

# S/MIME certificate manual

Installing and using S/MIME in Outlook (Windows)



(This page was intentionally left blank)

## Table of contents

1 Introduction .....	4
1.1 Download Sectigo certificate .....	5
1.2 Installing the certificate.....	7
1.3 Sending mail (encrypted/signed) .....	12

# 1 Introduction

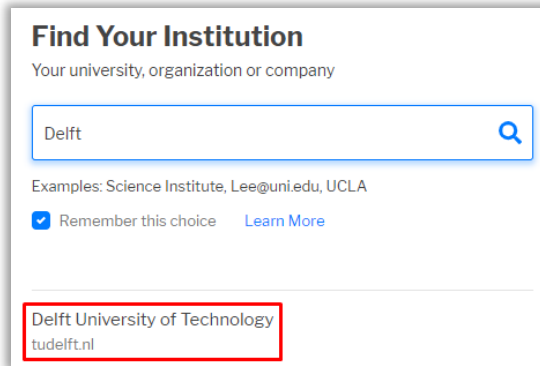
You can sign and/or encrypt your e-mail using your TU Delft mail account. This is done with S/MIME for which you will need to obtain a certificate. Certificates for TU Delft are handed out by GÉANT.

This manual describes how to generate a certificate and how you can subsequently configure S/MIME within Outlook (Windows).

## 1.1 Download Sectigo certificate

Certificates for TU Delft are handed out by GÉANT using the following instructions:

1. Open a browser and go to <https://edu.nl/sectigo-sso>
2. Find Your Institution by searching: “**Delft**”
3. Select “**Delft University of Technology**” (tudelft.nl)



**Find Your Institution**  
Your university, organization or company

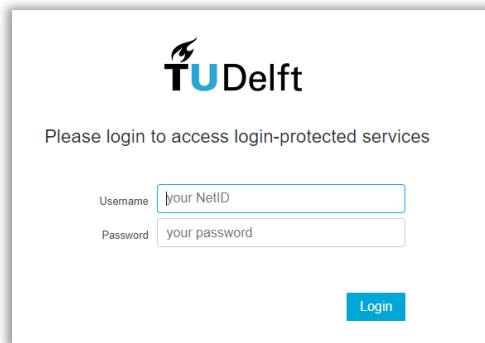
Delft

Examples: Science Institute, Lee@uni.edu, UCLA

Remember this choice [Learn More](#)

Delft University of Technology  
tudelft.nl

4. In the next screen, log in with your netID + password.



**TU Delft**

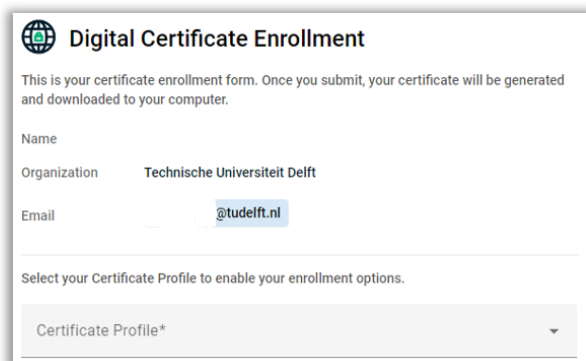
Please login to access login-protected services

Username

Password

Login

5. Review the information for logging in via SURFconext; click on “**Proceed to Cert Manager**”
6. You will arrive at the next screen. Select “**GÉANT email Signing and encryption**” via the dropdown menu:



**Digital Certificate Enrollment**

This is your certificate enrollment form. Once you submit, your certificate will be generated and downloaded to your computer.

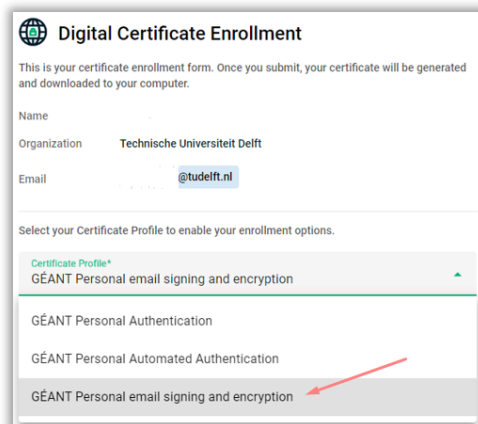
Name

Organization **Technische Universiteit Delft**

Email **@tudelft.nl**

Select your Certificate Profile to enable your enrollment options.

Certificate Profile\*



**Digital Certificate Enrollment**

This is your certificate enrollment form. Once you submit, your certificate will be generated and downloaded to your computer.

