Das Handbuch zu KGpg

Jean-Baptiste Mardelle
Rolf Eike Beer
Übersetzung: Sebastian Stein
Übersetzung: Rolf Eike Beer

Das Handbuch zu KGpg

Inhaltsverzeichnis

Zusammenfassung

KGpg ist eine einfache grafische Benutzeroberfläche für GnuPG (http://gnupg.org).

Kapitel 1

Einleitung

KGpg ist eine einfache Benutzeroberfläche für das sehr leistungsfähige Verschlüsselungswerkzeug GnuPG. GnuPG, auch bekannt als gpg, wird mit den meisten Distributionen ausgeliefert und sollte auf Ihrem System installiert sein. Sie können die aktuelle Version von http://gnupg.org beziehen.

Mit KGpg können Sie Dateien und E-Mails ver- und entschlüsseln, was eine viel sichere Kommunikation ermöglicht. Ein Kurzbeschreibung über Verschlüsselung mit gpg ist auf der GnuPG-Internetseite verfügbar.

Mit KGpg brauchen Sie die gpg Befehle und Optionen nicht zu kennen. Fast alles kann über wenige Mausklicks erledigt werden.

Kapitel 2

Grundlagen

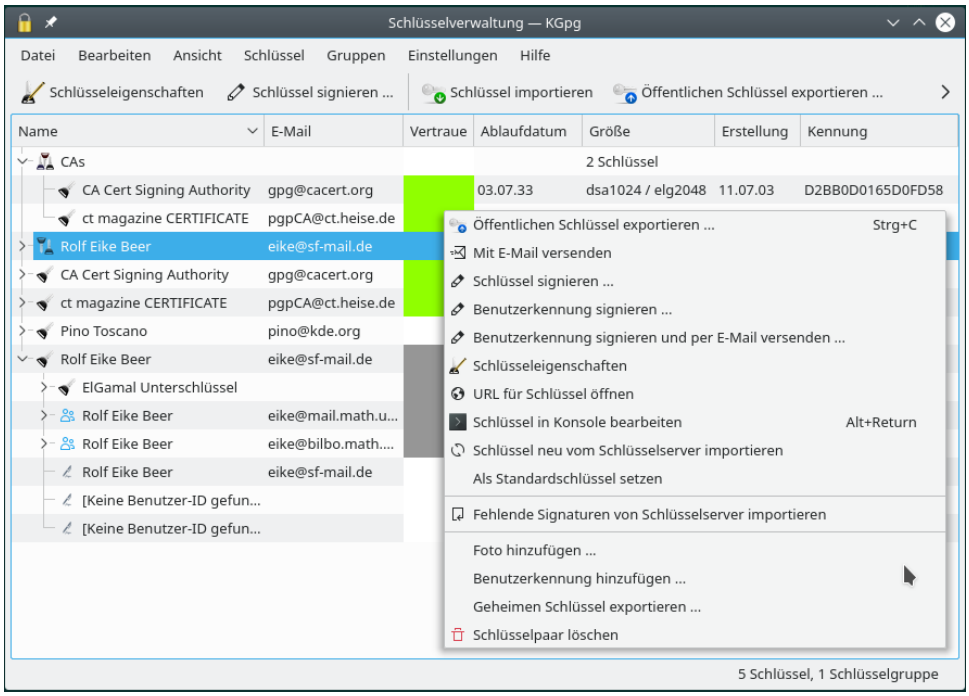
Hier ist eine Liste mit den Hauptkomponenten von KGpg:

Symbol im Systemabschnitt der Kontrollleiste

Nach dem Start von KGpg erscheint im Systemabschnitt der Kontrollleiste ein Miniprogramm. Durch einen Klick mit der linken Maustaste erscheint das Fenster zur Schlüsselverwaltung, durch einen Klick mit der rechten Maustaste erscheint ein Menü mit den wichtigsten Befehlen. Sie können dieses Verhalten in den KGpg-Einstellungen an Ihre persönlichen Vorlieben anpassen.

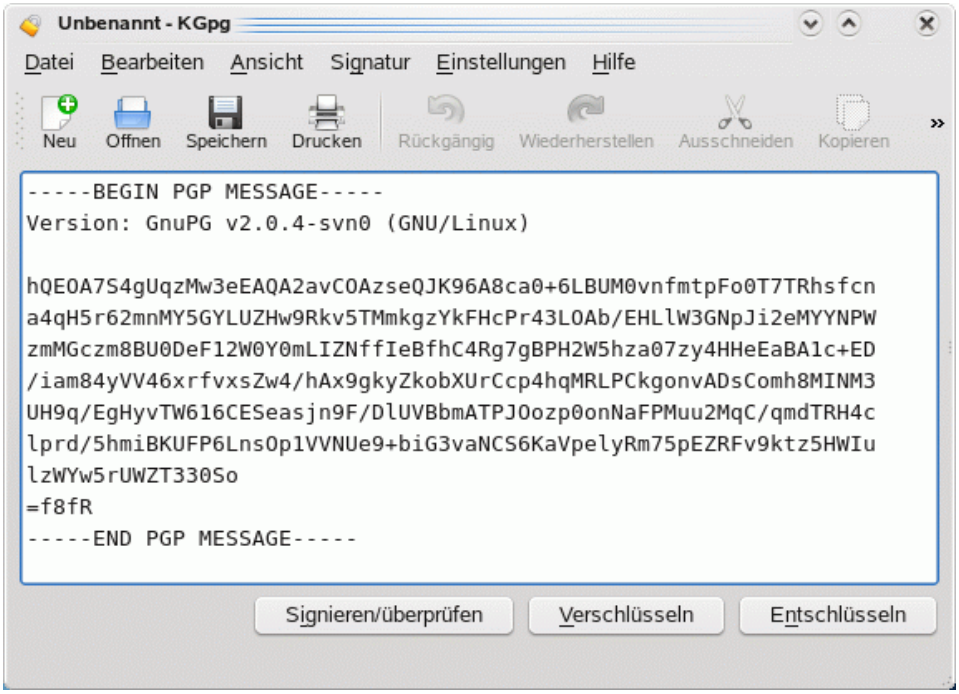
Das Miniprogramm von KGpg ist normalerweise als inaktiv markiert. Der Systemabschnitt der Kontrollleiste blendet im Normalfall alle inaktiven Miniprogramme aus, sofern Sie diese nicht anders konfigurieren. Näheres können Sie in der Plasma-Dokumentation nachlesen.

Fenster Schlüsselverwaltung



In diesem Fenster werden die Schlüssel zentral verwaltet. Um die Schlüsselverwaltung aufzurufen, klicken Sie mit der linken Maustaste auf das KGpg-Miniprogramm im Systemabschnitt der Kontrollleiste. Sie können Schlüssel importieren, exportieren, signieren und eigene Schlüssel bearbeiten. Die meisten Befehle stehen durch einen Klick mit der rechten Maustaste auf den Schlüssel zur Verfügung.

