

Einführung in die eMail- Verschlüsselung

Jürgen Kunert
ITEE - Hamburg

Was haben wir vor?

- Motivation
- Wie funktioniert eMail-Versand?
- Wie funktioniert Verschlüsselung?
- Welche Verschlüsselungsverfahren gibt es?
- Vergleich der Verfahren
- S/MIME – wie geht es konkret?
 - Notes
 - Thunderbird
- PGP

Warum Verschlüsseln?

- „Wir“ möchten nicht, dass vertrauliche Daten (Angebote, Patente, Werbematerialien, Steuerinfos, Rechtsanwaltskommunikation, ...) in die falschen Hände geraten
- Die Anzahl der Angriffe nimmt zu
- Die Angriffe werden immer einfacher
- Es wird immer schwieriger, IT-Sicherheit zu beherrschen
- DSGVO
- (Jungen) Mitarbeitern ist die Bedeutung von vertraulichen Daten nicht mehr so bewusst wie früher

Was hätten wir gern?

- Einfachheit für Anwender und Administratoren
- Möglichst wenig Aufwand/Arbeit
- Vertraulichkeit:
nur der gewünschte Empfänger darf den Inhalt lesen
- Authentizität:
Sicherstellen der Identität von Sender und Empfänger
- Integrität:
keine Verfälschung von Inhalten
- Weitere Schutzziele

Was passiert beim eMail-Senden?

- Analogie zum Fahrradkurier
- Mail-Spezifikationen enthalten keine Sicherungsfunktionen
- Daten können mitgelesen werden
- Daten können gefälscht werden
- Ein falscher Absender kann vorgetäuscht werden
- Metadaten werden auf Vorrat gespeichert

Verschlüsselung

- **Verschlüsselung** nennt man den Vorgang, bei dem ein klar lesbarer Text (oder Bilder, Audio, Video) mit Hilfe eines Verschlüsselungsverfahrens in eine „unleserliche“, das heißt nicht einfach interpretierbare Zeichenfolge umgewandelt wird. (Wikipedia)
- Parameter der Verschlüsselung sind:
 - ein oder auch mehrere Schlüssel
 - der verwendete Algorithmus
 - Die Implementierung des Algorithmus inkl. Paramtern

Einfach?



Wie arbeitet Verschlüsselung?

- Mathematisches Verfahren, um die Quelldaten mittels einer Schlüssel-Zeichenkette in ohne Schlüssel unlesbare Zieldaten zu verwandeln
- Rücktransfer ist nur mit dem passenden Schlüssel möglich
- Es gibt Verfahren, die nach dem heutigen Stand der Technik absolut sicher sind

Symmetrische Verschlüsselung

- Verwendung eines einzelnen Schlüssels
- Vorteile:
 - Einfach
 - Verwendung für gemeinsam genutzte Dateien
- Nachteile:
 - Ein einfaches Passwort ist unsicher
 - Austausch muss organisiert werden
 - Schlüssel darf nicht in unbefugte Hände gelangen
 - Anzahl der Schlüssel bezogen auf die Anzahl der Teilnehmer wächst quadratisch

Asymmetrische Verschlüsselung

- Verwendung von Schlüsselpaaren (öffentlicher und privater Schlüssel)
- Vorteile:
 - Jeder hat nur ein Schlüsselpaar
 - Hohe Sicherheit
 - Kein Schlüsselverteilungsproblem
- Nachteile:
 - Mathematisch komplex
 - Rechenaufwändig (kann auch ein Vorteil sein!)

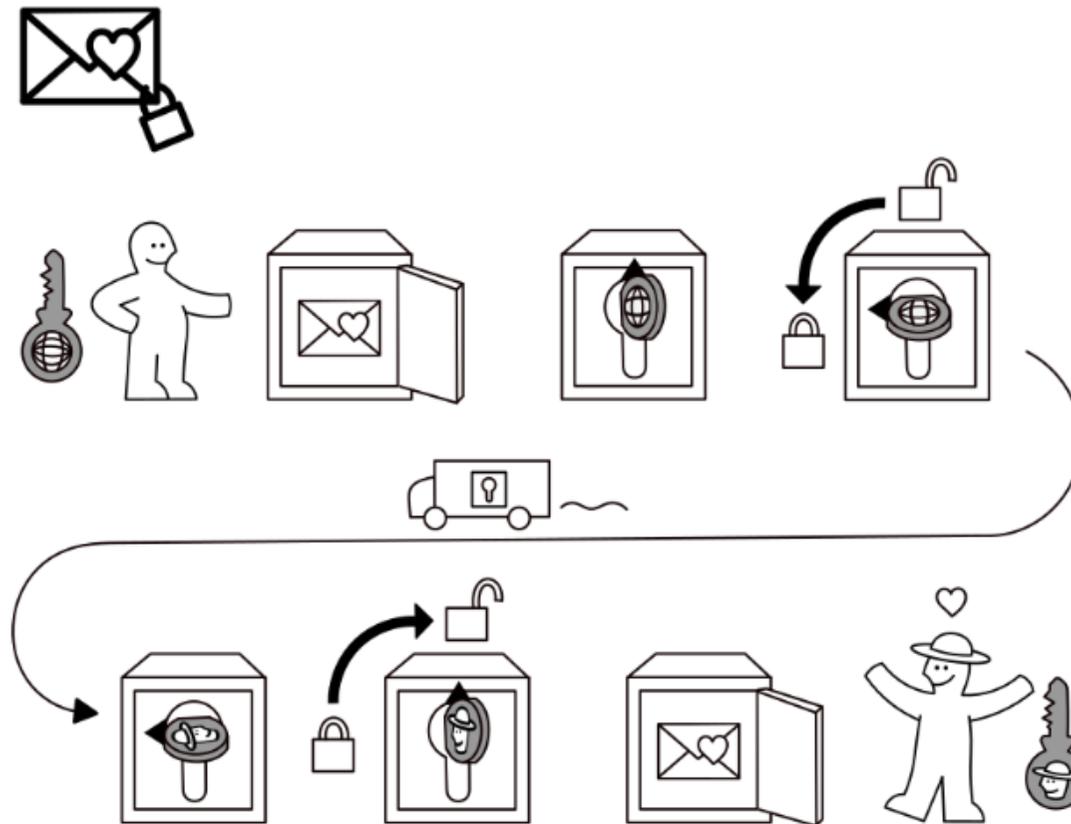
Asymmetrische Verschlüsselung: Vertrauen schaffen

Stimmt die Zuordnung eines Schlüssels zu einer Person (Authentizität)?

- Öffentliche Public-Key-Infrastruktur (PKI) (S/MIME, SSL)
Es gibt vertrauenswürdige(?) Zertifizierungsstellen, denen die Programme (Browser, eMail-Programme) vertrauen.
- Individuelle Public-Key-Infrastruktur (Notes/Domino, Eigene Zertifizierungsstelle)
- DE-Mail
- Direkter Schlüsselaustausch
- Web of Trust/Web des Vertrauens
Ein Schlüssel wird von einem oder vielen Benutzern als vertrauenswürdig anerkannt. Wenn der Schlüssel von einer Person meines Vertrauens beglaubigt wurde, dann kann ich dem auch vertrauen.
- Fingerprint (zur Verifikation des Schlüssels)

Public-Key-Infrastruktur

- Mit **Public-Key-Infrastruktur (PKI)** bezeichnet man in der Kryptologie ein System, das digitale Zertifikate ausstellen, verteilen und prüfen kann.

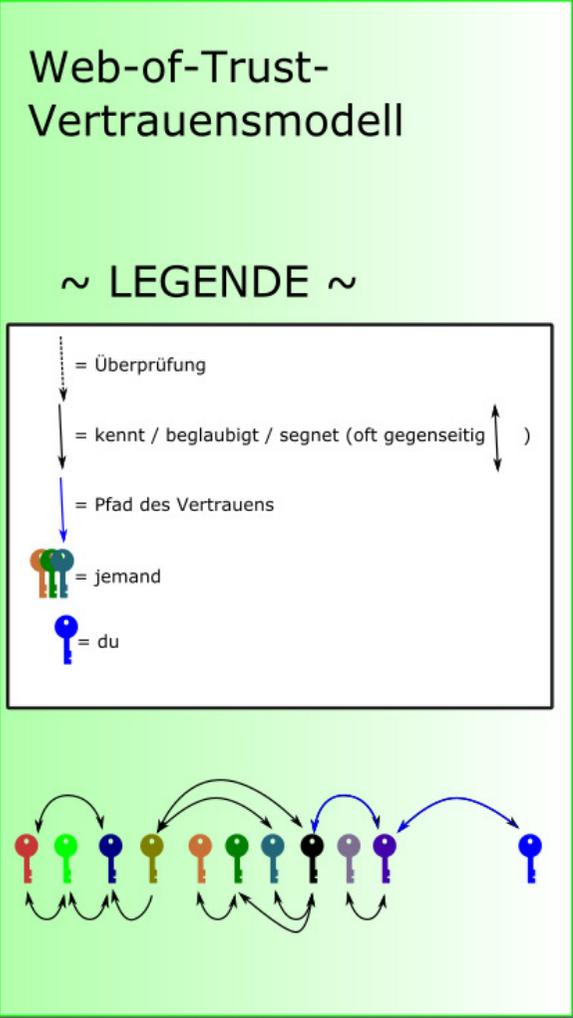
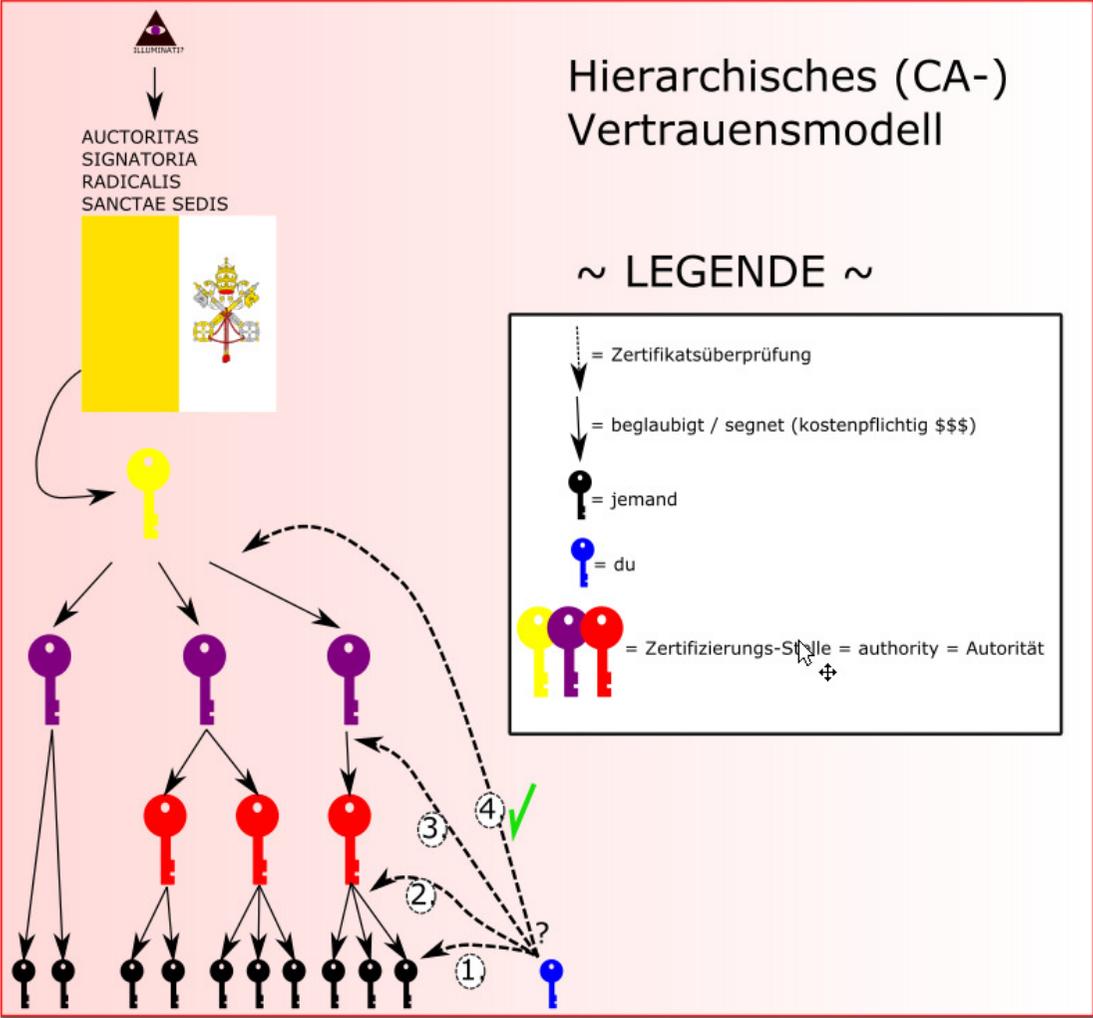


Quelle: <https://idea-instructions.com/>

PKI vs. Web of Trust

- Der wesentliche Unterschied zwischen S/MIME und PGP besteht im Vertrauensmodell: Worauf gründe ich mein Vertrauen in die Echtheit des öffentlichen Schlüssels eines Kommunikationspartners?
- Öffentliche Public-Key-Infrastruktur (PKI) (S/MIME, SSL)
Es gibt vertrauenswürdige Zertifizierungsstellen, denen die Programme (Browser, eMail-Programme) vertrauen.
- Web of Trust/Web des Vertrauens
Ein Schlüssel wird von einem oder vielen Benutzern als vertrauenswürdig anerkannt. Wenn der Schlüssel von einer Person meines Vertrauens beglaubigt wurde, dann kann ich dem auch vertrauen.
- PGP gibt dem technisch versierten Informatiker die vollständige Hoheit über sichere Verschlüsselung und ihn nicht von undurchsichtigen Zertifizierungsstellen abhängig macht. Dies hat zu der unglücklichen Entwicklung geführt, dass die Informatiker mit PGP eine für den Normalbürger schwieriger zu handhabende Technik verbreitet haben, anstatt auf die Propagierung vertrauenswürdiger und kostenloser Zertifizierungsstellen für S/MIME zu setzen.

PKI vs. Web of Trust



Copyright:
Pavel Blankocheck

Vertrauensmodell S/MIME

- S/MIME arbeitet grundsätzlich mit Zertifikaten nach dem X.509-Standard, wie sie auch bei SSL/TLS-gesicherten Webseiten eingesetzt werden (mit dem https-Protokoll). Ein Zertifikat umfasst im wesentlichen einen öffentlichen Schlüssel und eine Identitätsangabe des Schlüsselinhabers (im einfachsten Fall die E-Mail-Adresse, siehe Abb. 3). Durch Hinzufügung der digitalen Unterschrift einer Zertifizierungsstelle (certification authority, CA) wird das Ganze fälschungssicher gemacht. Für die Prüfung der Authentizität des Zertifikats ist daher die sichere Kenntnis des öffentlichen Schlüssels der Zertifizierungsstelle erforderlich; somit muss ein Zertifikat für die Zertifizierungsstelle vorliegen. Damit das Ganze nicht in einen Teufelskreis mündet, muss es Wurzel-Zertifizierungsstellen (root CAs) geben, die als a priori vertrauenswürdig – d.h. in jedem Fall korrekt arbeitend – postuliert werden. Deren sogenannte Stammzertifikate werden üblicherweise herstellerseitig in die Software eingebaut. Jede Zertifizierungsstelle ist demnach direkt oder indirekt von einer Wurzel-Zertifizierungsstelle zertifiziert, so dass sich insgesamt eine hierarchisch strukturierte Zertifizierungs-Infrastruktur (public-key infrastructure, PKI) ergibt. Zu beachten ist, dass ein gültiges, korrekt signiertes Zertifikat durchaus eine falsche Bindung Schlüssel \leftrightarrow Inhaber beinhalten kann, dass der Schlüssel also nicht echt ist – wenn nämlich der Aussteller des Zertifikats betrügerisch (oder technisch nachlässig) arbeitet. Daher kann ich mich letztlich nur dann auf ein Zertifikat verlassen, wenn ich allen Zertifizierungsstellen in der Kette bis zur Wurzel vertrauen kann.
- Quelle: <https://gi.de/informatiklexikon/sichere-e-mail-jetzt/>

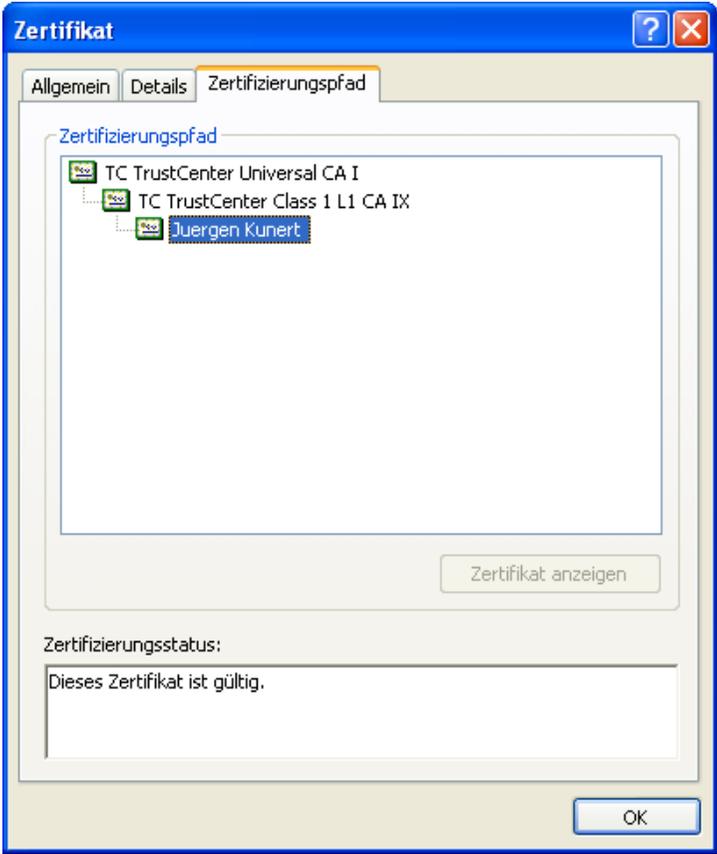
Vertrauensmodell PGP

- Sollte ich einer privatwirtschaftlich betriebenen Zertifizierungstelle vertrauen? Immerhin könnte man positiv argumentieren, dass eine solche Stelle „bei Strafe des Untergangs“ korrekt arbeiten muss. Sollte ich einer staatlich betriebenen Stelle vertrauen? Ist eine der Stellen vielleicht von der NSA unterwandert? Reale Vorfälle haben gezeigt, dass Skepsis angebracht ist [1]. Es gibt mannigfache Gründe, das Vertrauensmodell der hierarchischen PKI grundsätzlich abzulehnen und stattdessen auf persönliches Vertrauen zu setzen. PGP basiert auf einem Vertrauensmodell, das als Web of Trust (WoT) bezeichnet wird. Wenn ich vorsichtig bin, glaube ich an die Echtheit eines öffentlichen Schlüssels nur dann, wenn er mir von jemandem, dem ich in dieser Hinsicht vertraue, als sein Schlüssel „persönlich“ übergeben wurde (dafür gibt es verschiedene technische Varianten). Größere Flexibilität wird dadurch erreicht, dass globale Schlüsselverzeichnisse bereitgestellt werden und Zertifikate ähnlich wie bei einer PKI zum Einsatz kommen; diese werden aber nicht von Zertifizierungsstellen, sondern von individuellen Teilnehmern ausgestellt. Der Grad meines Vertrauens in ein solches Zertifikat hängt dann von zweierlei ab: Wie hoch ist mein Vertrauen in die Echtheit des öffentlichen Schlüssels des Signierenden? Wie hoch ist mein Vertrauen in die Rechtschaffenheit und Sorgfalt des Signierenden? Das WoT hat zudem noch weitere Probleme, weshalb PGP auch nicht gerade als Ideallösung gelten kann [5].
- Quelle: <https://gi.de/informatiklexikon/sichere-e-mail-jetzt/>

Zusammenhang zwischen Schlüssel und digitalem Zertifikat

- Ein **digitales Zertifikat** ist ein digitaler Datensatz, der bestimmte Eigenschaften von Personen oder Objekten bestätigt und dessen Authentizität und Integrität durch kryptografische Verfahren geprüft werden kann. Das digitale Zertifikat enthält insbesondere die zu seiner Prüfung erforderlichen Daten.
- Jedes digitale Zertifikat ist mit einem öffentlichen Schlüssel verknüpft, dem ein privater Schlüssel zugeordnet ist. Diesen privaten Schlüssel besitzt nur der Zertifikatsinhaber.
- Das Zertifikat, das den öffentlichen Schlüssel enthält, kann hingegen in einem Verzeichnis publiziert und so jedem zugänglich gemacht werden, der mit dem Inhaber eines Zertifikats sicher kommunizieren möchte.

