# gpg4o

Manual

Version 3.0

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 Microsoft Outlook 2010 ®

**gpg4o** was developed as an Add-In for Microsoft Outlook 2010 ® 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

# 3 Installation

## 3.1 Required Software

For installing you need the (GNU General Public License) GnuPG version 1.4.11 until version 2.0 which is exempt from charges and the Add-In **”gpg4o – gpg for Outlook 2010 ®”** developed by Giegerich & Partner.

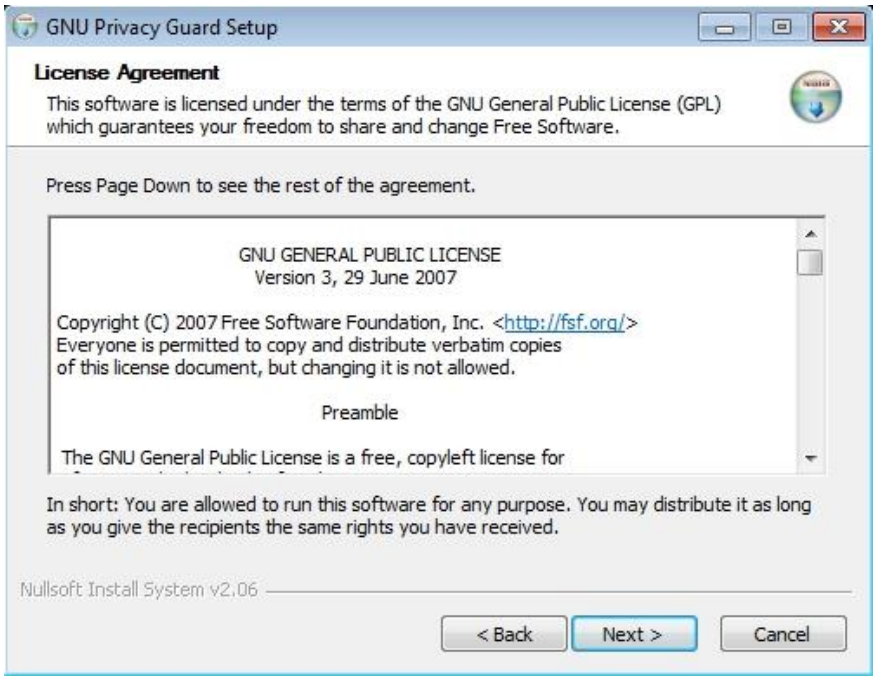
All necessary downloads can be found on:

www.gpg4o.de/en/product/downloads.html

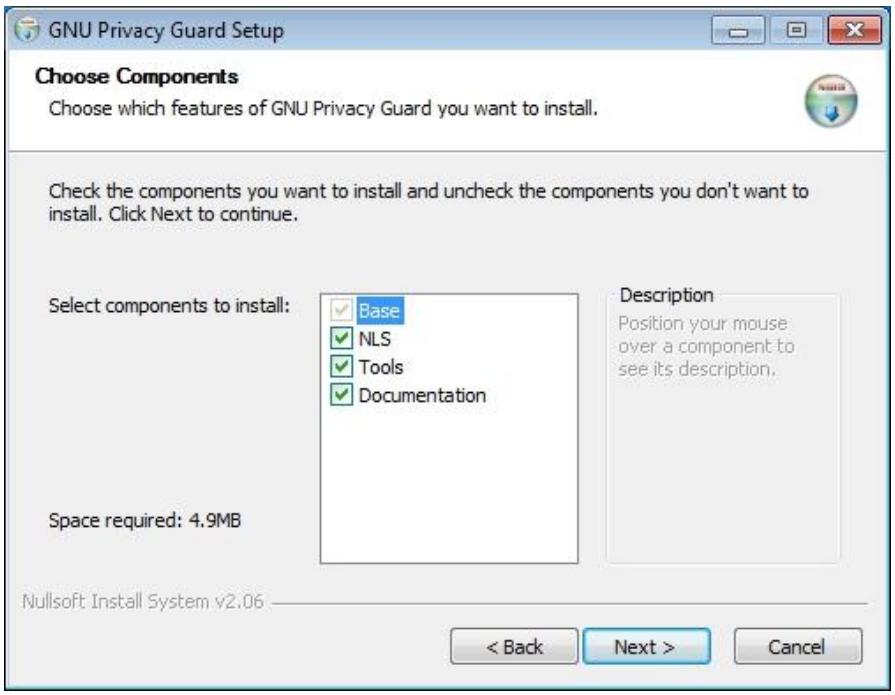
## 3.2 Installing GnuPG

After having downloaded GnuPG click ”Execute” in the download window of your browser in order to start the installation procedure of GnuPG. Alternatively, you may browse to your download folder and execute the file **"gnupg.exe"** there by double click. The window shown in the following will appear. Click **"Next"** in order to start the installation process. Please mind that you need an active Internet connection during the installation process in order to be able to download additional components if necessary (f. i. the .NET-Framework 4).

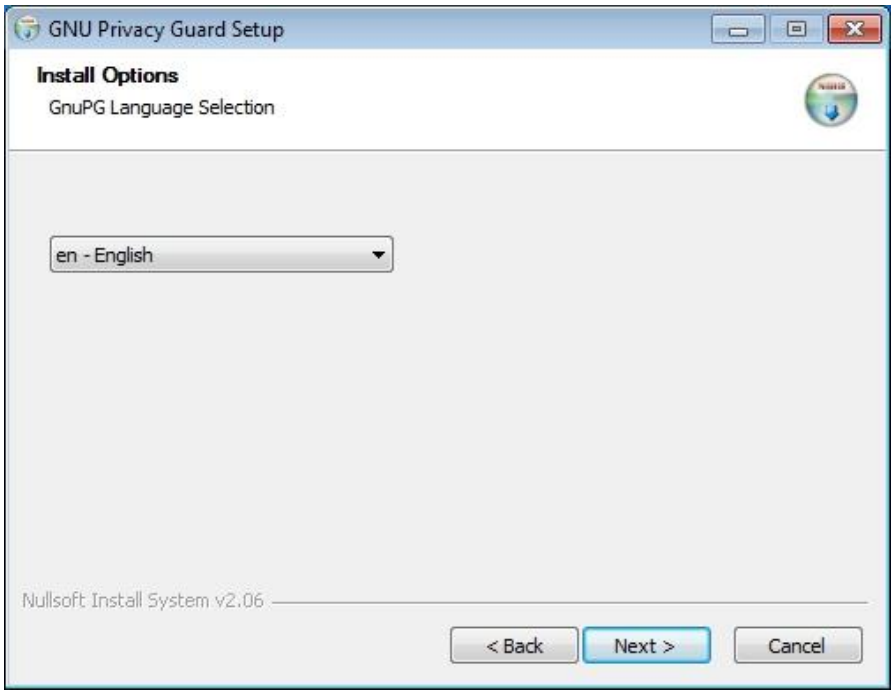

In the following dialogue you will see the License Agreement. Below the dialogue **”In short"** you will find a summary of the License Agreement with GnuPG. Once you have decided to accept the License Agreement (precondition for the installation), click **"Next"** and continue the installation.



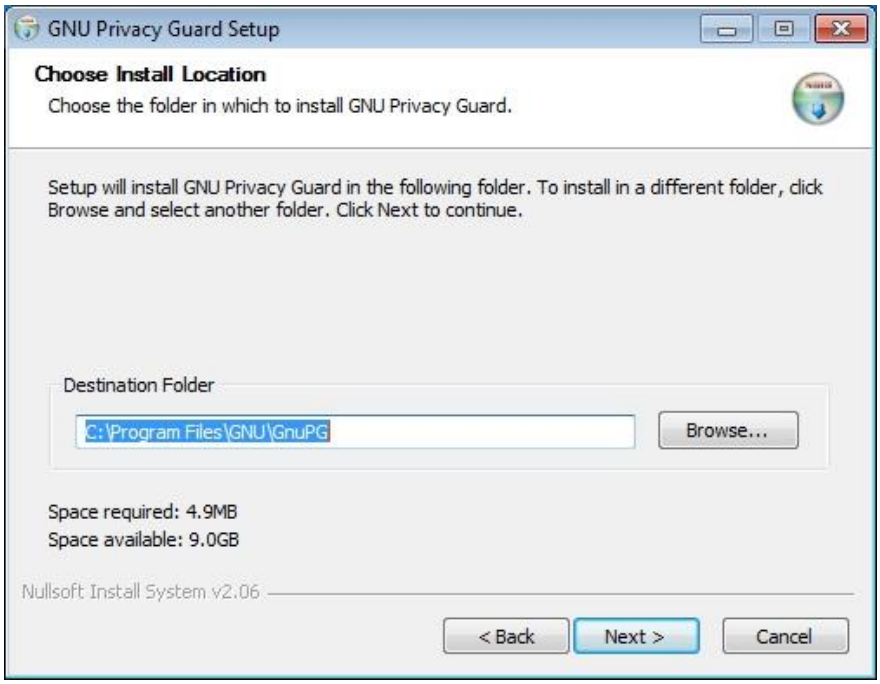

In the next dialogue you are asked to select the components to be installed. If you use GnuPG only for the utilization of **gpg4o** you can deactivate the checkmarks at **"NLS"** and **"Documentation"**.



