Entrust Datacard™

PURCHASING AND USING A PERSONAL SECURE EMAIL CERTIFICATE

Document issue: 12.1

Date of issue: March 2017

Entrust is a registered trademark of Entrust, Inc. in the United States and certain other countries. Entrust is a registered trademark of Entrust Limited in Canada. All other company and product names are trademarks or registered trademarks of their respective owners. The material provided in this document is for information purposes only. It is not intended to be advice. You should not act or abstain from acting based upon such information without first consulting a professional. ENTRUST DOES NOT WARRANT THE QUALITY, ACCURACY OR COMPLETENESS O F THE INFORMATION CONTAINED IN THIS ARTICLE. SUCH INFORMATION IS PROVIDED "AS IS" WITHOUT ANY REPRESENTATIONS AND/OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, BY USAGE OF TRADE, OR OTHERWISE, AND ENTRUST SPECIFICALLY DISCLAIMS ANY AND ALL REPRESENTATIONS, AND/OR WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT, OR FITNESS FOR A SPECIFIC PURPOSE.

© 2017 Entrust Inc. All rights reserved.

Table of contents

Revision and guide information

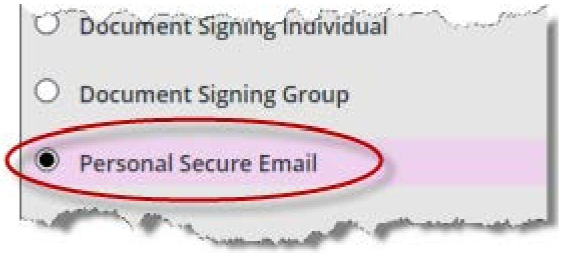
Revision	Section	Description
12.1	All	New guide

Although this guide can be printed out, it relies heavily on hyperlinks to other sections, so it is best viewed and used electronically.

Start your order

Purchasing and using an Entrust Datacard™ ***Personal Secure Email Certificate*** is easy; read on to find out how. (Terms in ***italics*** are in the glossary.)

1. Go to https://buy.entrust.net/index.html#/quoteOrder .

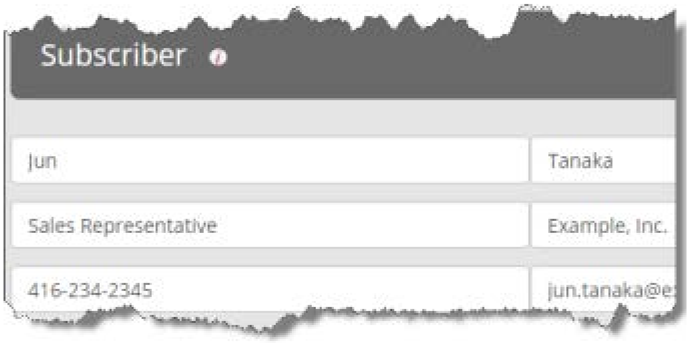


○ Document Signing Individual

○ Document Signing Group

● Personal Secure Email

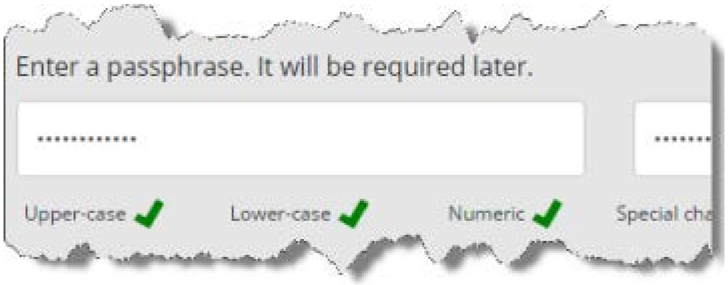
2. Select **Personal Secure Email**. Go here to learn more.
3. Click **Next**.



Subscriber

Jun	Tanaka
Sales Representative	Example, Inc.
416-234-2345	jun.tanaka@e

4. Enter the ***subscriber*** information. The information you provide will be written into the certificate.
5. Click **Next**. If the **Next** button is not available, it is because a field is still empty.

