Symantec Managed PKI Use-case Demo

Enabling OWA S/MIME

Confidence in a connected world. Symantec.

Use-case Overview

Enable an end-user to use Microsoft Outlook Web Access (OWA) to send and receive signed and encrypted emails (S/MIME). The user already has a certificate that is configured in Outlook for S/MIME. Additionally they now want to use their web browser with OWA and S/MIME support.

See the "MPKI WindowsPC SMIME PKIClient ManualApprove OutlookAutoConfig use-case demo.pdf" use-case document; which shows how to issue the certificate to the user with Outlook and is pre-requisite to this use-case.

Configuration Overview

In order to support OWA with S/MIME, the user must use Internet Explorer (IE) browser. Their S/MIME certificate(s) must be accessible to IE (in CAPI) and the *Microsoft Outlook Web Access S/MIME* control must be installed.

In this example the user has already enrolled for their secure email certificate. Their certificate and private key is stored in PKI Client which registers the certificate with CAPI, therefore making it accessible to Internet Explorer browser.

If the user wishes to use OWA from another machine where the certificate does not exist, they can export it from PKI Client (password protected .glck format) on the original machine where the certificate was issued, install PKI Client on the desired target machine and then import the .glck file. The .glck file not only securely stores their certificate and private key, but it also enforces the original policy settings at import such as requiring PIN protection.

(Note: If the certificate policy does not allow for export from PKI Client, another option would be to have the PKI Administrator perform a key recovery from PKI Manager. This of course assumes that key escrow was enabled on the original certificate profile when it was created, which is the default setting for a Secure Email certificate profile.)

Confidence in a connected world. Symantec.

End-user sending and receiving signed and encrypted emails using Outlook mail client and Outlook Web App.

End-user Video (04:25 mm:ss)
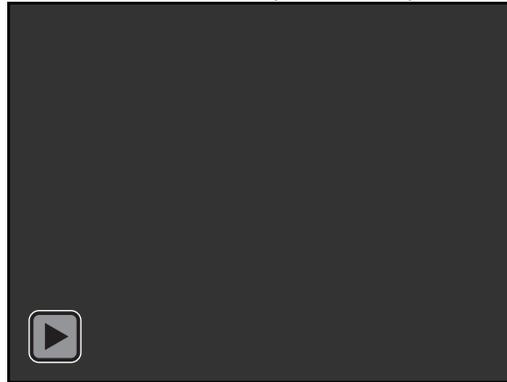
Watch a video of this procedure.
Click to start.
Right-click, choose "Full Screen Multimedia".
Press keyboard ESC to return.

S/MIME is working with Microsoft Outlook.
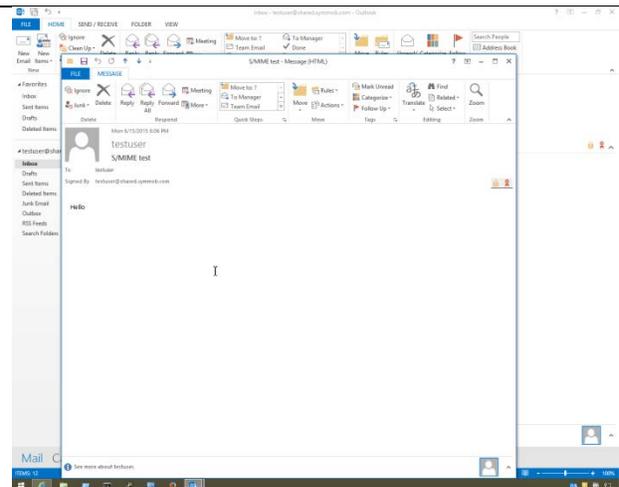
Using **Microsoft Internet Explorer**, sign in to **Outlook Web App**.

(Note: In this example environment, the **OWA** login page is strengthened **with Symantec VIP** two-factor authentication **2FA** using a **one-time security code**.)

Confidence in a connected world. ✓Symantec.

S/MIME is not supported in Conversation view.
To view this message in a new window, **click here**.

The content cannot be displayed because the S/MIME control is not installed.
To install S/MIME, **click here**.

