



Administratorhandbuch

GPG4O- Version 8.5

Handbuch für Administratoren

Inhalt

1	EINLEITUNG	3
2	INSTALLATION	4
2.1	Unbeaufsichtigte Installation	4
3	VERTEILUNG VON GPG4O IM UNTERNEHMEN	5
3.1	Einbindung in automatische Softwareverteilungssysteme	5
3.2	Offline Installation	5
3.3	Hinweise für den Betrieb auf einem Terminalserver	5
3.3.1	Installation von gpg4o	5
3.3.2	Datendatei im Roaming Verzeichnis	6
3.4	Verteilung der Lizenzdatei	6
3.5	gpg4o dauerhaft aktivieren	7
4	ZUSÄTZLICHE VERSCHLÜSSELUNGSEMPFÄNGER EINRICHTEN	8
5	GRUPPENRICHTLINIEN	9
5.1	Funktionsbeschränkungen	9
5.1.1	Backup	10
5.1.2	Lizenzierung	10
5.1.3	Schlüsselverwaltung	10
5.1.4	Senderegeln	13
5.2	Vorgegebene Einstellungen	13
5.2.1	Aktualisierungseinstellungen	13
5.2.2	Allgemeine Einstellungen	13
5.2.3	Einstellungen zu Schlüsselserversn	15
5.2.4	Einstellungen zur Ansicht	16
5.2.5	GnuPG Einstellungen	17
5.2.6	Protokollierungseinstellungen	19
5.2.7	Sicherungseinstellungen Datenverzeichnis	20
6	VERTEILEN DER SENDEREGLN	22



7	AUTOMATISIERTES ERSTELLEN VON SCHLÜSSELPAAREN	23
7.1	Vorbereitung	23
7.2	Erstellung der Schlüsselpaare	23
7.3	Sicherung der Schlüsselpaare	24
7.4	Verteilung der Schlüssel	24
8	GPG4O UPDATE ÜBER EINEN PROXY SERVER	25
9	PFADE ZU DEN DATEIEN VON GPG4O UND GNUPG	26
9.1	Benutzerverzeichnis	26
9.2	Lizenzdatei	26
9.3	Ordner für Logdateien	26
9.4	GnuPG Datenverzeichnis	26
9.5	Senderegeln	26
10	FIRMEN -UND KONTAKTINFORMATIONEN	27
10.1	Supportinformationen	27
10.2	Kontaktinformationen:	27



1 Einleitung

Dieses Dokument beschreibt für IT-Administratoren in Unternehmen die Installation und Konfiguration von gpg4o für die Nutzung an mehreren Computern in einem Netzwerkbetrieb. Privatnutzern empfehlen wir das „gpg4o Anwenderhandbuch“ zu lesen, in dem die allgemeine Einrichtung und Nutzung von gpg4o beschrieben wird.

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.



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.

```
gpg4o_setup.exe /quiet
```

Das Installationsprogramm überprüft, ob alle von gpg4o benötigten Komponenten vorhanden sind und installiert diese bei Bedarf automatisch mit. Die fehlenden Komponenten werden aus dem Internet heruntergeladen und installiert.

Für eine offline Installation von gpg4o lesen Sie bitte Kapitel 3.2.

Hinweis: Die von gpg4o benötigte OpenPGP-Implementierung GnuPG wird bei einer unbeaufsichtigten Installation nicht durch gpg4o installiert, sondern muss im Voraus installiert werden.



3 Verteilung von gpg4o im Unternehmen

3.1 Einbindung in automatische Softwareverteilungssysteme

Eine Verteilung von gpg4o in einem Netzwerk ist mit handelsüblichen Tools möglich. Das MSI-Paket können Sie mit dem folgenden Kommandozeilen Befehl extrahieren:

```
gpg4o_setup.exe /extract
```

3.2 Offline Installation

Falls Sie gpg4o ohne Internetverbindung installieren möchten, müssen die Installationsprogramme der oben genannten Pakete im selben Verzeichnis wie die „gpg4o_setup.exe“ vorliegen.

Sie finden die jeweiligen Installationspakete im Download Bereich unserer Seite im Abschnitt „Softwareseitige Systemvoraussetzungen“. <https://www.bayoosoft.com/e-mail-verschluesselung/>

3.3 Hinweise für den Betrieb auf einem Terminalserver

3.3.1 Installation von gpg4o

Bitte beachten sie, dass gpg4o standardmäßig eine zum Betrieb notwendige Datendatei temporär im „Temp“ Verzeichnis des Anwenders anlegt. Dieses Verzeichnis ist auf Terminalservern jedoch nicht persistent, was zu einer Fehlermeldung beim Start von Outlook führen kann. Diese Fehlermeldung lässt sich durch Aktivieren einer Gruppenrichtlinie jedoch verhindern. (siehe Kapitel 3.3.2) (*nur gpg4o v6 oder älter*).

