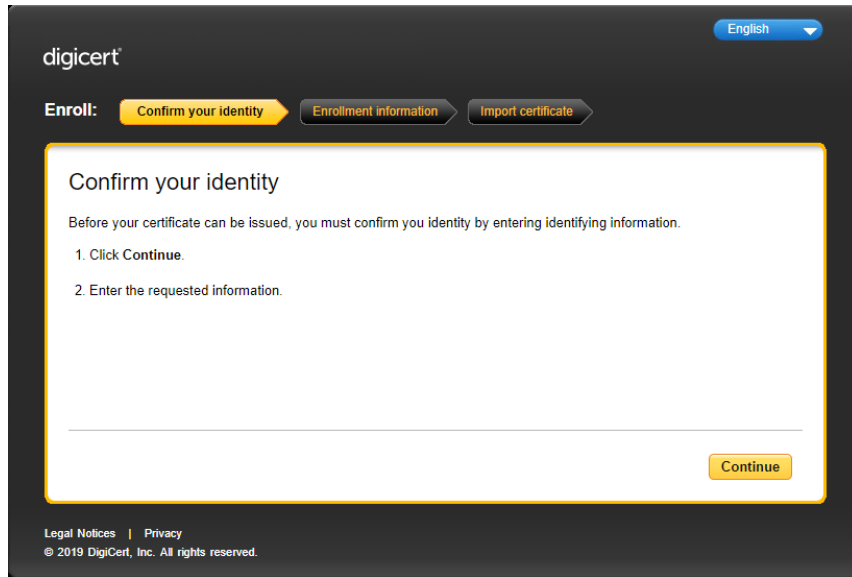


Please ensure you have completed all the steps in this document including the Outlook Email configuration steps for successful email encryption and signing services to function properly.

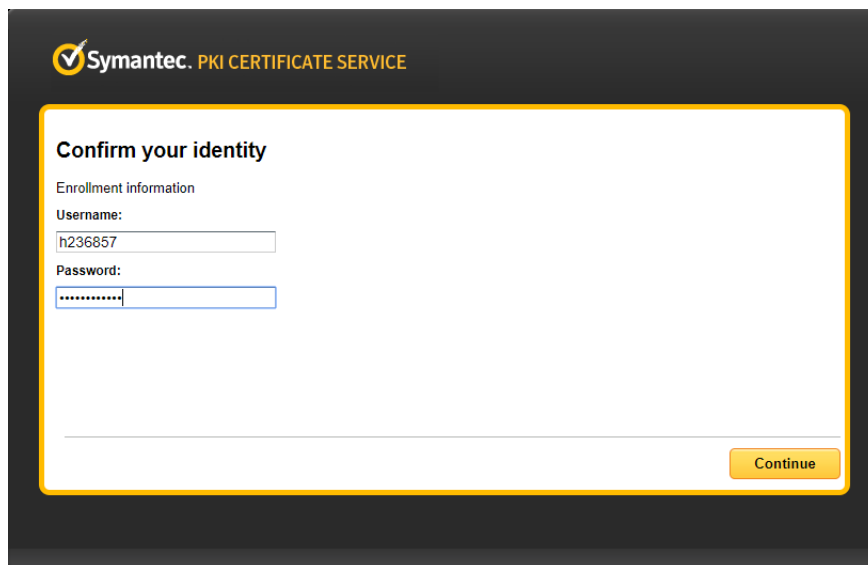
To obtain your PKI 2 Hon Public Identity certificate for use with Secure Email encryption:

1. Click on the link below to begin:  
[Hon Public Identity](#)
2. The **Symantec PKI Certificate Service** enrollment wizard starts. Click **Continue**.



The screenshot shows the DigiCert enrollment wizard interface. At the top left is the 'digicert' logo, and at the top right is a language dropdown menu set to 'English'. Below the logo is a progress bar with three steps: 'Confirm your identity' (highlighted in yellow), 'Enrollment information', and 'Import certificate'. The main content area is titled 'Confirm your identity' and contains the following text: 'Before your certificate can be issued, you must confirm your identity by entering identifying information.' Below this are two numbered instructions: '1. Click Continue.' and '2. Enter the requested information.' At the bottom right of the content area is a yellow 'Continue' button. At the bottom left, there are links for 'Legal Notices' and 'Privacy', and a copyright notice: '© 2019 DigiCert, Inc. All rights reserved.'

