BAYOOSOFT
MANAGEMENT SOFTWARE

User Guide

GPG4O - Version 8.5

Manual for End Users

Content

1 General

1.1 Audience of this document

This document describes the installation, configuration, and usage of gpg4o® on a single system for end users. System operators are advised to read the „gpg4o Administrator Manual“, which describes the general configuration and usage of group policies of gpg4o.

1.2 gpg4o – GPG for Outlook

Gpg4o is developed as an add-in for Microsoft Outlook 2010® and later and is supported by the 32- as well as by the 64-bit version.

Gpg4o assures a safe electronic communication by encrypting and decrypting emails and their file attachments. Of course, signing and verifying is also possible.

The integrated key management by gpg4o provides simple and uncomplicated handling of public keys.

The validity of external keys is verified based on the Web of Trust. For this purpose, information of known key owners is used.

1.3 GnuPG and OpenPGP

To use gpg4o, GnuPG is required, which can be installed by the user during initial setup. GnuPG is a free cryptography system. It is used for encrypting and decrypting data as well as for generating and verifying digital signatures. GnuPG implements the OpenPGP standard.

For information about GnuPG and the source code, see:

https://www.gnupg.org/

The General Public License (GPL) can be found at:

http://www.gnu.org/licenses/gpl.html

1.4 Key, keypair and key exchange

The OpenPGP standard used by gpg4o works according to the principle of asymmetric encryption. For this purpose, so-called public and private keys are used, which together form the so-called keypair. For beginners it is always a bit confusing what it is about and how they are connected to each other.

Basically, you always need the public key of your communication partner before you can send him an encrypted message. You must import this key at least once. Your communication partner also needs your public key in order to write encrypted emails.

You can easily attach your public key when composing an email and thus communicate it to your communication partners. In addition, there are so-called key servers on the Internet, to which you can upload your public key. For more information, see chapter 8.8.

The data is decrypted with the private key after you have entered the passphrase. By entering the passphrase, you confirm that you are authorized to access the decrypted data.

Attention: Never give out your private key and/or passphrase to anyone else! Otherwise, they can read your emails and sign them on your behalf.

The recipient of a signed email can verify the signature of your email - and thus detect changes to the email - when he or she has imported its „public“ key.

In short, you can distribute your „public“ key to everyone in the world with a clear conscience. In contrast to your „private“ key, which should always be kept in a safe place.

2 System requirements

Gpg4o has been developed for Microsoft Outlook 2010 (and later) on Microsoft Windows. Details about compatibility of gpg4o with certain operating systems versions can be found in the table below.

Operating system	Outlook 2013	Outlook 2016	Outlook 2019
Windows 10	✓	✓	✓
Mac OS	✗	✗	✗

Gpg4o is supported with 64-bit Outlook and 64 Bit Windows versions.

Gpg4o uses GnuPG, a free implementation of the OpenPGP standard. During the initial setup, a current GnuPG version supported by gpg4o is automatically installed.

3 Functional range

3.1 Versions functional range comparison

Funktion	Trial Version	Free Version	Full Version
PGP/Inline Encrypt, decrypt, sign emails	yes	yes	yes
PGP/MIME Encrypt, decrypt, sign emails	yes	yes	yes
Simultaneously usable email accounts	1	1	any number
Private/commercial use	yes /yes	yes /no	yes / yes
HTML E-Mails	yes	yes	yes
„Plain-Text“ emails	yes	yes	yes
Individual sending rules	yes	no	yes
Decrypted saving of emails	yes	no	yes
Automatic up-/download of keys	yes	no	yes
Check on GnuPG updates	yes	no	yes
Automatic homedir backup	yes	no	yes
Period of support by email [1]	45 days [2]	no [3]	1 year [4]
Period of update	45 days [2]	unlimited	1 year [4]
Period of usability	45 days [2]	unlimited	unlimited
Supported email servers			
Microsoft Exchange	yes	no	yes
POP3	yes	yes	yes
IMAP	yes	yes	yes
Outlook.com	yes	yes	yes
Hotmail.com	yes	yes	yes
Additional			
Compatible with DATEV installations	yes	no	yes

[1] To contact support, use the email address support@gpg4o.de. No telephone support is offered.

[2] Extension of the test period is possible on request.

[3] Support cannot be used.

[4] Depending on the duration of product maintenance (1 year after purchase, afterwards extensible by purchasing an extension of product maintenance: +1 year, +3 years, or +5 years)

3.2 PGP/Inline and PGP/MIME

Gpg4o can send/receive text and HTML emails in PGP/Inline and PGP/Mime format. It is also possible to verify PGP/MIME signed emails.

3.3 What happens to the test version after the expiration date?

You can only decrypt emails, that were received during the test period. After the test period, emails that are signed/encrypted can no longer be sent. To extend the test period, contact our support team.

3.4 What happens to the full version after the expiration of the product?

When the support has expired, gpg4o can be used further. This means that you can further send encrypted/signed emails and read encrypted/signed emails. However, you can no longer install updates or contact support.

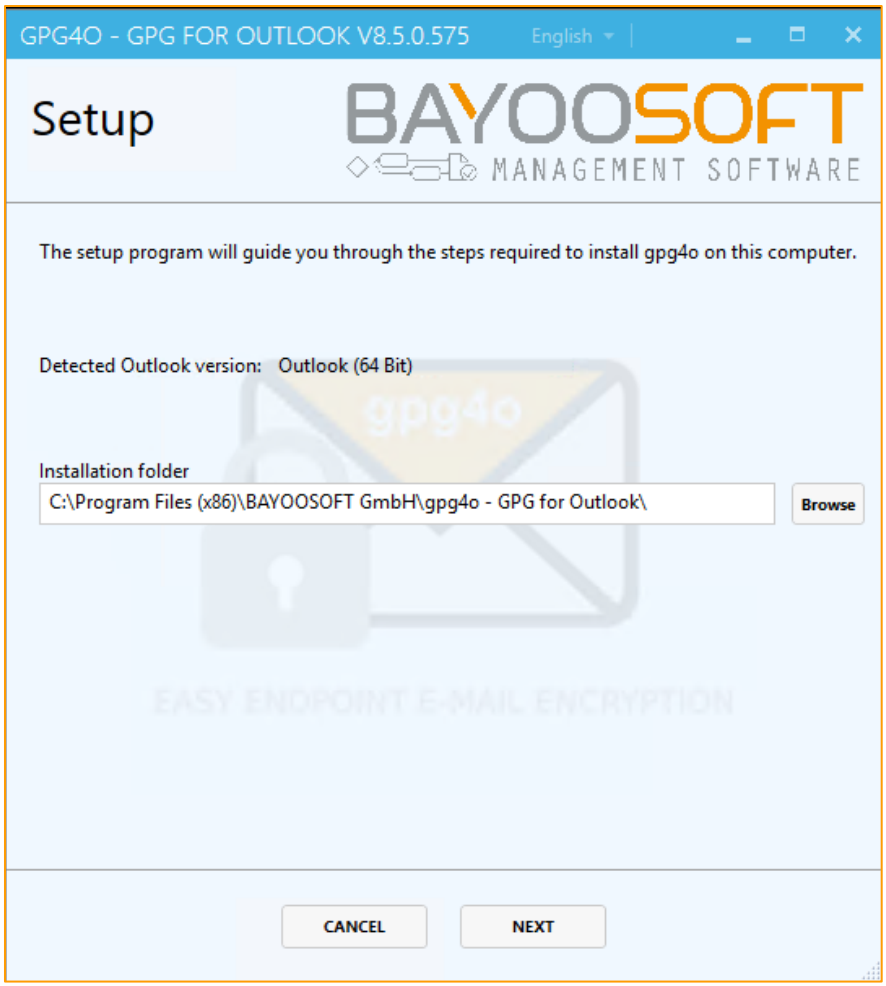
3.5 Duration of gpg4o Free

The free version of gpg4o is not limited to a time period and can always be updated to the newest version. Gpg4o Free functionality is limited. Furthermore, support cannot be granted.

4 Installation of gpg4o

Hint: You can find the latest version of gpg4o at https://www.bayoosoft.com/en/email-encryption/

You need local administrator rights for the installation. Please close the Microsoft Outlook application before installing gpg4o so that the installation can be executed correctly. Then double-click the file „gpg4o setup.exe“.

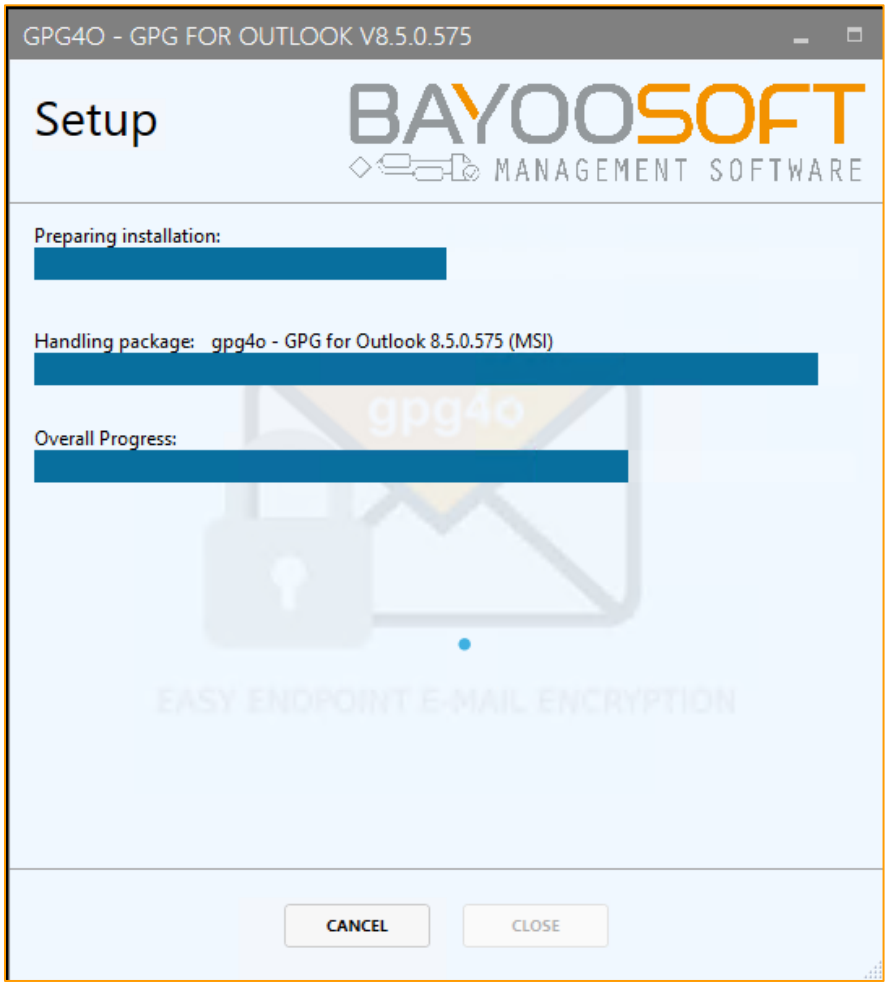


In the start dialog you will be asked for the installation path. The default setting is usually the right choice here. Confirm the installation path with “NEXT”.

By default, gpg4o is installed in this folder:

C:\Program Files (x86)\BAYOOSOFT\gpg4o - GPG for Outlook\

If you have decided to accept the End User License Agreement (prerequisite for installation), click “I accept the terms of the license agreement” first, and then click “INSTALL”.



After any missing system components have been downloaded and installed, gpg4o will be installed.

As soon as the installation of gpg4o has been successfully completed, now start Microsoft Outlook to start setting up gpg4o.

5 First configuration

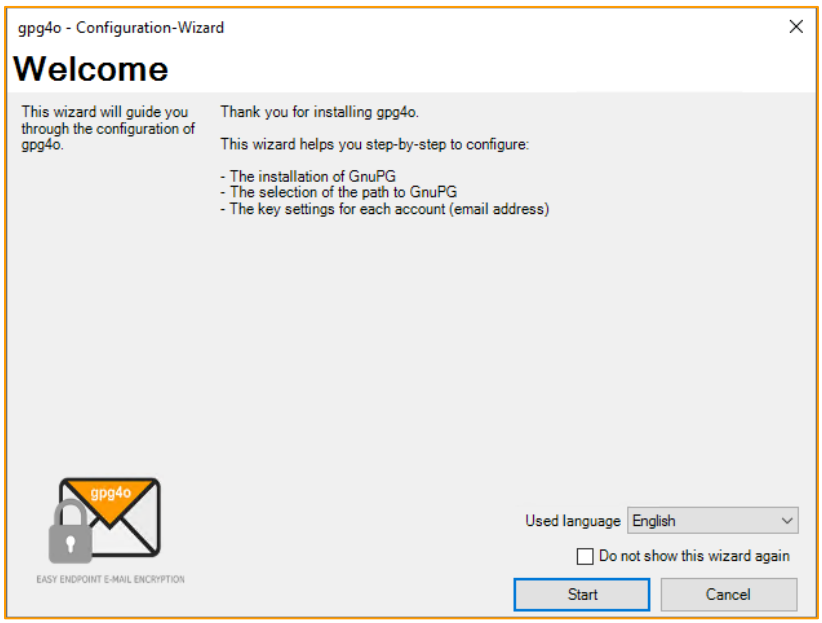
As soon as you start Microsoft Outlook after installing gpg4o, the Configuration Wizard will appear to help you set up the initial setup.

5.1 Simple configuration

5.1.1 Start

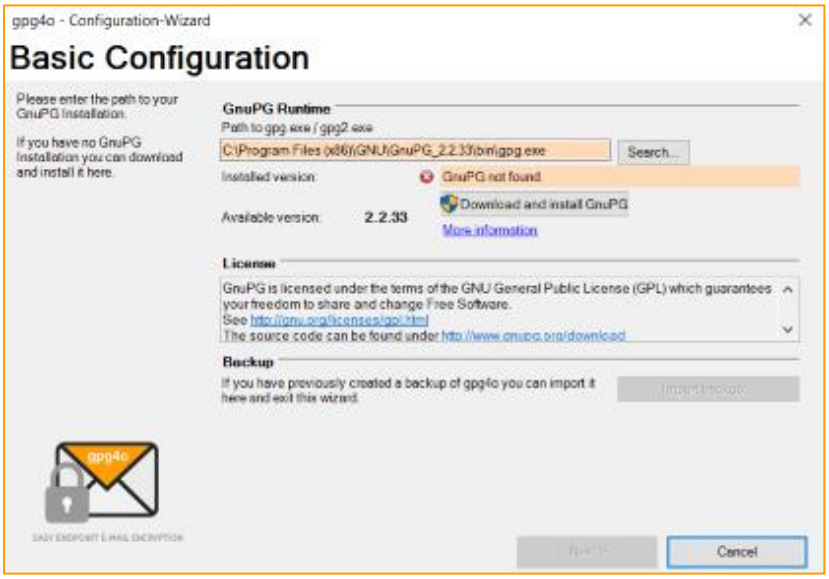
On the first page of the wizard, you can change the application's display language. Once you have made the language setting, click on "Start" to start the configuration.

You can click the "Cancel" button to exit the wizard, however it will be called each time Microsoft Outlook is started until it has been run through completely and an account is configured to use gpg4o.



5.1.2 Basic Configuration

The GnuPG component is set up on this page, which performs the encryption and decryption of the data.

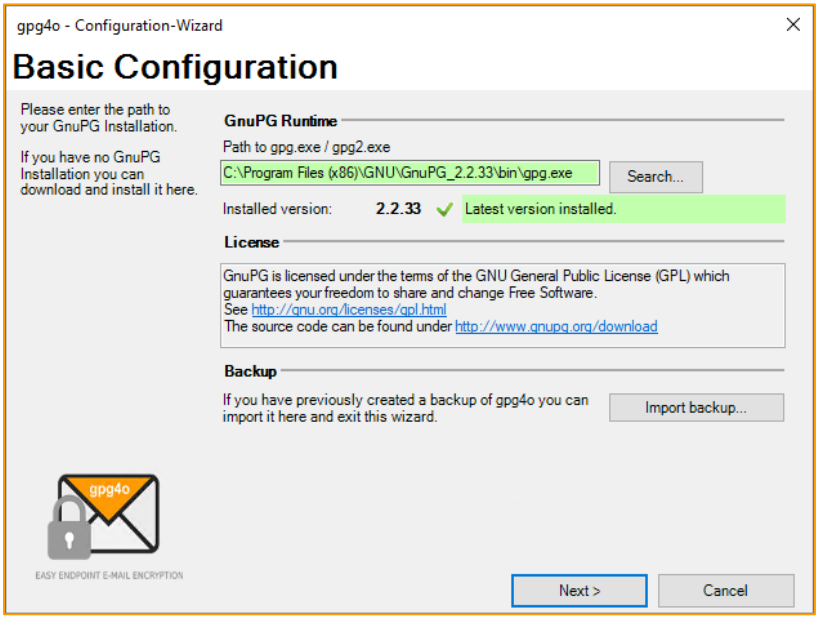


If GnuPG is already installed on your computer, the path will be automatically entered and highlighted in green. If an installed GnuPG was not found, the selection is highlighted in red.

If you have not yet installed GnuPG, start the installation by clicking on the button “Download and install GnuPG”.

Hint: Please make sure that the directory in which GnuPG is to be installed is empty.

After successful installation, the path is automatically copied to the settings, and you can continue with the configuration.

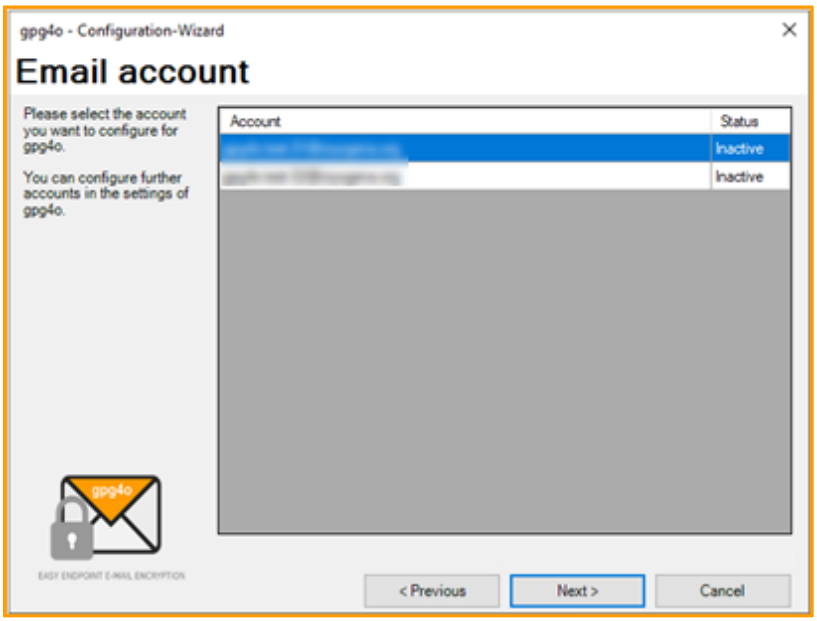


5.1.3 Email account

If multiple email accounts are set up in Microsoft Outlook, you can select the account for which gpg4o is initially set up here. We recommend selecting the email account that you are mainly working with.

Hint: After completing the wizard, you can set up additional accounts for use with gpg4o at any time.

If there is only one email account in Outlook, this page will be skipped and gpg4o will be set up automatically for the existing account.



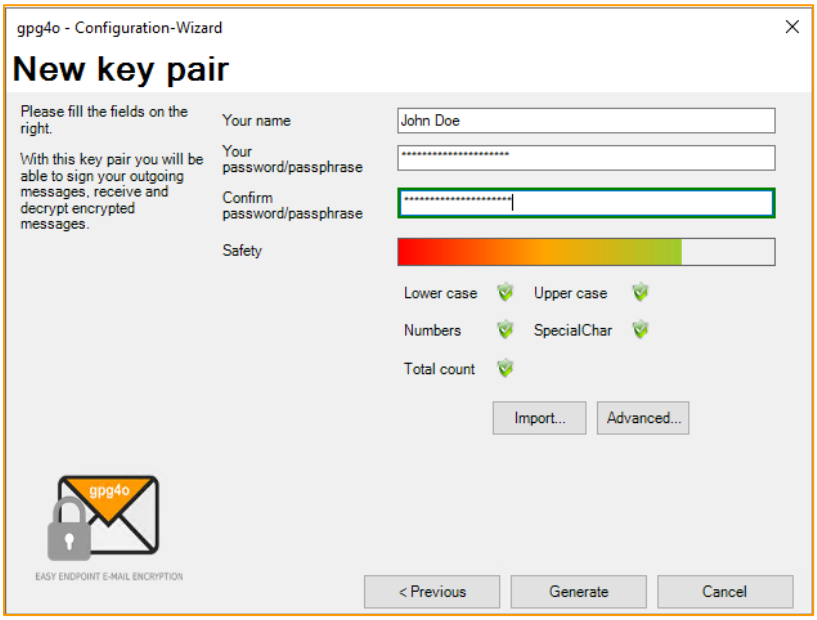
Select the account with which you want to use gpg4o and then click on “Next”.

The option "Activate S/MIME Integration" enables the selection of Outlook's own S/MIME encryption from within gpg4o when sending e-mails.

Attention: This is only the integration of the Outlook-specific function. An installed S/MIME certificate is required. This function is experimental, and so far, not supported.

5.1.4 Key creation

The following dialog box appears for configuring the new keypair.



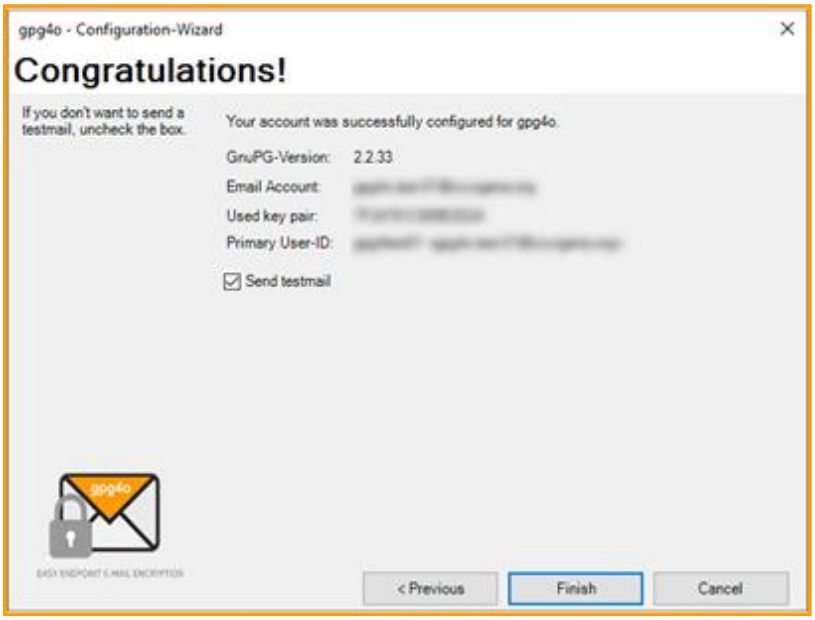
To create a new keypair, enter your name and a passphrase. The passphrase is required regularly to decrypt and sign emails.

Attention: Remember the passphrase you entered, because without it no decryption of your emails is possible! Neither gpg4o nor **BAYOOSOFT GmbH** know your secret passphrase and there is no way to recover a forgotten passphrase!

After you have filled in all required fields, click on “Generate” and your new keypair will be created.

5.1.5 Summary

Now that you have created a keypair, the summary of your institution will appear.



If you leave the checkbox "Send testmail" checked, you will automatically receive an encrypted test message to check the configuration of gpg4o.

Click "Finish" to complete the setup. In Chapter 6 the first steps of using gpg4o are explained.

5.2 Advanced configuration

This chapter provides more detailed information about the advanced configuration wizard options. As a first-time user, you can skip this chapter and start directly with Chapter 6.

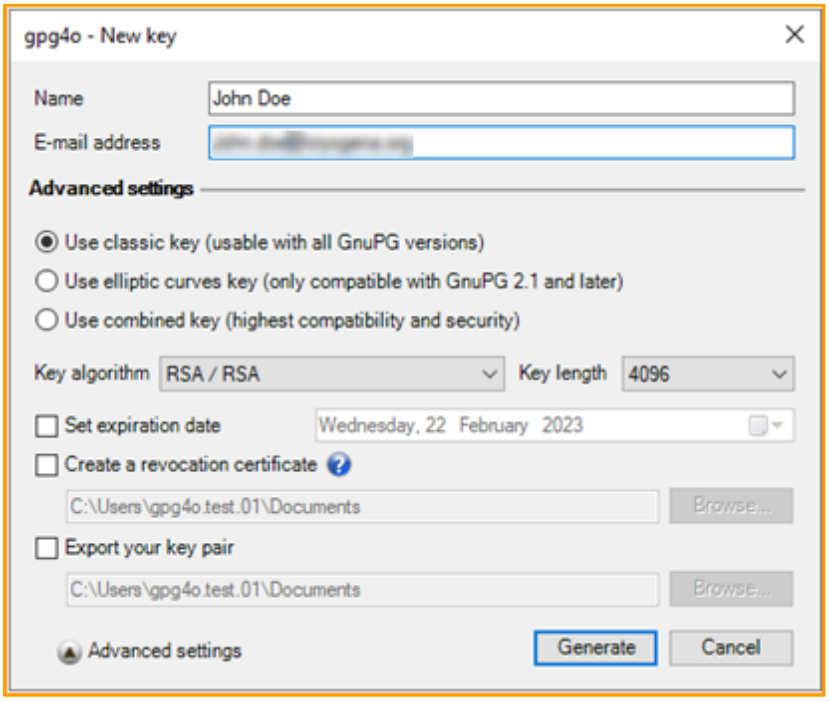
5.2.1 Basic Configuration

On this page, in addition to the installation of GnuPG, you have the possibility to import a backup. This is useful for restoring a previous configuration of gpg4o and the keys after reinstalling the operating system or changing computers.

For information on creating a data backup, see chapter 11.7.1.

5.2.2 Key creation

In the mask for key creation, you can see additional settings via the button “Advanced settings”.



Here you have the opportunity to influence the algorithms and the length of the key. The standard setting is already providing a high level of safety, however.

You can also specify an expiration date for the key. After this point in time, the key can no longer be used to sign or encrypt messages; decryption remains unaffected.

It is also possible to create a revocation certificate, which is important in case you forget the passphrase, lose access to the keypair (data loss) or if it falls into the hands of another person.

Attention: Please keep this certificate particularly well protected, as **no** passphrase is necessary for importing the certificate. Thus, any person in possession of this certificate can permanently and irrevocably make the keypair unusable!

