WIP – IKT Security Workshop

Informationssicherheit hat zum Ziel, die Verarbeitung, Speicherung und Kommunikation von Informationen so zu gestalten, dass die Vertraulichkeit, Verfügbarkeit und Integrität der Informationen und Systeme in ausreichendem Maß sichergestellt wird.

In den Kindertagen des (Personal-)Computers wurde unter Computersicherheit die Sicherstellung der korrekten Funktionalität von Hardware (Ausfall von z.B. Bandlaufwerken oder anderen mechanischen Bauteilen) und Software (richtige Installation und Wartung von Programmen) verstanden. Mit der Zeit änderten sich die Anforderungen an Computer (Internet, Speichermedien); die Aufgaben zur Computersicherheit mussten anders gestaltet werden. Somit bleibt der Begriff der Computersicherheit wandelbar und Spiegel der momentanen technologischen Welt.

Private und öffentliche Unternehmen sind heute in allen Bereichen ihrer Geschäftstätigkeit, Privatpersonen in den meisten Belangen des täglichen Lebens auf IT-Systeme angewiesen. Da neben der Abhängigkeit auch die Risiken für IT-Systeme in Unternehmungen in der Regel größer sind als für Computer und Netzwerke in privaten Haushalten, wird Informationssicherheit überwiegend in Unternehmen betrieben.

Inwieweit Computersicherheit auch für euch als Privatperson ein Thema ist, soll dieser Workshop zeigen.

Was bedeutet sicher:

Ein System wird als sicher bezeichnet, wenn der Aufwand für das Eindringen in das System höher ist als der daraus resultierende Nutzen für die AngreiferInnen. Deshalb ist es wichtig, die Hürde für einen erfolgreichen Einbruch möglichst hoch zu setzen und damit das Risiko zu reduzieren.

Wenn wir über Sicherheit sprechen, sollten wir uns überlegen was wir gegenüber Angriffen schützen möchten.

Es sind Daten (Informationen), die ihr gegen Mißbrauch (also Zugriff von fremden Personen) schützen möchtet. Es wird zwischen Datenschutz und Datensicherheit unterschieden. Informationen über das Datenschutzgesetz findet ihr unter
http://www.dsk.gv.at/dsg2000d.htm
Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 – DSG 2000).

Datenschutz

- Vertraulichkeit: Dateien dürfen nur von autorisierten BenutzerInnen gelesen werden.
- Übertragungssicherheit: Das Ausspähen der übertragenen Informationen zwischen Rechnern, Geräten und Benutzern soll verhindert werden.
- Privatsphäre: Persönlichkeitsdaten bzw. Anonymität müssen gewahrt bleiben.

Datensicherheit

- Funktionalität: Hardware und Software sollen erwartungsgemäß funktionieren.
- Integrität: Daten dürfen nicht unbemerkt verändert werden.
- Verfügbarkeit: Der Zugriff auf Daten muss innerhalb eines vereinbarten Zeitrahmens gewährleistet werden.
- Authentizität: Echtheit und Glaubwürdigkeit einer Person oder eines Dienstes müssen überprüfbar sein.
- Verbindlichkeit: Urheber von Veränderungen müssen erkennbar sein und dürfen Veränderung nicht abstreiten können.

Überwachung

Inzwischen wird in vielen Ländern der E-Mail-Verkehr vom Staat überwacht. In Deutschland sind seit dem Jahr 2005 InternetdienstanbieterInnen verpflichtet, entsprechende Hard- und Software bereit zu halten, um einer Überwachungsanordnung sofort Folge leisten zu können, ohne für die daraus erwachsenden Kosten einen finanziellen Ausgleich zu erhalten.

Authentizität und Schutz des Inhaltes

Die meisten E-Mail-Nachrichten werden im Klartext verschickt, können also prinzipiell auf jedem Rechner, den die Nachricht auf ihrem Weg vom Absender zum Empfänger passiert, gelesen werden. Zieht man eine Analogie zur Briefpost, ist eine E-Mail daher eher mit einer Postkarte vergleichbar als mit einem durch einen Umschlag vor neugierigen Blicken geschützten Brief.

Dies werden wir euch praktisch zeigen!

Ebenfalls ähnlich wie bei einem Brief oder einer Postkarte und genauso einfach lassen sich E-Mails mit einer falschen Absendeadresse verschicken, was zum Beispiel bei Spam (UCE/UBE) oft zu beobachten ist. Empfangsadresse, CC- und BCC-Adressen lassen sich gleichermaßen fälschen (address spoofing).

Die Lösung für diese beiden Probleme ist Verschlüsselung und Absenderauthentifizierung. Hierzu existieren (unter anderem) die Verfahren PGP und dessen freie Variante GnuPG, sowie S/MIME (vorwiegend im B2B-Bereich), die jedoch noch nicht besonders weit verbreitet sind. Selbst solche Verschlüsselungsverfahren decken lediglich den Inhalt der E-Mail ab, nicht die Betreff-Zeile oder das E-Mail-Datum. Dadurch können unter Umständen Rückschlüsse auf den Inhalt einer verschlüsselten Mail gezogen werden.

Überwachung ist ein Aspekt es Eingriffes in die Privatsphäre. Neben dieser Bedrohung für die IT-Sicherheit gehören weitere:

- **höhere Gewalt**, z.B. in Form von Blitzschlag, Feuer oder Überschwemmung
- Computerviren, Trojaner und Würmer, die zusammengefasst als **Malware** bezeichnet werden
- **Social Engineering**
- **Spoofing,** oder **Phishing,** wo eine falsche Identität vorgetäuscht wird
- **Hoax** (Falschmeldung)
- **Hacking, Cracking** sowie andere Formen von Sabotage
- **Spionage**, z.B. in Form von Man in the Middle Angriffen,

Wir gehen nicht auf alle diese Bedrohungen ein (z. B. höhere Gewalt). Computerviren Trojaner und Würmer, beispielsweise sind betriebssystemabhängig und bedrohen Windows System massiver als MacOS oder Linux. Hier ist auf eine regelmäßige Systempflege zu achten.

Social Engineering

Der Begriff Sozialkonstruktion bzw. englisch Social Engineering (auch Social Hacking) bezeichnet in der Soziologie das Erlangen vertraulicher Informationen durch Annäherung an GeheimnisträgerInnen mittels gesellschaftlicher Kontakte.

Dieses Vorgehen wird von Geheimdiensten und PrivatdetektivInnen seit langem praktiziert, der Begriff wird jedoch meist im Zusammenhang mit Computerkriminalität verwendet, da er hier das Gegenstück zum rein technischen Vorgehen (Engineering) beim Eindringen in fremde Systeme bildet.

Social Engeneering ist eine Strategie,Taktik oder auch Kunst Menschen zu analysieren, um auf ihr Profil zugeschnittene Werte weiterzugeben, die zu ihrem Nachteil führen (ca.99,9% aller Fälle). Social Engeneering ist ein Zusammenspiel von sozialer (Bekanntschaften), geistiger(Analyse) und körperlicher(Vokabular) Intuition, die einer Art Analyse-Berechnung gleicht. (mit Ergebnis = Manipulation)

Phishing
Phishing (engl. fishing = abfischen, die ursprünglich beim Kofferwort phreaking aufgetretene Abwandlung von f zu ph wird hier wegen der Konnotation der Hinterhältigkeit und betrügerischen Trickserei verwendet) ist eine Form der Tricktäuschung im Internet. Dabei wird per E-Mail versucht, den Empfänger irrezuführen und zur Herausgabe von Zugangsdaten und Passwörtern zu bewegen. Dies bezieht sich in den meisten Fällen auf Online-Banking und andere Bezahlsysteme.

