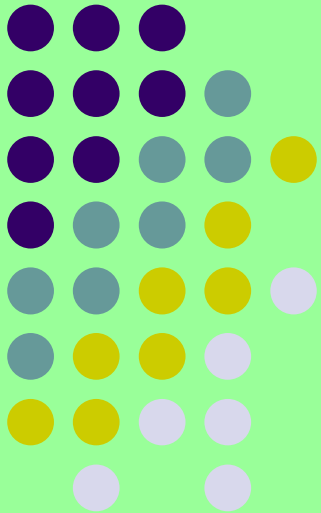
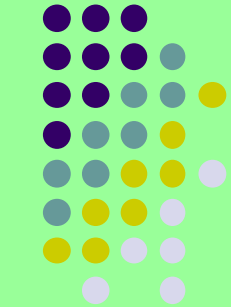
Verschlüsselung von e-Mails
(Überblick)

Verschlüsselungsarten:

- Übertragung via SSL/TLS o. STARTTLS
- e-Mail verschlüsseln
- e-Mail Inhalt als Datei verschlüsseln



Warum verschlüsseln?



Eine e-Mail ist wie eine Postkarte.

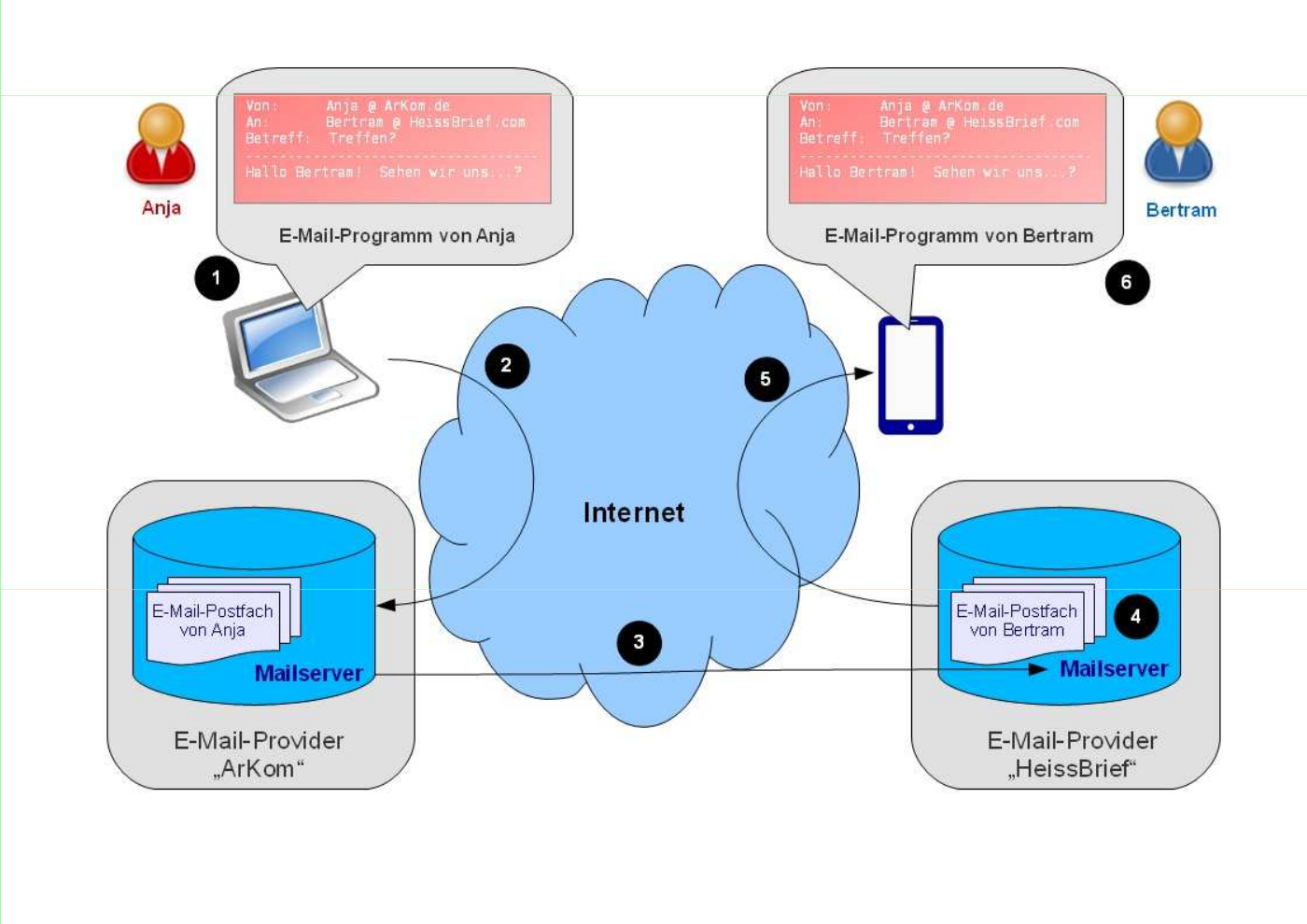
Offen für jeden zu lesen. Es fehlt der Briefumschlag.

Der virtuelle Briefumschlag einer e-Mail ist die Verschlüsselung.
Eine verschlüsselte e-Mail ist unlesbar.
Nur mit dem zugehörigen Schlüssel kann sie wieder entschlüsselt und damit lesbar gemacht werden.

Das hört sich leichter an als es in der Realität ist. Denn zwischen Sender und Empfänger ist ein langer Weg mit vielen unterschiedlichen Geräten, Protokollen und Programmen.

„Versandwege“

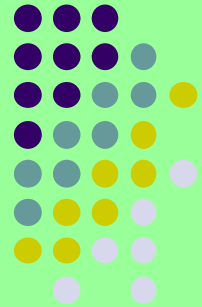
Die Geräte und Versandwege unterscheiden sich von der Postkarte erheblich, auch wenn die Sichtbarkeit der Inhalte ähnlich einfach ist.



Verlauf der e-Mail

- Erstellung der e-Mail auf dem Computer (Mit Hilfe eines e-Mail Clients)
- Versenden der e-Mail an das Postfach auf dem Mailserver des Providers
- Weiterleiten über die vielfältigen und verschlungenen Wege an den Mailserver des Empfänger Providers
- Abrufen der e-Mail vom Mailserver durch den Empfänger

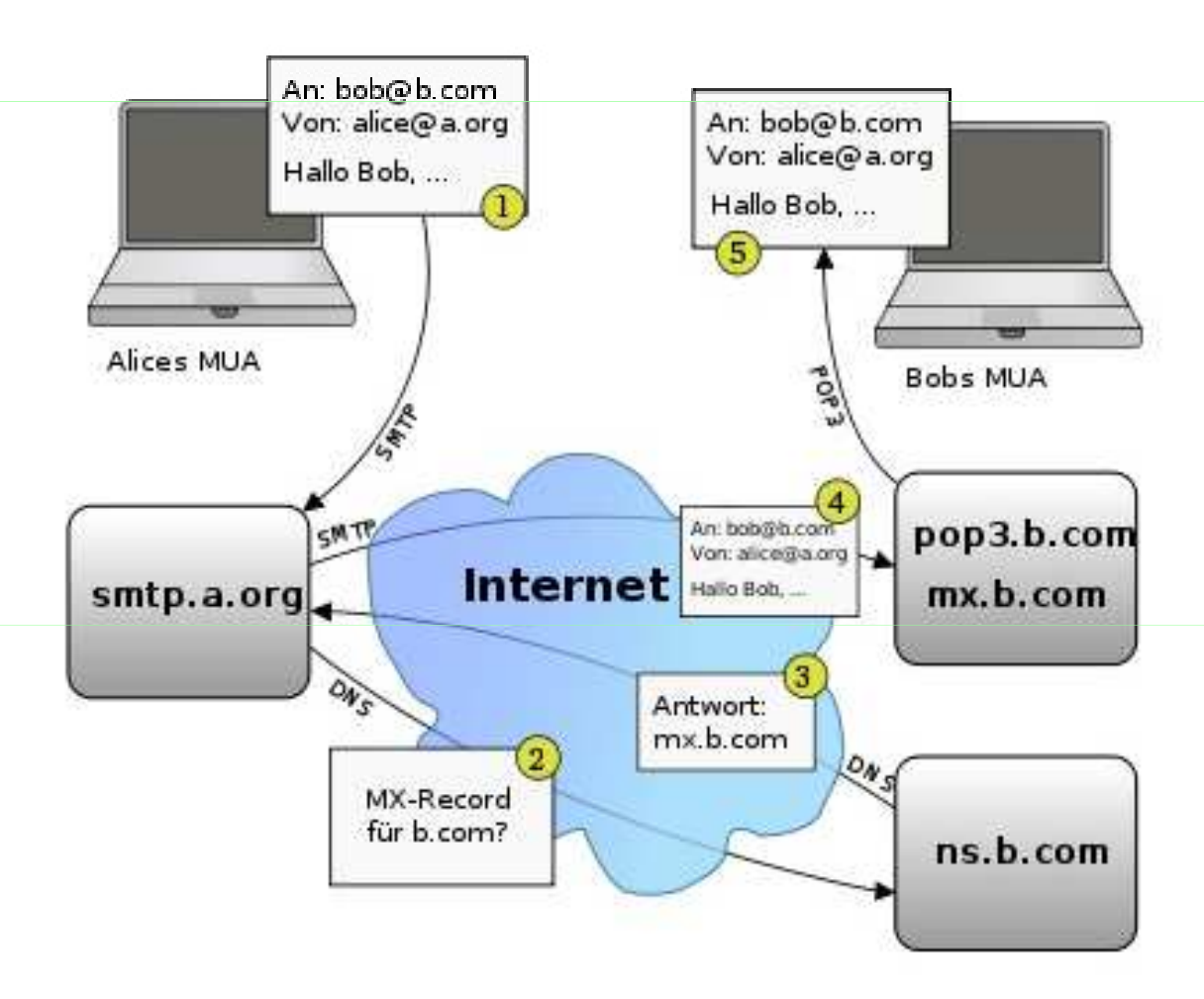
Techniken des Versands



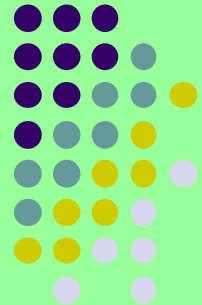
- e-Mail Client des Senders:
  Von e-Mail Adresse des Absenders an e-Mail Adresse des Empfängers. Eingebettet der Inhalt in Form von Text und Anlagen.
  Sendeprotokoll: SMTP an Mailserver/Absender
- Vom Mailserver/Absender Anfrage via DNS-Protokoll an DNS-Dienst:
  IP-Adresse für Name/Mailserver/Empfänger?
- Antwort vom DNS-Dienst an Mailserver/Absender:
  Die IP-Adresse für den Mailserver/Empfänger lautet:
  123.456.789.123
- Mailserver/Absender schickt e-Mail an IP-Adresse 123.456.789.123.
- Empfänger ruft via POP3-Protokoll die e-Mail von seinem Mailserver/Empfänger ab. Es ist auch das IMAP-Protokoll möglich, jedoch bleiben hier die Nachrichten auf dem Server.

Wie wird die e-Mail übertragen

Prinzipielle Darstellung



Risiken bei der Übertragung



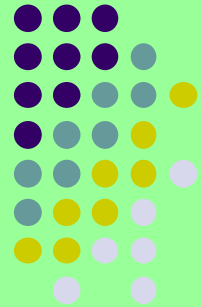
- Das Protokoll SMTP ist, wie der Name schon sagt, ein einfaches und unverschlüsseltes Protokoll.
  Der Inhalt der Nachricht (Textkörper) kann jederzeit mitgelesen werden. Von jedem Monitoring-Programm.

- Man kennt den Übertragungsweg im Internet nicht, weiß nicht, über welche Knoten und Server die Nachricht geleitet wird.

- Man muß davon ausgehen, daß nicht nur Geheimdienste die Nachrichten mitlesen.

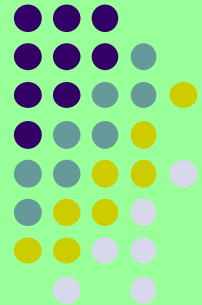
- Internet-Schutz bietet **keine** e-Mail Sicherheit
  Zwar werden eingehende e-Mails auf Malware geprüft, jedoch der Inhalt eingehender und ausgehender e-Mails nicht geschützt.

Beispiel SMTP-Protokoll



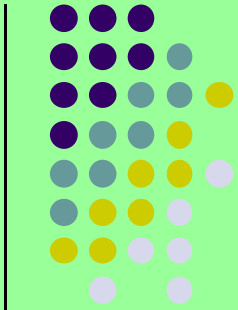
Client	Server	Erläuterung
telnet mail.example.com 25		Client ruft Server
	220 service ready	Server meldet sich bereit
HELO foobar.example.net		Client nennt seinen Namen
	250 OK	Server bestätigt
MAIL FROM:<sender@example.org>		Client nennt Absenderadresse
	250 OK	Server bestätigt
RCPT TO:<receiver@example.com>		Client nennt Empfängeradresse
	250 OK	Server bestätigt
DATA		Client kündigt Inhalt der E-Mail an
	354 start mail input	Server bereit für diesen längeren Vorgang
From: <sender@example.org> To: <receiver@example.com> Subject: Testmail Date: Thu, 26 Oct 2006 13:10:50 +0200 Lorem ipsum dolor sit amet, consectetur adipisici elit, sed eiusmod tempor incidunt ut labore et dolore magna aliqua. .		Client sendet Inhalt der E-Mail und markiert das Ende durch eine Zeile, die nur einen Punkt enthält. (Zwischen Header und Textkörper muss eine Leerzeile vorhanden sein, sonst wird beim Empfänger kein Textkörper angezeigt.)
	250 OK	Server bestätigt und übernimmt die Verantwortung für die Nachricht
QUIT		Client fordert Verbindungstrennung an
	221 closing channel	Server kündigt Trennung an

Sichere Übertragungsmöglichkeiten



- **https-Übertragung** (Bei fast allen Providern üblich)
  Bei Browser als e-Mail Client, wird hier **nicht** weiter betrachtet.
- **SSL/TLS** oder **STARTTLS**:
  Verschlüsselung zwischen Client und Mailserver
  Konsequenz:
  Der Übertragungsweg vom Client zum Mailserver ist verschlüsselt, die Mail selbst nicht.
  Der Weg vom Mailserver/Absender zum Mailserver/Empfänger ist unbekannt. Ob er verschlüsselt ist, weiß man nicht.
- **e-Mail-Verschlüsselung**
  Die e-Mail selbst wird verschlüsselt. Nur der Empfänger kann sie entschlüsseln.
  Auf dem gesamten Übertragungsweg ist die e-Mail für Unbefugte nicht lesbar.
- e-Mail Inhalt als **Datei** verschlüsseln
  Man kann auch den Inhalt der e-Mail in eine Datei packen und diese verschlüsseln. Wie das geht, entnehmen Sie meinem Vortrag vom Oktober 2015 / Verschlüsselungstechniken

SSL/TLS Verschlüsselung



Die SSL/TLS bzw. STARTTLS Verschlüsselung ist nur auf dem Übertragungsweg vom e-Mail Client des Absenders zum e-Mail Server des Absenders wirksam.

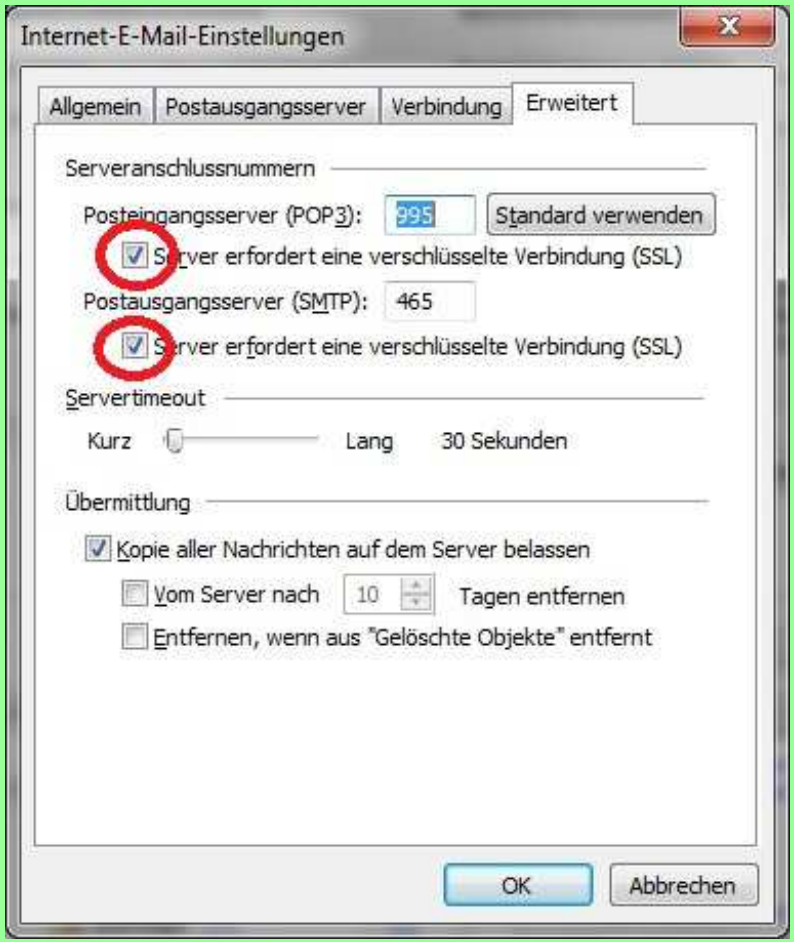
Trotzdem sollte man diese Verschlüsselung zusätzlich zu der e-Mail Verschlüsselung wählen. Es geht um die Account-Einwahl-Daten beim heimischen e-Mail Server. Diese sind bei unverschlüsseltem Versand für Unbefugte einsehbar.