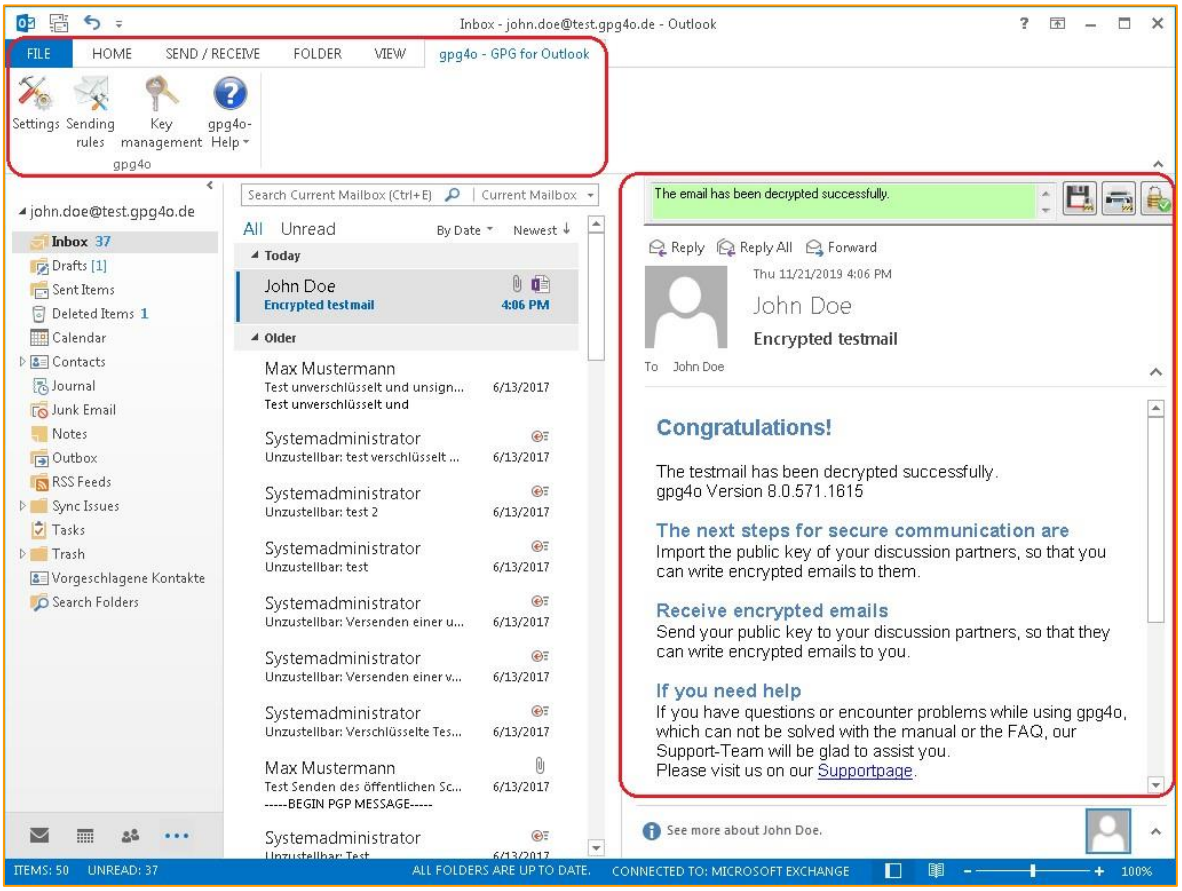
For more information on revocation certificates, see chapter 8.12.

Finally, you have the possibility to export the keypair. This data backup should be kept in a very secure manner. Note also that the exported keypair can only be used with the passport phrase that was entered during creation.

6 First steps with gpg4o

6.1 Overview

After successful installation of gpg4o you will see a new tab “gpg4o-GPG for Outlook” in Microsoft Outlook. There, you will find the settings of gpg4o, the sending rules, the key management and the gpg4o help.



If the email preview is enabled in Outlook, the encrypted or decrypted email is displayed in this area. This preview area is extended by gpg4o with an area for additional information and actions.

Detailed information about decryption and signatures are displayed on the left side of the preview. The text box is colored green if the decryption/signature check was successful.

Depending on the email message displayed, the following buttons/symbols may appear on the right-hand side:

Disk

Decrypts the displayed email permanently.

Printers

Prints the decrypted email displayed.

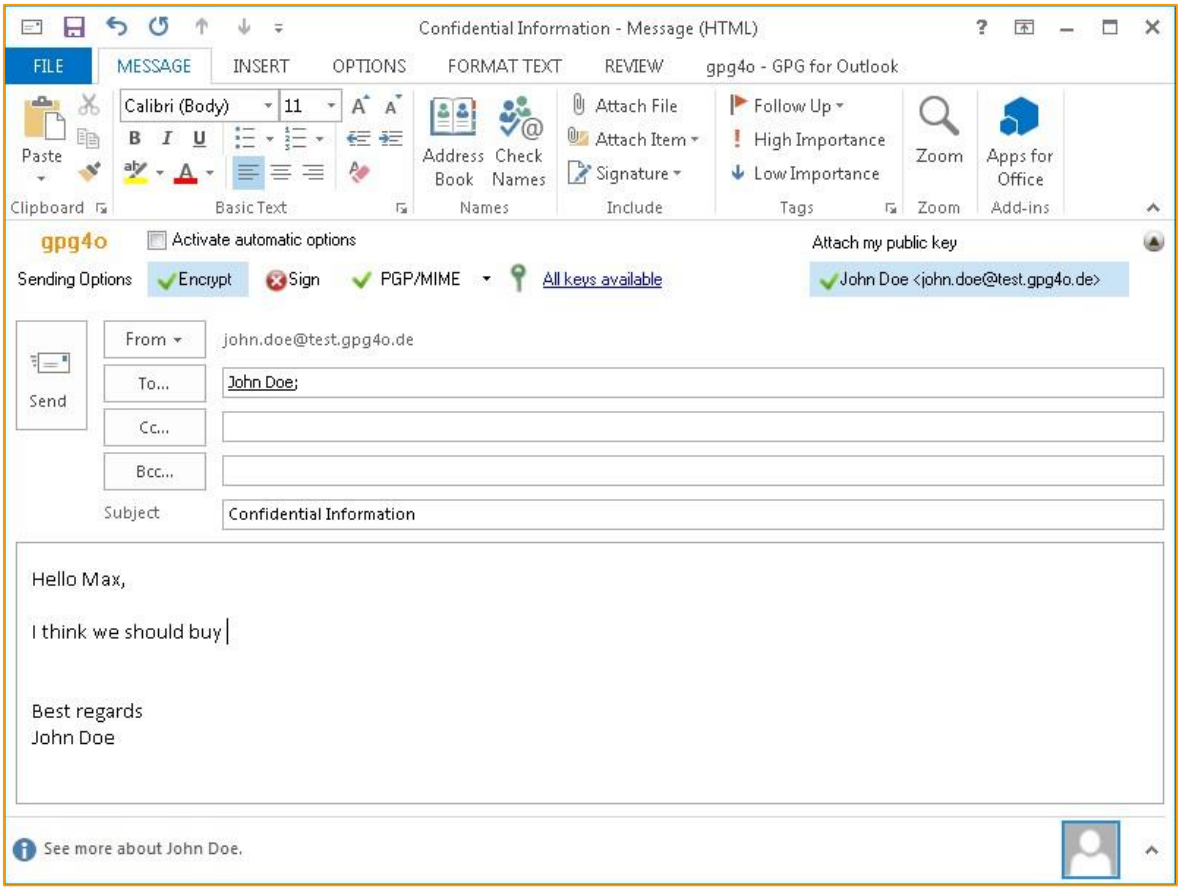
Lock

Email is displayed in encrypted form / Passphrase will not be cached.

More information on the symbols can be found from chapter 7.5.1.

6.2 Read and write encrypted emails

To send an encrypted or signed email, create a new email. The now opened window gpg4o displays a bar on top of it with the „Sending Options“ for this email.



With the buttons in the bar, you can specify for this email whether it should be sent encrypted and/or signed.

The third button sets the desired sending format of the email. These options are available:

- ?
- PGP/Inline
- PGP/Mime
- Encrypt Attachments only
- S/MIME. This function is experimental, and so far not supported.

When selecting "?" you will be asked for the sending format before the email is sent.

"PGP/Inline" is suitable when the recipient is reading his emails with a web browser. In every other case you should chose "PGP/Mime" as it adds more protection to the email.

With the button "Attach my public key" you can send your public key to the recipient. (See chapter 0)

Write an email to yourself, activate the encryption via the "Encrypt" button and send the email. If you have also activated the option "Sign", you will be asked for the passphrase shortly before sending the email.

Once the email has arrived, you can read it in Outlook preview or open it by double-clicking it. If you have sent the email without the option "Sign", you will now be prompted to enter your passphrase to perform the decryption. Once you have sent the signed email, your passphrase is still in the computer's working memory, so that you do not have to enter it again.

Attention: When displaying certain emails gpg4o will display a non-disable able warning, highlighting the issues of the integrity of that email. During May 2018 a security breach named „Efail" was published, which describes how an attacker can, under certain circumstances, modify a non-MDC encrypted email (Modification Detection Code) to guess parts of your private key. Gpg4o can detect these emails and prevents this by not decrypting such emails. In doing so, an attacker can no longer guess your private key by redirecting such emails.

6.3 Encrypt and sign

When you encrypt an email, only the person holding the key can read it. This also applies to the email attachments.

Hint: Please note that the encryption of emails does not involve anonymization, but only makes the content unreadable to third parties. If someone gains access to your email, they can still see who you are communicating with.

When you sign an email, a checksum is calculated from your text and any attachments that may be present and embedded in the email. This allows the recipient to use gpg4o or a similar program to check whether the text of the email was changed during transmission or not.

7 Utilizing gpg4o

After having configured gpg4o and after having generated corresponding keypairs for your email accounts you will now have to send your public key to your communication partners. A keypair consists of two keys: One private-key and one public-key. When generating the keypair you were asked to enter a passphrase for the keypair.

Attention: Never give your passphrase or your private key to another person! Any person coming into possession of your private key will be able to decrypt your emails and to sign new messages with your name. You should keep the passphrase as safe as your other passwords and never tell it to anyone else.

The following brief example shows the general application of gpg4o:

Person A wants to make encrypted communication with person B. He therefore sends an email with his public key to person B and asks for his public key. This key exchange has to be done once for every contact partner.

Person B is now in possession of person A's public key and is therefore immediately able to send an encrypted answer. Person B will now answer the demand, attaching his public key and encrypting the answer with person A's public key.

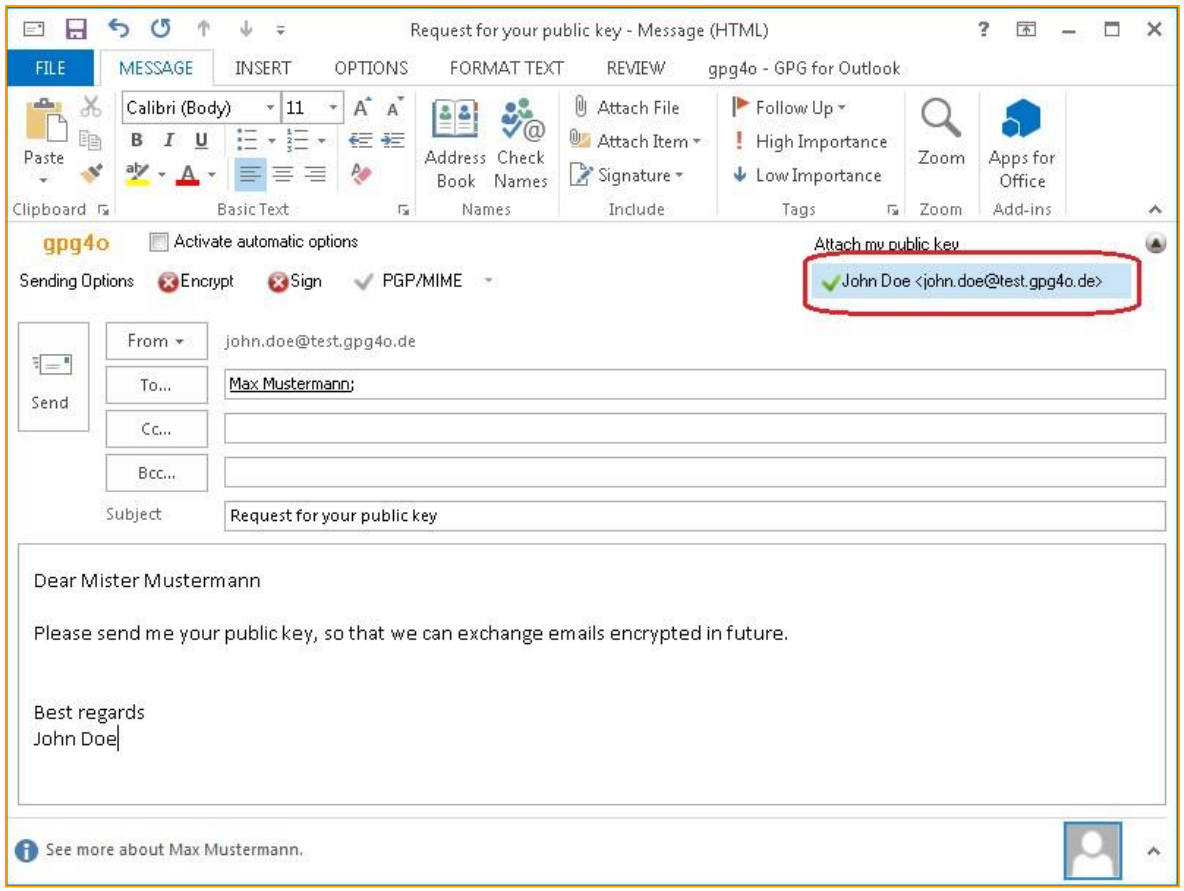
Person A then receives person B's encrypted email and decrypts said email with his own private key. Person A imports person B's public key and is now also able to encrypt to person B.

Hint: In order to be able to still read the emails sent by yourself, your own public key is always utilized to encrypt emails.

7.1 Sending public keys

In order to permit sending you encrypted emails you will have to distribute your public key to those persons which whom you intend to write encrypted messages in the future.

For this purpose, generate a new email and click the button “Attach my public key”. In doing so, your public key will be enclosed with this email as attachment. If desired, place a checkmark in the button “Sign” in order to digitally sign your email. If your communication partner has already imported your public key, it is not necessary to send the key another time.



Please keep in mind that when directly sending emails, the standard options you have chosen will be utilized unless you have defined sending rules (see chapter 10).

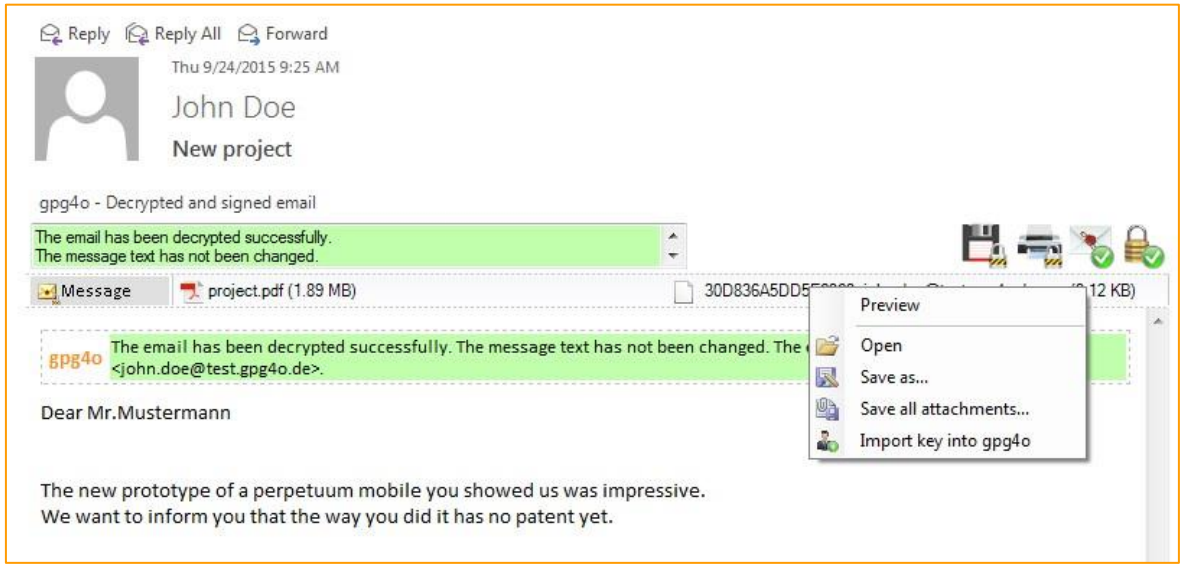
Hint: Pay attention whenever you are sending emails whether they should be encrypted or not.

The public key can be imported by all current encryption tools, which support the OpenPGP standard. It only contains the public part of the keypair, not the private one.

7.2 Importing public keys

If your communication partner sends you a key as an attachment of an email gpg4o now offers you to import this key, as soon as you read this email (see chapter 11.4.2).

If the dialog is not shown you still are able to import the key by right clicking the attachment and select the entry “import key into gpg4o” in the appearing context menu.

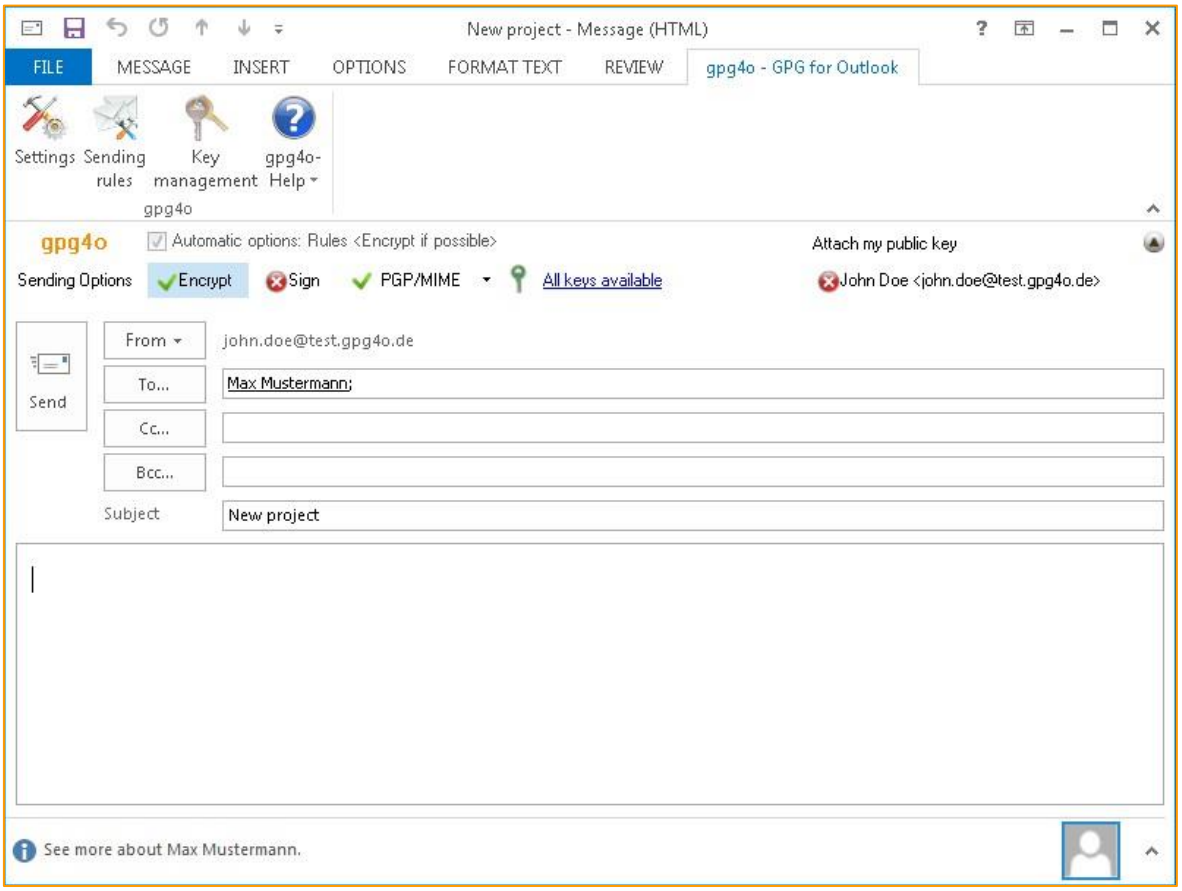


Alternatively, you have the possibility in the key management to import the key from a key server (see chapter 0).

As soon as you have imported the public key, you can send encrypted messages to this person and also verify signatures of his emails. This exchange of the public key must be made once with every communication partner with whom you intend to exchange encrypted or signed emails.

7.3 Sending encrypted and/or signed messages

If you write an email, the gpg4o sending options will be displayed to you under the menu ribbon, where you can choose to encrypt and/or sign the email.



Here, you can define whether your emails shall be encrypted and/or signed and whether your public key shall be attached to the email.

Before sending an email, press the button “Sign” or “Encrypt”, if you want to send it encrypted. If you press both buttons, your email will be sent encrypted and signed.

The third button sets the desired sending format of the email. These options are available:

- ?
- PGP/Inline
- PGP/Mime
- Encrypt Attachments only
- S/MIME. This function is experimental, and so far, not supported.

When selecting "?" you will be asked for the sending format before the email is sent.

"PGP/Inline" is suitable when the recipient is reading his emails with a web browser. In every other case you should chose "PGP/Mime" as it adds more protection to the email.

Hint: Please pay attention that emails cannot be signed when using "Encrypt Attachment only"

Furthermore, the sending options will show you whether you have all required public keys for the recipients of the email. However, this will only be done if the option for encryption is active.

If all public keys for the entered recipients are available, this will be symbolized by a green key in the sending options bar. If you do not have all public keys this will be shown to you by a red key.

If you have entered a key server in the setting „Auto import" (see chapter 11.6.2), the missing keys will be searched for on the indicated server and will be imported automatically into your keyring.

After having written the message completely and having selected the sending options, click "Send" as usual. If there are problems when sending the email (like unusable keys) you will be notified by gpg4o.

If you have selected the message to be sent signed you will now be asked to enter your passphrase. For this purpose, please use the passphrase which you have selected for your key during the configuration of gpg4o.

For all actions requiring the utilization of your private key you will be asked for your passphrase. GnuPG remembers the last entered passphrase for some time in the main memory, so you do not have to input it on successive actions.

Actions requiring the private key are as follows:

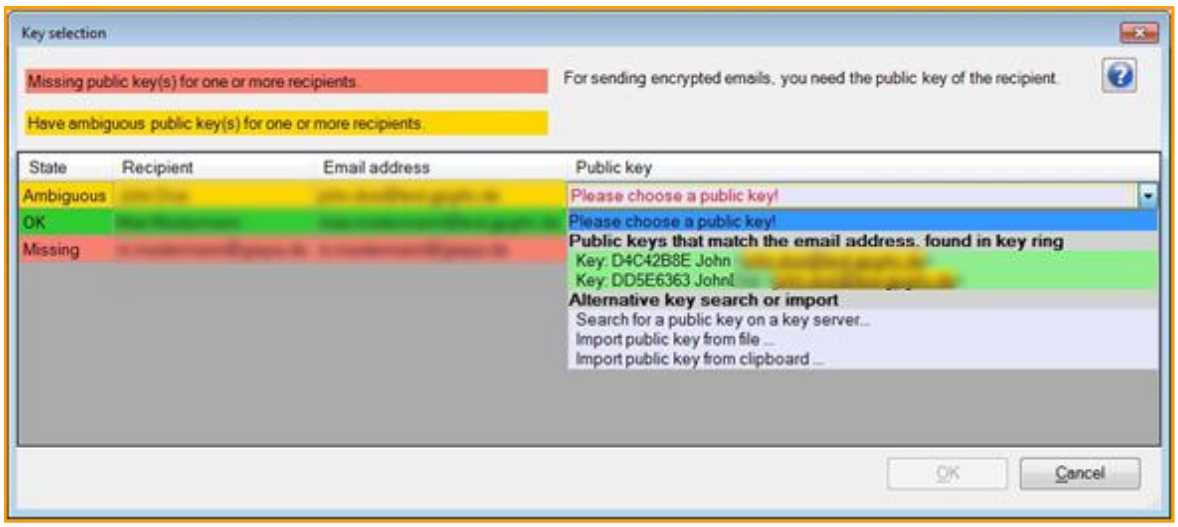
- Signing messages, attachments, or keys
- Decrypting of messages and attachments
- Generating revocation certificates
- Modification of the passphrase
- Adding Identities
- Setting the primary Identity

7.3.1 Manual assignment of keys

While composing an encrypted email it will be shown, if there is an appropriate key available for every recipient. If there is an auto import key server configured, it will be used to search for missing keys and if a suitable key was found, it will be imported automatically.

If no appropriate key was found, neither in your keyring nor the key server, this will be shown with a red key in the sending options panel. If this key is green, then the appropriate key for every recipient could be determined.

With a click on the key symbol or on the text alongside the symbol, the key selection dialog will be opened. Here you are now able to assign a specific key to a specific recipient manually.

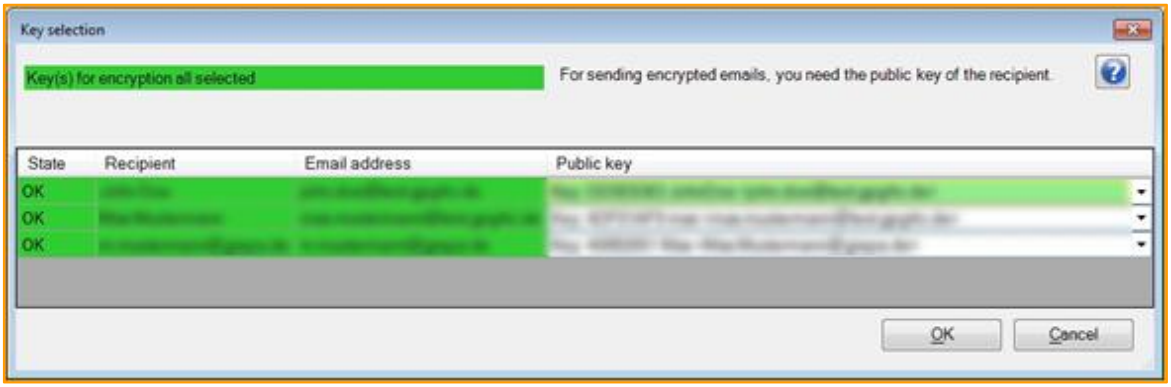


Here the background of the email addresses is colored according to the following system:

- Green: An appropriate key is available
- Yellow: There are at least two appropriate keys available
- Red: No appropriate key available

Now you can assign one or more keys to the different email addresses.

While sending an encrypted email to a list of contacts, you can either give the entire list a key or just set the keys individuals manually.



If each email address has been given a key and none of the lines are marked red or yellow, you can close the Dialog by clicking the "OK" button. The email can now be encrypted and sent.