Nachdem gpg4o auf dem Zielcomputer installiert wurde, benötigt jeder Benutzer von gpg4o eine Lizenzdatei. Die Lizenzdatei kann dem Anwender über einen Kopiervorgang in das gpg4o Benutzerverzeichnis (siehe Kapitel 3.4) zur Verfügung gestellt werden. Nach einem Neustart von Outlook erkennt und verwendet gpg4o diese Lizenzdatei. Alternativ können Sie den Pfad zur Lizenzdatei über eine Gruppenrichtlinie ändern. (siehe Kapitel 3.4)

Für den Einsatz von gpg4o auf einem Computer mit mehreren Benutzern kann es sein, dass manche Benutzer gar keine Lizenz erhalten sollen. Wird 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.

Damit der Benutzer hierdurch nicht bei seiner Arbeit gestört wird, haben wir eine spezielle Lizenzdatei („Cloak-Lizenz“) entworfen, welche gpg4o fast vollständig deaktiviert. Einzig der Import einer Lizenz aus einer E-Mail heraus bleibt vorhanden. Diese Cloak-Lizenz kann beim Support kostenlos angefordert werden.



Die Verteilung dieser speziellen Lizenzdatei erfolgt genauso wie bei einer regulären Lizenz und ist in Kapitel 3.4 beschrieben.

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

3.3.2 Datendatei im Roaming Verzeichnis

Nach der erfolgreichen Installation von gpg4o auf einem Terminalserver aktivieren sie bitte die Gruppenrichtlinie „Funktionsbeschränkungen\Allgemeine Einstellungen\Datendatei für Entschlüsselung im Roaming Verzeichnis ablegen“. Diese Richtlinie stellt sicher, dass die von gpg4o benötigte Datendatei im Roaming-Verzeichnis abgelegt wird. *(nur gpg4o v6 oder älter)*.

3.4 Verteilung der Lizenzdatei

Wenn Sie die Lizenz zentral verwalten möchten, ist es für Sie entscheidend, dass Sie jederzeit die Lizenzdatei auf den Computern der Anwender gegen eine aktualisierte Fassung austauschen können (z.B. nach einer Wartungsverlängerung). Dies können Sie über Startup-Skripte erledigen, oder Sie nutzen die Möglichkeit, gpg4o mithilfe der Gruppenrichtlinie „Funktionsbeschränkungen\Lizenzierung\Pfad zur Lizenzdatei vorgeben“ den Pfad zur Lizenzdatei vorzugeben. Dieser kann beispielsweise auf ein Netzlaufwerk zeigen.

Falls Sie den Pfad zur Lizenzdatei nicht manuell vorgeben möchten, müssen Sie diese an folgenden Ort kopieren:

%AppData%\BAYOOSOFT\gpg4o\LicenseInformation.lic



3.5 pgp4o dauerhaft aktivieren

Um pgp4o dauerhaft aktiviert zu halten, sind folgende DWORD Einträge in der Registry anzupassen oder anzulegen. Diese können Sie auch per Gruppenrichtlinien verteilen.

Sorgen Sie dafür, dass der Eintrag „LoadBehavior“ den Wert 3 hat. Sie finden ihn unter:

HKEY_CURRENT_USER\Software\Microsoft\Office\Outlook\Addins\pgp4o

Sorgen sie ebenfalls dafür, dass der Eintrag „pgp4o“ den Wert 1 hat. Diesen finden sie unter:

HKEY_CURRENT_USER\Software\Microsoft\Office\x.0\Outlook\Resiliency\DoNotDisableAddinList

Bitte beachten Sie, dass das „x“ die Versionsnummer ihrer Outlook Version repräsentiert, wobei „14“ für Outlook 2010, „15“ für Outlook 2013 und „16“ für Outlook 2016 als auch für Outlook 2019 steht.



4 Zusätzliche Verschlüsselungsempfänger einrichten

Manchmal ist es sinnvoll, dass alle verschlüsselten Nachrichten neben den in der E-Mail genannten Adressaten und dem Absender auch an einen weiteren Schlüssel verschlüsselt werden, z.B. zur Archivierung der E-Mail. Beachten Sie jedoch, dass das Eintragen eines weiteren Schlüssels auch von jedem anderen Empfänger der Nachricht gesehen wird, und dort unter Umständen falsch interpretiert werden könnte. Z.B. könnte das als Zeichen einer Überwachung gedeutet werden. Sie sollten also mit diesem Umstand möglichst offen umgehen.

Um einen zusätzlichen Schlüssel (hier Archiv-Schlüssel) für die Verschlüsselung aller Daten einzurichten, benötigen Sie Zugriff auf die `gpg.conf` Datei in den Benutzerverzeichnissen Ihrer Anwender. Üblicherweise befindet sich diese im Ordner `%AppData%\gnupg\`, außer Sie haben den Pfad zu den GnuPG Daten z.B. per Gruppenrichtlinie verändert. Im entsprechenden Verzeichnis befindet sich die `gpg.conf`, oder muss ggf. von Ihnen neu erzeugt werden. In dem Fall benötigen Sie nur eine leere Textdatei. Außerdem benötigen Sie die vollständige Schlüssel-ID des Archiv-Schlüssels, der verwendet werden soll. Öffnen Sie die Datei mit einem beliebigen Texteditor und ergänzen Sie folgende Zeile:

`encrypt-to <long key-id>` wobei Sie `<long key-id>` entsprechend ersetzen. Zuletzt speichern Sie die Datei ab.

