Giegerich & Partner

gpg4o

Administrator Manual

gpg4o Version 5.3

Table of Contents

1 Introduction

The purpose of the present manual is to provide administrators with a reference book for the possibilities of **gpg4o**. Amongst others a description of how to install and distribute **gpg4o** in the company is given in the manual.

From version 3.3 onwards, **gpg4o** has been optimized with its numerous improvements for application in companies. In particular, the configuration of **gpg4o** was extended such that it may be administrated via group policies now. With these group policies you can process the behavior or the settings of **gpg4o**, respectively, according to your demands.

2 Installation

gpg4o is installed for all users of a computer which is why the installation or an update, respectively, may only be made by users with administrative privileges. For utilizing **gpg4o** you do not require administrative privileges.

2.1 Unattended Installation

Reasons for an unattended installation:

- Remote installation on a client-PC in your company
- Installation on different client-PCs in your company
- Updating **gpg4o** on different client-PCs in your company.

For an installation of **gpg4o** without user interaction it is sufficient to indicate the parameter /quiet when calling the setup. **gpg4o** will then be installed on the computer without further feedback to the user.

```
gpg4o_setup.exe /quiet
```

If you utilize the downloaded **„gpg4o_setup.exe“** for installation it is not necessary to perform any further preliminary work. The installation program checks whether all components required by **gpg4o** are available and installs them automatically, if necessary. Please mind that **gpg4o** downloads the required packages via the Internet.

For an offline installation of **gpg4o** please regard the hints and prerequisites stated in the following chapter 3.1.

Hint: The required OpenPGP implementation is not deployed when installing **gpg4o** unattended. Instead you have to install **GnuPG** before the installation of **gpg4o**.

3 Distribution of gpg4o in the Company

3.1 Integration in automatic software distribution systems

If you perform the installation via **„gpg4o_setup.exe“** the packages described in this section will be installed automatically. If the installation shall be made via the MSI packages you have to make sure that the following components are existent on the target computer or that these components will be pre-installed.

A distribution of **gpg4o** within a network is possible with customary tools. You can unpack the MSI using this command:

```
gpg4o_setup.exe /extract
```

The following components have to be pre-installed in case of a silent installation:

- Microsoft .NET Framework 4.0 (Full Package) (only Vista and Windows 7)
- Microsoft Office 2010 Primary Interop Assemblies (not neccessary for Outlook 2013/2016)
- Microsoft Visual Studio 2010 Tools for Office Runtime (VSTO 4.0) (not neccessary for Outlook 2013/2016)

3.2 Offline Installation

In case you want to install **gpg4o** without or a slow internet connection you have to put the installation packages mentioned above into the same directory as the „gpg4o_setup.exe“.

You can find these packages on our downloads website in the section **„Software requirements“**.

https://www.giepa.de/products/gpg4o/downloads/?lang=en

3.3 Distribution to computers with multiple users (Terminalserver)

After having installed **gpg4o** on the target computer every user of **gpg4o** necessitates a license file. This license file can be made available to the user via a copy procedure into the **gpg4o** user directory (see chapter 8). After having restarted Outlook **gpg4o** will recognize and utilize this license file. Alternative you can change the path to the license file by using the group policy (see chapter 3.4)

For the utilization of **gpg4o** with a computer with multiple users there may be cases where some of the users shall not obtain any license at all. If **gpg4o** is not disabled in this case these users will fall into the trial mode which will be available for 45 days from the time of the first installation onwards. Afterwards, **gpg4o** cannot be utilized any longer and dialogs will appear requesting to purchase.

As this disturbs the user during his work we have designed a special license file for this (**„Cloak-License“**) which causes an almost entire deactivation of **gpg4o**. Only importing a license from within an attachment of an email will remain available. This **„Cloak-License“** can be requested from the support free of charge.

Distribution of this special license file takes place like any other license file and is described in chapter 3.4.

The other possibility to disable **gpg4o** is with the help of the group policies „Functional limitations\Licensing\Disable the use of gpg4o“. This has the same effect as the distribution of the cloak license, however, in most cases the effort is smaller.

3.4 License file distribution

In case you want to administrate licenses from a central point then you are able to roll out these at any time. For example this is the case when you have renewed your license subscription.