Editor-Fenster



Es handelt sich um einen einfachen Texteditor, in den Sie Text einfügen können, um diesen zu ver- oder entschlüsseln. Um den Editor zu öffnen, klicken Sie mit der rechten rechten Maustaste auf das KGpg-Miniprogramm im Systemabschnitt der Kontrollleiste oder wählen Sie **Datei** → **Editor öffnen** im Menü der Schlüsselverwaltung.

Integration in Dateiverwaltung

KGpg ist in Konqueror und Dolphin integriert. Das bedeutet, dass Sie durch einen Klick mit der rechten Maustaste auf eine Datei aus dem Menü **Aktionen** → **Datei verschlüsseln** auswählen können, um die Datei zu verschlüsseln. Durch einen Klick mit der linken Maustaste können Sie eine Datei entschlüsseln.

Kapitel 3

KGpg benutzen

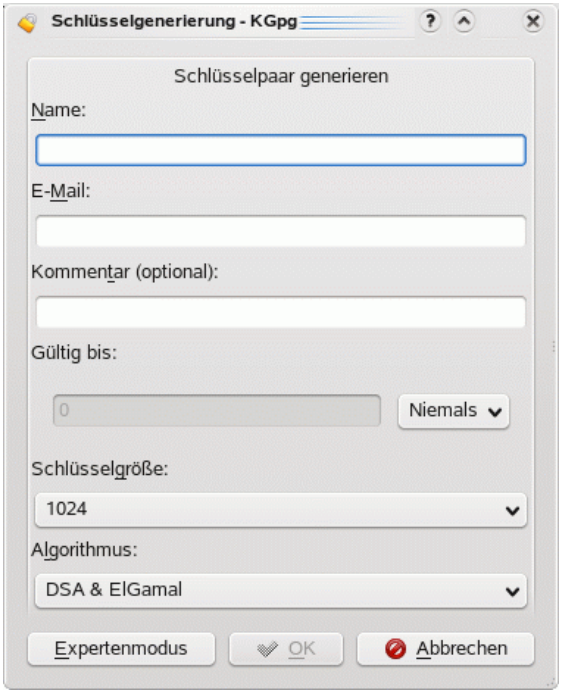
Es gibt 2 Möglichkeiten, um Ihre Daten zu verschlüsseln:

- Symmetrische Verschlüsselung: Ihre Daten werden mit einem Passwort verschlüsselt. Jeder, der einen Computer mit gpg hat, kann die Nachricht entschlüsseln, wenn Sie ihm den Schlüssel geben. Um eine symmetrische Verschlüsselung auszuführen, müssen Sie „Symmetrische Verschlüsselung" in den Optionen auswählen, wenn Sie nach dem Schlüssel zur Verschlüsselung gefragt werden.
- Verschlüsselung mit Schlüssel: Sie müssen zuerst ein mit einer Passphrase versehenes Schlüsselpaar (geheimer und öffentlicher Schlüssel) erzeugen. Bewahren Sie den geheimen Schlüssel an einem sicheren Ort auf und tauschen Sie Ihren öffentlichen Schlüssel mit Ihren Freunden aus. Um eine verschlüsselte Nachricht an Alex zu senden, müssen Sie die Nachricht mit dem öffentlichen Schlüssel von Alex verschlüsseln. Um die Nachricht zu entschlüsseln, braucht der Empfänger den geheimen Schlüssel von Alex und das Passwort.

Verschlüsselung mit Schlüsseln ist komplizierter, da Sie die Schlüssel mit Freunden austauschen müssen, aber wesentlich sicherer. Beachten Sie, dass Sie eine mit einem anderen öffentlichen Schlüssel verschlüsselte Nachricht nicht selbst entschlüsseln können. Sie können nur Nachrichten entschlüsseln, die mit dem eigenen öffentlichen Schlüssel verschlüsselt wurden.

3.1 Schlüssel erzeugen

Wenn Sie keinen eigenen Schlüssel besitzen, öffnet KGpg beim ersten Aufruf automatisch den Dialog zur Erzeugung eines Schlüssels. Sie können diesen Dialog auch aus der Schlüsselverwaltung über **Schlüssel** → **Schlüsselpaar generieren** erreichen.



Geben Sie Ihren Namen und E-Mail-Adresse ein und klicken Sie auf **Ok**. Dadurch wird ein Schlüssel für gpg mit den Standardeinstellungen erstellt. Benötigen Sie weitere Optionen, können Sie über den Knopf **Expertenmodus** ein Konsole-Fenster öffnen, das es Ihnen ermöglicht, alle Einstellungen von gpg zu beeinflussen.

Die Erfahrung zeigt, dass der erste Schlüssel benutzt wird, um damit zu Experimentieren und Erfahrungen zu sammeln. Dies führt z.B. zu fehlerhaften Benutzeridentitäten, Kommentaren, die man später bereut oder einfach vergessenen Passphrasen. Um zu verhindern das solche Schlüssel unbegrenzt gültig bleiben ist es meist eine gute Idee, die Lebenszeit des Schlüssels auf 12 Monate zu begrenzen. Sie können das Ablaufdatum des Schlüssels später im Fenster Schlüsseleigenschaften ändern.

3.2 Schlüssel sperren

Solange Sie den privaten Schlüssel und die Passphrase besitzen, können Sie einen abgelaufenen Schlüssel wieder benutzbar machen. Wenn Sie einen Schlüssel endgültig unbenutzbar machen möchten, müssen Sie ihn sperren. Das wird mittels einer speziellen Sperrsignatur erreicht, die zum Schlüssel hinzugefügt wird.

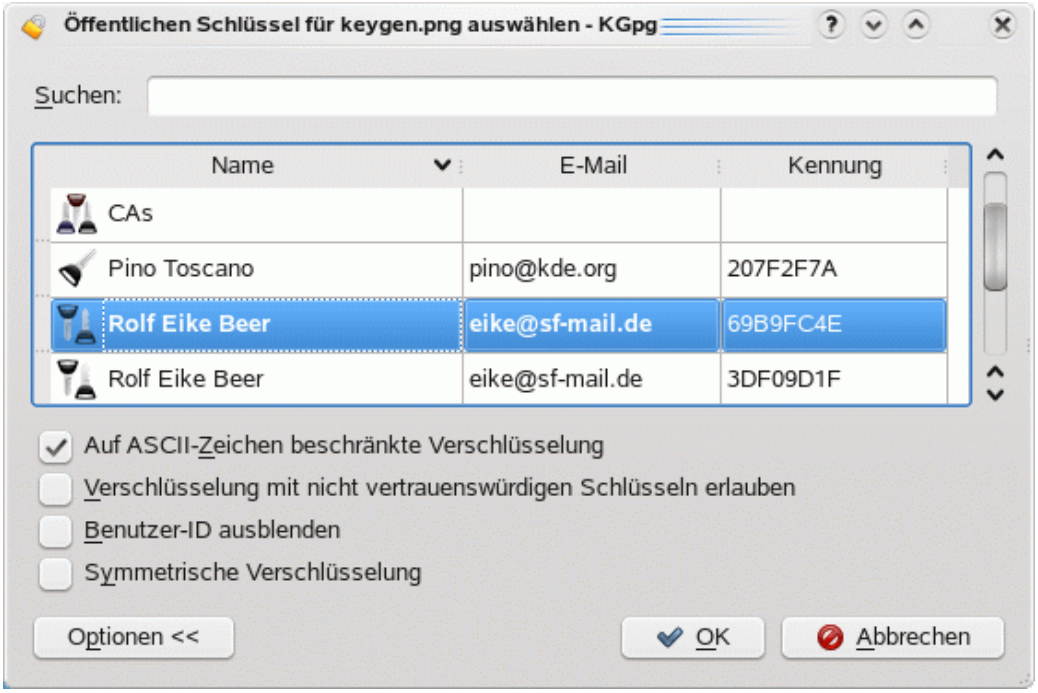
Eine Sperrsignatur kann zusammen mit dem Schlüssel erzeugt werden. In diesem Fall wird sie in einer gesonderten Datei gespeichert. Diese kann später in den Schlüsselbund importiert werden und wird dann an den Schlüssel angehängt und macht ihn damit unbrauchbar. Bitte beachten Sie, dass dazu das Passwort des Schlüssels nicht erforderlich ist. Deshalb sollten Sie die Datei mit der Sperrsignatur sicher aufbewahren, am besten getrennt von Ihrem privaten Schlüssel. Es ist ratsam, dazu einen Ort zu wählen, der nicht mit einem Computer verbunden ist, z. B. können Sie die Datei auf ein externes Speichermedium wie einen USB-Stick übertragen oder Sie drucken sie einfach aus.