Name

Organization **Technische Universiteit Delft**

Email **@tudelft.nl**

Select your Certificate Profile to enable your enrollment options.

Certificate Profile\*

GÉANT Personal email signing and encryption

GÉANT Personal Authentication

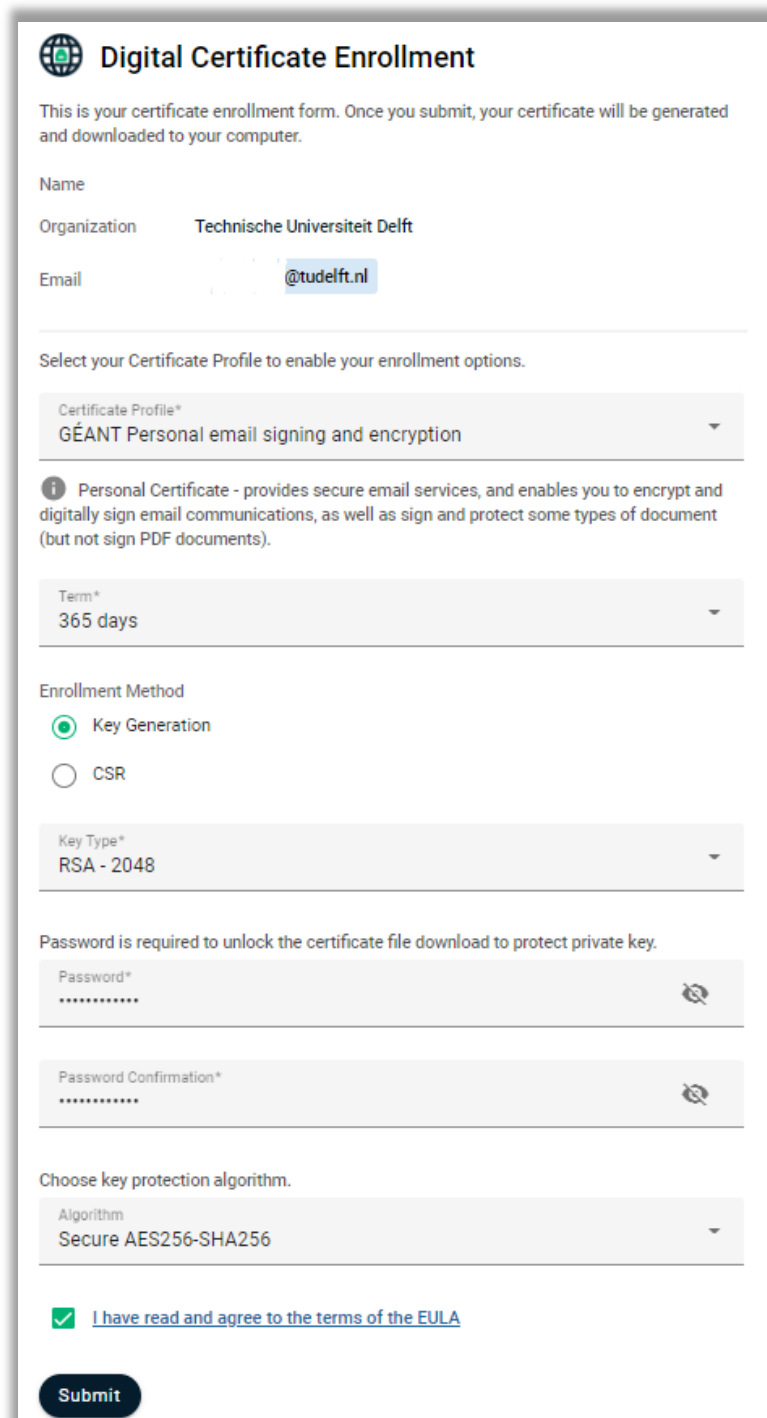
GÉANT Personal Automated Authentication

GÉANT Personal email signing and encryption

7. Choose the following settings to generate a working certificate for Windows:
  - Term:** 365 days
  - Enrollment Method:** Key Generation



- Key Type:** RSA – 2048
- Password:** save this password carefully, you will need it later when configuring in Outlook
- Key Protection Algorithm:** Secure AES256-SHA256
- Check the box to agree to the terms and click “**Submit**” to generate a certificate



**Digital Certificate Enrollment**

This is your certificate enrollment form. Once you submit, your certificate will be generated and downloaded to your computer.

Name

Organization Technische Universiteit Delft

Email [redacted]@tudelft.nl

Select your Certificate Profile to enable your enrollment options.