Zusammenhang zwischen Schlüssel und digitalem Zertifikat



Transportverschlüsselung

- Verschlüsselung des Transportwegs – Metadaten werden nicht offen gelegt
- Keine Verschlüsselung der einzelnen Nachricht
- Der Enduser muss fast nichts tun
- StartTLS
- Die meisten eMail-Provider setzen Transportverschlüsselung ein
- <https://www.totemo.com/de/aktuelles/blog/transport-vs-inhaltsverschluesselung>
- Quelle: c't

E-Mail-Provider stellen auf Transportverschlüsselung um

30.03.2014 12:15 Uhr – Urs Mansmann

 vorlesen

Nach monatelanger Vorbereitung ist ab Montag bei den E-Mail-Diensten von Freenet, GMX, Web.de, und der Telekom der E-Mail-Empfang und -Versand nur noch verschlüsselt möglich.

Ab Montag wird es ernst: Die E-Mail-Provider, die sich in der Initiative [E-Mail made in Germany](#) zusammengeschlossen haben, lassen dann den Austausch von E-Mails nur noch mit eingeschalteter Transportverschlüsselung zu. Für den Abruf per POP3 oder IMAP und den

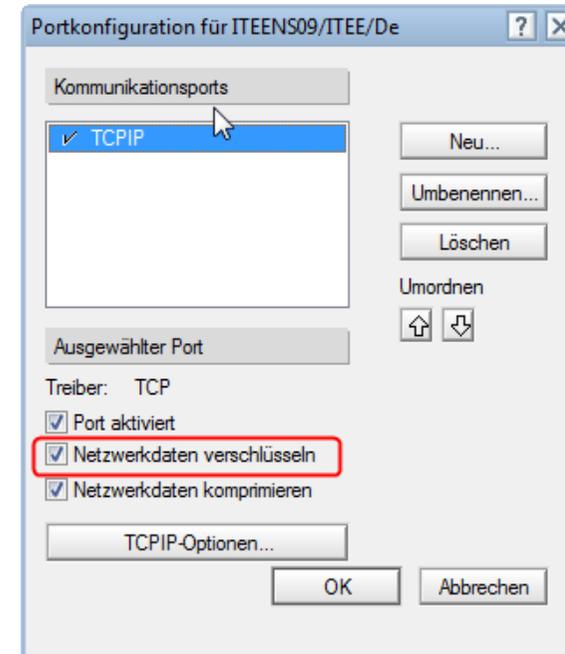
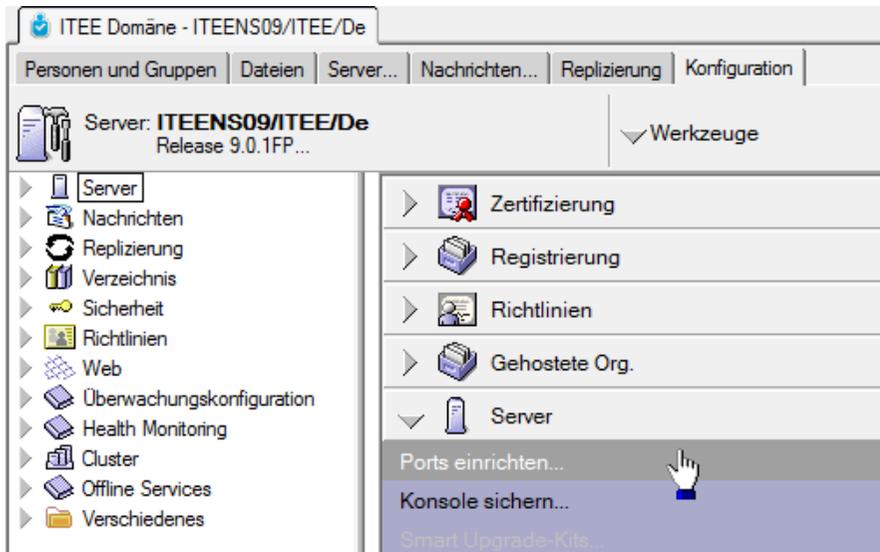
Transportverschlüsselung Ports (senden) 1

- Port 25: SMTP unverschlüsselt
- Port 465: SMTP mit SSL/TLS
- Port 587: SMTP mit STARTTLS
- Am Ende ist es völlig egal WELCHEN Port man nimmt. Es kommt immer SSL/TLS und SMTP zum Einsatz. Es wird historisch bedingt nur völlig durcheinander verwendet und vor allem bezeichnet. Wir geben verschiedene Ports an, auch weil Mailprogramme im Laufe der letzten 15 Jahre das unterschiedlich implementiert haben. Ein Uralt-Outlook kennt beispielsweise keinen Port 587 und wenn man dort SSL angibt, will es kramhaft Port 465 benutzen und/oder weigert sich, TLS auf Port 25 zu verwenden. Moderne Programme hingegen denken bei TLS sofort an die 25, ganz moderne denken sowieso an 587.
Es gibt keine "eine" Anleitung die alle Gepflogenheiten aus > 15 Jahren abdeckt. Jedes Programm macht, was es will.
"State of the Art" heute ist aus verschiedenen Gründen TLS auf 587.
Aber: Am Ende wirklich total egal.
- Quelle:
<https://userforum.mailbox.org/topic/dokumentation-zum-smtp-port-ist-uneindeutig>

Transportverschlüsselung Ports (senden) 2

- Unfortunately the downside of changing port numbers is that a number of email clients were made which only supported SSL/TLS over port 465 and not STARTTLS on 587. Clients are often very long lived, and so removing port 465 wasn't an option for many sites without annoying customers. Additionally, because port 465 was advertised as an option, many users with email clients that support both STARTTLS on 587 and SSL/TLS on 465 set them up to use 465 instead of 587. This makes it even harder to remove support for port 465, since lots of users have their email clients set up to use it.
- Currently, things seem relatively randomly split between people using SMTP SSL/TLS encrypted over port 465, and people using SMTP with STARTTLS upgrading over port 587.
- Quelle:
<https://www.fastmail.com/help/technical/ssltlsstarttls.html>

Transportverschlüsselung in Domino aktivieren - NRPC



Transportverschlüsselung in Domino aktivieren SMTP Inbound

1. Enable the "SMTP Listener task" via the Server document (Basics tab).
2. Enable SMTP Inbound "TCP/IP port status" in the Server document (Ports -> Internet Ports -> Mail tab).
3. Set the "SSL Port Status" to "Disabled" in the Server document (Ports -> Internet Ports -> Mail tab)
4. Enable "SSL negotiated over TCP/IP port" in the Configuration document (Router/SMTP -> Advanced -> Commands and Extensions tab).
5. Restart the SMTP Listener task.

Basics | Security | Client Upgrade | **Router/SMTP** | MIME | NOTES.INI Settings | ...

Basics | Restrictions and Controls... | Message Disclaimers | ... | **Advanced...**

Journaling | **Commands and Extensions** | Controls

Inbound SMTP Commands and Extensions		Outbound SMTP Commands and	
SIZE extension:	Enabled	SIZE extension:	Enabled
Pipelining extension:	Enabled	Pipelining extension:	Enabled
DSN extension:	Enabled	DSN extension:	Enabled
8 bit MIME extension:	Enabled	8 bit MIME extension:	Enabled
HELP command:	Disabled		
VERFY command:	Disabled		
EXPN command:	Disabled		
ETRN command:	Disabled		
SSL negotiated over TCP/IP port:	Enabled		

Transportverschlüsselung in Domino aktivieren SMTP Outbound 1

1. Set Negotiated SSL for the SMTP Outbound "TCP/IP port status" in the Server document (Ports -> Internet Ports -> Mail tab).
2. Set the "SSL Port Status" field to "Disabled".
3. Restart the Router task.

Web | Directory | Mail | DIIOP | Remote Debug Manager | Server Controller

Mail	Mail (IMAP)	Mail (POP)	Mail (SMTP Inbound)	Mail (SMTP Outbound)
TCP/IP port number:	143	110	25	25
TCP/IP port status:	Enabled	Enabled	Enabled	Negotiated SSL
Enforce server access settings:	Yes	Yes	No	N/A

Sample of what you see in a debug outfile with SMTPDebugIO enabled:

[06D8:0008-0324] R: STARTTLS

03/18/2003 04:05:56.74 PM [06D8:0008-0324] SMTP CITask StateMachine> Sent 24 bytes to 129.42.208.182

[06D8:0008-0324] S: 220 Ready to start TLS<CRLF>

<http://www-01.ibm.com/support/docview.wss?uid=swg21108352>

Inhaltsverschlüsselung

- Ende-zu-Ende-Verschlüsselung des Inhalts einer Nachricht
- Wir brauchen Schlüssel
- Wir brauchen Programme/Programmerweiterungen
- Metadaten (Betreff, Absender, Empfänger, Zeitpunkt) werden **nicht** verschlüsselt!

Inhaltsverschlüsselung – Alternativen (zu S/MIME)

- PGP
- Inhalt in verschlüsseltes PDF oder ZIP einpacken
- Eigenes Gateway zur Mail-Verschlüsselung (mit Schlüsselmanagement) (z.B. IQ-Suite oder CIPHERmail)
- DE-Mail
- Verschlüsselung über externen Dienstleister/Cloud – Webmail
- Steganografie
- Programm-eigene Verschlüsselungsmethoden (Notes Native Encryption, ...)

PGP

- steht für Pretty Good Privacy
- wurde von Phil Zimmermann entwickelt um allen Personen die Möglichkeit zu geben, ihre Privatsphäre zu schützen
- Ebenso wie S/MIME Internet-Standard
- Plug-Ins/Zusatzprogramme für den Mail-Client nötig
- Mindestens genauso sicher wie S/MIME, aber anders

PGP

- Web of Trust/Web des Vertrauens statt hierarchischen Zertifikaten
- Enigmail-Plugin für Thunderbird und Outlook
- Extra zu installieren
- Der User muss sich um die Schlüsselverwaltung kümmern
- Ein Schlüssel kann für mehrere eMail-Adressen verwendet werden (Im Gegensatz zu S/MIME)

De-Mail

- Nur Nutzer mit einer überprüften Identität können De-Mails versenden und empfangen. Denn jeder Nutzer muss sich vor Eröffnung seines De-Mail-Kontos, das nur von ihm genutzt werden kann, bei dem Anbieter seiner Wahl ausweisen. Bei De-Mail kann sich daher niemand hinter einer falschen Identität verstecken.
- De-Mail bietet eine gesetzlich abgesicherte Zustellung: Versand, Empfang und Inhalte von De-Mails können rechtswirksam nachgewiesen werden.
- Kommunikation mit Behörden
- De-Mails sind auf dem Transportweg immer verschlüsselt
- De-Mails werden verschlüsselt abgelegt
- Neben der Standard-Transportverschlüsselung können De-Mails optional auch Ende-zu-Ende-verschlüsselt werden. Diese Möglichkeit, besonders vertrauliche Dokumente zusätzlich zu schützen, wurde von den De-Mail-Anbietern so handhabbar gestaltet, dass sie seitdem auch von weniger versierten Anwendern genutzt werden kann.
- Bisher wenig akzeptiert
- Ist per Gesetz sicher!

De-Mail (Eigenwerbung)

- **Rechtssicher**
Rechtssicherheit auf der Basis des De-Mail Gesetzes
- **Verbindlich**
Nur eindeutig identifizierte Kommunikations-Partner
- **Nachweisbar**
Optionale Versand-/ Empfangsbestätigung Ihrer De-Mails
- **Technologisch sicher (per Gesetz)**
Ausschließlich deutsche Server & effektive Verschlüsselung
- **Ablösung des Faxes/Schriftform**

De-Mail

- <https://www.heise.de/thema/De-Mail>
- Zu Beginn gab es keine Ende-zu-Ende-Verschlüsselung
[https://www.heise.de/newsticker/meldung/30C3-E-Mail-
Unsicherheit-made-in-Germany-2072758.html](https://www.heise.de/newsticker/meldung/30C3-E-Mail-Unsicherheit-made-in-Germany-2072758.html)
(2013)

Verschlüsselungs-Gateway

- Eingebunden in der DMZ des Unternehmens zwischen Mailserver und Internet-Mail-Ein- und -Ausgang
- Die User merken nichts/wenig davon
- Benutzung des normalen Mailprogramms
- Automatische Schlüsselerzeugung und –Management sind möglich
- finanzieller Aufwand, extra Software und Hardware

CipherMail Email Encryption Gateway

- 3 Varianten, die sich in den Softwarekosten bzw. den Supportleistungen unterscheiden:
 - Update service
 - Remote monitoring
 - PDF cover page
 - Configurable portal logo
 - Certificate signing request (CSR) module
 - Webmail Messenger
 - Hardware Security Module (HSM) support
 - Remote CA connectors
 - Additional SMS providers
 - LDAP mail flow rules
 - Packages for RedHat/CentOS & Ubuntu
 - SAAS allowed
 - Company specific modifications supported
 - External database support (MySQL/MariaDB, Oracle)
 - HA clustering (Galera, Oracle)

S/MIME-Verschlüsselung im Client-Programm mit Bordmitteln

- Was brauche ich?
- Wie richte ich meinen Client ein?
- Was braucht die Gegenseite?
- Signierte und verschlüsselte Mails austauschen
 - Signierte Mail empfangen
 - Signierte Mail senden
 - Verschlüsselte Mail empfangen
 - Verschlüsselte Mail senden

Was brauche ich?

- Mein Schlüsselpaar (privater und öffentlicher Schlüssel)
- <meinSchlüssel>.p12
- Den öffentlichen Schlüssel des Empfängers
- Die richtigen Einstellungen am Client-Programm
- Die Einstellung zum Signieren bzw. Verschlüsseln

Woher bekomme ich mein S/MIME-Zertifikat? 1

- Suche nach „(kostenlose) smime zertifikate“

https://praxistipps.chip.de/koster

Kostenlose S/MIME-Zertifikate – Anbieter 3: comodo

- Laufzeit: Dieses kostenlose Zertifikat läuft ebenfalls für ein Jahr.
- Schutz: Neben dem Versand der E-Mails und den Anhängen wird hier ebenfalls die E-Mail-Signatur verschlüsselt.
- Sprache: Der Bestellprozess ist komplett auf Englisch.
- Fazit: Rundum sorglos-Paket mit einem Jahr Laufzeit - **Zum Angebot.**

COMODO
Creating Trust Online®

PERSONAL | SSL CERTIFICATES

Free Secure Email Certificate

Email Certificate (S/MIME) protect by encrypting & digitally signing.

★★★★★
4.8 / 5 of 4 Reviews

Free Email Certificate

Sign Up Now

Please use Mozilla® Firefox® or Microsoft® Internet Explorer® 8+ to collect your certificate.
Email Certificates cannot be collected using Google® Chrome® or Microsoft Edge.

Woher bekomme ich mein S/MIME-Zertifikat? 2

- Auf der comodo-Seite:

The screenshot shows the Comodo website's application page for a Secure Email Certificate. The browser address bar shows the URL: <https://secure.comodo.com/products/frontpage?area=SecureEmailCertificate¤cy=EUR®ion=Europ>. The page header includes the Comodo logo and contact information: "Order Online or Call Us: US + (888) 266-6361, INTL + (703) 581-6361".

The main content area is titled "Application for Secure Email Certificate" and is divided into several sections:

- Your Details:** Includes input fields for First Name (Ignatz), Last Name (Schlehenbrenner), Email Address (is2354@gmx.de), and a Country dropdown menu (Germany).
- Private Key Options:** Includes a Key Size (bits) dropdown menu (Hochgradig).
- Note:** A red warning states: "Note: Backup your private key! We do not get a copy of your private key at any time so, after completing this application procedure, we strongly advise you create a backup. Your certificate is useless without it. [More info](#)".
- Revocation Password:** Includes a text input field for the password and a checkbox for "Comodo Newsletter" (Opt in?).
- Subscriber Agreement:** Includes a text input field for the agreement.

On the right side, there is a sidebar titled "Secure Email Certificates" with two steps: "Step 1: Provide details for your certificate" and "Step 2: Collect and install your certificate".

Woher bekomme ich mein S/MIME-Zertifikat? 3

- Dann kommt eine eMail:

Betreff: Your certificate is ready for collection!

Datum: Sat, 09 Jun 2018 12:03:14 +0000

Von: Certificate Customer Services <secureemail@comodogroup.com>

An: Ignatz Schlehenbrenner <is2354@gmx.de>

Dear Ignatz Schlehenbrenner,

Congratulations - your free Secure Email Certificate is now ready for collection! You are now just a few minutes away from being able to secure your email!