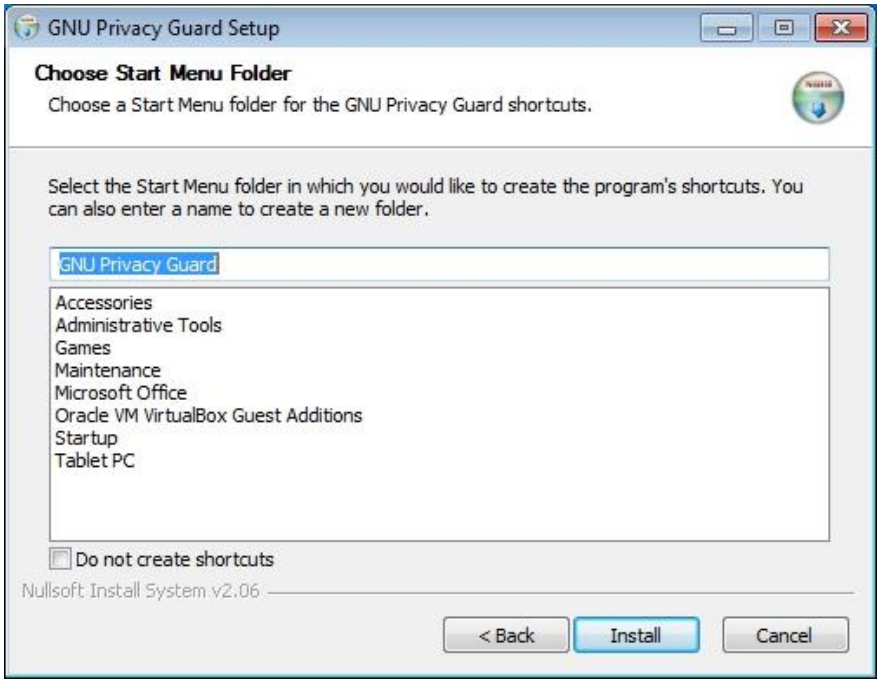
If, during the previous inquiry, you have also selected **"NLS"** to be installed a dialogue will appear after having clicked **"Next"** permitting you to define the desired language. The default language is that of your operating systems. In order to continue, please click **"Next"**.




In the next dialogue you will be asked to select the installation path. For most applications it is sufficient to adopt the preselection. Confirm the installation path with **"Next"**.

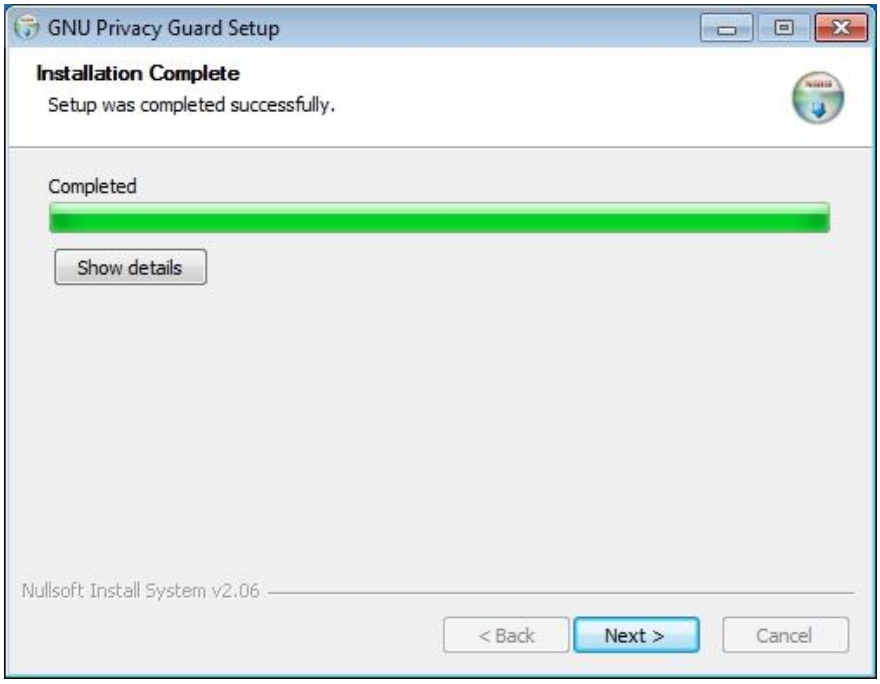


Afterwards, you may also define in which start menu folder the programs shortcuts shall be filed. Here, too, the preselection is generally the correct choice.

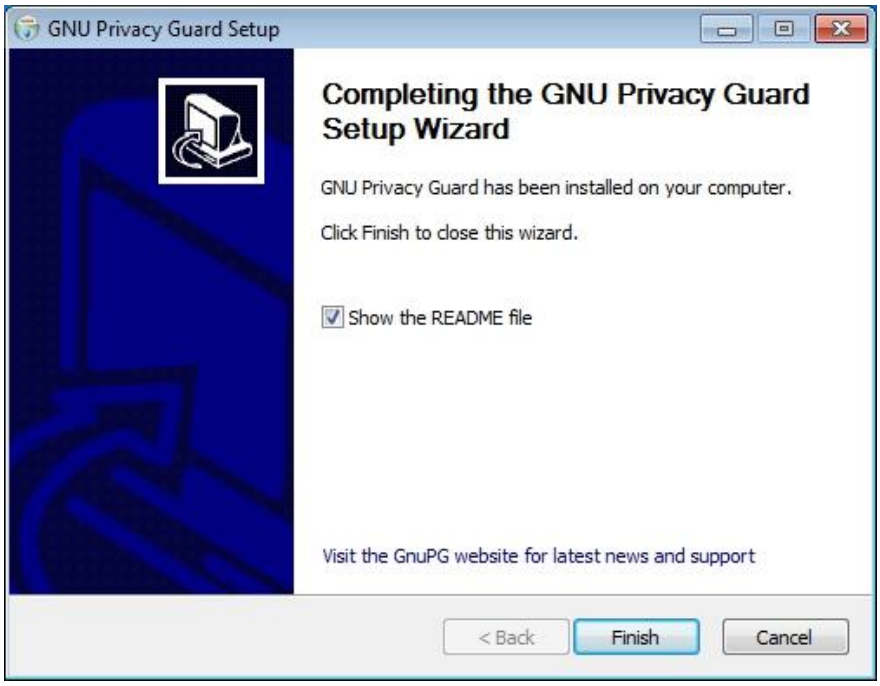



You may now assure yourself again that you have indicated all setups correctly. By clicking **"Install"** GnuPG will be installed on your computer.

In the terminal window you can see the installation details. By clicking **"Next"** you close the setup wizard.



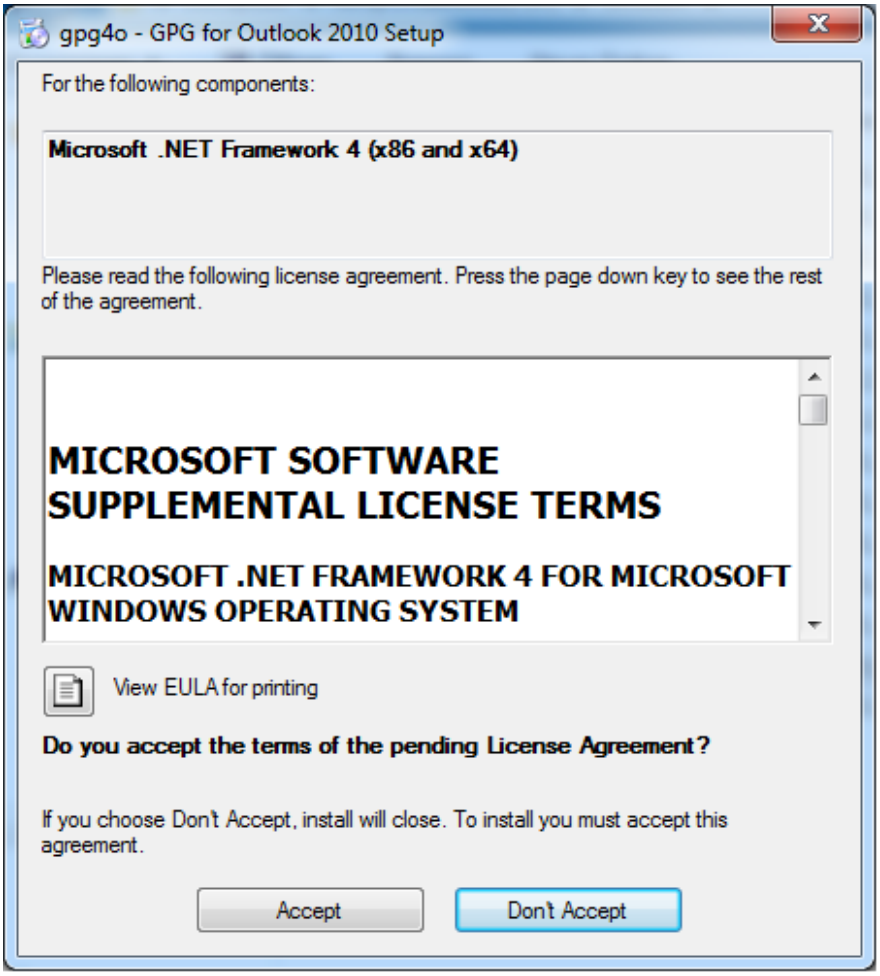

The installation of GnuPG has thus been completed and you may continue installing **gpg4o**.