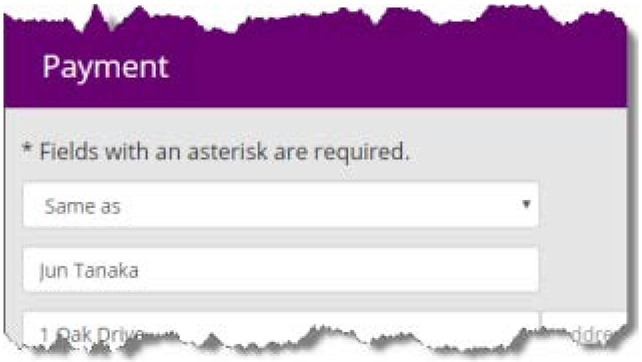


Enter a passphrase. It will be required later.

•••••••••••• •••••••

Upper-case ✓ Lower-case ✓ Numeric ✓ Special cha

6. Enter a passphrase that conforms to the rules. You will use the passphrase when you pick up the certificate.
7. Click **Next**.



Payment

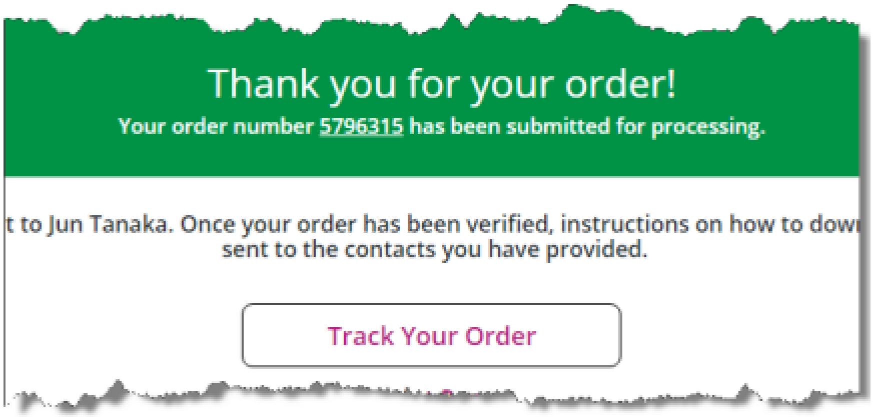
* Fields with an asterisk are required.

Same as

Jun Tanaka

1 Oak Drive

8. Enter billing information and accept the subscription agreement.
9. Click **Buy Now**. If the button is unavailable, it's because there is invalid or missing information.



Thank you for your order!

Your order number 5796315 has been submitted for processing.

t to Jun Tanaka. Once your order has been verified, instructions on how to dow
sent to the contacts you have provided.

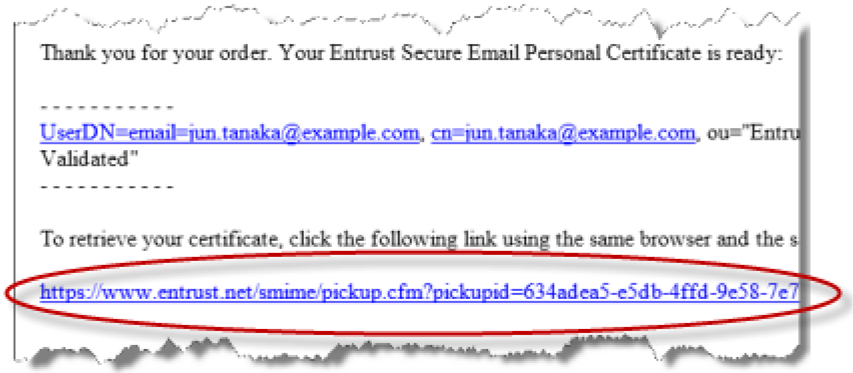
10. Review the **Thank you** message which contains your order number.

You are now ready to pick up and install your certificate.

