Hochschule Bochum, FB M
Labor für Betriebssysteme und Netzwerke
(Labor BsNw)

GNU PGP GPG4Win Version 2.3.1 Installation, Konfiguration und Einführung in die Verschlüsselung

Sichere Kommunikation via Email und sichere Dateiablage

Dipl.-Ing. Oliver Mathews und Prof. Dr. Markus Eikelberg

29.06.2015

Inhaltsverzeichnis

Installation und Ersteinrichtung von GPG4Win Version 2.3.1

Laden Sie von der URL
ftp://pc132w.bsnw.fb4.fh-bochum.de/eikelberg/support/ GNUPGP/GPG4WinV231
die Datei gpg4win-2.3.1.exe in den Ordner D:\GPG4Win\download herunter.

Führen Sie die Datei gpg4win-2.3.1.exe mit einem Doppelklick aus. Als Installationssprache wählen Sie <Deutsch> aus und folgen dem Installationsassistenten bis zum Fenster „Komponenten auswählen“. Im Fenster „Komponenten auswählen“ sollten die folgenden Komponenten für die Installation ausgewählt werden:

1) < GnuPG > der Hauptbestandteil (Kernel) des GPG Programms
2) < Kleopatra > grafische Oberfläche zum GPG Kernel
3) < GpgEX > Kontextmenüerweiterung für den Dateiexplorer
4) < Gpg4win-Kompendium> GPG Dokumentation

Bestätigen Sie Ihre Auswahl mit dem Button < Weiter> > und legen Sie als Installationspfad den Ordner D:\GPG4Win\install fest. Im nachfolgenden Fenster „Installationsoptionen“ wählen Sie Verknüpfungen für das <Startmenü> und die <Arbeitsfläche> aus. Bestätigen Sie Ihre Auswahl mit dem Button < Weiter> . Im Fenster „Startmenü-Ordner bestimmen“ nehmen Sie keine Änderungen vor und starten Sie die Installation mit dem Button <Installieren>. Die PGP Software wird jetzt installiert. Schließen Sie die Installation mit dem Button <Weiter> und dann <Fertig stellen> ab. Lassen Sie sich die ReadMe Datei nicht anzeigen.

Erstellen eines neuen persönlichen OpenPGP Zertifikats

Führen Sie das Programm Kleopatra aus. Kleopatra finden Sie im Startmenü von Windows wie folgt:

- „Start / Alle Apps / Gpg4Win / Kleopatra“ (Windows 10) bzw.
- "Start / Alle Programme / Gpg4Win / Kleopatra" (Windows 7)
-

In der Menüleiste im Programm Kleopatra wählen Sie „Datei / Neues Zertifikat“ und erstellen ein neues persönliches OpenPGP-Schlüsselpaar. Tragen Sie Ihren Vornamen und Nachnamen in das Feld <Name> ein, die E-Mail Adresse im Feld <E-Mail> und vergeben ggf. einen entsprechenden Kommentar. Öffnen Sie die <Erweiterten Einstellungen…> und aktivieren Sie zusätzlich im Bereich „Verwendung des Zertifikats“ die Option „Authentifizieren“. Bestätigen Sie Ihre Einstellungen mit dem Button <OK> und folgen Sie den Anweisungen des Assistenten zur Erstellung des Zertifikats mit dem Button <Weiter>. Im nächsten Schritt lassen Sie sich „Alle Details anzeigen“ und erstellen mit dem Button <Schlüssel erzeugen> Ihren persönlichen OpenPGP Schlüssel. Vergeben Sie im Fenster „pinentry“ eine Passphrase mit mindestens 8 Zeichen die aus Groß- und Kleinbuchstaben, Zahlen und Zeichen besteht ein. Eine mögliche Passphrase könnte wie folgt aussehen: Test01@Lab423 (Tipp: Versuchen Sie das die Qualität Ihres Passwortes so hoch wie möglich ist). Bestätigen Sie Ihre Eingabe mit dem Button <OK>. Wiederholen Sie die Eingabe der Passphrase und bestätigen Sie die Eingabe mit dem Button <OK>.
Nachdem Ihr Schlüsselpaar erfolgreich erzeugt wurde, erstellen Sie eine Sicherheitskopie des Schlüsselpaares. Um eine Sie eine Sicherheitskopie des Schlüsselpaares klicken Sie auf den Button < Sicherheitskopie Ihres Schlüsselpaares erstellen…> und speichern Ihren Schlüssel an einer geeigneten Stelle auf Ihrem Computer. Hier empfiehlt sich eine Kopie auf einen externen Laufwerk, sowie eine zusätzliche Kopie auf einem optischen Datenträger zu speichern und diesen an einem sicheren Ort (z.B. Safe, Bankschließfach) aufzubewahren. Die Meldung dass Ihr geheimes Zertifikat

gesichert wurde können Sie mit den Button <OK> bestätigen. Schließen Sie den Assistenten zur Erstellung eines Zertifikates mit dem Button <Fertigstellen>.
Hinweis: Die soeben erstellte Sicherung des Schlüsselpaares enthält Ihren öffentlichen und ihren privaten Schlüssel. Diese Datei darf keiner anderen Person zugänglich gemacht werden. Andere Nutzer erhalten nur den öffentlichen Schlüssel!

