KeyTalk agent for Mac manual

Contents

Company	KeyTalk BV
Author	MR van der Sman
Creation date	9 August 2015
Last updated	06 February 2026
Product	KeyTalk agent for Mac
Data classification	Public
Software version	7.9.0
Manual version	7.9.0.1

1. Introduction

The KeyTalk agent for Mac makes use of KeyTalk's native REST API using TCP port 443 (TLS 1.3) and 80 (AIA downloads and CDP based CRL verification of the KeyTalk private CA when applicable).

The KeyTalk agent supports private key rollover, and as such is commonly used to deploy S/MIME certificates and private keys to various devices used by the same user, or user group in case of Shared Mailbox S/MIME. Not just the current S/MIME certificate and private key, but also historic certificates and private keys when available.

Our KeyTalk Mac agent, can also be used stand-alone for, or in parallel to, other client certificate use-cases, such as: 802.1x network authentication certificates (both for user and device), VPN authentication certificates, and various others.

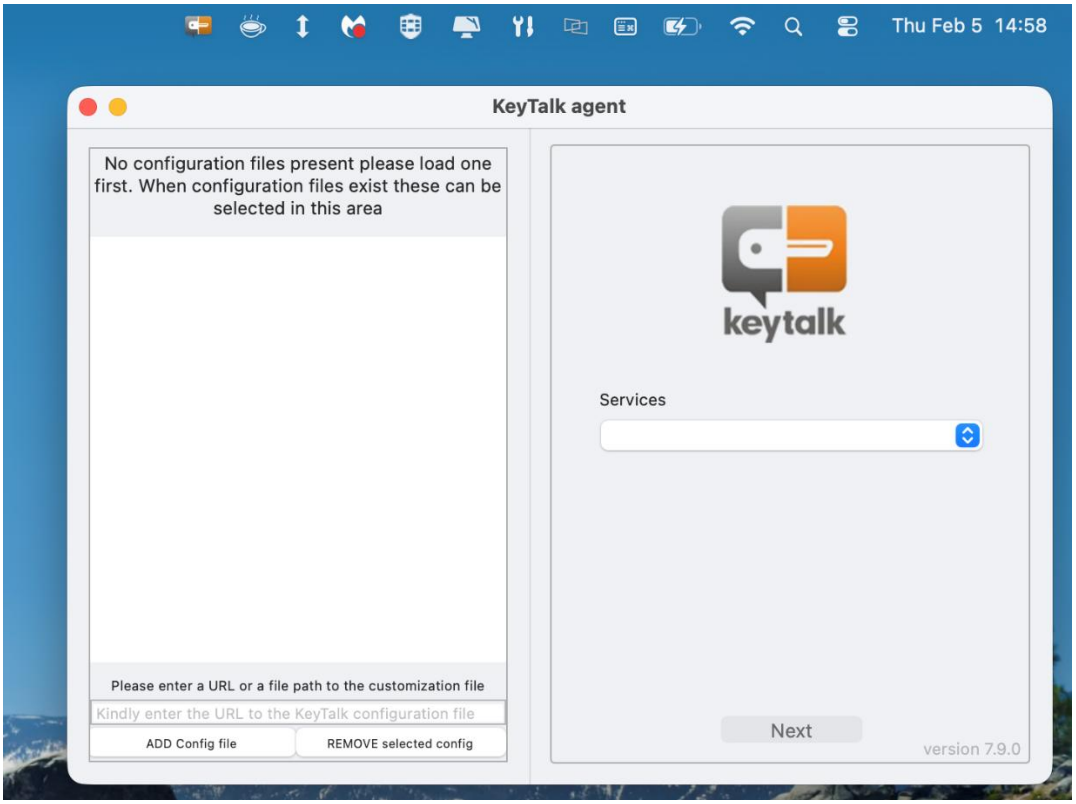
2. Installation

To install the KeyTalk agent for Mac, please visit the App Store for Mac:
https://apps.apple.com/us/app/keytalk-client/id1446009972?mt=12
Or download the KeyTalk for Mag agent in DMG or PKG format from https://keytalk.com/support

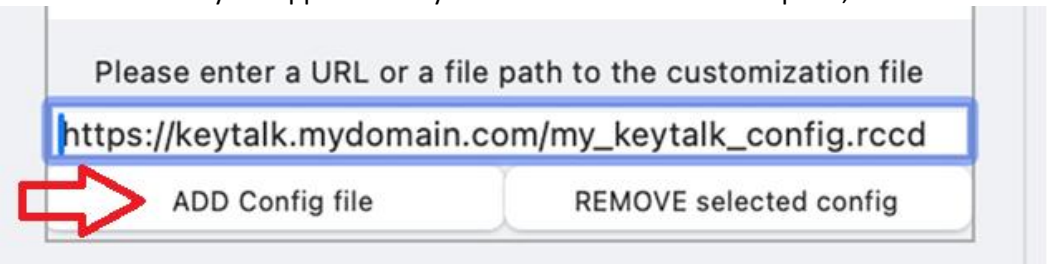
3. Configuration

3.1 Adding a KeyTalk configuration

After installation, the KeyTalk agent for Mac requires a KeyTalk Real Client Configuration Data (RCCD) file. This RCCD configuration file is provided by your IT department, or when you are the IT department, it can be obtained from your KeyTalk Certificate Template.



