Beschreibung der Einrichtung von PGP zur Kommunikation mit der Bayerischen Verwaltung

Stand: April 2006

I Inhaltsverzeichnis

II Begriffe und Abkürzungen[1]

PGP ***Pretty Good Privacy***

PGP ist ein bekanntes und sehr leistungsfähiges Verschlüsselungsprogramm, das hauptsächlich für E-Mails verwendet wird. Eine Entschlüsselung ist der Zielstelle nur möglich, wenn sie über den privaten Schlüssel verfügt.

PKI ***Public Key Infrastructure***

PKI erlaubt es Nutzern eines normalerweise unsicheren Netzwerkes (z.B. Internet), Daten und Informationen sicher auszutauschen. Das geschieht unter Verwendung eines privaten und eines öffentlichen Schlüssels. Beide Schlüssel werden mit demselben Algorithmus erzeugt, wobei der öffentliche nur zum Verschlüsseln geeignet ist. Mit dem privaten Schlüssel wird die Nachricht wieder entschlüsselt. Die bekannteste PKI ist PGP.

Verschlüsselung Als Verschlüsselung wird die Codierung von Daten zum Schutz vor unbefugten Zugriffen bezeichnet.

Kryptografie Unter Kryptographie versteht man die Verschlüsselung von Daten (Datenverschlüsselung) unter Verwendung komplexer Algorithmen, um sie vor unberechtigter Einsicht durch Dritte zu schützen. Gängige Verschlüsselungsmethoden sind das Vertauschen oder Ersetzen von Zeichen; oft wird auch noch ein Passwort als zusätzlicher Schutz eingesetzt. Die Sicherheit der Daten hängt vor allem von der Länge des verwendeten Schlüssels ab. Gängig ist heute ein 128-Bit-Schlüssel, den Hochleistungsrechensysteme erst nach mehreren Jahren Berechnungszeit knacken könnten. Im Internet hat die Verschlüsselung persönlicher Daten (E-Mails) in letzter Zeit immer mehr an Bedeutung gewonnen.

asymmetrische Verschlüsselung Verschlüsselungsverfahren, bei dem mit unterschiedlichen Schlüsseln ver- bzw. entschlüsselt wird.

Private Key ***Privater Schlüssel,*** nur dem Teilnehmer zugänglich, dient zum Entschlüsseln von Nachrichten und/oder zum digitalen Signieren.

Public Key ***Öffentlicher Schlüssel,*** allen Teilnehmern einer PKI bekannter Schlüssel, dient zum Verschlüsseln von Nachrichten und/oder zum Verifizieren einer digitalen Signatur.

Vertraulichkeit Unberechtigte Dritte können eine Nachricht nicht einsehen.

Digitale / elektronische Signatur Verfahren zur Anbringung von Unterschriften an elektronischen Dokumenten

[1] z T. aus „*Das M+T Computerlexikon“*, München: Markt+ Technik 2002.

1. Einführung

Das vorliegende Dokument soll Ihnen erläutern, wie eine sichere Kommunikation mit der Bayerischen Verwaltung eingerichtet und durchgeführt werden kann. Dabei wird im ersten Abschnitt auf die Intentionen einer sicheren Kommunikation eingegangen und Ihnen wird ein Produkt vorgestellt, welches sichere Kommunikation ermöglicht.
Der zweite Abschnitt befasst sich mit der Installation und Einstellung des Produktes, um sichere Kommunikation mit der Verwaltung nutzen zu können. Im dritten Teil schließlich wird beschrieben, wie Sie das vorgestellte Produkt nutzen können.

1.1 Kommunikation zwischen Bürger und Verwaltung

Die Bayerische Verwaltung hat es sich zur Aufgabe gemacht, die Technologien, die die neuen Medien (Computer, Internet etc.) zur Verfügung stellen, zu nutzen und so eine höhere Bürgernähe zu erreichen. Ziel dieser eGovernment-Initiative ist es, den Kontakt von Bürgern und Wirtschaft mit der Verwaltung und der Justiz auch online anzubieten. Um dem Informationsaustausch zwischen Bürger und Verwaltung ein höchstes Maß an Sicherheit zukommen zu lassen, ist es nötig den Informationsaustausch soweit abzusichern, dass nur berechtigte Personen Zugang zu den überlassenen Informationen haben. Dazu ist u.a. eine sichere Übertragung von E-Mails nötig.

Das vorliegende Dokument zeigt Ihnen eine Lösung zur sicheren Kommunikation mit den Bayerischen Behörden auf.

1.2 Was ist PGP

E-Mails passieren auf ihrem Weg vom Versender zum Empfänger verschiedenste Rechnersysteme. Wenn Sie unverschlüsselte E-Mails versenden, so ist es ohne größere Probleme möglich, diese E-Mails mitzulesen. Sie können eine unverschlüsselte E-Mail mit einer Postkarte vergleichen. Die Postkarte kann auf ihrem Weg vom Versender zum Empfänger von jedem gelesen werden, der in Kontakt mut der Postkarte kommt. Mit dem Programm PGP (Pretty Good Privacy) haben Sie die Möglichkeit E-Mails so zu verschlüsseln, dass nur der explizit angegebene Empfänger mit seinem Schlüssel die Nachricht wieder entschlüsseln und lesen kann.

PGP benutzt ein Public-Key Verfahren zur Verschlüsselung (d.h. unterschiedliche Schlüssel für Ver- und Entschlüsselung). Jeder Nutzer erstellt sich ein Schlüsselpaar bestehend aus dem öffentlichen Schlüssel (**Public Key**) und seinem privaten Schlüssel (**Private Key**). Der private Schlüssel ist der „geheime“ Schlüssel. Er entschlüsselt die Nachrichten die an Sie gesendet werden. Es darf niemand sonst Zugang zu diesem Schlüssel haben. Der öffentliche Schlüssel hingegen kann bzw. muss sogar weitergegeben werden. Dies ist möglich, in dem Sie Ihren öffentlichen Schlüssel in speziellen Verzeichnissen publik machen oder indem Sie diesen Schlüssel mit Ihren E-Mails verteilen (es wir zu einem späteren Zeitpunkt näher hierauf eingegangen). Dieses Vorgehen ist nötig, damit Ihnen jemand eine verschlüsselte E-Mail senden kann. Zusammengefasst bedeutet dies: **Mit Ihrem öffentlichen Schlüssel werden Nachrichten an Sie verschlüsselt, mit Ihrem privaten Schlüssel entschlüsseln Sie Nachrichten, die mit Ihrem öffentlichen Schlüssel verschlüsselt wurden.**

Dieses Dokument soll Ihnen beschreiben, wie Sie mit Hilfe der privaten und öffentlichen Schlüssel sicher mit der Bayerischen Verwaltung per E-Mail kommunizieren können.

1.3 Warum gerade PGP

Die Hauptgründe zur Nutzung von „Pretty Good Privacy“ (PGP) im privaten Gebrauch sind zum einen der Aspekt, dass das Programm kostenlos zur Verfügung steht, des Weiteren liegt die Schlüsselgenerierung in der Hand des Nutzers und muss nicht entgeltlich durch einen dritten erfolgen (dies ist zum Beispiel bei S/MIME der Fall).

Weiterhin lässt sich feststellen, dass PGP im Internet seit Jahren ein anerkannt sicherer De-facto-Standard für authentische und vertrauliche E-Mail ist.

1.4 Bezug von PGP

Hauptbezugsquelle von PGP für Privatpersonen stellt das Internet dar. Auf der Homepage des Herstellers von PGP-Software wird das Produkt zur Verfügung gestellt. Auf http://www.pgp.com/products/de/ finden Sie die Produkte mit deutscher Menüführung.