Das Verfahren per SSL ist veraltet und wird immer weniger angewandt, da es fehleranfällig ist.

Das neuere Verfahren TLS (STARTTLS) sollte immer vorgezogen werden wenn es angeboten wird.
Bis Outlook 2003 war nur SSL möglich, ab Outlook 2007 ist auch TLS bei Postausgang möglich.
Thunderbird unterstützt TLS und STARTTLS schon länger.

Outlook 2003 / SSL

Extras –> E-Mail Konten –> Vorhandenes Konto bearbeiten –>
Ändern –> Weitere Einstellungen -> Erweitert



Bei:
Posteingangsserver (POP3)
„Server erfordert eine verschlüsselte Verbindung (SSL)“
ist das Häkchen zu setzen.

Gleiches für
Postausgangsserver (SMTP)

Dabei ist zu beachten, daß andere Ports einzustellen sind. Meist genügt der Standardport, aber manche Provider verlangen spezielle Ports.

Outlook 2007 / SSL/TLS

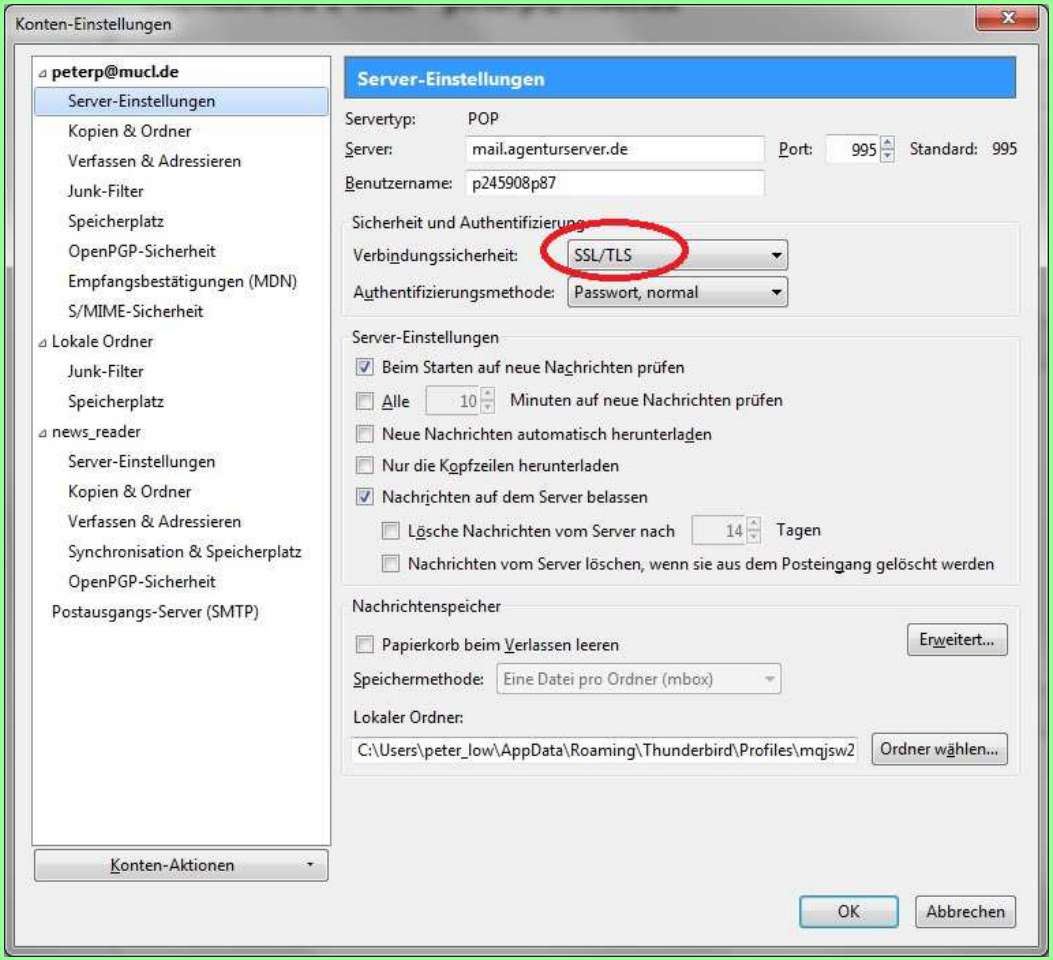
Extras –> Kontoeinstellungen –> e-Mail –> Ändern –> Weitere Einstellungen -> Erweitert

Bei:
Posteingangsserver (POP3)
„Server erfordert eine verschlüsselte Verbindung (SSL)“
ist das Häkchen zu setzen.

Bei:
Postausgangssserver kann zwischen SSL und TLS gewählt werden. TLS ist der Vorzug zu geben.

Thunderbird / TLS

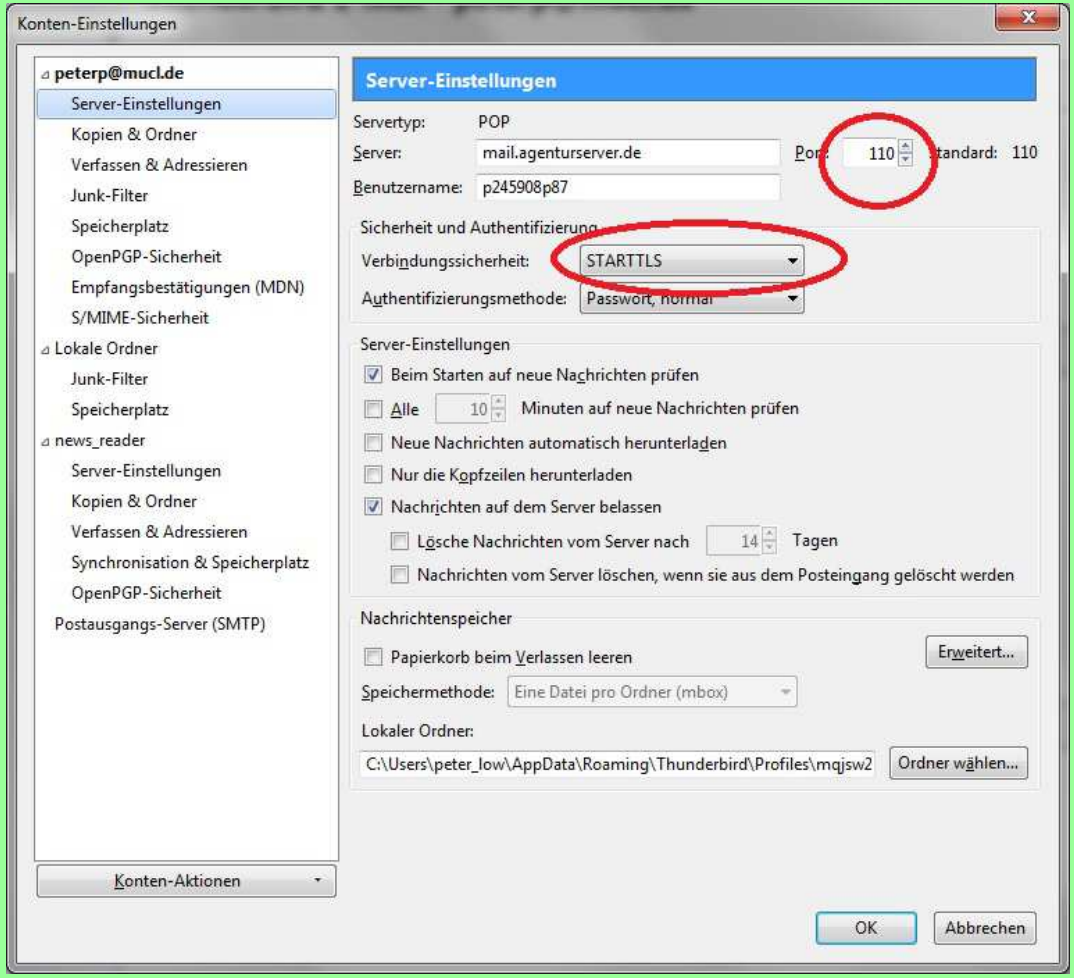
Extras –> Konteneinstellungen –> Server Einstellungen



Bei Verbindungssicherheit wird die Einstellung: SSL/TLS gewählt.
Thunderbird händelt die mögliche Einstellung mit dem Mail-Server aus. Gibt dabei TLS den Vorrang.

Thunderbird / TLS

Extras –> Konteneinstellungen –> Server Einstellungen



Hier kann auch STARTTLS eingestellt werden.

Thunderbird / TLS

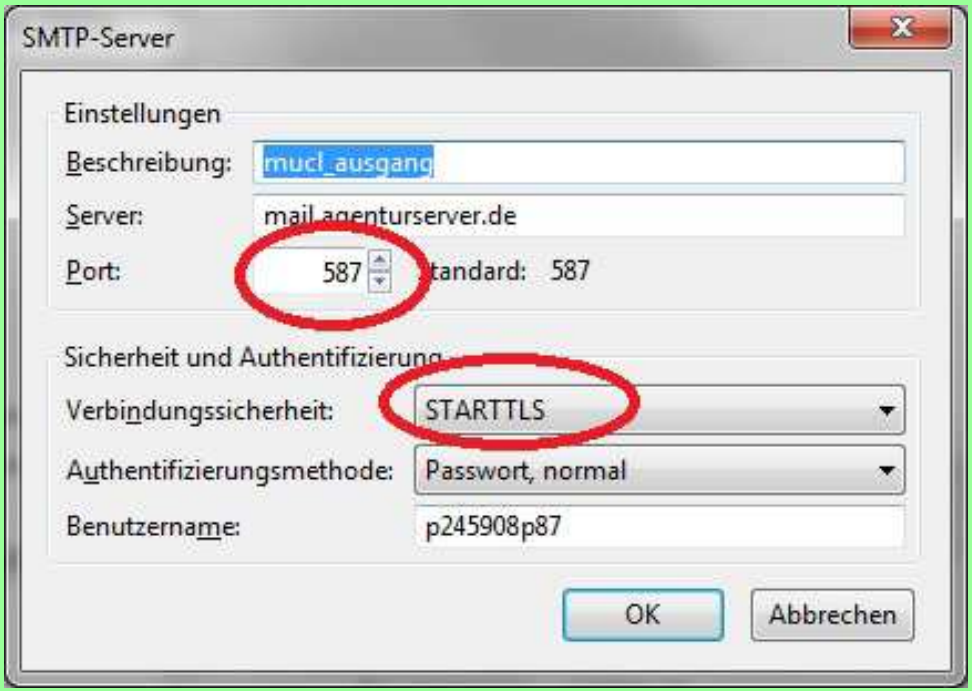
Extras –> Konteneinstellungen –> Postausgangsserver -> SMTP

Bei Verbindungssicherheit wird auch hier die Einstellung:
SSL/TLS
gewählt.

Thunderbird händelt die Einstellung mit dem Mail-Server aus, mit Vorzug auf TLS.

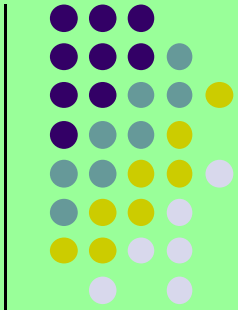
Thunderbird / TLS

Extras –> Konteneinstellungen –> Postausgangsserver -> SMTP



Auch beim Postausgangsserver läßt Thunderbird die Verbindungssicherheit STARTTLS zu.

Verschlüsselung der e-Mail



Das eigentliche Thema unseres Vortrags:

Die Verschlüsselung der e-Mail.

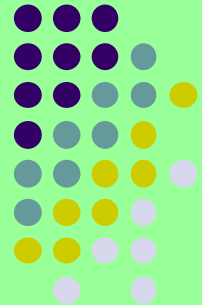
Prinzip:

Die e-Mail wird beim Absender verschlüsselt und erst dann abgeschickt. Auf dem ganzen Übertragungsweg ist sie niemals offen zu sehen.
Der Empfänger ist als Einziger authorisiert und auch in der Lage, die angekommene e-Mail zu entschlüsseln und zu lesen.

Arten der Verschlüsselung:

- VPN (Virtual Private Network): Zu sehr punktuell. Zu jedem Empfänger ist ein eigener VPN-Tunnel notwendig. Wird nicht näher darauf eingegangen.
- PKI (Public-Key-Infrastructure): Sehr aufwendig. Für Firmen gut geeignet, für Privatanwender zu aufwendig.
- S/MIME (Secure / Multipurpose Internet Mail Extensions): Externe Zertifikate notwendig.
- OpenPGP (Open Pretty Good Privacy): Einfach zu händeln, keine externe Zertifizierung notwendig. Trotzdem ziemlich sicher.

PKI (Public-Key-Infrastructure)



Mit **PKI** bezeichnet man in der **Kryptologie** ein System, das digitale Zertifikate ausstellen, verteilen und prüfen kann. Die innerhalb einer PKI ausgestellten Zertifikate werden zur Absicherung rechnergestützter Kommunikation verwendet.

Bestandteile einer PKI:

Digitale Zertifikate: Digital signierte elektronische Daten, die sich zum Nachweis der Echtheit von Objekten verwenden lassen.

Zertifizierungsstelle (Certificate Authority, CA): Organisation, die das CA-Zertifikat bereitstellt und die Signatur von Zertifikatsanträgen übernimmt.

Registrierungsstelle (Registration Authority, RA): Organisation, bei der Personen, Maschinen oder auch untergeordnete Zertifizierungsstellen Zertifikate beantragen können. Diese prüft die Richtigkeit der Daten im gewünschten Zertifikat und genehmigt den Zertifikatsantrag, der dann durch die Zertifizierungsstelle signiert wird.

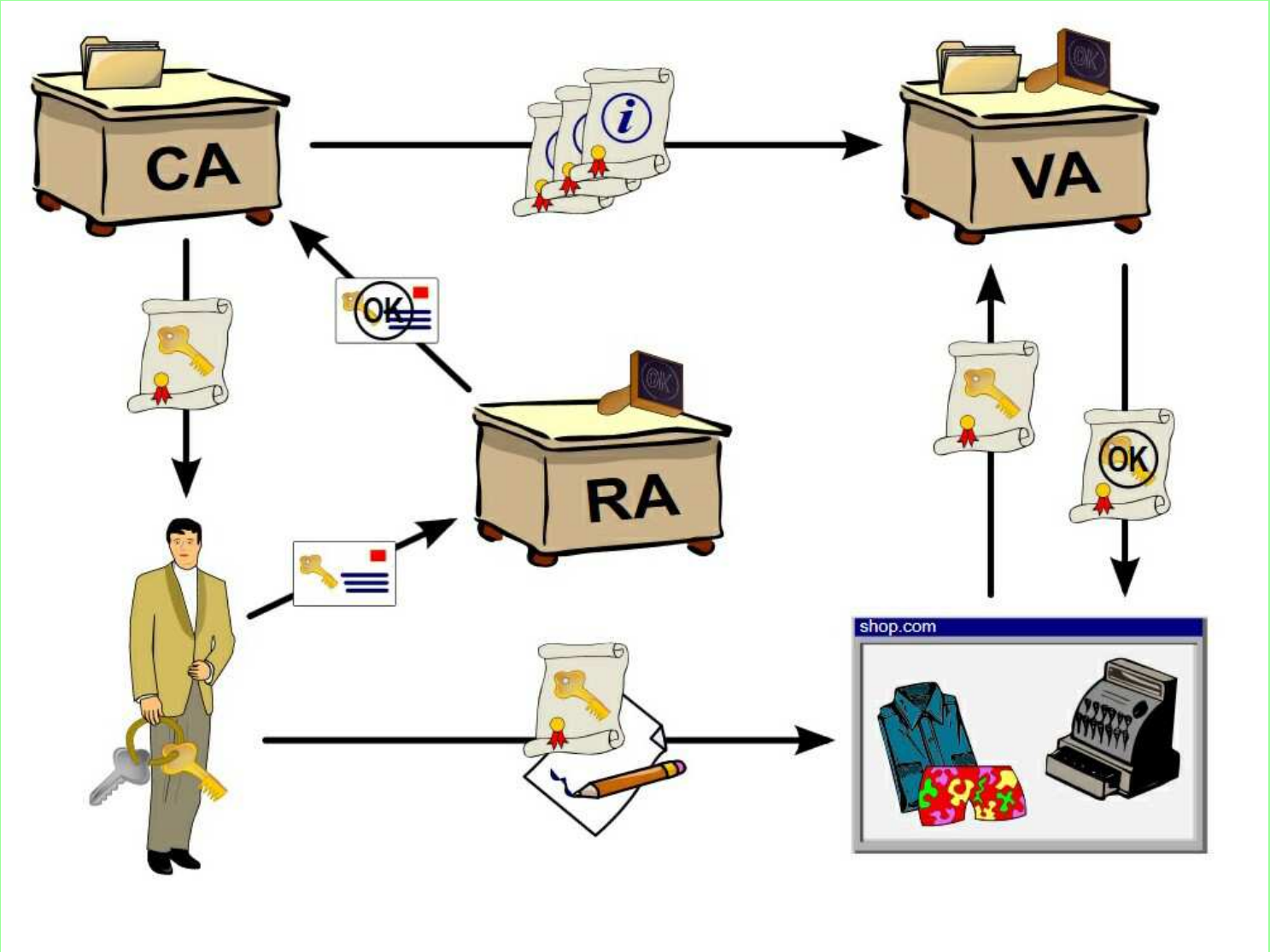
Zertifikatsperrliste

Verzeichnisdienst

Validierungsdienst

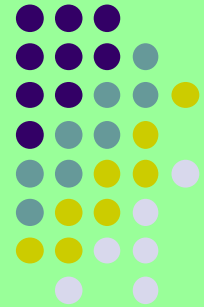
uvm.