Wenn Sie beim Erstellen Ihres Schlüssels keine Sperrsignatur erzeugt haben, können Sie das jederzeit nachholen. Rufen Sie dazu **Schlüssel** → **Schlüssel sperren** auf. Bei Bedarf können Sie die Sperrsignatur sofort in Ihren Schlüsselbund importieren.

3.3 Verschlüsselung von Daten

3.3.1 Verschlüsselung einer Datei in Konqueror oder Dolphin

Klicken Sie mit der rechten Maustaste auf die zu verschlüsselnde Datei. Wählen Sie **Aktionen → Datei verschlüsseln** aus dem erscheinenden Menü aus! Es wird das Fenster zur Auswahl des öffentlichen Schlüssels angezeigt. Wählen Sie den öffentlichen Schlüssel des Empfängers und klicken Sie auf **Verschlüsseln**. Die verschlüsselte Datei wird gespeichert mit der Dateierweiterung `.asc` oder `.gpg`, je nachdem ob **Auf ASCII-Zeichen beschränkte Verschlüsselung** gewählt wurde oder nicht. ASCII-verschlüsselte Dateien benutzen nur druckbare Zeichen zur Darstellung des Inhalts. Dadurch sind diese Dateien unempfindlicher gegen Beschädigungen beim Versand per Mail oder wenn Sie auf andere Systeme kopiert werden, allerdings sind sie um ein Drittel größer.



3.3.2 Text verschlüsseln mit dem KGpg-Miniprogramm

Sie können den Inhalt der Zwischenablage verschlüsseln, indem Sie **Zwischenablage verschlüsseln** im Menü des Miniprogramms wählen. Wenn Sie **Zwischenablage signieren/überprüfen** wählen, wird stattdessen der Text signiert. Beide Aktionen zeigen Ihnen das Ergebnis in einem neu geöffneten Editorfenster an.

3.3.3 Text mit dem KGpg-Editor verschlüsseln

Um Text mit dem Editor zu verschlüsseln, müssen Sie den Knopf **Verschlüsseln** betätigen. Es wird dann das Fenster zur Auswahl des öffentlichen Schlüssels angezeigt. Wählen Sie den Schlüssel und klicken Sie dann auf **Ok**. Die verschlüsselte Nachricht erscheint im Fenster des Editors.

Normalerweise können Sie nur vertrauenswürdige Schlüssel zum Verschlüsseln benutzen. Wenn Sie jedoch zum Beispiel eine verschlüsselte Nachricht an jemand Neues senden wollen, von dem Sie wissen, dass er einen GPG-Schlüssel besitzt, können Sie die Option **Verschlüsselung mit nicht vertrauenswürdigen Schlüsseln erlauben** aktivieren.

Mit Hilfe der Optionen **Immer verschlüsseln mit** und **Dateien verschlüsseln mit** in den KGpg-Einstellungen können Sie sicherstellen, dass Sie jede von Ihnen verschlüsselte Datei öffnen können, selbst wenn Sie mit einem fremden Schlüssel verschlüsselt wurde.

Für weitere Informationen über die Verschlüsselungsoptionen **Auf ASCII-Zeichen beschränkte Verschlüsselung**, **Verschlüsselung mit nicht vertrauenswürdigen Schlüsseln erlauben** und **Symmetrische Verschlüsselung** schauen Sie bitte in die Dokumentation oder Handbücher von gpg.

3.4 Entschlüsseln von Daten

3.4.1 Entschlüsselung einer Datei in Konqueror oder Dolphin

Klicken Sie mit der linken Maustaste auf die zu entschlüsselnde Datei. Geben Sie die Passphrase ein und die Datei wird entschlüsselt. Sie können eine verschlüsselte Textdatei weiterhin in das Editor Fenster von KGpg ziehen. Nach Eingabe der Passphrase wird der Text entschlüsselt und im Editor Fenster von KGpg angezeigt. Das Ziehen und Ablegen von entfernten Dateien ist ebenfalls möglich! Weiterhin können Sie **Datei** → **Datei entschlüsseln** aufrufen und die zu entschlüsselnde Datei auswählen.

3.4.2 Text entschlüsseln mit dem KGpg-Miniprogramm

Sie können den Inhalt der Zwischenablage entschlüsseln, indem Sie **Zwischenablage entschlüsseln** aus dem Menü den Miniprogramms wählen. Der entschlüsselte Text wird Ihnen in einem Editorfenster angezeigt.

