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

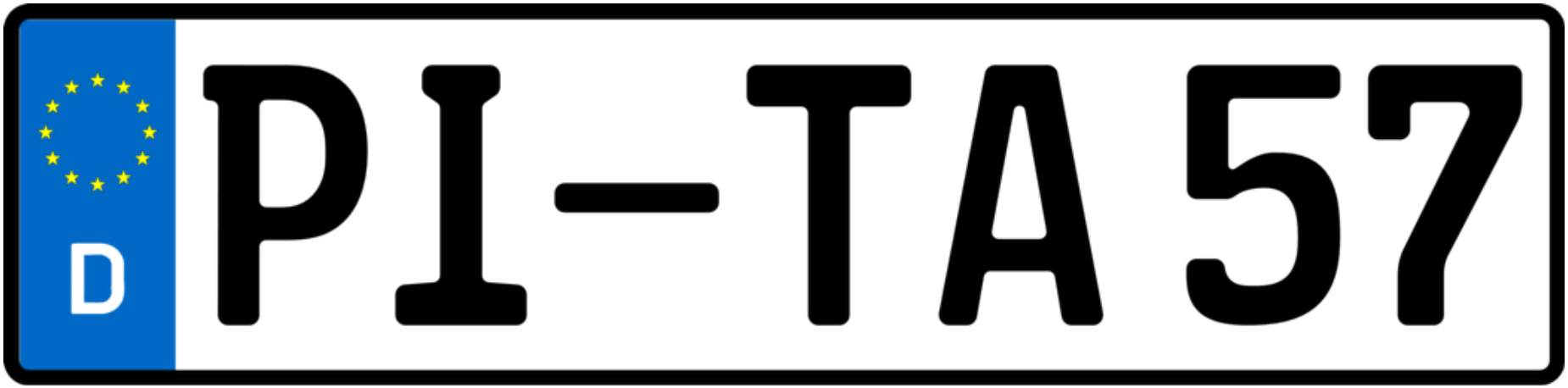
Was passiert beim eMail-Senden?

- 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!)

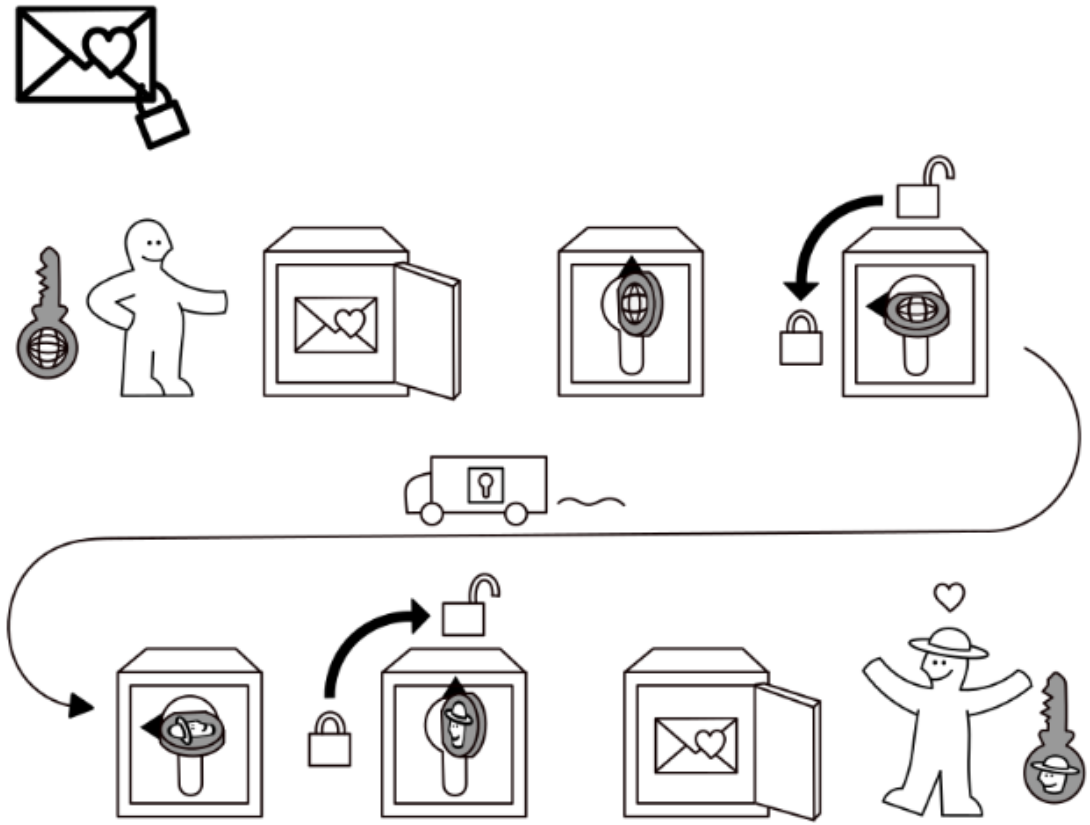
Asymmetrische Verschlüsselung: Vertrauen schaffen

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.

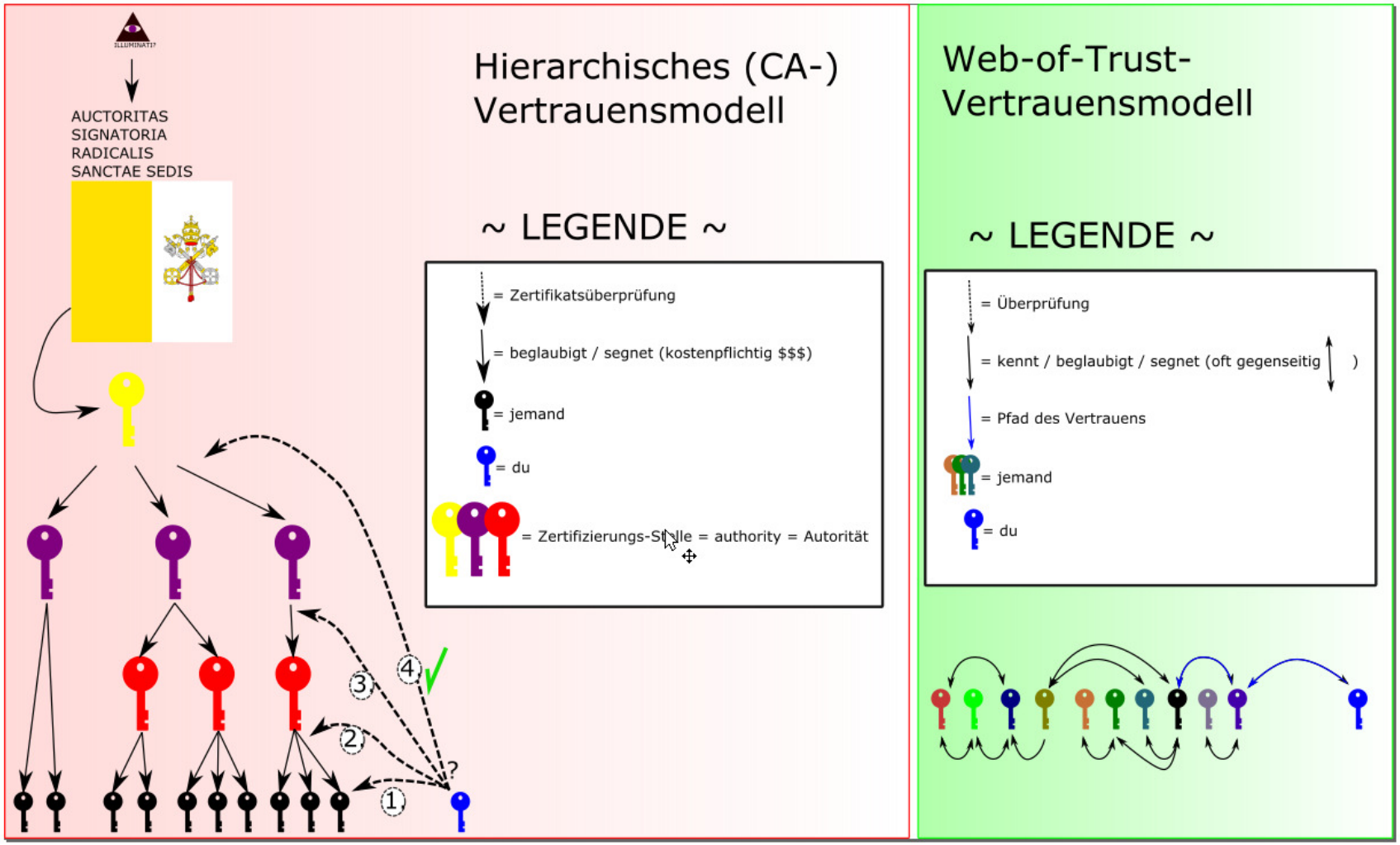


Quelle: https://idea-instructions.com/

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



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↔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/

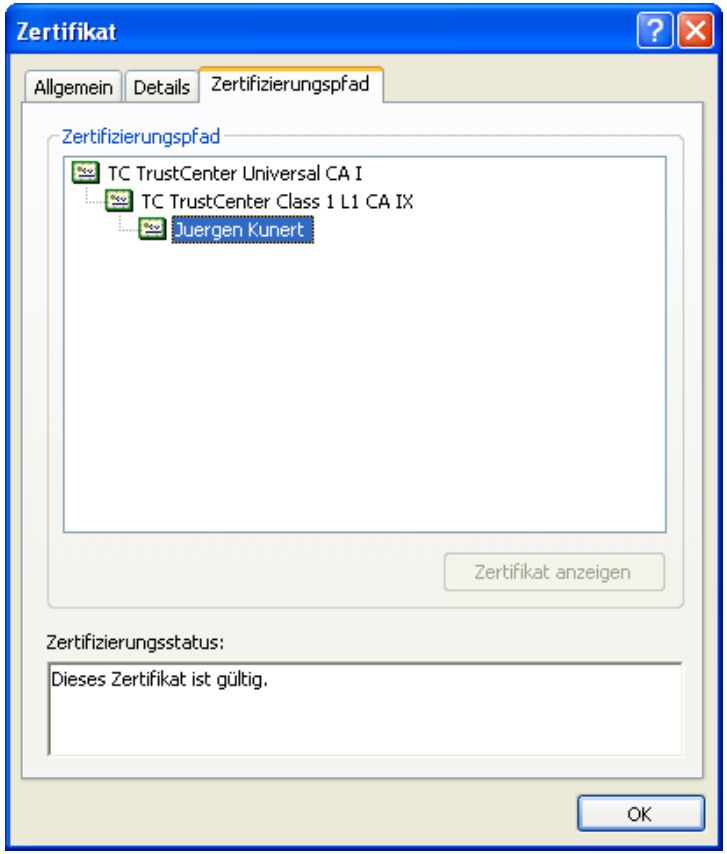
Vertrauensmodell PGP

- 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

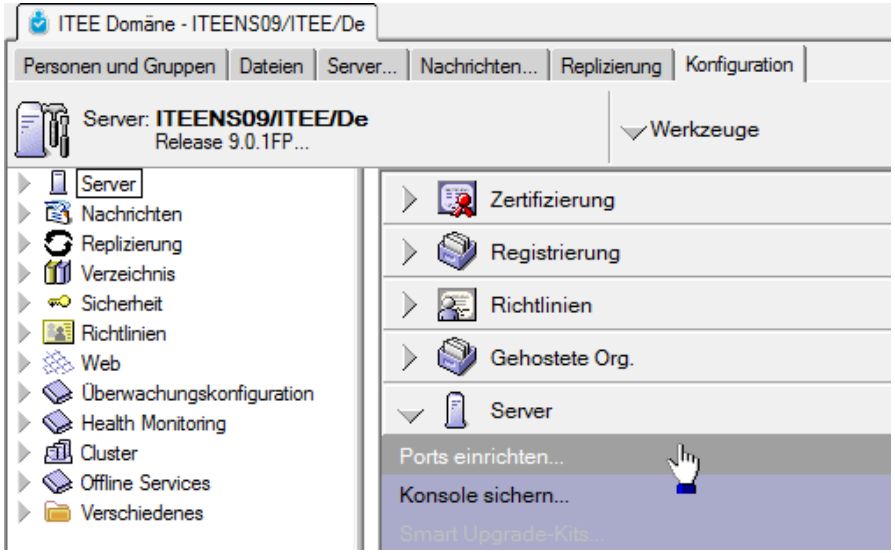
Transportverschlüsselung Ports (senden) 1

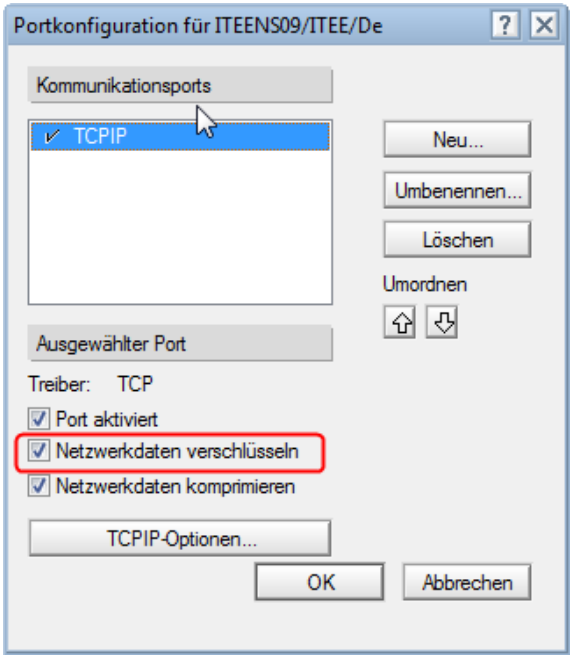
- Port 25: SMTP unverschlüsselt
- Port 465: SMTP mit SSL/TLS
- Port 587: SMTP mit STARTTLS
- Am Ende ist es völlig egal WELCHEN Port man nimmt. Es kommt immer SSL/TLS und SMTP zum Einsatz. Es wird historisch bedingt nur völlig durcheinander verwendet und vor allem bezeichnet. Wir geben verschiedene Ports an, auch weil Mailrpogramme 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 kramphaft 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

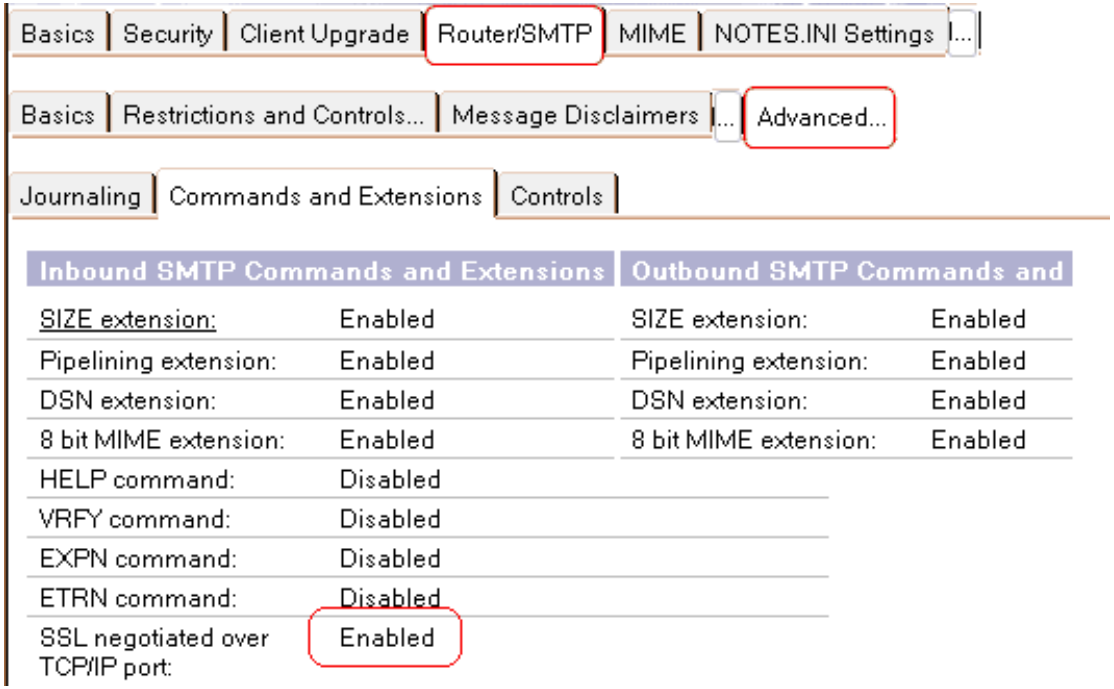
Transportverschlüsselung in Domino aktivieren - NRPC





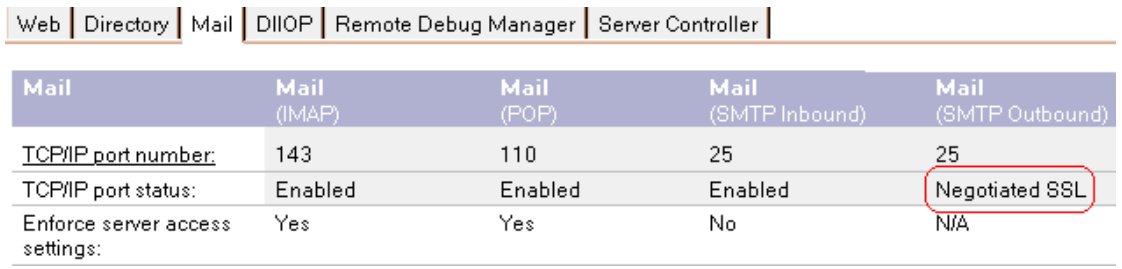
Transportverschlüsselung in Domino aktivieren SMTP Inbound

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.



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.



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-Mai 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 (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?

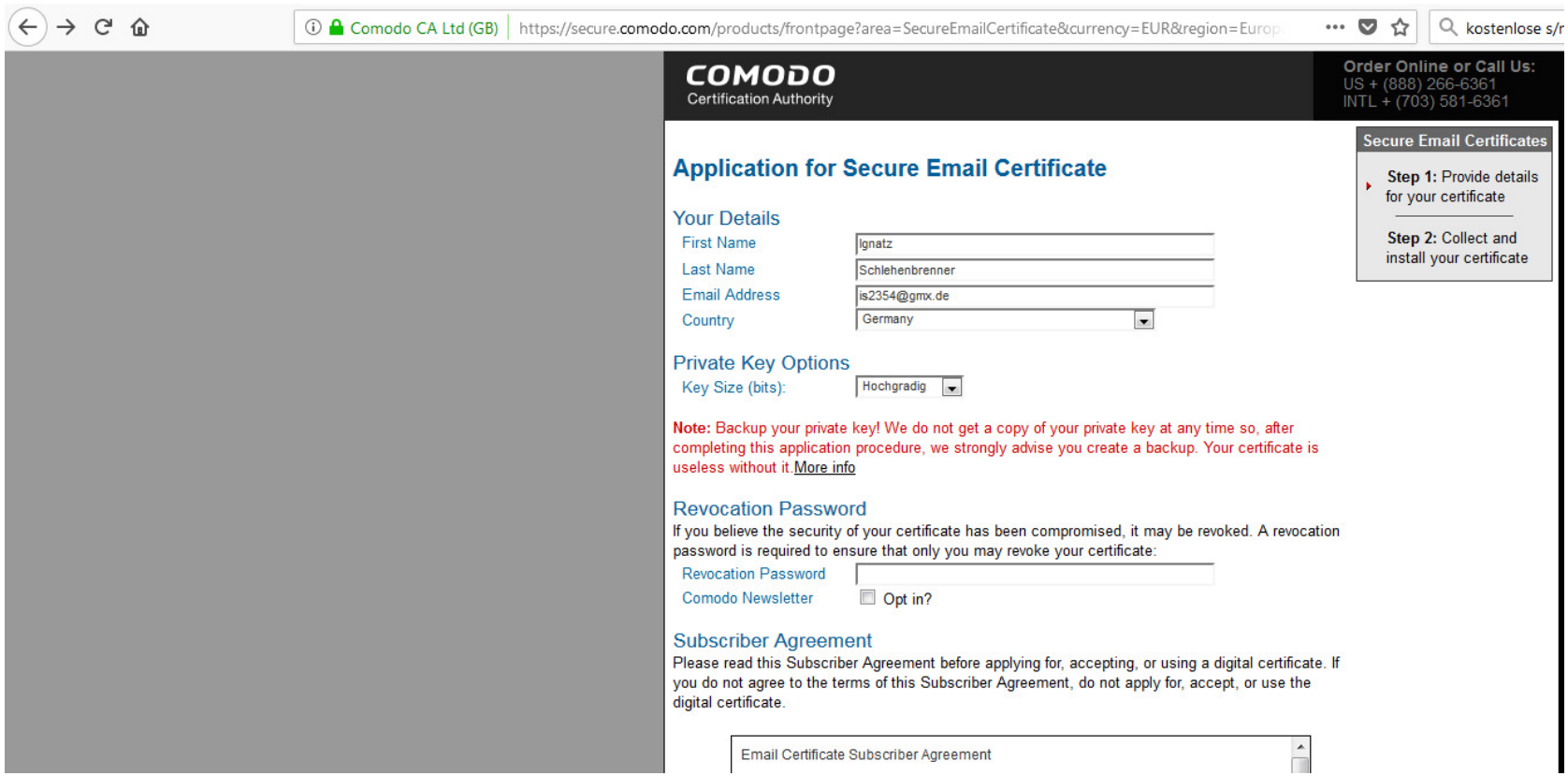
- Mein Schlüsselpaar (privater und öffentlicher Schlüssel)
- <meinSchlüssel>.p12
- Den öffentlichen Schlüssel des Empfängers
- Die richtigen Einstellungen am Client-Programm
- Die Einstellung zum Signieren bzw. Verschlüsseln

Woher bekomme ich mein S/MIME-Zertifikat? 1

- Suche nach
  „(kostenlose) smime zertifikate“

Woher bekomme ich mein S/MIME-Zertifikat? 2

- Auf der comodo-Seite:



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.

