Sichere E-Mails mit GnuPG

Verschlüsselung und Signatur von Salvatore Spadaro



Autor : Lizenz: Version: Datum : Salvatore Spadaro FDL (Free Documentation Licence) 0.1.1 beta 6. Dezember 2005

1 Weshalb sich Gedanken über Sicherheit machen?	3
2 Was ist Verschlüsselung?	5
2.1 symmetrische & asymmetrische Verschlüsselung	6
2.2 Vorteile & Nachteile der beiden Verfahren	6
2.3 Hybride Verschlüsselung	6
3 Was ist eine kryptografische Signatur?	7
4 Welche Krypto-Tools brauche ich?	9
4.1 Was ist GnuPG?	9
4.2 Warum geht diese Anleitung nicht auf PGP ein?	9
5 Installation von GnuPT-Light	10
6 Thunderbird Enigmail	14
6.1 Erstellung eines Keyrings	14
6.2 Erstellung eines Widerrufs-Zertifikats	18
6.3 Public Key auf Keyserver kopieren	19
6.4 Mails signieren	23
6.5 Mails verschlüsseln	26
7 Quellenangeben	28
7.1 Print-Medien	28
7.2 Internet	28
7.3 Grafiken	28

1 Weshalb sich Gedanken über Sicherheit machen?

"The security of electronic mail sent through the Internet may be described in exact three words: there is none." - Matt Bishop

Viele Leute fragen sich wozu sie den Mehr-Aufwand für die Einrichtung von Verschlüsselungs-Systemen wie GnuPG oder PGP betreiben sollen. PC-Lainen tun sich gewöhnlicherweise sehr schwer sich in das Thema Kryptografie bzw. Mail-Security einzuarbeiten – sie werden meist ohne Erklärungen oder gar Hilfestellungen mit Begriffen wie "RSA", "IDEA", "Public Key" u.a konfrontiert. Oft hört sich dieses Fachchinesisch viel komplizierter an als es ist. Sie müssen weder Kryptologe noch Informatiker sein um Ihre Mails zu verschlüsseln oder zu signieren – mit Hilfe dieser Anleitung wird es Ihnen möglich sein für ein gewisses Maß an Sicherheit zu sorgen.

Jetzt aber zurück zur zentralen Frage "Warum sollte man sich Gedanken über Sicherheit und Verschlüsselung machen?". Nun, die Frage wurde eigentlich bereits durch das Zitat von Matt Bishop beantwortet, die Sicherheit des Internets und damit auch des Mail-Verkehrs kann tatsächlich mit 3 Worten beschrieben werden: "Es gibt keine". Unter Berücksichtigung kryptografischer Signier- und Verschlüsselungsmethoden ist zwar immer noch keine 100prozentige Sicherheit gegeben, es ist aber Unterschied, ob Sie Bargeld in einem Schaufenster sichtbar aufbewahren oder es zu Hause in einem Möbeltresor verstecken. Der Versand von E-Mails verhält sich ähnlich wie das genannte Beispiel mit dem Geld – wird eine E-Mail verschickt, passiert sie einige Zwischenstationen ähnlich wie ein gewönlicher Brief, nur das es sich bei der E-Mail um Knotenpunkte und Router handelt und nicht um Brief- und Frachtzentren der deutschen Post. Der Haken an der Sache ist, dass E-Mails standardmäßig im Reintext übertragen werden und sich ohne größeren Aufwand von neugierigen Personen oder Hackern, abfangen, lesen oder sogar manipulieren lassen. Oft werden über solche Vorgehensweisen Viren in Netzwerke eingeschleust oder in schlimmeren Fällen Industriespionage betrieben, in diesen Fällen spricht man von der sogenannten "Men-in-the-Middle-Attack", wobei sich ein Spion mit Hilfe von spezieller Software bewusst zwischen den Sender und dem Empfänger einklinken kann um alle Informationen abzuhören.

Auch wenn die Mail-Korrespondenz privat ist, wollen Sie bestimmt nicht, dass sich Fremde Ihre Liebesbriefe unter den Nagel reisen oder sich als Ihre Freunde oder Bekannte ausgeben um an wichtige Informationen heranzukommen (Stichwort Social Engineering). Oder etwa doch? Oftmals werden vertraute Nachrichten wie z.B. wichtige Bestellungen, Rechnungen, Formulare usw. per Mail verschickt - meistens ist dem User leider nicht bewusst welche Auswirkungen eine unsichere Mail-Kommunikation haben kann. Will man die private oder geschäftliche E-Mailkorrospondenz sicherer gestalten sollte man sich mit den beiden kryptografischen Verfahren, Verschlüsselung und Signierung beschäftligen und mit Hilfe sogenannter "Krypto-Tools" welche noch beschrieben werden auseinander setzen.

