Giegerich & Partner

gpg4o

Administrator-Handbuch

gpg4o Version 3.4

Inhaltsverzeichnis

1 Einleitung

Dieses Handbuch soll dazu dienen Administratoren ein Nachschlagewerk für die Möglichkeiten von **gpg4o** in die Hand zu geben. In dem Handbuch wird u.a. beschrieben wie man **gpg4o** installiert und im Unternehmen verteilt.

gpg4o, ab der Version 3.3, ist mit seinen zahlreichen Verbesserungen für den Einsatz in Unternehmen optimiert worden. Vor allem wurde die Konfiguration von **gpg4o** dahingehend erweitert, dass sie sich nun über Gruppenrichtlinien verwalten lässt. Mit diesen Gruppenrichtlinien können Sie das Verhalten bzw. die Einstellungen von **gpg4o** nach Ihren Wünschen bearbeiten.

Beispiel für Gruppenrichtlinien:

Den Anwendern wird ein Schlüsselpaar zu Verfügung gestellt. Die Anwender sollen keine Schlüsselpaare löschen und keine Schlüssel neu erstellen können.

Folgende Gruppenrichtlinien müssen dafür aktiviert werden:

- Benutzer dürfen keine Schlüsselpaare löschen
- Benutzer dürfen keine Schlüssel erstellen

Mit diesen Einstellungen haben Sie sichergestellt das der Anwender keine eigenen Schlüssel erstellen und dem Ihm zur Verfügung gestellten Schlüssel nicht unabsichtlich löschen kann. Mit diesen Einstellungen müssen die Benutzer Ihr Schlüsselpaar von einer administrativen Instanz erhalten.

2 Installation

gpg4o wird für alle Anwender eines Computers installiert, weshalb die Installation bzw. ein Update nur von Benutzern mit Administrator-Rechten durchgeführt werden kann. Zur Verwendung von **gpg4o** sind keine Administrator-Rechte notwendig.

2.1 Unbeaufsichtigte Installation

Gründe für eine unbeaufsichtigte Installation:

- Entfernte Installation auf einen Client-PC in Ihrem Unternehmen
- Installation auf verschiedenen Client-PCs in Ihrem Unternehmen
- Updates für **gpg4o** auf verschiedenen Client-PCs in Ihrem Unternehmen einspielen

Für eine Installation von **gpg4o** ohne Benutzerinteraktion reicht es aus, bei Aufruf des Setups den Parameter /quiet anzugeben. **gpg4o** wird dann ohne weitere Rückmeldung an den Anwender auf dem Computer installiert. Folgende Komponenten (siehe 3.1 Liste der Komponenten) müssen bei einer Silent Installation vorinstalliert werden.

```
gpg4o_setup.exe /quiet
```

Sofern Sie zur Installation die heruntergeladene **„gpg4o_setup.exe“** verwenden, müssen keine weiteren Vorarbeiten durchgeführt werden. Das Installationsprogramm überprüft, ob alle von **gpg4o** benötigten Komponenten vorhanden sind und installiert diese bei Bedarf automatisch mit. Bitte beachten Sie dass **gpg4o** die benötigten Pakete über das Internet von der Microsoft Webseite herunterlädt, sofern die Installation nicht mit dem Parameter /quiet gestartet wurde.

3 Verteilung von gpg4o im Unternehmen

3.1 Einbindung in automatische Softwareverteilungssysteme

Das von der Webseite herunterladbare **gpg4o** Setup ist ein selbst extrahierendes Archiv dar, welches Microsoft Installer Pakete (MSI) für die Installation in 32 und 64 Bit Umgebungen beinhaltet.

Sie müssen gpg4o immer passend zur Office Installation installieren. Wenn bei den Benutzern ein 32 Bit Office installiert ist, muss auch gpg4o als 32 Bit installiert werden. Gleiches gilt für eine 64 Bit Installation.

Eine Verteilung von **gpg4o** in einem Netzwerk ist so mit handelsüblichen Tools möglich. Die MSI Pakete und zugehörigen Bootstrapper können Sie mittels eines Packprogrammes (wie beispielsweise 7Zip) aus dem Setup entpacken und diese in Ihr Programm zur Verteilung von Software einbinden.

Bitte beachten Sie, dass die entpackten Windows Installer Dateien vor Ihrer Verwendung zu **„gpg4oSetup.msi“** und **„setup.exe“** umbenannt werden müssen.

Wenn die Installation über die MSI Pakete erfolgen soll, muss sichergestellt werden, dass sich die folgenden Komponenten auf dem Zielcomputer befinden oder diese im Voraus installiert werden:

Folgende Komponenten müssen bei einer Silent Installation vorinstalliert sein.

- Microsoft .NET Framework 4.0 (Full Package)
- Microsoft Office 2010 Primary Interop Assemblies
- Microsoft Visual Studio 2010 Tools for Office Runtime (VSTO 4.0)

Diese Software-Pakete sind unabhängig von der auf dem Computer befindlichen Version von Microsoft Outlook® zu installieren.

Bitte beachten Sie, dass **gpg4o** ohne korrekte Installation dieser Systemvopraussetzungen nicht installiert werden kann. Wenn Sie die Installation über **„gpg4o_setup.exe“** oder **„setup.exe“** durchführen, werden die genannten Pakete automatisch installiert.

3.2 Verteilung auf Computern mit mehreren Benutzern (Terminalserver)

Nachdem **gpg4o** auf dem Zielcomputer installiert wurde, benötigt jeder Benutzer von **gpg4o** eine Lizenzdatei. Diese **„LicenseInformation.lic“** kann dem Anwender über einen Kopiervorgang in das **gpg4o** Benutzerverzeichnis (siehe Kapitel 7) zur Verfügung gestellt werden. Nach einem Neustart von Outlook erkennt und verwendet **gpg4o** diese Lizenzdatei.

