Sichere Kommunikation mit Hartgeld.com

von Hartgeld Leser

Mai 2010

Zusammenfassung

Dieser Artikel ist eine kleine Einführung in die sichere Kommunikation mit Hartgeld.com. Hierbei geht es primär um die Kommunikation per Email mit Hilfe von frei verfügbarer Verschlüsselungssoftware.

1 Einleitung

Email stellt heute ein wichtiges Mittel zur Kommunikation dar. Die Vorteile der Email liegen auf der Hand, sie ist quasi sofort und ohne nennenswerte Kosten zugestellt. Dafür gibt es auch einige Schwachstellen. Eine Email ist eher mit einer Postkarte, als mit einem Brief zu vergleichen. Jede der an der Zustellung beteiligten Stellen (und das sind eine Menge) kann potentiell die Nachricht mitlesen, da die Nachricht in Klartext versendet wird. Einen schützenden Briefumschlag gibt es nicht. Selbstverständlich kann man nicht die vielen Millionen Emails mitlesen, die täglich versandt werden, jedoch lässt sich eine Email auch automatisiert auf bestimmte Schlüsselwörter hin untersuchen und so aus den Millionen von Emails ausfiltern. Mit Hilfe von Verschlüsselung können Sie einer Email aber diesen „Briefumschlag“ geben, sogar mit einem weit besseren Schutz, als ein echter Briefumschlag einem Brief bieten könnte.

Die Gründe, warum Sie Ihre Nachrichten schützen wollen oder sollten, können vielfältig sein. Was immer es ist, es ist Ihr gutes Recht, Ihre Privatsphäre zu schützen. Machen Sie also von Verschlüsselung Gebrauch, wann immer Sie Ihre Nachrichten für vertraulich halten. Sie sollten aber bedenken, dass dies für Sie und den Empfänger mit einem zustätzlichen Aufwand verbunden ist. Verzichten Sie also bei trivialen Nachrichten darauf, und wenden Sie es nur dort, wo nötig an.

2 Verschlüsselungsverfahren

Es gibt verschiedene Arten der Verschlüsselung. Man kann grob unterscheiden zwischen symmetrischen und asymmetrischen Verfahren. Beim symmetrischen Verfahren tauschen Sender und Empfänger einen gemeinsamen, geheimen Schlüssel, z.B. ein nur beiden bekanntes Kennwort aus. Die Nachrcht wird mit diesem Schlüssel verund auch wieder entschlüsselt. Die Schwachstelle bei diesem Varfahren ist der Schlüsselaustausch. Dieser muss über einen sicheren Kanal stattfinden, z.B. bei einem persönlichen Treffen unter vier Augen. Gelingt es einem Angreifer den Schlüsselaustausch zu belauschen, ist die Nachricht nicht mehr sicher.

Beim asymmetrischen Verfahren entfällt der unsichere Austausch eines geheimen Schlüssels. Anstelle des gemeinsamen geheimen Schlüssels treten nun zwei Schlüssel für jede Partei: je ein öffentlicher und je ein privater Schlüssel. Der Sender und der Empfänger tauschen die *öffentlichen* Schlüssel aus. Der Sender verschlüsselt die Nachricht mit dem *öffentlichen* Schlüssel des Empfängers. Danach lässt sich die Nachricht aber nur noch mit dem geheimen, *privaten* Schlüssel des Empfängers wieder entschlüsseln. Da eine Entschlüsselung mit dem öffentlichen Schlüssel unmöglich ist, spielt es keine Rolle, ob der öffentliche Schlüssel einem Mithörer bekannt ist, oder nicht.