2 Was ist Verschlüsselung?

Die Verschlüsselung wird eingesetzt um einen Klartext mit Hilfe eines bestimmten Verschlüsselungs-Algorithmus in einen codierten Text umzuwandeln, dabei kommen je nach Verschlüsselungsverfahren ein oder mehrere Schlüssel (Keys) zum Einsatz um die Botschaft wieder zu entschlüsseln.

Die Wissenschaft der Verschlüsselungsmethoden wird als Kryptografie bezeichnet. Das Forschungsgebiet Kyrptoanalyse beschäftigt sich hingegen ausschließlich mit der Entschlüsselung und Überprüfung kryptografischer Verfahren (Kryto-Algorithmen).

Bekannte Verschlüsselungsalgorithmen sind z.B. ElGamal, CAST5, Triple DES (3DES), AES (Rijndael), Blowfish, RSA, IDEA u.v.m. In folgender Grafik wird Ihnen in vereinfachter Form, das Verschlüsselungschema dargestellt.



2.1 symmetrische & asymmetrische Verschlüsselung

Hauptunterschied zwischen "symmetrischer" und "asymmetrischer" Verschlüsselung ist, dass bei der symmetrischen Verschlüsselung nur 1 Schlüssel für die Ver- und Entschlüsselung zum Einsatz kommt. Die "asymmetrische" Verschlüsselung hingegeben verwendet Public Key und Private Key.

2.2 Vorteile & Nachteile der beiden Verfahren

Hauptunterschied zwischen "symmetrischer" und "asymmetrischer" Verschlüsselung ist, dass bei der symmetrischen Verschlüsselung nur 1 Schlüssel für die Ver- und Entschlüsselung zum Einsatz kommt. Die "asymmetrische" Verschlüsselung hingegeben verwendet Public Key und Private Key.

2.3 Hybride Verschlüsselung

Um die Vorteile der "symmetrischen" & "asymmetrischen" Verschlüsselung zu verbinden wurde das "Hypride Verschlüsselungsverfahren" entwickelt, dieses kommt bei "GPG" und "PGP" zum Einsatz.

3 Was ist eine kryptografische Signatur?

Eine kryptografische Signatur dient in erster Linie dazu die Identität des Absenders sicherzustellen, so dass gefälschte E-Mails sofort erkannt werden können. Mit Hilfe des privaten Schlüssels wird ein sogenannter Hash-Wert (Prüfsumme) gebildet und mit der signierten E-Mail verschickt, der Empfänger besorgt sich anschließend den Public Key des Senders und bildet ebenfalls den Hash-Wert der Mail – stimmen die beiden Prüfsummen überein wird die E-Mail als vertrauenswürdig eingestuft, es kann davon ausgegangen werden das die E-Mail nicht gefälscht wurde.

Signierung durch Absender:



Signierung durch Absender

Hinweis:

Die grafischen Abbildungen stammen aus der Anleitung Einführung in die Kryptographie von Network Associates, jetzt PGP Corporation, zu PGP 6.5.1 International.

Signaturprüfung durch Empfänger:



Signaturprüfung durch Empfänger

4 Welche Krypto-Tools brauche ich?

Für die E-Mail-Verschlüsselung/Signierung benötigt man drei Tools:

- GnuPG: übernimmt die Schlüssel-Erstellung
- Mozilla Thunderbird
- Enigmail: Plug-in f
 ür Thunderbird als GPG-Implementierung

Bevor Sie mit Thunderbird Enigmail einen Keyring erzeugen können, müssen Sie die Software GnuPG installieren, welche die Schlüsselerzeugung übernimmt. Mit Enigmail alleine können Sie noch keinen Schlüssel generieren! Die Schlüsselverwaltung des Tools WinPT (enthalten in der Krypto-Suite GnuPT) ist meiner Meinung nach besser als die Enigmail-Schluesselverwaltung wir empfehlen hnen trotzdem den Einsatz von GnuPT-Light, in diesem Paket ist die Schlüsselverwaltung WinPT nicht enthalten, der Grund warum wir Ihnen von WinPT abraten möchten, ist die Instabilität des Programms. Die aktuelle Version befindet sich noch im Entwicklungsstadium, bei Versuchen auf diversen Test-Rechnern kam zu Programm-Abstürzen.

4.1 Was ist GnuPG?

GnuPG läuft unter den meisten Betriebssystem, Linux, Windows, Mac OS etc. werden vollständig unterstützt. Das Programm wurde vom Bundesministerium für Wirtschaft und Arbeit (BMWA) und Bundesministerium für Inneres (BMI) unter der Aktion "Sicherheit im Internet" finanziell gefördert um Verschlüsselung für jedermann zu ermöglichen.

4.2 Warum geht diese Anleitung nicht auf PGP ein?

PGP unterscheidet sich vom Funktionsprinzip von GPG kaum. Ein kravierender Nachteil zu GPG ist aber, dass PGP mit kommerziellen und teilweise nicht offen gelegten Verschlüsselungsverfahren arbeitet, dies ist eine gewisse Sicherheitslücke da die propritäre Software keinen Zugriff auf den Quellcode gewährt, dies bürgt immer die Gefahr von sog. Backdoors (Hintertüren).