Your Collection Password is: 123456verystrongpasswordbutonlyfake

1. Open this webpage: https://secure.comodo.com/products/!SecureEmailCertificate_Collec2
2. Enter your email address, is2354@gmx.de,
where requested on the webpage.
3. Copy and paste your Collection Password where requested on the webpage.
4. Click the Submit button.

Your free Secure Email Certificate will then be installed. Please visit www.comodogroup.com/support for guidance on configuring your email client to use your certificate to secure email.

NOTE: We strongly recommend that you export your certificate to a safe place in case you need to reload it later. For details, please see http://www.instantssl.com/ssl-certificate-support/server_faq/ssl-email-certificate-faq.html

If you need to revoke your Comodo FREE Personal Secure Email Certificate then

Woher bekomme ich mein S/MIME-Zertifikat? 4

- Jetzt wird das Zertifikat installiert (Im Firefox-Zertifikatsspeicher):

The screenshot shows a web browser window with the address bar displaying "Comodo CA Ltd (GB)" and the URL "https://secure.comodo.com/products/!SecureEmailCertificate_Collec2". The page content includes the Comodo logo and "Certification Authority" text. A main heading reads "Collection of Secure Email Certificate" with a sub-heading "Attempting to collect and install your Free Certificate...". A sidebar titled "Secure Email Certificates" contains two steps: "Step 1: Provide details for your certificate" (marked with a red checkmark) and "Step 2: Collect and install your certificate" (marked with a red arrow). The footer contains the text "© Copyright 2018. All rights reserved." and "Saturday June 9, 2018".

Woher bekomme ich mein S/MIME-Zertifikat? 4a

Die CA führt den kompletten Vorgang auf einer Webseite aus: die Generierung des privaten Schlüssel inklusive Sicherung mit einer Passphrase, die Generierung des Certification Request (CSR), die Signierung des CSR und die Erstellung der Zertifikatsdatei mit privatem und öffentlichem Schlüssel.

Die CAs versprechen, dass der private Schlüssel im Browser des Nutzers generiert wird und nicht auf den Server der CA hochgeladen wird. Es ist aber für die CA möglich, den privaten Schlüssel unbemerkt zu kompromittieren.

Woher bekomme ich mein S/MIME-Zertifikat? 4b



1. Generieren eines passwortgeschützten privaten Schlüssels in der Datei "*mein.key*":
> openssl genrsa -out mein.key -des3 4096
2. Generieren eines Certification Request (CSR) in der Datei "*mein.csr*", die folgenden Daten werden dabei abgefragt:
> openssl req -new -key mein.key -out mein.csr
Enter pass phrase for mein.key:
....
Country Name (2 letter code) [AU]: **DE**
State or Province Name (full name) []: **Berlin**
Locality Name (eg, city) []: **Berlin**
Organization Name (eg, company) []: **privat**
Organizational Unit Name (eg, section) []:
Common Name (eg, YOUR name) []: **Max Musterman**
Email Address []: **max@musterman.de**
3. Den CSR übergibt man der CA. Die Datei enthält nur den öffentlichen Schlüssel.
Die CA signiert diesen CSR und man erhält ein signiertes Zertifikat als Datei "*mein.crt*" via E-Mail oder als Download.
4. Das Zertifikat "*mein.crt*" kann man an alle Kommunikationspartner verteilen.
5. Für den Import im eigenen E-Mail Client fügt man privaten Schlüssel und signiertes Zertifikat zu einer PKCS12-Datei "*mein.p12*" zusammen.
> openssl pkcs12 -export -in mein.crt -inkey mein.key -out mein.p12
Diese passwortgeschützte Datei kann in allen E-Mail Clients importiert werden und sollte sicher verwahrt werden.

Woher bekomme ich mein S/MIME-Zertifikat? 5

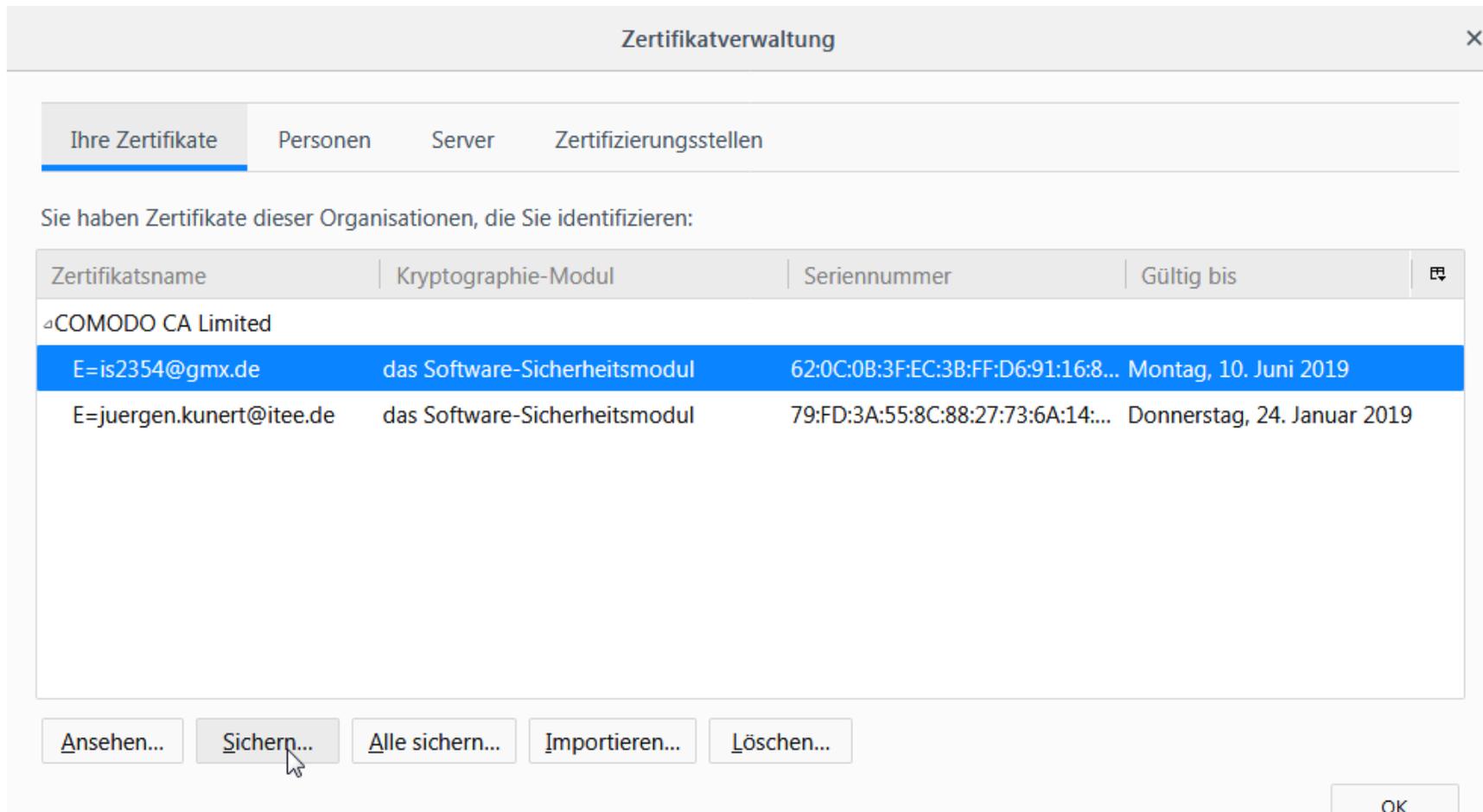
- Wo finde ich das Zertifikat?
- Im Zertifikatsspeicher
- Firefox: Einstellungen -> Datenschutz und Sicherheit -> Zertifikate

The screenshot shows the Firefox 'Zertifikatverwaltung' (Certificate Manager) window. The address bar shows 'Firefox about:preferences#privacy' and a search bar with 'kostenlose s/mime z'. The left sidebar contains navigation options: 'Allgemein', 'Suche', 'Datenschutz & Sicherheit', and 'Firefox-Konto'. The main content area is titled 'Zertifikatverwaltung' and has tabs for 'Ihre Zertifikate', 'Personen', 'Server', and 'Zertifizierungsstellen'. Below the tabs, it states 'Sie haben Zertifikate dieser Organisationen, die Sie identifizieren:'. A table lists certificates from 'COMODO CA Limited'.

Zertifikatsname	Kryptographie-Modul	Seriennummer	Gültig bis	
COMODO CA Limited				
E=is2354@gmx.de	das Software-Sicherheitsmodul	62:0C:0B:3F:EC:3B:FF:D6:91:16:8...	Montag, 10. Juni 2019	
E=juergen.kunert@itee.de	das Software-Sicherheitsmodul	79:FD:3A:55:8C:88:27:73:6A:14:...	Donnerstag, 24. Januar 2019	

Woher bekomme ich mein S/MIME-Zertifikat? 6

- Zertifikat exportieren:



Zertifikatverwaltung

Ihre Zertifikate | Personen | Server | Zertifizierungsstellen

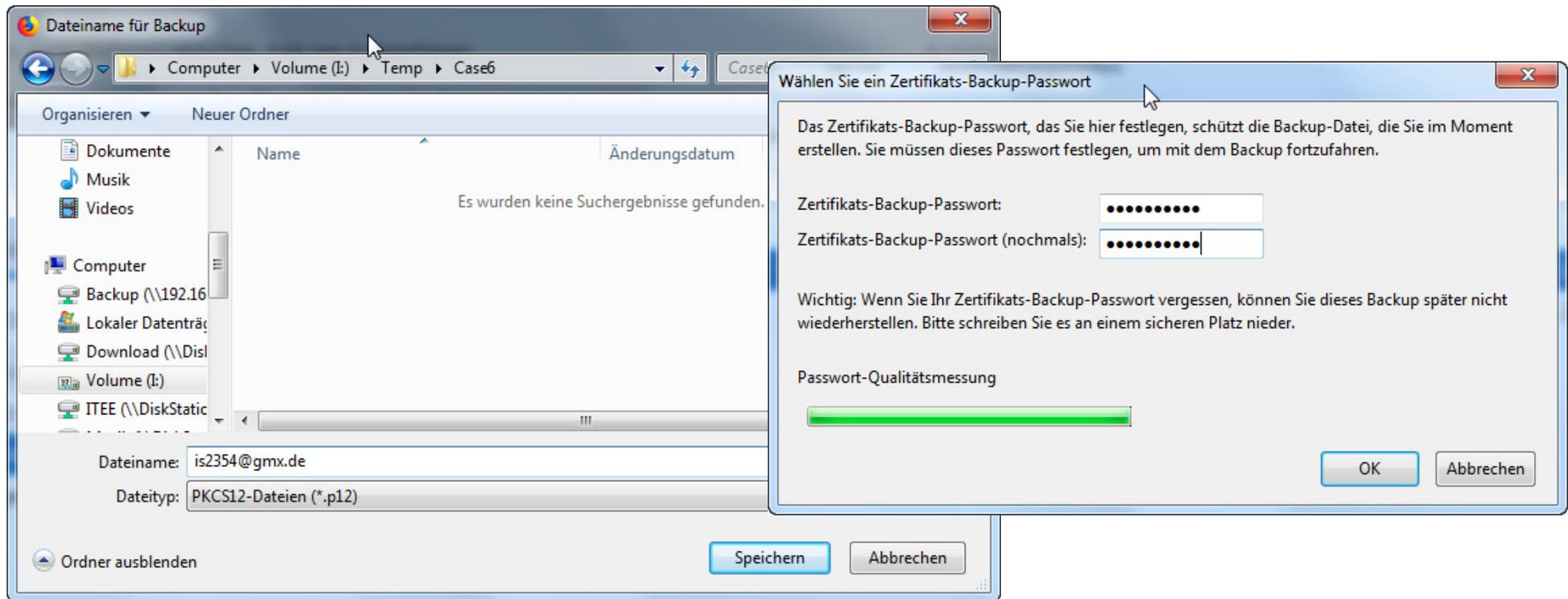
Sie haben Zertifikate dieser Organisationen, die Sie identifizieren:

Zertifikatsname	Kryptographie-Modul	Seriennummer	Gültig bis
COMODO CA Limited			
E=is2354@gmx.de	das Software-Sicherheitsmodul	62:0C:0B:3F:EC:3B:FF:D6:91:16:8...	Montag, 10. Juni 2019
E=juergen.kunert@itee.de	das Software-Sicherheitsmodul	79:FD:3A:55:8C:88:27:73:6A:14:...	Donnerstag, 24. Januar 2019

Ansehen... | Sichern... | Alle sichern... | Importieren... | Löschen... | OK

Woher bekomme ich mein S/MIME-Zertifikat? 7

- Zertifikat exportieren:



Woher bekomme ich mein S/MIME-Zertifikat? 9

Zertifikat in Datei:

 is2354@gmx.de.p12	09.06.2018 14:30	Privater Informati...	7 KB
---	------------------	-----------------------	------

Ein einmal kompromittierter Schlüssel ist **nicht mehr sicher!**

- Sichern vor unberechtigtem Zugriff!

Wenn der Schlüssel weg ist, kann nicht mehr entschlüsselt werden!

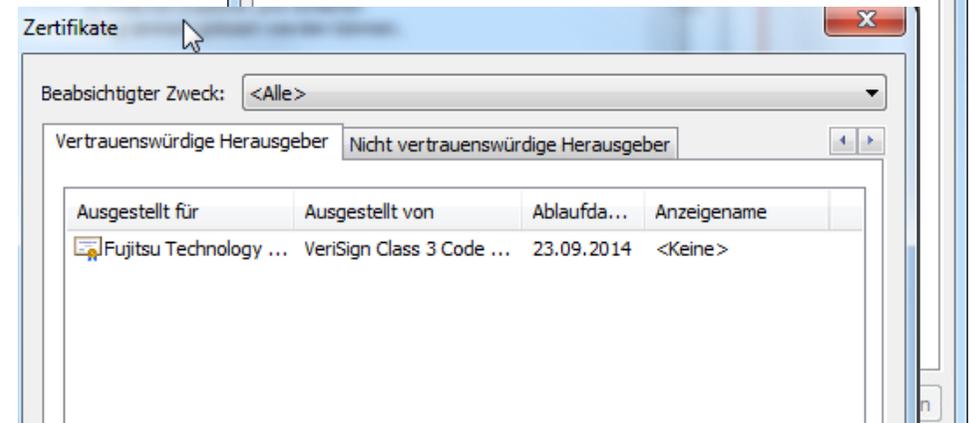
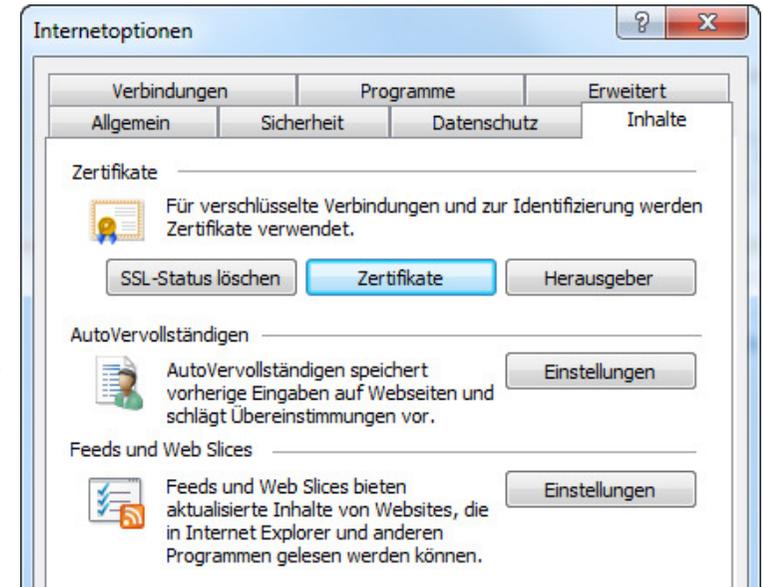
- Backup!

Woher bekomme ich mein S/MIME-Zertifikat? 8

- Genauso wie hier mit einem kostenlosen Zertifikat funktioniert es mit käuflichen Zertifikaten
- Verschlüsselungs-Gateways können die Schlüsselerzeugung und den Austausch automatisieren
- Der Domino-CA-Prozess kann S/MIME-Zertifikate erstellen, die jedoch nicht von einer vertrauenswürdigen Zertifizierungsstelle signiert sind.
- Es wird erwartet, dass Letsencrypt S/MIME-Zertifikate herausgibt

Wo werden Zertifikate gespeichert?