Importieren eines vorhandenen privaten PGP Schlüssels

Klicken Sie in der Haupt-Werkzeugleiste auf <Zertifikate importieren> und wechseln Sie in das entsprechenden Laufwerk bzw. Ordner in dem sich Ihr persönlicher PGP Schlüssel befindet. Wählen Sie diesen aus und klicken Sie auf den Button <Öffnen>. Bestätigen Sie den erfolgreichen Import des PGP Schlüssels mit einem Klick auf den Button <OK>. Im unteren Bereich des Fensters wechseln Sie in die Registerkarte „Meine Zertifikate“ und wählen dort Ihren persönlichen PGP Schlüssel aus. Öffnen Sie das Kontextmenü (rechte Maustaste auf Ihren PGP Schlüssel) zu Ihrem PGP Schlüssel und wählen „Inhaber-Vertrauenswürdigkeit ändern“ aus. Wählen Sie die Option „Dies ist ein eigenes Zertifikat“ aus und bestätigen Ihre Auswahl mit dem Button <OK>. Das Informationsfenster zur Änderung der Vertrauenswürdigkeit können Sie mit dem Button <OK> bestätigen.

Importieren eines öffentlichen Schlüssels

Klicken Sie in der Haupt-Werkzeugleiste auf <Zertifikate importieren> und wechseln Sie in das entsprechenden Laufwerk bzw. Ordner in dem sich die zu importierenden öffentlichen PGP Schlüssel befinden. Wählen Sie die zu importierenden öffentlichen Schlüssel aus und klicken Sie auf den Button <Öffnen>. Bestätigen Sie den erfolgreichen Import der PGP Schlüssel mit einem Klick auf den Button <OK>.
Um die Vertrauenswürdigkeit des importierten Zertifikates zu erhöhen, gehen Sie nun wie folgt vor: Verschaffen Sie sich den "Fingerprint" des soeben importierten Zertifikates. Die Fingerabdrücke der Zertifikate von Hr. Eikelberg, Hr. Mathews und Hr. Brückmann sind z. Bsp. auf der Homepage des Web-Servers pc132w.bsnw.fb4.fh-bochum.de veröffentlicht. Gehen Sie anschließend wie folgt weiter vor:
Wechseln Sie im unteren Bereich des Fensters von Kleopatra in die Registerkarte „Andere Zertifikate“. Öffnen Sie das Kontextmenü (rechte Maustaste auf einen PGP Schlüssel) und wählen Sie „Zertifikat Beglaubigen“ aus. Im ersten Schritt setzen Sie einen Haken an die Benutzerkennung und einen weiteren Haken an „Ich habe den Fingerabdruck überprüft“ und bestätigen Ihr Eingaben mit dem Button <Weiter>. Im zweiten Schritt wählen Sie die Option „Nur für mich selbst beglaubigen“ aus bestätigen Ihr Eingaben mit dem Button <Beglaubigen>. Beenden den Assistenten mit dem Button <Fertigstellen>. Die Beglaubigten PGP Schlüssel werden in die Registerkarte „Vertrauenswürdige Zertifikate“ verschoben.
Öffnen Sie nun in der Registerkarte "Vertrauenswürdige Zertifikate" erneut das Kontextmenü zu dem soeben importierten PGP Schlüssel und wählen Sie "Zertifikatdetails". In der Registerkarte "Übersicht" wird der Fingerabdruck des Zertifikates angezeigt. Überprüfen Sie, ob der angezeigte Fingerabdruck des Zertifikats mit dem auf anderem Wege bekannt gemachten Fingerabdruck übereinstimmt. Wenn dies nicht zutrifft, ist das Zertifikat von der Qualität "Ich vertraue ihnen NICHT". Stimmen die Fingerabdrücke überein, ist das Zertifikat von der Qualität "Es wird sehr sorgfältig geprüft". Tragen sie diese Qualität nun wie folgt in GNU PGP ein:

Öffnen Sie in der Registerkarte "Vertrauenswürdige Zertifikate" erneut das Kontextmenü zu dem importierten PGP Schlüssel und wählen „Inhaber-Vertrauenswürdigkeit ändern“ aus. Wählen Sie je nach Situation die Option "Ich vertraue ihnen NICHT" oder die Option „Es wird sorgfältig geprüft“ aus und bestätigen Ihre Auswahl mit dem Button <OK>. Das Informationsfenster zur Änderung der Vertrauenswürdigkeit können Sie mit dem Button <OK> bestätigen.

