gpg4o

Manual

Version 3.1

Softwareentwicklung | IT-Sicherheit
Giegerich & Partner
Robert-Bosch-Str. 18
D-63303 Dreieich
Fon: +49 (0) 61 03 - 58 81-0
Fax: +49 (0) 61 03 - 58 81-39
Mail: info@giepa.de
Web: www.giepa.de

Table of Contents

1 General

gpg4o – GPG for Outlook ®

gpg4o was developed as an Add-In for Microsoft Outlook 2010 ® and Microsoft Outlook 2013 ® 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 the simple and uncomplicated handling of public keys.

The validity of external keys is verified by means of the **Web of Trust function**. For this purpose information of known key owners is used.

2 System Requirements

In order to be able to utilize **gpg4o**, your system must fulfill at least the following requirements:

Operating system: Microsoft Windows ® XP SP3, Windows Vista ® SP1 or higher, Windows 7; 32- or 64-Bit Versions

Email program: Microsoft Outlook 2010 ®, 32- or 64-Bit Version,
Microsoft Outlook 2013 ®, 32- or 64-Bit Version

GnuPG: from Version 1.4.13

3 Installation

3.1 Software

The latest download version of gpg4o can be found at
http://www.gpg4o.de/en/product/downloads.html

You can have GnuPG 1.4.13 installed during the first setting of gpg4o. (Also compare paragraph 3.3)

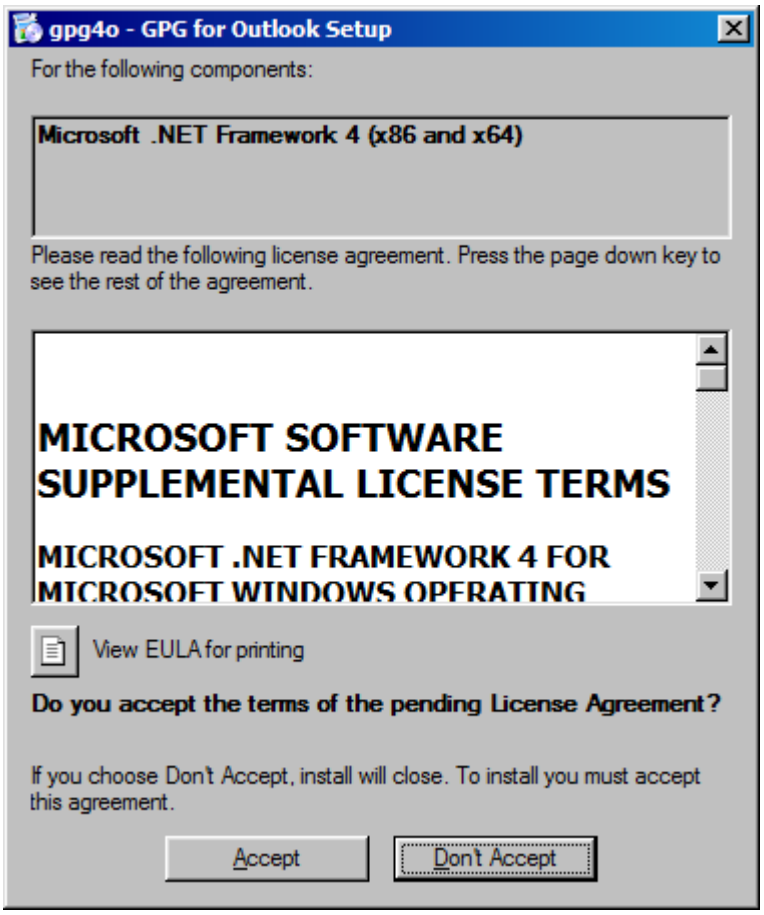
Information and the source code of GnuPG can be found at
http://www.gnupg.org/

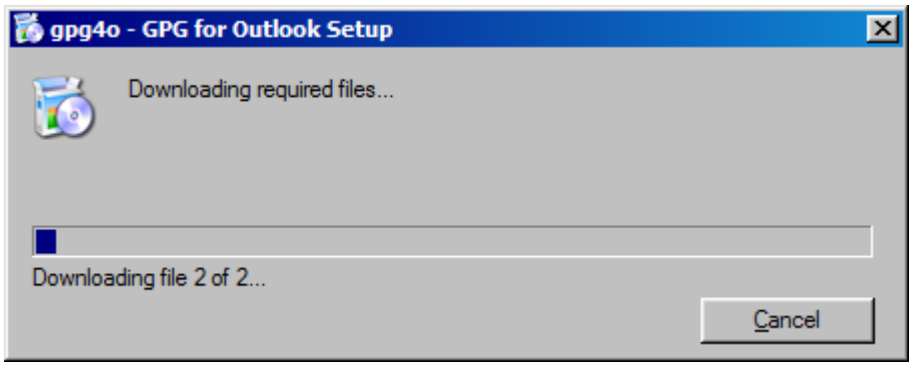
The General Public License (GPL) can be found at
http://gnu.org/licenses/gpl.html

3.2 Installing gpg4o

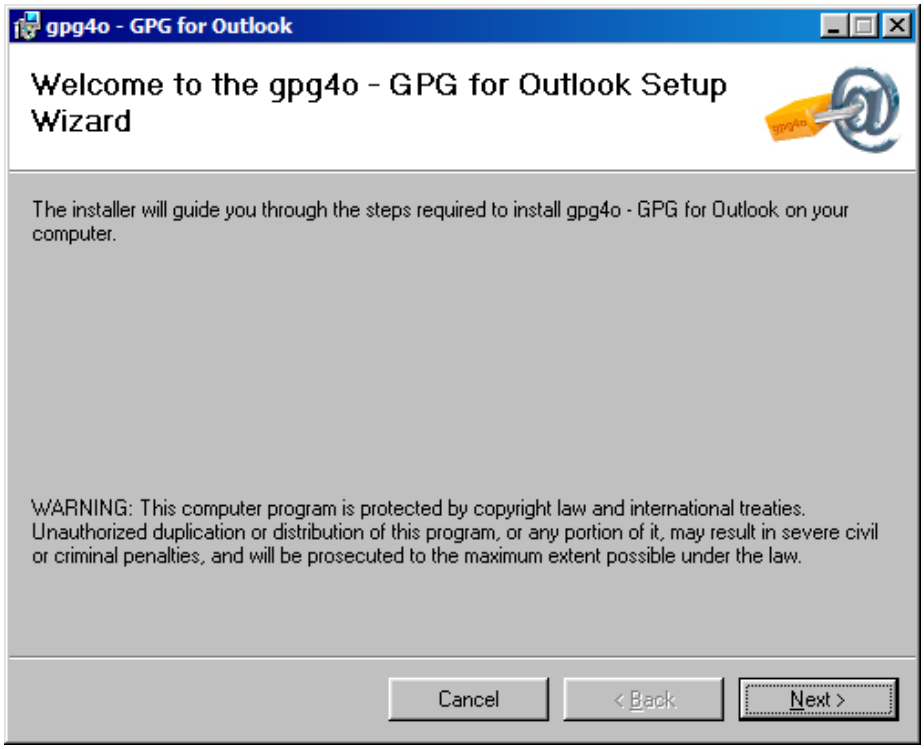
For installation you need administrator authorizations. Before installing **gpg4o** please close the application Microsoft Outlook ®, as otherwise, there might be problems during installation. Having done this, execute the file **„gpg4o_setup.exe“** by double-click.

The installation will start now. In doing so, the presence of all required components (for example .NET Framework 4) is checked. Missing components will then automatically be installed.

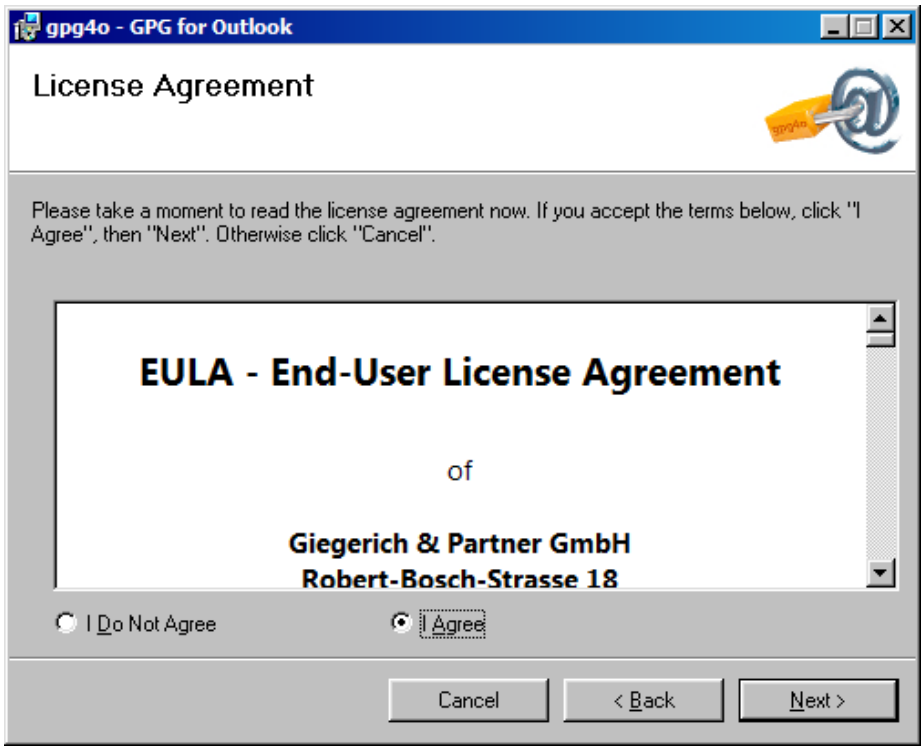




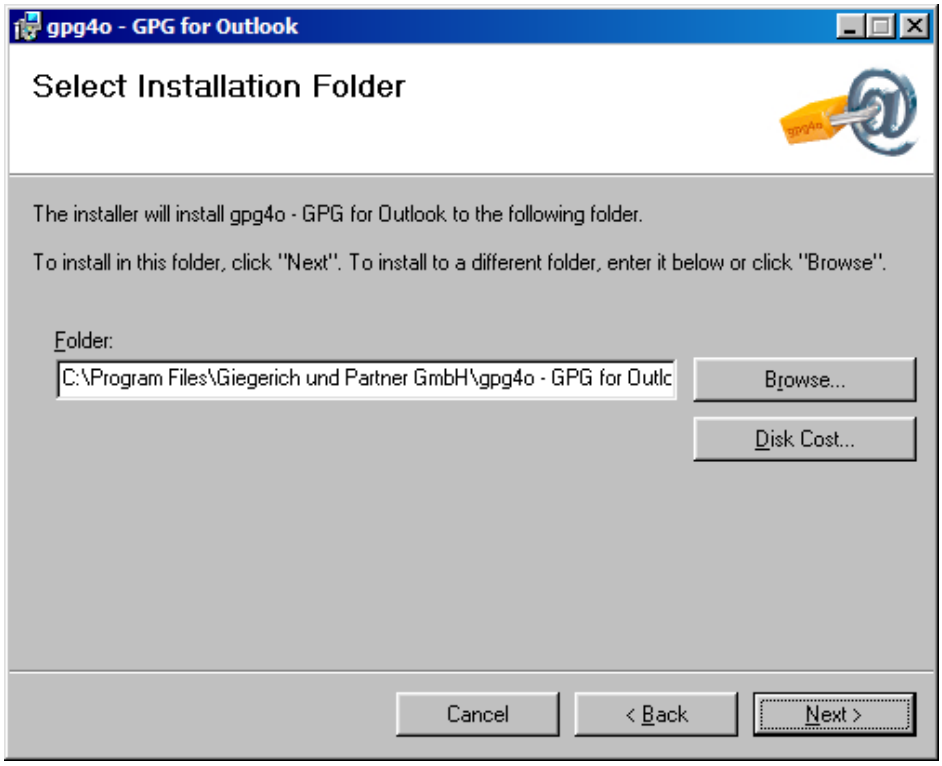
As soon as all the necessary components have been installed, the wizard will continue installing **gpg4o**. Click on **„Next“** to continue the installation process.