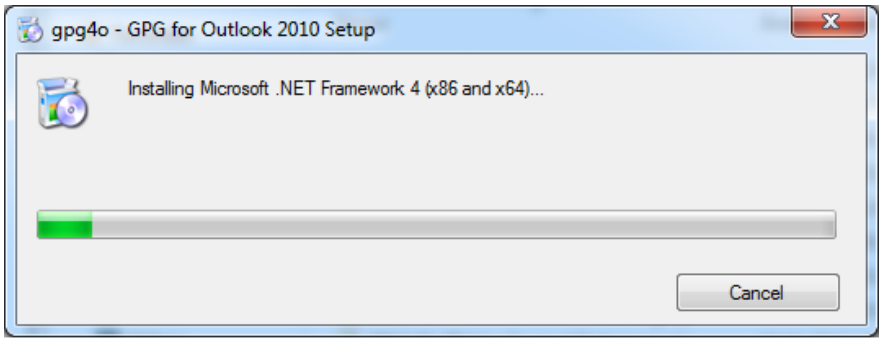


## 3.3 Installing gpg4o

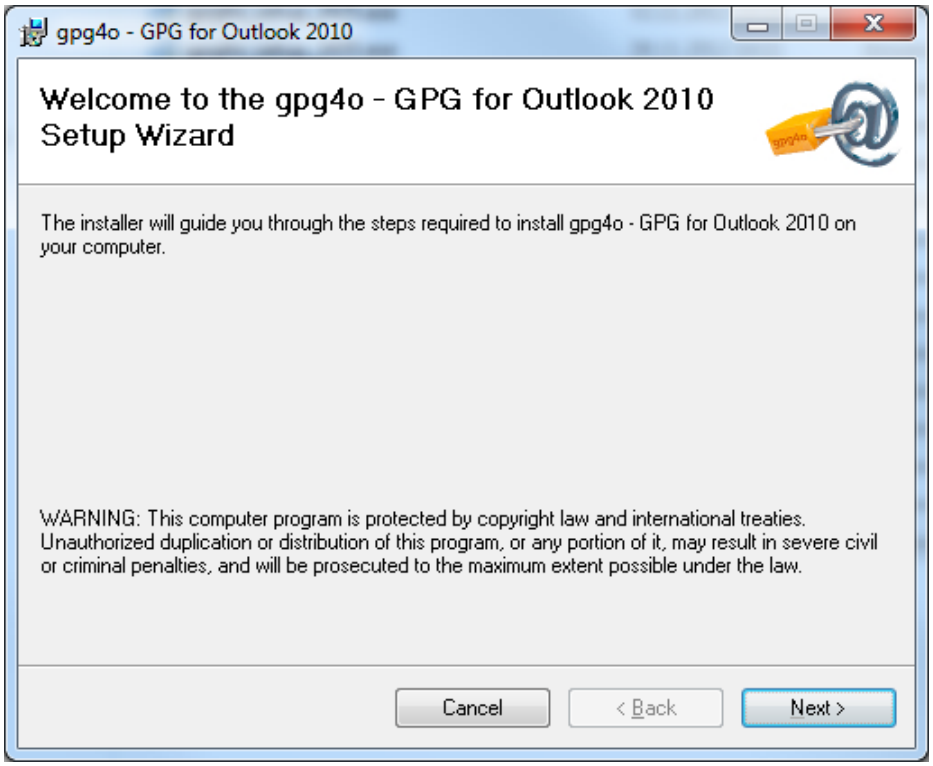
Before installing **gpg4o** please close the application Microsoft Outlook 2010 ®, as otherwise, there might be problems during installation. Having done this, execute the file **"gpg4o_setup.exe"** by double-click.

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.



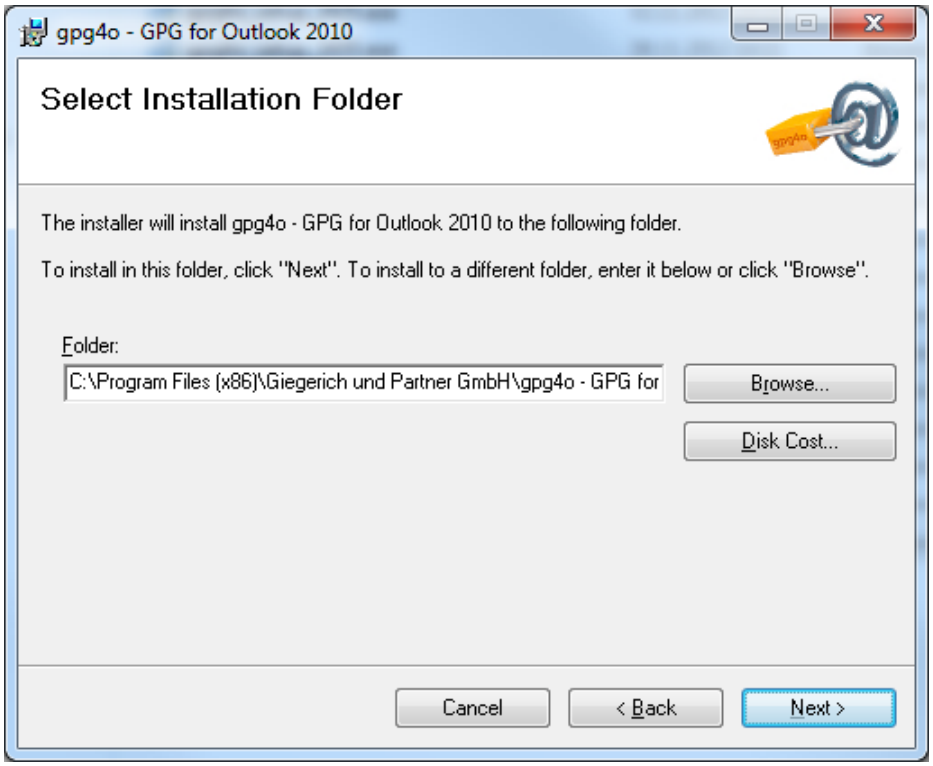




As soon as all the necessary components have been installed, the wizard will continue installing **gpg4o**. Click on **„Next“** to start the installation process.

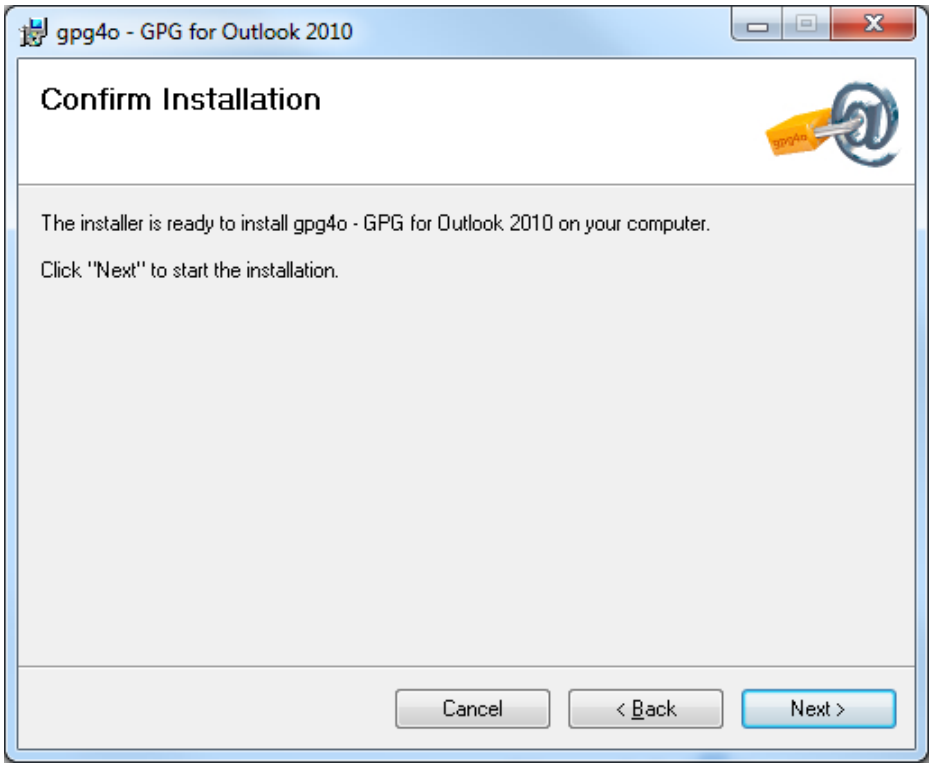



In the following dialogue you will see the End-User License Agreement. Once you have decided to accept the License Agreement (precondition for the installation), select the radio-button next to **"I Agree"**, click **"Next"** and continue the installation.

