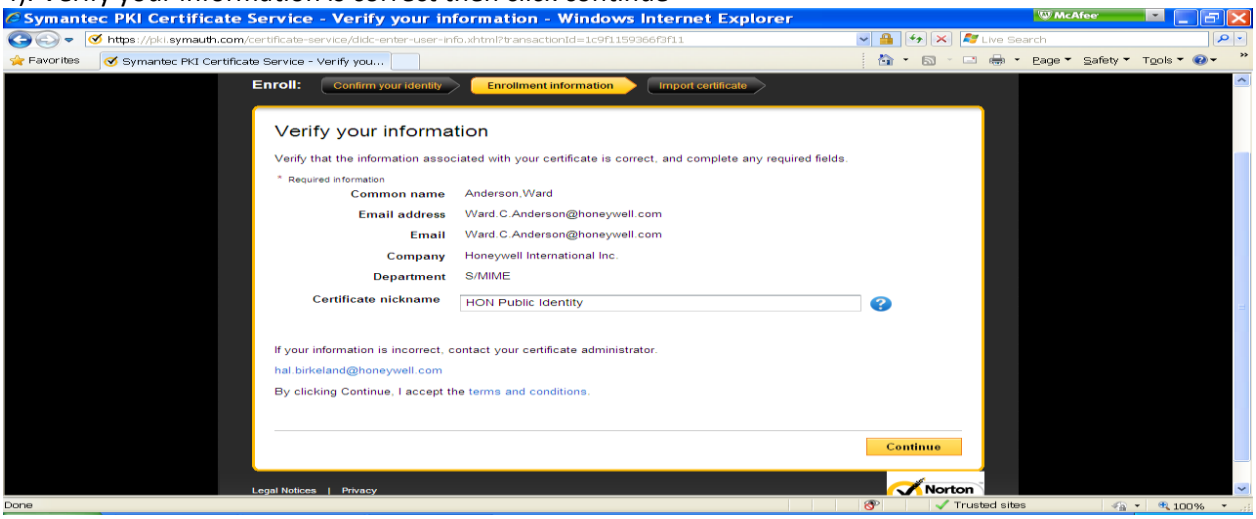
2). Click the <Continue> button to proceed



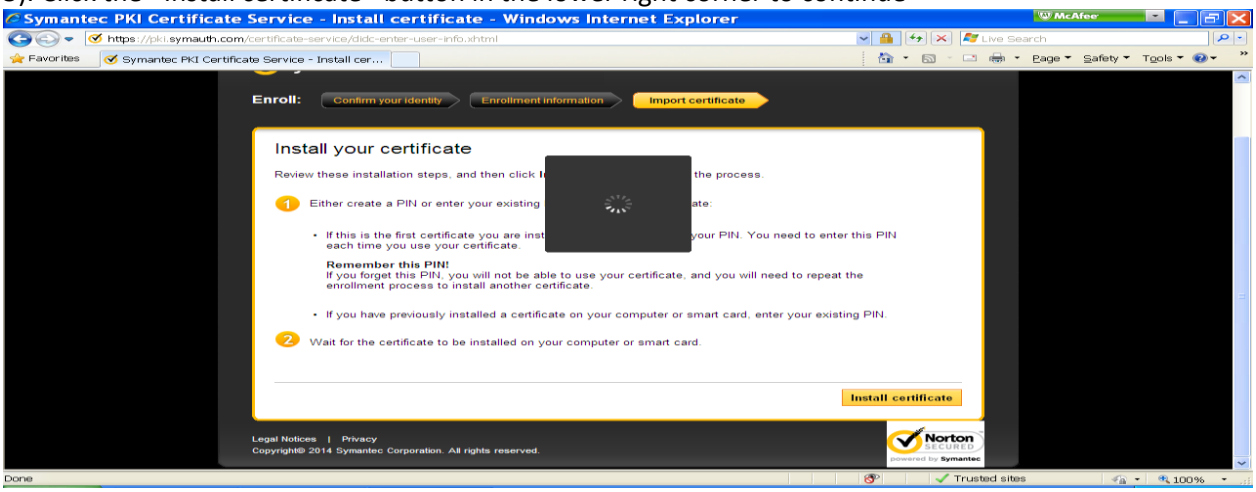
3). Enter your **Eid** as (Username) and LDAP password then click continue