3.4.3 Text mit KGpg Editor entschlüsseln

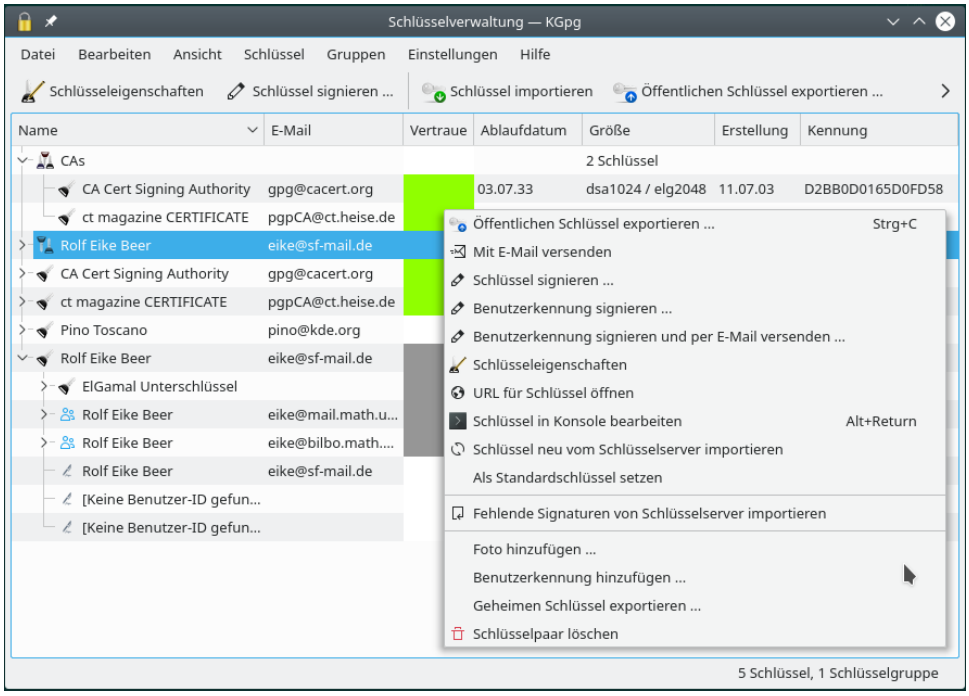
Fügen Sie den zu entschlüsselnden Text in das Editor Fenster ein und klicken Sie auf den Knopf **Entschlüsseln**. Sie werden zur Eingabe der Passphrase aufgefordert.

3.5 Schlüsselverwaltung

Alle grundlegenden Befehle zur Schlüsselverwaltung können mit KGpg ausgeführt werden. Mit einem Klick mit der linken Maustaste auf das KGpg-Miniprogramm im Systemabschnitt der Kontrollleiste wird das Fenster zur Schlüsselverwaltung aufgerufen. Die meisten Befehle sind über einen Klick mit der rechten Maustaste auf den entsprechenden Schlüssel verfügbar. Um Schlüssel zu importieren oder zu exportieren, ziehen Sie sie in das Fenster oder aus dem Fenster heraus oder benutzen Sie die Kurzbefehle „Kopieren" und „Einfügen".

Sie können einen öffentlichen Schlüssel als E-Mail, in die Zwischenablage, zu einem Schlüsselserver oder zu einer lokalen Datei exportieren. Benutzen Sie die Einstellungen im Exportdialog, um alles zu exportieren, um ohne Attribute wie Fotokennungen zu exportieren oder einen sauberen Schlüssel d. h. den Schlüssel einschließlich seiner Unterschlüssel aber ohne Signaturen zu exportieren.

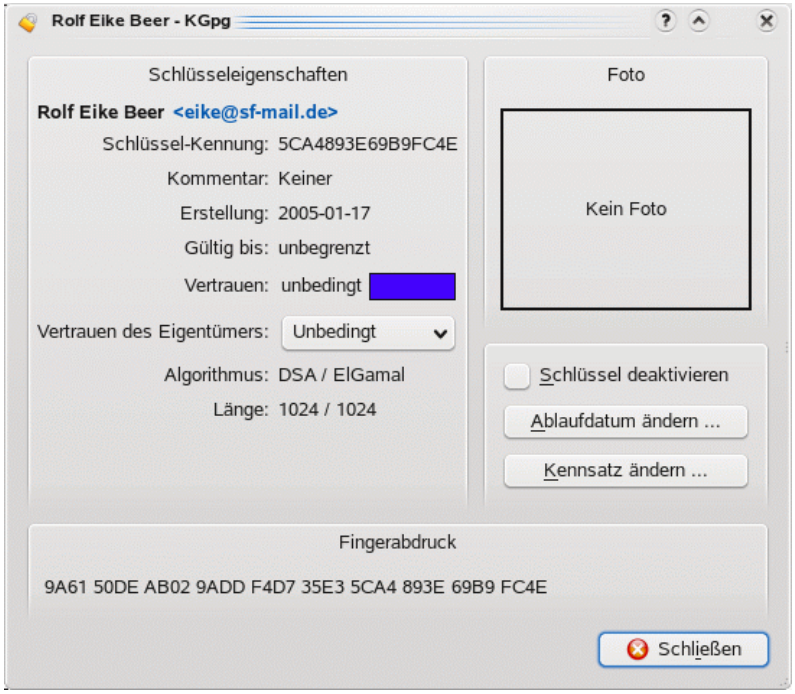
3.5.1 Schlüsselverwaltung



In diesem Beispiel sehen Sie eine Schlüsselgruppe aus zwei Schlüsseln sowie zwei Schlüsselpaare und drei öffentliche Schlüssel. Das erste Schlüsselpaar ist abgelaufen, das Zweite hingegen ist absolut vertrauenswürdig und ist außerdem der Standardschlüssel (fette Schrift). Zwei der öffentlichen Schlüssel sind vollständig vertrauenswürdig, der Letzte nur eingeschränkt. Der letzte Schlüssel ist ausgeklappt. Zu sehen sind der ElGamal-Unterschlüssel, eine weitere Benutzeridentität (beide ebenfalls eingeschränkt vertrauenswürdig) sowie einige der Signaturen.

Signaturen ermöglichen die Navigation durch den Schlüsselbund. Ein Doppelklick auf eine Signatur oder einen Schlüssel, der Mitglied einer Schlüsselgruppe ist, und der zugehörige Schlüssel wird ausgewählt.

3.5.2 Schlüsseleigenschaften



Im Gegensatz zur Schlüsselverwaltung, die für allgemeine Aktionen mit einem oder mehreren Schlüsseln zuständig ist, erlaubt Ihnen dieser Dialog, Eigenschaften eines einzelnen Schlüssels zu verändern. Sie erreichen diesen Dialog indem Sie in der Schlüsselverwaltung die Eingabetaste drücken oder einen Doppelklick auf einen Schlüssel ausführen.

In diesem Dialog können Sie für ihre geheimen Schlüssel die Passphrase und das Ablaufdatum ändern. Für alle Schlüssel stellen Sie hier auch das Vertrauen in den Besitzer dieses Schlüssels ein.