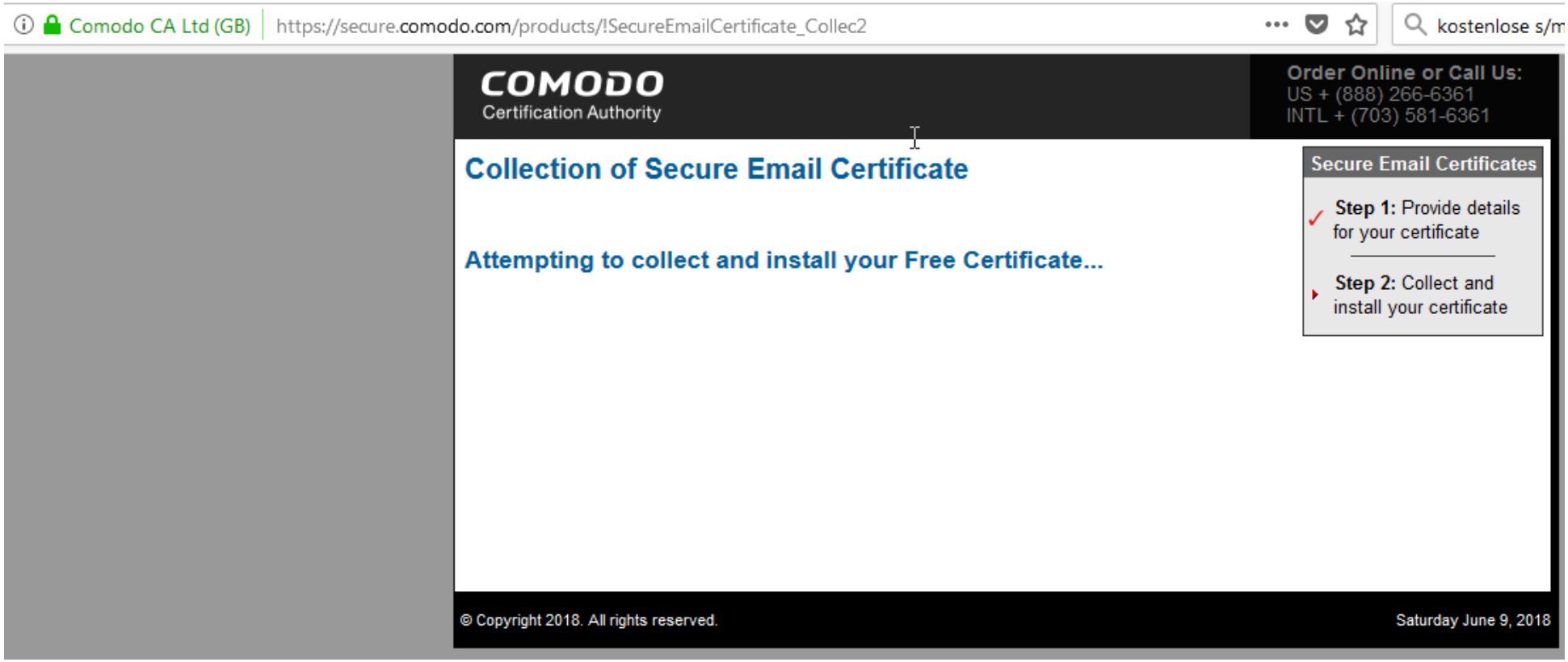
Your free Secure Email Certificate will then be installed. Please visit www.comodogroup.com/support for guidance on configuring your email client to use your certificate to secure email.

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):



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.

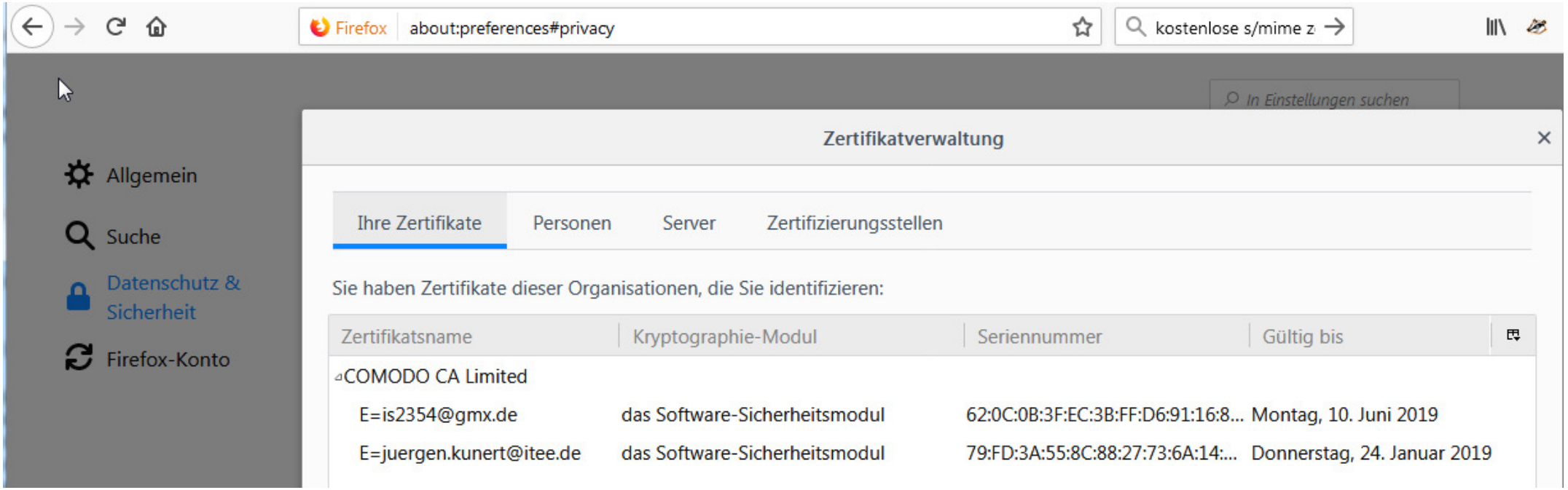
Die CAs versprechen, dass der private Schlüssel im Browser des Nutzers generiert wird und nicht auf den Server der CA hochgeladen wird. Es ist aber für die CA möglich, den privaten Schlüssel unbemerkt zu kompromittieren.

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 Downloac
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.

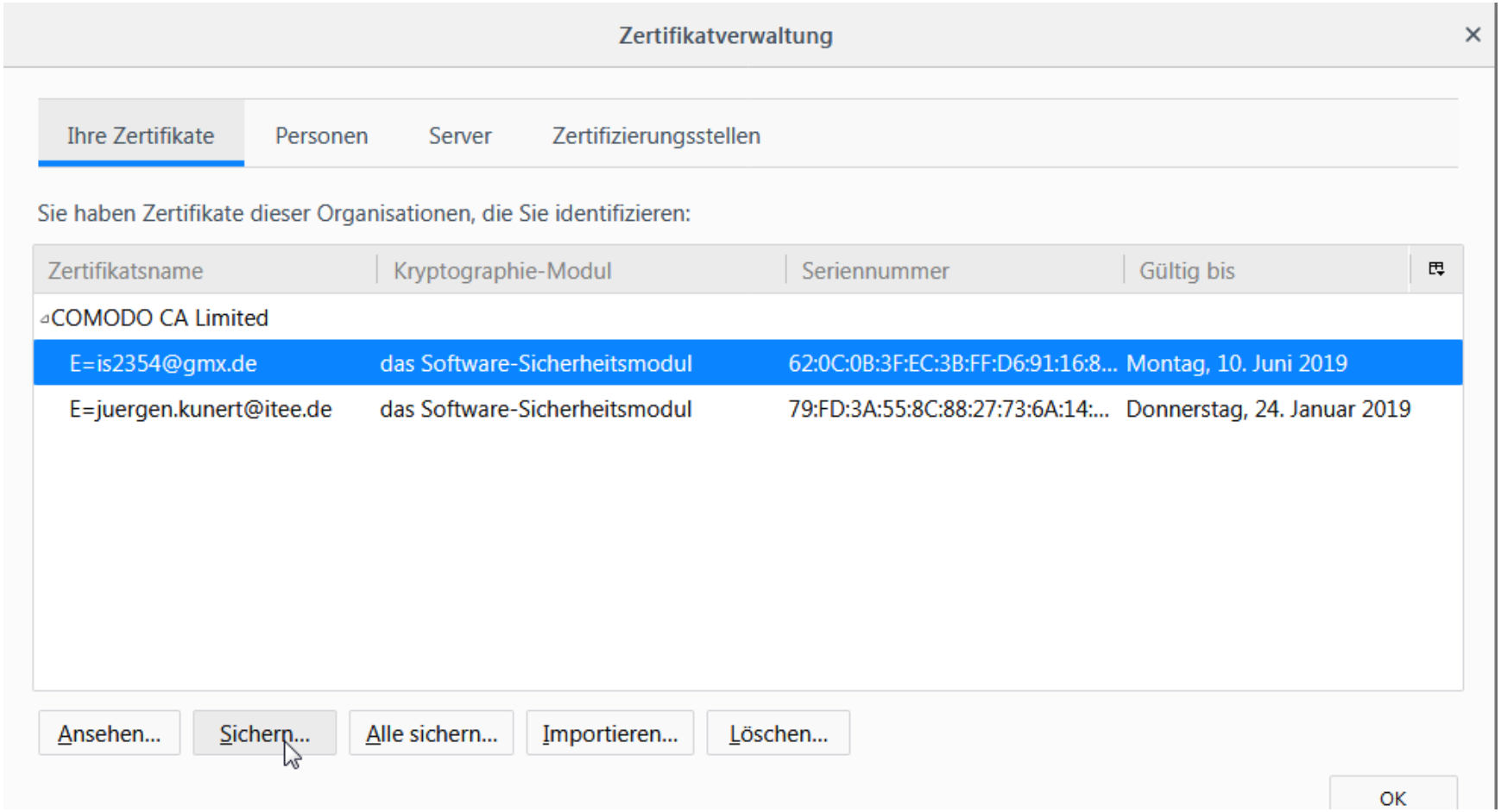
Woher bekomme ich mein S/MIME-Zertifikat? 5

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



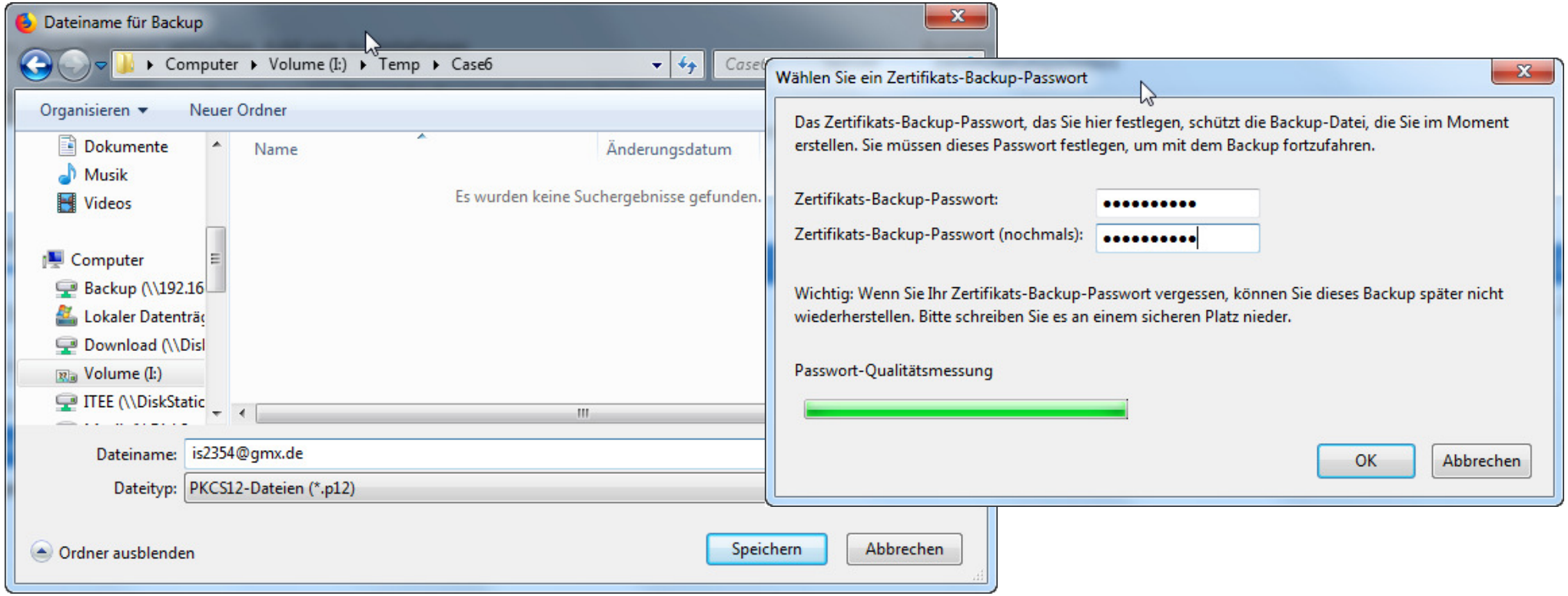
Woher bekomme ich mein S/MIME-Zertifikat? 6

- Zertifikat exportieren:



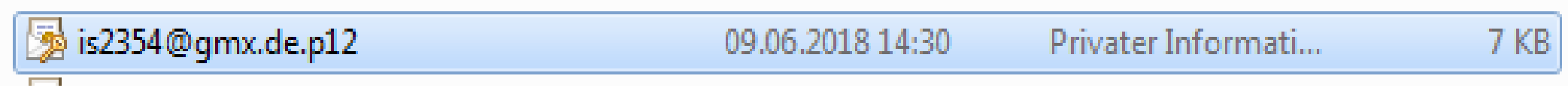
Woher bekomme ich mein S/MIME-Zertifikat? 7

- Zertifikat exportieren:



Woher bekomme ich mein S/MIME-Zertifikat? 9

Zertifikat in Datei:



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

- Sichern vor unberechtigtem Zugriff!

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

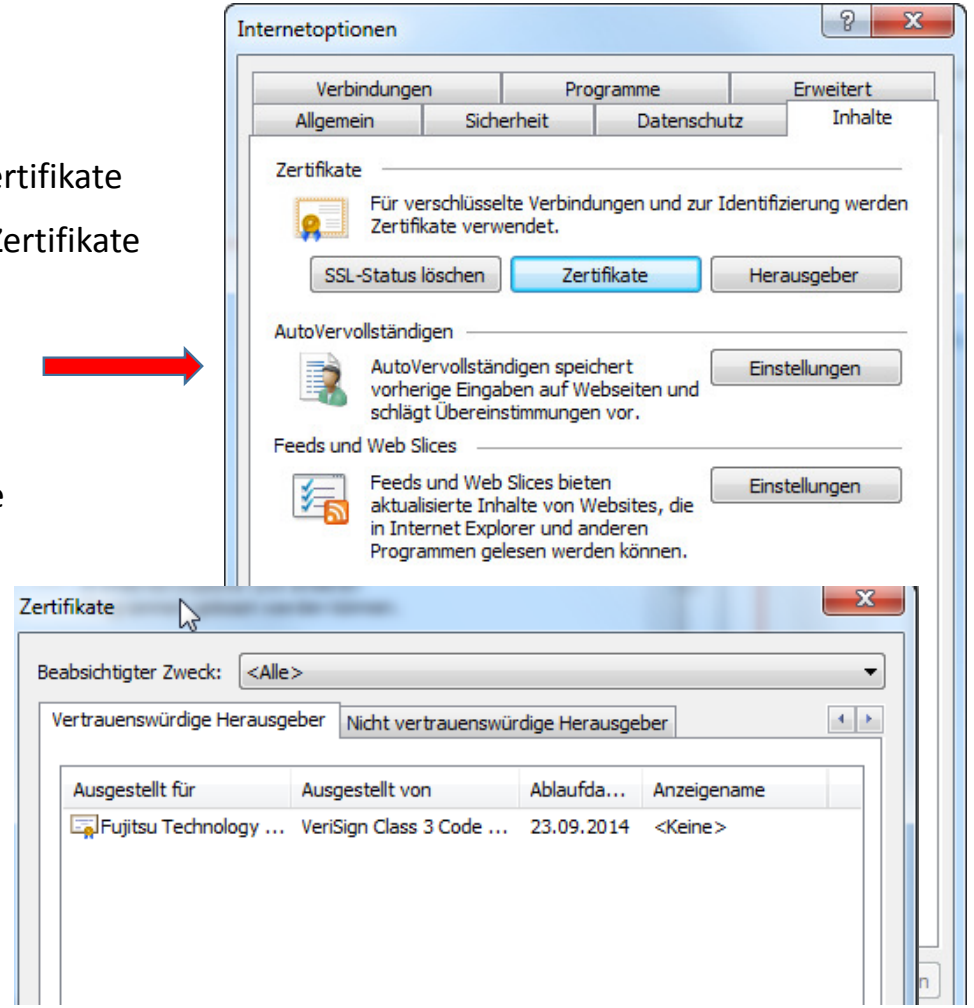
- Backup!

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

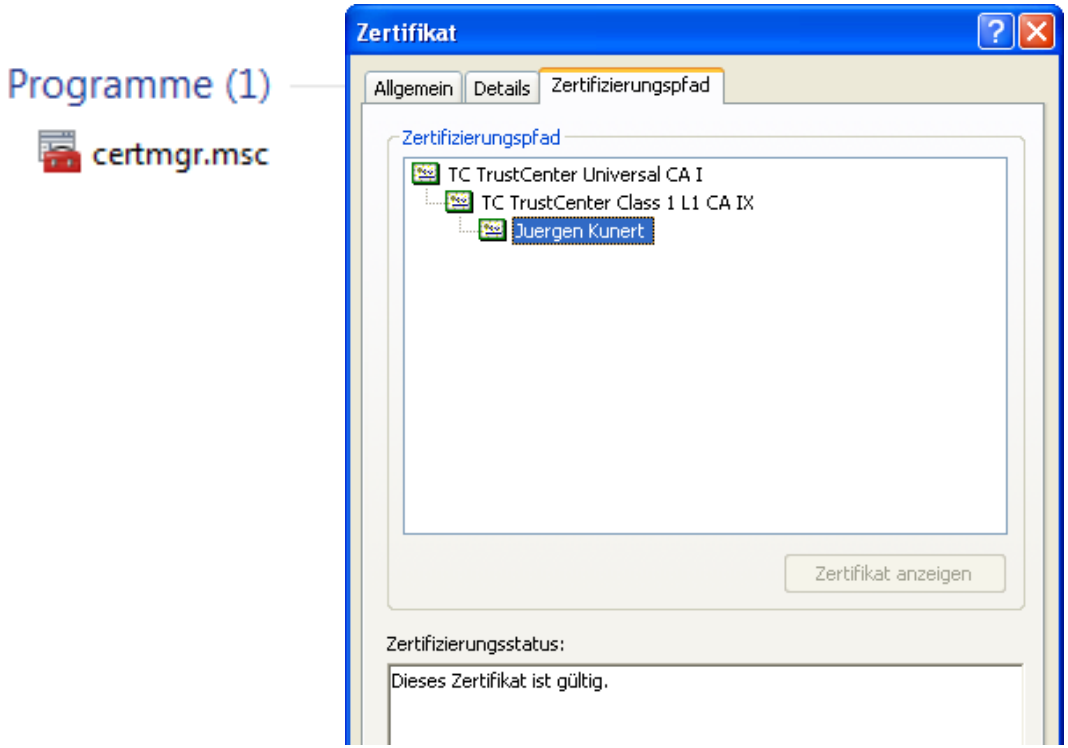
Wo werden Zertifikate gespeichert?