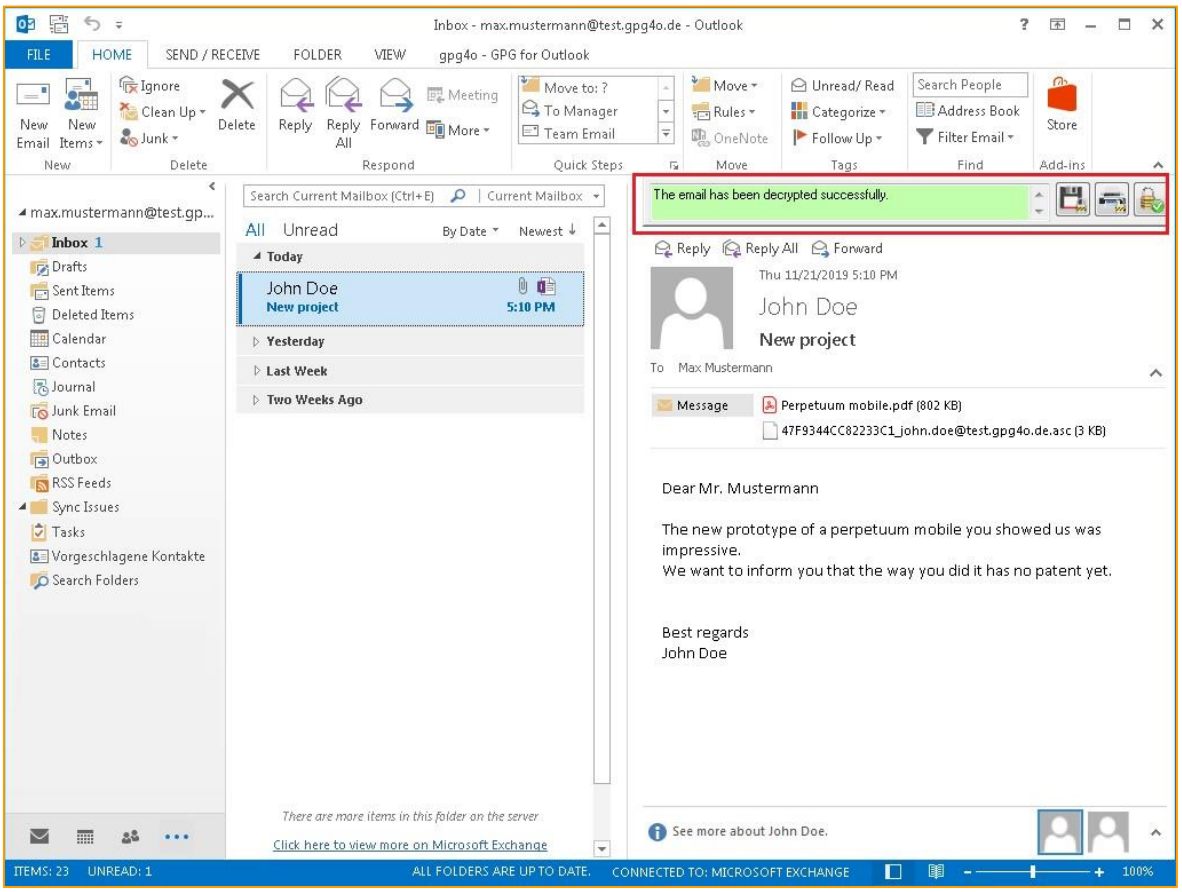
7.3.2 Virtual accounts

While composing a new email you can select from which account you want to send your email, by clicking on the "From" button. For every email address listed there, gpg4o will create a virtual account. This virtual account can be configured in your settings by opening the account management (see chapter 11.3). Therefore, you are able to use gpg4o for every single virtual account.

An account's email address cannot be used for the registration of the license.

Hint: If an email address is deleted inside the "From" field, the corresponding virtual account will be deleted.

7.4 Receiving encrypted and/or signed messages



Decryption status and actions

- Save emails decrypted
- Print preview
- Signed
- Encrypted / Forget cached passphrase

The symbols signalize whether the email was received as encrypted or signed email. Here, certain actions are at your disposal. For example, you may save the message permanently decrypted or open the print preview of the decrypted message (see chapter 7.5). For this purpose, simply click the corresponding symbol.

7.5 Working with decrypted emails

7.5.1 Save permanently decrypted

For simpler archiving gpg4o also offers the possibility to save messages with permanent decryption.

For this purpose, click the symbol “Save email decrypted” in the reading pane of gpg4o. You can now choose whether the email should be decrypted and saved in the Outlook mailbox or as a file on the hard disk.

Attention: If the email is located in a synchronized folder the message will become also readable on the server. You should therefore utilize this function with appropriate caution.

In addition, you can also export all PGP-encrypted e-mails within a folder in decrypted form.

The selected folder is preselected for export. In the following dialogue you have the option to change this selection and to also select the following options:

- Should already existing files be overwritten?
- Should subfolders also be exported?
- Should non-encrypted emails also be exported?
- Should the encrypted e-mails be exported in both unencrypted and encrypted form?

Hint: Please note that this functionality is not available in gpg4o Free.

7.5.2 Printing encrypted messages

For printing an encrypted message, said message has to be decrypted before (see chapter 7.4.

Having done that, you have two possibilities of printing your decrypted message. If you have activated the reading pane of Outlook, you can print the email by clicking the “Print preview” symbol in the preview.

Otherwise, you can also open the email by double-click and print it there as usual with the button combination “CTRL + P” or by clicking “File” and then “Print”.

Hint: In the test version printing of encrypted messages is not possible via the button shown above.

7.5.3 Show encrypted

The email is displayed in an encrypted state, as if no passphrase had been entered for decryption. In addition, the passphrase currently in memory is removed, so that it must be re-entered for further decryption.

7.6 Encryption status of an email

The colored box to the left of the action icons displays information about the validity of the signature and the decryption status.

Four colors are used to quickly capture the status:

- **Green** means that the email was decrypted correctly. If the email has been signed, this color indicates that the message and any attachments have not been modified during transmission.
- **Turquoise** means that the signing key is unknown, or the key has not yet been confirmed/signed. (see chapter 8.10.4)
- **Red** means that the email could not be decrypted or that the message or its attachments were changed during transmission.
- **Yellow** means that the sender address does not exist in the identities of the key.

To determine the status of the signature, gpg4o not only checks whether the message has been changed, but also whether the sender of the email matches the signing key. This verification is performed using the sender's email address and the identities in the signing key.

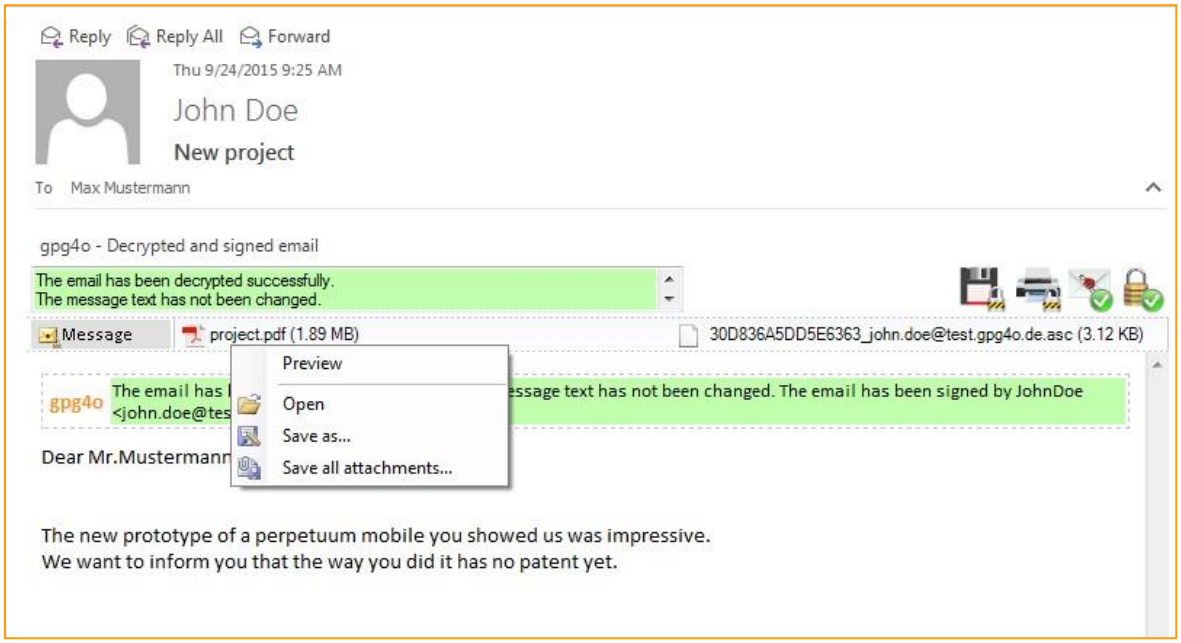
7.7 Import of an unknown key

The ID of a key is shown if no matching key is found in the key ring while checking a signed email. To check the signature of this email you will have to import this key manually by using the ID within the key management. See chapter 0 for more information.

7.8 Send and receive encrypted attachments

As soon as you send an encrypted email containing an attachment gpg4o will do the rest for you quite automatically. You can attach files to your emails as normal without having to worry about the details. As soon as the “Encrypt” check mark is placed all attachments will be encrypted as well in addition to the text of the email.

If you have received an encrypted email with attachment, you can either save the encrypted attachment or open it directly. For this purpose, the context menu (Click right mouse button on the attachment) offers you the options “Preview”, “Open”, “Save as...” and “Save all attachments...”.

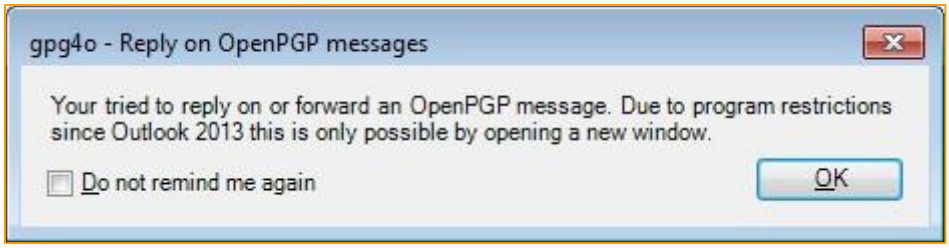


Alternatively, you may also save the attachment in a folder using drag and drop.

With the option “Preview” or with a simple click on the attachment it will be shown in the display as you know it from Microsoft Outlook.

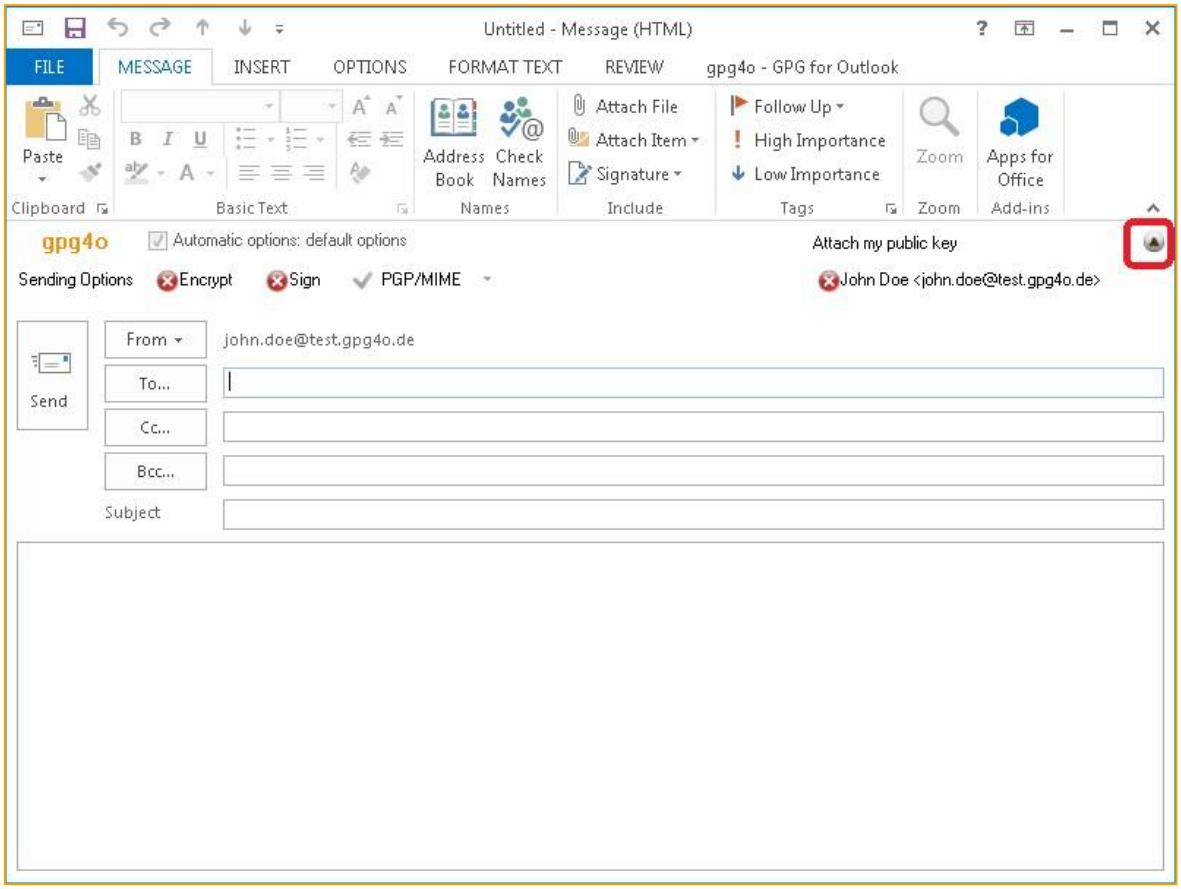
7.9 Reply/Forward emails in Outlook 2013 onwards

If you want to answer or forward an encrypted email in Microsoft Outlook 2013 (or later), the answer to be written will not open in a window of its own by default. Thus, there will not be all functions of gpg4o at your disposal. In order to be able to make use of all functions the email has to get a window of its own. If this occurs gpg4o will point it out to you.



If you do not want to be informed of this fact again place the check mark with “Do not remind me again”. Via the button “OK” you continue the action.

7.10 Hide send options



In order to put more space at your disposal for the email editor you can fold up the sending options or hide them completely.

If gpg4o is enabled for utilization with an account, you can fold up the sending options via the button with the arrow in the right upper corner of the sending options bar and also fold it down again.

The sending options remember the last state so that when creating another email, they will be displayed to you in the same way as before.

If the account is not configured for utilization with gpg4o a button will be shown instead of the arrow with an “X”. If you click on it the sending options will not be shown any longer in the future in case of inactive accounts.

You can undo this in the settings on the page „View“ (see chapter 11.1.2).

8 Key Management

With the key management of gpg4o you can manage the keys generated or imported by you. You can also look at all key details, generate new keys, revoke old keys, delete and much more.

8.1 General information regarding keys

As we often use some OpenPGP-specific terms we would first of all like to give you a brief explanation of those terms.

Every „Keypair“ consists of a private and a public key. The public key is calculated from the private key. Inversely, however, this is not possible. That is why you as a key owner always own the public and the private key, your communication partners, however, only have your public key.

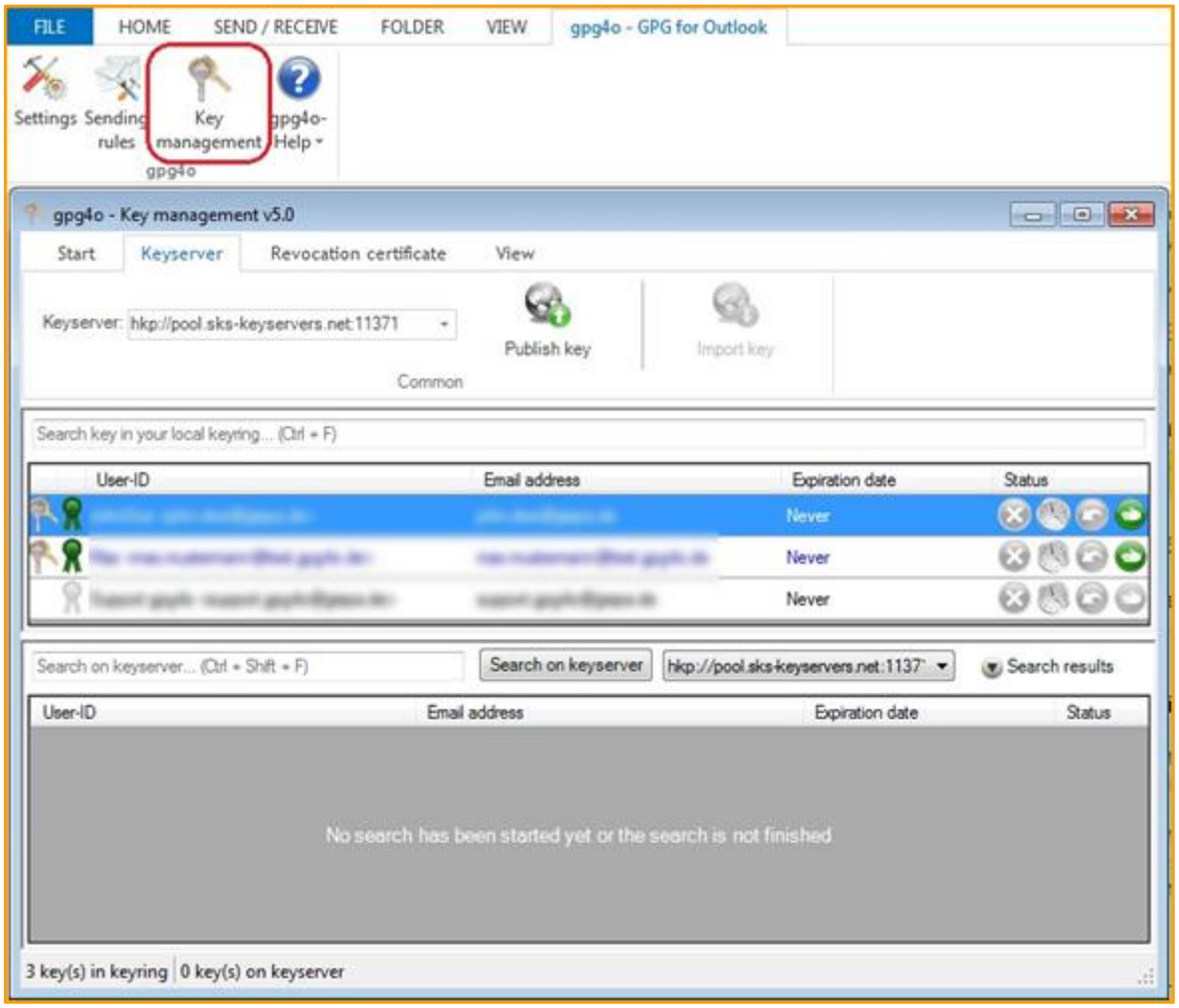
Your communication partners encrypt messages to you with your public key. You then decrypt them again with the private key. For signatures the principle is exactly the other way around. You sign a message with your private key, the recipient checks the signature with your public key.

In addition, every key comprises one „Primary key“ and an optional number of „Subkeys“. If you generate a key with gpg4o one subkey will always be generated as well, other OpenPGP applications, however, can generate a much greater number of subkeys. In gpg4o they will only be indicated for the sake of completeness, for you as a user, they actually have hardly any importance.

Furthermore, a key is provided with one or more „User-IDs“ which corresponds to a description of the key which can be read by human beings. Such a User-ID usually consists of the owner’s complete name and his email address. As one key may have more than one User-IDs it can also be utilized for more than one email address.

8.2 Overview

In order to open the key management of gpg4o please click “gpg4o-GPG for Outlook” in the menu ribbon of Microsoft Outlook and then “Key management”.

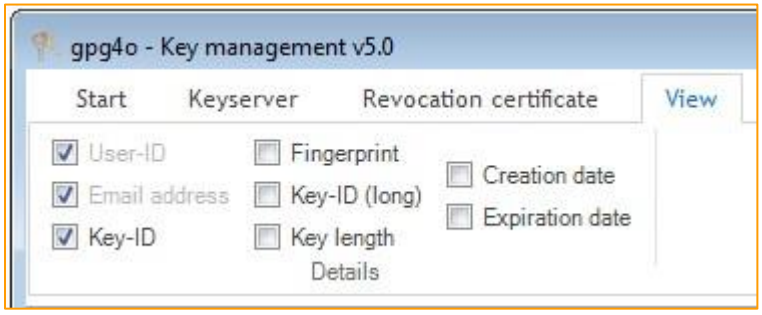


In the overview you can see all the keys which are contained in your keyring. Here, your own keys as well as imported keys will be displayed to you.

Most actions can be performed in several ways. The two most important methods for performing an action are the menu ribbon in the upper section of the key management and the context menu which you get to when clicking the right mouse button on the selected key(s).

Furthermore, many actions can also be applied simultaneously for more than one keys. To this end simply select several keys with the button “CTRL” and select or deselect further keys.

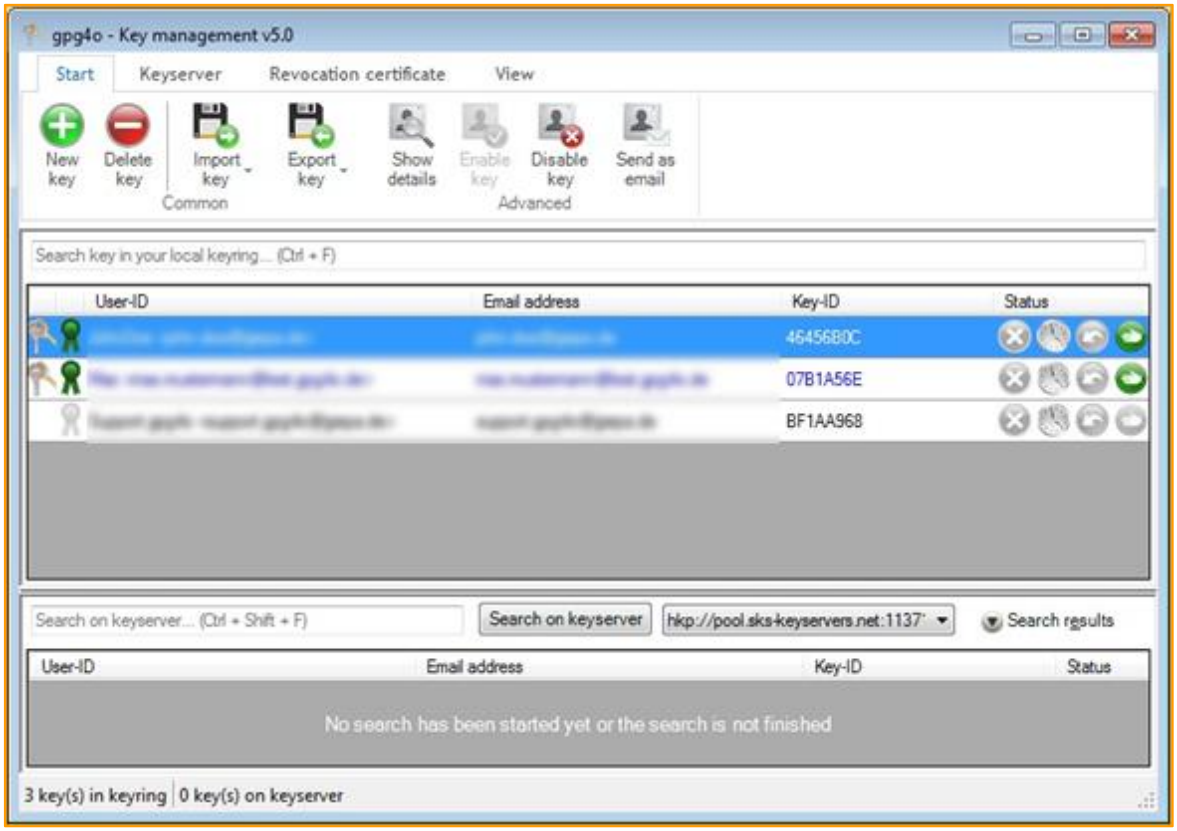
8.3 Modifying view



In the menu ribbon of the key management, you can set via “View” which columns you want to show or hide, respectively.

Moreover, the columns can be sorted. If you want to sort the view by means of a column, simply click the column title. Every further click on the same column reverses the sorting.

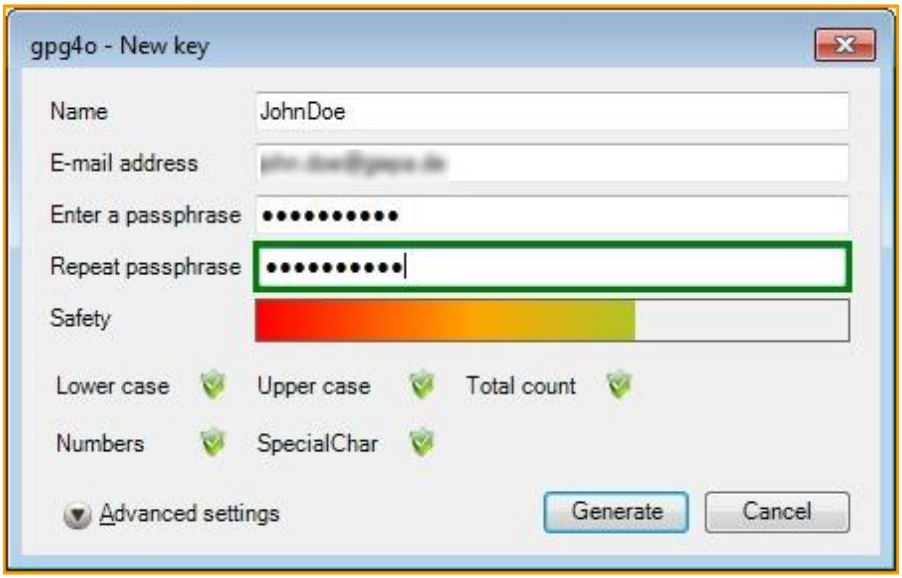
8.4 Filtering keys



In addition, you have the possibility of filtering the view. For this purpose, enter a search term into the field „Search key in your local keyring...“ in order to show only suitable keys. Such a search term may be an email address or a name for example or only a part of it.

8.5 Generating new keys

In order to generate another keypair, please click the option “New key” in the menu ribbon “Start”. In the dialog appearing then please enter the required data as you have already done when configuring gpg4o.



If you want to set further options such as the expire date for the new key, please click “Advanced settings”. As soon as you have entered all required data, click “Generate”.

Hint: The generation of the keypair may take a little time.

8.6 Deleting keys

In order to delete a key, you have to select it and choose the option “Delete key” in the menu ribbon “Start”.

Attention: Please mind that the deletion of a key is irreversible. However, you can import a key again which you have exported before.

Hint: If you delete a keypair, the private as well as the public key will be deleted. If the keypair to be deleted is stored in the gpg4o settings of an account this setting becomes invalid. In this case gpg4o will open the settings dialog after deletion in order to permit you the selection of another keypair.

8.7 Enabling/Disabling keys

If you disable a key, it will not be used for encrypting any longer. This makes sense, if you have more than one public key for the same email address of one contact if, however, you only utilize one of the public keys for encrypting. All further actions will remain unaffected. For disabling one or several keys you select them and click in the menu ribbon on the "Disable key" button. Contrarily, you can enable those keys again which you have disabled before by means of the button "Enable key".

Hint: If the keypair to be disabled is stored in the gpg4o settings for one account this setting will become invalid. In this case gpg4o will open the settings dialog after disabling in order to let you select another keypair.