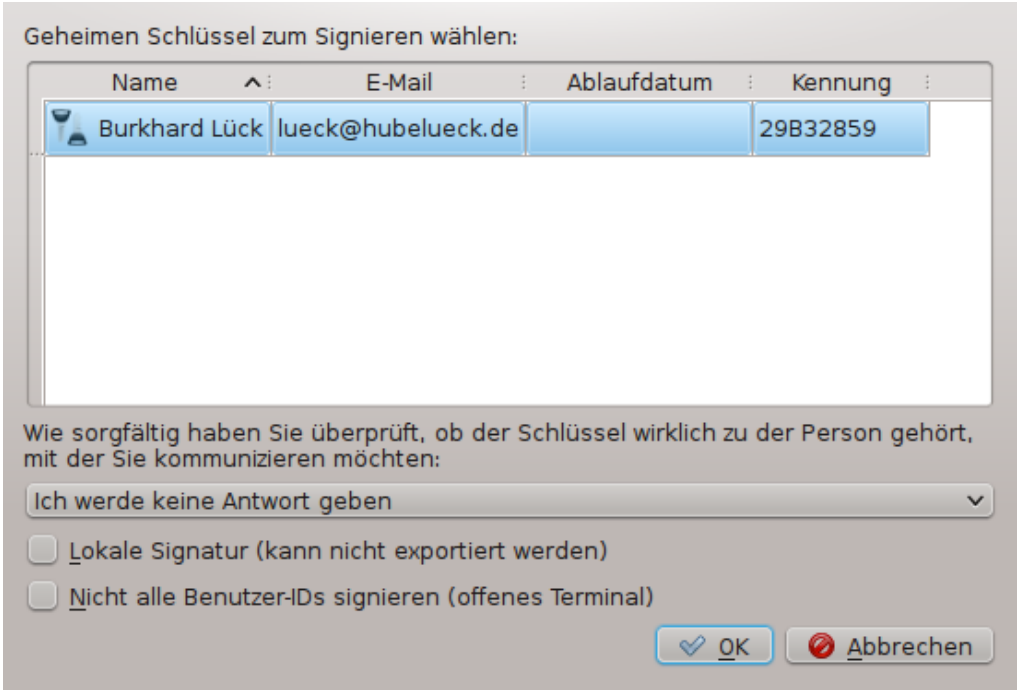
Dieser Wert gibt an, wie sehr Sie dem Besitzer des Schlüssels beim Signieren anderer Schlüssel vertrauen. Mit Hilfe dieses Wertes wird ihr eigenes Netz des Vertrauens aufgebaut. Zunächst vertrauen Sie nur den Schlüsseln, die sie selbst signiert haben. Wenn Sie den Besitzern dieser Schlüssel auch vertrauen, vertrauen Sie damit auch den Schlüsseln die von ihnen signiert wurden, ohne diese selbst signiert zu haben.

3.5.3 Schlüssel signieren

Wenn Sie den Schlüssel von jemand anderem (nennen wir sie Alice) signieren, dann erklären Sie damit, dass Sie sicher sind, dass der Schlüssel der angegebenen Person gehört und er vertrauenswürdig ist. Aus diesem Grund sollten Sie diese Überprüfung auch tatsächlich durchgeführt haben. Normalerweise heißt das, dass Sie sich mit Alice getroffen haben und mindestens eines ihrer Ausweisdokumente überprüft sowie den vollständigen Fingerabdruck ihres Schlüssels von ihr erhalten haben. Anschließend würden Sie Alice' Schlüssel signieren und den signierten Schlüssel auf einen Schlüsselserver übertragen so das jeder sehen kann das Sie Alice' Identität überprüft haben. In der Regel wird Alice bei diesem Treffen auch Ihre Identität prüfen und Ihren Schlüssel signieren, sodass die Schlüssel gegenseitig signiert sind. Sollte nur einer von Ihnen bei dem Treffen die entsprechenden Unterlagen zur Hand haben würde die Signatur nur in eine Richtung erfolgen.

Wie aber würde man so einem Schlüssel von jemandem vertrauen können der am anderen Ende der Welt lebt? Sie kommunizieren vielleicht regelmäßig mit ihr, haben aber keine Möglichkeit sie in absehbarer Zeit persönlich zu treffen.

Wenn Sie ihren Schlüssel markieren und dann **Schlüssel signieren ...** wählen erscheint das Fenster in dem Sie die Optionen für das Signieren des Schlüssels wählen können.



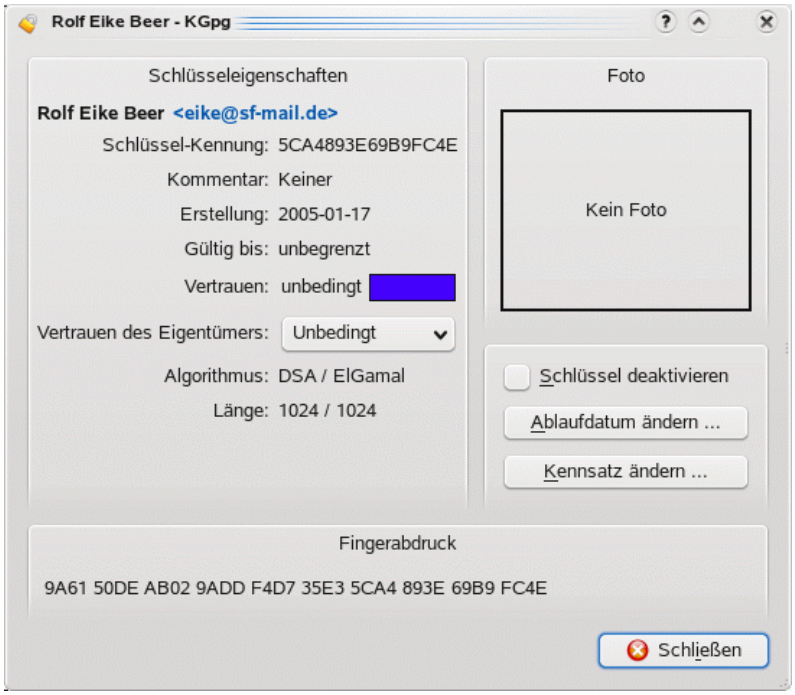
Zunächst können Sie den Schlüssel wählen, mit dem signiert werden soll. Dann können Sie eingeben wie genau Sie überprüft haben, dass die Inhaberin des Schlüssels wirklich die ist, für die sie sich ausgibt. Diese Angabe wird zusammen mit der Signatur gespeichert und dient anderen als Hinweis, die diese Signatur benötigen (näheres dazu später). Schließlich kommt die Option, die Ihnen helfen kann wenn Sie Alice nicht persönlich treffen kann: **Lokale Signatur (kann nicht exportiert werden)**. Wenn Sie diese Option wählen wird eine spezielle Signatur erzeugt, die ihren Schlüsselbund unter keinen Umständen verlassen kann.

Doch warum ist es eigentlich wichtig wie genau Sie die Alice' Identität überprüft haben? Wen geht das etwas an? Das hängt mit der zweiten Möglichkeit zusammen mit der Sie die Vertrauenswürdigkeit von Alice' Schlüssel überprüfen können. Denken Sie zum Beispiel an Trent. Von ihm wissen Sie, dass er ebenfalls ein Schlüsselpaar besitzt. Und er ist ein Weltenbummler, der jeden Monat auf mindestens zwei Kontinenten unterwegs ist. Mit ein wenig Glück ist er demnächst in der Nähe von Alice unterwegs. Zunächst werden Sie Sich also mit Trent treffen und mit ihm Schlüssel signieren. Dann werden Sie Alice mitteilen das Trent demnächst in ihrer Nähe unterwegs ist und sie bitten mit ihm ebenfalls Schlüssel zu signieren. Wenn all dies geschehen ist wissen Sie, dass Sie Trents Schlüssel vertrauen können und Trent weiß das Alice' Schlüssel vertrauenswürdig ist. Wenn Sie jetzt Vertrauen in Trents Überprüfung des Schlüssels von Alice haben können Sie auch ihrem Schlüssel vertrauen.

