

hQGMA4zJmb2qRccfAQv+PP0ICikBIeraqIREjf67wz1aG44Fcsi/0nZpzq53cn1b
dy00IcziXtKXI27PNK0hmYN8mBcjo5Pc2ZFgnacnVR/gVMk00GoWkHf9TCZ/ExmQ
XK4CGR7ETkRY7NdBVTct+NsmQA9UJynCf0TIZFWvJcSwLKIDHn/qK6kF9YkH7Ebl
tAJk63XkKh76iqzx+ohAGAvxc8w/7N/cCdScLZ+xswpSB7EP0tSc37i1FbDtzGAm
vcTHYbuMlbs9ieANoxv/zWP1+PmAYV/FKmr41j33Sor1oAXmTukb0H9hYw01bOPP

GpgOL Outlook Add-In

Quick guide for users

Document version: 2.1

Introduction

This guide is a tutorial for end users to get started with the GpgOL Outlook Add-In. It describes step-by-step how to encrypt and sign mails in Microsoft Outlook. In addition, you will get useful tips that will support you in your work with GpgOL.

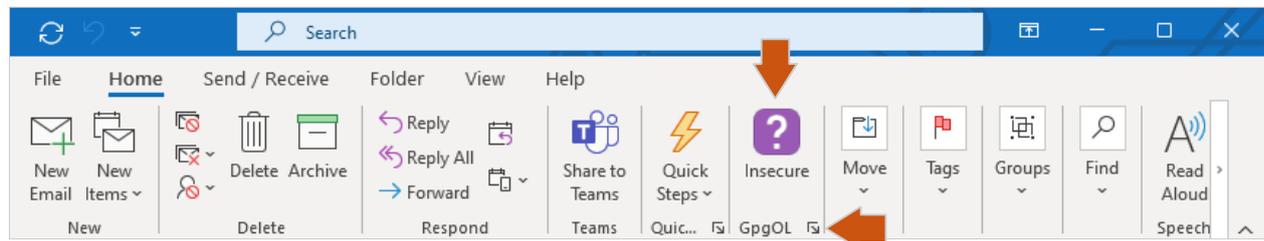
GpgOL is a component of GnuPG VS-Desktop® and GnuPG Desktop® and works in concert with the certificate manager Kleopatra.

GpgOL Outlook Add-In's goal is to make secure mailing feel as straightforward as the non-secure way. Mail traffic is considered secure if it cannot be modified, faked or read during transmission – like a postcard that is put into an opaque envelope that is sealed with wax before being mailed. Your recipient can check the wax seal to see if you were really the sender and if the envelope has been opened and possibly falsified by a third party.

All mails for which it cannot be technically ensured that they are unchanged will be displayed by GpgOL as insecure. Be always careful with such mails! Even if you receive a mail from your own server and it remains on your own network, this does not provide safety. Attackers could have taken over the server and taken control of all insecure message traffic.

1 The GpgOL-Button in Outlook

The GpgOL Outlook Add-In uses only a single button as interface:



- The button shows the security level of the mail displayed
- If it is activated in a new mail, it will be encrypted and signed
- By moving the mouse pointer over the button, the tooltip of GpgOL shows up
- The configuration menu can be reached via the "corner"-symbol next to the Text GpgOL

Note



Use the "Customize ribbon" option in Outlook to integrate GpgOL individually into your workspace.