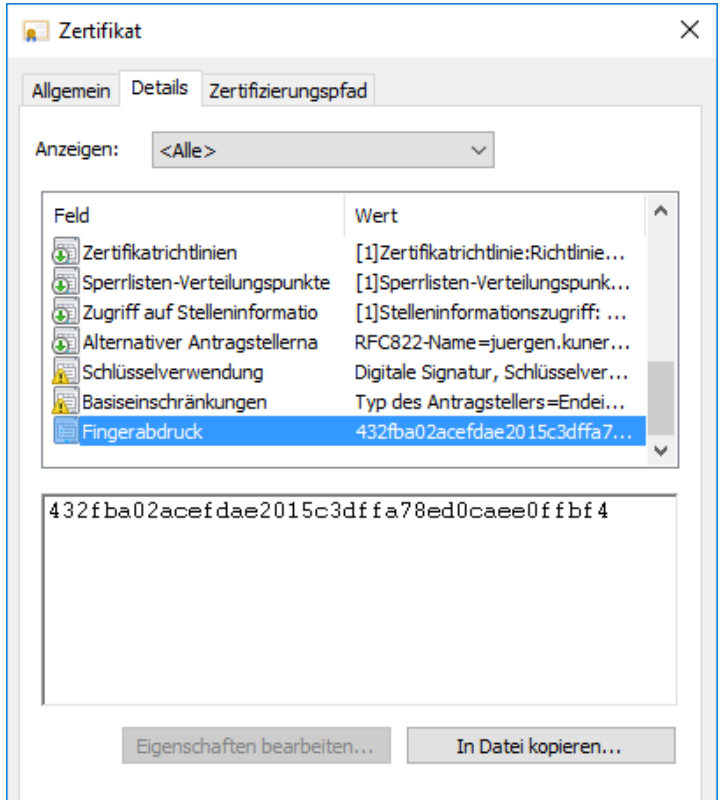
- Notes & Domino: Adressbücher (fremde Zertifikate)
- Notes: ID-File (eigenes Zertifikat)
- Firefox: intern -> Einstellungen -> Datenschutz und Sicherheit -> Zertifikate
- Chrome: intern -> Einstellungen -> Datenschutz und Sicherheit -> Zertifikate
- Edge: Windows-Zertifikatsspeicher
- Safari: Mac OS 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

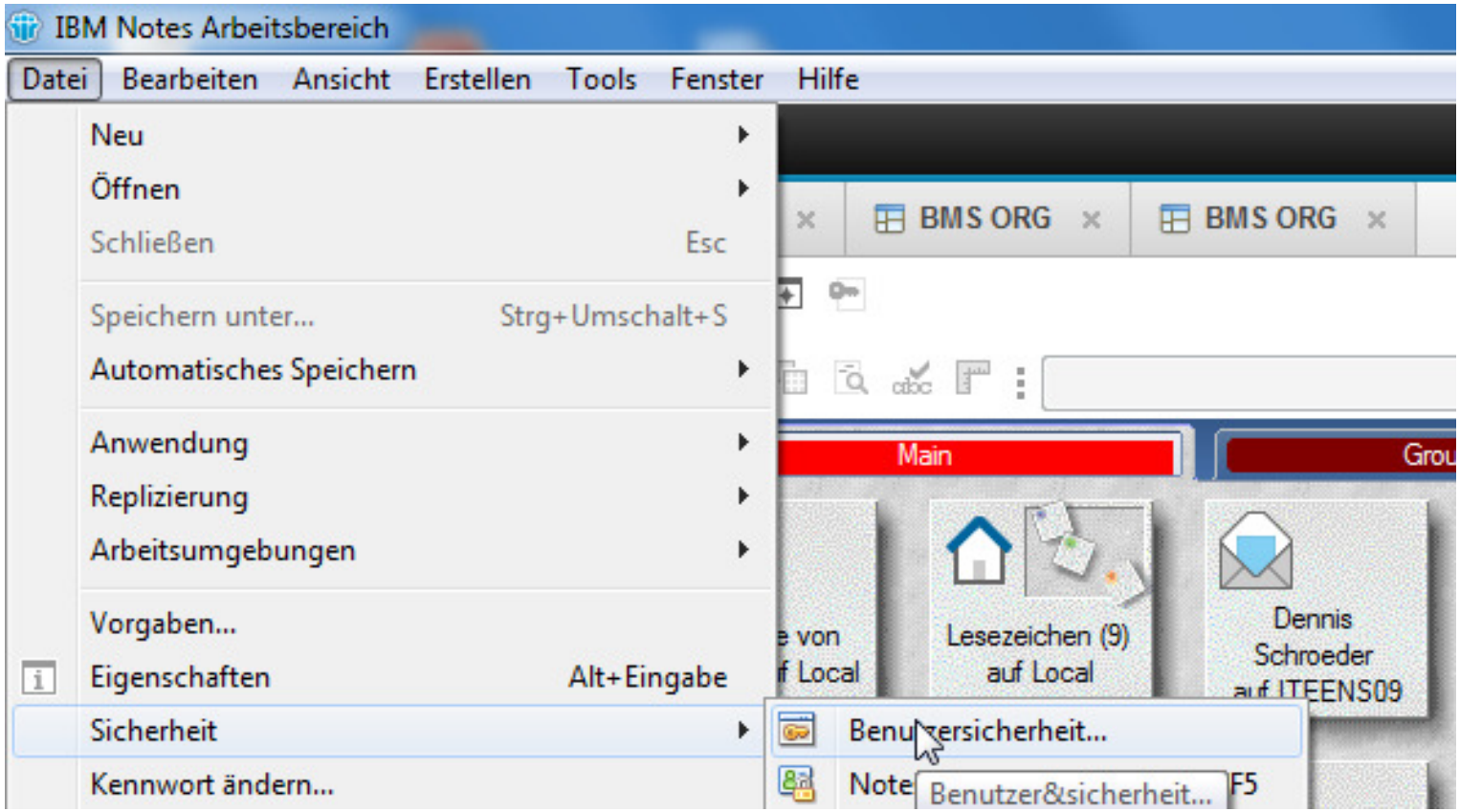




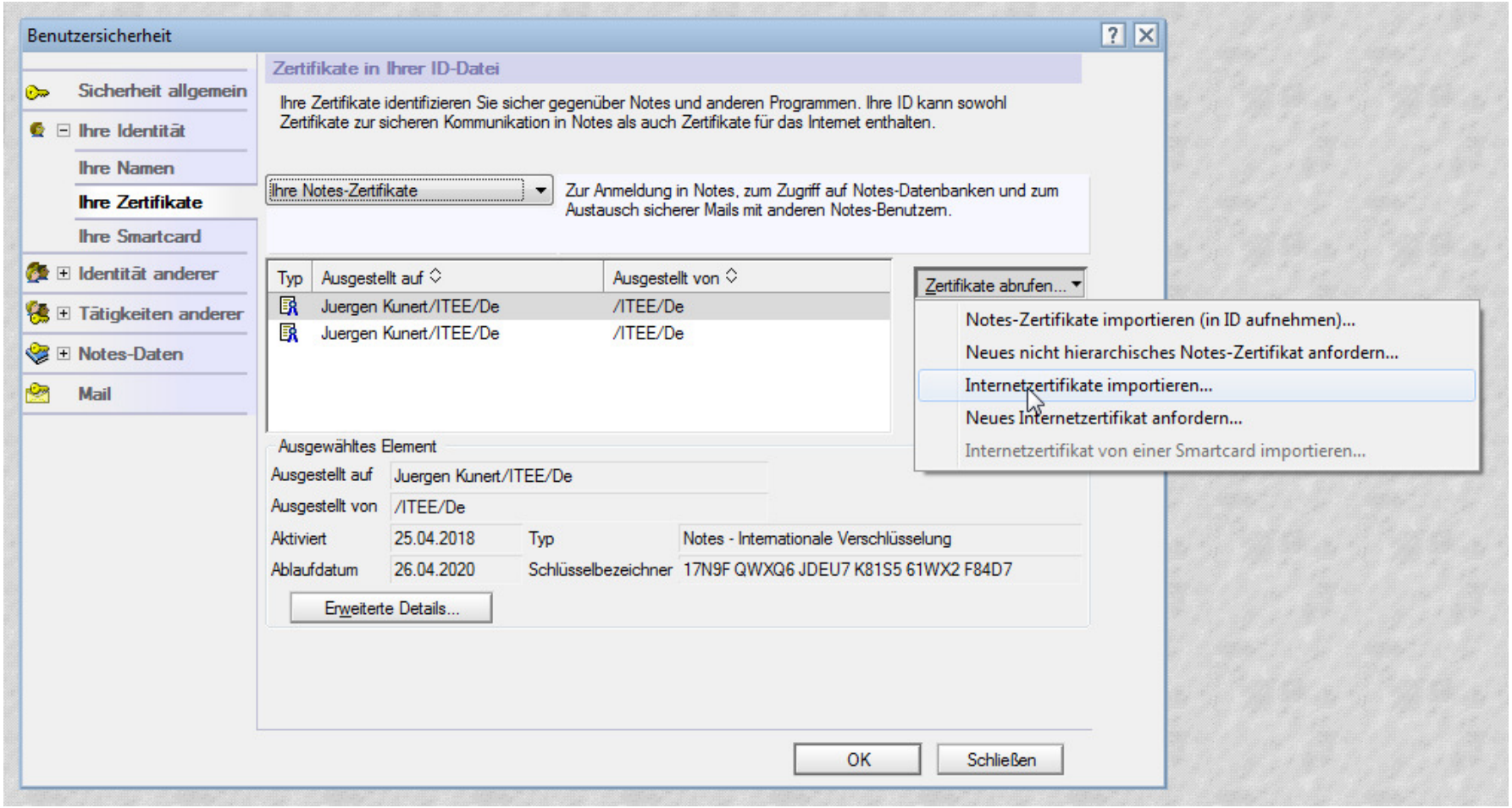
S/MIME-Verschlüsselung im Client-Programm mit Bordmitteln

- 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

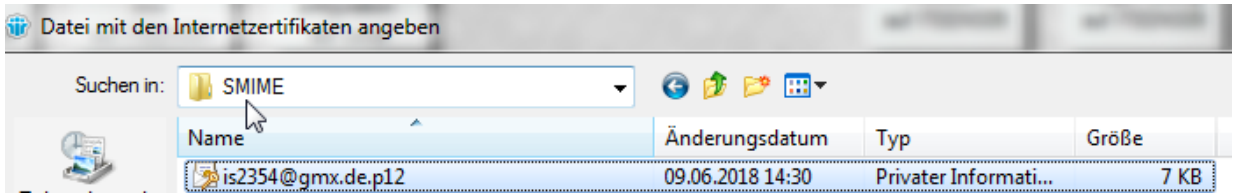
Wie installiere ich ein S/MIME-Zertifikat in Notes? 1

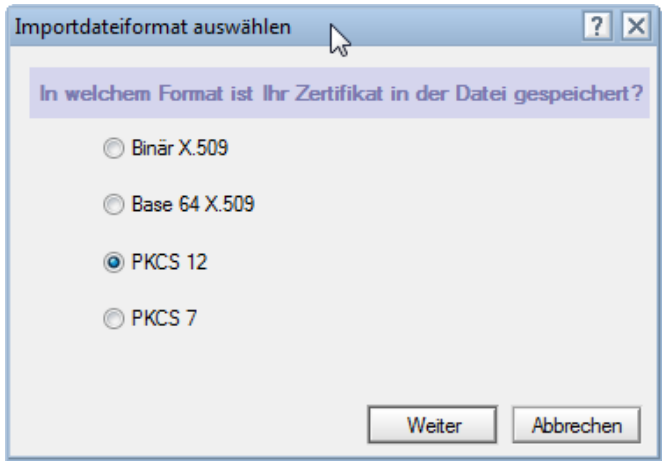


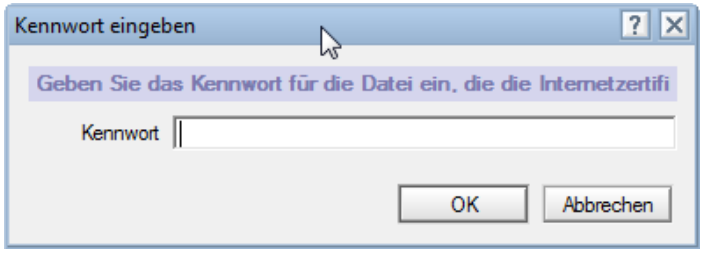
Wie installiere ich ein S/MIME-Zertifikat in Notes? 2



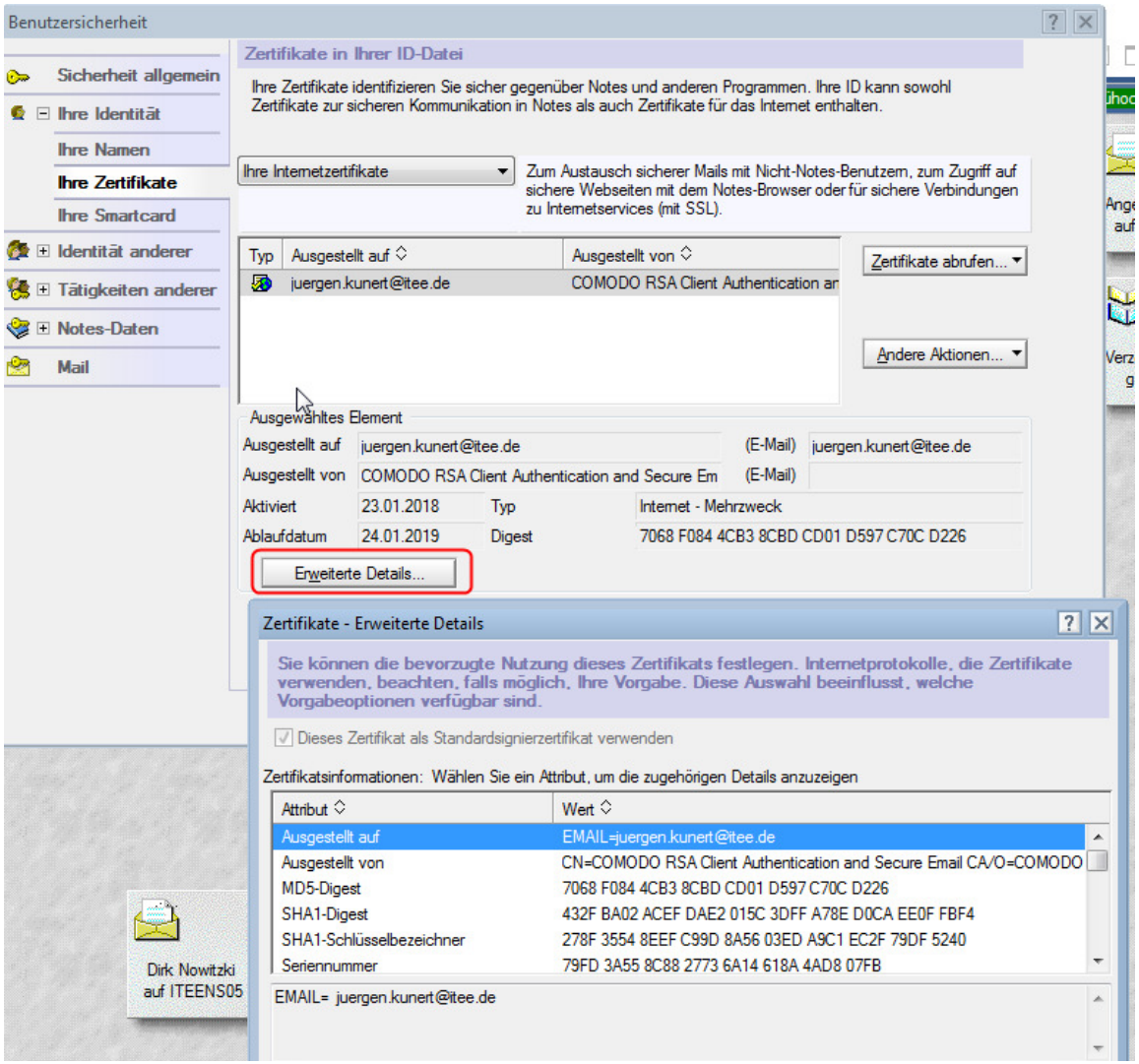
Wie installiere ich ein S/MIME-Zertifikat in Notes? 3







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

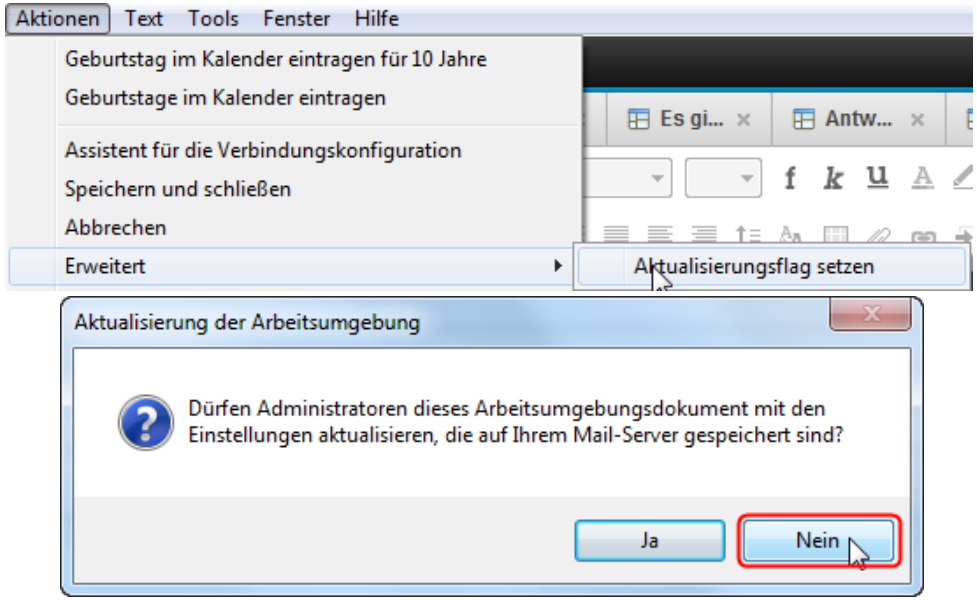


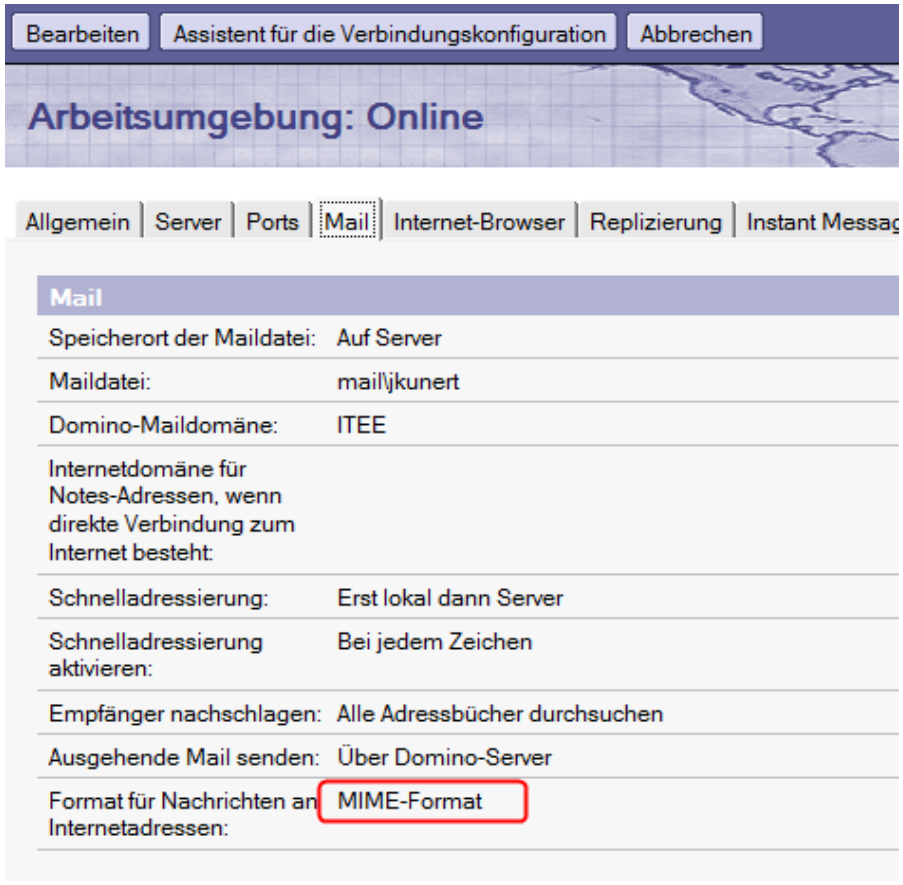
Was kann ich jetzt damit machen?

