



How to trust and enable S/MIME certificates in Office 365 Exchange Online using Chrome/Edge &

How to configure S/MIME for Outlook for Windows, Outlook Mobile for iOS and Android, Outlook for Mac, Mac Mail, and OWA & Exchange Online

Creation date	05 November 2019
Last updated	24 March 2024
Latest changed topics	Browser based S/MIME support
Author	M.R. van der Sman
Data classification	Public

Disclaimer: No rights can be derived from this document. KeyTalk 1 BV or its author cannot be held liable for possible inaccuracies or omissions in this document, or for any loss or damage which may arise from using any information contained herein.

Contents

1. Introduction	3
2. Trusting your and other people's S/MIME certificates on Office 365	3
2.1 Get an SST (Serialized-certificate STore) file	3
2.2 Connect to Office 365.....	5
2.2 Upload your SST file to Office 365.....	5
3. Windows Outlook on the Web and S/MIME email encryption & digital signing.....	6
3.1 Install the S/MIME Control extension	6
3.2 Exchange on-prem only: Configure the S/MIME extension.....	9
3.3 Download and install the S/MIME control.....	10
3.4 Additional settings in Outlook on the Web (former OWA).....	10
4. OWA / Exchange Online S/MIME email encryption and digital signing on Mac.....	11
5. Outlook for Android and S/MIME email encryption and digital signing	11
6. Samsung email for Android and S/MIME email encryption and digital signing	12
7. Outlook for iOS and S/MIME email encryption and digital signing	13
7.1 Outlook for iOS and S/MIME using Shared Mailboxes.....	15
8. Mail for iOS and S/MIME email encryption and digital signing.....	16
9. Mac Mail and S/MIME email encryption and digital signing	17
10. Outlook for Mac and S/MIME email encryption and digital signing	17
11. Mac and S/MIME on a CAC	18
12. Outlook for Windows and S/MIME email encryption & digital signing.....	18
12.1 Enable S/MIME digital signing and email encryption.....	18
12.2 Enable LDAP based key server / LDAP S/MIME Address Book	19
13. Uncommon errors on S/MIME encryption and Digital Signing	23
13.1 MacMail: The digital signature isn't valid or trusted.	23
13.2 Email arrives as blank with "smime.p7m" attachment.....	23
13.3 Email arrives as blank	23
13.4 Untrusted digital signature	23

1. Introduction

With the Internet containing a lot of information on S/MIME, but various subjects being fragmented across many different websites, this document is an attempt to get most S/MIME related configuration and usability information into 1 easy to understand document.

KeyTalk specializes in PKI certificate management, and (semi-)automated X.509 certificate distribution for user device endpoints, servers, network equipment and Internet-of-Things (IoT).

KeyTalk's Certificate & Key Management and Distribution Solution not only distributes and installs a certificate and private key, but also auto configures target applications to make use of the installed certificate and key when possible.

This document describes how to enable S/MIME certificate based email encryption and digital signing for Office 365 / Exchange Online, with and without the use of KeyTalk.

Additionally, this document describes how to manually configure S/MIME email encryption and digital signing for Outlook for Android, Outlook for iOS, Outlook for Windows, Outlook for Mac, MacMail, OWA, Exchange Online and several other popular mail clients.

2. Trusting your and other people's S/MIME certificates on Office 365

Unlike an on-premises Exchange environment, the O365 Exchange Online does not trust any publicly trusted or privately trusted Root CAs and intermediate CAs, under which S/MIME certificates have been issued.

A common error you may encounter when NOT updating your Exchange and Office 365 Exchange CA trust chains include:



With Exchange Online, and Outlook for Android & iOS and Outlook for Mac relying on Office 365 CA trusts, the first step is to enable the appropriate CA trusts on your O365 environment. These steps are not required when you just use desktop/laptop Windows Outlook, or Outlook for Mac.

2.1 Get an SST (Serialized-certificate SToRe) file

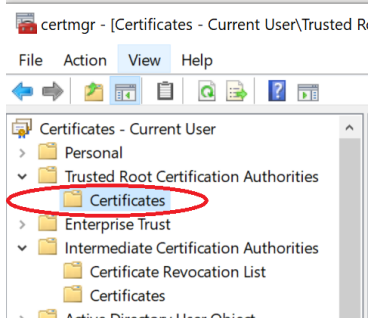
It is advised to carefully select which CAs you wish to trust in your Office 365 environment. Office 365 will actually validate the SST content and refuse to upload invalid CA Roots and Intermediates.

Your certificate with thumbprint 4765557AF418C68A641199146A7E556AA8242996 has expired. For S/MIME functionality to work correctly, please import an SST file with all valid certificates.

Pre generated sample SST file (DigiCert, GlobalSign and Sectigo S/MIME issuing CA for Class 1 and 2 S/MIME trust):
<https://downloads.keytalk.com/downloads/samples/virtualcertcollection.sst>

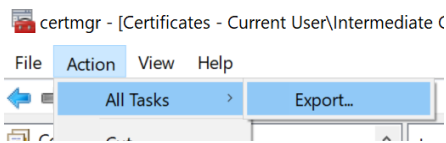
Follow the following steps to create your own SST file using a **Windows environment**:

- Open Powershell or Command Prompt and start 'certmgr' or MMC with the certificate snapin.
- Move or copy Intermediate CAs from the Intermediate Certification Authorities to the Trusted Root Certification Authorities, as the SST export can only deal with 1 folder.
- Select the 'Trusted Root Certification Authorities', and select 'Certificates'

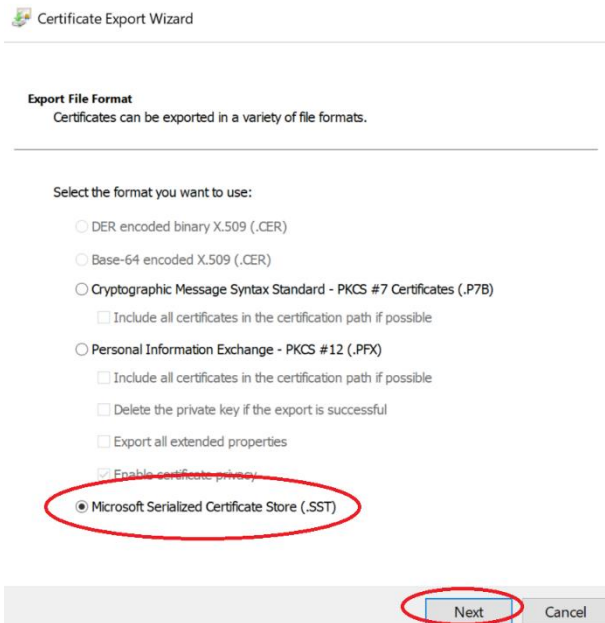


- d) Select (hold CTRL) all the valid (ie non-expired) Root CAs and Intermediate CAs (you moved under b)) you wish to trust in Office 365, select minimally 2, and **only select non-expired**

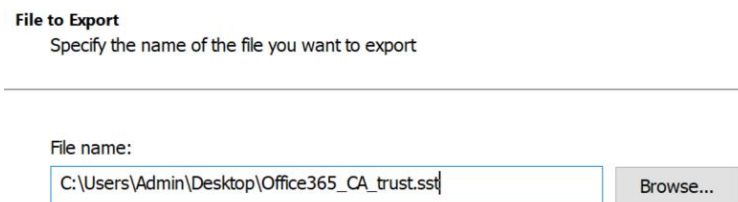
- e) Select 'Action' -> 'Export'



- f) Select 'SST' -> 'Next'



- g) Give the SST file a name and optionally select a location



- h) Finish the export



2.2 Connect to Office 365

Now that you have the trusted Root SST file, you need to upload this SST into Office 365.

- a) Should you not have PowerShell 7 installed, kindly install it.
If using a Mac, ensure OpenSSL is installed as well (both 1.1.1 and 3.0 are supported with PowerShell 7)

Open PowerShell 7 and install "Azure Active Directory V3 PowerShell module "

Install the Exchange Online Powershell V3 module, execute the following command:

```
Install-Module -Name ExchangeOnlineManagement -force
```

To ensure the latest updates are installed, execute the following command:

```
Update-Module -Name ExchangeOnlineManagement
```

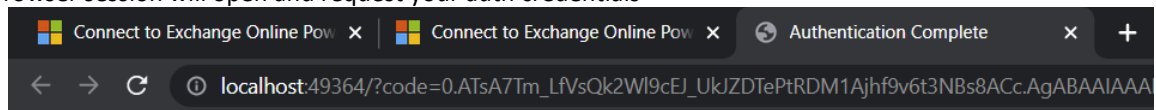
Load the Exchange Online module, execute the following command:

```
Import-Module ExchangeOnlineManagement
```

- b) Connect to Office365 with your appropriate admin account using the following command:

```
Connect-ExchangeOnline -UserPrincipalName navin@contoso.com
```

A browser session will open and request your auth credentials



Authentication complete. You can return to the application. Feel free to close this browser tab.