8.8 Exporting keys

Apart from the sending of your own public key (see chapter 7.1) you can export your own keys or those of your contacts, respectively, here in the key management, too. Choose the key(s) you want to export and click on "Export key" in the menu. You can export the key(s) into the file system or into the clipboard.

An export into the file system is logical if you want to transfer the key(s) to another computer or onto your smartphone. You will be asked where you want to save the key if you have selected "Export key to file...". As soon as you have selected a folder where the key should be saved, please click on "OK".

Copying to clipboard is useful if you want to use the key(s) in a different program, website, or in a blog post without having to use a separate file. If you have selected „Export key to clipboard", the keys are copied to the Windows clipboard, and you can paste the keys into any text field by pressing "CTRL+V".

If one of the selected keys is a keypair (you own the private key), you will be asked whether you only want to export the public key or the private key. This selection is applied to all keypairs of the selection.

Attention: You should never give your private key to anyone else. Use this function only as a data backup or to transport your keypair to another computer.

Tip: You can also export keys to the file system or to an email using drag and drop.

8.9 Importing keys

You can also import a key into the key management. To do this, click on the button “Import key” or „Import key from clipboard”.

Public keys can be published on websites in text form. To import these keys into your own key ring, highlight the text and copy it with “CTRL+C”. Afterwards, you can easily import the key with “Import key from clipboard” and use it.

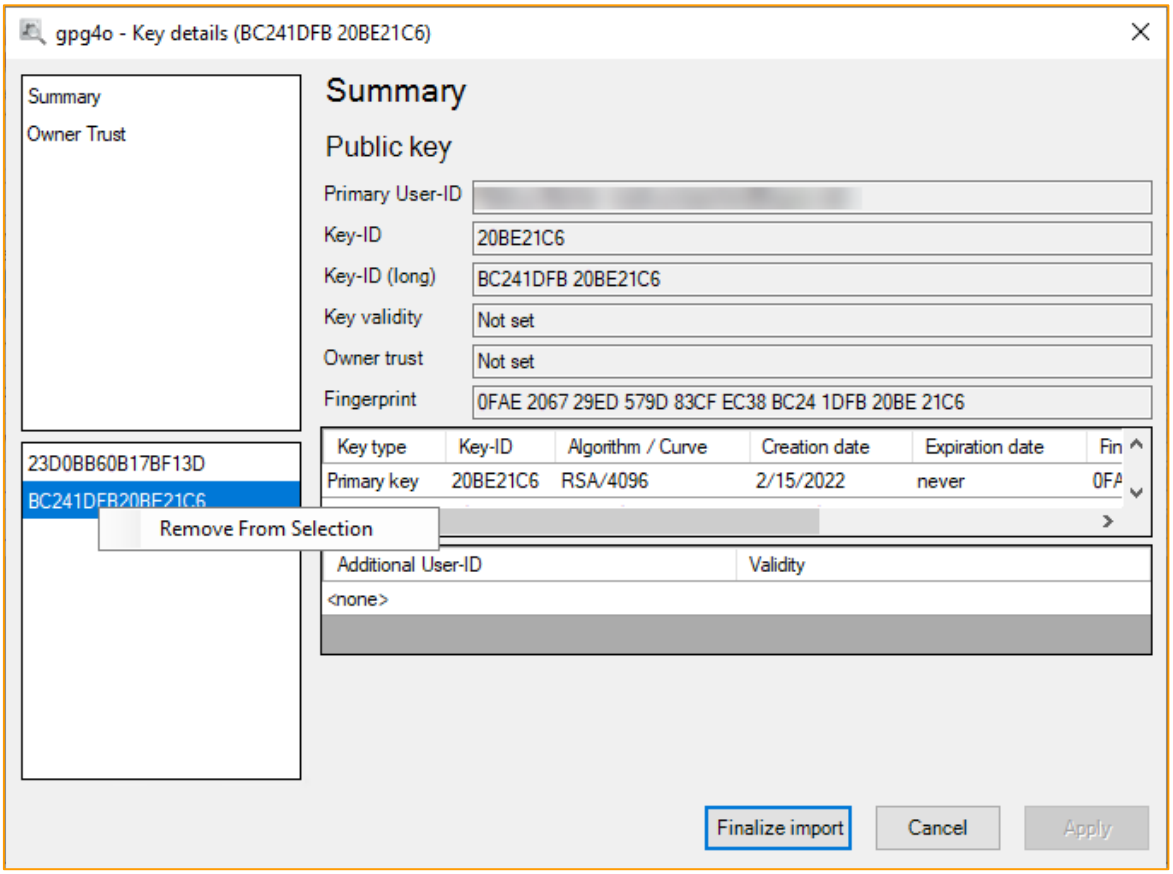
If you have selected “Import key from file…”, a dialog will appear in which you can choose a key file to import. The selected key will be imported when you click “OK”.

Tip: You can also import keys from the file system per drag and drop.

If one of the keys to be imported was issued for an email address for which you have already imported a key, you will be asked again as a precaution whether you want to disable the already existing key before importing the new one.

If the same key is concerned you do not need to have any more worries as differences between the keys will be automatically consolidated.

Afterwards, a summary will appear of the keys to be imported containing all necessary information.



Here, you can still exclude individual keys from being imported, if necessary, by clicking the right mouse button on the key to be excluded and by clicking “Remove from Selection”. You can also determine the owner trust for the key to be imported (see chapter 8.10.6). For this purpose, click the menu item “Owner Trust” first and select the new owner trust for the keys there.

Attention: Please make sure that the key to be imported comes from the person specified as key owner. Get into contact with that person and ask for the fingerprint of that key to be absolutely certain. Please also read chapter 8.10.4 for more information.

In order to finish the import of the key(s), click “Finish”.

After importing you will be able to confirm the identities. Others will thus be able to determine that you confirmed the affiliation of that key to the specified person. For more information, read chapter 8.10.4.

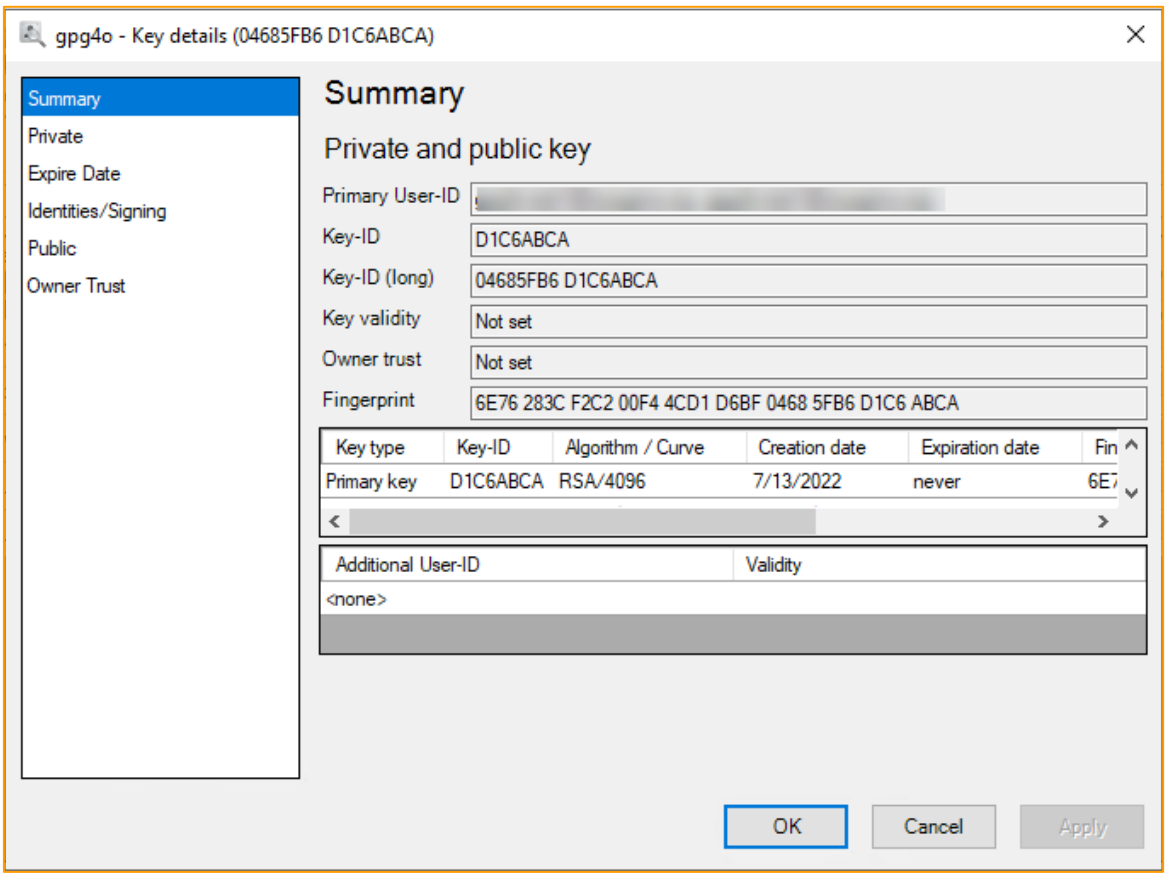
8.10 Key Details

In order to look at one or more keys in detail, you can click “Show details” in the menu ribbon “Start” in the context menu.

The key details have been subdivided into several sections, which are listed on the left side in the menu. The section „Private“ is only visible for keypairs. In order to change to another section simply click the name of the section.

8.10.1 Summary

On the summary page, you can see the most important information with regard to the selected key. The „Key-ID“ and the „Fingerprint“ identify the key, the Key-ID being a short form of the fingerprint. The fingerprint should be synchronized during the exchange of the keys, best by telephone (see chapter 8.10.4).



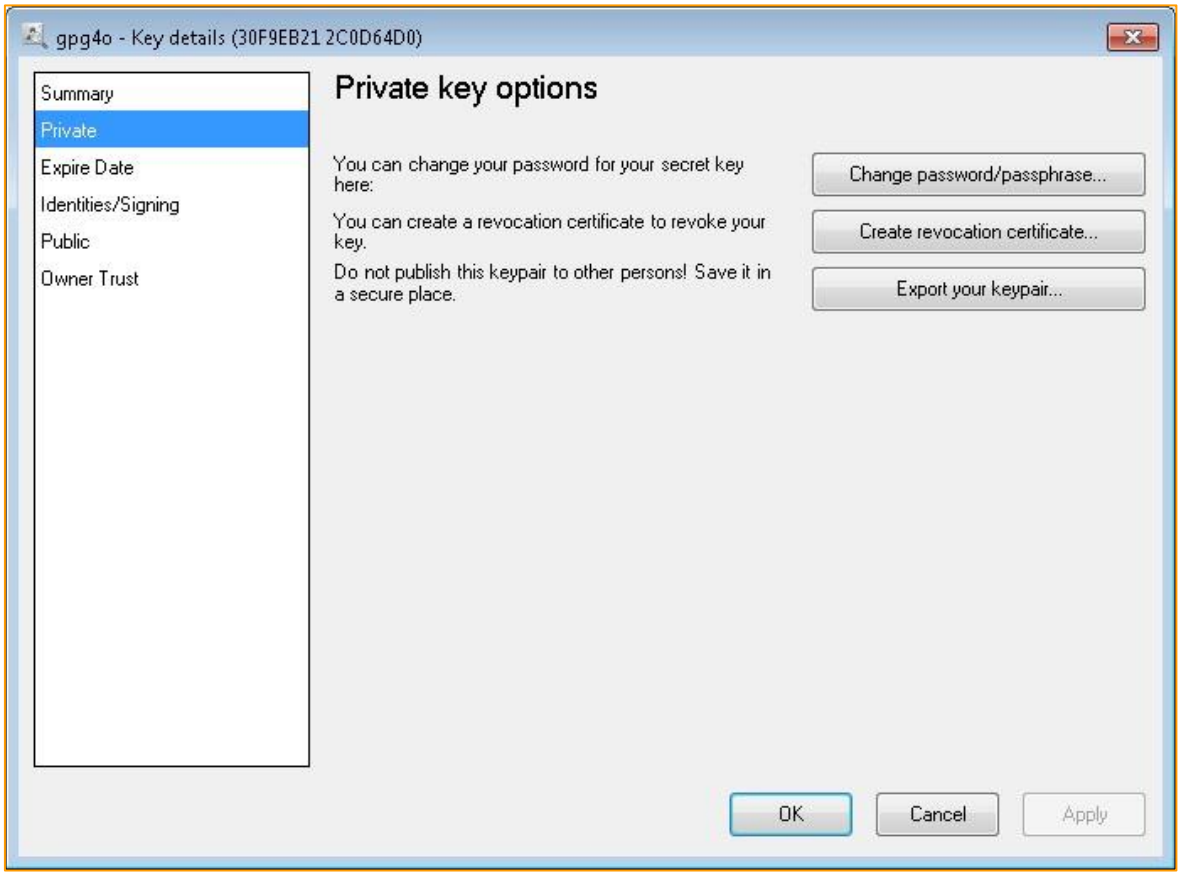
Additionally, the „Owner Trust“ and the „Key Validity“ are indicated. You can define the owner trust yourself (see chapter 8.10.6), the key validity will be determined by means of already existing signatures and the owner trust of the signee.

The term „Key Validity“ means, whether a key has been identified as valid by own signatures or by those of trusted keys. Here, the „Web of Trust“ also plays an important part. A key is valid if it

- Was signed by one of your own keys
- Was signed by another key owner whom you trust fully
- Was signed by at least 3 other key owners whom you trust marginally

8.10.2 Private key

If you open the section „Private“ in the details of a keypair, you can modify the passphrase of the key, generate a revocation certificate or backup the complete keypair.



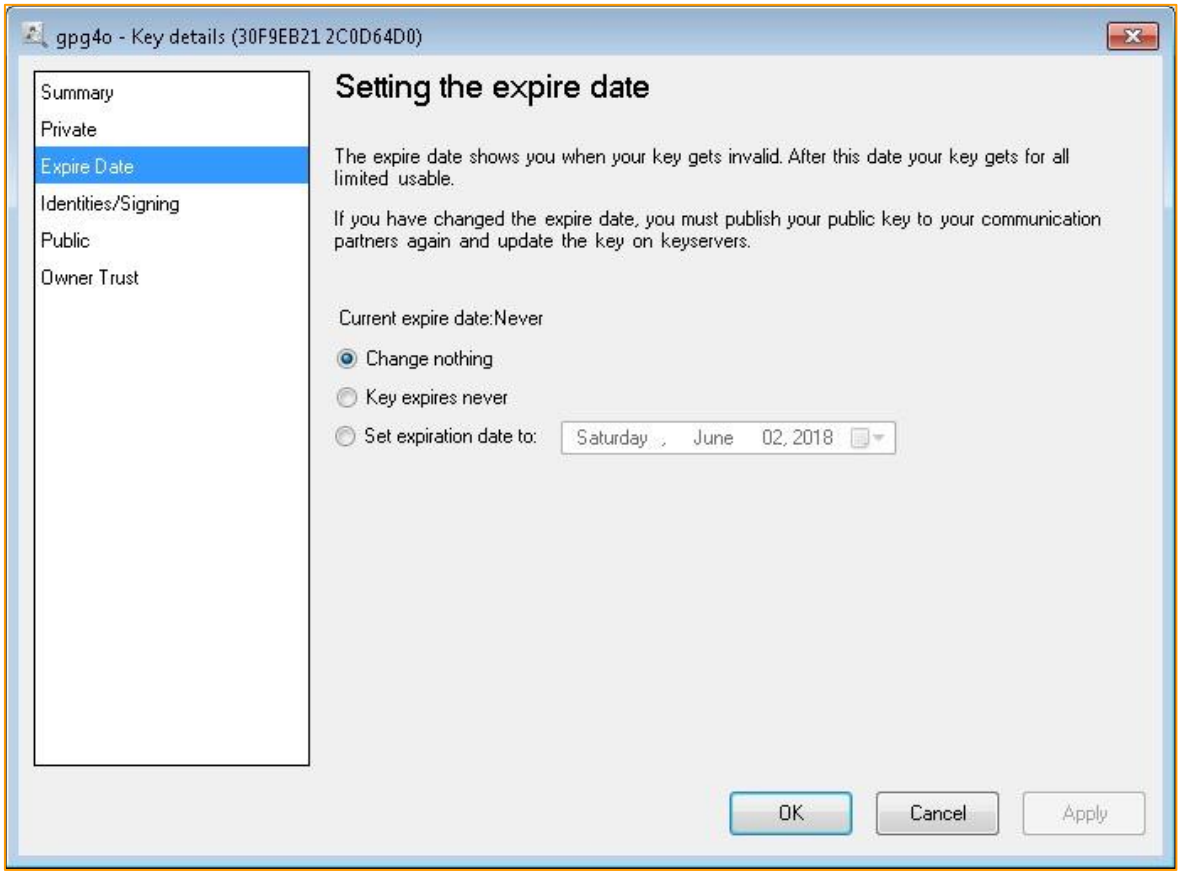
Attention: You should never give the data backup with your private key or the revocation certificate to anyone else.

8.10.3 Expire date

If a keypair was given an expiration date and this date has passed, your communication partners can no longer use your key to encrypt emails and therefore are not able to send encrypted emails.
This is useful if you lost the password for the keypair and don't have a revocation certificate (see chapter 8.12).

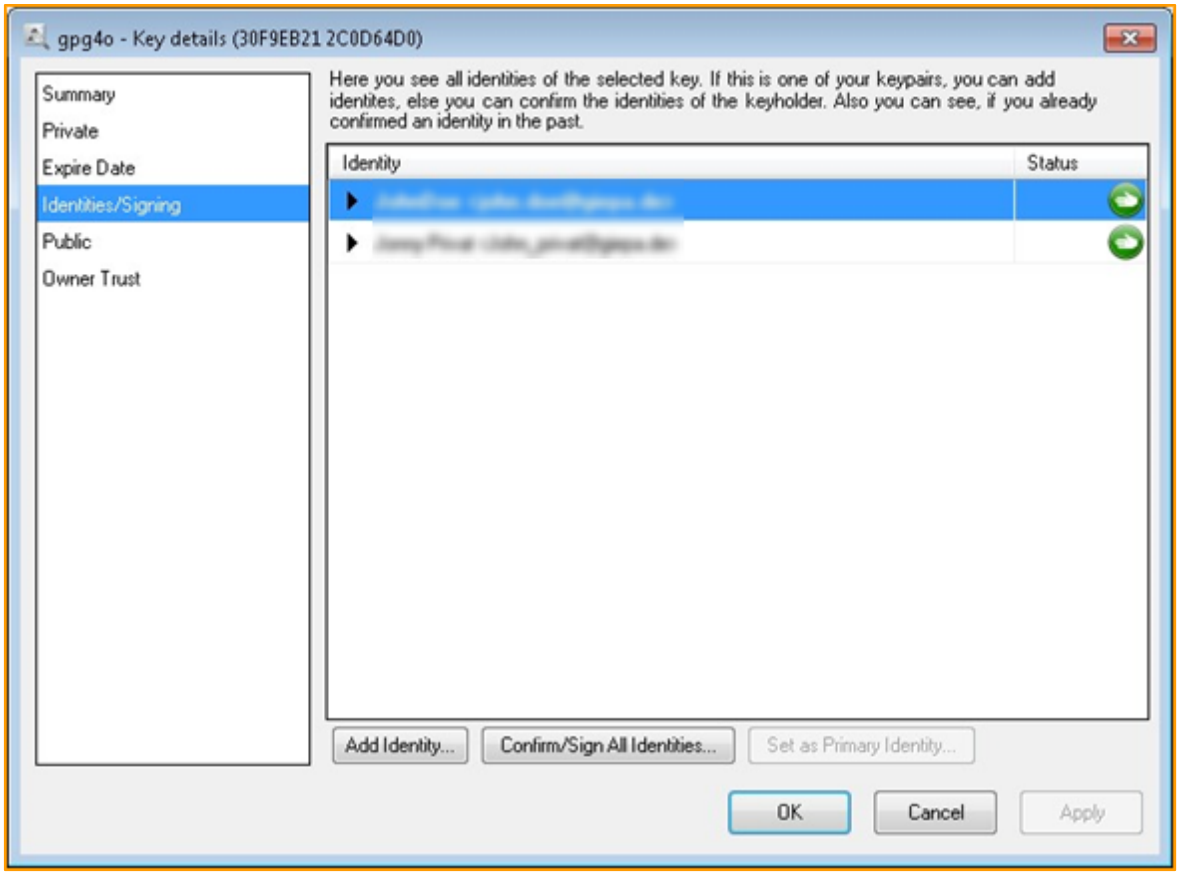
Hint: If you give a keypair an expiration date, you must change the date regularly and send the updated public key to your communication partners.

You can also choose to remove the expiration date by choosing the option "Key never expires". Your keypair will be usable forever.

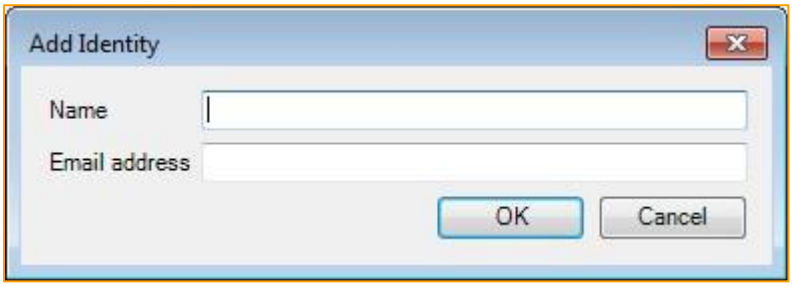


8.10.4 Identities/Signing

In this area, all of the identities (User-IDs) for the given key are displayed. For keypairs, you can add an identity or choose a main identity. For public keys, you can confirm an identity (sign) and hereby validate it.
Keys can be created by anyone with any name or email. It is thus necessary to check any key before using it to make sure it originated from the given person. Details on how to do so can be found below.



To add a new identity to a keypair, click on "Add Identity..." and enter the name and email address for the identity. Clicking on "OK" creates the new identity for the key.



All programs that work with GnuPG, show the primary identity of a key. You can change the primary identity of the key to the currently selected identity by clicking “Set as Primary Identity…”. The selected identity will be the primary identity from there on.

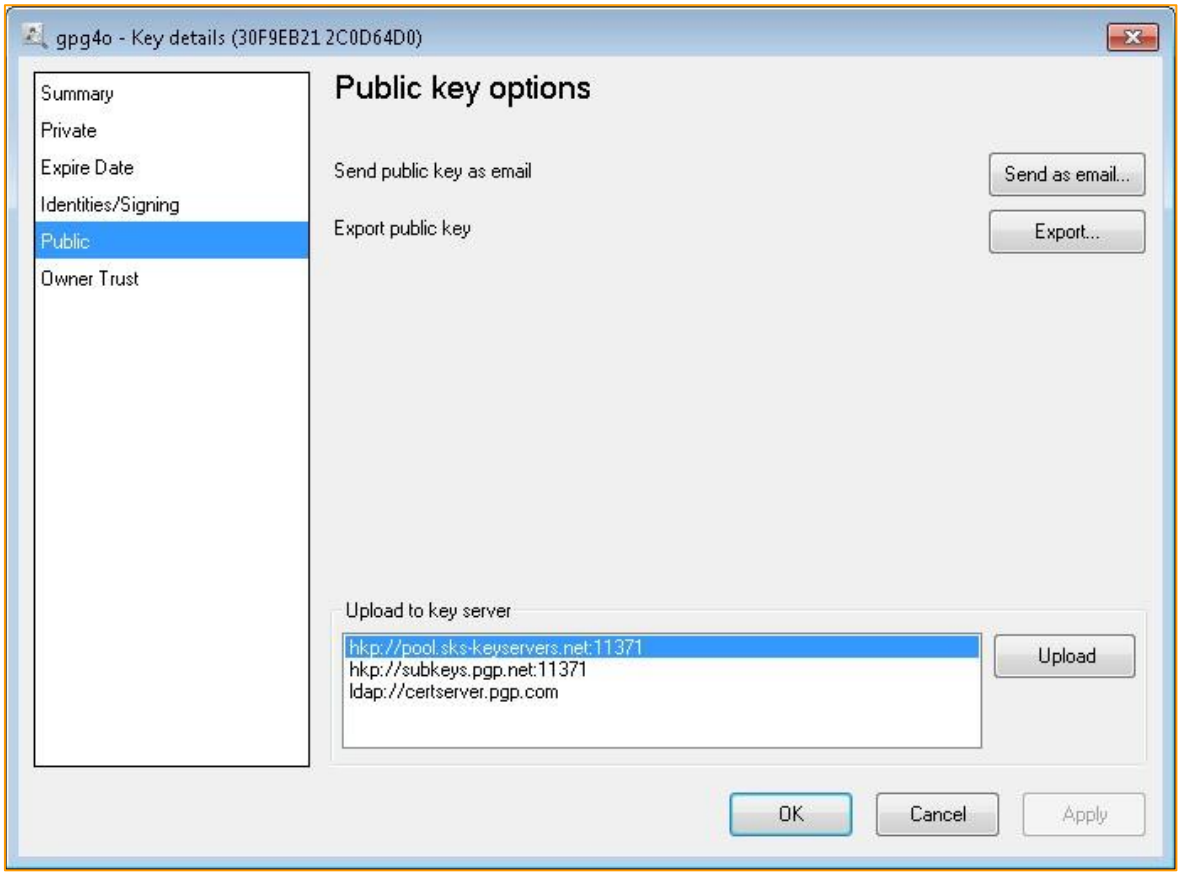
If you want to validate a public key and all of its identities, click on the button “Confirm/Sign All Identities…”.

Afterwards, indicate how sure you are about the authenticity of the signed key. With this selection, the strength of the signature is determined. Clicking on “OK” will apply the signature of the key.

Hint: To be sure that the key belongs to the given person, you should compare the fingerprint personally. You can contact the creator via telephone, fax, SMS, messenger, etc… and compare the fingerprint. Emails are not suited for this verification as they can be faked via „Man-in-the-Middle“ attacks. Only when the present fingerprint is the same as the one given by the key creator you have received the same key and can start using it. If the fingerprints are different, you have received a forged key. Please do not sign or use this key!

8.10.5 Public key

On this page possibilities of how to distribute your public key have been placed at your disposal.

