Stand: 23.02.2014

Erhöhen der Sicherheit im Online Informationsaustausch

Von Peter Jadasch

eMail ist aus dem heutigen Geschäftsleben nicht mehr wegzudenken. Alle Arten von Dateien werden mittlerweile an eine eMail angehängt und nicht nur firmenintern versendet. Selbst wenn es die Absicht war, eine nur firmeninterne Weitergabe der Datei vorzunehmen, wird die eMail im Internet oft über eine unbekannte Anzahl Mailserver übertragen. Es ist kein Einzelfall, daß ein Mitarbeiter sich die eMails an seinen privaten Account weiter routen läßt weil er von zuhause ebenso arbeiten kann. Ist dies soweit eingerichtet oder durch die Geschäftsleitungen autorisiert, gelangen auch interne Firmen-eMails ins Internet.
Jeder Administrator eines Mailservers hat die Möglichkeit, die für eine gewisse Zeit auf seinem Mailserver verbleibenden eMails einzusehen. Eine Kopie hat die gleiche Qualität wie das Original und ist schnell über einen Script-Befehl automatisch erstellt.
Stelle man sich vor, eine ungeschützte eMail, die über das Internet übertragen wird, hat den Status einer Ansichtskarte, die jeder, der sie in die Hand bekommt beim Weiterleiten, einsehen und lesen kann. Und wer würde schon Firmeninterna auf einer Ansichts- oder Postkarte versenden wollen.
Erst geschützte eMail-Übertragung ist nur mit erheblichem Aufwand einzusehen. Das hätte den Status eines zugeklebten Briefumschlags, der dem Briefgeheimnis unterliegt und dessen unbefugtes Öffnen strafbewehrt ist.

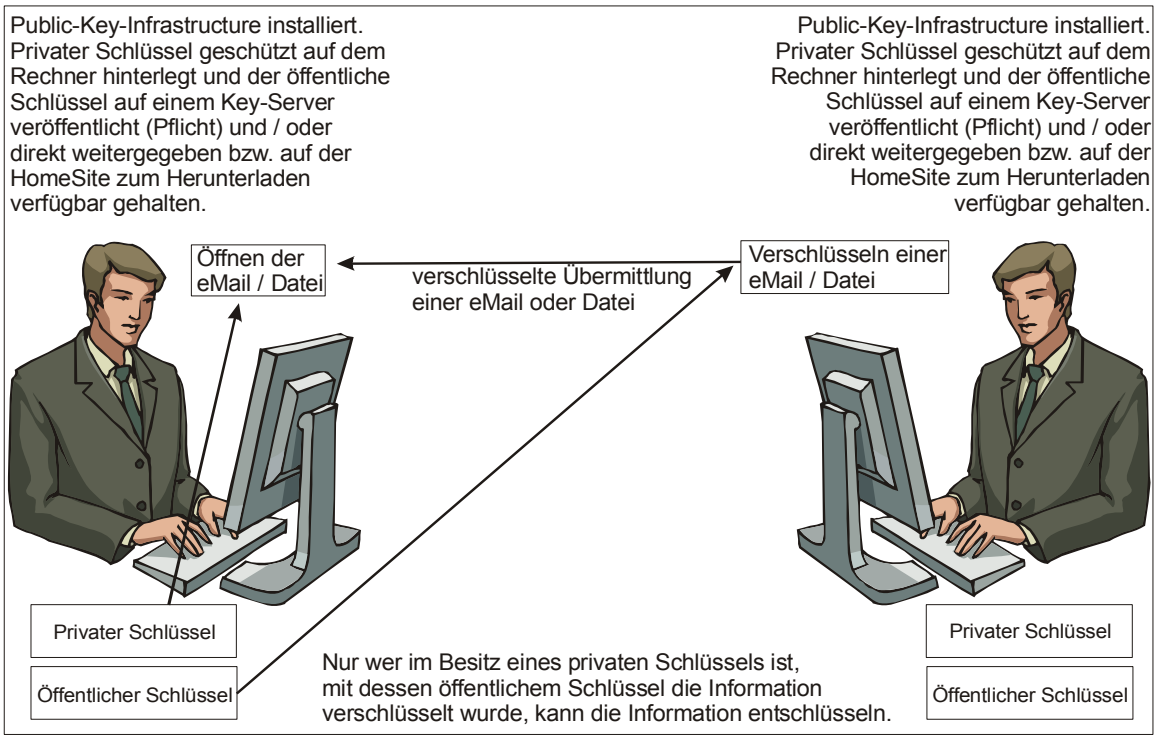
Das Internet ist kein rechtsfreier Raum bedeutete unser damaliger Innenminister Schäuble und gab damit preis, daß er nicht verstanden hat, daß seine Macht nur bis zur Grenze reicht, das Internet jedoch weit darüber hinaus geht. Zudem haben seine Versuche der Onlinedurchsuchung durch den sogenannten "Bundestrojaner" gezeigt, daß er für die Staatsorgane das reklamiert, was er allen anderen Internetnutzern verwehren will. Die angestrebten Einschränkungen waren schon sehr weit gediehen. Die bereits eingeführte, aber vom Verfassungsgericht wieder "kassierte", sechsmonatige Vorratsdatenspeicherung ist ein solches Indiz dafür. Ein Generalverdacht für jeden Internetnutzer war durch die Vorratsdatenspeicherung eingeführt worden, der die im Grundgesetz verankerte Unschuldsvermutung komplett in Frage gestellt. Diese Umkehrung der Unschuldsvermutung wurde dann vom Verfassungsgericht auch als nicht verfassungskonform beurteilt und die Vorratsdatenspeicherung zur Aussetzung angewiesen. Der Versuch, durch den Schäuble nachfolgenden Innenminister de Maizière, der dann sogar wieder seinen Nachfolger Friedrich mit dem Posten des Innenministers "beerbt" hat, und auch dieser Friedrich, wollte über die EU-Rahmenrichtlinien einen solchen Vorratsspeicher-Mechanismus wieder einzuführen. Dies zeigt die wahren Absichten solcher Menschen. Die politische Naivität jedoch, mit der Friedrich die Enttarnung des Bundestrojaners durch den ChaosComputerClub (CCC) in den Medien kommentiert und den illegalen Trojanereinsatz zu rechtfertigt versucht, zeigt ganz klar eine Strategie der Überwachung der Bürger mit System für die Zukunft. Die von Edward Snowden offengelegten Spionagepraktiken der amerikanischen NSA, dem englischen GCHQ und den deutschen Geheimdiensten BND und Verfassungsschutz setzten dem ganzen Spuk noch das "Sahnehäubchen" auf. Mit der gespielten Entrüstung von Friedrich hat er seiner eigenen Glaubwürdigkeit keinen guten Dienst erwiesen, denn anschließend wurde bekannt, daß sein Protest bei der amerikanischen NSA eher ein Nachfragen nach den erhobenen Daten war. Solchen Praktiken ist entschiedener entgegenzutreten.

Es ist in Deutschland mittlerweile zwar verboten gewisse Internetwerkzeuge auch nur im Besitz zu haben (im sog. Hacker-Paragraphen § 202c StGB ist dies geregelt), aber der Gesetzesarm des Innenministers reicht immer nur bis zur Landesgrenze.
Im Internet ist es vollkommen egal, ob jemand sich im Nachbarhaus befindet und einen Internetanschluß zu korrumpieren versucht oder in einer sicheren staatlichen Institution in USA, England, Rußland oder China. Die Mittel und Möglichkeiten sind vollkommen identisch. Den Nachbarn könnten die Häscher des Innenministers erreichen und dingfest machen, den staatlich bezahlten Hacker aus China werden sie nicht einmal ansatzweise zu Gesicht bekommen. Industriespionage ist nicht nur in Rußland und China staatlich unterstützt. Die USA und England stehen dem um Nichts nach, sie hängen diese Tätigkeit nur nicht "an die große Glocke". Selbst die Verfassung des Vereinigten Königreichs von Großbritannien sieht vor, "... daß die Dienste den wirtschaftlichen Nutzen des Landes zu mehren haben." Es ist wenig Phantasie notwendig, herauszufinden was damit gemeint sein könnte.

Es ist alles aus dem wirtschaftlichen oder auch gesellschaftlichen Geschehen eines Landes von Nutzen. Besonders Firmen die mit fest vergebenen TCP/IP-Adressen ins Internet gehen sind von Interesse, da sich die dahinter verbergende Firma leicht identifizieren läßt und der gesamte unverschlüsselte Datenverkehr nur gescannt werden braucht. Im Zeit alter von PetaByte Speicherkapazität wird erst einmal alles aufgezeichnet und über algorithmische Suchkriterien der Datenbestand nach interessanten Themen oder Schlagwörtern abgesucht. So mancher wäre erstaunt, was auf diese Weise an vertraulichen oder geheimen Informationen öffentlich zu beschaffen ist, wenn man sie anschließend mit bekannten Ereignissen verknüpft.

Solchen ungewollten Informationsabflüssen ist entgegenzuwirken. Einfache Mechanismen der Verschlüsselung können dafür eingesetzt werden, die seit Jahren im Internet frei erhältlich sind und fast ein Maximum an Sicherheit bieten. Sicherlich wäre Herr Schäuble ebenso wie Herr de Maizière und Herr Friedrich nicht glücklich darüber, wenn der Einsatz von Verschlüsselung weiter um sich greift. Dann haben auch die Staatsorgane keine Chance mehr eMail-Verkehr unbeobachtet mitzulesen. Die Entschlüsselung eines mit 2048 Bit verschlüsselten Dokuments dauert im Mittel mittlerweile Monate, wenn nicht gar Jahre unter Einsatz eines Hochleistungsrechners heutiger Zeit. Und nach der langen Zeit ist der Inhalt längst kein Geheimnis mehr.

Das Verbieten von Ende zu Ende Verschlüsselung mit Verschlüsselungssoftware würde allerdings allen Bürgern die Augen öffnen was die wirklichen Ziele des Staates sind, nämlich Überwachung bis ins Detail. Deshalb ist auch der von der Post als ePostbrief angepriesene Dienst auf der einen Seite und als De-Mail von der Telekom, GMX.de und Web.de auf der anderen Seite eine staatskonforme Lösung von elektronischen Postdiensten mit eigener gesetzlicher Grundlage. Denn da wird offensichtlich, daß die von den Betreibern behauptete Vertraulichkeit nur eine Farce sein kann, wenn ein Ausdrucken und im Briefumschlag Zustellen durch den Dienstleister möglich ist. Nur eine Ende-zu-Ende Verschlüsselung ist nicht nur vertraulich, sondern sie ist sogar geheim. Dann allerdings macht ein Ausdrucken und dann Zustellen keinen Sinn, da die Darstellung wie kryptischer Buchstabensalat aussehen würde, wie in der Abbildung weiter unten mit der verschlüsselten eMail zu sehen ist.



Die Veranschaulichung der Funktionsweise einer PKI

Somit sollte geschäftlicher eMail-Austausch bzw. eMail-Anhänge versenden immer Ende zu Ende verschlüsselt erfolgen, damit ungewollter Informationsabfluß nicht stattfinden kann. Um den Einstieg in die Verfahren der Public-Key-Infrastructur (PKI) nutzen zu können, muß das Wissen darüber aber erst einmal vorhanden sein. Deshalb wird hier ein Extrakt vorgestellt, wie das Verfahren angewendet wird und wo die dafür benötigten Komponenten kostenlos bezogen werden können. Denn obwohl mit dem

BSI der Staat die Entwicklung dieser Verfahren beauftragt hat[1], hat er, respektive die Ermittlungsbehörden, eigentlich kein Interesse daran, daß sich kryptographierter Informationsaustausch weiter verbreitet. Denn er ist dann mit einfachen Mitteln, wie im Moment noch der offene Mailaustausch, nicht mehr zu kontrollieren.

Im kleinen Rahmen sind Einzelplatzlösungen ausreichend. Für größere Firmen oder Netzwerkstrukturen sind zwar ebenfalls Verfahren verfügbar, jedoch nicht kostenlos.

Primär wird hier in diesem Dokument auf Einzelplatzlösungen verwiesen, weil Informationsaustausch vertraulicher Art i.d.R. zwischen zwei realen Personen stattfindet. Jedoch auch kleine Gruppen sind verschlüsselt ansprechbar, wenn alle öffentlichen Schlüssel vorhanden sind. Hat jeder dieser Personen eine PKI installiert, sind Austausche auch zwischen allen möglich. Das entstehende Problem dabei ist die Schlüsselverwaltung, wenn die Gruppen zu groß werden oder mehr noch einzelne Personen mehreren Gruppen zugeordnet werden müssen. Mehrfaches vorhalten des gleichen Schlüssels in verschiedenen Gruppenzuordnungen würde früher oder später zu Versionskonflikten führen. Die Schlüsselverwaltung ist somit der größte Hinderungsgrund in großen Infrastrukturen eine Publik-Key-Infrastruktur einzuführen. Aber alles nacheinander, erst einmal das "Wie geht's".

Ein weiterer Vorteil einer PKI ist, nachdem Schlüssel ausgetauscht sind, das Validieren der Signatur einer Nachricht. Durch eine angehängte Signatur an eine eMail z.B. oder eine Datei, die mittels des persönlichen Schlüssels erzeugt wird, kann ein Empfänger immer feststellen ob die eMail oder die Datei wirklich von dem vorgegebenen Versender stammt, wenn er mittels des öffentlichen Schlüssels überprüfen kann, ob die Signatur stimmt (Authentifizierung).

Poolverschlüsselung ist ebenfalls möglich. Das heißt, soll an eine Gruppe von z.B. 5 Projektmitglie - dern eine verschlüsselte eMail mit Anhang verschickt werden, ist es möglich die entsprechenden 5 öffentlichen Schlüssel herzunehmen, um die eMail und/oder den Dateianhang zu verschlüsseln, und alle 5 Zielpersonen können die eMail bzw. den Dateianhang mit ihrem privaten Schlüssel öffnen.

Lösung der Defizite durch eine PKI

Der Ursprung der PKI ist in seiner jetzigen Form schon mehr als 30 Jahre alt. Die ersten Algorithmen sind allerdings sehr schnell entschlüsselt worden und waren daher untauglich, dem zu erreichenden Zweck zu dienen.
Die Entwicklung ging weiter und wurde mit zunehmend stabileren Algorithmen, die schwieriger zu "knacken" waren, zu einem praktikablen Werkzeug. Es gibt kommerzielle Verschlüsselungswerkzeuge, die einen weiten Rahmen von Möglichkeiten bieten firmenweit Verschlüsselung zu implementieren. Phil Zimmermann –ein Protagonist pro Verschlüsselung der ersten Stunde-- hatte Anfang der 90er Jahre in s einer Firma PGP.com eine weitreichende Palette von Verschlüsselungswerkzeugen basierend auf OpenPGP angeboten. Die private Nutzung war von vornherein kostenlos. Diese Verfahrensweise ist von der Firma Symantec allerdings abgeschafft worden, nachdem sie PGP.com aufkaufte. Die Versionen der Verschlüsselung sind nun alle kommerziell und auch umstritten, da die Quellcodes nicht mehr offen liegen, also von Außenstehenden nicht eingesehen und überprüft werden können.
Das Bundesministerium für Wirtschaft hat in den frühen 90er Jahren des letzten Jahrhunderts im Rahmen der Aktion "Sicherheit im Internet" noch die Forschung und Entwicklung von Verschlüsselungssoftware im GNU Privacy Projekt unterstützt. Aus diesem geförderten Projekt ist in Fortführung ein Werkzeug entwickelt worden, das sich auf die OpenPGP-Implementierung stützt, sich als Open Source[2] immer größerer Beliebtheit erfreut und zudem noch als die sicherste Verschlüsselungssoftware gilt (siehe auch http://www.gnupp.de/warum.html). In 2005 wurde vom BSI die Entwicklung einer Benutzungsoberfläche für GPG4win beauftragt, die heute als Kleopatra in einem Gesamtpaket unter **GPG4win.de** zur Verfügung steht.

Verfahrensweise zur Installation einer PKI

Das aus dem GNU Privacy Projekt entstandene kostenloses Verschlüsselungswerkzeug für Windows und weitgehend alle UNIX-Derivate ist frei und kostenlos aus dem Internet beziehbar.

