Microsoft Office Outlook Edition

Revision History			
Rev.	Date (YYYY/MM/DD)	Description	Editor
V.1.0	2015/4/1	First revision	NII
V.1.1	2016/12/26	Amendment with addition of [NII Open Domain S/MIME CA] as a new Certificate Authority	NII
V2.0	2018/2/26	Supported environment update: Outlook 2013 or later	NII

Table of Content

1. Installing the S/MIME Certificate

1-1. Operating Environment

The procedures only in the following environment are described in this document:

Supported environment:
Microsoft Office Outlook 2013 or later

1-2. Prerequisites

The prerequisites for using the S/MIME Certificate in Microsoft Office Outlook are described.
Replace the technical terms according to the user environment in which the S/MIME Certificate will be used. (The procedures required for Microsoft Office Outlook 2013 are described in this document.)

| Prerequisites |
|---|
| 1. The S/MIME Certificate has been installed in the web browser (described in the User's Manuals for Installation in Different Web Browsers: Microsoft Internet Explorer Edition); and
2. Microsoft Office Outlook 2013 or later is installed. |

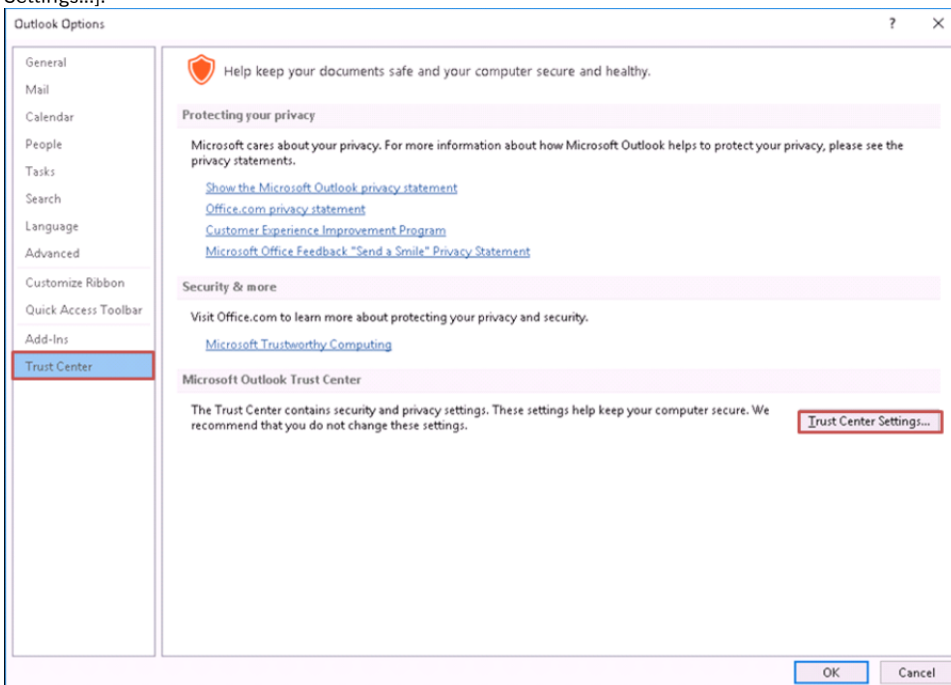## 1-3. Install Procedure

Installing the Certificate

**1.** Open Microsoft Office Outlook and click on the [File] tab.
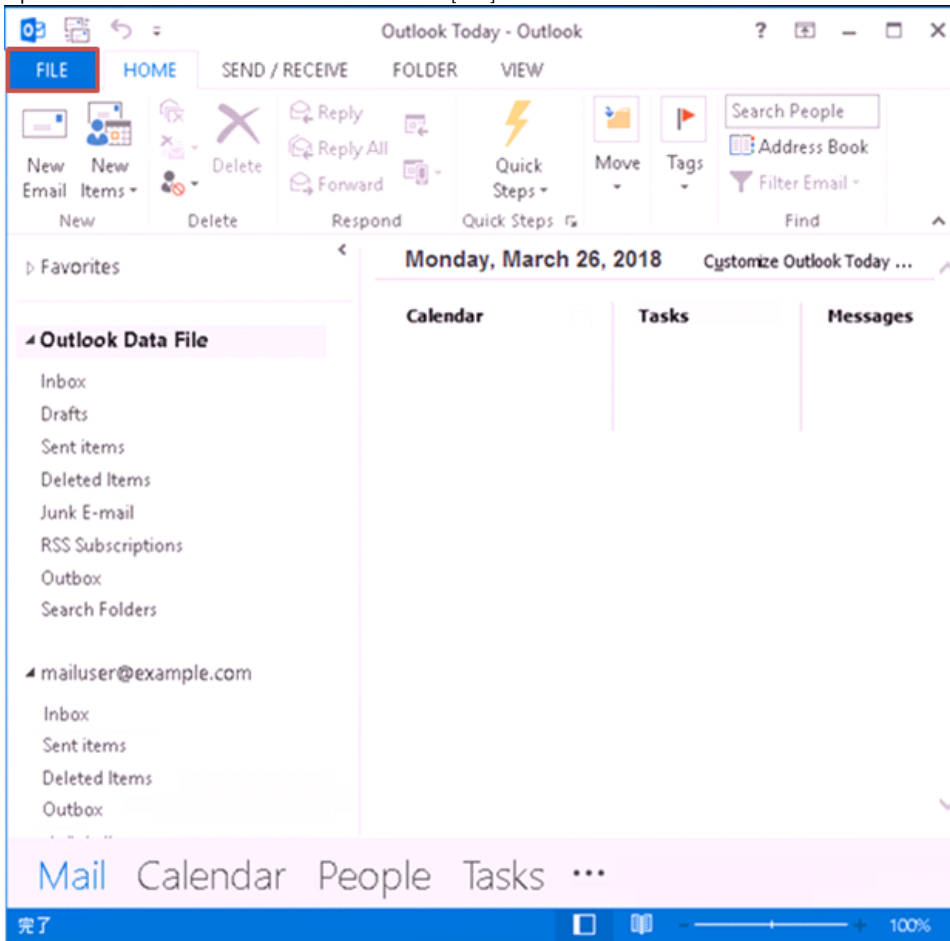
2. Click [Options] in the menu list on the left side of the [Account Information] screen.
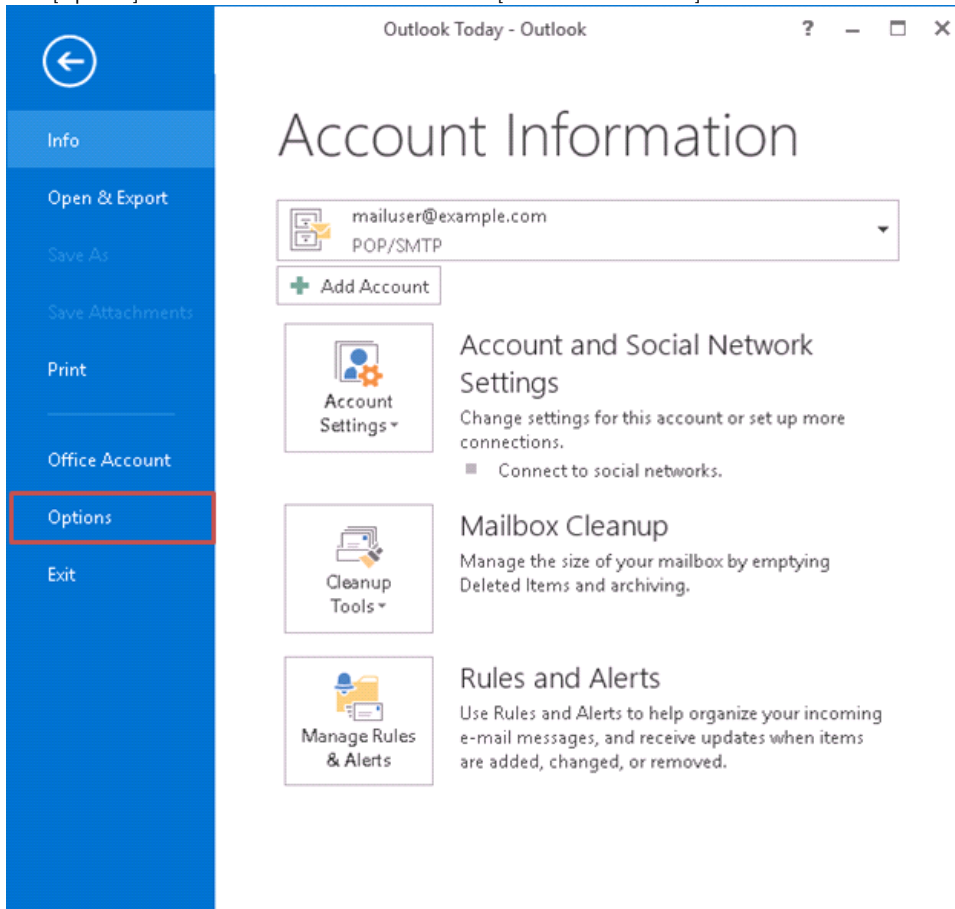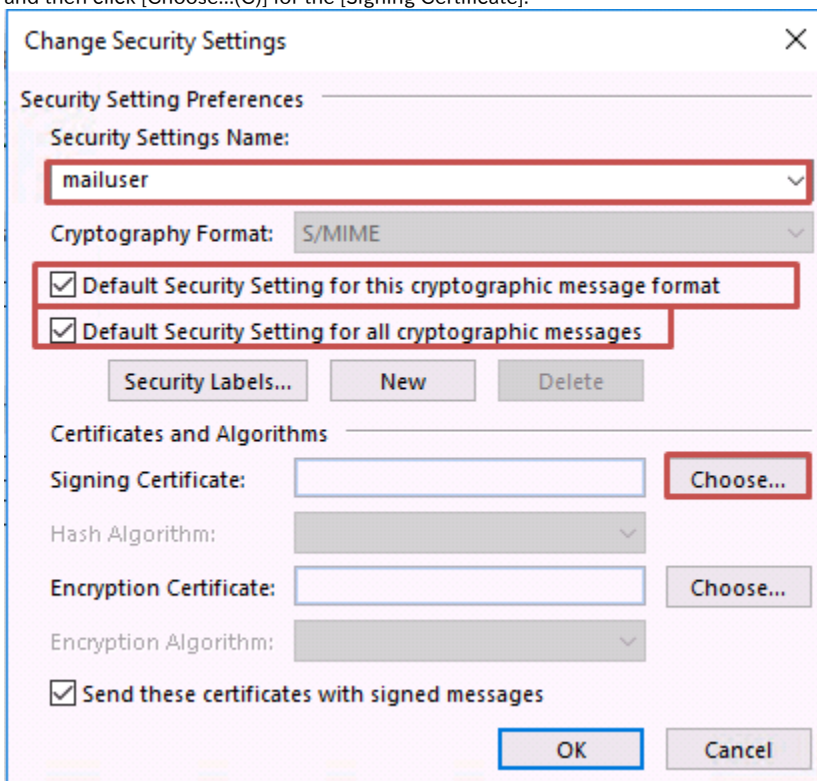