Für den Einsatz von **gpg4o** auf einem Computer mit mehreren Benutzern kann es sein, dass manche Benutzer gar keine Lizenz erhalten sollen. Wenn man **gpg4o** hier nicht deaktiviert, fallen diese Benutzer in den Test-Modus, der ab der ersten Installation 45 Tage lang zur Verfügung steht. Danach kann **gpg4o** nicht mehr genutzt werden und es erscheinen Dialoge, die zum Kauf auffordern.

Da dies den Benutzer bei seiner Arbeit stört, haben wir hierfür eine spezielle Lizenzdatei (**„Cloak-Lizenz“**) entworfen, welche **gpg4o** optisch fast vollständig deaktiviert. Einzig der Import einer Lizenz aus einer E-Mail heraus bleibt vorhanden. Zusätzlich werden viele Funk-

tionen von **gpg4o** erst gar nicht geladen, sodass auch der Start von Outlook beschleunigt wird. Diese **„Cloak-Lizenz“** kann beim Support kostenlos angefordert werden.

Die Cloak-Lizenz kann man als Administrator unbeaufsichtigt an die Benutzer, die kein **gpg4o** benutzen sollen, verteilen. Die Cloak-Lizenz muss unter dem Dateinamen **„LicenseInformation.lic“** in das **gpg4o** Benutzerverzeichnis (siehe Kapitel 7) kopiert werden.

Die andere Möglichkeit **gpg4o** zu deaktivieren, besteht mit der Gruppenrichtlinien „Funktionsbeschränkungen\Lizenzierung\Benutzung von gpg4o deaktivieren“. Dies hat die gleiche Auswirkung wie die Cloak-Lizenz zu verteilen, stellt jedoch in den meisten Fällen einen geringeren Aufwand dar.

4 Gruppenrichtlinien

Administratoren können, seit der Version 3.3, die Verwendung von Programmfunktionalitäten und -einstellungen von **gpg4o** über Gruppenrichtlinien einschränken. Die Konfiguration von **gpg4o** wurde dahingehend erweitert, dass sie sich über Gruppenrichtlinien einstellen lässt. Hierzu stehen die Template-Formate ADM sowie ADMX zur Verfügung, welche Sie kostenlos vom Support beziehen können. Das ADM-Format brauchen Sie nur, wenn Sie noch Computer mit Windows XP administrieren. Alle neueren Windows Versionen unterstützen beide Template-Formate ADM sowie ADMX.

Sie finden die Richtlinien im Gruppenrichtlinienverwaltungs-Editor unter Benutzereinstellungen\Giegerich & Partner - gpg4o. Alle Richtlinien enthalten eine Erklärung, welche aussagt, wie sich das Programm beim Anwender verhält, wenn die Richtlinie aktiviert bzw. deaktiviert wird, und wie das Standardverhalten ist. Grundsätzlich gilt jedoch für alle Einstellungen, dass beim Aktivieren bzw. Deaktivieren die Einstellung vorgegeben wird, der Benutzer diese also nicht mehr ändern kann.

Nachfolgend finden Sie eine Auflistung der Richtlinien und deren zusätzliche Erklärungen für **gpg4o**. Die Voreinstellungen von **gpg4o** werden genannt (Die Erstinstallation von **gpg4o** benutzt diese Voreinstellungen.):

4.1 Funktionsbeschränkungen

- Benutzer dürfen E-Mails nicht entschlüsselt speichern
  - „Wenn Sie die Richtlinie aktivieren, können die Benutzer keine E-Mails mehr dauerhaft entschlüsselt speichern. Wenn Sie die Richtlinie deaktivieren, können die Benutzer E-Mails über die zugehörige Schaltfläche dauerhaft entschlüsselt abspeichern.“
  - [Voreinstellung: Die Richtlinie ist deaktiviert.]

4.1.1 Backup

- Benutzer dürfen keine Backups importieren
  - „Wenn Sie die Richtlinie aktivieren, können die Benutzer keine Backups mehr in den Einstellungen bzw. dem Konfigurationsassistenten importieren. Wenn Sie die Richtlinie deaktivieren, können die Benutzer Backups importieren, wobei je nach Zustand der Richtlinie ”Benutzer dürfen keine Lizenzen importieren”der Import der Lizenz übersprungen wird.“
  - [Voreinstellung: Die Richtlinie ist deaktiviert.]
- Benutzer dürfen keine Backups exportieren
  - „Wenn Sie die Richtlinie aktivieren, können die Benutzer keine Backups mehr in den Einstellungen exportieren. Wenn Sie die Richtlinie deaktivieren, können die Benutzer Backups exportieren.“
  - [Voreinstellung: Die Richtlinie ist deaktiviert.]

4.1.2 Lizenzierung

- Benutzer dürfen keine Lizenzen importieren
  - „Wenn Sie diese Richtlinie aktivieren, können die Benutzer keine Lizenzdateien mehr importieren, weder aus einer E-Mail heraus, noch vom Dateisystem. Außerdem wird beim Import eines Backups die Lizenz ignoriert. Wenn Sie die Richtlinie deaktivieren, können Benutzer Lizenzdateien importieren. Außerdem wird der Import der Lizenz beim Importieren eines Backups nicht übersprungen.“
  - [Voreinstellung: Die Richtlinie ist deaktiviert.]
- Benutzung von gpg4o deaktivieren
  - „Wenn Sie die Richtlinie aktivieren, wird gpg4o bei den Benutzern weitestgehend deaktiviert. Es bleibt lediglich der Import von Lizenzdateien aus E-Mails heraus aktiv, soweit dies nicht ebenfalls über eine Richtlinie deaktiviert wurde. Wenn Sie die Richtlinie deaktivieren, wird gpg4o geladen und ist normal benutzbar im Rahmen der Lizenz.“
  - [Voreinstellung: Die Richtlinie ist deaktiviert.]