Testen können Sie das Ergebnis, indem Sie anschließend in `gpg4o` eine Testmail senden (siehe Einstellungen -> Kontoeinstellungen), und in der Leseansicht einen Doppelklick auf die grüne Leiste über der Nachricht machen, während Sie die `Strg`-Taste gedrückt halten. Sie sehen nun einige Debug-Informationen, in denen die Empfänger-Schlüssel zu finden sind. Beachten Sie, dass es sich dabei um die Schlüssel-IDs der Unterschlüssel handelt. Die Schlüssel-IDs Ihres Unterschlüssels finden Sie in den Schlüsseldetails des Archivschlüssels. Alternativ öffnen Sie die verschlüsselte Nachricht auf einem anderen Computer, auf dem sich nur der geheime Schlüssel des Archiv-Schlüssels befindet. Sie sollten die Nachricht dort nun ebenfalls entschlüsseln können.



EASY ENDPOINT E-MAIL ENCRYPTION

5 Gruppenrichtlinien

Administratoren können seit 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 Ihnen die ADMX Dateien zur Verfügung, welche Sie von unserer Webseite herunterladen oder über unseren Support beziehen können. Alle neueren Windows Versionen unterstützen das Template-Format ADMX.

Sie finden die Richtlinien im Gruppenrichtlinienverwaltungs-Editor unter Benutzereinstellungen\BAYOOSOFT - gpg4o. Alle Richtlinien enthalten eine Erklärung, welche aussagt, wie sich das Programm beim Anwender verhält, wenn die Richtlinie aktiviert beziehungsweise 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 demnach nicht mehr ändern kann.

Ein Beispiel für die Anwendung von 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, dass 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.

Nachfolgend sind die Richtlinien mitsamt Erklärung und der Standardeinstellung aufgelistet:

5.1 Funktionsbeschränkungen

- Benutzer dürfen E-Mails nicht entschlüsselt speichern
 - Wenn Sie die Richtlinie aktivieren, können die Benutzer keine E-Mails mehr dauerhaft entschlüsselt speichern. Standardmäßig können die Benutzer E-Mails über die zugehörige Schaltfläche dauerhaft entschlüsselt abspeichern.
- Benutzer dürfen Passphrasen nicht dauerhaft speichern (*gpg4o v6*)
 - Wenn Sie die Richtlinie aktivieren, können die Benutzer Passphrasen nicht mehr dauerhaft speichern. Standardmäßig können die Benutzer Passphrasen in den gpg4o Kontoeinstellungen dauerhaft speichern (*nur gpg4o v6 oder älter*).



5.1.1 Backup

- Benutzer dürfen keine Backups exportieren
 - Wenn Sie die Richtlinie aktivieren, können die Benutzer keine Backups mehr in den Einstellungen exportieren. Standardmäßig können die Benutzer Backups exportieren.
- Benutzer dürfen keine Backups importieren
 - Wenn Sie die Richtlinie aktivieren, können die Benutzer keine Backups mehr in den Einstellungen bzw. dem Konfigurationsassistenten importieren. Standardmäßig können die Benutzer Backups importieren, wobei je nach Zustand der Richtlinie "Benutzer dürfen keine Lizenzen importieren" der Import der Lizenz übersprungen wird.

5.1.2 Lizenzierung

- 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. Standardmäßig wird gpg4o geladen und ist normal benutzbar im Rahmen der Lizenz.
- Benutzer dürfen keine Lizenzen importieren (*gpg4o v6*)
 - 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. Standardmäßig können Benutzer Lizenzdateien importieren. Außerdem wird der Import der Lizenz beim Importieren eines Backups nicht übersprungen (*nur gpg4o v6 oder älter*).
- Pfad zur Lizenzdatei vorgeben
 - Wenn Sie diese Richtlinie aktivieren, wird die Lizenzdatei des Benutzers nicht mehr vom Standardpfad geladen, sondern vom von Ihnen angegebenen Pfad. Sie können auch einen UNC-Pfad benutzen. Sollte der Pfad einmal nicht zur Verfügung stehen, wird die zuletzt erfolgreich geladene Lizenz aus dem lokalen Cache geladen. Standardmäßig wird die Lizenz vom Standardpfad im Roaming Verzeichnis des Benutzers geladen.

5.1.3 Schlüsselverwaltung

- 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. Standardmäßig können die Benutzer auf ihre Schlüsselpaare Rückzugszertifikate anwenden.