Spoofing
Spoofing (aus dem Englischen, zu deutsch: „Manipulation“ oder „Verschleierung“) nennt man verschiedene Täuschungsversuche in Computernetzwerken zur Verschleierung der eigenen Identität.

Hoax

Ein Hoax (engl., Jux, Scherz, Schabernack; auch Schwindel) bezeichnet im Deutschen eine Falschmeldung, die sich per E-Mail, Instant Messenger oder auf anderen Wegen (SMS, MMS, ...) verbreitet, von vielen für wahr gehalten und daher an viele Freunde weitergeleitet wird. Das Wort kommt wahrscheinlich aus der Verkürzung von „Hokus” aus „Hokuspokus”. Ein Hoax kann auch als moderne Form der Zeitungsente oder als „Urban legend“ betrachtet werden.

Hacking

Hacking bezeichnet die Tätigkeit von ComputerexpertInnen, die aufgrund von fundiertem technischen Fachwissen Sicherheitslücken in Computersystemen aufzuspüren und ihre Erkenntnisse veröffentlichen, wodurch sie einen wertvollen Beitrag zu einer sichereren Softwareerzeugung leisten.

Während beim Hacken wirkliche Profis am Werk sind, stellen eine größere Bedrohung, die sogenannten Skriptkiddie dar.

Im Bereich der Computersicherheit steht der Begriff Skriptkiddie für eine Person, die keinE SicherheitsexpertIn ist, jedoch in einer meist unreifen Art vorgefertigte Programme oder Routinen benutzt, um Sicherheitsbarrieren zu überwinden oder um Vandalismus zu betreiben. Im Gegensatz zu einem Hacker agiert ein Skriptkiddie ohne Kenntnis darüber, wie die verwendete Schwachstelle funktioniert und wie sich neue Sicherheitslücken aufspüren lassen.

Cracken

Beim Cracken wird meist compilierte Software aufgebrochen und fremder Code in das Programm eingebracht. Das bekannteste Beispiele ist das Cracken vom Kopierschutz.

Spionage
Wie kann Spionage (Überwachung) aussehen:

- **Brute-Force-Methode**

Alle möglichen Schlüssel werden nacheinander durchprobiert. Die Reihenfolge wird gegebenenfalls nach der Wahrscheinlichkeit ausgewählt. Diese Methode ist auch bei modernen Verschlüsselungsverfahren sinnvoll, wenn von der Verwendung eines relativ schwachen Passwortes ausgegangen werden kann. Schon auf handelsüblichen Computern (Stand 2005) können ohne Weiteres mehrere hunderttausend Schlüssel pro Sekunde ausprobiert werden. Ein halbwegs ausgerüsteter Angreifer kann mehrere Millionen Schlüssel pro Sekunde testen.

- **Wörterbuch-Angriff**

Alle Schlüssel aus speziell zu diesem Zweck angefertigten Passwortsammlungen werden nacheinander durchprobiert. Die Reihenfolge wird gegebenenfalls nach der Wahrscheinlichkeit ausgewählt. Diese Methode ist auch bei modernen Verschlüsselungsverfahren sinnvoll, wenn von der Verwendung eines relativ einfachen Passwortes ausgegangen werden kann.

Auch das Ausprobieren aller denkbaren Wörter ist ohne weiteres möglich. Bei einem aktiven Wortschatz von 50.000 Wörtern pro Sprache können selbst auf handelsüblichen Rechnern dutzende Sprachen innerhalb weniger Sekunden ausprobiert werden. Ein einzelnes Wort als Schlüssel ist daher sehr unsicher.

- **Man-In-The-Middle-Angriff**

Man-In-The-Middle-Angriffe bedeutet dass auf einem Server die Daten abgefangen und manipuliert werden können.

Abhilfe durch Kryptografie

Kryptografie bzw. Kryptographie (vom griechischen kryptós, „verborgen“, und gráphein, „schreiben“) ist im ursprünglichen Sinne die Wissenschaft der Verschlüsselung von Informationen („Geheimschriften“). Heutzutage beschäftigt sie sich allgemein mit dem Schutz von Daten durch deren Transformation, in der Regel unter Einbeziehung von geheimen Schlüsseln. Die Kryptografie bildet mit der Kryptanalyse zusammen die Kryptologie.

Die moderne Kryptografie hat vier Hauptziele zum Schutz von Informationen:

- **Vertraulichkeit:** Nur dazu berechtigte Personen sollten in der Lage sein, die Daten oder die Nachricht zu lesen oder Informationen über ihren Inhalt zu erlangen.
- **Integrität:** Der Empfänger sollte in der Lage sein festzustellen, ob die Daten oder die Nachricht nach ihrer Erzeugung verändert wurden.

- **Authentizität:** Der Urheber der Daten bzw. der Absender der Nachricht sollte eindeutig identifizierbar sein, und seine Urheberschaft sollte nachprüfbar sein.
- **Verbindlichkeit:** Der Urheber von Daten oder Absender einer Nachricht sollte nicht in der Lage sein seine Urheberschaft zu bestreiten, d.h. sie sollte sich gegenüber Dritten nachweisen lassen.

Kryptografische Verfahren und Systeme dienen nicht notwendigerweise allen genannten Zielen.

Sensible Daten verschlüsseln

Daten, die nicht in die Hände Dritter geraten sollen, sollten durch geeignete Maßnahmen verschlüsselt werden. Dies betrifft nicht nur Daten die zwischen zwei bestimmten Rechnern ausgetauscht werden, sondern auch entsprechende Daten, die sich auf Massenspeichern befinden, und beim Übertragen sensibler Daten, wie zum Beispiel Kreditkartennummern, während des Surfens im Internet. Ein Zugriff auf die Inhalte darf nur dann möglich sein, wenn die Beteiligten über den richtigen Schlüssel verfügen. Besonders gefährdet sind unverschlüsselte, kabellose Netze, wie zum Beispiel nicht konfigurierte WLANs, da hierbei Unbefugte unbemerkt Zugriff auf die Daten und sogar die Kontrolle über den ungeschützten Computer erlangen können.

Passwörter, persönliche Identifikationsnummern (PIN) und Transaktionsnummern (TAN) dürfen auf keinen Fall unverschlüsselt gespeichert oder übertragen werden.

PGP – Pretty Good Privacy
Der Briefumschlag für elektronische Post
Grundsätzliches

Wozu E-Mails verschlüsseln?
E-Mails werden unverschlüsselt durch das Internet transportiert. Das heisst, es ist einerseits auch für andere als die gemeinten EmpfängerInnen möglich die E-Mailkommunikation mitzuverfolgen und bedeutet andererseits, dass es leicht ist diese auch zu manipulieren und damit zu stören. Der Grund wieso jemand an unserer E-Mailkommunikation Interesse hat, oder weshalb diese von Dritten verändert werden sollte, ist in den menschlichen Eigenschaften zu finden. Es gibt immer NeiderInnen oder feindlich gesinnte Menschen, die mit allen Mitteln versuchen werden, unsere Bemühungen und Tätigkeiten zu stören oder zu verhindern.