3. Input your EID (as **Username**) and LDAP **Password** and click on **Continue**.



The screenshot shows the Symantec PKI Certificate Service enrollment wizard interface. At the top left is the Symantec logo and the text 'Symantec. PKI CERTIFICATE SERVICE'. The main content area is titled 'Confirm your identity' and contains the following text: 'Enrollment information'. Below this are two input fields: 'Username:' with the value 'h236857' and 'Password:' with a masked password '\*\*\*\*\*'. At the bottom right of the content area is a yellow 'Continue' button.

4. Verify your information and that **HON Public Identity** is listed in the **Certificate nickname** field. If the information is valid then click on **Continue**. If it is not, discontinue this process and contact your certificate administrator

The screenshot shows the 'Verify your information' step in the digicert enrollment process. At the top, there are three navigation buttons: 'Confirm your identity', 'Enrollment information' (which is highlighted), and 'Import certificate'. Below the navigation, the title 'Verify your information' is displayed. A sub-header reads: 'Verify that the information associated with your certificate is correct, and complete any required fields.' The form contains the following fields:

- Common name: DE,Devdoot
- Email address: Devdoot.De@Honeywell.com
- Email: Devdoot.De@Honeywell.com
- Company: Honeywell International Inc.
- Department: S/MIME
- Certificate nickname: HON Public Identity (with a help icon)

Below the form, there is a note: 'If your information is incorrect, contact IT Service Desk. [ITServiceDesk@Honeywell.com](mailto:ITServiceDesk@Honeywell.com)' and a statement: 'By clicking Continue, I accept the [terms and conditions](#).' At the bottom left, there is a red asterisk and the text '\* Required information'. At the bottom right, there is a yellow 'Continue' button.

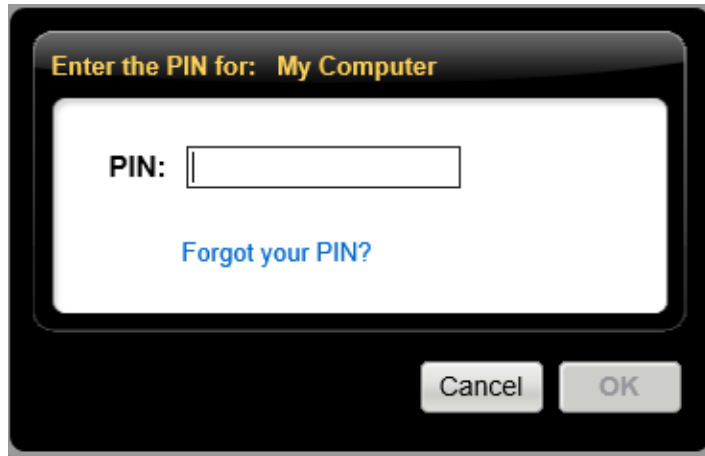
5. **Install your Certificate** screen displays. Review the installation steps and click **Install Certificate**.

The screenshot shows the 'Install your certificate' step in the digicert enrollment process. At the top, there are three navigation buttons: 'Confirm your identity', 'Enrollment information', and 'Import certificate' (which is highlighted). Below the navigation, the title 'Install your certificate' is displayed. A sub-header reads: 'Review these installation steps, and then click **Install Certificate** to complete the process.' The steps are:

1. Either create a PIN or enter your existing PIN. (A loading spinner is visible in the background of this step.)
  - If this is the first certificate you are installing, you must create a new PIN. You need to enter this PIN each time you use your certificate.
  - Remember this PIN!**  
If you forget this PIN, you will not be able to use your certificate, and you will need to repeat the enrollment process to install another certificate.
  - If you have previously installed a certificate on your computer or smart card, enter your existing PIN.
2. Wait for the certificate to be installed on your computer or smart card.

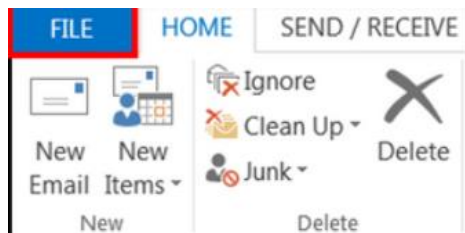
At the bottom right, there is a yellow 'Install certificate' button.