Pick up and install your certificate

1. Go to the computer where the certificate will be used.
2. On this computer, check your email for this message:

```
Entrust Certificate Ready: Order <your_order_number>
```



Thank you for your order. Your Entrust Secure Email Personal Certificate is ready:

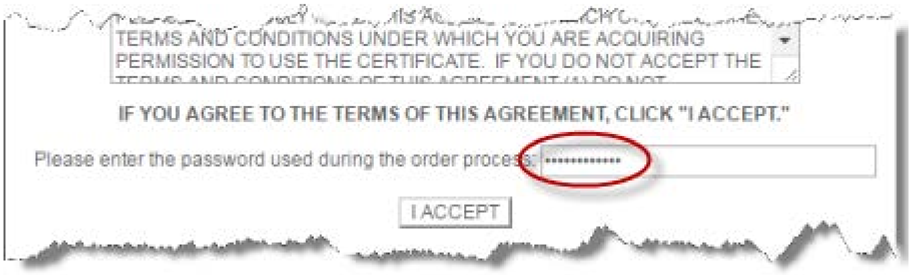
UserDN=email=jun.tanaka@example.com, cn=jun.tanaka@example.com, ou="Entru
Validated"

To retrieve your certificate, click the following link using the same browser and the s

https://www.entrust.net/smime/pickup.cfm?pickupid=634adea5-e5db-4ffd-9e58-7e7

3. Click the second link in the email.

   An agreement page opens.
4. Read the agreement.



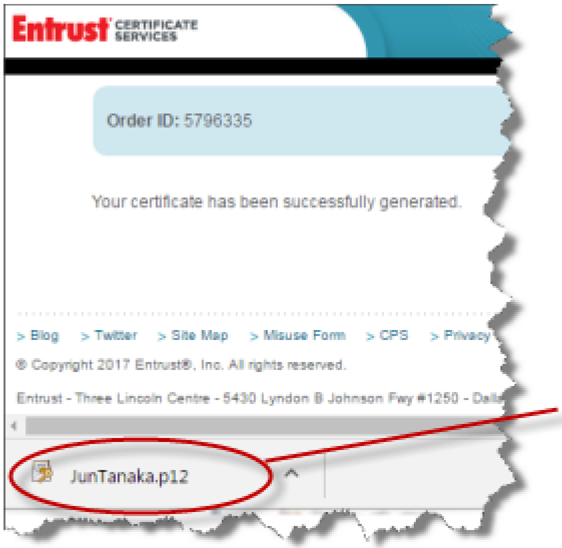
TERMS AND CONDITIONS UNDER WHICH YOU ARE ACQUIRING
PERMISSION TO USE THE CERTIFICATE. IF YOU DO NOT ACCEPT THE

IF YOU AGREE TO THE TERMS OF THIS AGREEMENT, CLICK "I ACCEPT."

Please enter the password used during the order process: •••••••••••••

5. Enter the passphrase you created when you ordered the certificate.
6. Click **I ACCEPT**.

   The certificate downloads.



Order ID: 5796335

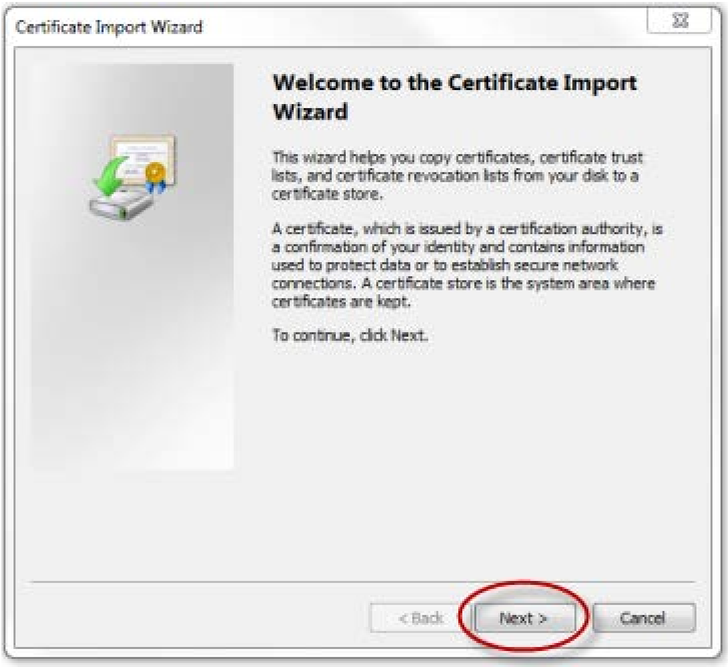
Your certificate has been successfully generated.