5 Installation von GnuPT-Light

Gleich zu Beginn der GnuPT-Light-Installation werden Sie auf folgendes hingewiesen: Sollten Sie nicht als Hauptbenutzer/Administrator angemeldet sein, so muss der Installationsordner angepasst werden.

Setup	×
?	Wichtige Information zur Installation mit lediglich Benutzerrechten: Wenn Sie auf Ihrem PC unter Windows 2000/XP/2003 lediglich Benutzer- Rechte und keine Hauptbenutzer/Administrator-Rechte besitzen, dann müssen Sie das Installations-Verzeichnis von 'C:\Programme' nach 'Dokumente und Einstellungen\IhrBenutzername' ändern.

Klicken Sie auf "Weiter" um mit der Installation fortzufahren:



Bitte die Lizenzbedingungen (GNU GPL) durchlesen und die Vereinbarung bestätigen:

Nachfolgend erscheinen "Wichtige Informationen zur Installation" die Sie sich bitte auch aufmerksam durchlesen. Weiter geht's mit "Weiter" ;-)

Setup	X
Information Lesen Sie bitte folgende, wichtige Informationen bevor Sie fortfahren.	z
Klicken Sie auf "Weiter", sobald Sie bereit sind mit dem Setup fortzufahren.	
Wichtige Informationen zur Installation	-
Dieses Installations-Programm installiert lediglich den Gnu P rivacy G uard (GnuPG) auf Ihrem PC. Sollten Sie auch eine grafische Oberfläche benötigen, dann laden Sie bitte dieses Installations-Programm herunter: <u>http://www.equipmente.de/viewtopic.php?p=864#864</u>	
Sie sollten alle installierten, älteren Versionen von GnuPG zuerst deinstallieren, bevor Sie fortfahren.	
Info <u>http://www.equipmente.de</u> < <u>Z</u> urück <u>W</u> eiter >	Abbrechen

Bitte den Pfad für die Installation angeben (dieser kann je nach Konfiguration unterschiedlich sein)

Setup
Ziel-Ordner wählen Wohin soll GnuPT-Light 0.4 installiert werden?
Das Setup wird GnuPT-Light 0.4 in den folgenden Ordner installieren.
Klicken Sie auf "Weiter", um fortzufahren. Klicken Sie auf "Durchsuchen", falls Sie einen anderen Ordner auswählen möchten.
C:\Programme\GPG\GnuPT-Light Durchsuchen
Mindestens 3,1 MB freier Speicherplatz ist erforderlich.
Info <u>http://www.equipmente.de</u> < <u>∠</u> urück <u>W</u> eiter > Abbrechen

Falls Sie bereits über GPG-Schlüssel verfügen bitte das entsprechende Verzeichnis angeben, andernfalls ist es ratsam eines an einem sichern Ort (USB-Stick, Diskette etc.) zu erstellen.

Setup	×
Home Verzeichnis Hier können Sie festlegen, in welchem Verzeichnis Sie Ihre Schlüss ablegen möchten.	elpaare
Bitte geben Sie ein Verzeichnis für Ihre Schlüsselpaare (Keyrings) a	n:
K:\gpgkeys	Du <u>r</u> chsuchen
<u>I</u> nfo <u>http://www.equipmente.de</u> < <u>Z</u> urück <u>W</u> e	iter > Abbrechen

Übersicht der Installations-Einstellungen:

Setup	×
Installation durchführen Das Setup ist jetzt bereit, GnuPT-Light 0.4 auf Ihren Computer zu installieren.	<i>*</i>
Klicken Sie auf "Installieren", um mit der Installation zu beginnen, oder auf "Zurück", um Ihre Einstellungen zu überprüfen oder zu ändern.	
Ziel-Ordner: C:\Programme\GPG\GnuPT-Light	
Setup-Typ: Vollständige Installation	
Ausgewählte Komponenten: GnuPG 1.4.2 Sprachdatei Deutsch	
Startmenü-Ordner: GnuPT-Light	
Info <u>http://www.equipmente.de</u> < <u>Zurück</u> Installieren Abbrechen	

Auswahl des Zielverzeichnisses für die GnuPT-Light-Verknüpfung (Startmenü).

Setup
Startmenü-Ordner auswählen Wo soll das Setup die Programm-Verknüpfungen anlegen?
Das Setup wird die Programm-Verknüpfungen im folgenden Startmenü-Ordner anlegen. Klicken Sie auf "Weiter", um fortzufahren. Klicken Sie auf "Durchsuchen", falls Sie
einen anderen Ordner auswählen möchten.
Info <u>http://www.equipmente.de</u> < <u>Z</u> urück <u>W</u> eiter > Abbrechen

Am Ende der Installation erscheint noch ein Hinweisfenster das über die erfolgreiche Installation berichtet. Daneben können Sie sich noch Produktinfos ansehen (empfehlenswert falls Sie mit GnuPT nicht vertraut sind).