Abgesehen davon ist für dritte der Sinn einer E-Mailkommunikation und um was es wirklich geht, oft gar nicht verständlich, weil die mitlesende Person die Hintergründe und Zusammenhänge gar nicht kennt und dann falsche Schlußfolgerungen zieht. Diese Schlußfolgerungen können zu völligem Fehlverhalten führen und tatsächlichen Schaden

verursachen. (z.B.: „Das wird ein Bomben Fest“)
Abseits von den berechtigten Sorgen, dass Informationen in falsche Hände geraten, gibt es auch einen ganz einfachen Grund weshalb wir E-Mails verschlüsseln wollen: Wir haben ein Recht auf Privatsphäre und wir verschicken unsere Post schließlich auch in einem Kuvert.

Definitionen:

- **Schlüssel:** Als Schlüssel wird in diesem Zusammenhang eine Folge von Zahlen bezeichnet. Die Umwandlung der lesbaren Nachricht in die „Geheim“botschaft erfolgt auf Basis dieser Zahlenfolge nach einer mathematischen Formel.

- **verschlüsseln:** Aus einer lesbaren Nachricht eine „Geheim“botschaft machen.

- **entschlüsseln:** Aus einer „Geheim“botschaft eine lesbare Nachricht machen.

- **Kryptografie:** Bezeichnet Methoden der Verschlüsselung (Chiffrierung) und Entschlüsselung (Dechiffrierung) von Informationen.

- **Privatsphäre:** Eine Nachricht soll nur von den gewünschten AdressatInnen gelesen werden.

- **Authentifikation:** Eine Nachricht soll überprüfbarer Weise von der Person stammen, von der sie zu sein scheint.

- **Signatur:** Hierbei handelt es sich um ein „Echheitszertifikat“ für die Nachricht. Der/die VersenderIn signiert (=verschlüsselt mit dem privaten Schlüssel) einen signifikanten Teil der Nachricht und erzeugt die sogenannte Signatur. Das ist eine Zahlenfolge, die von dem/r EmpfängerIn verwendet werden kann um die Echtheit (=das also die Nachricht während des Transports durch das Internet nicht verändert wurde) festzustellen. (Dabei wird der öffentliche Schlüssel der/s Absenderin/s zum Entschlüsseln verwendet)

- **Komfort:** Die AnwenderInnen sollen sich keine unnötigen Gedanken darüber machen müssen, wo welcher Schlüssel aufbewahrt wird und welche Schlüssel für den Nachrichtenaustausch mit wem benutzt werden müssen.

Was ist PGP/GnuPG(Gnu Privacy Guard)?
PGP wurde Anfang 1990 von Philip Zimmerman entwickelt und diente militärischen Zwecke. Es ist ein Verfahren zur Verschlüsselung von Daten und damit ein wichtiges Werkzeug für eine E-Mail Kommunikation, die nicht von allen mitgelesen werden kann. E-Mails werden in der Regel vollkommen unverschlüsselt über das Internet übertragen. Das muß nicht sein. Wir können den Inhalt vor dem Verschicken verschlüsseln. Das ist so wie wenn wir den Brief in ein Kuvert steckten. Der/die EmpfängerIn muß die E-Mail dann wieder entschlüsseln und kann dann den Inhalt lesen. Das ist dann so wie wenn er/sie den Brief öffnet.

Früher war PGP Freeware und vollkommen kostenlos für jedermann. Mittlerweile ist dies

leider nicht mehr der Fall und die Standard PGP Version kostet Geld. Es gibt nur eine kostenlose Personal Version, die aber nicht in vorhandene E-Mail Programme eingebunden werden kann.

Deswegen und weil bei den neueren Versionen der Quellcode nicht mehr bzw. erst später freigegeben worden sind ist, wurde eine Gnu PGP Version entwickelt. Diese Version ist Open Source unter der GPL Lizenz. GnuPG hält sich an den 1997 entwickelten OpenPGP Standard und somit können auch GnuPG und PGP BenutzerInnen gegenseitig ihre E-Mails ver- bzw. entschlüsseln.

PGP verwendet ein Verschlüsselungverfahren, das auf öffentliche und private Schlüssel basiert. Was genau dies bedeutet und wie PGP in der Praxis funktioniert, folgt weiter unten.

Ich beziehe mich in diesem Tutorial auf die GnuPG Version, da wie gesagt die aktuelle PGP Version nicht mehr kostenlos zu bekommen ist. Wenn ich im Tutorial also PGP schreibe, dann meine ich damit auch GnuPG.

Die verschiedenen Verschlüsselungstechniken

Symmetrische Kryptografie
Es gibt einen Schlüssel, der für das Ver- und für das Entschlüsseln benutzt wird.
Diese Art von Verschlüsselung hat den Vorteil, dass sie sehr schnell berechnet werden kann und es genügen relativ kurze Schlüssel(128-256Bit), damit die Daten sicher sind. Aber die Nachteile liegen eigentlich auf der Hand. Bevor man einen symmetrischen Schlüssel benutzen kann, muss dieser erst einmal mit der/m EmpfängerIn ausgetauscht werden und das auf einem hinreichend sicheren Kanal. Ich kann diesen Schlüssel also nicht einfach mal per Mail verschicken, da eine E-Mail nun mal nicht sicher ist.

Dann ist die Schlüsselanzahl noch ein gewaltiges Problem. Damit jedeR mit jedem/r sicher kommunizieren kann, benötigt man bei n TeilnehmerInnen n*(n-1)/2 Schlüssel, das wären bei 20 TeilnehmerInnen schon 190 verschiedene Schlüssel. Das ist praktisch kaum machbar, also fällt die symmetrische Verschlüsselung eigentlich schon einmal für die E-Mail Kommunikation weg.

Asymmetrische Kryptografie
Hier gibt es einmal einen privaten Schlüssel und einen zweiten öffentlichen Schlüssel. Der private Schlüssel muss geheim bleiben und der öffentliche Schlüssel kann und muss zugänglich sein. Dazu ein Beispiel:
Alice will Bob Daten schicken. Da diese Daten aber privat sind, müssen sie verschlüsselt werden.

Nun schickt Bob zu Alice erst einmal seinen öffentlichen Schlüssel. Da dieser nicht geheim ist, kann Bob diesen Schlüssel z.B. einfach per E-Mail an Alice verschicken. Alice verschlüsselt nun die Daten mit Hilfe des öffentlichen Schlüssels von Bob und verschickt diese Daten nun an ihn. Nachdem Bob die Daten bekommen hat, kann er diese Daten wieder mit Hilfe seines privaten Schlüsseln entschlüsseln.

Allgemein gesagt bedeutet dies: Der/die VersenderIn muss die Daten immer mit dem öffentlichen Schlüssel des/r Empfängers/in verschlüsseln und der/die Empfänger/in entschlüsselt diese Daten mit seinem/ihrem privaten Schlüssel.

Da die öffentlichen Schlüssel nicht geschützt werden müssen und vielleicht durch einen öffentlichen Schlüssel-Server erreichbar sind, ist die asymmetrische Verschlüsselung in dieser Hinsicht für unsere E-Mail Kommunikation geeignet. Aber auch die asymmetrische Verschlüsselung hat ihre Nachteile. Sie basiert auf sehr komplexen mathematischen Formeln(Primzahlenzerlegung, diskrete Logarithmus) und verwendet relativ lange Schlüssel (1024 - 4096 bit). Dadurch ist die Verschlüsselung zu langsam für die Datenmengen von (grossen) E-Mail-Nachrichten.