---

[1] https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2013/Keine_Hintertuer_in_Gpg4win_30072013.html

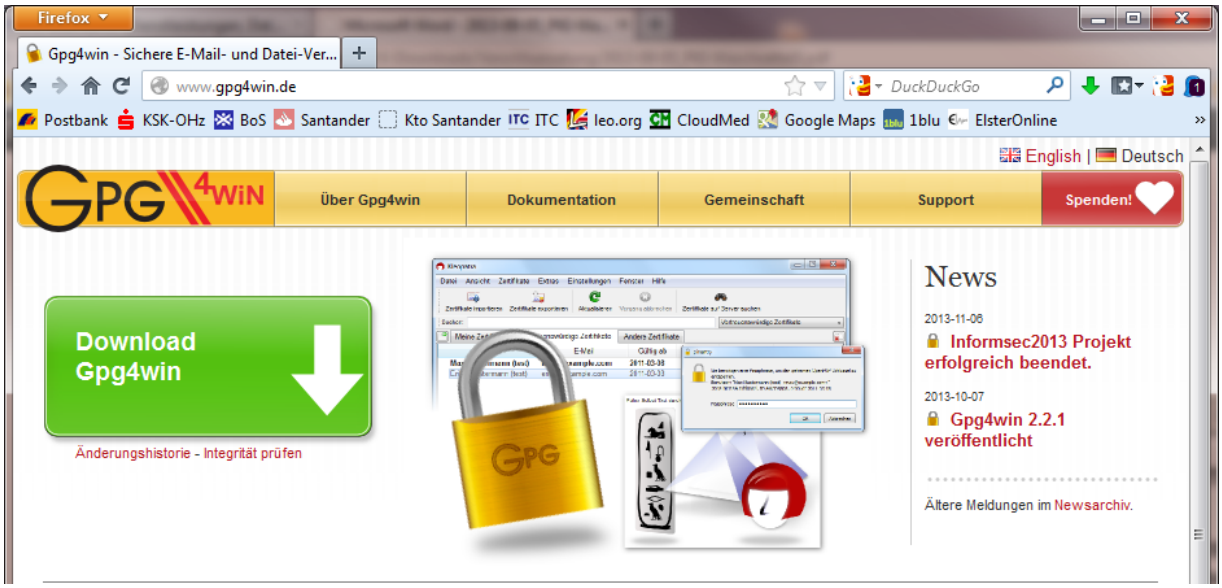
[2] OpenSource bedeutet, der Quellcode des Programms ist öffentlich und kann von jedem eingesehen werden. Fachleute können so überprüfen, ob das Programm fehlerfrei ist und keine "Hintertüren" mit nicht dokumentierten Funktionen besitzt.

In jeder Linux-Distribution ist die OpenPGP Implementierung in irgendeiner Variante immer zu finden, so daß in der OpenSource-Community die Linux einsetzt Verschlüsselung schon sehr bekannt aber leider nicht sehr verbreitet eingesetzt wird.

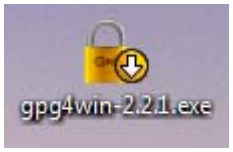
Trotzdem herrscht nicht nur bei Bürgerrechtlern, Datenschützern und IT-Sicherheitsexperten die Meinung vor, daß wenigstens das Angebot vorhanden sein muß zu verschlüsseln, damit jeder selbst entscheiden kann, ob er die Na chricht nun schnell so lo sschickt oder ob eine vertrauliche Übermittlung die bessere Wahl wäre.

In Linux sind die Installationsressourcen in der Grundkonfiguration schon vorhanden und müssen nur installiert werden. Das Erzeugen des Schlüsselpaars ist dann noch einmal eine konzentrationserfordernde Aufgabe. Jedoch macht man diese Aufgabe einmal und hat dann ein Schlüsselpaar, das sich immer wieder einbinden läßt, wenn die Gültigkeit noch nicht abgelaufen ist.

1. Für Windows lassen sich für das freie und kostenlose Gpg4win (das nun in der Version 2.2.1 vorliegt Stand: 16.01.2014) von der gesponserten Internetseite >http://www.gpg4win.de/< das benötigte Softwarepaket herunterladen und die Datei in ein In stallationsverzeichnis kopieren oder auf den Desktop legen.



Früher genügte die light Version ohne die Kommandozeilenoption. Nur seit das Schlüsselverwaltungstool Kleopatra mit installiert werden sollte, weil es eine sehr komfortable Nutzung erlaubt, ist es besser die Vollversion auszuwählen. Dort sind auch gleich die Handbücher mit dabei. Denn diese hier vorliegende Anleitung wird wohl vorwiegend von Kryptographieneulingen in Anspruch genommen werden, so daß weiterführende Informationen sinnvoll sind.



Das heruntergeladene Programm auf dem Desktop.

2. Durch Doppelklick die Software installieren.

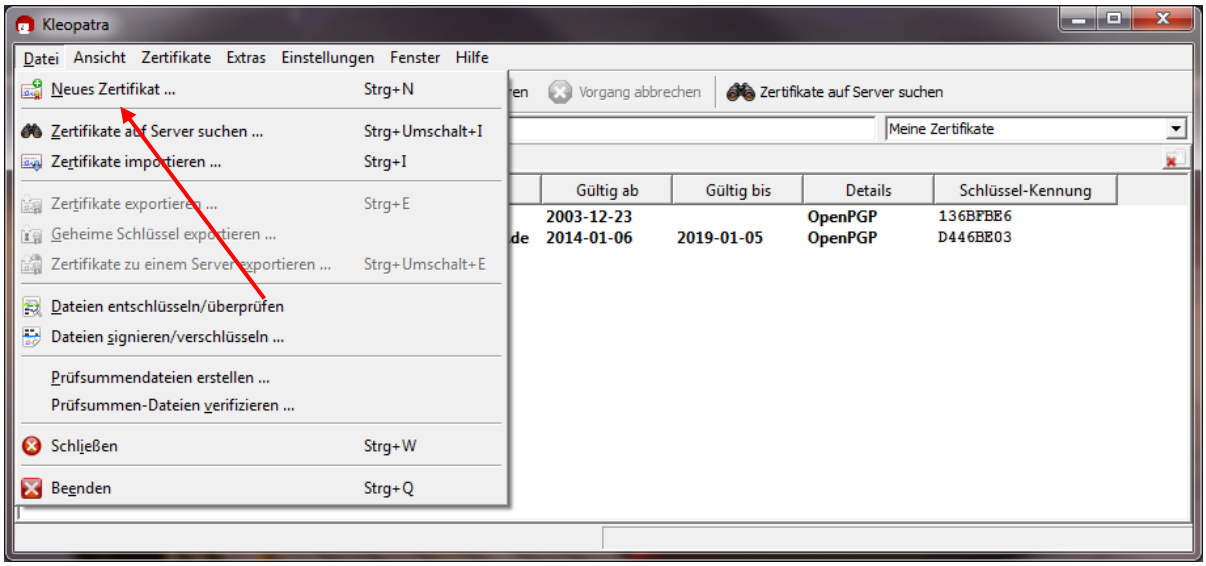
Es kann der Windows Privacy Tray installiert werden oder Kleopatra als Benutzungsoberfläche. Dies muß vor der Installation ausgewählt werden. Das Symbol wird dann in der Werkzeugleiste abgelegt. Meine Empfehlung lautet ganz klar: Kleopatra!

Kleopatra als Icon in der Taskleiste

3. Ein Schlüsselbund erzeugen mit einem öffentlichen und einem privaten Schlüssel. Die benötigte Passphrase zum Absichern des privaten Schlüssels muß gut gewählt werden.

Das Bundesamt für Sicherheit in der Informationstechnik hat auf seiner Internetseite eine Empfehlung für das Erstellen von Paßwörtern zusammengestellt, deren Befolgung in jeder Hinsicht zu empfehlen ist.

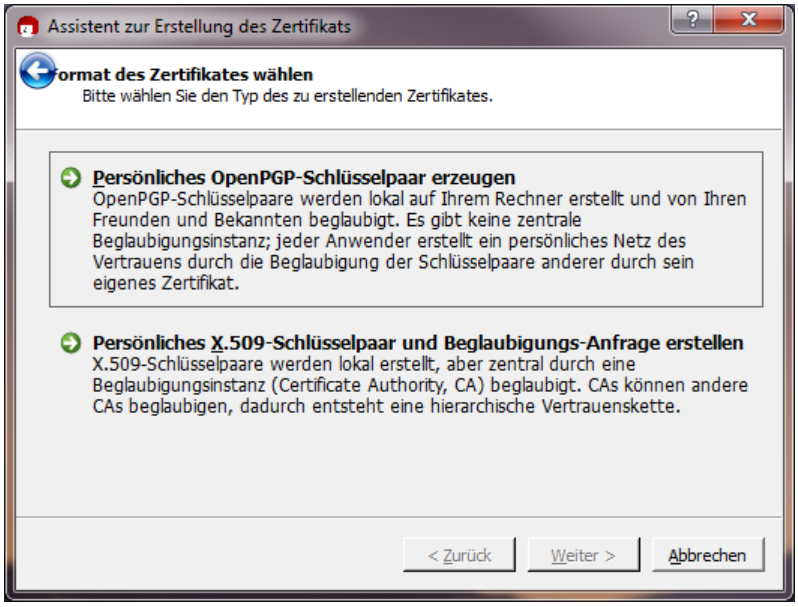
https://www.bsi-fuer-buerger.de/BSIFB/DE/MeinPC/Passwoerter/passwoerter_node.html



Ruft man den Menüpunkt "Neues Zertifikat" auf erscheint eine Abfrage, ob ein bei einem TrustCenter zu beglaubigendes Schlüsselpaar erstellt werden soll (siehe nachfolgende Abbildung) oder ein lokal-erstelltes Zertifikat, das von vertrauenswürdigen Menschen beglaubigt wird. Die in einem TrustCenter zu beglaubigende Zertifikate sind i.d.R. kostenpflichtig. Allerdings gibt es für den privaten Gebrauch zum Ausprobieren bei TC-TrustCenter[1] z.B. ein kostenloses Zertifikat für ein Jahr.

Ein persönliches Zertifikat kann Laufzeiten bis zu drei Jahren haben und kostet dann zwischen EUR 30,- und EUR 40,-.

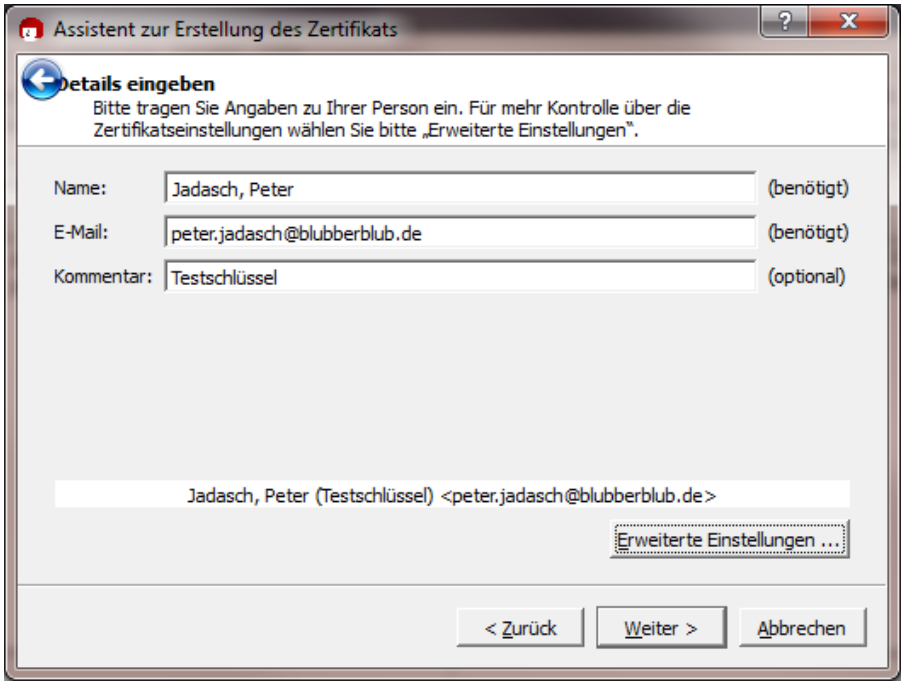
[1] http://www.trustcenter.de



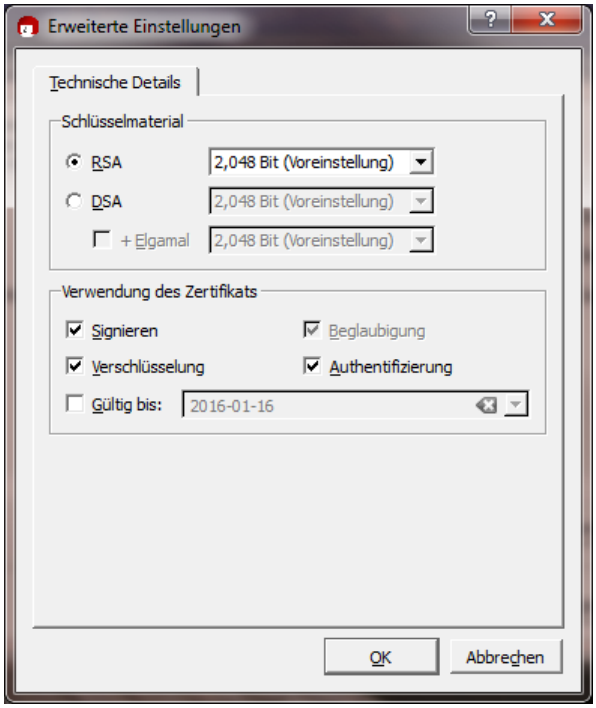
Ein Business-Zertifikat hat dort zwei Vertrauensstufen und kostete 2011 mit einer Laufzeit zwischen einem und drei Jahren von EUR 70,- bis EUR 170,-.

Ein privates Schlüsselzertifikatspaar ist für unsere Zwecke ausreichend. Es sollte anschließend nur von so vielen vertrauensvollen PKI-Benutzern wie möglich signiert werden. Möglichst Menschen mit denen man persönlich bekannt ist.

Wählt man das persönliche OpenPGP Schlüsselpaar aus, müssen noch ein paar Angaben gemacht werden…



Die erweiterten Einstellungen geben die Möglichkeit den Verschlüsselungsalgorithmus zu wählen, ob das Zertifikat zum Signieren und Verschlüsseln verwendet werden soll, was immer sinnvoll ist, und ob die Laufzeit eingeschränkt werden soll.



Sind alle Einstellungen gemacht und ist mit Weiter der Erstellungsprozeß angestoßen worden, muß die Paßphrase eingegeben werden.

Hierfür ist es sinnvoll sich einen gut zu merken den Satz auszudenken, den man selbst nicht vergißt. Ein Beispiel wäre: >An meinem 18 Geburtstag hat es heftig geregnet.<

Wobei die spitzen Klammern NICHT mitzählen, aber der Punkt als Sonderzeichen. Der ganze Satz wäre etwas lang. Also kürzen wir die Paßphrase auf 10 Zeichen, indem nur jeweils der erste Buchstabe verwendet, aber Groß- und Kleinschreibung beibehalten wird.

Am18Ghehg.

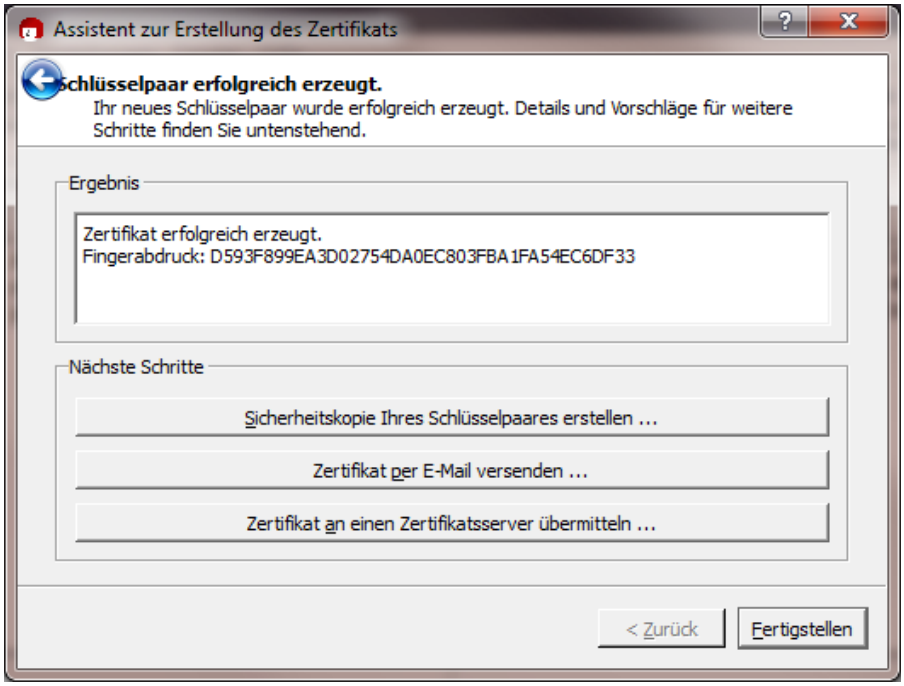
Damit sind es 10 (k) Zeichen, Groß- und Kleinschreibung ist verwendet worden, Ziffern kommen zum Einsatz und Satzzeichen. Grundsätzlich gilt allerdings, je länger die Paßphrase gewählt wird, desto sicherer ist sie, weil der Exponent der Verschlüsselungstiefe entsprechend wächst (siehe unten).