- 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. Standardmäßig 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.
- Benutzer dürfen keine Schlüssel erstellen
 - Wenn Sie diese Richtlinie aktivieren, können die Benutzer keine Schlüssel erstellen. Eine administrative Instanz muss zur Verfügung stehen, welche die Schlüssel erstellt, verwaltet und an die Benutzer ausgibt. Standardmäßig können die Benutzer ihre eigenen Schlüssel erstellen.
- Benutzer dürfen keine Rückzugsertifikate erstellen
 - Wenn Sie diese Richtlinie aktivieren, können die Benutzer keine Rückzugsertifikate für ihre Schlüsselpaare erstellen. Diese müssen dann durch eine administrative Instanz erzeugt werden, die eine Kopie des Schlüsselpaares hat. Standardmäßig können die Benutzer Rückzugsertifikate für ihre Schlüsselpaare erstellen.
- Benutzer dürfen keine Schlüsselpaare löschen
 - Wenn Sie diese Richtlinie aktivieren, können die Benutzer keine Schlüsselpaare aus ihrem Schlüsselring löschen. Standardmäßig können die Benutzer Schlüsselpaare aus ihrem Schlüsselring löschen.
- 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. Standardmäßig können die Benutzer öffentliche Schlüssel aus ihrem Schlüsselring löschen.
- Benutzer dürfen keine Schlüssel (de)-aktivieren
 - Wenn Sie diese Richtlinie aktivieren, können die Benutzer keine Schlüssel in ihrem Schlüsselring aktivieren bzw. deaktivieren. Standardmäßig können die Benutzer Schlüssel in ihrem Schlüsselring aktivieren bzw. deaktivieren.
- Benutzer dürfen keine Schlüsselpaare exportieren
 - Wenn Sie diese Richtlinie aktivieren, können die Benutzer keine Schlüsselpaare als Datei exportieren. Standardmäßig können die Benutzer Schlüsselpaare exportieren.
- Benutzer dürfen keine öffentlichen 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. Standardmäßig können die Benutzer öffentliche Schlüssel exportieren und per E-Mail versenden.



- Benutzer dürfen keine Schlüsselpaare importieren
 - Wenn Sie diese Richtlinie aktivieren, können die Benutzer keine Schlüsselpaare aus Dateien, Anhängen oder der Zwischenablage importieren. Standardmäßig können die Benutzer Schlüsselpaare aus den genannten Medien importieren.
- Benutzer dürfen keine öffentlichen 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 Schlüsselserversn. Standardmäßig können die Benutzer öffentliche Schlüssel aus den genannten Medien importieren.
- Benutzer dürfen keine Schlüssel von Schlüsselservers herunterladen
 - Wenn Sie diese Richtlinie aktivieren, können die Benutzer keine öffentlichen Schlüssel von Schlüsselserversn herunterladen. Dies gilt nicht für den Server zum automatischen Herunterladen von Schlüsseln. Standardmäßig können die Benutzer öffentliche Schlüssel von Schlüsselserversn herunterladen.
- Benutzer dürfen keine Schlüssel auf Schlüsselservers hochladen
 - Wenn Sie diese Richtlinie aktivieren, können die Benutzer keine öffentlichen Schlüssel auf Schlüsselservers hochladen. Dies betrifft auch den öffentlichen Teil der eigenen Schlüsselpaare. Standardmäßig können die Benutzer öffentliche Schlüssel auf Schlüsselservers hochladen.
- 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. Standardmäßig können die Benutzer das Besitzervertrauen von Schlüsseln in ihrem Schlüsselring setzen bzw. ändern.
- Benutzer dürfen Schlüssel nicht öffentlich signieren
 - Wenn Sie diese Richtlinie aktivieren, können die Benutzer keine Schlüssel signieren. Die Schlüssel müssen durch eine administrative Instanz signiert werden. Standardmäßig können die Benutzer Schlüssel signieren. Diese Richtlinie bezieht sich nur auf die exportierbare Signatur, nicht auf die lokale Signatur.
- Benutzer dürfen Schlüssel nicht lokal signieren
 - Wenn Sie diese Richtlinie aktivieren, können die Benutzer keine Schlüssel lokal signieren. Standardmäßig können die Benutzer Schlüssel lokal signieren. Diese Richtlinie bezieht sich nur auf die nicht exportierbare **lokale** Signatur.
- Benutzer dürfen Schlüsselpaare nicht verlängern
 - Wenn Sie diese Richtlinie aktivieren, können die Benutzer das Ablaufdatum von Schlüsselpaaren nachträglich nicht mehr verändern. Standardmäßig können die Benutzer das Ablaufdatum von Schlüsselpaaren nachträglich verändern.



5.1.4 Senderegeln

- Benutzer dürfen keine Senderegeln erstellen
 - Wenn Sie die Richtlinie aktivieren, können die Benutzer keine Senderegeln erstellen. Standardmäßig können die Benutzer Senderegeln erstellen.
- Benutzer dürfen keine Senderegeln löschen
 - Wenn Sie die Richtlinie aktivieren, können die Benutzer keine Senderegeln löschen. Standardmäßig können die Benutzer Senderegeln löschen.
- Benutzer dürfen keine Senderegeln verändern
 - Wenn Sie die Richtlinie aktivieren, können die Benutzer bestehende Senderegeln nicht editieren. Standardmäßig können die Benutzer bestehende Senderegeln editieren.

5.2 Vorgegebene Einstellungen

5.2.1 Aktualisierungseinstellungen

- 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. Standardmäßig können die Benutzer selbst die Einstellungen zu Updates beeinflussen.