4.1.3 Senderegeln

- Benutzer dürfen keine Senderegeln erstellen
  - „Wenn Sie die Richtlinie aktivieren, können die Benutzer keine Senderegeln erstellen. Wenn Sie die Richtlinie deaktivieren, können die Benutzer Senderegeln erstellen.“
  - [Voreinstellung: Die Richtlinie ist deaktiviert.]
- Benutzer dürfen keine Senderegeln löschen
  - „Wenn Sie die Richtlinie aktivieren, können die Benutzer keine Senderegeln löschen. Wenn Sie die Richtlinie deaktivieren, können die Benutzer Senderegeln löschen.“
  - [Voreinstellung: Die Richtlinie ist deaktiviert.]
- Benutzer dürfen keine Senderegeln verändern
  - „Wenn Sie die Richtlinie aktivieren, können die Benutzer bestehende Senderegeln nicht editieren. Wenn Sie die Richtlinie deaktivieren, können die Benutzer bestehende Senderegeln editieren.“
  - [Voreinstellung: Die Richtlinie ist deaktiviert.]

4.1.4 Schlüsselverwaltung

- Benutzer dürfen keine Schlüssel erstellen
  - „Wenn Sie diese Richtlinie aktivieren, können die Benutzer keine Schlüssel erstellen. In diesem Fall muss eine administrative Instanz zur Verfügung stehen, welche die Schlüssel erstellt, verwaltet und an die Benutzer ausgibt. Wenn Sie diese Richtlinie deaktivieren, können die Benutzer ihre eigenen Schlüssel erstellen."
  - [Voreinstellung: Die Richtlinie ist deaktiviert.]
- Benutzer dürfen keine öffentlichen Schlüssel löschen
  - „Wenn Sie diese Richtlinie aktivieren, können die Benutzer keine öffentlichen Schlüssel aus ihrem Schlüsselring löschen. Diese Richtlinie wirkt sich jedoch nicht auf das Löschen von Schlüsselpaaren aus. Wenn Sie diese Richtlinie deaktivieren, können die Benutzer öffentliche Schlüssel aus ihrem Schlüsselring löschen."
  - [Voreinstellung: Die Richtlinie ist deaktiviert.]
- Benutzer dürfen keine Schlüsselpaare löschen
  - „Wenn Sie diese Richtlinie aktivieren, können die Benutzer Schlüsselpaare aus ihrem Schlüsselring löschen. Wenn Sie diese Richtlinie deaktivieren, können die Benutzer Schlüsselpaare aus ihrem Schlüsselring löschen."
  - [Voreinstellung: Die Richtlinie ist deaktiviert.]
- Benutzer dürfen keine öffentliche Schlüssel importieren
  - „Wenn Sie diese Richtlinie aktivieren, können die Benutzer keine öffentlichen Schlüssel aus Dateien, Anhängen oder der Zwischenablage importieren. Davon ausgenommen ist das Importieren öffentlicher Schlüssel von Schlüsselservern. Wenn Sie diese Richtlinie deaktivieren, können die Benutzer öffentliche Schlüssel aus den genannten Medien importieren."
  - [Voreinstellung: Die Richtlinie ist deaktiviert.]
- Benutzer dürfen keine Schlüsselpaare importieren
  - „Wenn Sie diese Richtlinie aktivieren, können die Benutzer keine Schlüsselpaare aus Dateien, Anhängen oder der Zwischenablage importieren. Wenn Sie diese Richtlinie deaktivieren, können die Benutzer Schlüsselpaare aus den genannten Medien importieren."
  - [Voreinstellung: Die Richtlinie ist deaktiviert.]
- Benutzer dürfen keine öffentliche Schlüssel exportieren
  - „Wenn Sie diese Richtlinie aktivieren, können die Benutzer keine öffentlichen Schlüssel exportieren oder per E-Mail versenden. Davon ausgenommen ist das Exportieren von öffentlichen Schlüsseln auf Schlüsselserver. Wenn Sie diese Richtlinie deaktivieren, können die Benutzer öffentliche Schlüssel exportieren und per E-Mail versenden."
  - [Voreinstellung: Die Richtlinie ist deaktiviert.]