1.4.1 PGP Freeware 8.01 DE

Die für Privatanwender kostenfreie Version von PGP finden Sie unter der Adresse http://www.pgp.com/products/de/freeware.html. Die folgende Beschreibung bezieht sich ausschließlich auf diese Freeware-Version.

1.4.2 Unterschiede zu anderen Versionen

Hauptunterschied der Freeware-Version zu den kostenpflichtigen PGP Produkten besteht in den fehlenden Plug-Ins für verschiedene Mailprogramme. Diese Plug-Ins ermöglichen es komfortabel E-Mails zu verschlüsseln, da sie sich direkt in die Mailprogramme integrieren. Die Verschlüsselung mit der Freewareversion wird auf einem anderen Weg durchgeführt, ist aber ebenso effektiv.
Neben den Plug-Ins bietet die Vollversion auch die Möglichkeit ganze Laufwerke zu verschlüsseln. Für nähere Informationen zu den verschiedenen Produkten können Sie die Homepage von PGP (http://www.pgp.com) zu Rate ziehen.

1.4.3 Empfehlung

Sind Sie erst einmal nur daran interessiert E-Mails zu verschlüsseln, ist es ratsam vorerst die kostenfreie Freewareversion zu nutzen. Sollten Sie zu einem späteren Zeitpunkt Bedarf an den Möglichkeiten der Vollversion haben, können Sie diese immer noch erwerben und Ihre vorhandenen Einstellungen übernehmen.

2. Installation und Einstellung von PGP

2.1. Installation von PGP

Bei der hier dargestellten Installation handelt es sich um PGP in der Version 8.0.1 mit deutscher Menüführung. Die Installation wird für eine Microsoft Windows Umgebung beschrieben. Eine ältere Version von PGP bzw. die Installation unter anderen Betriebssystemen kann von der hier beschriebenen Vorgehensweise abweichen. Für diesen Fall hält die Internetseite http://www.pgpsupport.com/ Installationsanleitungen bereit. Dabei ist jedoch zu beachten, dass diese in englischer Sprache verfasst sind.

2.1.1 Systemvoraussetzungen

Die PGP Corporation selbst gibt folgende Mindestsystemvoraussetzungen an:

- Pentium 166 oder ein höherer Prozessor
- Windows 98, Windows Millennium Edition (ME), Windows NT 4.0 (Service Pack 6a), Windows 2000 (Service Pack 3), Windows XP (Service Pack 1)
- 32 MB physikalischer RAM-Speicher
- 32 MB Festplattenspeicher

2.1.2 Die Installationsroutine

Zur Zeit der Erstellung dieser Dokumentation stand das PGP-Programm als ZIP-Datei auf der Homepage des Herstellers bereit. Diese Datei stellt ein gepacktes Verzeichnis dar, welches weitere Dateien enthält. Um dieses Verzeichnis wieder zugänglich zu machen, ist es nötig die ZIP-Datei zu entpacken. Wenn Sie Windows XP nutzen ist dieser Dienst bereits integriert und Sie können sich durch einen Doppelklick auf die ZIP-Datei deren Inhalt anzeigen lassen. Nutzen Sie eine ältere Version von Windows, müssen Sie zuerst ein Programm installieren, welches Ihnen die Möglichkeit gibt das Archiv zu öffnen. Programme hierfür sind z.B. WinZip oder WinRAR. Nähere Informationen finden Sie auf den Webseiten: http://www.winrar.de/ , http://www.winzip.de/ .

Zum Starten der Installation entpacken Sie bitte das herunter geladene ZIP-Archiv in ein beliebiges Verzeichnis. Anschließend starten Sie die Installation durch Doppelklick auf die Datei ***PGP8.EXE***.

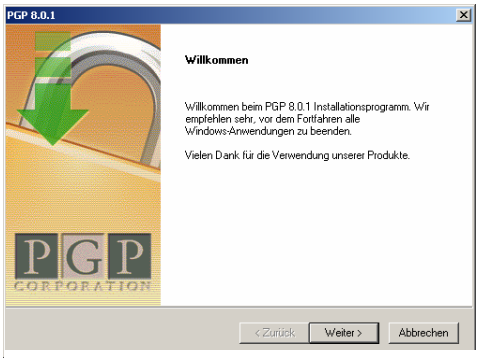

Abbildung 1: Willkommen

Nachdem das Programm die Installation vorbereitet hat, sehen Sie nebenstehendes Willkommensfenster. Um zum nächsten Schritt zu gelangen klicken Sie auf ***Weiter*.**

Das nun erscheinende Fenster zeigt Ihnen die Lizenzvereinbarung zur Nutzung von PGP an. Um die Installation fortzusetzen, lesen Sie sich die Vereinbarung durch und akzeptieren Sie diese mit ***Ja***.

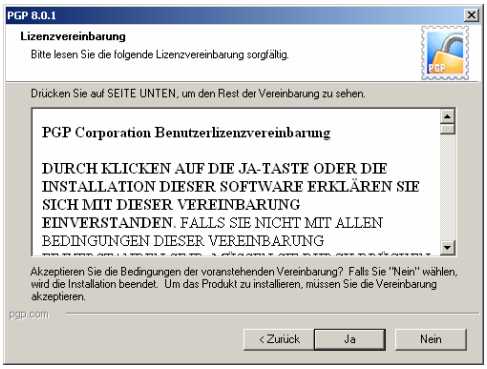

Abbildung 2: Lizenzvereinbarung

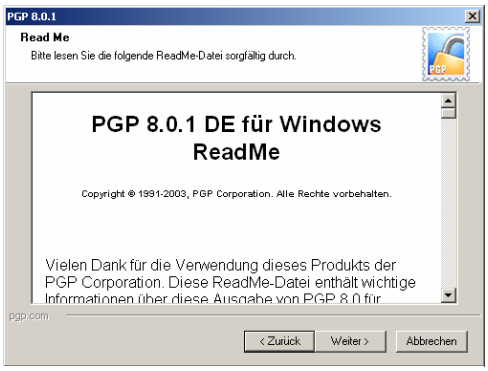

Abbildung 3: ReadMe

Lesen Sie sich die „PGP 8.0.1 DE für Windows ReadMe“ durch und gehen Sie auf ***Weiter*** um die Installation fortzusetzen.

Das ReadMe enthält u.a. Informationen über: Funktionen in PGP 8.0 für Windows, Änderungen seit PGP 8.0, Systemanforderungen, Lizenzvergabe, Installationsanweisungen, Zusätzliche Informationen, Dokumentation, Kontaktaufnahme mit der PGP Corporation und dem Copyright;

Bei Benutzertyp geben Sie an, dass Sie ein „***neuer Benutzer***“ sind. Dies ist nötig um Ihren PGP-Schlüssel erstellen zu können. Sollten Sie bereits PGP-Schlüssel besitzen, so können Sie diese importieren in dem Sie jetzt angeben **„Ja, ich habe Schlüsselbunde“**. Für die weitere Beschreibung wird davon ausgegangen, dass Sie neue Schlüssel erstellen müssen. Klicken Sie auf ***Weiter***, um die Installation fortzusetzen.