Wer nun mit einer Brute-Force Attacke das Paßwort entschlüsseln will, muß alle Permutationen auf dem möglichen Zeichenvorrat durchprobieren.

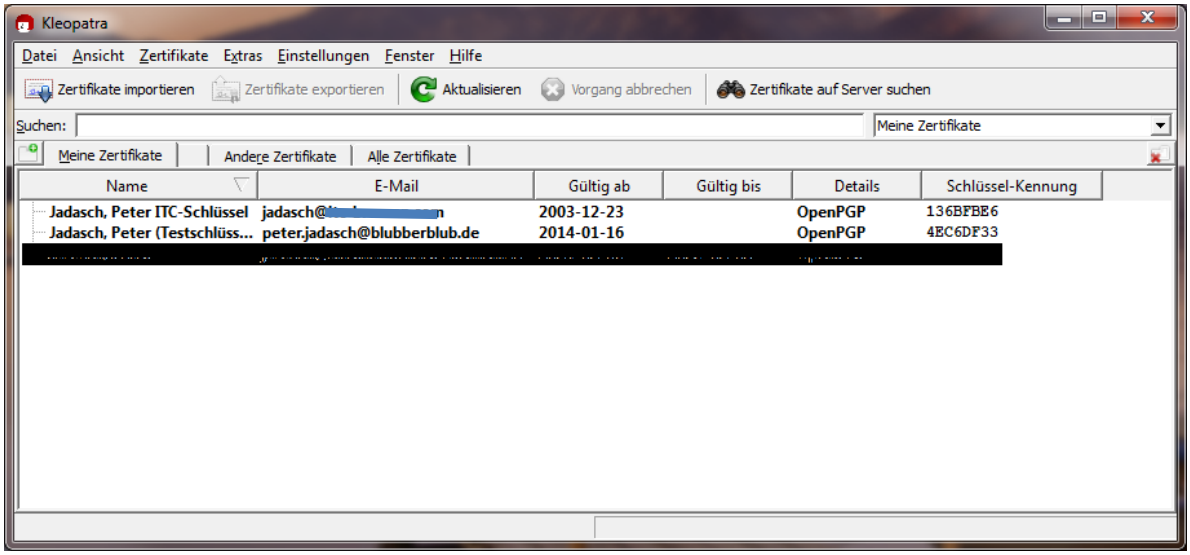
Eine normale Tastatur hat 1 Tastenreihe mit 13 Zeichen, 2 Tastenreihen mit 12 und eine mit 11 Tasten. Das ergibt zusammen 48 mindestens doppelt belegte Tasten. 12 Tasten sind über Alt-GR mit einer 3ten Belegung ansprechbar. Somit sind 48 x 2 + 12 = 108 Zeichen auf einer normalen Computertastatur erreichbar. Das ist unser Zeichenvorrat (n) für ein Paßwort, der für ein "Knacken" durchprobiert werden muß. Die Anzahl der zu prüfenden Möglichkeiten errechnet sich nach der Formel n^k-1

108^{10}-1 = 2,15 10^{20} oder 215.892.499.727.278.669.823 entspricht 215,9 Trilliarden Möglichkeiten.

Da läßt sich schon eine Weile dran rechnen, bis die Paßphrase entschlüsselt ist.



Für den persönlichen Gebrauch im Bekanntenkreis oder in der Arbeitsgruppe des Projekts z.B., in dem sich alle kennen, lassen sich die öffentlichen Schlüssel leicht persönlich austauschen oder per eMail zuschicken, da sie ja öffentlich sind. Aber auch über einen Schlüsselserver die Schlüssel zu verteilen wird angeboten.



Der eigene Schüsselbund muß selbst signiert werden, wenn es nicht automatisch geschieht. Dies gelingt durch markieren des Schlüssels in der Liste und Aufrufen des Menüs
Zertifikate/Zertifikat beglaubigen … .

Fremde importierte Zertifikate müssen, bevor sie verwendet werden können, ebenfalls signiert/ zertifiziert und die gewünschte Vertrauensstellung festgelegt werden. Dies geschieht über das Menü Zertifikate/Vertrauensstatus ändern.

Ein Schlüsselpaar in diesem Kontext wird immer für eine eMail-Adresse erstellt. Der öffentliche Schlüssel kann über Datei/Zertifikate exportieren als *.asc Datei abgespeichert und weitergegeben werden.

Jetzt ist theoretisch zumindest schon das Signieren von Dokumenten oder eMails möglich. Verschlüsselung ist jedoch nur sinnvoll, wenn man eMail oder Dateien versenden möchte und dies geschützt zu tun gedenkt.

Damit verschlüsselte eMail empfangen werden kann und das Verschlüsseln von Dateianhängen möglich wird, ist es notwendig den eigenen **öffentlichen** Schlüssel (Public Key) weiterzugeben, damit mittels dieses Schlüssels verschlüsselt werden kann, denn dann ist derjenige der Einzige, der die Verschlüsselung mit dem privaten Schlüssel wieder lösen kann.
Die Weitergabe kann zum Einen über einen Schlüsselserver geschehen, auf dem allerdings einmal abgelegte Schlüssel nur mit einer Widerrufsignatur gelöscht werden können oder NIE wieder (deshalb sorgfältig arbeiten). Die vielen "Schlüsselleichen" auf den Schlüsselservern sprechen Bände, und ich spreche aus eigener Erfahrung :-)
Zum Anderen lassen sich solche Schlüssel auf der HomeSite zum Herunterladen ablegen oder aber die Schlüssel werden bei Bedarf per eMail versendet. Da es öffentliche Schlüssel sind, kann/muß den jeder haben, der eine verschlüsselte Nachricht oder Datei an den Besitzer schicken will, denn nur der kann die Verschlüsselung mit seinem privaten Schlüssel öffnen.
Unter dem Menüpunkt Datei/Zertifikate-exportieren besteht eine Möglichkeit zum "Exportieren...", wenn ein Schlüssel vorher ausgewählt wurde und markiert ist. Es wird der Name des Schlüssels angeboten mit der Endung *.asc . Diese Datei bietet sich an leicht zugänglich in einem Verzeichnis abzulegen, da sie immer wieder für die Weitergabe an Partner, die verschlüsselt kommunizieren möchten, bereitliegen muß. Sie kann offen als eMail-Anhang versendet werden.

Das Importieren von Schlüsseln geht analog zum Exportieren. Nur daß jetzt die *.asc Datei ausgewählt und importiert werden muß. Taucht der Schlüssel im Schlüsselbundfenster auf, ist die Vertrauensstellung noch festzulegen. Dies ist nur möglich, wenn das Zertifikat vorher signiert wurde, danach kann die Vertrauensstellung geändert werden über das Menü Zertifikate/Vertrauensstatus ändern.

Diese Prozedur ist für jeden importierten Schlüssel zu wiederholen.

Es ist eine Vertrauenssteigerung wenn so viel wie möglich Benutzer, die sich gegenseitig vertrauen, ihre Schlüssel gegenseitig signieren. Je mehr Signaturen ein öffentlicher Schlüssel hat, desto mehr Menschen vertrauen dem Besitzer. Im besten Fall signiert eine vertrauenswürdige Institution wie ein TrustCenter oder ähnlich. Solche Signaturen sind kommerzieller Natur und i.d.R. kostenpflichtig mit einer Jahresgebühr.
Der Heise Verlag hat auf der CeBIT jedes Jahr einen Stand, an dem es möglich ist einen personalisierten Schlüssel mit Namen, der selbst signiert ist, mit einer Signatur des Verlags zu versehen. Da der Schlüssel mit dem der Heise Verlag diese Signatur ausführt durch ein TrustCenter beglaubigt ist, hat dies einen sehr hohen Stellenwert in der Glaubwürdigkeit.

Dies bedeutet, daß die Kryptographieverfahren auch zur Identifikation herangezogen werden können und damit die Herkunft einer eMail oder Datei überprüft werden kann. Ist eine eMail mit einem Fingerprint des privaten Schlüssels signiert, kann der Empfänger der Mail sich den öffentlichen Schlüssel des Absenders beschaffen und damit überprüfen, ob die Signatur stimmt. Das schafft Sicherheit gegen Betrug.

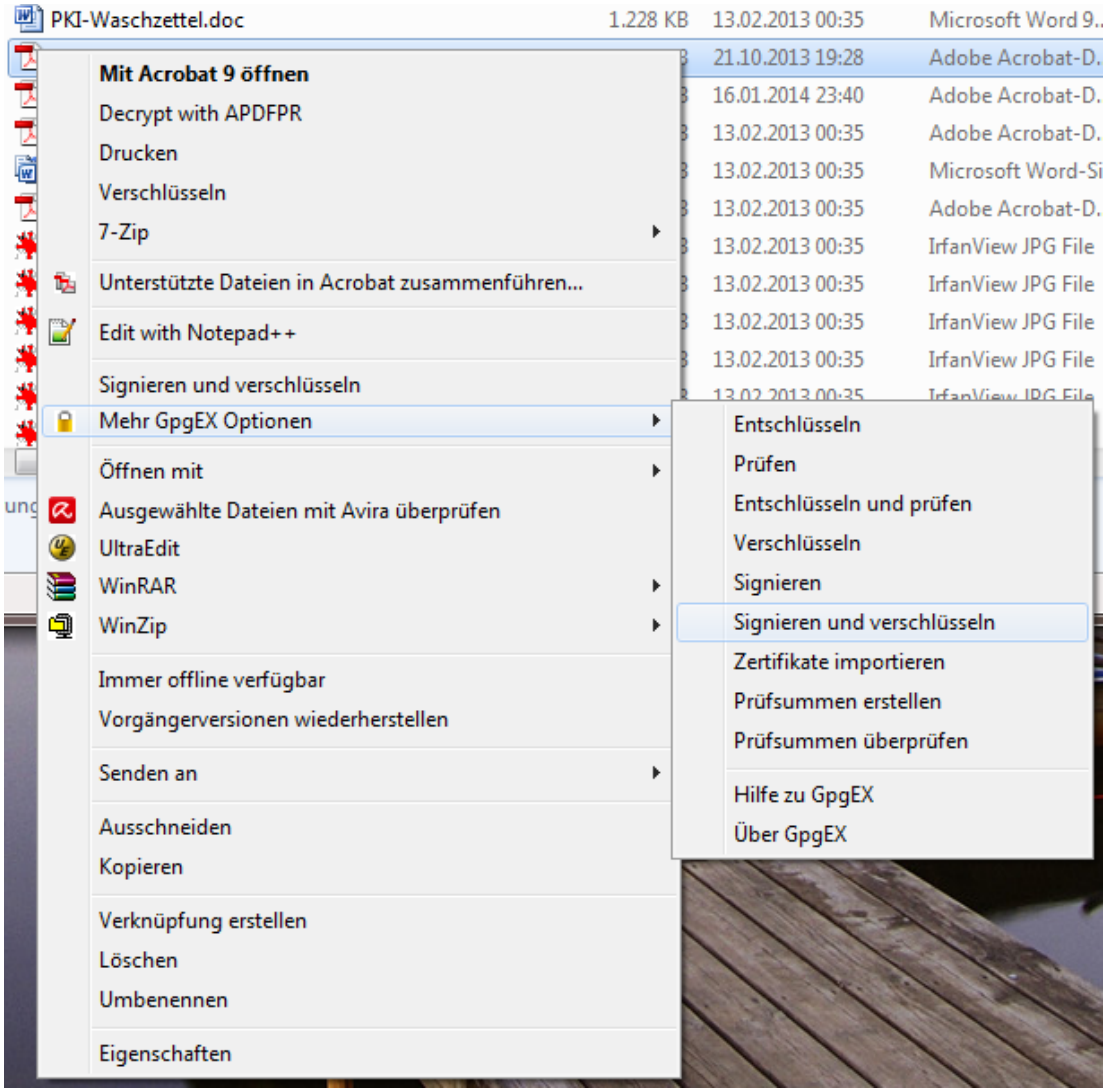
Benutzung der Verschlüsselungssoftware

Dateien oder Anhänge verschlüsseln

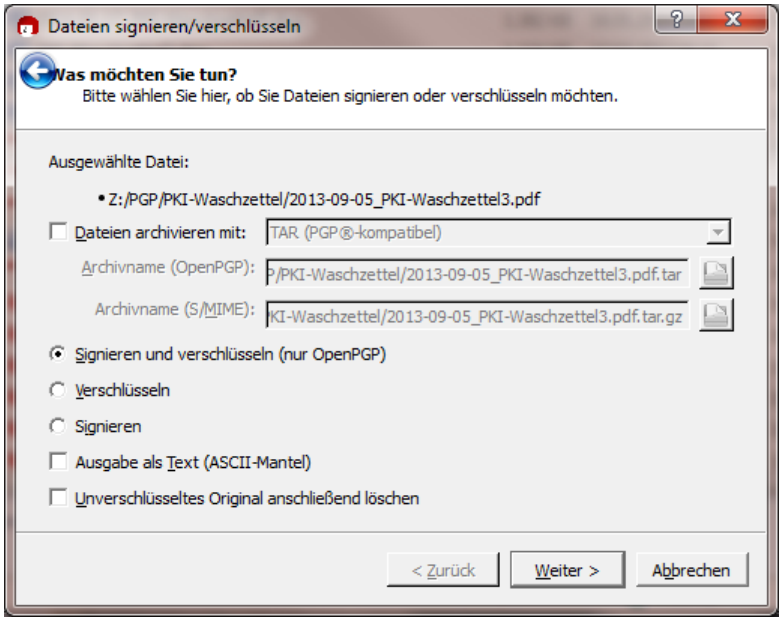
Im Regelfall wird es so sein, daß eine Datei mit Firmeninterna geschützt als Anhang per eMail versendet werden soll und daher verschlüsselt wird. Die zugehörige eMail ist dann oft nur mit Grußformeln oder kurzen Erklärungen gefüllt und muß nicht unbedingt geschützt werden. Das ist der einfachste Fall.

Im Dateimanager (meistens unter Windows der Explorer) wird die zu verschlüsselnde Datei markiert und mit der rechten Maustaste das Kontextmenü geöffnet. Hier wird ein Menü (GpgEX) angeboten, das verschiedene Funktionen anbietet (siehe nachfolgende Abbildung).

Signieren + Verschlüsseln bietet sich als ständige zu verwendende Funktion an, weil der Empfänger dann die Herkunft der Datei überprüfen kann.

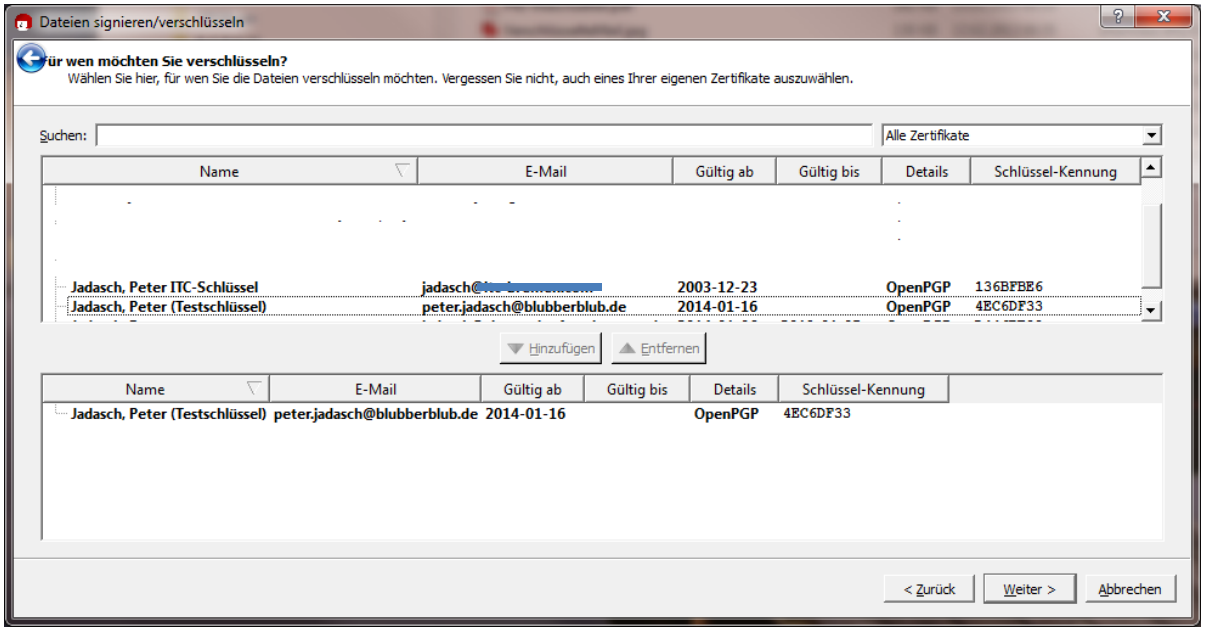


Die ausgewählte Datei mit der rechten Mouse-Taste anklicken



Signieren und verschlüsseln wählen und Weiter klicken.