PKI (Public-Key-Infrastructure)



Schema einer Public-Key-Infrastruktur
CA: certification authority
RA: registration authority
VA: validation authority

S/MIME (Secure / Multipurpose Internet Mail Extensions)

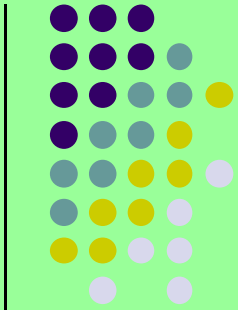


Bei **S/MIME** kommen externe Zertifikate zum Einsatz. Die fürs Ausstellen zuständigen Zertifizierungsstellen (CAs) sind zumeist identisch mit den CAs, die auch SSL-Zertifikate vergeben dürfen. Kostenlose S/MIME-Zertifikate stellen beispielsweise Start SSL oder die Comodo-Tochter Instant SSL aus. Anders als bei SSL bezeugt das Zertifikat jedoch nicht die Echtheit eines Web- oder E-Mail-Servers, sondern die Authentizität einer einzelnen E-Mail-Adresse. Um den Kommunikationspartnern den öffentlichen Teil des Zertifikats zukommen zu lassen, genügt der Versand einer signierten E-Mail. Der Empfänger speichert diesen Teil im E-Mail-Client und kann von nun an verschlüsselte Nachrichten mit der Gegenseite austauschen.

Nachteil: Für das Verfahren mit S/MIME wird eine Zertifizierungsstelle benötigt.
Zwar gibt es kostenlose Zertifikate, aber es bleibt der Aufwand bei der Zertifizierungsstelle Zertifikate zu beantragen bzw. zu verlängern.
Seit einiger Zeit ist es möglich, Zertifikate selbst zu erstellen.

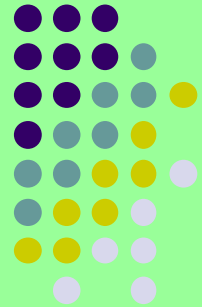
Sicherheit: Sicherer als OpenPGP ist S/MIME nicht. Hier treffen zwei Glaubensgemeinschaften aufeinander, die ihr vertretenes Verfahren vehement verteidigen.

OpenPGP (Open Pretty Good Privacy)



- OpenPGP ist ein standardisiertes Datenformat für verschlüsselte und digital signierte Daten. Auch wird das Format von Zertifikaten festgelegt, die landläufig als „Schlüssel“ bezeichnet werden.
- Es basiert auf dem Format, das von PGP 5 eingeführt wurde, und ist im RFC 4880 standardisiert.
- OpenPGP benutzt eine hybride Verschlüsselung, die die Vorteile asymmetrischer Kryptosysteme (sichere Schlüsselübertragung) mit denen symmetrischer Kryptosysteme (hohe Geschwindigkeit) kombiniert.
- Statt wie bei einem symmetrischen System nur einen Schlüssel sowohl für Ver- als auch Entschlüsselung zu verwenden, besteht bei einem asymmetrischen System ein Schlüsselpaar aus zwei zusammengehörigen Schlüsseln, einem öffentlichen und einem geheimen.
  Daten, die mit dem öffentlichen Schlüssel verschlüsselt wurden, können nur mit dem geheimen Schlüssel wieder entschlüsselt werden; es ist nicht möglich, die Verschlüsselung mit dem öffentlichen Schlüssel aufzuheben. Mit dem asymmetrischen Verfahren wird ein symmetrischer Sitzungsschlüssel verschlüsselt, mit dem wiederum die eigentlichen Daten verschlüsselt werden.

Verschlüsselungsprogramme

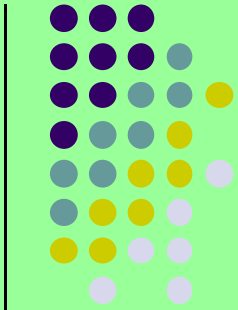


Welche Möglichkeiten bestehen zur Realisierung der Verschlüsselung in den gängigsten e-Mail Clients?

Windows/Outlook:

Gpg4Win ist ein Programm für Windows zum Verschlüsseln und Signieren von e-Mails, Dateien und Ordner. Es ist freie Software.
https://www.gpg4win.de/index-de.html
https://www.gpg4win.de/download-de.html
Anders als der Name vermuten läßt, unterstützt Gpg4Win die beiden kryptografischen Standards OpenPGP und S/MIME (X.509).
Das Einrichten von X.509-Wurzelzertifikaten ist durch Gpg4win stark vereinfacht worden und ermöglicht so auch unerfahrenen Anwendern die einfache Verwendung von S/MIME. Für komplexere Anforderungen werden Systemadministratoren durch eine Anleitung bei der Einrichtung einer systemweiten Wurzel-Vertrauensstellung unterstützt.

Gpg4Win



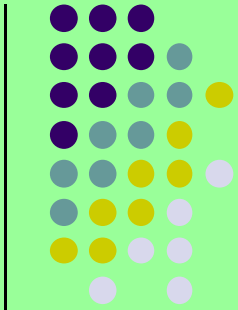
Hohe Algorithmenstärken in GnuPG

Gpg4win ist die offizielle GnuPG Distribution für Windows und bietet damit die gewohnt hohe Sicherheit von GnuPG. GnuPG hält sich an die Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

Bei der Erstellung von OpenPGP- und X.509-Zertifikaten wird eine voreingestellte Schlüssellänge von 2048 bit verwendet. Es sind Schlüssellängen bis 4096 bit möglich. Als Signatur- und Verschlüsselungsverfahren kommt RSA zum Einsatz.

RSA (Rivest, Shamir und Adleman) ist ein asymmetrisches kryptographisches Verfahren, das sowohl zum Verschlüsseln als auch zum digitalen Signieren verwendet werden kann. Es verwendet ein Schlüsselpaar, bestehend aus einem privaten Schlüssel, der zum Entschlüsseln oder Signieren von Daten verwendet wird, und einem öffentlichen Schlüssel, mit dem man verschlüsselt oder Signaturen prüft. Der private Schlüssel wird geheim gehalten und kann nur mit extrem hohem Aufwand aus dem öffentlichen Schlüssel berechnet werden.

GnuPG (Gnu Privacy Guard)



- GnuPG oder GPG (GNU Privacy Guard; englisch für GNU-Privatsphärenschutz) ist ein freies Kryptographiesystem. Es dient zum Ver- und Entschlüsseln von Daten sowie zum Erzeugen und Prüfen elektronischer Signaturen.

- Das Programm implementiert den OpenPGP-Standard nach RFC 4880 und wurde als Ersatz für PGP entwickelt. Versionen ab 2.0 implementieren auch den S/MIME-Standard. GnuPG benutzt standardmäßig nur patentfreie Algorithmen und wird unter der GNU-GPL vertrieben. Es kann unter GNU/Linux, Mac OS X und diversen anderen unixoiden Systemen sowie unter Microsoft Windows betrieben werden.

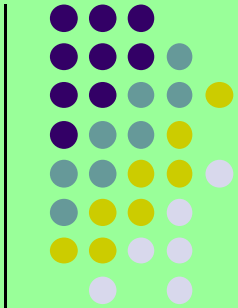
Gpg4Win

- **E-Mail**

- **Signieren und Verschlüsseln**
- Das mitgelieferte Outlook-Plugin GpgOL ermöglicht E-Mails direkt in Microsoft Outlook zu signieren und zu verschlüsseln. Dabei werden auch Anhänge verschlüsselt. Das Signaturprüfen und Entschlüsseln funktioniert genauso einfach direkt in Outlook.

- **Benutzerfreundliche Zertifikatsauswahl**
- Die Auswahl des richtigen E-Mail-Zertifikats übernimmt Kleopatra - und zwar anhand der richtigen E-Mail-Adresse. Sollten Sie mehrere passende Zertifikate installiert haben, bietet Kleopatra Ihnen die Zertifikatsvorauswahl in einem übersichtlichen Dialog an.
- Für "Viel-Benutzer" bietet Gpg4win die Möglichkeit, die Zertifikatsbestätigung nur im Konfliktfall anzuzeigen. Damit entfällt z.B. das regelmäßige Bestätigen eines eindeutig passenden Zertifikats beim E-Mail signieren und verschlüsseln. Das Arbeiten läuft so wesentlich zügiger - ohne Verlust der Sicherheit.

Gpg4Win



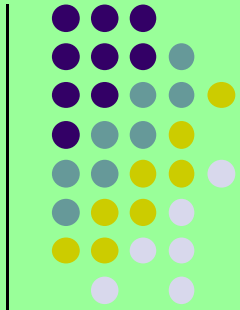
- **Zertifikatsverwaltung mit Kleopatra**

- Zertifikate sicher und komfortabel verwalten
- Kleopatra ist der bevorzugte Zertifikatsmanager in Gpg4win. Kleopatra ermöglicht Ihnen die einfache Verwaltung alle Zertifikate (OpenPGP und S/MIME).

- **Zertifikatsserver**
- Kleopatra bietet einen einfachen Im- und Export von Zertifikaten von bzw. zu OpenPGP-Zertifikatsservern (auch Schlüsselserver) und X.509-(LDAP-) Zertifikatsservern.

- OpenPGP-Zertifikate beglaubigen
- Durch das Beglaubigen (auch signieren) von einem anderen, Ihnen vertrauten, OpenPGP-Zertifikat bringt Kleopatra dieses Zertifikat in eine neue Vertrauensstufe - gekennzeichnet als "vertrauenswürdiges Zertifikat".

Thunderbird / Enigmail

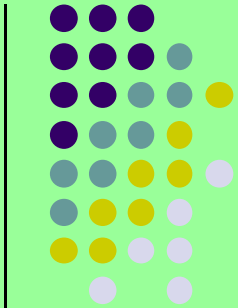


Enigmail integriert OpenPGP-Verschlüsselung und Authentifizierung in Thunderbird und andere Mozilla-basierten E-Mail-Programme (wie SeaMonkey und Postbox). Dabei stellt Enigmail die Benutzeroberfläche zur Verfügung, während die Verschlüsselung selbst von GnuPG im Hintergrund vorgenommen wird.

GnuPG ist eine kostenlos und frei (Open-Source) verfügbare OpenPGP-Software. Enigmail kann nicht mit der kommerziellen Software PGP in Thunderbird verwendet werden, ist aber in Kombination mit GnuPG kompatibel zu PGP, so dass Sie auch über verschlüsselte E-Mails mit jeglichen (Open-)PGP-Anwendern kommunizieren können. Zudem unterstützt Enigmail nicht nur den älteren Inline-PGP-Standard, sondern auch den moderneren Standard PGP/MIME, um HTML-Mails und Attachments zu verschlüsseln und zu unterschreiben.

Enigmail enthält unter anderem eine Schlüsselverwaltung, um Schlüssel zu erzeugen, die Vertrauensstellung von Schlüsseln anzupassen oder auch Schlüssel zu signieren. Alle Funktionen Enigmails beziehen sich auf die Kommunikation mit E-Mail. Um Datei-basierte Aufgaben zu erledigen, wie das Signieren von Dateien, benötigen Sie bei Bedarf eine externe Schlüsselverwaltung/Software.

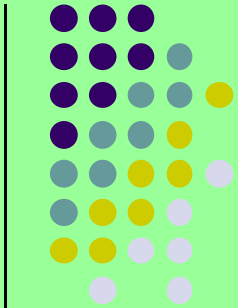
Enigmail (Addon für Thunderbird)



Voraussetzungen für Enigmail

Neben Thunderbird und einer passenden Enigmail-Version benötigt man die mit Enigmail funktionierende OpenPGP Verschlüsselungs-Software GnuPG. In neueren Enigmail-Versionen kann man den Download und das Installieren der GnuPG-Software direkt aus Enigmails Einrichtungs-Assistenten heraus starten und muss sich nicht mehr manuell darum kümmern (dies gilt unter Windows und Mac OS X). Sie können bei Bedarf GnuPG auch selbst von http://gnupg.org/download/index.de.html oder (im Fall von Linux) evtl. aus dem entsprechenden "Repository" Ihres Linux-Builds herunterladen. Die aktuellen Versionen für Windows enthalten inzwischen auch ein Installationsprogramm, das die Installation relativ einfach macht.

Enigmail (Addon für Thunderbird)

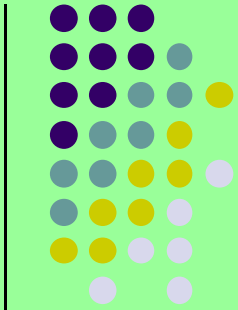


Enigmail-Installation

Installieren Sie Thunderbird (vermutlich schon geschehen). Es ist vor der Enigmail-Installation auf jeden Fall erforderlich, dass Sie Thunderbird installiert und Ihr E-Mail-Konto in Thunderbird grundlegend konfiguriert haben, so dass Sie damit bereits arbeiten (also Nachrichten senden und empfangen) können.

Wenn Sie eine offizielle Version von Thunderbird installiert haben und verwenden, können Sie Enigmail von AMO (**a**ddons.**m**ozilla.**o**rg) herunterladen bzw. direkt in Thunderbird über den **Add-ons-Manager** laden und installieren.

Enigmail (Addon für Thunderbird)



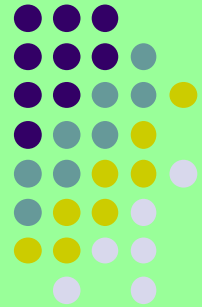
Enigmail einrichten

Enigmail bietet einen komfortablen Assistenten, der mit ausführlichen Erklärungen durch die einzelnen Schritte der Konfiguration führt. Wenn Sie Enigmail jetzt das erste Mal in Thunderbird installiert haben und einen der Menüpunkte des Menüs Enigmail aufrufen, wird der Assistent automatisch gestartet. Sie können den Assistenten auch nachträglich über das Menü Enigmail ➔ Einrichtungs-Assistent aufrufen.

GnuPG-Installation

Der Einrichtungs-Assistent prüft, ob GnuPG bereits auf Ihrem System installiert ist. Wenn GnuPG nicht gefunden wird, bietet der Assistent unter Windows und OS X den passenden GnuPG-Download inklusive Installation an. Falls Sie wissen, dass GnuPG auf Ihrem System doch schon installiert ist, können Sie mit dem Assistenten auch den korrekten Dateipfad zur GnuPG-Anwendung aufsuchen, so dass Enigmail dann im Weiteren darauf zugreifen kann.

Enigmail (Addon für Thunderbird)

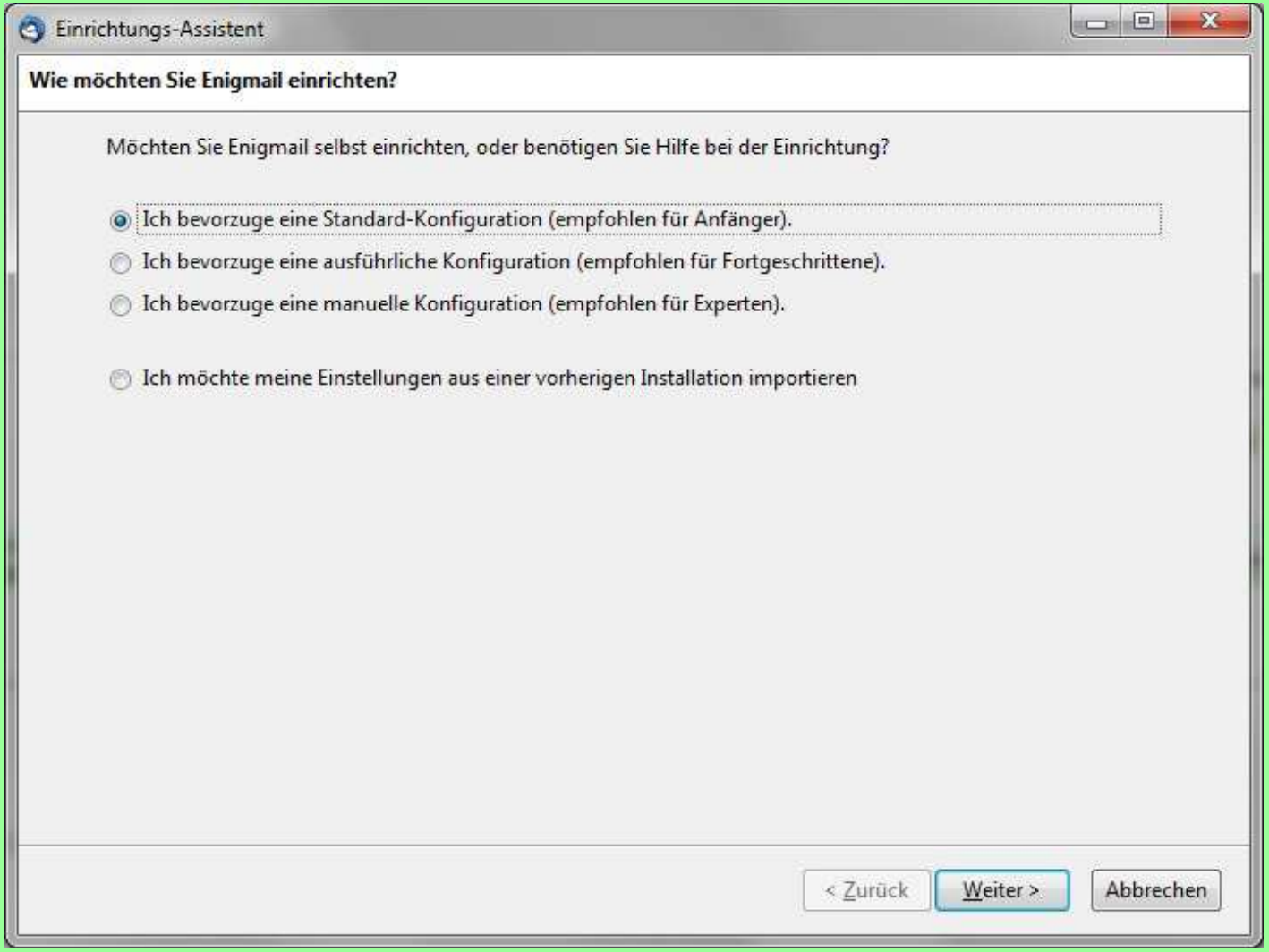


Grundlegende Einstellungen Enigmails

Nach der GnuPG-Installation geht der Einrichtungs-Assistent weiter und hilft Ihnen ein paar notwendige Einstellungen für Enigmail zu machen und, falls noch nicht vorhanden, ein Schlüsselpaar (öffentlicher + zugehöriger privater Schlüssel) für Sie zu erstellen.