- Benutzer dürfen keine Schlüsselpaare exportieren
  - „Wenn Sie diese Richtlinie aktivieren, können die Benutzer keine Schlüsselpaare als Datei exportieren. Wenn Sie diese Richtlinie deaktivieren, können die Benutzer Schlüsselpaare exportieren.“
  - [Voreinstellung: Die Richtlinie ist deaktiviert.]
- Benutzer dürfen keine Schlüssel (de)-aktivieren
  - „Wenn Sie diese Richtlinie aktivieren, können die Benutzer keine Schlüssel in ihrem Schlüsselring aktivieren bzw. deaktivieren. Wenn Sie diese Richtlinie deaktivieren, können die Benutzer Schlüssel in ihrem Schlüsselring aktivieren bzw. deaktivieren.“
  - [Voreinstellung: Die Richtlinie ist deaktiviert.]
- Benutzer dürfen keine Rückzugszertifikate erstellen
  - „Wenn Sie diese Richtlinie aktivieren, können die Benutzer keine Rückzugszertifikate für ihre Schlüsselpaare erstellen. Diese müssen dann durch eine administrative Instanz erzeugt werden, die eine Kopie des Schlüsselpaares hat. Wenn Sie diese Richtlinie deaktivieren, können die Benutzer Rückzugszertifikate für ihre Schlüsselpaare erstellen.“
  - [Voreinstellung: Die Richtlinie ist deaktiviert.]
- Benutzer dürfen keine Rückzugszertifikate anwenden
  - „Wenn Sie diese Richtlinie aktivieren, können die Benutzer keine Rückzugszertifikate auf ihre Schlüsselpaare anwenden. Dies muss dann durch eine administrative Instanz geschehen, welche den zurückgezogenen Schlüssel dann neu auch verteilen muss. Wenn Sie diese Richtlinie deaktivieren, können die Benutzer auf ihre Schlüsselpaare Rückzugszertifikate anwenden.“
  - [Voreinstellung: Die Richtlinie ist deaktiviert.]
- Benutzer dürfen keine Schlüssel auf Schlüsselserver hochladen
  - „Wenn Sie diese Richtlinie aktivieren, können die Benutzer keine öffentlichen Schlüssel auf Schlüsselserver hochladen. Dies betrifft auch den öffentlichen Teil der eigenen Schlüsselpaare. Wenn Sie diese Richtlinie deaktivieren, können die Benutzer öffentliche Schlüssel auf Schlüsselserver hochladen.“
  - [Voreinstellung: Die Richtlinie ist deaktiviert.]
- Benutzer dürfen keine Schlüssel von Schlüsselserver herunterladen
  - „Wenn Sie diese Richtlinie aktivieren, können die Benutzer keine öffentlichen Schlüssel von Schlüsselservern herunterladen. Dies gilt nicht für den Server zum automatischen Herunterladen von Schlüsseln. Wenn Sie diese Richtlinie deaktivieren, können die Benutzer öffentliche Schlüssel von Schlüsselservern herunterladen.“
  - [Voreinstellung: Die Richtlinie ist deaktiviert.]

- Benutzer dürfen die Passphrase ihrer Schlüsselpaare nicht ändern
  - „Wenn Sie diese Richtlinie aktivieren, können die Benutzer die Passphrase von Schlüsselpaaren in ihrem Schlüsselring nicht ändern. Wenn Sie diese Richtlinie deaktivieren, können die Benutzer die Passphrase von Schlüsselpaaren in ihrem Schlüsselring ändern. Dies ändert nicht den Schlüssel selbst. Somit bleiben Kopien des Schlüssels davon unberührt und funktionsfähig“
  - [Voreinstellung: Die Richtlinie ist deaktiviert.]
- Benutzer dürfen Schlüssel nicht signieren
  - „Wenn Sie diese Richtlinie aktivieren, können die Benutzer keine Schlüssel signieren. In diesem Fall müssen die Schlüssel durch eine administrative Instanz signiert werden. Wenn Sie diese Richtlinie deaktivieren, können die Benutzer Schlüssel signieren. Diese Richtlinie bezieht sich nur auf die exportierbare Signatur, nicht auf die lokale Signatur.“
  - [Voreinstellung: Die Richtlinie ist deaktiviert.]
- Benutzer dürfen Schlüssel nicht lokal signieren
  - „Wenn Sie diese Richtlinie aktivieren, können die Benutzer keine Schlüssel lokal signieren. Wenn Sie diese Richtlinie deaktivieren, können die Benutzer Schlüssel lokal signieren. Diese Richtlinie bezieht sich nur auf die nicht exportierbare „lokale“ Signatur.“
  - [Voreinstellung: Die Richtlinie ist deaktiviert.]
- Benutzer dürfen das Besitzervertrauen von Schlüsseln nicht setzen/ändern
  - „Wenn Sie diese Richtlinie aktivieren, können die Benutzer das Besitzervertrauen von Schlüsseln in ihrem Schlüsselring nicht mehr setzen bzw. ändern. Wenn Sie diese Richtlinie deaktivieren, können die Benutzer das Besitzervertrauen von Schlüsseln in ihrem Schlüsselring setzen bzw. ändern.“
  - [Voreinstellung: Die Richtlinie ist deaktiviert.]

4.2 Vorgegebene Einstellungen

4.2.1 Allgemeine Einstellungen

- E-Mails in öffentlichen Ordner entschlüsseln
  - „Wenn Sie diese Richtlinie aktivieren, wird gpg4o versuchen, E-Mails in öffentlichen Ordnern zu entschlüsseln bzw. wird die Signatur überprüfen. Zur Entschlüsselung wird natürlich das korrekte Schlüsselpaar benötigt. Wenn Sie diese Richtlinie deaktivieren, wird gpg4o in öffentlichen Ordnern keine E-Mails verarbeiten. Wenn Sie diese Richtlinie konfigurieren, können die Benutzer diese Einstellung nicht mehr selbst festlegen."
  - [Voreinstellung: Die Richtlinie ist nicht konfiguriert. Die Einstellung ist aktiviert.]
- Entschlüsselungsinfo in Inspektoren anzeigen
  - „Wenn Sie diese Richtlinie aktivieren, wird gpg4o beim Öffnen einer Nachricht in einem eigenen Fenster (Inspektor) den Verschlüsselungsstatus am Anfang der Nachricht einfügen. Wenn Sie diese Richtlinie deaktivieren, wird gpg4o in diesem Fall keinen Verschlüsselungsstatus in die Nachricht einfügen. Wenn Sie diese Richtlinie konfigurieren, können die Benutzer diese Einstellung nicht mehr selbst festlegen."
  - [Voreinstellung: Die Richtlinie ist nicht konfiguriert. Die Einstellung ist deaktiviert.]
- Entschlüsselungsinfo beim dauerhaften Entschlüsseln einbinden
  - „Wenn Sie diese Richtlinie aktivieren, wird gpg4o beim dauerhaften Entschlüsseln einer Nachricht den Verschlüsselungsstatus am Anfang der Nachricht eingefügen. Wenn Sie diese Richtlinie deaktivieren, wird gpg4o in diesem Fall keinen Verschlüsselungsstatus in die Nachricht einfügen. Wenn Sie diese Richtlinie konfigurieren, können die Benutzer diese Einstellung nicht mehr selbst festlegen."
  - [Voreinstellung: Die Richtlinie ist nicht konfiguriert. Die Einstellung ist aktiviert.]
- Entschlüsselungsinfo in der gpg4o-Leseansicht anzeigen
  - „Wenn Sie diese Richtlinie aktivieren, wird gpg4o beim Lesen einer Nachricht in der gpg4o-Leseansicht den Verschlüsselungsstatus auch am Anfang der Nachricht einfügen. Wenn Sie diese Richtlinie deaktivieren, wird gpg4o in diesem Fall keinen Verschlüsselungsstatus einfügen, sondern nur die Nachricht selbst anzeigen. Wenn Sie diese Richtlinie konfigurieren, können die Benutzer diese Einstellung nicht mehr selbst festlegen."
  - [Voreinstellung: Die Richtlinie ist nicht konfiguriert. Die Einstellung ist aktiviert.]