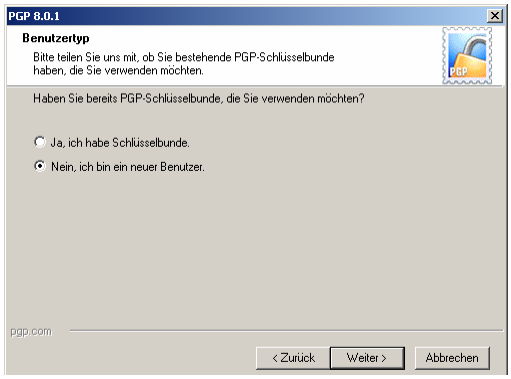

Abbildung 4: Benutzertyp

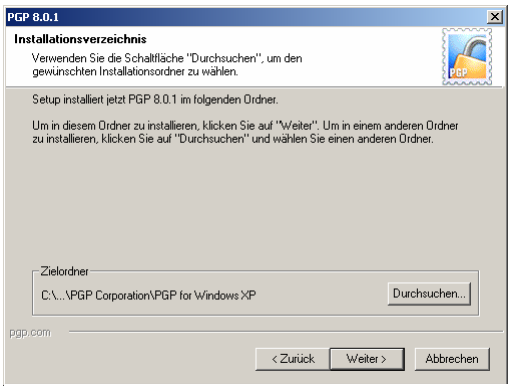

Abbildung 5: Installationsverzeichnis

Um das vom System vorgeschlagene Installationsverzeichnis zu akzeptieren gehen Sie auf ***Weiter***. Sie können den Installationspfad auch anpassen, indem Sie auf ***Durchsuchen*** klicken und Angeben, wohin PGP installiert werden soll.

Nun können Sie die Komponenten wählen, die installiert werden sollen. Arbeiten Sie mit der Freewareversion, also ohne Lizenznummer, wird empfohlen <u>alle bereits gesetzten Häkchen zu deaktivieren</u> (einfach auf das gesetzte Häkchen klicken). Dies ist erforderlich, um Fehlermeldungen in Outlook, Outlook Express etc. aufgrund fehlender Lizenz zu vermeiden. Nach Ihrer Auswahl gehen Sie auf ***Weiter***.

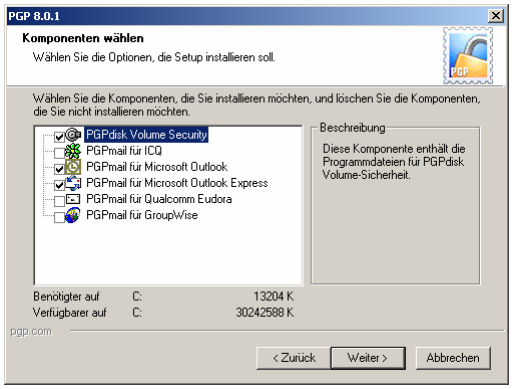

Abbildung 6: Komponenten auswählen

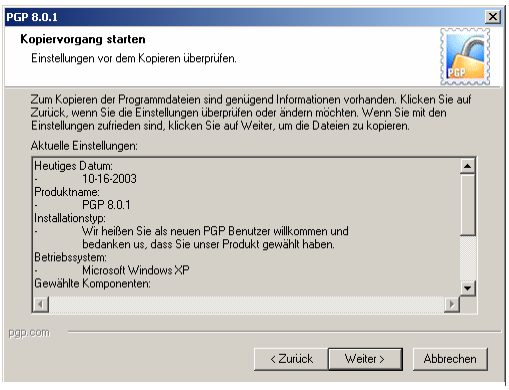

Abbildung 7: Kopiervorgang starten

Das Installationsprogramm zeigt Ihnen nun noch einmal die getroffenen Einstellungen an. Um diese zu akzeptieren und den Kopiervorgang zu starten gehen Sie auf ***Weiter***.

Die erforderlichen Dateien werden nun auf die Festplatte überspielt.

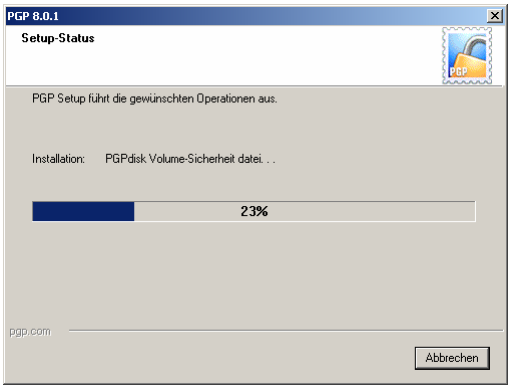

Abbildung 8: Setup-Status

Abbildung 9: Installation beendet

Nachdem alle erforderlichen Dateien kopiert sind, ist zum Abschluss der Installation ein Neustart des Computers erforderlich. Um diesen Neustart durchzuführen klicken Sie auf ***Fertigstellen***.

Die Installation ist an dieser Stelle beendet. Im nächsten Abschnitt wird beschrieben, wie Sie PGP einrichten und benutzen können.

2.2 PGP – der erste Programmstart

Nachdem Sie PGP wie im Abschnitt 2.1.2 installiert und Ihr System neu gestartet haben, werden Sie feststellen, dass sich im Infobereich Ihrer Taskleiste ein neues Symbol etabliert hat:  .

Dieses **„PGPtray“** dient quasi als „Kommandozentrale“ für Ihre zukünftigen PGP-Aktivitäten.

Auch unter ***Start ➔ Programme*** hat die Installationsroutine von PGP eine Programmgruppe eingerichtet.

Abbildung 10: Start → Programme → PGP

In der Regel wird nach dem Neustart nebenstehende „PGP-Lizenzautorisierung“ erscheinen. Da Sie zur Nutzung der Freewareversion keinen Lizenzschlüssel benötigen, schließen Sie dieses Fenster durch Betätigen der Schaltfläche ***Später***.

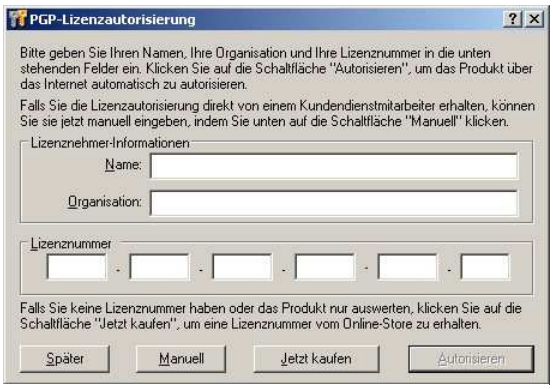

Abbildung 11: PGP-Lizenzautorisierung

2.2.1 Erzeugung eines Schlüsselpaares

Ist der PGP-Schlüsselerstellungs-Assistent bereits gestartet, können Sie auf Seite 13 ab Abbildung 14: **PGP Schlüsselerstellungs-Assistent** fortsetzen.

Sollte der Assistent nicht starten, können Sie diesen manuell aufrufen, indem Sie nachfolgende Schritte ausführen.

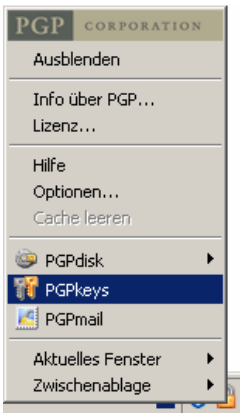

Abbildung 12:
Start PGPkeys

Zur Erstellung eines Schlüsselpaares, bestehend aus privatem und öffentlichem Schlüssel, starten Sie ***PGPkeys*** z.B. aus dem PGP-Tray heraus.

Anschließend gehen Sie auf den Menüpunkt ***Schlüssel ➔ Neuer Schlüssel,*** um den PGP-Schlüsselerstellungs-Assistent zu starten.