Ein sehr bekanntes asymmetrisches Verschlüsselungsverfahren ist PGP. PGP steht für Pretty Good Privacy, zu deutsch „ziemlich gute Privatsphäre“. Wer mehr darüber wissen will, findet im Internet dazu zahlreiche Informationen. PGP wird sowohl kommerziell angeboten (http://www.pgp.com), als auch in diversen kostenlosen Open-Source-Varianten. Die Open-Source-Varianten nutzen „OpenPGP“ gemäß RFC4880. Dies wird von der kommerziellen Va-

riante ebenso unterstützt. Ein weitverbreitetes, kostenloses Open-Source-Programm ist „GnuPG“. GnuPG selbst ist ein kommandozeilenbasiertes Programm, also eher benutzerunfreundlich. Daher empfehlen wir - besonders für Nutzer von Microsoft Windows Betriebssystemen - den Einsatz von GnuPT oder Gpg4Win, die zwar auf GnuPG basieren, aber zusätzliche grafische Benutzerschnittstellen zur Anwendung und Verwaltung von GnuPG zur Verfügung stellen.

Für GnuPT stellen wir hier eine Anleitung bereit, für Gpg4Win besuchen Sie bitte die Webseite http://www.gpg4win.org und informieren sich dort.

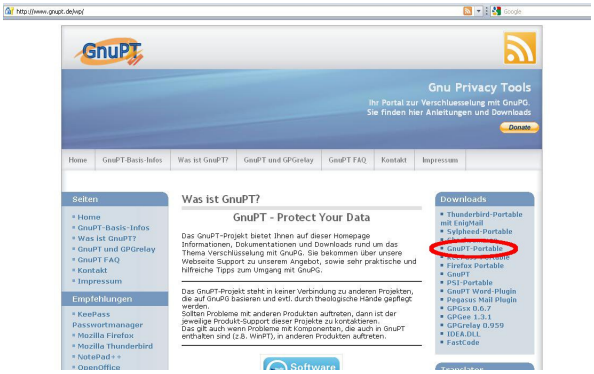

Abbildung 1: Die GnuPT Webseite

3 GnuPT

GnuPT ist eigentlich nichts weiter als ein Installationsprogramm für Windows, das Ihnen die von Ihnen gewünschten Programme installiert und aktuell hält. Es basiert, wie gesagt, auf GnuPG, das das eigentliche Verschlüsselungsprogramm ist. Zusätzlich nutzt es ein Programm namens WinPT, das der Schlüsselverwaltung dient. WinPT steht für „Windows Privacy Tray“ und ist eine Windowsanwendung, die im Hintergrund läuft und über das „System Tray“ in den Vordergrund gebracht werden kann. Mit WinPT kann man nicht nur die Schlüssel verwalten, sondern damit auch bequem Dateien oder den Inhalt der Zwischenablage ver- und entschlüsseln.

GnuPT gibt es auch in einer portablen Anwendnung (GnuPT-Portable), die auf einem USB-Stick oder ähnlichem installiert werden kann, und so an mehreren Rechnern ohne weitere Installation eingesetzt werden kann.

Abbildung 2: GnuPT-Portable Download

3.1 GunPT-Portable installieren

GnuPT und GnuPT-Portable finden Sie auf der Webseite http://www.gnupt.de (siehe Bild 1).

- Klicken Sie unter „Downloads“ auf „GnuPT-Portable“.
- Klicken Sie auf der neu geladenen Seite den Link „GnuPT-Portable-DOWNLOAD“ an.
- Es erscheint ein Dialog, in dem Sie bitte „Speichern“ oder „Speichern unter...“ wählen, je