- Notes & Domino: Adressbücher (fremde Zertifikate)
- Notes: ID-File (eigenes Zertifikat)
- Firefox: intern -> Einstellungen -> Datenschutz und Sicherheit -> Zertifikate
- Chrome: intern -> Einstellungen -> Datenschutz und Sicherheit -> Zertifikate
- Edge: Windows-Zertifikatsspeicher
- Safari: Mac OS Schlüsselbund
- Windows 10: „Computerzertifikate verwalten“
- Windows 7: Internet Explorer/Internetoptionen/Inhalte/Zertifikate
- Mac OSX: Schlüsselbund
- Android: eigener Zertifikatsspeicher
- iOS: eigener Zertifikatsspeicher
- Outlook: Outlook und Windows
- Thunderbird: eigener Zertifikatsspeicher

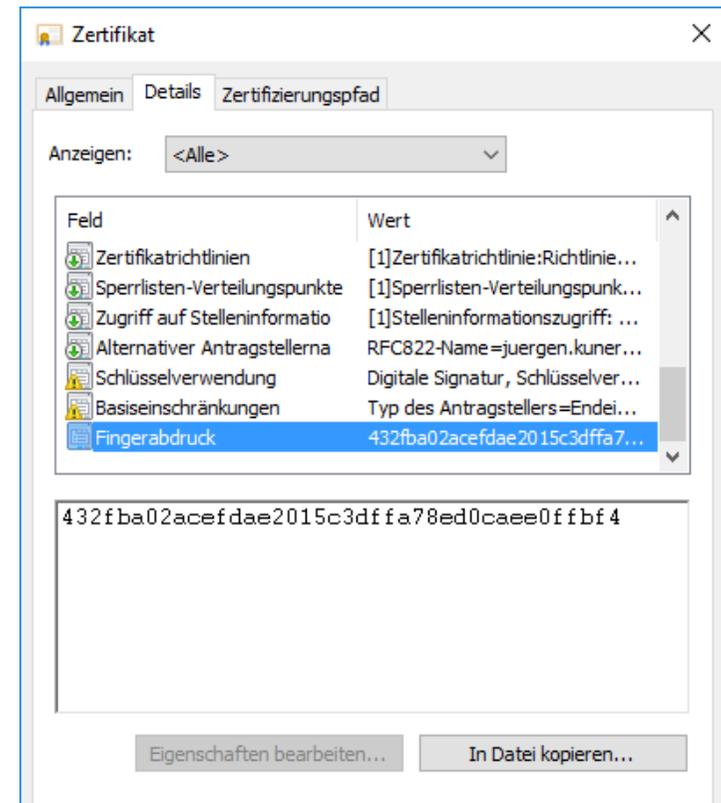
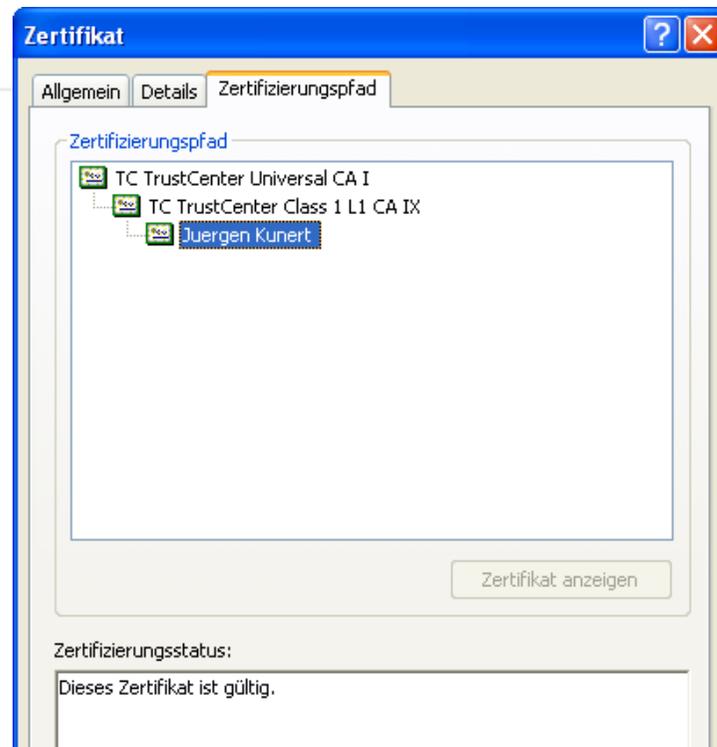


Wie prüfe ich die Validität eines Zertifikats?

- Der Browser oder das eMail-Programm machen das für mich 😊
- Fingerabdruck/Fingerprint

Programme (1)

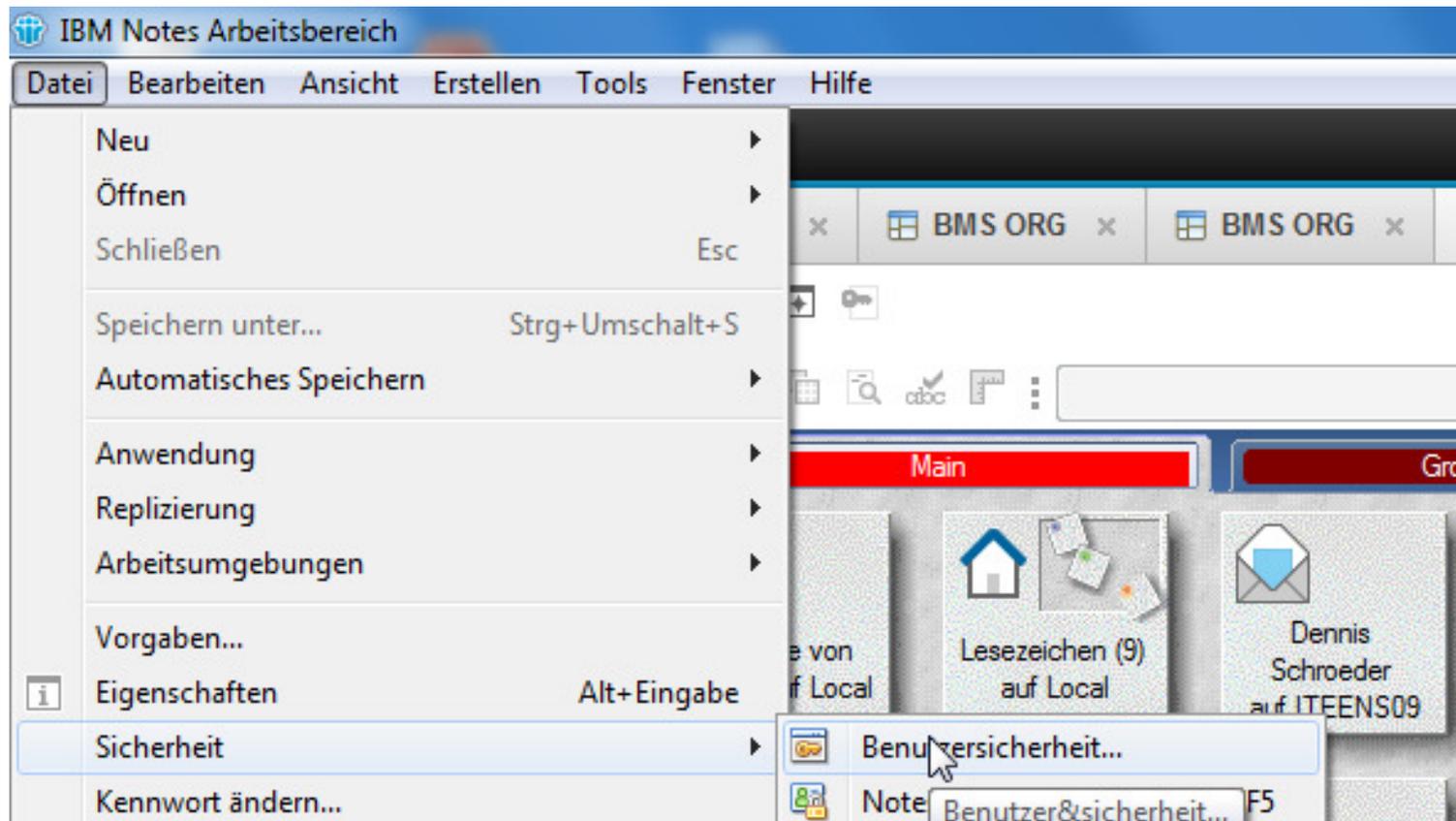
 certmgr.msc



S/MIME-Verschlüsselung im Client-Programm mit Bordmitteln

- Was brauche ich?
- **Wie richte ich meinen Notes-Client ein?**
- Was braucht die Gegenseite?
- Signierte und verschlüsselte Mails austauschen
 - Signierte Mail empfangen
 - Signierte Mail senden
 - Verschlüsselte Mail empfangen
 - Verschlüsselte Mail senden

Wie installiere ich ein S/MIME-Zertifikat in Notes? 1



Wie installiere ich ein S/MIME-Zertifikat in Notes? 2

Benutzersicherheit

Zertifikate in Ihrer ID-Datei

Ihre Zertifikate identifizieren Sie sicher gegenüber Notes und anderen Programmen. Ihre ID kann sowohl Zertifikate zur sicheren Kommunikation in Notes als auch Zertifikate für das Internet enthalten.

Ihre Notes-Zertifikate Zur Anmeldung in Notes, zum Zugriff auf Notes-Datenbanken und zum Austausch sicherer Mails mit anderen Notes-Benutzern.

Typ	Ausgestellt auf	Ausgestellt von
	Juergen Kunert/ITEE/De	/ITEE/De
	Juergen Kunert/ITEE/De	/ITEE/De

Zertifikate abrufen...

- Notes-Zertifikate importieren (in ID aufnehmen)...
- Neues nicht hierarchisches Notes-Zertifikat anfordern...
- Internetzertifikate importieren...**
- Neues Internetzertifikat anfordern...
- Internetzertifikat von einer Smartcard importieren...

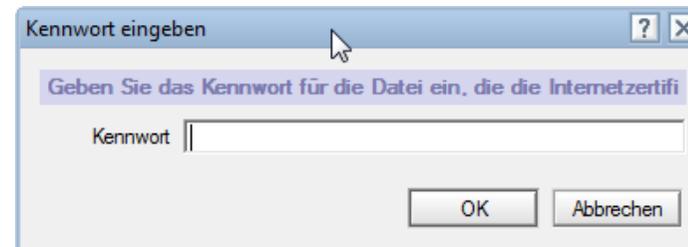
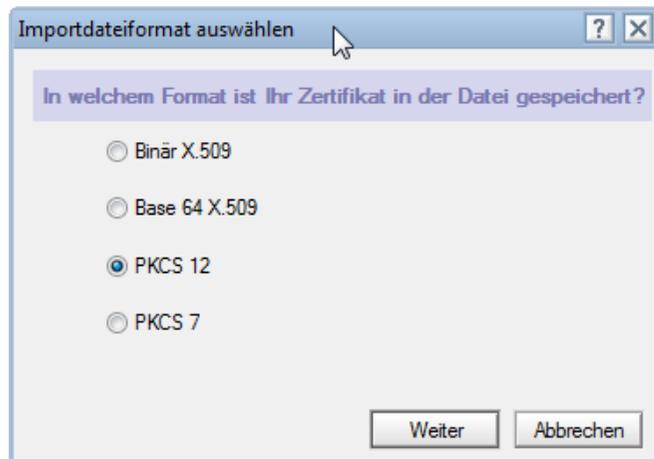
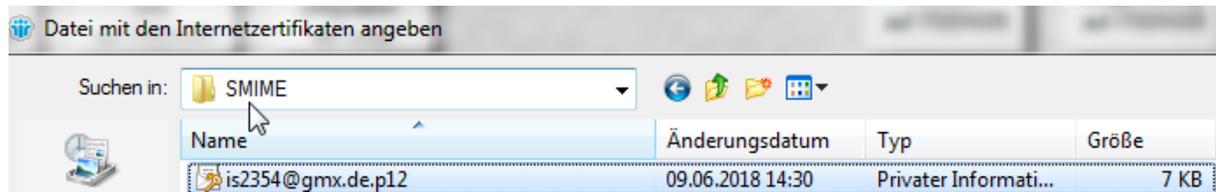
Ausgewähltes Element

Ausgestellt auf: Juergen Kunert/ITEE/De
 Ausgestellt von: /ITEE/De
 Aktiviert: 25.04.2018 Typ: Notes - Internationale Verschlüsselung
 Ablaufdatum: 26.04.2020 Schlüsselbezeichner: 17N9F QWXQ6 JDEU7 K81S5 61WX2 F84D7

[Erweiterte Details...](#)

OK Schließen

Wie installiere ich ein S/MIME-Zertifikat in Notes? 3



Wie installiere ich ein S/MIME-Zertifikat in Notes? 4

The screenshot shows the 'Benutzersicherheit' (User Security) control panel window. The left sidebar is expanded to 'Ihre Zertifikate' (Your Certificates). The main area is titled 'Zertifikate in Ihrer ID-Datei' (Certificates in your ID file). Below this, there is a section for 'Ihre Internetzertifikate' (Your Internet certificates) with a dropdown menu and a text box explaining their use for secure mail and web connections. A table lists certificates, with one selected: 'juergen.kunert@itee.de' issued by 'COMODO RSA Client Authentication and Secure Em'. Below the table, the 'Ausgewähltes Element' (Selected element) section shows details for the selected certificate, including the issuer, activation date, and digest. A red box highlights the 'Erweiterte Details...' (Advanced details...) button. A second window, 'Zertifikate - Erweiterte Details' (Certificates - Advanced details), is open, showing options to use the certificate as a standard signing certificate and a table of certificate information attributes.

Zertifikate in Ihrer ID-Datei

Ihre Zertifikate identifizieren Sie sicher gegenüber Notes und anderen Programmen. Ihre ID kann sowohl Zertifikate zur sicheren Kommunikation in Notes als auch Zertifikate für das Internet enthalten.

Ihre Internetzertifikate

Zum Austausch sicherer Mails mit Nicht-Notes-Benutzern, zum Zugriff auf sichere Webseiten mit dem Notes-Browser oder für sichere Verbindungen zu Internetservices (mit SSL).

Typ	Ausgestellt auf	Ausgestellt von
	juergen.kunert@itee.de	COMODO RSA Client Authentication and Secure Em

Ausgewähltes Element

Ausgestellt auf: juergen.kunert@itee.de (E-Mail)

Ausgestellt von: COMODO RSA Client Authentication and Secure Em (E-Mail)

Aktiviert: 23.01.2018 Typ: Internet - Mehrzweck

Ablaufdatum: 24.01.2019 Digest: 7068 F084 4CB3 8CBD CD01 D597 C70C D226

Zertifikate - Erweiterte Details

Sie können die bevorzugte Nutzung dieses Zertifikats festlegen. Internetprotokolle, die Zertifikate verwenden, beachten, falls möglich, Ihre Vorgabe. Diese Auswahl beeinflusst, welche Vorgabeoptionen verfügbar sind.

Dieses Zertifikat als Standardsignierzertifikat verwenden

Zertifikatsinformationen: Wählen Sie ein Attribut, um die zugehörigen Details anzuzeigen

Attribut	Wert
Ausgestellt auf	EMAIL=juergen.kunert@itee.de
Ausgestellt von	CN=COMODO RSA Client Authentication and Secure Email CA/O=COMODO
MD5-Digest	7068 F084 4CB3 8CBD CD01 D597 C70C D226
SHA1-Digest	432F BA02 ACEF DAE2 015C 3DF A78E D0CA EE0F FBF4
SHA1-Schlüsselbezeichner	278F 3554 8EEF C99D 8A56 03ED A9C1 EC2F 79DF 5240
Seriennummer	79FD 3A55 8C88 2773 6A14 618A 4AD8 07FB
EMAIL=	juergen.kunert@itee.de

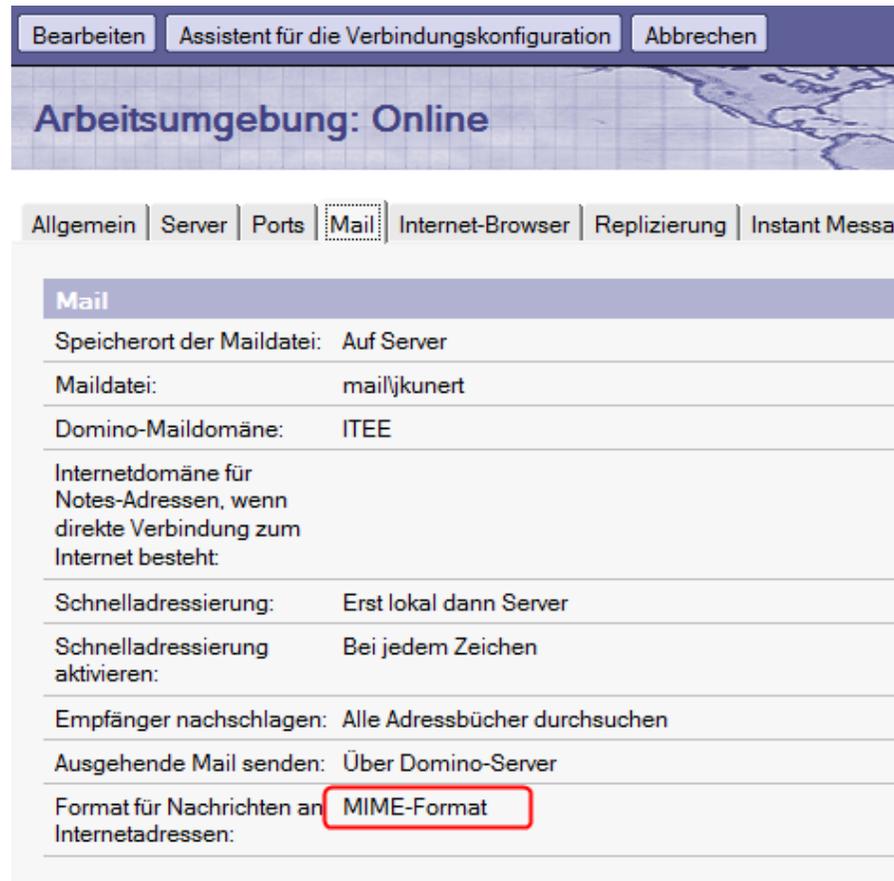
Dirk Nowitzki
auf ITEENS05

Was kann ich jetzt damit machen?

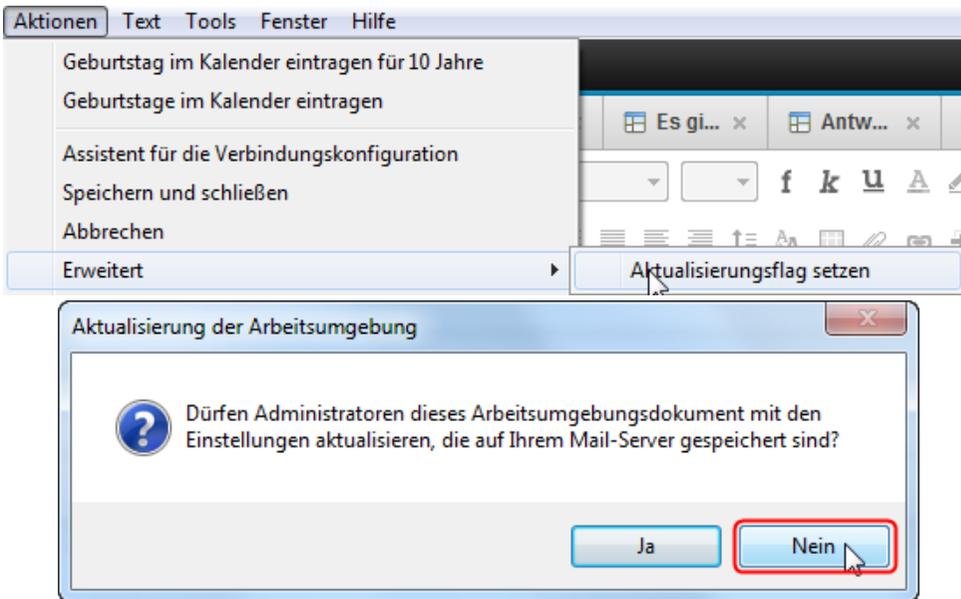
- Ich kann verschlüsselte eMails empfangen
- Ich kann signierte eMails senden – und meinen öffentlichen Schlüssel

Notes-Konfiguration Arbeitsumgebung

- Ohne MIME geht es nicht und es kommen auch keine Fehlermeldungen!
- Achtung:
Ggf. Kollision mit anderen Zusatzprogrammen (Signatur, ...)



Seite 30



Was kann ich jetzt damit machen?