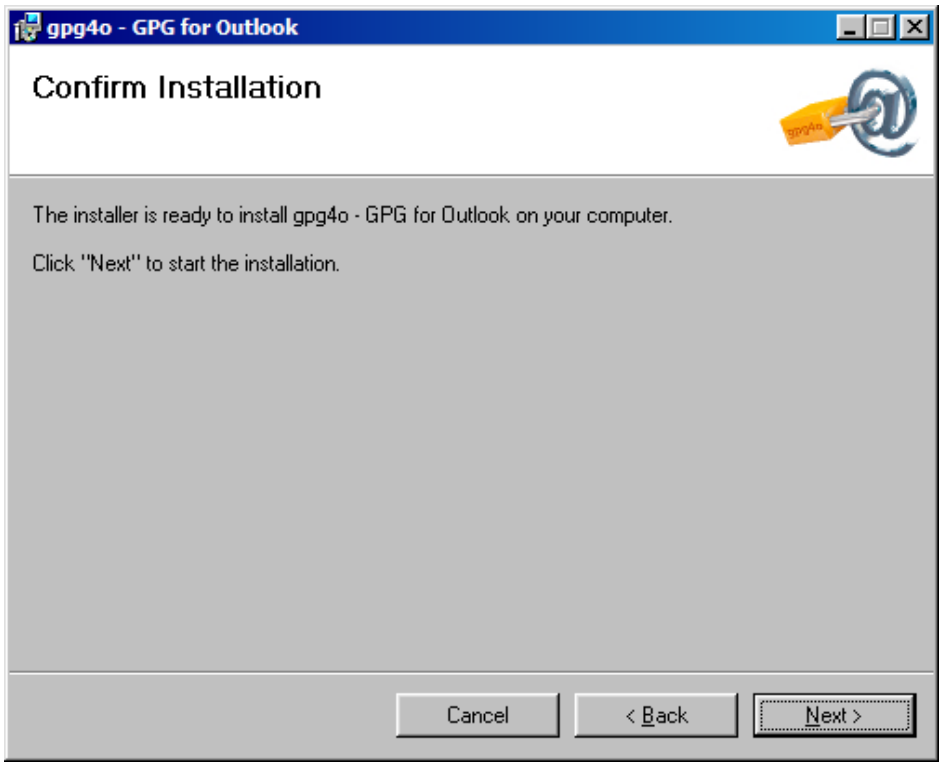
In the following dialogue you will see the End-User License Agreement. Once you have decided to accept the License Agreement (precondition for the installation), select the radio-button next to **„I Agree”**, click **„Next“** and continue the installation.



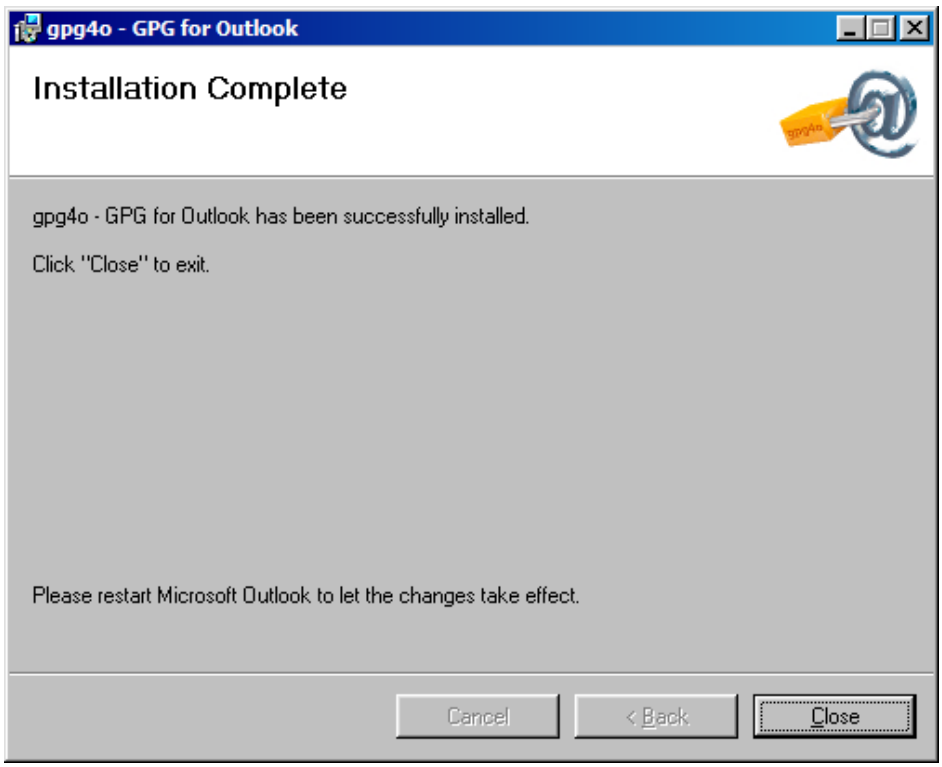
In the following dialog you will be asked, to set the installation path. Here the default setting is normally the best choice. Confirm the installation path by clicking on **„Next".**



After having clicked **„Next"** the installation procedure will be started by **gpg4o**.



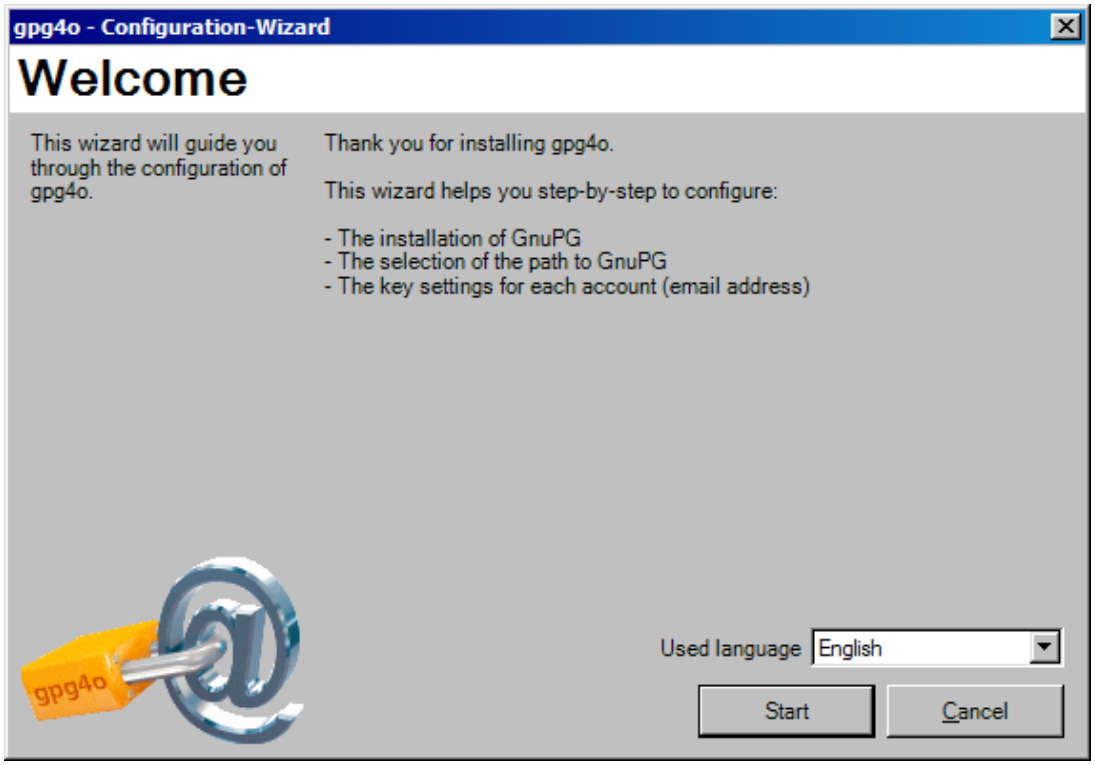
Now the installation of **gpg4o** is completed. You can start the configuration of **gpg4o** by restarting Microsoft Outlook ®.



3.3 Setting gpg4o

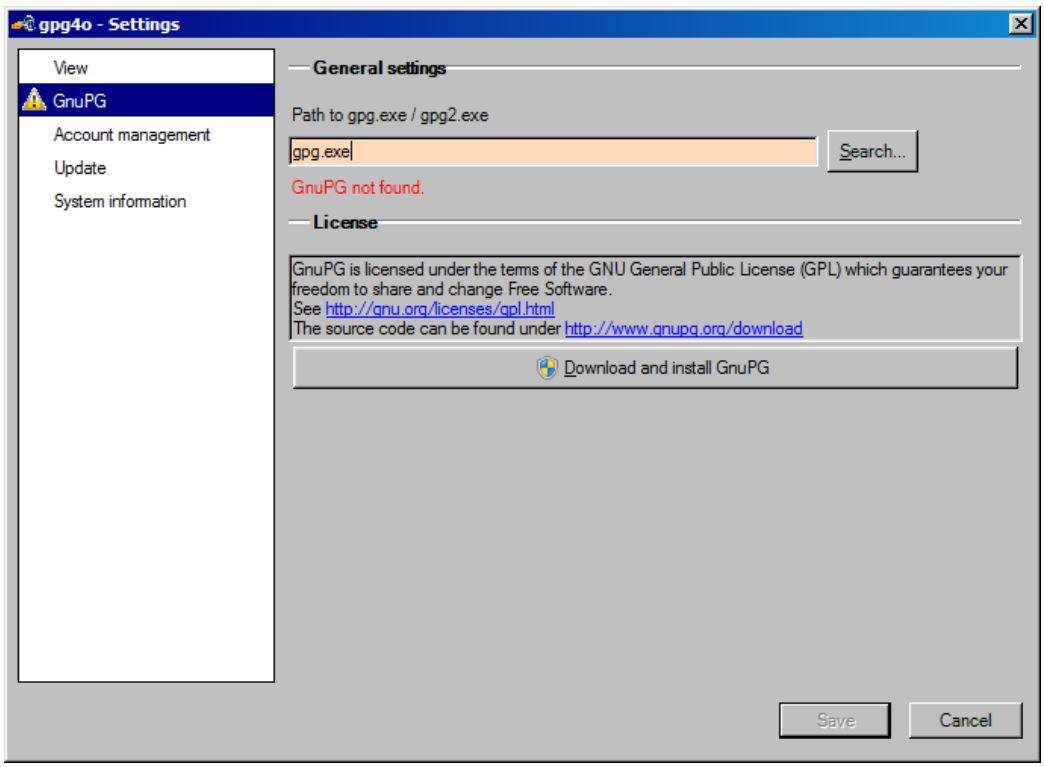
Start Microsoft Outlook ® now in order to begin the setting of your new software. The configuration wizard appears which will help you to set up **gpg4o**. Click **„Next“,** in order to start the configuration.