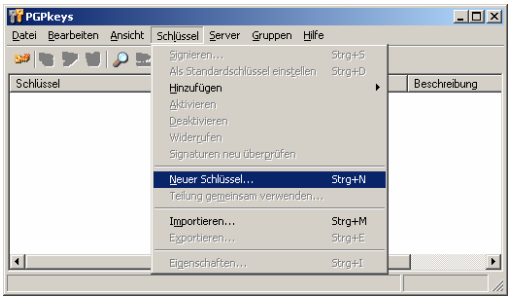

Abbildung 13: PGPkeys - Neuer Schlüssel

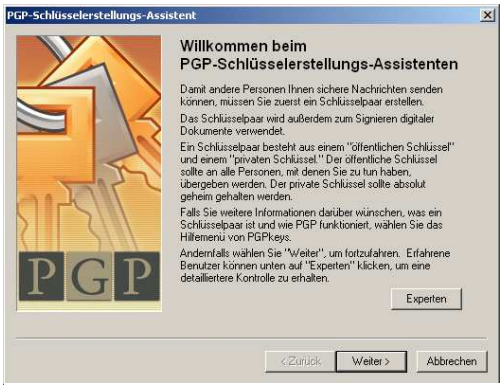

Abbildung 14: PGP Schlüsselerstellungs-Assistent

Nachdem der Assistent gestartet ist, klicken Sie auf ***Weiter***, um die Schlüsselerstellung fortzusetzen. (Die Einstellungen unter ***Experten*** sind an dieser Stelle nicht von Bedeutung, da nur mit den Standardeinstellungen gearbeitet wird.)

Im nächsten Fenster geben Sie Ihren vollständigen Namen und Ihre E-Mail Adresse an. Anschließend auf ***Weiter*** klicken, um den Vorgang fortzusetzen.

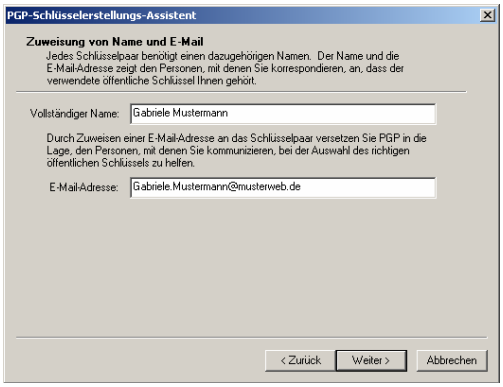

Abbildung 15: Zuweisung von Name und E-Mail

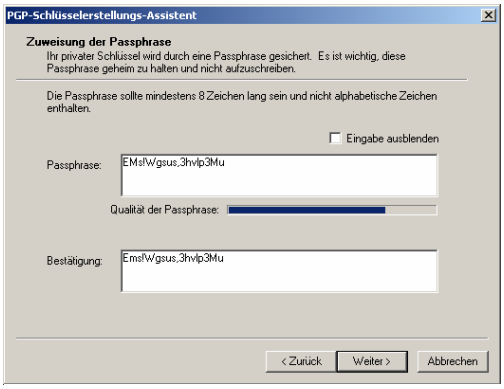

Abbildung 16: Zuweisung der Passphrase

Denken Sie sich ein Passwort aus und geben Sie dieses als „Passphrase“ an. Für nähere Informationen zur Erstellung einer geeigneten Passphrase erhalten Sie auf Seite 16 im Abschnitt **„Exkurs: Tipps zur Wahl der Passphrase“** mehr Informationen.

Bestätigen Sie das eingegebene Kennwort durch eine nochmalige Eingabe im Feld **Bestätigung**. Das von Ihnen gewählte Passwort sollte mindestens 8 Zeichen lang sein und sowohl aus Groß- und Kleinbuchstaben bestehen, als auch Zahlen und Sonderzeichen enthalten. Um die Passworteingabe sichtbar zu machen, deaktivieren Sie das Häkchen im Kästchen ***Eingabe Ausblenden***. Ein Klick auf ***Weiter*** startet die Schlüsselgenerierung.

Nach erfolgreicher Erstellung Ihres Schlüsselpaares erscheint nebenstehendes Fenster. Bestätigen Sie die Kenntnisnahme durch einen Klick auf ***Weiter***.

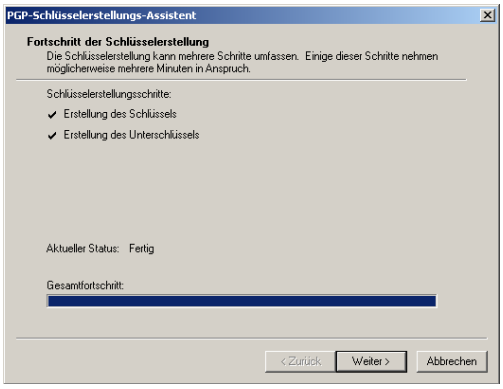

Abbildung 17: Fortschritt der Schlüsselerstellung

Abbildung 18: Beenden des Schlüsse-lerstellungs-Assistenten

Der PGP Schlüsselerstellungs-Assistent hat nun ein auf Sie festgelegtes Schlüsselpaar erstellt. Um den Assistenten zu beenden, drücken Sie auf ***Fertigstellen***.

Haben Sie die Schlüsselgenerierung selbst initiiert, erscheint Ihr Schlüssel in der PGPkeys-Anzeige, ähnlich der Abbildung 19: PGPkeys mit eigenem Schlüssel.

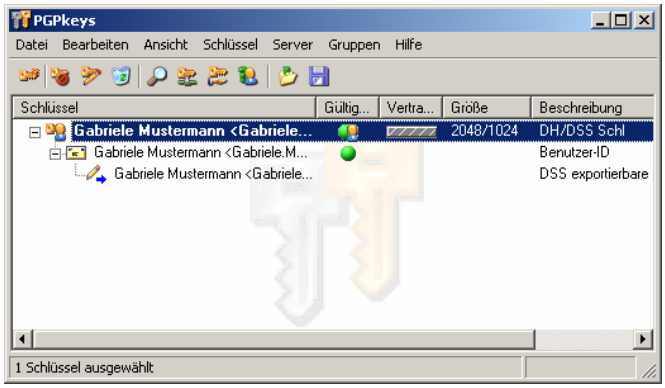

Abbildung 19: PGPkeys mit eigenem Schlüssel

Nachfolgend sehen Sie die unterschiedlichen Symbole und deren Bedeutung, die neben einem Schlüssel in PGPkeys vorkommen können.

- Sie besitzen den privaten und öffentlichen Schlüssel
- Sie besitzen den öffentlichen Schlüssel
- Der Schlüssel wurde widerrufen
- Der Gültigkeitszeitraum des Schlüssels ist abgelaufen

Exkurs: Tipps zur Wahl der Passphrase

Anders als Sie es vielleicht aus anderen Anwendungen oder dem Sprachgebrauch kennen, hat sich im PGP-Umfeld der Begriff Passphrase als Synonym für Passwort bzw. Kennwort durchgesetzt. Diese Wortwahl soll verdeutlichen, dass ein einzelnes Wort keine ausreichende Sicherheit bildet. Die Sicherheit und der Nutzen von PGP basiert auf der Geheimhaltung und der wohl überlegten Wahl einer geeigneten Passphrase, da diese den Zugang zum privaten Schlüssel und damit zur verschlüsselten Kommunikation ermöglicht.
Ein einfaches Pass***wort*** ist durch einen so genannten lexikalischen Angriff leicht zu ermitteln. Dabei werden z.B. alle Einträge eines Wörterbuches auf den Schlüssel durchprobiert. (Dies wird selbstverständlich durch ein eigenes Programm durchgeführt).
Um eine Passphrase zu erstellen, die nicht im Wörterbuch steht aber dennoch leicht zu merken ist, gibt es verschiedene Ansätze. Im Folgenden soll auf eine Möglichkeit eingegangen werden.