Certificate Profile\*  
GÉANT Personal email signing and encryption

**i** Personal Certificate - provides secure email services, and enables you to encrypt and digitally sign email communications, as well as sign and protect some types of document (but not sign PDF documents).

Term\*  
365 days

Enrollment Method

Key Generation

CSR

Key Type\*  
RSA - 2048

Password is required to unlock the certificate file download to protect private key.

Password\*  
.....

Password Confirmation\*  
.....

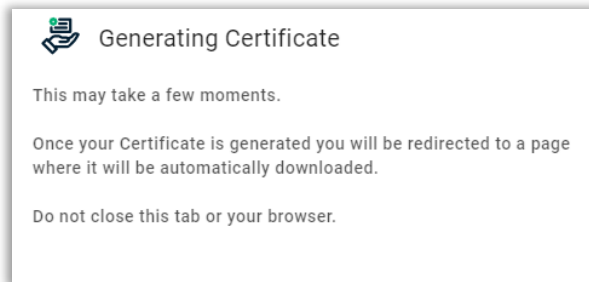
Choose key protection algorithm.

Algorithm  
Secure AES256-SHA256

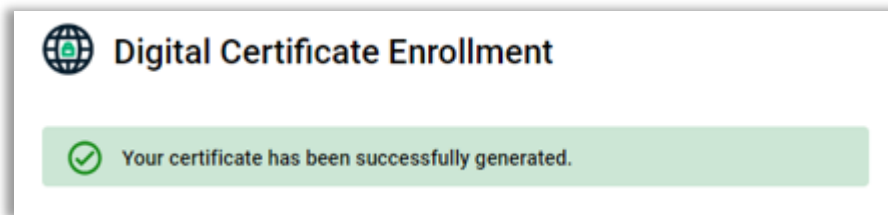
I have read and agree to the terms of the [EULA](#)

**Submit**

8. The certificate is being generated, this may take a while. Do not close this tab or your browser



9. A message will appear stating that the certificate has been successfully generated and downloaded

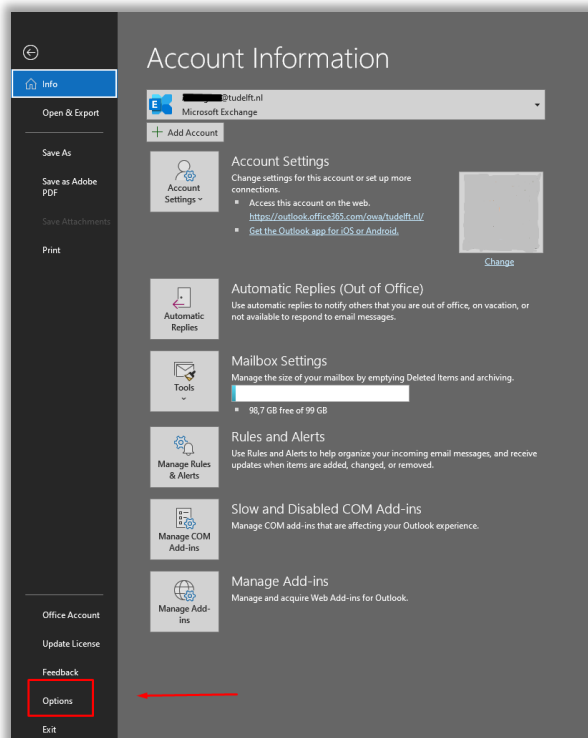


**Please note:** Save and store your encrypted certificate (certs.p12) for future use. Note that you can only decrypt your own encrypted mail with the certificate with which you previously encrypted it. If you lose this certificate there is no way of retrieving the original message!