You can achieve this by using a startup script or you set path to the new license file by using the group policy „Functional restrictions\Licensing\Determine path to license file“. This policy can point to a folder in your network for example.

If you don’t want to set the path to the license file manually you have to copy it into the following directory:

```
%AppData%\Giegerich & Partner GmbH\gpg4o\LicenseInformation.lic
```

4 Group Policies

Since version 3.3, administrators can limit the utilization of program functions and program settings of **gpg4o** via group policies. The configuration of **gpg4o** was extended such that it can be set via group policies. For this purpose the template-formats ADM as well as ADMX are available which you can request from the support free of charge. All newer Windows versions support template-format ADMX.

You can find the policies in the group policy administration editor under user configurations\Giegerich & Partner - gpg4o. All policies contain an explanation, stating how the program will behave with the user if the policy is enabled or disabled, respectively and what the standard behavior is like. A general rule for all settings is that when activating or deactivating, respectively, the setting is given, which means that the user cannot modify it later.

Example of Group Policies:

A keypair is placed at the disposal of the users. The users shall not be able to delete keypairs or to generate new keys.

The following group policies have to be activated for that purpose:

- Users must not delete keypairs
- Users must not generate keypairs

With these settings you have made sure that the user will not be able to generate his own keys and will not be able to unintentionally delete keys that have been placed at his disposal. With these settings the users must obtain their keypair from an administrative authority.

In the following you will find a list of the policies and their additional explanations for **gpg4o**. The presettings of **gpg4o** are indicated. (The initial installation of **gpg4o** utilizes these presettings.)

4.1 Functional Restrictions

- Users must not save emails permanently decrypted
  - If you enable the policy the users will not be able to save emails permanently decrypted any longer. If you disable the policy the users will be able to save emails permanently decrypted via the corresponding button.
  - The policy is disabled.

4.1.1 Backup

- Users must not export any backups
  - If you enable the policy the users will no longer be able to export any backups in the settings. If you disable the policy the users can export backups.
  - The policy is disabled.
- Users must not import any backups
  - If you enable the policy users will not be able any longer to import backups in the settings or the configuration wizard, respectively. If you disable the policy the users can import backups, however, depending on the status of the policy "Users

must not import any licenses", importing of the license will be skipped.

- The policy is disabled.

4.1.2 Licensing

- Disable the use of gpg4o
  - If you enable the policy gpg4o will be disabled with the users to the greatest extent. Only the import of license files from an email will remain active as far as this has not also been disabled by means of a policy. If you disable the policy gpg4o will be loaded and is normally usable within the scope of the license.
  - The policy is disabled.
- Users must not import any licenses
  - If you enable this policy the users will no longer be able to import any license files, neither from an email nor from the file system. Additionally, the license will be ignored when importing a backup. If you disable the policy users can import license files. In addition, when importing a backup the import of the license will not be skipped.
  - The policy is disabled.
- Determine path to license file
  - If you enable this policy, the license file of the user will not be loaded from the default location anymore but from the path you selected. You can also use a UNC path. Should the path be not available, the last successfully loaded license is loaded from the local cache. If you disable this policy, the license will be loaded from the default path in the users roaming directory.
  - The policy is disabled.

4.1.3 Key Management

- Users must not apply any revocation certificates
  - If you enable this policy the users will not be able to apply any revocation certificates to their keypairs. This will then have to be done by an administrative authority. Said administrative authority must then redistribute the revoked key. If you disable this policy the users will be able to apply revocation certificates to their keypairs.
  - The policy is disabled.
- Users must not modify the passphrase of their keypairs
  - If you enable this policy the users will not be able to modify the passphrase of keypairs in their keyring. If you disable this policy the users will be able to modify the passphrase of keypairs in their keyring. This does not modify the key itself. Thus, copies of the key will remain unaffected and functional.
  - The policy is disabled.
- Users must not generate any keys