Hybride Kryptografie - PGP
Die Vorteile von beiden Verfahren wird nun in der hybriden Kryptografie verschmolzen. Anstatt nun die komplette Nachricht mit einem asymmetrischen Schlüssel zu verschlüsseln, wird in der hybriden Kryptografie die Nachricht mit einem symmetrischen Schlüssel verschlüsselt. Anschließend wird dieser symmetrische Schlüssel mit dem öffentlichen Schlüssel des/r Empfängers/in asymmetrisch verschlüsselt.
Der/die EmpfängerIn entschlüsselt asymmetrisch nun mit Hilfe seines/ihres privaten Schlüssels den symmetrischen Schlüssel und kann dann damit die Nachricht symmetrisch entschlüsseln.
Damit ist die Verschlüsselung schnell und man hat keine Probleme mit dem Schlüsselaustausch. Sie ist somit optimal für die E-Mail Kommunikation geeignet.

Ein anderes Beispiel für eine hybride Verschlüsselung wären SSL Verbindungen, also immer wenn der Web Browser eine verschlüsselte Verbindung zu einem Server aufnimmt. Dies drückt sich in der Adresszeile dadurch aus, dass zu Beginn https://...(das s steht für sicher im Sinne von verschlüsselt, nicht mitlesbar) steht, und in der Statuszeile des Webbrowsers ein geschlossenes Vorhängeschloss-Symbol angezeigt wird.

Anwendung von PGP
1. Erzeugung des Schlüsselpaares
   Als erstes muss jedeR PGP BenutzerIn sich ein Schlüsselpaar generieren. Dort ist der private und der öffentlich Schlüssel enthalten.

2. Bekanntgabe des öffentlichen Schlüssels
   Zusätzlich müssen noch die öffentlichen Schlüssel der KommunikationspartnerInnen bekannt sein, bzw. diesen der eigene öffentliche Schlüssel bekannt gegeben werden. Diese Schlüssel sind auf verschiedene Wege erhältlich. Per E-Mail, auf Diskette oder auch von einem öffentlichen Schlüsselserver, auf dem die BenutzerInnen ihre öffentliche Schlüssel speichern können. Am sichersten ist allerdings den Schlüssel direkt von der Person ausgedruckt und übergeben zu bekommen. Das geschieht am besten bei einer sogenannten „Key-signing“-Party

3. Verschlüsseln von E-Mails
   Die Nachrichten werden immer mit dem öffentlichen Schlüssel des/r Empfängers/in verschlüsselt und dieser kann dann mit seinem privaten Schlüssel diese Nachricht wieder entschlüsseln.
   Eine Nachricht, die der/die VersenderIn mit dem öffentlichen Schlüssels des/r Empfängers/in verschlüsselt hat, kann der/die VersenderIn nicht wieder entschlüsseln. Das Entschlüsseln funktioniert nur mit dem dazugehörigem privaten Schlüssel.

4. „Unterschreiben“ von E-Mails
   Mit PGP ist es nicht nur möglich E-Mail zu verschlüsseln, sondern man kann diese auch noch, unabhängig von der Verschlüsselung, signieren bzw. "unterschreiben".
   Das Signieren läuft ganz ähnlich ab, wie die Verschlüsselung, nur dass der/die VersenderIn die E-Mail mit seinem/ihrem privaten Schlüssel signiert (=verschlüsselt).

5. Kontrollieren der Signatur
   Der/Die EmpfängerIn kann nun diese Signatur mit Hilfe des öffentlichen Schlüssels von dem/r VersenderIn auf ihre Gültigkeit überprüfen. Somit ist sichergestellt, dass die E-Mail wirklich von dem/r angegebenen VersenderIn kommt und das diese E-Mail unterwegs nicht verändert worden ist.

Kochrezept GPG/PGP
Voraussetzungen:
Thunderbird mit OpenPGP Erweiterung

Das gewählte E-Mailprogramm eignet sich wegen seiner freien Verfügbarkeit und der sehr gut gestalteten OpenPGP Erweiterung hervorragend um PGP auch praktikabel und einigermaßen komfortabel verwenden zu können.

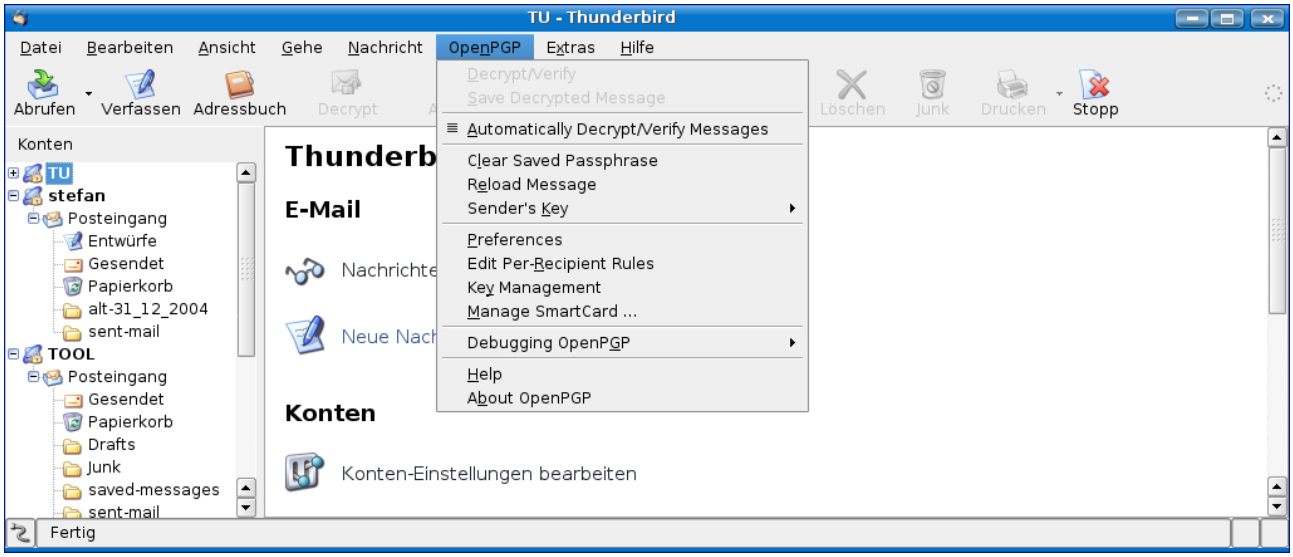
GPG Programm

Dieses muß ebenfalls installiert sein, da es die Ent- und Verschlüsselung vornimmt und auch für die Schlüsselerzeugung zuständig ist. Es kann über die OpenPGP Erweiterung von Thunderbird bequem genutzt werden.