Abbildung 3: GnuPT-Portable Willkommensmeldung

Abbildung 4: Installationsverzeichnis für GnuPT-Portable wählen

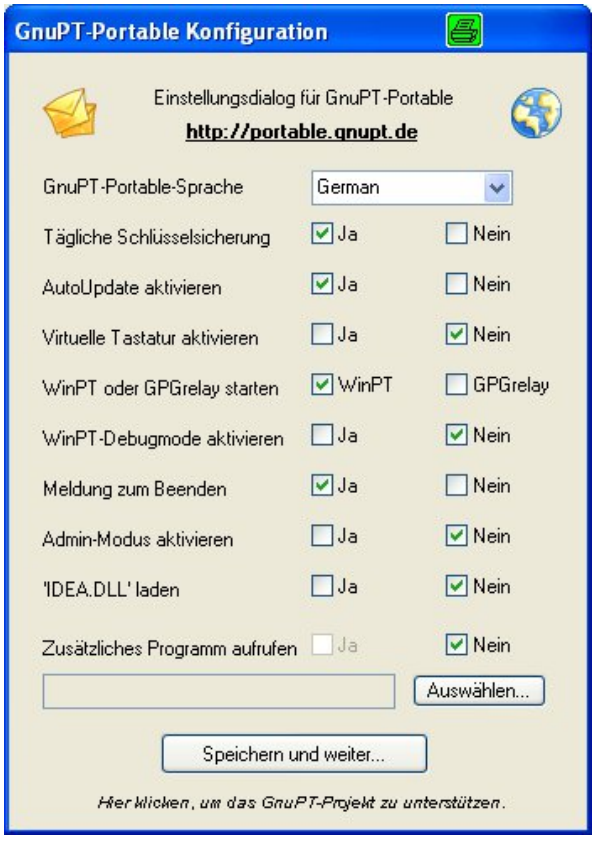

Abbildung 5: Konfiguration für GnuPT-Portable wählen

nach verwendetem Browser. Speichern Sie die Datei „gnupt-portable.zip“ auf Ihrem Rechner ab.

- Extrahieren Sie die ZIP-Datei „gnupt-portable.zip“. Es wird nur eine Datei „GnuPT-Portable-Edition.exe“ extrahiert.
- Führen Sie „GnuPT-Portable-Edition.exe“ aus (Doppelklick). Es erscheint eine Willkommensmeldung (siehe Bild 3), die Sie nach dem Lesen bitte mit „OK“ bestätigen.
- Danach sehen Sie den Extrahierassistenten mit dem Fenstertitel „GnuPT - Protect Your Data“. Tragen Sie dort den Zielort für die Installation von GnuPT-Portable ein (das darf auch ein USB-Stick oder sonstiger mobiler Speicher sein). Mit einem Klick auf „...“ können Sie durch Ihr Dateisystem navigieren und einen geeigneten Speicherort wählen. Klicken Sie dann auf „Entpacken“ (siehe Bild 4).
- GnuPT startet anschließend automatisch. Sie sehen zunächst den Konfigurationsdialog (siehe Bild 5). Für dieses Beispiel wählen wir die Standardeinstellungen und klicken einfach nur „Speichern und weiter“. Warten Sie ein ein paar Sekunden.
- GnuPT wird höchstwahrscheinlich weitere Komponenten nachladen müssen. Dann erscheint eine entsprechende Meldung (siehe Bild 6). Bestätigen Sie die Meldung mit „Ja“.
- Wenn Sie an dieser Stelle eine Fehlermeldung sehen, dann konnte GnuPT keine Internetverbindung herstellen. Beheben Sie das Verbindungsproblem und starten Sie GnuPT-Portable neu (*Installationsort*\GnuPT-Portable.exe). Eine mögliche Ursache könnte ein zwischengeschalteter Proxy sein. Falls Sie einen Proxy nutzen, öffnen Sie die Konfigurationsdatei (*Installationsort*\GnuPT-Portable.ini), suchen Sie den mit [Proxy] beginnenden Abschnitt, und tragen Sie dort Ihren Proxyserver ein. Meist genügt es Proxy=0 in Proxy=1 zu ändern, dann holt sich GnuPT die Proxy-Einstellungen aus den Einstellungen des Internet Explorer. Hilfe dazu finden Sie auch in der Hilfedatei (*Installationsort*\GnuPT-Portable.de.chm).

