HYPERSECU®

Securing Outlook Email with the HYP2003

2018-10-17

HSTE-NB0007-RV 1.1

HYPERSECU INFORMATION SYSTEMS INC

#200-6191 Westminster Hwy, Richmond, BC V7C 4V4 Canada
1 (604) 279-2000| hypersecu.com

Table of Contents

Introduction

Using the HYP2003, you can digitally sign and encrypt your emails in platforms such as Microsoft Outlook. Digital signing will protect your identity in case your email is ever compromised. Any email sent without your digital signature will be considered untrusted.

Before you can digitally sign or secure your emails in Outlook, you must have an email digital certificate from a valid certificate authority.

Requirements

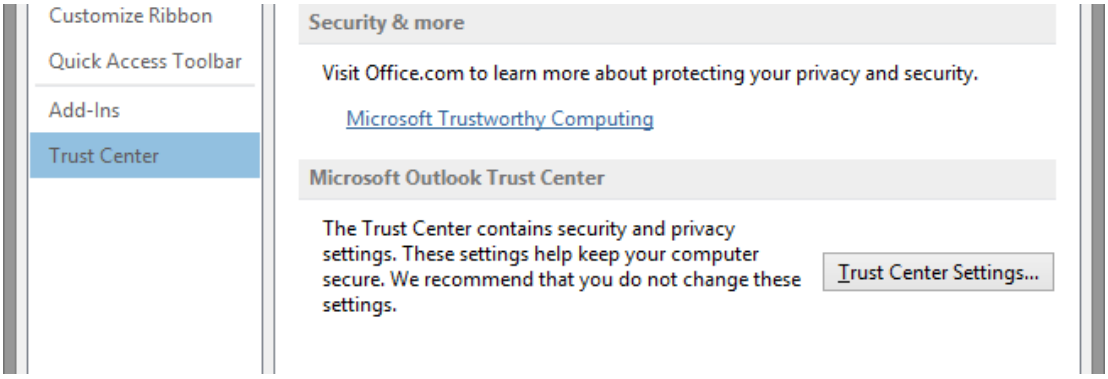
- HYP2003 token
- A valid email digital certificate enrolled on the HYP2003 token
- The latest version of HyperPKI Manager for HYP2003
- Microsoft Outlook 2007 or above
- Windows XP or above

Securing Your Emails

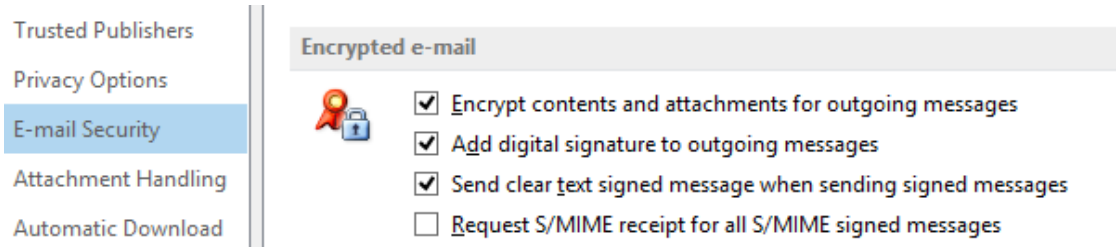
Configuring Outlook for the HYP2003

Most recent versions of Microsoft Outlook allow for digital signing and encryption. This guide will discuss enabling digital signing with the HYP2003 for Outlook 2013. Variations in procedures may exist for earlier versions of Outlook.

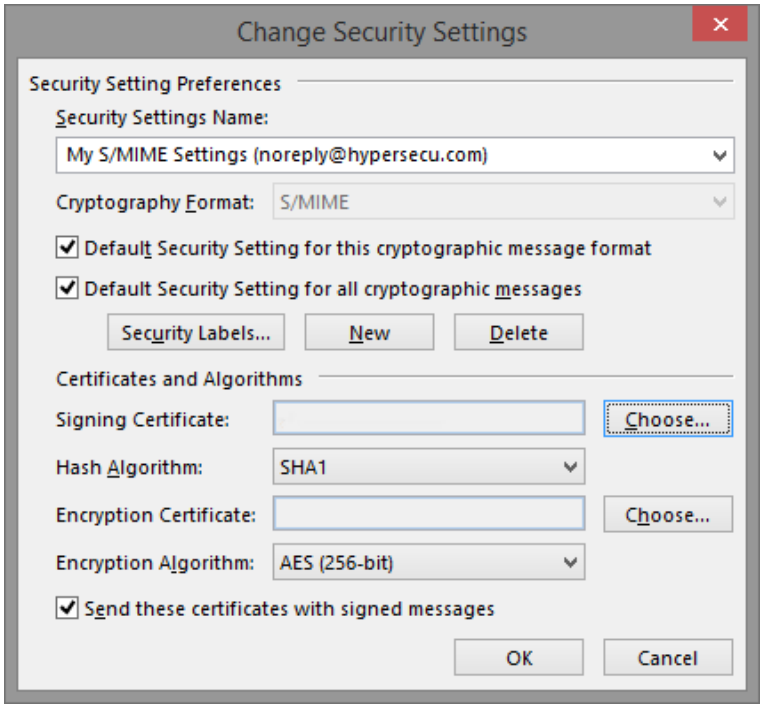
1. In the File menu, click **Options**.
2. In the Outlook Options window, select the **Trust Center** tab and click **Trust Center Settings...**