  - If you enable this policy the users will not be able to generate any keys. In this case an administrative authority must be available which generates and manages the keys and which issues them to the users. If you disable this policy the users will be able to generate their own keys.
  - The policy is disabled.
- Users must not generate any revocation certificates
  - If you enable this policy the users will not be able to generate any revocation certificates for their keypairs. These revocation certificates will then have to be generated by an administrative authority having a copy of the keypair. If you disable this policy the users will be able to generate revocation certificates for their keypairs.
  - The policy is disabled.
- Users must not delete any keypairs
  - If you enable this policy the users will not be able to delete keypairs from their keyring. If you disable this policy the users will be able to delete keypairs from their keyring.
  - The policy is disabled.
- Users must not delete any public keys
  - If you enable this policy the users will not be able to delete any public keys from their keyring. However, this policy does not have any influence when deleting keypairs. If you disable this policy the users will be able to delete public keys from their keyring.
  - The policy is disabled.
- Users must not enable or disable any keys
  - If you enable this policy the users will not be able to enable or disable any keys in their keyring. If you disable this policy the users will be able to enable or disable keys in their keyring.
  - The policy is disabled.
- Users must not export any keypairs
  - If you enable this policy the users will not be able to export any keypairs as a file. If you disable this policy the users will be able to export keypairs.
  - The policy is disabled.
- Users must not export any public keys
  - If you enable this policy the users will not be able to export any public keys or to send them by email. This excludes exporting public keys to keyservers. If you disable this policy the users will be able to export public keys and to send them by email.
  - The policy is disabled.
- Users must not import any keypairs

  - If you enable this policy the users will not be able to import any keypairs from files, attachments or from the clipboard. If you disable this policy the users will be able to import keypairs from the mentioned media.
  - The policy is disabled.
- Users must not import any public keys
  - If you enable this policy the users will not be able to import any public keys from files, attachments or from the clipboard. This excludes importing public keys from keyservers. If you disable this policy the users will be able to import public keys from the mentioned media.
  - The policy is disabled.
- Users must not download any keys from keyservers
  - If you enable this policy the users will not be able to import any public keys from keyservers. This does not apply to the server for the automatic downloading of keys. If you disable this policy the users will be able to import public keys from keyservers.
  - The policy is disabled.
- Users must not upload any keys to keyservers
  - If you enable this policy the users will not be able to upload any public keys to keyservers. This also applies to the public part of the own keypairs. If you disable this policy the users will be able to upload public keys to keyservers.
  - The policy is disabled.
- Users must not set/modify the owner trust of keys
  - If you enable this policy the users will not be able any longer to set or modify the owner trust of keys in their keyring. If you disable this policy the users will be able to set or modify the owner trust of keys in their keyring.
  - The policy is disabled.
- Users must not sign keys
  - If you enable this policy the users will not be able to sign any keys. In this case the keys will have to be signed by an administrative authority. If you disable this policy the users will be able to sign keys. This policy only refers to the exportable signature and not to local signatures.
  - The policy is disabled.
- Users must not locally sign keys
  - If you enable this policy the users will not be able to locally sign keys. If you disable this policy the users will be able to locally sign keys. This policy only refers to the not exportable „local“ signature.
  - The policy is disabled.
- Users must not extend keys
  - If you enable this policy the users will not be able to extend the expire date of any keypair. If you disable this policy the users will be able to extend keypairs.
  - The policy is disabled.

4.1.4 Sending Rules

- Users must not generate any sending rules
  - If you enable the policy the users will not be able to generate any sending rules. If you disable the policy the users will be able to generate sending rules.
  - The policy is disabled.
- Users must not delete any sending rules
  - If you enable the policy the users will not be able to delete any sending rules. If you disable the policy the users will be able to delete sending rules.
  - The policy is disabled.
- Users must not modify any sending rules
  - If you enable the policy the users will not be able to edit existing sending rules. If you disable the policy the users will be able to edit existing sending rules.
  - The policy is disabled.

4.2 Default Settings

4.2.1 Update Settings

- Also look for beta versions when checking for gpg4o updates
  - If you enable this policy gpg4o will also search for beta versions when checking for updates. If you disable this policy gpg4o will only search for final versions. The exception are update requests out of beta or release candidate versions. They will also search for beta or release candidate versions. If you configure this policy the users will no longer be able to determine this setting by themselves.
  - The policy is disabled. gpg4o will not search for beta versions.
- Determine update behavior of gpg4o
  - If you enable this policy gpg4o will search for updates according to your selection. Mind, however, that even with automatic search for updates this installation will still have to be confirmed by the users before they will be installed. If you disable this policy the users will be able to influence the settings with regard to updates by themselves.
  - The policy is disabled. gpg4o will automatically search for updates.