6 Thunderbird Enigmail

Wenn Sie E-Mails verschlüsseln und entschlüsseln möchten benötigen Sie einen Public Key und einen Private Key, diese beiden Schlüssel sind mathematisch gesehen voneinander abhängig, so dass es nicht ausreichend ist nur den geheimen privaten Schlüssel zu besitzen! Damit keine Schlüssel verloren gehen werden diese in sog. Keyrings (Schlüsselbund) abgelegt – Private Keys werden dem Private Keyring hinzugefügt, Public Keys gehören dem Public Keyring an – neben den Schlüsseln werden auch Zertifikate und andere zugehörige Schlüsseldaten in den Keyrings abgespeichert – so ist es möglich den Public-Key mit einem persönlichen Foto zu versehen. In diesem Abschnitt ist beschrieben wie mit der Thunderbird-Erweiterung "Enigmail" (integrierte Schlüsselverwaltung) eigene Keyrings für den gesicherten Mail-Verkehr angelegt werden können.

6.1 Erstellung eines Keyrings

Bevor wir an die Erstellung eines Keyrings (Public Key & Private Key) gehen, ist es ratsam zu prüfen, ob der Pfad zur gpg.exe stimmt. Ist der Pfad nicht korrekt angegeben funktioniert die Schlüssel-Erzeugung nicht. Gehen Sie auf "Konten-Einstellungen bearbeiten" -> "openPGP-Sicherheit" -> "Erweitert" -> Registerreiter "Allgemein" -> "Pfad zur GnuPG-Anwendung". Sollte der Pfad nicht korrekt sein, bitte anpassen!

En	igmail Einstellungen 🛛 🗙	I I
	Allgemein Senden Schlüsselauswahl PGP/MIME Erweitert Fehlersuche	
	Allgemeine Einstellungen	
	Pfad zur GnuPG-Anwendung C:\Programme\GnuPT-Light\GPG\gr	
	Zusätzliche Parameter für GnuPG	
	Passphrasen-Einstellungen	
	Passphrase für 9999 Minuten im Cache behalten	
	Schlüssel ohne Passphrase verwenden	
	Schlüssel-Server:	
	www.dfn-pca.de/pgpkserv, http://www.dfn-pca.de/pgpkserv, random.sks.keyserver.penguin	
	Beispiel: sks.dnsalias.net, pgp.mit.edu, ldap://certserver.pgp.com	
	Zurücksetzen	
	OK Abbrechen	

gnu.exe im Installationsverzeichnis auswählen (nur falls Pfad nicht korrekt).

GnuPG-Anwendu	ung finden	<u>?</u> ×
<u>S</u> uchen in:	🔄 GPG 💽 🗲 🛍 🐨 📰 🕶	
Verlauf Desktop Eigene Dateien	Doc iconv.dll gnupg.nls gpg.exe gpgkeys_finger.exe gpgkeys_hkp.exe gpgkeys_http.exe gpgkeys_ldap.exe gpgsplit.exe	
	Dateiname: gpg.exe Image: Öffm Dateityp: Alle Dateien Abbre	ien chen

Nach Abschluss der vorangegangenen Arbeitsschritte, geht es jetzt endlich an die Erzeugung des Keyrings. Menü "Enigmail" -> "OpenPGP-Schlüsselverwaltung".



In der Enigmail-Schluesselverwaltung gehen Sie auf "Erzeugen" -> "Neues

Schlüsselpaar".

	🥞 Oper	nPGP-Schlüs	selverwalt	ung			
	<u>D</u> atei	<u>B</u> earbeiten	<u>A</u> nzeigen	<u>S</u> chlüssel-Server	<u>E</u> rzeugen		
	Zeige Sc	hlüssel, derer	n Benutzer-II) D oder Schlüssel-ID I	<u>N</u> eues S	Schlüsselpaar	
ı.					<u>W</u> iderru	ıfszertifikat	

Anschließend klicken Sie auf "Schlüsselpaar erzeugen"

Um den Vorgang abzuschließen und das Schlüsselpaar zu erzeugen bestätigen Sie diese Meldung bitte mit "Ja".

Enigmail Bestätigung		
?	Erzeuge öffentlichen und privaten Schlüssel für 'hans mustermann <mustermann@sicheremails.de>'?</mustermann@sicheremails.de>	
	<u>]a</u>	

Die Schlüsselerzeugung dauerte auf dem Testrechner (AMD Athlon 1700MHz mit 512 MB SD-RAM) ca. 5 Minuten, wenn Sie nicht gerade ein Power-Rechner oder Dual-Prozessor-System zur Verfügung haben, können Sie in der Zwischenzeit einen Kaffee trinken gehen.

Im Fenster "Konsole zur Schlüssel-Erzeugung" erscheint jetzt nochmals eine Zusammenfassung der Schlüssel-Eigenschaften (Verschlüsselungs-Algorithmen, Schlüsselstärke usw.). Hinter dem Eintrag "Expire-Date:" werden laufend Pluszeichen, Punkte etc. dargestellt – dies bedeutet, dass der Prozess der Schlüssel-Erzeugung gerade läuft.