2.2 Upload your SST file to Office 365

Now that a validated connection to Office 365 exists, you can upload your SST file as generated under [chapter 2.1](#)

Follow the following steps to upload your SST:

- a) Run the following command, replacing the sample SST filename and location with your own:

```
Set-SmimeConfig -SMIMECertificateIssuingCA ([System.IO.File]::ReadAllBytes('C:\My Documents\myvirtualcertcollection.sst'))
```

```
PS C:\> Set-SmimeConfig -SMIMECertificateIssuingCA ([System.IO.File]::ReadAllBytes('C:\virtualcertcollection.sst'))  
WARNING: The command completed successfully but no settings of 'Smime Configuration' have been modified.  
PS C:\>
```

When invalid/expired CA trust certificates are part of your SST you will see an error and will need to regenerate your SST file.

When the SST you are uploading is the same as a previously uploaded SST, you will see a confirmation that no modifications have been made.

- b) After successfully uploading your SST file, wait roughly 30 minutes for the sync to kick in.

When using Outlook Mobile, or Exchange Online, your used S/MIME certificate issuer should now be trusted.

3. Windows Outlook on the Web and S/MIME email encryption & digital signing

With Internet Explorer being phased out, Edge and Chrome on Windows nowadays do support S/MIME for Windows Outlook on the Web (former OWA) as well

First follow [Chapter 2](#). Before commencing the below steps.

In reference to Microsoft's formal article for supporting S/MIME using Edge or Chrome:

<https://learn.microsoft.com/en-us/exchange/security-and-compliance/smime-exo/configure-smime-exo#step-4-configure-policies-to-install-the-smime-extensions-in-web-browsers>

Contrary to what Microsoft states, it is not required to be local domain joined, nor Entra ID joined.

The same results can be achieved by applying some Windows Registry changes when not working with a domain joined Windows device.

3.1 Install the S/MIME Control extension

Using S/MIME in the browser requires the Microsoft S/MIME Control extension to be installed by means of a Registry value or Group Policy.

Both methods have the same result, as the Group Policy sets the exact same Registry value.

3.1.1 Registry change method

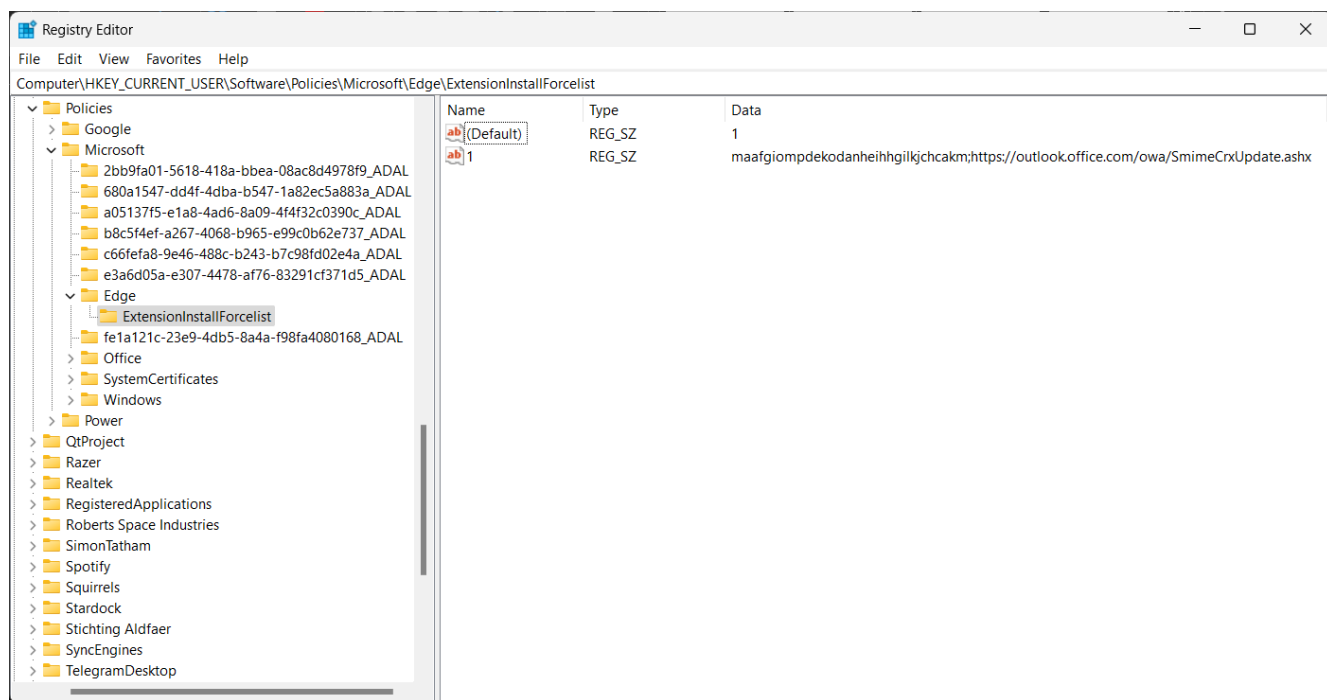
To have the browser install the Microsoft S/MIME extension, you'll have to set the [ExtensionInstallForceList](#) value in the Registry.

Key Microsoft Edge:

`HKEY_CURRENT_USER\Software\Policies\Microsoft\Edge\ExtensionInstallForceList`

Value Name: 1

Value type: REG_SZ



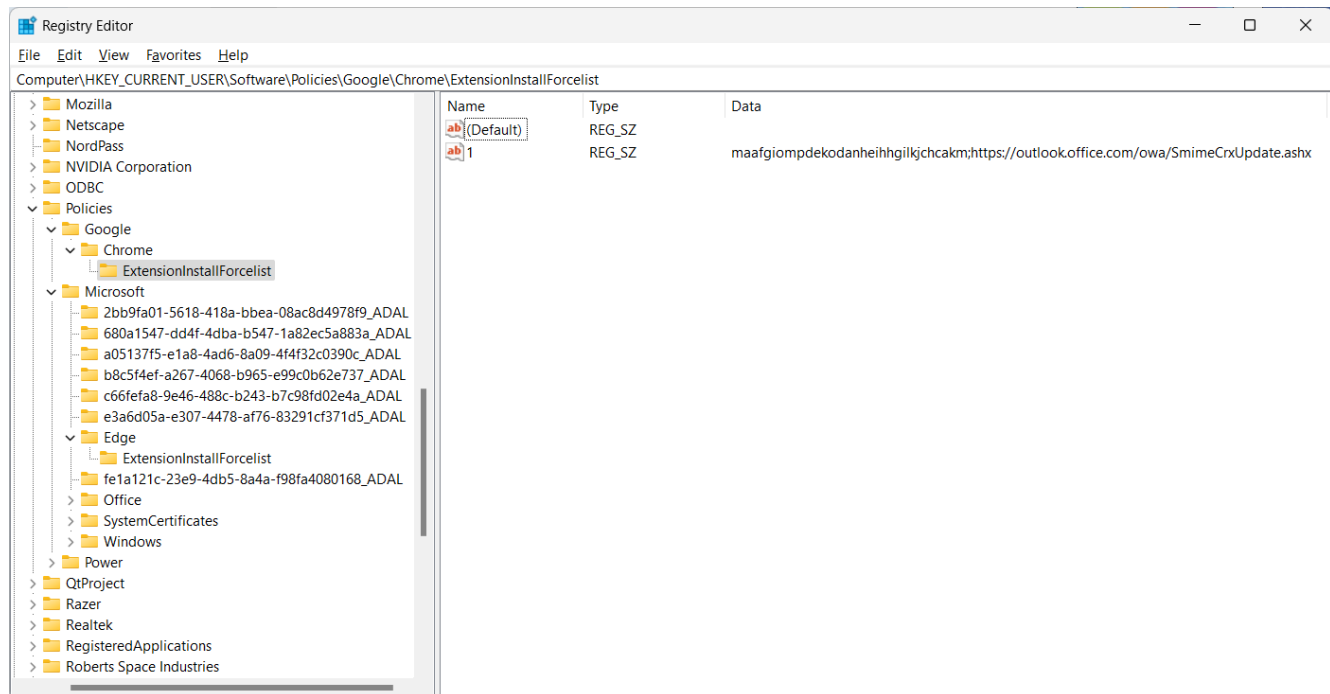
Registry entry for Edge to use S/MIME with Office 365 Outlook on the Web

Key Google Chrome:

`HKEY_CURRENT_USER\Software\Policies\Google\Chrome\ExtensionInstallForcelist`

Value Name: 1

Value type: REG_SZ



Registry entry for Chrome to use S/MIME with Office 365 Outlook on the Web

Value Office 365:

`maafgiompdekodanheihhgilkjchcakm;https://outlook.office.com/owa/SmimeCrxUpdate.ashx`

Value Exchange On-Premises:

`maafgiompdekodanheihhgilkjchcakm;https://<your OWA url>/owa/SmimeCrxUpdate.ashx`

3.1.2 Group Policy method

To set the registry value above, you can also use the Group Policy templates.