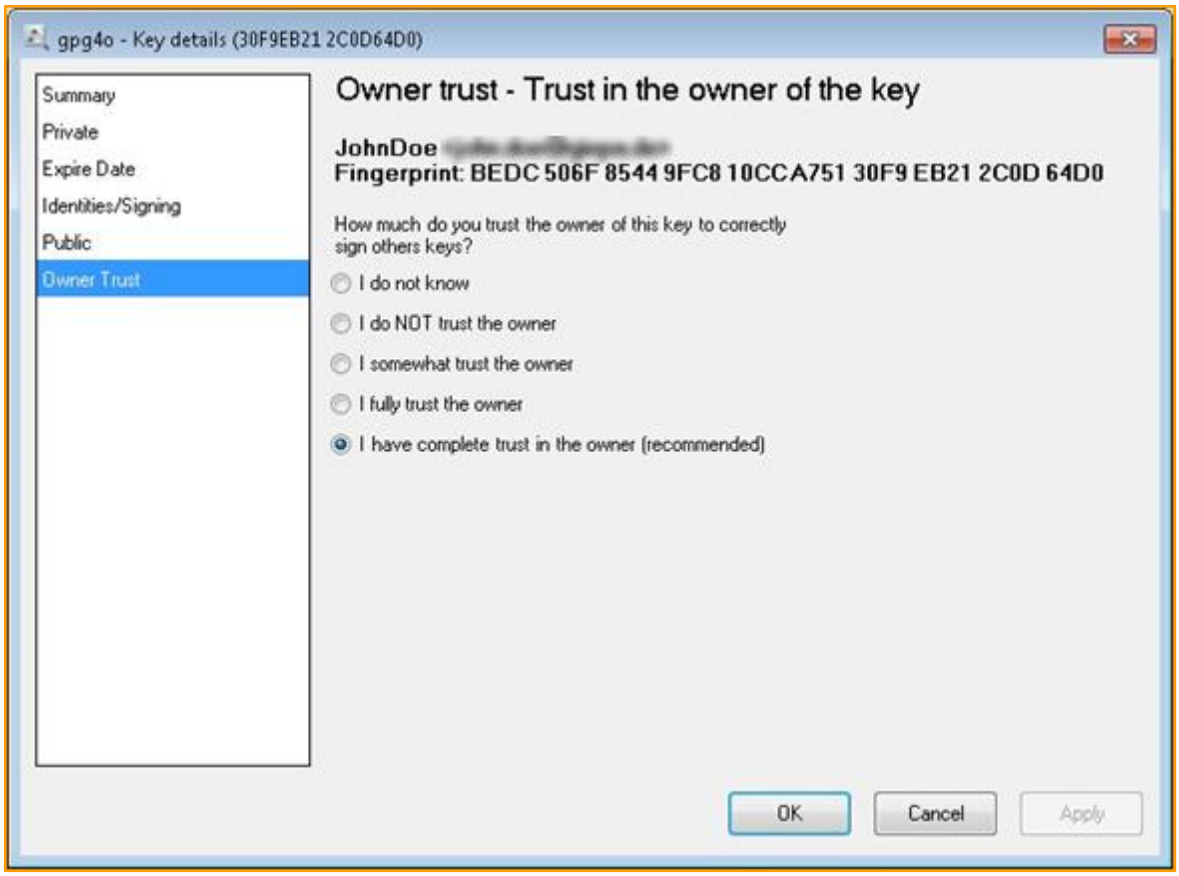


You can send your public key as an attachment to a new email or upload it to a key server from where it can be imported by your contact partners. Moreover, you have the possibility of exporting the public key as a file on your computer or a removable medium such as a USB-stick.

Tip: All those functions are also directly available to you in the overview by pressing the right mouse button on a key.

8.10.6 Define Owner Trust

By means of the owner trust, you can define how much you trust your contacts to sign foreign keys and to classify them to be true. This permits to determine the key validity of other keys on the basis of its signatures. If another key was signed by the issuer of the key, the owner trust of whom you set here will have direct influence on the key validity of the other key. This principle is called „Web of Trust“. In this connection also consider chapter 8.10.1.



There are several selection possibilities at your disposal in order to define the trust in this contact. You should however only choose the option “I have complete trust in the owner” for own keys, as this option will have another influence on the key validity as it is not intended for foreign keys.

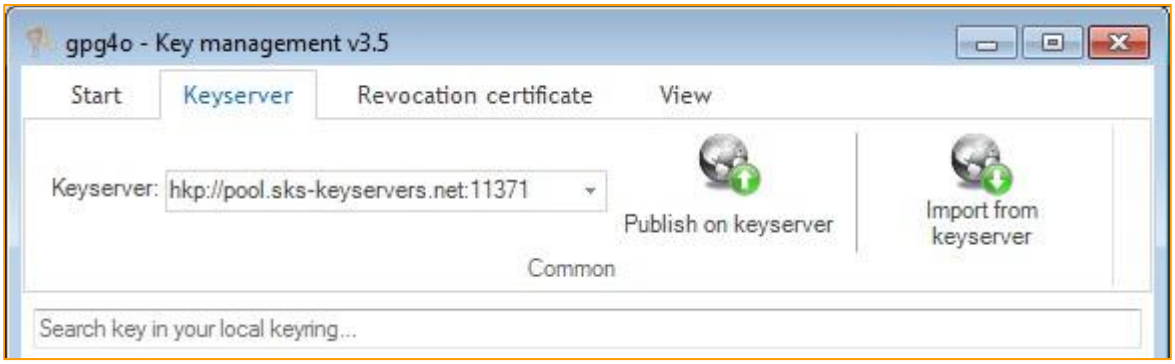
The level of trust indicated by you remains a secret of GnuPG and will, with the exception of the integrated backup function, never be exported or transmitted to anyone else.

Tip: You can also modify the owner trust directly by clicking the right mouse button on a key in the overview.

8.11 Utilization of key servers

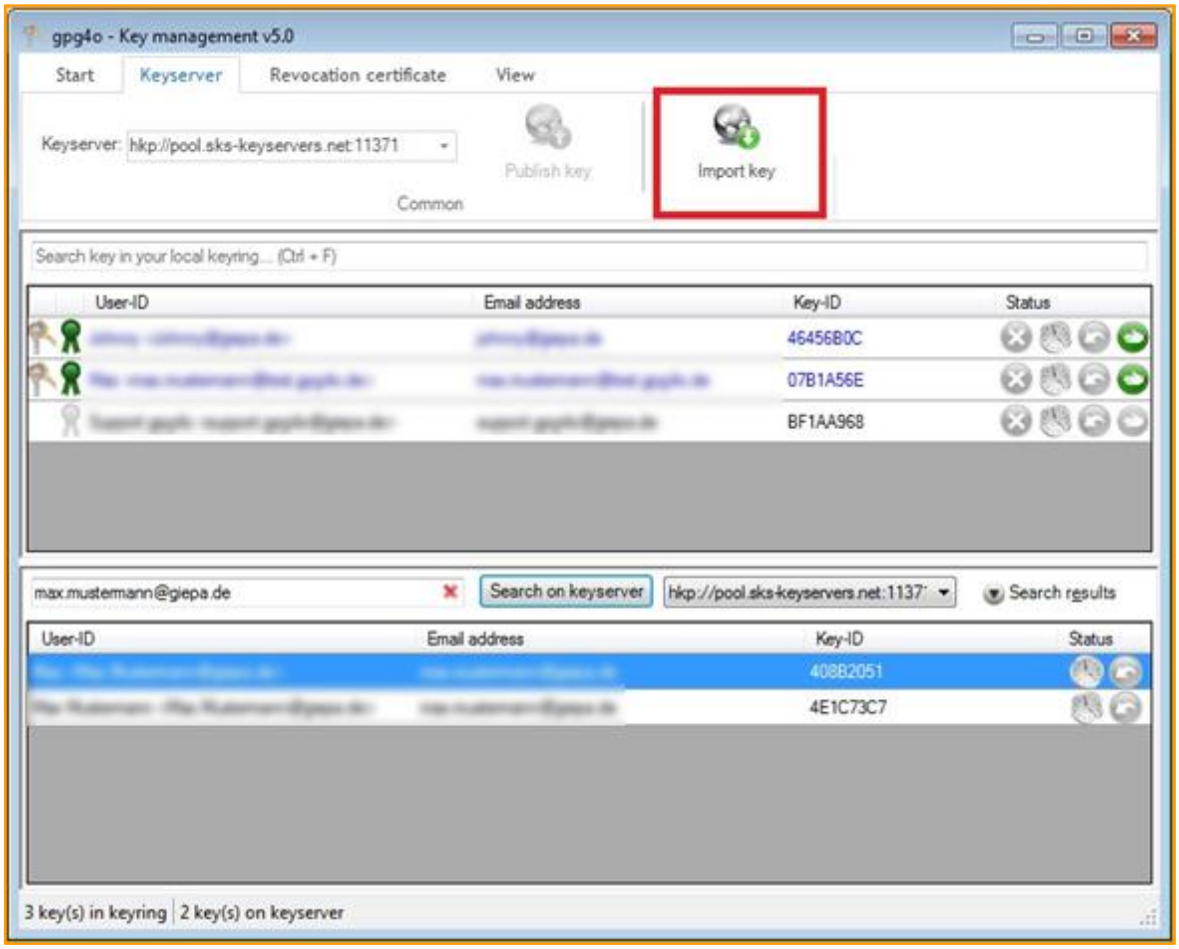
In addition to the possibilities to send keys per email, described in the chapters 7.1 and 7.2, you can also upload your public key on a key server on the Internet and from there also import public keys of your communication partners.

For this purpose, go back to the overview of the key management and select your key.
Change to the tab “Key server” in the menu ribbon and select the key server on which you want to upload your key.



Click the button “Publish on key server” then in order to upload the currently selected key(s).
Now, you only have to inform your communication partner of the selected key server so that he will be able to import your public key from there.

For importing a key from a key server, you can enter your communication partner’s name or key-ID in the search field in the lower section of the key management.



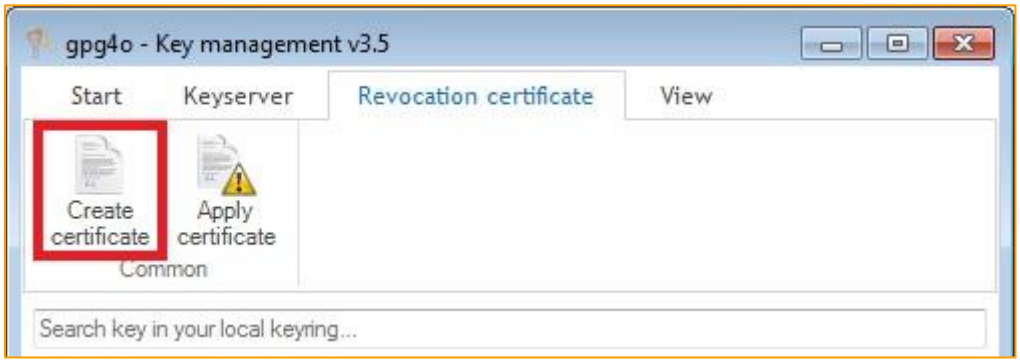
If the searched key is found, you can select it and import it via the button “Import key” from key server.

Tip: You can also import the key via a click on the right mouse button on the key which has been found or by holding the pressed left mouse button and drawing the key into the above list.

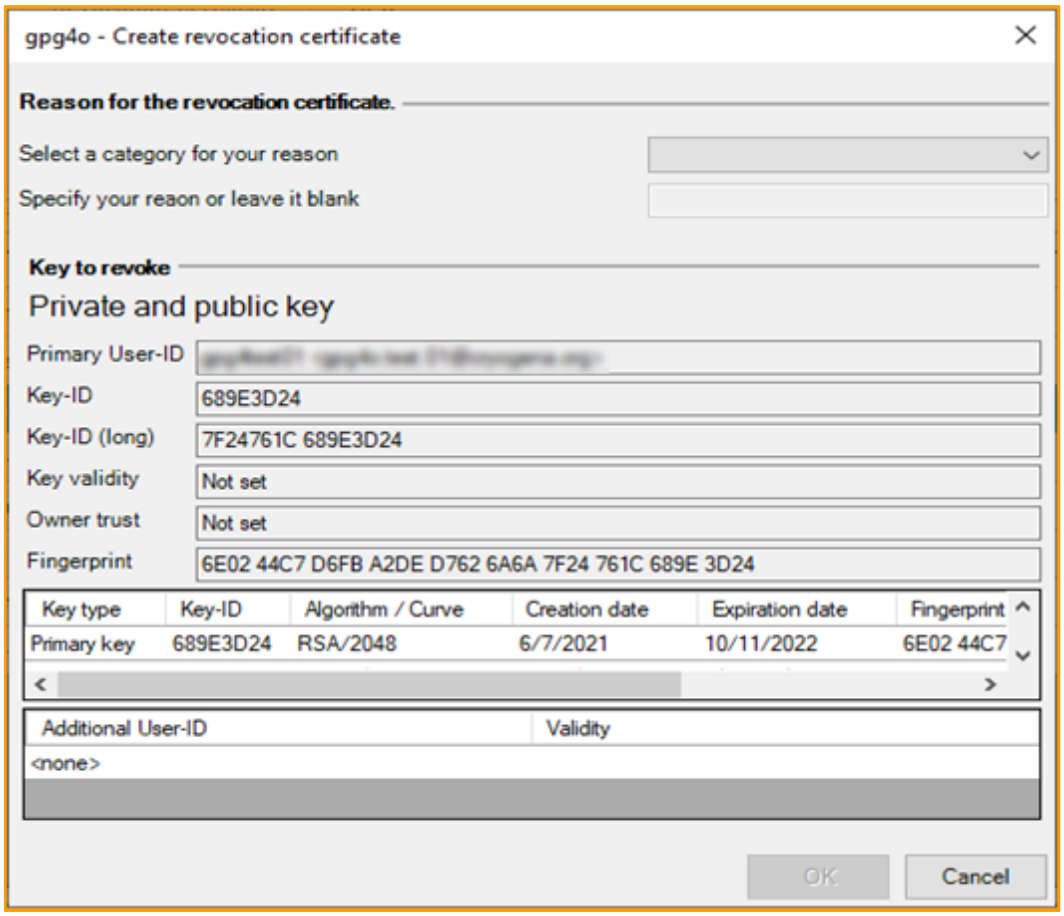
8.12 Generating Revocation Certificate

With a revocation certificate, a key can be permanently and irrevocably declared invalid. With a public key declared invalid, your communication partners can no longer write encrypted emails to you. This makes sense, for example, in case that another person has taken possession of your private key and, thus, it cannot be secured any longer that emails signed with it have actually been generated by you.

To generate a revocation certificate, please choose the corresponding key in the overview of the key management. Then select the button “Create certificate” via the menu ribbon Revocation certificate” in the tab.



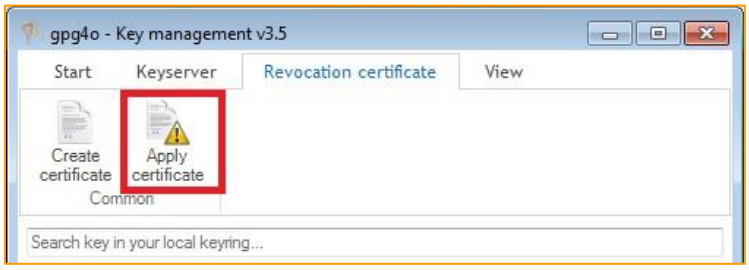
You will be asked for the reason why you want to generate a revocation certificate and can furthermore write a comment on it specifying the reason or furnishing additional information. This can be, for example, the key-ID of the new key which your contact partners shall utilize afterwards.



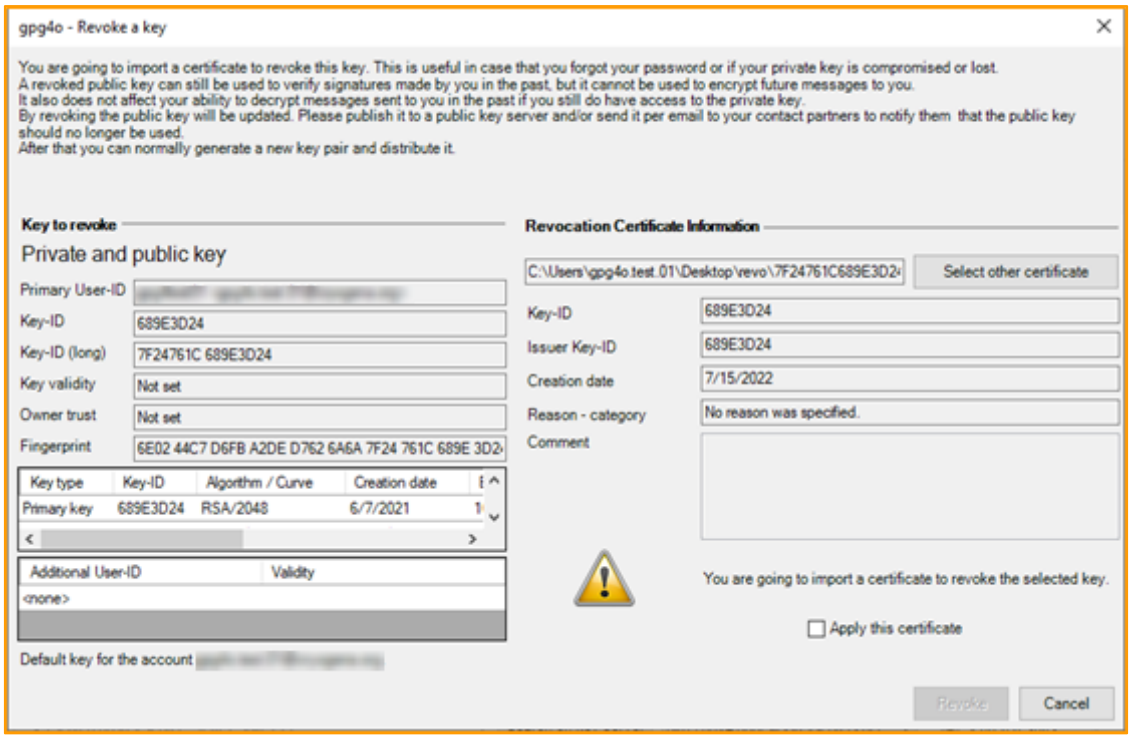
After having entered the reason, click “OK” and indicate the folder where the revocation certificate shall be saved.

8.13 Applying Revocation Certificate

For the revocation of a key, select it first and then go to “Apply certificate” in the tab “Revocation certificate” in the menu ribbon of the key management.



Select the revocation certificate in the appearing file selection dialog and afterwards click “Open”.



First, check the information of the revocation certificate. If you are sure that you want to apply the revocation certificate place a checkmark with “Apply this certificate” and click “Revoke”.

Attention: By revoking, the key is made permanently unusable! Because of the public key is being updated, it therefore needs to be redistributed to your communication partners. If you have published the key on a key server too, you need to upload the updated key again to take effect.

9 Usage of GnuPG 2.1 and later versions

The changes of gpg4o that have been made to adjust to GnuPG 2.1, are described in this section. Furthermore, this section gives important hints on how to use GnuPG 2.1.

Gpg4o Version 5.0 supports GnuPG 2.1. Problems can arise in your key ring due to upgrading to GnuPG 2.1 that are not caused by gpg4o. This is caused by the restructured format of the key ring that comes with GnuPG 2.1.

To keep the changes to GnuPG 2.1 as simple as possible and to avoid losing data in your key ring, it is recommended to follow the following steps:

Please make a backup of gpg4o. (see chapter 11.7)

Change to a stable version of GnuPG 2.1 in the settings of gpg4o and select GnuPG.

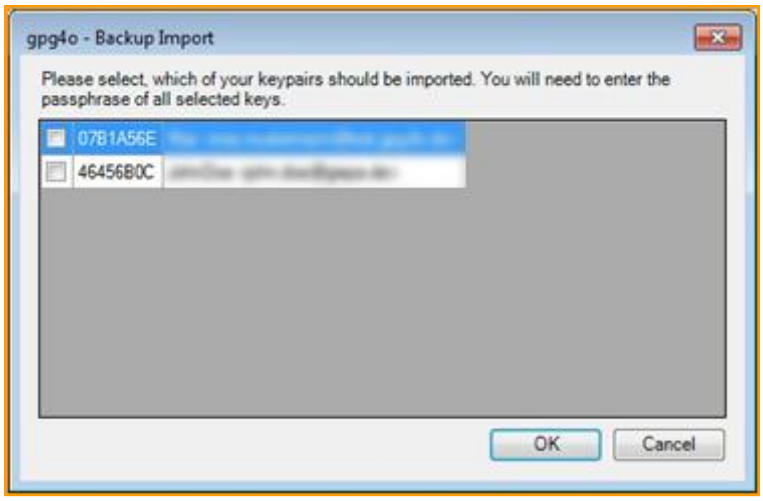
Import the previously created backup.

Hint: Please note that when you import your backup, that you need to have the passphrases of all private keys that are in your key ring.

9.1 Import/Export of keypairs

GnuPG 2.1 requires the passphrase when you are importing or exporting a keypair. Therefore, a following dialog appears for the input of the passphrase, when importing or exporting a keypair through the key management or backup (see chapter 11.7).

In both cases, you need to enter the passphrase for each keypair that is in the key ring. While importing a backup, you will be shown all keypairs and will have the option to exclude keypairs that you no longer need.



While importing a backup, you can choose to import keypairs with help of a selection dialog.

Hint: After switching to GnuPG 2.1, it may be that not all of the keypairs will be visible in the key management. This is caused by because GnuPG 2.1 no longer supports the use of keypairs with old safety mechanisms. In this case, you should create a new keypair based on the current safety standard (see chapter 8.12).

10 Sending Rules

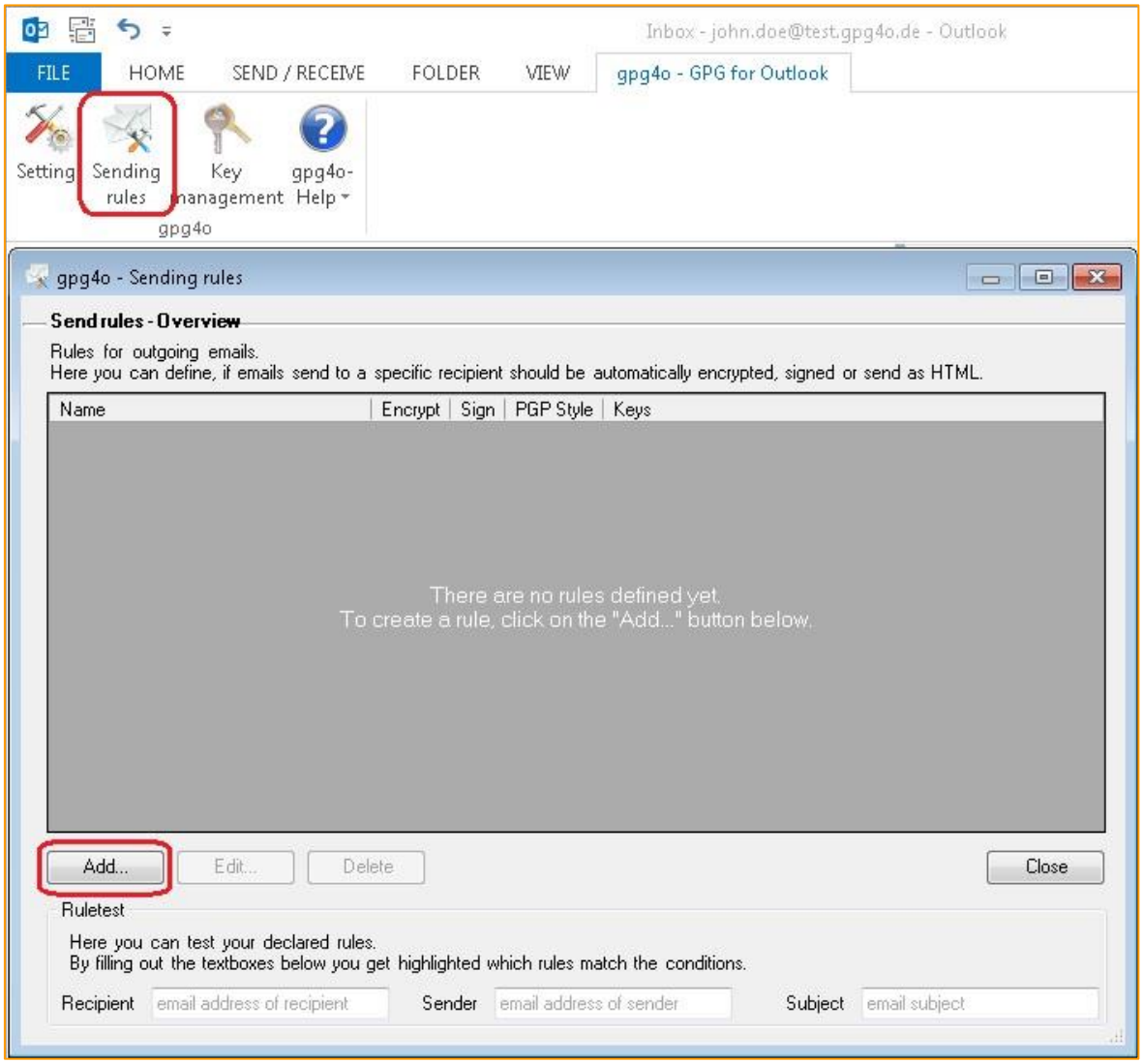
In order to prevent you from having to manually select the settings for encrypting and signing for each of your emails, sending rules have been provided in gpg4o performing this task for you.

Attention: Please not that you can only test the sending rules in gpg4o Free but cannot be used.

10.1 Management of Sending Rules

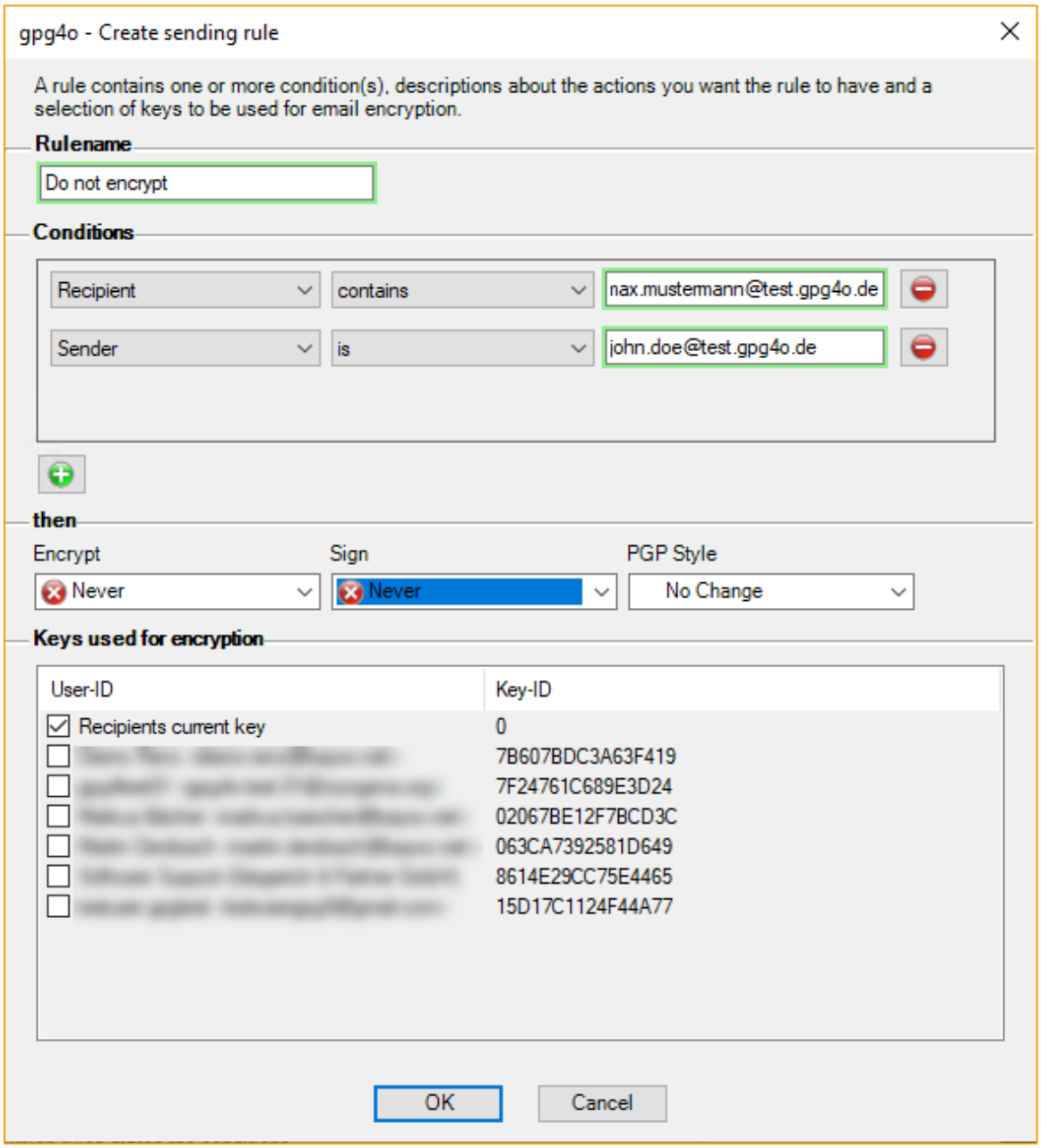
In the overview of the sending rules, you have the possibility of sorting and testing your existing rules without any influence on the rule evaluation.