- Wenn alles fehlerfrei läuft, sehen Sie im System Tray jeweils neue Info-Bubbles („Lade xxx.yyy herunter“). Warten Sie, bis ein neuer Dialog erscheint.
- Fahren Sie mit Abschnitt 3.2 fort.

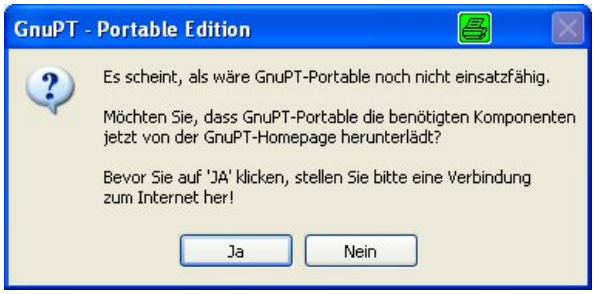

Abbildung 6: Komonenten nachladen

Abbildung 7: GnuPT - Erster Start

3.2 GnuPT - Erste Schritte

- Typischerweise haben Sie noch keine Schlüsselringe auf Ihrem System. Falls doch, wird Ihnen ein Import angeboten.
- Der Normalfall ist jedoch, dass Sie direkt mit dem Dialog „GnuPT - Erster Start“ beginnen werden, wie in Bild 7 dargestellt. Wählen Sie die für Sie richtige Option. Für Neulinge wäre das die voreingestellte Option „GnuPG Schlüsselpaar erzeugen“.

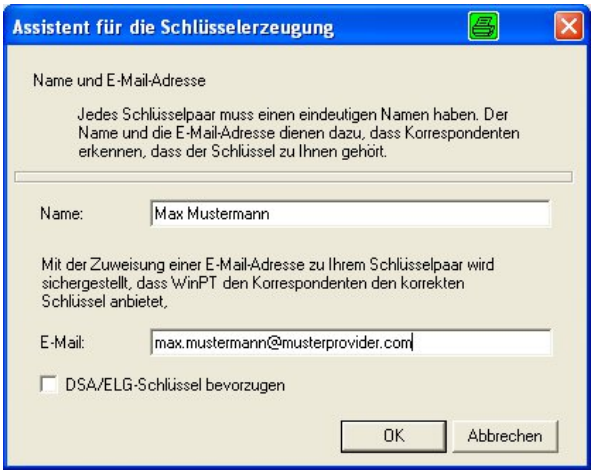

Abbildung 8: Schlüsselpaar erstellen

- Geben Sie Ihren Namen und Ihre Emailadresse ein (Bild 8) und klicken Sie „OK“.
- Geben Sie im nächsten Dialog ein sehr gutes Paswort ein, mit dem Sie Ihren privaten Schlüssel schützen. Merken Sie es sich gut!
- Geben Sie im nächsten Dialog das gleiche Paswort nochmal ein.
- Anschließend erscheint ein Dialog, während der Schlüssel erzeugt wird. Bewegen Sie die Maus dabei zufällig hin und her.
- Danach erscheint noch eine Meldung, dass der Schlüssel fertig erstellt wurde.
- Abschließend wird ein Backup der Schlüsselbunde vorgeschlagen. Sie sollten unbedingt ein Backup der Schlüsselbunde auf einem unabhängigen Datenträger erstellen, der jedoch nur Ihrem Zugriff unterliegt.

Beachten Sie, dass insbesondere Ihr geheimer Schlüssel und Schlüsselbund nie in die Hände Dritter gelangen sollten!

3.3 Schlüsselverwaltung

Nach einem Start von GnuPT-Portable erscheint im System Tray (das ist der Bereich in der Taskleiste unten rechts) ein Schlüsselsymbol von der

Abbildung 9: Symbol von WinPT im System Tray

Abbildung 10: Menü von WinPT

Anwendung WinPT (Bild 9). Mit einem Mausklick darauf öffnet man das Menü von WinPT (Bild 10).