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

Notes-Konfiguration Arbeitsumgebung

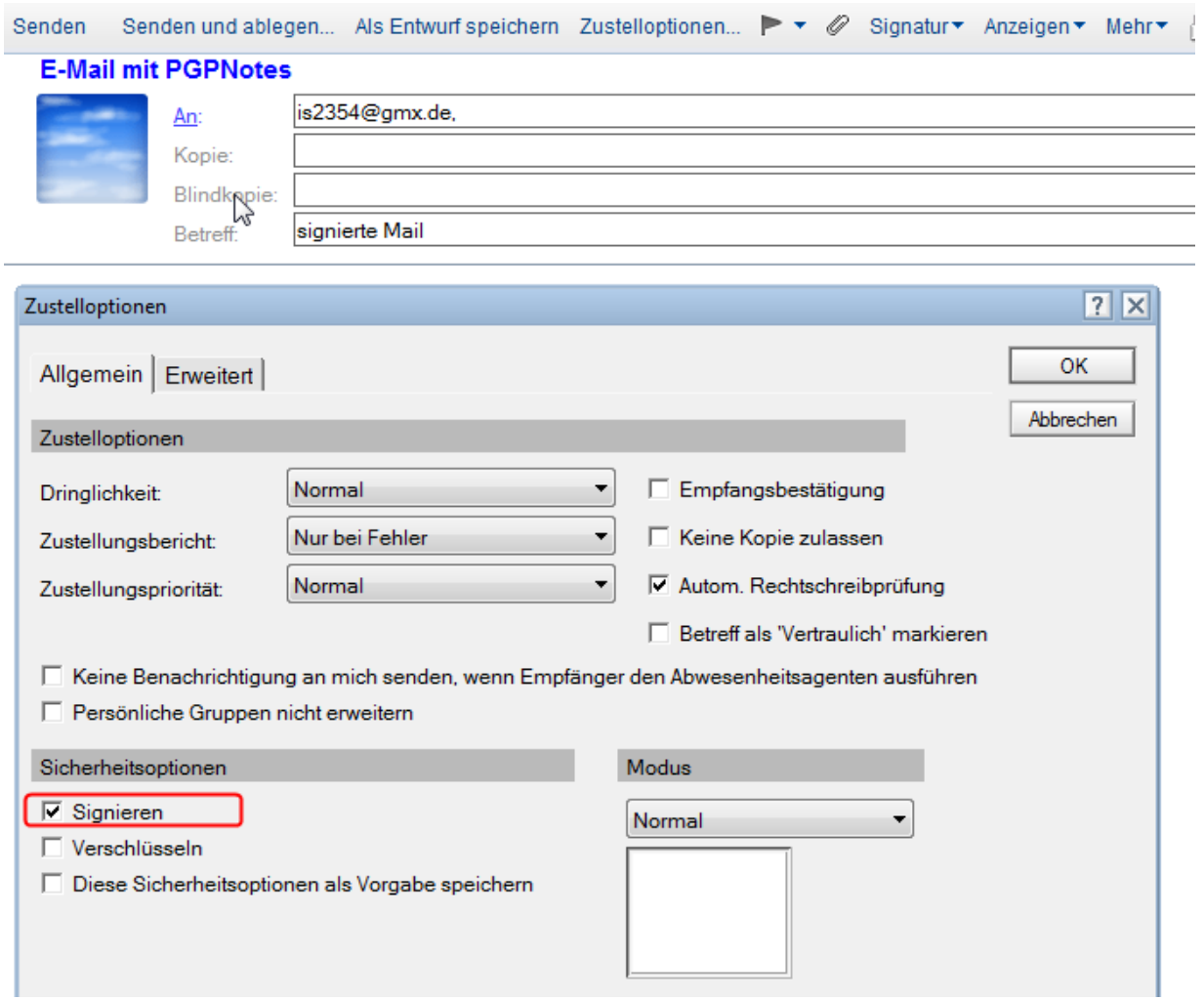
- Ohne MIME geht es nicht
  und es kommen auch keine
  Fehlermeldungen!
- Achtung:
  Ggf. Kollision mit anderen
  Zusatzprogrammen (Signatur, …)





Was kann ich jetzt damit machen?

- Ich kann signierte eMails senden
- und meinen öffentlichen Schlüssel



eMail-Verschlüsselung mit Bordmitteln

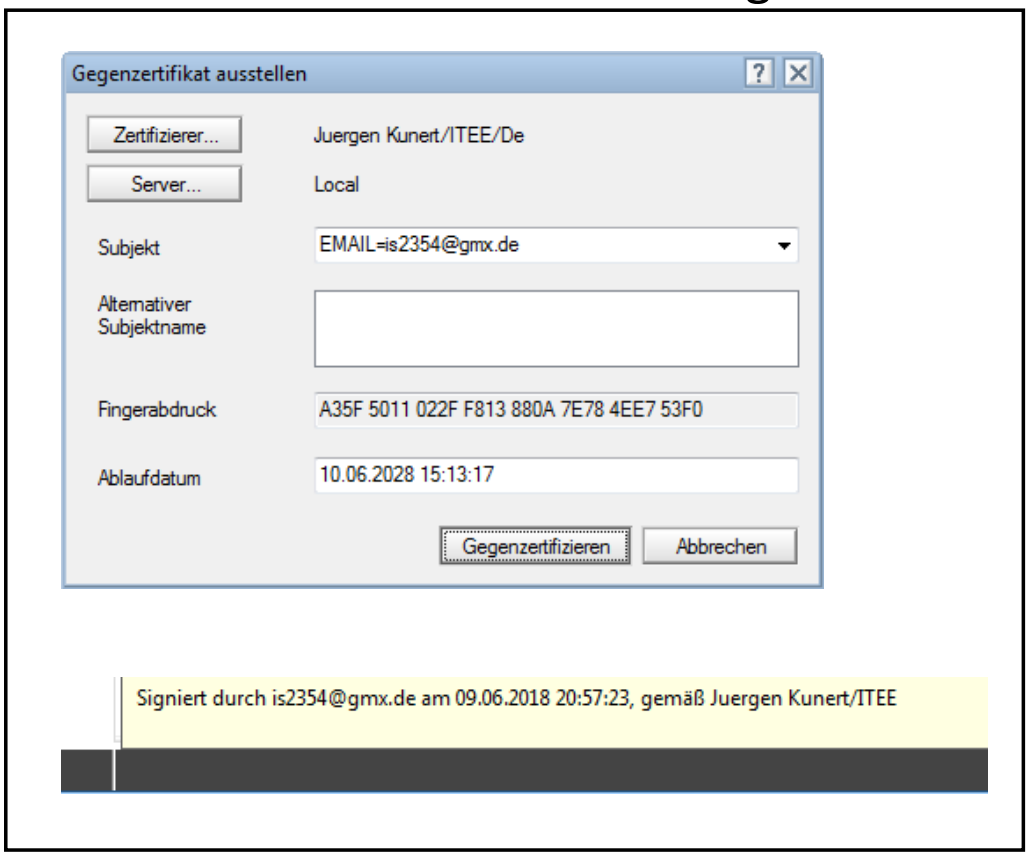
- Was brauche ich?
- Wie richte ich meinen Notes-Client ein?
- Was braucht die Gegenseite?
- Signierte und verschlüsselte Mails austauschen
  - Signierte Mail empfangen
  - Signierte Mail senden
  - Verschlüsselte Mail empfangen
  - Verschlüsselte Mail senden

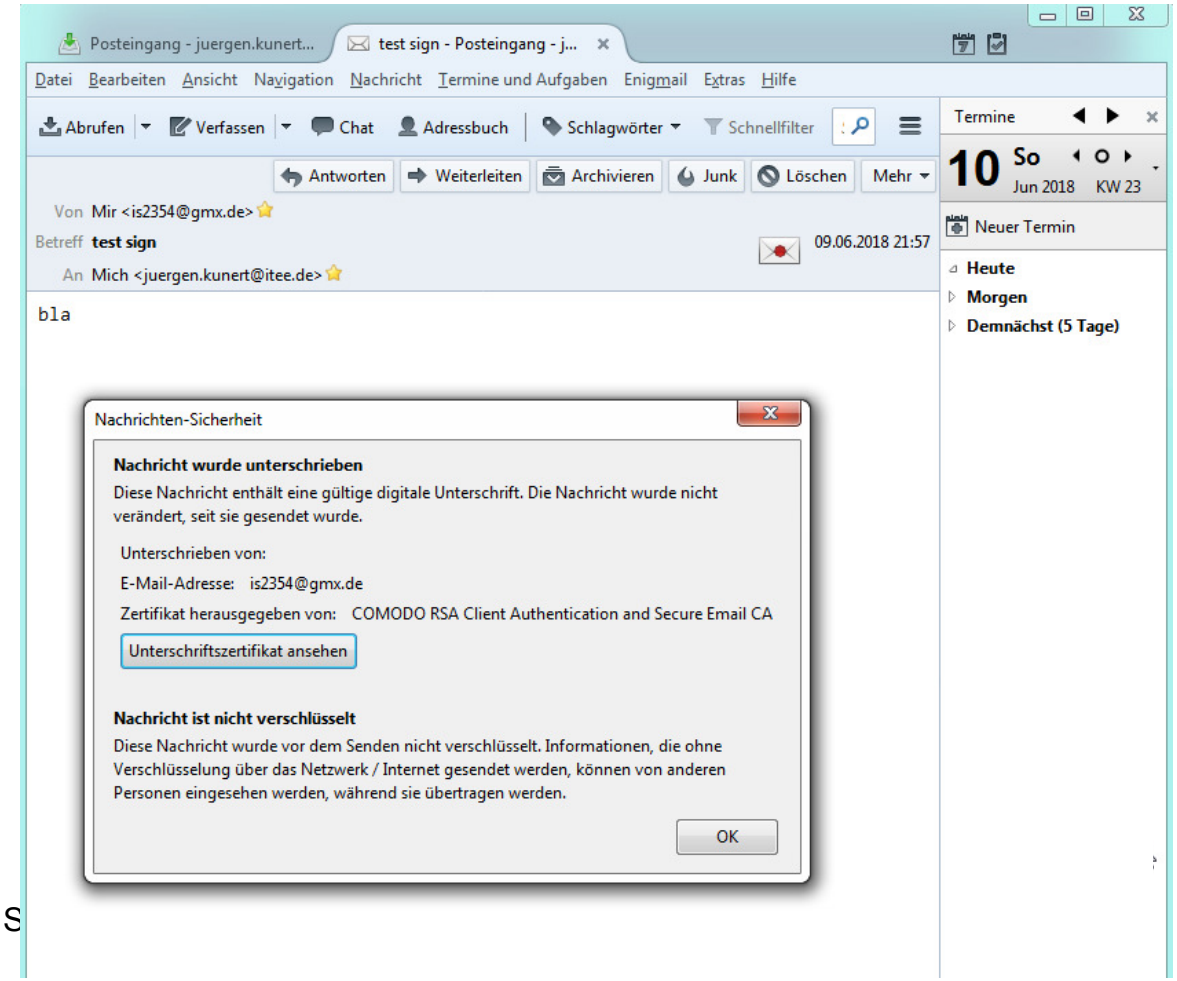
Wie bekommt der Empfänger meinen öffentlichen Schlüssel?

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

Wie sieht das beim Empfänger aus?

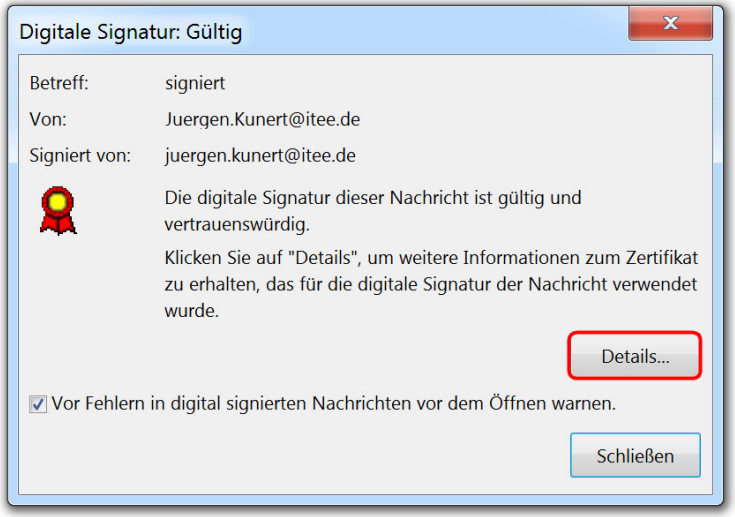
- Ich sende eine von mir signierte eMail



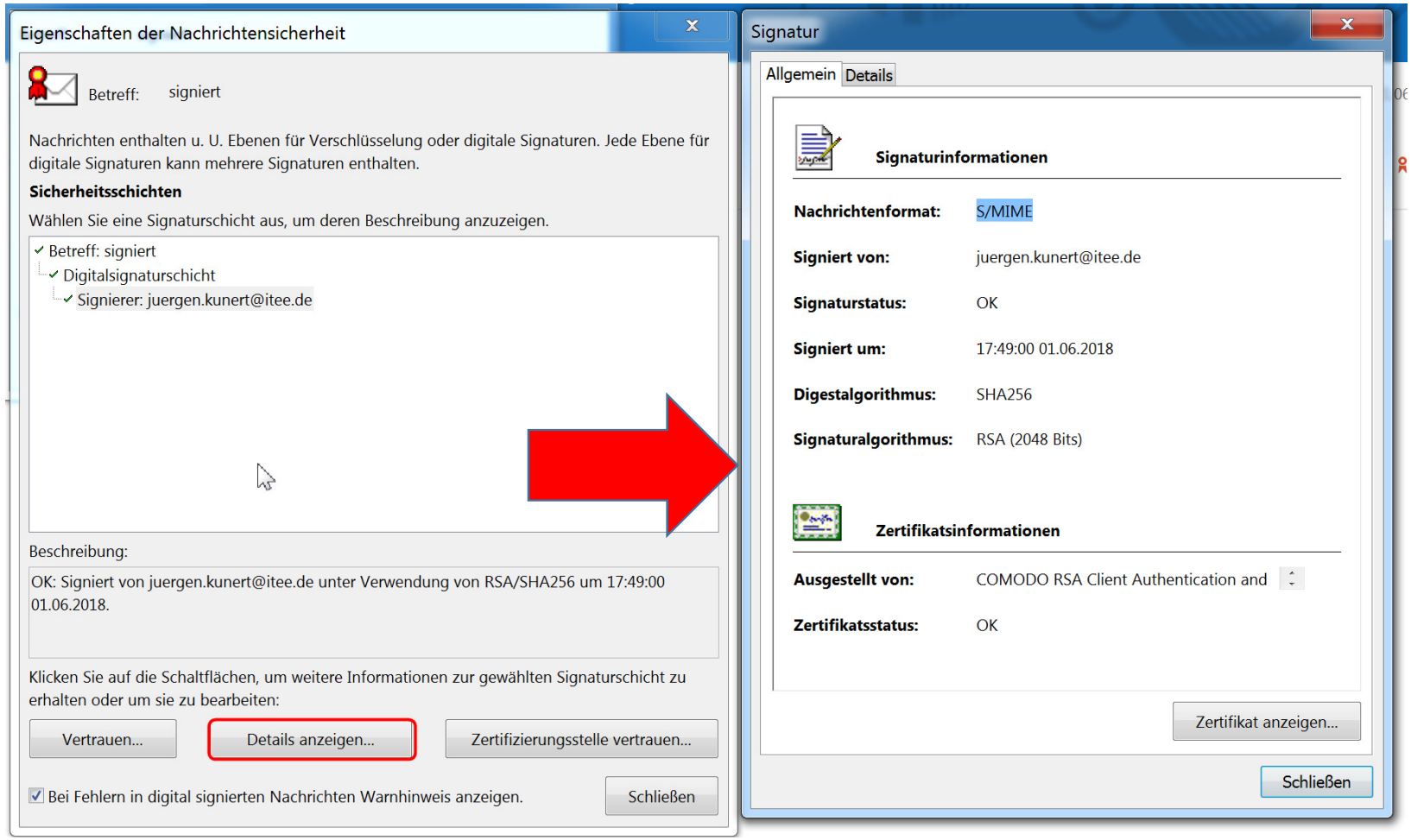


Wie sieht das beim Empfänger in Outlook aus? 1

- Ich sende eine von mir signierte eMail



Wie sieht das beim Empfänger in Outlook aus? 2



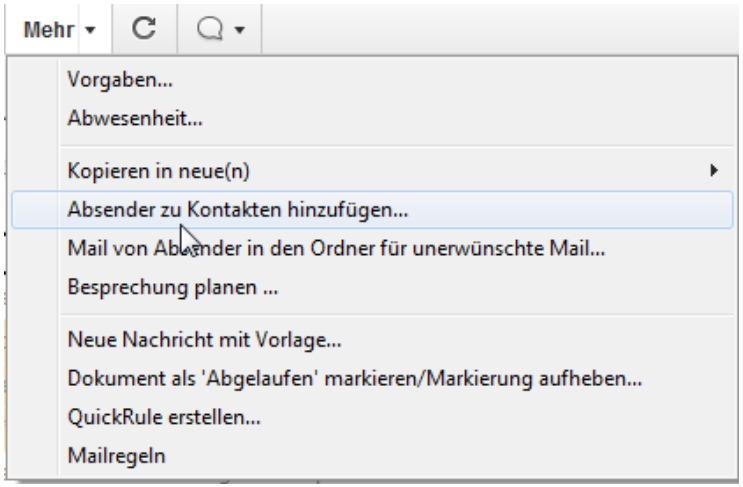
Was braucht die Gegenseite?

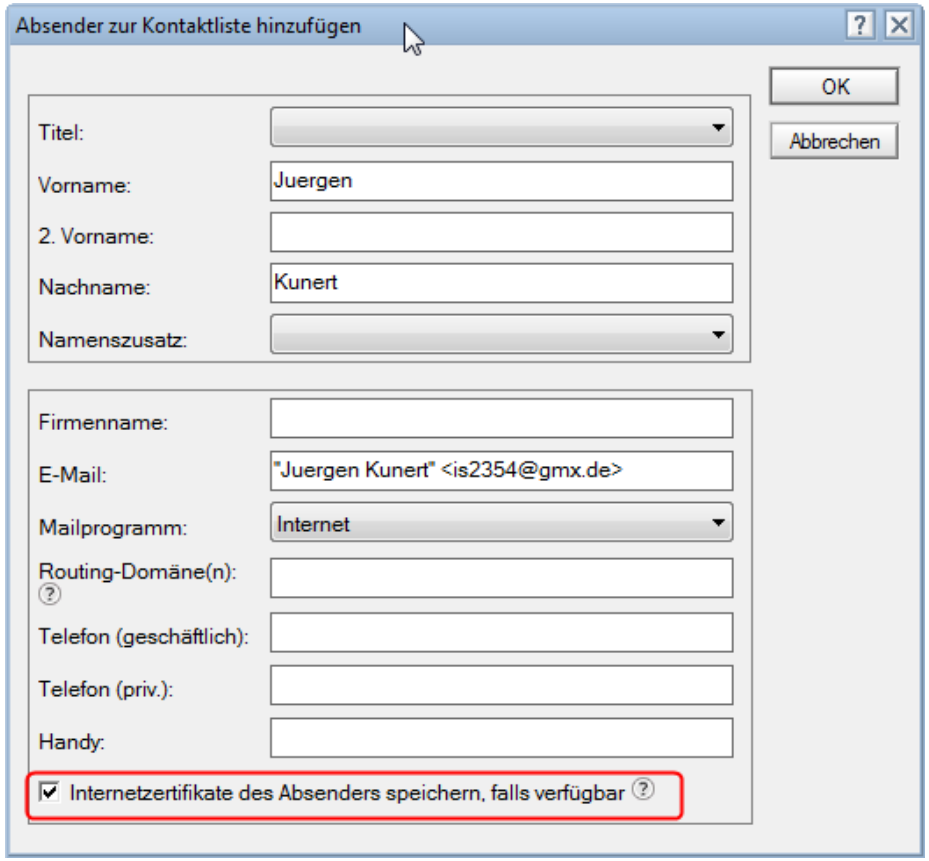
- Ihr/sein Schlüsselpaar (privater und öffentlicher Schlüssel)
- meinen öffentlichen Schlüssel (Schlüssel des Empfängers)
- Die richtigen Einstellungen in seinem Mail-Client

Wie richte ich meinen Notes-Client ein?

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

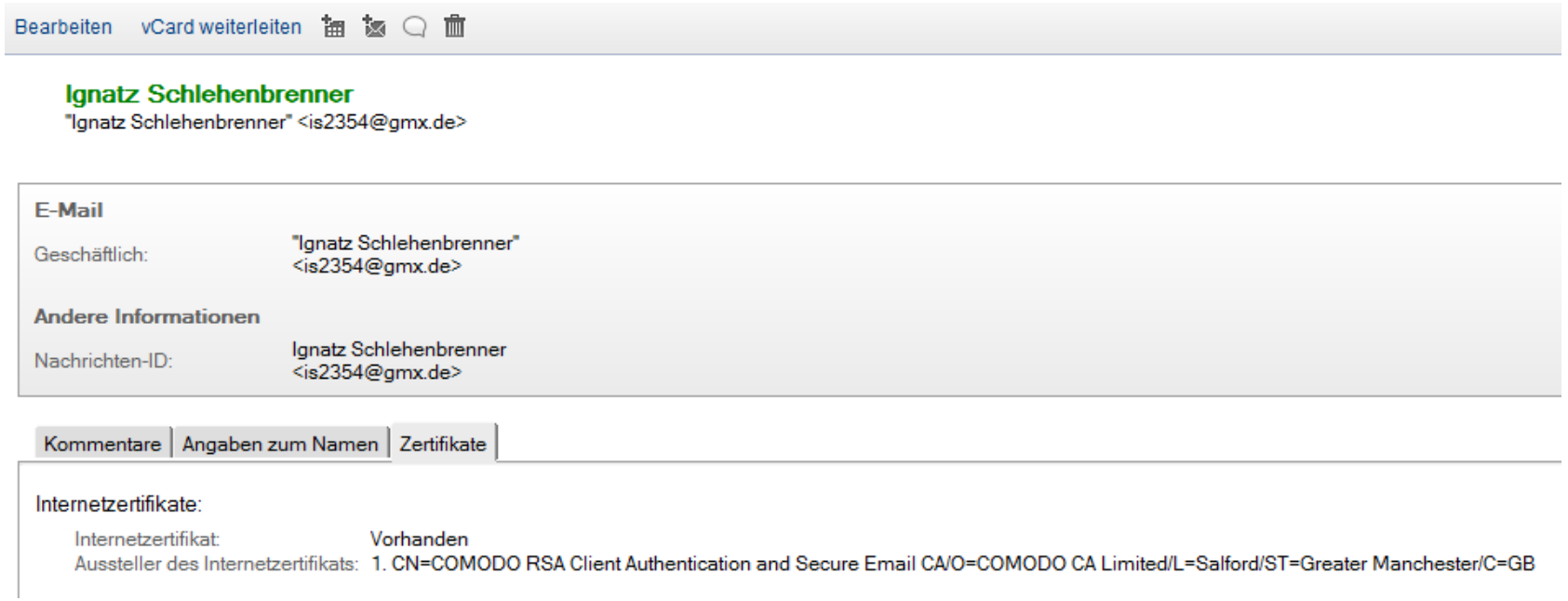
Kontakt und Schlüssel in Adressbuch importieren 1





Kontakt und Schlüssel in Adressbuch importieren 2

So sieht es dann im Adressbuch aus:



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

Was habe ich davon?