In addition you have the possibility of changing the language of **gpg4o**. Once you have performed the language setting, click **„Start“**, in order to continue the configuration.



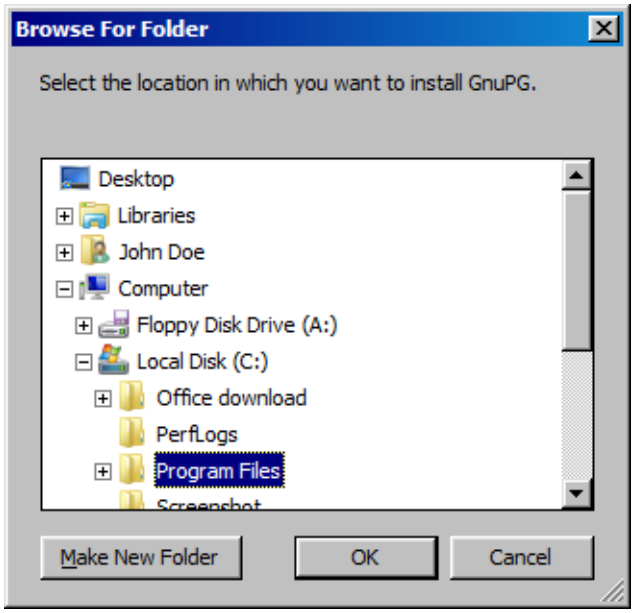
If the installation path of GnuPG is not found the selection will be highlighted reddish. In this case click **„Search“**, search on your hard disk for the GnuPG-Installation and select the file **„gpg.exe“** or **„gpg2.exe“** in the installation folder. The installation path should now be highlighted green.

You can also download GnuPG from the Internet and have it installed. For this purpose, click **„Download and install GnuPG“**

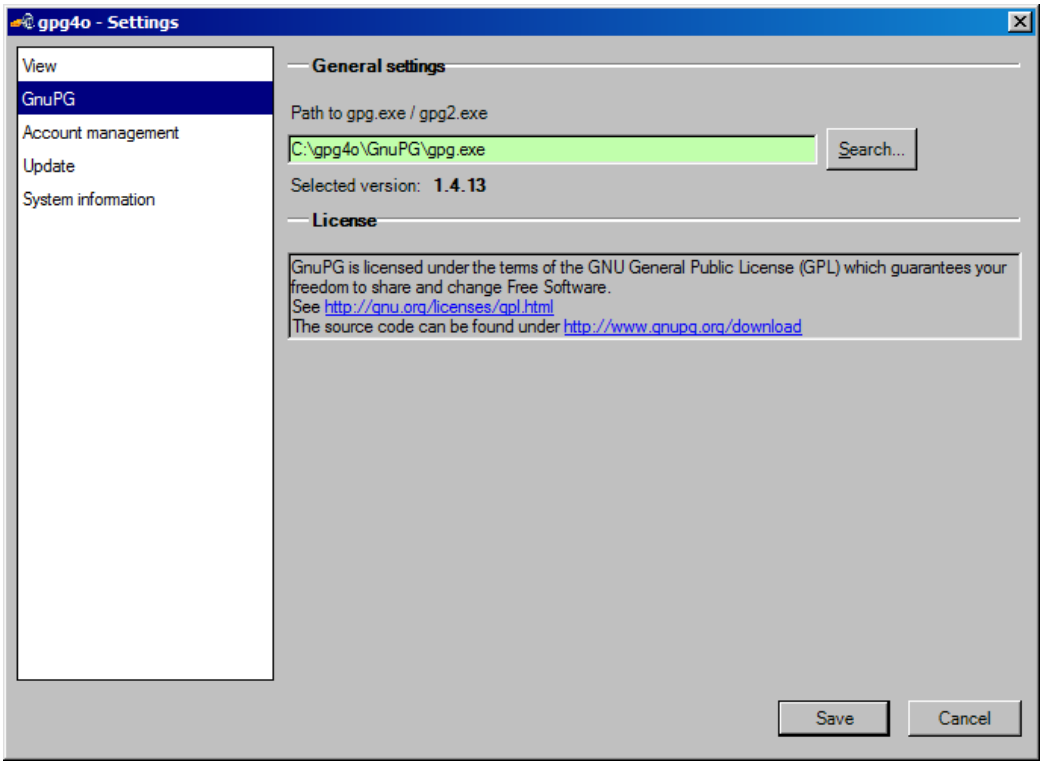


View if no gpg.exe was found.

If you decide to download GnuPG from the Internet you will be demanded the path where GnuPG shall be installed. Here, choose an empty folder or make a new one.

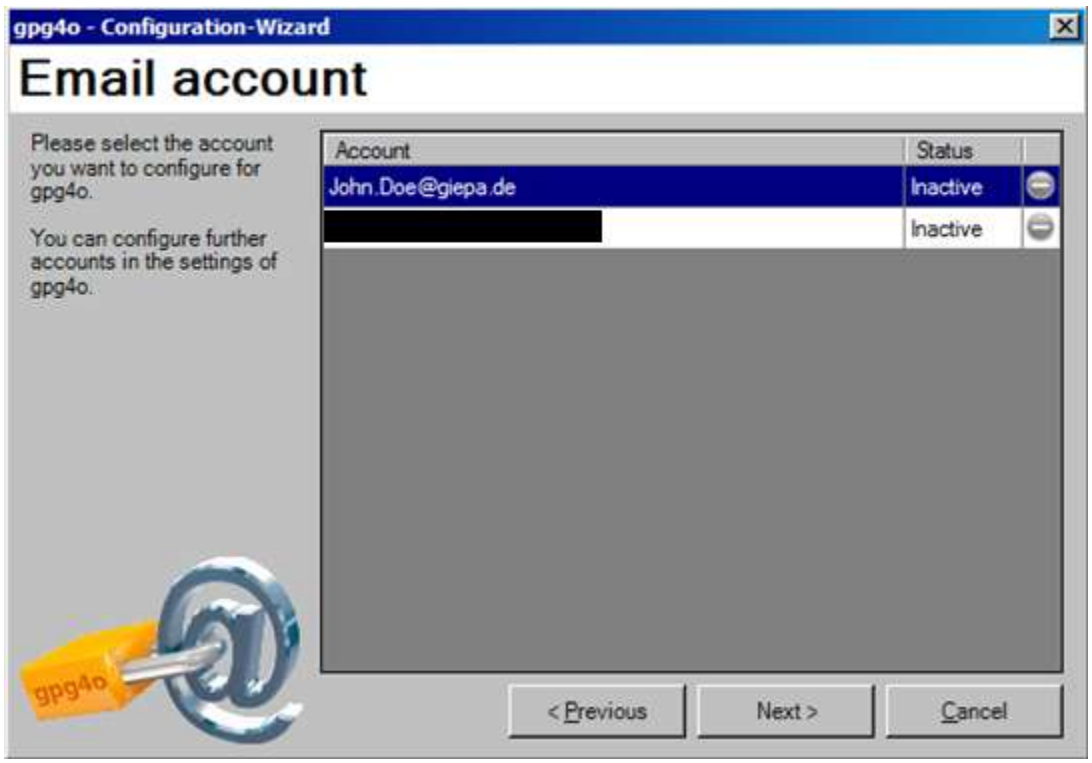


After successful installation the path will be automatically adopted into the settings and you may continue the configuration.

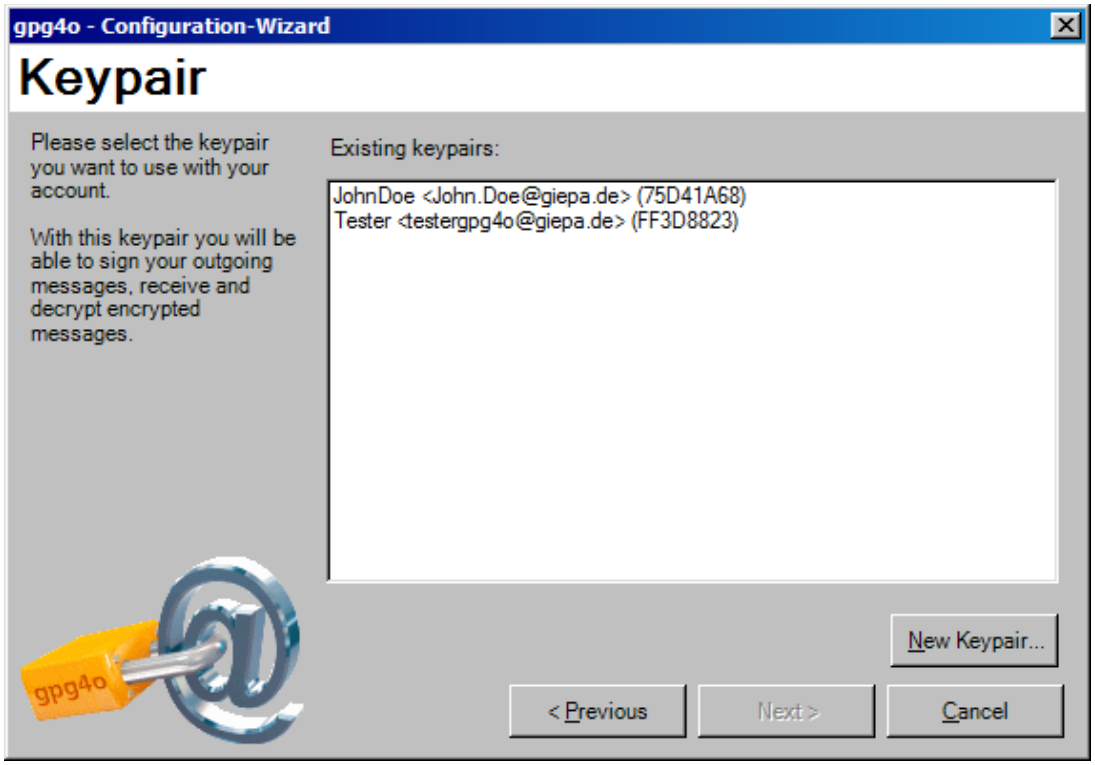


Alternatively, you can import a backup of gpg4o here (also compare 8.4.2).