Download: [Google Chrome Group Policy Templates](#)

Download: [Microsoft Edge Group Policy Templates](#)

For instructions on how to install and use Group Policy templates you can use the guide;

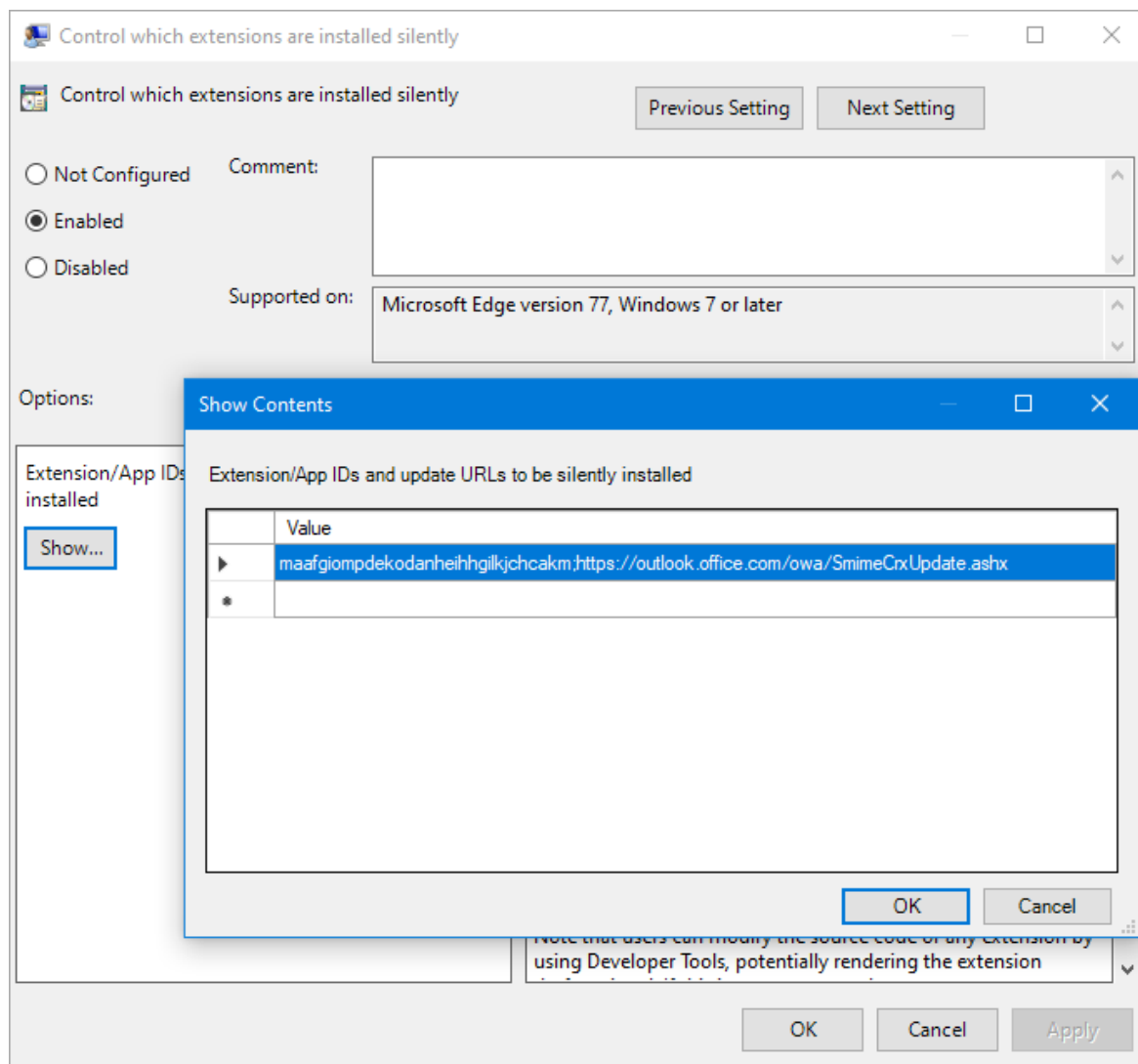
[Setting Outlook Group Policies](#).

You can find the policy setting in the following location;

- ✓ Google Chrome:
User Configuration-> Administrative Templates-> Google-> Google Chrome-> Extensions-> Configure the list of force-installed apps and extensions
- ✓ Microsoft Edge
User Configuration-> Administrative Templates-> Microsoft Edge-> Extensions-> Control which extensions are installed silently

Set the policy setting to Enabled and click on the “Show...” button to add the following value;

- ✓ Office 365
`maafgiompdekodanheihhgilkjhcakm;https://outlook.office.com/owa/SmimeCrxUpdate.ashx`
- ✓ Exchange On-Premises:
`maafgiompdekodanheihhgilkjhcakm;https://<yourOWAurl>/owa/SmimeCrxUpdate.ashx`




Setting the ExtensionInstallForcelist value in the Group Policy Editor to install the S/MIME extension.

3.2 Exchange on-prem only: Configure the S/MIME extension

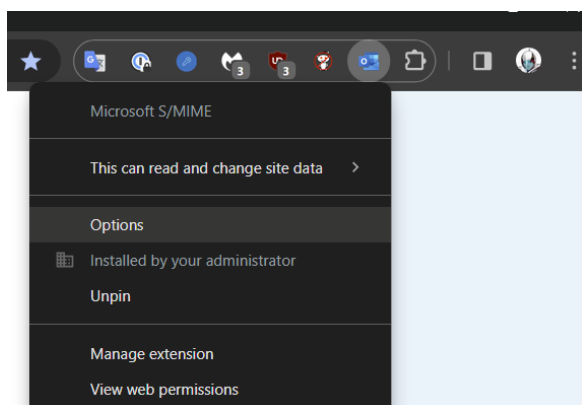
Skip this step when using Office 365 or Outlook.com

When you are using a mailbox hosted in an On-Premises Exchange environment, then you must add the Outlook on the Web domain to the “Allowed domains” list.

 The S/MIME message wasn't decrypted successfully. S/MIME isn't configured to work with the current domain. You can add it in S/MIME Extension options page in the settings for your browser. [click here](#).

Message shown when NOT having your OWA url added to the trusted domains list

To add your domain to the Allowed domains list, click on the “click here” link in the infobar message or click on the Outlook icon right from the Address Bar and choose: (Extension) Options.



Alternatively open in:

Google Chrome: <chrome-extension://maafgiompdekodanheihhgilkjchcakm/Options.html>

Microsoft Edge: <extension://maafgiompdekodanheihhgilkjchcakm/Options.html>

Microsoft S/MIME options

What website do you use to sign in to Outlook on the web?

S/MIME can encrypt and decrypt messages using Outlook on the web. To enable S/MIME, choose which website domains you use to sign in to Outlook on the web.

- ☒ Microsoft websites. For example, Office.com or Outlook.com.
 - ☒ Other work or school website domains. For example, if you sign in to Outlook on the web with <https://mail.contoso.com/mail>, then type "mail.contoso.com" in the box below.
- Only add domains that you trust.

owa.keytalk.com

Save

Add your On-Premises mail domain to the S/MIME Control options.

3.3 Download and install the S/MIME control

After installing the extension, you still won't be able to open S/MIME encrypted messages. The infobar instructs you to install the S/MIME control and contains a link to download this control.


 The content can't be displayed because the S/MIME control isn't installed. To install S/MIME, [click here](#).

For Office 365, the *click here* link points to [this location](#)

For Exchange On-Premises, it points to: <https://<your OWA url>/owa/smime/SmimeOutlookWebChrome.msi>

The S/MIME control installer is actually intended for direct deployment, therefore the installation of this package is silent and doesn't give any feedback whether the installation was successful or not. You can still install it manually and it doesn't require administrator permissions to install it for most domain configurations. Once it installed successfully, it will also show in your Apps list in Windows Settings.