- Entschlüsselungsinfo in gedruckte E-Mails einbinden
  - „Wenn Sie diese Richtlinie aktivieren, wird gpg4o beim Drucken einer Nachricht über die Drucken Schaltfläche in der gpg4o-Leseansicht den Verschlüsselungsstatus am Anfang der Nachricht einfügen. Wenn Sie diese Richtlinie deaktivieren, wird gpg4o in diesem Fall keinen Verschlüsselungsstatus einfügen. Wenn Sie diese Richtlinie konfigurieren, können die Benutzer diese Einstellung nicht mehr selbst festlegen."
  - [Voreinstellung: Die Richtlinie ist nicht konfiguriert. Die Einstellung ist aktiviert.]
- Entschlüsselungsinfo in Antworten anzeigen
  - „Wenn Sie diese Richtlinie aktivieren, wird gpg4o beim Beantworten bzw. Weiterleiten einer Nachricht die Verschlüsselungsstatus am Anfang der Originalnachricht einfügen. Wenn Sie diese Richtlinie deaktivieren, wird gpg4o in diesem Fall keine Entschlüsselungsinfo in die Originalnachricht einfügen. Wenn Sie diese Richtlinie konfigurieren, können die Benutzer diese Einstellung nicht mehr selbst festlegen."
  - [Voreinstellung: Die Richtlinie ist nicht konfiguriert. Die Einstellung ist aktiviert.]
- Dauer des Zwischenspeichern einer Passphrase bei Verwendung des GnuPG Agents (GnuPG 2.0.x)
  - „Diese Richtlinie bezieht sich nur auf Benutzer, die GnuPG 2.0.x mit dem GnuPG Agent einsetzen. Wenn Sie diese Richtlinie aktivieren, wird der GnuPG Agent eingegebene Passphrasen für die von Ihnen angegebene Dauer zwischenspeichern. Die Dauer wird für jeden privaten Schlüssel separat gezählt. Wenn ein privater Schlüssel länger als die angegebene Dauer nicht genutzt wurde, wird der Benutzer bei der nächsten Verwendung wieder nach der Passphrase gefragt. Wenn Sie die Richtlinie deaktivieren, können die Benutzer die Dauer selbst festlegen."
  - [Voreinstellung: Die Richtlinie ist deaktiviert. Die Passphrasen werden 5 Minuten zwischengespeichert.]
- Dauer des Zwischenspeichern einer Passphrase bei Verwendung von GnuPG 1.4.x vorgeben
  - „Diese Richtlinie bezieht sich nur auf Benutzer, die GnuPG 1.4.x einsetzen. Wenn Sie diese Richtlinie aktivieren, wird gpg4o die zuletzt eingegebene Passphrase für die von Ihnen angegebene Dauer zwischenspeichern. Wenn ein anderer Schlüssel benutzt wird als zuletzt und die Passphrasen unterscheiden sich, muss der Benutzer die Passphrase des anderen Schlüssels eingeben. Wenn Sie diese Richtlinie deaktivieren, können die Benutzer die Dauer selbst festlegen."
  - [Voreinstellung: Die Richtlinie ist deaktiviert. Die Passphrasen werden bis zum Beenden von Outlook zwischengespeichert.]

- Anhangnamen verbergen
  - „Wenn Sie diese Richtlinie aktivieren, werden Dateinamen von E-Mail Anhängen bei den Benutzern verborgen. Somit erscheinen in verschlüsselter Form Dateinamen wie Attachment1.pgp anstatt des echten Dateinamens mit angehängter Dateiendung. Diese Art der Verschlüsselung von Dateien wird aber nicht von allen OpenPGP-Implementierungen unterstützt. Wenn Sie diese Richtlinie deaktivieren, werden die Dateinamen nicht verborgen. Es erscheint dann zum Beispiel der Dateiname Abrechnung.xlsx.pgp. Diese Variante lässt zwar Rückschlüsse auf den Inhalt der Dateien zu, ist aber kompatibler mit anderen OpenPGP-Implementierungen. Wenn Sie diese Richtlinie konfigurieren, können die Benutzer diese Einstellung nicht mehr selbst festlegen.“
  - [Voreinstellung: Die Richtlinie ist nicht konfiguriert. Die Anhangnamen werden verborgen.]
- Sprache
  - „Wenn Sie diese Richtlinie aktivieren, wird bei den Benutzern beim nächsten Start von Outlook gpg4o in der von Ihnen ausgewählten Sprache gestartet. Wenn Sie diese Richtlinie deaktivieren, können die Benutzer die ihre bevorzugte Sprache selbst einstellen.“
  - [Voreinstellung: Die Richtlinie ist deaktiviert. Die Standardsprache ist die Systemsprache, wenn sie von gpg4o unterstützt wird, ansonsten Englisch.]
- Schlüsseln immer vertrauen
  - „Wenn Sie diese Richtlinie aktivieren, können die Benutzer an alle Schlüsselbesitzer verschlüsselte Nachrichten versenden und alle Signaturen der Schlüsselbesitzer prüfen - unabhängig vom Web of Trust. Auch wenn dies einfacher für die Benutzer ist, sollten Sie diese Richtlinie nicht aktivieren, da es die Benutzung von nicht vertrauenswürdigen Schlüsseln ermöglicht. Wenn Sie diese Richtlinie deaktivieren, müssen Schlüssel zuerst über das Web of Trust validiert werden, bevor sie benutzt werden können. Wenn Sie diese Richtlinie konfigurieren, können die Benutzer diese Einstellung nicht mehr selbst festlegen.“
  - [Voreinstellung: Die Richtlinie ist nicht konfiguriert. Den Schlüsseln wird immer vertraut.]
- GnuPG Datenverzeichnis vorgeben
  - „Wenn Sie diese Richtlinie aktivieren, wird gpg4o die Schlüsselringe aus dem von Ihnen angegebenen Datenverzeichnis laden. Der Pfad sollte daher eine benutzerspezifische Systemvariable nutzen, damit nicht alle Nutzer auf die gleichen Schlüsselringe zugreifen. Wenn Sie diese Richtlinie deaktivieren, können die Benutzer selbst das Datenverzeichnis einstellen.“
  - [Voreinstellung: Die Richtlinie ist deaktiviert. Das Standardverzeichnis ist „%AppData%\gnupg“.]