3. In the [Outlook Options] dialog box, select [Trust Center] in the list of options on the left side of the dialog box and then click [Trust Center Settings...].
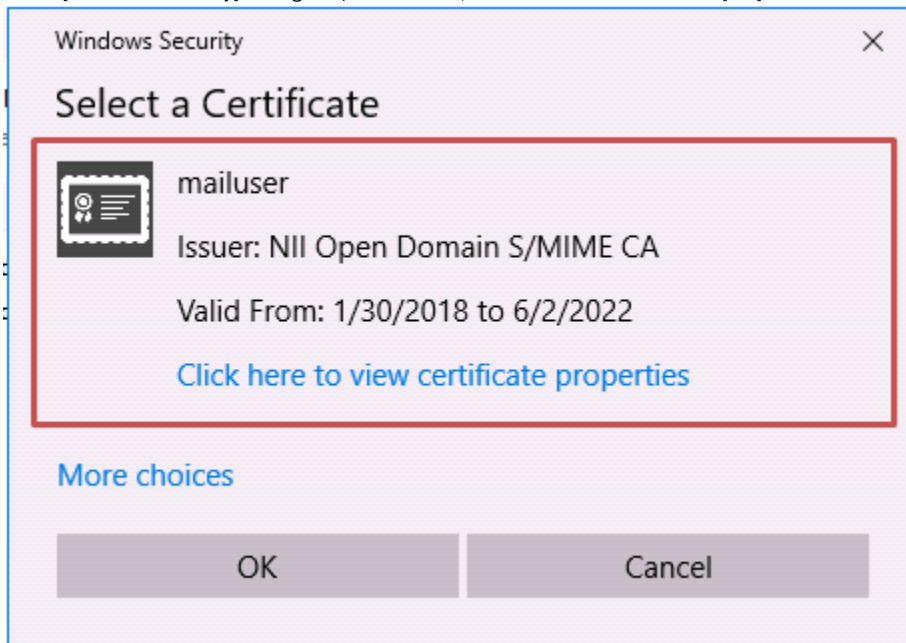

4. In the [Trust Center] dialog box, select [E-mail Security] in the list of options on the left side.
   Check the [Add digital signature to outgoing messages (D)] and [Send clear text signed message when sending signed messages (T)] checkboxes and click [Settings...(S)].
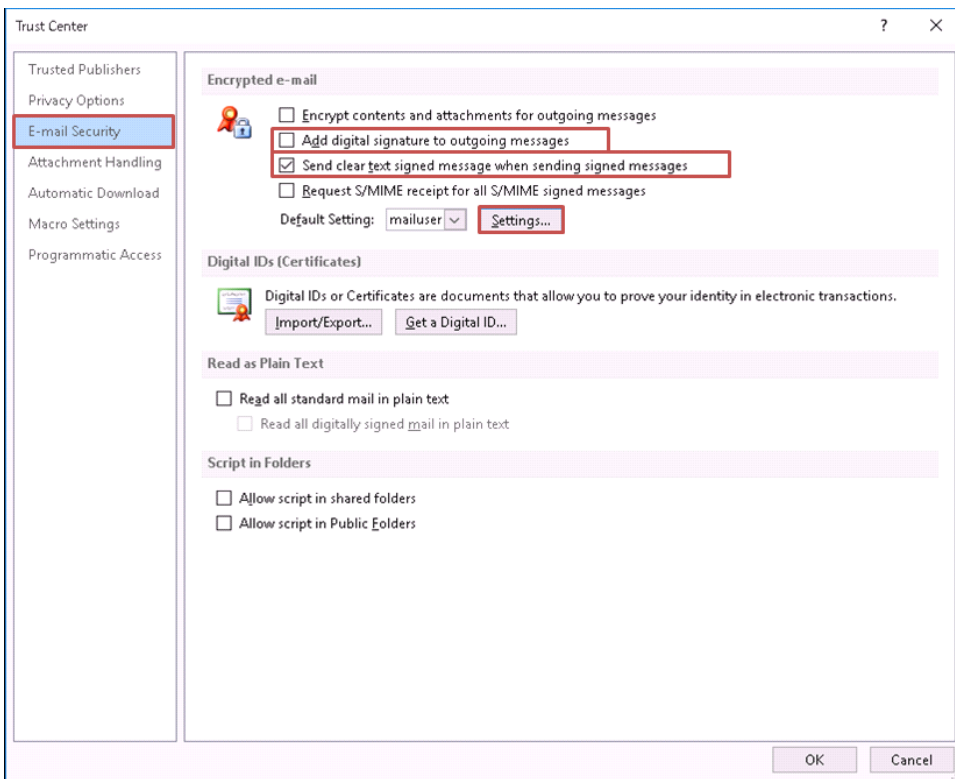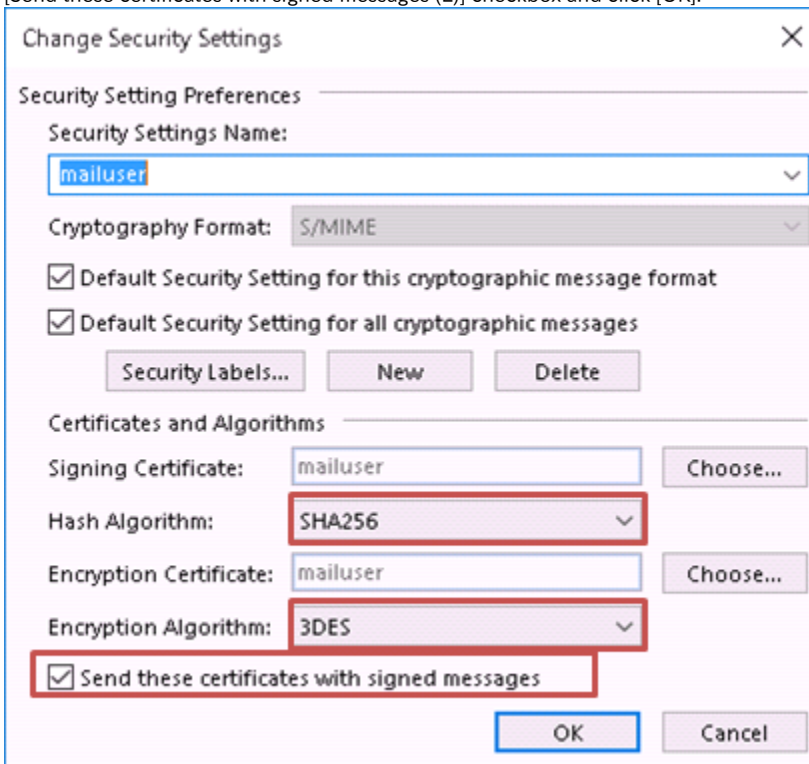
5. The [Change Security Settings] dialog box will appear. Enter any string in the [Security Settings Name:] box.
Check both [Default Security Setting for this cryptographic message format (T)] and [Default Security Setting for all cryptographic messages (M)] checkboxes,
and then click [Choose...(C)] for the [Signing Certificate].