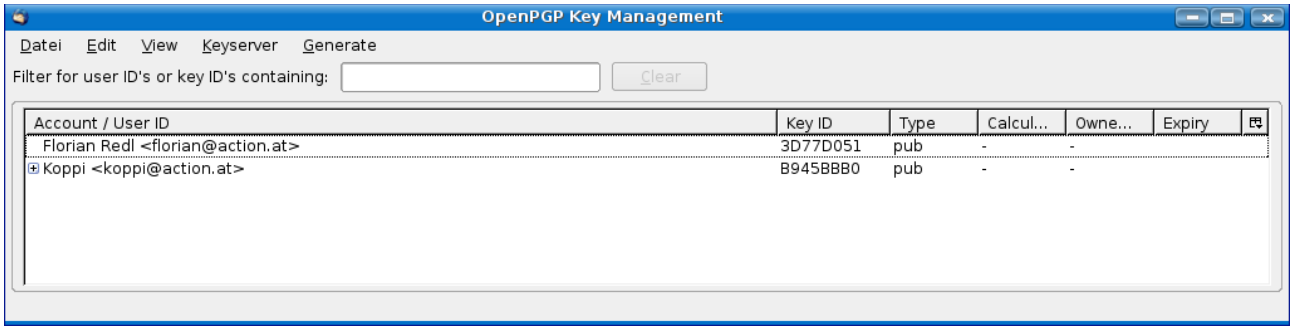
Jetzt geht es los!

1. Thunderbird starten.

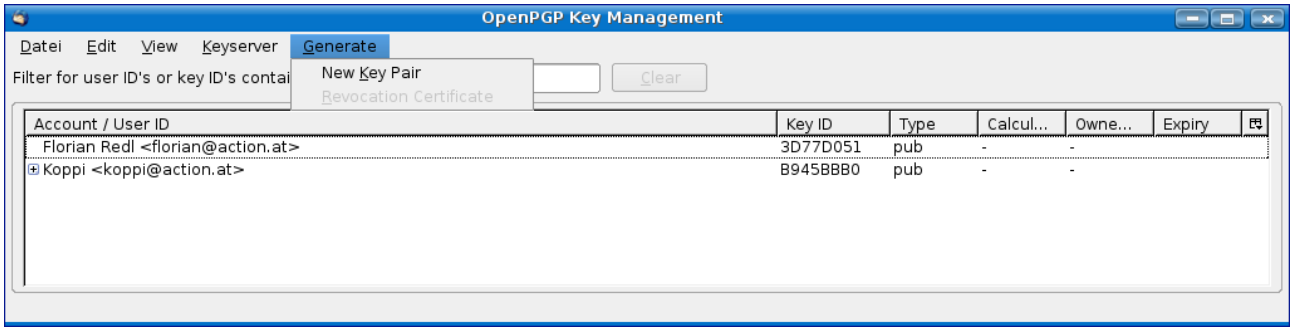
2. Im Menü „OpenPGP“ den Punkt „Key Management“ anclicken.



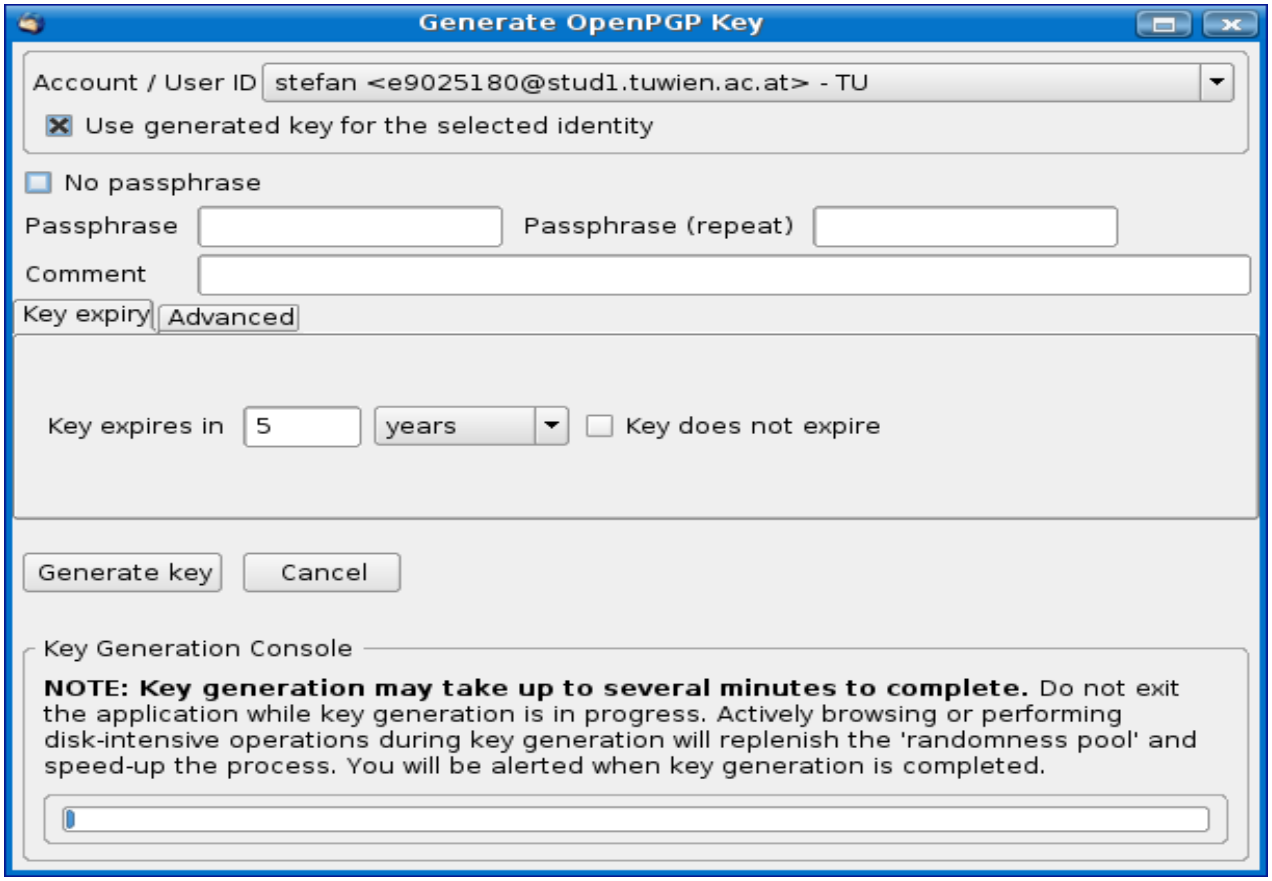
3. Es erscheint ein Fenster mit dem Titel „OpenPGP Key Management“. Hier werden die bereits vorhandenen Schlüssel – sofern welche vorhanden – in Listenform angezeigt.



4. Im Menü „Generate“clicken wir „New Key Pair“ an, um für uns ein neues Schlüsselpaar zu erzeugen.



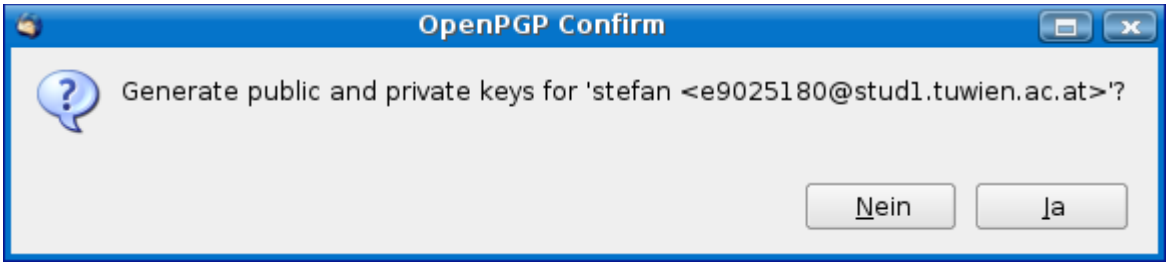
5. Erneut öffnet sich ein weiteres Dialogfenster. In diesem wird unsere email Adresse angezeigt und wir könnten einige Einstellungen vornehmen. Wir beschränken uns hier auf die notwendigsten.