- GnuPG-Kopfzeilen unterbinden
  - „Wenn Sie diese Richtlinie aktivieren, wird das Einfügen der GnuPG Versionszeile sowie des Kommentares mit der gpg4o Version unterbunden. Dies kann aus Sicherheitsgründen sinnvoll sein. Wenn Sie diese Richtlinie deaktivieren, werden die o.g. Zeilen immer eingefügt. Dies erleichtert im Fehlerfall die Fehlersuche beim Empfänger. Wenn Sie diese Richtlinie konfigurieren, können die Benutzer diese Einstellung nicht mehr selbst festlegen.“
  - [Voreinstellung: Die Richtlinie ist nicht konfiguriert. Die Kopfzeilen werden eingefügt.]
- Pfad zu GnuPG vorgeben
  - „Wenn Sie diese Richtlinie aktivieren, wird gpg4o die GnuPG-Installation am von Ihnen angegebenen Pfad nutzen. Sie können im Pfad auch Systemvariable nutzen. Wenn Sie diese Richtlinie deaktivieren, können die Benutzer selbst den Pfad zur GnuPG Installation einstellen.“
  - [Voreinstellung: Die Richtlinie ist deaktiviert. Der Pfad wird automatisch ermittelt. Standardmäßig wird GnuPG über die Registry gesucht, danach unter „%ProgramFiles(x86)%\GNU\GnuPG“ mit den Dateinamen gpg.exe bzw. gpg2.exe.]
- Sendeoptionen bei inaktiven gpg4o-Konten ausblenden
  - „Wenn Sie diese Richtlinie aktivieren, werden die Benutzer die gpg4o Sendeoptionen nur beim Verfassen von E-Mails aus einem aktiven E-Mail Konten heraus sehen. Wenn Sie diese Richtlinie deaktivieren, werden die Sendeoptionen bei allen neuen E-Mails angezeigt. Wenn Sie diese Richtlinie konfigurieren, können die Benutzer diese Einstellung nicht mehr selbst festlegen.“
  - [Voreinstellung: Die Richtlinie ist nicht konfiguriert. Die Sendeoptionen werden immer angezeigt.]
- Den GnuPG Agent beim Beenden von Outlook ebenfalls beenden
  - „Wenn Sie diese Richtlinie aktivieren, wird der GnuPG Agent beim Beenden von Outlook ebenfalls beendet. Somit werden alle gespeicherten Passphrasen vergessen und müssen beim erneuten Starten von Outlook bei Bedarf wieder eingegeben werden. Wenn Sie diese Richtlinie deaktivieren, wird der GnuPG Agent nicht beendet, wenn Outlook beendet wird. Passphrasen sind auch nach einem Neustart von Outlook verfügbar, soweit die Dauer der Zwischenspeicherung nicht überschritten wurde. Wenn Sie diese Richtlinie konfigurieren, können die Benutzer diese Einstellung nicht mehr selbst festlegen.“
  - [Voreinstellung: Die Richtlinie ist nicht konfiguriert. Der GnuPG Agent wird nicht mit Outlook beendet.]