Enter the URL for your applicable KeyTalk instance certificate template, and select ADD Config file:



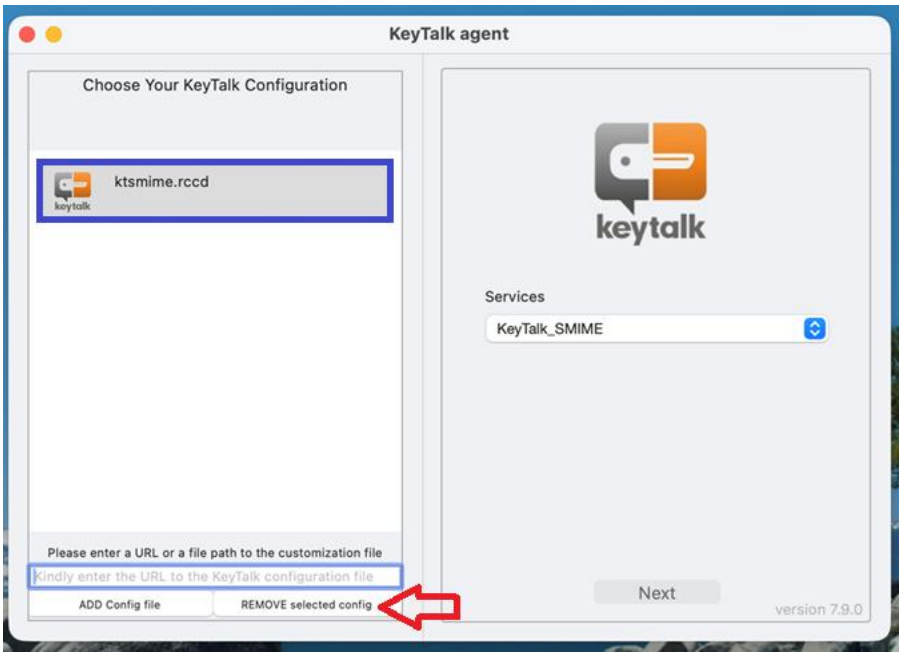
The URL can look similar to: https://keytalk.mydomain.com.com.my_keytalk_config.rccd

But can also look like:
https://keytalk.keytalk.com:443/public/1.6.9/rccd?uid=d20550bb930098e09baf48dd7a0905fb

Currently there is no generic method to mass deploy a KeyTalk agent PKG or DMG package with the KeyTalk RRCD configuration made part of the mass deployment method.
Please contact your KeyTalk account representative should you have a need for mass deployment.

3.2 Removing a KeyTalk configuration

Should an imported configuration need to be removed, you can simply select the KeyTalk configuration on the left side in your agent, and select “REMOVE selected config”