Sichern bzw. Exportieren des privaten Schlüssels

Zum Exportieren eines privaten Schlüssels wechseln Sie im unteren Fensterteil in die Registerkarte „Meine Zertifikate“, markieren Ihren PGP Schlüssel und wählen im Menü „Datei / Geheime Schlüssel exportieren…“. Aktivieren Sie die Option "ASCII-Mantel". Wählen Sie anschließend einen Speicherort aus, an dem Sie den privaten Schlüssel speichern möchten (wird dieser Schritt vergessen, so wird die Datei im Verzeichnis D:\GPG4Win\install gespeichert!). Vergeben Sie einen eindeutigen Dateinamen (z.B. Nachmame_Vorname_PRIVAT.asc) und drücken Sie auf den Button <Speichern>. Das Informationsfenster „Exportieren des geheimen Schlüssels“ können Sie mit dem Button <OK> bestätigen.

Hinweis: Beachten Sie obige Hinweise zur Speicherung des exportierten Schlüssels. Die Sicherung des Schlüsselpaares enthält Ihren öffentlichen und ihren privaten Schlüssel!

Exportieren des öffentlichen Schlüssels

Zum Exportieren des öffentlichen Teils Ihres Schlüssels wechseln Sie im unteren Fensterteil in die Registerkarte „Meine Zertifikate“, und klicken Sie in der Haupt-Werkzeugleiste auf <Zertifikate exportieren>. Wählen Sie einen Speicherort aus, an dem Sie den öffentlichen Teil des Schlüssels speichern möchten. Vergeben Sie einen eindeutigen Dateinamen (z.B. Nachmame_Vorname.asc) und drücken Sie auf den Button <Speichern>.

Hinweis:

Die Schlüssel werden im Windows im Verzeichnis

- C:\Users\willi\AppData\Roaming\gnupgp bzw.
- C:\Benutzer\willi\AppData\Roaming\gnupgp

gespeichert, wenn Sie mit dem Benutzerkonto willi arbeiten. Wenn Gnu PGP fehlerhaft arbeitet, kann der Inhalt dieses Verzeichnisses komplett gelöscht werden. In diesem Fall müssen aber alle Schlüssel zuvor exportiert und anschließend wieder neu in GNU PGP importiert werden.

Allgemeine Einstellungen

Führen Sie das Programm Kleopatra aus. In der Menüleiste im Programm Kleopatra wählen Sie „Einstellungen / Kleopatra einrichten…“. Konfigurieren Sie Kleopatra wie folgt:

- Unter „Kryptografie-Aktionen“ in der Registerkarte „Datei-Aktionen“ aktivieren Sie die Option „OpenPGP-verschlüsselte Dateien mit der Dateierweiterung „pgp“ anstatt „gpg“ erzeugen“.
- Unter „GnuPG-System“ in der Registerkarte „GPG Agent“ tragen Sie im Bereich „Optionen zur Einstellung der Sicherheit“ im Punkt „Lasse PINs im Cache nach N Sekunden verfallen“ eine 0 ein. Somit wird Ihre persönliche Passphrase nicht im Cache behalten und Sie müssen diese bei jeder Ent- bzw. -Verschlüsselung eingeben. Im Punkt „Lasse SSH Schlüssel im Cache nach N Sekunden verfallen“ tragen Sie ebenfalls eine 0 ein.

Verschlüsseln und Entschlüsseln einer Datei

Verschlüsseln von Dateien über den Windows Explorer

Dateien können, nachdem Sie markiert im Windows Explorer markiert sind, über das Kontextmenü „Mehr Gpgex Optionen/ Signieren und Verschlüsseln“ verschlüsselt werden. Wählen Sie im ersten Fenster die Option „Signieren und verschlüsseln (nur OpenPGP)“ aus. *Wenn Sie die Originaldatei nicht behalten wollen, können Sie auch einen Haken an „Unverschlüsseltes Original anschließend löschen“ setzten*. Treffen Sie sonst **keine** weiteren Einstellungen. Klicken Sie auf den Button <Weiter>. Im nächsten Fenster wählen Sie die PGP Schlüssel der Personen aus, die diese Datei entschlüsseln dürfen. Vergessen Sie nicht Ihren Eigenen PGP Schlüssel mit auszuwählen. Fügen Sie über den Button <Hinzufügen> die markierten Empfängerschlüssel dem unteren Fensterbereich hinzu und klicken Sie auf den Button <Weiter>. Im Fenster „Dateien signieren/verschlüsseln“ wählen Sie im Bereich „OpenPGP-Signaturzertifikat“ Ihr persönliches PGP Zertifikat aus. Wenn Sie dieses Zertifikat dauerhaft benutzen wollen, lassen Sie den Haken „Diese Einstellung als Voreinstellung verwenden“ aktiviert. Klicken Sie auf den Button <Signieren & Verschlüsseln>. Geben Sie jetzt das Passwort für Ihren PGP Schlüsseln ein und klicken auf den Button <OK>. Schließen Sie das Ergebnis Fenster über den Button <Fertigstellen>.