- Ich kann signierte eMails senden
- und meinen öffentlichen Schlüssel

Senden Senden und ablegen... Als Entwurf speichern Zustelloptionen... Signatur Anzeigen Mehr

E-Mail mit PGPNotes

 An: is2354@gmx.de
Kopie:
Blindkopie:
Betreff: signierte Mail

Zustelloptionen

Allgemein | **Erweitert**

OK
Abbrechen

Zustelloptionen

Dringlichkeit: Normal Empfangsbestätigung
Zustellungsbericht: Nur bei Fehler Keine Kopie zulassen
Zustellungspriorität: Normal Autom. Rechtschreibprüfung
 Betreff als 'Vertraulich' markieren
 Keine Benachrichtigung an mich senden, wenn Empfänger den Abwesenheitsagenten ausführen
 Persönliche Gruppen nicht erweitern

Sicherheitsoptionen Modus

Signieren Verschlüsseln Diese Sicherheitsoptionen als Vorgabe speichern

Normal

eMail-Verschlüsselung mit Bordmitteln

- Was brauche ich?
- Wie richte ich meinen Notes-Client ein?
- **Was braucht die Gegenseite?**
- Signierte und verschlüsselte Mails austauschen
 - Signierte Mail empfangen
 - Signierte Mail senden
 - Verschlüsselte Mail empfangen
 - Verschlüsselte Mail senden

Wie bekommt der Empfänger meinen öffentlichen Schlüssel?

- Ich sende eine von mir signierte eMail
- als eMail mit Anhang
- Veröffentlichen auf der Webseite

Wie sieht das beim Empfänger aus?

- Ich sende eine von mir signierte eMail

Gegenzertifikat ausstellen

Zertifizierer...	Juergen Kunert/ITEE/De
Server...	Local
Subjekt	EMAIL=is2354@gmx.de
Alternativer Subjektname	
Fingerabdruck	A35F 5011 022F F813 880A 7E78 4EE7 53F0
Ablaufdatum	10.06.2028 15:13:17

Gegenzertifizieren Abbrechen

Signiert durch is2354@gmx.de am 09.06.2018 20:57:23, gemäß Juergen Kunert/ITEE

Posteingang - juergen.kunert... test sign - Posteingang - j...

Datei Bearbeiten Ansicht Navigation Nachricht Termine und Aufgaben Enigmail Extras Hilfe

Abrufen Verfassen Chat Adressbuch Schlagwörter Schnellfilter

Antworten Weiterleiten Archivieren Junk Löschen Mehr

Von Mir <is2354@gmx.de>

Betreff test sign

09.06.2018 21:57

An Mich <juergen.kunert@itee.de>

bla

Nachrichten-Sicherheit

Nachricht wurde unterschrieben
Diese Nachricht enthält eine gültige digitale Unterschrift. Die Nachricht wurde nicht verändert, seit sie gesendet wurde.

Unterschrieben von:
E-Mail-Adresse: is2354@gmx.de
Zertifikat herausgegeben von: COMODO RSA Client Authentication and Secure Email CA

Unterschriftszertifikat ansehen

Nachricht ist nicht verschlüsselt
Diese Nachricht wurde vor dem Senden nicht verschlüsselt. Informationen, die ohne Verschlüsselung über das Netzwerk / Internet gesendet werden, können von anderen Personen eingesehen werden, während sie übertragen werden.

OK

Wie sieht das beim Empfänger in Outlook aus? 1

- Ich sende eine von mir signierte eMail

 Fr 01.06.2018 17:49
Juergen.Kunert@itee.de
signiert

An is2354@gmx.de

Signiert von juergen.kunert@itee.de



Wie sieht das beim Empfänger in Outlook aus? 2

The image shows two overlapping dialog boxes from Microsoft Outlook. The left dialog, titled 'Eigenschaften der Nachrichtensicherheit', displays the security layers for a signed message. The right dialog, titled 'Signatur', shows the signature details. A red arrow points from the 'Details anzeigen...' button in the left dialog to the 'Signatur' dialog.

Eigenschaften der Nachrichtensicherheit

Betreff: signiert

Nachrichten enthalten u. U. Ebenen für Verschlüsselung oder digitale Signaturen. Jede Ebene für digitale Signaturen kann mehrere Signaturen enthalten.

Sicherheitsschichten

Wählen Sie eine Signaturschicht aus, um deren Beschreibung anzuzeigen.

- ✓ Betreff: signiert
 - ✓ Digitalsignaturschicht
 - ✓ Signierer: juergen.kunert@itee.de

Beschreibung:
OK: Signiert von juergen.kunert@itee.de unter Verwendung von RSA/SHA256 um 17:49:00 01.06.2018.

Klicken Sie auf die Schaltflächen, um weitere Informationen zur gewählten Signaturschicht zu erhalten oder um sie zu bearbeiten:

Vertrauen... **Details anzeigen...** Zertifizierungsstelle vertrauen...

Bei Fehlern in digital signierten Nachrichten Warnhinweis anzeigen. Schließen

Signatur

Allgemein Details

Signaturinformationen

Nachrichtenformat: S/MIME

Signiert von: juergen.kunert@itee.de

Signaturstatus: OK

Signiert um: 17:49:00 01.06.2018

Digestalgorithmus: SHA256

Signaturalgorithmus: RSA (2048 Bits)

Zertifikatsinformationen

Ausgestellt von: COMODO RSA Client Authentication and

Zertifikatsstatus: OK

Zertifikat anzeigen...

Schließen

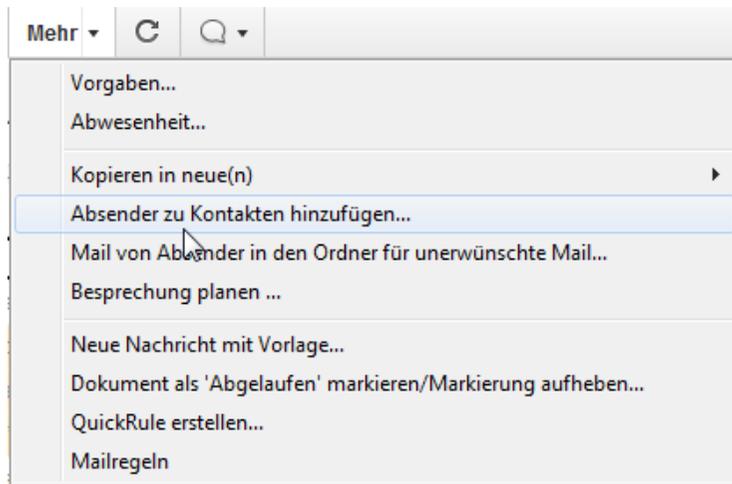
Was braucht die Gegenseite?

- Ihr/sein Schlüsselpaar (privater und öffentlicher Schlüssel)
- meinen öffentlichen Schlüssel (Schlüssel des Empfängers)
- Die richtigen Einstellungen in seinem Mail-Client

Wie richte ich meinen Notes-Client ein?

- Zertifikat mit privatem Schlüssel in Notes importieren
- Öffentliche Schlüssel der Mail-Empfänger in Adressbuch einfügen

Kontakt und Schlüssel in Adressbuch importieren 1



A screenshot of a dialog box titled 'Absender zur Kontaktliste hinzufügen'. The dialog contains several input fields and a checkbox. The fields are: 'Titel:' (dropdown), 'Vorname:' (text box with 'Juergen'), '2. Vorname:' (text box), 'Nachname:' (text box with 'Kunert'), 'Namenszusatz:' (dropdown), 'Firmenname:' (text box), 'E-Mail:' (text box with '"Juergen Kunert" <is2354@gmx.de>'), 'Mailprogramm:' (dropdown with 'Internet'), 'Routing-Domäne(n):' (text box with a question mark icon), 'Telefon (geschäftlich):' (text box), 'Telefon (priv.):' (text box), and 'Handy:' (text box). At the bottom, there is a checkbox labeled 'Internetzertifikate des Absenders speichern, falls verfügbar' with a question mark icon, which is checked. On the right side of the dialog, there are 'OK' and 'Abbrechen' buttons.

Kontakt und Schlüssel in Adressbuch importieren 2

So sieht es dann im Adressbuch aus:

Bearbeiten vCard weiterleiten    

Ignatz Schlehenbrenner
"Ignatz Schlehenbrenner" <is2354@gmx.de>

E-Mail

Geschäftlich: "Ignatz Schlehenbrenner" <is2354@gmx.de>

Andere Informationen

Nachrichten-ID: Ignatz Schlehenbrenner <is2354@gmx.de>

Kommentare | Angaben zum Namen | **Zertifikate**

Internetzertifikate:

Internetzertifikat: Vorhanden
Aussteller des Internetzertifikats: 1. CN=COMODO RSA Client Authentication and Secure Email CA/O=COMODO CA Limited/L=Salford/ST=Greater Manchester/C=GB

Achtung: Wenn im kontakt bereits ein Notes-Zertifikat enthalten ist, muss dies zuerst entfernt werden.

Was habe ich davon?

- Ich kann signierte Mails verschicken
- Ich kann Mails lesen, die mit meinem Public Key verschlüsselt sind

eMail-Verschlüsselung mit Bordmitteln

- Was brauche ich?
- Was braucht die Gegenseite?
- Wie richte ich meinen Notes-Client ein?
- **Signierte und verschlüsselte Mails austauschen**
 - Signierte Mail empfangen
 - Signierte Mail senden
 - Verschlüsselte Mail empfangen
 - Verschlüsselte Mail senden

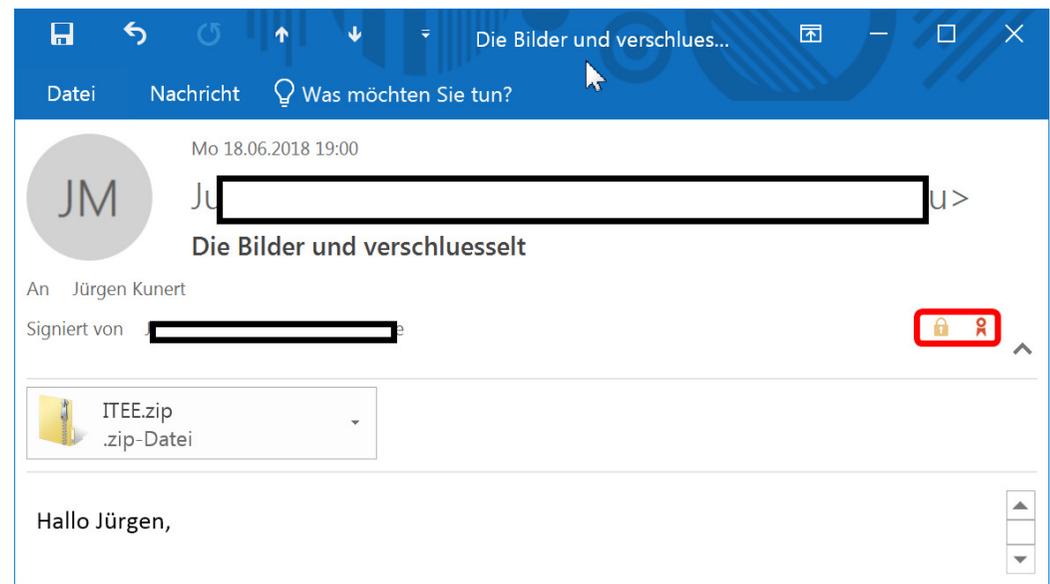
Signierte Mail senden

- Was habe ich davon?
 - Ich übermittle meinen privaten Schlüssel an den Empfänger
- So sieht das dann aus:

The screenshot shows the Outlook interface during the process of sending a signed email. The 'Optionen' ribbon is active, displaying the 'Verschlüsseln' (Encrypt) and 'Signieren' (Sign) buttons. The 'Betreff' (Subject) field shows 'Verschlüsselte Mail'. A 'Dokument' window is open, displaying the details of the 'Sign' field: Feldname: Sign, Datentyp: Text, Datenlänge: 1 Byte, Seq.-Num.: 1, Doppeleintrags-ID: 0, and Feld-Flags: SUMMARY. The main window shows the email composition area with the 'An:' field set to 'is2354@gmx.de' and the 'Betreff:' field set to 'signierte Mail'. A status bar at the bottom indicates 'Nachricht wird signiert...' and 'Mail wurde zur Zustellung abgegeben. (1 Person/Gruppe)'.

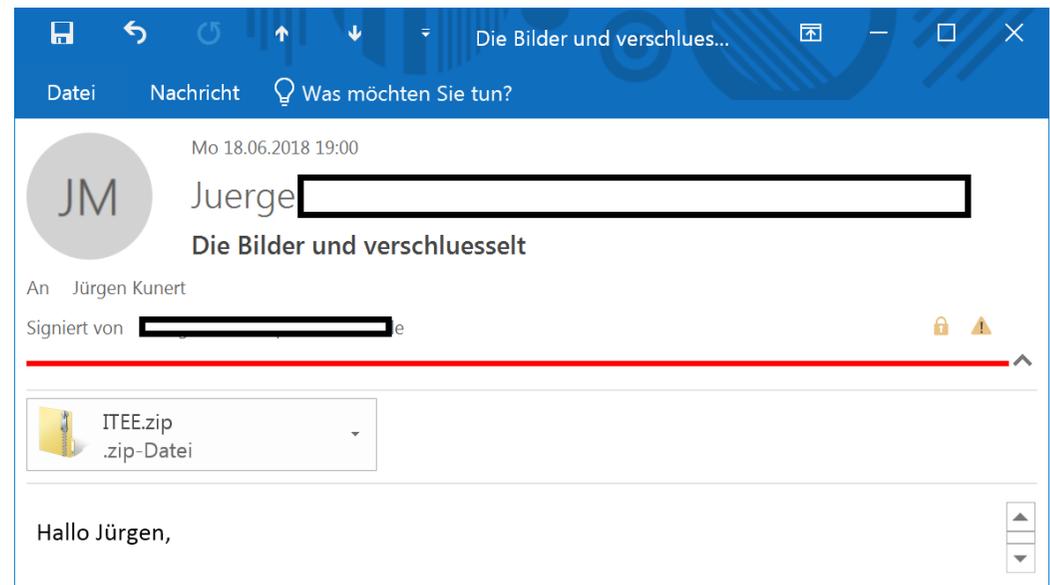
Signierte Mail empfangen

- Was habe ich davon?
 - Die eMail wurde von jemandem versendet, der Zugriff auf seinen privaten Schlüssel hatte
 - Wenn die Signatur intakt ist, wurde die eMail nicht verändert
- So sieht das dann aus:



Signierte Mail empfangen

- Was habe ich davon?
 - Die eMail wurde von jemandem versendet, der Zugriff auf den privaten Schlüssel hatte
 - Wenn die Signatur intakt ist, wurde die eMail nicht verändert
- So sieht das dann aus:

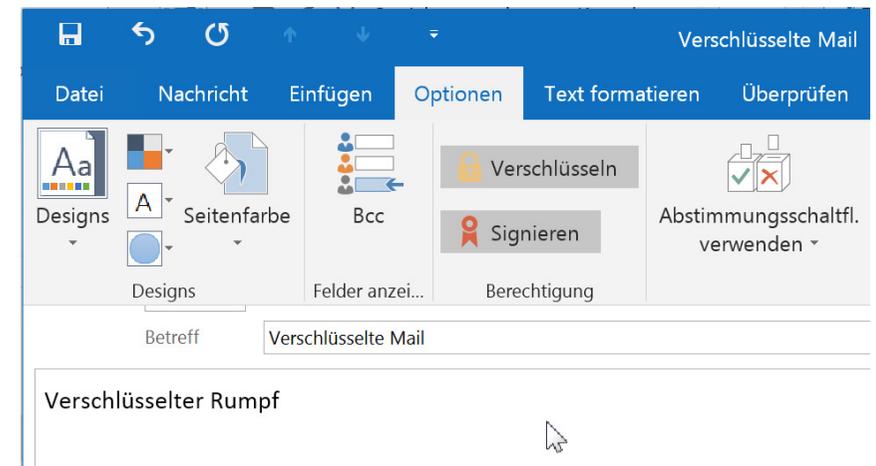


Verschlüsselte Mail senden

- Was habe ich davon?
 - Die eMail kann auf dem Transportweg nicht gelesen werden
- So sieht das dann aus:



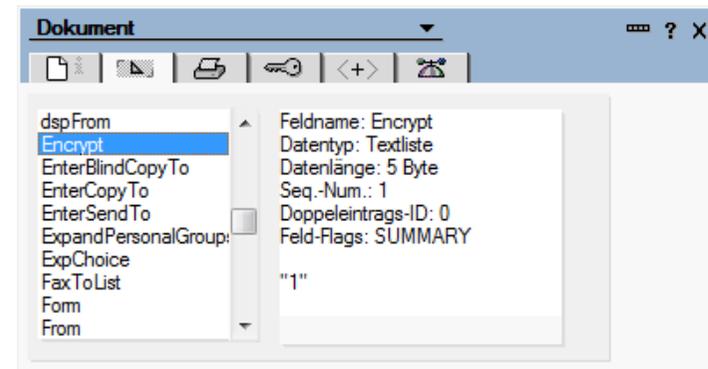
Richtig wäre: mit dem öffentlichen Schlüssel des Empfängers verschlüsselt



Verschlüsselte Mail empfangen

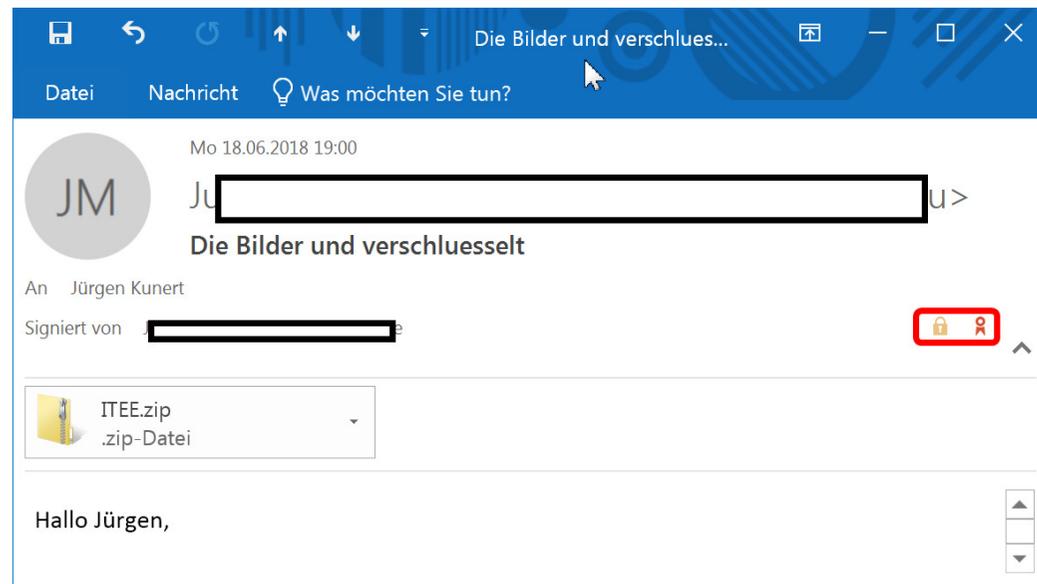
- Was habe ich davon?
 - Die eMail wurde von jemandem versendet, der Zugriff auf meinen öffentlichen Schlüssel hatte
 - Der Inhalt konnte auf dem Transportweg nicht gelesen werden
- So sieht das dann aus:

Dokument wird entschlüsselt...