5.2.2 Allgemeine Einstellungen

- E-Mails immer klonen statt kopieren (*gpg4o v6*)
 - Wenn Sie diese Richtlinie aktivieren, werden E-Mails zum Entschlüsseln immer von gpg4o geklont. Standardmäßig wird die Outlook-eigene Kopieroutine verwendet und die E-Mails nicht geklont, sofern möglich.
- Nutzer dürfen keine unsicheren E-Mails mit fehlendem MDC-Schutz entschlüsseln
 - Wenn Sie diese Richtlinie aktivieren, können Nutzer keine E-Mails mit fehlendem MDC-Schutz öffnen.
Wenn Sie diese Richtlinie deaktivieren, können Nutzer E-Mails mit fehlendem MDC-Schutz öffnen
- E-Mails in öffentlichen Ordner entschlüsseln (*gpg4o v6*)
 - Standardmäßig versucht gpg4o, E-Mails in öffentlichen Ordnern zu entschlüsseln und deren Signatur zu überprüfen. (Zur Entschlüsselung wird der zugehörige private Schlüssel benötigt.) Wenn Sie diese Richtlinie deaktivieren, wird gpg4o in öffentlichen Ordnern keine E-Mails verarbeiten.



- Erkennung von OpenPGP Schlüsseln in Anhängen
 - Standardmäßig sucht gpg4o bei Anzeige einer E-Mail nach OpenPGP Schlüsseln in den Anhängen und bietet dem Anwender einen Import dieser an. Wenn Sie diese Richtlinie deaktivieren, sucht gpg4o nicht nach Schlüsseln und bietet dem Anwender keinen Import an. Beachten Sie, dass zusätzlich der Import von öffentlichen Schlüsseln oder Schlüsselpaaren erlaubt sein muss.
- Erkennung von gpg4o Lizenzdateien in Anhängen (*gpg4o v6*)
 - Standardmäßig sucht gpg4o bei Anzeige einer E-Mail nach Lizenzdateien in den Anhängen und bietet dem Anwender einen Import dieser an. Wenn Sie diese Richtlinie deaktivieren, sucht gpg4o nicht nach Lizenzdateien und bietet dem Anwender keinen Import an. Beachten Sie, dass zusätzlich der Import von Lizenzdateien erlaubt sein muss (*nur gpg4o v6 oder älter*).
- Erweiterte Signaturüberprüfung benutzen
 - Wenn Sie diese Richtlinie aktivieren, werden auch PGP/MIME Signaturen von E-Mails überprüft, die nicht verschlüsselt sind. Dies kann jedoch je nach Mailserver und Konfiguration fehlschlagen. Standardmäßig ist die Überprüfung von Signaturen in PGP/MIME E-Mails, die nur signiert und nicht auch noch verschlüsselt sind, nicht aktiv.
- Vertriebliche Anfragen auf eine eigene E-Mail-Adresse umleiten
 - Wenn Sie diese Richtlinie aktivieren, können Sie eine E-Mail-Adresse angeben, an die Vertriebsanfragen gesendet werden. Die Standard-E-Mail-Adresse ist sales@gpg4o.de.
- Supportanfragen auf eine eigene E-Mail-Adresse umleiten
 - Wenn Sie diese Richtlinie aktivieren, können Sie eine E-Mail-Adresse angeben, an die Supportanfragen gesendet werden. Die Standard-E-Mail-Adresse ist support@gpg4o.de
- Anhang Namen verbergen
 - Standardmäßig 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.
- Hinweis auf bald ablaufende Schlüsselpaare
 - Standardmäßig werden Schlüsselpaare, die für einen Account verwendet werden und in den nächsten 30 Tagen ablaufen, mit einem Hinweis dem Nutzer angezeigt. Durch diesen Hinweis bekommen die Nutzer die Möglichkeit Ihre Schlüssel direkt um ein Jahr zu verlängern. Wenn Sie diese Richtlinie deaktivieren, wird dem Nutzer kein Hinweis auf bald ablaufende Schlüsselpaare angezeigt.