Ein sinnvoller Ansatz ist es, ein Sprichwort, ein Zitat oder auch eine Textzeile aus einem Lied zu nehmen, dessen erste Buchstaben das Passwort bilden werden.
Aus „**E**in **M**ännlein **s**teht **i**m **W**alde **g**anz **s**till **u**nd **s**tumm," wird beispielsweise: **EMsiWgsus**. Behalten sie die Groß- und Kleinschreibung ruhig bei, sie vergrößert die Qualität ihrer Passphrase.
Bereits jetzt haben Sie ein Passwort, das in keinem Wörterbuch zu finden sein dürfte. Um die Komplexität noch zu erhöhen lassen sie die Satzzeichen in der Passphrase. In dem Beispiel wird das Komma an das Ende gestellt: **EMsiWgsus,**. Weiterhin lassen sich einige Buchstaben durch Zahlen und Sonderzeichen ersetzen z.B. das g durch eine 9, eine 3 ersetzt das E und das s wird durch das $ ersetzt: **3M$iW9$u$,** .
Das Verfahren lässt sich beliebig erweitern. Der Phantasie sind in dieser Hinsicht keine Grenzen gesetzt.

Versuchen Sie immer, die Passphrase "merkbar" zu halten. Denn nur, wenn Sie sie auswendig wissen, kann sie wirklich sicher sein.

Weiterführende Informationen zum Thema Passphrase-Längen finden Sie auf der Internetseite: http://www.metaner.de/1pw/brute-force.html.

2.2.2 Einrichten des Bayern Keyservers

Um die Nachrichten verschlüsselt an die Empfänger der Verwaltung senden zu können ist es nötig, den öffentlichen Schlüssel des Empfängers zu kennen. Die Bayerische Verwaltung hat daher einen eigenen PGP-Keyserver aufgesetzt, auf dem alle öffentlichen PGP-Schlüssel der Bayerischen Verwaltung und damit einer Vielzahl von Behörden zur Verfügung stehen. Um diese Schlüssel verwenden zu können, müssen Sie den Keyserver der Bayerischen Verwaltung in PGP einrichten. Eine Erreichbarkeit der einzelnen Behörden ist in fast allen Fällen durch die zentrale Poststelle gegeben, die auch E-Mails in Empfang nimmt und an die zuständigen Ansprechpartner weiterleitet. Die erforderliche Einrichtung des Bayerischen Keyservers wird im Folgenden beschrieben.

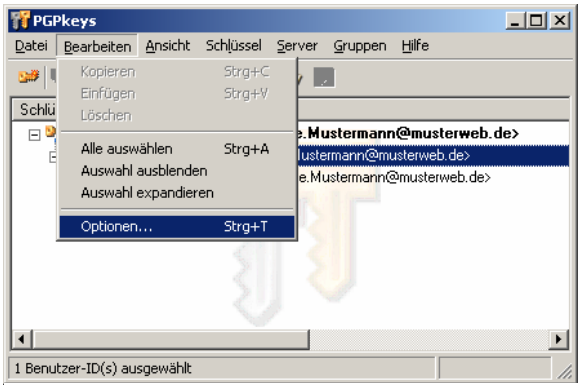

Abbildung 20: PGPkeys Optionen

Starten Sie zunächst PGPkeys aus dem PGP-Tray heraus (siehe Abbildung 12).
Nach dem Start von PGPkeys wählen Sie den Menüpunkt ***Bearbeiten*** und dort den Eintrag ***Optionen***, um in die Einstellungen zu gelangen.

Wenn Sie im Fenster „PGP Optionen“ auf den Reiter ***Server*** klicken, gelangen Sie zu nebenstehender Ansicht. In der Regel finden Sie hier vordefinierte Keyserver, die an dieser Stelle nicht berücksichtigt werden, da die Bayerische Verwaltung einen eigenen Keyserver zur Verfügung stellt. Um einen neuen Server hinzuzufügen, betätigen Sie die Schaltfläche ***Neu***.

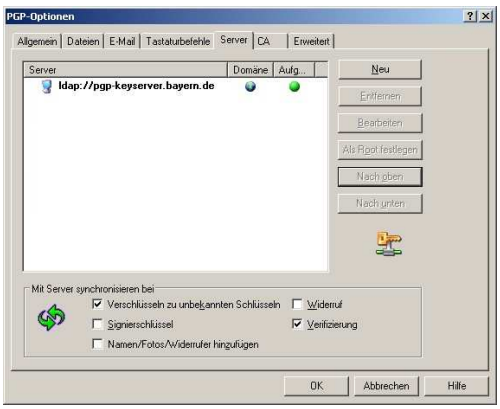

Abbildung 21: Optionen - Server

Für einen Zugriff auf den PGP-Keyserver der Bayerischen Verwaltung steht Ihnen folgende Möglichkeit zur Verfügung:

Name: pgp-keyserver.bayern.de

Port / Anschluss: 389 (LDAP)

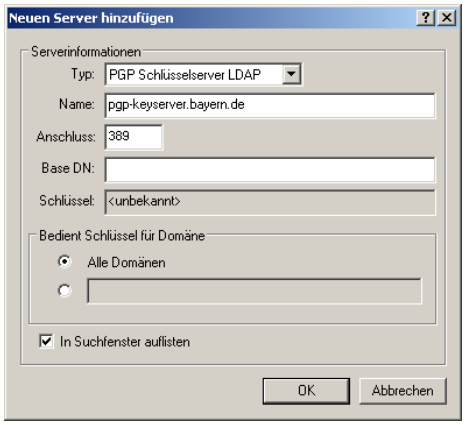

Abbildung 22: Servereinrichtung

Außer den vorstehenden Einträgen sind keine weiteren Einstellungen nötig, um den Keyserver der Bayerischen Verwaltung nutzen zu können. Bestätigen Sie Ihre Eingabe jeweils durch drücken der Schaltfläche ***OK***.

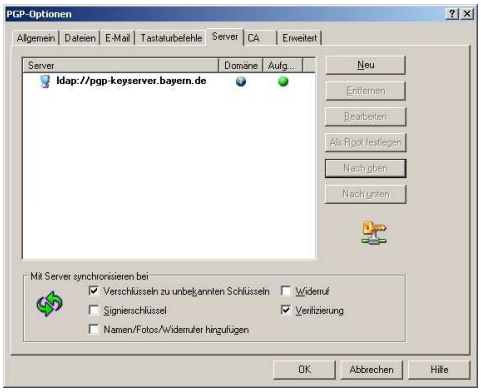

Abbildung 23: Liste der Servereinträge

Nachdem Sie den Servereintrag vorgenommen haben, ist dieser in der Optionen-Ansicht unter Server aufgelistet.

Gehen Sie auf ***OK*** um die vorgenommenen Einstellungen zu übernehmen und zu PGPkeys zurückzukehren.

Sie haben nun die Möglichkeit, die öffentlichen PGP-Schlüssel des Empfängers / der Empfangsbehörde abzufragen und an diese eine verschlüsselte Nachricht zu senden, die nur von dem entsprechenden Empfänger / der Empfangsbehörde geöffnet werden kann. Wie die Suche im Detail funktioniert, wird in Abschnitt 3 dieser Dokumentation näher erläutert.