> Blog > Twitter > Site Map > Misuse Form > CPS > Privacy
© Copyright 2017 Entrust®, Inc. All rights reserved.
Entrust - Three Lincoln Centre - 5430 Lyndon B Johnson Fwy #1250 - Dall
JunTanaka.p12

The downloaded certificate, as it appears in Chrome. Other browsers display the certificate differently.

7. Open the P12 file.

   A wizard appears.



Certificate Import Wizard

Welcome to the Certificate Import Wizard

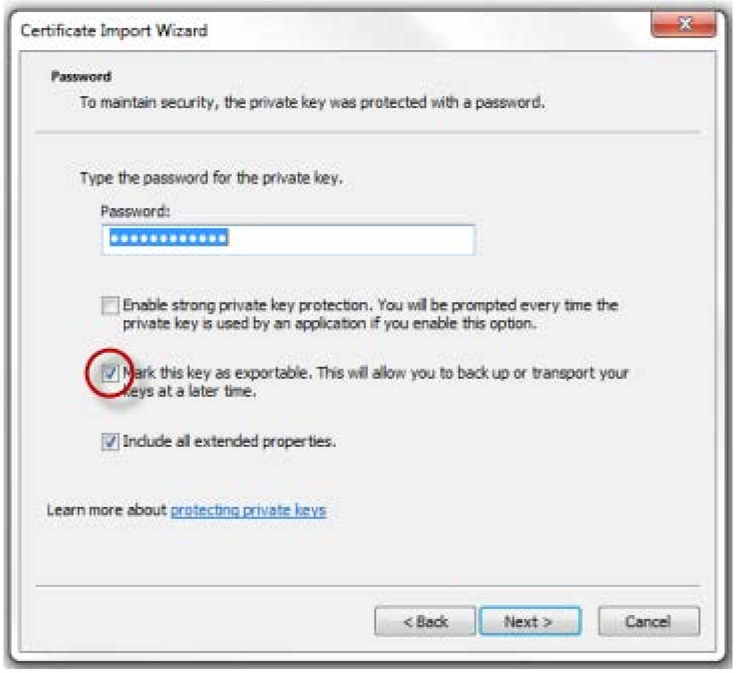
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

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.

8. Click **Next**.
9. On the **File to Import** page, leave the defaults and click **Next**.

   The **Password** dialog box appears.



Certificate Import Wizard

Password

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password: •••••••••••••

□ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

☑ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

☑ Include all extended properties.

Learn more about protecting private keys

10. On the **Password** page:

    a. Specify a password. It can be different from the passphrase you specified earlier.

    b. Select or deselect **Enable strong private key protection**, as desired.

    c. (Highly recommended.) Select **Mark this key as exportable** if you might use your certificate (and corresponding private key) on another computer or mobile device in the future. If you don't make the key exportable, then the certificate can only be used on the current computer.

    d. Leave **Include all extended properties** selected.

    e. Click **Next**.

11. On the **Certificate Store** page, leave the default and click **Next**.

12. Click **Finish**.

13. On the success message, click **OK**.

    You have now picked up and installed your certificate to your computer. You can now begin using it to secure email.

Supported email applications

To use your Personal Secure Email Certificate, you'll need an email application that complies with the Secure/Multipurpose Internet Mail Extensions (S/MIME) standard. Examples:

- Microsoft® Outlook® 2007 and later*
- Mozilla® Thunderbird®
- Mobile device email applications. See this topic for all information related to mobile.

* Outlook 2003 also works but is no longer supported by Microsoft and is therefore not included in this guide.