- Domänenbasierte Schlüsselsuche verwenden (*gpg4o v6*)
 - Wenn Sie diese Richtlinie aktivieren, wird beim Verschlüsseln von Nachrichten an Empfänger, für die kein passender Schlüssel gefunden werden kann, ein alternativer Schlüssel in den lokal vorhandenen gesucht. Standardmäßig versucht gpg4o nicht fehlende Schlüssel anhand der Domäne des Empfängers zu ermitteln (*nur gpg4o v6 oder älter*).
- Dateierdung .gpg für verschlüsselte Anhänge verwenden
 - Wenn Sie die Richtlinie aktivieren, wird beim Verschlüsseln von Anhängen immer die Dateierdung .gpg verwendet. Standardmäßig wird beim Verschlüsseln von Anhängen immer die Dateierdung .gpg verwendet.
- Den gpg4o-internen Paketparser verwenden
 - Standardmäßig 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.
- Entschlüsselung in einer eigenen Datendatei vollziehen (*gpg4o v6*)
 - E-Mails werden vor der Entschlüsselung mit gpg4o immer zuerst an einen Ort kopiert/geklont, von dem aus keine Synchronisation mit dem Server stattfindet. Standardmäßig wird dafür die Datendatei gpg4oTemp.pst verwendet. Wenn Sie diese Richtlinie deaktivieren, wird stattdessen ein Order Temp unterhalb des Posteinganges angelegt und dessen Synchronisation 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 (*nur gpg4o v6 oder älter*).
- Erkennung von veralteten MD5 Schlüsselpaaren
 - Standardmäßig wird beim gpg4o Start eine Prüfung auf veraltete MD5 Schlüsselpaare ausgeführt. Werden solche Schlüsselpaare erkannt, werden diese dem Nutzer zur Aktualisierung auf einen modernen Signaturalgorithmus angeboten. Bei der Deaktivierung der Richtlinie wird diese Überprüfung nicht durchgeführt.
- Datendatei für Entschlüsselung im Roaming Verzeichnis ablegen (*gpg4o v6*)
 - Standardmäßig legt gpg4o die zur Entschlüsselung verwendete Datendatei im %Temp% Verzeichnis des Benutzers ab. Im Terminalserver Betrieb kann dies beim Programmstart zu Problemen führen, was durch Aktivierung dieser Richtlinie verhindert werden kann. gpg4o legt die Datendatei in diesem Fall im Roaming Verzeichnis ab (*nur gpg4o v6 oder älter*).

5.2.3 Einstellungen zu Schlüsselserversn

- Automatischen Import auch für Signaturprüfung erlauben
 - Wenn Sie diese Richtlinie aktivieren, können die Benutzer den automatischen Import von Schlüsseln auch für die Signaturprüfung nutzen. Es muss ein Server für den Automatischen Import zur Verfügung stehen. Standardmäßig können die Benutzer für die Signaturprüfung den Automatischen Import selbst festlegen.



- Key server-Liste vorgeben
 - Wenn Sie diese Richtlinie aktivieren, können die Benutzer nur die angegebenen Key Server benutzen. Hierzu müssen Sie die URL des Key Servers 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) und 3 (Beides erlaubt) haben. Formatiert wird der Wert, indem man den numerischen Wert der Berechtigung für den Download anbringt, gefolgt von einem Semikolon und dem Wert für den Upload.

Die Angabe von „hkp://keys.company.com 3;1“ resultiert in einem einzelnen für die Benutzer verfügbaren Key Server, welcher für das manuelle Herunterladen und Hochladen von Schlüsseln sowie für das automatische Importieren fehlender Schlüssel beim Schreiben von E-Mails benutzt werden kann.

Standardmäßig können die Benutzer die Schlüsselserver selbst festlegen.
- Lokal vorhandene Schlüssel aktualisieren
 - Wenn Sie diese Richtlinie aktivieren, werden bei Verfassen einer neuen E-Mail die Schlüssel der Empfänger in den lokalen Schlüsselring des Anwenders heruntergeladen, auch wenn diese dort bereits vorhanden sind. Der Schlüsselring des Anwenders wird somit aktuell gehalten. Voraussetzung für diese Funktionalität ist die Aktivierung des automatischen Imports durch Vorgabe von Schlüsselservern und Konfiguration zum automatischen Download.
 - Voreinstellung: Die Richtlinie ist deaktiviert.

5.2.4 Einstellungen zur Ansicht

- Entschlüsselungsinformation in Inspektoren anzeigen (*gpg4o v6*)
 - Wenn Sie diese Richtlinie aktivieren, wird gpg4o beim Öffnen einer Nachricht in einem eigenen Fenster (Inspektor) den Verschlüsselungsstatus am Anfang der Nachricht einfügen. Standardmäßig fügt gpg4o keinen Verschlüsselungsstatus ein (*nur gpg4o v6 oder älter*).
- Entschlüsselungsinformation beim dauerhaften Entschlüsseln einbinden (*gpg4o v6*)
 - Standardmäßig fügt gpg4o beim dauerhaften Entschlüsseln einer Nachricht den Verschlüsselungsstatus am Anfang der Nachricht ein. Wenn Sie diese Richtlinie deaktivieren, wird gpg4o keinen Verschlüsselungsstatus in die Nachricht einfügen (*nur gpg4o v6 oder älter*).
- Entschlüsselungsinformation in der gpg4o-Leseansicht anzeigen (*gpg4o v6*)
 - Standardmäßig fügt gpg4o beim Lesen einer Nachricht in der gpg4o-Leseansicht den Verschlüsselungsstatus auch am Anfang der Nachricht ein. Wenn Sie diese Richtlinie deaktivieren, wird gpg4o keinen Verschlüsselungsstatus einfügen, sondern nur die Nachricht selbst anzeigen (*nur gpg4o v6 oder älter*).