- Updateverhalten von gpg4o vorgeben
  - „Wenn Sie diese Richtlinie aktivieren, wird gpg4o entsprechend Ihrer Auswahl nach Updates suchen. Beachten Sie aber, dass auch bei automatischer Suche nach Updates diese Installation noch durch die Benutzer bestätigt werden muß, bevor sie installiert werden. Wenn Sie diese Richtlinie deaktivieren, können die Benutzer selbst die Einstellungen zu Updates beeinflussen.“
  - [Voreinstellung: Die Richtlinie ist deaktiviert. gpg4o sucht automatisch nach Updates.]
- Domänenbasierte Schlüsselsuche verwenden
  - „Wenn Sie diese Richtlinie aktivieren, wird beim Verschlüsseln von Nachrichten an Empfänger, für die kein passender Schlüssel gefunden werden kann, ein alternativer Schlüssel angeboten. Die Suche nach diesem alternativen Schlüssel basiert auf der Domäne der E-Mail Adresse des Empfängers. Die Benutzer können diesen Vorschlag annehmen oder selbst einen Schlüssel auswählen, mit dem die Nachricht verschlüsselt werden soll. Wenn Sie diese Richtlinie deaktivieren, müssen die Benutzer die Auswahl eines zu verwendenden Schlüssels in solch einem Fall generell immer übernehmen. Wenn Sie diese Richtlinie konfigurieren, können die Benutzer diese Einstellung nicht mehr selbst festlegen.“
  - [Voreinstellung: Die Richtlinie ist nicht konfiguriert. Die domänenbasierte Schlüsselsuche ist deaktiviert.]
- Dateiendung .gpg für verschlüsselte Anhänge verwenden
  - „Wenn Sie die Richtlinie aktivieren, wird beim Verschlüsseln von Anhängen immer die Dateiendung .gpg verwendet. Wenn Sie die Richtlinie deaktivieren, wird beim Verschlüsseln von Anhängen immer die Dateiendung .pgp verwendet. Wenn Sie diese Richtlinie konfigurieren, können die Benutzer diese Einstellung nicht mehr selbst festlegen.“
  - [Voreinstellung: Die Richtlinie ist nicht konfiguriert. gpg4o benutzt die Dateiendung .pgp.]
- Den gpg4o-internen Paketparser verwenden
  - „Wenn Sie diese Richtlinie aktivieren, wird gpg4o die Daten in OpenPGP-Paketen weitestgehend selbstständig analysieren, um Rechenzeit zu sparen. Es kann hierbei aber bei manchen Anhängen zu Problemen kommen. In dem Fall wird gpg4o GnuPG zur Analyse benutzen. Wenn Sie diese Richtlinie deaktivieren, wird gpg4o immer GnuPG zur Analyse der OpenPGP-Daten benutzen.“
  - [Voreinstellung: Die Richtlinie ist nicht konfiguriert. Die Einstellung ist aktiviert.]

- E-Mails immer klonen statt kopieren
  - „Wenn Sie diese Richtlinie aktivieren, werden E-Mails zum Entschlüsseln immer von gpg4o geklont. Wenn Sie diese Richtlinie deaktivieren, wird die Outlook-eigene Kopierroutine verwendet, wenn dies möglich ist.“
  - [Voreinstellung: Die Richtlinie ist nicht konfiguriert. Die Einstellung ist deaktiviert.]
- Entschlüsselung in einer eigenen Datendatei vollziehen
  - „E-Mails werden vor der Entschlüsselung mit gpg4o immer zuerst an einen Ort kopiert/geklont, von dem aus keine Syncronisation mit dem Server stattfindet. Wenn Sie diese Richtlinie aktivieren, wird dafür die Datendatei gpg4oTemp.pst verwendet. Wenn Sie diese Richtlinie deaktivieren, wird stattdesen ein Order Temp unterhalb des Posteinganges angelegt und dessen Symcronisation mit dem Server unterbunden. Da diese Unterbindung nicht in allen Fällen gewährleistet werden kann, sollten Sie diese Richtlinie nur bei Problemen mit der Datendatei deaktivieren.“
  - [Voreinstellung: Die Richtlinie ist nicht konfiguriert. Die Einstellung ist aktiviert.]
- Timeout eines GnuPG Prozeses vorgeben
  - „Wenn Sie diese Richtlinie aktivieren, legen Sie damit die Dauer fest, wie lange gpg4o auf das ordnungsgemäße Beenden eines GnuPG-Aufrufes wartet, bevor es den Benutzer auf einen eventuellen Fehler hinweist. Der Nutzer kann dem Prozess dann nochmals Zeit geben, um sauber zu beenden, oder ihn beenden lassen. Wenn Sie diese Richtlinie deaktivieren, wird die Standardeinstellung von 15 Sekunden verwendet. Dieser Wert kann derzeit nicht vom Benutzer in den Einstellungen von gpg4o konfiguriert werden. Wenn Sie auf einigen Computern Probleme mit zu lange laufenden GnuPG-Prozessen haben, sollten Sie diese Richtlinie aktivieren und den Prozessen mehr Zeit geben.“
  - [Voreinstellung: Die Richtlinie ist deaktiviert. Es wird die Standardeinstellung von 15 Sekunden (Wert: 15000 ms) verwendet.]

4.2.2 Einstellungen zu Schlüsselservern

- Keyserver-Liste vorgeben
  - „Wenn Sie diese Richtlinie aktivieren, können die Benutzer nur die angegebenen Keyserver benutzen. Hierzu müssen Sie die URI des Keyservers und dessen Berechtigungen eingeben. Die Berechtigungen sind in Download und Upload unterteilt und können die Werte 0 (Nicht erlaubt), 1 (Nur manuelle erlaubt), 2 (Nur automatisch erlaubt) and 3 (Beides erlaubt) haben. Formatiert wird der Wert, indem man den numerischen Wert der Berechtigung für den Download anbingt, gefolgt von einem Semikolon und dem Wert für den Upload.

    Beispiel:

    hkp://keys.company.com 3;1

    Dies resultiert in einem einzelnen für die Benutzer verfügbaren Keyserver, welcher für das manuelle herunterladen und hochladen von Schlüsseln sowie für das automatische Importieren fehlender Schlüssel beim Schreiben von E-Mails benutzt werden kann. Wenn Sie diese Richtlinie deaktivieren, können die Benutzer die Schlüsselserver selbst festlegen. “
  - [Voreinstellung: Die Richtlinie ist deaktiviert.]

5 Automatisiertes Erstellen von Schlüsselpaaren

gpg4o bietet Ihnen die Möglichkeit, mehrere Schlüsselpaare in einem Durchlauf zu erzeugen. Dies ist beispielsweise dann sinnvoll, wenn Sie bei erstmaligem Einsatz von **gpg4o** in einem Unternehmen viele Mitarbeiter mit Schlüsselpaaren ausstatten müssen.