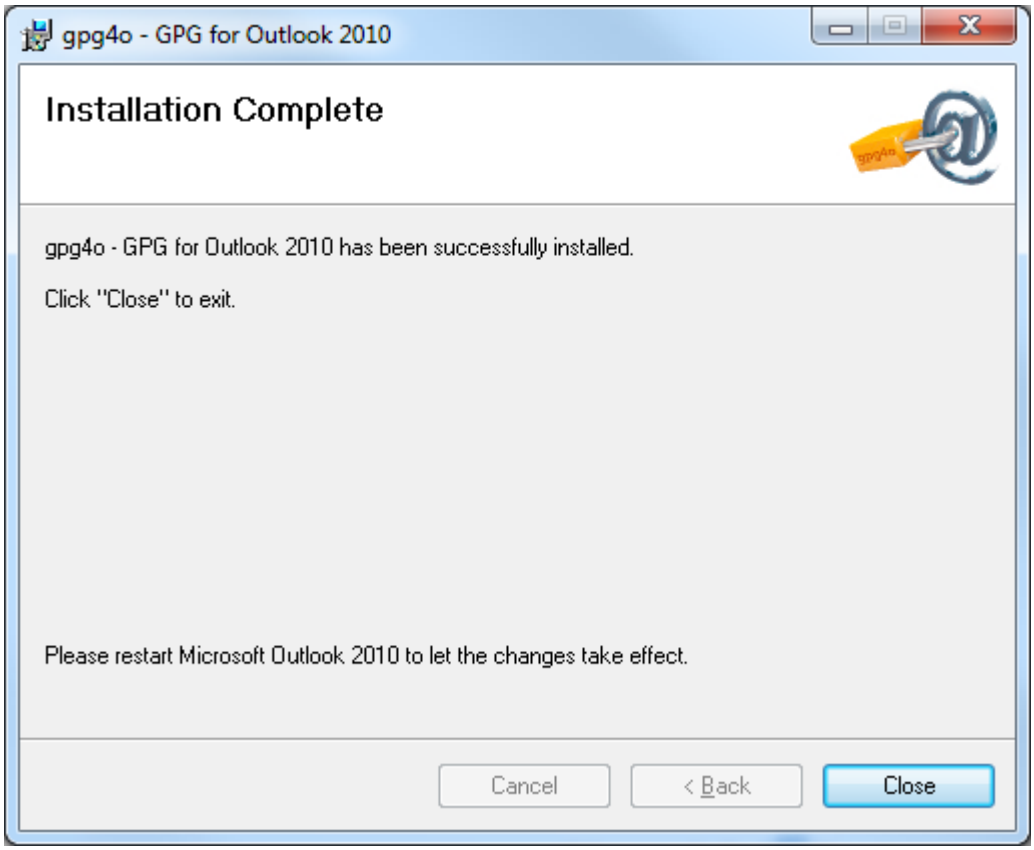

In the following dialog you will be asked, to set the installation path. Here the default setting is normally the best choice. Confirm the installation path by clicking on **„Next".**




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

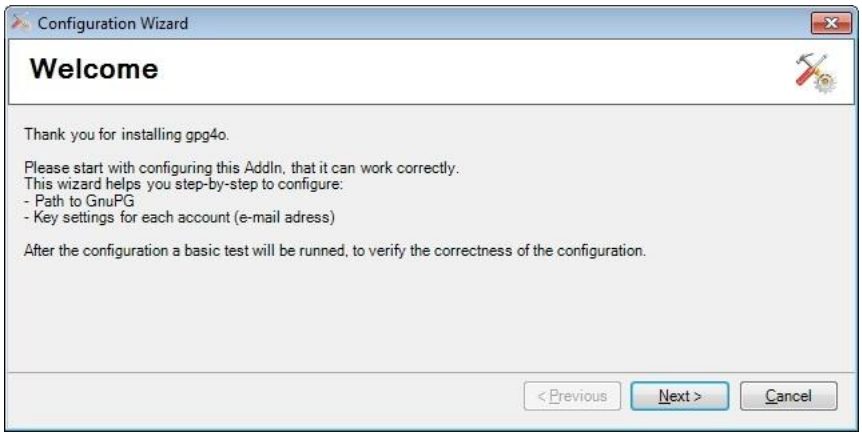



Now the installation of **gpg4o** is completed. You can start the configuration of **gpg4o** by restarting Microsoft Outlook 2010 ®.

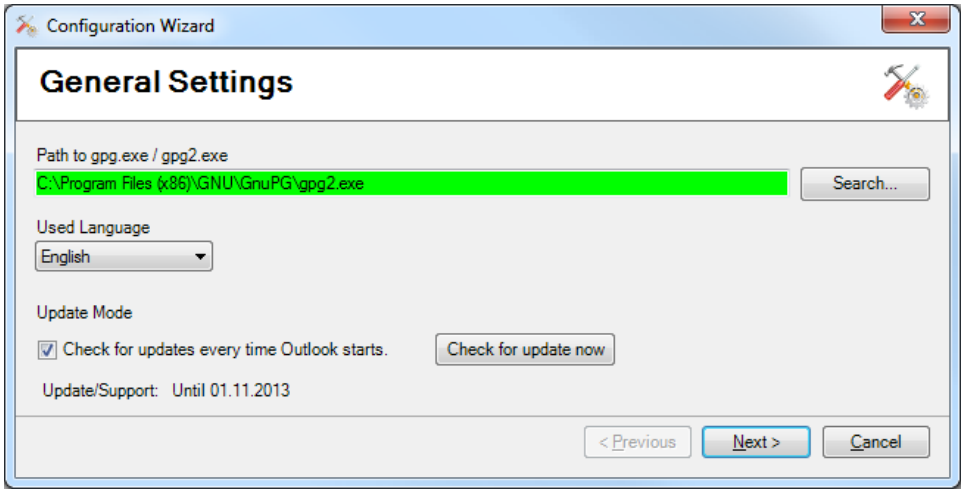

gpg4o - GPG for Outlook 2010
Installation Complete
gpg4o - GPG for Outlook 2010 has been successfully installed.
Click "Close" to exit.
Please restart Microsoft Outlook 2010 to let the changes take effect.
Cancel
< Back
Close

## 3.4 Setting gpg4o

Start Microsoft Outlook 2010 ® 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.




First of all, the installation path of GnuPG is inquired. Here, the default path of the GnuPG-Installation should generally appear. If this is not the case the selection will be highlighted red. In this case click **"Search"** and search for the GnuPG-installation on your hard disk and select the file **"gpg.exe"** or **"gpg2.exe"** in the installation folder. The installation path should now be highlighted green. Furthermore, you have the possibility of altering the language of **gpg4o**. Once you have made all the settings, click **"Next"** in order to continue the configuration.

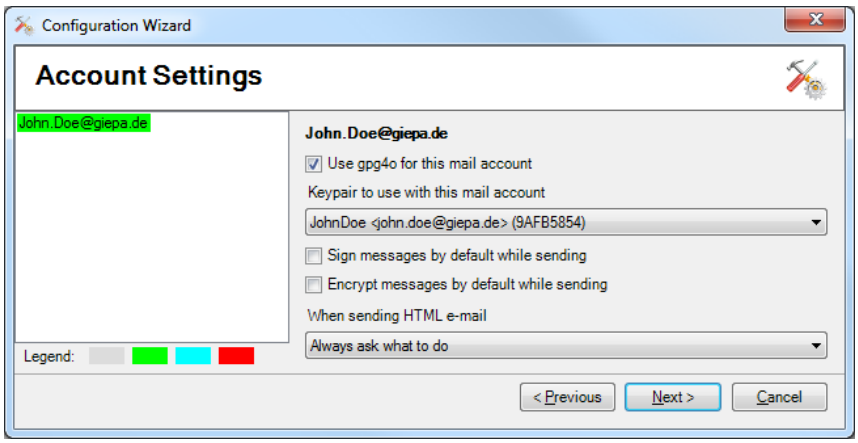


Next the individual email accounts will be configured (usually one email address corresponds to one email account). To this end select the desired email account on the left side of the configuration wizard.