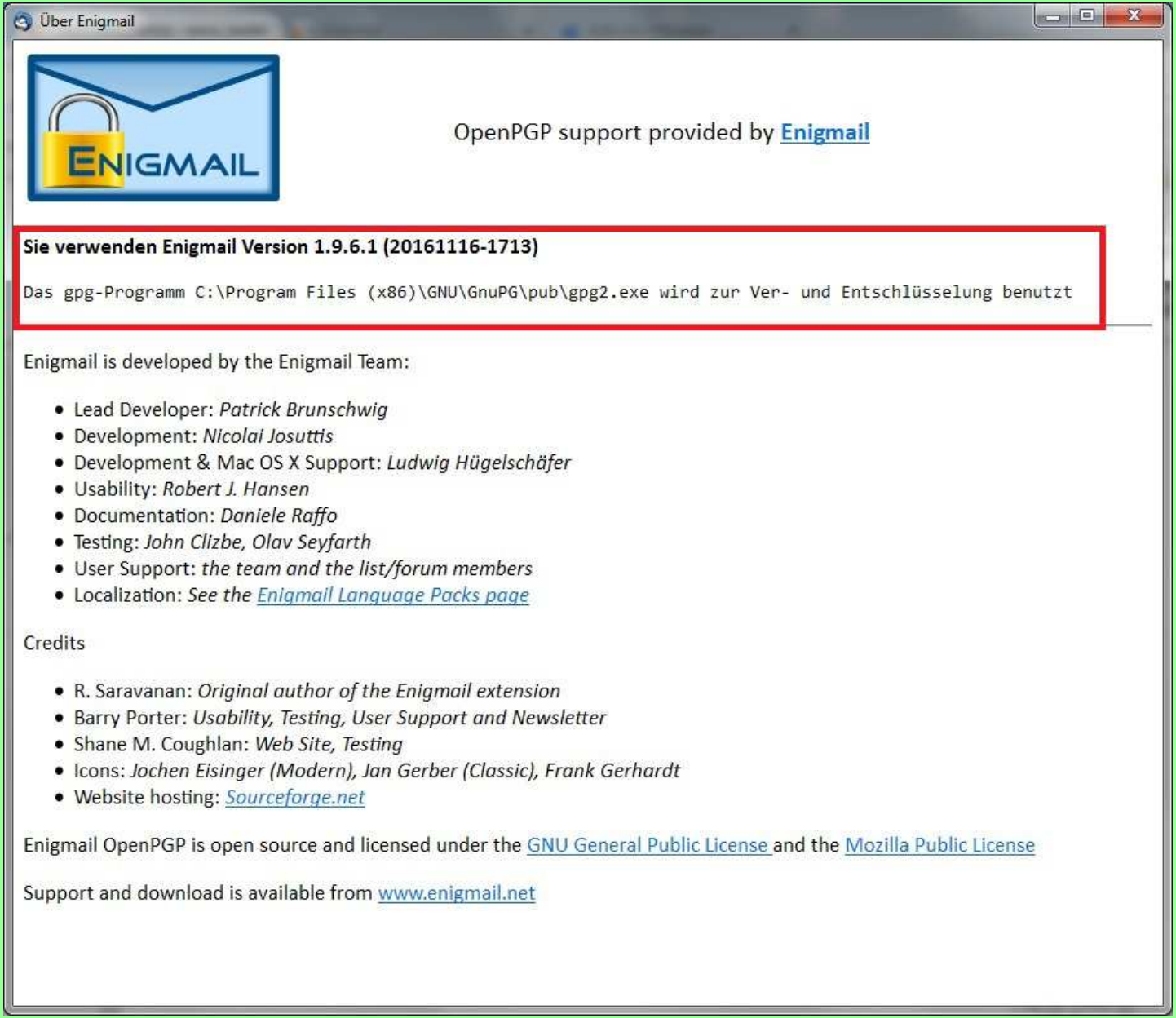
Enigmail (Addon für Thunderbird)

Einrichtungsassistent:



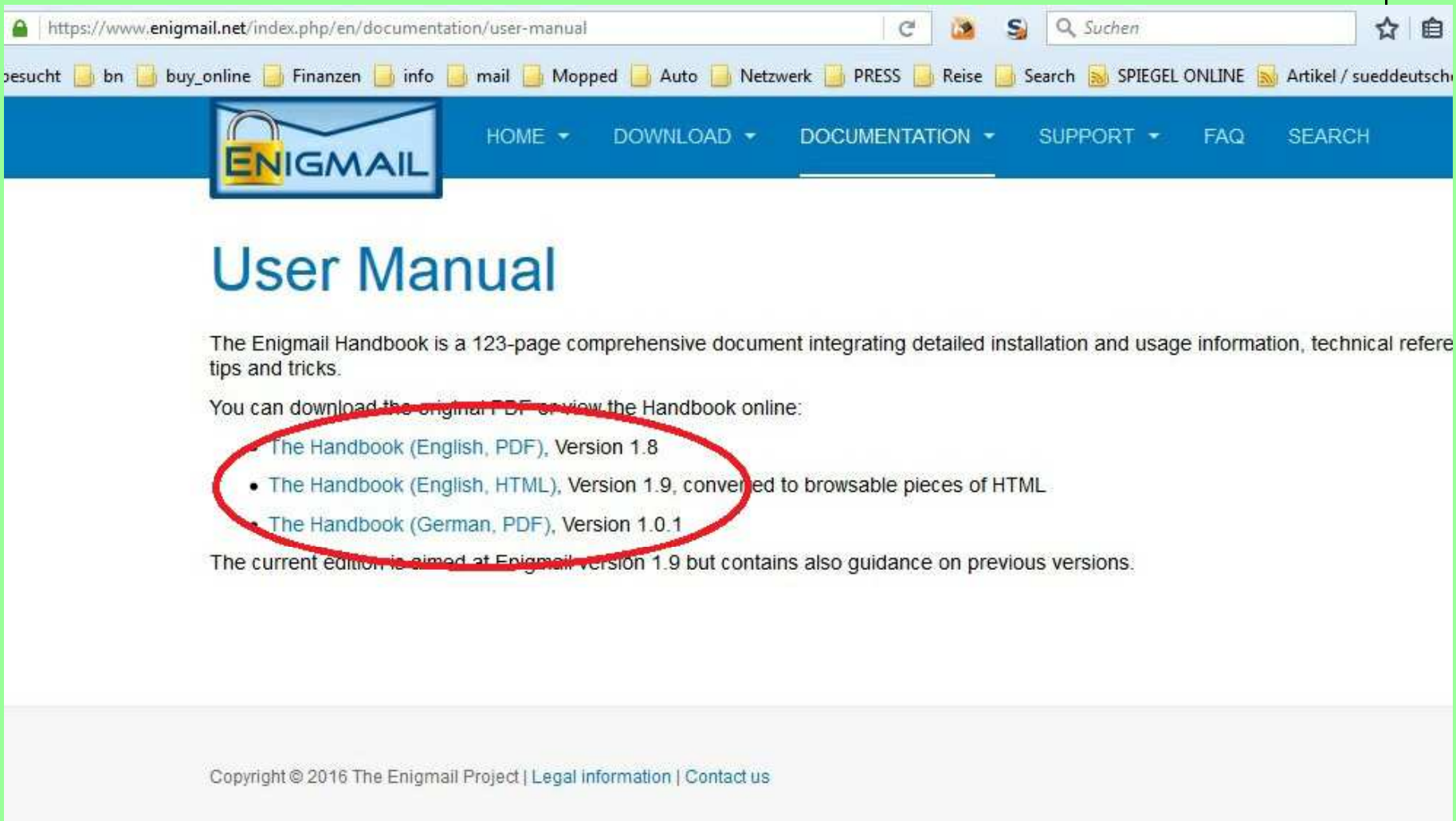
Thunderbird / Enigmail

Enigmail Version:



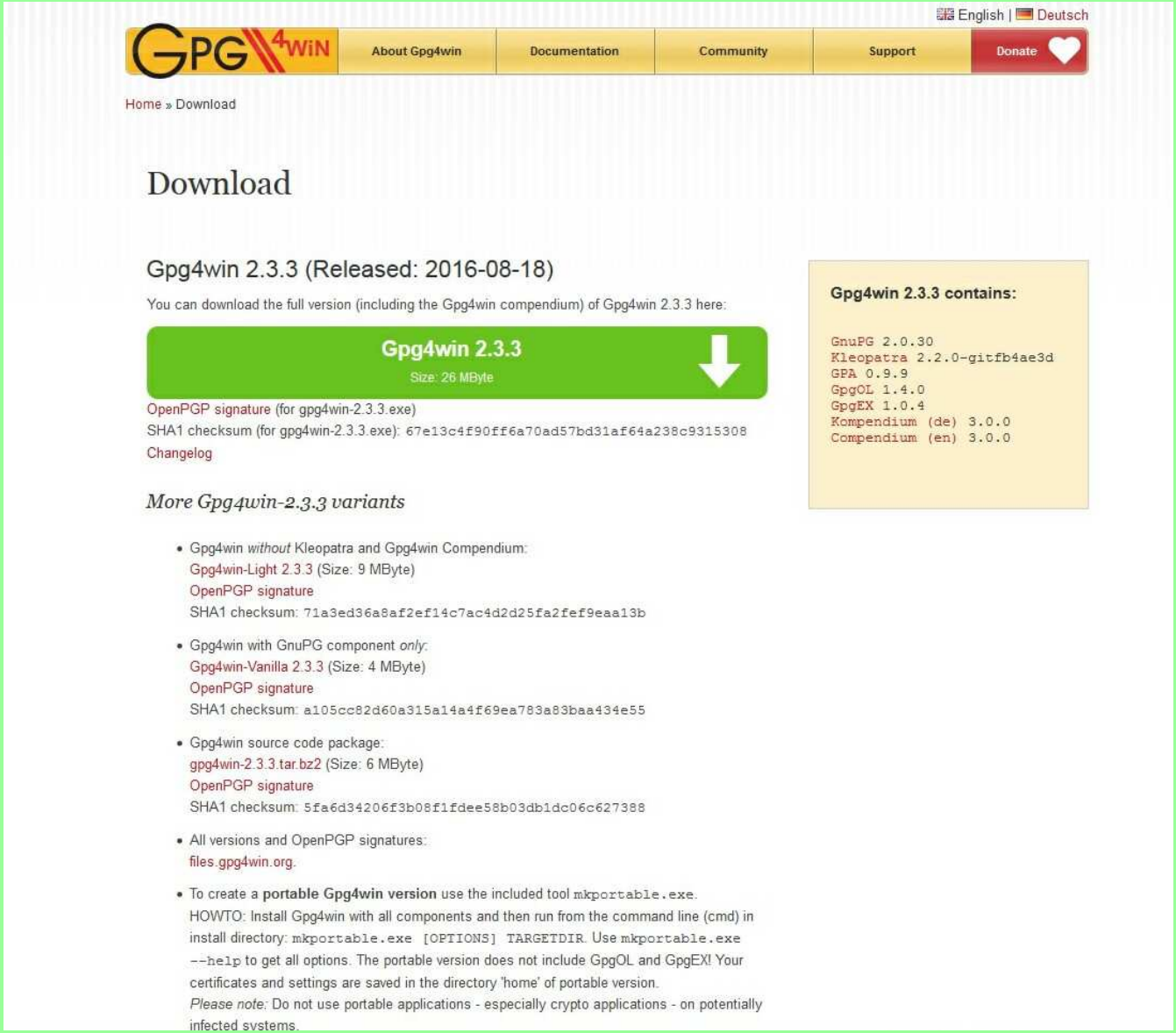
Thunderbird / Enigmail

Bedienungsanleitung in Deutsch bzw. Englisch:



Gpg4Win / Outlook

Downloadseite und aktuelle Version (Link -> Folie 19):



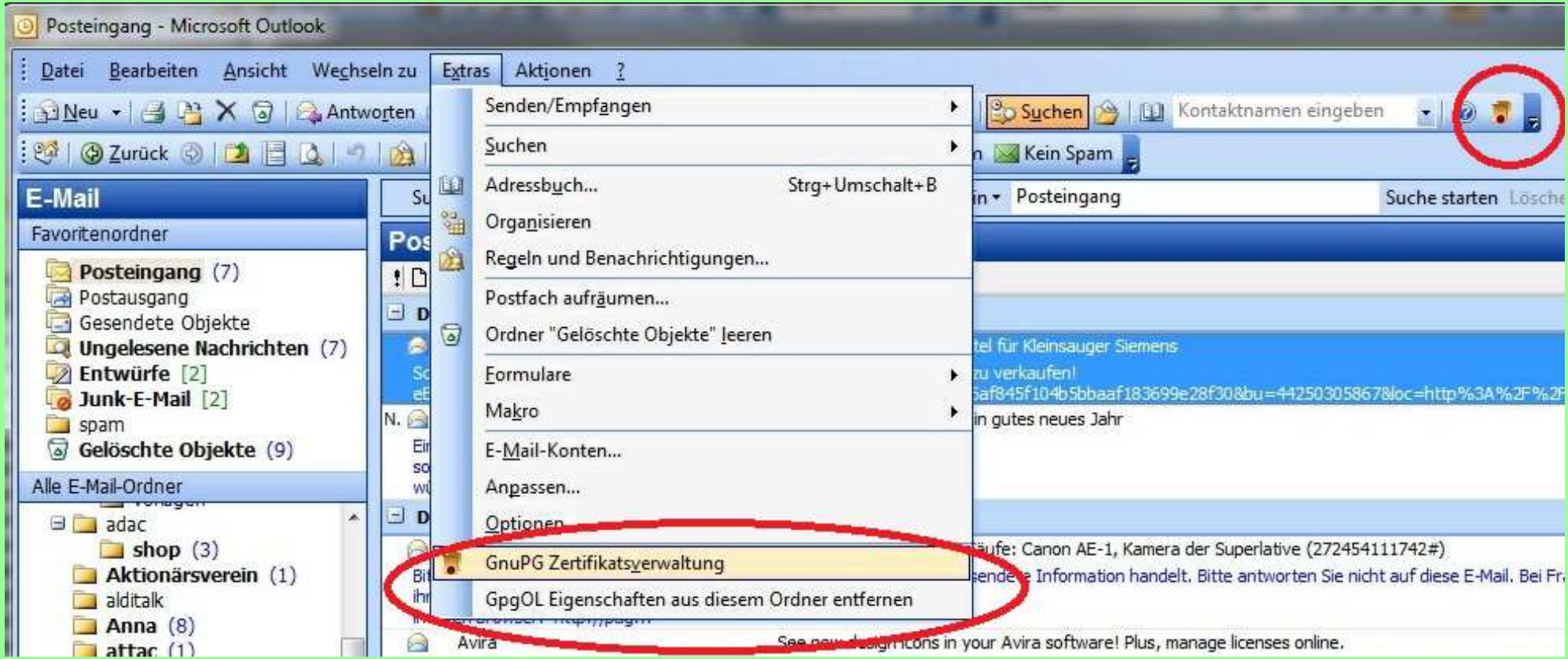
Gpg4win 2.3.3 enthält:
GnuPG 2.0.30
Kleopatra 2.2.0-gitgfb4ae3d
GPA 0.9.9
GpgOL 1.4.0
GpgEX 1.0.4
Kompendium (de) 3.0.0
Compendium (en) 3.0.0

Dateiname:
gpg4win-2.3.3.exe
ca. 25 MByte

Einfache Installation mit Auswahl der gewünschten Komponenten.
Outlook sollte geschlossen sein.
Kleopatra sollte unbedingt mit installiert werden.