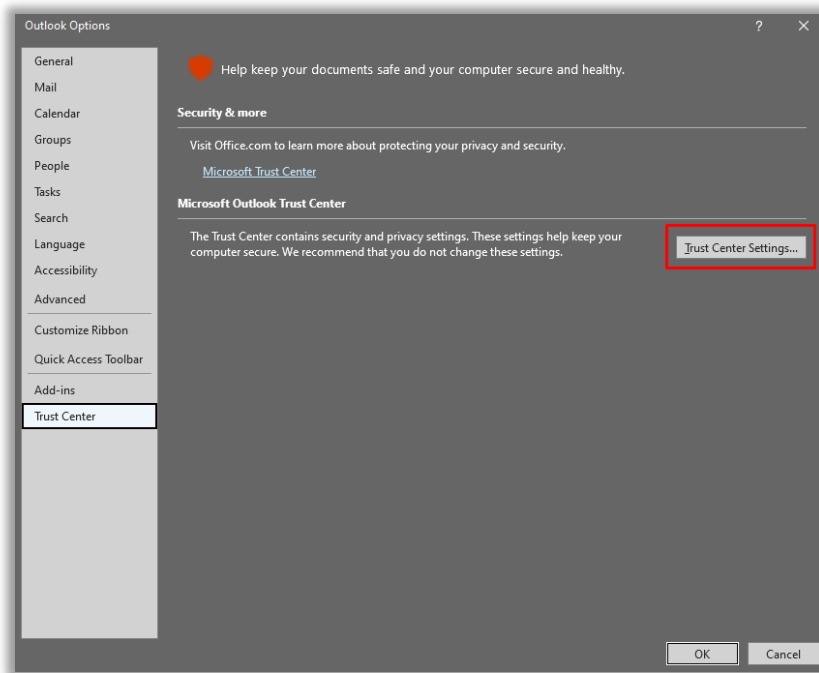
## 1.2 Installing the certificate

Now that the certificate has been downloaded, you can configure it in Outlook. Follow the steps below:

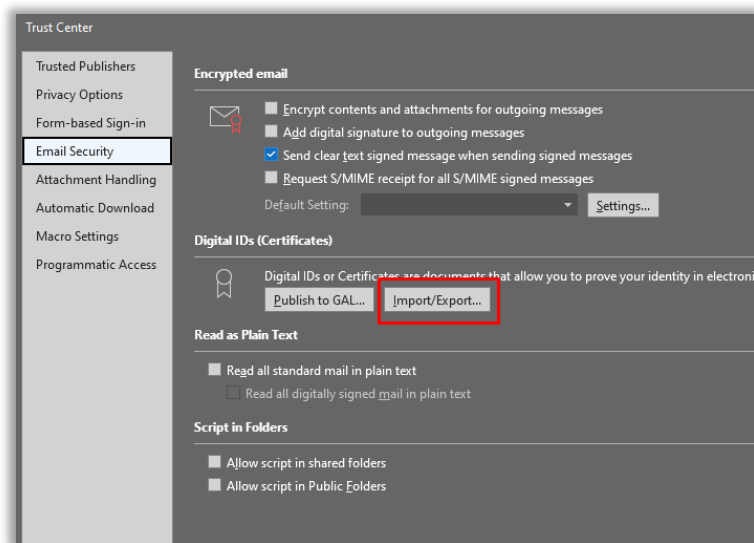
10. Open Outlook and click on **"File"** at the top of your toolbar and choose **"Options"** at the bottom:



11. Then click on “Trust Center” -> “Trust Center Settings”:

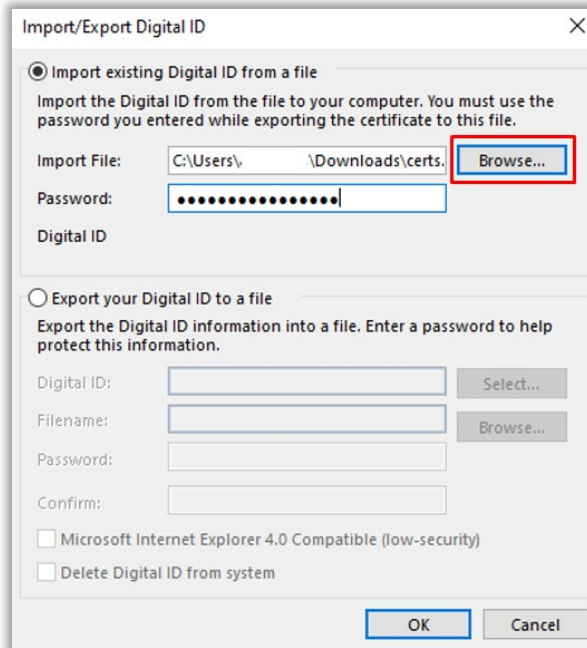


12. Then click on “Email security” -> “Import/Export”

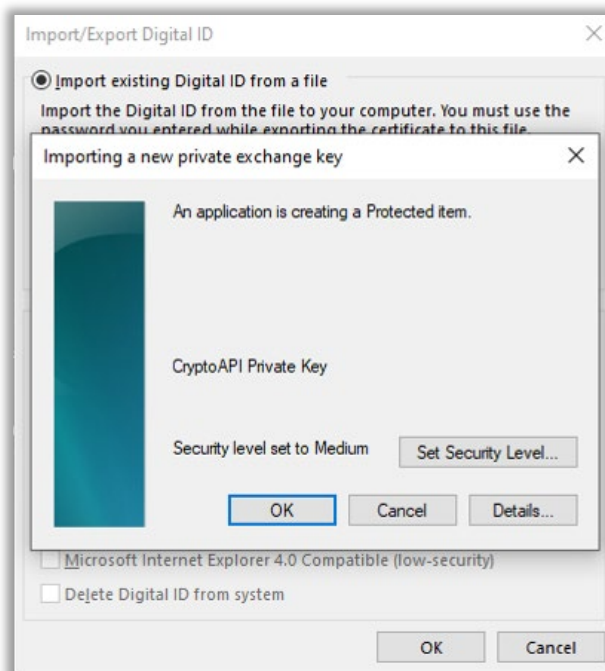




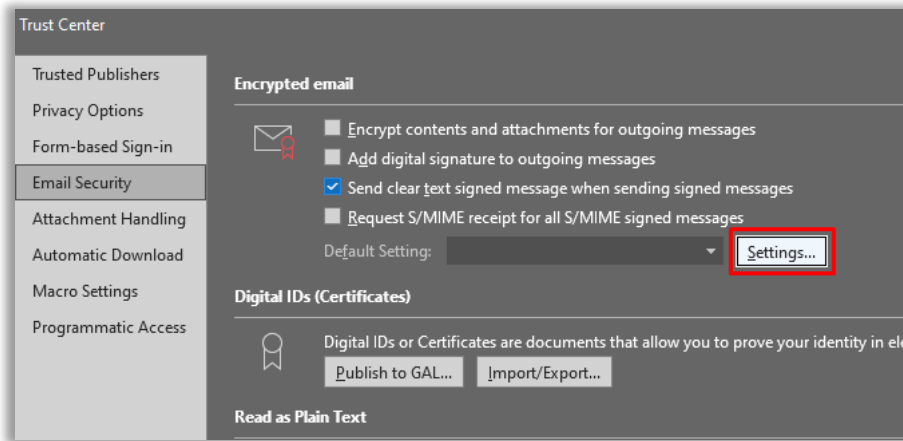
13. In the next screen, click **“Browse”** to navigate to the S/MIME certificate that was created/downloaded in step 9. Enter the corresponding password and click **“OK”**



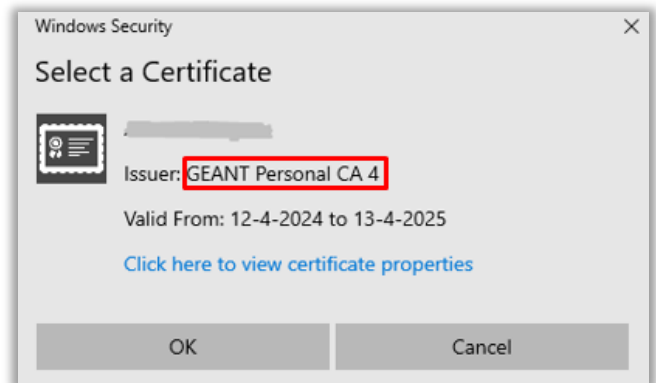
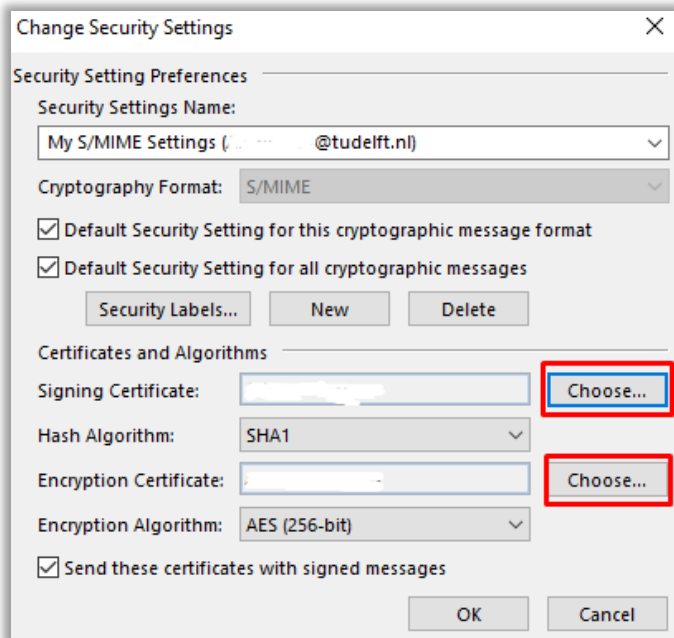
14. A new message will appear. Click on **“OK”**