In the following window select the account with which you want to utilize **gpg4o** and having done this click **„Next >”**.

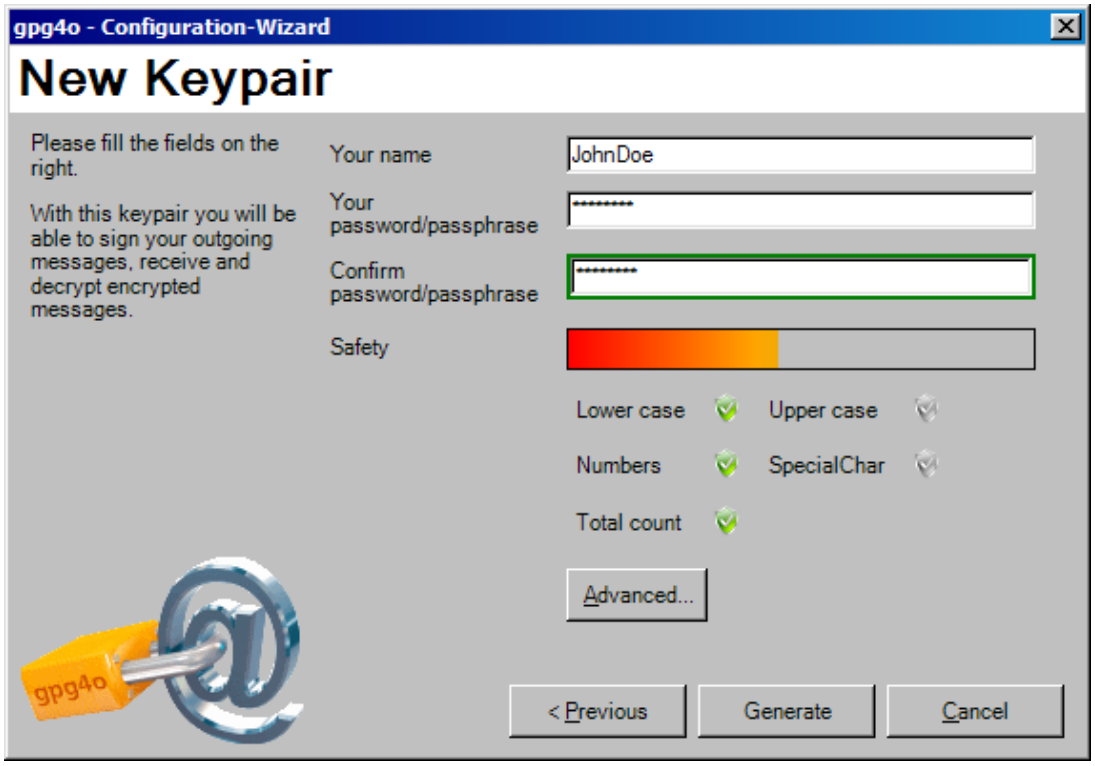


Subsequently, you can select a keypair from the list out of possibly existing private keys.

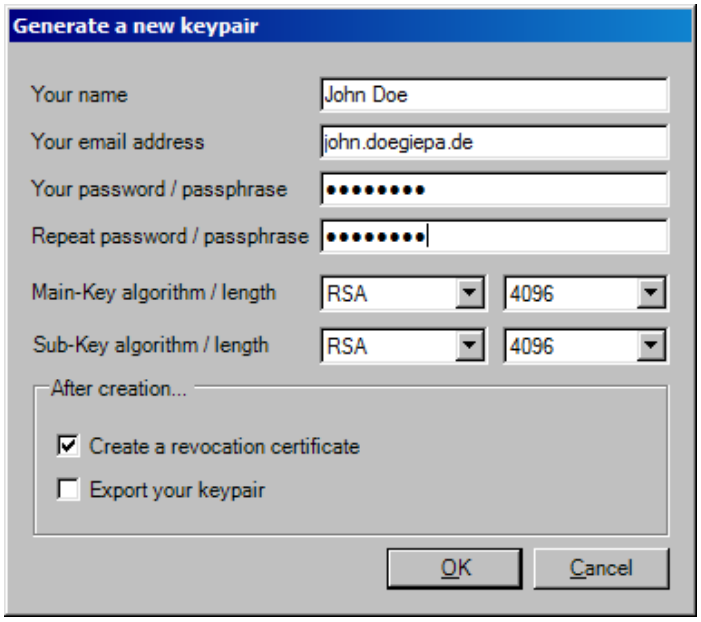


Or you will have to generate a new keypair for your selected account.

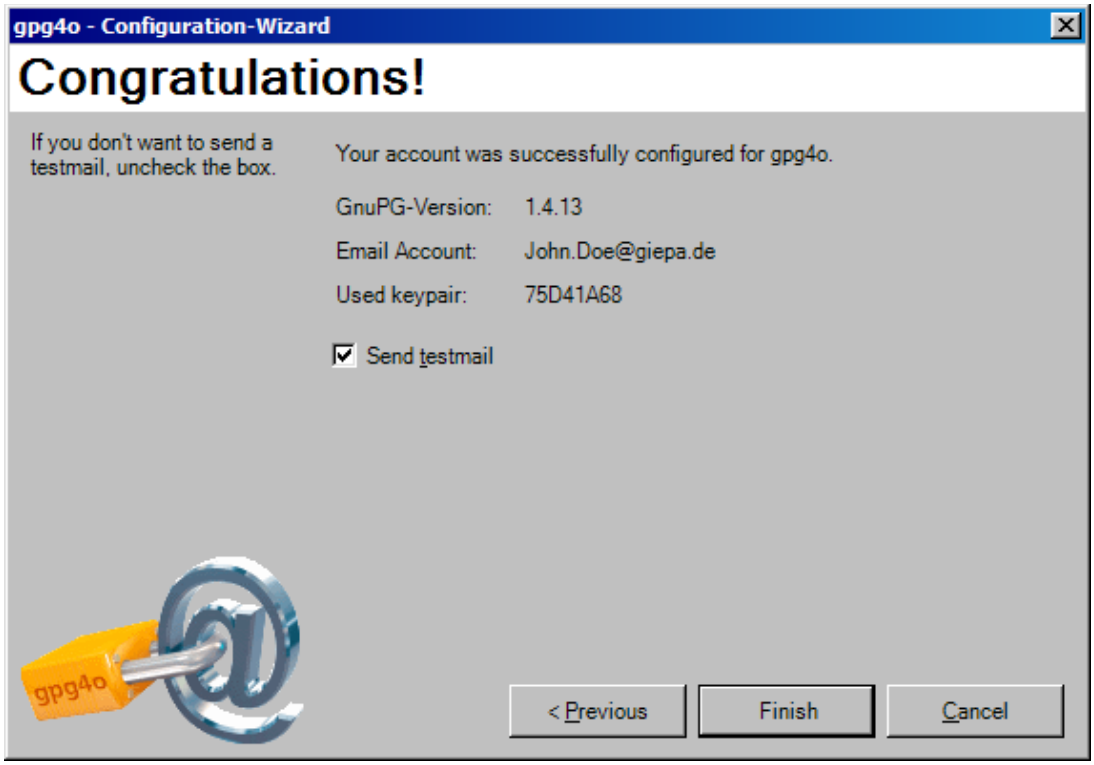
In order to generate a new keypair enter your name first, as shown in the screenshot below, as well as a passphrase. After having filled all required fields, click **„Generate“** and your new keypair will be generated.



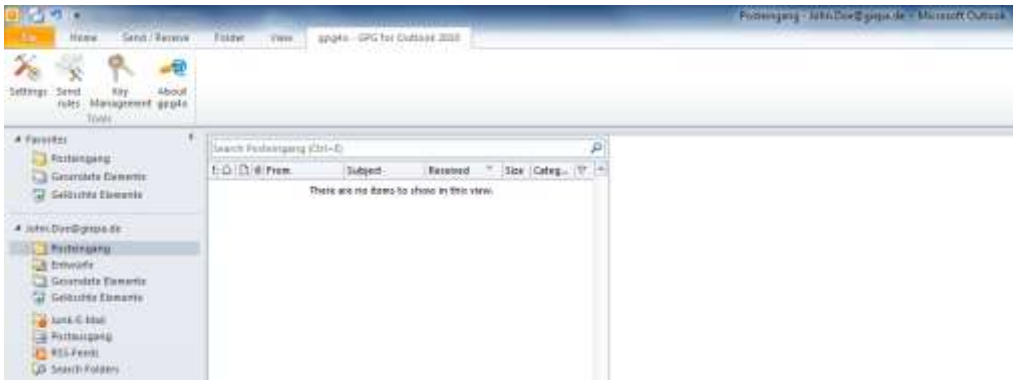
If you want to make further settings for your new keypair you can call up the advanced key settings by clicking **„Advanced…“**.



Finally, you will find again a brief summary which email account was configured with which keypair as well as the GnuPG-Version you utilize. If you leave the checkmark with **„Send testmail“** an encrypted test message will be sent to you automatically with which you can check the configuration of **gpg4o** as soon as you have clicked **„Finish“**.



After a successful installation you will see a new flag named **„gpg4o - GPG for Outlook ®“**, if you look at the menu bar in Microsoft Outlook ®. Here, you will find the key management, send rules and the possibility of modifying your settings.

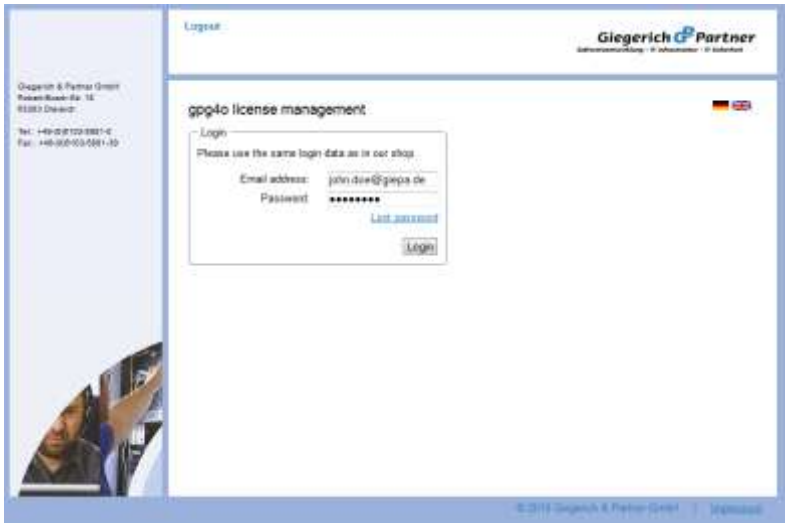


In order to obtain further information with regard to **gpg4o** please click **„About gpg4o“**. In the window appearing then you can find additional information concerning your license and the currently utilized version.

4 License-Files

4.1 Generating and Importing License-Files

After having processed the online-ordering of **gpg4o** you can manage your licenses via our web interface (http://licmgmt.giepa.de/). 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.