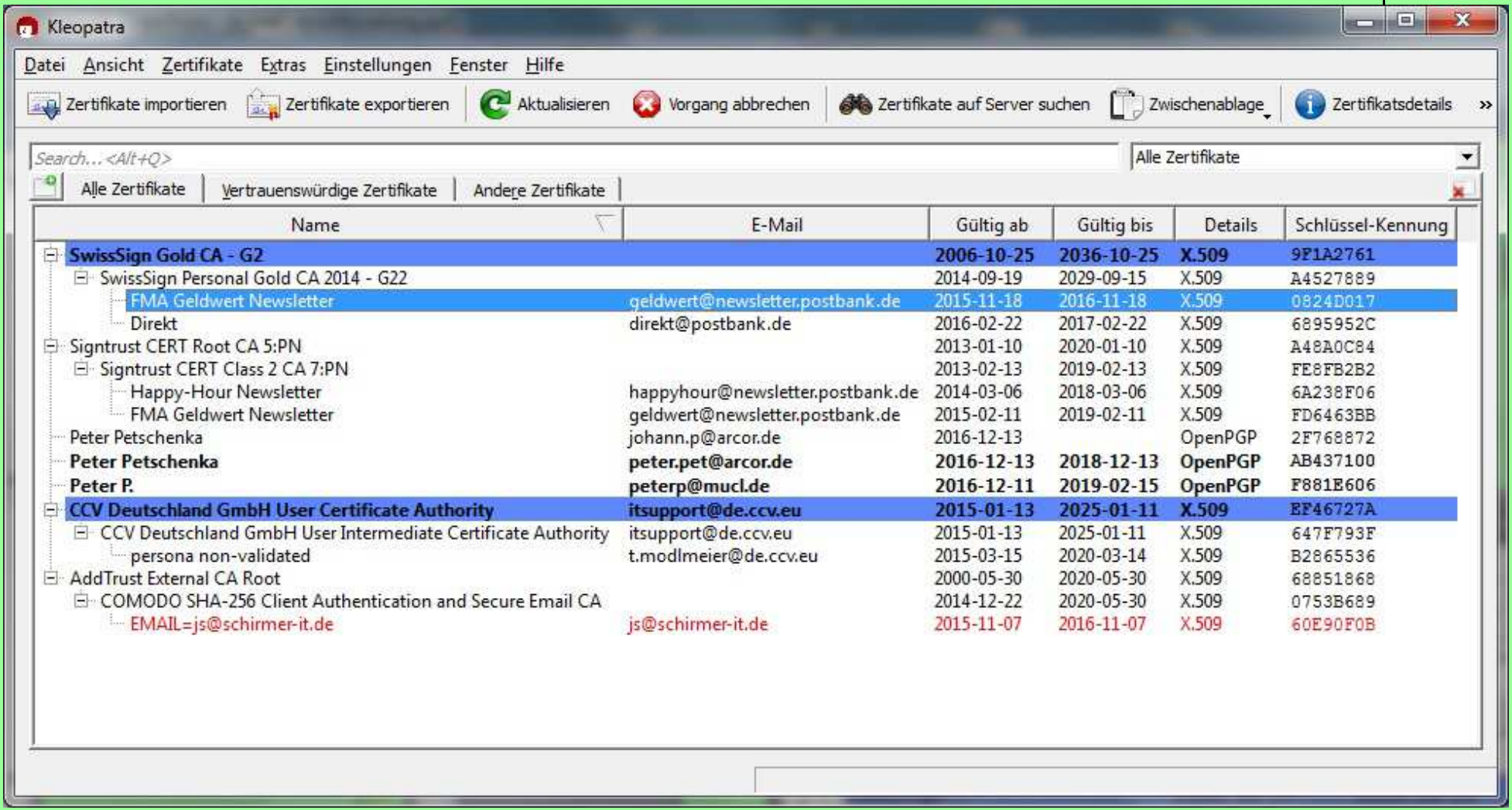
Gpg4Win / Outlook

Nach Installation von Gpg4win und damit auch GpgOL für Outlook und Starten von Outlook ergibt sich folgender Zusatz bei Outlook:



Outlook: Schlüssel herstellen

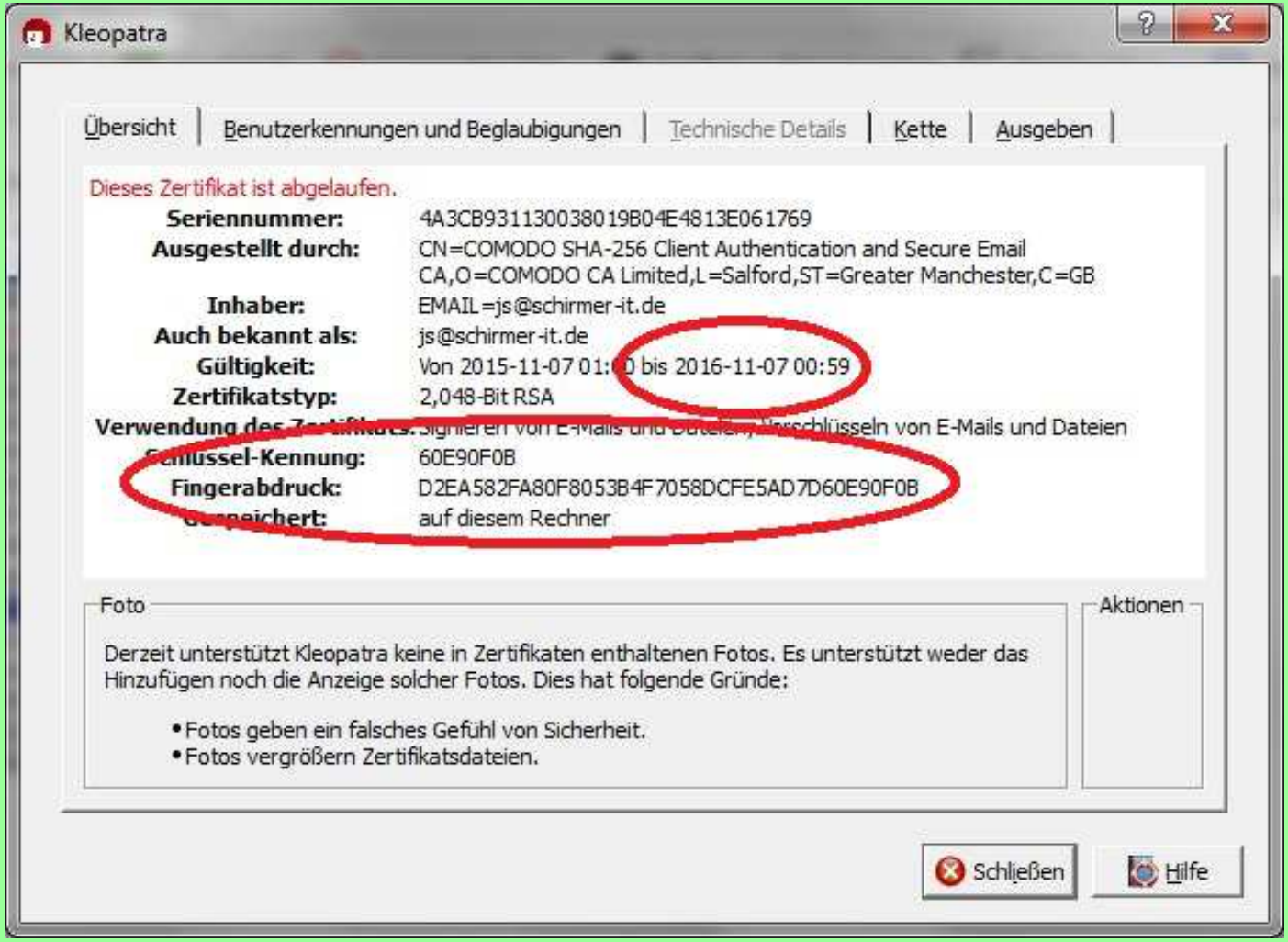
Mit Kleopatra werden Schlüssel verwaltet/erzeugt:



Name	E-Mail	Gültig ab	Gültig bis	Details	Schlüssel-Kennung
SwissSign Gold CA - G2		**2006-10-25**	**2036-10-25**	**X.509**	**9F1A2761**
SwissSign Personal Gold CA 2014 - G22		2014-09-19	2029-09-15	X.509	A4527889
FMA Geldwert Newsletter	geldwert@newsletter.postbank.de	2015-11-18	2016-11-18	X.509	0824D017
Direkt	direkt@postbank.de	2016-02-22	2017-02-22	X.509	6895952C
Signtrust CERT Root CA 5:PN		2013-01-10	2020-01-10	X.509	A48A0C84
Signtrust CERT Class 2 CA 7:PN		2013-02-13	2019-02-13	X.509	FE8FB2B2
Happy-Hour Newsletter	happyhour@newsletter.postbank.de	2014-03-06	2018-03-06	X.509	6A238F06
FMA Geldwert Newsletter	geldwert@newsletter.postbank.de	2015-02-11	2019-02-11	X.509	FD6463BB
Peter Petschenka	johann.p@arcor.de	2016-12-13		OpenPGP	2F768872
Peter Petschenka	**peter.pet@arcor.de**	**2016-12-13**	**2018-12-13**	**OpenPGP**	AB437100
Peter P.	**peterp@mucl.de**	**2016-12-11**	**2019-02-15**	**OpenPGP**	F881E606
CCV Deutschland GmbH User Certificate Authority	**itsupport@de.ccv.eu**	**2015-01-13**	**2025-01-11**	**X.509**	EF46727A
CCV Deutschland GmbH User Intermediate Certificate Authority	itsupport@de.ccv.eu	2015-01-13	2025-01-11	X.509	647F793F
persona non-validated	t.modlmeier@de.ccv.eu	2015-03-15	2020-03-14	X.509	B2865536
AddTrust External CA Root		2000-05-30	2020-05-30	X.509	68851868
COMODO SHA-256 Client Authentication and Secure Email CA		2014-12-22	2020-05-30	X.509	0753B689
EMAIL=js@schirmer-it.de	js@schirmer-it.de	2015-11-07	2016-11-07	X.509	60E90F0B

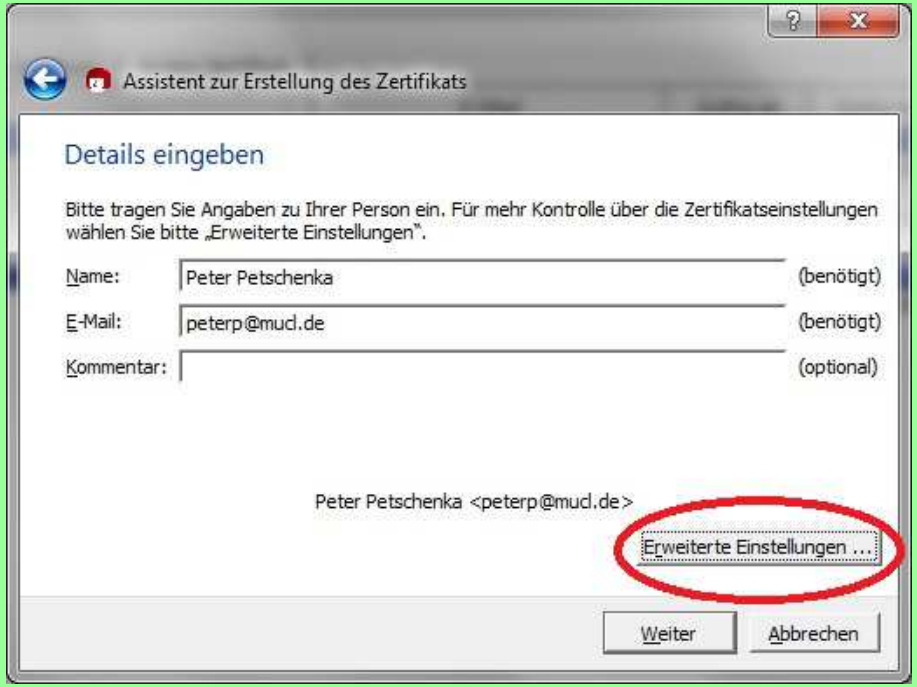
Kleopatra: Schlüsseldetails

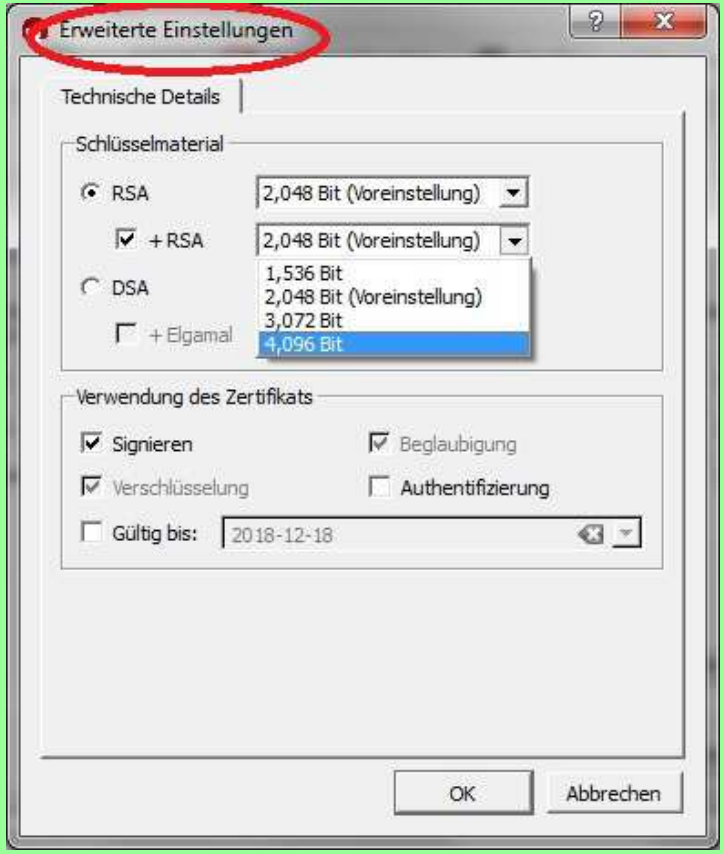
Details eines **ungültigen** Schlüssels (Importe):



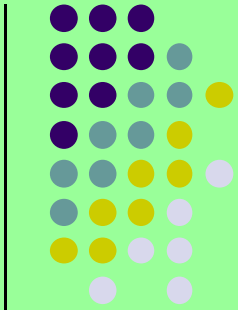
Kleopatra: Neues Zertifikat

Datei -> Neues Zertifikat -> Persönliches OpenPGP Schlüsselpaar erzeugen.





Kleopatra: neues Zertifikat



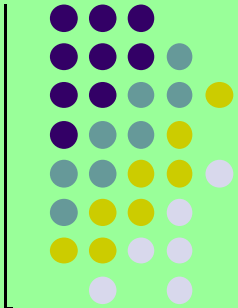
Am Ende der Zertifikatserstellung wird eine Passphrase verlangt. Das ist nichts weiter als ein Passwort.

Dieses sollte ausreichend lang und komplex sein, um dem Sicherheitsstandard gerecht zu werden.

Weiter empfiehlt es sich, dieses Passwort auf Papier zu notieren, nicht auf dem PC.

Diese Passphrase muß, wie üblich, zweimal eingegeben werden und ist dann gültig.

Kleopatra: Zertifikat exportieren



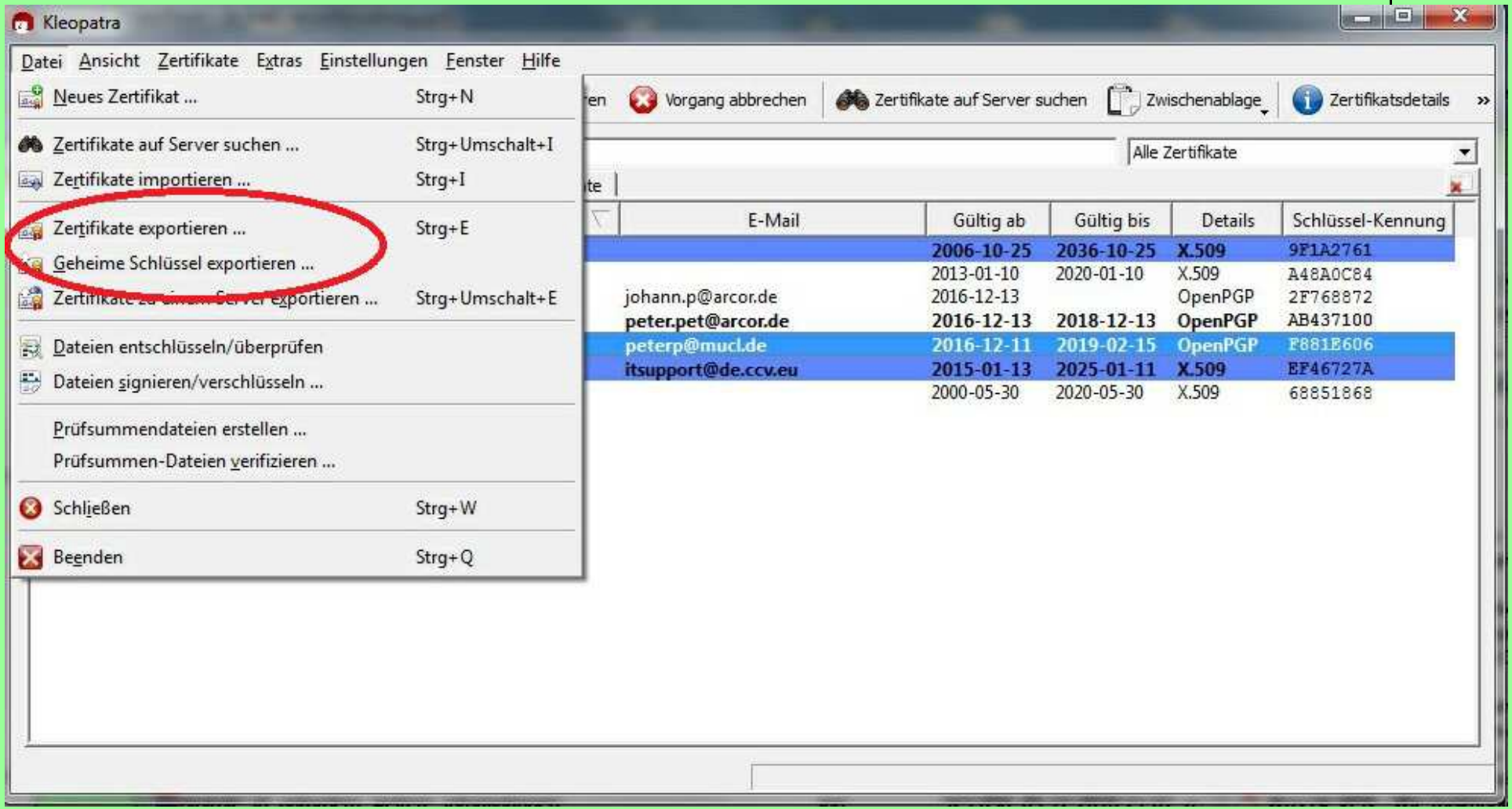
Nach Erzeugung des eigenen Zertifikats kann dieses exportiert werden. Es kann auch der geheime Schlüssel exportiert werden, aber das sollte man nur für sich selbst vornehmen und den geheimen Schlüssel nicht weitergeben.