3. Nutzung von PGP

Im folgenden Abschnitt wird der Umgang mit PGP beschrieben. Es wird Ihnen aufgezeigt, wie Sie E-Mails ver- bzw. entschlüsseln können. Um jedoch eine verschlüsselte Nachricht an einen Empfänger senden zu können, ist es nötig, dessen öffentlichen Schlüssel zu kennen. Mit diesem werden die Nachrichten später verschlüsselt. Es wird daher im Folgenden darauf eingegangen, wie der öffentliche Schlüssel eines Empfängers in der Bayerischen Verwaltung in Erfahrung gebracht wird.

3.1 Nutzung der öffentlichen Schlüssel der Bayerischen Verwaltung

Die im vorigen Abschnitt beschriebene Einrichtung des Bayerischen Keyservers gibt uns an dieser Stelle die Möglichkeit, den benötigten öffentlichen Schlüssel des Empfängers in der Verwaltung in Erfahrung zu bringen. Öffnen Sie zunächst PGPkeys. (Abbildung 12: Start PGPkeys). ***Für die Suche ist eine aktive Internetverbindung nötig!***

Die Suche wird gestartet, in dem Sie unter dem Menüpunkt ***Server*** den Eintrag ***Suchen*** betätigen.

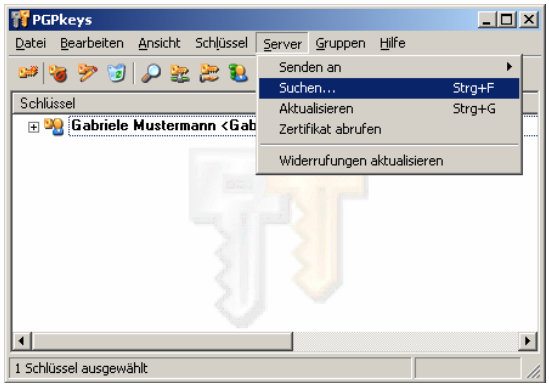

Abbildung 24: PGPkeys - Suchen..

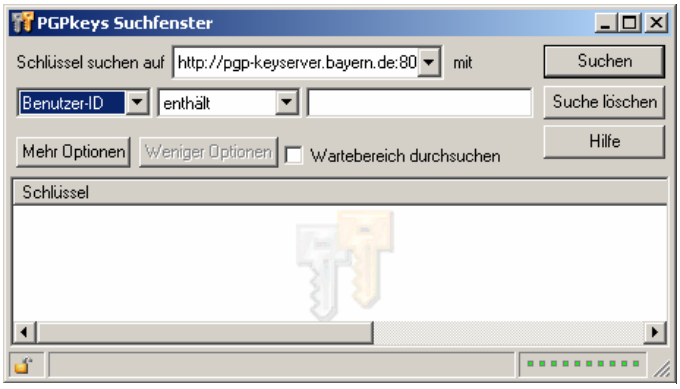

Abbildung 25: Suchfenster

In dem Feld „***Schlüssel suchen auf***“ muss der ***pgp-keyserver.bayern.de*** angegeben sein. Benutzen Sie das Pull-down-Menü, um den Server Auszuwählen. Dabei spielt es keine Rolle, ob Sie den ***LDAP-*** oder ***HTTP-***Server

für die Suche heranziehen. Beide liefern Ihnen das gleiche Ergebnis.

Nebenstehendes Fenster zeigt die Ergebnisse für eine beispielhafte Suche nach dem öffentlichen Schlüssel des Finanzamts München. Geben Sie dazu den Suchbegriff „Finanzamt Muenchen“ ein und betätigen Sie mit ***Suchen***. (Bei den Umlauten ä, ö und ü kann es sinnvoll sein, die Suche zusätzlich mit der äquivalenten Buchstabenfolge ae, oe oder ue durchzuführen. Dieses resultiert aus älteren PGP-Versionen, die Umlaute nicht verarbeiten können.)

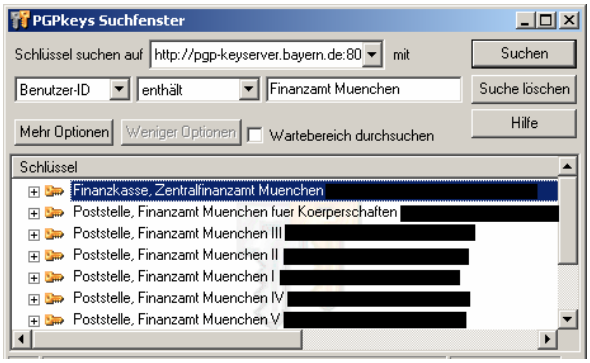

Abbildung 26: Beispielsuche

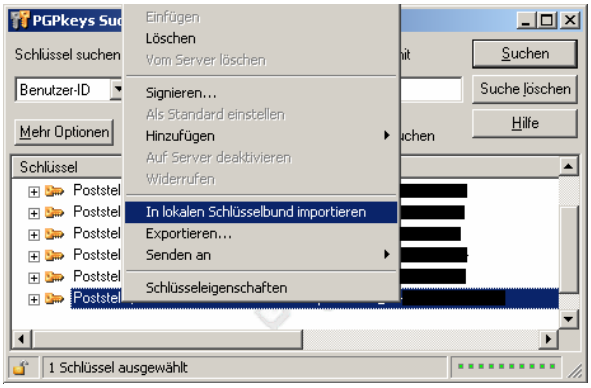

Abbildung 27: Öffentlichen Schlüssel importieren

Den von Ihnen benötigten Schlüssel müssen Sie in Ihren „privaten Schlüsselbund“ importieren. Dies erreichen Sie, indem Sie mit der ***rechten Maustaste*** auf den jeweiligen Schlüssel klicken und anschließend in dem sich öffnenden Fenster den Menüpunkt „***In lokalen Schlüsselbund importieren***“ betätigen. Beenden Sie die Suche, indem Sie das Suchfenster durch klicken auf ☒ im oberen rechten Fensterrand schließen.

Ähnlich der „Abbildung 28: PGPkeys mit importiertem Schlüssel“ wird der soeben importierte Schlüssel in der Anzeige von PGPkeys erscheinen.

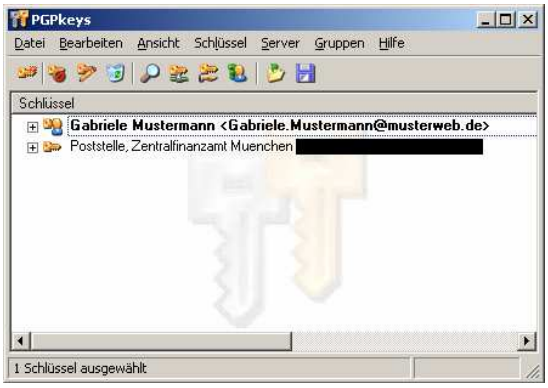

Abbildung 28: PGPkeys mit importiertem Schlüssel

3.2. Verschlüsseln / Entschlüsseln

3.2.1 Verschlüsseln von E-Mails

Beachten Sie, dass das hier erläuterte Verfahren für die Freeware Version gilt und nicht die Plug-Ins der Vollversion genutzt werden.

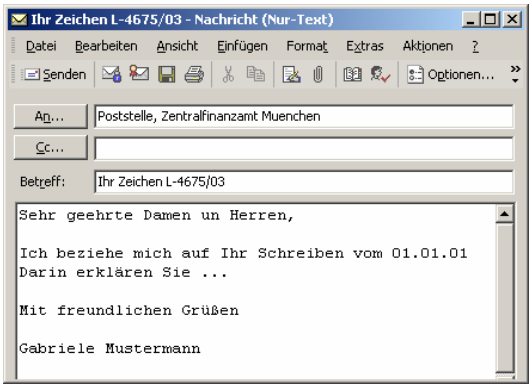

Abbildung 29: E-Mail schreiben

Schreiben Sie Ihre E-Mail wie gewohnt mit dem von Ihnen bevorzugten Programm.