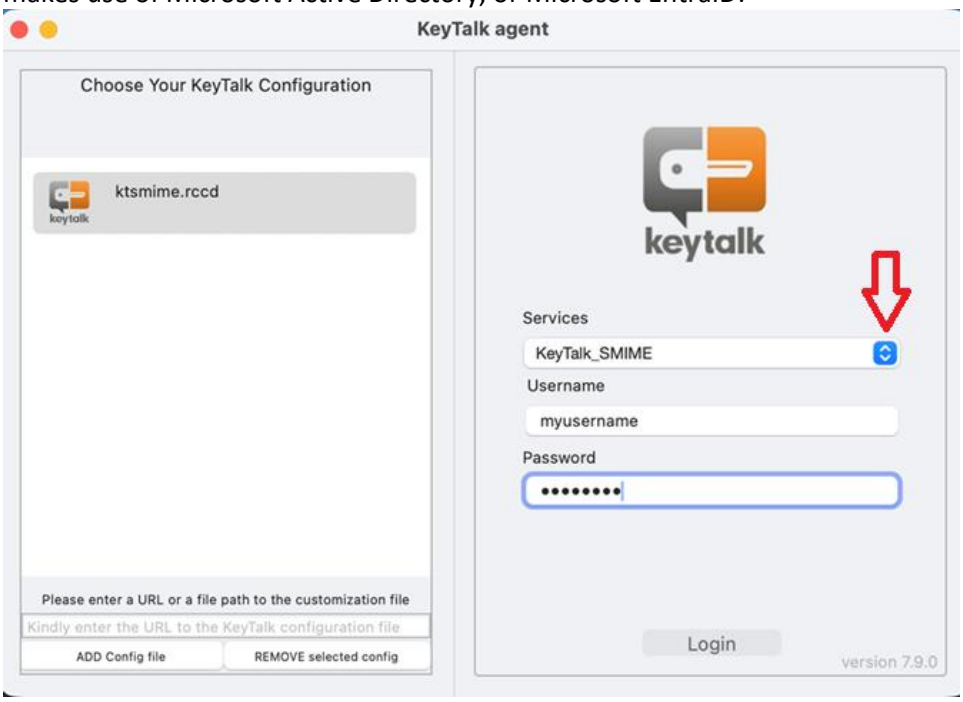
4. Using the KeyTalk agent for Mac

4.1 Using a configured certificate service

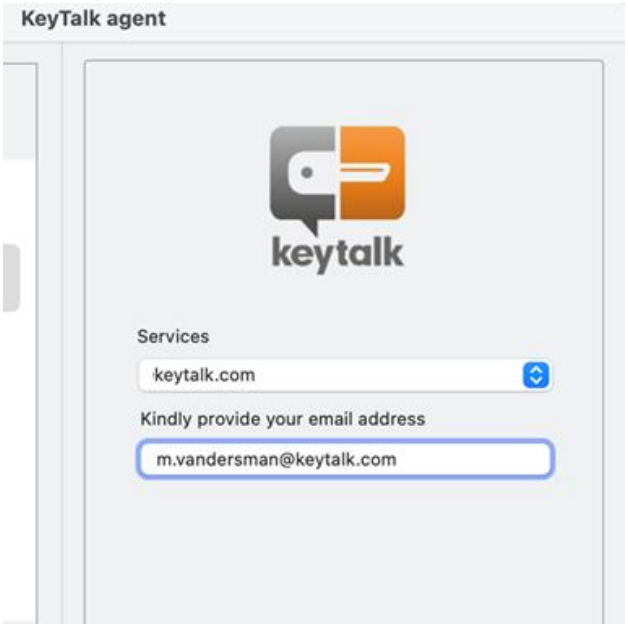
When at least 1 KeyTalk RCCD configuration has been loaded into the KeyTalk agent for Mac, the Certificate **Services** selection tab on the right side allows for the selection of 1 or more certificate templates as configured on your KeyTalk Certificate Life Cycle management solution.

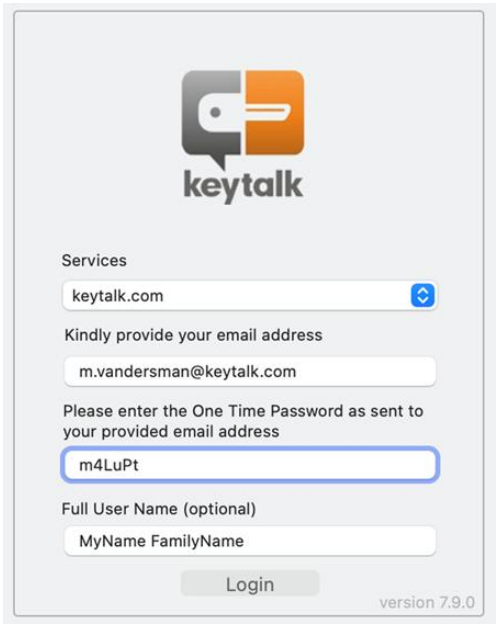
After having selected the Service, select **Next**.
The KeyTalk agent for Mac will fetch the authentication requirements from the KeyTalk Certificate Life Cycle management server.

In most enterprise cases either a username/password field will show, typically used when your company makes use of Microsoft Active Directory, or Microsoft EntraID:



However, it is not uncommon to also show:

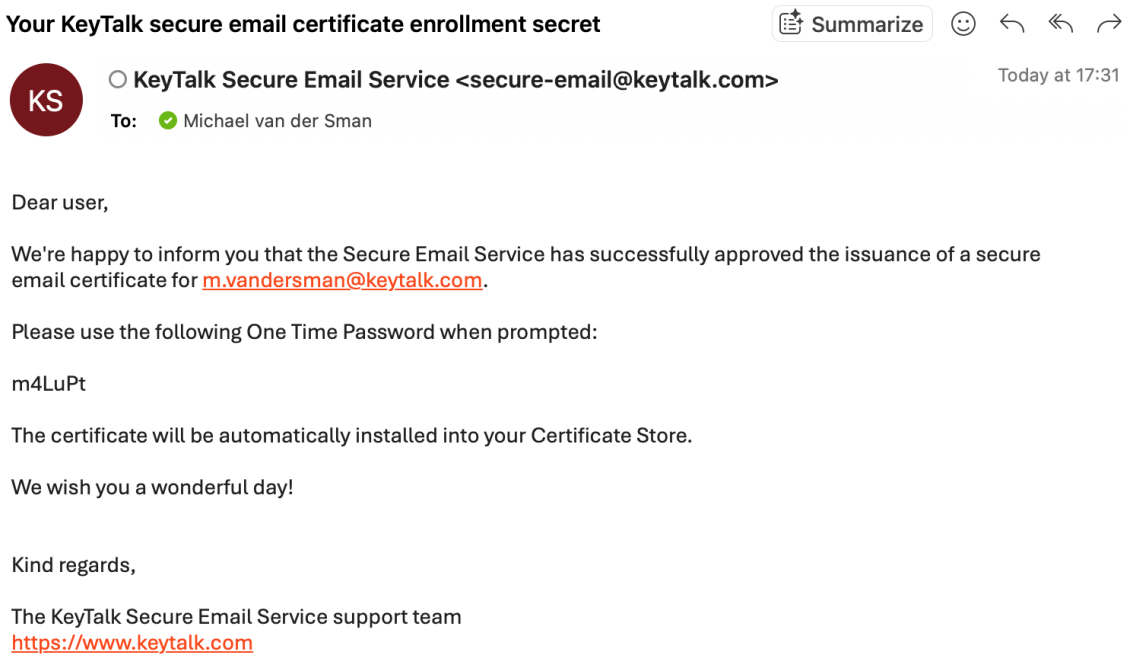




4.1.1 KeyTalk's optional mail based OTP

Some certificate use-case require ownership or at least authorized read access to an email address tied to a KeyTalk supported certificate request.

The KeyTalk Certificate Life Cycle management server will in these cases send an email with a 20 minute valid OTP for that particular request. It will look similar to:



Your KeyTalk secure email certificate enrollment secret

Summarize

KS

KeyTalk Secure Email Service <secure-email@keytalk.com>

Today at 17:31

To: Michael van der Sman

Dear user,

We're happy to inform you that the Secure Email Service has successfully approved the issuance of a secure email certificate for m.vandersman@keytalk.com.

Please use the following One Time Password when prompted:

m4LuPt

The certificate will be automatically installed into your Certificate Store.

We wish you a wonderful day!

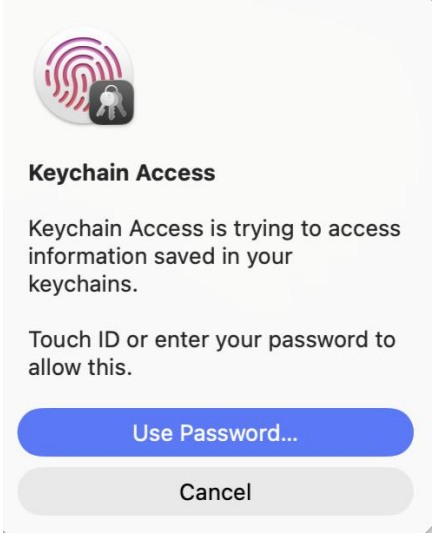
Kind regards,

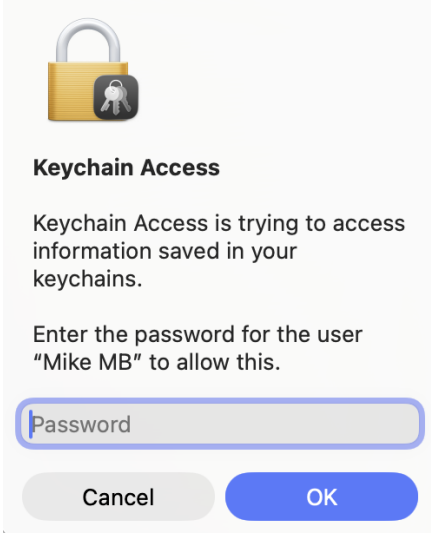
The KeyTalk Secure Email Service support team
https://www.keytalk.com

4.2 Installation of obtained certificates and keys

The KeyTalk agent for Mac will automatically install any obtained certificates and private keys after a positive authentication.

While installation has been automated, it is likely that your Mac needs you to authorize the installation of the certificate and private key. Typically the approval is granted by typing your Mac login password or by reading of your Mac configured biometrics.



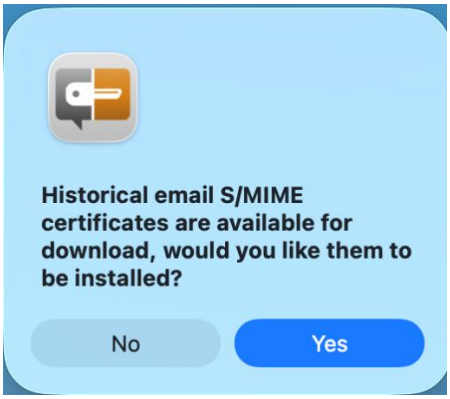


4.3 Installation of historic certificates

Should the KeyTalk Certificate Life Cycle management server also contain historically issued certificates and private key, it will trigger the KeyTalk agent for Mac to ask the user for approval to allow these to be installed.

This allows for the reading of historically encrypted emails stored in Apple Mail or Outlook for Mac.

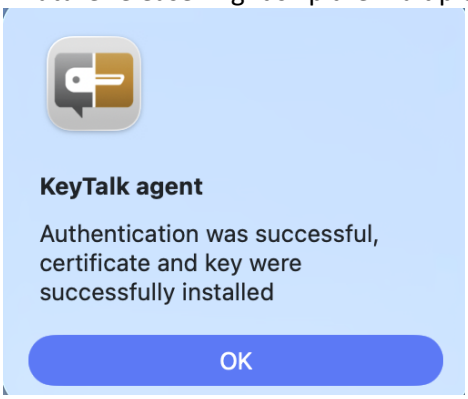
Select YES to allow these historic certificates and private keys to be installed.