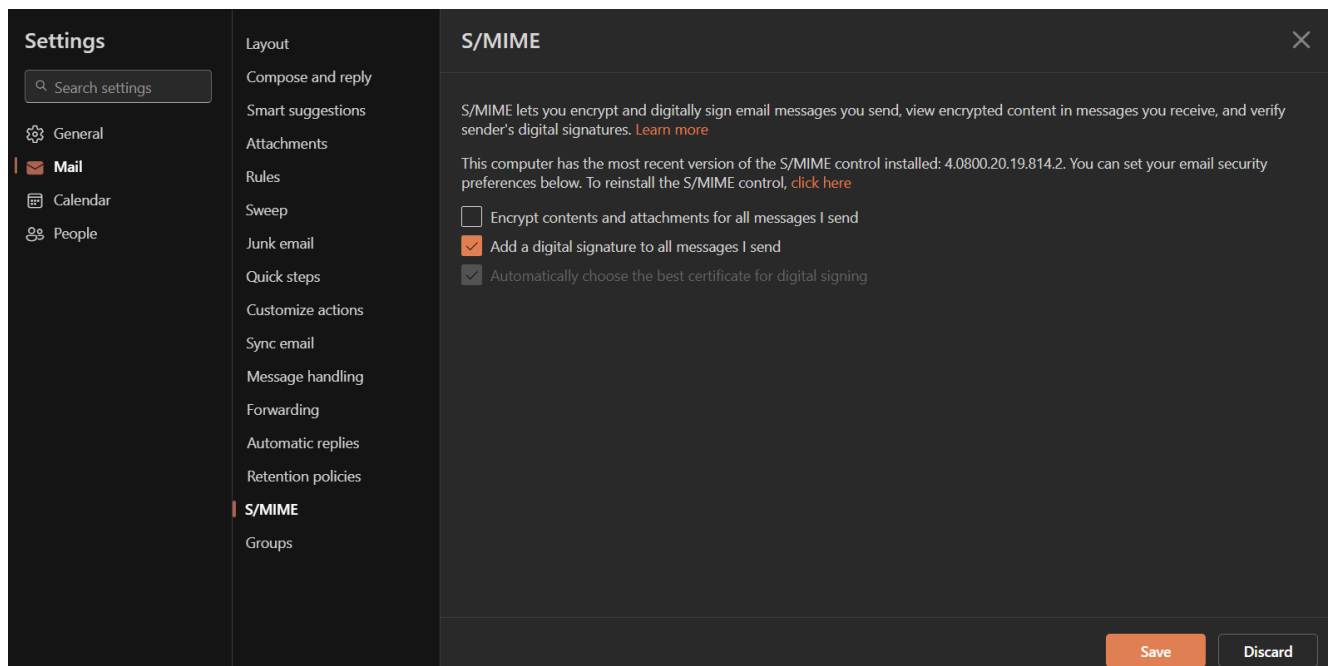
Restart the browser and you should be able to read and send S/MIME encrypted emails as well as adding digital signatures to emails. The browser infobar will show the following information when the message can be decrypted and the digital signature can be verified.

 The digital signature for <b.barnau@keytalk.com> on this message is valid and trusted. For more information, [click here](#).

3.4 Additional settings in Outlook on the Web (former OWA)

With S/MIME now properly installed and configured in your browser, you can now also configure additional S/MIME setting in Outlook on the Web.

- ✓ Office 365
Gear icon in the top right-> View all Outlook settings-> Mail-> [S/MIME](#)
- ✓ Exchange 2019 / 2016 / 2013
Gear icon in the top right-> Options-> Mail-> S/MIME



4. OWA / Exchange Online S/MIME email encryption and digital signing on Mac

Currently MacOS based browsers are not supported by Microsoft for Outlook on the Web with S/MIME

5. Outlook for Android and S/MIME email encryption and digital signing

Outlook for Android requires the S/MIME certificate and private key to be available in the Android certificate store.

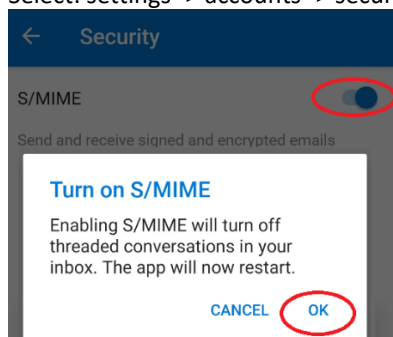
Follow the following steps to enable S/MIME email encryption and digital signing on Outlook for Android:

- a) Ensure that your Office 365 environment trusts the issuing CA Root and intermediate CAs (see [chapter 2](#))
- b) Ensure your inter company S/MIME certificates are known in your Active Directory (AD) and/or Azure Active Directory (AAD) for each user in its "UserCertificate" attribute and/or "UserSmimeCertificate" attribute. This ensures that when one of your AD users wants to send an encrypted email to another AD user, the public details are fetched automatically by Outlook for Android.
This is not a requirement when you just want to use digital signing.

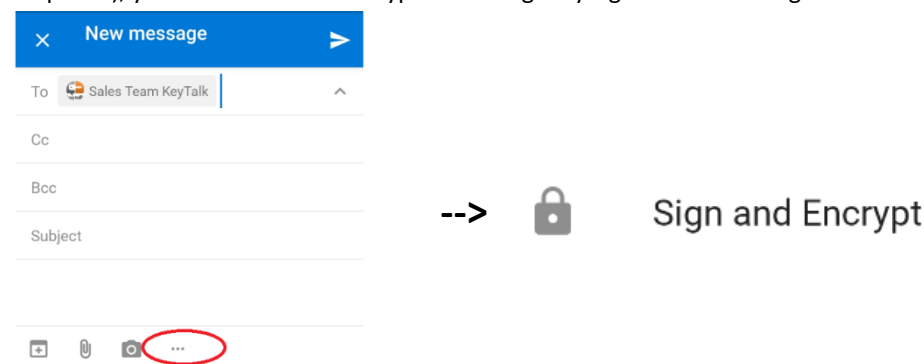
The KeyTalk Certificate and Key Management solution can automatically write newly issued S/MIME certificates into the "UserCertificate" attribute of your Active Directory or Azure Active Directory for your users (and remove expired/revoked S/MIME certificates).

Using AzureADConnect will synchronize your user AD attributes to Azure AD ensuring your S/MIME certificates are also known in Azure AD.

- c) Either get the S/MIME certificate and key installed by means of the KeyTalk app for Android (<https://play.google.com/store/apps/details?id=com.keytalk.nextgen5>), or use a manual deployment (we recommend emailing the PFX and installing it from within Outlook Mobile), or a Mobile Device Management (MDM) solution such as Intune, MobileIron, VMware AirWatch or Blackberry Work
- d) Configure the Outlook for Android app to make use of S/MIME.
Select: settings -> accounts -> security -> Switch S/MIME to on



- e) Provided the certificate got installed, and Office 365 got configured to trust your S/MIME issuing CA and root (see chapter 2), you can now write encrypted and digitally signed emails using:

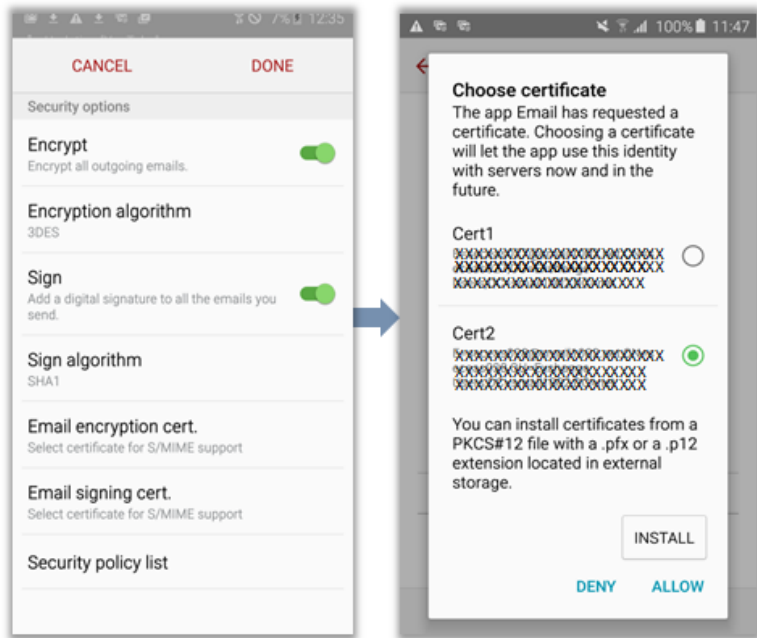


Sending encrypted emails using Outlook Mobile, required the recipient's S/MIME cert to be available in your AD or Azure AD, or be stored locally in your Outlook Mobile.

6. Samsung email for Android and S/MIME email encryption and digital signing

Samsung email for Android natively supports S/MIME based email encryption and digital signing. To configure it follow the following steps:

- a) Open the Samsung email client.
- b) Tap **More** (the 3 lines) > **Settings**.
- c) Select the required email account.
- d) Under **Security options**, you can enable the Encryption and Signing features.
- e) To enable encryption for all outgoing emails:
 - Select **Encrypt**.
 - Select the required client certificate.
 - Tap **Allow** if you want to use a certificate which is already installed or tap **INSTALL** to install new certificates

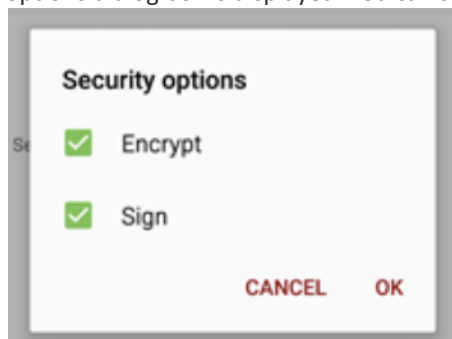


NOTE: If a pop-up screen to set the secure screen lock is displayed, you must first set the device password to continue.

NOTE: If the certificate(s) are not installed, you will get an error message stating, certificate not installed.

- f) To enable signing for all outgoing emails:
 - Select the **Sign** option.
 - Select the required client certificate and tap **Allow** if you want to use a certificate which is already installed or tap **INSTALL** to install new certificates.