4.2.2 General Settings

- Always clone mails instead of copying them
  - If you enable this policy gpg4o will clone emails for decryption. If you disable this policy the outlook internal copy routine will be used if possible.
  - The policy is not configured. The setting is disabled.
- Decrypting of emails in public folders
  - If you enable this policy gpg4o will try to decrypt emails in public folders or will check the signature, respectively. Of course the correct keypair is necessary for

decrypting the emails. If you disable this policy gpg4o will not process any emails in public folders. If you configure this policy the users will no longer be able to determine this setting by themselves.

  - The policy is not configured. The setting is enabled.

- Find OpenPGP keys in attachments
  - If you enable this policy gpg4o searches for OpenPGP keys among the attachments of an email that shall be displayed and offers the user to import them. If you disable this policy gpg4o will not search for OpenPGP keys among attachments. The import of public keys or keypairs has to be allowed.
  - The policy is not configured. The setting is enabled.
- Find gpg4o licenses in attachments
  - If you enable this policy gpg4o searches for its license files among the attachments of an email that shall be displayed and offers the user to import them. If you disable this policy gpg4o will not search for its license files. The import of license files has to be allowed.
  - The policy is not configured. The setting is enabled.
- Use advanced signature check
  - If you enable this policy PGP/MIME signatures without encryption will also be checked. This can fail depending on the mailserver and its configuration. If you disable this policy gpg4o will only check normal signatures. Of course PGP/MIME encrypted and signed emails will be checked. If you configure this policy the users will no longer be able to determine this setting by themselves.
  - The policy is not configured. The setting is disabled.
- Redirect sales requests to an own email address
  - If you enable this policy you can enter an email address, that will be used for sales-inquiries.
  - The policy is disabled. The default email address is sales@giepa.de
- Redirect support requests to an own email address
  - If you enable this policy you can enter an email address, that will be used for technical inquiries.
  - The policy is disabled. The default email address is support.gpg4o@giepa.de
- Hide filename
  - If you enable this policy the original filenames of email attachments will be hidden when they are going to be encrypted. Thus, encrypted filenames such as attachment1.pgp will appear instead of the actual filename with attached file extension. However, this manner of encrypting files is not supported by all OpenPGP-implementations. If you disable this policy the filenames will not be hidden. For example, the filename Invoice.xlsx.pgp will appear then. Indeed this variant allows conclusions to be drawn with regard to the contents of the files but it is better compatible with other OpenPGP-implementations. If you configure this policy the users will not be able any longer to determine this setting by themselves.

  - The policy is not configured. The filenames will be hidden.
- Utilize domain based key search
  - If you enable this policy an alternative key will be offered when encrypting messages to recipients for whom it is impossible to find a suitable key. The search for this alternative key is based on the domain of the recipient's email address. The users can accept this proposal or select a key on their own with which the message shall be encrypted. If you disable this policy the users will generally always have to do the selection of a key to be utilized in such a case. If you configure this policy the users will no longer be able to determine this setting by themselves.
  - The policy is not configured. The domain based key search is disabled.
- Use the file extension .gpg for encrypted attachments
  - If you enable this policy the file extension .gpg will always be used for encrypted attachments. If you disable this policy the file extension .pgp will always be used for encrypted attachments. If you configure this policy the users will no longer be able to determine this setting by themselves.
  - The policy is not configured. The setting is enabled.
- Hint for expiring keypairs
  - If you enable this policy users gets a hint if a accountkey will be expired until the next 30 days. With this hint the users get also the posibility to extend their keys for one more year. If you disable this policy the users do not get a hint for expiring keypairs. If you configure this policy the users will no longer be able to determine this setting by themselves.
  - The policy is not configured. The setting is enabled.
- Use the gpg4o-internal packet parser
  - If you enable this policy gpg4o will analyze the data of OpenPGP packets largly independent to save computing time. This can cause problems with some attachments. In this cases gpg4o will use GnuPG for analysis. If you disable this policy gpg4o will always use GnuPG to analyze the OpenPGP data.
  - The policy is not configured. The setting is enabled.
- Perform decryption in a separate outlook data file
  - Before decrypting emails are always copied/cloned to a place from where they will not be syncronized with the server. If you enable this policy the datafile gpg4oTemo.pst will be used for this. If you disable this policy a folder called Temp below your inbox will be used instead and its syncronisation with the server will be prevented. Because this prevention can not be guaranteed in all cases you should disable this policy only if having problems using the datafile.
  - The policy is not configured. The setting is enabled.
- Detect keypairs with outdated MD5 signature algorithm
  - If you enable this policy gpg4o detects keypairs with the outdated MD5 signature algorithm. If any keypairs are found the user gets the opportunity to update these keypairs to a modern signature algorithm. If you disable this policy the check for outdated keypairs will never be done.
  - The policy is not configured. The setting is enabled.

