1. **What are the prerequisites for obtaining a PKI digital certificate?**
   - Intranet / Internet access.
   - Business partners must allow network traffic over ports 9100, 9101, and 9102.
   - The Symantec PKI client must be installed on the PC (laptop / desktop).
   - If you do not have a Honeywell-managed device, you will need Admin privileges for that device for installing the PKI Client software from the Symantec website.

2. **What browsers can I use for enrolling for PKI certificates?**
   Most Honeywell standard browsers are supported. Please refer to the following list for specific details.
   - Google Chrome is qualified by Symantec for certificate enrollment.
   - Mozilla Firefox is qualified by Symantec for certificate enrollment.
   - Internet Explorer:
     - IE8: Not supported. Please use Chrome.
     - IE9: Supported.
     - IE10: Supported.
     - IE11: Supported (with Win 8.1 only).

3. **Why does Google Chrome show a prompt about manually installing a missing component?**
   Google Chrome is qualified by Symantec for certificate enrollment. However, Chrome requires an extension before you can enroll for a PKI certificate. If the PKI client is installed but the Chrome extension is missing when you enroll for a PKI certificate, Chrome will prompt you for the missing component. If you are prompted because the Chrome extension is missing, the steps below describe how to enable the missing extension:
   1. Open Chrome and navigate to the tools pull-down menu to open the settings option.
   2. Click Tools > Extensions.
   3. Ensure the Symantec PKI Client Plugin Extension option is enabled.
   4. Close and re-open Chrome, then proceed to the certificate enrollment link to continue.

4. **Why do I get a white panel when enrolling for a new certificate in Internet Explorer?**
   Please use the Google Chrome browser instead of Internet Explorer.
   If Chrome is not already installed on your machine, you can download and install it from the Software Center (Start > All Programs > Microsoft System Center 2012 R2 >
After launching Chrome, you may be prompted to enable the PKI Client extension. If so, please accept.

5. Why does the message “Smart card not detected” display when renewing my PKI certificate?
   Please use Google Chrome or Mozilla Firefox to enroll for PKI certificates. Both of these alternative standard browsers are available for download from the System Software Center store (Start > All Programs > Microsoft System Center 2012 R2 > Software Center).

6. How do I know which certificate to get for the different services offered?
   - For VPN (HRA AnyConnect remote) and Internal Honeywell Wi-Fi authentication certificates, enroll for the HON Private Identity certificate.
   - For Secure Email, enroll for the HON Public Identity certificate. This certificate is used for sending and receiving encrypted and or digitally-signed email messages between internal employees, as well as external or third parties with compatible encryption capabilities.
   - For electronic document signing (such as Adobe Acrobat files and others that are capable of allowing digital signing), enroll for the HON Adobe CDS Signing certificate. This certificate differs from the Email encryption certificate whereas it is provisioned to and stored on a smart card. You MUST have a FIPS 140-2 compatible card reader, smartcard token and compatible software to successfully enroll and use this type of certificate.

7. How often do I need to get a new certificate?
   All certificates are renewed every 3 years.

8. How do I renew my certificate prior to expiration and will I be notified in advance?
   Certificates are setup when the new computer is delivered. Certificates are configured to be active for 3 years. Because computers are typically replaced every 3 years, certificate renewal is generally not needed.

   However, in the case of some contractors, certificate renewal may be required. When that happens, a message will display on the computer, starting 30 days before the certificate expires. Click the link in the message to start the renewal. After completing the renewal, your certificate will automatically be issued to your PC and the renewal prompts will cease at that time.

9. Will I be required to use a password for my certificates?
   Yes. The Honeywell standards require password protection for both compliance and security guidance. The password is actually what Symantec calls a PIN or the Symantec PKI Client PIN. This PIN must be at least 8 alpha-numeric characters and may include non-ASCII characters.

   While each certificate is “unlocked” separately, the PKI PIN is generated upon your initial certificate enrollment and will be the same for all certificates that are issued on the same device.

10. Can I change my new PKI PIN (password)?
    You do not have to change your PKI PIN, but you can. Use the Symantec PKI client < Change Pin > option. This will change the pin for all PKI certificates on the device.

11. Do I have to change my PKI PIN (password)?
    No, you do not have to change your PKI PIN.

12. What happens if I use the PKI PIN reset option in the Symantec PKI client?
    The PKI PIN reset function is used if you have forgotten your PKI PIN. Only use this option if you cannot recall what your PKI PIN is as the reset function will actually remove your PKI certificate(s) from your PC and you will then browse to the PKI 2 website to re-enroll for all PKI 2 certificates and complete HRA or Outlook configuration steps.

13. Are there languages other than English available for use?
    Yes. While English is the standard global language at Honeywell, the Symantec PKI client offers limited language choices. The menu to change the language format to your choice is available in the initial certificate enrollment window of the PKI Certificate Service.
Click on the dropdown button in the upper right-hand corner to change the default to your choice.

14. **Are the PKI certificates exportable for use on multiple PC’s (devices) or for backup purposes?**
   1. No. Exporting the certificate is no longer an option in PKI service, for security and compliance purposes, as recommended by Honeywell Global Security and industry standards. Certificates are now effective for 36 months, rather than 12 months, making such exports largely unnecessary.

   2. While authentication certificates are not exportable, duplicate enrollment is allowed. Individuals whose role requires multiple devices can enroll for PKI certificates on each device.

   3. The Secure Email (encryption) certificates are NOT exportable, but duplicate enrollment is allowed by using the certificate enrollment process for use on multiple PC’s if needed. This option allows for one certificate managing all sent and received encrypted / signed messages from multiple devices using the same certificate.

   4. The Mobile Device Management team provisions certificates and profiles to your mobile device for you, eliminating the need for you to export certificates.

15. **Is there information regarding Mobile Device Management related to PKI certificates?**
   Yes, please visit the links below for the specific device listed and the individual FAQs for each.

   - For all iOS device browse to http://go.honeywell.com/Apple.
   - For Samsung Android device browse to http://go.honeywell.com/Samsung.
   - For Windows Phone 8 device browse to http://go.honeywell.com/WP8.

16. **Why does the message “Unable to locate your certificate” appear?**
   This error message can occur while attempting to send or receive an encrypted email message. The message occurs because the PKI 2 HON Public Identity certificate on the device has not been provisioned and configured to your Microsoft Outlook email client on the device that received the error message.

   To resolve this issue:

   1. Navigate to the [PKI 2 website](http://honeywell.com/sites/ipc/Pages/mpki.aspx) using the device where the error occurred.
   2. Click Step 2 to open the PKI 2 Secure Email (encryption) Standard End-User Guide.
   3. Follow all the steps in that document to provision the HON Public Identity certificate to your device and guide you through the Outlook Configuration steps.

   The steps above will enable your new certificate for use with encryption. If you have previously enrolled for the certificate from a different device, this process will simply download a copy of the current valid certificate, not provision a new certificate.

   If problems do continue, please contact the Honeywell Service Desk