6. In the [Windows Security] dialog box, select the S/MIME Certificate and click [OK].

Windows Security   ✕

Select a Certificate

mailuser

Issuer: NII Open Domain S/MIME CA

Valid From: 1/30/2018 to 6/2/2022

Click here to view certificate properties

More choices

OK   Cancel

7. Select [SHA256] from the [Hash Algorithm (A):] drop down list and [3DES] from the [Encryption Algorithm (L):] drop down list. Check the [Send these certificates with signed messages (E)] checkbox and click [OK].

Change Security Settings   ✕

Security Setting Preferences

Security Settings Name:

mailuser

Cryptography Format: S/MIME

☑ Default Security Setting for this cryptographic message format

☑ Default Security Setting for all cryptographic messages

Security Labels...   New   Delete

Certificates and Algorithms

Signing Certificate: mailuser   Choose...

Hash Algorithm: SHA256

Encryption Certificate: mailuser   Choose...

Encryption Algorithm: 3DES

☑ Send these certificates with signed messages

OK   Cancel

Note: Select a relevant Hash Algorithm for the user environment.
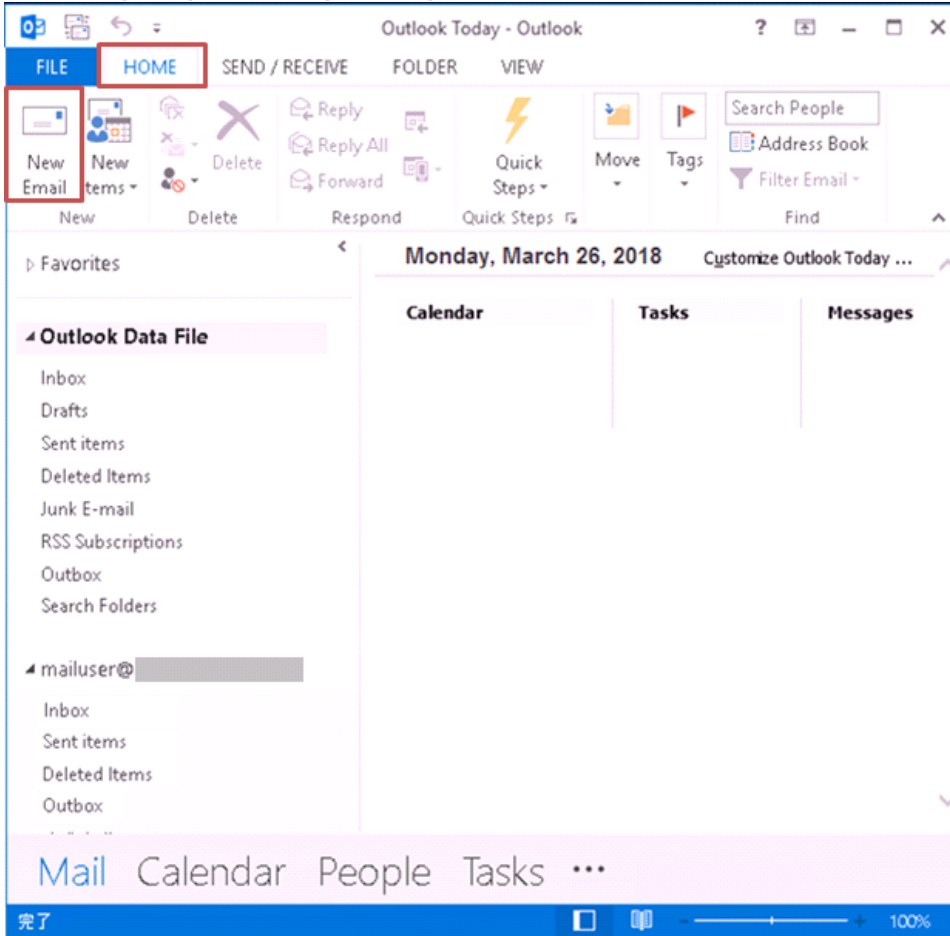
8. Click [OK].
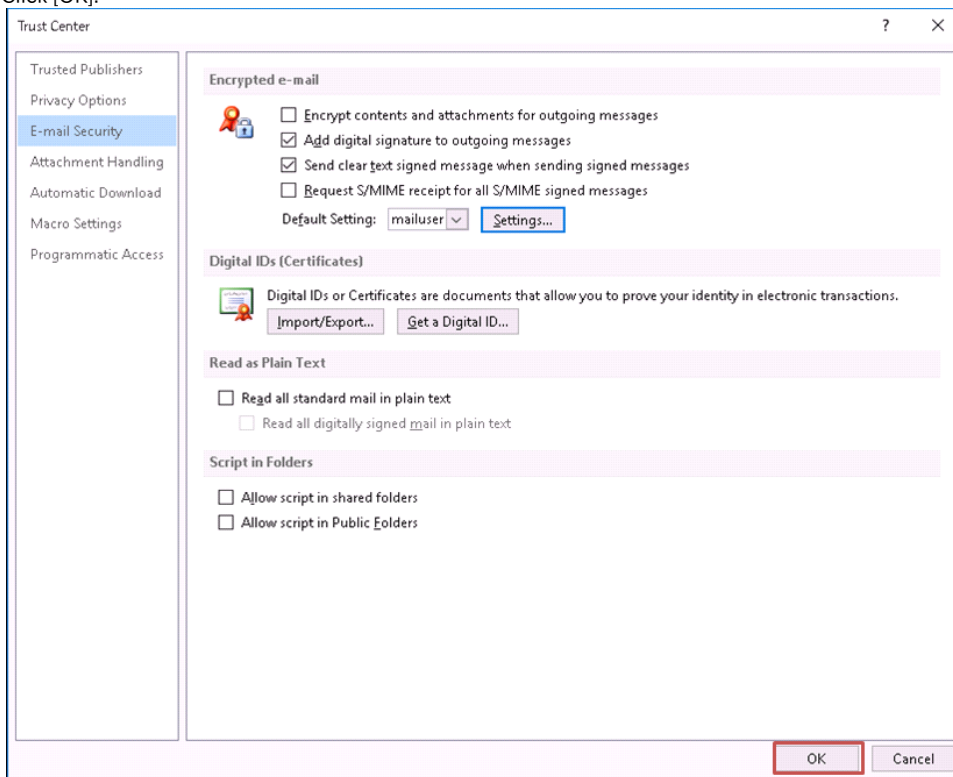
9. Click [OK].
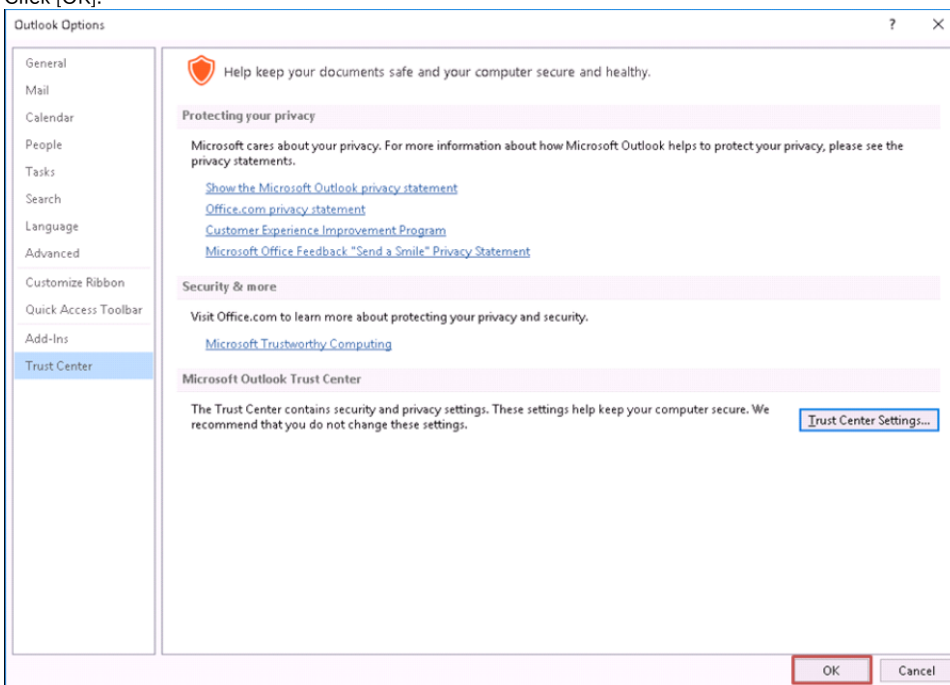
This completes the S/MIME Certificate installation.
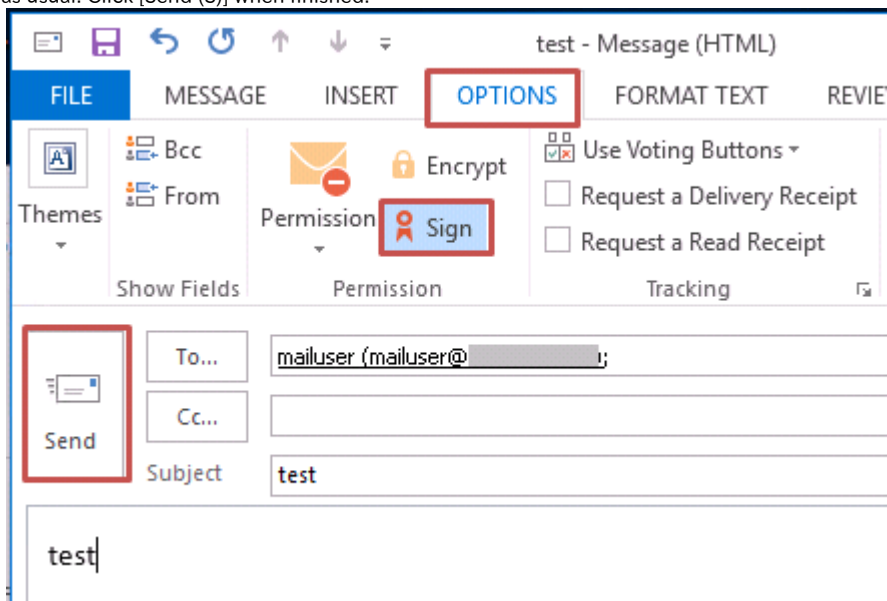
2. Sending Digitally Signed E-mails