2 Send mails

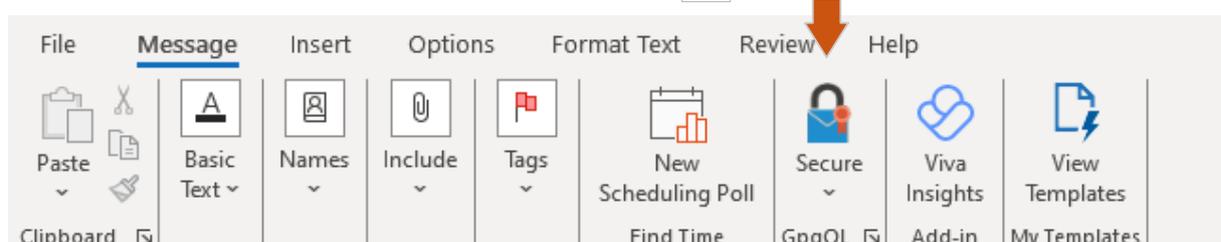
Note



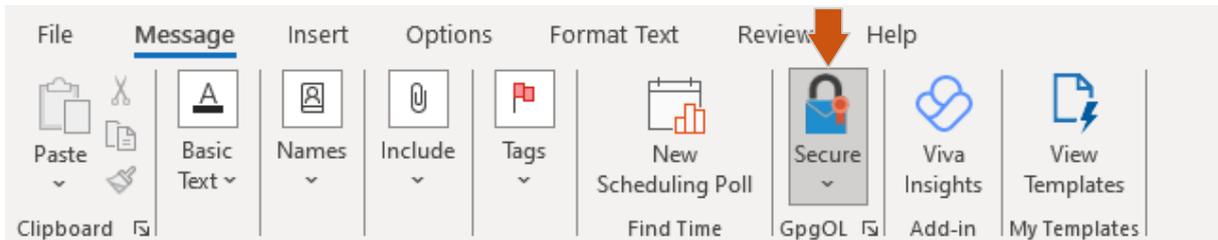
You can only encrypt emails either for recipients with OpenPGP or recipients with S/MIME certificates; it is not possible to mix certificate types in GpgOL.

In addition, to use VS-NfD compliant encryption via S/MIME, the corresponding option must first be activated in the GpgOL settings; see section.

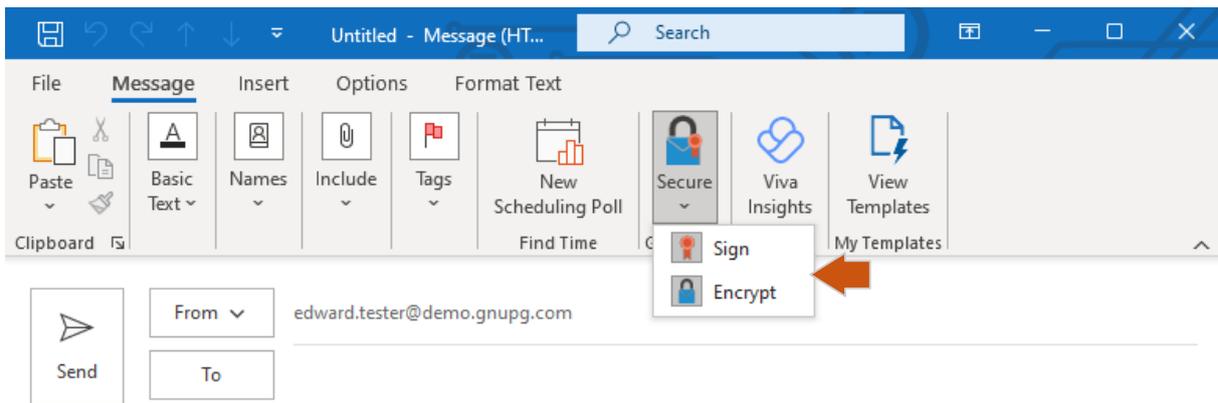
When composing mails, GpgOL shows you the -Button (Secure):



If it is activated, it is highlighted and your mail will be signed and encrypted:



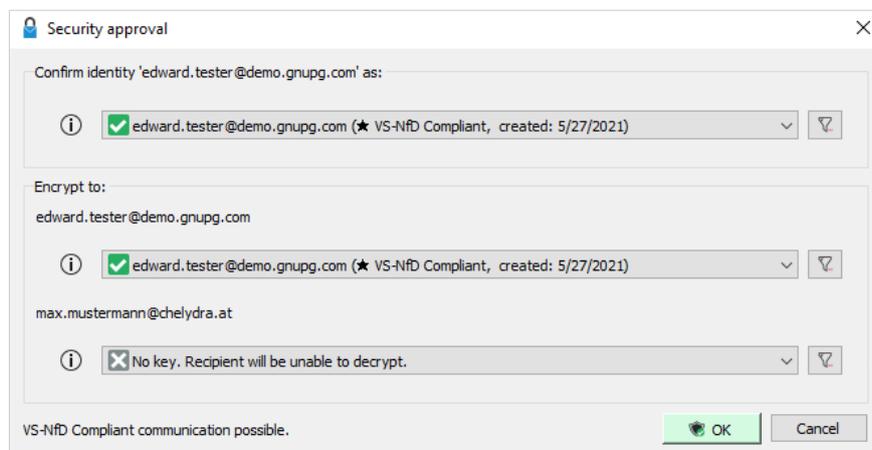
The submenu also allows you to choose whether to only **Sign** or only **Encrypt** messages. But it is recommended to use both together:



2.1 The security approval dialog

In the default setting the "Security approval" dialog is only displayed if no suitable VS-NfD compliant¹ certificate was found for at least one recipient address. In this case, the dialog offers you the option to select a different recipient key.

By clicking the -button (remove filter) to the right of the recipient line, you can select any certificate. Even ones without an associated mail address:



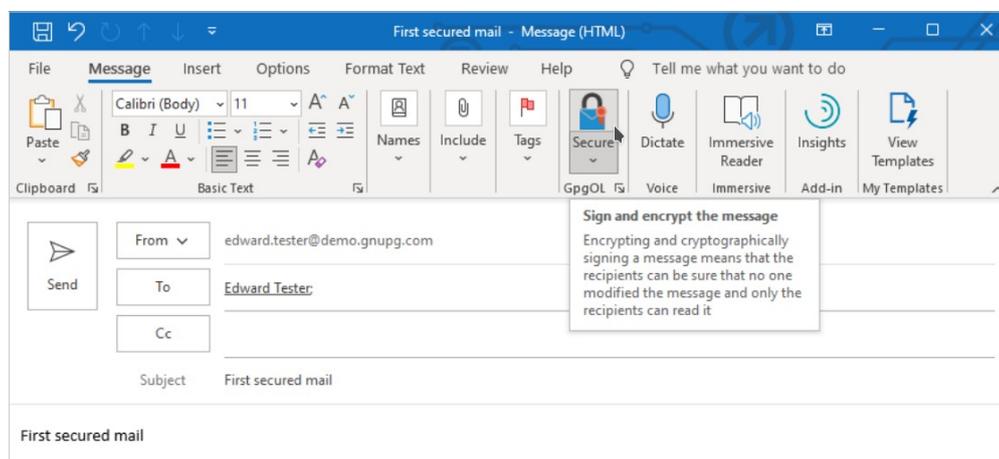
¹ GnuPG Desktop[®] does not require VS-NfD compliant keys.

 **Important**

If you do not select a certificate in the "Encrypt for others" section or if there are fewer certificates than recipients of the mail, the recipient(s) will not be able to decrypt your message! They will not receive an unencrypted mail. The sent mail can only be decrypted with one of the keys you have selected.

2.2 Sending the first secured mail

We recommend sending the first secured mail to yourself, to familiarize yourself with the workflow. First activate the Secure-button  in the new mail window, then write a short message and maybe attach a file:



 **Important**

Mails are encrypted including all attachments. **The subject will not be encrypted**, so that the recipient may always see what the mail is about.

GpgOL uses "keys" aka "certificates" for securing mails. If you do not have your own key yet, you will be shown the security approval dialog after clicking **Send**. In this case click on **Generate** to create your personal OpenPGP keypair:




Note

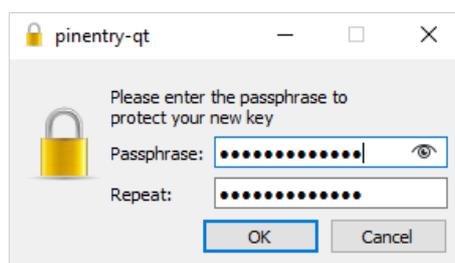
If you want to add a name to the key in addition to the mail address or want to change the default settings, you have to generate a key in advance using Kleopatra.

You will be asked for the password / passphrase you want to use for your key.