Die wichtigsten Felder sind hier nun das Passphrase-Feld mit der Bezeichnung „Passphrase“ und daneben das Wiederholungsfeld „Passphrase (repeat)“.
Hier geben wir jeweils unsere geheime Passphrase ein. (Die Passphrase sollte mindestens 12 Zeichen haben und eine Mischung von Groß- und Kleinbuchstaben sowie Zahlen sein. Beispiel: „KriegundFrieden1947“)

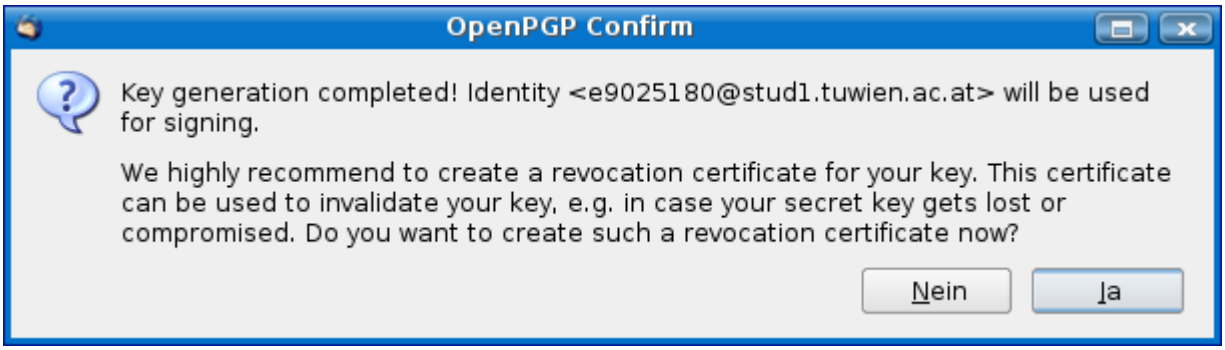
6. Sobald wir unsere geheime Passphrase eingegeben haben, clicken wir auf den Knopf mit der Beschriftung „Generate key“.

7. Nun erscheint eine Box (Fenster) mit der Frage ob wir einen privaten und öffentlichen Schlüssel für die angegebene email-Adresse erzeugen möchten. Diese Frage beantworten wir indem wir auf den Knopf mit „ja“clicken.



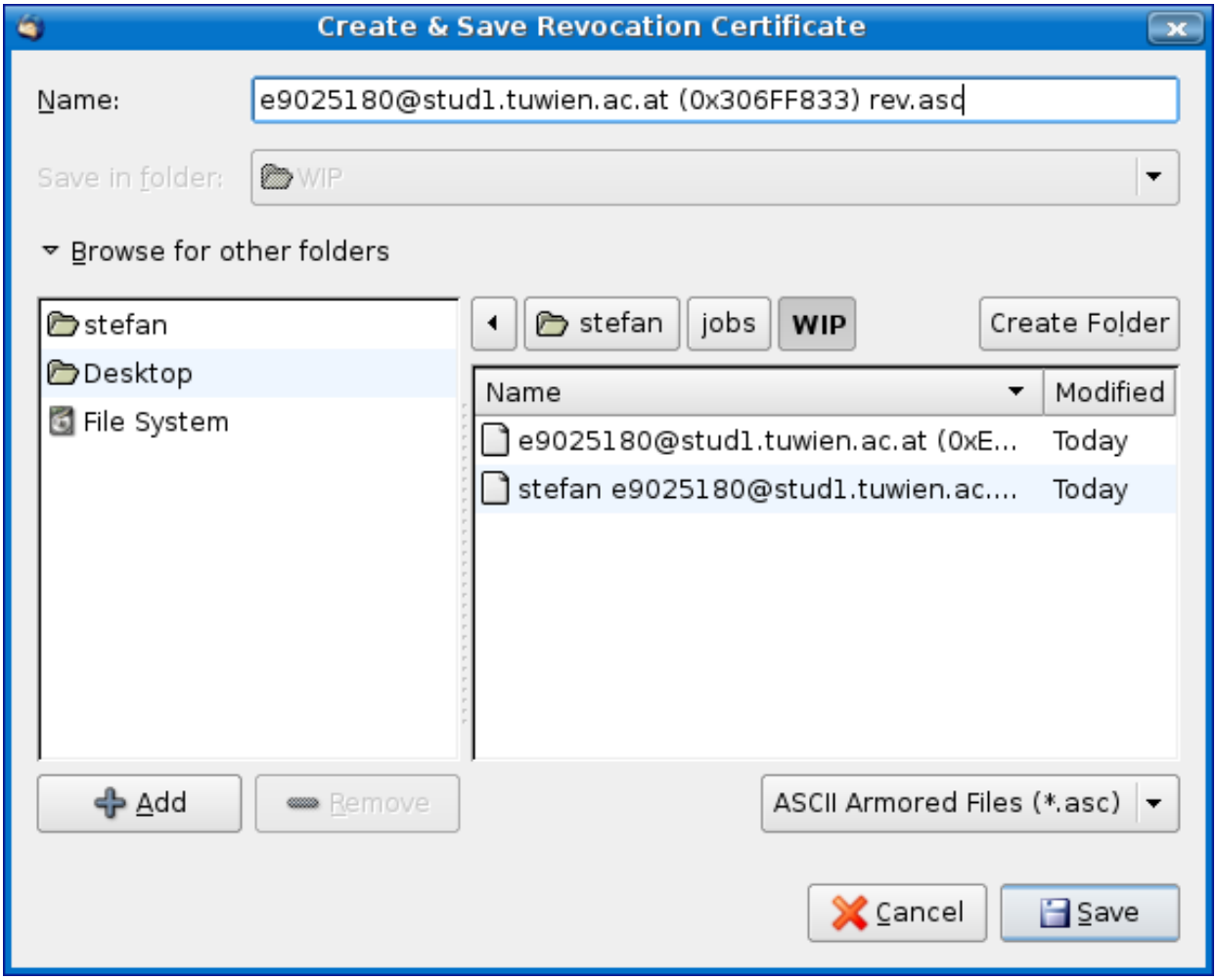
8. Nun verschwindet die Fragebox (das Fragefenster) und es scheint nichts zu passieren. Tatsächlich wir im Hintergrund das Schlüsselpaar erzeugt. Wir können und sollen jetzt irgendetwas beliebiges machen. Z.B. ein kleines Spiel am Computer spielen, im Internet herumsurfen, unsere Dateien auf dem Computer zusammenräumen oder uns ein Lied vom Computer vorspielen lassen. Dies hilft bei der Generierung von Zufallszahlen, die notwendig sind um ein gutes Schlüsselpaar zu erzeugen. Ich möchte an dieser Stelle jedoch nicht weiter auf die mathematischen Modelle die hier zugrunde liegen eingehen.

9. Sobald das Schlüsselpaar erzeugt ist, erscheint ein Dialogfenster mit der entsprechenden Information und der Frage ob auch der Revocationsschlüssel erzeugt werden soll.