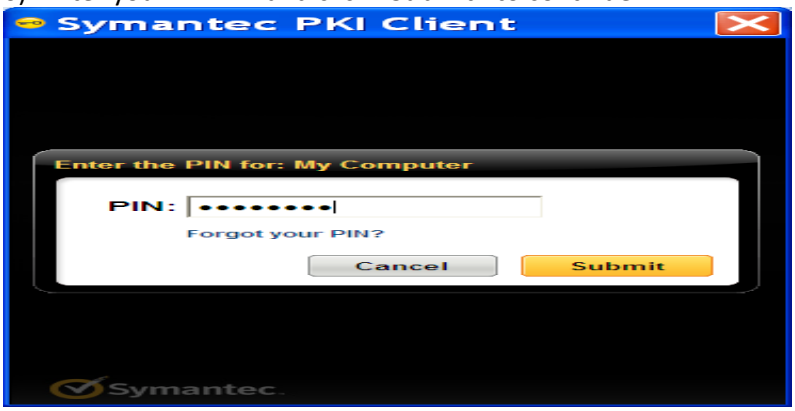
4). Verify your information is correct then click continue



5). Click the <Install certificate> button in the lower right corner to continue



6). Enter your PKI PIN and click <Submit> to continue

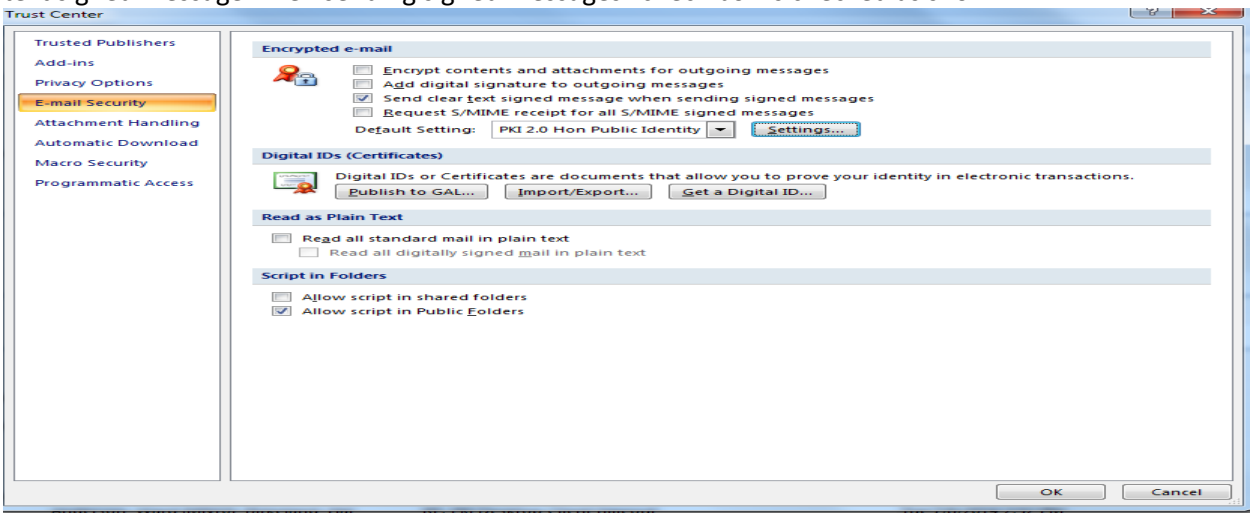


7). Once you receive the confirmation window that “Your certificate enrollment is now complete” Close your browser window and proceed to the Post enrollment instructions below to configure Microsoft Outlook in order to utilize your new certificate for email encryption and digital signing.

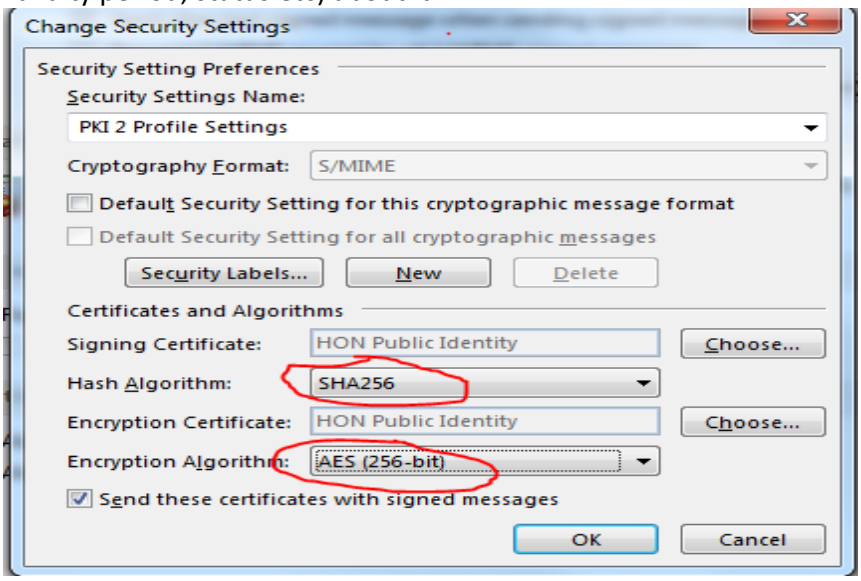
Post Certificate Enrollment steps to configure Microsoft Outlook 2010 & 2013 (O365) for email encryption and digital signing to utilize your new PKI certificate.