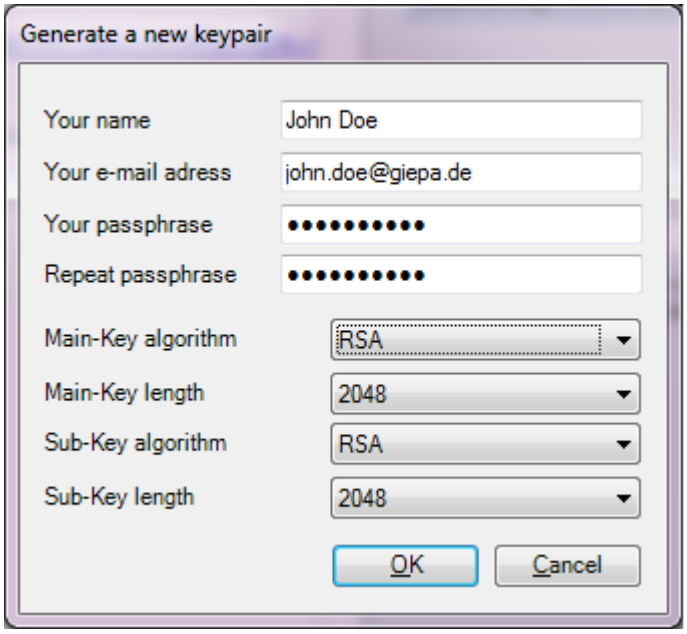
On the right side you will find the corresponding updated settings. Activate the checkmark at **"Use gpg4o for this account"**. Thus, the add-in supports the marked account.

With the selection box **"Keypair to use with this account"** you define which keypair shall be used for signing and decrypting messages.

With the next two check boxes the default behaviour of **gpg4o** with regard to sending of emails is determined. The preselected default is no signing and/or encrypting of emails. The function of the lowest option is to determine whether when sending HTML-mails a default enquiry has to be made if said mails shall be converted into the plain text format.



If you do not have a keypair for your email address yet you can generate a new keypair via the selection menu. For this purpose click **"Generate new keypair"** in the selection box **"Keypair to use with this mail account"**. In the following dialogue enter your name and the desired passphrase (password). In addition, you may also define the length of the two keys (main-key and sub-key) Afterwards, click **"OK"**.

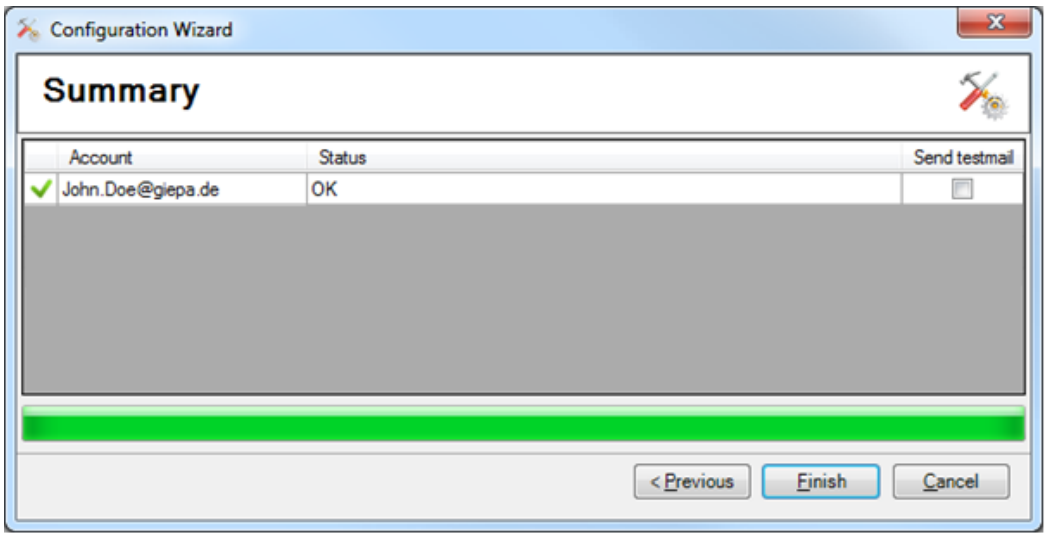



*Note: The longer the key the higher the quality and, thus, the security of encryption of your emails and their attachments.*

After the information that the keypair has now been generated the entry fields will be deactivated. At that time it is no longer possible to modify the entries. In the left bottom of the dialogue field a progress bar appears. The time required for generating the key mostly depends on the hardware utilized by you. It is possible that this procedure can take 30 seconds or more. After the keypair has been generated you will get back to the configuration wizard. Here, you will now see the newly generated key. If you use several email accounts, repeat the procedure described for the other email addresses.

Finally, the keypairs are checked and the result will be displayed on the **“Summary”** page.

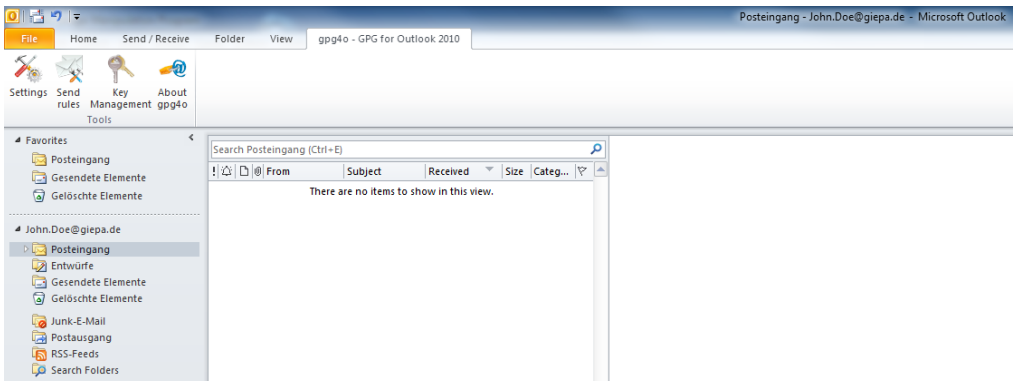
By placing a checkmark in the last column **„Send testmail“** you can check your **gpg4o** installation. For this you will receive a testmail after completing the **„Configuration Wizard“**.




If errors occur here, please send an email with the log-files to [support.gpg4o@giepa.de](mailto:support.gpg4o@giepa.de). In **chapter 6**, **"Miscellaneous"** you can find a description of how to find the log-files and how to send them to us.

Click **"Finish"** in the configuration wizard now in order to terminate the configuration.

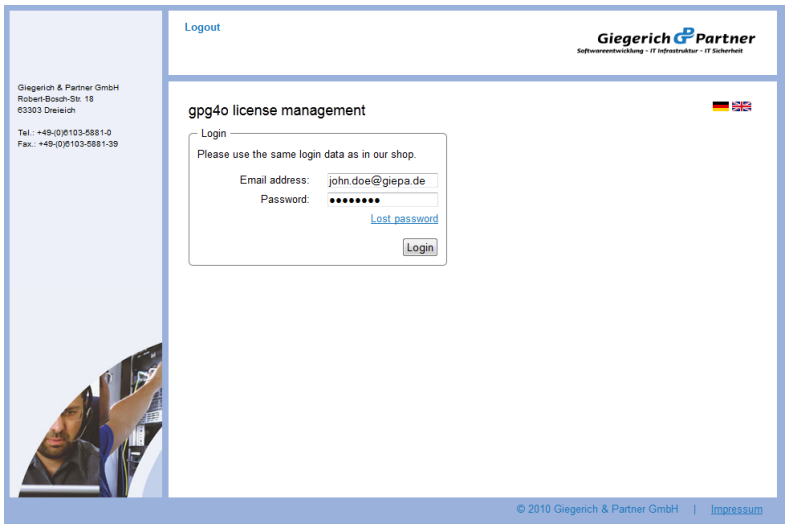
After a successful installation you will see a new flag named **"gpg4o - GPG for Outlook 2010 ®", i**f you look at the menu bar in Microsoft Outlook 2010 ®. Here, you will find the key management and the possibility of modifying your settings.




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.