In order to make alterations to your licensing, click the **pen-symbol** (**Edit**).

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.

Subsequently, you can choose whether you want to download the license file directly or whether 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.

Email addresses which have already been entered can be individually adapted via the push-buttons **„Edit"** and **„Delete"**.

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

Now you can import the license. For this purpose open Microsoft Outlook ® and choose **„gpg4o – GPG for Outlook ®"** in the ribbon. There click the push-button **„About gpg4o"**. In the information window appearing now choose the item **„Import license"**. A file selection dialogue will appear. Browse to your license and choose **„Open"**. Now, your license file is imported and a corresponding message will appear which you can confirm by clicking **„OK"**.

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**.**

4.2 Period of Validity of the License

During the period of validity of the license you have the possibility to make use of the support in case of questions or problems. You may also obtain updates and install them. **gpg4o** works with a single license even with two computers and with several email addresses as long as the licensed email address is set in Microsoft Outlook ® with both computers. With the first download of the license the period of validity starts.

If the period of validity has elapsed it is possible to further utilize **gpg4o**. That means that you may continue to send encrypted/signed emails and to read encrypted/signed emails. However, you do not have the possibility any longer to install new updates.

4.3 Extension of the Product Maintenance

With an extension you can obtain new product updates for **gpg4o**. It is also possible to contact the support via emails for the purchased period of time. The duration of validity of the license is increased by the number of years of the extension.

The developer team of **gpg4o** improves the program continually and integrates customers' suggestions into a new version. After having purchased an extension this license will have to be imported into **gpg4o** one time.

5 Utilizing gpg4o

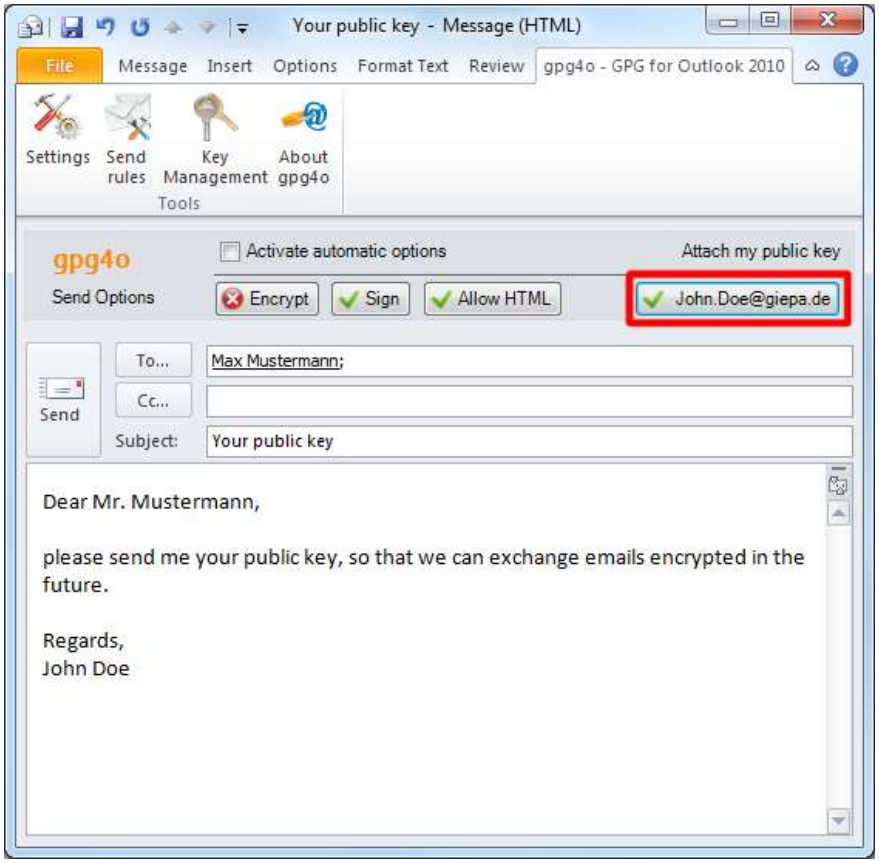
After **gpg4o** has been configured and corresponding keypairs for your email accounts have been generated you now have to inform your communication partners of your public key. A keypair consists of two keys: One private-key and one public-key. When generating the keypair you were asked to enter a passphrase (password) for the keypair.

You must **NEVER** send your passphrase or your private key**!**

You should keep this passphrase as safely as your other passwords and should **never tell it to anyone else**.

5.1 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 you are kindly asked to generate a new email and to click the button below **„Attach my public key“**. In doing so, your public key will be enclosed with this mail 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.



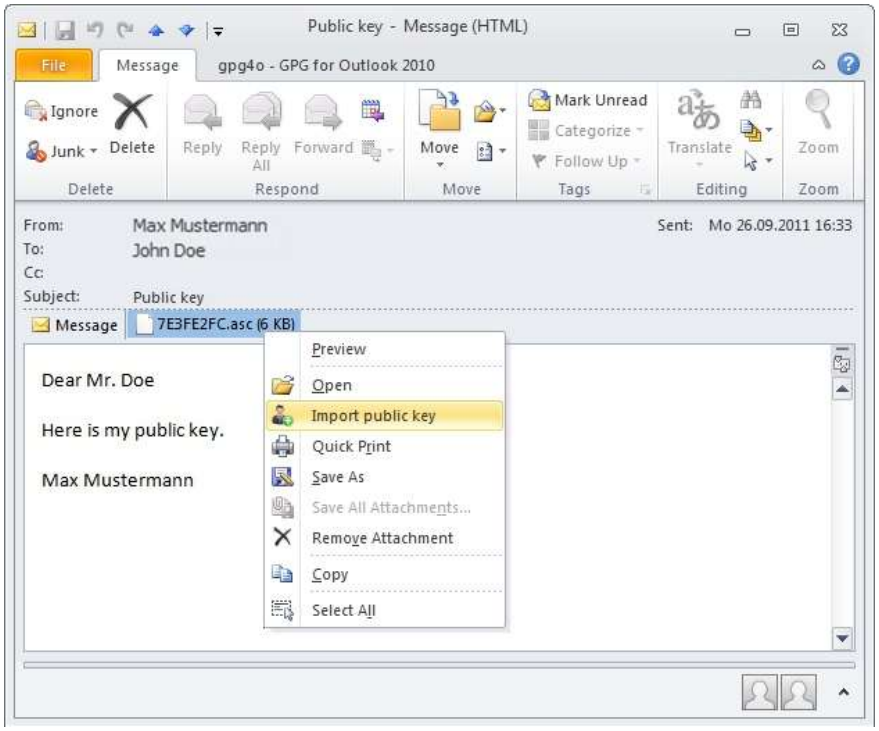
Please mind that when directly sending emails, the standard options you have chosen will be utilized unless you have defined rules (compare **chapter 7**). Mind carefully, when you encrypt emails and when you don't.

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

You must **NEVER** send your passphrase or your private key**!**

5.2 Importing Public Keys

In order to be able to send an email encrypted or to verify a received, signed email you need the sender's public key. If your communication partner sends you a key as an attachment of an email you may import said key in the menu ribbon with the help of the context-menu as well as via the menu entry **„Import public key“** into your key management. Furthermore, you have the possibility of importing the key from a key server (compare **paragraph 6.2**). This exchange of the public key must be performed once with each communication partner with whom you want to exchange encrypted emails.

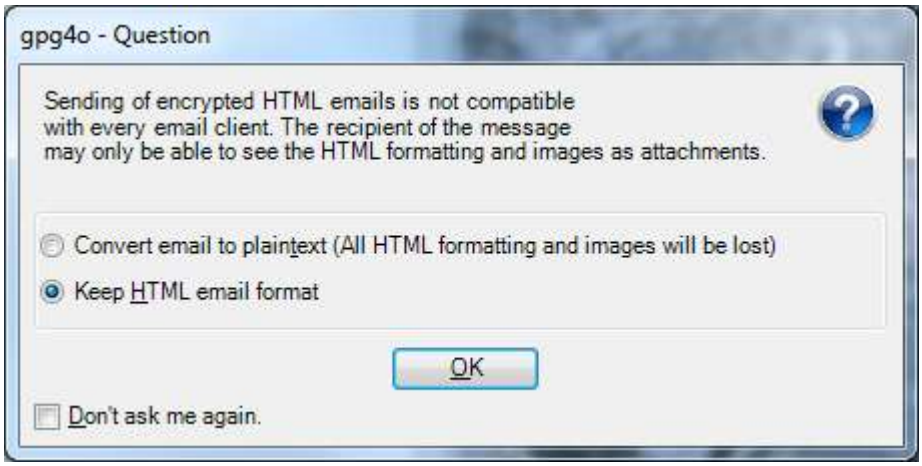


5.3 Sending Encrypted and/or Signed Messages

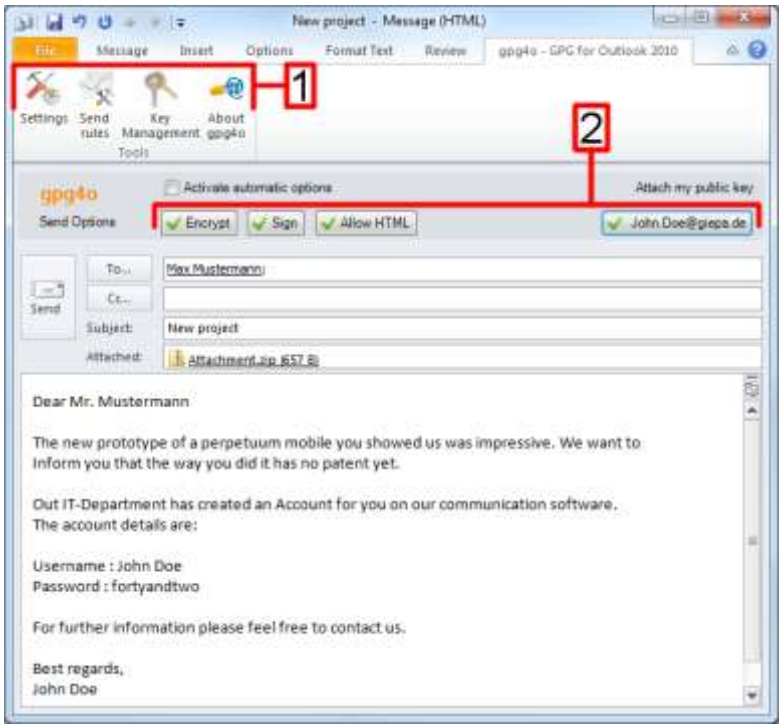
You can now send encrypted and/or signed emails. In order to guarantee the best possible compatibility with all current email programs you should write your emails in plain text format. Of course, you also have the possibility of sending emails in HTML-format. A corresponding selection possibility will appear as soon as you choose the option **„Encrypt message”**.

If you want to define your selection as default you will have to activate the checkmark ***„Don’t ask me again”***.

In the account settings (see **paragraph 8.3**) you can reset this option.