3. Select the **E-mail Security** tab and enable the relevant settings:
   - To encrypt all outgoing emails by default, check **Encrypt contents and attachments for outgoing messages**.
   - To digitally sign all outgoing emails by default, check **Add digital signature to outgoing messages**.
   - To manually sign and encrypt your outgoing emails, *Signing and Encrypting an Outgoing Message* on page 5.



4. In the Change Security Settings window, choose your Signing Certificate and Encryption Certificate.



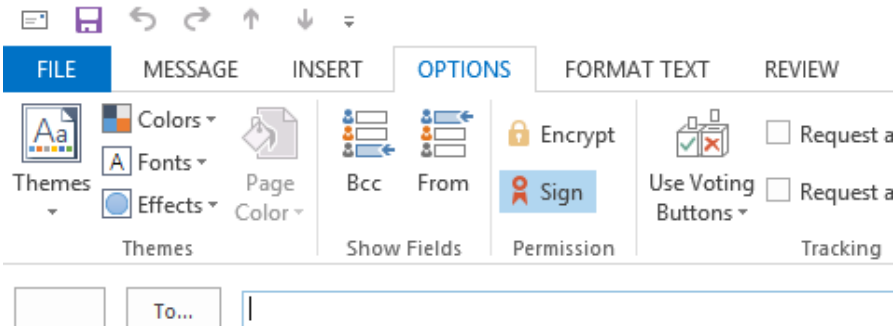
5. Click **OK**.

Signing and Encrypting an Outgoing Message

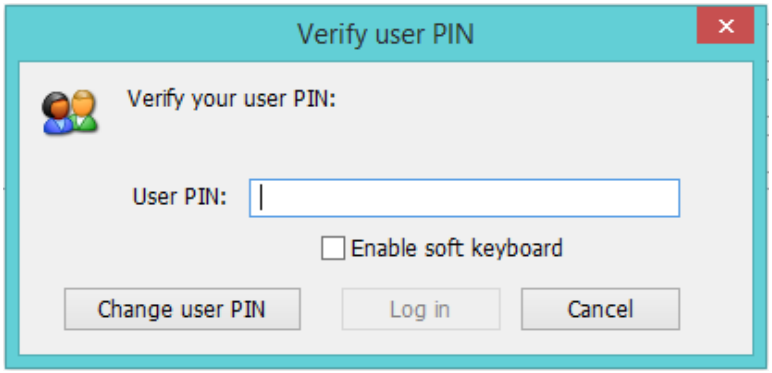
If you've enabled automatic signing and encryption in your Trust Center settings, all outgoing messages will be signed and encrypted by default and you will be prompted to enter your PIN when necessary.

If you have not enabled automatic signing and encryption, you must turn these options on manually each time you create a new email.

1. Ensure the HYP2003 is inserted into a valid USB port.
2. Click **New Email** and select the **Options** tab.
3. Under Permissions, enable the relevant options:
   - To encrypt your outgoing message, click **Encrypt**.
   - To digitally sign your message, click **Sign**.



4. Compose your message and click **Send**.
5. If you are prompted, enter your PIN.



NOTE: Only someone in possession of a valid digital certificate of their own can view an encrypted message. Ensure that your contacts are able to open encrypted emails before sending one.

Decrypting an Incoming Message

To decrypt an incoming message:

1. Ensure you have inserted the HYP2003 containing your digital certificate into a valid USB port.
2. Enter your PIN if prompted.

IMPORTANT: If you permanently delete or remove your certificate, you will no longer have access to previously encrypted emails. Do not delete old certificates if you still wish to access former emails.