Mit einem Klick auf „Schlüsselverwaltung...“ öffnet man die WinPT-Schlüsselverwaltung. Dort sieht man zunächst nur seinen eigenen Schlüssel (genauer das eigene Schlüssel*paar*).

Besorgen Sie sich nun die öffentlichen Schlüssel der Empfänger, mit denen Sie kommunizieren möchten. Dazu gibt es mehrere Wege:

- Lassen Sie sich den *öffentlichen* Schlüssel als Datei per Email zusenden. Speichern Sie ihn auf Ihrem Dateisystem ab und importieren Sie ihn mit dem Befehl „Schlüssel/Importieren...“.
- Laden Sie den *öffentlichen* Schlüssel von einer Webseite herunter. Speichern Sie ihn auf Ihrem Dateisystem ab und importieren Sie ihn mit dem Befehl „Schlüssel/Importieren...“. Alternativ kann er direkt via HTTP importiert werden, wenn Sie die URL zum Schlüssel kennen. Nutzen Sie in diesem Fall den Befehl „Schlüssel/Import via HTTP...“.
- Laden Sie den *öffentlichen* Schlüssel von einem Schlüsselserver herunter (Menü „Schlüsselserver“).
- Lassen Sie sich den *öffentlichen* Schlüssel auf einem Datenträger geben (Menü „Schlüssel/Importieren...“).

Für den öffentlichen Schlüssel von Hartgeld.com wählen Sie bitte die Variante „Schlüssel/Import via HTTP...“ und nutzen Sie folgende URL: „http://www.hartgeld.com/filesadmin/div/WalterEichelburg-at-hartgeld-com_PGPpubKey.asc“. Sollte das fehlschlagen, besuchen Sie mit Ihrem Browser bitte die Seite „http://www.hartgeld.com/secure-mails.htm“. Dort finden Sie einen Link zur Schlüsseldatei „WalterEichelburg-at-hartgeld-com_PGPpubKey.asc“. Klicken Sie mit der rechten Maustaste auf den Link und wählen Sie „Speichern unter...“ bzw. „Ziel speichern unter...“ oder „Verlinkten Inhalt speichern als...“, oder was immer Ihr Browser für die Speicherfunktion als Text nennt. Speichern Sie die Schlüsseldatei auf Ihrem Rechner ab und wählen Sie danach in der Schlüsselverwaltung das Menü „Schlüssel/Importieren...“. Wählen Sie dann die

eben gespeicherte Schlüsseldatei und klicken Sie auf „OK“.

Nach einem erfolgreichen Import erscheint der Schlüssel in Ihrer Schlüsselverwaltungsliste und steht nun für die Verwendung bereit.

3.4 Eigenen öffentlichen Schlüssel bereitstellen

Um Ihren eigenenen öffentlichen Schlüssel anderen bereitzustellen, gehen Sie so vor:

- Wählen Sie in der Schlüsselverwaltung Ihr eigenes Schlüsselpaar aus.
- Klicken Sie den Befehl „Schlüssel/Exportieren. . . “ an.
- Speichern Sie den *öffentlichen* Schlüssel ab und senden Sie ihn an alle Leute, denen Sie eine verschlüsselte Kommunikation mit Ihnen anbieten wollen. Sie können den Schlüssel getrost auch auf einer Webseite oder einem Schlüsselserver veröffentlichen.
- Achten Sie aber darauf, Ihren *privaten* Schlüssel niemals außer Hand zu geben!

3.5 Weitere Funktionen der Schlüsselverwaltung

Weitere Funktionen der Schlüsselverwaltung entnehmen Sie bitte der Hilfedatei von WinPT, zu finden unter *Installationsverzeichnis*\WinPT\winpt.de.chm.

3.6 Nachricht verschlüsseln

Um eine Nachricht zu verschlüsseln, gibt es mehrere Wege. Wir zeigen einen allgemeingültigen, dafür vielleicht nicht den elegantesten.