Important

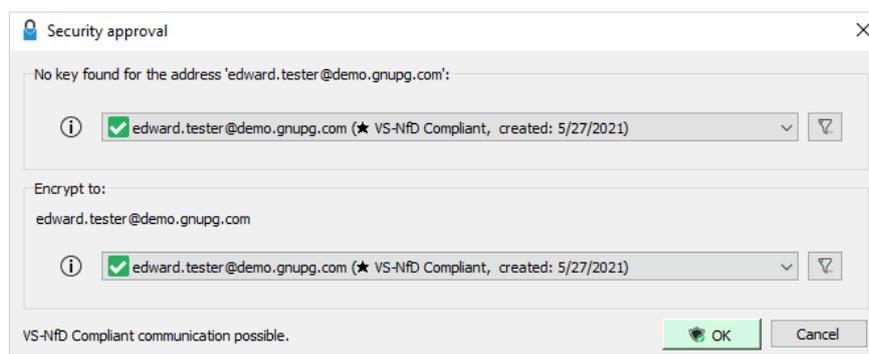
The password protects your own secret key on your file system. **It can neither be recovered nor reset. If you forget or lose your password, your certificate will be unusable!** It is therefore important that you record the password and keep it safe and VS-NfD compliant!

Enter a secure passphrase corresponding to your organizational password guidelines and click **OK** :


Note

You can set how long the password does not have to be re-entered in the configuration menu under "GnuPG System (Technical)" > "Private Keys" > "Expire cached PINs after N seconds":

After generating the key, it can be used immediately. Click on **OK** :

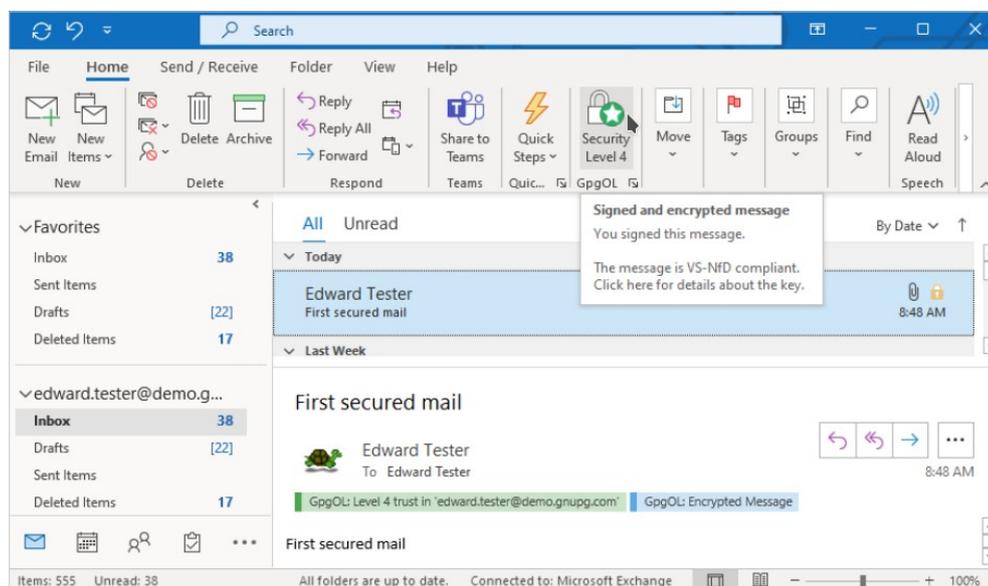


For further information please also consult the quick guide "Sign and encrypt with GnuPG VS-Desktop®". There you will learn – among other things - about what you need to do, so that others can encrypt messages to you.