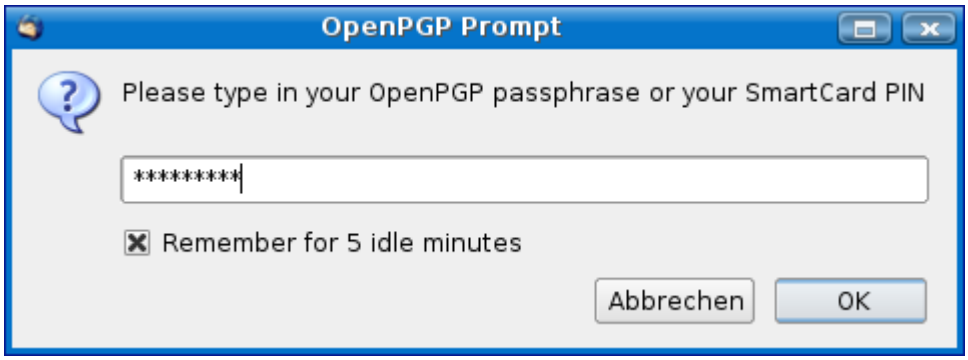


Dabei handelt es sich um einen Schlüssel, mit dessen Hilfe ein veröffentlichter Schlüssel wieder aus dem Verkehr gezogen werden kann. Dies ist notwendig falls die Passphrase vergessen wird oder der Schlüssel in falsche Hände geraten ist. Allerdings sollte auch dieser Schlüssel gut verwahrt werden, da auch Dritte diesen Schlüssel zum deaktivieren verwenden können! Am besten wird der Revocationsschlüssel auf einem externen Speicher, wie Diskette, CD oder USB Stick gespeichert und dieser Speicher sollte vor Dritten geschützt aufbewahrt werden. Wir clicken auf den Knopf „Ja“.

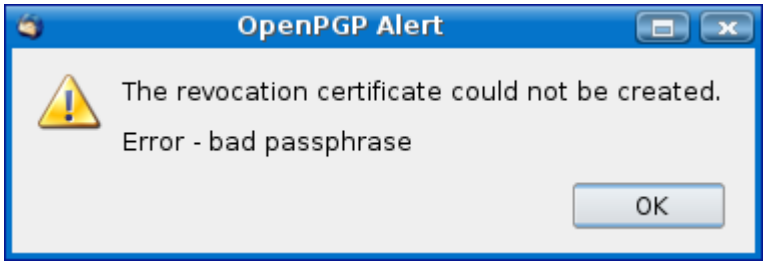
10. Es erscheint ein Speicherdialogfenster, wo wir nun angeben können wohin der Revocationsschlüssel gespeichert werden soll. Wir können diesem auch einen unverdächtigeren Namen geben. Es handelt sich dabei um eine reine Textdatei, die wir bei Bedarf laden und anwenden können. (siehe dazu Punkt Revocation – Schlüsselrückruf)



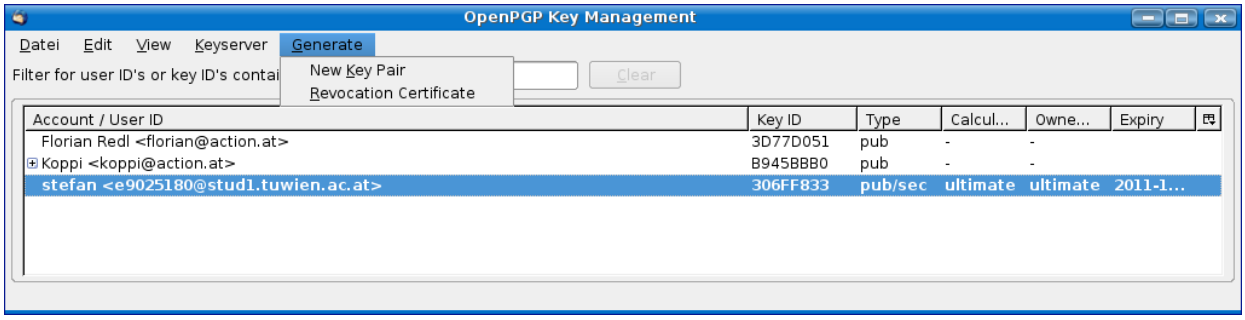
11. Es erscheint eine Dialogfenster mit der Aufforderung unsere Passphrase einzugeben. Bevor der Schlüssel tatsächlich erzeugt wird müssen wir nun zum ersten Mal nach der Einrichtung unsere Passphrase eingeben. Hoffentlich haben wir sie uns gut gemerkt!



12. Falls wir uns geirrt haben erscheint die Meldung, dass unser Passphrase falsch war und wir müssen auf den Knopf „Ok“ clicken. Der Revocationsschlüssel wurde in diesem Fall NICHT erzeugt!!

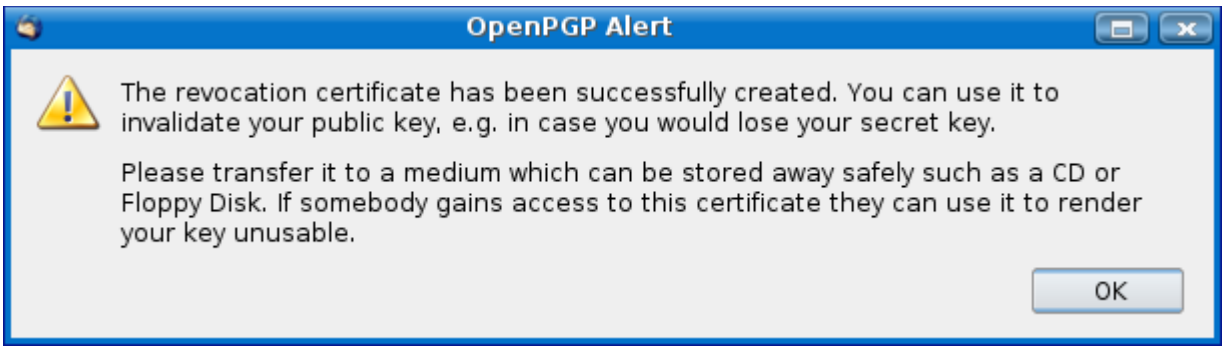


13. Um diesen im Nachhinein doch noch zu erzeugen clicken wir mit der linken Maustaste auf unser neu erzeugtes Schlüsselpaar in der Schlüsselliste im Fenster mit dem Titel „OpenPGP Key Management“. Unser Schlüssel ist in Fettbuchstaben hervorgehoben und nachdem wir ihn angeclickt, sprich selektiert haben clicken wir wieder auf das Menü „Generate. Dort wählen wir nun den 2. Eintrag nämlich den