Hinweis: Wenn Sie eine Datei nur für den eigenen Zweck verschlüsseln wollen, z.B. eine Passwortdatei, sollte nur Ihr persönlicher Benutzerschlüssel zum Verschlüsseln benutzt werden. Kein andere öffentlicher Benutzerschlüssel sollte hinzugefügt werden.

Entschlüsseln von Dateien über den Windows Explorer

Dateien können, in dem Sie markiert werden, über das Kontextmenü „Mehr Gpgex Optionen / Entschlüsseln und prüfen“ entschlüsselt werden. Im Fenster „Dateien &entschlüsseln/überprüfen“ nehmen Sie keine Einstellungen vor und klicken auf den Button <Entschlüsseln/überprüfen>. Geben Sie Ihre Passphrase zu Ihren PGP Schlüsse ein bestätigen mit dem Button <OK>. Im Fenster Ergebnisse könne Sie sich Details über die Signatur des Erstellers der Datei ansehen. Schließen Sie das Ergebnis Fenster mit dem Button <OK>. Die entschlüsselte Datei befindet sich im selben Verzeichnis wie die verschlüsselte Datei.

Verschlüsseln von Dateien über Kleopatra

Das Verschlüsseln von Dateien kann alternativ auch direkt über die Benutzeroberfläche von Kleopatra erfolgen. Öffnen Sie Kleopatra und wählen in der Menüleiste „Datei/ Dateien signieren /verschlüsseln“ aus. Es öffnet Sich ein Windows Explorer, indem Sie Ihre zu entschlüsselnde Datei Auswählen. Im ersten Fenster wählen Sie die Option „Signieren und verschlüsseln (nur OpenPGP)“ aus. *Wenn Sie die Originaldatei nicht behalten wollen, können Sie auch einen Haken an „Unverschlüsseltes Original anschließend löschen“ setzten*. Treffen Sie sonst **keine** weiteren Einstellungen. Klicken Sie auf den Button <Weiter>. Im nächsten Fenster markieren Sie die PGP Schlüssel, der Personen die diese Datei entschlüsseln dürfen. Vergessen Sie nicht Ihren Eigenen PGP Schlüssel mit zu markieren. Fügen Sie über den Button <Hinzufügen> die markierten Empfängerschlüssel dem unteren Fensterbereich hinzu und klicken Sie auf den Button <Weiter>. Im Fenster „Dateien signieren/verschlüsseln“ wählen Sie im Bereich „OpenPGP-Signaturzertifikat“ Ihr persönliches PGP Zertifikat aus. Wenn Sie dieses Zertifikat dauerhaft benutzen wollen, lassen Sie den Haken „Diese Einstellung als Voreinstellung verwenden“ aktiviert. Klicken Sie auf den Button <Signieren & Verschlüsseln>. Geben Sie jetzt das Passwort für Ihren PGP Schlüsseln ein und klicken auf den Button <OK>. Schließen Sie das Ergebnis Fenster über den Button <Fertigstellen>.

Hinweis: Wenn Sie eine Datei nur für den eigenen Zweck verschlüsseln wollen, z.B. eine Passwortdatei, sollte nur Ihr persönlicher Benutzerschlüssel zum Verschlüsseln benutzt werden. Kein andere öffentlicher Benutzerschlüssel sollte hinzugefügt werden.

Entschlüsseln von Dateien über Kleopatra

Ein anderer Weg zum Entschlüsseln von Dateien kann direkt über die Benutzeroberfläche von Kleopatra erfolgen. Öffnen Sie Kleopatra und wählen in der Menüleiste „Datei/ Dateien entschlüsseln/überprüfen“ aus. Es öffnet Sich ein Windows Explorer, indem Sie Ihre zu entschlüsselnde Datei Auswählen. Im Fenster „Dateien &entschlüsseln/überprüfen“ nehmen Sie keine Einstellungen vor und klicken auf den Button <Entschlüsseln/überprüfen>. Geben Sie Ihre Passphrase zu Ihren PGP Schlüsse ein bestätigen mit dem Button <OK>. Im Fenster Ergebnisse könne Sie sich Details über die Signatur des Erstellers de Datei ansehen. Schließen Sie das Ergebnis Fenster mit dem Button <OK>. Die entschlüsselte Datei befindet sich im selben Verzeichnis wie die verschlüsselte Datei.