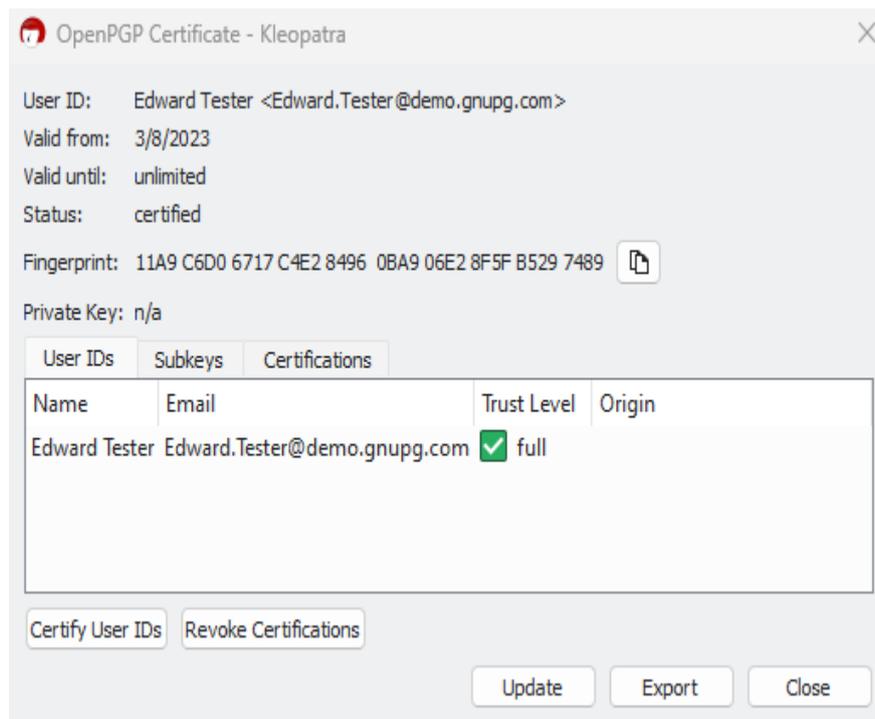
3 View mails

When you view a mail, whether in a separate window or in the message list, it is automatically decrypted. You will be asked for your password / passphrase if necessary.

If you hover the mouse pointer over the GpgOL-button within a signed mail, information about the signature and encryption of it will be displayed:



If you click on the GpgOL-button within a signed mail, Kleopatra opens and shows more information about the certificate used:



 **Note**

The certificate manager Kleopatra, the graphical frontend of GnuPG VS-Desktop® and GnuPG Desktop®, allows you to easily manage your keys/certificates. Here you can specify, e.g., whether you trust a third-party certificate by signing (= certifying) it.

3.1 Security levels for the identity verification of received mails

 **Note**

These security levels for received mails are not VS-NfD relevant, but give a clue for assessing the authenticity of the mail. More information is shown in the tooltip of GpgOL.

It is crucial for the exchange of VS-NfD information that the certificate of your communication partner is marked as VS-NfD compliant in Kleopatra. This corresponds to the levels 3 or 4 listed below. Only then can you send encrypted mails to other parties with GpgOL without receiving a warning.

The GpgOL Outlook Add-In uses different security levels for authentication depending on the trust status, which makes it easy to map organizational measures. It can take a second for the security level of a newly selected mail to be displayed correctly:

Security level 0 (Insecure/Encrypted); no validation



The key of the communication partner is unknown or the mail is not signed.

Security level 1; Validation by mail address



GpgOL does not make any trust statements about the identity of the key/certificate holder here, but uses the certificate for encryption. This level protects against passive attackers, but not against active "man in the middle"-attacks.

Security level 2; Limited identity validation



The communication partner's key was automatically delivered by their provider via a secure connection. This is only possible, if the provider uses "Web Key Directory"². There is a basic trust that the sender controls the mail address from which the message was sent.

Security level 3; Identity certification



The identity of the communication partner has been authenticated with a trusted certificate. This level protects against active attackers.

Security level 4; Validation by direct trust



The user himself or a certification manager of his organization has checked the fingerprint of the key and signed it.

4 The certificate manager Kleopatra as crypto address book

GpgOL uses the certificate manager Kleopatra to retrieve the appropriate certificates for its communication partners. Based on your configuration, it additionally searches in external sources (Active Directory, X509 certificate server, Web Key Directory, etc.).