Run the **owasmime.msi** installer.

Confidence in a connected world.   ✔Symantec.
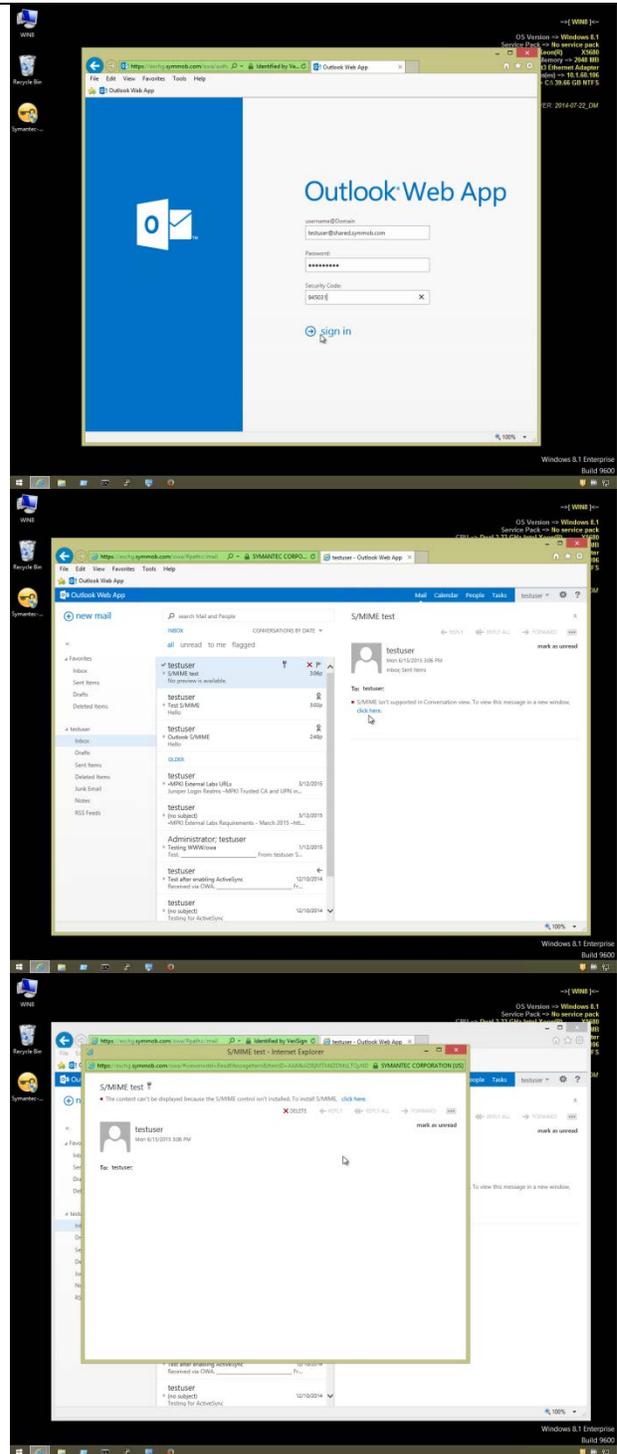
Please wait while Windows configures **Microsoft S/MIME ActiveX Control**.

The S/MIME control was successfully installed on this computer. Before you can send and view S/MIME messages in Outlook Web App, you need to **sign out and sign back in**.

Open the S/MIME message again, and wait for the control and page to load.