- Entschlüsselungsinformation in gedruckte E-Mails einbinden (*gpg4o v6*)
 - Standardmäßig fügt gpg4o beim Drucken einer Nachricht über die Drucken Schaltfläche in der gpg4o-Leseansicht den Verschlüsselungsstatus am Anfang der Nachricht ein. Wenn Sie diese Richtlinie deaktivieren, wird gpg4o keinen Verschlüsselungsstatus einfügen (*nur gpg4o v6 oder älter*).
- Entschlüsselungsinformation in Antworten anzeigen (*gpg4o v6*)
 - Standardmäßig fügt gpg4o beim Beantworten bzw. Weiterleiten einer Nachricht die Verschlüsselungsstatus am Anfang der Originalnachricht ein. Wenn Sie diese Richtlinie deaktivieren, wird gpg4o keine Entschlüsselungsinformation in die Originalnachricht einfügen (*nur gpg4o v6 oder älter*).
- Sprache festlegen
 - Wenn Sie diese Richtlinie aktivieren, wird bei den Benutzern beim nächsten Start von Outlook gpg4o in der von Ihnen ausgewählten Sprache gestartet. Standardmäßig können die Benutzer ihre bevorzugte Sprache selbst einstellen.
 - Die Standardsprache ist die Systemsprache, wenn sie bei gpg4o verfügbar ist, ansonsten ist es Englisch
- Sendeoptionen bei inaktiven Konten ausblenden
 - Standardmäßig werden die gpg4o Sendeoptionen auch dann angezeigt, wenn eine neue E-Mail in einem inaktiven Konto erstellt wird.

5.2.5 GnuPG Einstellungen

- GnuPG-Versionsinformationen bei jedem Outlook-Start aktualisieren
 - Standardmäßig wird bei jedem Outlook Start die Liste der von gpg4o unterstützten GnuPG Versionen aus dem Internet aktualisiert. Wenn Sie diese Richtlinie deaktivieren, wird die Liste der von gpg4o unterstützten GnuPG Versionen nicht aktualisiert.
- Nicht auf andere installierbare GnuPG Versionen hinweisen
 - Wenn Sie diese Richtlinie aktivieren, wird gpg4o keinen Hinweis auf andere installierbare GnuPG Versionen anzeigen.
 - Standardmäßig weist gpg4o auf andere installierbare GnuPG Versionen hin.
- Nicht auf unbekannte GnuPG Versionen hinweisen
 - Wenn Sie diese Richtlinie aktivieren, wird gpg4o kein Hinweis auf unbekannte GnuPG Versionen anzeigen.
 - Standardmäßig weist gpg4o auf unbekannte GnuPG Versionen hin.



- Dauer des Zwischenspeicherns einer Passphrase bei Verwendung des GnuPG Agent (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.
 - Standardmäßig werden die Passphrasen 5 Minuten zwischengespeichert.
- Dauer des Zwischenspeicherns einer Passphrase bei Verwendung von GnuPG 1.4.x vorgeben (*gpg4o v6*)
 - 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.
 - Standardmäßig werden Passphrasen bis zum Beenden von Outlook zwischengespeichert (*nur gpg4o v6 oder älter*).
- 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. Standardmäßig können die Benutzer selbst das Datenverzeichnis einstellen.
 - Das Standardverzeichnis ist „%AppData%\gnupg“.
 - Bitte beachten Sie, dass bei manueller Anlage des Registry Keys der Datentyp `REG_EXPAND_SZ` ist, da andernfalls die Ersetzung des Pfades in *gpg4o* nicht funktioniert.
- 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.
 - Standardmäßig wird der Pfad automatisch ermittelt. GnuPG wird über die Registry gesucht, danach unter „%ProgramFiles(x86)%\GNU\GnuPG“ mit den Dateinamen *gpg.exe* bzw. *gpg2.exe*.
 - Bitte beachten Sie, dass bei manueller Anlage des Registry Keys der Datentyp `REG_EXPAND_SZ` ist, da andernfalls die Ersetzung des Pfades in *gpg4o* nicht funktioniert.



- Timeout eines GnuPG Prozesses 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. Standardmäßig 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 langen laufenden GnuPG-Prozessen haben, sollten Sie diese Richtlinie aktivieren und den Prozessen mehr Zeit geben.
 - Es wird die Standardeinstellung von 15 Sekunden (Wert: 15000 ms) verwendet.
- 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.
 - Standardmäßig wird immer allen Schlüsseln vertraut.
- GnuPG-Kopfzeilen unterbinden
 - Wenn Sie diese Richtlinie aktivieren, wird das Einfügen der GnuPG Versionsangabe sowie des Kommentars mit der gpg4o Version unterbunden. Dies kann aus Sicherheitsgründen sinnvoll sein. Standardmäßig werden diese Zeilen immer eingefügt. Dies erleichtert im Fehlerfall die Fehlersuche beim Empfänger.
- 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. Standardmäßig 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.

5.2.6 Protokollierungseinstellungen

- Detaillevel der Logausgaben festlegen
 - Wenn Sie diese Richtlinie aktivieren, können Sie das Logging-Verhalten von gpg4o angeben. Standardmäßig schreibt gpg4o alle Logausgaben, jedoch ohne Zeitmessungen und Stack Traces.
 - Voreinstellung: Die Richtlinie ist auf Log Level 6 (Alle Logausgaben) konfiguriert.