Verschlüsselte Mail in Outlook empfangen

- Was habe ich davon?
 - Die eMail wurde von jemandem versendet, der Zugriff auf meinen öffentlichen Schlüssel hatte
 - Der Inhalt konnte auf dem Transportweg nicht gelesen werden
- So sieht das dann aus:



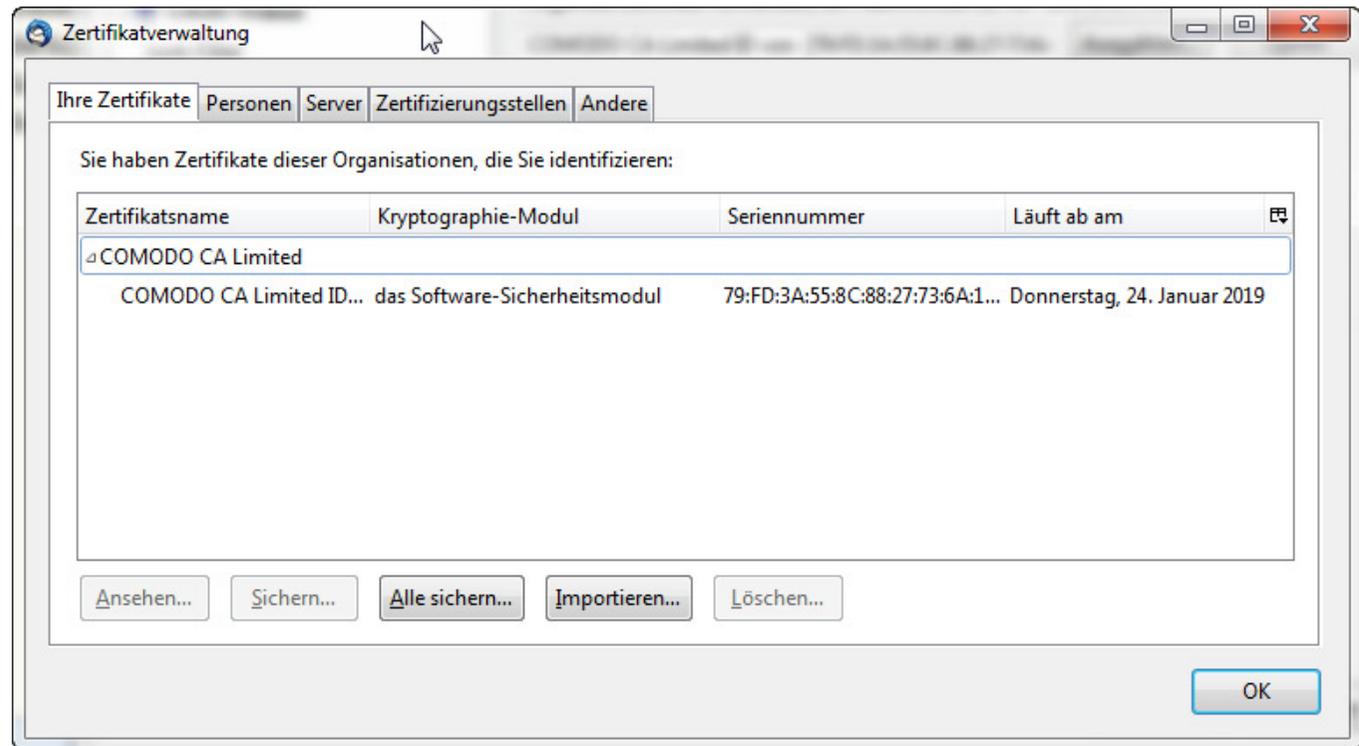
Das Selbe in Thunderbird

- So sieht eine empfangene verschlüsselte Mail aus, wenn das Zertifikat noch nicht installiert wurde:



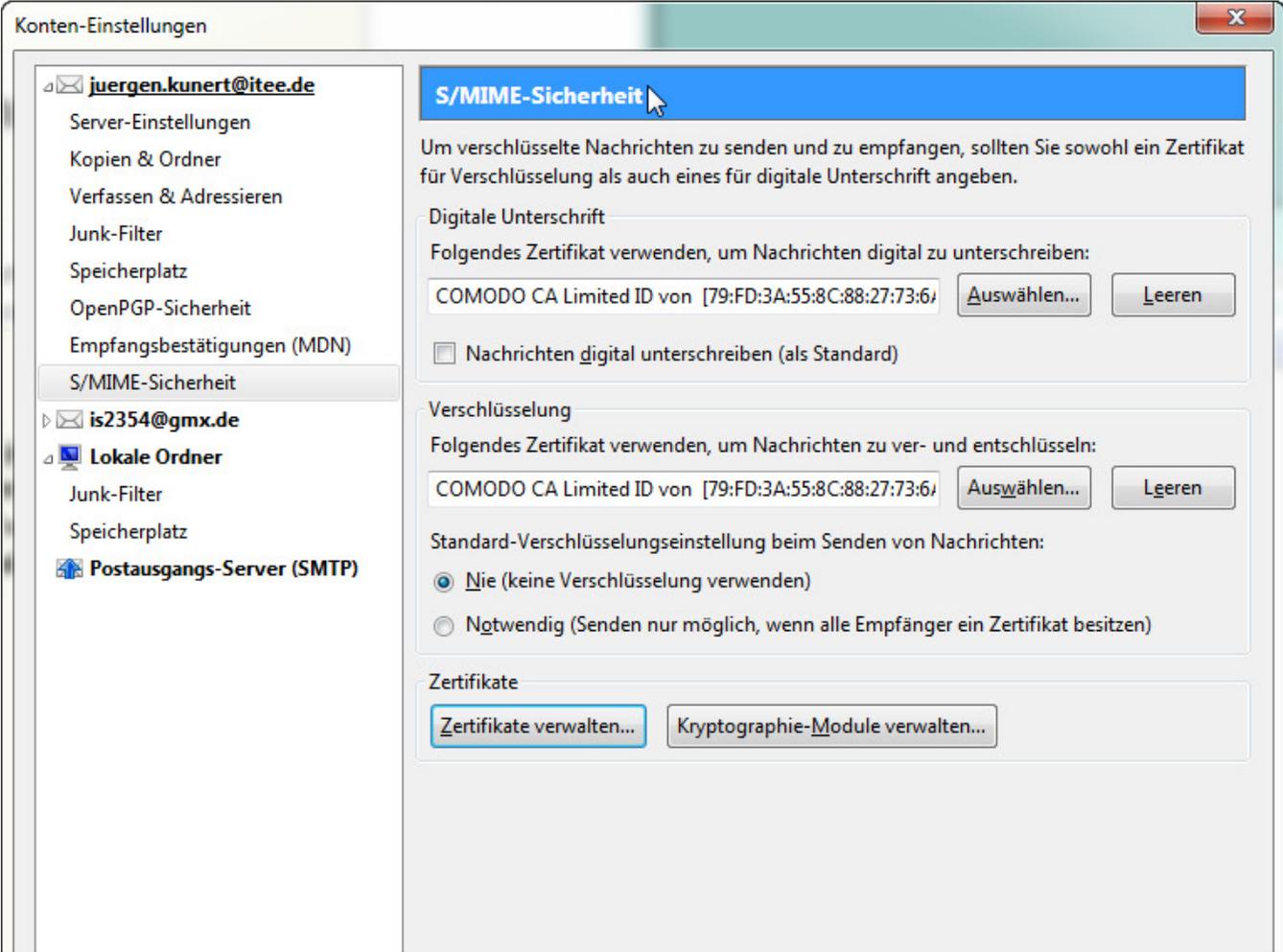
Das Selbe in Thunderbird

- Zertifikat in Zertifikatsverwaltung importieren



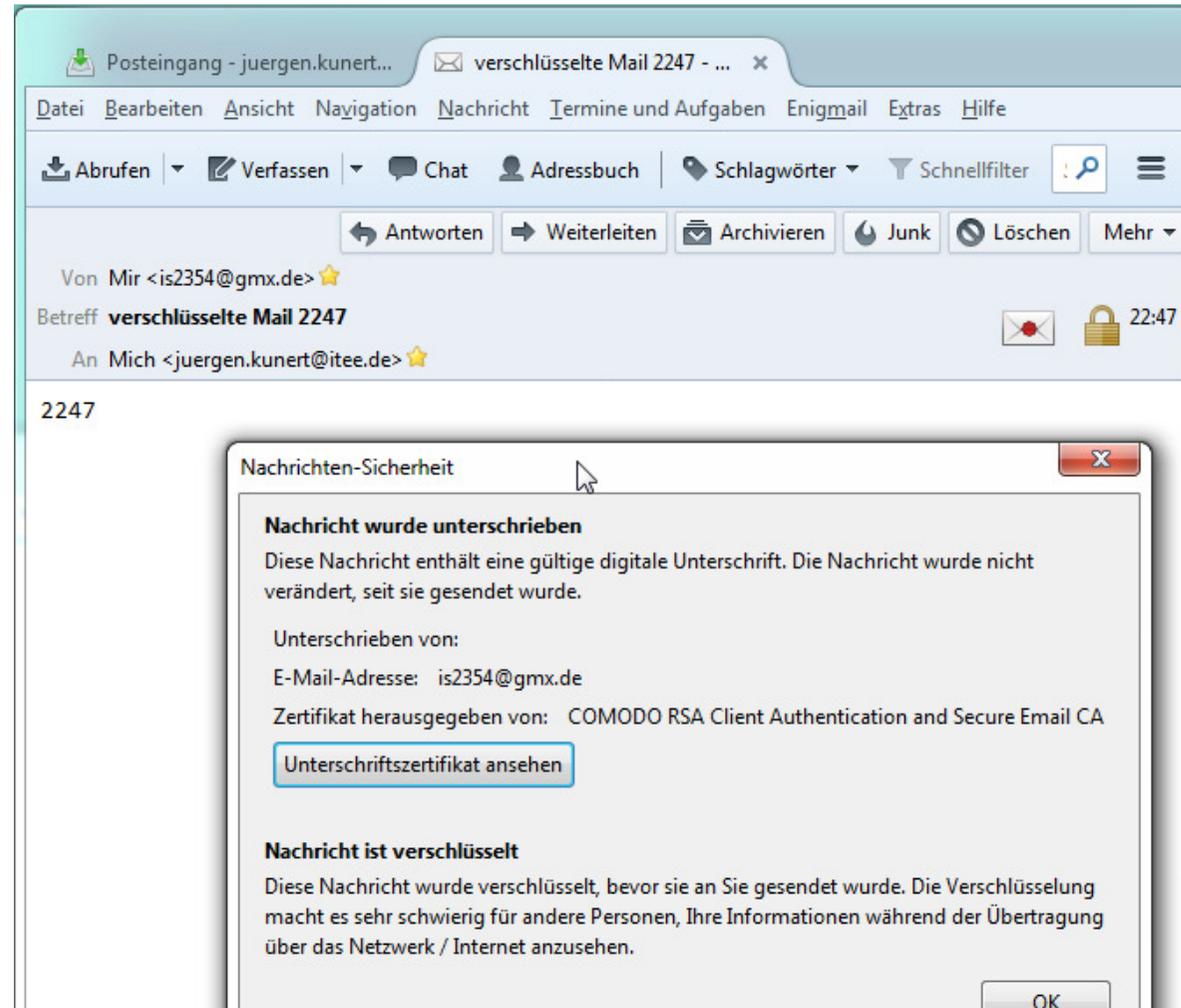
Das Selbe in Thunderbird

- Zertifikat aus Zertifikatsspeicher konfigurieren



Das Selbe in Thunderbird

... und schon kann man die Mail entschlüsseln



Mobil - Vorbereitungen

- Notes-ID muss zur Verfügung stehen:
 - Im ID-Vault oder importiert in die MailDB
- Für den Import in die MailDB gibt es mehrere Möglichkeiten:
 - Traveler-Webseite: mycompany.de/traveler
 - Import per iNotes
 - Mobile Device Management-Systeme

Mobil – was geht?

1. Aussage von „vorsichtigen Personen“:
verschlüsselte Mails haben nichts auf Smartphones zu suchen,
das Smartphone kann verloren gehen
2. iOS:
 - S/MIME und Notes Native Encryption von Verse unterstützt
3. Android:
 - Only Domino-encrypted mail is supported on the IBM Verse client.
Encrypted calendar, to-do, and notebook entries are not supported.
SMIME encryption is unavailable.
4. iNotes: supported

Mobil – iOS native Mail

< Eingang ^ v



Juergen Kunert

An: juergen.kunert@itee.de

[Details](#)

JK

verschlüsselt und signiert 844

Heute um 08:45

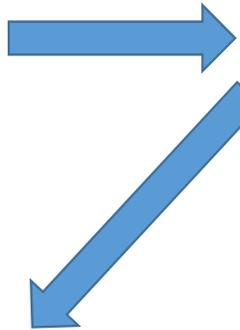
Diese E-Mail hat keinen Inhalt.

Mobil – iOS Verse

verschlüsselt und signiert 844

 Juergen Kunert
An: mich
08:45 [Details](#)

Diese E-Mail ist verschlüsselt.
[Zum Anzeigen der Nachricht herunterladen.](#)



Notes-ID-Kennwort
Geben Sie Ihr Notes-ID-Kennwort ein

[Abbrechen](#) [OK](#)

verschlüsselt und signiert 844

 Juergen Kunert
An: mich
08:45 [Details](#)

Diese E-Mail ist verschlüsselt.
Herunterladen...

verschlüsselt und signiert 844

 Juergen Kunert
An: mich
08:45 [Details](#)

1 Anhang

 smime.p7s - 3,88 KB

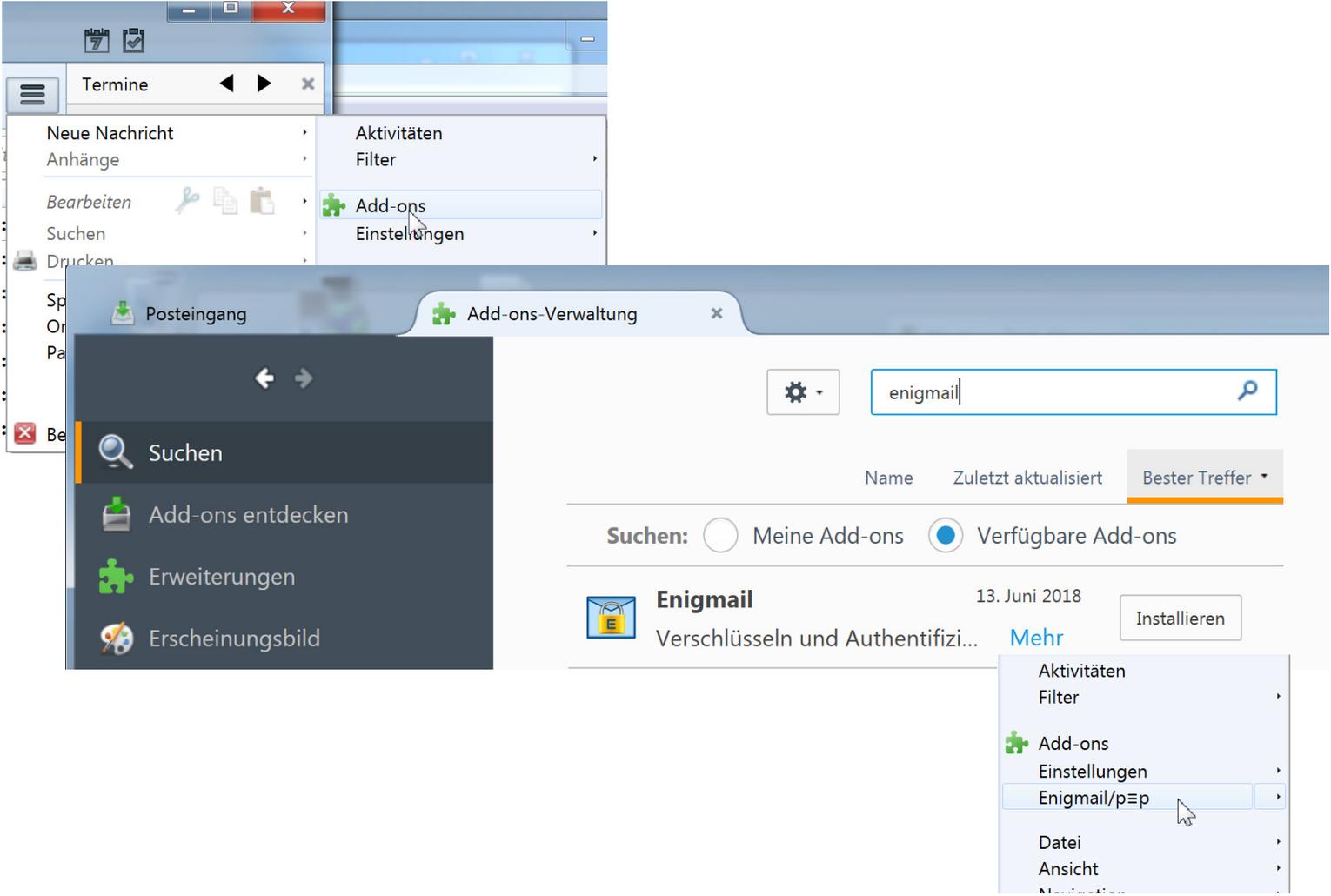
Diese E-Mail ist verschlüsselt und digital signiert.
[Zum Anzeigen der Nachricht herunterladen.](#)