If you want to apply S/MIME only for a specific email, go to: **Message Composer** > **MORE** > **Security Options**. The Security options dialog box is displayed. You can select the Encrypt & Sign options based on the requirement.



7. Outlook for iOS and S/MIME email encryption and digital signing

Outlook for iOS requires the S/MIME certificate and private key to be available in the iOS Microsoft publisher keychain, this is a different keychain than the default iOS system keychain.

At the time of writing this guide, the only way to get your S/MIME certificate and key in an automated manner into the iOS Microsoft publisher keychain is by using Intune MDM.

When you don't use Intune the only manual way to make S/MIME work is by opening the certificate as an email sent attachment in Outlook for iOS and manually installing it. Other MDM solutions such as JAMF, MobileIron or AirWatch will not work with Outlook for iOS or iPadOS.

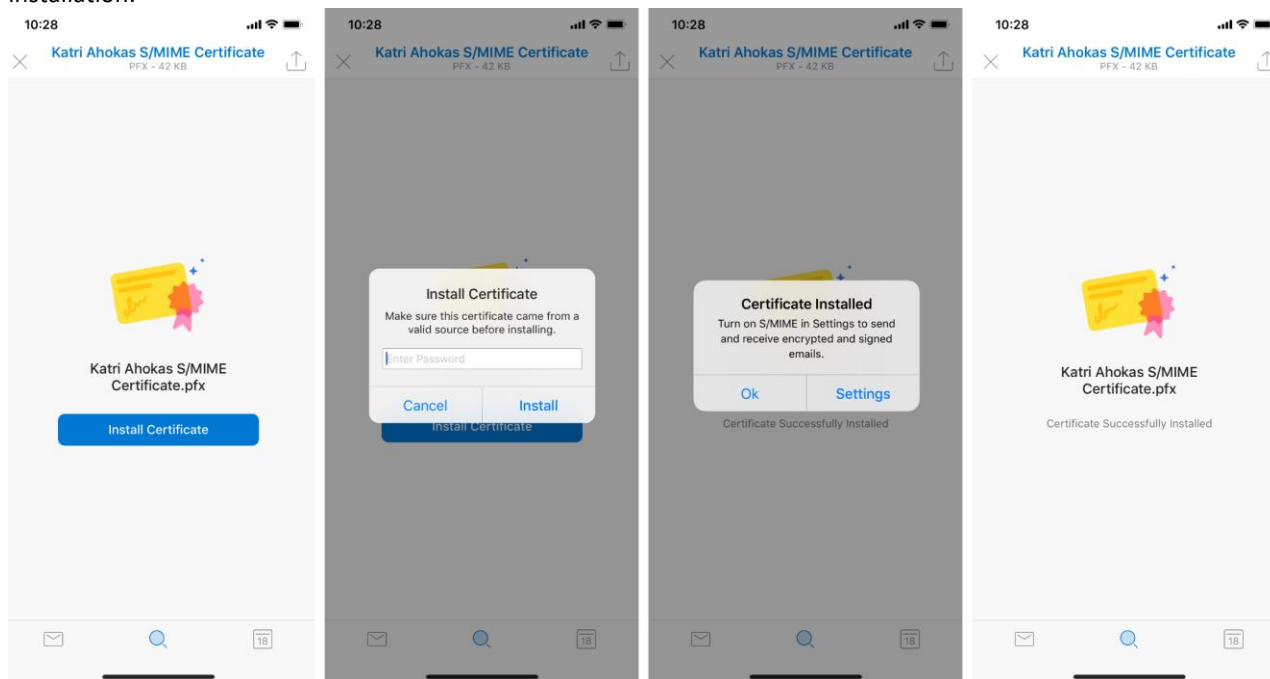
Follow the following steps to enable S/MIME email encryption and digital signing on Outlook for iOS:

- a) Ensure that your Office 365 environment trusts the issuing CA's and Root (see [chapter 2](#))
- b) Ensure your inter company S/MIME certificates are known in your Active Directory (AD) and/or Azure Active Directory (AAD) for each user in its "UserCertificate" attribute and/or "UserSmimeCertificate" attribute. This ensures that when one of your AD users wants to send an encrypted email to another AD user, the public details are fetched automatically by Outlook for Android. This is not a requirement when you just want to use digital signing.

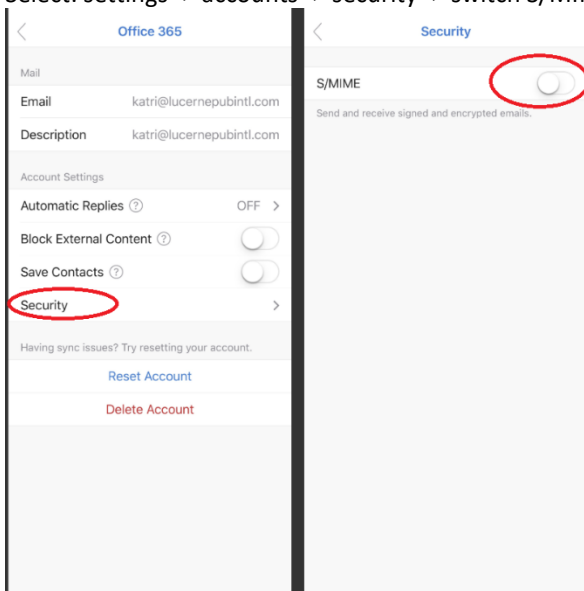
The KeyTalk Certificate and Key Management solution can automatically write newly issued S/MIME certificates into the "UserCertificate" attribute of your Active Directory or Azure Active Directory for your users (and remove expired/revoked S/MIME certificates).

Using AzureADConnect will synchronize your user AD attributes to Azure AD ensuring your S/MIME certificates are also known in Azure AD.

- c) Get the S/MIME certificate and key installed by means of Intune. When you don't have Intune the only option to install it in Outlook for iOS is by sending it as an attachment to an email and opening it in Outlook for iOS to trigger the manual installation.

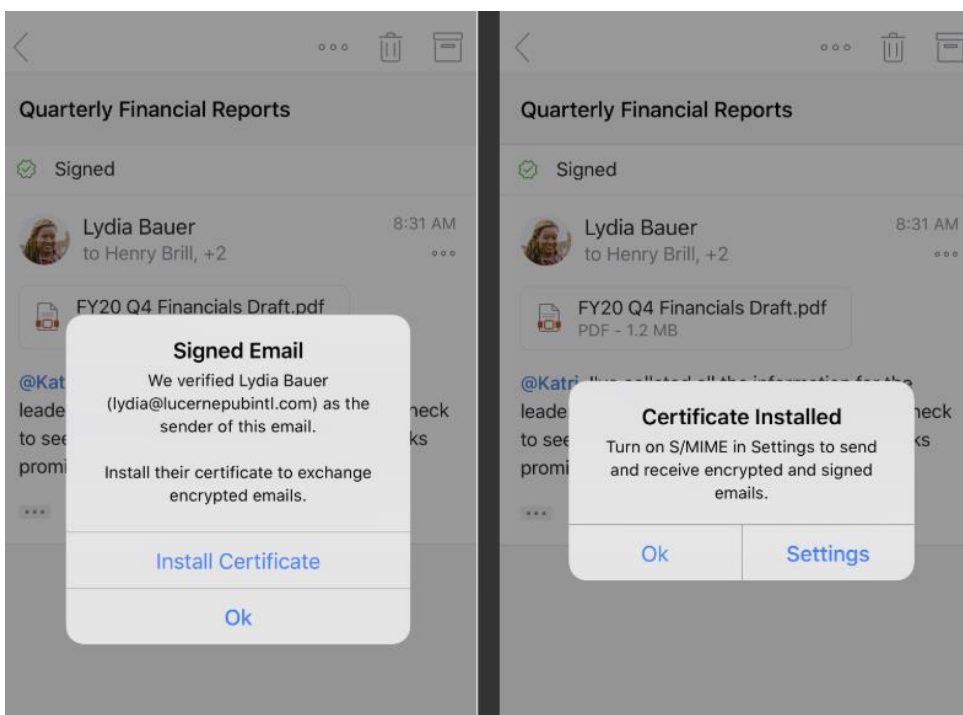


- d) Configure the Outlook for iOS app to make use of S/MIME.
Select: settings -> accounts -> security -> switch S/MIME to on