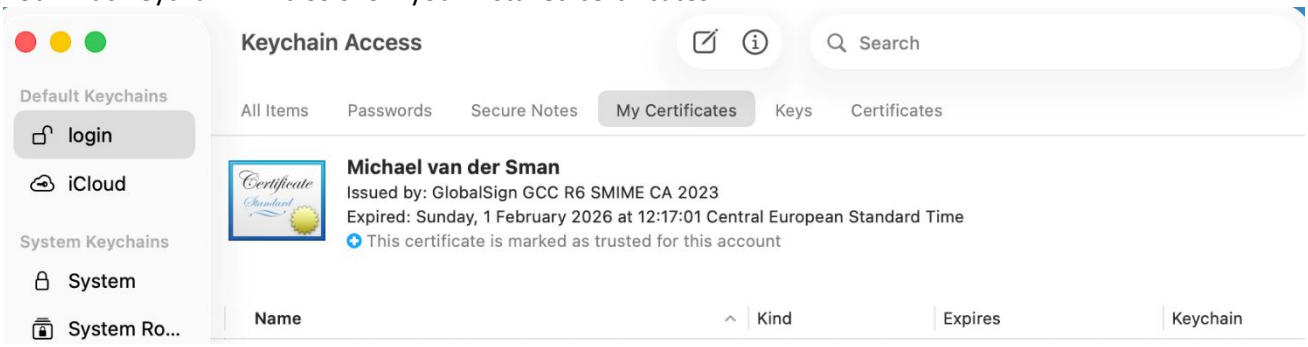
4.4 Confirmation of obtained and installed certificates

The KeyTalk agent for Mac will provide a confirmation pop-up message to confirm an obtained certificate, and when applicable its private key, was installed.

Should multiple certificates get installed, then multiple pop-ups will confirm this per certificate.
A future release might skip the multiple pop-ups.



Your Mac Keychain will also show your installed certificates:



5. S/MIME secure email certificates and Mac based email

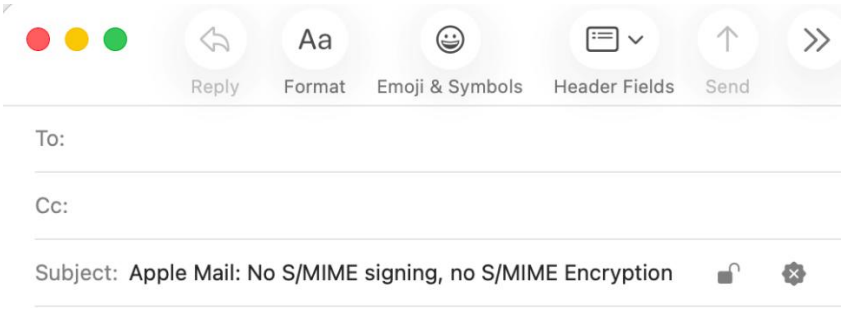
The majority of Mac users will make use of either Apple Mail, and/or Outlook for Mac.
The KeyTalk agent for Mac only installs relevant certificates and private keys. It cannot configure mail clients on Mac, as Apple makes this impossible for non-Mobile-Device-Management third party applications.

5.1 Apple Mail and S/MIME

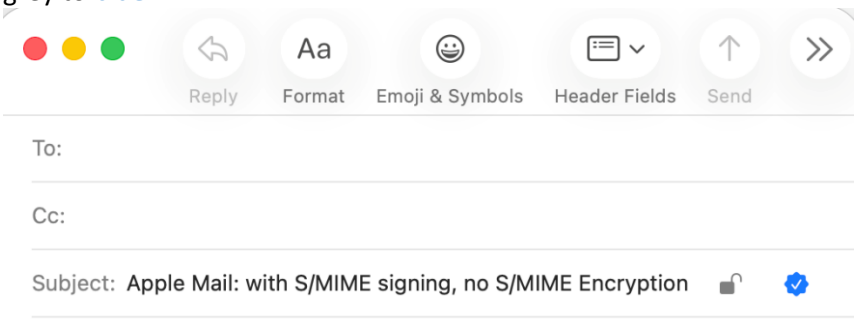
As of MacOS 26, Apple Mail will auto detect when a valid trusted S/MIME certificate and private key are available in the Mac Keychain, for a configured email address.

So nothing needs to be configured by a user on Mac Mail to make the S/MIME certificate available for their email address.