4.2.3 Keyserver Settings

- Allow automatic import for verification
  - If you enable this policy the users can use the automatic import for signature verification. A server must be available for automatic import
  - The policy is disabled. The setting is disabled.
- Determine keyserver list
  - If you enable this policy the users can only use the given keyservers. You need to enter the keyservers URI and their privileges.

    The privileges are separated into download and export and can have the values 0 (Not allowed), 1 (Only manually allowed), 2 (Only automatically allowed) and 3 (Both allowed). The value needs to be formatted by entering the numeric value of the download privileges followed by a semicolon and the upload privileges.

    Entering „hkp://keys.company.com 3;1 “ results in a single keyserver available to the users, which can be used for downloading and uploading keys manually and also automatically import missing keys while writing emails from this server.

    If you disable this policy the users will be able to determine their keyservers by themselves.
  - The policy is disabled.
- Update locally existing keys
  - If you enable this policy keys will be imported into the users keyring even when they exist there already. So the keyring of the user is kept up to date. Prerequisite is that you have configured at least one keyserver in the list of keyservers as a source for automatic download of keys.
  - The policy is disabled.

4.2.4 View Settings

- Show encryption status in inspectors
  - If you enable this policy gpg4o will insert the encryption status at the beginning of the message when opening a message in an own window (Inspector). If you disable this policy gpg4o will not insert any encryption status in the message in this case. If you configure this policy the users will no longer be able to determine this setting by themselves.
  - The policy is not configured. The setting is disabled.
- Link encryption status in permanently decrypted messages
  - If you enable this policy gpg4o will insert the encryption status at the beginning of the message during permanent decryption. If you disable this policy gpg4o will not insert any encryption status in the message in this case. If you configure this policy the users will no longer be able to determine this setting by themselves.
  - The policy is not configured. The setting is enabled.
- Show encryption status in the gpg4o reading pane

  - If you enable this policy gpg4o will also insert the encryption status at the beginning of the message when reading a message in the gpg4o reading pane. If you disable this policy gpg4o will not insert any encryption status in this case but only display the message itself. If you configure this policy the users will not be able any longer to determine this setting by themselves.
  - The policy is not configured. The setting is enabled.
- Show encryption status with printed emails
  - If you enable this policy gpg4o will insert the encryption status at the beginning of the message when printing a message via the button Print in the gpg4o reading pane. If you disable this policy gpg4o will not insert any encryption status in this case. If you configure this policy the users will no longer be able to determine this setting by themselves.
  - The policy is not configured. The setting is enabled.
- Show encryption status in answers
  - If you enable this policy gpg4o will insert the encryption status at the beginning of the original message when answering or forwarding a message. If you disable this policy gpg4o will not insert any decrypting information into the original message in this case. If you configure this policy the users will no longer be able to determine this setting by themselves.
  - The policy is not configured. The setting is enabled.
- Language selection
  - If you enable this policy gpg4o will be started with the language selected by you when the users start Outlook the next time. If you disable this policy the users will be able to set their preferred language by themselves.
  - The policy is disabled. The default language is the system language if it is available with gpg4o, otherwise it is English.
- Hide send options with inactive gpg4o-accounts
  - If you enable this policy the users will see the gpg4o send options only when generating emails from an active email account. If you disable this policy the send options will be displayed for all new emails. If you configure this policy the users will no longer be able to determine this setting by themselves.
  - The policy is not configured. The send options are always displayed.