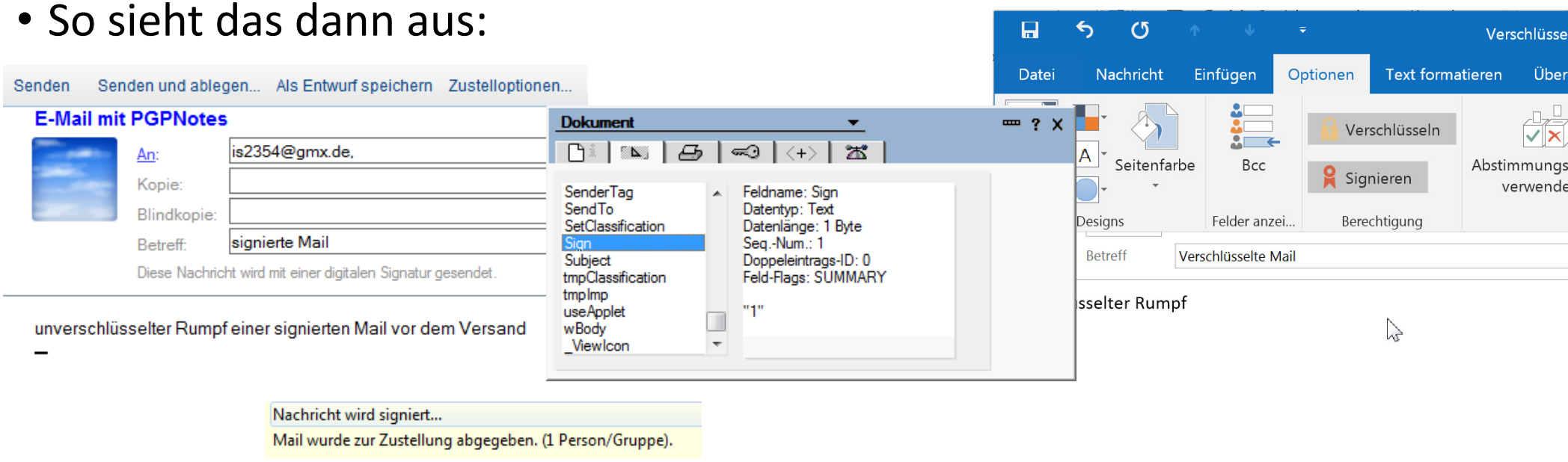
- Ich kann signierte Mails verschicken
- Ich kann Mails lesen, die mit meinem Public Key verschlüsselt sind

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

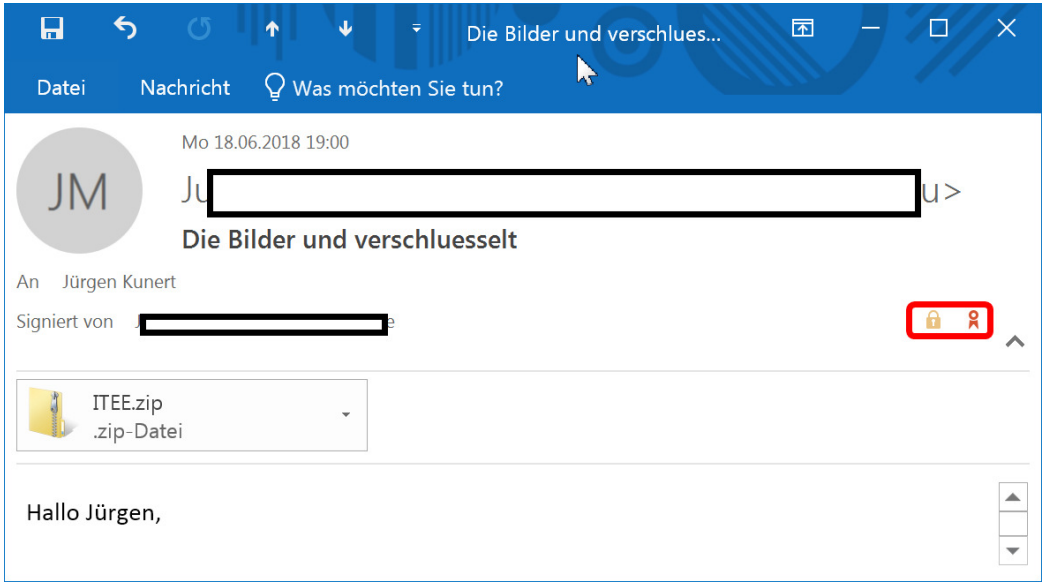
Signierte Mail senden

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



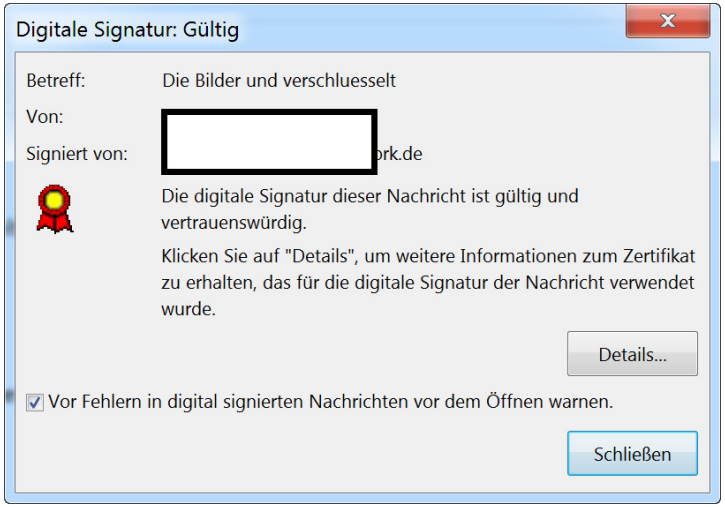
Signierte Mail empfangen

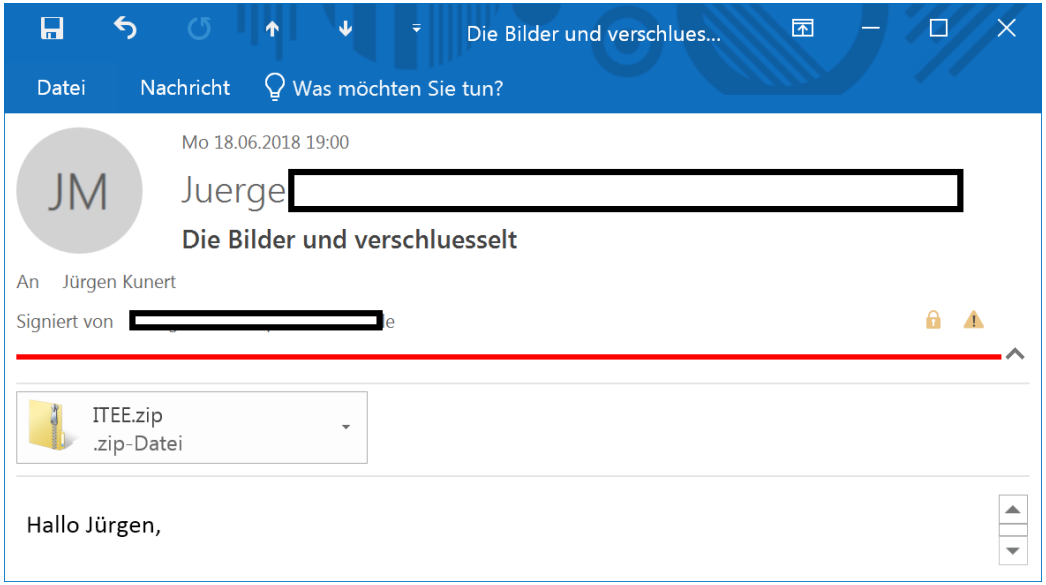
- Was habe ich davon?
  - Die eMail wurde von jemandem versendet, der Zugriff auf seinen privaten Schlüssel hatte
  - Wenn die Signatur intakt ist, wurde die eMail nicht verändert
- So sieht das dann aus:



Signierte Mail empfangen

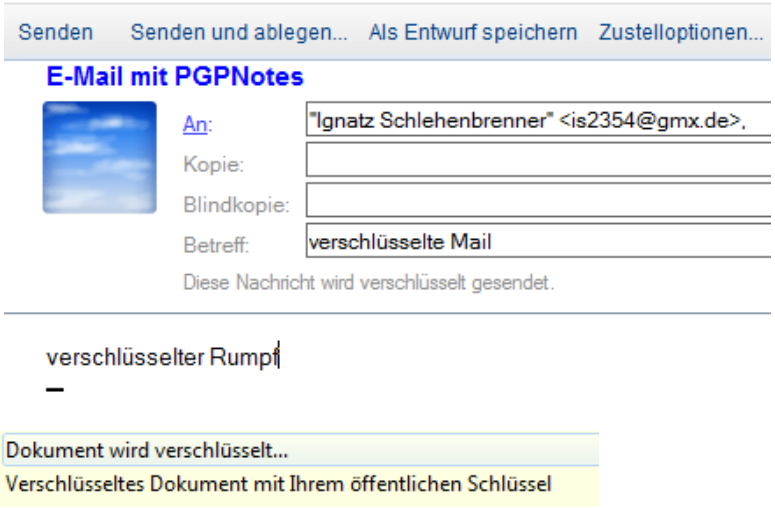
- Was habe ich davon?
  - Die eMail wurde von jemandem versendet, der Zugriff auf den privaten Schlüssel hatte
  - Wenn die Signatur intakt ist, wurde die eMail nicht verändert
- So sieht das dann aus:

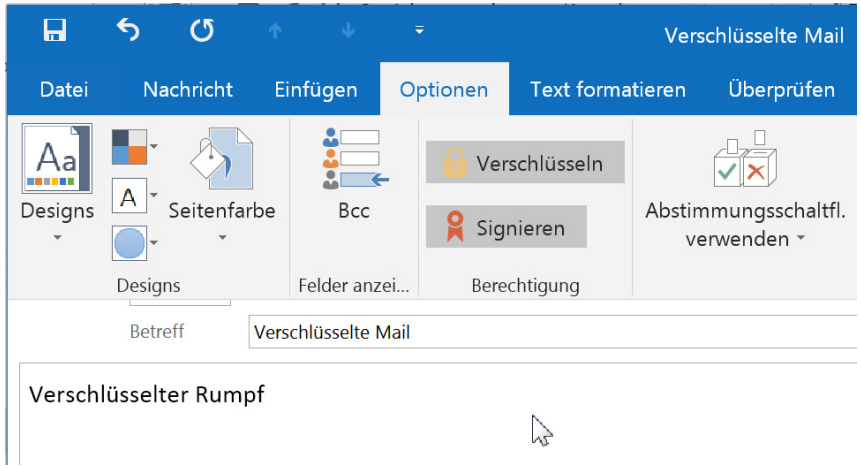




Verschlüsselte Mail senden

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

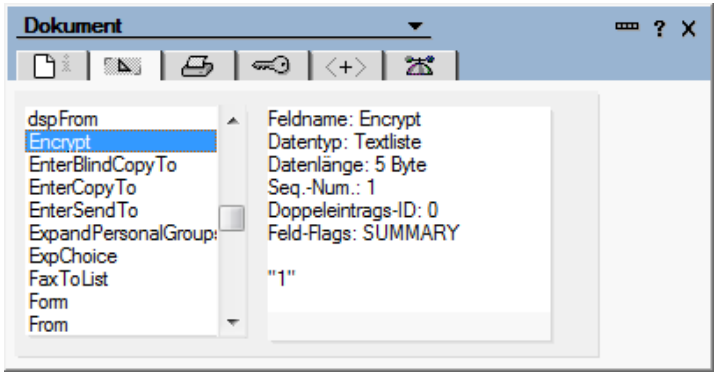




Richtig wäre: mit dem öffentlichen Schlüssel des Empfängers verschlüsselt

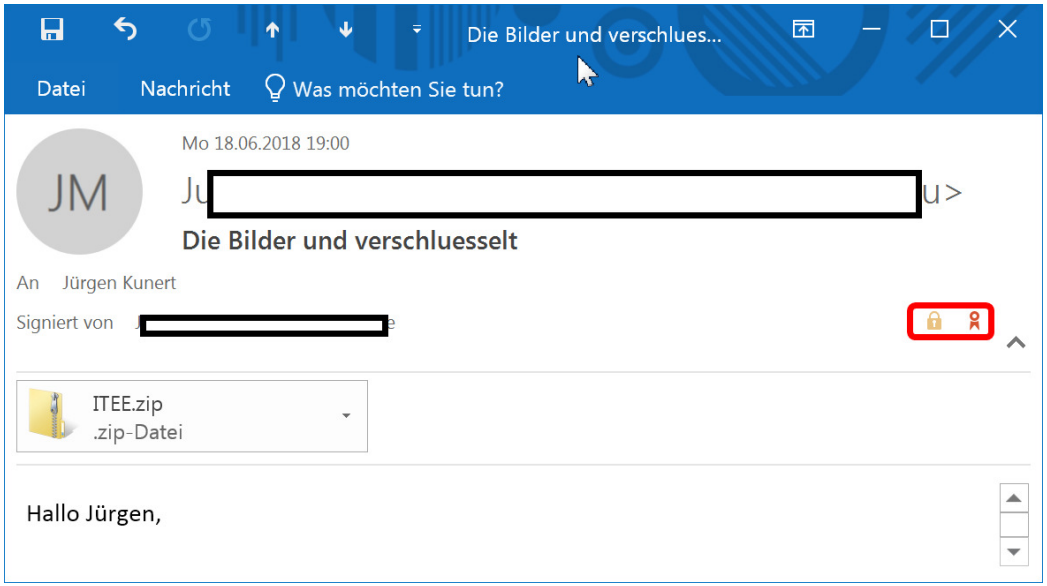
Verschlüsselte Mail empfangen

- 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:



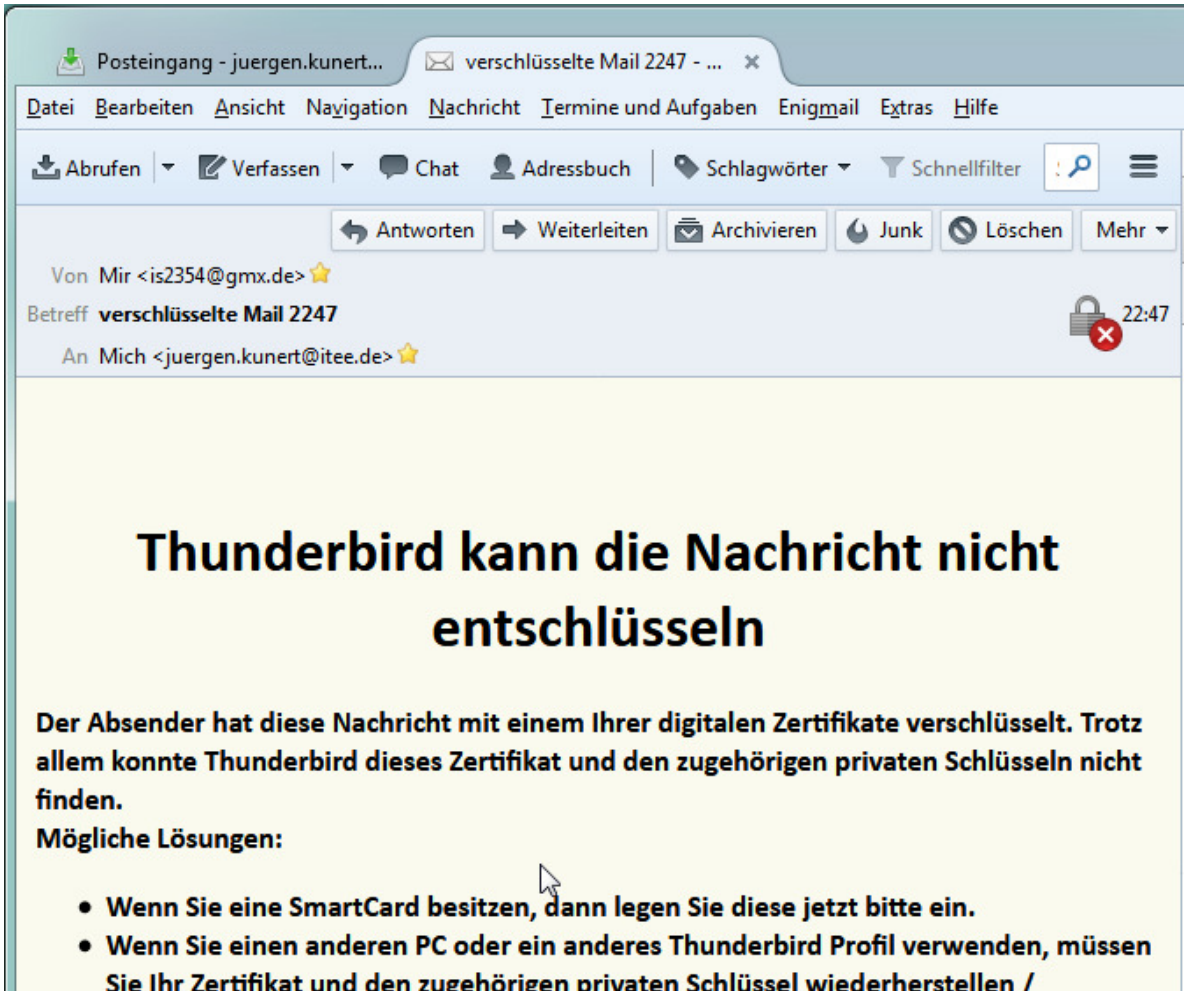
Verschlüsselte Mail in Outlook empfangen

- 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:



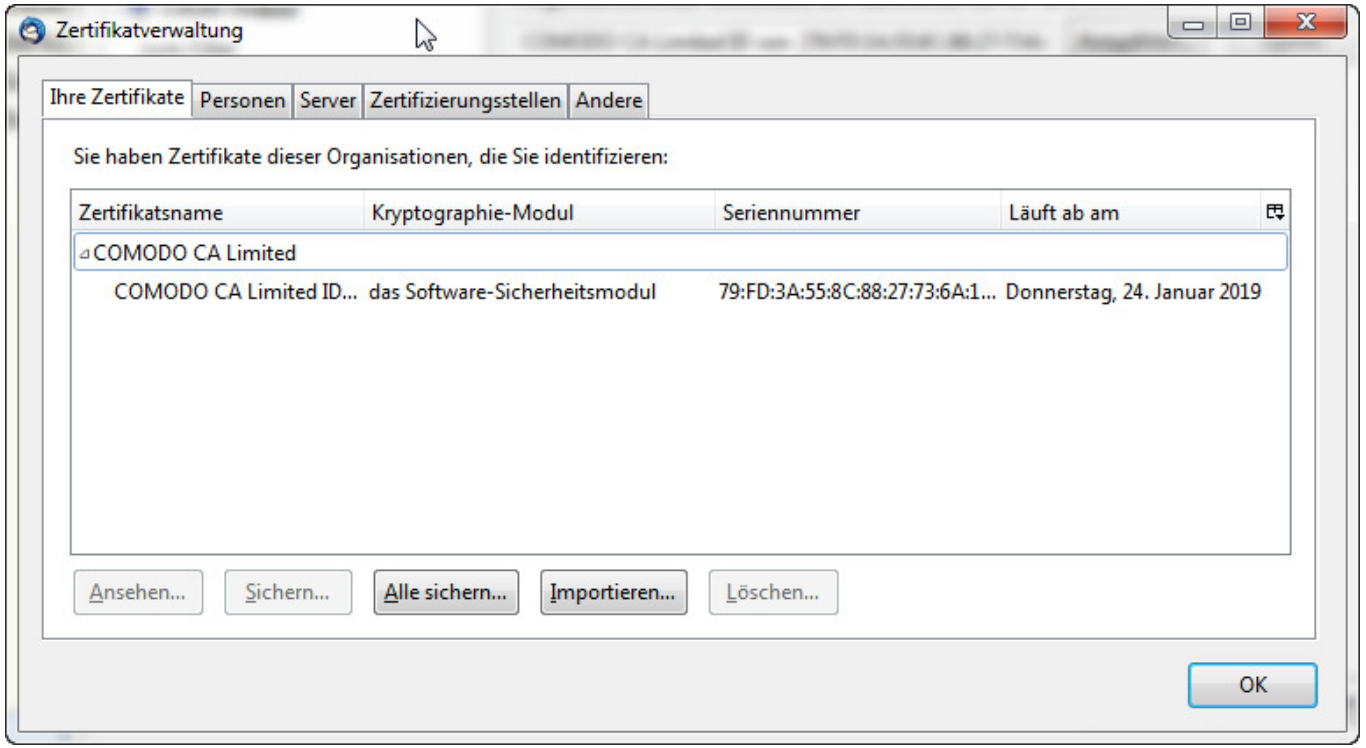
Das Selbe in Thunderbird

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



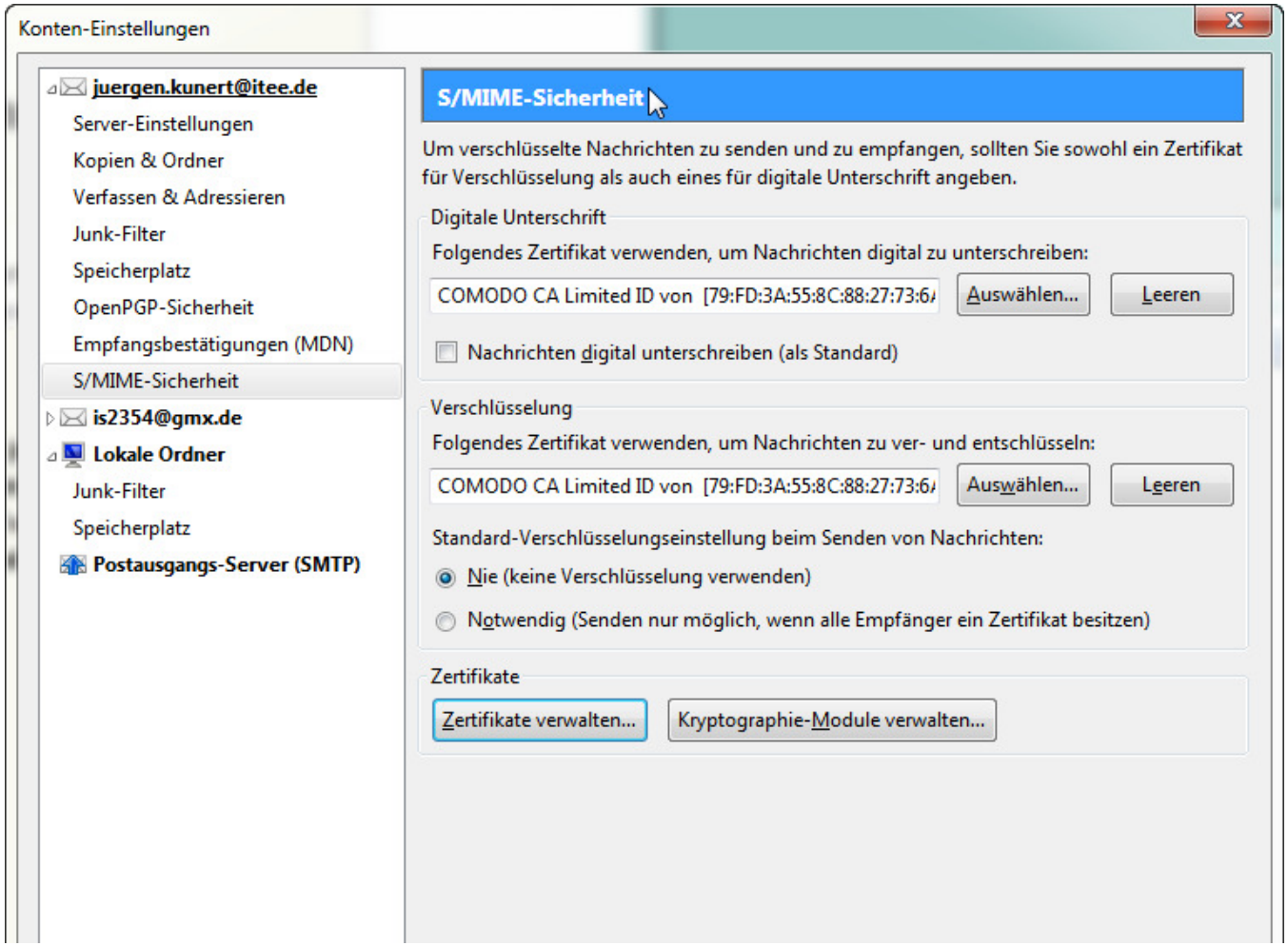
Das Selbe in Thunderbird

- Zertifikat in Zertifikatsverwaltung importieren



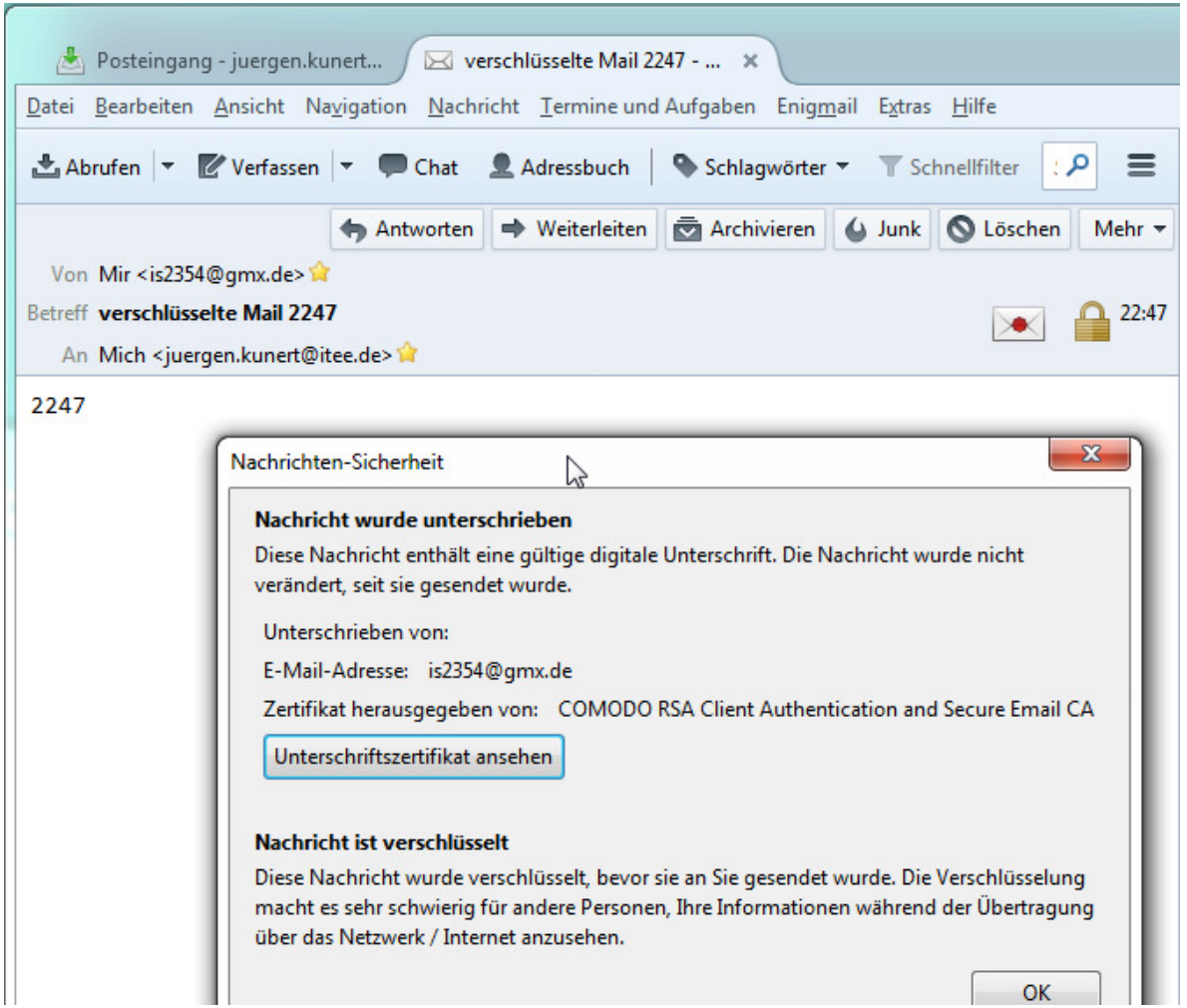
Das Selbe in Thunderbird

- Zertifikat aus Zertifikatsspeicher konfigurieren



Das Selbe in Thunderbird

… und schon kann man die Mail entschlüsseln



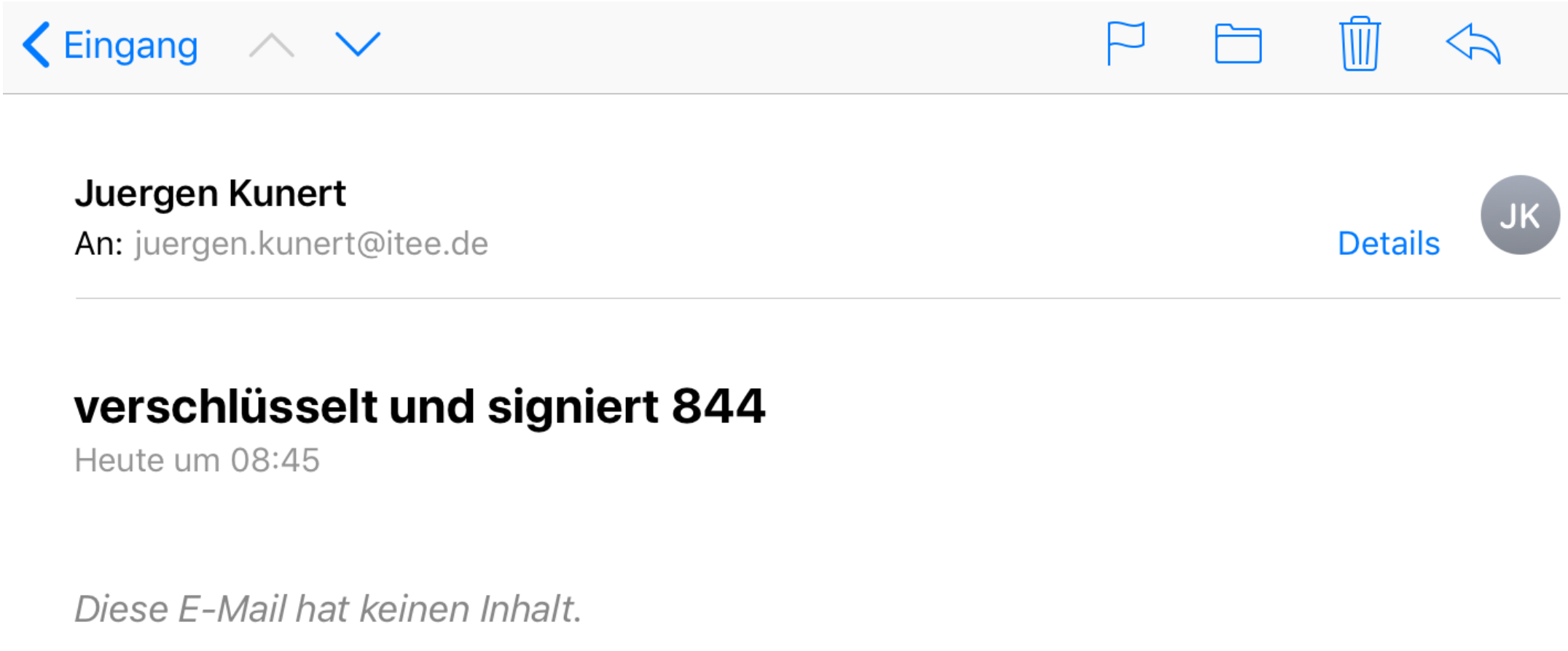
Mobil - Vorbereitungen

- 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

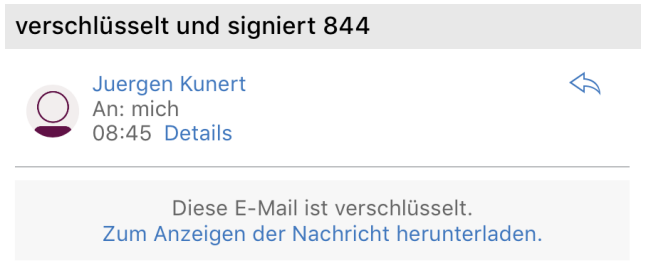
Mobil – was geht?

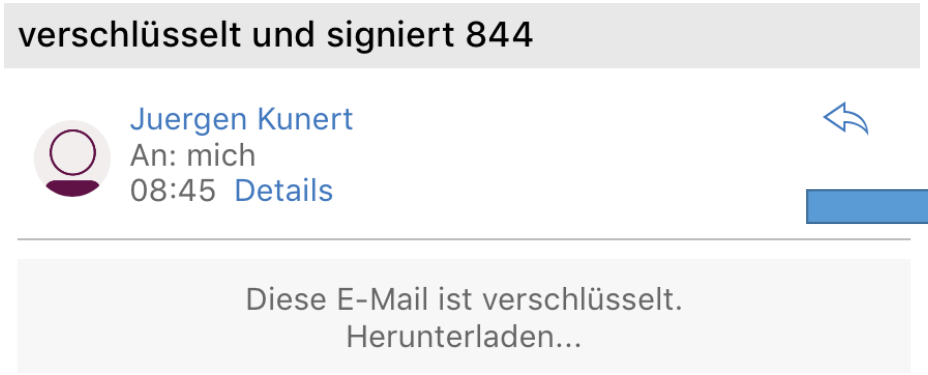
1. Aussage von „vorsichtigen Personen“:
   verschlüsselte Mails haben nichts auf Smartphones zu suchen,
   das Smartphone kann verloren gehen
2. iOS:
   - S/MIME und Notes Native Encryption von Verse unterstützt
3. Android:
   - Only Domino-encrypted mail is supported on the IBM Verse client. Encrypted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