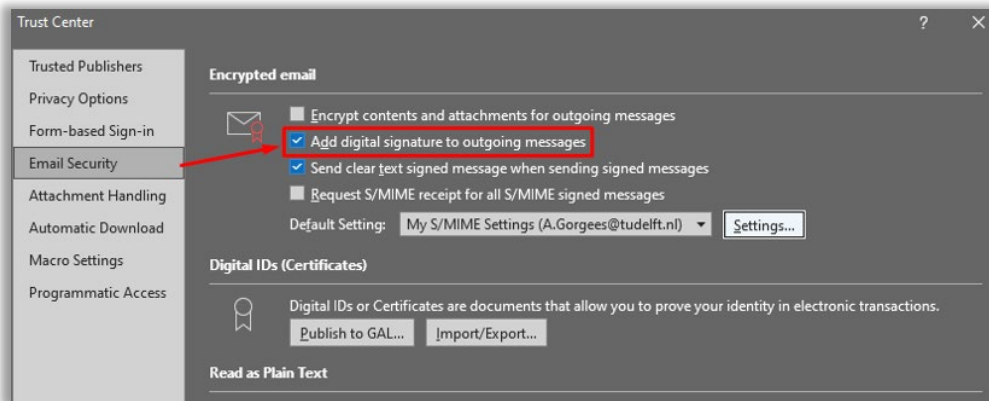
15. Then choose **“Settings...”**:



16. Make sure the following checkboxes are checked. Then click **“Choose”** to verify that the correct certificate has been selected (GEANT Personal CA4, also check the “valid from” date)..



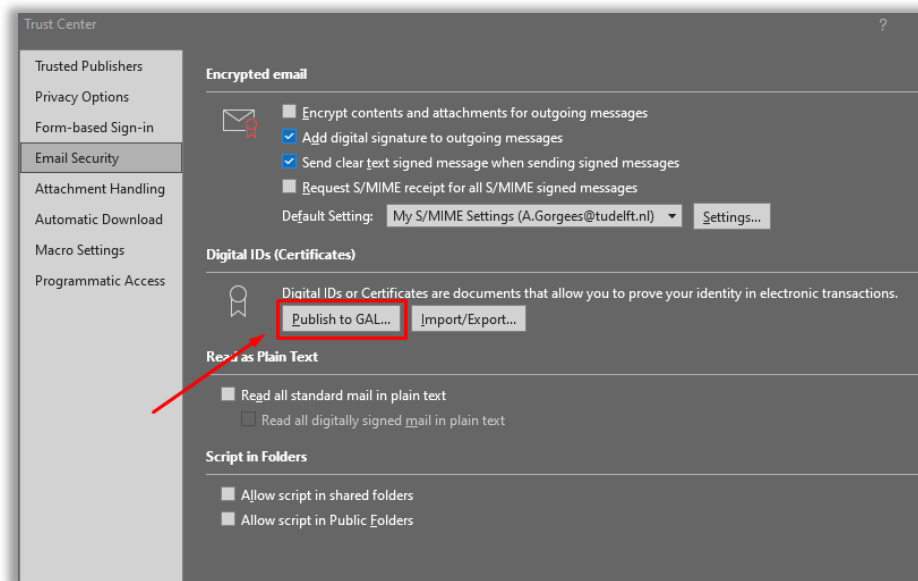
17. If this is the case, click “OK” -> “OK”. Then check the following box in Trust Center to provide your outgoing messages with a digital signature as default: **“Add digital signature to outgoing messages”**:



The **“Send clear text signed message when sending signed messages”** option is enabled by default to ensure that recipients who do not have S/MIME security can read the messages you send (recommended to leave this enabled).

Optional: **“Request S/MIME receipt for all S/MIME signed messages”** if you want to verify that your digitally signed email message has been received unchanged by the intended recipients. When you select this option, the verification information will be sent to you in a separate message.

18. **Tip:** In Trust Center Settings, click on **“Publish to GAL...”**.