Before sending your email, set the checkmark for **„Sign"** if you intend to send your email signed or for **„Encrypt"** to send it encrypted. If you selected both your email will be send signed and encrypted. Continue with a click on **„Send"**.

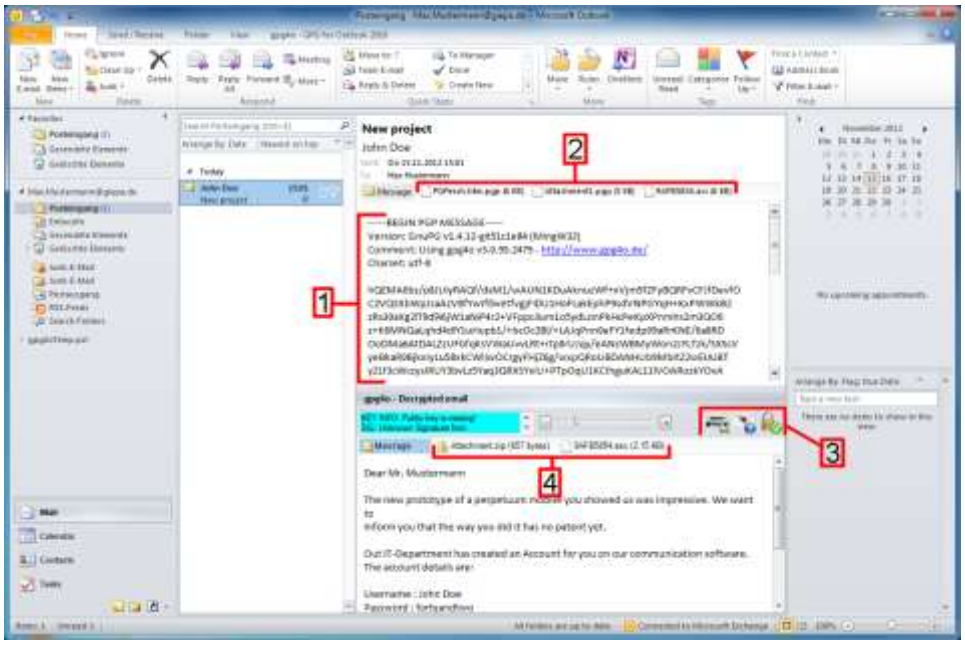


1 – Settings for gpg4o
2 – Here you can set, if your email gets encrypted and/or signed and if you want to send your public key as attachment.

You will now be asked to enter your passphrase (password). For this purpose kindly use the passphrase you have chosen for your key when setting **gpg4o**.

5.4 Receiving of Encrypted and/or Signed Messages

If you receive an encrypted and/or signed email another field will be shown below the read-only view. Here, you can now read the emails decrypted or without signature blocks. In addition, symbols signalize whether the email was received as encrypted or signed mail. In this case the coloured box on the left will show the validity of the signature.



1 - Encrypted email

2 - Encrypted attachment and public key of Mr. Mustermann

3 - Decryption status

4 - Decrypted attachment and public key of Mr. Mustermann

5.5 Sending and Receiving Encrypted Attachments

As soon as you send an encrypted email which contains an attachment or as soon as you receive such an email **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 check mark is placed with **„encrypt“** all attachments will be encrypted as well in addition to the text of the email.

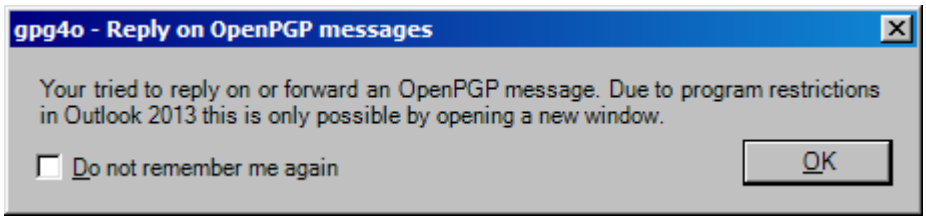
If you receive an encrypted email with attachment you can either save the attachment or open it directly. For this purpose the options **„Preview“**, **„Open“**, **„Save as…“** and **„Save all attachments…“** are placed at your disposal in the context menu (click right mouse button on the attachment).

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

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 ®.

5.6 Reply/Forwarding of Emails under Office 2013

If you want to answer an encrypted email in Microsoft Outlook 2013 ® or if you want to pass it on, 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. This can be achieved by clicking the button **„OK“** in the message displayed.



6 Keys

6.1 Definition of Key Trust

In principle the transfer of public keys is safe as long as you can trust the persons who receive your public key. However, it cannot be excluded that a third party generates a public key in your name and circulates it. If this person has access to your emails it can decrypt and read them with the faked public key. Having done this, the third person could then send you the emails again with your original public key so that you will not notice that your emails were compromised. In order to avoid such a situation there is the possibility of signing keys and, thus, guaranteeing their authenticity.

For this purpose click the item **„Key management“** in the ribbon **„gpg4o - GPG for Outlook ®“** and select the key you want to sign. When clicking the right mouse button a context menu will appear where you choose the item **„Sign...“**. In the following dialogue you can define with which key you want to sign. Furthermore, you can indicate how sure you are of the authenticity of the key to be signed. With this selection the strength of the signature is defined.

You can additionally define to which extent you trust your contacts to sign external keys and to classify them as authentic. For this purpose select one key from the key management and click the entry **„Define trust...“** in the context menu (click right mouse button). In the following dialogue several selection options have been placed at your disposal in order to define the trust into this contact. You should only choose the option **„I trust him absolutely“** for your own keys, however, as this option also has an influence on the behaviour of the validity of the keys and is not intended for external keys. The trust level indicated by you remains a secret of GnuPG and will never be exported or transferred to others.

6.2 Utilization of Key Servers

In addition to the possibilities with regard to the sending of keys, explained in the **paragraphs 4.1 and 4.2**, you may also distribute your public key via a key server and, at the same time, import public keys of your communication partners from it.

For this purpose click the item **„Key management“** in the ribbon **„gpg4o - GPG for Outlook ®“** and select your key. When clicking the right mouse button the context menu will open from which you choose the entry **„Upload key to key server…“**. Here, you have the possibility to select a key server and to make your public key accessible with it. 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.

For importing a key via a key server, click the item **„Key management“** in the ribbon **„gpg4o - GPG for Outlook ®“**. In the menu bar of the new window, click **„Key“** and there **„Search key server…“**. Here, you have the possibility of entering the name or the key-ID of your communication partner and of selecting the key server to be utilized. If the searched key is found you will be able to choose and import it.

6.3 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 for the 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. In the key management you have to select the key for which a revocation certificate shall be generated. You will be asked to indicate the reason why you want to generate a revocation certificate. After having entered the reason, indicate the folder where the revocation certificate shall be saved.

In order to withdraw a key you have to import its revocation certificate. Thus, this key becomes permanently unusable. With the withdrawal the public key is updated and must therefore be uploaded to the key server and/or be transmitted to your communication partners. If you have imported a revocation certificate for a key you will have to generate a new keypair and have to upload its public key to a key server and/or distribute it to your communication partners by email.

7 Send Rules

In order to prevent you from having to indicate the settings for encrypting and signing for each of your emails there are send rules in **gpg4o** doing that for you (see **paragraph 7.2**).

In this window you also have the possibility of activating the domain based key search (see **paragraph 7.1**).

7.1 Domain Based Key Search

In order to prevent you from having to search a corresponding key for every missing key of a recipient or if you possess a global key for a certain company you may activate the **„domain based key search"**. Thus, a possible matching key from the domain of the recipient will be automatically proposed to you from your key list in case of a missing key.

For activating the **domain based key search** click the item **„Send rules"** in the ribbon **„gpg4o - GPG for Outlook ®"**. In the appearing window, place a check mark with **domain based key search**. **gpg4o** will do the rest for you.

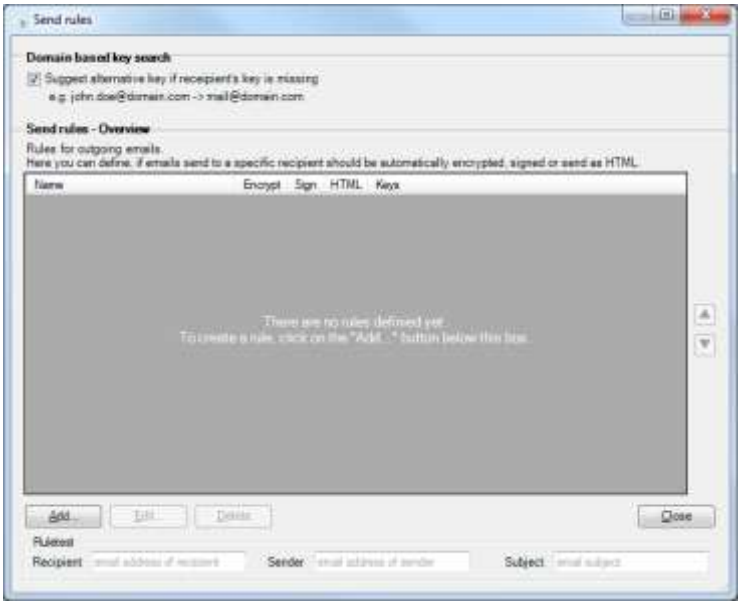
If you write an email to **„Max.Mustermann@giepa.de"** but if you do not possess a key for this recipient, **gpg4o** will now offer you an alternative key from the relative domain.

If you refuse this key you may select another key for encrypting your email as usual.

7.2 Management of Send Rules

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

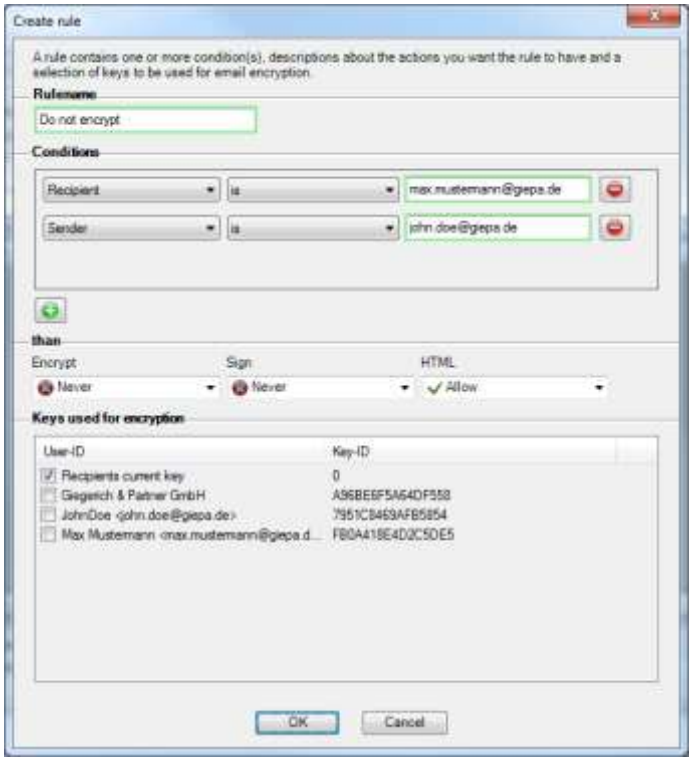
For this purpose click the item **„Send rules“** in the ribbon **„gpg4o - GPG for Outlook ®“**.