4.2.5 GnuPG Settings

- Online update GnuPG version information every time Outlook starts
  - If you enable this policy the list of GnuPG versions will be updated from the internet every time outlook is started. If you disable this policy the list will not be updated. If you configure this policy the users will no longer be able to determine this setting by themselves.
  - The policy is activated. Online update GnuPG version information every time Outlook starts
- Don’t show notification about other installable GnuPG versions

  - If you enable this policy gpg4o will not notify about other installable GnuPG versions.
  - The policy is deactivated.
- Don't show notification about unknown GnuPG versions
  - If you enable this policy gpg4o will not notify about GnuPG versions that it doesn't know.
  - The policy is deactivated.
- Caching time of a passphrase when utilizing the GnuPG agent (GnuPG 2.0.x)
  - This policy only applies to those users who utilize GnuPG 2.0.x with the GnuPG agent. If you enable this policy the GnuPG agent will cache passphrases entered for the period of time indicated by you. The duration is counted separately for every private key. If a private key is not used for more than the indicated period of time the user will be demanded the passphrase again during the next utilization. If you disable this policy the users will be able to determine the duration by themselves.
  - The policy is disabled. The passphrases will be cached for 5 minutes.
- Caching time of a passphrase when utilizing GnuPG 1.4.x
  - This policy only applies to users who utilize GnuPG 1.4.x. If you enable this policy gpg4o will cache the last entered passphrase for the period of time indicated by you. If another key is used than that used last and if the passphrases differ the user will have to enter the passphrase of the other key. If you disable this policy the users will be able to determine the duration by themselves.
  - The policy is disabled. The passphrases will be cached until quitting Outlook.
- Determine GnuPG home directory
  - If you enable this policy gpg4o will load the keyrings from the directory indicated by you. That is why the path should use a user-specific system variable in order to exclude the situation that all users access the same keyrings. If you disable this policy the users will be able to set the directory by themselves.
  - The policy is disabled. The default directory will be taken: %AppData%\gnupg
  - Please keep in mind that the type of the registry key has to be `REG_EXPAND_SZ` in case you create this key manually as otherwise gpg4o is not able to resolve the entry.
- Determine path to GnuPG
  - If you enable this policy gpg4o will utilize the GnuPG-installation under the path indicated by you. You can also use system variables under the path. If you disable this policy the users will be able to determine the path to the GnuPG installation by themselves.
  - The path will be identified automatically. By default GnuPG will be searched via the registry or alternatively under %ProgramFiles(x86)%\GNU\

    GnuPG will be searched with the filenames gpg.exe or gpg2.exe, respectively.

  - Please keep in mind that the type of the registry key has to be `REG_EXPAND_SZ` in case you create this key manually as otherwise gpg4o is not able to resolve the entry.

- Determine timeout of GnuPG processes
  - If you enable this policy you determine the duration of how long gpg4o will wait for the GnuPG processes to end normally before it will inform the user about a potential error. The user can then give the process more time to end or terminate the process. If you disable this policy the default value of 15 seconds will be used. This value cannot be configured by the users in the configuration of gpg4o. If you encounter problems with long running GnuPG processes on some computers, you should enable this policy to give them more time.
  - The policy is not configured. The default setting of 15 seconds (value: 15000 ms) wil be used.
- Always trust keys
  - If you enable this policy the users will be able to send encrypted messages to all key owners and to check all signatures of the key owners - irrespective of the web of trust. Even though this is easier for the users you should not activate this policy as it permits the use of untrustworthy keys. If you disable this policy keys will have to be validated by the web of trust first before they can be used. If you configure this policy the users will no longer be able to determine this setting by themselves.
  - The policy is not configured. The setting is enabled.
- Disable GnuPG-headers
  - If you enable this policy the insertion of the GnuPG version line as well as the annotation with the gpg4o version will be disabled. This may be reasonable for security reasons. If you disable this policy the above mentioned lines will always be inserted. In case of a bug this facilitates debugging with the recipient. If you configure this policy the users will no longer be able to determine this setting by themselves.
  - The policy is not configured. The headers will be inserted.
- Quit GnuPG agent as well when quitting Outlook
  - If you enable this policy the GnuPG agent will also be quitted when quitting Outlook. Thus, all saved passphrases will be forgotten and will have to be entered again, if necessary, when rebooting Outlook. If you disable this policy the GnuPG agent will not be quitted when quitting Outlook. Passphrases will be available as well after rebooting Outlook as far as the period of caching is not exceeded. If you configure this policy the users will no longer be able to determine this setting by themselves.
  - The policy is not configured. The GnuPG agent is not quitted with Outlook.