~ Konsole zur Schlüssel-Erzeugung
ACHTUNG: Die Erzeugung eines Schlüssels kann mehrere Minuten dauern. Beenden Sie die Anwendung während dieser Zeit nicht. Da der Zufallsgenerator von Aktivität auf dem Rechner abhängt, wird empfohlen z.B. im Webbrowser aktiv zu surfen, um die Geschwindigkeit der Schlüsselerzeugung zu beschleunigen. Sie werden informiert, sobald der Schlüssel fertiggestellt ist.
Key-Length: 1024
Subkey-Type: ELG-E
Subkey-Length: 4096
Name-Real: hans mustermann
Name-Email: mustermann@sicheremails.de
Expire-Date: 0+++++.++++++++++.++++++++++++++++++
.+++++.++++>+++++++++++++++++++++++++++
++>+++++>++++++.>.+++++
▼

6.2 Erstellung eines Widerrufs-Zertifikats

Nachdem das Key Pair erstellt wurde, erscheint eine Erfolgsmeldung. Des weiteren ist es empfehlenswert ein Widerrufszertifikat (Revokation Key) zu erstellen, falls man seine Passphrase des Privaten Schlüssels vergessen hat, kann man auf diese Weise den Public Key vom Keyserver löschen (ansonsten bleibt der Pub Key für alle Zeiten unwiderruflich auf dem Keyserver!).

Enigmail	Bestätigung 🔀
?	Schlüsselerzeugung abgeschlossen. Benutzer-ID <mustermann@sicheremails.de> wird zum Unterschreiben verwendet.</mustermann@sicheremails.de>
	Es wird dringend empfohlen, dass Sie nun Widerrufszertifikat für Ihren Schlüssel erzeugen. Dieses Zertifikat benötigen Sie, um Ihren Schlüssel bei Bedarf für ungültig zu erklären (z.B. wenn der Schlüssel missbraucht, verloren oder gestohlen wird).
	Möchten Sie nun das zugehörige Widerrufszertifikat erzeugen?

Nach einem Klick auf "Ja", erscheint ein Fenster in dem Sie den Speicherort für das Widerrufs-Zertifikat auswählen können. Ideal ist es, das Widerrufs-Zertifikat verschlüsselt oder an einem sicheren Ort abzulegen. Wird einer zweiten Person Zugriff auf dieses gewährt, kann er Ihren Public-Key vom Key-Server löschen, dies kann vor allem sehr ärgerlich sein, wenn Sie Ihren Public Key bereits an einen größeren Kontaktkreis weiter gegeben haben.

Widerrufszertifi	kat erzeugen & speichern	? ×
Spejchern in:	: 🖳 Arbeitsplatz 💽 🗢 🗈 📸 🎟 -	
Verlauf	➡ 31⁄2-Diskette (A:) ■ win2k (C:)	
Desktop		
Netzwerkumg	Dateiname: Imustermann@sicheremails.de (0x5C8110C1) rev Spe Dateityp: ASCII Armored Dateien (*.asc) Abbr	ichern echen

Abschließend müssen Sie zur Erzeugung des Widerrufs-Zertifikats noch Ihre Passphrase eingeben, ansonsten könnte jeder der Zugriff zu Ihrem Rechner hat ein solches Zertifikat erzeugen!

Enigmail	×
?	Bitte geben Sie Ihre OpenPGP-Passphrase oder SmartCard-PIN ein

	🔽 Erst nach 9999 Minuten Untätigkeit vergessen
	OK Abbrechen

Nach einem Klick auf "OK" sollte eine Bestätigung erscheinen, in welcher Sie

über die erfolgreiche Erstellung des Widerrufs-Zertifikats benachrichtigt werden.

Enigmail	Meldung X
	Das Widerrufszertifikat wurde erfolgreich erzeugt. Sie können es nutzen, um Ihren öffentlichen Schlüssel für ungültig zu erklären (z. B.: im Fall, dass Sie Ihren privaten Schlüssel verloren haben).
	Bitte bewahren Sie das Widerrufszertifikat nur an einem sicheren Ort (wie Diskette oder CD) auf. Wenn andere Personen Zugriff darauf erhalten, könnten diese Ihren Schlüssel unbrauchbar machen.
	ОК

6.3 Public Key auf Keyserver kopieren

Um den Public Key der Öffentlichkeit bekannt zu machen, kann man Ihn

innerhalb der OpenPGP-Schlüsselverwaltung auf einen Keyserver kopieren

(hochladen).