Nun geht der "Schlüsselkasten" auf und alle importierten öffentlichen Schlüssel der PKI-Partner sind aufgelistet. Durch anklicken des gewünschten Schlüssels im oberen Fenster und >Hinzufügen< klikken wird er in das untere Fenster übernommen. Sollen mehrere Menschen die verschlüsselte Datei öffnen können, müssen deren Schlüssel ebenfalls in das untere Fenster übernommen werden.



eMail ent- oder verschlüsseln

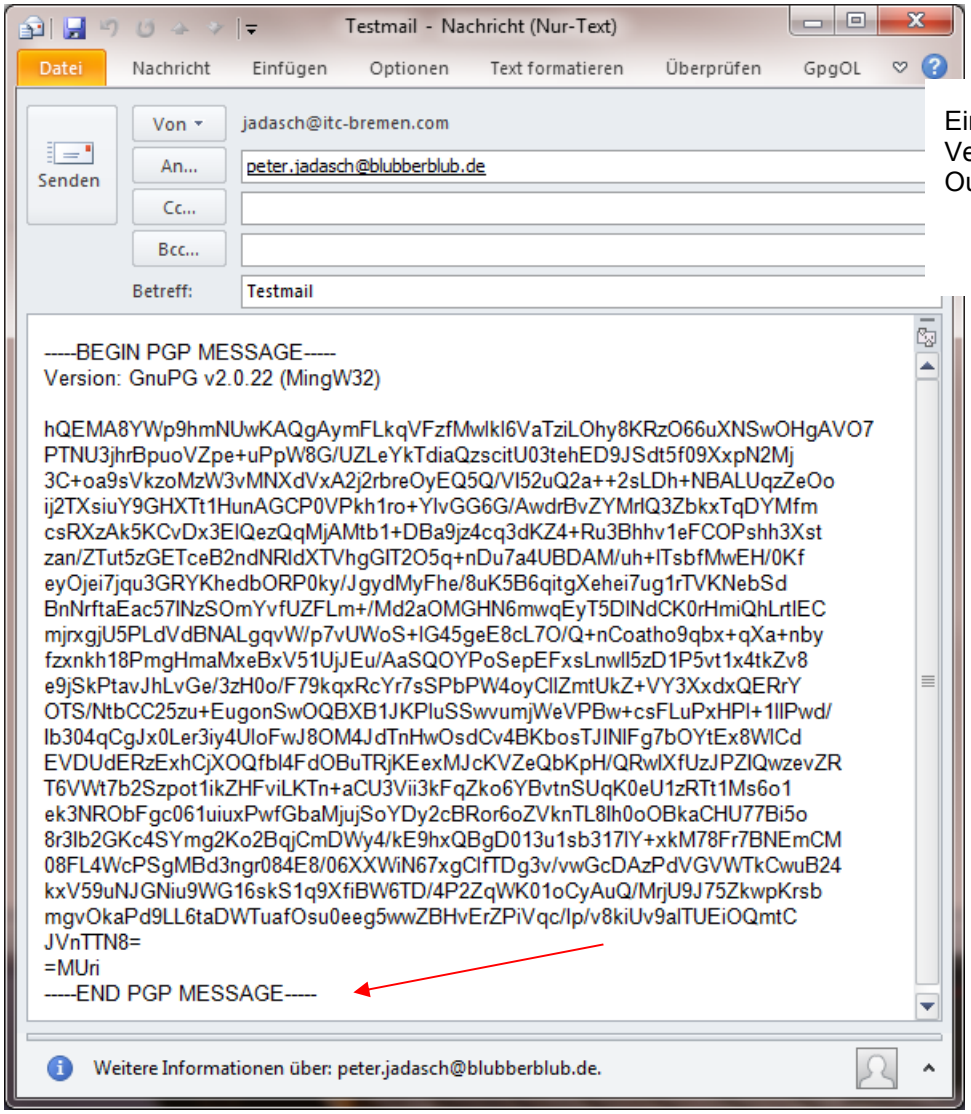
Entschlüsseln

Senden Sie eine eMail an einen Partner, der eine PKI installiert hat und übermitteln ihm ihren öffentlichen Schlüssel als Anhang (die *.asc Datei).

Lassen sie sich eine verschlüsselte eMail zusenden und versuchen diese zu entschlüsseln.

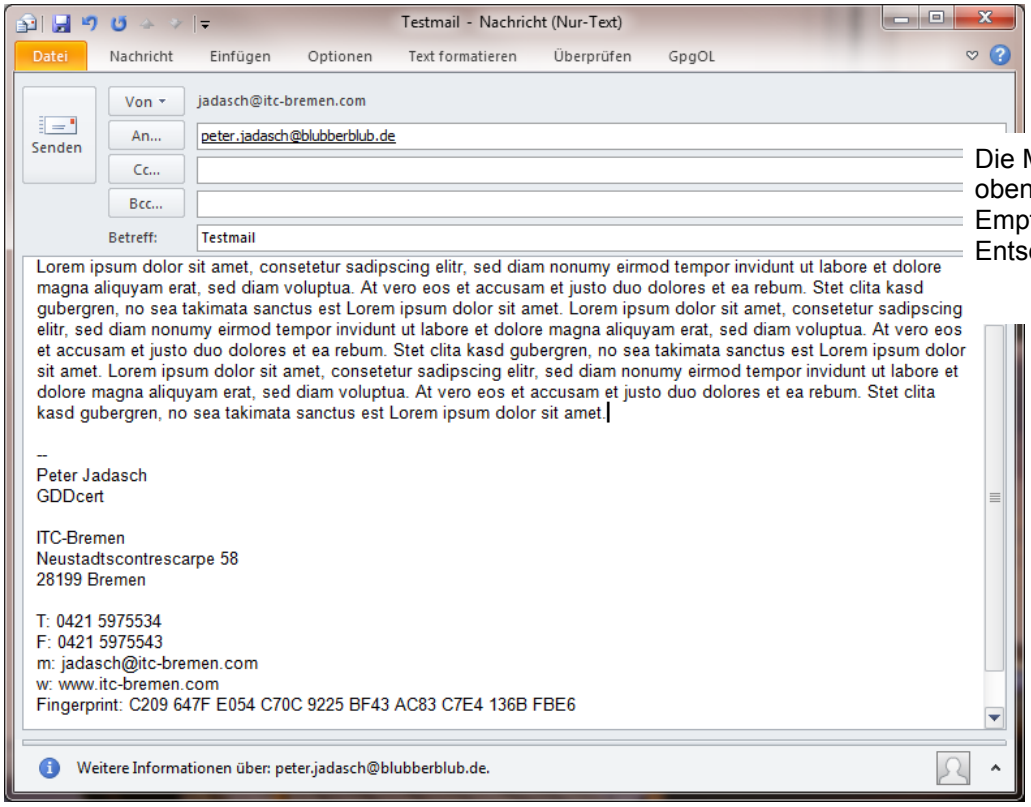
Markieren Sie die Mail im Posteingang und öffnen Sie sie mit Doppelklick, so daß ein separates Fenster entsteht.

Die eMail sieht dann ungefähr wie in der nachfolgenden Abbildung von Outlook2010 aus.



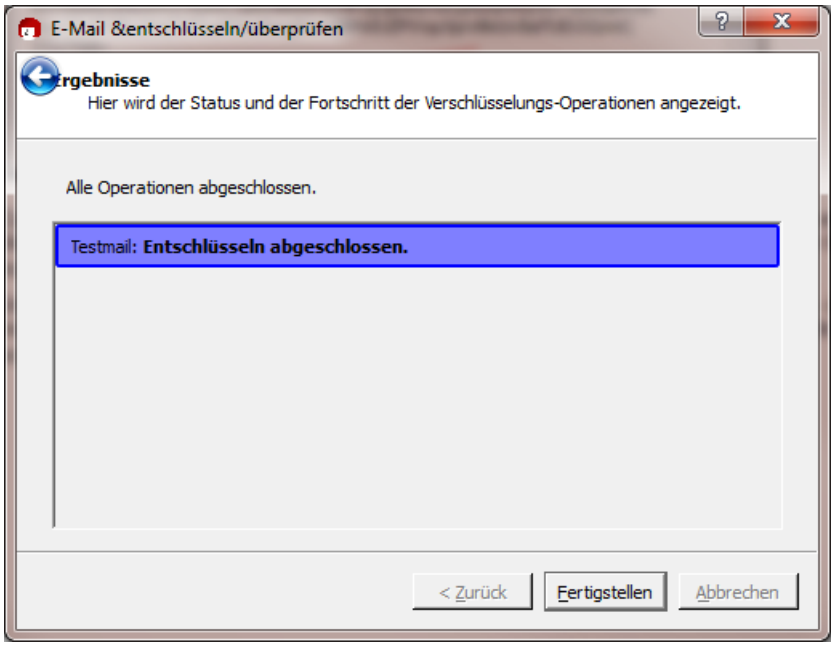
Eine Mail nach der Verschlüsselung in Outlook2010

Zum **Entschlüsseln** rufen Sie den Menüpunkt GpgOL auf und klicken auf Entschlüsseln.



Die Mail vom Bild oben nach dem Empfang und der Entschlüsselung

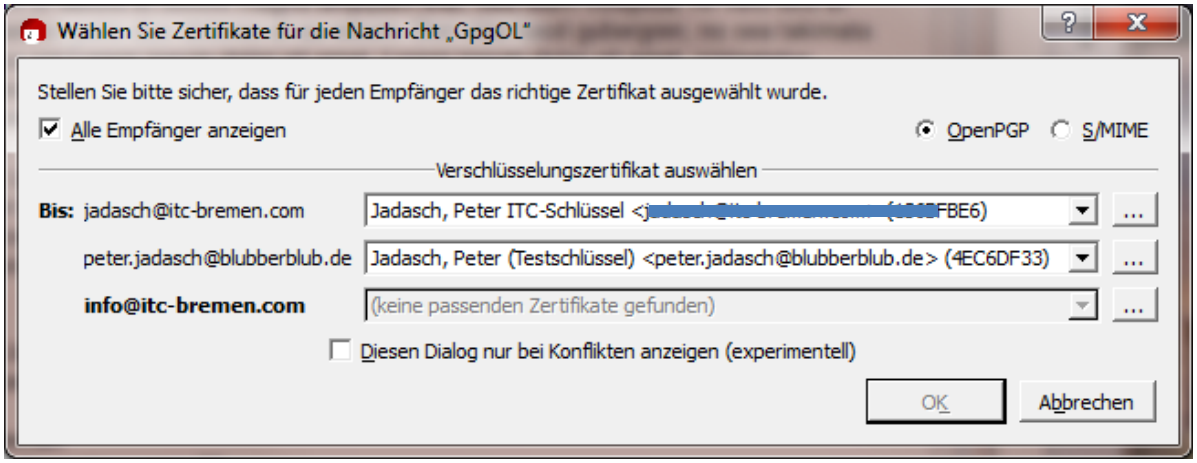
Umgehend ist der Klartext sichtbar, wie im oberen Bild dargestellt ist und eine Rückmeldefenster fibt Auskunft darüber, daß die Entschlüsselung abgeschlossen ist (nachfolgende Abbildung).



Verschlüsseln

Zum Verschlüsseln öffnen Sie im Edito rfenster in de m Sie die Mail gesch rieben haben wieder den Menüpunkt GpgOL und klicken auf Verschlüsseln.

Kontrollieren Sie im erscheinenden Fenster, ob die Absenderadresse und die Empfängeradresse richtig ist. Anhand des Editorfensters ist die Vorauswahl i.d.R. ok. Wählen sie im erscheinenden Fenster den öffentlichen Schlüssel ihres/r Adressaten und bestätigen die Verschlüsselung mit ihrer Paßphrase.

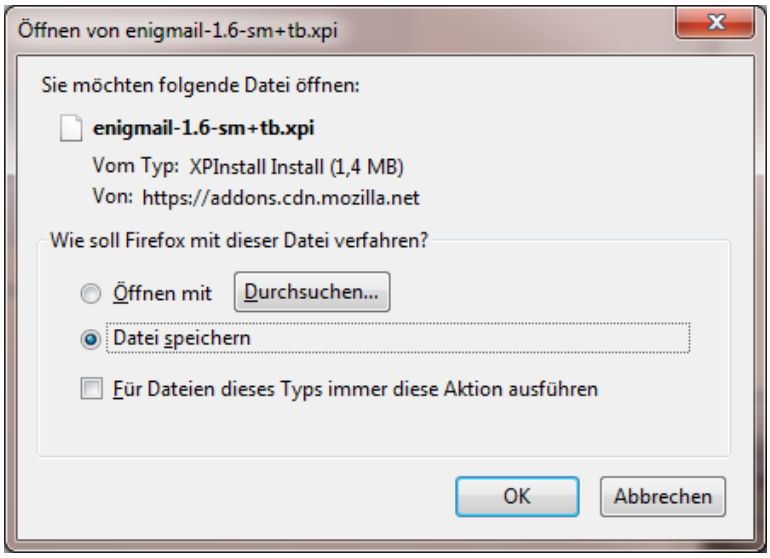


Sollten mehrere Adressaten angesprochen werden ergeben sich, wie in der Abbildung oben, weitere Zeilen mit den entsprechenden Zertifikaten.[1]
Ein Fenster geht auf, in dem Sie Ihre Paßphrase einzugeben haben, um die Mail zu versenden.

[1] In diesem Fall hat die zusätzliche Adresse info@itc-bremen.com kein Zertifikat, weshalb darauf hingewiesen wird.

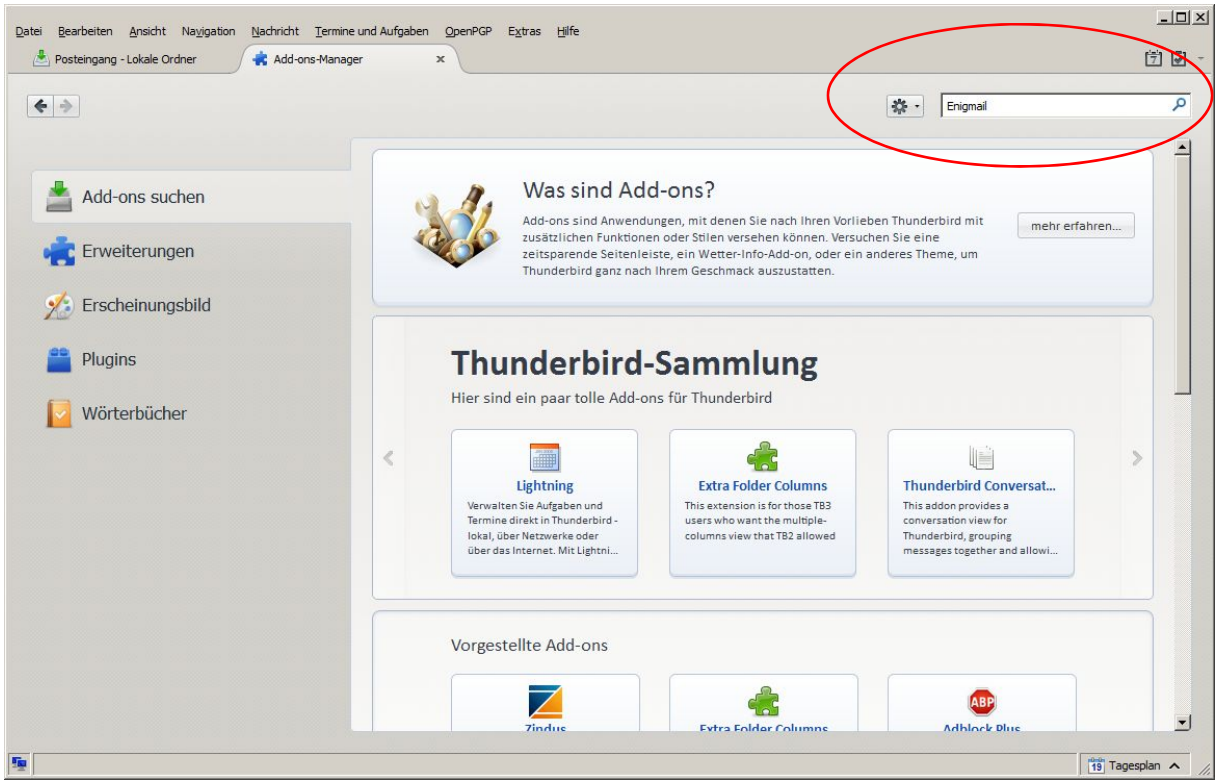
Plug-in zur Erleichterung der Benutzung von Verschlüsselung im Mailer Thunderbird

Für Mozilla Thunderbird ist im Internet[1] eine Datei namens >enigmail-1.6-sm+tb.xpi< (oder neuerer Versionsnummer) verfügbar.