Nachdem Sie die Nachricht fertig geschrieben haben, klicken Sie mit der rechten Maustaste auf den ***PGPtray*** und wählen unter dem Menüpunkt ***Aktuelles Fenster*** den Eintrag ***Verschlüsseln***. (Achten Sie darauf, dass das Fenster, in dem Sie die E-Mail geschrieben haben als letztes aktiviert war.) Alternativ können Sie auch ***Verschlüsseln & Signieren*** wählen. In diesem Fall werden Sie zu einem späteren Zeitpunkt aufgefordert Ihre Passphrase einzugeben. Dies ist erforderlich, um die Signierung durchführen zu können.

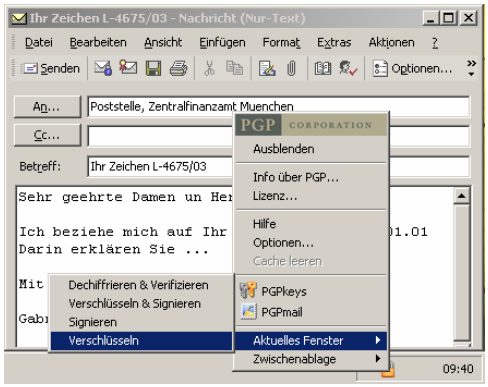

Abbildung 30: E-Mail verschlüsseln

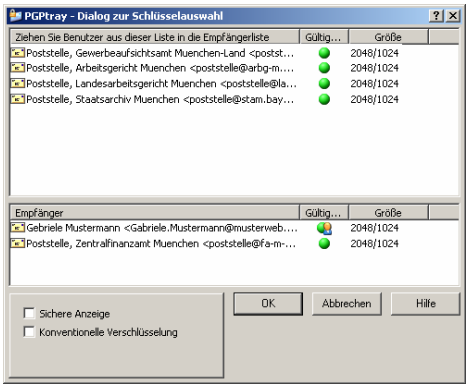

Abbildung 31: Schlüsselauswahl

Wählen Sie nun den öffentlichen Schlüssel des Empfängers Ihrer E-Mail aus, in dem Sie den Eintrag durch ***doppelklicken*** in die untere Fensterhälfte ***Empfänger*** befördern. Es ist ratsam den eigenen Schlüssel unter Empfänger zu belassen, um die Nachricht zu einem späteren Zeitpunkt selber wieder entschlüsseln zu können. Nach Auswahl aller Empfänger betätigen Sie die Schaltfläche ***OK***. Ist der gewünschte Empfänger noch nicht in der oberen Auswahlliste aufgeführt, müssen Sie zuerst den Schlüssel wie in Abschnitt „3.1 Nutzung der öffentlichen Schlüssel der Bayerischen Verwaltung“ beschrieben importieren.

Ihre E-Mail ist nun verschlüsselt und weist zum größten Teil kryptische Zeichen auf. Sie können die E-Mail nun an den Empfänger senden. Nur der richtige Empfänger wird in der Lage sein die E-Mail mit seinem privaten Schlüssel zu entschlüsseln.

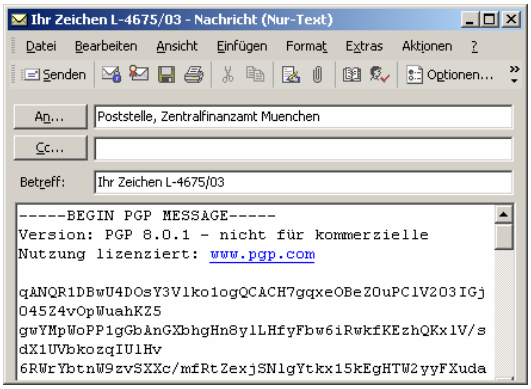

Abbildung 32: Verschlüsselte E-Mail

3.2.2 Entschlüsseln von E-Mails

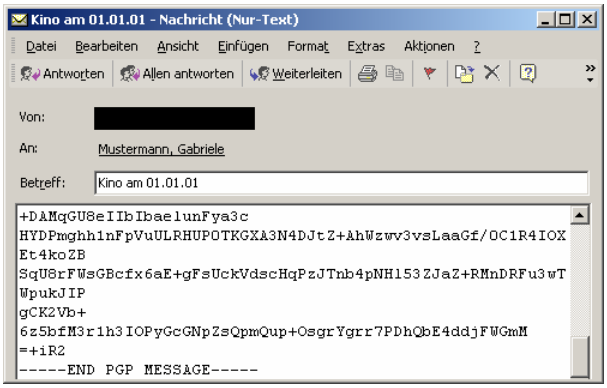

Abbildung 33: Verschlüsselt empfangene E-Mail

Im Weiteren wird darauf eingegangen, wie Sie als Empfänger eine verschlüsselte E-Mail entschlüsseln und wieder lesbar machen können. Zu Testzwecken können Sie auch eine E-Mail entschlüsseln, die Sie selbst mit Ihrem öffentlichen Schlüssel verschlüsselt haben.

Achten Sie darauf, dass Sie zuerst in den Text der E-Mail klicken. Anschließend mit der rechten Maustaste auf den ***PGPtray*** klicken und unter dem Menüpunkt ***Aktuelles Fenster*** den Eintrag ***Dechiffrieren & Verifizieren*** wählen.

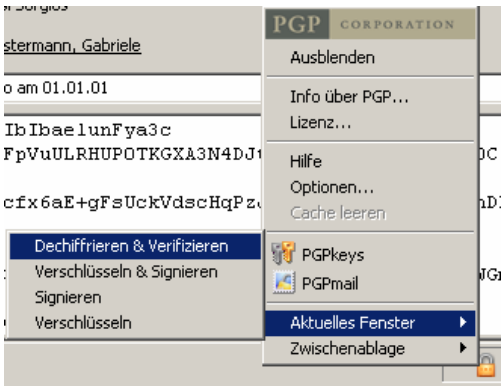

Abbildung 34: PGPtray Dechiffrieren & Verifizieren

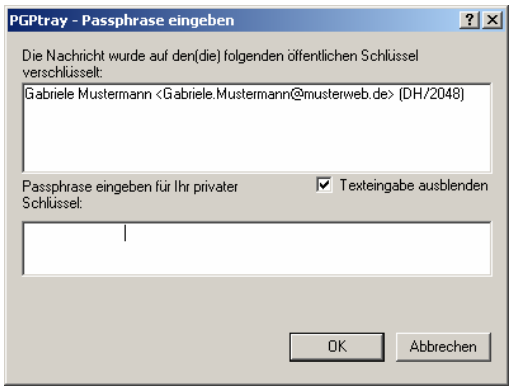

Abbildung 35: Entschlüsselung Eingabe der Passphrase

Das nun folgende Fenster fordert Sie auf, die Passphrase für Ihren privaten Schlüssel einzugeben. Ohne die Eingabe Ihrer gültigen Passphrase ist eine Entschlüsselung der E-Mail nicht möglich. Nach Eingabe der Passphrase bestätigen Sie diese durch drücken von ***OK***.

Haben Sie die Passphrase korrekt eingegeben, erscheint ein neues Fenster mit der entschlüsselten Nachricht. Sie können den Inhalt dieses Fensters ***Kopieren*** oder durch drücken von ***OK*** schließen.