🗣 OpenPGP-Schlüsselverwaltung								
Date	ei <u>B</u> earbeiten	<u>A</u> nzeigen	<u>S</u> chlüssel-Server	Erzeugen				
Zeig	e Schlüssel, dere	n Benutzer-II	Ausgewählte S Schlüssel s <u>u</u> che					
	enutzer-ID		Schlüssel hochladen					
	hans mustern	nann <mus< td=""><td colspan="3">Alle Schlüssel aktualisieren</td></mus<>	Alle Schlüssel aktualisieren					

Suchen Sie sich einen Keyserver aus, auf den Sie Ihren Public Key übertragen möchten.

Schlüssel-Server	auswählen 🗾
Sende folgende öl Schlüssel-Server: <mustermann@sid< td=""><td>fentliche Schlüssel an einen 0x5C8110C1 - hans mustermann :heremails.de></td></mustermann@sid<>	fentliche Schlüssel an einen 0x5C8110C1 - hans mustermann :heremails.de>
Schlüssel-Server	http://www.keys.de.pgp.net/
	OK Abbrechen

In der Regel spielt dies keine Rolle, da sich die Keyserver untereinander synchronisieren. Bitte beachten Sie, dass dies nicht bei allen Key-Servern der Fall ist. Um auf Nummer sicher zu gehen, ob Ihr Public Key auf den Keyserver XY übertragen wurde, suchen Sie Ihn über die Key-ID -> Menü "Schlüssel-Server" -> "Schlüssel suchen". Konnte der Public-Key nicht auf dem Key-Server gefunden werden, können Sie einen erneuten Versuch starten.

Schlüssel-Server auswählen						
Suche nach Schlüssel Schlüssel-Server	pgp.dtype.org	•				
	OK Abbreche	en 🗌				

Wenn bereits ein Schlüsselpaar erstellt wurde oder Sie bereits eines besitzen,

sind sie nur noch einen Katzensprung von der eigentlichen

Mail-Signierung/Verschlüsselung entfernt.

Gehen Sie in die Einstellungen Ihres Mail-Kontos, öffnen Sie dazu folgende Menüpunkte: "Konten-Einstellungen bearbeiten" -> "OpenPGP-Sicherheit" Falls Ihr Schlüsselpaar noch nicht ausgewählt ist müssen Sie dies unter "Schlüssel auswählen" nachholen.

Konten							
OpenPGP-Sicherheit (Enigmail)							
OpenPGP-Verschlüsselung und Unterschrift von Nachrichten wird von Enigmail ermöglicht. GnuPG (GPG) muss installiert sein, um die Funktionen nutzen zu können.							
 E-Mail-Adresse dieses Kontos verwenden, um OpenPGP-Schlüssel zu identifizieren Spezielle OpenPGP-Schlüssel-ID verwenden (0x1234ABCD): 0x1DFD8725 Schlüssel auswählen Nachrichten Verfassen Standard-Einstellungen Unverschlüsselte Nachrichten standardmäßig unterschreiben Verschlüsselte Nachrichten standardmäßig unterschreiben Nachrichten standardmäßig verschlüsseln 							
Erweitert							
Sende 'OpenPGP'-Kopfzeile Sende OpenPGP-Schlüssel-ID Sende URL, um Schlüssel zu empfangen: http://pgpkeys.pca.dfn.de:11371/							
OK Abbrechen							

Möchten Sie Ihre Nachrichten standardmäßig verschlüsseln/signieren, so setzten Sie die entsprechenden Haken. In den meisten Fällen ist es ausreichend, eine Mail standardmäßig zu signieren, da man in erster Linie die Identität des Absenders mithilfe der kryptografischen Signatur überprüfen möchte. Das Senden der OpenPGP-Schlüssel-ID ist sinnvoll, da der Mailempfänger über diese den Public Key des Mail-Absenders in die OpenPGP-Schlüsselverwaltung importieren kann – hierzu muss allerdings auch der korrekte Pfad des Keyserver eingetragen werden, mit der Key-ID alleine kann "Thunderbird Enigmail" nichts anfangen.

Eine andere Methode den Public Key dem Empfänger zu überbringen, ist die Möglichkeit ihn per Mail-Anhang als ASCII-Datei zu verschicken:

Hierzu markieren Sie in der OpenPGP-Schlüsselverwaltung Ihren Schlüsselbund, mit einem Rechtsklick gelangen Sie in das Kontextmenü, bitte auf "Öffentliche Schlüssel per E-Mail senden" klicken.

🧟 Ope	nPGP-Schlü	sselverwalt	ung							
<u>D</u> atei	<u>B</u> earbeiten	<u>A</u> nzeigen	<u>S</u> chlüssel-Server	Erzeugen						
Zeige S	ichlüssel, derei	n Benutzer-II	D oder Schlüssel-ID I	folgendes enthalten:						
Benutzer-ID Schlüssel-ID										
h	ans mustern	nann <mus< td=""><td>termann@sicher</td><td>emails de > 50811001 In Zwischenablage exportieren</td></mus<>	termann@sicher	emails de > 50811001 In Zwischenablage exportieren						
				In Datei exportieren						
				Öffentliche Schlüssel per E-Mail senden						
				Auf Schlüssel-Server hochladen						
				Von Schlüssel-Server aktualisieren						
				Unterschreiben						
				Vertrauenswürdigkeit festlegen						
				Deaktivieren						
				Zurückziehen						
				Löschen						
				Benutzer-IDs verwalten						
				Widerrufszertifikat erzeugen & speichern						
				Unterschriften anzeigen						
				Foto-ID anzeigen						
				Schlusseleigenscharten						

6.4 Mails signieren

Um eine Mail zu signieren müssen Sie zuerst eine neue öffnen (STRG + N), danach wählen Sie im Menü "Enigmail" -> "Nachricht unterschreiben" aus (Haken muss gesetzt sein). Sollten sie Ihre Mails standardmäßig signieren, können Sie diesen Schritt selbstverständlich überspringen.