4.2.6 Log Settings

- Determine the verbosity of logging

  - If you enable this policy you can set the logging behavior for gpg4o. By default gpg4o logs all activities except for the time measurements and stacktraces.
  - The policy is configured. The default setting is LogLevel 6
- Limit the maximum amount of log files
  - If you enable this policy you can set the maximum amount of log files.
  - The default amount is 30 log files.
- Logging in case of extended signature checking
  - If you enable this policy the external library gpg4oH will be able to write log outputs. If you disable this policy gpg4oH will not write any log outputs. This policy is should only be changed in case of issues.
  - The policy is activated.

4.2.7 Homedir backup settings

- (De)Activate automatic GnuPG homedir backups
  - If you enable this policy a daily backup of the GnuPG home directory will be created as a zip archive.
  - When activated the user won't be able to modify the destination directory and the amount of backups to keep anymore.
  - This feature is only available for users with professional license.
  - The policy is deactivated.
- Maximum count of homedir backups to keep
  - Declare the maximum count of kept backups of the GnuPG home directory.
  - Default: 60 backups are kept.
- Path to destination directory for homedir backups
  - Set the directory for the GnuPG home directory backups.
  - The path can not contain a backslash at the end.
  - Default: %AppData%\Giegerich & Partner GmbH\gpg4o\Backup
  - Please keep in mind that the type of the registry key has to be `REG_EXPAND_SZ` in case you create this key manually as otherwise gpg4o is not able to resolve the entry.

5 Distribution of sending rules

Please create the sending rules on a computer with **gpg4o**. Then copy the file **„Rulelist.xml“** to the desired computers. The file resides in the user directory of **gpg4o**. (see chapter 8)

To prevent users from modifying the sending rules you can activate group policies. (see chapter 4.1.4)

6 Automated Generation of Keypairs

gpg4o offers you the possibility of generating several keypairs in one flow. This is reasonable for example if during initial operation of **gpg4o** in a company you have to equip many employees with keypairs.

For this you only need a functionally set **gpg4o** with empty keyrings and a CSV-file with the data of the keypairs to be generated.

6.1 Preparation

The setting of **gpg4o** must be functional and the GnuPG keyrings should be empty. This can be achieved by renaming the directory for the keyrings with closed Outlook.

You can find the storage locations of the **gpg4o** and **GnuPG** files referenced in the present paragraph in the chapter 8.

Attention: The keyrings contain your private key which you need for decrypting emails. That is why you should not delete the keyrings or overwrite a backup!

The data of the keypairs to be generated must be available in a CSV-file (Comma Separated Values).

The CSV-file comprises the data separated from another by semicolon per line „ ; “ for every individual keypair and consists of three columns for name and first name, the email address and the passphrase:

```
Mrs. Smith, Erika;Erika.Smith@work.com;passphrase
Karl-Heinz Smith;Karl-Heinz.Smith@work.com;passphrase
John Doe;JohnDoe@work.com;passphrase
```

Please mind that the file does not contain a header with column identifiers.

Attention: The CSV-File should be stored in a secure place!

6.2 Generation of the Keypairs

You can then call the dialog (New Key) in Outlook via the key management in order to generate a new keypair. Here, the algorithm to be utilized for the keys, the length of the primary and subkey and the expire date can be selected as well.

If you enter the text „[csv]“ in the field **„Name“** in this dialog and if you click the button **„OK“** an file dialog will be opened. There you can choose your saved CSV-file. The keys will be generated once you open the file.

The thus generated keys will afterwards be available via the **gpg4o** key management. Already existing keys will be identified by means of the email address and will not be generated/overwritten so that there will not be the risk of duplicates.