****Please skip to page 5 for Office 365 / Outlook 2013 instructions.**

1). Open MS Outlook
2). Click on **Tools** ->**Trust Center** ->Click on **E-mail Security** ->Click on **Settings** tab. Make sure "Send clear text signed message when sending signed messages" check box is checked as shown

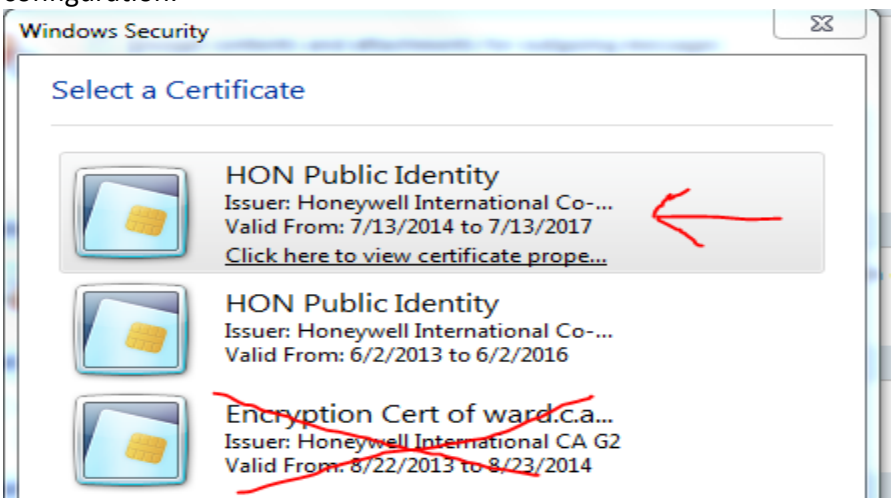


3). Ensure all the check-boxes are checked in the **Change Security Settings** pop-up.
4). Click on each **Choose** button individually & select your latest valid certificate in the **Select Certificate** pop-up and click on **OK**. You can click on the certificate to know more details (Issued to, validity period, status etc) about it.



5. Please ensure the Hash Algorithm is selected to SHA2 (SHA256) & Encryption Algorithm to AES (256-bit) for Security Settings. Click **OK** → **Apply** → **Ok** to complete.

Please see the example of pop-up window for certificate selection shown below.
6). Choose the **Hon Public Identity** certificate for your new encryption & signing certificate configuration.



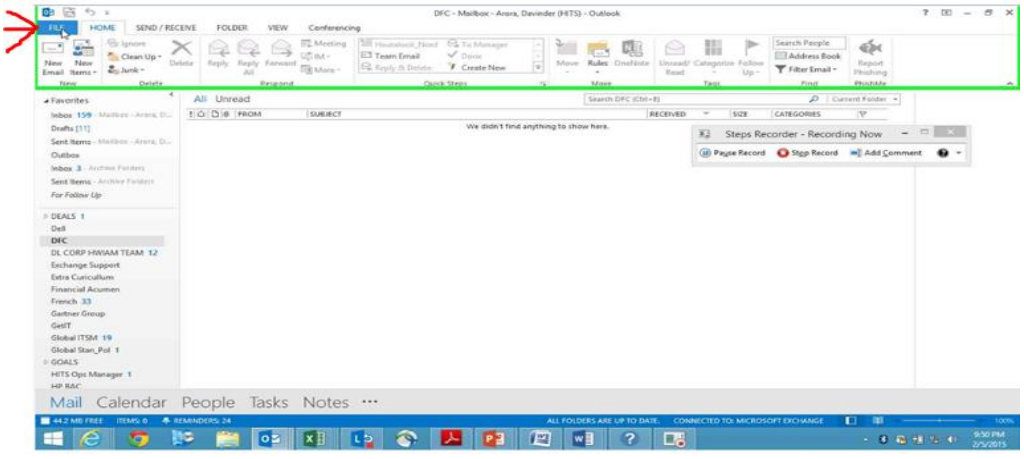
7). Restart your outlook to save the configuration changes.
Your outlook is now successfully configured for sending/reading encrypted emails.