Das Zertifikat ist der sogenannte „öffentliche Schlüssel“ der dem e-Mail Empfänger bekannt gemacht werden muß, damit er die verschlüsselte Mail des Senders entschlüsseln kann.

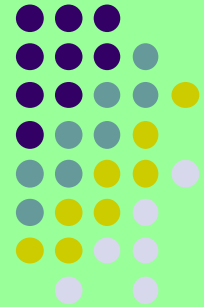
Mit dem asymmetrischen Verschlüsselungsverfahren, einem geheimen Schlüssel und einem öffentlichen Schlüssel, dem Zertifikat, wird mit OpenPGP der Ver- und Entschlüsselungsmechanismus zwischen Sender und Empfänger hergestellt.

Kleopatra: Zertifikat exportieren

Datei -> Zertifikate exportieren:



Kleopatra: Zertifikat exportieren



Das Zertifikat wird als Datei mit der Endung .asc (Voreinstellung) gespeichert.

Dieses Zertifikat sendet man entweder als Dateianhang oder als Text in der Mail an den Empfänger.

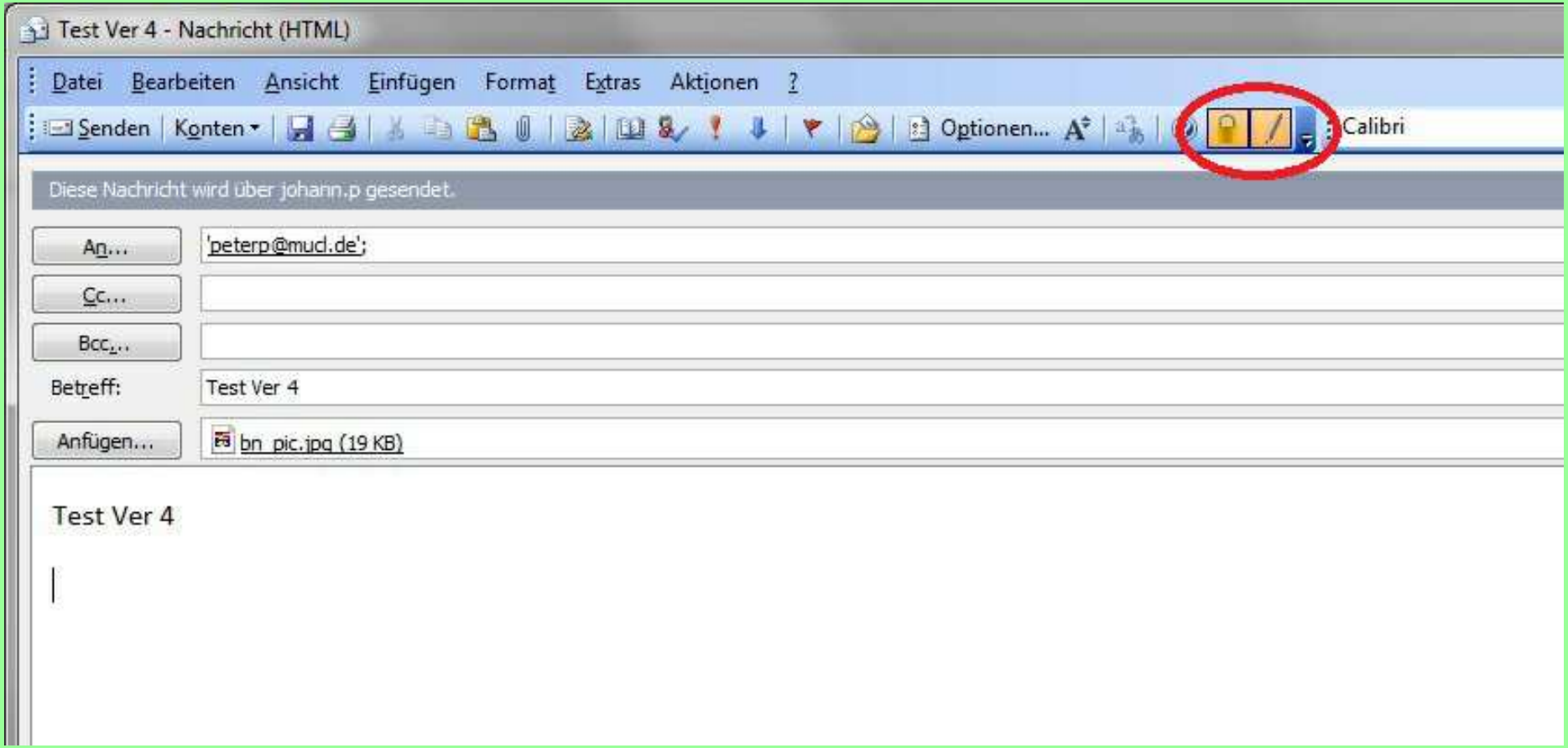
Der Empfänger importiert das Zertifikat und beglaubigt es. Zur Vorsicht kann er vorher telefonisch die Schlüsselkennung und den Fingerabdruck mit dem Sender auf Übereinstimmung vergleichen.

Dann sendet der Empfänger sein Zertifikat in einer bereits verschlüsselten Mail an den Erstsender und kann auch eine Signatur einstellen.

Der Erstsender entschlüsselt die verschlüsselte Mail mit seinem geheimen Schlüssel und installiert den öffentlichen Schlüssel des Zweitsenders. Nach einer Beglaubigung sind die Schlüssel auf beiden Seiten auf Vertrauenswürdigkeit eingestellt und nun können beliebig verschlüsselte oder siginierte oder verschlüsselt und signierte e-Mails ausgetauscht werden.

Outlook: Verschlüsselte Nachricht versenden

Unter Umständen kann beim Absenden das Passwort verlangt werden.

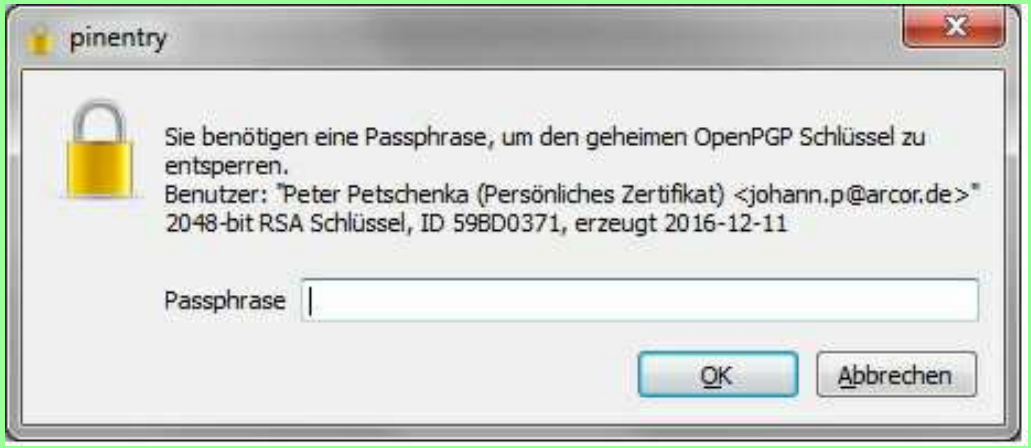


Outlook: Verschlüsselte Nachricht empfangen

Die verschlüsselte Nachricht liegt ganz normal im Posteingang und ist gekennzeichnet durch das Verschlüsselungssymbol am Zeilenbeginn.

Outlook: e-Mail entschlüsseln

Beim Anklicken der verschlüsselten e-Mail öffnet sich ein Fenster, indem die Passphrase verlangt wird.



Outlook: e-Mail entschlüsseln

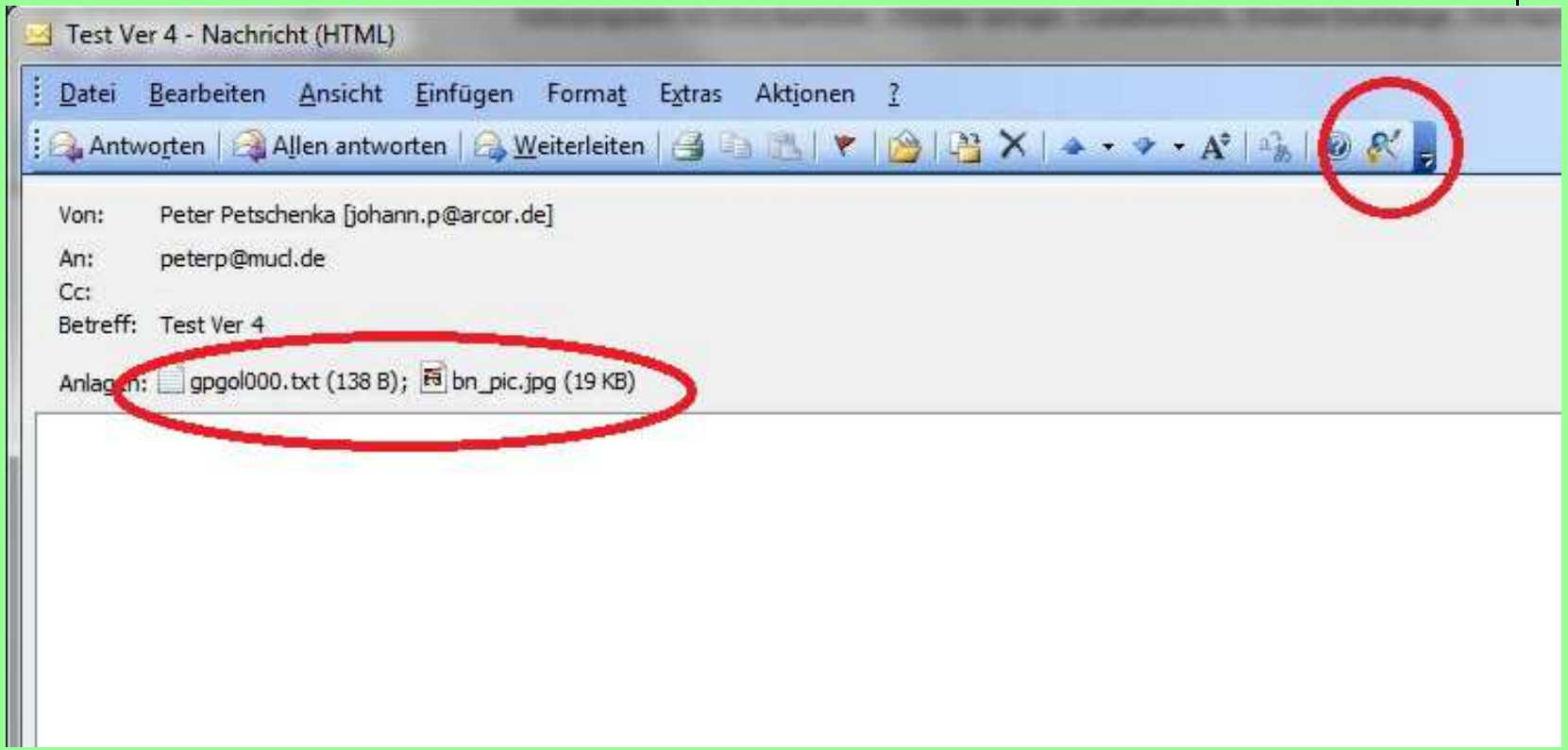
Nach Eingabe der gültigen Passphrase wird die e-Mail entschlüsselt und das Ergebnis angezeigt.

In diesem Fall war die Mail verschlüsselt **und** signiert.

Beide Verfahren laufen zusammen ab.

Outlook: entschlüsselte e-Mail

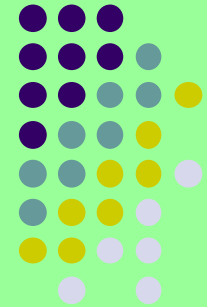
Die entschlüsselte e-Mail in Outlook sieht dann wie folgt aus:



Die Nachricht ist im Textfile gpgol000.txt enthalten, das Attachment daneben.

Mit dem Button im rechten roten Kreis kann die Signatur nochmal überprüft werden.

Thunderbird / Enigmail



Die Bezeichnung Enigmail kommt Ihnen sicher bekannt vor.

Im zweiten Weltkrieg setzte die deutsche Wehrmacht die Verschlüsselung von Nachrichten mit der legendären Verschlüsselungsmaschine **Enigma** ein.
Es dauerte sehr lange, bis diese Maschine durch eine große Anzahl britischer Experten geknackt wurde. Das zeigt ihre große Wirksamkeit.
Zum Verhängnis wurde ihr schließlich ihr symmetrisches Verfahren.

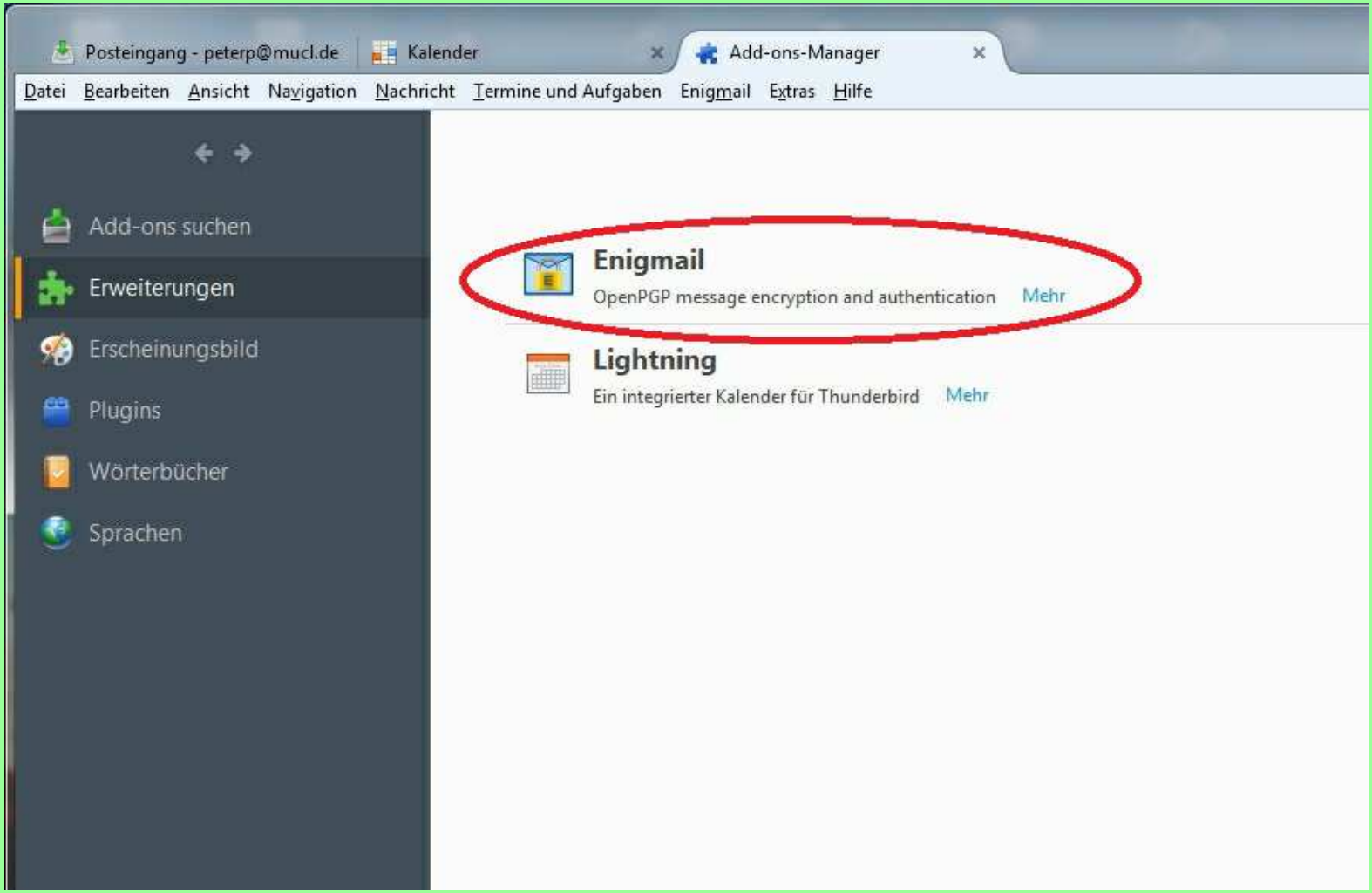
Die Entwickler des Thunderbird-Add-ons „Enigmail“ zeigen mit der Namensgebung des Add-ons den hohen Anspruch an Sicherheit, den sie mit ihrem Tool bereitstellen.

Mit Enigmail verschlüsselte e-Mails können mit Gpg4win in Outlook entschlüsselt werden und umgekehrt. Denn Enigmail nutzt ebenso wie Gpg4win das GnuPG zum Ver-/Entschlüsseln.

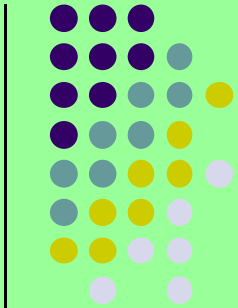
Das Add-on Enigmail ist kostenlos.