For creating a new rule click the button **„Add“** in the overview.

Enter a name for this new rule in the opening window. Afterwards, complete the conditions. When working out the conditions mind to design them as specifically as possible in order to avoid later conflicts.

Having done this, choose the encryption options to be utilized and the public keys of the recipient(s). The keys will be utilized later for encrypting when sending the email if the rule is applied. If you want **gpg4o** to select the matching key for you, just leave the selection with **„Recipient's current key"**. Otherwise choose those keys here which shall be utilized for encrypting the email.



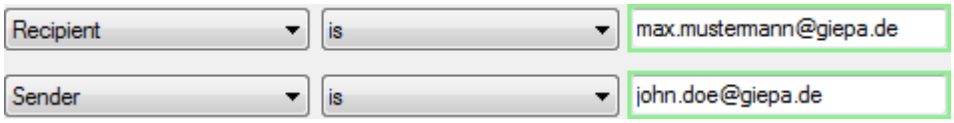
7.3 Rule Evaluation

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.

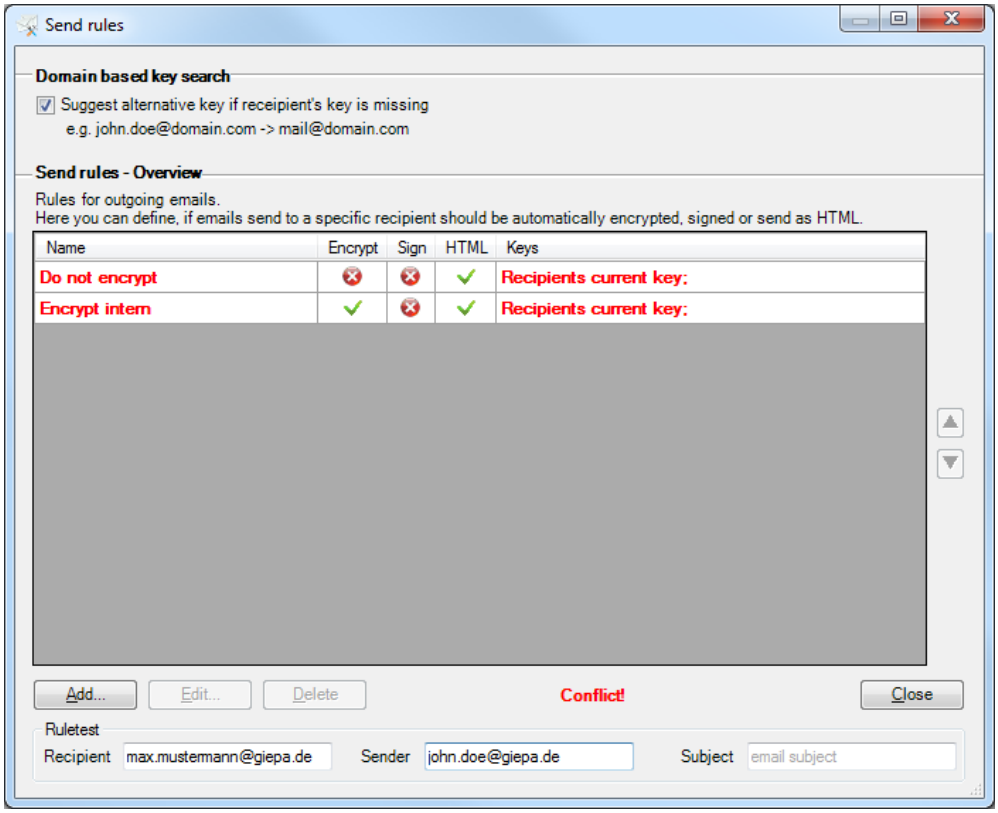
The following example shows two rules:

Rule **„Do not encrypt“** contains two conditions:



Rule **„Encrypt intern“** contains one condition:

If you write an email to **max.mustermann@giepa.de** now and if you select **john.doe@giepa.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 may add a further condition to the rule **„Encrypt intern“** for a sender who is not **john.doe@giepa.de**.

8 Setting

With the settings you can adjust important options of gpg4o. Modifications of the options, even if menu points are exchanged, only become effective after saving.

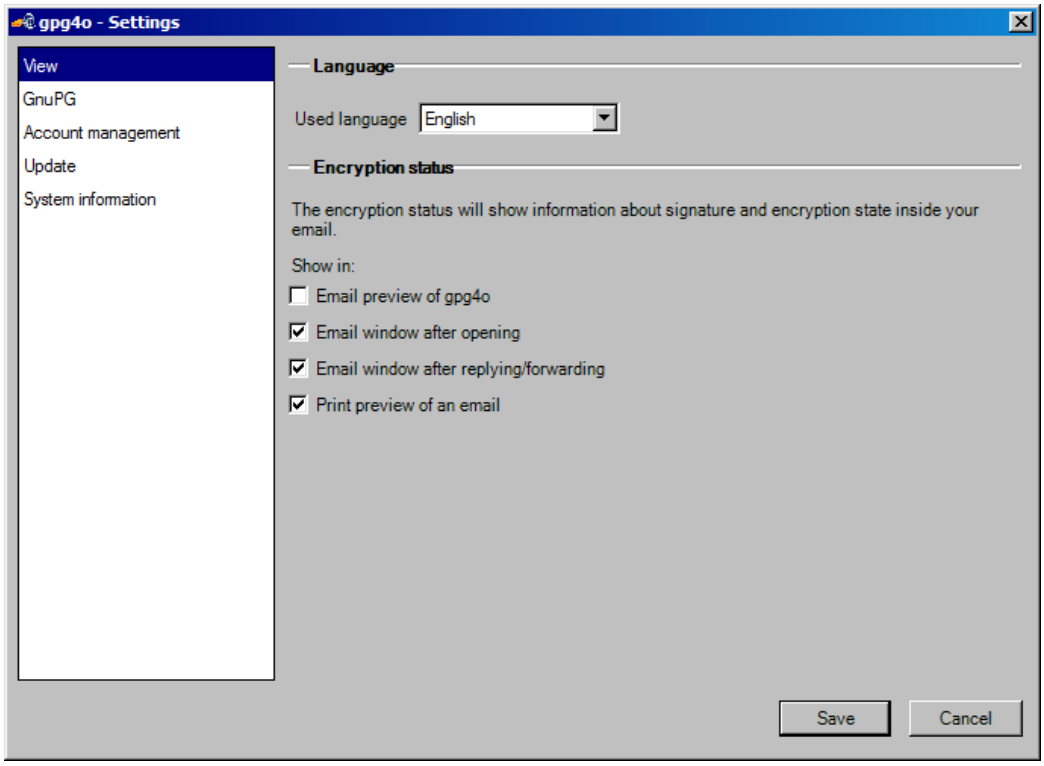
8.1 View

8.1.1 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.

8.1.2 Encryption Status

Here, you may select in which areas of gpg4o the information with regard to decryption and signature shall be displayed to you within an email. By default the display is only shown in the normal email preview.



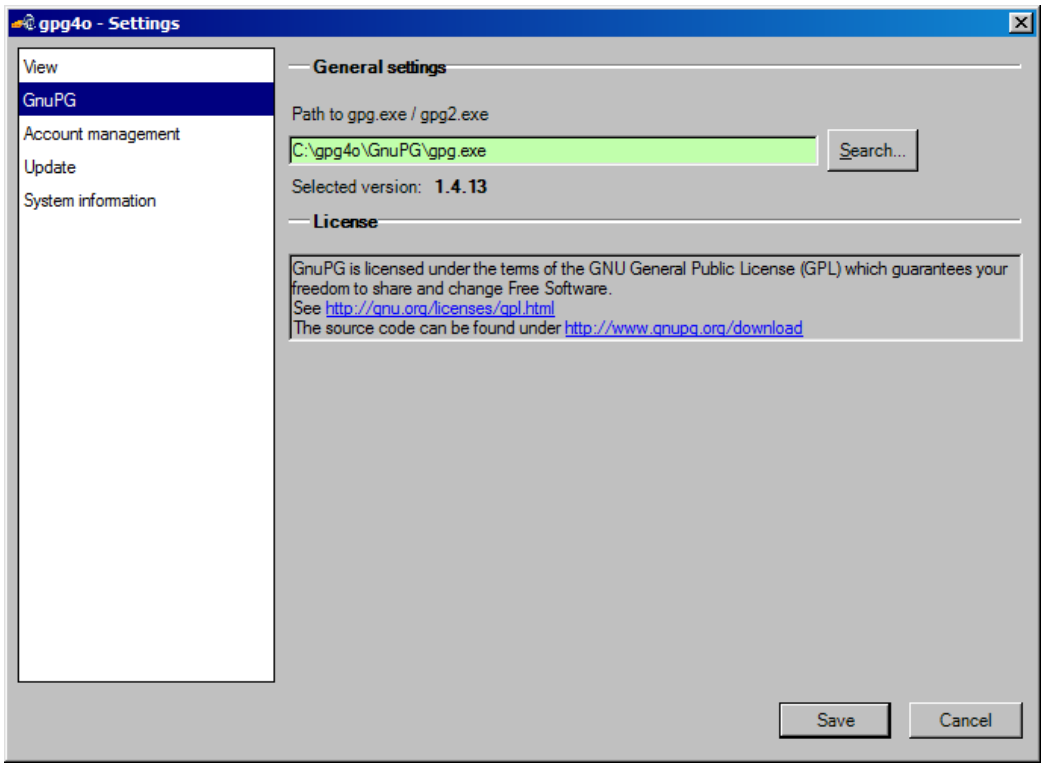
8.2 GnuPG

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

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“** 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.