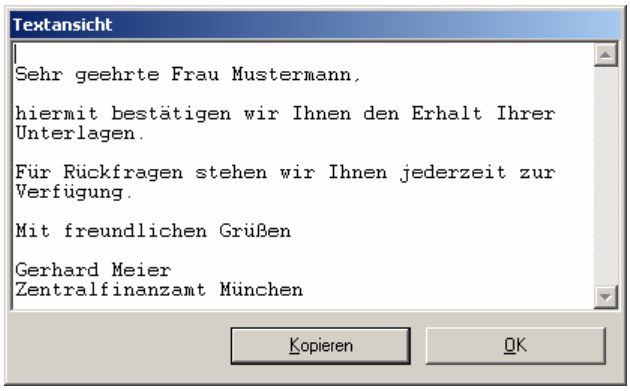

Abbildung 36: Textansicht der entschlüsselten Mail

Mit der vorstehenden Beschreibung sind Sie nun in der Lage E-Mails zu ver- und entschlüsseln.

3.3 Verschlüsseln von Datei-Anhängen

Die bisher beschriebene Methode ist ausreichend, wenn Sie ausschließlich E-Mails mit Text versenden. Sollten Sie der E-Mail eine Datei anhängen und diese wie beschrieben verschlüsseln, so ist zwar der Text verschlüsselt, nicht jedoch die angefügte Datei. Da Sie ein Interesse daran haben, dass auch die angehangene Datei verschlüsselt wird (diese wird in der Regel sensiblere Daten enthalten als der eigentliche E-Mail-Text) wird im Folgenden kurz darauf eingegangen, wie Sie auch Dateien mit PGP verschlüsseln können.

Wählen Sie in Ihrem Datei-Explorer die zu verschlüsselnde Datei. Wenn Sie mit der rechten Maustaste nun auf diese Datei klicken, öffnet sich ein Menü mit dem Unterpunkt ***PGP***. Gehen Sie auf diesen Menüpunkt und wählen Sie dort den Unterpunkt ***Verschlüsseln***. Nun öffnet sich ein Fenster ähnlich der Abbildung 31: Schlüsselauswahl. Wählen Sie den öffentlichen Schlüssel des Empfängers der Datei und gehen Sie anschließend auf ***OK***.
Es wird nun eine neue Datei erstellt, die genau so heißt wie die alte, jedoch zusätzlich die Erweiterung .pgp beinhaltet (aus Test.txt wird Test.txt.pgp). Diese Datei müssen Sie nun an Ihre verschlüsselte E-Mail anhängen.
Haben Sie einen verschlüsselten Anhang erhalten, so speichern Sie diesen zunächst in einem beliebigen Verzeichnis. Durch Doppelklicken auf diese Datei werden Sie aufgefordert Ihre Passphrase einzugeben (siehe Abbildung 35: Entschlüsselung Eingabe der Passphrase). Anschließend können Sie angeben unter welchem Namen Sie die entschlüsselte Datei speichern möchten. Die entschlüsselte Datei steht nun wieder für weitere Nutzungen zur Verfügung.

3.4 Weitergabe des eigenen öffentlichen Schlüssels

Damit Andere die Möglichkeit bekommen Ihnen verschlüsselte E-Mails zu senden, ist es nötig, diesen Personen Zugang zu Ihrem öffentlichen Schlüssel zu gewähren. Dies kann auf verschiedene Weise erfolgen.
Die erste Möglichkeit sieht vor, dass Sie Ihren öffentlichen Schlüssel dadurch weitergeben, indem Sie ihn an die von Ihnen geschriebenen E-Mails anhängen. Dafür ist es zunächst erforderlich, den öffentlichen Schlüssel in eine Datei zu exportieren.

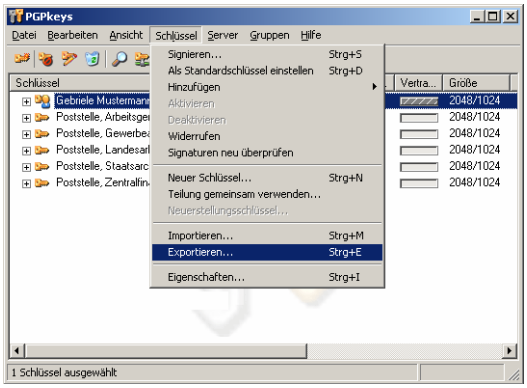

Abbildung 37: Öffentlichen Schlüssel exportieren

Öffnen Sie PGPkeys, klicken Sie auf Ihren Schlüssel, so dass dieser markiert ist und wählen Sie im Menüpunkt ***Schlüssel*** den Unterpunkt ***Exportieren…***.

Sie werden nun aufgefordert den Schlüssel zu Speichern. Wenn sie den empfohlenen Namen akzeptieren, gehen Sie einfach auf ***Speichern***.

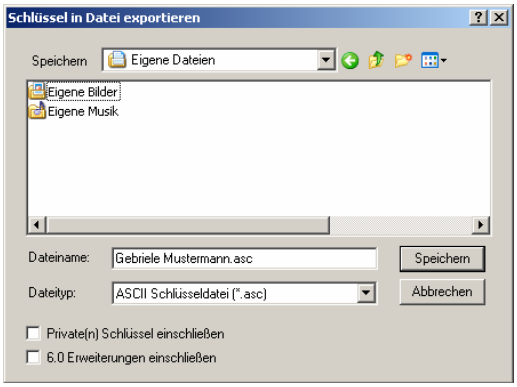

Abbildung 38: Schlüssel speichern

Die nun erstellte Datei enthält Ihren öffentlichen Schlüssel im ASCII-Format. Hängen Sie diese Datei an Ihre zukünftigen Mails an und der jeweilige Empfänger kann diesen Schlüssel bei sich importieren und Ihnen zukünftig verschlüsselte E-Mails zukommen lassen.

Einige E-Mail-Programme erlauben auch einen einfacheren Weg: markieren Sie mit der Maus Ihren Schlüssel in PGPkeys und halten Sie die Maustaste gedrückt. Ziehen Sie nun den Mauszeiger in den geschriebenen E-Mail-Text und es wird automatisch eine Datei mit der Erweiterung ***.asc*** angehängt. Sollte jedoch nur eine lange Zeichenfolge im E-Mailtext entstehen, wird dieses vereinfachte Vorgehen von Ihrer E-Mail-Applikation nicht unterstützt.

Eine weitere Möglichkeit der Veröffentlichung bieten sog. PGP-Keyserver, wie Sie sie schon aus Abschnitt „2.2.2 **Einrichten des Bayern Keyserver**“ kennen. Um Ihren Schlüssel auf einem bekannten Keyserver zu veröffentlichen, klicken Sie mit der rechten Maustaste auf Ihren Schlüssel in PGPkeys. Im nun öffnenden Menü gehen

sie auf ***Senden an*** und wählen den Keyserver aus, an den der Schlüssel gesendet werden soll. Es ist zu empfehlen einen der voreingestellten Keyserver zu nutzen (nicht einen Keyserver der Bayerischen Verwaltung).

4. Zusammenfassung

Dieses Dokument hatte zum Ziel, Ihnen ein grundsätzliches Verständnis zur Verschlüsselung im Umgang mit PGP zu liefern. Sollte dies Ihr Interesse geweckt haben, können Sie u.a. auf den nachstehenden Internetseiten weiterführende Informationen abrufen.

http://www.helmbold.de/pgp/index.htm
http://www.datenschutzzentrum.de/selbstdatenschutz/pgp/wozu.htm
http://www.pgpfueralle.de (Mit Video-Animationen zur Installation)