5.1.1 Signing email with S/MIME

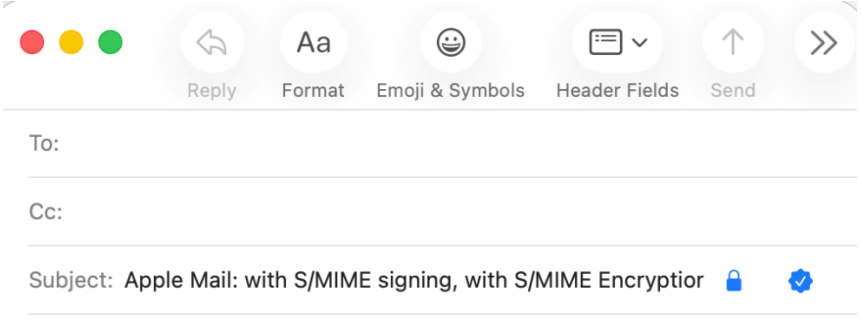


When writing a new email, or replying to an email, the symbols to the right can be selected to sign the email using an available trusted and valid S/MIME certificate. The signing symbol will turn from grey to blue:



5.1.2 Encrypting email with S/MIME

To encrypt an email, the recipient's email address valid and trusted S/MIME certificate details must be known in your address list.
The symbols to the right can be selected to sign and encrypt the email using an available trusted and valid S/MIME certificate. The signing symbol will turn from grey to blue:

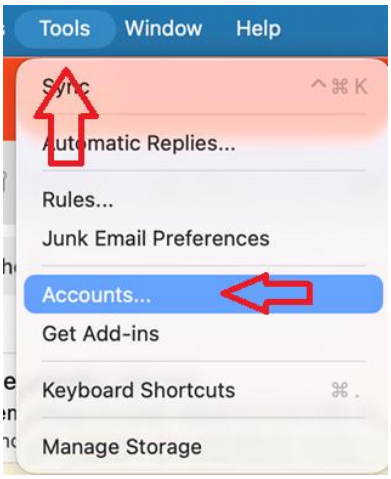


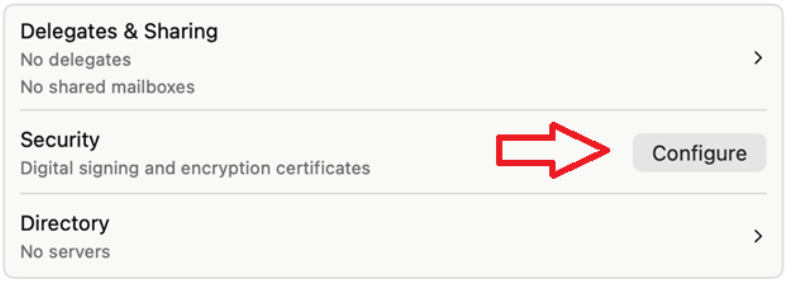
5.2 Outlook for Mac and S/MIME

As of MacOS 26, Outlook for Mac should auto detect when a valid trusted S/MIME certificate and private key are available in the Mac Keychain, for a configured email address.

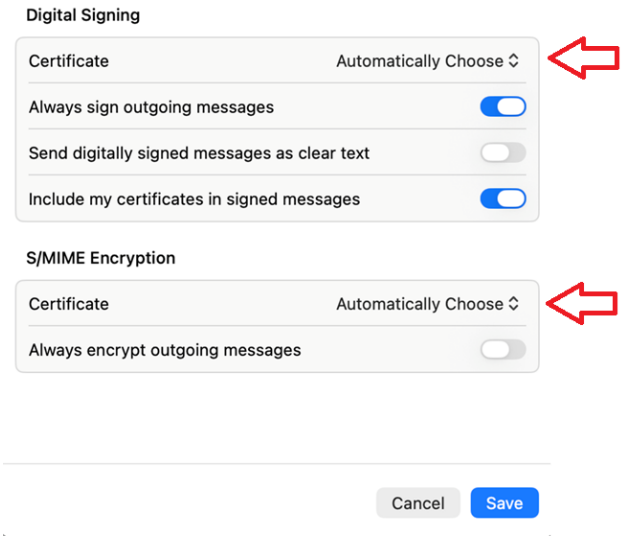
However, in practice Outlook for Mac may not always apply the correct S/MIME certificate, requiring the user to overrule default Outlook for Mac configuration for S/MIME.

To manually overrule S/MIME settings in Outlook for Mac follow these steps:

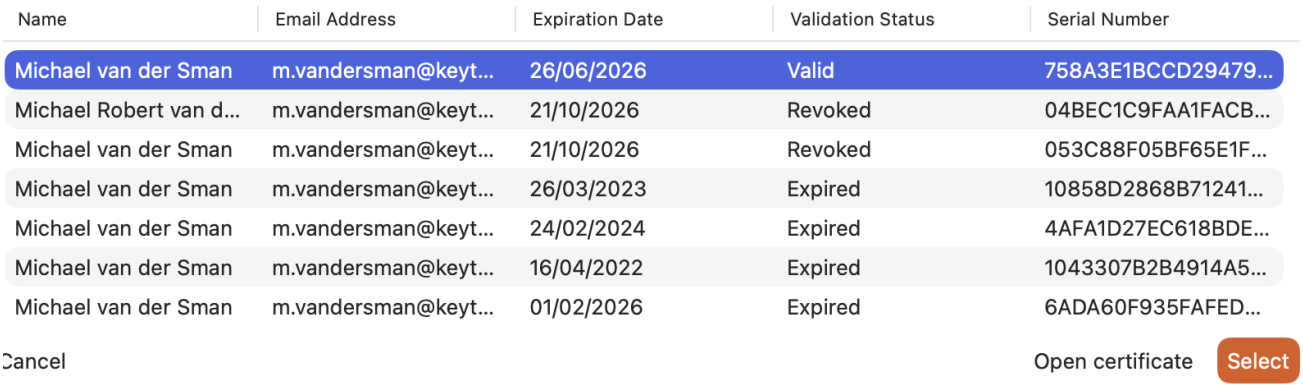




Change "Automatically Choose", to the certificate you want to use and select Save:

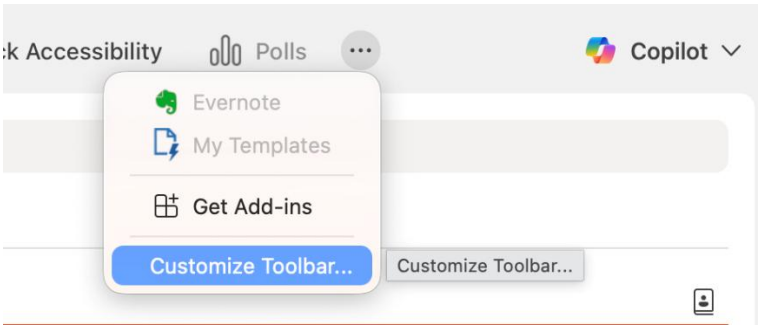


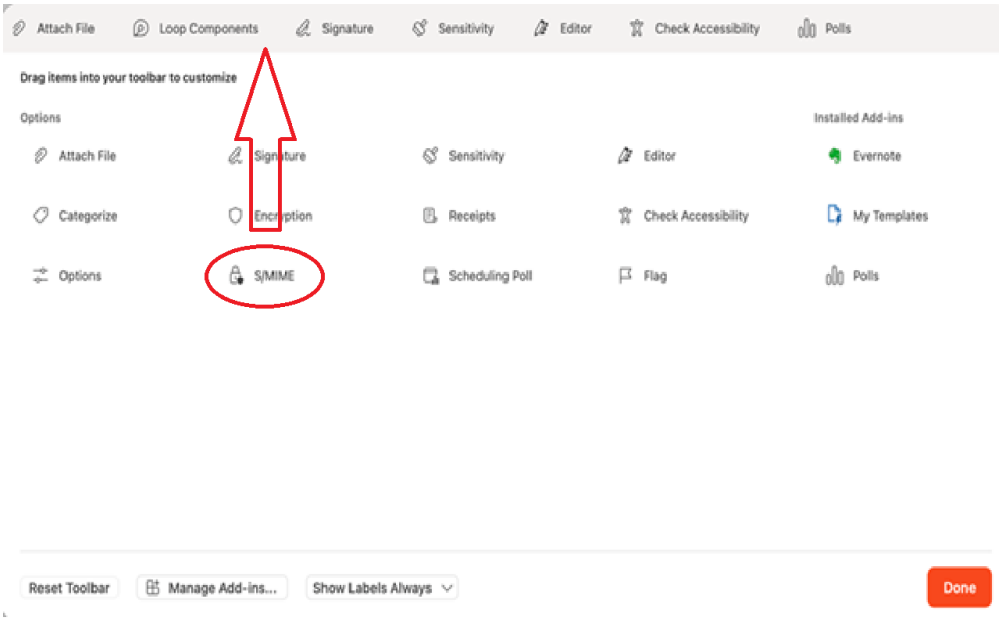
Select the certificate you want to use for the selected mail account in Outlook for Mac:



5.2.1 Enabling S/MIME option in Outlook mail toolbar

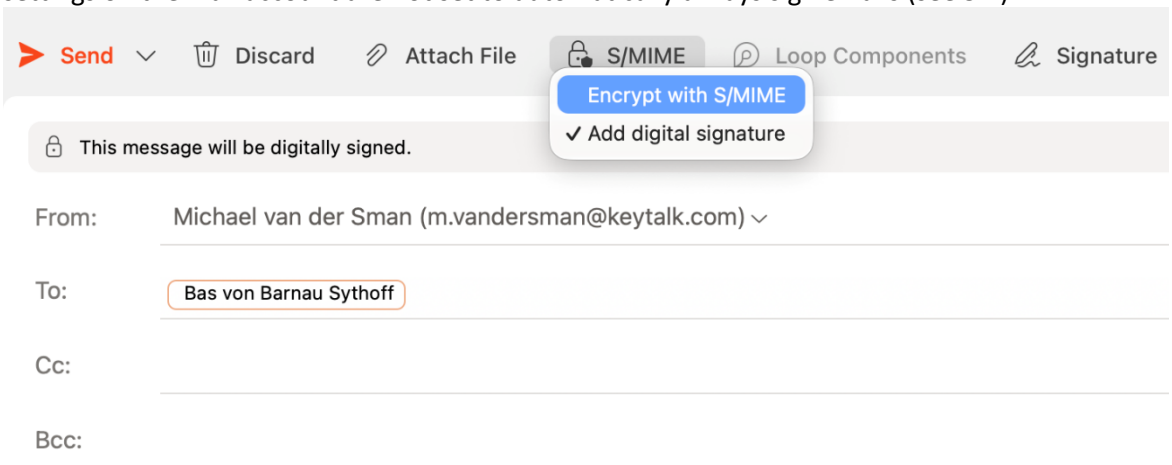
When writing an email, the interface to applied S/MIME settings might be missing.
Should this be the case, the user can easily add S/MIME to the Outlook for Mac mail toolbar.