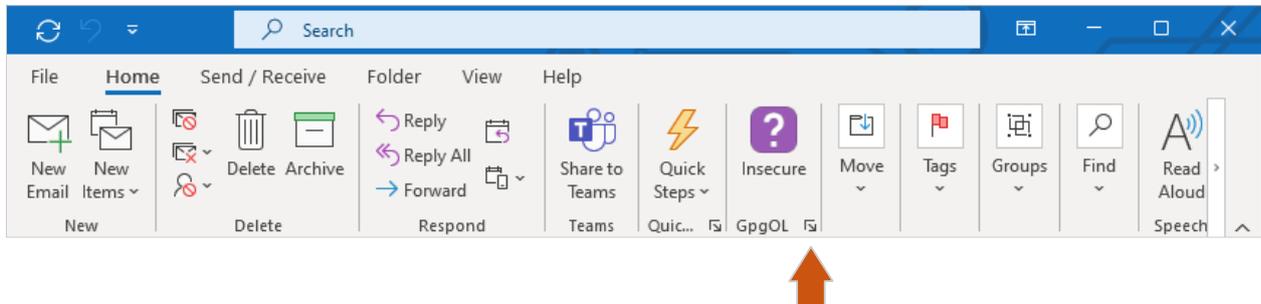
The choice is made via the mail address. If several VS-NfD compliant or trusted certificates are available for a mail address, the newest one is selected.

For a shared mail address, you must first create a group in Kleopatra. See the quick guide "Group-feature of GnuPG VS-Desktop" for this.