Confidence in a connected world. ✓Symantec.
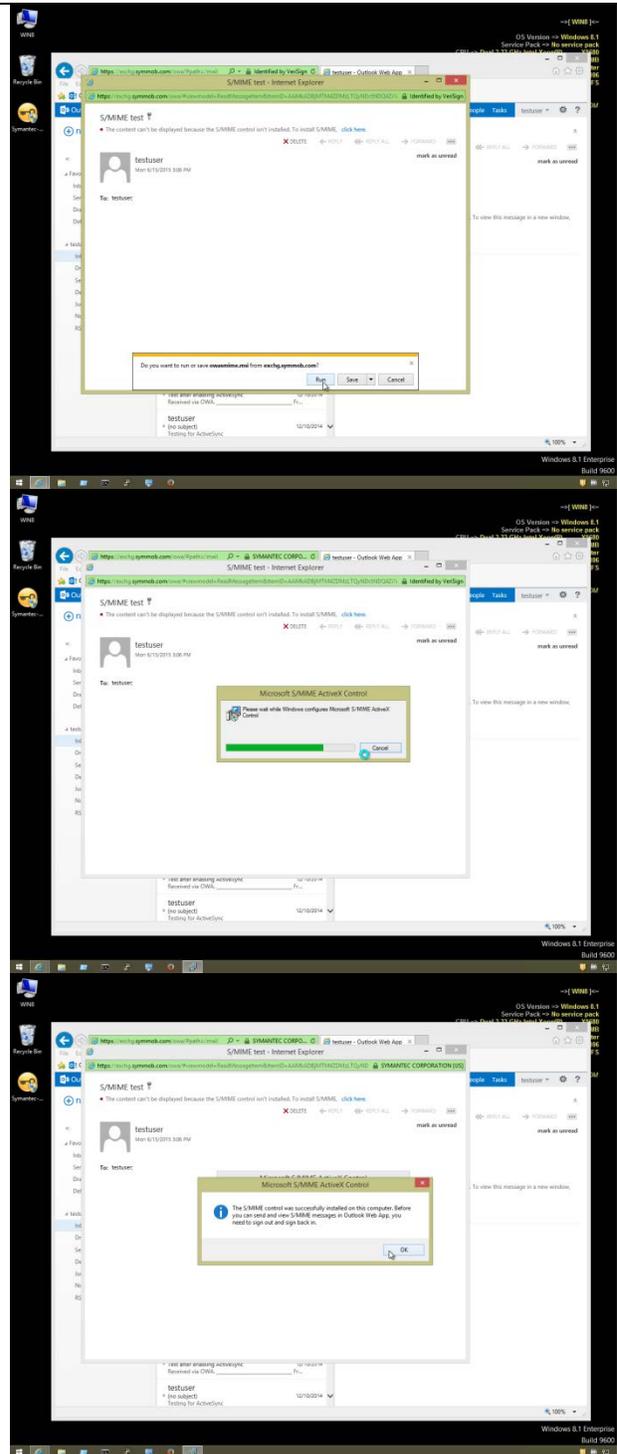
If your certificate policy requires a PIN to access the certificate store, **enter the PIN**.

The message is readable.

The digital signature on this message is valid and trusted. For more information, **click here**.

Digital signature information is displayed.