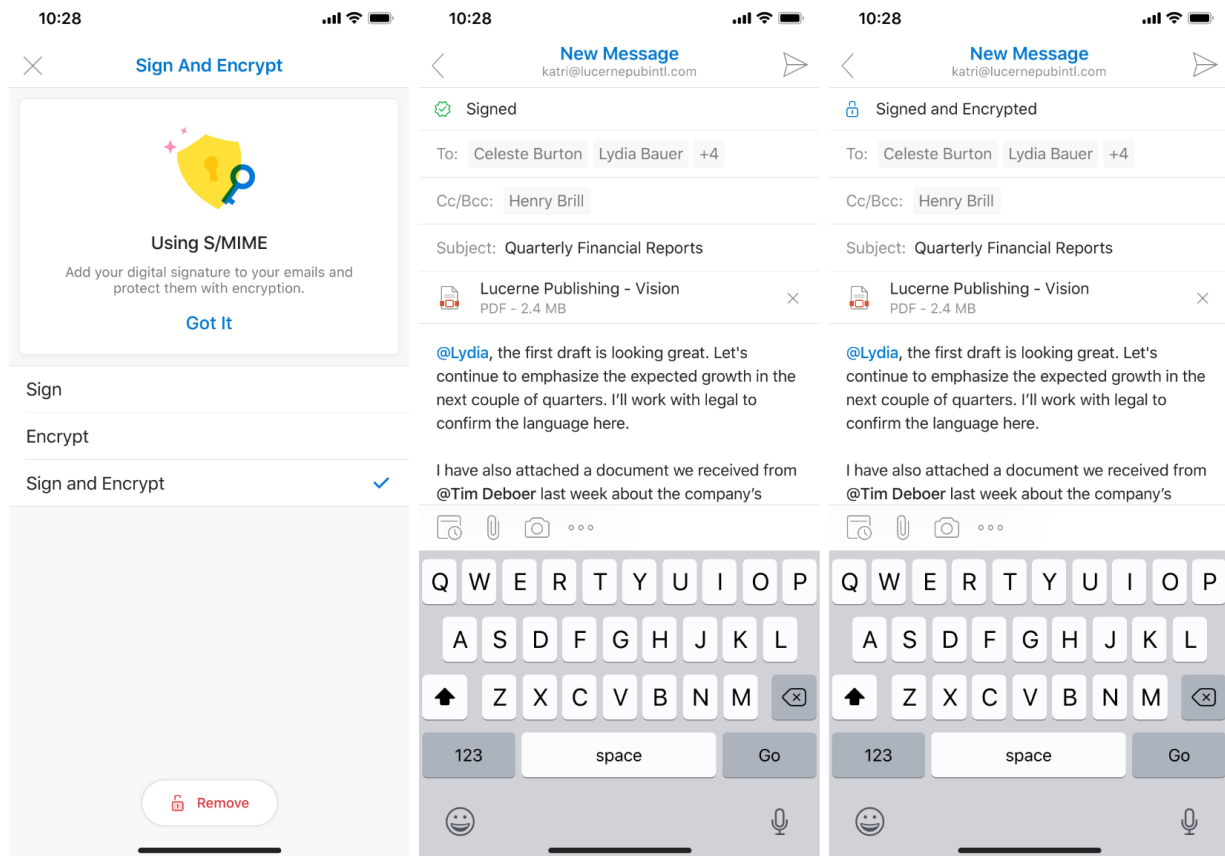


- e) Provided the certificate got installed properly, and Office 365 got configured to trust your S/MIME issuing CAs and Root (See chapter 2), you can now write encrypted and digitally signed emails to users who's certificate got listed in your (Azure)AD, and to those who's certificate was explicitly manually saved to the iOS Microsoft publisher keychain.

To save a person's certificate to the iOS Microsoft publisher keychain, users can install a sender's public certificate key by tapping the S/MIME status bar. The certificate will be installed on the user's device, specifically in the Microsoft publisher keychain in iOS.



- f) By tapping on the **ellipse** and tapping **Sign and Encrypt**, the various S/MIME options are presented. Selecting an S/MIME option enables the respective action on the email when it is sent (drafts are not signed or encrypted), assuming the sender has a valid certificate.



7.1 Outlook for iOS and S/MIME using Shared Mailboxes

To make use of S/MIME for a Shared Mailbox, ensure that S/MIME is configured for your user's mailaccount that's been granted rights to the SharedMailbox. The user must be able to at least "send on behalf of"

Once this is done, install the SharedMailBox S/MIME, using either Intune or manually as an attachment opened from within the mailbox.

After the installation you can send signed and/or encrypted email messages using the SharedMailBox

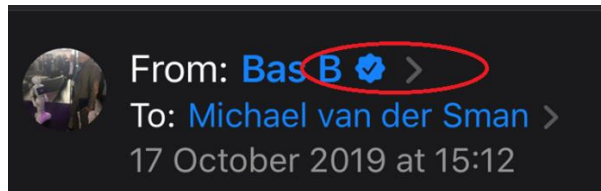
8. Mail for iOS and S/MIME email encryption and digital signing

Apple's native email client "Mail" by default supports S/MIME.

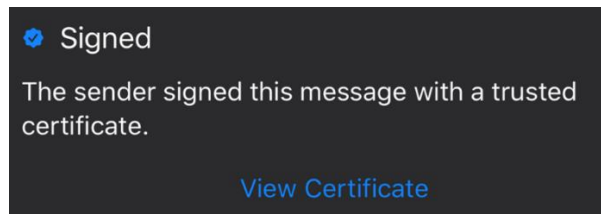
To manually configure S/MIME for iOS Mail, follow the following steps:

- a) Install the S/MIME certificate and key using KeyTalk's app when you have deployed a KeyTalk server (<https://apps.apple.com/us/app/keytalk/id1407184884?ls=1>) or use an MDM or manual process.
To verify the successful S/MIME certificate profile installation, open your iOS Settings -> General -> Profiles
- b) Optionally install the S/MIME certificate issuing CA and intermediate CA certificates.
While S/MIME digital signing and encryption will work fine without it, it prevents unwanted warnings when receiving encrypted or digitally signed emails using the same CA issuing source for S/MIME.
- c) Open your iOS Settings -> Passwords & Accounts -> Your mail account -> Account -> Advanced Settings -> Sign / Encrypt by default -> select your S/MIME certificate profile -> Done
- d) To digitally sign any email message, follow the settings under 5c
- e) To encrypt any email message, the recipients MUST either exist in your (Azure) Active Directory with a valid certificate in their "UserCertificate" and/or "UserSmimeCertificate" attribute, OR the recipients must exist with their public S/MIME certificate in the iOS system local keychain (usually used when someone is not from your company or organization).
The local keychain option requires you to have manually saved someone's S/MIME certificate by selecting a signed messages you received from them and selecting their digital signature and save it. (<https://support.apple.com/en-us/HT202345>)

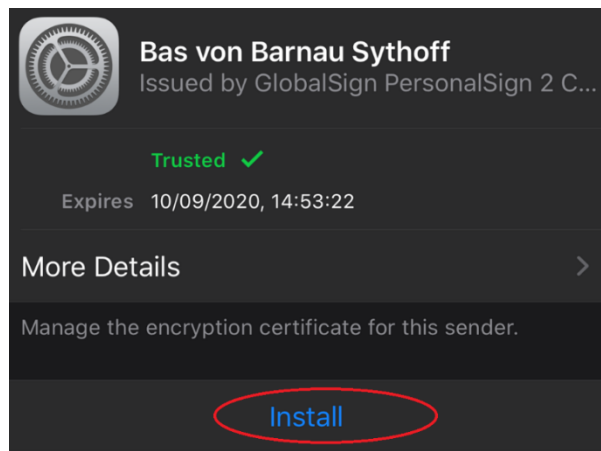
Digital signed email:



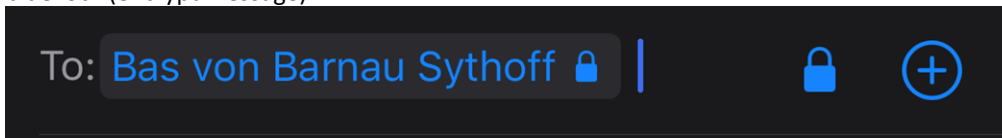
Inspect signature:



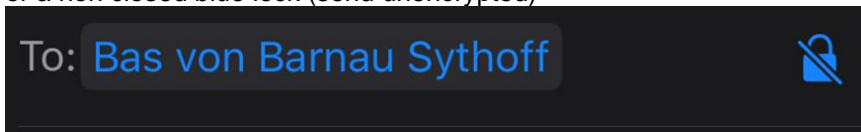
View and install:



- f) Provided the recipients public S/MIME details can be found (see 5e), when you write an email you can select a closed blue lock (encrypt message)



or a non closed blue lock (send unencrypted)



by tapping the lock symbol when tapping the recipients email address

- g) When manually installing a new S/MIME certificate and private key onto your iOS and iPadOS device, your old S/MIME is not automatically deselected.
Ensure you select your newly installed S/MIME after installation in accordance to step c)

9. Mac Mail and S/MIME email encryption and digital signing

Apple's native email client Mac Mail by default supports S/MIME email encryption and digital signing.

To enable S/MIME email encryption and digital signing follow these steps:

- Install the S/MIME certificate and key using KeyTalk's app when you have deployed a KeyTalk server (<https://apps.apple.com/us/app/keytalk-client/id1446009972>) or use an MDM or manual process.
- When your MacMail application was still running close it.
- Open your MacMail application, and it should auto-detect your installed S/MIME email encryption and digital signing certificate and key, provided your email account matches with the email address in the S/MIME certificate.