- Maximale Anzahl an Logdateien festlegen (*gpg4o v6*)
 - Wenn Sie diese Richtlinie aktivieren, können Sie die maximale Anzahl an Logdateien von *gpg4o* festlegen.
 - Voreinstellung: Die Richtlinie ist auf eine maximale Anzahl von 30 Logdateien konfiguriert (*nur gpg4o v6 oder älter*).
- Logausgaben bei erweiterter Signaturprüfung (*gpg4o v6*)
 - Standardmäßig wird bei Verwendung der erweiterten Signaturprüfung die Log Umleitung in die externe Bibliothek *gpg4oH* aktiviert. Wenn Sie diese Richtlinie deaktivieren, wird das Logging nicht umgeleitet. Diese Richtlinie sollte nur im Fehlerfall geändert werden (*nur gpg4o v6 oder älter*).

5.2.7 Sicherungseinstellungen Datenverzeichnis

- Automatische GnuPG Datenverzeichnis Sicherung (de)aktivieren
 - Wenn Sie diese Richtlinie aktivieren, wird täglich eine Sicherung des GnuPG Datenverzeichnis als Zip-Archiv erstellt.
 - Wenn aktiviert kann der Anwender das Zielverzeichnis sowie die Anzahl der zu behaltenden Sicherungen nicht mehr ändern.
 - Diese Funktionalität steht nur Nutzern mit Professional Lizenz zur Verfügung.
 - Standardmäßig wird keine Sicherung als Zip-Archiv erstellt.
- Anzahl aufzubewahrender Sicherungen
 - Gibt die Anzahl der maximal aufgehobenen GnuPG Datenverzeichnis Sicherungen an.
 - Voreinstellung: Es werden 60 Sicherungen behalten.
- Zielverzeichnis für automatische Sicherungen
 - Das Verzeichnis für alle GnuPG Datenverzeichnis Sicherungen angeben.
 - Der Pfad darf nicht mit einem Backslash abgeschlossen werden.
 - Voreinstellung: %AppData%\BAYOOSOFT\gpg4o\Backup
 - Bitte beachten Sie, dass bei manueller Anlage des Registry Keys der Datentyp `REG_EXPAND_SZ` ist, da andernfalls die Ersetzung des Pfades in *gpg4o* nicht funktioniert.



- Häufigkeit der Sicherung
 - Legt fest wie häufig das GnuPG Datenverzeichnis gesichert wird.
 - Voreinstellung: Es wird alle 1440 Minuten (24 Stunden) eine Sicherung erstellt.



6 Verteilen der Senderegeln

Erstellen Sie dazu bitte die gewünschten Senderegeln an einem Computer mit gpg4o. Kopieren Sie danach die Datei „Rulelist.xml“, die im Benutzerverzeichnis liegt. (siehe Kapitel 9)

Die Datei „Rulelist.xml“ können Sie an die Anwender verteilen, die Ihre gewünschten Senderegeln benutzen sollen. Um den Anwender keine Möglichkeit zu geben Ihre Senderegeln zu bearbeiten, können Sie folgende Gruppenrichtlinien (Siehe Kapitel 5.1.4) aktivieren.



7 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.

7.1 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 9.

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 der Endung **.csv** abgespeichert werden.

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.

Achtung: Die CSV-Datei sollte an einem sicheren Ort gespeichert werden!

7.2 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, die Länge des Haupt- und Unterschlüssels und das Ablaufdatum ausgewählt werden.

Wenn Sie in diesem Dialog im Feld „Name“ den Text „[csv]“ eintragen und auf die Schaltfläche „OK“ klicken, öffnet sich ein Datei-Dialog. In diesem Dialog kann die von Ihnen zuvor gespeicherte CSV-Datei ausgewählt werden. Durch das Öffnen der Datei werden die Schlüsselpaare 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.

7.3 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 9. Die dazugehörigen Passphrasen sollen bitte mit abgesichert werden

7.4 Verteilung der Schlüssel

Die erzeugten öffentlichen Schlüssel können über die gpg4o Schlüsselverwaltung einzeln in das Dateisystem exportiert oder auf einen Schlüsselservers 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 9) 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!



8 gpg4o Update über einen Proxy Server

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.



9 Pfade zu den Dateien von gpg4o und GnuPG

9.1 Benutzerverzeichnis

%AppData%\BAYOOSOFT\gpg4o\

9.2 Lizenzdatei

%AppData%\BAYOOSOFT\gpg4o\LicenseInformation.lic

9.3 Ordner für Logdateien

%AppData%\BAYOOSOFT\gpg4o\LogFiles\

9.4 GnuPG Datenverzeichnis

%AppData%\gnupg\

9.5 Senderegeln

%AppData%\BAYOOSOFT\gpg4o\Rulelist.xml

10 Firmen -und Kontaktinformationen

10.1 Supportinformationen

Bitte nutzen Sie die nachfolgende E-Mail-Adresse um den Support bezogen auf gpg4o von **BAYOOSOFT GmbH**: support@gpg4o.de

10.2 Kontaktinformationen:

BAYOOSOFT GmbH

Machtlfinger Straße 11

81379 München

Deutschland

Internet: <https://www.bayoosoft.com/e-mail-verschluesselung/>



EASY ENDPOINT E-MAIL ENCRYPTION