verschlüsselter Rumpf 844

PGP

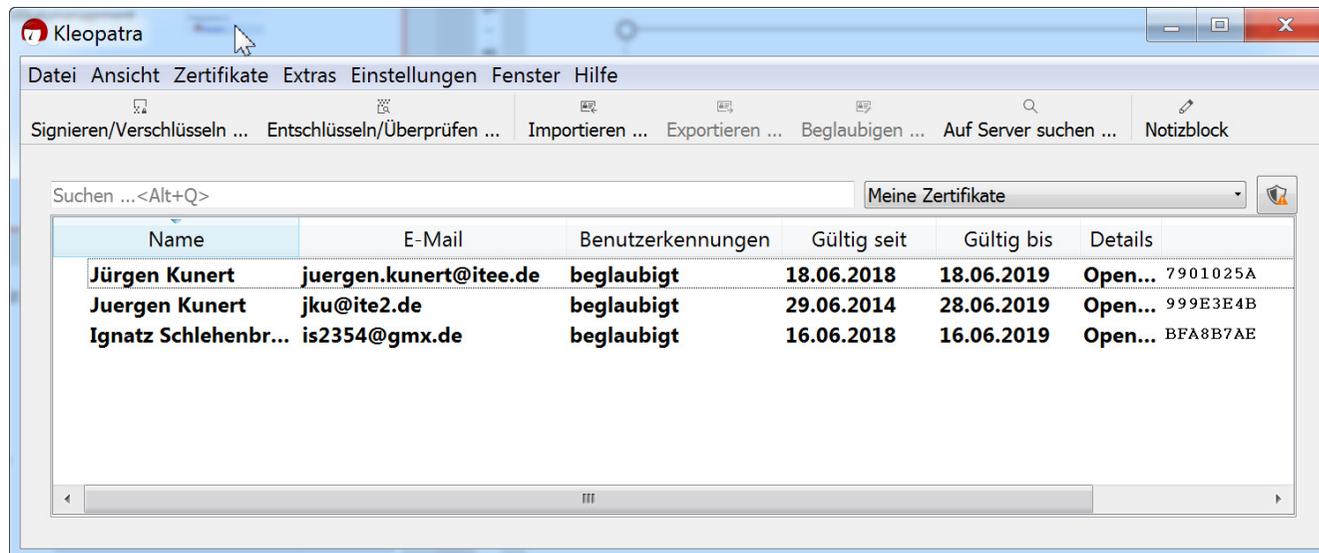
Thunderbird mit PGP

- GPG4Win und Enigmail installieren



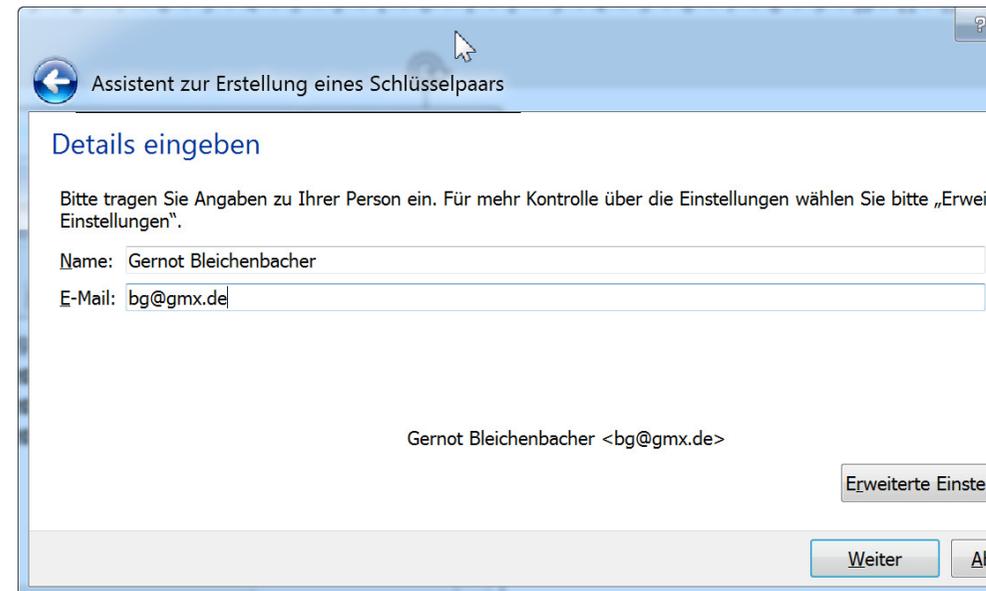
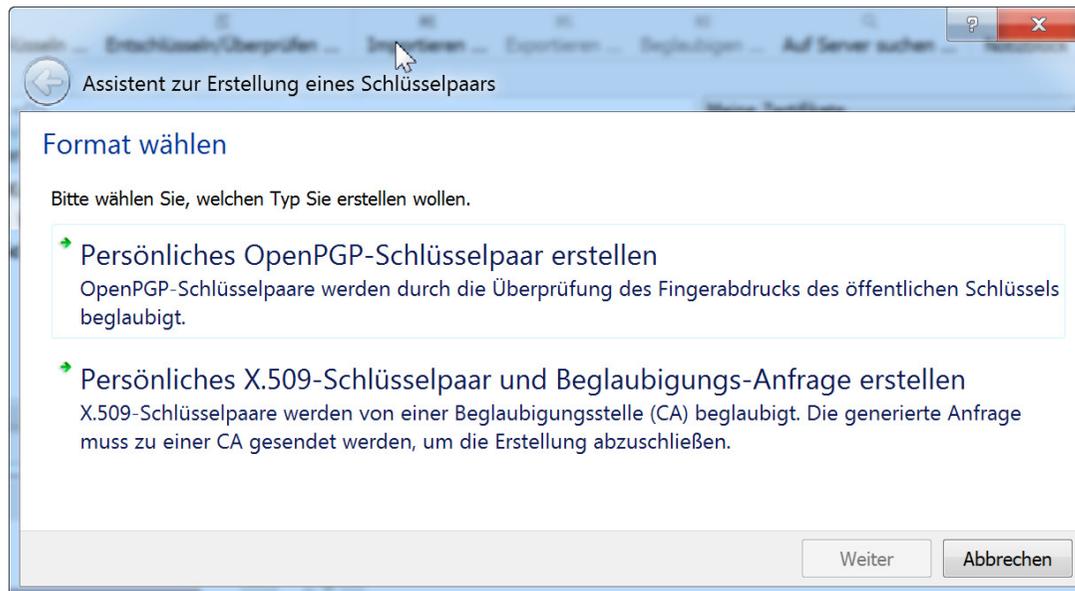
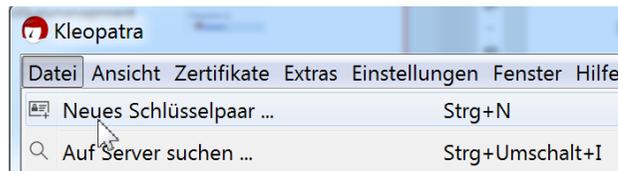
GPG4 Win - Kleopatra

- Kleopatra: Zertifikatsmanagement



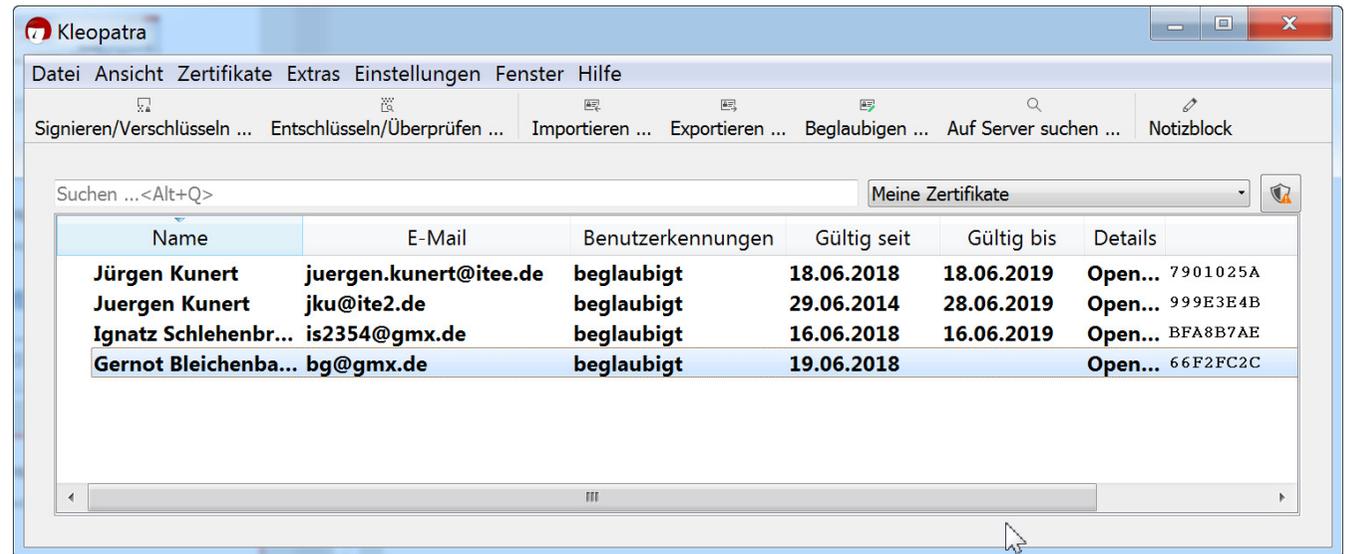
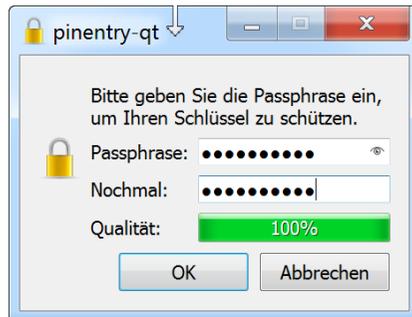
GPG4 Win - Kleopatra

- Schlüsselpaar erzeugen 1



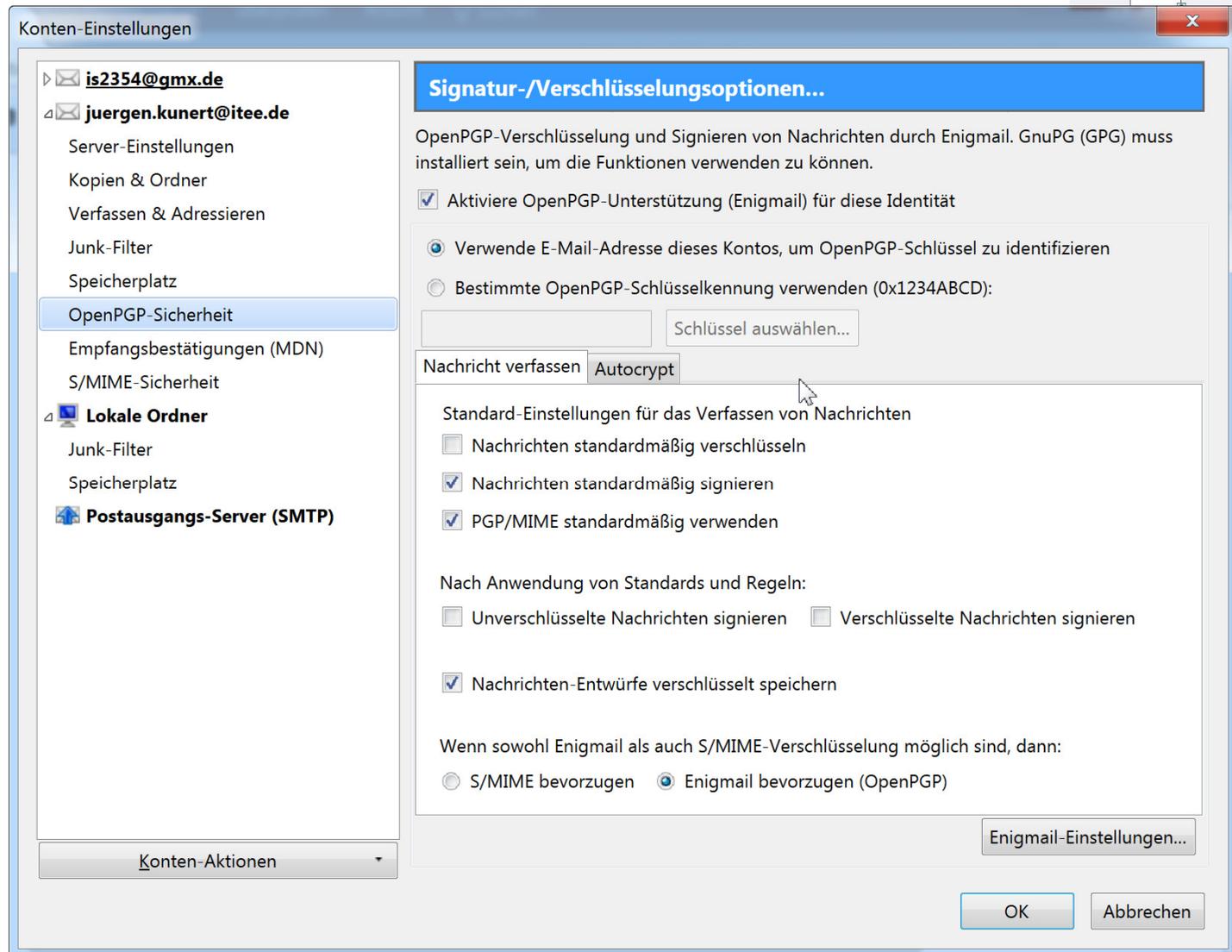
GPG4 Win - Kleopatra

- Schlüsselpaar erzeugen 2



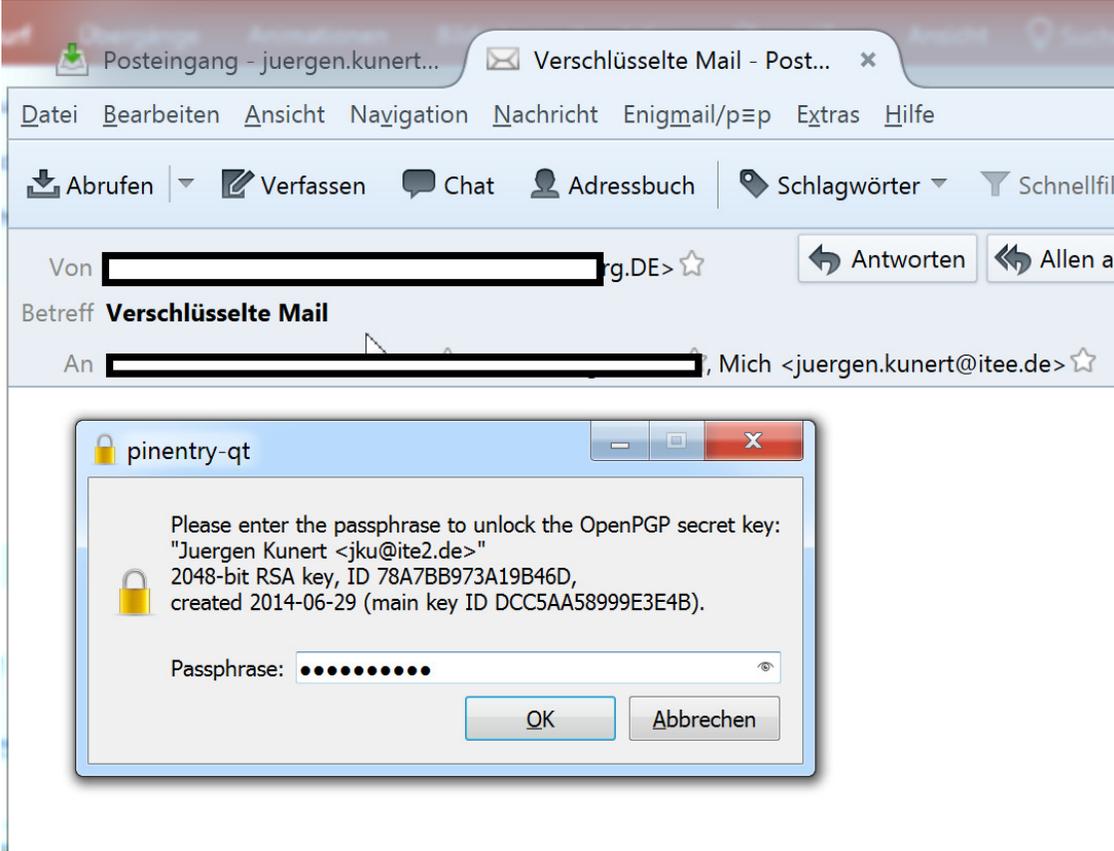
Thunderbird mit PGP

- Enigmail konfigurieren



Thunderbird mit PGP

- Enigmail
verschlüsselte eMail



Thunderbird mit PGP

- Enigmail
verschlüsselte
eMail
empfangen



Thunderbird mit PGP

- Enigmail Sicherheitsinfo

Enigmail Information

i Enigmail-Sicherheitsinfo:

Entschlüsselte Nachricht

Korrekte Signatur: [redacted] <[redacted]@[redacted].de>

Schlüsselkennung: [redacted] 06.18, 09:29

Schlüssel-Fingerab: [redacted] 224D F996 7B8A F9BF

Verwendete Algorithmen: RSA und SHA256

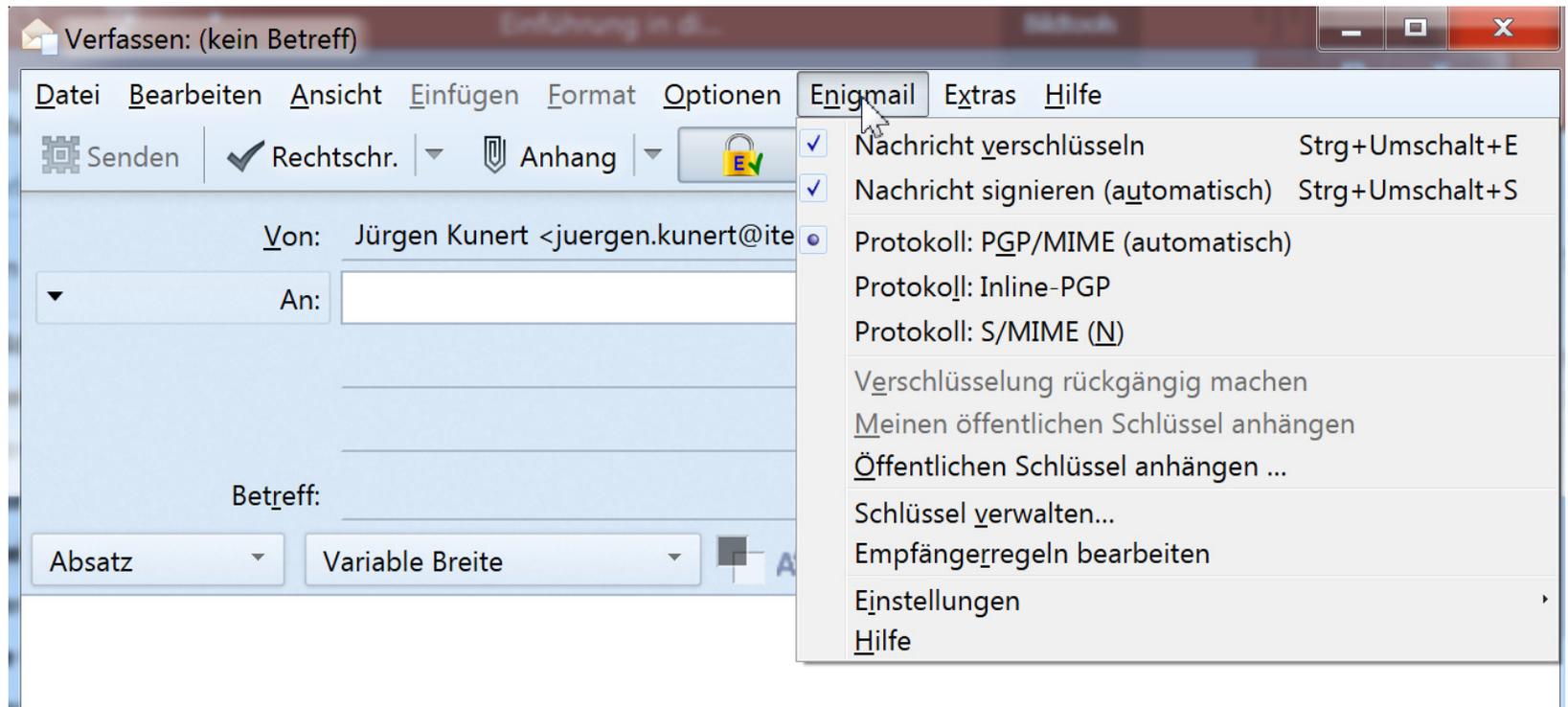
Hinweis: Die Nachricht wurde mit folgenden Benutzer-IDs / Schlüsseln verschlüsselt:

- 0xE3 [redacted]
- 0x78 [redacted]
- 0x0E [redacted] <[redacted]@denburg.de>),
- 0x04 [redacted] >),
- 0xF4 [redacted] <[redacted].de>)

Schließen

Thunderbird mit PGP

- Enigmail
verschlüsselt und signiert senden



PGPNotes

- PGPNotes enables Lotus Notes users to **conveniently encrypt and decrypt messages/attachments** using [PGP](#) or [GnuPG](#), all from within the Notes client itself.
- Eine Teilmaske und eine DLL sind zu installieren
- Man benötigt ebenso GPG4Win für die Zertifikateverwaltung und die Ver-/Entschlüsselungsalgorithmen

PGPNotes - Senden

Senden Senden und ablegen... Als Entwurf speichern Zustelloptionen... ► ✎ Signatur▼ Anzeigen▼ Mehr▼  PGP Encrypt/Send

Enhanced with PGPNotes

 An:
Kopie:
Blindkopie:
Betreff:

vertraulicher Nutztex

Eigenschaften der Verschlüsselung

Nachricht:

Dateianhang

Eigenen öffentlichen Schlüssel:

pinentry-qt

 Sie benötigen eine Passphrase, um den geheimen OpenPGP Schlüssel zu entsperren:
"Juergen Kunert <juergen.kunert@fiff.de>"
2048-Bit RSA Schlüssel, ID DCC5AA58999E3E4B,
erzeugt 2014-06-29.

Passphrase:

PGPNotes - Empfangen

Neu ▾ Antwort ▾ Allen antworten ▾ Weiterleiten ▾



hallo
Ursula An: Jürgen Kunert

Von: [redacted].de>
An: "Jürgen Kunert" <Juergen.Kunert@itee.de>

▼ 1 Anhang



encrypted.asc



att1jwrd.dat

Speichern und ablegen... Speichern und schließen ▶ Anzeigen ▾ Mehr ▾ PGP Forward

Enhanced with PGPNotes



An: "Jürgen Kunert" <Juergen.Kunert@itee.de>
Kopie: [empty]
Blindkopie: [empty]
Betreff: hallo
Von: [redacted].de> - Sonntag 09.09.2018 15:35

▼ 1 Anhang



encrypted.asc

Lieber Jürgen,
entschlüsselter Text
[Dateianhang: Honig Preis .odt]

Anzeigen

Öffentliche(n) Schlüssel verarbeiten

Dateianhang

Dateinamen	Dateigröße	Nur signieren
Honig Preis .odt	1.64MB	

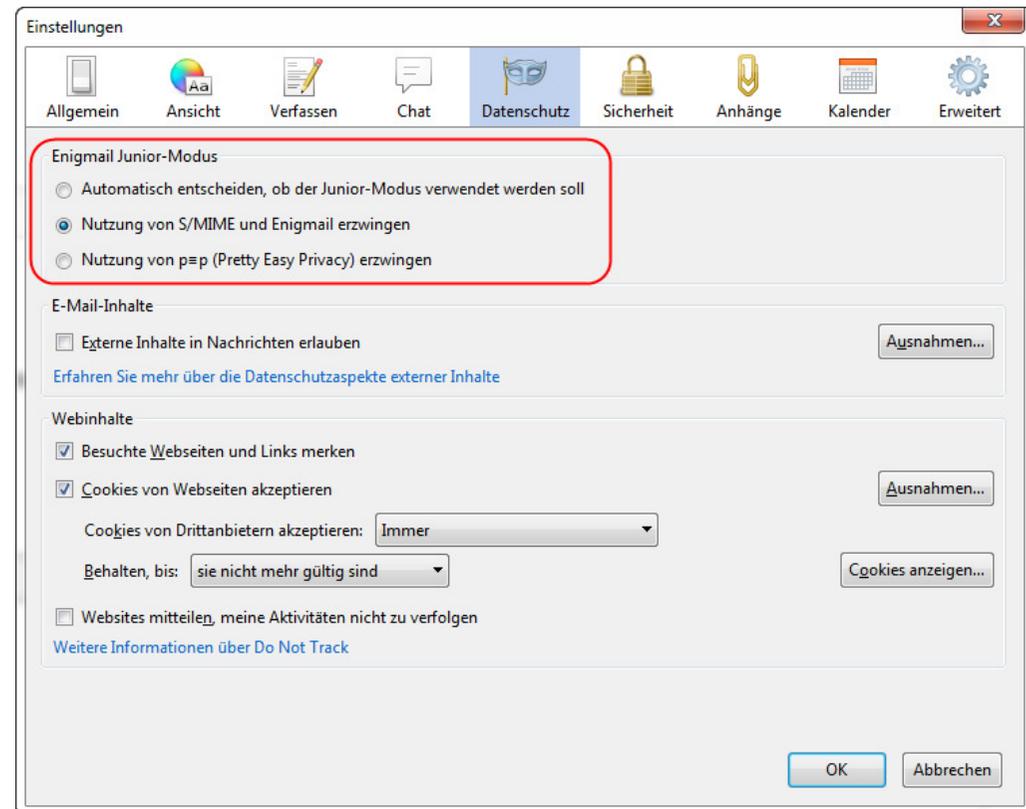
Pretty Easy Privacy **p≡p**

- **pretty Easy privacy** (abgekürzt p≡p oder pEp) oder zu Deutsch *Ziemlich einfache Privatsphäre* ist eine [Open-Source-Verschlüsselungs](#)-Software, die es dem Nutzer erlaubt, seine Online-Kommunikation vor fremden Einblicken zu schützen. Dabei sind die erforderlichen Prozesse automatisiert.
- p≡p generiert für den Benutzer automatisch ein [Schlüsselpaar](#) oder importiert es von einem lokalen PGP ([Pretty Good Privacy](#))-Client. Die Software verschlüsselt die Kommunikation auch dann, wenn der Empfänger einen anderen PGP- oder [S/MIME](#)-Client als p≡p installiert hat.
- Quelle: Wikipedia

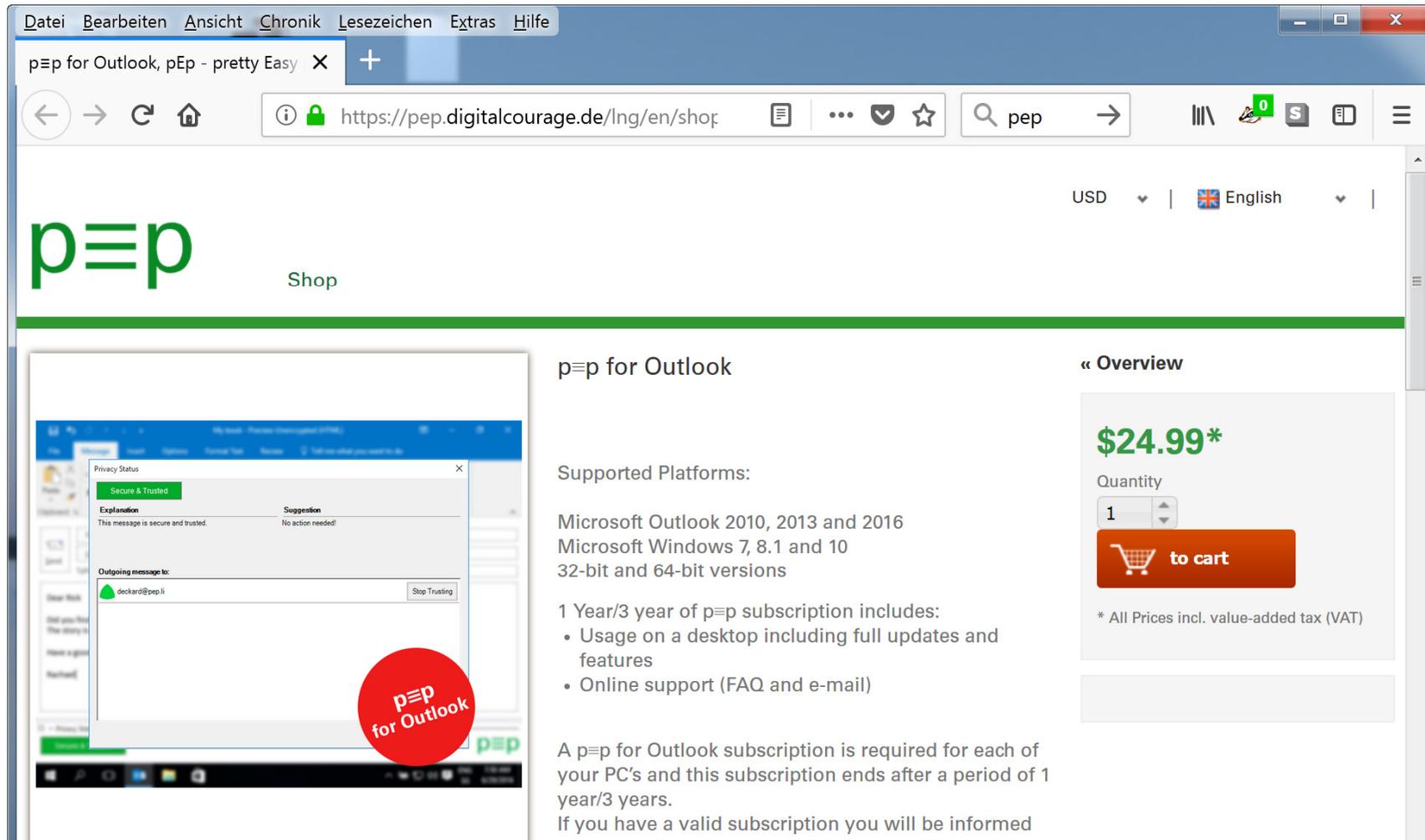
Pretty Easy Privacy



- Umstellen von PEP auf PGP:
Extras/Einstellungen
(natürlich nicht unter
Enigmail/Einstellungen)



pEp for Outlook



File Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe

pEp for Outlook, pEp - pretty Easy X +

https://pep.digitalcourage.de/lng/en/shop

USD | English

pEp Shop

pEp for Outlook

Supported Platforms:

- Microsoft Outlook 2010, 2013 and 2016
- Microsoft Windows 7, 8.1 and 10
- 32-bit and 64-bit versions

1 Year/3 year of pEp subscription includes:

- Usage on a desktop including full updates and features
- Online support (FAQ and e-mail)

A pEp for Outlook subscription is required for each of your PC's and this subscription ends after a period of 1 year/3 years.
If you have a valid subscription you will be informed

« Overview

\$24.99*

Quantity: 1

[to cart](#)

* All Prices incl. value-added tax (VAT)

pEp for Outlook

Nachteile der Verschlüsselung mit Bordmitteln

1. Erklärungsbedarf
2. Administrativer Aufwand (Client)
3. Die User sind verantwortlich
4. Mail-Journaling funktioniert nicht mehr für diese Mails
5. Was macht der Virens Scanner, das Signaturprogramm, etc. mit der verschlüsselten Mail?
6. Mail-Archivierung
7. Verfügbarkeit für die Steuerprüfung!
8. Ab und zu hakt es mal und der User bekommt es nicht mit!

„Efail“- Schwachstelle

Die Angreifer fangen die verschlüsselte Mail des Absenders ab und manipulieren sie mit aktiven HTML-Inhalten, zum Beispiel mit Bildern oder Darstellungscodierungen, sogenannten Styles. Danach wird die so präparierte Mail an den Empfänger geschickt. Das Sicherheitsproblem entsteht, wenn im eMail-Programm des Empfängers das automatische Nachladen von HTML-Inhalten vorkonfiguriert ist. Dessen eMail-Client entschlüsselt die eMail und lädt gleichzeitig alle externen HTML-Inhalte. Beim Laden bekommen die Angreifer – ohne dass der Empfänger es merkt – auch den jetzt lesbaren Text der Mail zugeschickt. Ein Angreifer entschlüsselt die Mail also nicht selbst. Vielmehr lässt er den Empfänger die Nachricht entschlüsseln und dann den Klartext durch manipulierte HTML-Inhalte an einen Server unter seiner Kontrolle schicken.

„Efail“-Schwachstelle

- <https://www.heise.de/ct/ausgabe/2018-12-Efail-Erfolgreiche-Angriffe-auf-E-Mail-Verschluesselung-4056263.htm>
- https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/efail_schwachstellen.html
- <https://www.egovernment-computing.de/nicht-das-verschluesselungsverfahren-sondern-die-implementierung-ist-das-problem-a-722351/>
- Amüsant:
<https://www.youtube.com/watch?v=fJE38REArEs>
Golem eFail:
<https://www.youtube.com/watch?v=HZGawmoS3qg>

Was tun? Aspekte für eine Auswahl

- Abhängig von der Anzahl der Kommunikationspartner
- Abhängig von Gesetzen und Rechtsprechung
- Abhängig von Vertretungsregelungen
- Bei Ende-zu-Ende-Verschlüsselung kommt der Virens Scanner erst auf dem Mail-Client zum Zuge
- Mail-Archivierung, Zusatzprogramme auf dem Client?
- Backup
- Kosten
- Usability für die Endbenutzer

Literatur/Quellen

- <https://www.privacy-handbuch.de/>
- https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/EMails_verschluesseln.html
- <https://www.bundesdruckerei.de/de/whitepaper-e-mail-verschluesselung>
- http://de.wikipedia.org/wiki/E-Mail-Verschl%C3%BCsselung#S.2FMIME-basierte_E-Mail-Verschl.C3.BCsselung_und_-Signatur_im_Detail
- <http://en.wikipedia.org/wiki/S/MIME>
- <http://www.kryptowissen.de/schutzziele.php> zwei Artikel in der c't 18/2012
- https://www.computerwoche.de/a/so-verschluesseln-sie-ihre-e-mails-richtig,3545112?tap=b28622df41dd36065e45ac10cd10d28a&utm_source=Security&utm_medium=email&utm_campaign=newsletter&r=768639720977988&lid=897098&pm_In=10
- <http://www.computerwoche.de/security/2510521/#>
- <https://www.heise.de/tipps-tricks/PDFs-sicher-verschluesseln-so-klappt-s-3918234.html>
- <https://www.heise.de/tipps-tricks/ZIP-Archiv-mit-einem-Passwort-schuetzen-So-geht-s-3907870.html>
- <https://pep.foundation/docs/pEp-whitepaper.pdf>

Jürgen Kunert

ITEE

Informationstechnologie Effizient Einsetzen

Sandkrugweg 57a

22457 Hamburg

Juergen.Kunert@itee.de

**Vielen Dank für eure
Aufmerksamkeit!**

The End



Steganografie

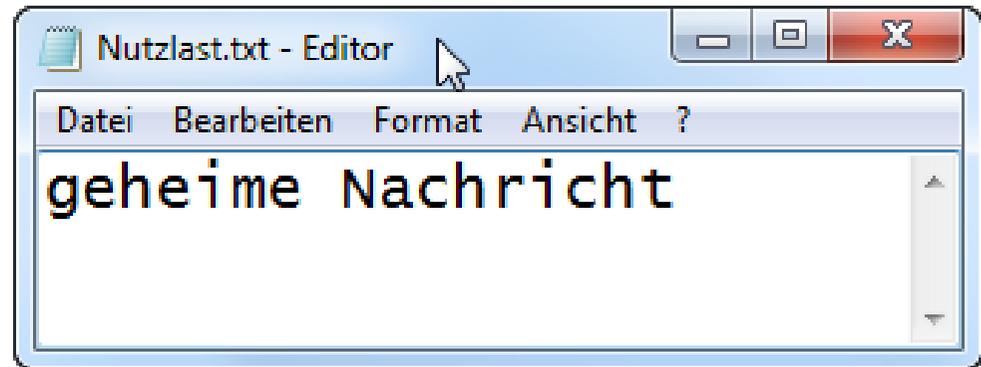
- Steganografie ist die Kunst oder Wissenschaft der verborgenen Speicherung oder Übermittlung von Informationen in einem Trägermedium (Container). (Wikipedia)
- Verstecken der Nachricht in einem Foto, Video, Audio
- Dass eine Nachricht übersandt wird, fällt nicht (so leicht) auf (Wettstreit zwischen Kryptografie und Kryptoanalyse)
- <https://www.heise.de/ix/artikel/Tarnen-und-Taeuschen-1919755.html>
- Auch Malware kann versteckt werden

Steganografie-Programm

- SteganoG



+



Steganografie-Programm

- SteganoG

Name	Datum	Typ	Größe	Änderungsdatum
P1000654 - SaveCopy.bmp	10.06.2018 13:05	IrfanView BMP File	35.157 KB	10.06.2018 13:05
Nutzlast.txt	10.06.2018 13:06	TXT-Datei	1 KB	10.06.2018 13:06
P1000654.bmp	10.06.2018 13:05	IrfanView BMP File	35.157 KB	10.06.2018 13:09