Configure Outlook or Thunderbird

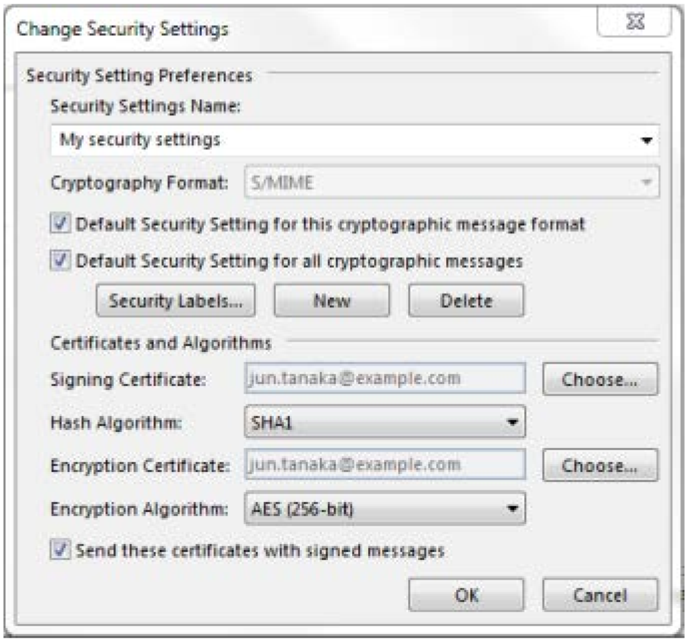
You'll need to configure your mail application to 'see' your Personal Secure Email Certificate.

Configure Outlook 2016, 2013, 2010, 2007

1. In Outlook, click **File**.
2. From the list on the left, click **Options**.
3. From the list on the left, click **Trust Center**, and in the main pane click **Trust Center Settings**.
4. From the list on the left, click **E-mail Security**, and in the main pane, click **Settings**.

   The **Change Security Settings** dialog box appears.
5. Next to **Signing Certificate**, click **Choose** and select the certificate you just imported.
6. Next to **Encryption Certificate**, click **Choose** and select the certificate you just imported.
7. Ensure **Send these certificates with signed messages** is selected.

   The dialog box should look like this:



Change Security Settings

Security Setting Preferences

Security Settings Name: My security settings

Cryptography Format: S/MIME

☑ Default Security Setting for this cryptographic message format

☑ Default Security Setting for all cryptographic messages

Certificates and Algorithms

Signing Certificate: jun.tanaka@example.com

Hash Algorithm: SHA1

Encryption Certificate: jun.tanaka@example.com

Encryption Algorithm: AES (256-bit)

☑ Send these certificates with signed messages

8. Click **OK** on all open dialog boxes.

   You're now ready to sign and encrypt email.

Configure Thunderbird

- See this webpage for instructions. You're now ready to sign and encrypt email.

Digitally sign email

To learn how to ***digitally sign*** email, click one of the links below.

- Digitally sign email in Outlook 2016, 2013, 2010, and 2007
- Digitally sign email in Thunderbird

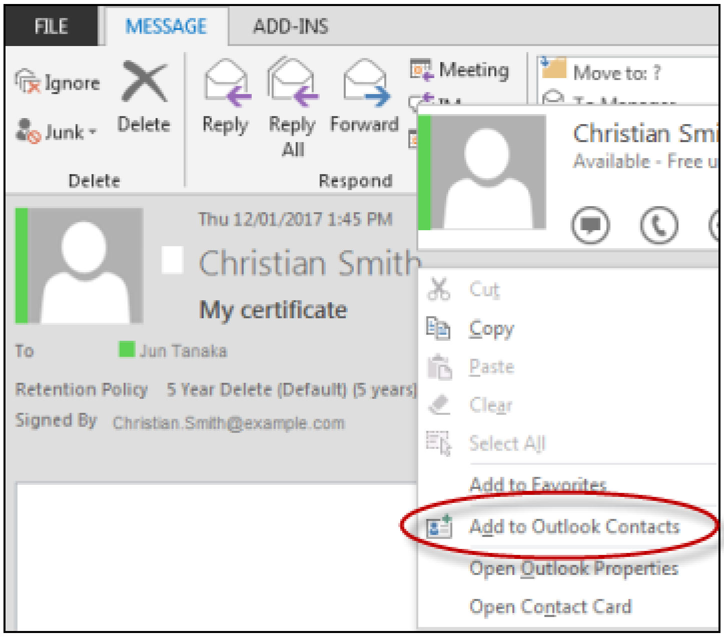
Encrypt email

To ***encrypt*** email for someone, you'll need *their certificate*. (You can't use your own certificate.) Conversely, if other people want to encrypt email *for you*, they'll need *your* certificate.

Use the instructions that follow to exchange certificates and encrypt for each other.