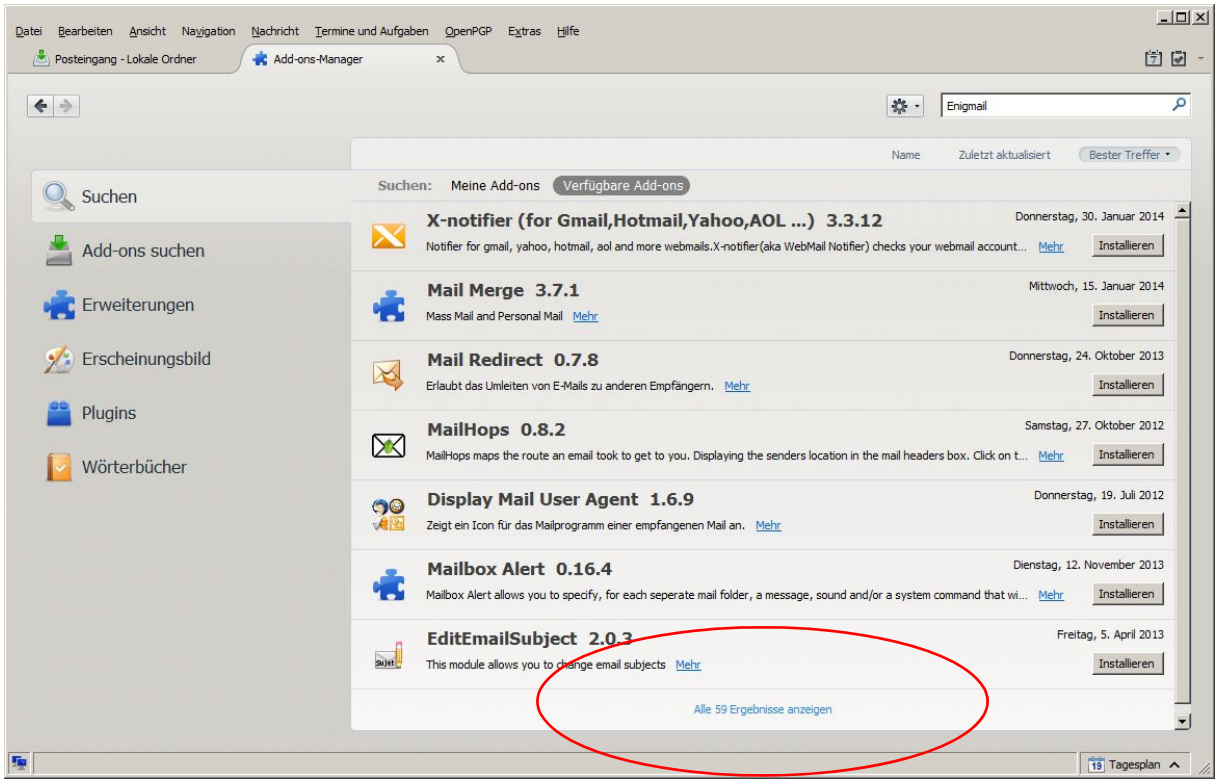
Entweder man lädt sie als Datei herunter, speichert sie in ein beliebiges Verzeichnis und startet die Installation durch Aufrufen des Installieren Buttons im Add-on Fenster. (Dort das "Zahnrad" herunterklappen und auswählen "Add-on aus Datei installieren".)

Die für die Benutzung erforderliche Benutzungsoberfläche wird als Add-on in Thunderbird installiert. Wird der Menüpunkt Extras/Add-on aufgerufen, läßt sich bei Add-ons suchen im Suchfeld Enigmail angeben

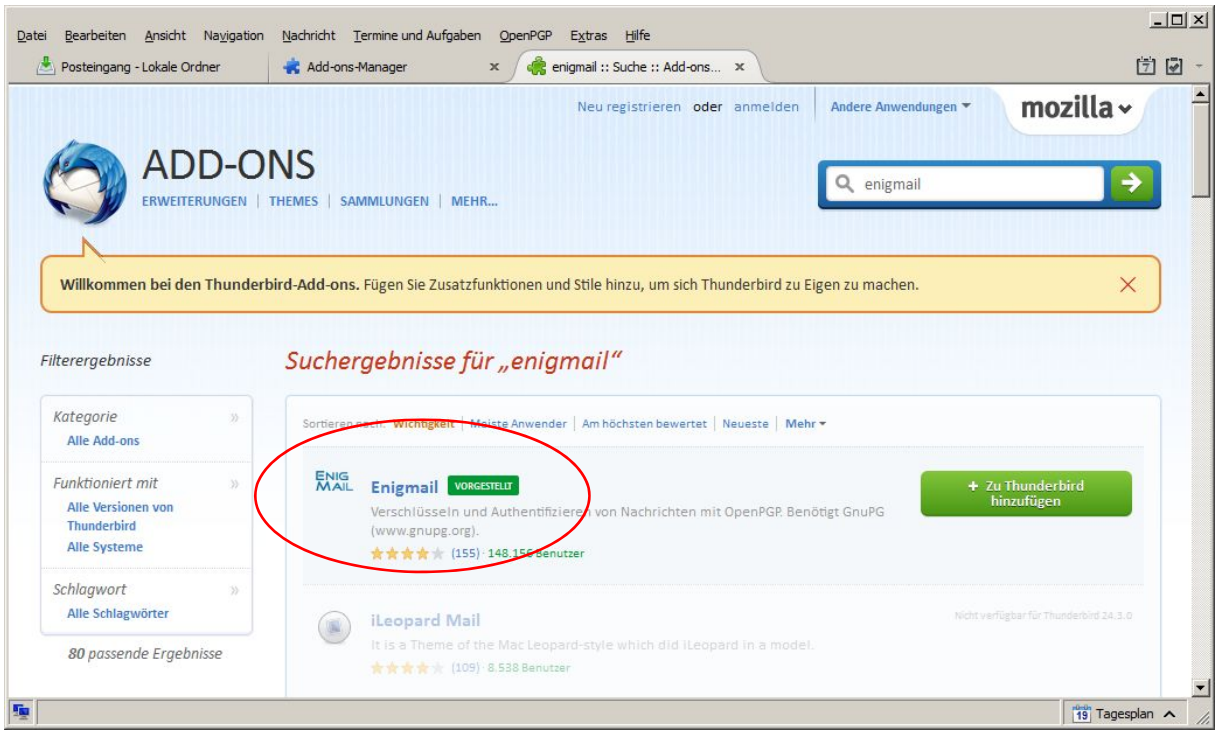


[1] https://addons.mozilla.org/de/thunderbird/addon/enigmail/

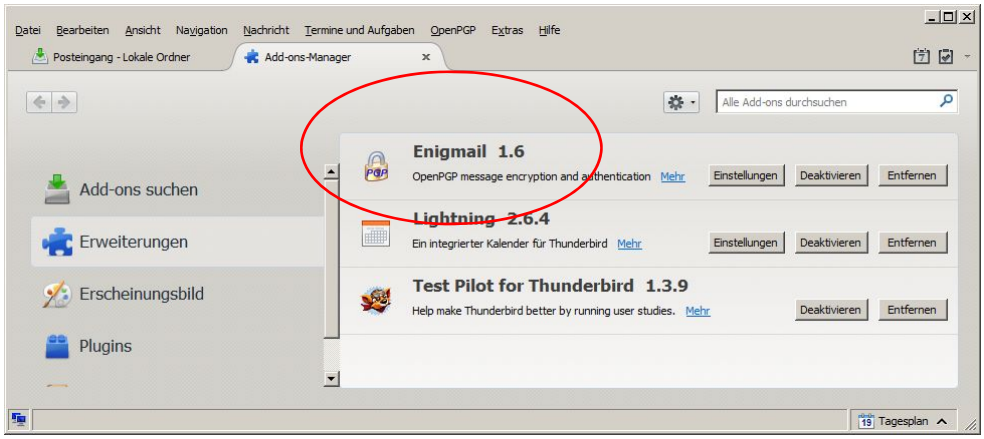
Aufgelistet werden mögliche Add-ons, die Funktionen von Thunderbird ergänzen oder Funktionen komfortabler machen. Hier kann jeder nach seiner Facon "seinen" Thunderbird zusammenstellen. Ist Enigmail in der aufgeführten Liste NICHT aufgeführt, versteckt sich das Add-on unter dem Link zu den weiteren Ergebnissen (siehe Abbildung unten).



Dieser Link führt auf die Webseite von Thunderbird und bietet noch mehr Auswahl. Ist der Cursor über der Auswahl, erscheint rechts ein Button "Zu Thunderbird hinzufügen". Wird der betätigt, wird Thunderbird installiert.



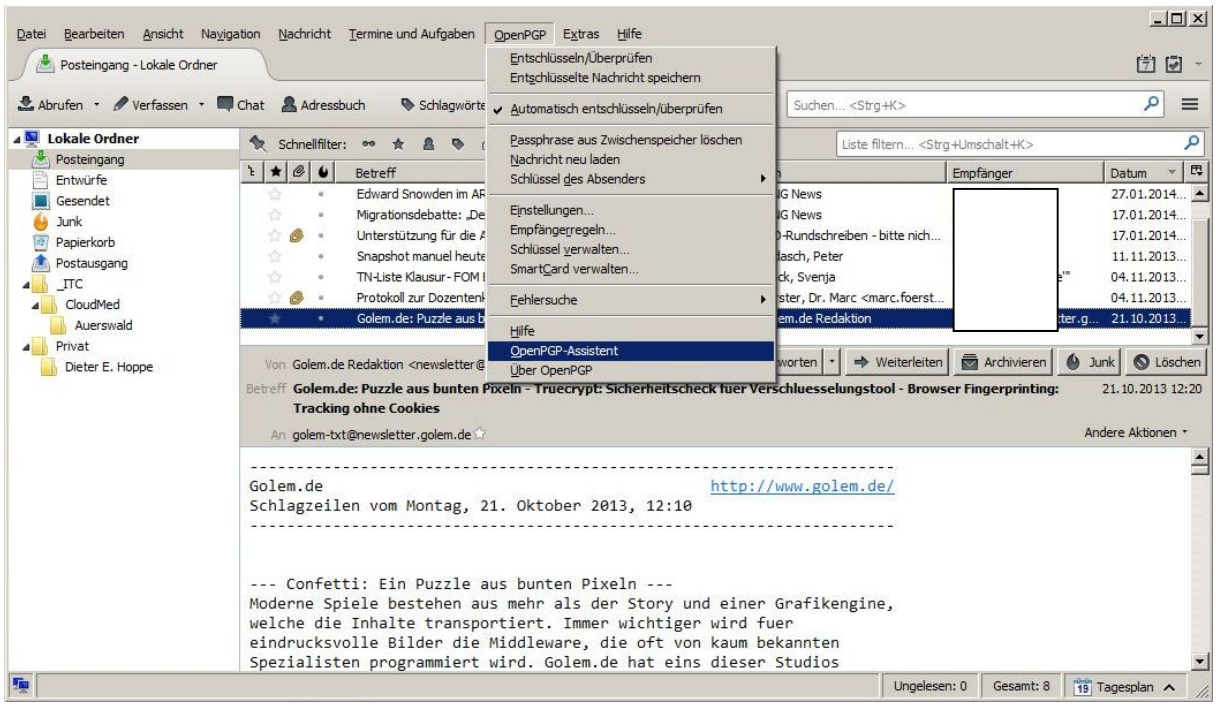
Ist Enigmail dann einmal installiert, taucht es unter Erweiterungen auf.



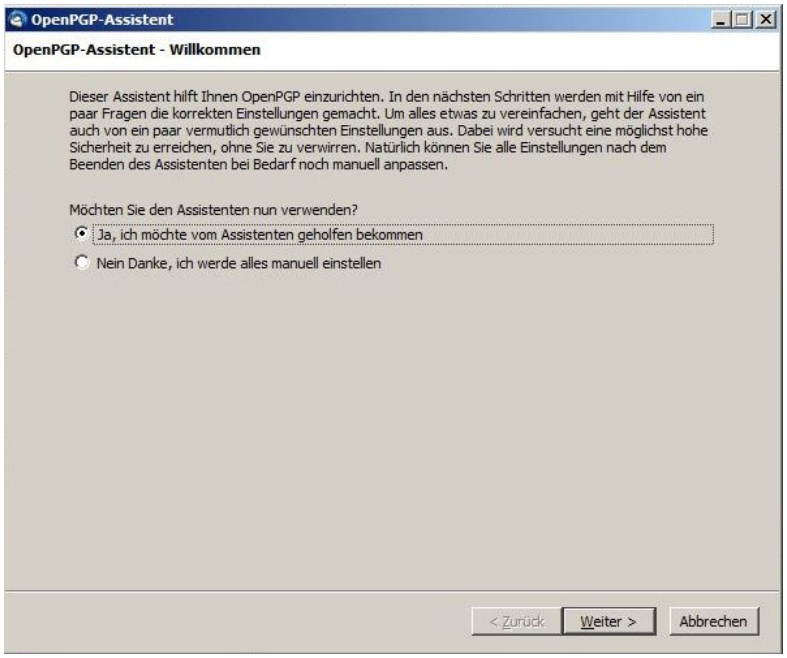
Nun kann mit der Konfiguration begonnen werden und der Erzeugung der beiden benötigten Schlüssel. Ist bereits ein Schlüsselpaar vorhanden (geheimer und öffentlicher Schlüssel) können sie importiert werden. Die Erzeugung neuer Schlüssel kann dann entfallen.

Die entsprechenden eMail-Adressen müssen bereits eingerichtet sein.

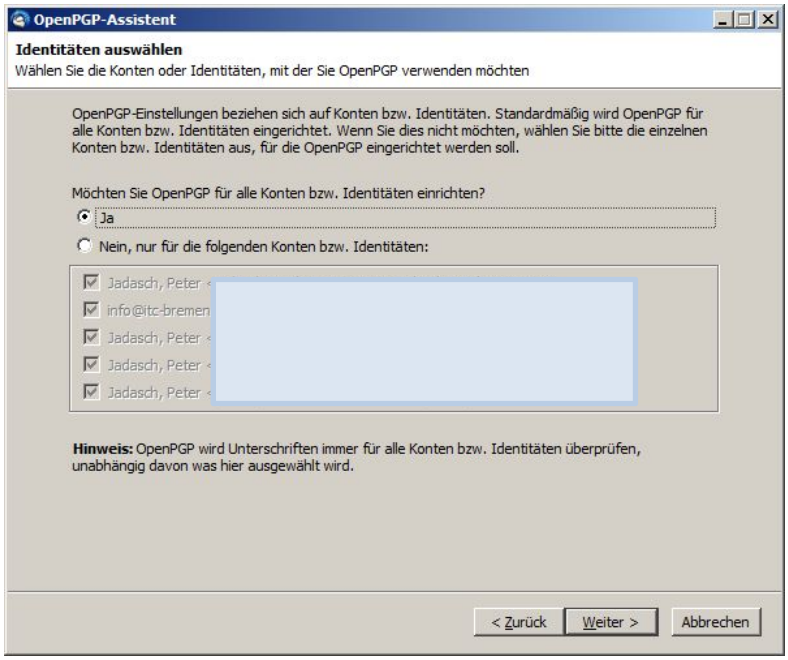
In der Menüleiste ist nun ein Menüpunkt OpenPGP zu finden. Öffnet man diesen Menüpunkt, ist der vorletzte Eintrag OpenPGP-Assistent. Dieser Assistent führt durch die Konfiguration und hilft anschließend bei der Erstellung eines 2048Bit Schlüssels.