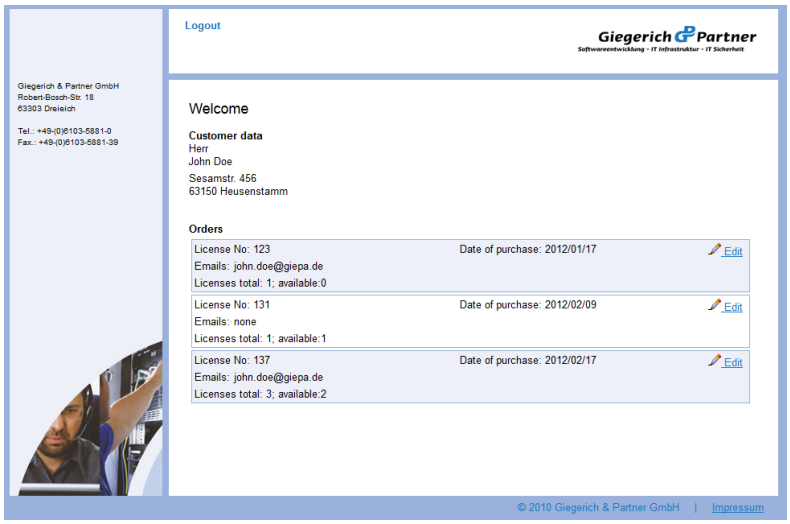
## 3.5 Generating and Importing License-Files

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 license).



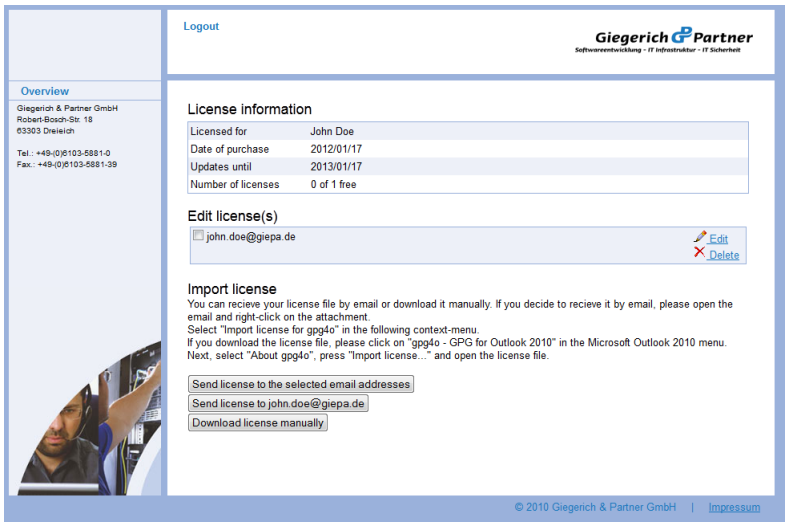

Now enter the email address you desire. In order to be able to enter several email addresses at once, separate them from each other with a new line.

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 2010 ® and choose **”gpg4o – GPG for Outlook 2010 ®”** 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 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.

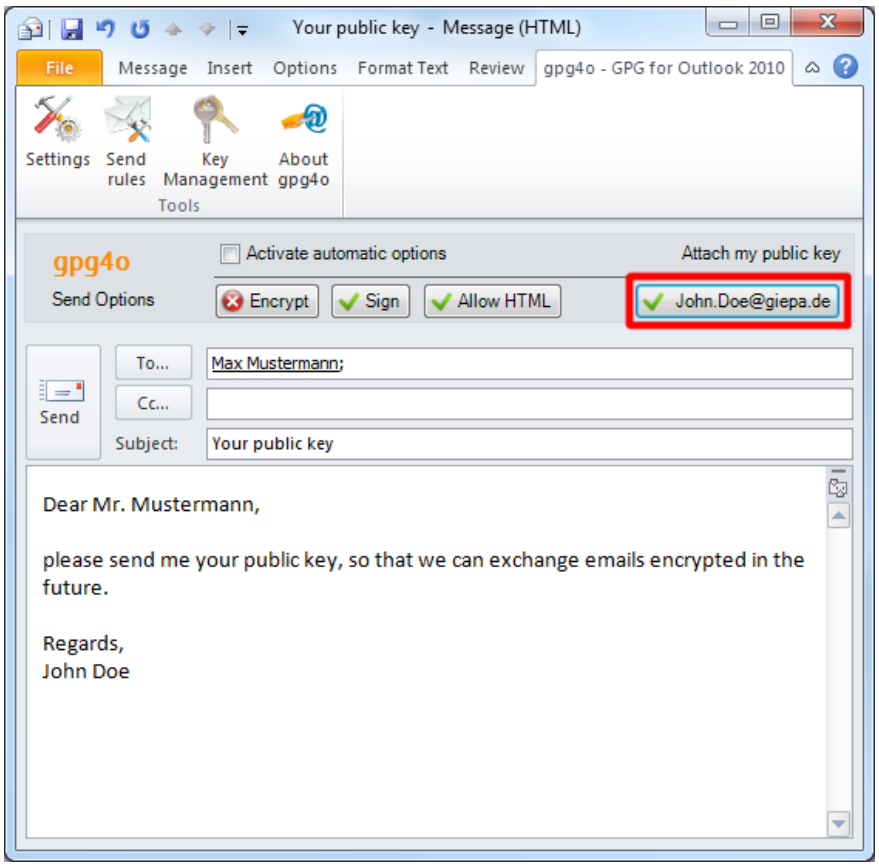
Like all other of your passwords you should keep this passphrase safe and **should not tell it to third parties**.

## 4.1 Sending Public Keys

In order to send an encrypted and/or signed email you generated a new email message. Browse to **"gpg4o - GnuPG for Outlook 2010 ®"** via the menu bar. There additional sending options are placed at your disposal. Place a checkmark in the check box **"Attach my public key"** and, if desired, in the check box **"Sign message"**. Write your email in ”plain text format” now and send it. This email will now be automatically provided with an attachment comprising your public key.

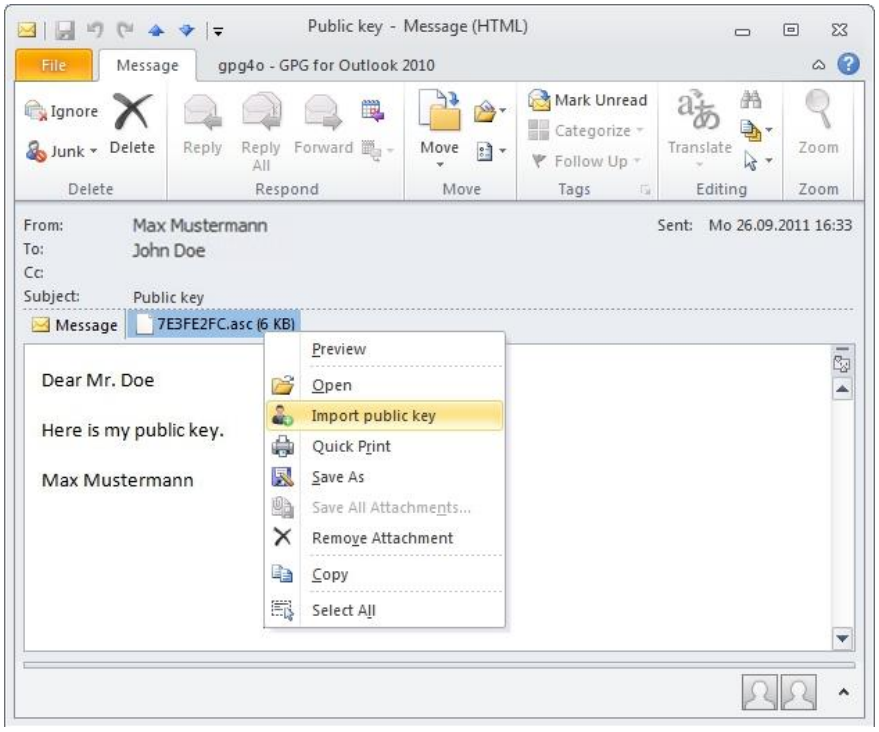
If your communication partner has already imported your public key it is not necessary to send the key another time. Mind that when directly sending emails the default options selected by you are utilized, insofar as you have not specified any rules (see **chapter 5**). Pay careful attention when you encrypt emails and when you do not.

The public key can be imported by all current encryption tools which support the OpenPGP-Standard. It comprises only the public part of the keypair, not the private part. You must **NEVER** send your passphrase or your private-key!



## 4.2 Importing Public Keys

In order to be able to send an email as an encrypted mail or in order to verify a signed email you need the so-called public key from the sender. If the recipient sends you a key as an attachment you can import it via the context menu (click right mouse button on the attachment) into your key management or via the ribbon by clicking on **“Import public key”**. Also you have the possibility to import a key from a key server (see **Chapter 4.8**). This exchange of the public key must be made once with every email contact with whom you want to exchange encrypted emails.