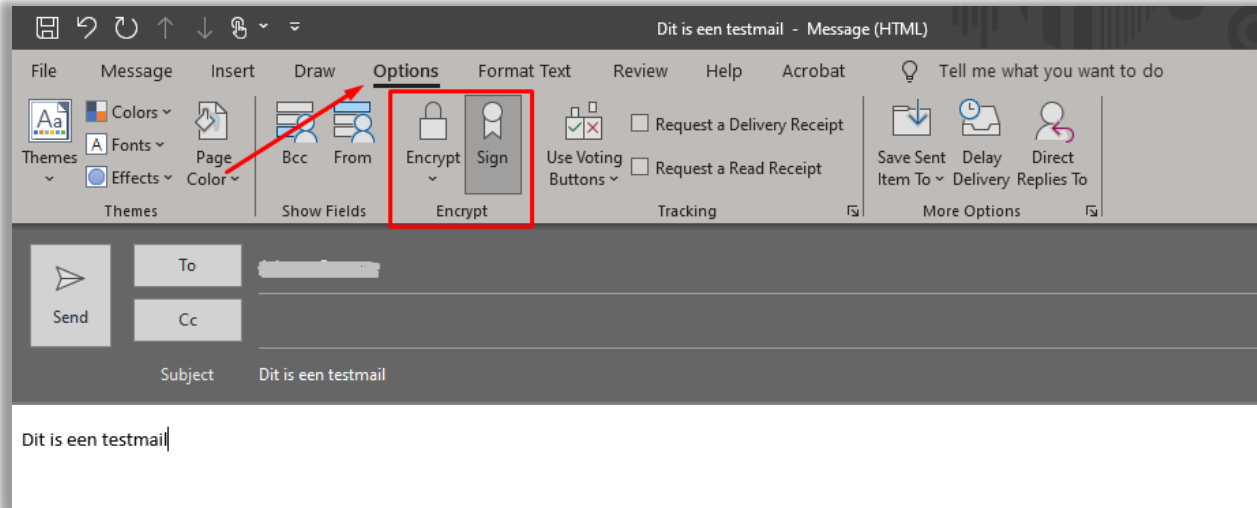


This will publish your certificate to the “Global Address List”. This is a centralized directory of email addresses and contact information within an organization's email system. This way, users can send encrypted emails to you without having to add you to their Outlook contacts first (described later in the guide). In some cases, it may take up to 48 hours for the S/MIME certificate to be published to the GAL via the “Publish to GAL” functionality.

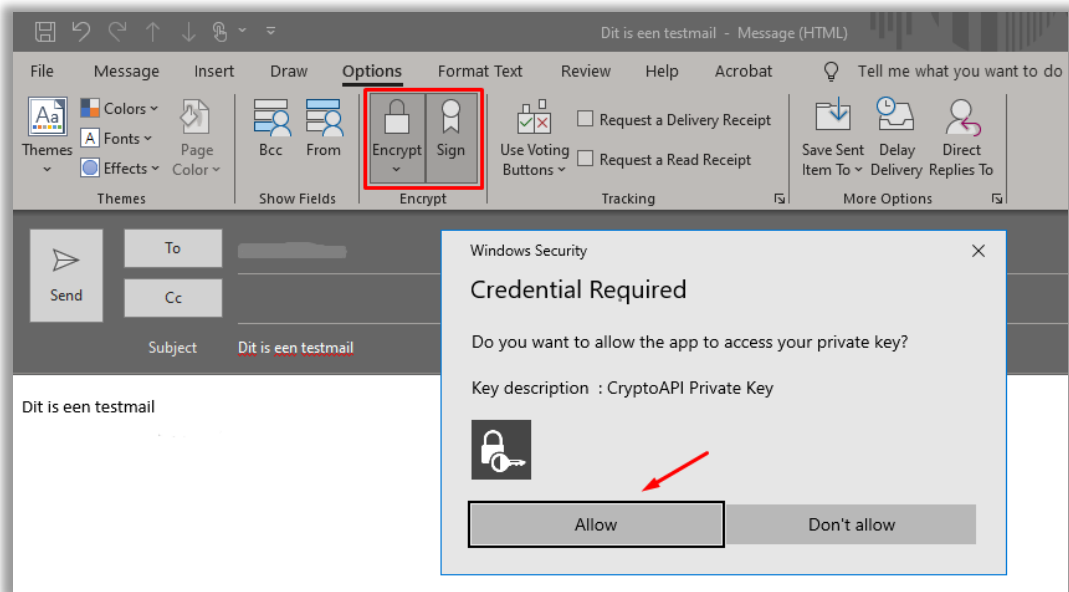
19. **Success!** You have now finished configuring your S/MIME settings. Now close all screens by clicking “OK”.