Confidence in a connected world. ✓Symantec.
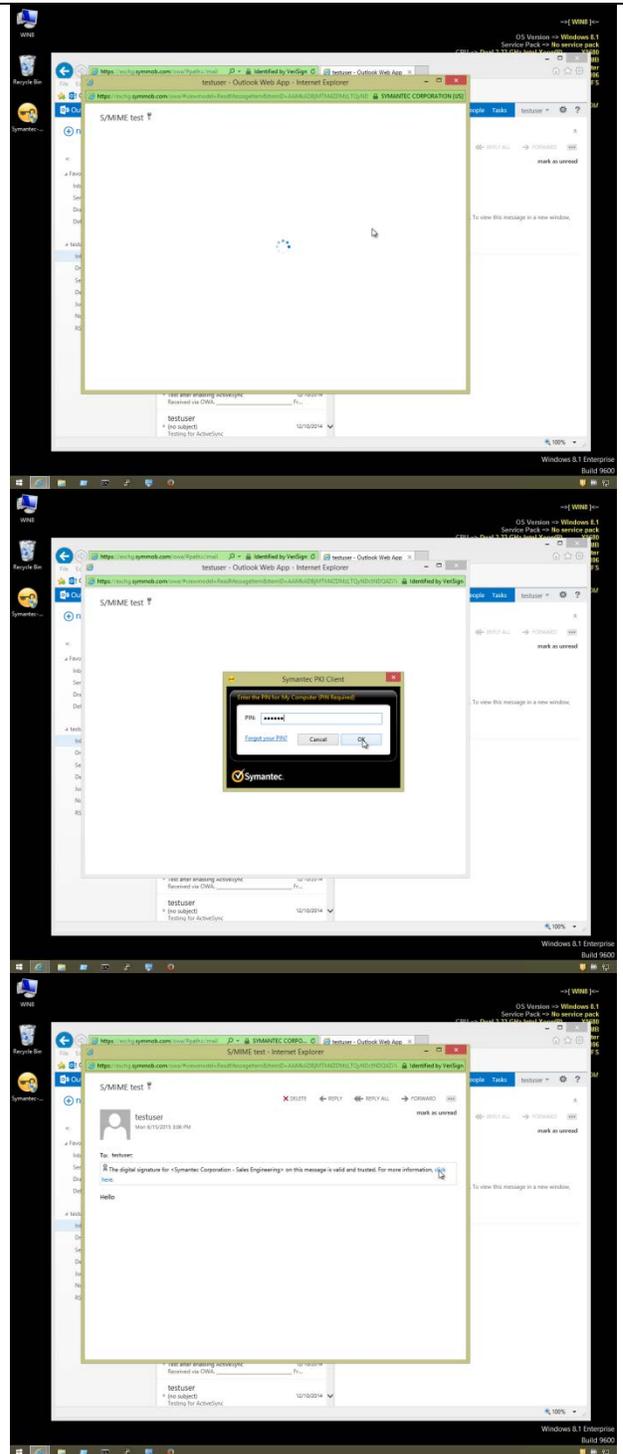
Next, reply to the message.

Digital signature and encryption features can be disabled/enabled in the **extended menu | show message options**.

Enable the check boxes for:
        Encrypt this message (S/MIME)
        Digitally sign this message (S/MIME)

Confidence in a connected world. ✔Symantec.
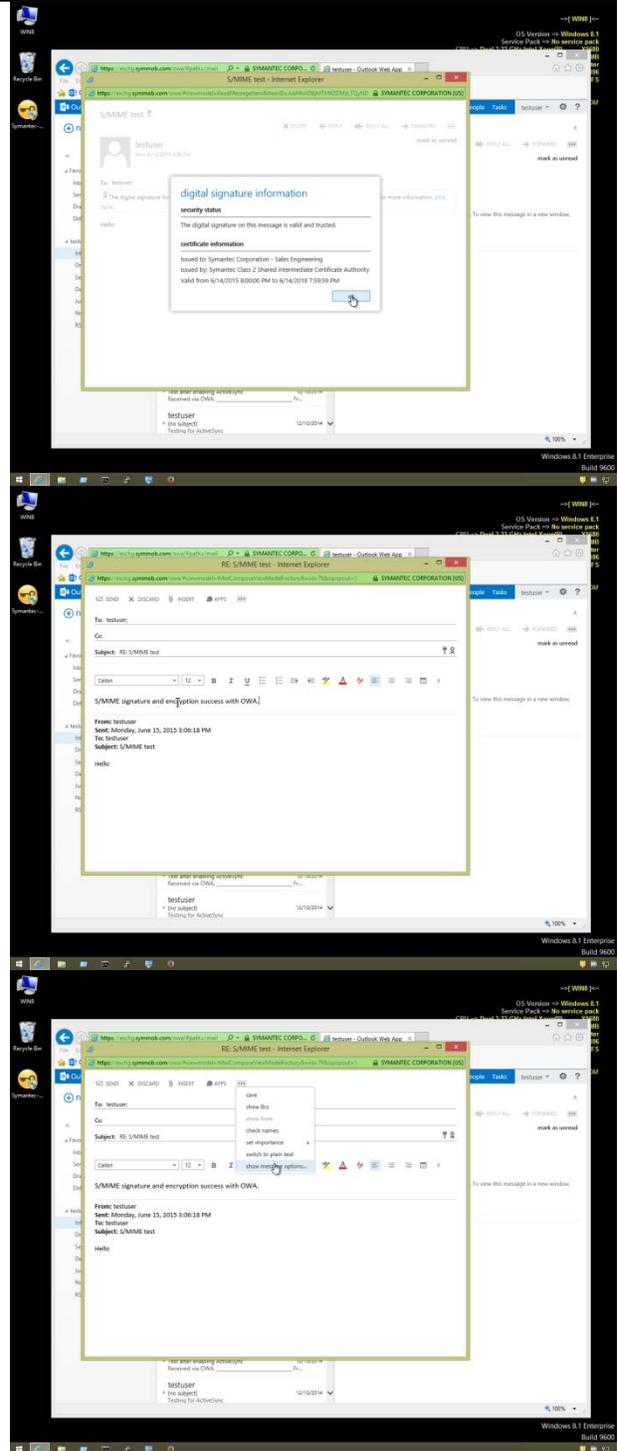
Send the message.