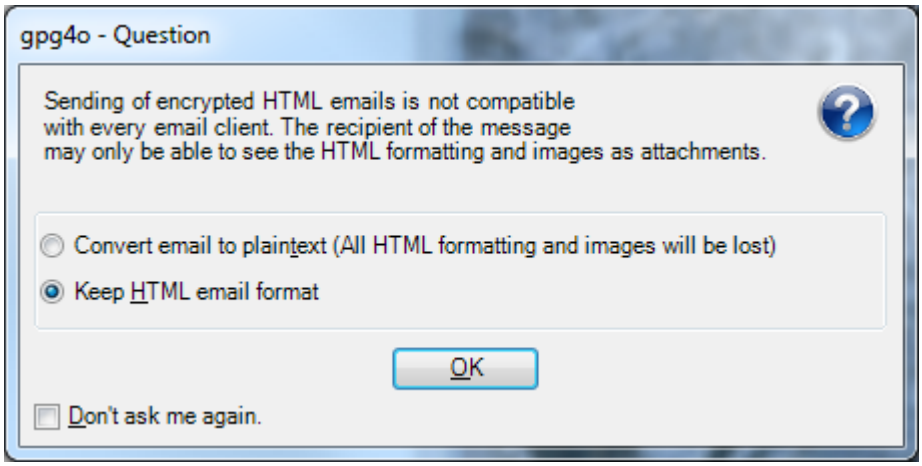


## 4.3 Sending Encrypted and/or Signed Messages

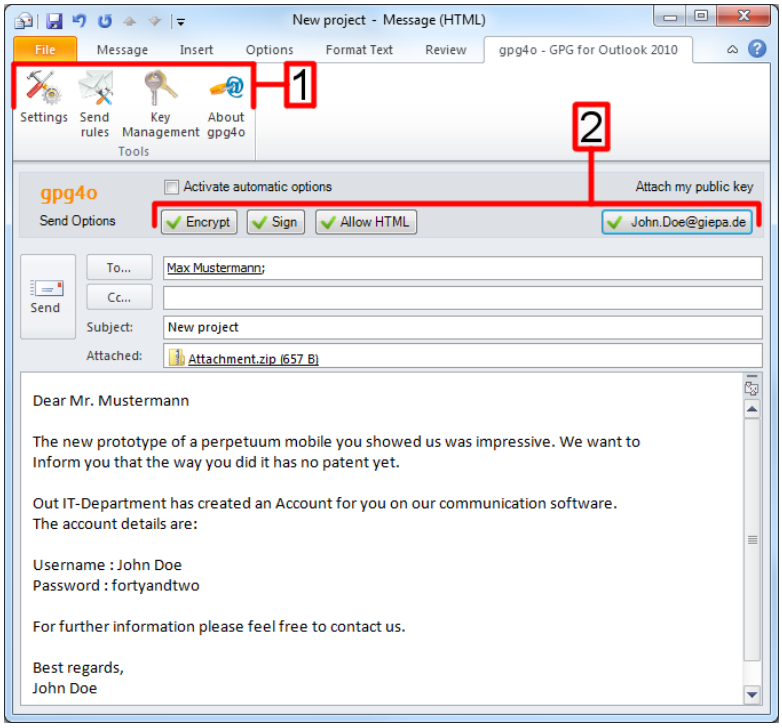
You can now send encrypted and/or signed emails. In order to guarantee the best possible compatibility with all current email programs you should write your emails in plain text format. Of course, you also have the possibility of sending emails in HTML-format. A corresponding selection possibility will 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 3.4**) 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”**.

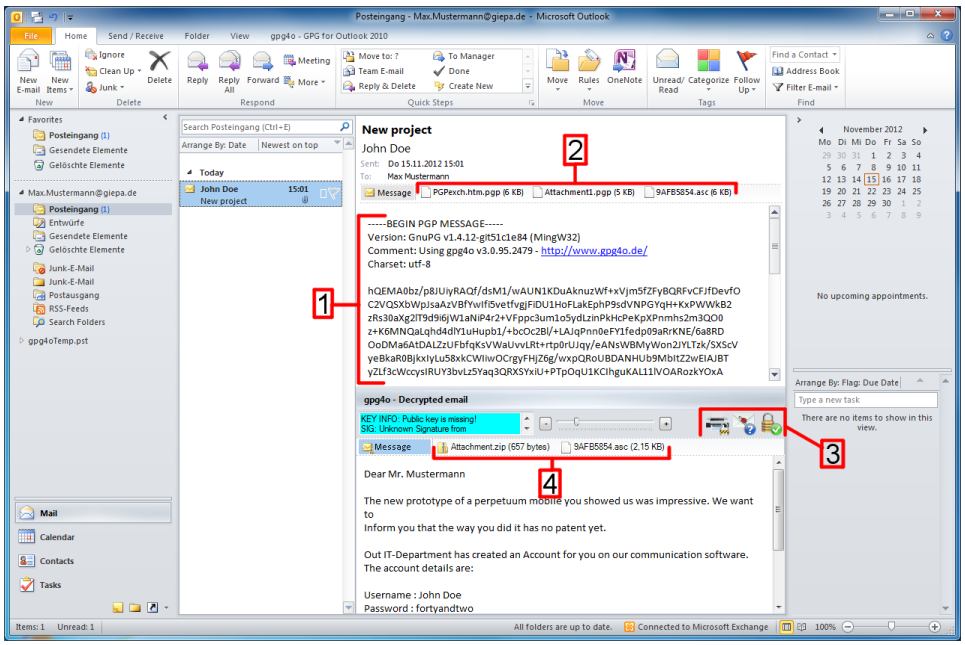



*1 – Settings for gpg4o*
*2 – Here you can set, if your email gets encrypted and/or signed and if you want to send your public key as attachment.*

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**.

## 4.4 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*

## 4.5 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…**“ und „**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 2010 ®.

## 4.6 Definition of Key Trust

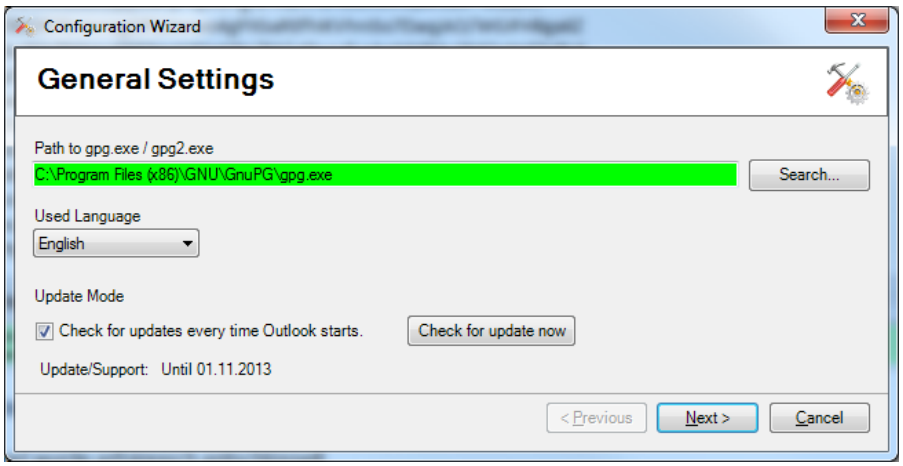
In principle the transfer of public keys is safe as long as you can trust the persons who receive your public key. However, it cannot be excluded that a third party generates a public key in your name and circulates it. If this person has access to your emails it can decrypt and read them with the faked 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 2010 ®"** 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.

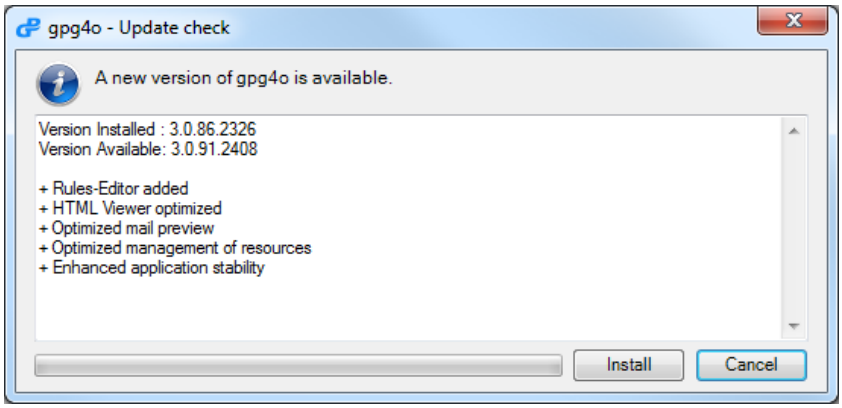
You can additionally define to which extent you trust your contacts to sign external keys and to classify them as authentic. For this purpose select one key from the key management and click the entry **"Define trust..."** in the context menu (click right mouse button). In the following dialogue several 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.