### 1.3 Sending mail (encrypted/signed)

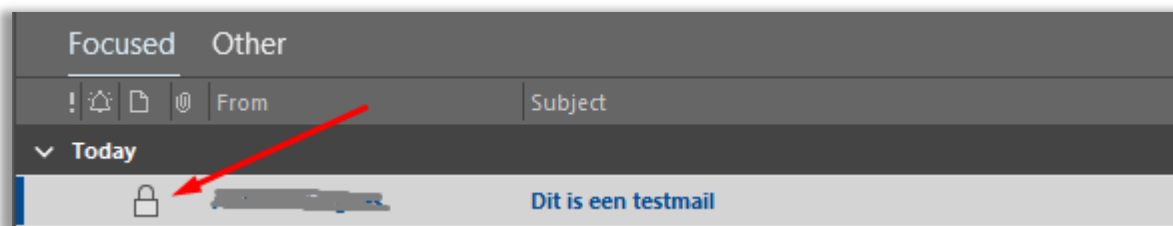
Now go back to the Outlook home screen and click on **“New Email”** to compose a new email. Click on **“Options”** at the top of your toolbar. The options **“Encrypt”** and **“Sign”** are visible here. **“Sign”** is now enabled by default due to the settings from the previous step. This can be seen because this button is highlighted..



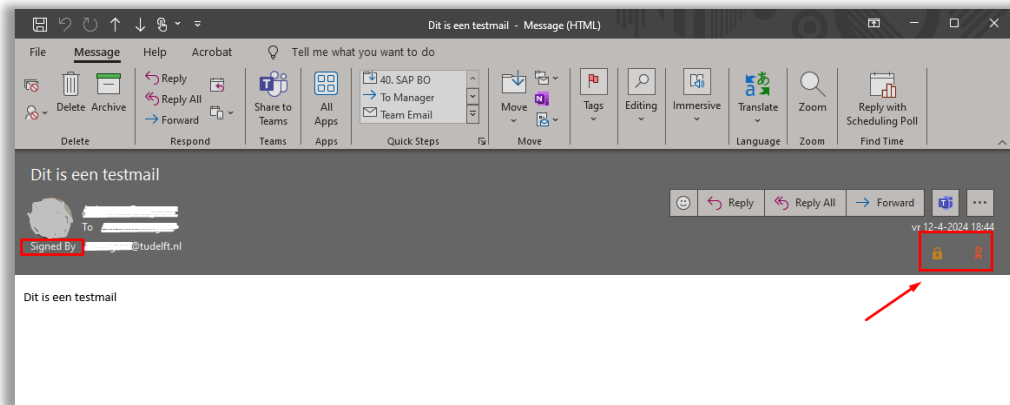
If you want to encrypt a message, click on **“Encrypt”**. Then click on **“Send”**. A pop-up window will follow for confirmation. Click on **“Allow”**.



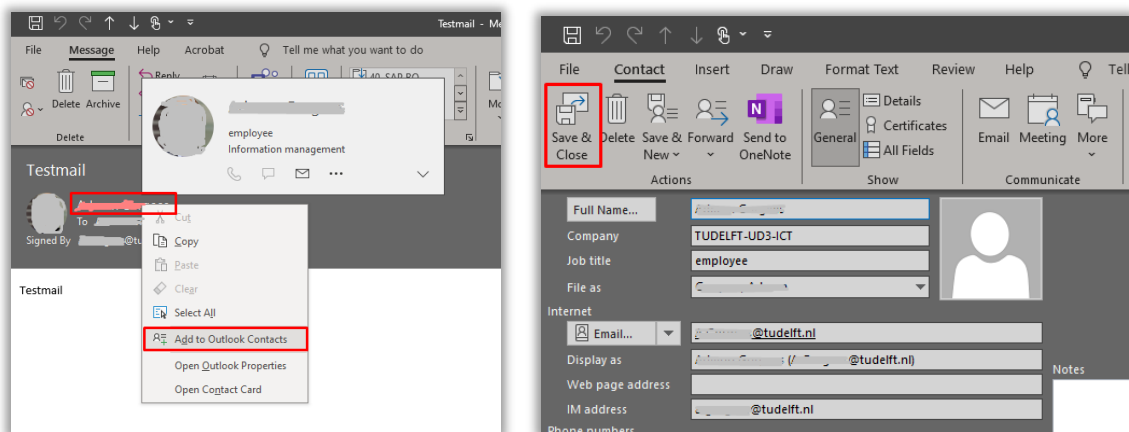
The message is now sent encrypted. The recipient will see the following when receiving the email. This icon shows that the message has been sent encrypted.



When opening the email you will see the following: **Signed by:** mailadres@tudelft.nl followed by two icons (encrypted + signed icon):



**Note:** to send an encrypted message it is necessary that the public certificate of the receiving party is known. You do this by opening a "signed" email that you have received and then adding this person to your Outlook-contacts. Open a "signed" mail -> right-click on the person's name -> **Add to Outlook Contacts** -> **Save & Close**:



Your contact has now been successfully saved to your Outlook contacts. By opening the contact details you can view the certificate properties (if available): click on "**Certificates**" -> Properties