For that, click. „Sending rules" in the menu ribbon "gpg4o – GPG for Outlook"



For generating a new rule click the button “Add…” in the overview. In the field „Rulename“, you enter an expressive name for this new rule. Having done that, complete the conditions. When working out the conditions, be sure to make them as specifically as possible in order to avoid later conflicts.

Afterwards, you select the encryption options to be utilized and the recipient’s public keys. The keys will be utilized later for encrypting when sending the email if the rule is applied. If you want gpg4o to select the appropriate key for you, leave the selection with Recipient’s current key. Otherwise select the keys which shall be utilized for encrypting the email.



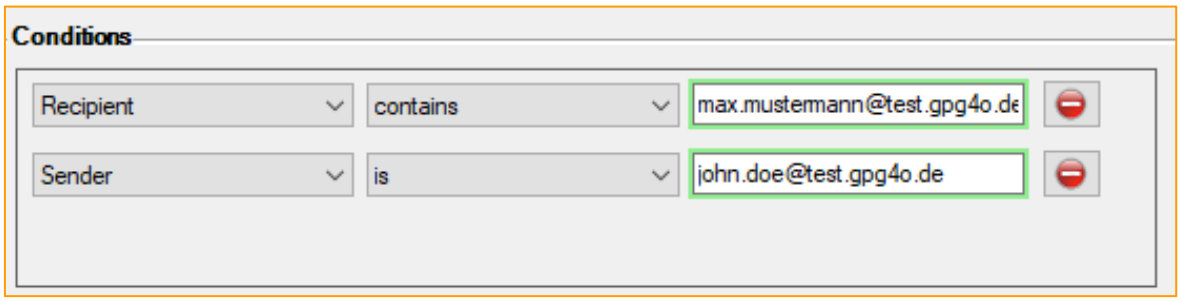
10.2 Rule evaluation

In order to apply a rule when sending an email, all preconditions indicated in the domain „Conditions“ have to be fulfilled.

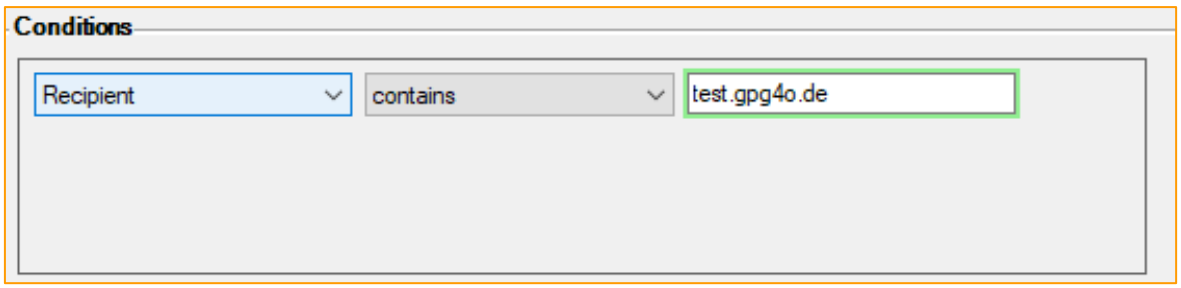
When creating a new email, all your rules are browsed, and all matching rules are selected. This selection is based exclusively on the conditions of the individual rules and not on the classification in the rules list.

The following example shows two rules:

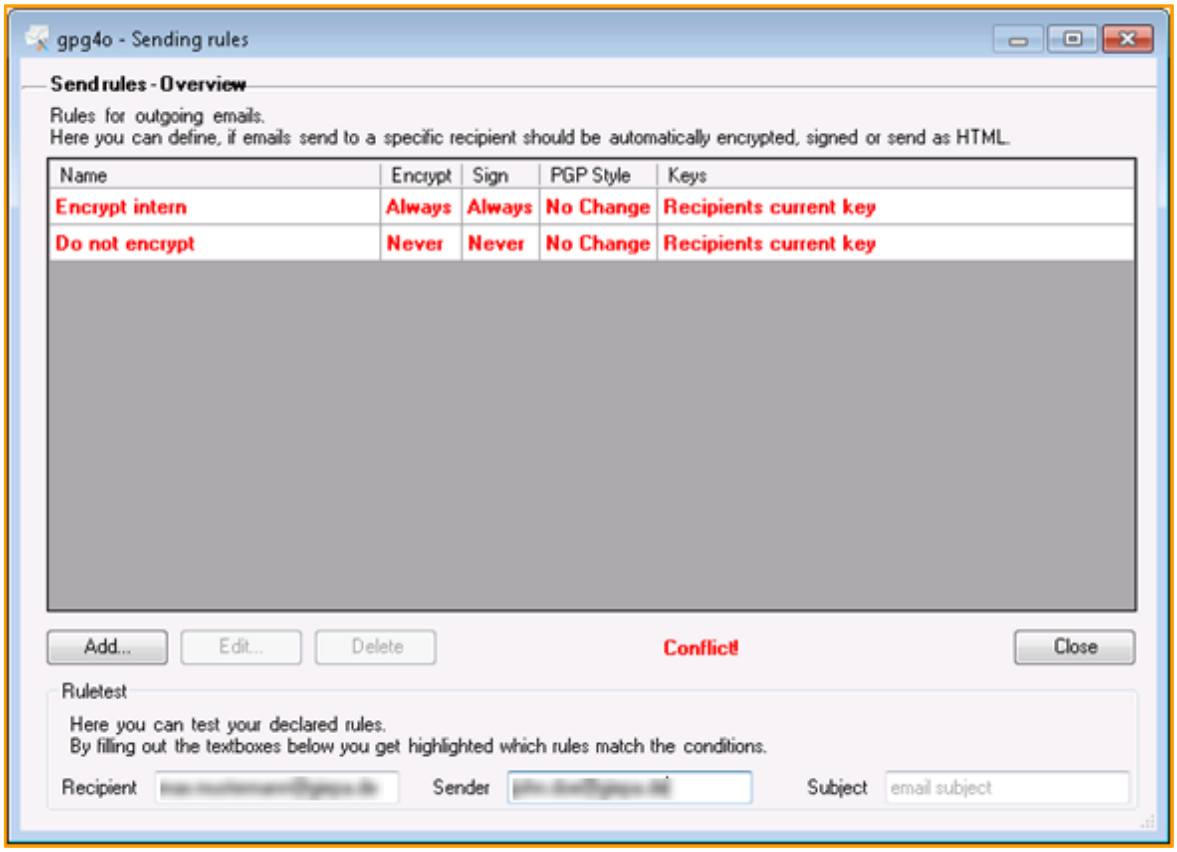
Rule „Do not encrypt“ contains two conditions:



Rule „Encrypt intern“ contains one condition:



If you write an email to **max.mustermann@test.gpg4o.de** now and if you select **john.doe@test.gpg4o.de** as sender, both of your rules will apply. Thus, you will come into conflict as the settings for encrypting within the rules are different.



In order to avoid this conflict in the future, you can add further conditions to the rule „Encrypt intern“:

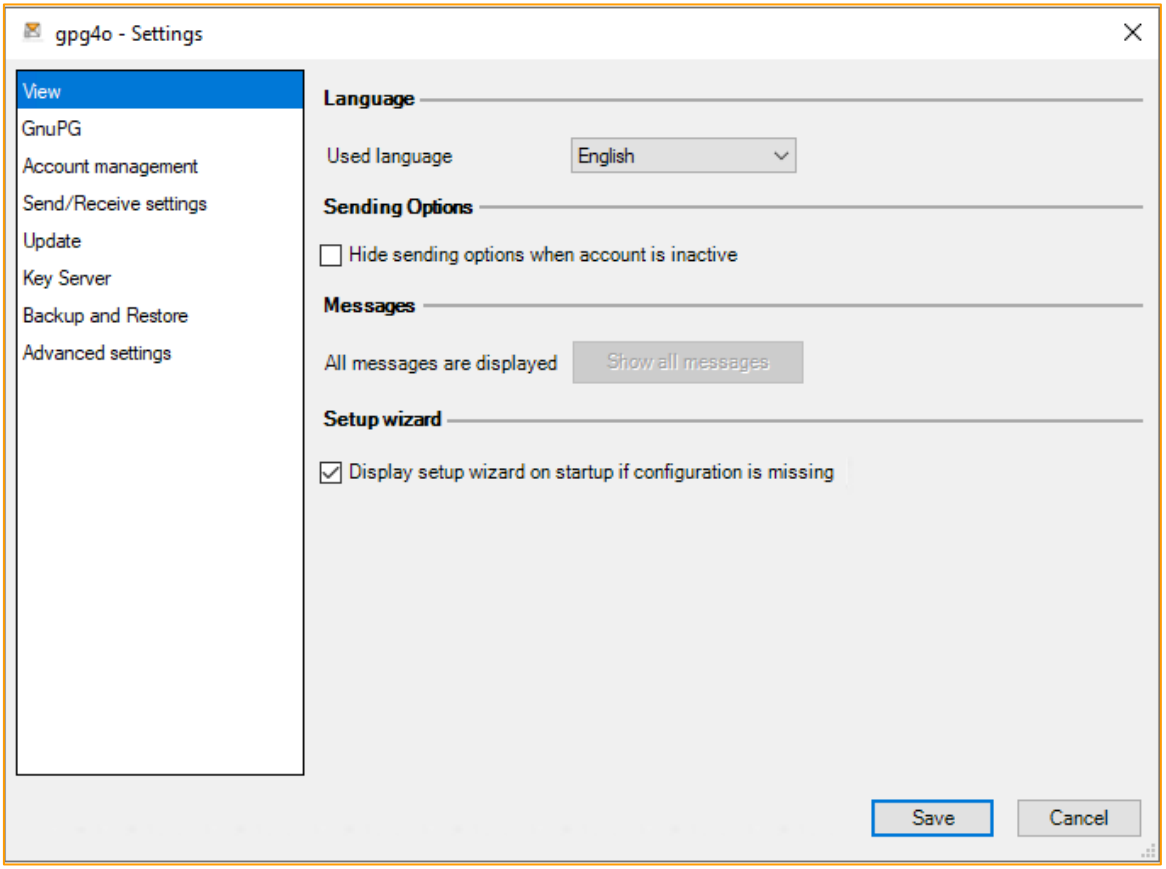
Recipient is not **max.mustermann@test.gpg4o.de**
Sender is not **john.doe@testgpg4o.de**

11 Settings

Through the settings, you can adjust important options of gpg4o. Modifications of your settings, even if you switch between menu points, only become effective after saving.

11.1 View

On this page, the general configuration settings are displayed permitting to adapt the aspect of gpg4o and the integration into Microsoft Outlook.



11.1.1 Language

The language may be adjusted between German and English. Please mind that when modifying the language, the settings have to be closed and opened again.

11.1.2 Sending Options

If this configuration setting is active, the ribbon with the sending options will be hidden when generating an email and the selected sending account has not been enabled for utilization with gpg4o.

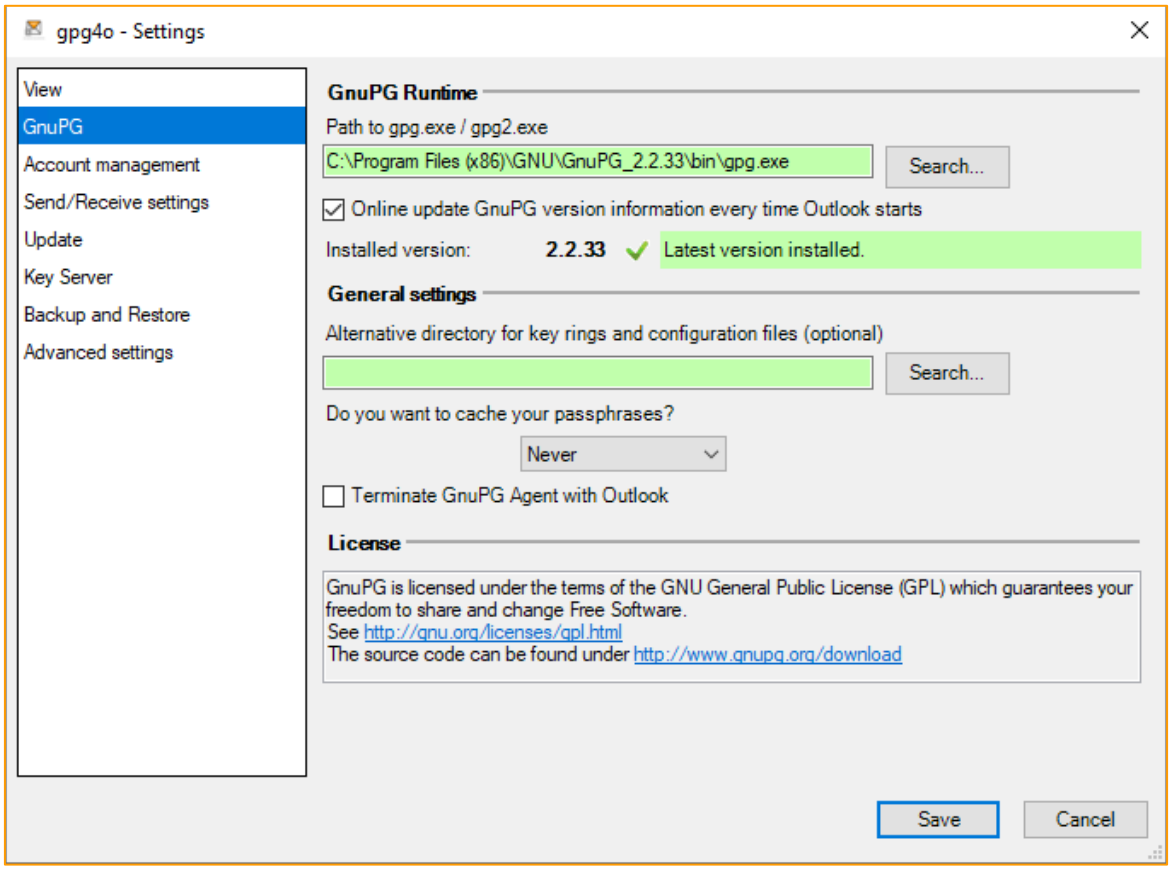
If the configuration setting is not active the sending options will also be indicated in case of inactive accounts.

11.1.3 Messages

As the user, you can decide whether or not you want to deactivate the repeating question so that it does not appear anymore. An example would be the message box which appears when a newer GnuPG version is found online within the start of Outlook. By confirming this through the button, you are activating all deactivated messages again.

11.2 GnuPG

On the page GnuPG, the version and the path to the installed GnuPG are displayed.

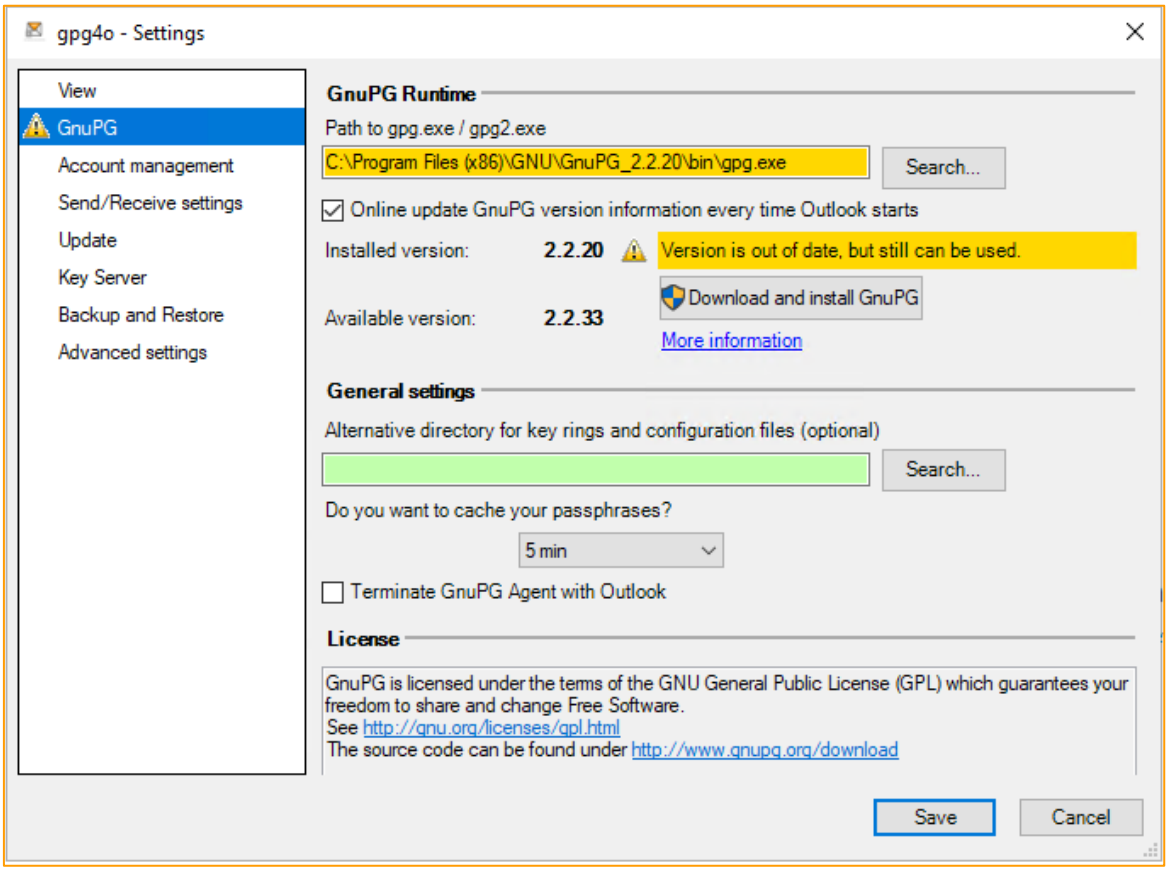


11.2.1 Path to gpg.exe/gpg2.exe

If necessary, you can also convert to other installations of GnuPG with the help of the button “Search…”.

If you have not yet installed GnuPG, the button “Download and install GnuPG” will be shown to you below the version number with which you can download GnuPG from the Internet and install it. Here, the procedure is the same as with the installation by the configuration wizard. Here, you will also find information with regard to the license of GnuPG and you have the possibility of obtaining further information by means of the links, if available.

11.2.2 GnuPG version checking



Gpg4o uses GnuPG to encrypt emails. This program is constantly being developed and receives regular updates and new features. To keep GnuPG up to date, please activate the option “Online update GnuPG version information every time Outlook starts”.

You receive a message when starting Outlook, when a new version of GnuPG has been released. You can then decide whether or not you want to install this new version. Confirming the question with "Yes" will redirect you to the page GnuPG of the gpg4o settings. There you can click on the button "Download and install GnuPG" which will download and install the latest version.

Hint: Please note that this functionality is not available in gpg4o Free.

11.2.3 GnuPG directory

By default, GnuPG saves its keyring in the application folder of your user profile. If you want to make use of another directory instead you can select an alternative directory here. This directory will then be utilized in the future instead of the default directory of GnuPG.

Hint: Already imported or generated keys will not be copied and will no longer be available in the new directory. In the old directory, however, they will still be existent. In order to be able to access these keys you have to export them before and import them again after having changed to an alternative directory (see chapter 8).

11.2.4 Buffering of the passphrase

You can determine here how long the passphrases you have entered shall be buffered. The minimum duration of how long the passphrases are buffered, is one minute.

11.2.5 GnuPG Agent

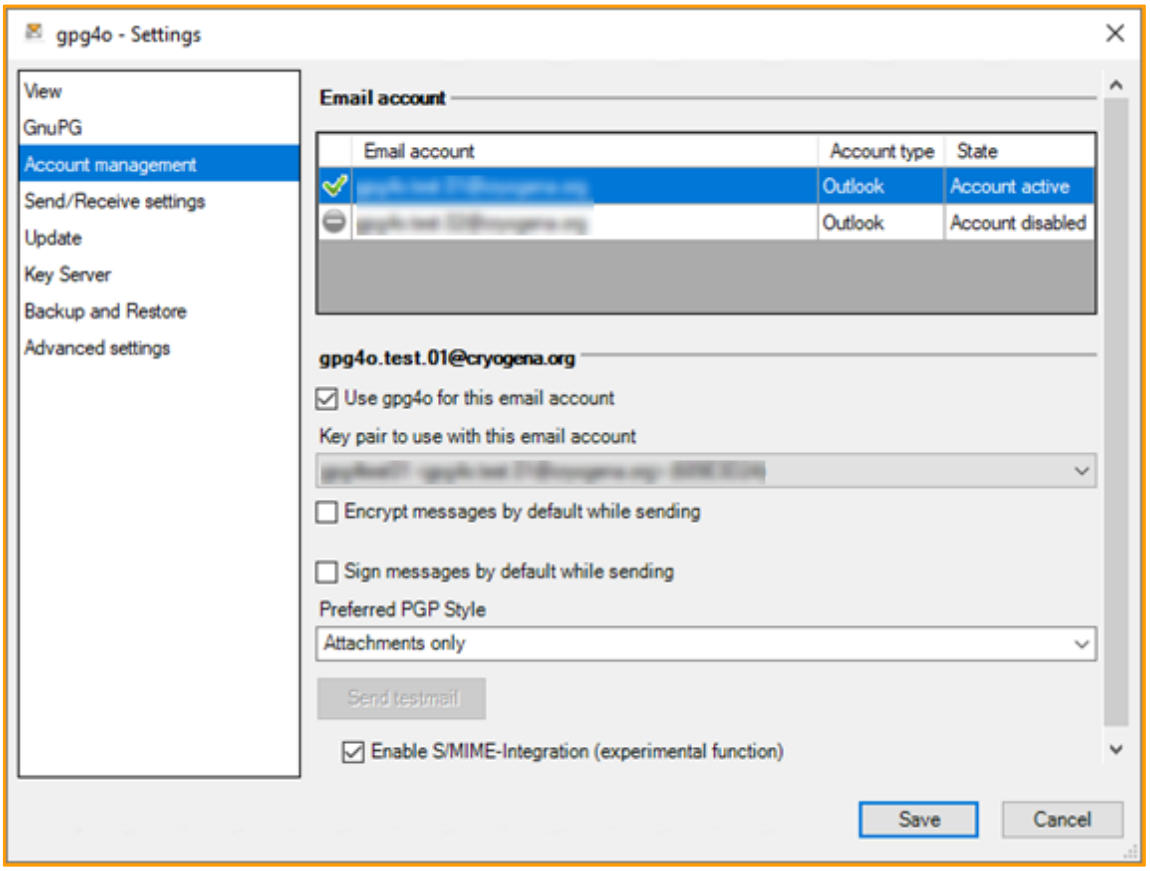
Since GnuPG 2.0 the GnuPG Agent is applied in order to buffer the passphrase. The agent is automatically started as soon as a GnuPG action in gpg4o is made. However, when closing Microsoft Outlook, the GnuPG agent is not terminated by default. Thus, buffered passphrases are not reset which might produce a security risk.

If you enable this option, the GnuPG Agent will be terminated automatically with Microsoft Outlook thus removing preliminarily entered passphrases from the memory.

Hint: The starting of the GnuPG Agent may take some seconds. This can be noticed in particular if you select the first email for decrypting.

11.3 Account management

On this page the configuration of the individual email accounts is performed (usually one email address corresponds to an account in Microsoft Outlook).



Under the name of the selected email account, you will find the associated settings "*Use gpg4o for this email account*". Place the checkmark with if you want to decrypt messages in this email account or if you want to send messages encrypted and/or signed.

Hint: If you do not want to encrypt or sign at all in an email account you should disable gpg4o for this account.

With the selection box "Keypair to user with this email account" you define which keypair shall be utilized for signing messages.

With the next two check boxes the default behavior of gpg4o with regard to the sending of emails is determined. If you choose messages to be encrypted by default you also have to define whether only the attachments or the entire message shall be encrypted.

With the selection box „Preferred sending format“ you can select the format that will be used when creating a new email. You can choose between the options „PGP/Mime“, “PGP/Inline”, “S/MIME” (This function is experimental, and so far, not supported.), “Encrypt Attachments only” and “Ask before sending”.