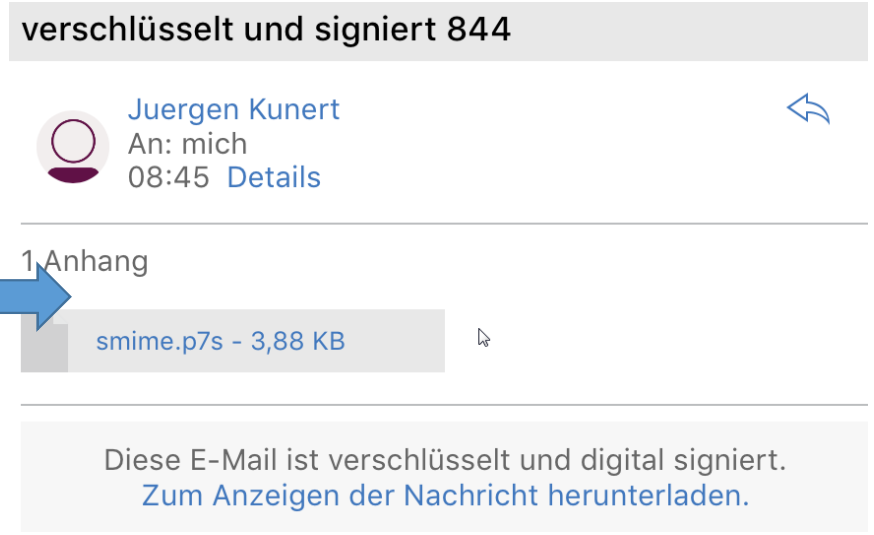
Mobil – iOS native Mail



Mobil – iOS Verse





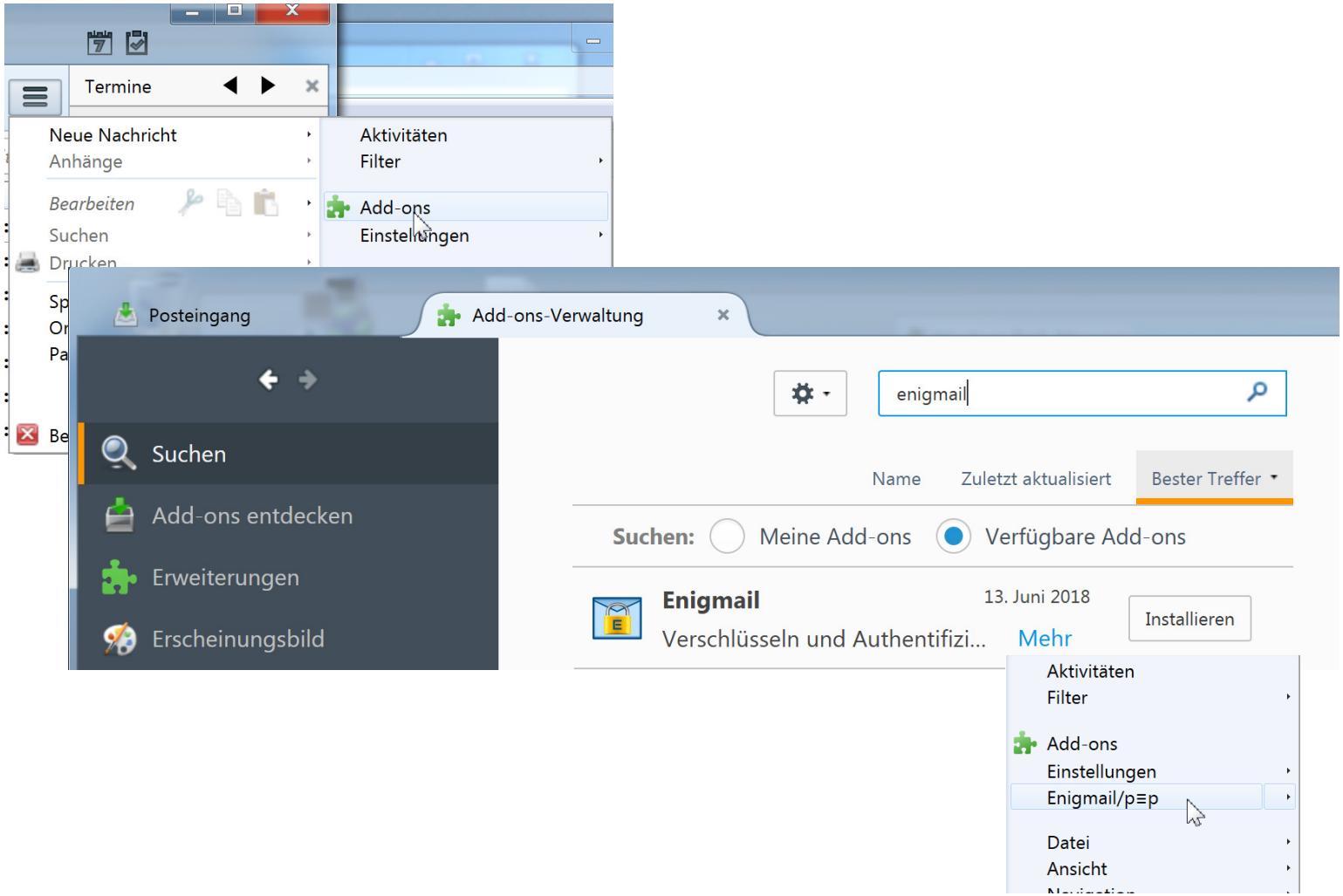


verschlüsselter Rumpf 844

PGP

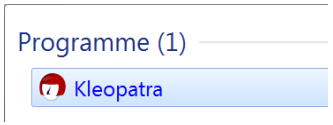
Thunderbird mit PGP

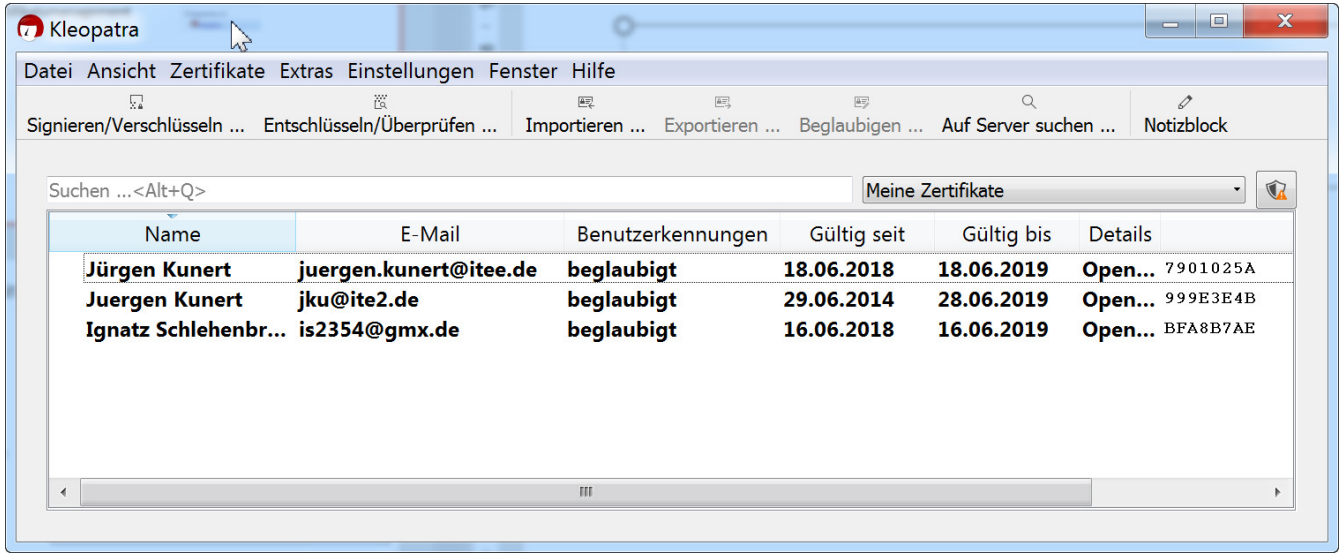
- GPG4Win und Enigmail installieren



GPG4 Win - Kleopatra

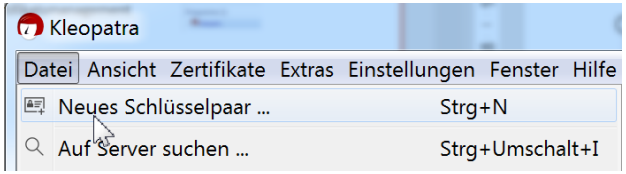
- Kleopatra: Zertifikatsmanagement

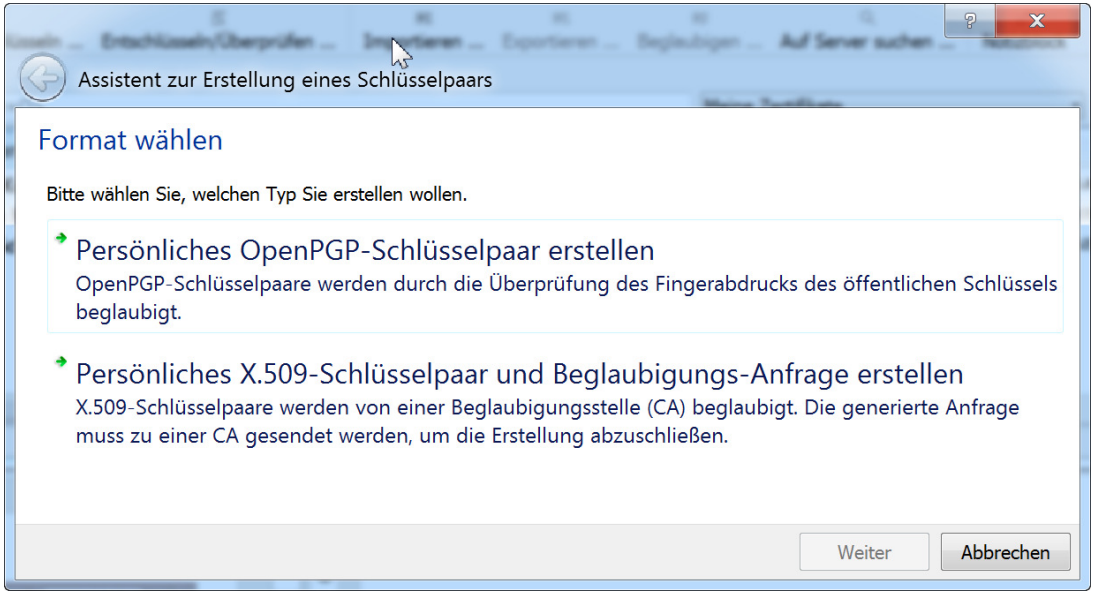


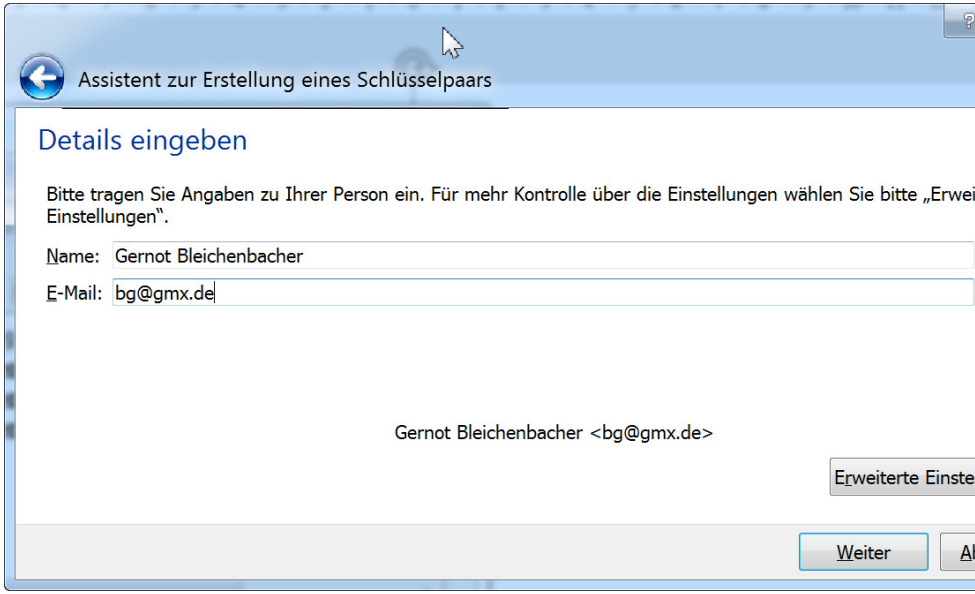


GPG4 Win - Kleopatra

- Schlüsselpaar erzeugen 1

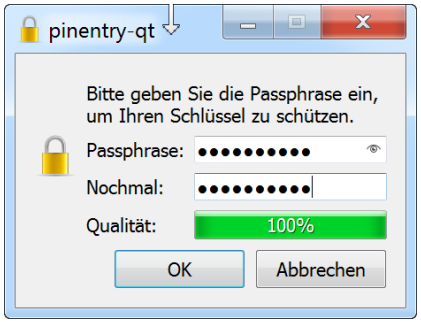


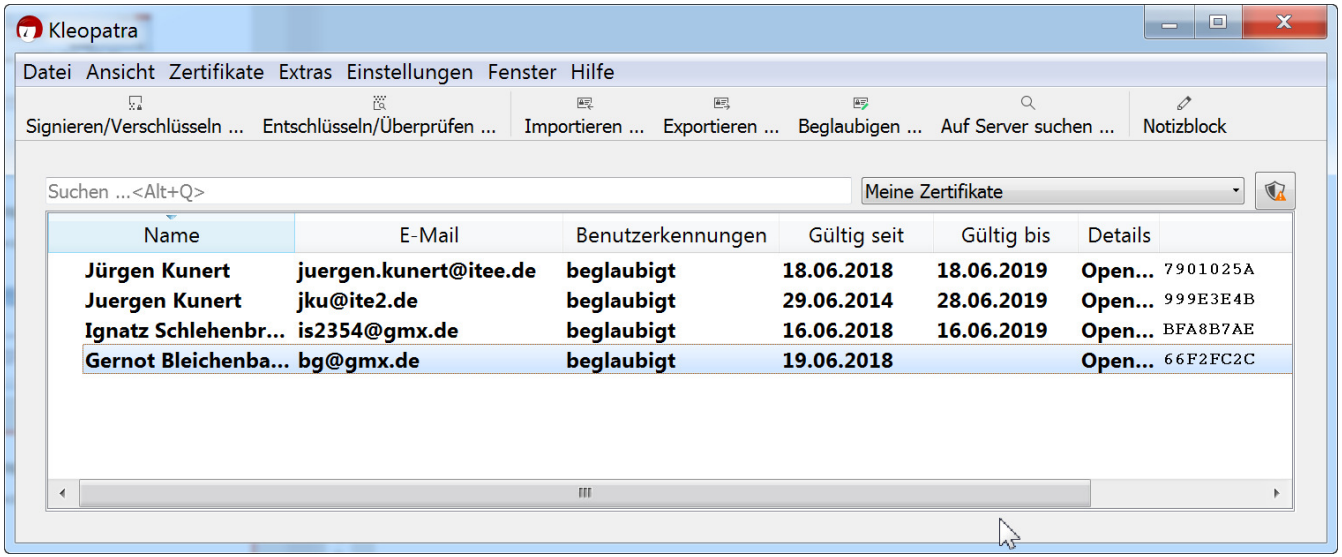




GPG4 Win - Kleopatra

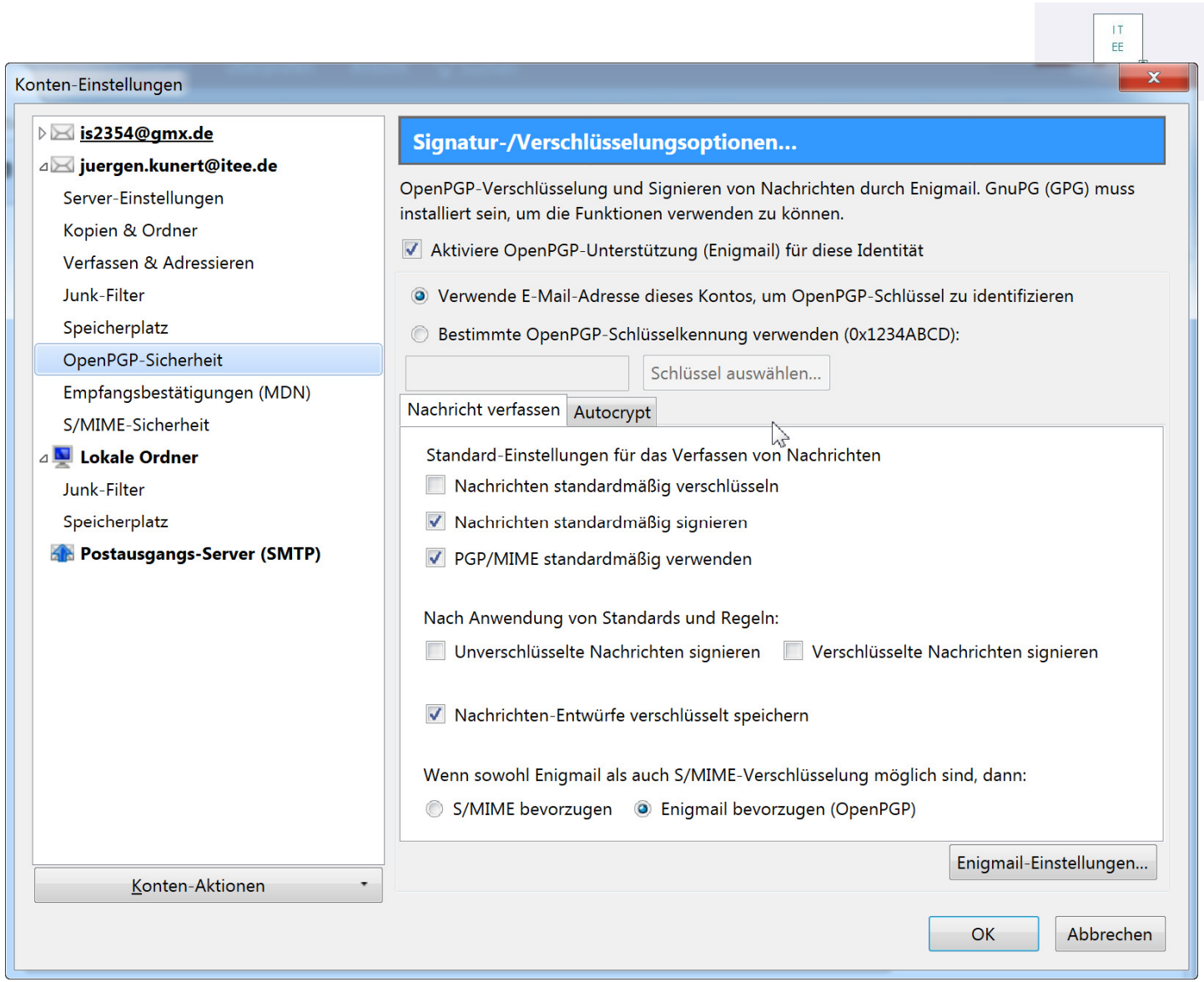
- Schlüsselpaar erzeugen 2





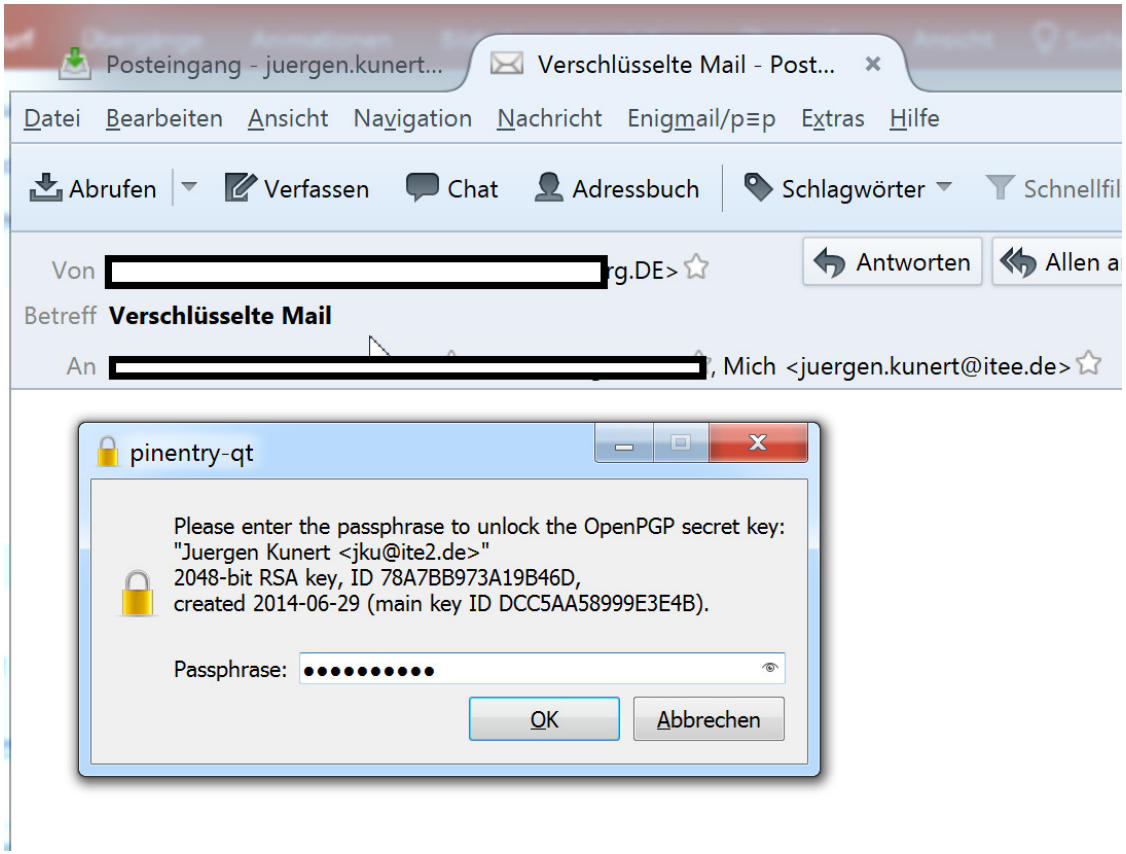
Thunderbird mit PGP

- Enigmail konfigurieren



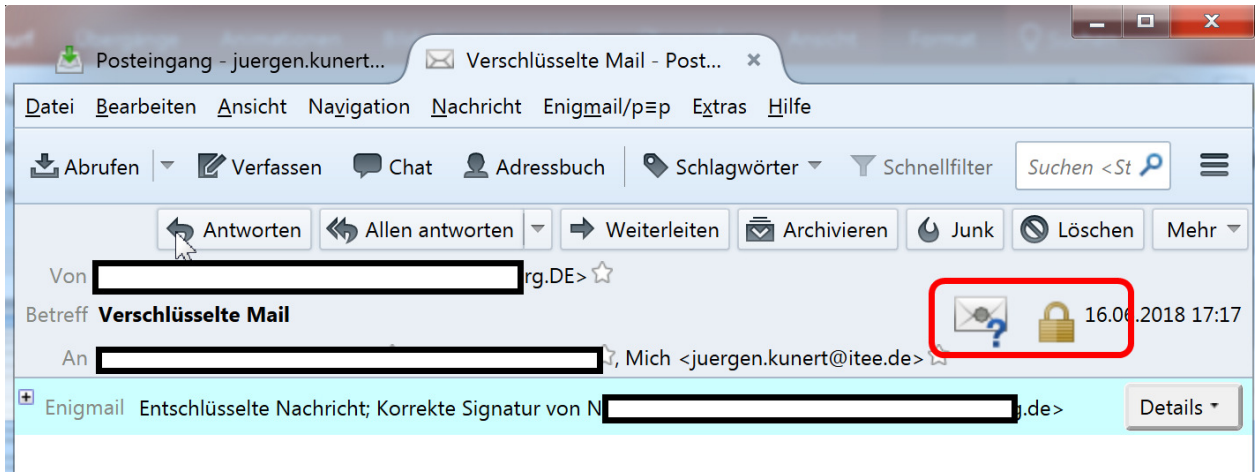
Thunderbird mit PGP

- Enigmail
  verschlüsselte eMail



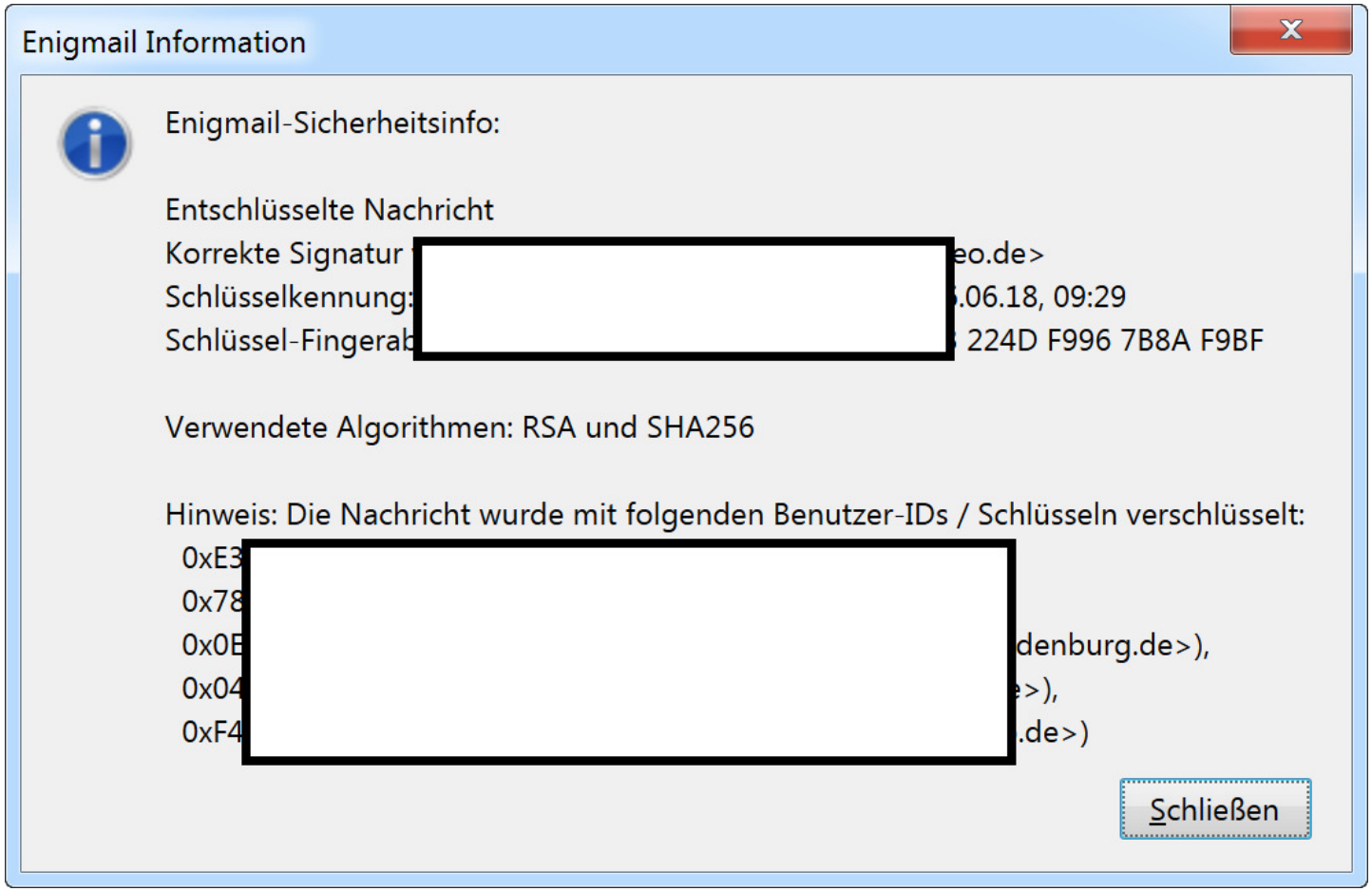
Thunderbird mit PGP

- Enigmail verschlüsselte eMail empfangen



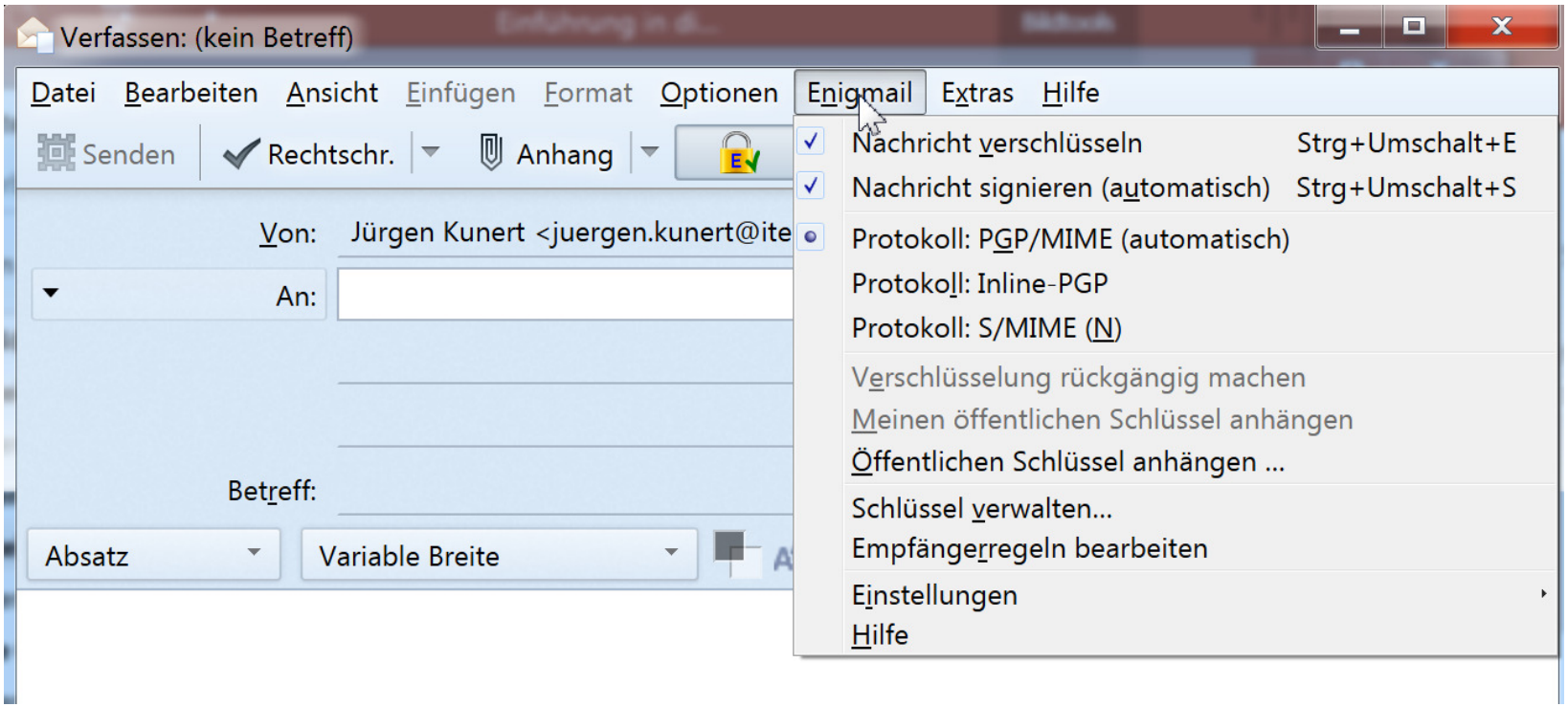
Thunderbird mit PGP

- Enigmail Sicherheitsinfo



Thunderbird mit PGP

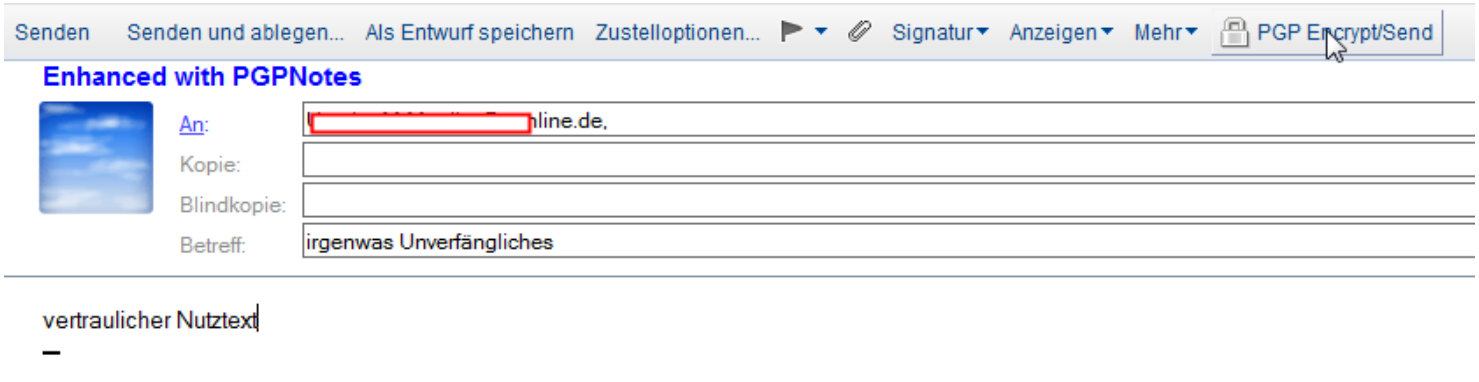
- Enigmail
  verschlüsselt und signiert senden

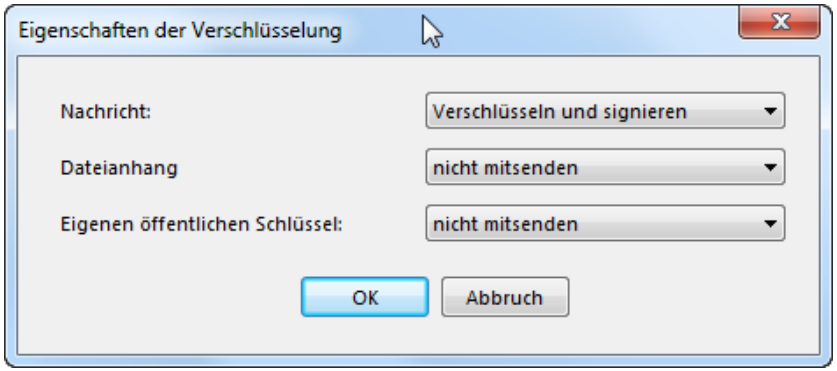