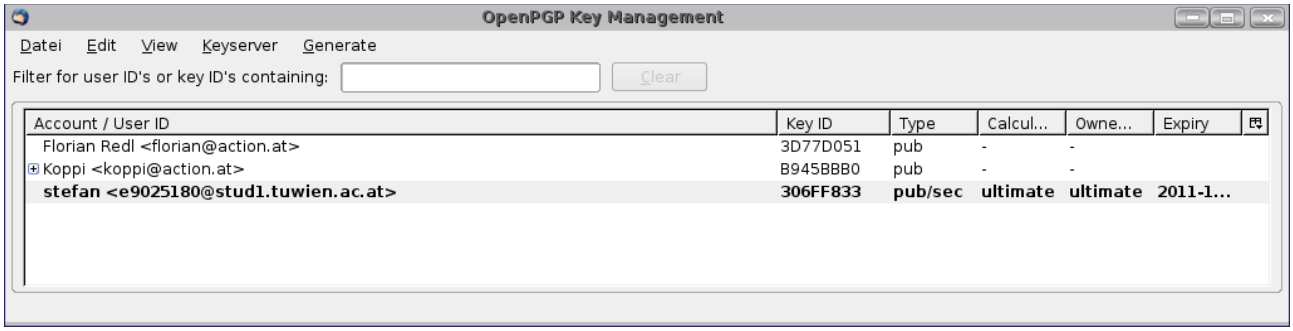
Punkt „Revocation Certificate“ aus.
Es erscheint wieder das Speicherdialogfenster, wo wir erneut den vorgeschlagenen Namen ändern können, den Speicherordner wählen und sodann auf den Knopf „Save“ zum Speichern drücken können. Jetzt geht es weiter bei Punkt 11.!

14. Wenn nun alles geklappt hat erhalten wir die Meldung über die erfolgreiche

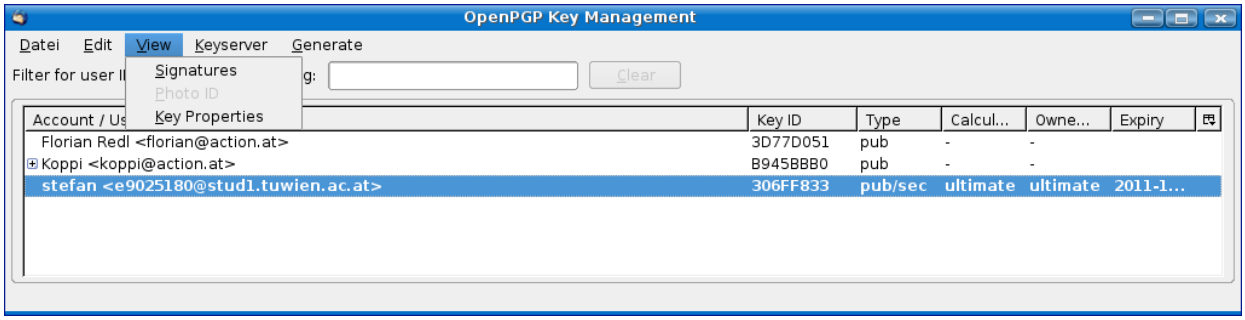


Erstellung des Revocationsschlüssels sowie den Hinweis wie dieser verwahrt werden sollte. Wir bestätigen diese Information indem wir auf „Ok“ clicken.

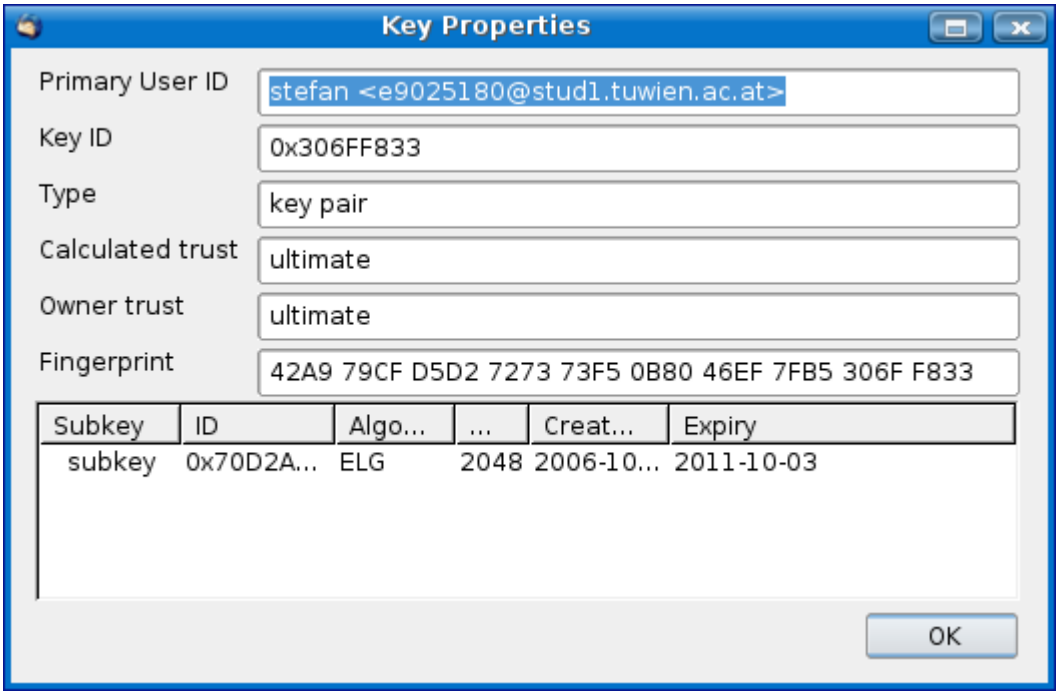
15. Fertig!!!
    Wir sehen nun unseren Schlüssel in der Schlüsselliste des Fensters mit dem Titel „OpenPGP Key Management“.



16. Eine sehr wichtige Funktion ist das Anzeigen des sogenannten Fingerprints. Hierbei handelt es sich um eine Folge von Zahlen aus dem Hexadezimalsystem anhand derer die Echtheit eines Schlüssels gegen geprüft werden kann. Wir selektieren unseren Schlüssel und wählen im Menü „View“ den Punkt „Key properties“ aus um den Fingerprint unseres Schlüssels abzulesen..



17. Es erscheint Informationsfenster mit Informationen über unseren Schlüssel. Hier können wir nun den Fingerprint unseres Schlüssels in unsere PGP-Keysigningpartyliste oben rechts eintragen. Damit ermöglichen wir den anderen die Kontrolle, ob sie unseren echten öffentlichen Schlüssel von uns haben. Denn wenn der fingerprint, den sie von uns haben mit dem von uns notierten übereinstimmt dann verwenden sie tatsächlich den von uns erzeugten öffentlichen Schlüssel!



18. Die fingerprints von den anderen öffentlichen Schlüsseln erfahren wir indem wir in Schlüsselliste den entsprechenden Schlüssel anclicken und wiederum im Menü „View“ den Eintrag „Key properties“ auswählen!

Workshop Facts
Donnerstag 9.November 2006
LeiterInnen: Pam, Peter, Petra, Stefan

Literatur:

Die Kunst der Täuschung; Risikofaktor; Mensch Kevin D. Mitnick; Mitp-Verlag; Auflage: 1 (April 2003) ISBN 3-826-1569-7

Die mitp-Hacker-Bibel; Ryan Russel et al; Mitp-Verlag; Auflage: 2 (2004) ISBN 978-3-8266-0926-8

Snort, Acid & Co.; Einbruchserkennung mit Linux; Thomas Bechtold, Peer Heinlein; open source PRESS (2004) ISBN 3-937514-03-1

Computersicherheit; Technik, Methoden, Schutz; Michael Diederich; WIKI Press ISBN-10: 3-86640-007-1

Ein wirklich guter Link: http://de.wikipedia.org/wiki/Computersicherheit