Sie benötigen hierzu nur ein funktionsfähig eingerichtetes **gpg4o** mit leeren Schlüsselringen und eine CSV-Datei mit den Daten der zu erstellenden Schlüsselpaaren.

5.1 Vorbereitung

gpg4o muss funktionsfähig eingerichtet sein und die GnuPG Schlüsselringe sollten leer sein. Dies können Sie erreichen, indem Sie das Verzeichnis für die Schlüsselringe bei geschlossenem Outlook umbenennen.

Die in diesem Abschnitt referenzierten Speicherorte der **gpg4o** und **GnuPG** Daten finden Sie in Kapitel 7.

Achtung: Die Schlüsselringe beinhalten Ihren privaten Schlüssel, den Sie zur Entschlüsselung von E-Mails benötigen. Sie sollten die Schlüsselringe daher nicht löschen oder eine Sicherung überschreiben!

Die Daten der zu erstellenden Schlüsselpaare müssen in einer CSV-Datei (Comma Separated Values) mit dem Namen **„userlist.csv“** im **gpg4o** Benutzerverzeichnis vorliegen.

Die CSV-Datei beinhaltet pro Zeile die mit Semikolon „ ; “ voneinander getrennten Daten für ein einzelnes Schlüsselpaar und setzt sich aus drei Spalten für Name und Vorname, der E-Mail Adresse und der Passphrase zusammen:

```
Musterfrau, Erika;Erika.Musterfrau@work.com;passphrase
Karl-Heinz Mustermann;Karl-Heinz.Mustermann@work.com;passphrase
John Doe;JohnDoe@work.com;passphrase
```

Beachten Sie, dass die Datei keine Kopfzeile mit Spaltenbezeichnern beinhaltet.

5.2 Erstellung der Schlüsselpaare

Danach kann in Outlook über die Schlüsselverwaltung der Dialog (Neuer Schlüssel) zur Erstellung eines neuen Schlüsselpaares aufgerufen werden. Hier kann zusätzlich der für die Schlüssel zu verwendende Algorithmus und die Länge des Haupt- und Unterschlüssels ausgewählt werden.

Wenn Sie in diesem Dialog im Feld **„Name“** den Text „[csv]“ eintragen und auf die Schaltfläche **„OK“** klicken, werden die Schlüsselpaare anhand der Daten aus der CSV-Datei erzeugt.

Die so erzeugten Schlüssel stehen danach über die **gpg4o** Schlüsselverwaltung zur Verfügung. Bereits vorhandene Schlüssel werden anhand der E-Mail Adresse identifiziert und nicht erstellt/überschrieben, so dass keine Duplikate entstehen können.

5.3 Sicherung der Schlüsselpaare

Hinweis: Sie sollten beim Erstellen der Schlüsselpaare immer eine sichere Passphrase benutzen.

Hinweis: Nachdem die Schlüsselpaare erzeugt wurden, sollten Sie eine Sicherung dieser anlegen. Dazu sichern Sie einfach die beiden Dateien **„secring.gpg“** und **„pubring.gpg“** zu finden im GnuPG Datenverzeichnis siehe Kapitel 7. Die dazugehörigen Passphrasen sollen bitte mit abgesichert werden

5.4 Verteilung der Schlüssel

Die erzeugten öffentlichen Schlüssel können über die **gpg4o** Schlüsselverwaltung einzeln in das Dateisystem exportiert oder auf einen Schlüsselserver hochgeladen werden, so dass die Benutzer sich diese in ihren Schlüsselring importieren können.

Tipp: In der Schlüsselverwaltung können auch mehrere Schlüssel auf einmal markiert werden.

Sofern es sich um eine erstmalige Installation in Ihrem Unternehmen handelt und alle Benutzer die im vorherigen Abschnitt generierten öffentlichen Schlüssel erhalten sollen, können Sie die Datei **„pubring.gpg“** im GnuPG Datenverzeichnis (siehe Kapitel 7) auf die Zielcomputer kopieren.

Den privaten Schlüssel exportieren Sie bitte auf einen Datenträger (USB-Stick, CD/DVD, ...) oder ein speziell gesichertes Netzlaufwerk und lassen diesen dem jeweiligen Benutzer zukommen, so dass dieser das Schlüsselpaar über die **gpg4o** Schlüsselverwaltung importieren kann.

Achtung: Lassen Sie den Benutzern ihre Schlüsselpaare nur über einen abgesicherten Weg zukommen, da sonst die Gefahr besteht, dass Unberechtigte E-Mails entschlüsseln oder in fremdem Namen unterschreiben können.

Hinweis: Nach dem Import des privaten Schlüssels auf den Rechner des Benutzers, muß die Passphrase vom Benutzer geändert werden!

6 gpg4o Update über einem Proxy Servers

Zum Verbindungsaufbau mit dem Updateserver über einen Proxy Server nutzt **gpg4o** die Netzwerk-Einstellungen, welche direkt in Ihrem System konfiguriert sind. Um eine Verbindung über einen Proxy Server aufzubauen, müssen Sie diesen in Ihren Internetoptionen eintragen.

Diese finden Sie in der **„Systemsteuerung“** von Windows in den **„Internetoptionen“**.

Öffnen Sie im folgenden Fenster den Reiter **„Verbindungen“** und klicken Sie im unteren Bereich auf die Schaltfläche **„LAN-Einstellungen“**.

In diesem neuen Fenster können Sie nun die Adresse des gewünschten Proxy Servers beziehungsweise ein automatisches Konfigurationsskript eintragen, damit **gpg4o** eine Verbindung zu dem Updateserver (o.ä.) aufbauen kann.

7 Pfade zu den Dateien von gpg4o und GnuPG

7.1 Benutzerverzeichnis

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

7.2 Lizenzdatei

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

7.3 Ordner für Logdateien

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

7.4 GnuPG Datenverzeichnis

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