Once you have completed all the above steps please revert to the PKI 2 website (click here PKI 2) and complete Step # 3. This is the revocation of your legacy PKI 1 certificate and will complete your request.

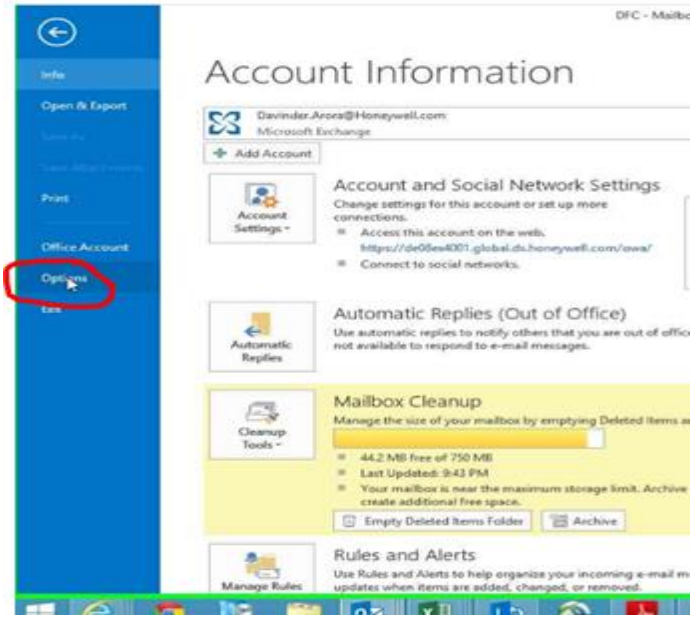
Post Certificate Enrollment steps to configure Microsoft Outlook 2013 for email encryption and digital signature utilizing your new PKI certificate.