² <https://wiki.gnupg.org/WKD>

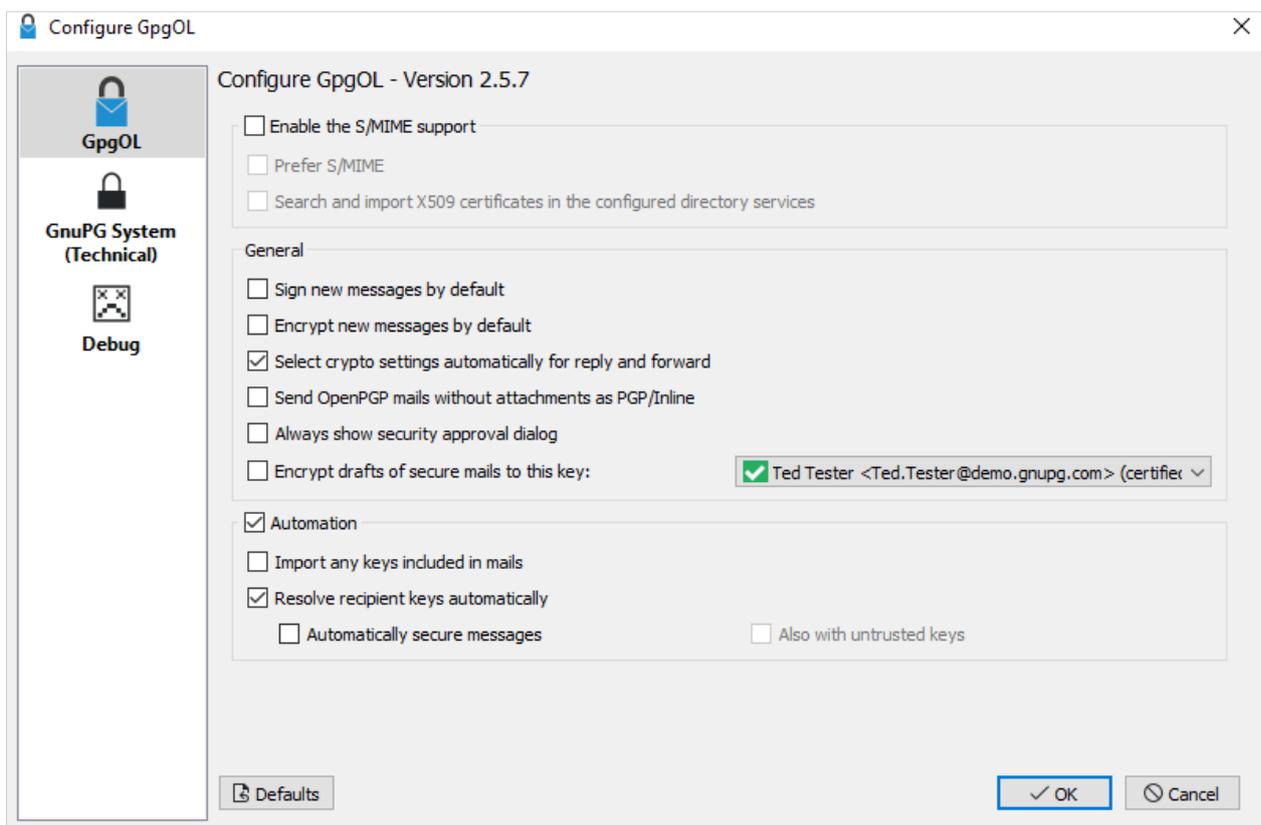
5 The GpgOL configuration menu

You can reach the configuration menu via the "corner" symbol to the right of the text GpgOL:



5.1 Important options

The GpgOL configuration menu offers many mostly self-explanatory settings.



Explanations of some important options follow:

Enable the S/MIME support

Since Outlook itself supports S/MIME, S/MIME support for GpgOL is disabled by default. For VS-NfD compliant encryption using S/MIME, this option must be selected.

Prefer S/MIME

If S/MIME and OpenPGP certificates are available, S/MIME will be preferred.

X.509 Zertifikate in den konfigurierten Verzeichnisdiensten suchen u. importieren

This option enables sending an automatic search request to the directory service configured in the GnuPG system for each recipient of a mail that does not have a valid certificate. These certificates will be imported and then used automatically if their certification is trusted.

If you combine this option with "Automatically secure messages", a search query is generated even for mails that are not to be encrypted. With this setting, the server can recognize who is your communication partner. It is recommended to activate this option only when the certificate server for your organization is under your control.

Select crypto settings automatically for reply and forward

When replying or forwarding, the crypto settings are applied based on the originating mail. Encrypted mails are therefore replied to or forwarded in encrypted form by default.

Send OpenPGP mails without attachments as PGP/Inline

Your mails will not be sent in PGP/MIME format if you do not have an attachment, i.e. the mail body will be replaced by a "PGP Message".

PGP/Inline has the disadvantage that attachments cannot be saved in a user-friendly way and also the encoding is not clearly defined. You should use this option only in exceptional cases if your communication partner does not use a PGP/MIME capable mail client.

Always show security approval dialog

The security approval dialog is also displayed if a trusted or VS-NfD compliant certificate is found for all recipients and not only if something is missing.

Encrypt drafts of secured mails to this key (certificate)

Especially if your drafts and autosaves are not only stored locally but also on the mail server, this option can provide an additional security benefit. It prevents unencrypted content from being stored on the server before you send a secured mail.


Important

GpgOL can only know whether you want to save a mail encrypted if you have already activated the Secure-button  before writing your message.

Import any keys (certificates) included in mails

Certificates that are attached to mails or attached in the autocrypt header will be get imported. Those keys will be shown by GpgOL as "untrusted" as long as they are not certified. They can help you to automatically secure communication with a low protection requirement.

Resolve recipient keys (certificates) automatically

It will automatically be search for keys both locally and in the key sources configured in the GnuPG system (usually Active Directory and Web Key Directory). If the option "Search and import X.509 certificates in the configured directory services" is enabled, this is also performed for S/MIME.

Automatically secure messages

GpgOL automatically toggles the Secure-button  as soon as trusted keys are detected for all recipients. The additional option "Also with untrusted keys" allows to use untrusted keys from autocrypt headers as well. In many cases, this already provides sufficient protection against passive attacks, e.g. against simple interception of your mail communication.

However, since these certificates do not meet the requirements for VS-NfD, you have to confirm again that you still want to encrypt before sending the mail.

Appendix

This document has been published under the license "Attribution-Share Alike 4.0 International (CC BY-SA 4.0)". The legally binding license agreement can be found at:

<https://creativecommons.org/licenses/by-sa/4.0/deed.en>

GnuPG VS-Desktop® is a registered trademark of g10 Code GmbH.