Diese Beziehungen zwischen den verschiedenen Schlüsseln und ihren Besitzern formen ein sogenanntes Netz des Vertrauens. Innerhalb dieses Netzes gibt es einige Parameter, die die Vertrauenswürdigkeit eines bestimmten Schlüssels bestimmen. Zunächst ist da die Angabe, wie genau die Identität des Besitzers überprüft wurde. Das ist der Wert den Sie oben im Fenster mit den Signaturoptionen wählen konnten. Sie werden wahrscheinlich wissen wie Sie die Echtheit eines Ausweises aus Ihrem Heimatland überprüfen können, aber einer aus einem anderen Land wird Ihnen wohl mehr Probleme bereiten. Sie werden also wahrscheinlich eine gute Aussage über die Identität von Trent treffen können weil Sie seinen Ausweis überprüft haben und er Ihrem eigenen sehr ähnlich ist. Trent hingegen wird sich über Alice' Identität nicht ganz so sicher sein, auch wenn er sowohl ihren Ausweis als auch ihren Führerschein geprüft hat, da er sich nicht wirklich sicher ist wie die dortigen Dokumente zu prüfen sind.

Der nächste Parameter ist wie sehr Sie einer anderen Person trauen das Sie fremde Identitäten prüft. Sie wissen das Trent dabei sehr sorgfältig vorgeht. Jörg hingegen ist niemanden den Sie

als besonders clever einschätzen würden. Er hat kaum einen Blick auf Ihren Ausweis geworfen als Sie Sich mit ihm getroffen haben. Sie sind Sich also sicher, dass Jörg tatsächlich die Person ist, die er zu sein vorgibt. Er hingegen scheint sich dafür nicht wirklich zu interessieren. Sie haben also ein hohes Vertrauen in den Schlüssel von Jörg, allerdings nur ein sehr geringes in seine Signaturen. Wenn Sie den Dialog Schlüsseleigenschaften für einen Schlüssel öffnen finden Sie dort das Feld **Vertrauen in den Eigentümer**. Dieser Wert gibt an wie sehr Sie den Signaturen, die mit diesem Schlüssel erzeugt wurden, vertrauen. Dieser Wert wird nicht exportiert, er spiegelt ausschließlich Ihre persönliche Einschätzung wieder.



Jetzt sollten Sie eine Vorstellung davon haben wie das Netz des Vertrauens entsteht, was die Werte für Vertrauen in Schlüssel und Eigentümer bedeuten und warum Sie bei der Überprüfung der Identität beim Signieren von Schlüsseln immer sorgfältig vorgehen sollten: jemand anderes könnte auf Ihr Urteil angewiesen sein. Ein Glied in der Kette ist allerdings bis jetzt noch gar nicht überprüft worden: die E-Mail-Adressen der Schlüssel, die Sie signieren. Eine neue Benutzerkennung mit Ihrem Namen und der Adresse von Alice oder Trent können Sie Ihrem eigenen Schlüssel mit einigen wenigen Mausklicks hinzufügen. Sie haben überprüft das Trent seinen Schlüssel wirklich besitzt. Aber niemand hat bisher überprüft ob sich auch die E-Mail-Adressen in seinem Schlüssel unter seiner Kontrolle befinden.

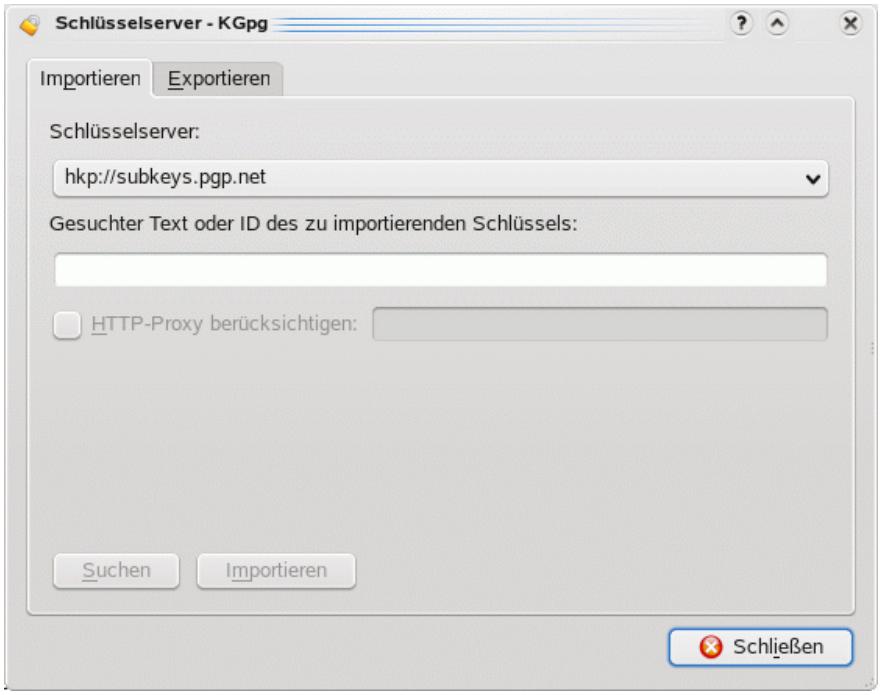
Wenn Sie hingegen **Benutzerkennung signieren und per E-Mail versenden ...** wählen können Sie diese Lücke schließen. Der Grundgedanke hinter dieser Funktion ist das der Schlüssel wie gewohnt signiert und hinterher in einzelne Teile aufgeteilt wird. Jeder Teil enthält nur eine einzelne Benutzerkennung und Ihre Signatur dieser Kennung. Dieser Teil wird jetzt mit Trents Schlüssel verschlüsselt und an die E-Mail-Adresse geschickt, die in der Benutzerkennung enthalten ist. Nur wenn Trent diese Mail erhält und entschlüsseln kann erhält er Ihre Signatur und kann sie in seinen Schlüsselbund importieren. Sie hingegen werden keine Ihrer Signaturen auf einen Schlüsselserver senden, das ist ausschließlich Sache von Trent. Sobald Ihre Signaturen von seinem Schlüssel auf einem Schlüsselserver hochgeladen werden, können Sie wirklich sicher sein das Trent sowohl den Schlüssel als auch die E-Mail-Adressen wirklich besitzt. Die Signaturen, die Sie mit dieser Funktion erzeugen, werden nicht Teil Ihres Schlüsselbundes, Trents Schlüssel wird also hinterher immer noch als nicht vertrauenswürdig eingestuft sein. Sobald Trent die E-Mails mit den Signaturen erhalten und in seinen Schlüsselbund importiert hat kann er diese auf einen Schlüsselserver hochladen. Wenn Sie seinen Schlüssel dann erneut von einem Schlüsselserver herunterladen werden Sie die neuen Signaturen ebenfalls erhalten. Auch wenn das auf den ersten Blick sehr umständlich klingt wird nur so sichergestellt, das Sie nicht versehentlich einige seiner Benutzerkennungen für vertrauenswürdig halten, die er gar nicht kontrolliert. Nur

bei den Signaturen, die auf einem Schlüsselserver zur Verfügung gestellt werden, kann jeder einschließlich Ihnen sicher sein, dass er die zugehörigen E-Mail-Adressen wirklich besitzt.