2-1. How to Send Digitally Signed E-mails

How to Send Digitally Signed E-mails

1. Click on the [HOME] tab and then [New Email].

2. The [MESSAGE] tab screen will appear. Select [OPTIONS] tab to confirm that the [Sign] button is active, and then create the new message as usual. Click [Send (S)] when finished.
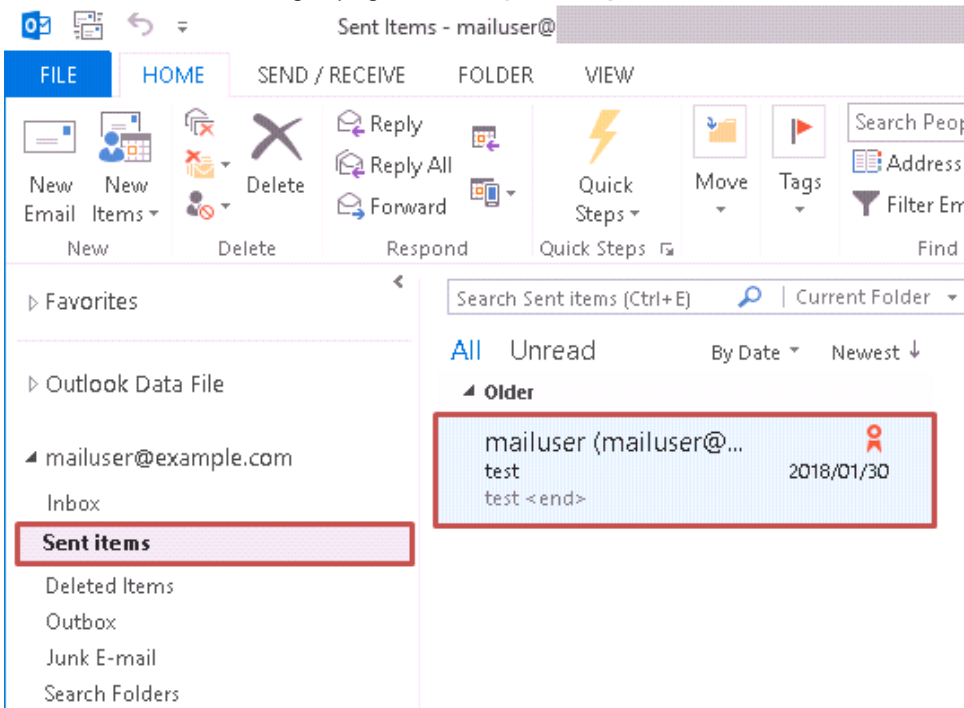

Note: If you do not use the digital signature, click the [Sign] button to deactivate the signature and then click [Send (S)].
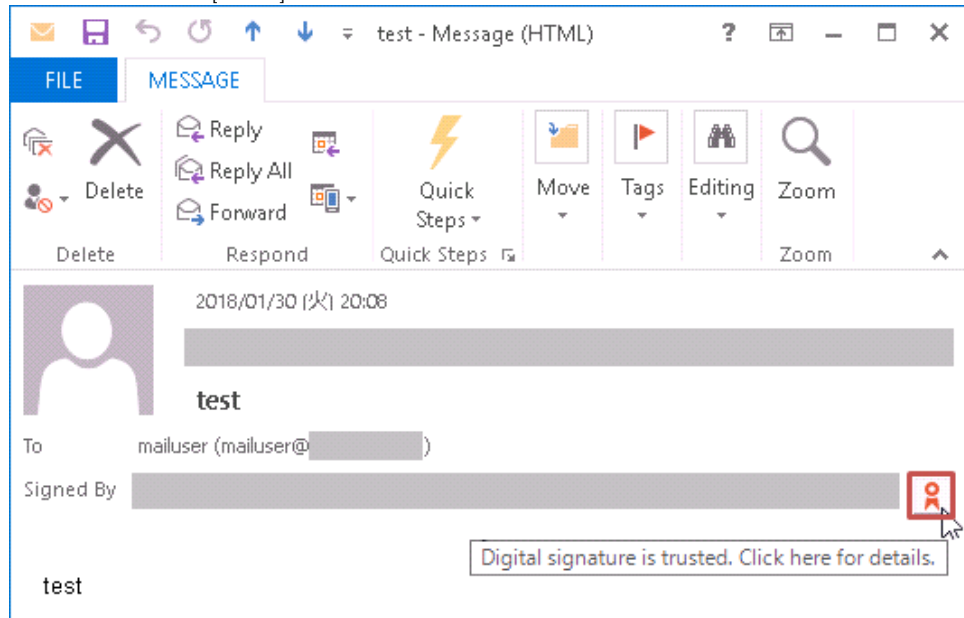This completes sending digitally signed e-mails.