10.Outlook for Mac and S/MIME email encryption and digital signing

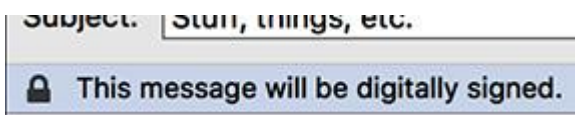
Use these instructions to enable Outlook to use client certificates to digitally sign and encrypt email.

Enable digital signing and encryption

- If you have just installed your certificate on your Mac, close Outlook and then restart it.
- From the Outlook menu, select Preferences > Accounts. Select your email account, click Advanced, and then select the Security tab.
- In the "Digital signing" section, select your certificate from the drop-down menu.
For "Signing algorithm", the default value of SHA-256 is appropriate for most situations.
- For the best usability, enable the following options:
 - Sign outgoing messages
 - Send digitally signed messages as clear text
 - Include my certificates in signed messages
- In the "Encryption" section, select your certificate from the drop-down menu.
- For "Encryption algorithm", ASE-256 is the best option. It is not necessary to check Encrypt outgoing messages; each email message can be optionally encrypted when you compose it.
- Click OK to save your changes and exit Outlook Preferences.

Sign email

By default, your email messages will be digitally signed. To indicate signing, a lock icon with the text "This message will be digitally signed" will appear in the lower left of the message header when you compose an email message:



If you do not want to sign a message, from the Options tab of the mail message, click Sign so that it is not selected.

You may not want to sign messages to mailing lists, because S/MIME digital signatures are attachments, which some lists do not accept.

Encrypt email

Address and compose your email message. From the Options tab of the mail message, click Encrypt so that it is selected.

If Outlook is unable to find certificates for everyone to whom the message is addressed, you will be prompted to search the Active Directory for user certificates. If Outlook is still unable to find certificates for all addressees, you will be prompted to send the message unencrypted.

11. Mac and S/MIME on a CAC

Should you have a smartcard/CAC with an S/MIME certificate and key, and wish to decrypt your smime.p7m email attachments, install the following program to make this easily possible: <https://github.com/AF-VCD/Mrs-SMIME>

12. Outlook for Windows and S/MIME email encryption & digital signing

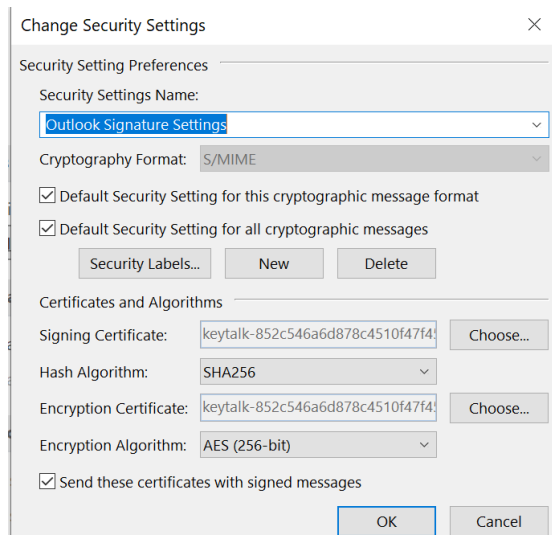
Outlook for Windows supports S/MIME based digital signing and email encryption.

12.1 Enable S/MIME digital signing and email encryption

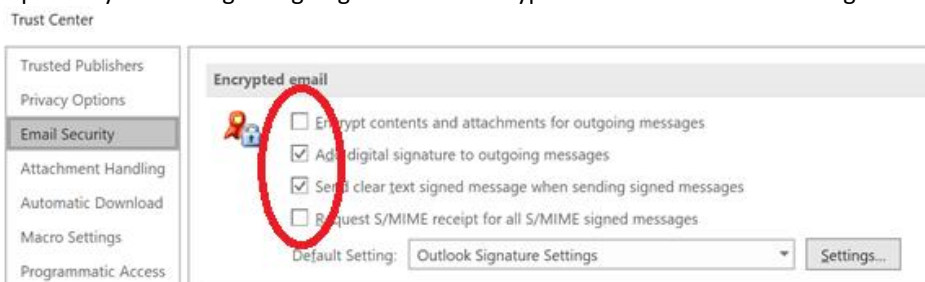
- Use the KeyTalk agent to automatically install your user's S/MIME certificate and key. The KeyTalk agent will auto configure Outlook for S/MIME and thus enable digital signing and email encryption. The next steps will not need to be followed.

When you do not use the KeyTalk solution, install the user's certificate and key manually or by means of an MDM.

- Select: File -> Options -> Trust Center -> Trust Center Settings -> Email Security
- Select Settings to configure Outlook to make use of your installed S/MIME certificate and key.



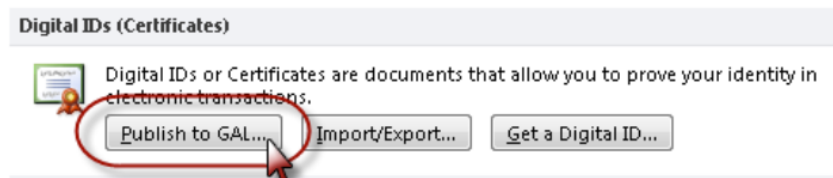
- d) Give your settings a name
- e) Select your Signing Certificate and the Hash Algorithm. It is recommended to use SHA256
- f) Select your Encryption Certificate and the Encryption Algorithm. It is recommended to use AES 256-bit
- g) Select OK
- h) Optionally set the digital signing and email encryption defaults for new messages



It is recommended to select “Add digital signature to outgoing messages.”

Some versions of Outlook may require the option “Send clear test signed message when sending signed messages.”

- i) If you are unsure whether or not your corporate environment has your S/MIME certificate in the Active Directory or Azure Active Directory, you can optionally publish your certificate to the Global Address List (GAL). This option is only available in Outlook when you have only 1 email account configured under your Outlook profile.



12.2 Enable LDAP based key server / LDAP S/MIME Address Book

In order to send an encrypted S/MIME message, the public key of the recipient must be known.

Often the recipient will be a company colleague, who exists in your corporate AD/Azure AD or LDAP, and likely already has a known S/MIME certificate which Outlook can directly read from the Global Address List (GAL).

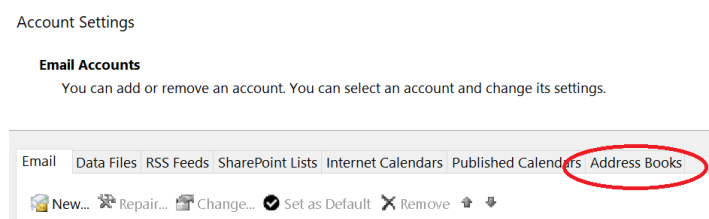
But when sending S/MIME encrypted emails to someone outside the organization you must either have received their S/MIME certificate as part of a digitally signed email, or make use of an LDAP Key Server or LDAP S/MIME address book.

Outlook for desktops/laptops supports the use of these LDAP Key Server or LDAP S/MIME address book. KeyTalk even provides one as part of its KeyTalk Certificate & Key Management and Enrolment solution.

To configure such an LDAP Key Server / LDAP S/MIME Address Book, follow the following steps:

- a) Use the KeyTalk client to install your user’s S/MIME certificate and key. The KeyTalk client will not only auto configure Outlook for S/MIME and thus enable digital signing and email encryption, but also configure Outlook for Windows to make use of your configured LDAP Key Server / LDAP S/MIME Address Book. The next manual steps will therefore not need to be followed.

In Outlook, select: File -> Account Settings -> Account Settings -> Address Books -> New



b) Select LDAP

Add Account

Directory or Address Book Type
You can choose the type of directory or address book you'd like to add.

☒ **Internet Directory Service (LDAP)**
Connect to an LDAP server to find and verify email addresses and other information.

☐ **Additional Address Books**
Connect to an address book to find and verify email addresses and other information.

c) Enter the name of the LDAP Key Server / LDAP S/MIME Address book.

Do not include ldap:// nor ldaps://

Do not include port numbers such as :389 or :636

When your Admin instructed you to make use of authentication, also enter the authentication credentials:

Add Account

Directory Service (LDAP) Settings
You can enter the required settings to access information in a directory service.

Server Information
Type the name of the directory server your Internet service provider or system administrator has given you.
Server Name:

Logon Information
☐ This server requires me to log on
User Name:
Password:
☐ Require Secure Password Authentication (SPA)

d) Select "More Settings"

e) Under "Connection" provide a descriptive name

Enter the port number. If no port number was provided and your LDAP server starts with ldap:// then use the default 389 and do not checkmark Use SSL. When your LDAP server starts with ldaps:// then use port 636 and checkmark Use SSL.