3.6 Arbeiten mit Schlüsselservern

3.6.1 Kommunikation mit Schlüsselservern

Der öffentliche Teil eines Schlüsselpaares wird normalerweise auf einem Schlüsselserver gespeichert. Diese Server erlauben es jedem, den öffentlichen Schlüssel zu einem Namen oder einer E-Mail-Adresse zu finden. Die Signaturen werden ebenfalls auf den Servern abgelegt.

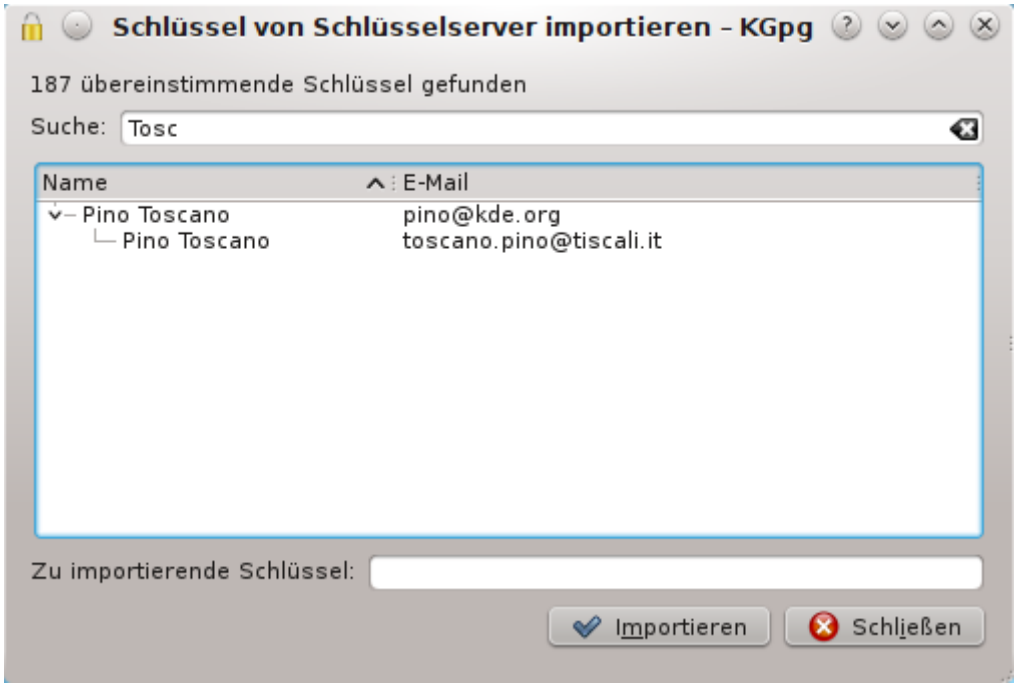


Dieser Dialog ermöglicht Ihnen den Zugriff auf die Schlüsselserver. Sie können auf dem Server nach Schlüsseln suchen und sie von dort in Ihren Schlüsselring herunterladen sowie Schlüssel auf den Server hochladen. Ein Beispiel für das Suchen und Herunterladen ist, wenn Sie eine Mail an jemand Neues schicken möchten. Wenn Sie die Mail verschlüsseln möchten, können Sie auf dem Schlüsselserver suchen, ob ein öffentlicher Schlüssel Ihrer Kontaktperson vorhanden ist. Wenn Sie ein neues Schlüsselpaar angelegt oder den Schlüssel von jemand anderem signiert haben, werden Sie normalerweise den Schlüssel und die neuen Signaturen auf den Schlüsselserver hochladen.

Die meisten Schlüsselserver tauschen die Schlüssel untereinander aus, sodass Sie vergleichbare Suchergebnisse unabhängig davon erhalten, auf welchem Server Sie suchen. Da es Ausnahmen von dieser Regel gibt, können Sie in diesem Dialog auswählen, mit welchen Schlüsselserver Sie arbeiten möchten. Es ist normalerweise eine gute Idee einen Standardschlüsselserver zu wählen, der sich in Ihrer Nähe befindet (z. B. in Ihrem Land oder wenigstens auf Ihrem Kontinent), da diese meist schneller auf Ihre Anfragen reagieren.

Bitte beachten Sie, dass alles, was Sie auf einen Schlüsselserver hochladen, dort normalerweise für immer bleibt. Dies ist einer der Gründe, weshalb Sie die Lebensdauer Ihrer Schlüssel begrenzen sollten. Beachten Sie außerdem, dass die Schlüsselserver zeitweise von Spammern nach E-Mailadressen durchsucht werden.

3.6.2 Suchergebnisse des Schlüsselservers



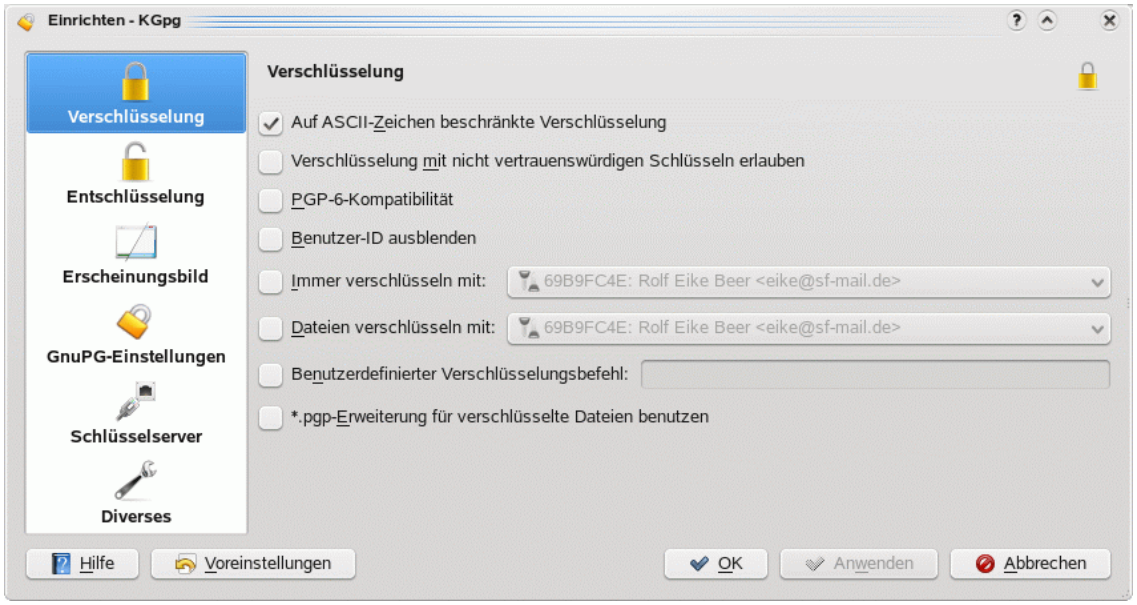
Die Suchergebnisse werden in diesem Fenster angezeigt. Im Bild ist das Ergebnis einer Suche nach ˝@kde.org˝ dargestellt, die insgesamt 244 Übereinstimmungen erzielte. Mit Hilfe des Suchfeldes wurde dies auf einen einzelnen Schlüssel eingegrenzt. Dieser Schlüssel liefert gleich eine doppelte Übereinstimmung, da sowohl die primäre Kennung als auch eine der Benutzerkennungen den Suchbegriff enthalten.