The digital signature on this message is valid and trusted.

Just for fun, return to **Outlook** mail client.

Confidence in a connected world. ✓Symantec
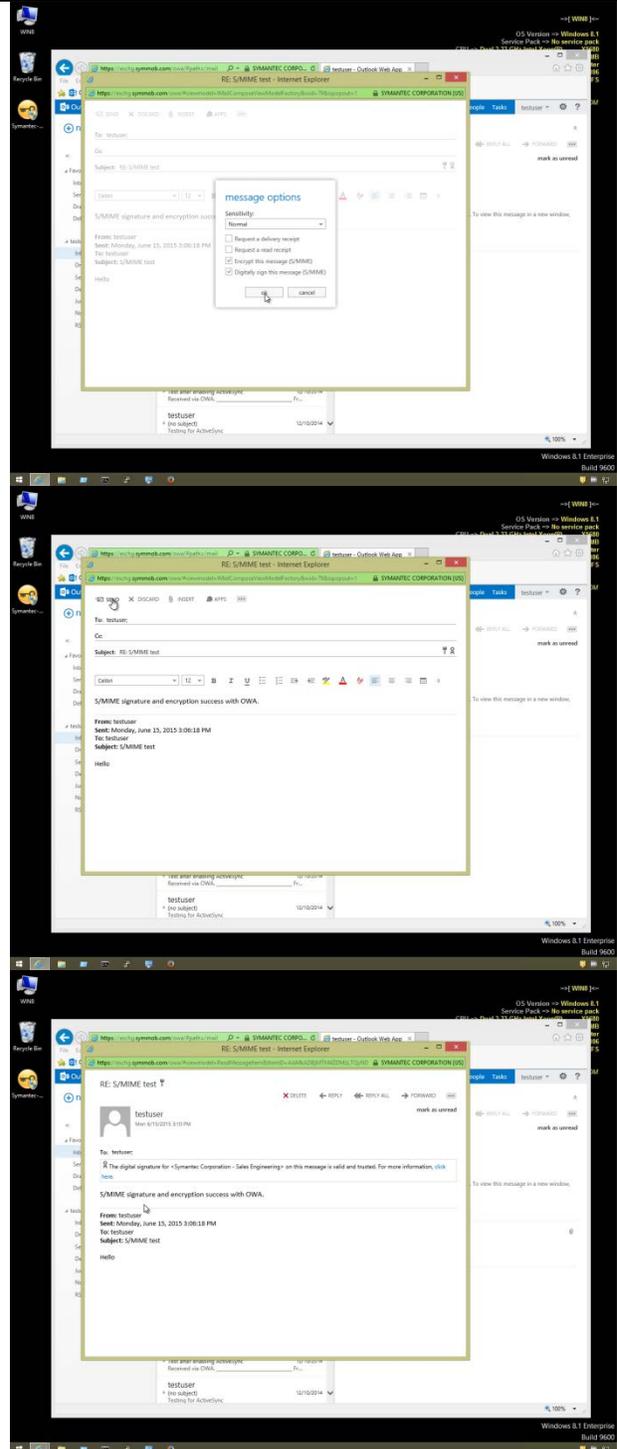
PKI Client prompts you to enter your certificate store PIN.

Outlook mail client displays the signed and encrypted message in the conversation view window.

Confidence in a connected world. Symantec.