6. At **Enter the PIN** popup window, enter your **Symantec PKI PIN**. Click **Submit**.

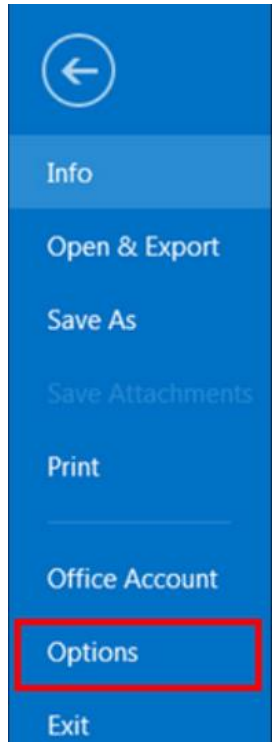


**Note:** If installing the first certificate on the laptop, you must create and confirm the PIN that will be used to access the PKI certificate

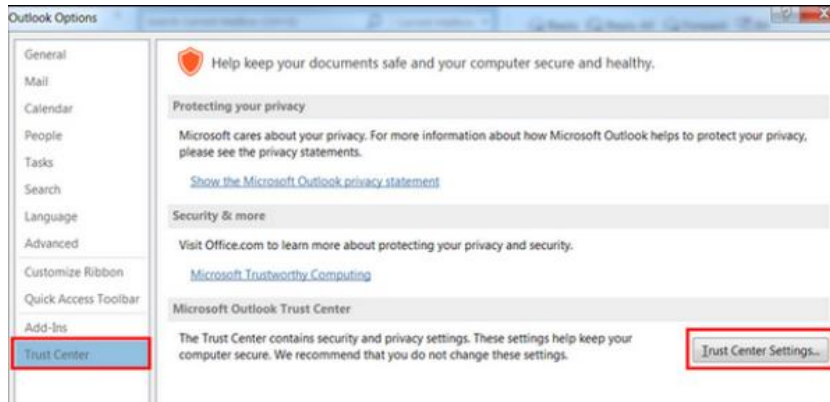
7. Click **OK**. The Installing your certificate window opens, displaying the progress of the certificate installation. The PKI certificate will take approximately 30 to 90 seconds to install
  8. When the installation is completed, a message displays indicating the certificate enrollment.
  9. Close the browser window.
- **To configure Microsoft Outlook 2013 and 2016 for email encryption and digital signature: -**
    1. Go to **File** in Outlook



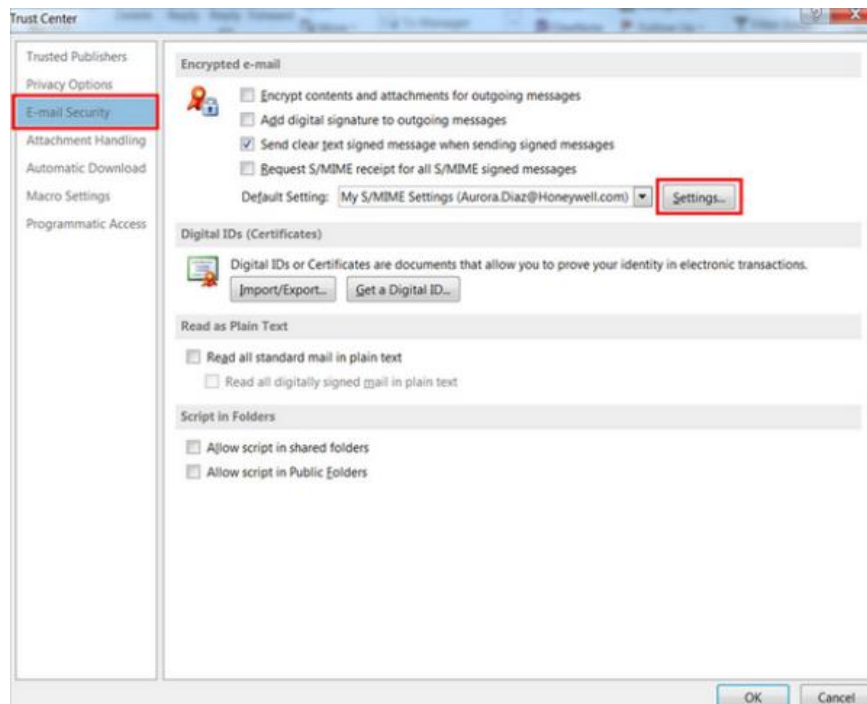
2. In the left panel go to **Options**.