Sie können eines oder auch mehrere der Suchergebnisse markieren um die betreffenden Schlüssel in Ihren Schlüsselbund zu importieren. Die IDs der markierten Schlüssel werden im Feld **Zu importierende Schlüssel:** im unteren Bereich des Fensters angezeigt. Wenn Sie die Schaltfläche **Importieren** betätigen, werden die ausgewählten Schlüssel vom Schlüsselserver geladen und in Ihren Schlüsselring eingefügt.

3.7 KGpg einstellen

Die Einstellmöglichkeiten erreichen Sie das KGpg-Miniprogramm im Systemabschnitt der Kontrollleiste (Klick mit der rechten Maustaste auf das Miniprogramm) oder über das Hauptmenü (**Einstellungen** → **KGpg einrichten ...**). Sie können Standardparameter für Verschlüsselung, Entschlüsselung, Benutzeroberfläche und das Miniprogramm einstellen. Die meisten Verschlüsselungseinstellungen hängen direkt mit gpg zusammen und sind in den gpg-Handbüchern dokumentiert.

3.7.1 Verschlüsselung



Hier können Sie Einstellungen vornehmen, die das Verschlüsselungsverhalten von GnuPG beeinflussen. Für eine detaillierte Beschreibung der einzelnen Einstellungen lesen Sie bitte das Handbuch zu GnuPG.

- **Auf ASCII-Zeichen beschränkte Verschlüsselung**: dies bewirkt, dass die verschlüsselten Dateien in einem auf druckbare ASCII-Zeichen beschränkten Format mit kurzen Zeilen gespeichert werden. Diese Dateien sind größer als die in binärem Format gespeicherten Dateien, lassen sich aber z. B. leichter per Mail verschicken.
- **Verschlüsselung mit nicht vertrauenswürdigen Schlüsseln erlauben**: dies erlaubt auch Schlüssel für die Verschlüsselung zu verwenden denen Sie nicht vertrauen.
- **PGP-6-Kompatibilität**: die verschlüsselten Dateien werden kompatibel zum älteren PGP6-Standard gespeichert. Da dies einige zusätzliche Funktionen deaktiviert sollten Sie diese Option nur verwenden wenn Sie sie wirklich benötigen.
- **Benutzer-ID ausblenden**: dies entfernt alle Hinweise auf den Empfänger aus der verschlüsselten Datei. Falls die Übertragung der Datei abgefangen wird können dadurch keine Informationen über den Empfänger der Datei gewonnen werden. Wenn der Empfänger allerdings mehrere Schlüssel besitzt muss er bei der Entschlüsselung alle durchprobieren um den richtigen zu finden.
- **Immer verschlüsseln mit**: bei jeder Verschlüsselung wird zusätzlich dieser Schlüssel benutzt. Wenn Sie hier einen Ihrer privaten Schlüssel eintragen können Sie sicherstellen, dass Sie alle verschlüsselten Daten später noch lesen können. Im Gegenzug werden die Nachrichten größer.
- **Dateien verschlüsseln mit**: verhält sich wie **Immer verschlüsseln mit** für die Verschlüsselung von Dateien.
- **Benutzerdefinierter Verschlüsselungsbefehl**: wenn Sie besondere Optionen an GnuPG übergeben möchten können Sie diese hier eintragen. Normalerweise benötigen Sie dies nicht.
- ***.pgp-Erweiterung für verschlüsselte Dateien benutzen**: wenn Sie diese Option aktivieren erhalten werden die verschlüsselten Dateien mit der Erweiterung `.pgp` gespeichert, ansonsten mit der Erweiterung `.gpg`.

3.7.2 Entschlüsselung

Hier können Sie einen speziellen Befehl für die Entschlüsselung angeben. Diese Option wird selten benötigt und ist nur für Benutzer gedacht, die mit den Befehlszeilenoptionen von GnuPG vertraut sind.

3.7.3 Erscheinungsbild

In diesem Abschnitt kann das Erscheinungsbild von KGpg geändert werden. Sie können hier die Farben einstellen, die die verschiedenen Vertrauensstufen in der Schlüsselverwaltung repräsentieren sowie die Schriftart, die im Editor verwendet wird.

3.7.4 GnuPG-Einstellungen

Hier können Sie den **Programmpfad** sowie den Pfad und den Namen der **Einrichtungsdatei** einstellen. Beim ersten Programmstart werden diese Werte automatisch gesetzt.

Die Benutzung des GnuPG-Agenten macht die Arbeit mit GnuPG komfortabler, da Sie nicht mehr bei jeder Operation ihren Kennsatz eingeben müssen. Er wird nach der ersten Benutzung für eine gewisse Zeit im Speicher gehalten. Jede weitere Aktion, die normalerweise die Eingabe des Kennsatzes erfordern würde, kann so unmittelbar ausgeführt werden. Andererseits ermöglicht dies auch anderen Ihren Schlüssel zu missbrauchen wenn diese Zugriff auf Ihre Sitzung erhalten können.

3.7.5 Schlüsselserver

Hier können Sie eine Liste der Schlüsselserver erstellen, die Ihnen im Fenster Schlüsselserver zur Verfügung steht. Wenn Sie GnuPG auf der Befehlszeile benutzen wird der Server benutzt, den Sie hier als Standardserver festlegen.

Da das Protokoll, das zur Kommunikation mit den Schlüsselservern verwendet wird, HTTP-basiert ist kann es in manchen Netzwerken notwendig sein die Option **Falls vorhanden, HTTP-Proxy benutzen** zu aktivieren.

3.7.6 Diverses

Dieser Abschnitt fasst einige Optionen zusammen, die thematisch keinem der anderen Abschnitte zugeordnet werden können. Sie können hier **KGpg automatisch beim Anmelden starten** lassen. Die Option **Mit der Maus getroffene Auswahl anstelle des Inhalts der Zwischenablage benutzen** steuert, ob das Einfügen von Text mit der mittleren Maustaste oder über Tastenkürzel geschieht.

Sie können weiterhin festlegen, ob KGpg im Systemabschnitt der Kontrollleiste angezeigt wird und welche Aktion ausgeführt wird, wenn Sie mit der linken Maustaste auf das Symbol klicken. Wenn KGpg in der Kontrollleiste angezeigt wird führt das Schließen der Fenster dazu, dass das Programm minimiert wird. Wenn diese Option deaktiviert ist, beendet das Schließen des letzten Fensters das Programm.

Kapitel 4

Danksagungen und Lizenz

KGpg

Übersetzung Sebastian Steinseb.stein@hpfsc.de, Rolf Eike Beer kde@opensource.sf-tec.de