- Klicken Sie auf das WinPT-Symbol im System Tray.
- Wählen Sie den Befehl „Zwischenablage/Bearbeiten“. Es öffnet sich ein simpler Texteditor, der zu WinPT gehört („Editor für die Zwischenablage“).
- Schreiben Sie darin Ihre Nachricht. Löschen Sie vorher ggf. noch darin enthaltenen Text.
- Speichern Sie Ihre Nachricht für sich selbst ab, wenn Sie sie für sich aufbewahren möchten.
- Wählen Sie im „Editor für die Zwischenablage“ den Befehl „GPG/Verschlüsseln“. Es öffnet sich ein Dialog mit allen Schlüsseln, die Sie in Ihrem Schlüsselbund haben. Klicken Sie den Schlüssel des Empfängers Ihrer Nachricht an. Sie können auch mehrere Schlüssel markieren, wenn Sie die Nachricht an mehrere Empfänger senden wollen.
- Ggf. wird nachgefragt, ob Sie einen gewähten Schlüssel überspringen wollen, falls dieser noch nicht als vertrauenswürdig eingestuft ist. Klicken Sie „Nein“, wenn Sie den Schlüssel tatsächlich verwenden wollen.
- Nachdem die Nachricht verschlüsselt wurde, klicken Sie „Bearbeiten/Kopieren“ oder gleich die Schaltfläche „Kopieren“ links unten. Damit ist die Verschlüsselte Nachricht nun in der Zwischenablage.
- Fügen Sie den Inhalt der Zwischenablage in die Email an den Empfänger ein. Verwenden Sie als Email-Format bitte „Nur-Text“, keine HTML- oder Rich-Text-Emails!
- Senden Sie die Email wie gewohnt ab.

Für elegantere Wege lesen Sie bitte in der WinPT- und GnuPT-Dokumentation oder im Internet nach.

3.7 Nachricht entschlüsseln

Um eine Nachricht zu entschlüsseln, gibt es mehrere Wege. Wir zeigen einen allgemeingültigen, dafür vielleicht nicht den elegantesten.

- Öffnen Sie die Email mit der verschlüsselten Nachricht.
- Kopieren Sie die gesamte Nachricht oder zumindest den Teil zwischen „——BEGIN PGP MESSAGE——“ und „——END PGP MESSAGE——“ in die Zwischenablage (Tastenkombination Ctrl+A, Ctrl+C bei fokussiertem Text der Email).
- Klicken Sie auf das WinPT-Symbol im System Tray.

- Wählen Sie den Befehl „Zwischenablage/Bearbeiten“. Es öffnet sich ein simpler Texteditor, der zu WinPT gehört („Editor für die Zwischenablage“). Darin sollte nun die vorher kopierte Email sein.
- Wählen Sie im „Editor für die Zwischenablage“ den Befehl „GPG/Entschlüsseln“. Es öffnet sich ein Dialog mit allen Schlüsseln, die Sie in Ihrem Schlüsselbund haben. Klicken Sie Ihren eigenen Schlüssel an. Wenn Sie mehrere verschiedene nutzen, wählen Sie den für die verwendete Emailadresse passenden.
- Geben Sie das Passwort für Ihren geheimen Schlüssel ein. Die Nachricht wird dann entschlüsselt.
- Speichern Sie Ihre Nachricht für sich selbst ab, wenn Sie sie für sich aufbewahren möchten.

4 Weiteres

Wir haben Ihnen hier nur die wichtigsten, einfachsten Dinge zur Verschlüsselung von Emails mit GnuPT gezeigt. GnuPT kann noch viel mehr (z.B. beliebige Dateien verschlüsseln) oder Daten signieren. Auch Symmetrische Verschlüsselung kann damit durchgeführt werden (mit allen verbundenen Nachteilen). Bitte informieren Sie sich bei weiterem Interesse in den entsprechenden Hilfedateien zu GunPT und WinPT.