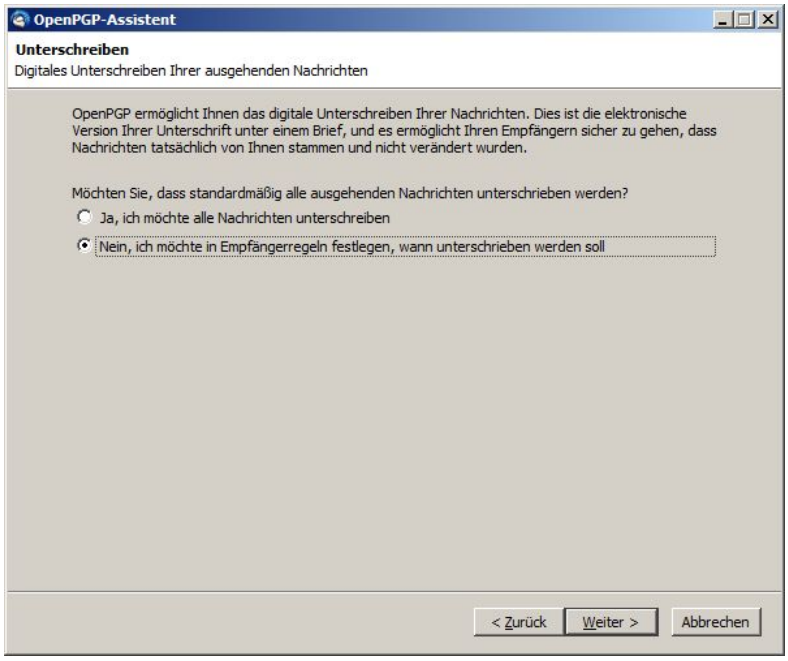
Zu Anfang wird entschieden, ob der Assistent die Führung übernimmt oder die Einrichtung manuell erfolgen soll. wer nicht viel Erfahrung mit der Einrichtung von Mailern hat, sollte sich mit dem Assistenten "anfreunden". Er stellt die grundsätzlichen Dinge ein und leitet dann zur Schlüsselerstellung über.



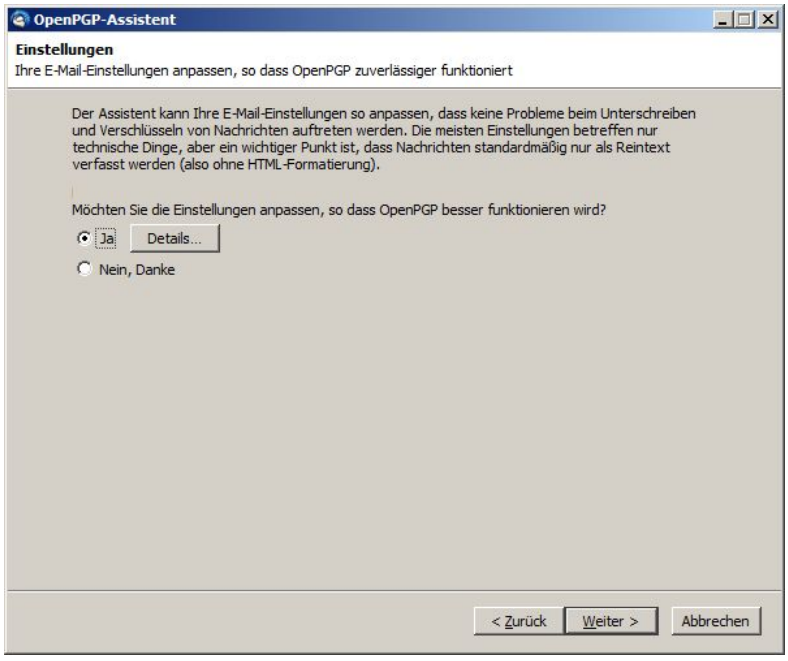
Die Auswahl, für welche der eingerichteten eMail-Adressen ein Schlüsselpaar erzeugt werden soll, kann zum Einen hier getroffen werden durch eine explizite Auswahl, aber auch später lassen sich noch einzelne Adressen bestimmen.



Im folgenden Fenster kann festgelegt werden, ob alle Nachrichten beim Senden mit einer Signatur versehen werden oder ob von Fall zu Fall entschieden werden kann, eine Signatur anzuhängen.



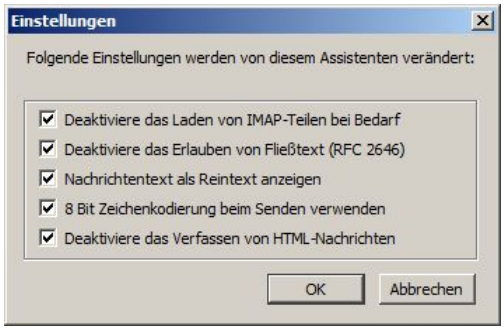
Die Auswahl von Details ist noch sinnvoll, weil doch einige Erkenntnisse verloren gehen, wen der Assistent etwas einstellt von dem der Benutzer dann anschließend nichts weiß.



Z.B. ist entscheidend, ob es sich um ein POP3[1] eMail-Konto handelt oder ein IMAP[2] eMail-Konto. Denn bei POP werden die gesamten eMails von Server heruntergeladen und im Mailer (Outlook oder Thunderbird) verwaltet.

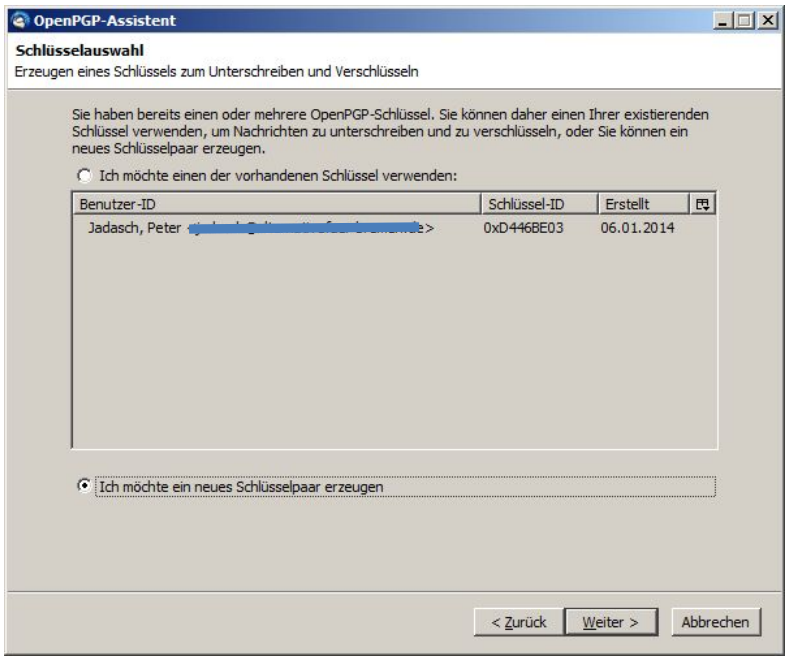
Bei IMAP verbleiben die Mails auf dem Server und es werden beim Abruf nur die Adressköpfe (Header) der Mails herunter geladen. Ist eine Mail verschlüsselt, muß sie bei IMAP vollkommen anders behandelt werden als bei POP.

[1] POP3 = PostOfficeProtocol 3te Generation
[2] InternetMessageAccessProtocol



So ist die erste Funktion aus der Abbildung oben dem IMAP Zugriff geschuldet.

Die Konvertierung von Texten aus allen Formaten in 8Bit codierten Reintext ist beim Verschlüsseln die einfachste Variante. Dazu muß allerdings der Mailer auf reine Textmails umgestellt werden, was der nächste Punkt eindrucksvoll ausweist.



Die Erzeugung des Schlüsselpaars ist noch einmal ein Konzentration erforderndes Ereignis, das allerdings durch den Assistenten sehr vereinfacht wird.

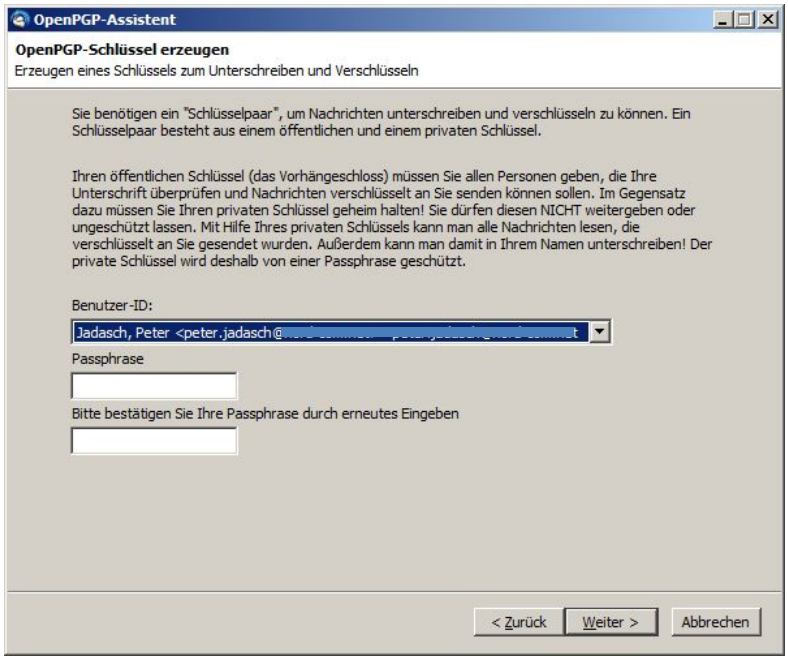
Wählt man die Erzeugung eines neuen Schlüsselpaares aus (Abbildung oben), beginnt die Prozedur mit der Auswahl der eMail-Adresse, für die ein verschlüsseltes Versenden erfolgen soll (siehe nachfolgende Abbildung).

Danach ist eine Paßphrase (Paßwort) einzugeben und zu wiederholen. Die Wiederholung ist notwendig, falls man sich einmal verschreibt und die Paßphrase anders abgespeichert wird als man es in Erinnerung hat, wird man anschließend bei der Eingabe ständig Fehlermeldungen erhalten die Paßphrase sei falsch (was faktisch ja auch stimmt).

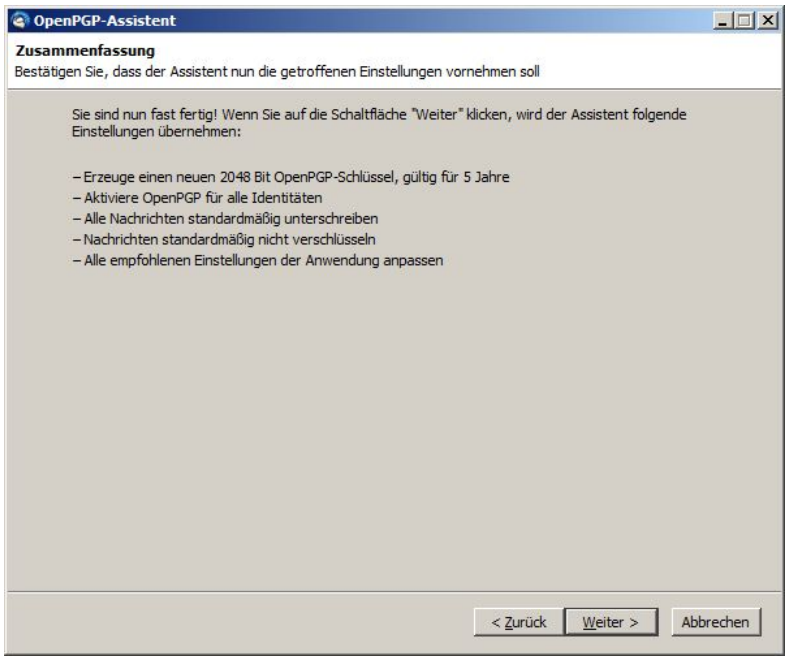
Das BSI hat eine ganz brauchbare Beschreibung veröffentlicht, wie Paßphrasen aufgebaut sein sollten:

https://www.bsi-fuer-buerger.de/BSIFB/DE/MeinPC/Passwoerter/passwoerter_node.html

Letztlich geht es darum eine Paßphrase so aufzubauen, daß der folgende Buchstabe nicht erraten werden kann.

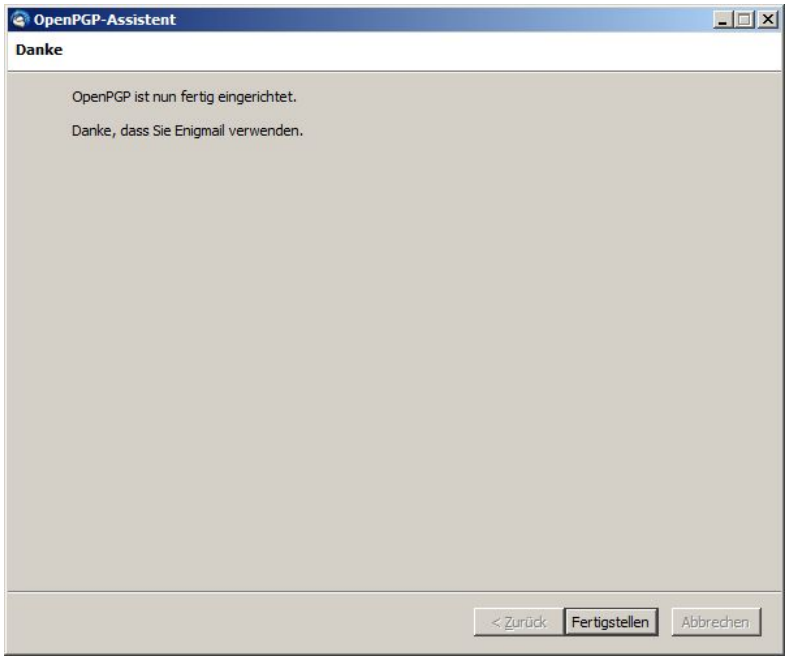


Nach Eingabe der Paßphrase und Betätigen von Weiter erscheint ein Fenster mit einem Fortschrittsbalken und einer Fläche, auf der mit der Maus hin und her "gewischt" werden muß. Das erzeugt Koordinatenwerte in einer bestimmten Reihenfolge, die mit großer Wahrscheinlichkeit kein zweites Mal auf diese Weise erzeugt werden kann. So ist diese Zufälligkeit unique und der Schlüssel damit einmalig.



Der Assistent erzeugt immer Schlüssel für nur 5 Jahre. Dies kann anschließend in den Schlüsselattributen allerdings geändert werden.

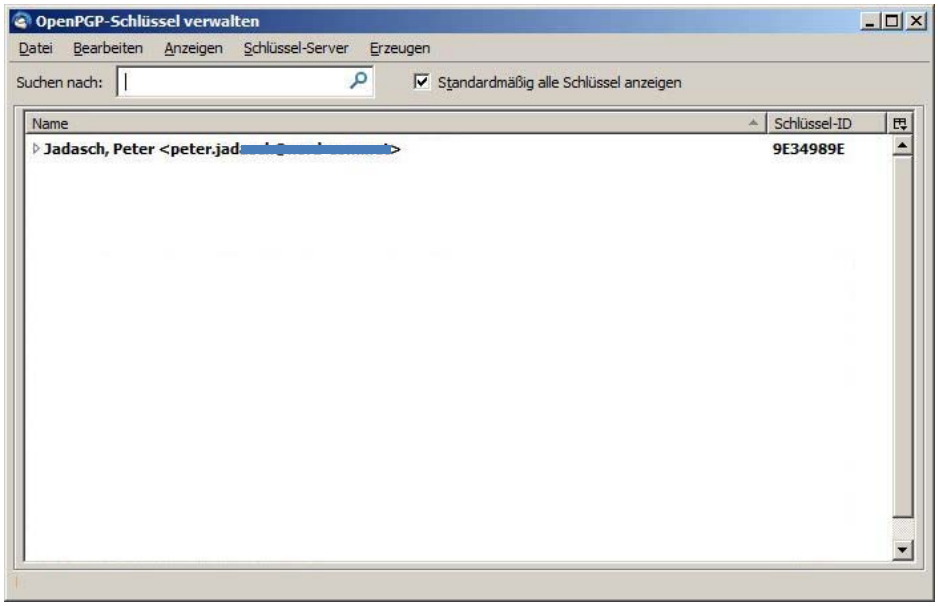
Damit ist die Einrichtung und Schlüsselerzeugung beendet.