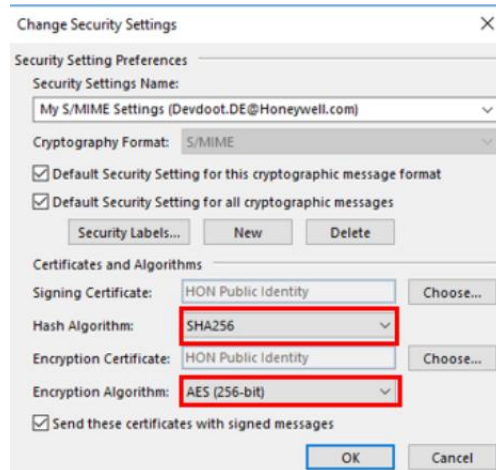
3. Select the **Trust Center** tab and click on **Trust Center Settings**.



4. Select the **Email Security** tab and click on the **Settings...** button.

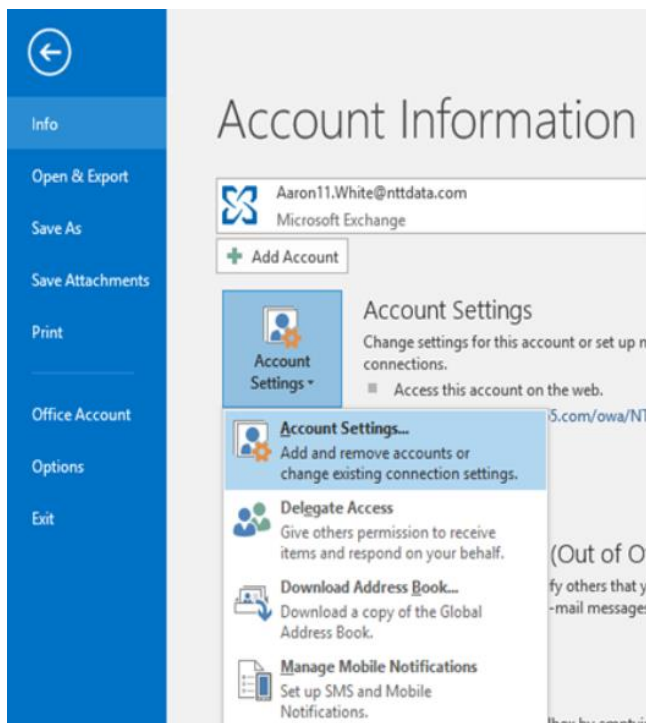


5. Click the drop-down in the Hash Algorithm and select SHA256 and Click the drop-down in Encryption Algorithm and select AES (256-bit). Click OK and Restart Outlook.