1). Open Microsoft Outlook 365

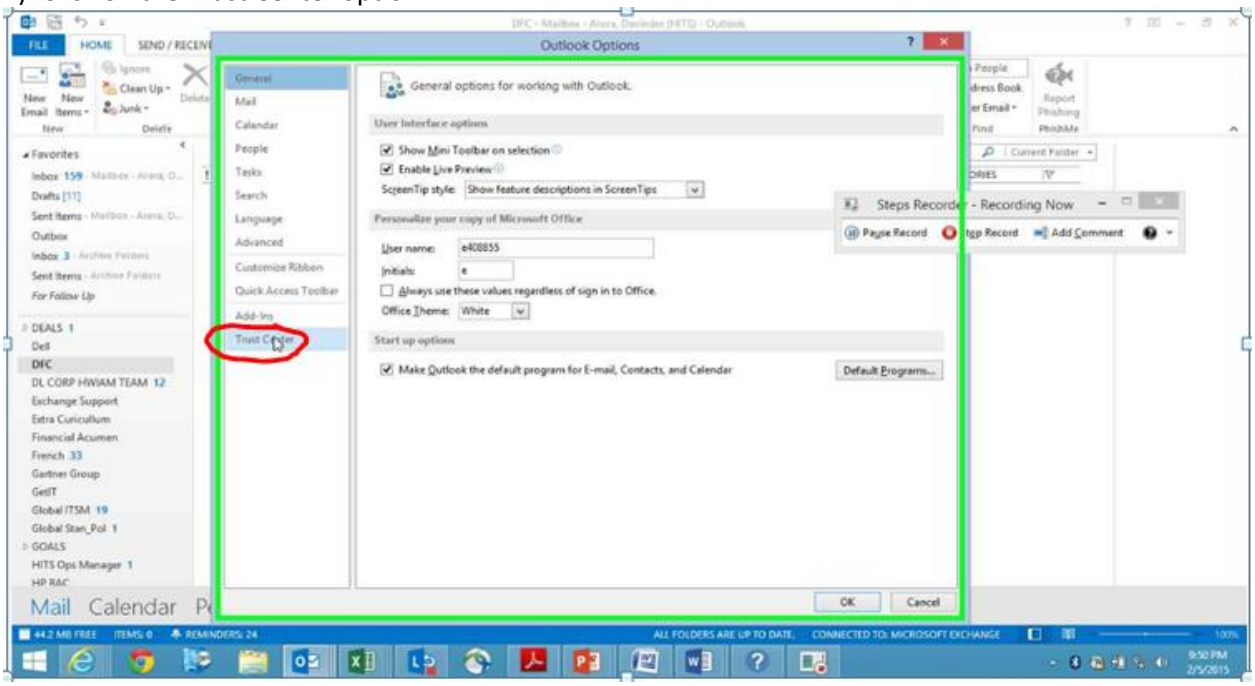
2). Click on the File pull down Menu



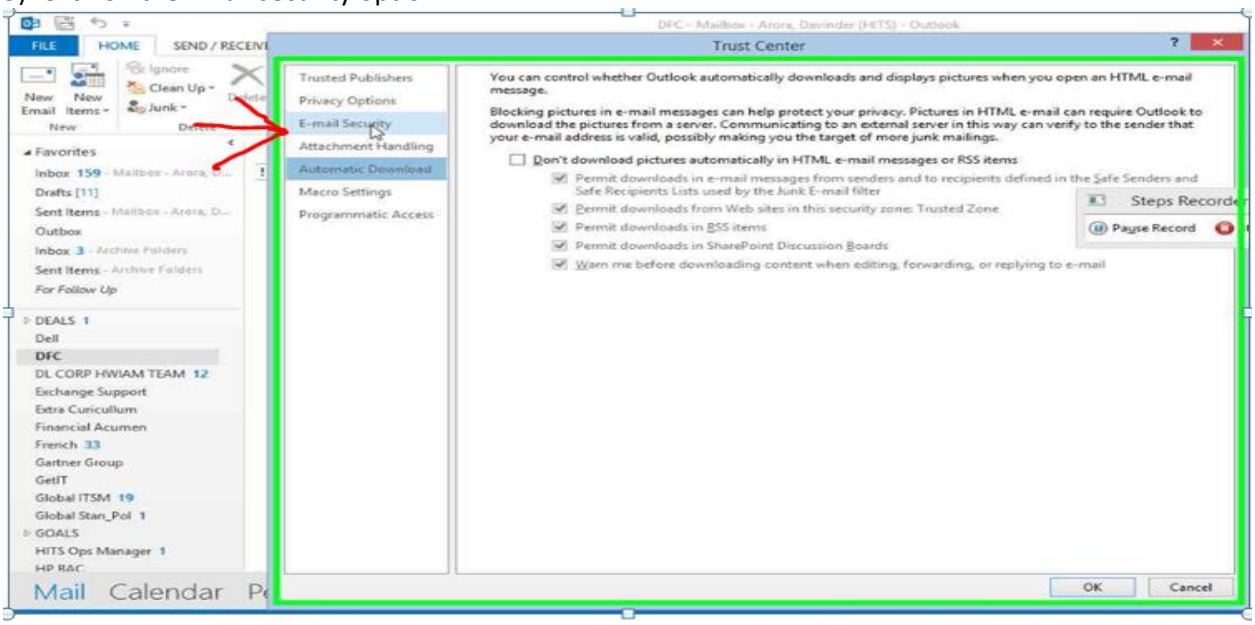
3). Click on the Options menu



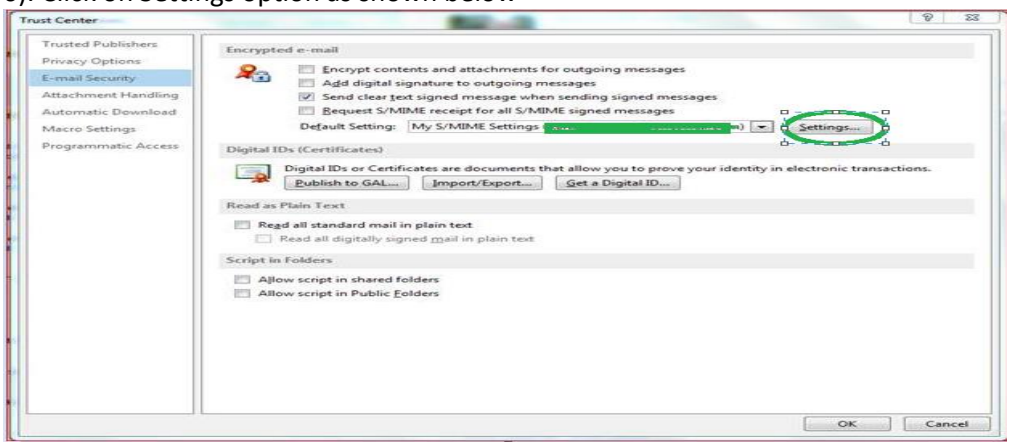
4). Click on the Trust Center option



5). Click on the Email security option

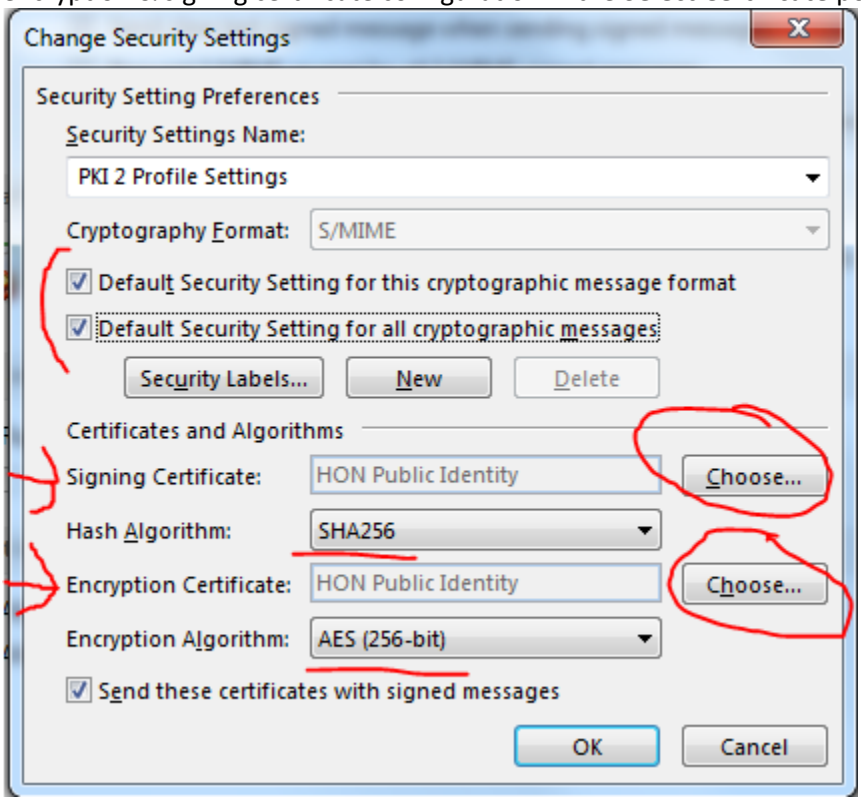


6). Click on Settings option as shown below

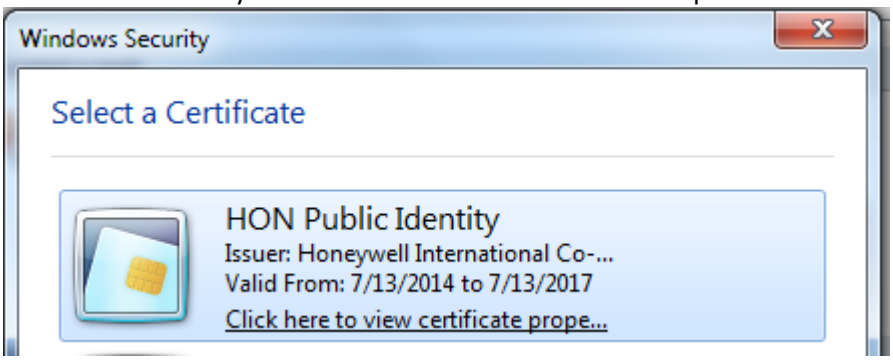


Ensure all the check-boxes are enabled in the **Change Security Settings** pop-up window and also ensure the Hash Algorithm is selected to SHA2 (SHA256) & Encryption Algorithm to AES (256-bit) respectively in the Change Security Settings window as seen below then continue.

7). Click on each **Choose** button individually & select the **Hon Public Identity** certificate for your new encryption & signing certificate configuration in the **Select Certificate** pop-up and click on **OK**



The Select Certificate window should appear and the correct PKI 2 HON Public Identity certificate sample is shown below for your review and awareness for the Step 7 'Choose' selections above.



8). Restart your outlook to save the configuration changes.
Your outlook is now successfully configured for sending/reading encrypted emails.

Once you have completed all the above steps please revert to the PKI 2 website (click here PKI 2) and complete Step # 3. This is the revocation of your legacy PKI 1 certificate and will complete your request.