## 4.7 Obtaining Software Updates

In the configuration wizard you may execute a manual check for updates on the first page by clicking the corresponding button **"Check for update now"**. If this check shall be made regularly, place the check mark with **„Check for updates every time Outlook starts"**. Thus, a new version of pg4o is searched whenever Outlook is started and is offered to you for installation.




The installation of the update is made in the background and does not require any confirmations on your part. After completion of the installation you should start Outlook again so that modifications are effective.



## 4.8 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 2010 ®“** 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 2010 ®“**. 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.

# 5 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 5.2**).

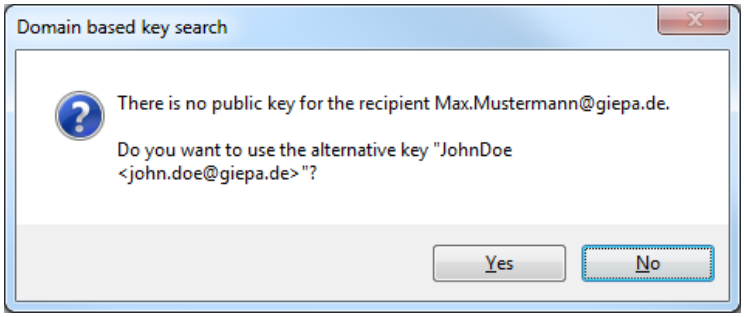
In this window you also have the possibility of activating the domain based key search (see **paragraph 5.1**).

## 5.1 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 2010 ®“**. 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.

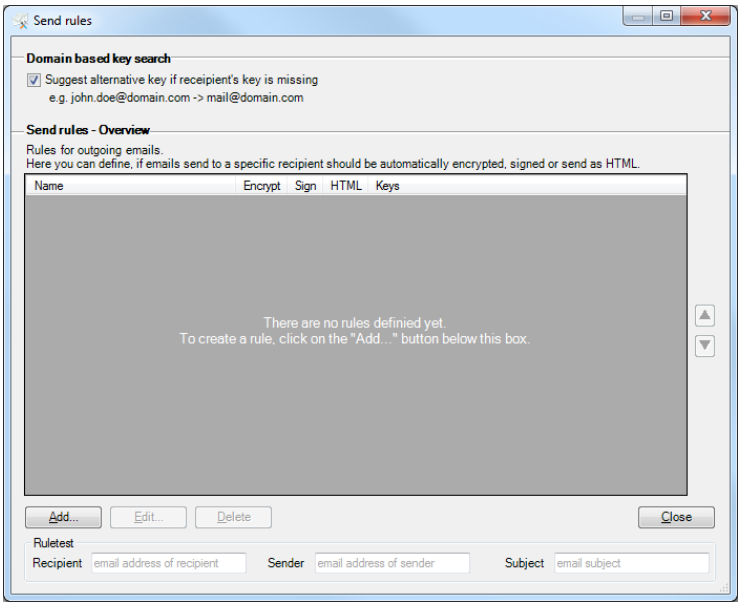



If you refuse this key you may select another key for encrypting your email as usual.

## 5.2 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.

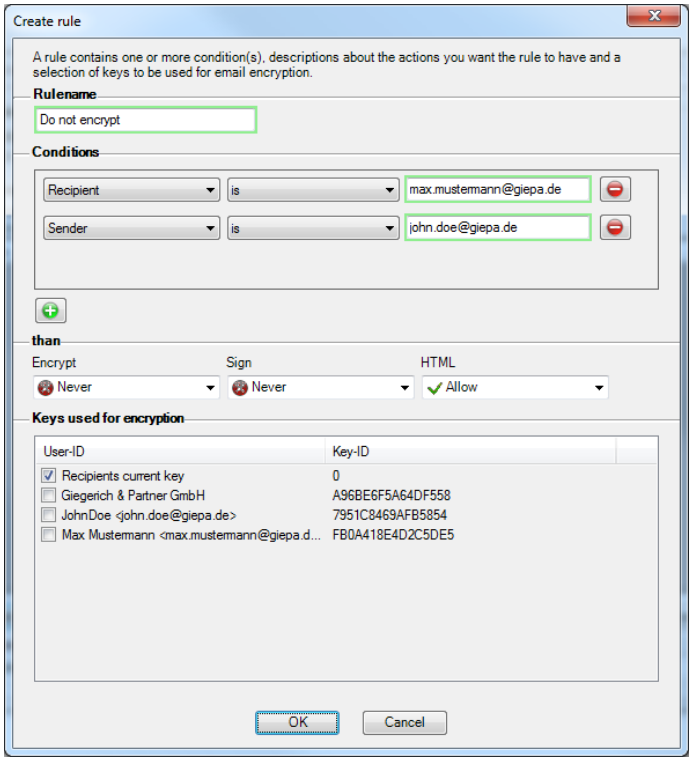
For this purpose click the item **„Send rules“** in the ribbon **„gpg4o - GPG for Outlook 2010 ®“**.




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.



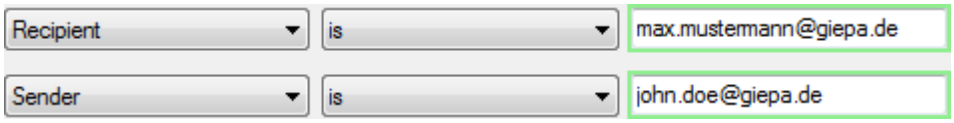
## 5.3 Rule Evaluation

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.

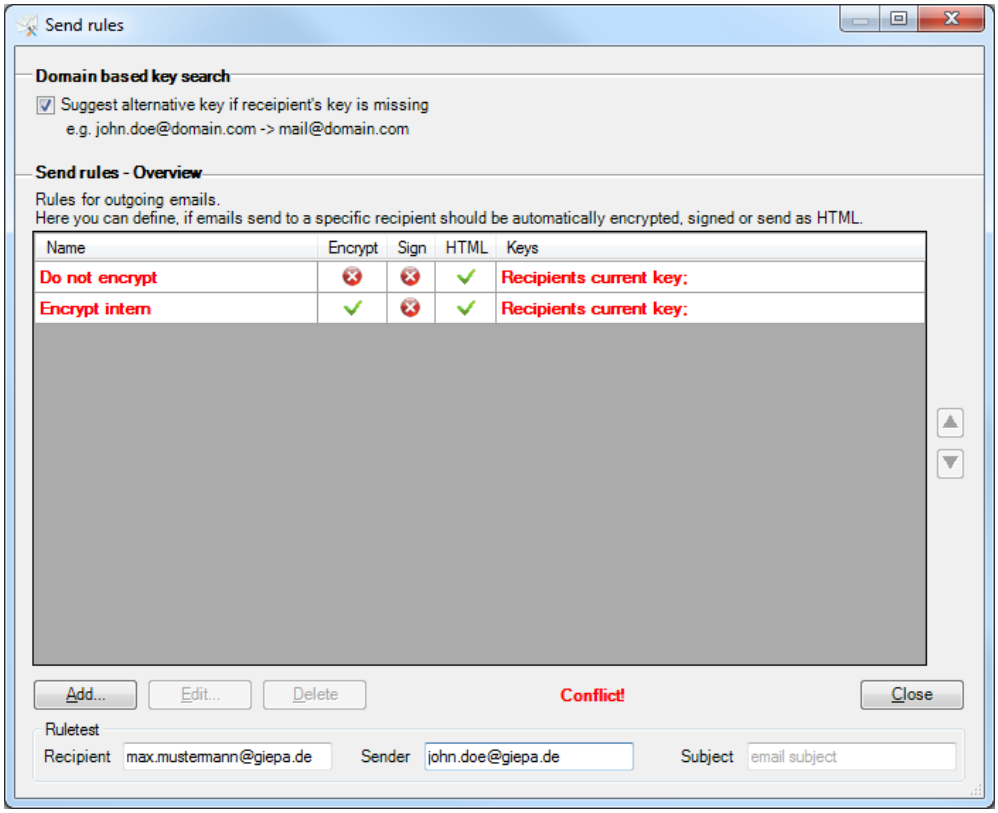
**The following example shows two rules:**

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




**„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**.

# 6 Miscellaneous

## 6.1 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 2010 ®"** in the ribbon menu of Microsoft Office 2010 ® 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.

## 6.2 Sending Log-Files

In order to send a log-file to our support, click **"gpg4o – gpg for Outlook 2010 ®"** in the ribbon menu of Microsoft Office 2010 ®. 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.

## 6.3 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.

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

## 7.1 Uninstalling under Windows Vista or Windows 7

In order to uninstall **gpg4o** click **"System control"** 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 2010 ®"** and click **"Uninstall"** in the menu.

## 7.2 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 2010 ®"** and click **"Remove"**.