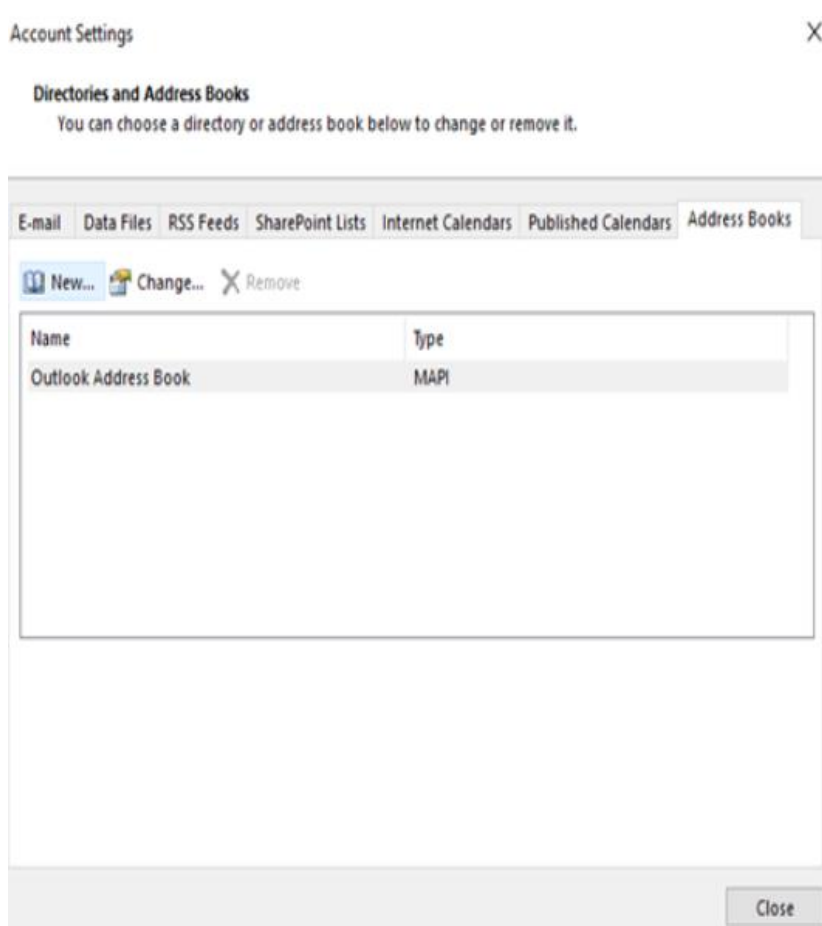


## To add the PKI Directory to Outlook

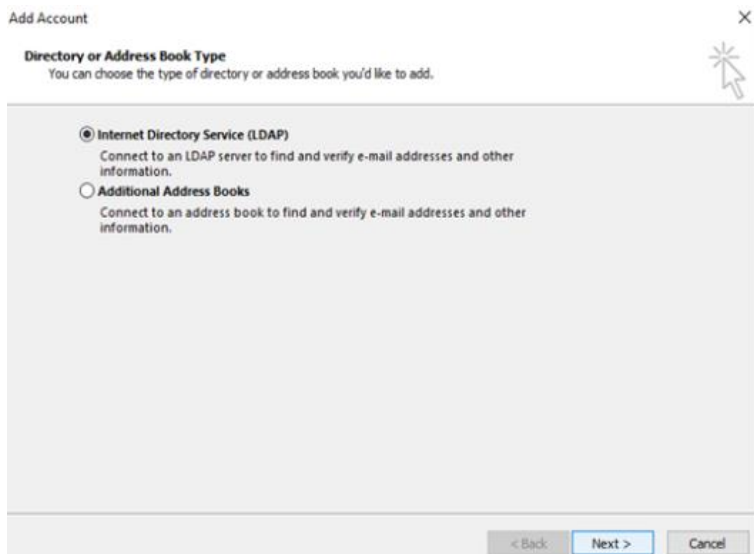
1. Go to **File** in Outlook, select the **Account Settings** drop down menu and open **Account Settings**.



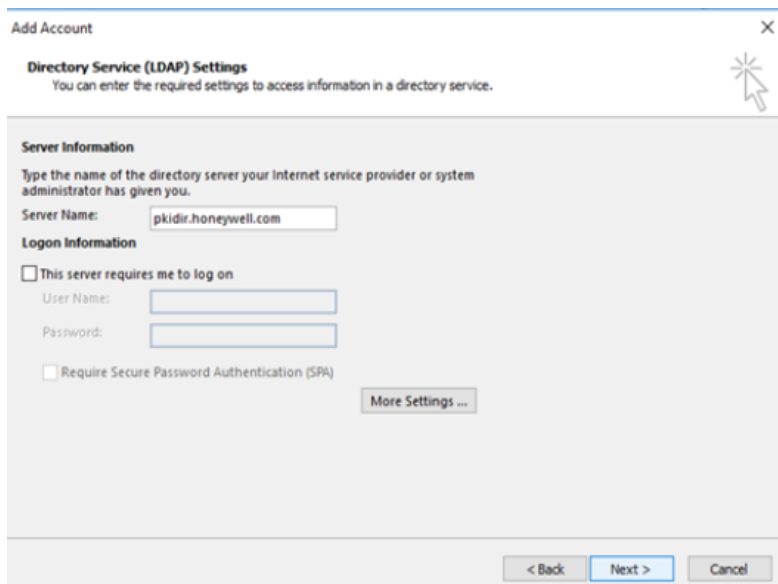
2. Go to the **Address Books** tab and select **New**.



3. Select **Internet Directory Service (LDAP)** and choose **Next**



4. Add **pkidir.honeywell.com** to the **Server Name** and choose **Next**



5. Click on **Finish**

Microsoft Outlook will need to be restarted for the changes to go into effect but is now configured to send and read encrypted emails.