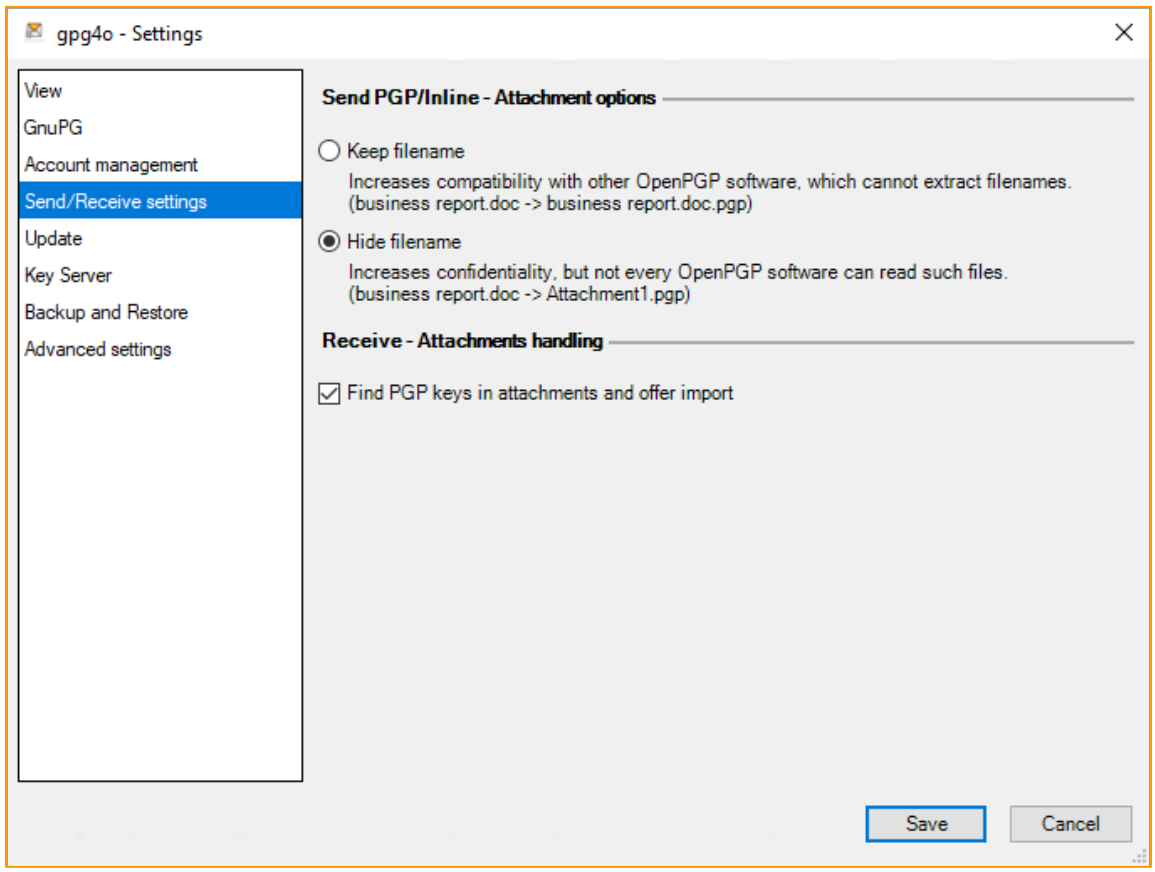
„PGP/Inline“ is useful if your communication partners mainly read their emails within a web browser. This format is easier to process for email readers but offers less protection against modifications.

„PGP/Mime“ is a format that makes it attackers more difficult to modify the email or even prevents modifications and therefore is to be seen more secure. However not every email software is able to correctly process this format which can cause signatures not to be verified for example.

If you regularly necessitate other configurations for certain situations, you can set them with the help of the sending rules (see chapter 10).

You can send a test mail for the selected account. You can verify with the received test mail whether encrypting and decrypting work correctly with your settings.

11.4 Settings for Sending and Receiving



11.4.1 Send - Attachment options

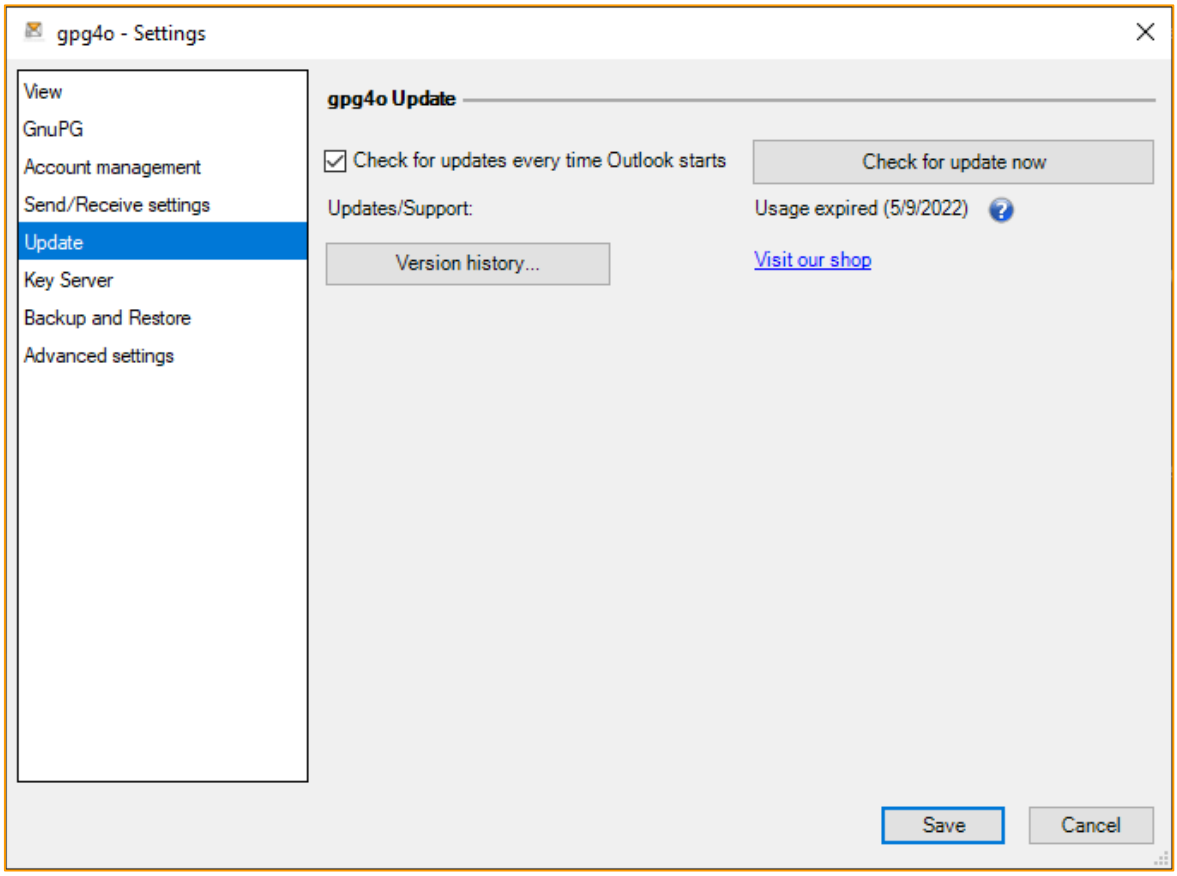
Many OpenPGP-applications do not only encrypt the email and the attachments but also the file names of the attachments. Gpg4o masters this technique and uses it as standard. However, not every OpenPGP-application is compatible with this technique. Therefore, you should activate the option “Keep filename” if a recipient cannot decrypt the file names.

11.4.2 Receive - Attachment handling

You can activate the attachment handling to automatically get a hint when key(s) and/or license(s) are contained as attachment in an email. The hint shows you on the one hand that the specific files are contained in the email and on the other hand offers you an import for the files.

11.5 Update

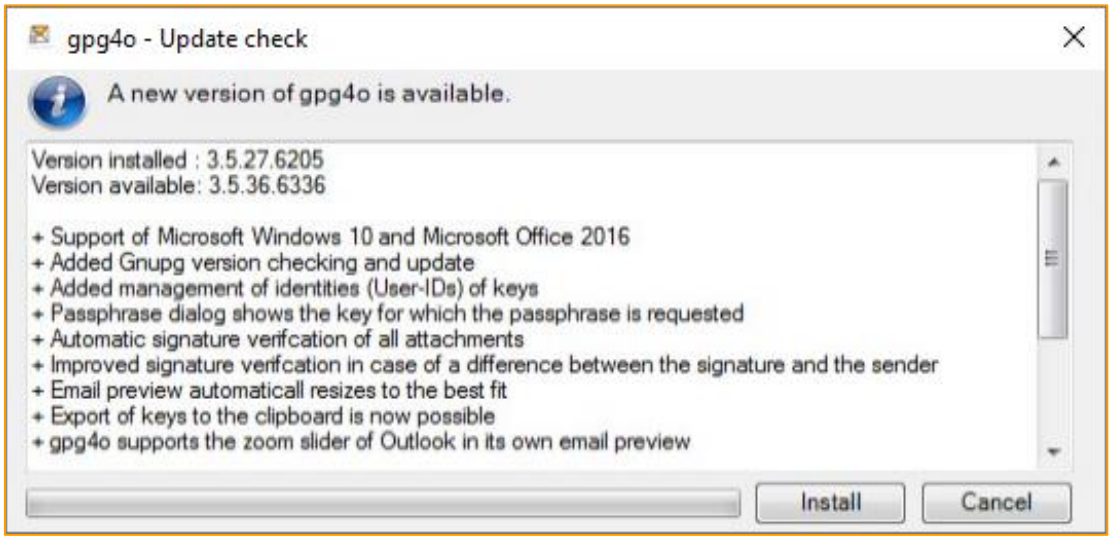
On this page you can set the check for updates of gpg4o or run it manually.



11.5.1 Update of gpg4o

The developers of gpg4o regularly extend the software, improve its usability, and add new features (customers' desires).

On this page you can perform a manual check for updates by clicking the button "Check for update now". If this verification shall be performed regularly place the checkmark with "Check for updates every time Outlook starts". By this, every time you start Microsoft Outlook, a newer version of gpg4o is searched and this version is offered to you for installation.



The installation is started by clicking on “Install”. You can find out more about the installation process in chapter 4. You should restart Microsoft Outlook after the installation, so that the changes are activated.

When the installation is finished, you should restart Outlook so that the modifications become effective.

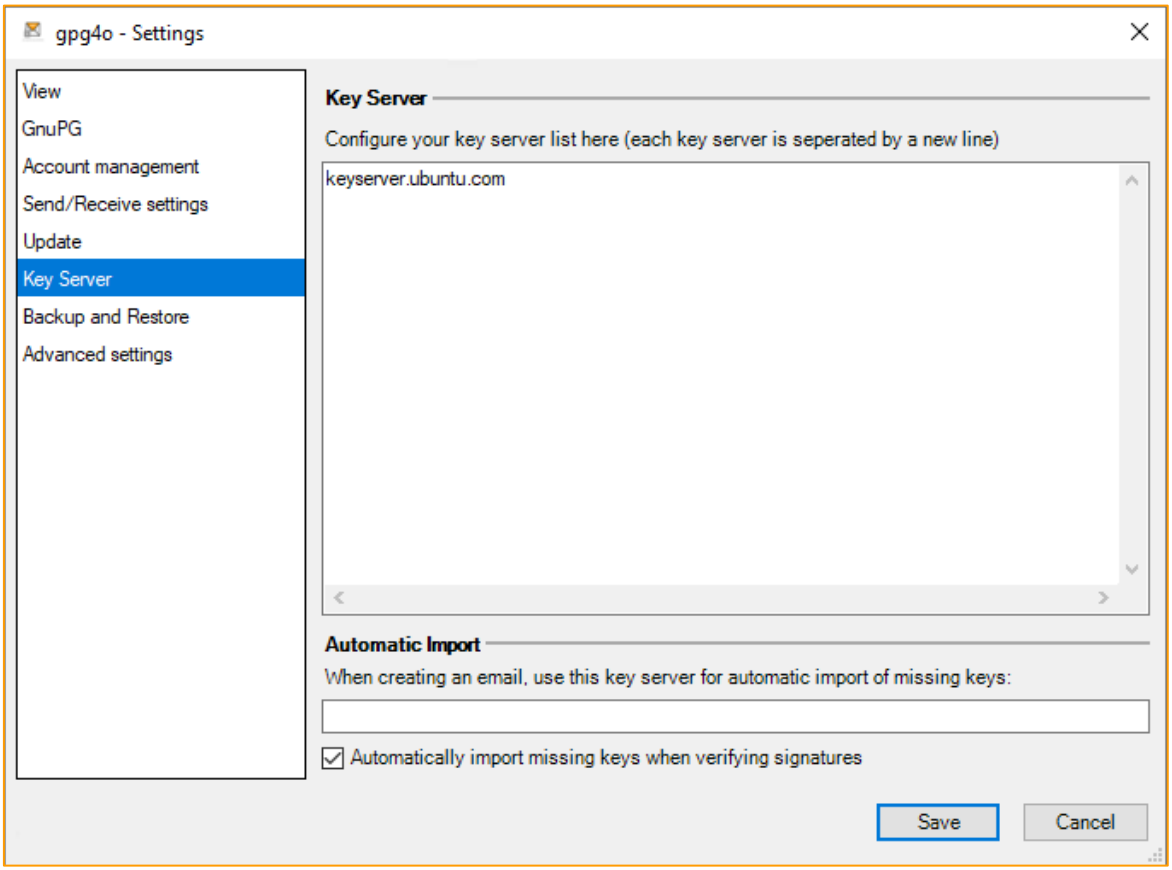
With the link “Visit our Shop”, you can purchase a license of gpg4o or an extension of the product maintenance of gpg4o.

In the “Version history...”, the individual releases and their improvements of gpg4o can be looked up.

Note: With the release of version 8.5.1, you will have to perform 2 automatic updates in succession in order to update completely. A corresponding note will be displayed in the update window. Follow the instructions to complete the update.

11.6 Key server

On the page „Key Server“, you have the possibility of displaying and editing the key servers utilized by gpg4o.



11.6.1 Key server

In order to add a new key server, enter its address as a new line in the text field.

Hint: Keep in mind that the address of the key servers will not be checked with regard to validity and that a wrong server cannot be reached.

In order to remove a key server, remove its entry in the text field. Thus, this key server will not be utilized in gpg4o anymore.

The listed key servers are used to manually import missing keys while checking email signatures. Please note that the only servers using HKP or HKPS protocol are used.

11.6.2 Automatic Import

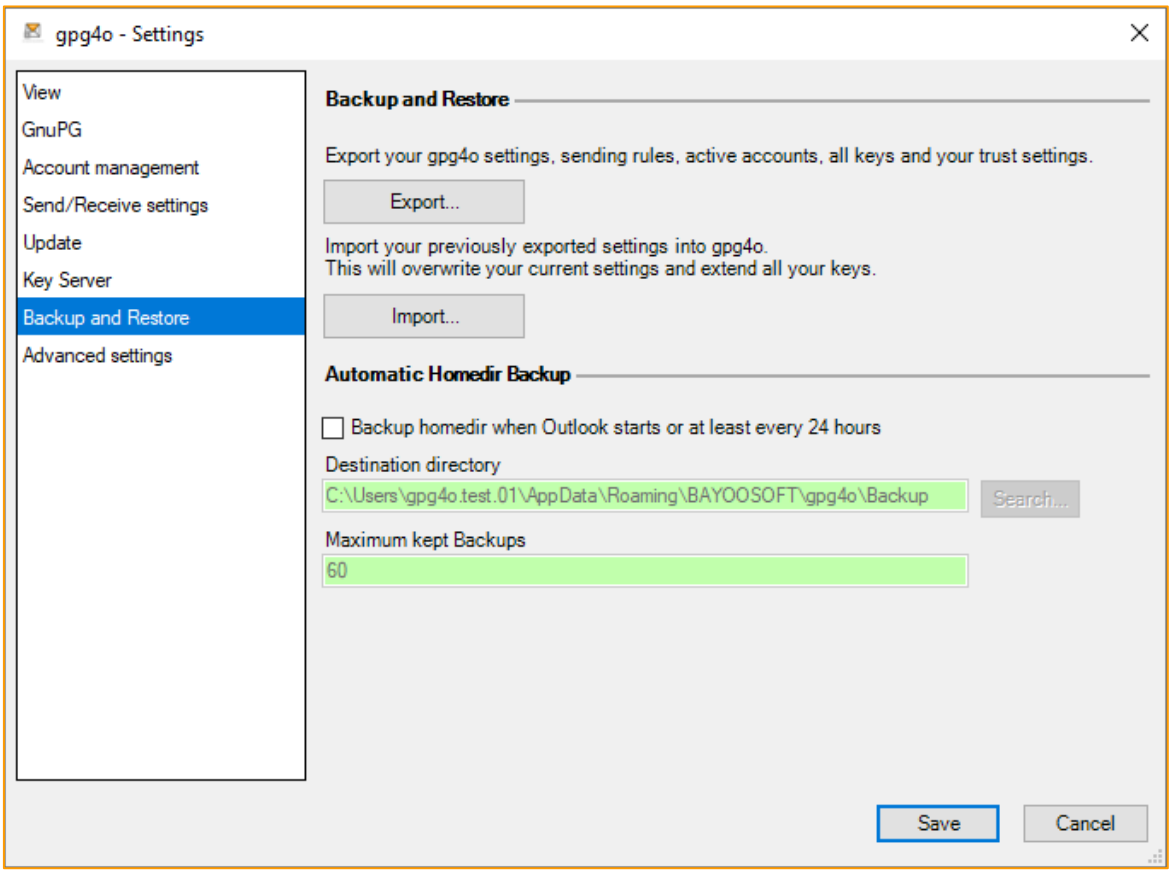
Here you can enter a key server, with which keys are automatically imported into your key ring, while you are writing emails. This is useful if you host a private key server and only upload valid keys. The server entered in this field does not have to be entered into the list of all key servers, to be used.

Missing keys are automatically imported into the local key ring, by activating “Auto import missing keys when verifying signatures”.

Hint: Please note that this functionality is not available in gpg4o Free.

11.7 Backup

On this page you can import a saved backup or generate one, respectively. Above all, a backup protects you from the loss of your keys in case of hardware failures. In addition, it can be used to transfer your settings and keys to a new computer.



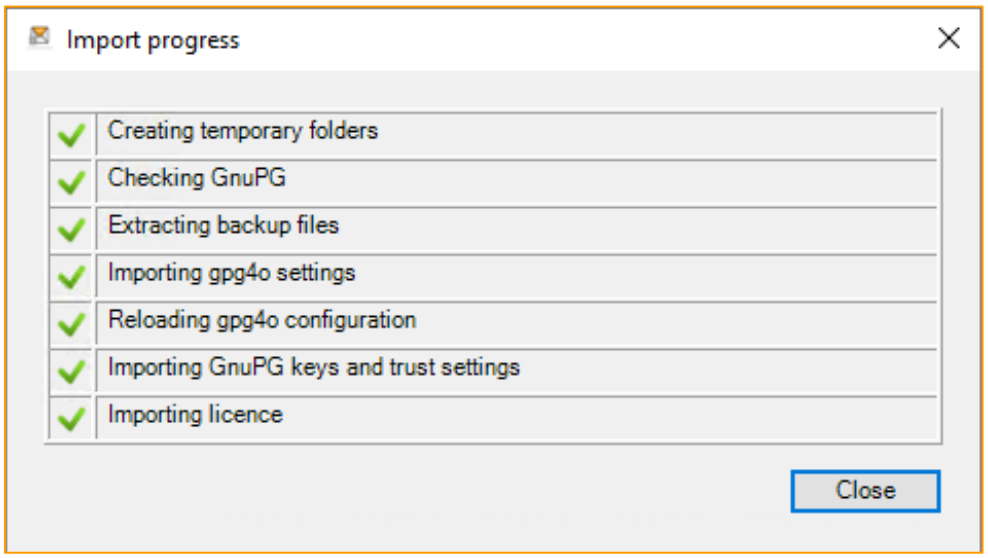
11.7.1 Backup and Restore

You can choose to perform a manual backup or import an existing backup. This backup protects you from losing your key and saves your current gpg4o-configuration, if, for example, the data can no longer be read from your hard drive. You must save the backup on a separate storage device, like a USB stick, external hard drive, or CD/DVD, and safely store it.

Through the button “Export”, you can generate a new backup. It comprises of the following data:

- All the keys, public keys as well as keypairs
- The trust settings of the keys
- The complete configuration of gpg4o including all account-settings
- All defined sending rules
- The gpg4o license file

With the button “Import” you reload your preliminarily exported settings of gpg4o and, thus, overwrite your current ones. Your keyring will be extended by the newly added keys and those keys which were deleted since the last export, will be included again.



Tip: A backup may also be utilized in order to move gpg4o to another computer.

Attention: Only save the backup on your own physical data storage medium. You should never upload the backup into the cloud.

11.7.2 Automatic Homedir Backup

A backup of the entire key ring is completed directly after saving the settings if “Backup homedir when Outlook starts or at least every 24 hours” is enabled. The data is saved as a Zip file in the specified path. The backup file is created in the specified path and should only be changed if you are aware of the problems that could arise if the path is no longer available or if another problem arises.

If the maximum number of backups is reached, the oldest one is deleted in order to create a new one.

„Next Backup“ shows you the date at which the next backup will be created.

Hint: Please note that the recovery of automatically created backups through the user interface of gpg4o is not possible. These backups have to be recovered by hand. Please contact your technical administrator or the support of gpg4o if you require assistance.

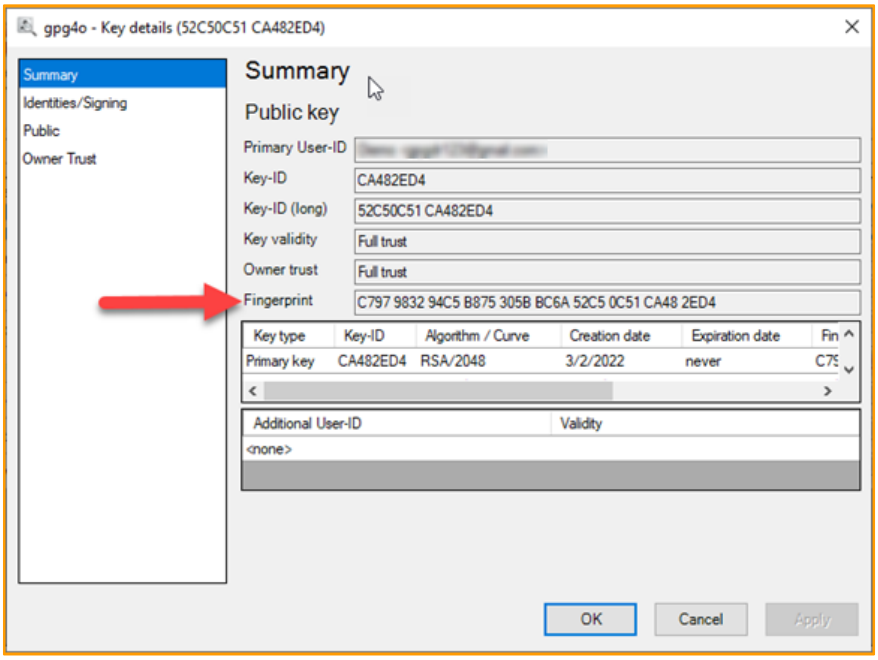
11.8 Advanced settings

On this page you will find settings which do not necessitate any modifications in the normal operation, or which do not require a better knowledge of the OpenPGP-Encryption. We kindly ask you not to modify anything here if you do not know about the consequences of these modifications.

11.8.1 Always treat all keys as valid

It is true that deactivating this option will improve safety, however, it will also increase complexity and will require a considerable additional effort regarding the key management. If you disable this option, you will only be able to encrypt emails to be sent to those recipients whose key you have signed or whose key has been recognized as valid by the „Web of Trust“.

Example: Please open the key management and search for the key you want to check. Select the key and open the key details.



Please compare the fingerprint in the key details with the fingerprint, given to you by the key owner: If the given fingerprint matches the fingerprint that is listed in the key details, you can confirm the key. Afterwards, the key can be used for safe communication.

To validate a key, please read the paragraph „Identities/Signing“ (see chapter 8.10.4).

Hint: You have to check and validate each and every key if you have deactivated the switch „Always treat all keys as valid“, before you can use them.

11.8.2 Hint for expiring account keys

If you activate this option, you will get a hint when one of your active account keys expires within 30 days or is already expired. The hint shows you all affected keys and offers you to extend all shown keys. With the agreement all keys get extended by one year.

Tip: In the key details you can set the expire date of your keypairs exactly (see chapter 8.10.3)

11.8.3 Insert GnuPG and gpg4o information in outgoing emails

If you encrypt and/or sign an email with gpg4o the GnuPG-Version and the gpg4o-Version will be inserted in the GnuPG headlines if the option is active. As this has also been implemented like that for other OpenPGP-solutions this option is enabled as a standard. If you deactivate this setting and one of your recipients has problems with decrypting and/or displaying the email, he will not be able to read with which software the email was encrypted.

11.8.4 Advanced signature check activation

By default, this option is enabled. By disabling this option, you globally disable signature checks for PGP/MIME signed emails.

11.8.5 Automatic Export

Here you can enter a key server, where the public keys are uploaded to, as soon as there are changes to the key. This is useful if you host your own key server. Changes, for example, are imports of a key from another server or file, revocation of a keypair, adding or edits to an identity, or signing of an unknown key. Through this, you can be sure that the newest public key is on the key server.

Hint: Please note that this functionality is not available in gpg4o Free.

11.8.6 Log Level

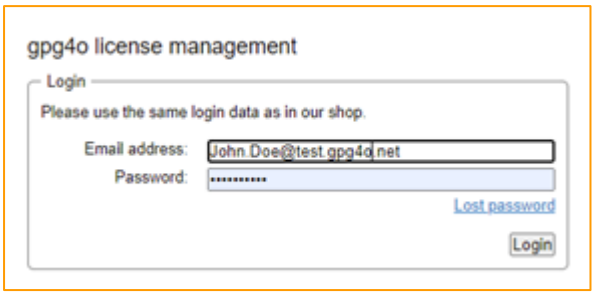
Here you can choose the log level. By default, this option is set to „Normal“. With the level „None“ logging is disabled and no logfiles will be created anymore. In addition to that the zip-file of logfiles will not be created when contacting support (see chapter 13.2).

Hint: Please keep in mind that the support work is more difficult when logging is disabled

12 License files

12.1 Generating and importing license files

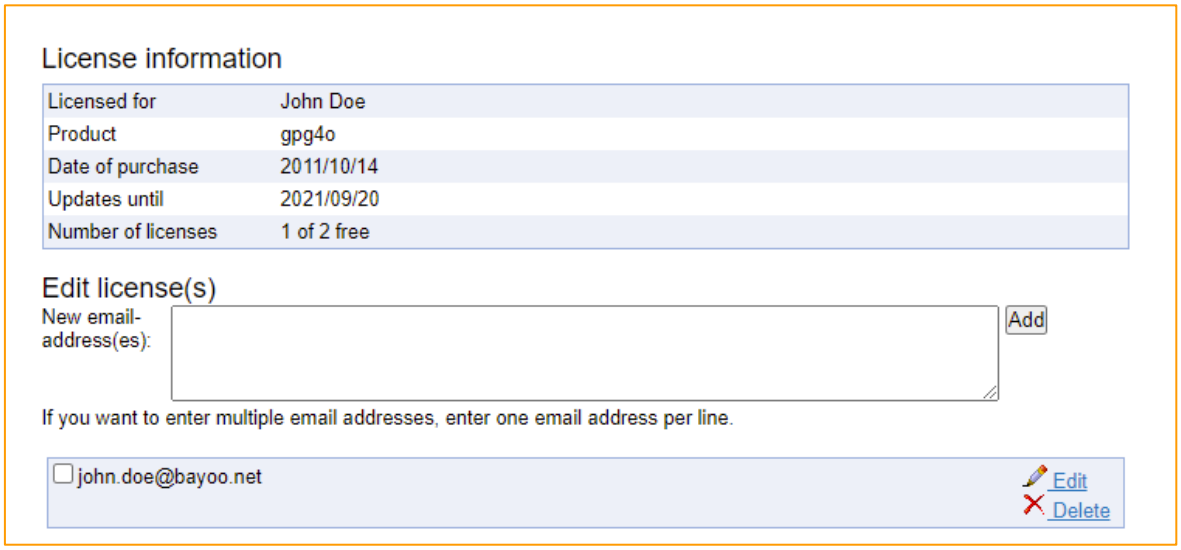
After having processed the online ordering of gpg4o you can manage your licenses via our web interface https://licmgmt.giepa.de/index.php?lang=en For login you utilize the same access data that you use in our shop.