Thunderbird / Enigmail

Im Add-on Manager von Thunderbird sieht das installierte Enigmail so aus:



Thunderbird / Enigmail



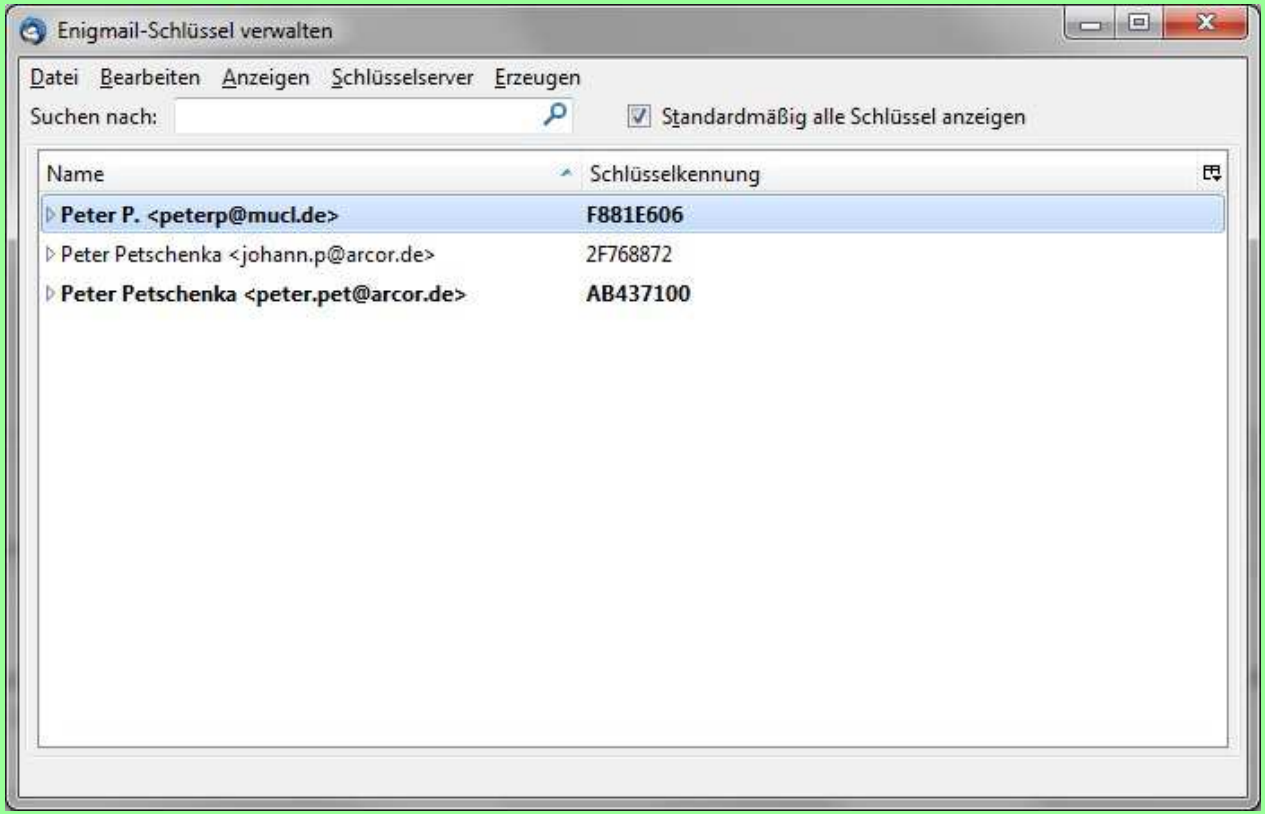
Download von Thunderbird und Enigmail:
https://www.mozilla.org/de/thunderbird/
https://addons.mozilla.org/de/thunderbird/addon/enigmail/

Enigmail integriert OpenPGP-Verschlüsselung und Authentifizierung in Thunderbird und andere Mozilla-basierten E-Mail-Programme (wie SeaMonkey und Postbox). Dabei stellt Enigmail die Benutzeroberfläche zur Verfügung, während die Verschlüsselung selbst von GnuPG im Hintergrund vorgenommen wird.

GnuPG ist eine kostenlos und frei (Open-Source) verfügbare OpenPGP-Software. Enigmail kann nicht mit der kommerziellen Software PGP in Thunderbird verwendet werden, ist aber in Kombination mit GnuPG kompatibel zu PGP, so dass Sie auch über verschlüsselte E-Mails mit jeglichen (Open-)PGP-Anwendern kommunizieren können. Zudem unterstützt Enigmail nicht nur den älteren Inline-PGP-Standard, sondern auch den moderneren Standard PGP/MIME, um HTML-Mails und Attachments zu verschlüsseln und zu unterschreiben.

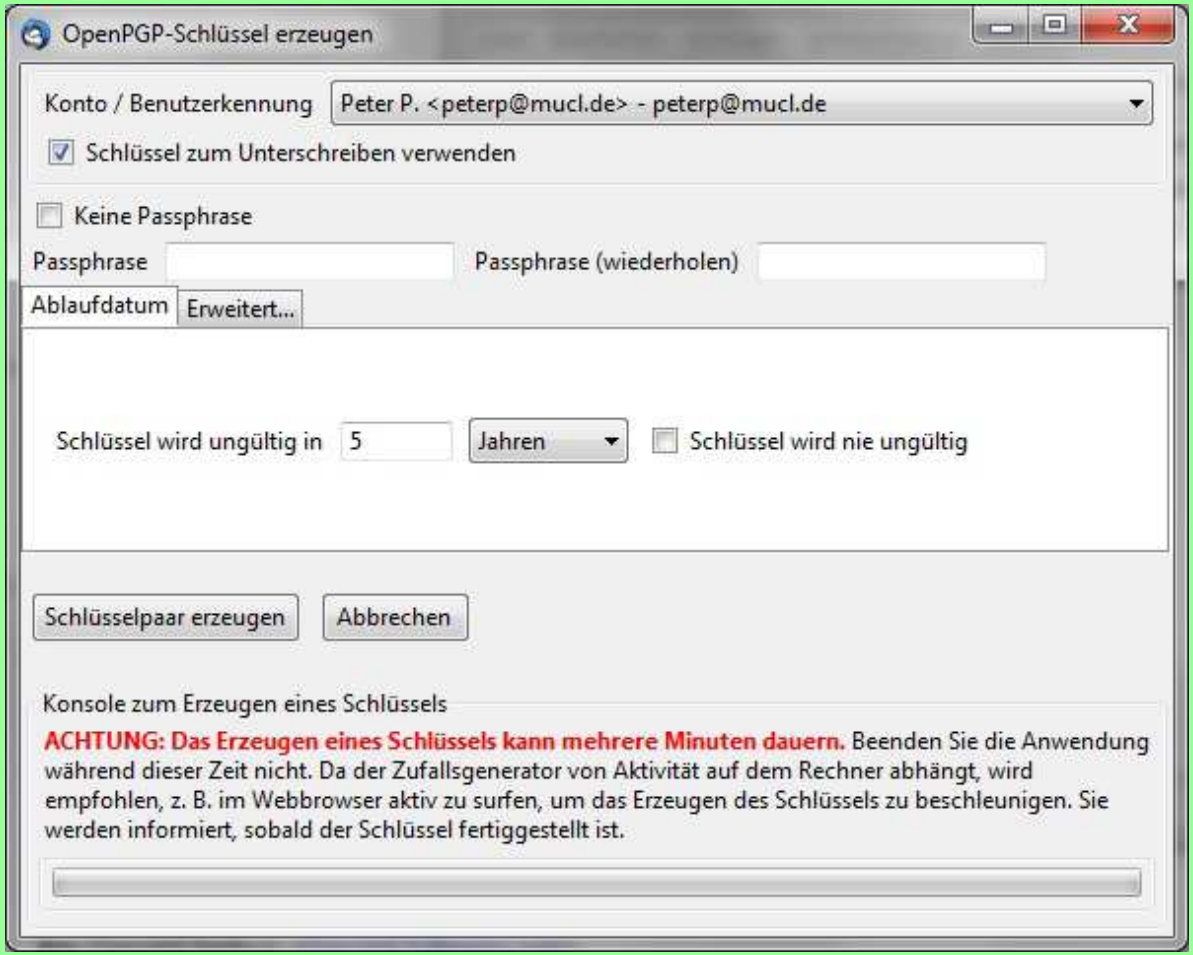
Thunderbird / Enigmail

Enigmail enthält unter anderem eine Schlüsselverwaltung, um Schlüssel zu erzeugen, die Vertrauensstellung von Schlüsseln anzupassen oder auch Schlüssel zu signieren. Alle Funktionen Enigmails beziehen sich auf die Kommunikation mit E-Mail. Um Datei-basierte Aufgaben zu erledigen, wie das Signieren von Dateien, benötigen Sie bei Bedarf eine externe Schlüsselverwaltung/Software (s. Gpg4win).



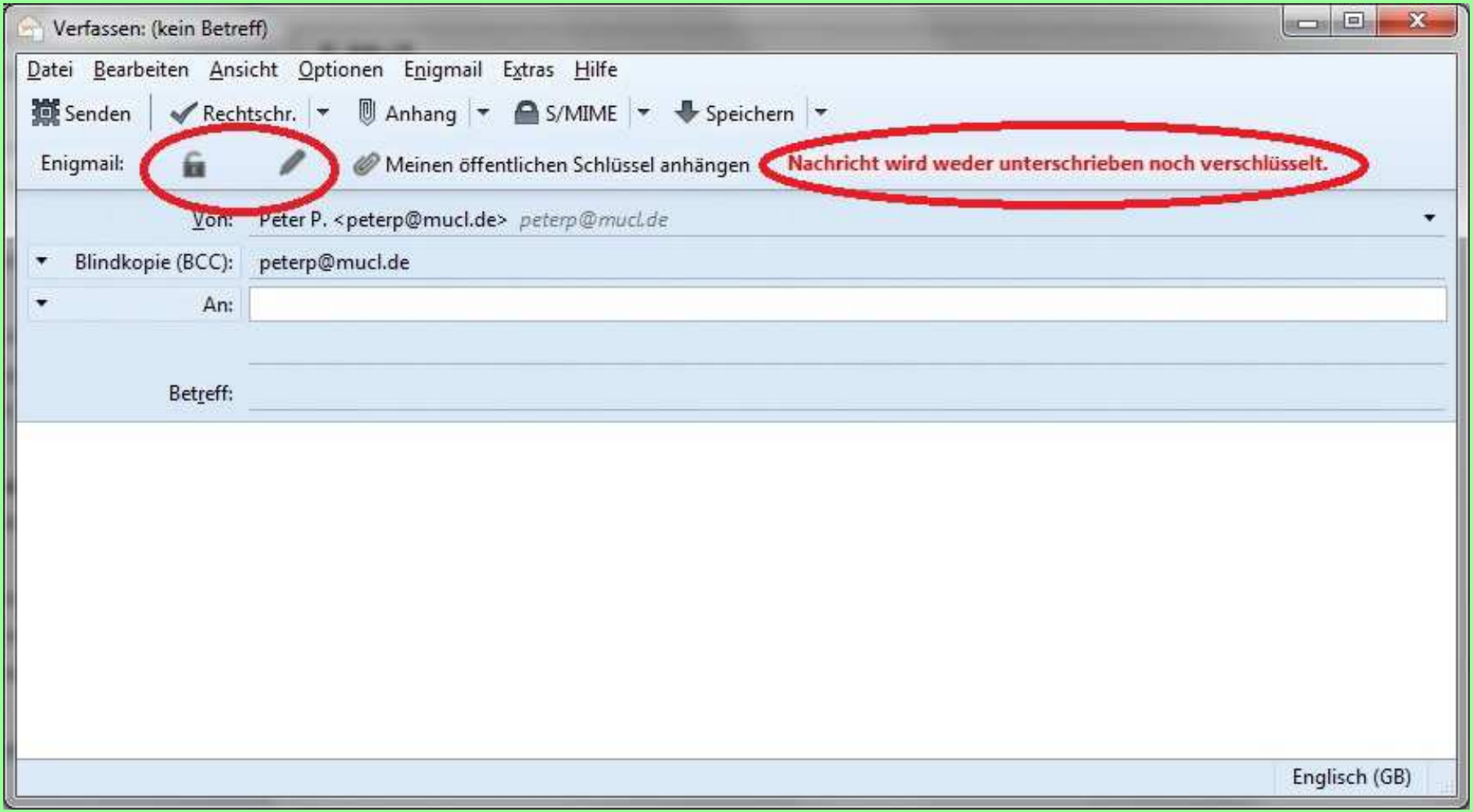
Thunderbird / Enigmail

Enigmail: Neuer Schlüssel



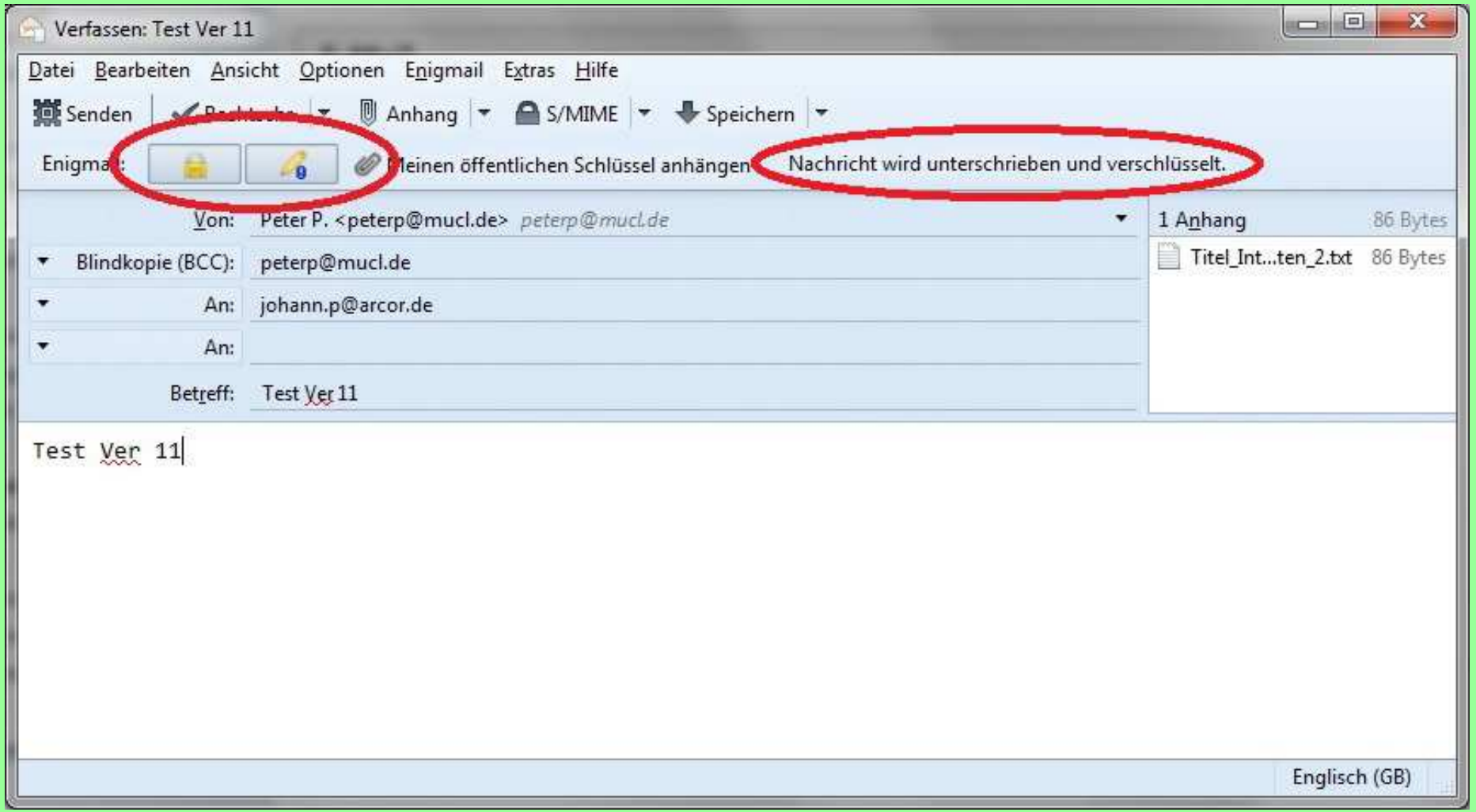
Thunderbird / Enigmail

Nachricht unverschlüsselt senden:



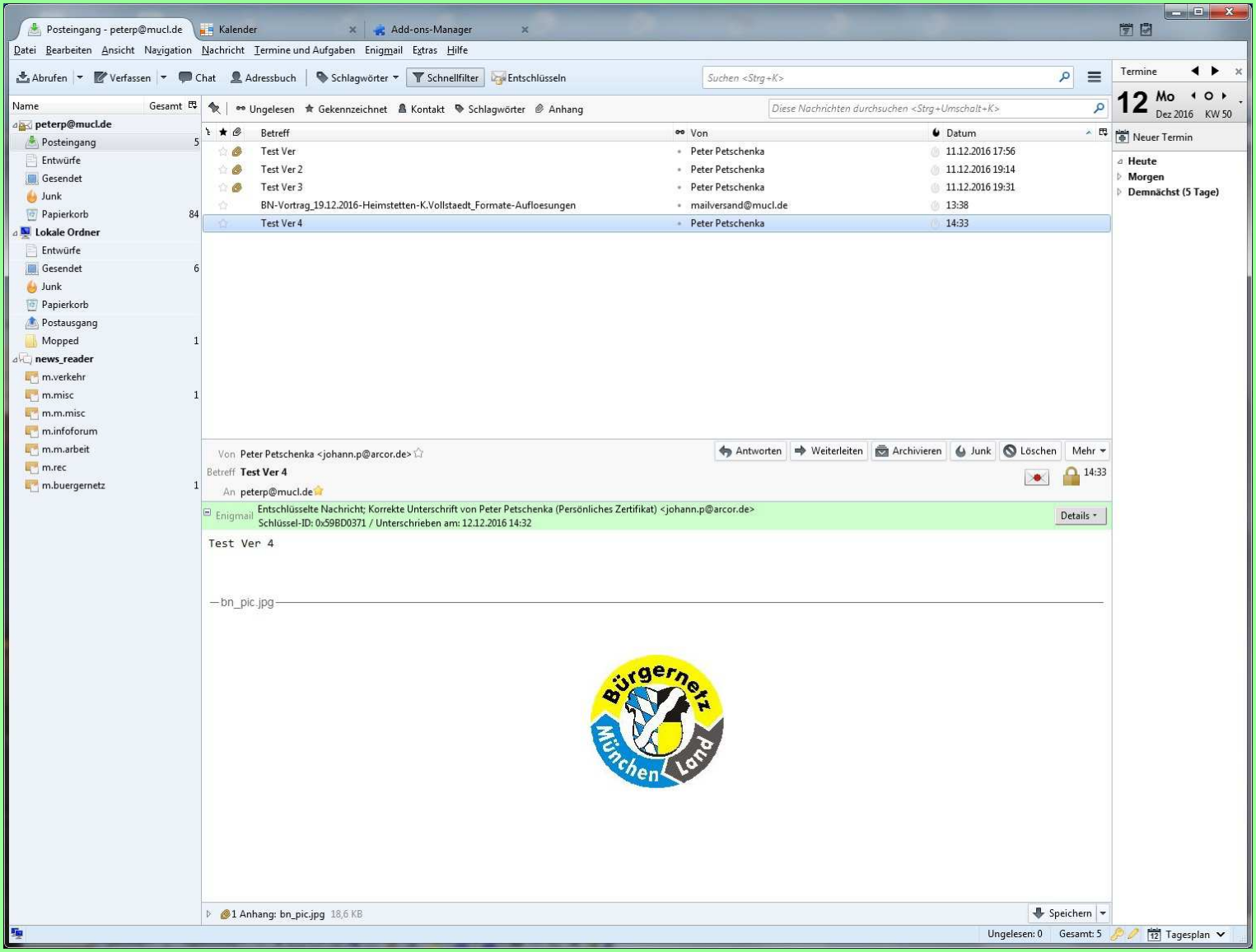
Thunderbird / Enigmail

Nachricht verschlüsselt und signiert versenden:



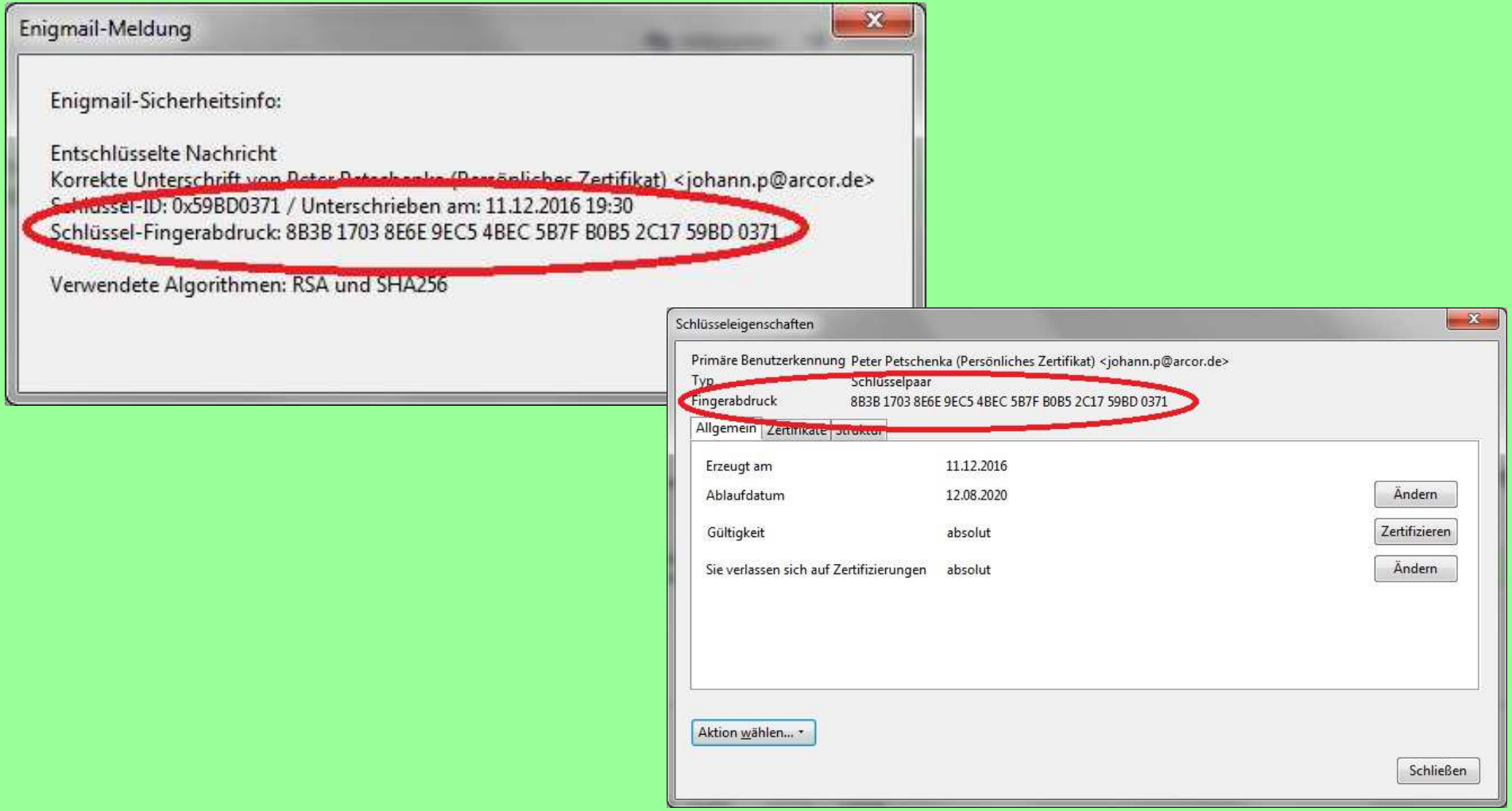
Thunderbird / Enigmail

Entschlüsselte Nachricht:



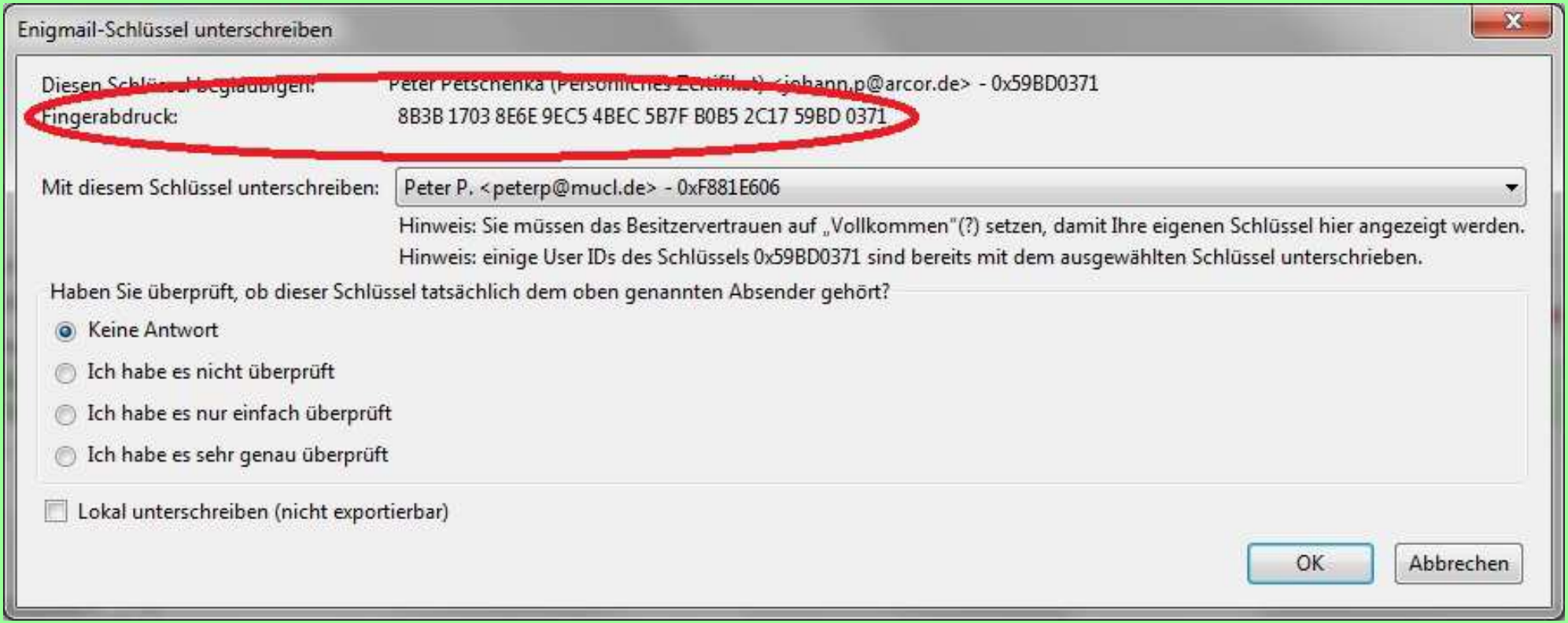
Thunderbird / Enigmail

Detail-Infos:



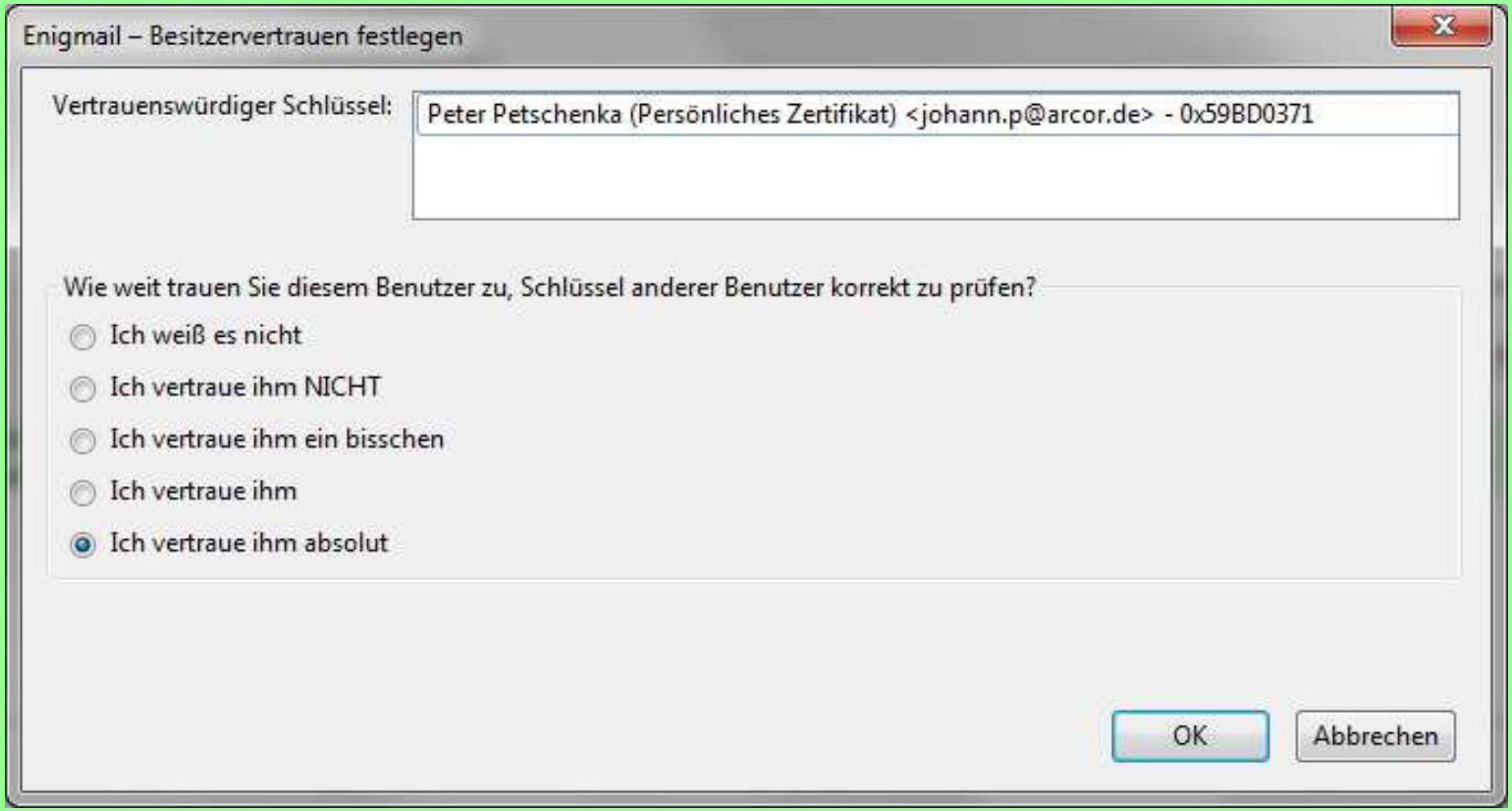
Thunderbird / Enigmail

Weitere Detail-Infos:



Thunderbird / Enigmail

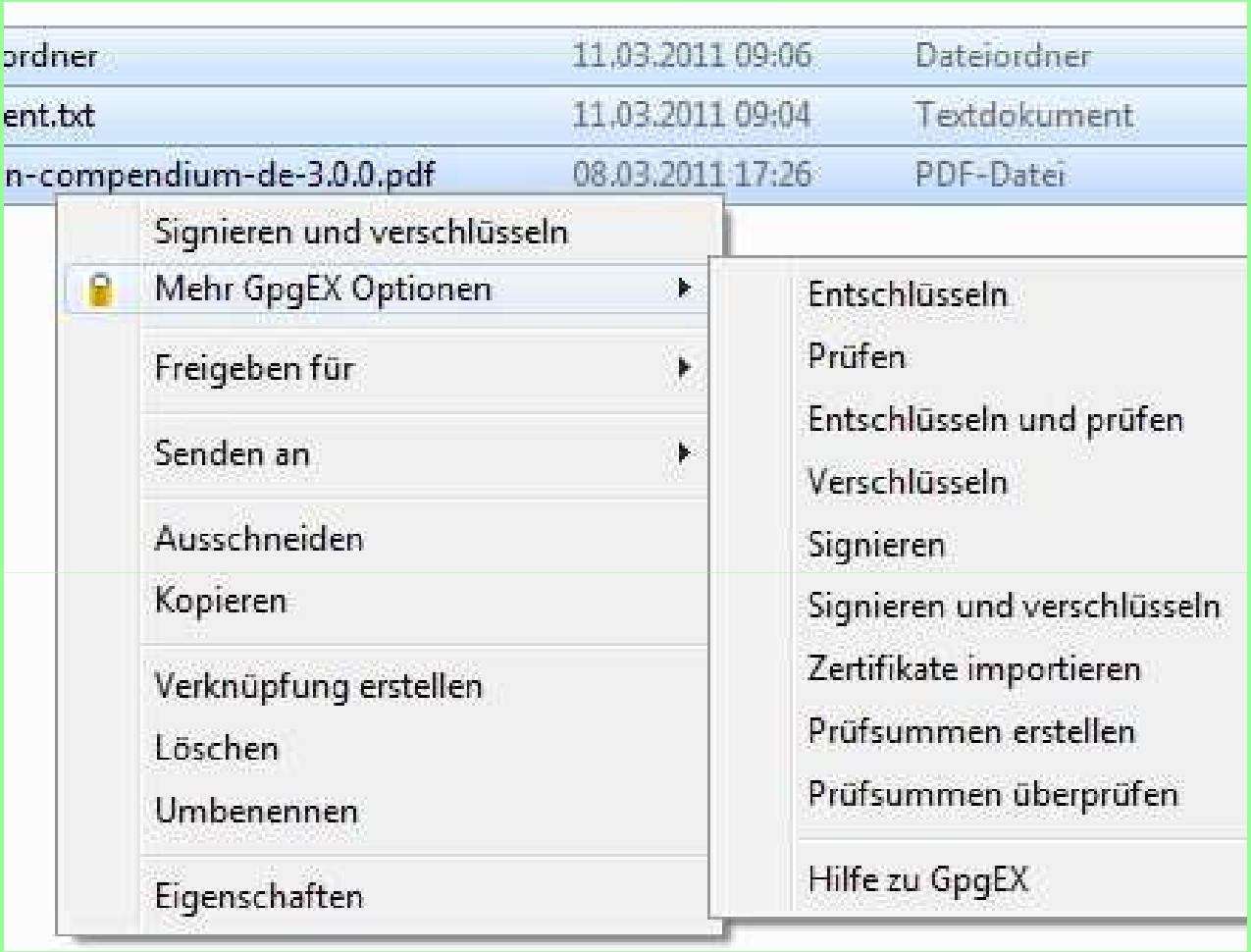
Weitere Detail-Infos:



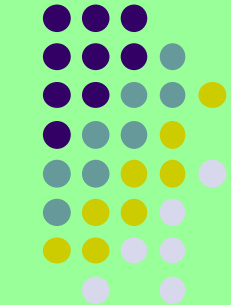
OpenPGP: Dateiverschlüsselung

Im Paket Gpg4win ist auch ein Tool zur Dateiverschlüsselung mitgeliefert.

Dieses Tool **GpgEX** integriert sich in den Windows Explorer und auch andere gute Dateimanager und läßt sich dadurch gut bedienen.

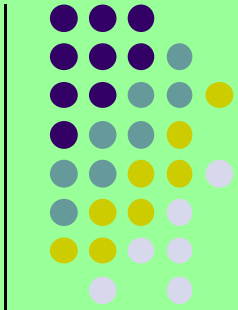


e-Mail Verschlüsselung



Quellennachweis:
Wikipedia
GBS (Group Business Software)
Bundesministerium für Wirtschaft und Technologie
g10 Code GmbH
Intevation GmbH
Enigmail
GnuPG
Mozilla
OpenSource
The Bletchley Park Trust Reports – The Turing Bombe" von Frank Carter, Januar 2000

e-Mail Verschlüsselung



Vielen Dank für Ihre Geduld.

Bitte stellen Sie jetzt Ihre Fragen