Exchange certificates

1. Each of you must send a digitally signed email to one another. Your respective certificates will be included in your email messages.
2. Each of you must add the other's certificate to your computer or device. Follow these instructions.
   - In Outlook:
     i. Double-click the signed message that you received from the other person.
     ii. Right-click the sender's name.



     iii. Click **Add to Outlook Contacts**, or **Update new information from this contact to the existing one**, whichever is available. The effect is that the certificate gets added to the sender's contact entry, and you can now use it to encrypt for them.
   - In Thunderbird:
     i. Take no action.

     Thunderbird automatically adds valid certificates to the **Other People's** tab of your **Certificate Manager** when you receive signed messages from them.

Encrypt email

After exchanging certificates, you can encrypt messages for each other.

- Encrypt email in Outlook 2016, 2013, 2010, and 2007
- Encrypt email in Thunderbird

Can I use my certificate with Gmail or other free webmail applications?

No, but you can map your Gmail, Hotmail, Yahoo! and other webmail accounts to Outlook or another email application that supports your certificate.

Go to one of these links for instructions on mapping your webmail to Outlook or Thunderbird:

- Instructions for mapping mail from Gmail to Outlook
- Instructions for mapping mail from Hotmail or Outlook.com to Outlook
- Instructions for mapping mail from Hotmail or Outlook.com to Thunderbird
- Instructions for mapping mail from Yahoo! to Outlook or Thunderbird

Can I use my certificate on my mobile device?

Yes, if you're using a supported device.

Supported devices:

- Apple® iOS 5 device and later
- BlackBerry® 10.3.1 and later
- Windows Mobile™ 10 device and later

Note: At the time of writing, Android does not provide native support for ***S/MIME*** and Personal Secure Email Certificates.

If your device is supported, follow the instructions below to set it up with your certificate.

Set up your certificate on your mobile device

1. Export the certificate, following these instructions:
    a. Open Internet Explorer®. (Do not use Chrome or another browser.)

b. Click ⚙ > **Internet Options** > **Content** tab > **Certificates**.

c. From the **Personal** tab, find your Personal Secure Email Certificate and double-click it.

d. Click the **Details** tab and then click **Copy to File**.

e. In the wizard, click **Next**.

f. Click **Yes**, **export the private key** and click **Next**. If this option is not available, it might be because you didn't make the key exportable when you initially imported the certificate to the computer.

g. Select **Personal Information Exchange – PKCS #12 (.PFX)** and leave everything else deselected. Click **Next**.

h. Type and confirm a password. You'll need to use it when you import the certificate to your mobile device. Click **Next**.

i. In the **File name** field, enter `C:\<yourname>.pfx`, and click **Next**.

Example: `C:\AliceSmith.pfx`

j. Click **Finish**.

k. Click **OK** on all open dialog boxes.

You have now exported your Personal Secure Email Certificate to a file on your `C:\` drive.

2. Email yourself the PFX file. Make sure it's available on your mobile device.
3. Open the email and tap the certificate to install it. When prompted, enter the same password you entered when you exported the certificate.
4. Enable S/MIME and start encrypting and signing. Follow the instructions for your device type.
   - Apple iOS 5 or higher instructions
   - BlackBerry Q10 instructions (these instructions work for any 10.3.1 or 10.3.2 device)
   - Windows 10 Mobile instructions

Glossary

Term	Definition
Digitally sign	When you digitally sign an email message, you are telling the recipient that it was you, and not an imposter, who sent the email. A valid digital signature also proves to that the email has not been tampered with.
Encrypt	When you encrypt an email message, you are scrambling it to prevent eavesdroppers from being able to read the contents while in transit or storage. Only the intended recipients are able to decrypt the message.
Entrust Certificate Services	A web-based platform that simplifies certificate management with 24x7 access to detailed technical insights for end-to-end lifecycle management of all of your digital certificates. Your technical contact is given access to this application when you order.
Personal Secure Email Certificate	An S/MIME certificate that you can use to encrypt and digitally sign email.
S/MIME	Secure/Multipurpose Internet Mail Extensions. S/MIME is a standard for digitally encrypting and signing email.
Subscriber	The person to whom the Personal Secure Email Certificate belongs. The subscriber is notified when the certificate requires a renewal or update.