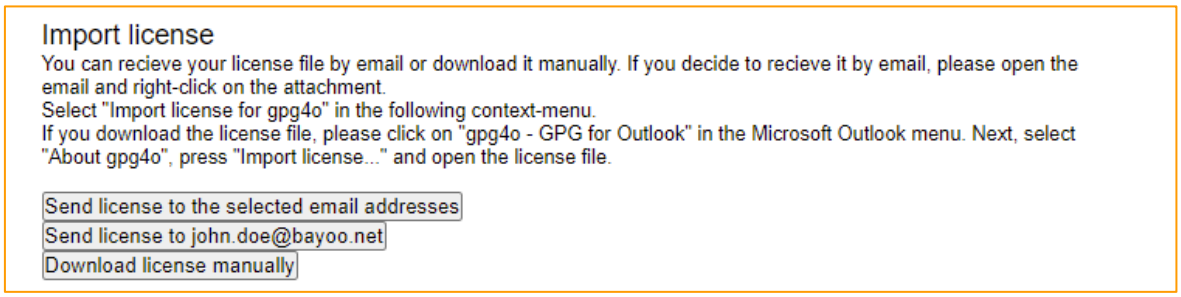
In the following menu you can see a summary of your licenses. You can see how many licenses are at your disposal altogether and how many of them are already utilized or which of them are still available.

Moreover, you can see the date until which updates will be placed at your disposal.

In order to make alterations to your licensing, click the pen-symbol “Edit”.



Subsequently, you can choose whether you want to download the license file directly or you want to have it sent by email. Alternatively, you can also define by checkmarks to which email addresses the license shall be sent. Here, you can select individual addresses or all addresses.



Now you can import the license. For this purpose, open Microsoft Outlook and choose “gpg-4o-Help” from the “gpg4o-GPG for Outlook” ribbon and select “About gpg4o”. There you click on “Import license…”

A file selection dialog will appear. Browse to your license and choose. Now, your license file is imported, and a corresponding message will appear which you can confirm by clicking “OK”.

When you have received a license file within an email, gpg4o now offers you to import this license if it is better than then one you have installed at the moment (see chapter 11.4.2).

It is also possible to import the license file once you have received it by email as file attachment. For this purpose, click the right mouse button on the file attachment and choose the item “Import license for gpg4o” in the context menu.

Now enter the email address you desire. In order to be able to enter several email addresses at once, separate them from each other with a new line. Email addresses which have already been entered can be individually adapted via the “Edit” and “Delete” buttons.

12.2 Period of validity of the license

The license of gpg4o entitles you to the unlimited use of gpg4o with the licensed email address. The period of validity of the license starts with the first download of the license file. Gpg4o is licensed for each real person. Therefore, gpg4o also works with only one license at several computers as well as with further email addresses within the same installation, as long as the licensed email address is configured within Microsoft Outlook.

12.3 Period of validity of the product maintenance/support

During the period of validity of the product maintenance/support you will receive product updates with numerous new functions of gpg4o. Furthermore, you have the possibility to make use of the support via email support@gpg4o.de in case of questions or problems.

If the period of validity of the product maintenance/support has elapsed gpg4o can still be used. That means that you can continue to send encrypted/signed emails and read encrypted/signed emails as well. However, you do not have the possibility any longer to install new updates and to contact the support.

12.4 Extension of the product maintenance/support

The team of developers of gpg4o permanently improve the program and integrate customers' suggestions into new versions. With an extension of the product maintenance, you may obtain new versions of gpg4o which were published after expiration of your product maintenance/support. In addition, you also extend the possibility of contacting the support via email. The period of validity of the product maintenance/support is extended by the number of purchased years of extension. Thus, the expiration date of the product maintenance/support is extended by the purchased years.

Example 1:

Original expiration date: 1st April 2021

On 1st February 2021 you purchase an extension of one year, in the first year after having bought gpg4o.

Expiration date after having bought the extension: 1st April 2022

Example 2:

Original expiration date: 1st April 2021

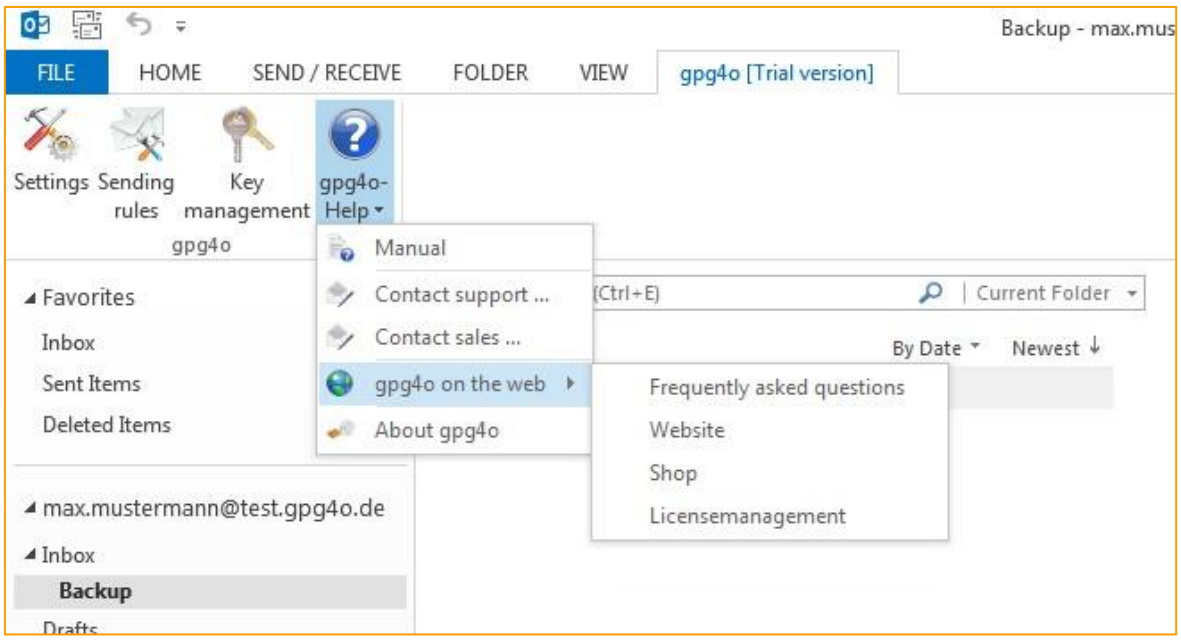
On 1st June 2021, after expiration of the product maintenance, you purchase an extension of one year.

Expiration date after the purchase of the extension: 1st April 2022 Here, you have a loss of 2 months of support and update.

Hint: After having purchased an extension this new, modified license file will have to be imported once into gpg4o

13 Help Center

Via the help center you will get simple and quick access to all important information regarding the utilization of gpg4o.



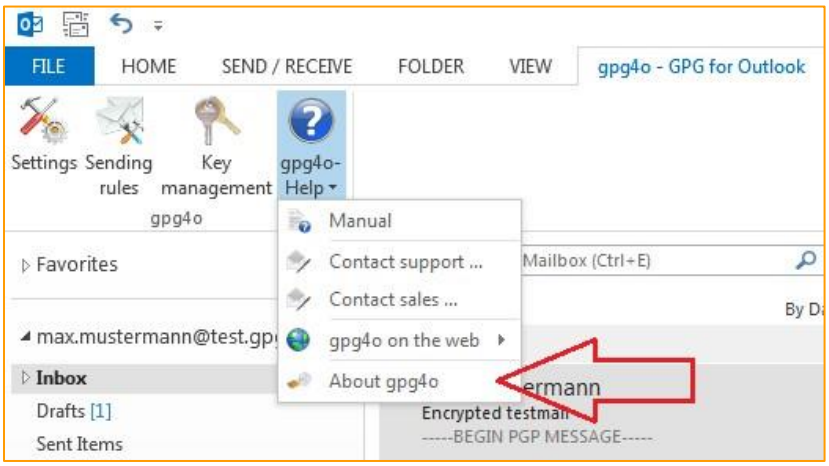
Here, you can open the manual, write an email to the technical support or to the sales department or inform yourself about gpg4o on the Internet.

Via the menu entry “gpg4o on the Web”, you will gain access to the following Web pages:

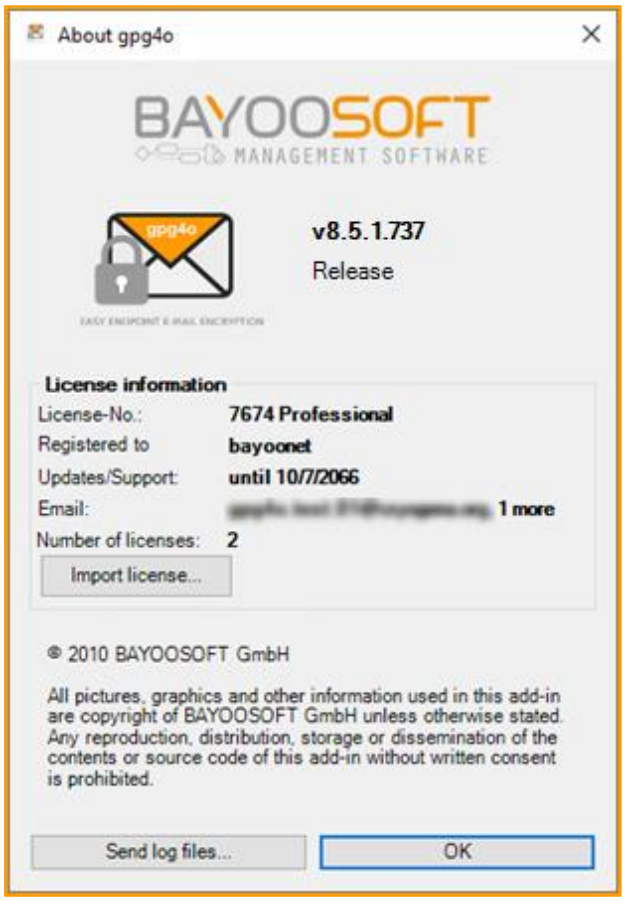
- “Frequently asked questions”
- “Website”
- “Shop”
- “License management”

In addition, you can call up the “About gpg4o” dialog where the installed version of gpg4o and information with regard to your license will be displayed to you. In this dialog there is also the possibility of importing a license file (see chapter 13.1).

13.1 Information about gpg4o

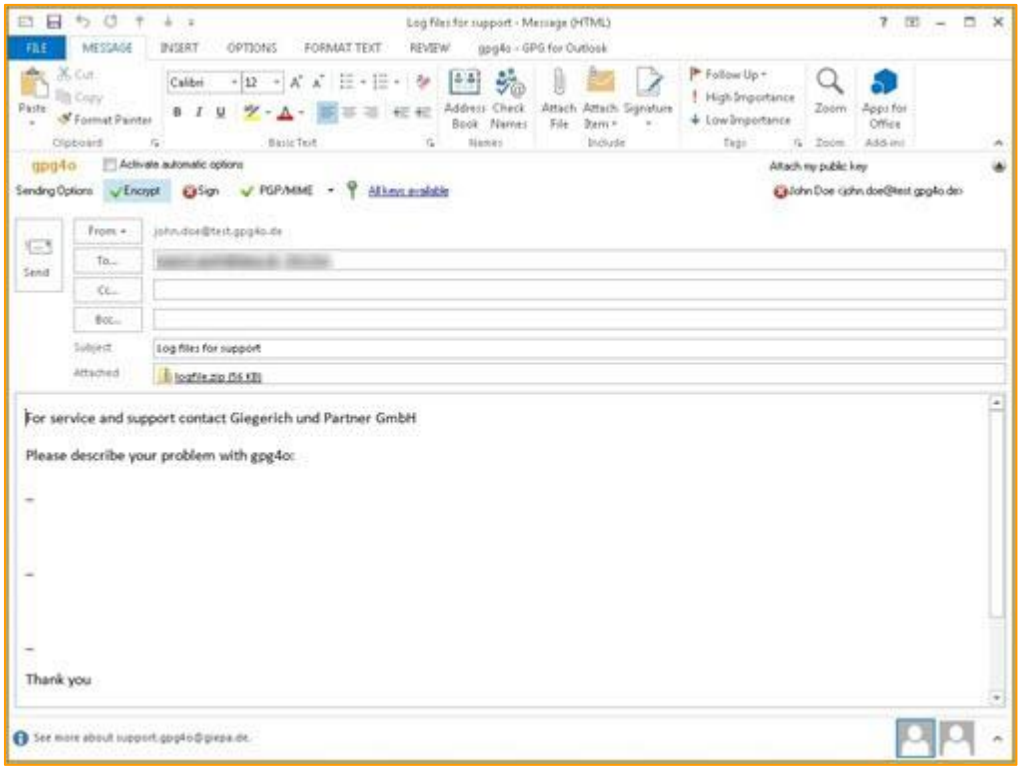


For more information to gpg4o, please click on “gpg4o-Help” and. “About gpg4o”. In the following window, you can see information to your license and information to the currently installed version



13.2 Sending log-files

In order to send the log files to our support, please click “gpg4o-GPG for Outlook” in the menu ribbon of Microsoft Outlook. Here, select the button “Help Center” and click the entry “Contact support…” then. Then, a preconfigured email will open automatically with the log files as attachment.



You are kindly asked to give a precise description of the error that occurred and of the steps which you have carried out shortly before said error showed. In doing so, you help us localize the error source and offer you a solution as fast as possible.

13.3 Contents of log-files

In order to optimize the efficiency of our development in the elimination of possibly occurring errors, status reports are written into so-called log-files by gpg4o. These status reports contain neither personal information nor passwords or contents of emails. Before sending the email together with the log-files you can see the information passed on by unpacking the attached zip-file. All files contained therein consist of plain text.

13.4 Help in gpg4o Free

The Free Version of gpg4o does not have access to support.

14 Miscellaneous

14.1 What is to be done in case of errors?

We kindly ask you to help us disclose and correct errors.

In order to be able to rapidly correct appearing errors we need a maximum of details concerning the error occurred. We kindly ask you to send us the error reports as well as the log files via the corresponding email provided in gpg4o (see chapter 13.2).

If you have questions, critical remarks, or suggestions for improvement we kindly ask you to submit them to us in the same way, for we are always receptive to listen to your problems.

14.2 Utility programs

For certain problems, gpg4o is installed with programs to analyze and correct itself. These programs are installed in the installation path of gpg4o and can be executed there.

14.2.1 Maintenance Registry

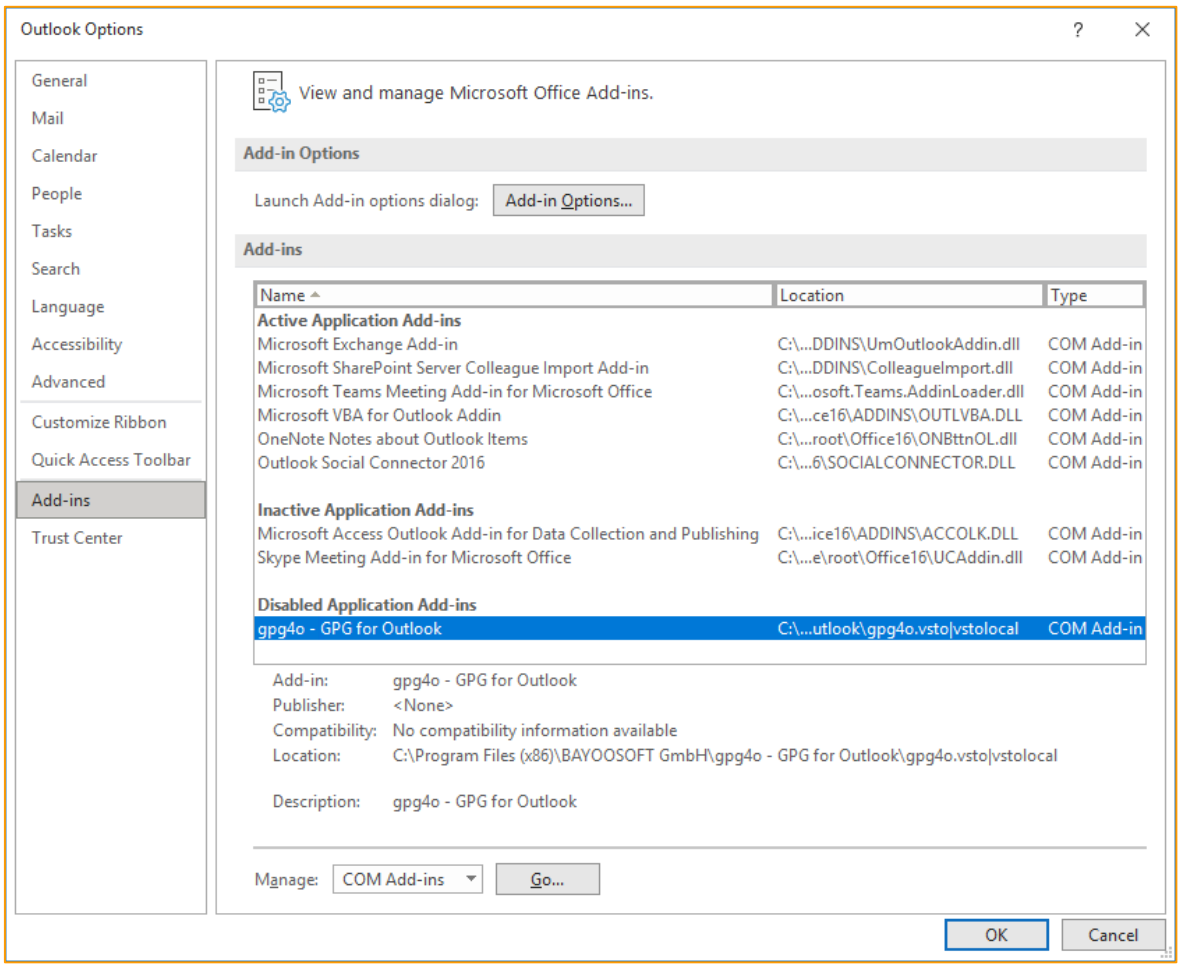
Use this program if gpg4o won't stay activated after each start of Outlook or if gpg4o needs to be started manually each time. Please note that this program requires administrator rights to make corrections.

14.2.2 Maintenance Logfiles

Creates a Zip file out of the log files of gpg4o and attaches these to a new email that can be sent to the support.

14.3 gpg4o does not start

If gpg4o is not visible anymore, there are several possibilities of reactivating the add-in again. First of all, kindly open your Outlook options by clicking “File” in the menu ribbon and selecting the menu item “Options” there. In the following window, click on the left side “Add-Ins”



Now, search on the right side the entry “gpg4o-GPG for Outlook”. If gpg4o can be found under the item „Disabled Application Add-ins“, you are asked to follow chapter 14.3.1.

If gpg4o can be found under the item „Inactive Application Add-ins“, please follow chapter 14.3.2

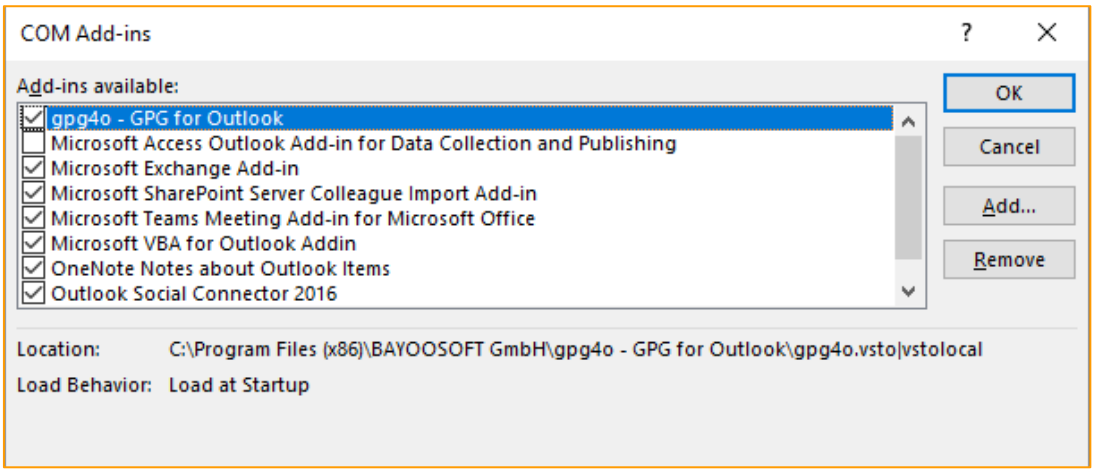
14.3.1 Disabled application add-ins

In the lower section next to the “Go…” button, select the entry „Disabled elements“ and afterwards click the button “Go…”. In the window opened then select the entry “gpg4o-GPG for Outlook” and click the “Enable” button. Having done that, close the window by clicking “Close”. After a moment gpg4o will be loaded again. Otherwise, it might be necessary to enable gpg4o subsequently via the procedure described in chapter 14.3.2.

14.3.2 COM-Add-Ins

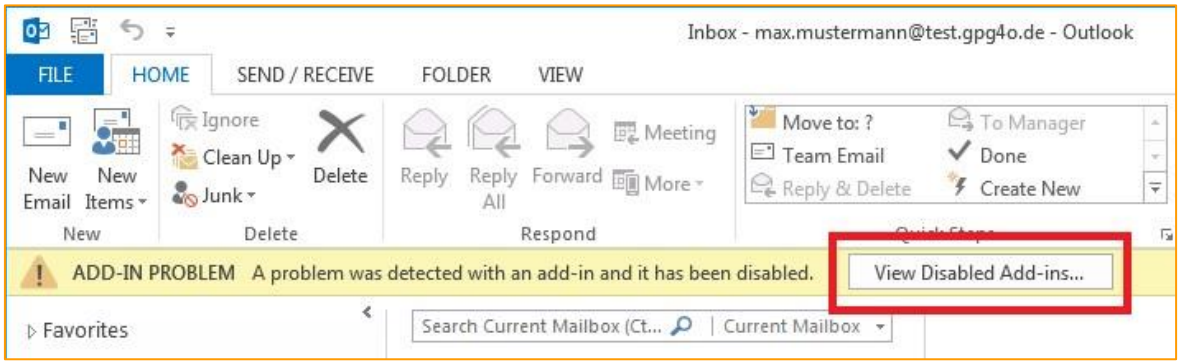
Please note that Outlook is started with administrative rights, so that the following changes are permanently applied.

In the lower section next to the “Go…” button, select the entry „COM-Add-Ins“ and click the button “Go…” then. In the window opened then search for the entry “gpg4o-GPG for Outlook” and place a checkmark in front of it. Afterwards, close the window by clicking “OK”. After a moment gpg4o should be reloaded. Otherwise, there is perhaps an essential problem. In this case you are asked to contact the support (see chapter 13.2).

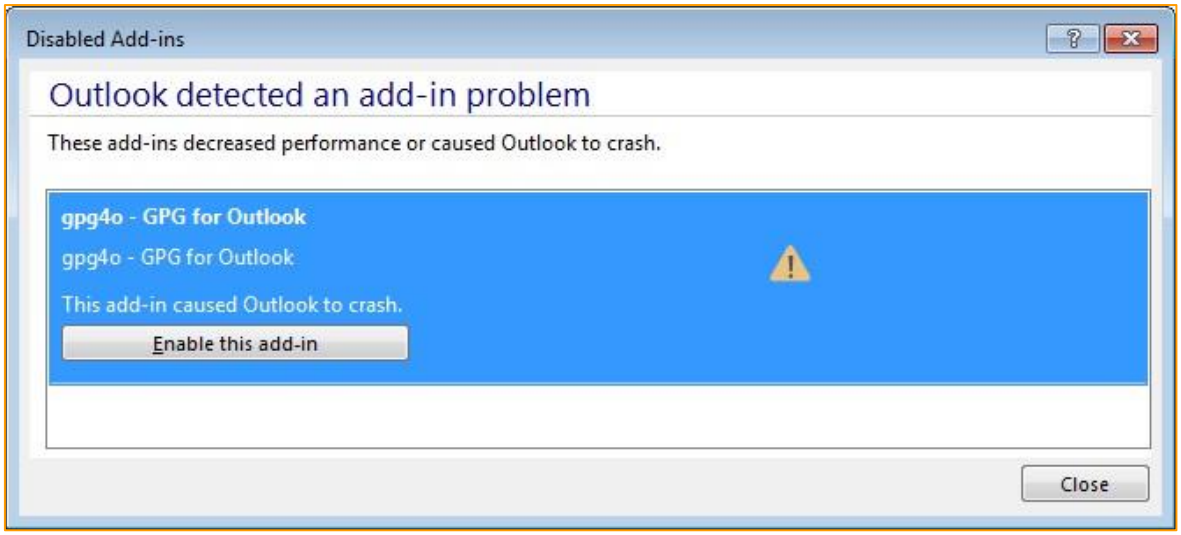


14.3.3 Microsoft Outlook 2013 and Outlook 2016

Outlook 2013 and Outlook 2016 analyze the load times of add-ins and automatically disables add-ins with ordinarily longer uploading times.



If this is true for you, please go to “File” in the menu ribbon and there to “Manage Add-Ins”.



Select gpg4o and press the “Enable this add-in” button. Afterwards, please click the button “Close”

15 Uninstalling

If you uninstall gpg4o or also GnuPG, all generated and imported keys will remain and will be at your disposal again after a new installation.

15.1 Delete personal data

If you want to delete your keys completely, you should do this via the key management and uninstall gpg4o only then.

Alternatively, you delete the directory of GnuPG. In this directory you will find all personal data managed by GnuPG (Keyrings, trust settings and program configurations).

In addition, you should also delete the gpg4o user directory and the Microsoft Outlook configuration directory. In these directories you can find the personal settings of gpg4o.

15.1.1 GnuPG directory

%AppData%\Roaming\gnupg

Attention: Please mind that not only the program gpg4o accesses GnuPG-keys. Deleting the data may influence other programs. By deleting the key data, you will permanently lose access to your encrypted emails! Without the matching keys your emails cannot be decrypted.

15.1.2 gpg4o user directory

%AppData%\Roaming\BAYOOSOFT\gpg4o\

15.1.3 Microsoft Outlook configuration directory

%AppData%\Local\Microsoft_Corporation\gpg4o.vsto_...

This path varies depending on the computer and may be existent several times in similar form.

15.2 Uninstalling gpg4o

In order to uninstall gpg4o click “Control Panel” in the Windows start menu and browse to the item “Programs”. You will now see the list of all programs installed on your computer. Select “gpg4o-GPG for Outlook” and click “Uninstall” in the menu.

15.3 Uninstalling GnuPG

In order to uninstall GnuPG click “Control Panel” in the Windows start menu and browse to the item “Programs”. You will now see a list of all programs installed on your computer. Select the installed GnuPG and click “Uninstall” in the menu.

16 Company and support contact information

16.1 Support contact information

Please use the following email address to contact the **BAYOOSOFT GmbH** support for issues relating to gpg4o: support@gpg4o.de

General contact information:

BAYOOSOFT GmbH

Machtlfinger Straße 11

81379 München

Germany

Web: https://www.bayoosoft.com/en/email-encryption/