Importieren öffentlicher Schlüssel von eMail-Partnern

Um verschlüsselt zu kommunizieren oder besser, um jemandem eine verschlüsselte eMail zukommen lassen zu können, benötigt man dessen öffentlichen Schlüssel.

Nach dem Installieren eines Mailers, dem Einrichten der eMail-Adressen, des Verschlüsselungstools Enigmail und der Schlüsselerstellung, ist das Importieren der öffentlichen Schlüssel (public key) der Kommunikationspartner der nächste Schritt.

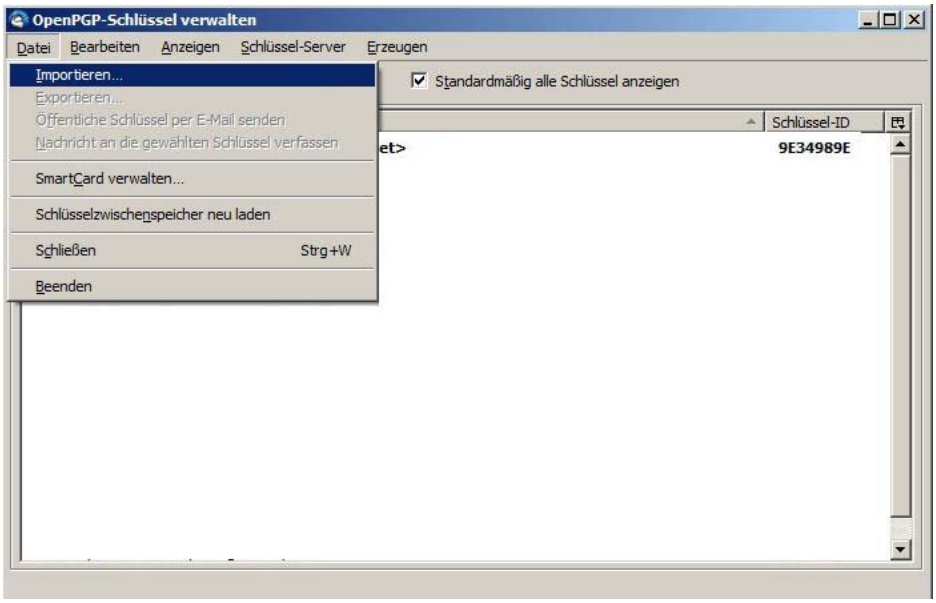


Der jeweilige Kommunikationspartner muß seinen öffentlichen Schlüssel exportieren, indem er ihn in eine einfache Textdatei kopiert. Der Schlüssel sieht dann in etwa so aus:

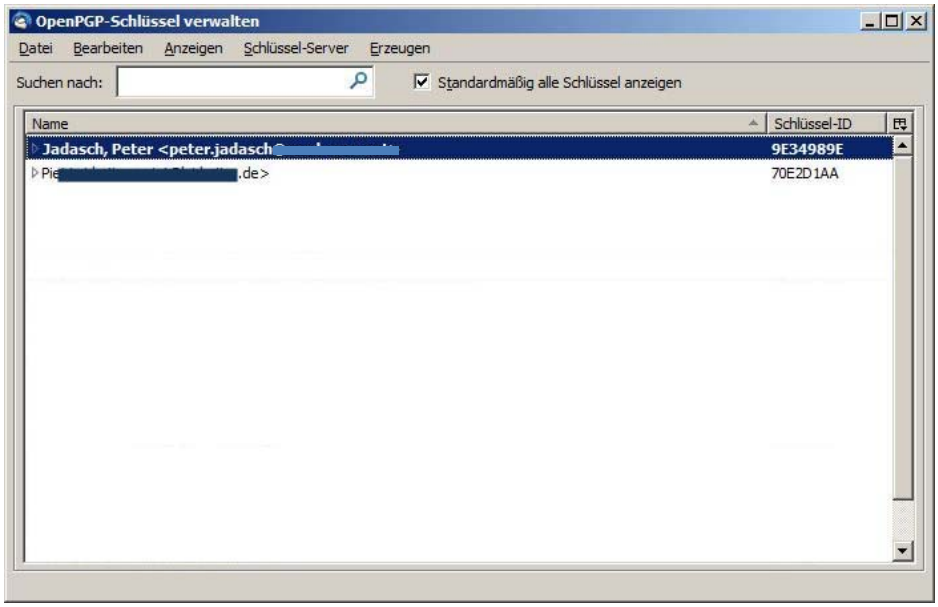
```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGP 8.0.1

mQENBD/oRxIBCACkJD2fTuJAIFf5NwHPTC8rKPvYFZv0IDI6CNW5WK5/m+kLO+o3
KEhOT7AeXl6Hooj0j1Q/od8loO5VRmHAiZMpyvh3LtHcrPOHZiBeM8JIC42XU9oG
jzyi2mgRSgJD1MVBZtBiL41fy0lysCQJtRvdlO3G4EynvyooLOxcivCTPEn9tk9E
WqIhp8hcdRVobi7nGfOWl4lIazTz2uQhQ9BjdZNiCOd4crH4Wp2dGA1xfOVKX5nW
0t4iKjgoMkvFuWC3r7uRbiREeR7pvtj8VTpLPehHseBFJ5HCJrt9+cRrRW4uYv7A
9SBU8thT3fdaxkJ8XA4h4MCPlZdA/U7oWBzfABEBAAG0NkphZGFzY2gsIFBldGVy
IElUQy1TY2hsw7xzc2VsIDxqYWRhc2NoQGl0Yy1icmVtZW4uY29tPokBLgQQAQIA
GAUCP+hHEggLCQgHAwIBCgIZAQUbAwAAAAKCRCsg8fkE2v75tbmB/9AYjPNr65K
kR1SfsX5Dw7ZLVPo6o17zGg+E8XbTui3xHVpQjuX82KHkPASiH1S2xuw+1okfxo0
z1ADCFiwwWzhPfV1y3uty9oMgP9dOQVe+q9hFhtal+Rsg7FVaLf318h/37b1HyzS
Ffa6YnmgIwIKeGLZttvWSqA9PKvemOB8gIzzQ1JdhbMHZPdK1ZCndN/Ww1QGTNNi
X6PSa+yvP7XTT8HPE0J4YF3mMy4uUBv4W6x+q4q1HBsLcpqMsQ9kPuUH927ztC37
4f/MvFCcDfsLX/AuhNAe+/bX2fAgIKS6a+PAL/jZOyJVWSSSBySnbgIZhK8JxOrn
tQ9xid55qnThuQENBD/oRxUBCADLTg3g8Pwn8q22vuCVMwbfXk2cnD/7a7CZaWaP
7zpTr40gVbprf+/YZMv55E2EWYruUeDqvKdwL0yGRqFOCQkmtNL+kkuy2GkcxzwQ
on42NVQ4UzqRq2m1q0P187gpw7Cd7DkE4Z50J+852o8vMMqmX6u9HfzDEWkEhqgP
AAZKGxFfVH19Q4ayuYMzTEMYd8XL2MrKSLZG/rgsACHmL/R3PAwCOtGiKNDcTSsa
3t2NJRiFMAp5z7Pvxu61tdekMdhK1dXngHr+bK9ikABQuKBnNvbekuJygch44OpZ
i+tq/prIQiiecXrPo9DLFMpbL+DTFe7+ktRcm/oE2DSzesAJABEBAAGJASIEGAEC
AAwFAj/oRxUFGwwAAAAACgkQrIPH5BNr++adGwf+Opmd4bhveiYHFGPlzAxDGN96
FMmCWDS3goms4CkLGeb2oXbWSH1WgE9YGBYxe7CBi04ZBxnPBgJ0NvxnUY4nFPsw
FRwkDdlZJ1AsoGKGCar9HAoix71PAeHnKYUkdwy5vacqr9F77yA/xcR3/lmSUeJo
fVgCEE2pQezAmaPSaeM+e9w1DYnkceulVK/h8GDN/wk4WxTtZTPFmLCg5Ei2aoom
GW1CapKS5AFsDNqCCXQjXpkVQ0ivcqF+K/IkhXaqN+OIfA42CwioEYFTiPy3Frep
kMZ4tfFT+rnlUOxC6XrrV2gpDNcwZ+Mtq39SWb7cHRuPtNFpcveYu6AUDajMiw==
=1LFP
-----END PGP PUBLIC KEY BLOCK-----
```

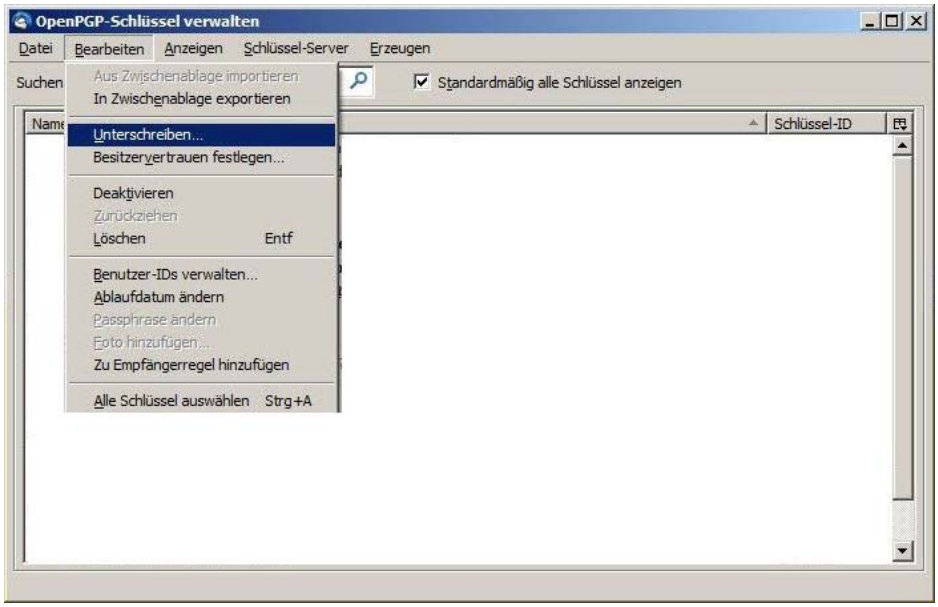
Wird die Datei dann als {Name}_pubkey.asc abgespeichert und offen (z.B. per eMail) versendet, kann sie beim Kommunikationspartner über die Importfunktion in seine Schlüsselverwaltung übernommen werden.

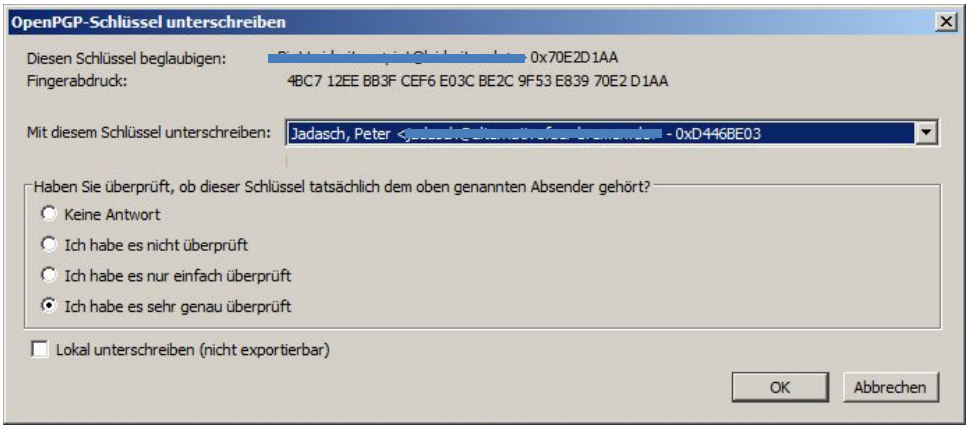


Ist der öffentliche Schlüssel in der Schlüsselverwaltung (oder auch Schlüsselbund) eingetragen, muß vor der ersten Verwendung die Gültigkeit bestätigt werden und wie weit dem Schlüsselinhaber vertraut wird.

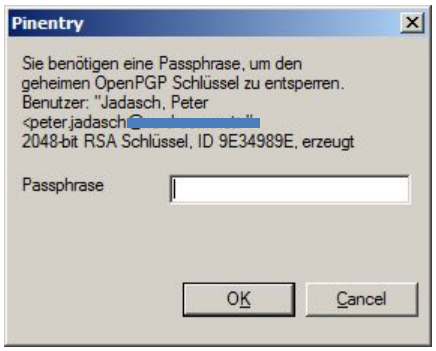


Dazu ruft man im Menü unter Bearbeiten den Punkt Unterschreiben auf.

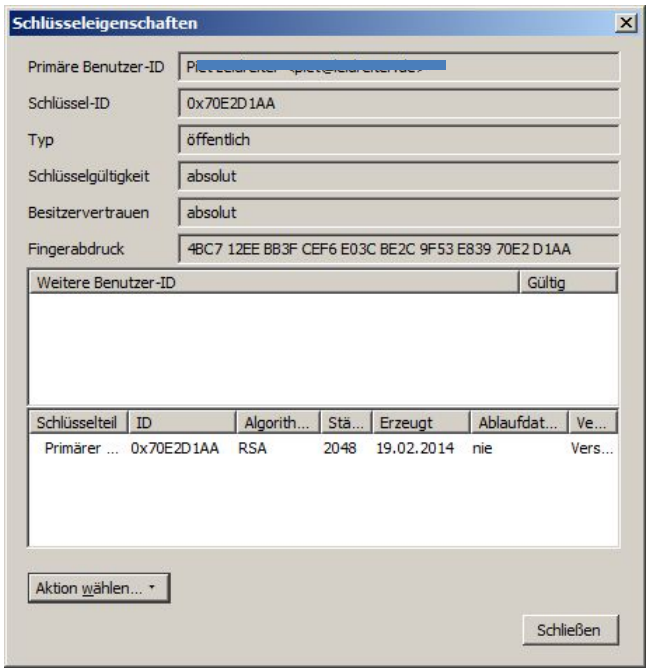




Mit dem Signieren eines fremden Schlüssels wird die Benutzung des Schlüssels freigeschaltet und man stellt dem Schlüsselinhaber einen Vertrauensbeweis aus. Wird dazu noch das Feld Lokal unterschreiben leer gelassen, kann der Schlüssel mit dieser Signatur weitergegeben werden. Dann kann jeder der den Schlüssel erhält, sehen, wer dem Schlüsselbesitzer das Vertrauen ausspricht. Das ist in diesem Sinne auch so gewollt, denn je mehr Signaturen ein Schlüssel hat und je mehr Menschen mit ihrer Signatur das Vertrauen bestätigt haben, desto vertrauenswürdiger wird der Schlüsselbesitzer sein und je glaubwürdiger ist für einen Fremden, daß dieser Schlüssel wirklich der ausgewiesenen Person gehört. Dieses Verfahren zeigt somit ebenso wie ein von einer CA[1] ausgegebenes Zertifikat ein Vertrauensstatus an. Es nennt sich Netz des Vertrauens (Web of trust).