2-2. How to Confirm a Sent E-mail That Was Digitally Signed

How to Confirm a Sent E-mail That Was Digitally Signed

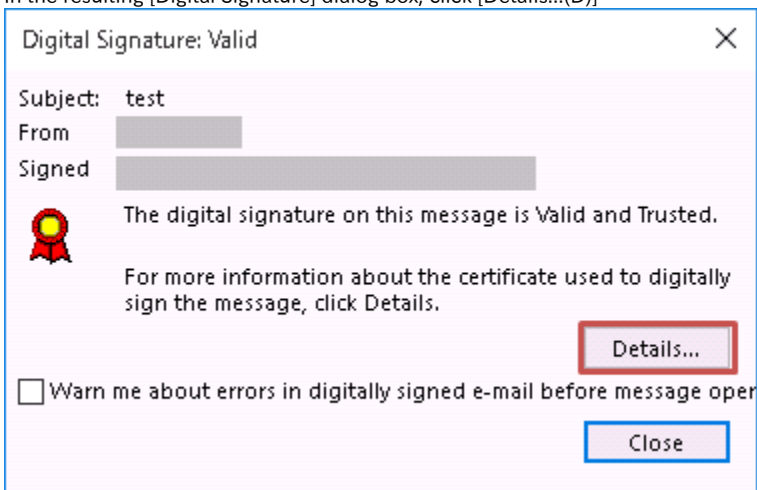1. Select a sent e-mail that was digitally signed from the [Sent Items].
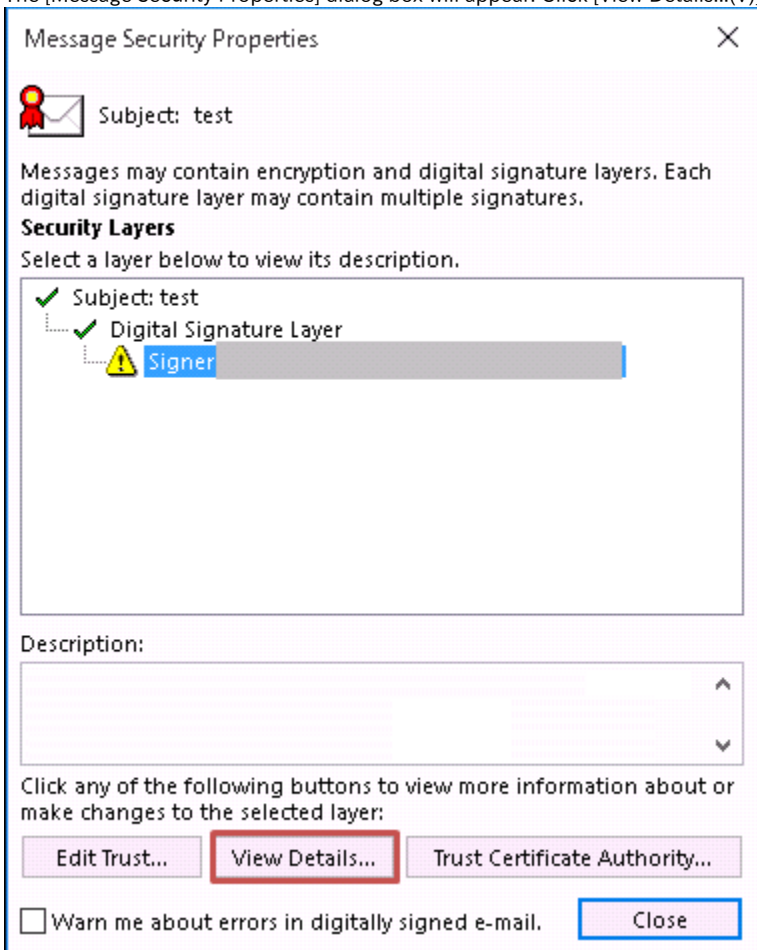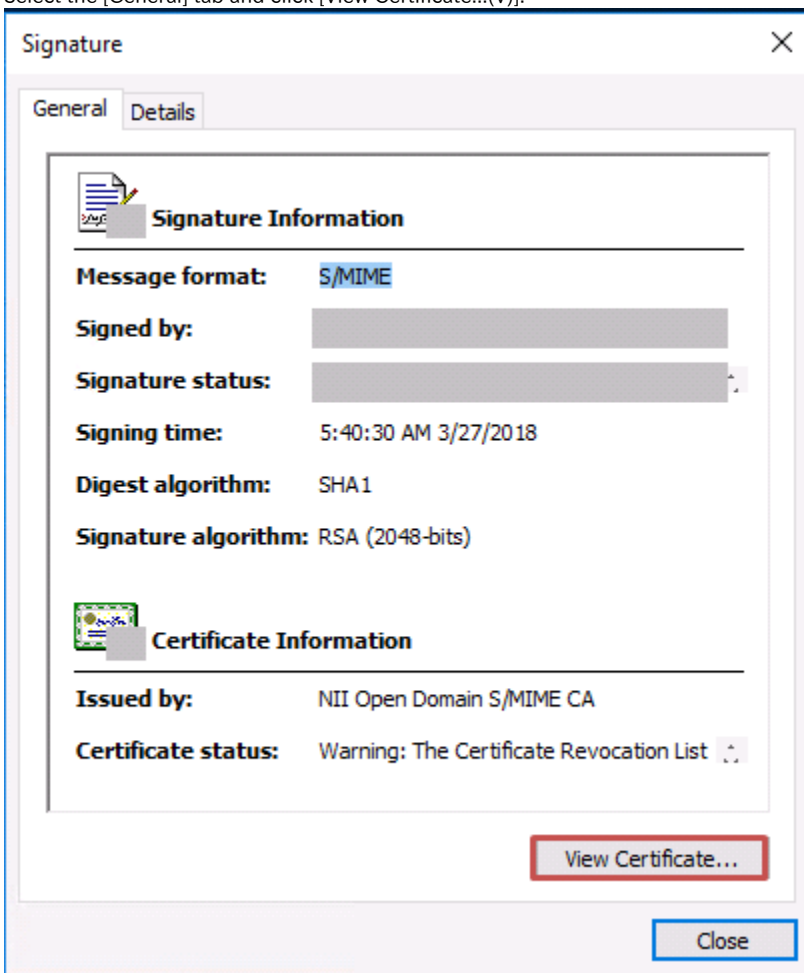