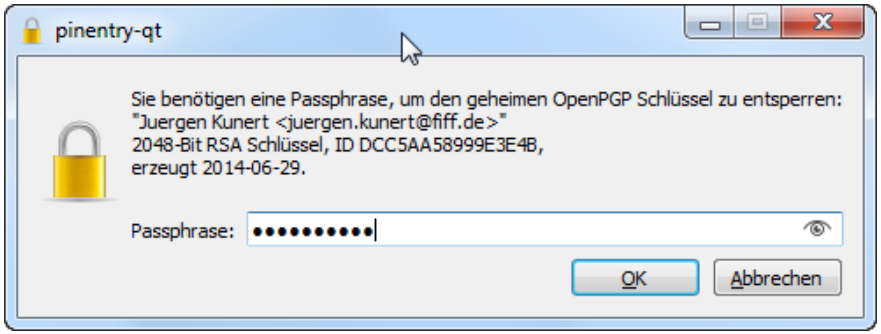
PGPNotes

- 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

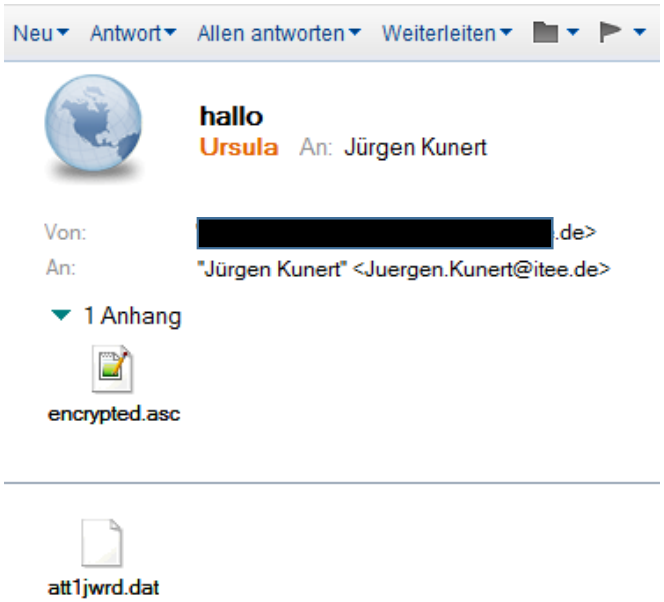
PGPNotes - Senden

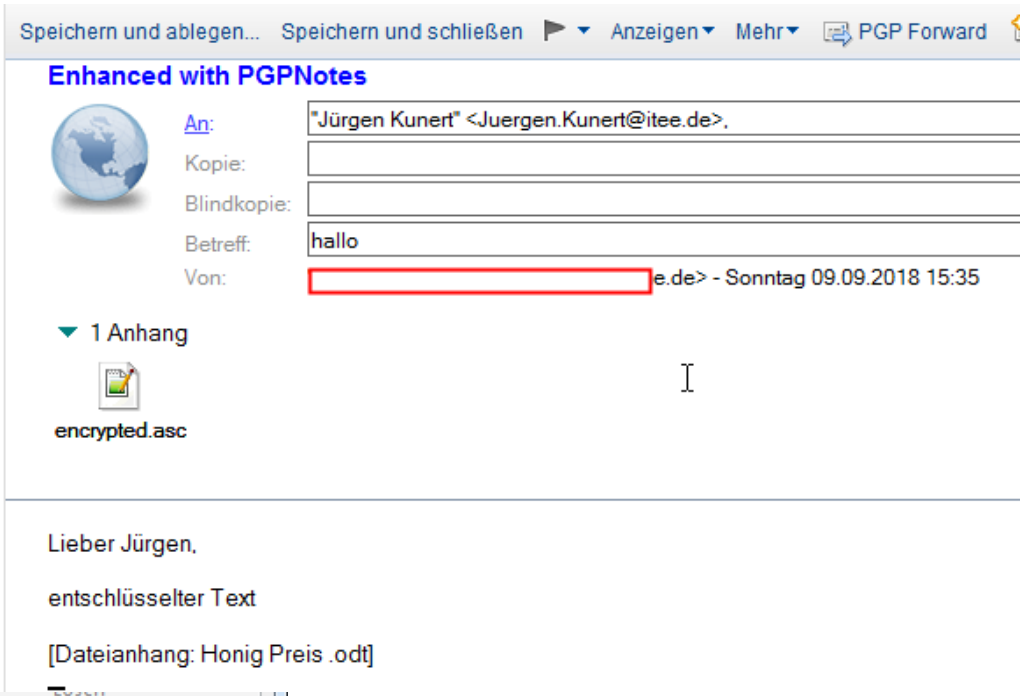


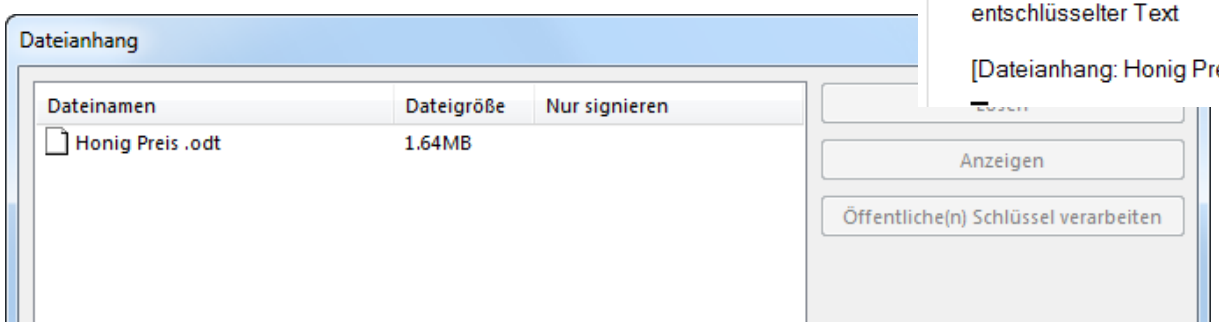




PGPNotes - Empfangen





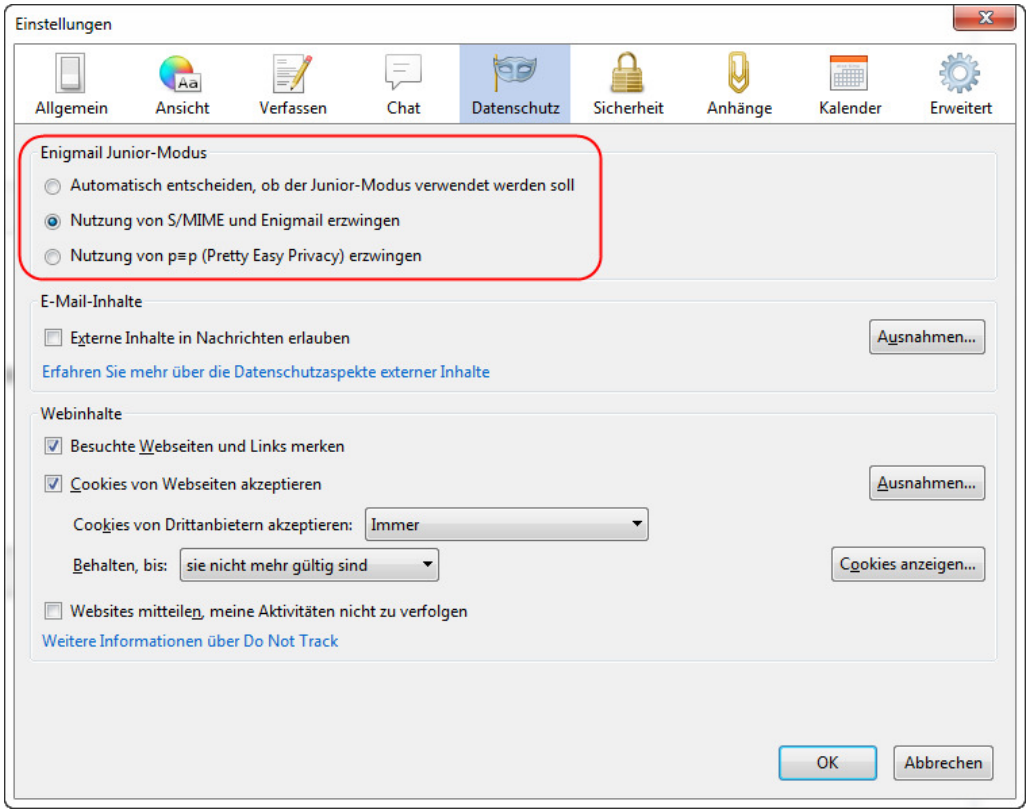


Pretty Easy Privacy p≡p

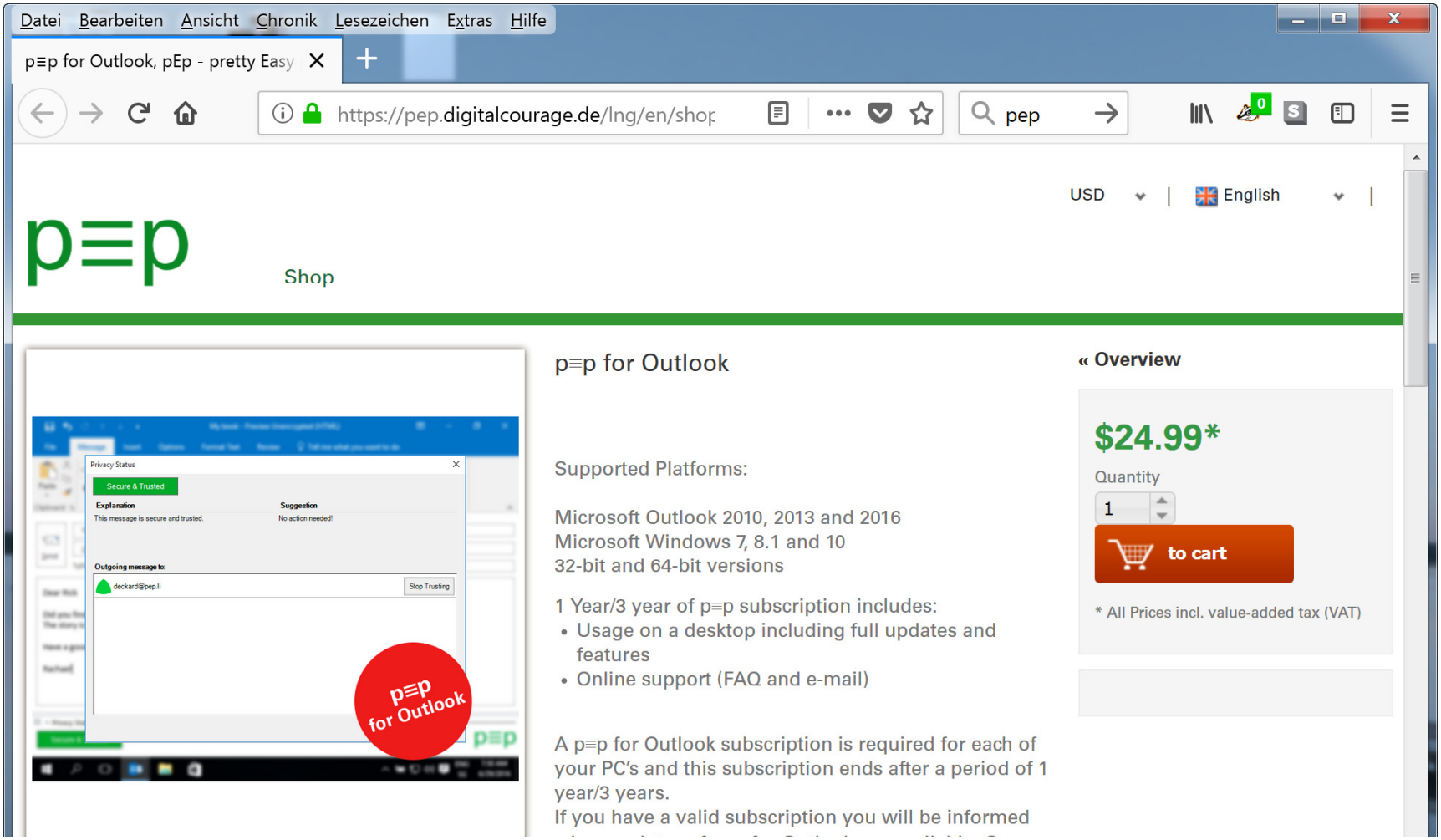
- **pretty Easy privacy** (abgekürzt p≡p oder pEp) oder zu Deutsch *Ziemlich einfache Privatsphäre* ist eine Open-Source-Verschlüsselungs-Software, die es dem Nutzer erlaubt, seine Online-Kommunikation vor fremden Einblicken zu schützen. Dabei sind die erforderlichen Prozesse automatisiert.
- p≡p generiert 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 p≡p

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



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 Virenscanner, 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 Virenscanner 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.phpzwei 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_ln=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

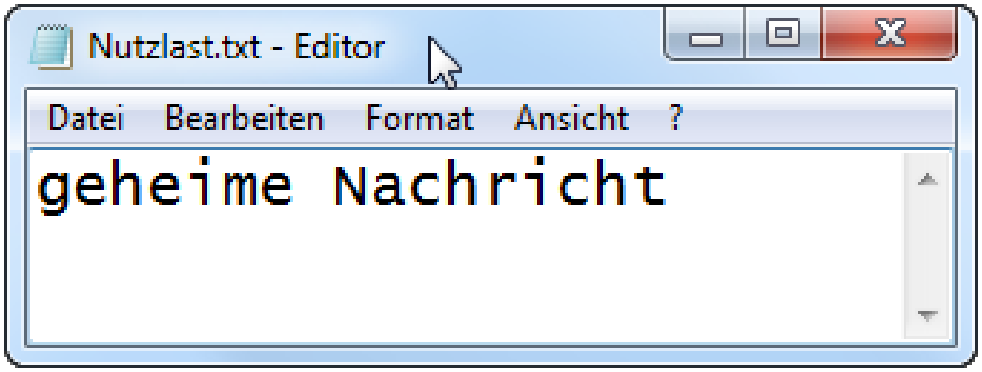
Steganografie

- 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