<u>ר</u>	E <u>n</u> igmail Ex <u>t</u> ras <u>H</u> ilfe	4
	✓ Nachricht unterschreiben Strg+Umschalt+S	
•	Nachricht verschlüsseln Strg+Umschalt+P	
erm	<u>P</u> GP/MIME verwenden Enigmail-Empfängerregeln ignorieren	
	Ein <u>s</u> tellungen • Enigmail-Empfänge <u>r</u> regeln	
	V <u>e</u> rschlüsselung rückgängig machen <u>M</u> einen öffentlichen Schlüssel anhängen <u>Ö</u> ffentlichen Schlüssel anhängen <u>P</u> assphrase aus Cache löschen	
Γ	Hilfe	
		ı

Zu Testzwecken sollte man eine Mail an einen anderen angelegten Mail-Account schicken:

🐮 Verfassen: gpg test 📃 🔍									
<u>D</u> atei	<u>B</u> earbeiten	<u>A</u> nsicht	<u>E</u> infügen	F <u>o</u> rmat	<u>E</u> instellungen	E <u>n</u> igmail	Ex <u>t</u> ras	<u>H</u> ilfe	
Senden	Kontakt	e Red	ABC thtschr.	0 Anhang	- 🔒 - OpenPGP -	S/MIME	• s	2 peicherr	י () ו
Von:	hans musterm	ann <mus< td=""><td>termann@si</td><td>cheremails</td><td>.de> - musterr</td><td>nann@siche</td><td>remails.d</td><td>e</td><td>•</td></mus<>	termann@si	cheremails	.de> - musterr	nann@siche	remails.d	e	•
Betreff:	An:	i lorenzo	o@gnaderer	r.de					
Norma	ler Text 💌	Variabl	e Breite		•	/A /A	В	Ι	<u>U</u>
gpg t	est								

Wenn der Public-Key des Absenders bereits in die OpenPGP-Schlüsselverwaltung eingetragen wurde, kann der Empfänger die signierte/unterschriebene Mail verifizieren (überprüfen). Allerdings erscheint anfangs die Meldung "UNVERTRAUTE Korrekte Unterschrift von hans mustermann mustermann@sicheremails.de". Dies liegt daran, dass dem Public-Key des Mail-Absenders noch nicht vertraut wurde.

🤹 test gpg -	Mozilla Thu	underbird					
<u>D</u> atei <u>B</u> earb	eiten <u>A</u> nsi	icht <u>G</u> ehe	<u>N</u> achricht	<u>E</u> nigmail	Ex <u>t</u> ras	Hilfe	
Abrufen Ve	vrfassen A	dressbuch	Entschlüse	seln		en Allen antworten	Weiterleiten
🖻 Enigmail:	UNVERTRAI Schlüssel-IE	UTE Korrekte): 0x5C8110	Unterschrift C1 / Untersch	von hans m rieben am:	ustermann 11.10.200	n <mustermann@sich 05 16:00</mustermann@sich 	eremails.de>
 Betreff: Von: Datum: An: 	test gpg hans muste 16:00 lorenzo@gr	ermann <mus naderer.de</mus 	termann@sicf	neremails.d	<u>e></u>		Øz
test gpg							

Am besten gehen Sie wieder in die OpenPGP-Schluesselverwaltung um das

Vertrauen des importierten Public Key festzulegen.

ኛ OpenPGP-Schlüsselverwaltung							
Datei Bearbeiten Anzeigen Schlüssel-Server Erzeugen							
Zeige S	ichlüssel, derei	n Benutzer-II) od	er Schlüssel-ID folgendes enthalten:			
Ber	utzer-ID				S	chlüssel-ID	
h	ans mustern	nann <mus< td=""><td>teri</td><td>mann@sicheremails.de></td><td>5(</td><td>8110C1 .</td></mus<>	teri	mann@sicheremails.de>	5(8110C1 .	
				In Zwischenablage exportieren			
				In Datei exportieren			
				Öffentliche Schlüssel per E-Mail senden			
				Auf Schlüssel-Server hochladen			
				Von Schlüssel-Server aktualisieren			
	Unterschreiben				-		
				Vertrauenswürdigkeit festlegen			
					=		
				Deaktivieren			
				_			
			Benutzer-IDs verwalten				
			Widerrufszertifikat erzeugen & speichern				
			Unterschriften anzeigen				
			Foto-ID anzeigen				
				Schlüsseleigenschaften			
						I	

Das Vertrauen muss auf "Ich vertraue ihm absolut" angehakt werden. Tun Sie das nur wenn Sie den Fingerprint des Public-Keys (vorzugsweise telefonisch) überprüft haben oder sich absolut sicher sind, dass die Mailadresse der richtigen Person angehört, ansonsten ist die Signatur nutzlos!