8.3 Account Management

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

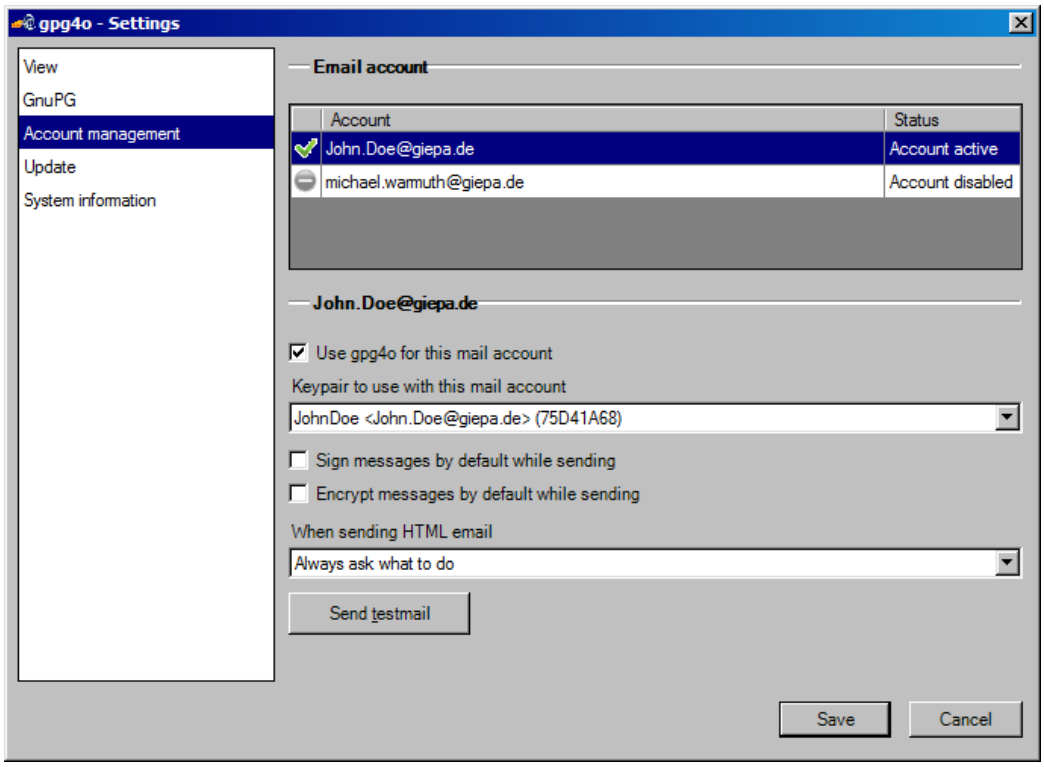
Under the name of the selected email you will find the corresponding current settings. Activate the checkmark at **„Use gpg4o for this account“**. Now, the add-in will support the marked account.

With the selection box **„Keypair to use with this mail account“** you define which keypair shall be utilized for signing and decrypting messages.

With the next two check boxes the default behaviour of **gpg4o** with regard to the sending of emails is defined. In the preliminary setting emails are not signed and/or encrypted by default. You can perform further settings with the help of the send rules (also compare **chapter 7**).

The selection box **„When sending HTML emails“** serves the purpose of defining whether when sending emails in HTML-format you have to be asked if this email shall be converted by default to the plain text format before.

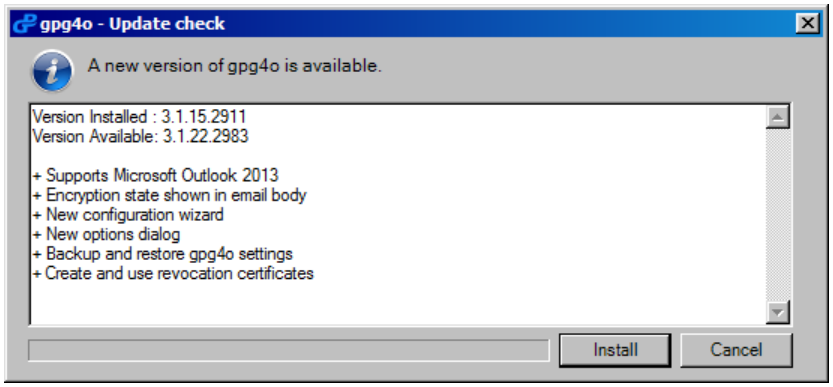
You may perform a test for the selected account and send a test email to the account. With the test email received you can check whether encryption and decryption work correctly with your settings.



8.4 Update

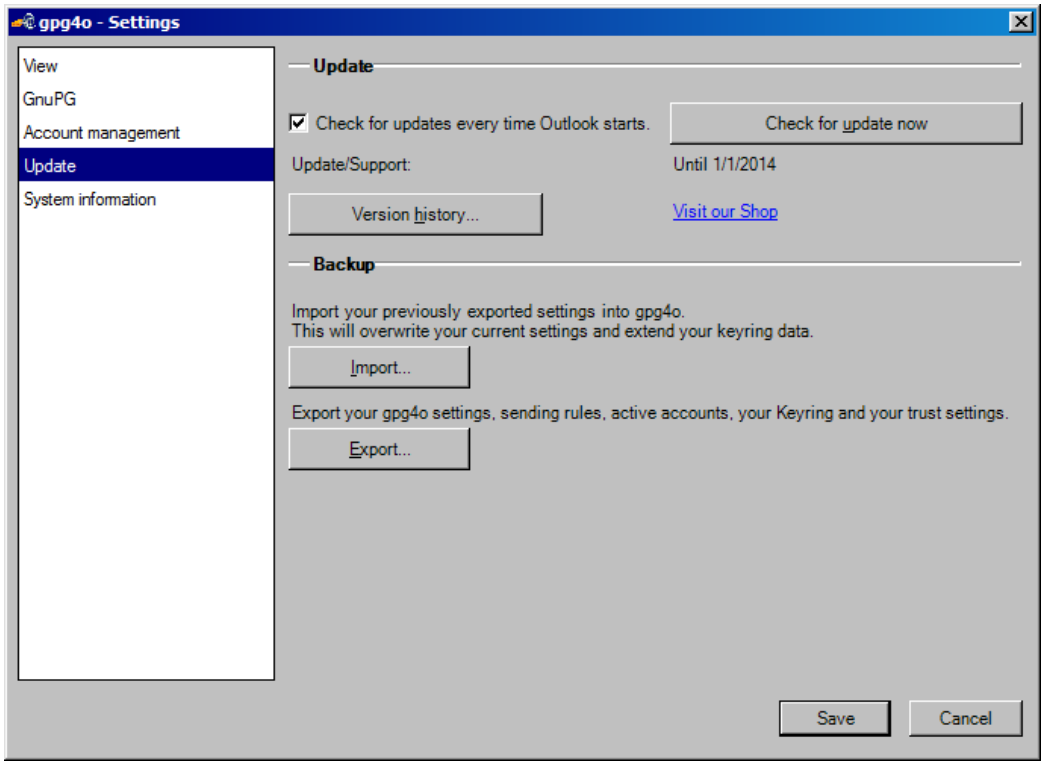
8.4.1 Update

On this page you can perform a manual verification with regard to updates by clicking the button **„Update check“**.



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 updates are installed in the background and do not require any confirmations on your part. When the installation is finished you should make a new start of 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.

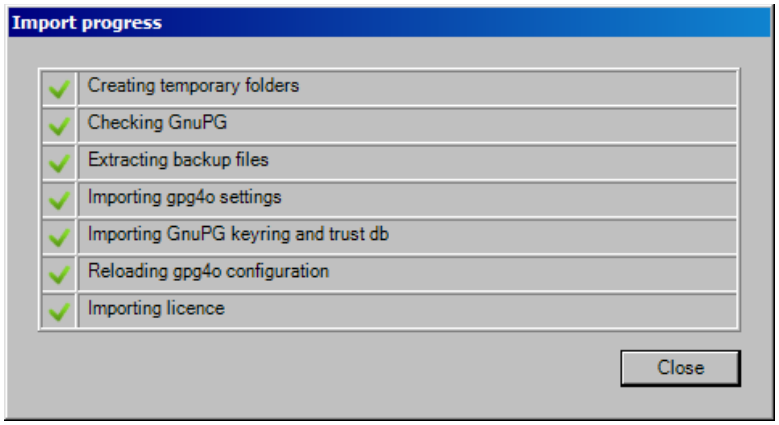
In the **„Version history…“** the individual releases and their improvements of gpg4o can be looked up.

8.4.2 Backup

On this page you can restore a saved backup or generate a backup, respectively. It is useful to generate a backup if you want to move to another computer with the system.

With **„Export“** your **gpg4o** settings, the send rules, the active accounts and your keyring with the trust settings are saved.

„Import“ your previously exported settings into gpg4o. This will overwrite your current settings. Your keyring is extended with the newly added keys and keys which were deleted since the last export, are included again.



Progress display of import

8.5 System Information

In the system information you can find details regarding the product gpg4o, the license, the operating system and GnuPG. There you can see, among others, the installation paths of the individual products.

9 Miscellaneous

9.1 What Is to Be Done in Case of Errors?

Unfortunately it is not always possible to completely exclude errors in software products and installations. Precisely in complex environments errors may happen which do not occur during development.

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

In order to be able to rapidly correct occurring errors we need detailed information of them.

- Please furnish all the details of the error occurred.
- Describe also the circumstances which have led to the error in order to permit us to reproduce it.
- Please inform us of the version utilized by you. You can see it by clicking **„gpg4o - gpg for Outlook ®“** in the ribbon menu of Microsoft Office ® and by selecting the push button **„About gpg4o“** in the following window.

Please send us the error reports as well as the log files via the contact form provided for this purpose (see **paragraph 6.2**).

If you have suggestions for improvement please send them to us via the same contact form for we always lend a ready ear to you for such problems.

9.2 Sending Log-Files

In order to send a log-file to our support, click **„gpg4o – gpg for Outlook ®“** in the ribbon menu of Microsoft Office ®. Here choose the push button **„About gpg4o“** and in the dialogue appearing then click **„Send Log-Files“**. Then, a preconfigured email will open automatically with the log-files as attachment.

9.3 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.

10 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.

10.1 Uninstalling under Windows XP

In order to uninstall **gpg4o** click **„System control"** in the Windows start menu and browse to the item **„Software"**. You will now see the list of all programs installed on your computer. Select **„gpg4o – GPG for Outlook ®"** and click **„Remove"**.

The same is true for a GnuPG-installation under XP.

10.2 Uninstalling under Windows Vista, 7 or 8

In order to uninstall **gpg4o** click **„Control Panel"** in the Windows start menu and browse to the item **„Programs"** there and afterwards to **„Uninstall Program"**. You will now see the list of all programs installed on your computer. Select **„gpg4o – GPG for Outlook ®"** and click **„Uninstall"** in the menu.

10.3 Uninstalling GnuPG

In order to uninstall **GnuPG** click **„System control"** in the Windows start menu and browse to the item **„Programs"** there and subsequently to the item **„Uninstall Program"**. You will now see a list of all programs installed on your computer. Select the installed **GnuPG** and click **„Uninstall"** in the menu.

10.4 Delete Personal Data

After having uninstalled **gpg4o** and **GnuPG** personal data will remain on the computer.

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

You can also delete the „Folder 1“ in which all personal **GnuPG** data can be found (personal keys, certificates, trust settings and program configurations).

In addition, you should also delete „Folder 2“ and „Folder 3“, there are the personal settings of gpg4o.

Folder 1:

C:\Users\<NAME>\AppData\roaming\gnupg

Folder 2:

C:\Users\<NAME>\AppData\roaming\giegerich&partner\gpg4o

Folder 3:

C:\Users\<NAME>\AppData\local\Microsoft_Corporation\gpg4o.vstXXXXXX

Please mind that the program **gpg4o** is not the **only** one which has access to **GnuPG-keys**. Deleting the data may have negative influence on other programs.

Important Note

By deleting the key files you permanently lose access to your encrypted emails! Without the matching keys your emails cannot be decrypted.