5.2.1 Signing email with S/MIME

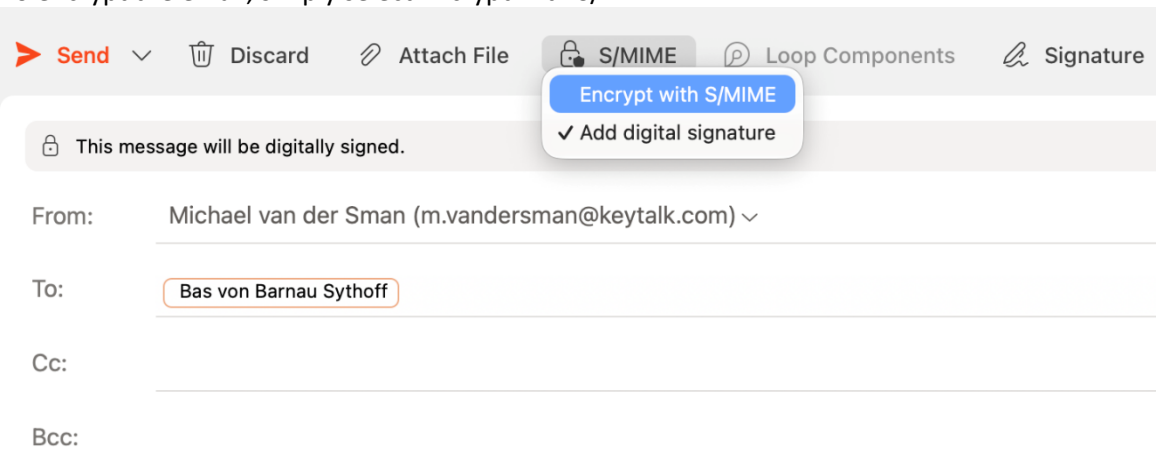
When writing a new email, or replying to an email, you can select to sign an email, when the generic S/MIME settings on the mail account are not set to automatically always sign emails (see 5.2):



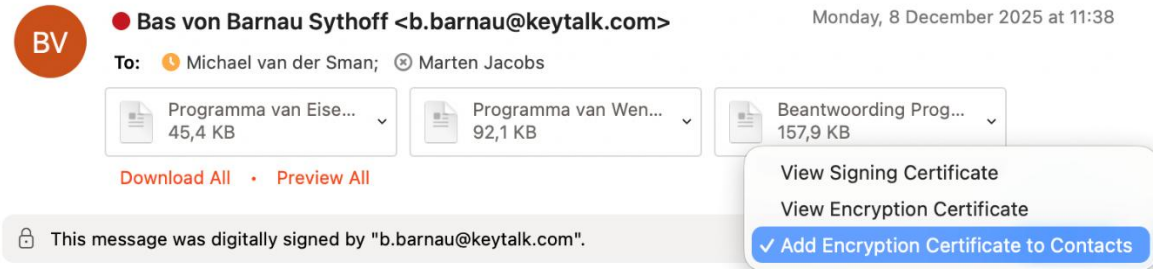
5.2.2 Encrypting email with S/MIME

To encrypt an email, the recipient's email address valid and trusted S/MIME certificate details must be known in your address list.
Especially when a recipient is an internal recipient, their valid S/MIME certificate is likely known via Outlook's Global Address List as managed by your company's DEVOPS team.

To encrypt the email, simply select Encrypt with S/MIME:



Should a recipient's S/MIME certificate not be made available via your Outlook's Global Address List, you can make use of a received email sent by the recipient and store their S/MIME certificate by right clicking their digital signature of that email:



6. KeyTalk support and contact details

KeyTalk provides third line support to its commercial partners

For 1st and 2nd line support please contact your IT department or your KeyTalk supplier, and include a description of your problem together with the KeyTalk Agent for Mac logfile.

Should you have a need to directly contact KeyTalk for technical support, please raise a ticket via email: support@keytalk.com or visit https://support.keytalk.com

Should you have commercial related questions, please email us at: sales@keytalk.com

Our office details:

Company name:	KeyTalk BV
Dutch Chamber of Commerce registration:	59072555
VAT number:	NL853305766B01
KeyTalk HQ address:	Maanlander 47 3824MN Amersfoort The Netherlands