Enigmail - Schlüssel-Vertrauenswürdigkeit festlegen						
Zu bewertender Schlüssel: hans mustermann <mustermann@sic< td=""></mustermann@sic<>						
Wie hoch ist Ihr Vertrauen in den Schlüssel?						
C Ich weiß es nicht						
C Ich vertraue ihm NICHT						
C Ich vertraue ihm nur gering						
C Ich vertraue ihm voll						
Ich vertraue ihm absolut						
OK Abbrechen						

Wurde die Vertrauenswürdigkeit richtig gesetzt, wird jetzt wie gewollt die

Meldung "Korrekte Unterschrift von…" als Enigmail-Kommentar ausgegebenen:

🤹 test	- Mozilla Th	underbir	d					
<u>D</u> atei	<u>B</u> earbeiten	<u>A</u> nsicht	<u>G</u> ehe	<u>N</u> achricht	<u>E</u> nigmail	Ex <u>t</u> ras	<u>H</u> ilfe	
Abrufer	verfasse	n Adres) sbuch	Entschlüs:	seln	Antworter	Allen antworten	Weiterleiten
🖻 Eniç	ymail: Korrel Schlüs	kte Unters ssel-ID: 0x	chrift voi 5C81100	n hans muste 11 / Untersch	rmann <mu rieben am:</mu 	ustermann@ 11.10.2005	sicheremails.de> 16:12	
🖻 Be	etreff: test							
Von: hans mustermann <mustermann@sicheremails.de></mustermann@sicheremails.de>								
D	atum: 16:12	2					Q	~ I
	An: <u>suppo</u>	ort@pearl-	online.ne	<u>et</u>				
Enigr	mail							
2								II.

6.5 Mails verschlüsseln

Erstellen Sie zunächst wieder eine neue E-Mail (STRG + N). Anschließend bei

"Enigmail" -> "Nachricht verschlüsseln" einen Haken setzten.



Bevor die Nachricht verschlüsselt wird, kommt eine Meldung – diese bitte bestätigen:

Enigmail Bestätigung						
?	VERSCHLÜSSELTE Nachricht an folgende Empfänger senden: lorenzo@gnaderer.de Hinweis: Die Nachricht wurde mit folgenden Benutzer-IDs / Schlüsseln verschlüsselt: lorenzo@gnaderer.de					
	<u>]</u> a <u>N</u> ein					

So sieht die Nachricht in verschlüsselter Form aus:



Normalerweise sollte Enigmail die Nachricht automatisch entschlüsseln (mit

dem Private Key), ist dies nicht der Fall gehen Sie bitte auf "Enigmail" ->

"Entschlüsseln/Überprüfen".

Die Nachricht sollte dann im Klartext erscheinen – auch zu erkennen am

Schlüsselsymbol und dem Enigmail-Kommentar "Entschlüsselte Nachricht":

餐 verschluesselt - Mozilla Thunder	bird						
<u>D</u> atei <u>B</u> earbeiten <u>A</u> nsicht <u>G</u> ehe	<u>N</u> achricht <u>E</u> nigmail	Ex <u>t</u> ras <u>H</u> i	lfe				
i 🖓 🙀	M	2	5				
Abrufen Verfassen Adressbuch	Entschlüsseln	Antworten	Allen antworten	Weiterleiter			
😑 Enigmail: Entschlüsselte Nachricht							
Betreff: verschluesselt							
Von: <u>hans mustermann <must< u=""> Datum: 16:40</must<></u>	ermann@sicheremails.c	<u>1e></u>		- 😥			
An: lorenzo@gnaderer.de				<u> </u>			
verschluesselt							
5				<u> </u>			

So sieht eine E-Mail aus die sowohl verifiziert (Signatur) als auch entschlüsselt wurde:



Hat alles geklappt wird ein "Kugelschreibersymbol" und ein "Schloss" angezeigt,

ein grün hinterlegtes Enigmail-Kommentar, wie in der Abbildung zu sehen ist,

gibt die Erfolgs-Bestätigung nochmals in Text-Form aus.

7 Quellenangeben

7.1 Print-Medien

Internet-Sicherheit f
ür Einsteiger von Alexander Otto (Galileo Computing)

7.2 Internet

- www.google.de
- www.wikipedia.de
- http://kai.iks-jena.de/pgp/gpg/
- Einführung in die Kryptographie von Network Associates

7.3 Grafiken

• Grafiken zur Signierung von Network Associates