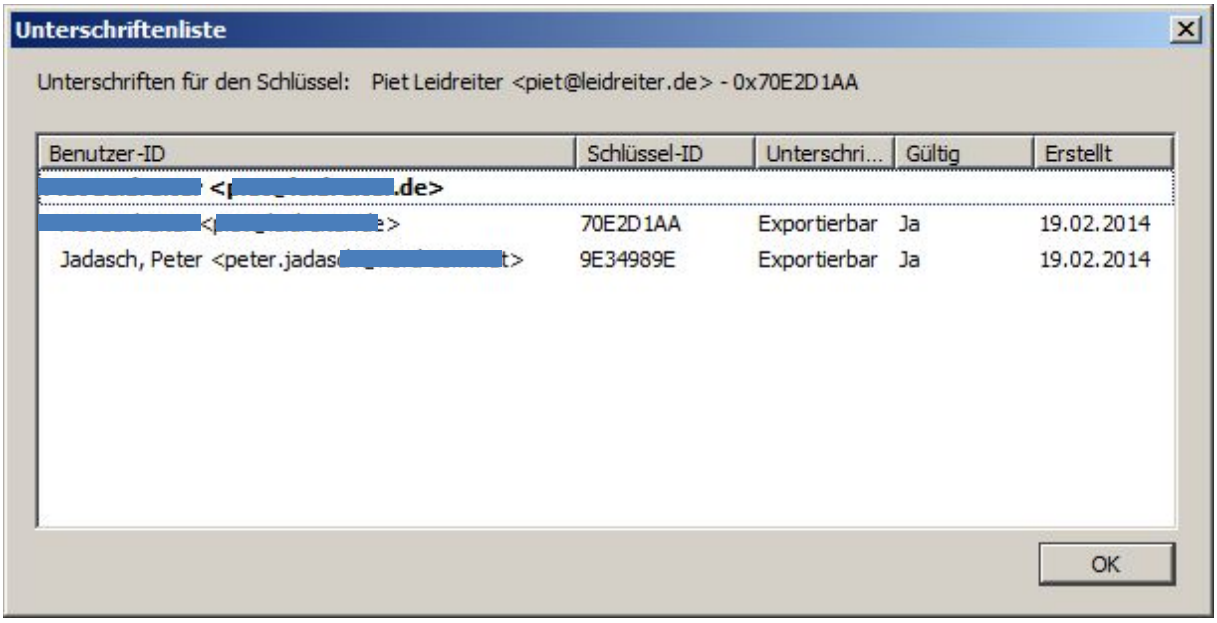


Nachdem geklärt ist, wie genau der Schlüssel geprüft wurde, wird mit OK die Eingabe der eigenen Paßphrase angefragt. Danach ist der Schlüssel signiert. Dies ist überprüfbar, wenn der entsprechende Schlüssel markiert ist und mit der rechten Maustaste das Kontextmenü aufgerufen wird. Dort ist der letzte Menüpunkt Schlüsseleigenschaften.



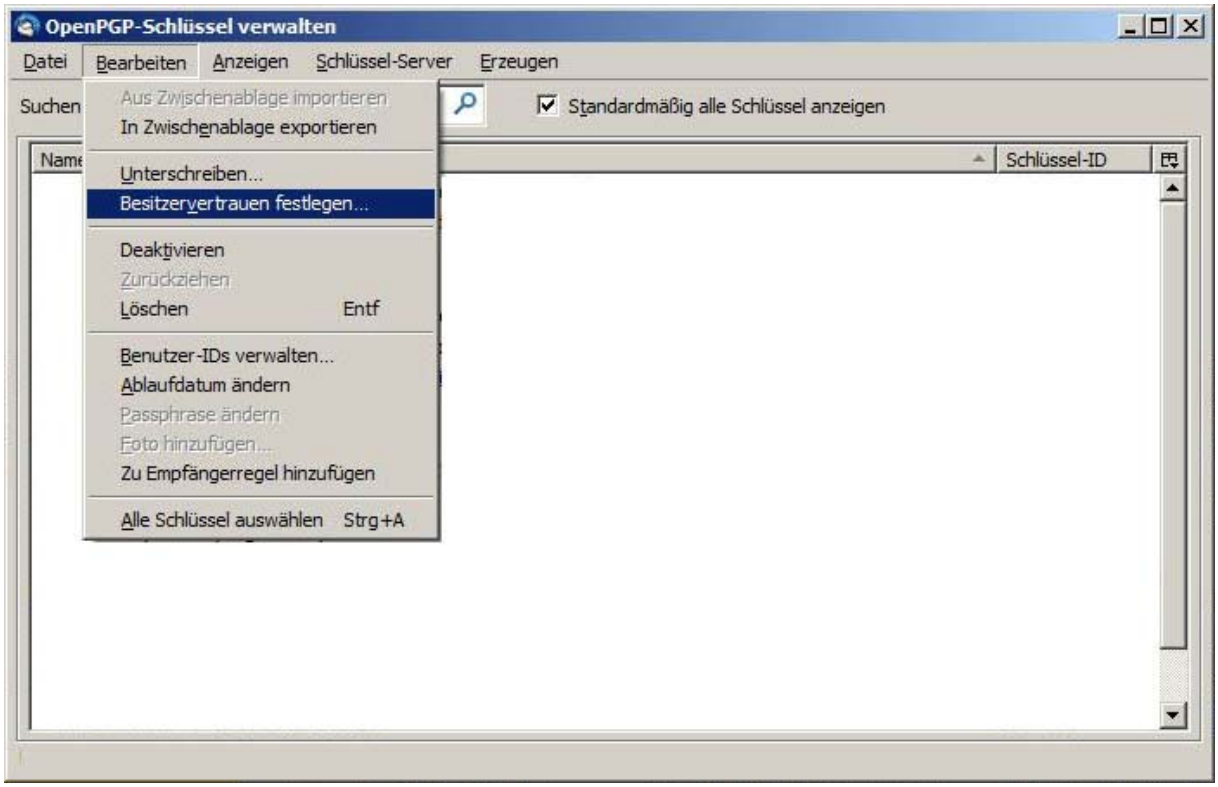
Wird nun gewünscht die Unterschriften zu sehen wer diesem Schlüsselbesitzer alles vertraut, kann beim Pull down Menü "Aktion wählen" den Menüpunkt "Unterschriften anzeigen" wählen und bekommt dann alle Signaturen dieses Schlüssels angezeigt.

[1] CA = Certification Authority oder Zertifizierungsinstanz (TrustCenter)



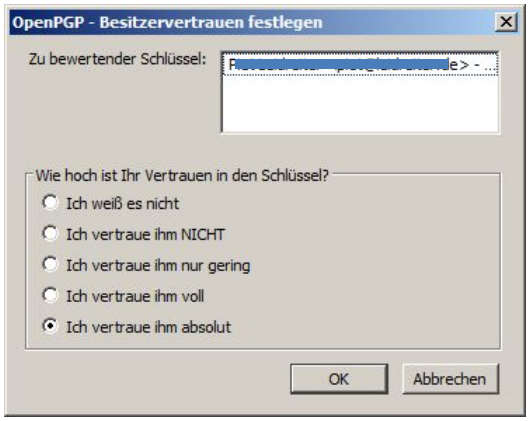
Einstellen des Vertrauensstatus

Da das signieren von eMails beim Versenden sehr automatisiert stattfindet, sind Voreinstellungen vorzunehmen, die ohne weiteren Eingriff das Versenden ermöglichen. Dazu gehört das Einstellen der Vertrauensstellung des jeweiligen Kommunikationspartners.



Das Vertrauen in einen Schlüssel oder auch das Besitzer-Vertrauen genannt, legt fest in wie weit dem Besitzer des Schlüssels vertraut wird. Das bedeutet auch, daß Schlüssel, die von einem Besitzer unterschrieben wurden, die gleiche Vertrauensstufe erhalten wie der jeweilige Besitzer selbst. Um das Besitzervertrauen eines Schlüssels festzulegen, wird im Schlüssel-Verwaltungstool der Schlüssel

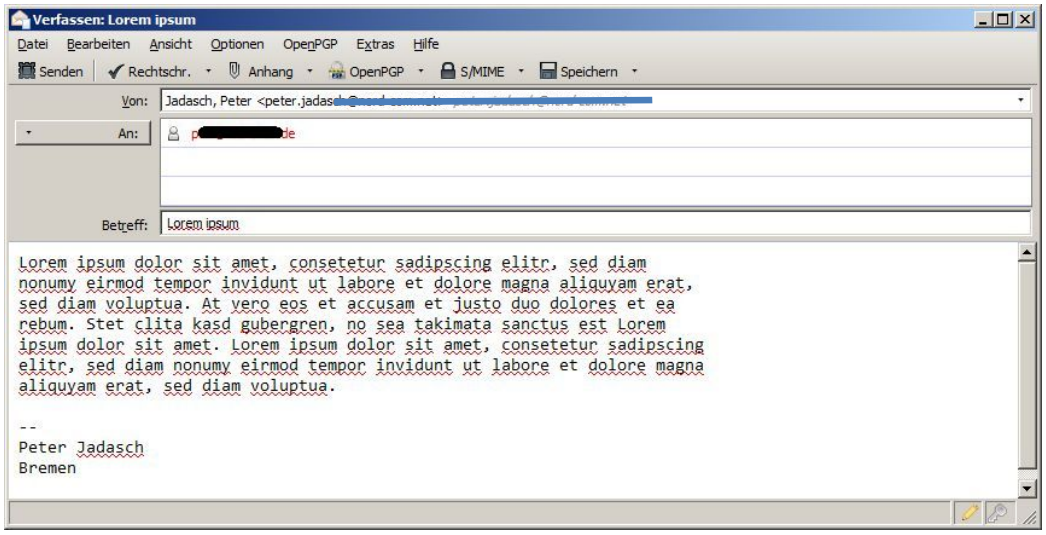
ausgewählt und dann über den Menüpunkt Bearbeiten dort der Menüpunkt Besitzervertrauen festlegen gewählt.



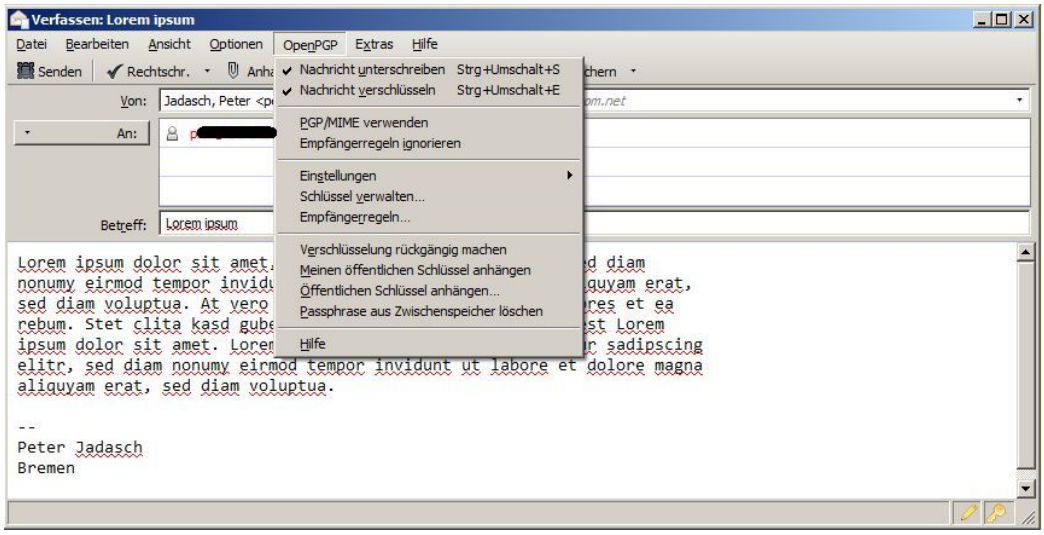
In dem dann folgenden Fenster wird eine der fünf Vertrauensstufen ausgewählt. Nachdem Sie auf Ok geklickt haben, wird im Schlüssel-Verwaltungstool in der Spalte Besitzer-Vertrauen das Vertrauen in den Besitzer angezeigt.

Versenden von verschlüsselter eMail

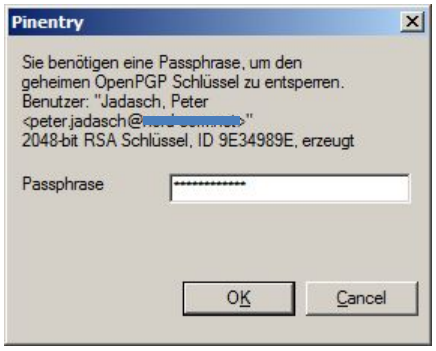
Der Schlüssel des Adressaten ist mit der eMail-Adresse verbunden und wird bei Auswahl der Adresse auch aufgerufen.



Werden nun unter dem Menüpunkt OpenPGP die beiden Menüpunkte "Nachricht unterschreiben" und/oder "Nachricht verschlüsseln" ausgewählt, wird beim betätigen von Senden die Mail verschlüsselt und das Fenster zur Eingabe der Paßphrase geht auf (siehe die folgenden beiden Abbildungen).

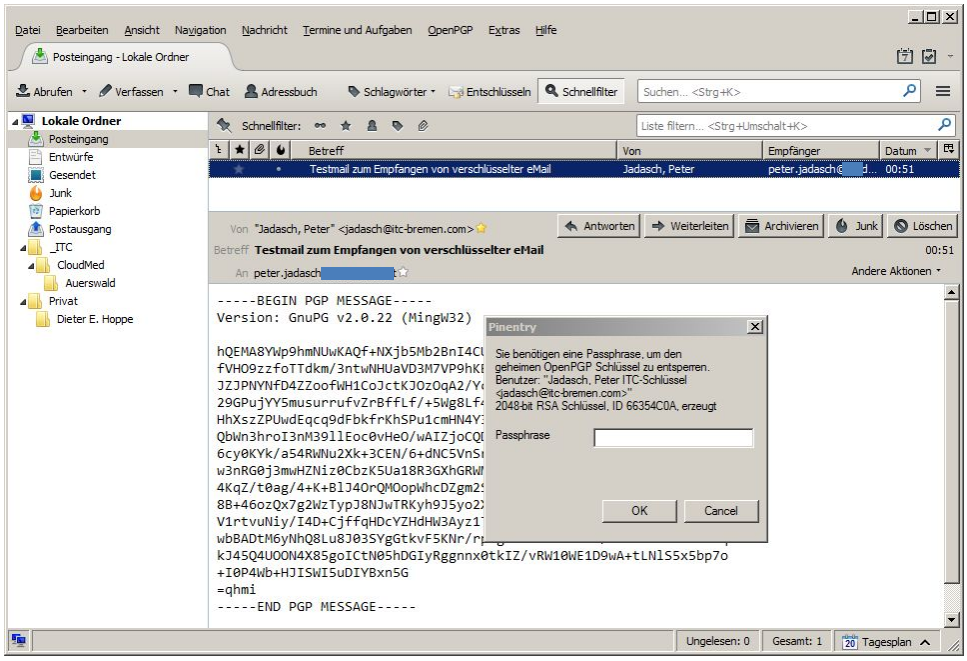


Nach Eingabe der Paßphrase wird die eMail verschlüsselt versendet.

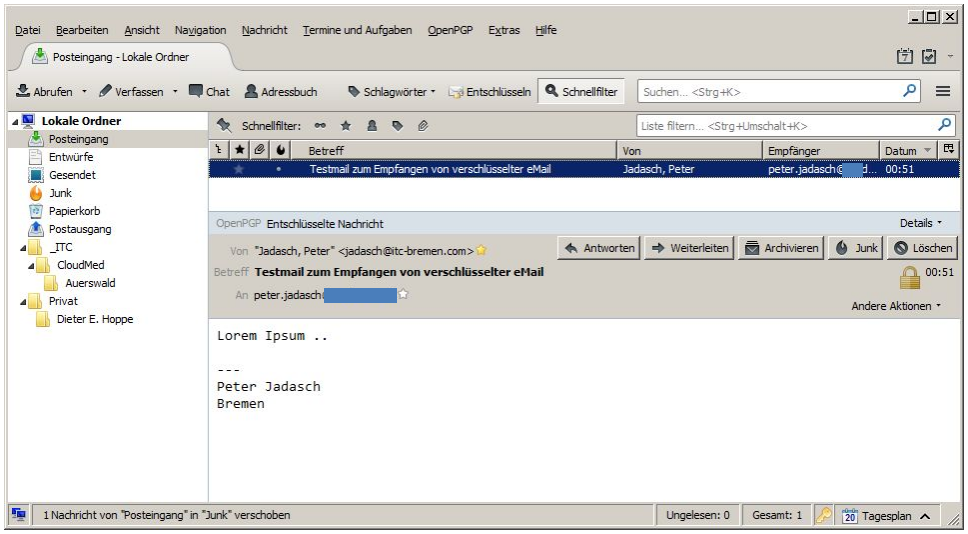


Empfangen von verschlüsselter eMail

Wird eine eMail verschlüsselt empfangen, muß sie zur Entschlüsselung in der Liste markiert werden.



Mit einem Doppelklick öffnet sich das Fenster zur Eingabe der Paßphrase und nach der Eingabe erscheint die Mail im Klartext. Sie läßt sich dann im Klartext abspeichern.



Bremen im Februar 2014

peter jadasch

Dieses Dokument ist nach besten Wissen und Gewissen erstellt worden. Trotzdem ist es möglich, daß es nicht fehlerfrei ist. Für die Befolgung der GPG4Win-Anleitung oben wird jede Haftung daher ausgeschlossen. Deshalb ist die Referenz das Kompendium von der Downloadseite …
http://gpg4win.de/doc/de/gpg4win-compendium.html
oder nachfolgende Versionen.