6.3 Backup of the Keypairs

Hint: You should always use a safe passphrase for the generation of the keypairs

Hint: After having generated the keypairs you should make a backup of those keypairs. For that purpose you simply have to save the two files **„secring.gpg“** and **„pubring.gpg“** which can be found in the GnuPG directory see chapter 8. The associated passphrases shall be saved as well

6.4 Distribution of the Keys

The generated public keys can be exported individually into the file system via the **gpg4o** key management or can be uploaded to a keyserver so that the users will be able to import them on their keyring.

Tip: With the key management it is also possible to highlight several keys at the same time.

If it is a question of an initial installation in your company and all the users shall receive the public keys generated in the previous paragraph you can copy the file **„pubring.gpg“** in the GnuPG directory (see chapter 8) to the target computers.

Now you export the private key to a data storage medium (USB-stick, CD/DVD, ...) or to a specially secured network drive and send it to the individual user so that he or she may import the keypair with the **gpg4o** key management.

Attention: You should only let the users receive their keypairs via a secured path as otherwise there will be the risk that unauthorized persons might decrypt emails or sign them under the name of another person.

Hint: After having imported the private key into the user's computer the passphrase will have to be changed by the user!

7 gpg4o Update via a Proxy Server

For connection establishment with the update server via a proxy server **gpg4o** uses the network settings which are directly configured in your system. In order to establish connection via a proxy server you have to enter said proxy server into your Internet options.

You can find these Internet options under the **„Control panel“** of Windows under the **„Internet options“**.

Open the tab **„Connections“** in the following window and click on the button **„LAN settings“** in the lower section.

In the following window you can now enter the address of the desired proxy server or an automatic configuration script in order to permit **gpg4o** to build up a connection with the update server (or similar).

8 Paths to the Files of gpg4o and GnuPG

8.1 User directory

```
%AppData%\Giegerich & Partner GmbH\gpg4o\
```

8.2 License file

```
%AppData%\Giegerich & Partner GmbH\gpg4o\LicenseInformation.lic
```

8.3 Folder for log files

```
%AppData%\Giegerich & Partner GmbH\gpg4o\LogFiles\
```

8.4 GnuPG directory

```
%AppData%\gnupg\
```

8.5 Sending rules

```
%AppData%\Giegerich & Partner GmbH\gpg4o\Rulelist.xml
```

9 Company and support contact information

9.1 About Giegerich & Partner GmbH

Company Profile

Giegerich & Partner is your reliable solution developer. We create efficient IT Infrastructures, care for your IT Security, develop high quality software solutions and refine standard solutions. Your individual needs as a customer set the pace for our work which does not end with the delivery of any solution. We are well known for accompanying the whole solution lifecycle beginning with the very first idea until rollout of the last implementation. And we do that with competent people, not with anonymous call centers.

Who and Where

With 30 employees near Frankfurt/Main – Germany we support over 3000 customers worldwide in now over 70 countries when it comes to IT Security, software development and email encryption. As a member of the TeleTrust federation in Germany we have obligated ourselves to provide secure IT Security solutions without backdoors. This allows us to be a member of the group “IT Security made in Germany”.

Our Mission

We deliver reliable and Tailor-made IT Solutions. Filled with energy, passion and a high skill level, we work for your success with our solution. With us as a partner, you can concentrate on your core business. We care about the (IT) rest. That’s what we do: Tailor-made IT.

Values

Highly competent people are important, but not enough. Since we are an owner driven company, we know that reliability, sustainability, personality and partnership are fundamental values for a working relationship with customers, suppliers and employees. Real people are in the center of our companies universe, not machines. You will experience this by having your personal way of support, long term contact persons and competence. They help you with the technology we provide that helps you run your business as reliable as possible.

Please visit our website at https://www.giepa.de

9.2 Support contact information

Please use the following email address to contact the **Giegerich & Partner GmbH** support for issues relating to **gpg4o**:

support.gpg4o@giepa.de

You can also use the web contact form at:

https://www.giepa.de/contact/?lang=en

General contact information:

Giegerich & Partner GmbH

Robert-Bosch-Str. 18

D-63303 Dreieich

Germany

Phone: +49 (0)6103-5881-0

Web: https://www.giepa.de/?lang=en