Microsoft LDAP Directory

Connection Search

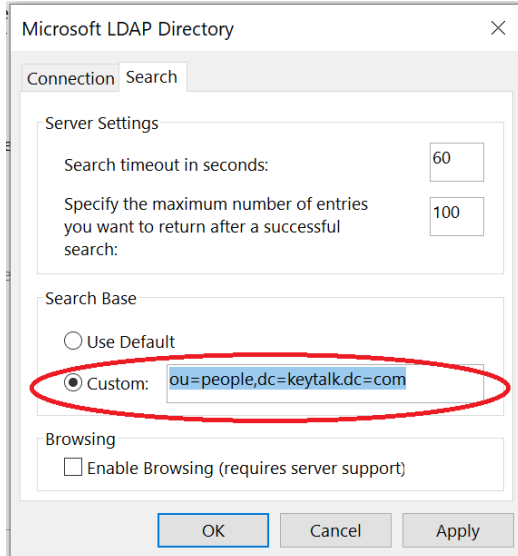
Display Name
The display name as it appears in the Address Book

Connection Details
Port:
Use Secure Sockets Layer ☒

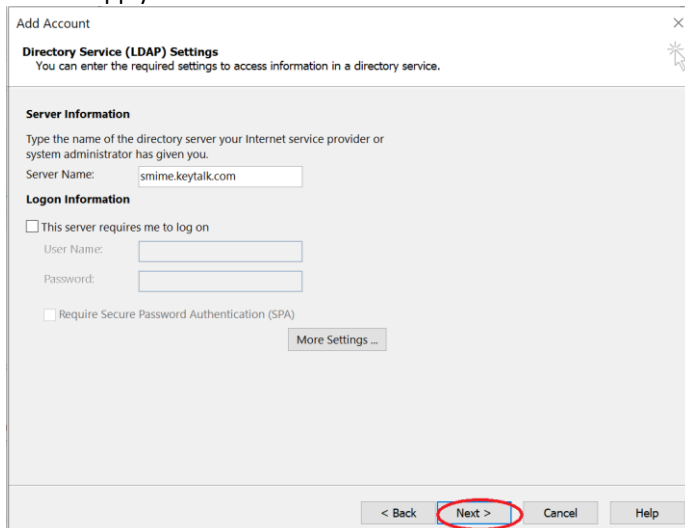
f) Select "Apply"

g) Go to the "Search" tab and set the provided search value

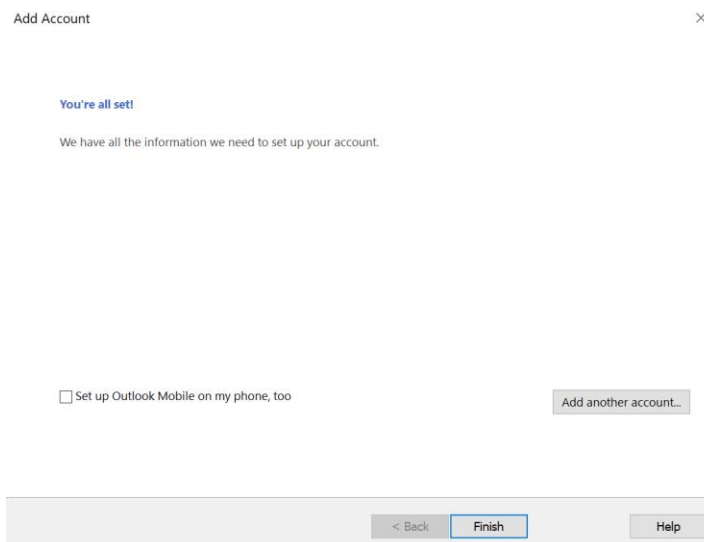
When no search value was provided, leave it at default, otherwise use custom and enter the custom search:



h) Select “Apply” -> Select “OK” -> Select “Next”



i) Select “Finish”



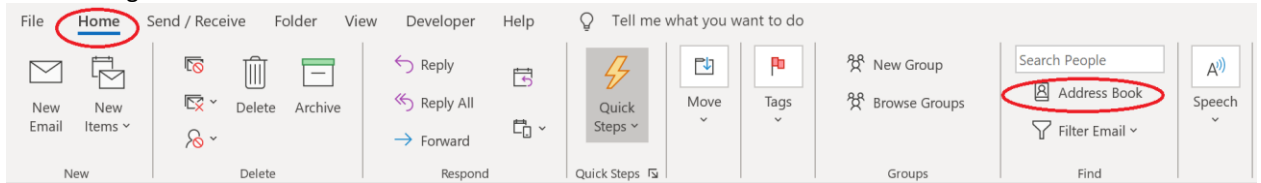
j) Close Outlook and restart Outlook to effectuate the newly added LDAP Key Server / LDAP S/MIME Address Book.

Now validate if Outlook actually added the LDAP Address Book as an active searchable resource.

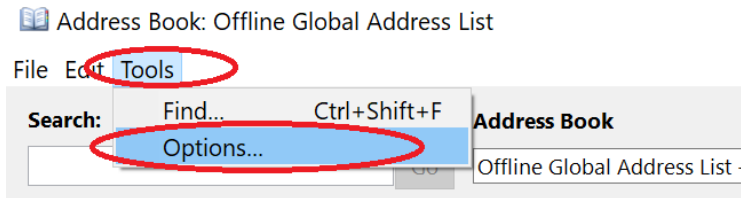
In corporate environments sometimes Group Policy Objects (GPOs) may result in the added LDAP not being made an active resource in Outlook.

To validate this, perform the following steps:

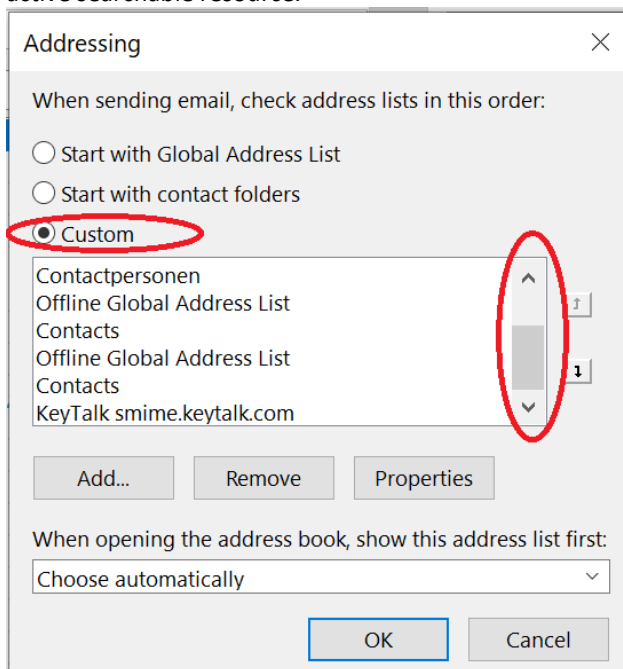
- k) In Outlook go to “Home” -> Select “Address Book”



- l) Select “Tools” -> “Options”



- m) Select “Custom” and scroll through the list to validate that your LDAP S/MIME Address Book has been added as an active searchable resource.



When your LDAP S/MIME Address Book is showing, congratulations, you should now be able to automatically search S/MIME details of recipients when they exist in your list of address books.

If your LDAP S/MIME Address Book is NOT showing, select “Add” to add it.

13. Uncommon errors on S/MIME encryption and Digital Signing

13.1 MacMail: The digital signature isn't valid or trusted.



Your users receive this message when several factors are combined:

- a) The user makes use of a Mac with MacMail, and
- b) The received email was digitally signed or encrypted by a trusted CA provider, and
- c) The mail is fetched from an Exchange server, and
- d) The user uses MacMail mail preview (doesn't open the full email)

On 15 April 2021 KeyTalk reported a bug to Apple, that when the above criteria are met, and the digital signing method used is "clear text digital signing" (contrary to opaque signing), in preview mode MacMail will give a false positive on the validity of the email, and state the mail was possibly tampered with.

The proper solution is for Apple to come with a fix.

Until that time, the sender should either use opaque digital signing (remove the checkbox in Outlook for windows, under Trust Center settings and Email Security), or....

The Mac users needs to verify in MacMail that the signature is trusted by actually opening the email. MacMail will then show the signature as either valid or not.

If its not valid in full email view, then the signature is indeed wrong and likely the email was tampered with.

13.2 Email arrives as blank with "smime.p7m" attachment

The email was sent using opaque digital signing and/or encryption. Some mobile email clients, and some desktop/laptop email clients cannot deal with opaque digital signing and/or encryption. This includes third party software such as email inspection solutions.

The most likely solutions are:

- a) Have the sender use clear text digital signing (instead of opaque signing), or
- b) Have the recipient make use of a p7m reader, such as provided by Ciphermail

13.3 Email arrives as blank

See 14.2, however highly likely the mail was intercepted by a third party mail inspection solution, which is unable to deal with S/MIME digital signing in general, and because of that removes the p7m content as it cannot be inspected.

13.4 Untrusted digital signature

When a third party email inspection solutions verifies an email, it sometimes adds a text message to the email body. This will immediately invalidate the digital signature.

The proper way a third party email inspection solution should add indicators to a digitally signed email, is by adding the original emails as an attachment to a new email, and solely add the indicators to the new email.