2. Click on the small red [ribbon] icon.

3. In the resulting [Digital Signature] dialog box, click [Details...(D)]


4. The [Message Security Properties] dialog box will appear. Click [View Details...(V)].

5. Select the [General] tab and click [View Certificate...(V)].

Signature ✕

General | Details

Signature Information

Message format:	S/MIME
Signed by:	
Signature status:	
Signing time:	5:40:30 AM 3/27/2018
Digest algorithm:	SHA1
Signature algorithm:	RSA (2048-bits)

Certificate Information

Issued by:	NII Open Domain S/MIME CA
Certificate status:	Warning: The Certificate Revocation List

View Certificate...

Close

6. Select the [Certificate Path] tab to make sure that the [Certificate status (S)] gives "This certificate is OK."
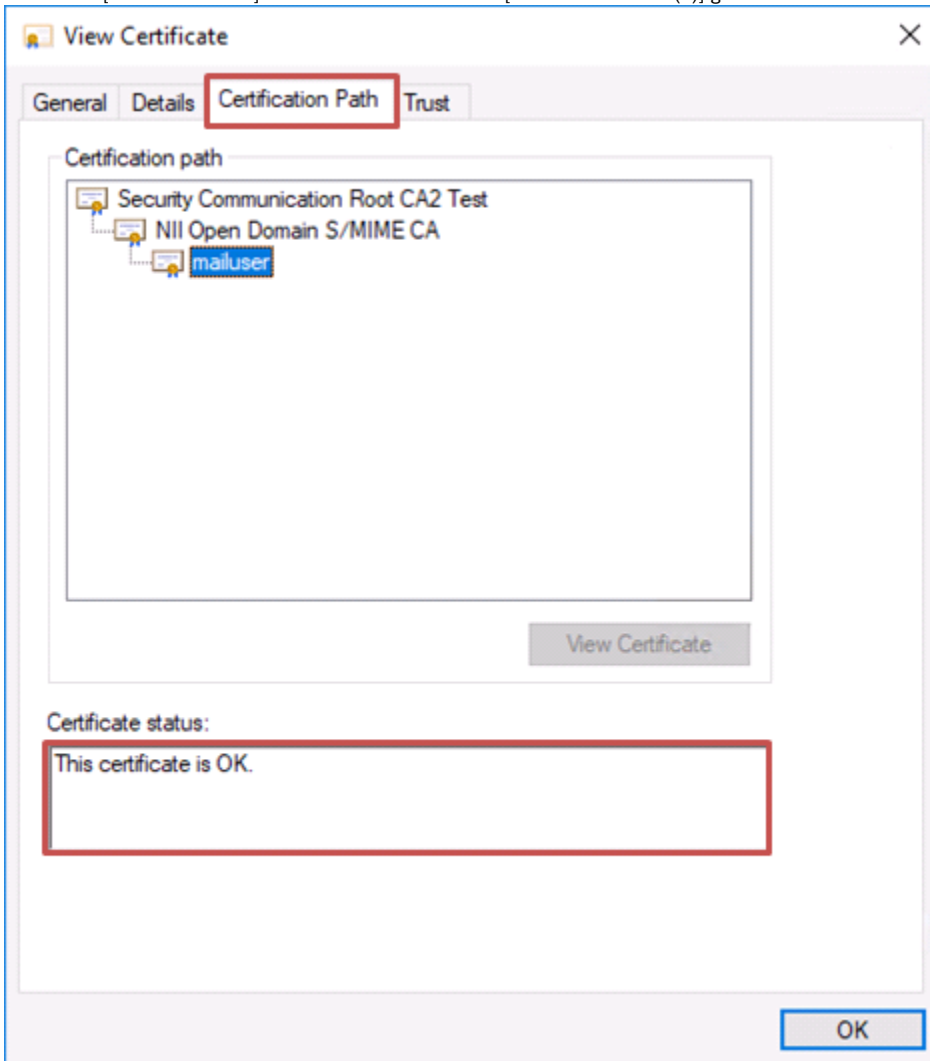
This completes confirmation of a sent e-mail that was digitally signed.