eMail Verschlüsselung und TLS/SSL für Einsteiger

1. S/MIME-Verschlüsselung & Alternativen
2. TLS/SSL-Jump-Start

Agenda

- Warum?
- Grundlagen der Verschlüsselung
- eMail-Verschlüsselung im Allgemeinen
- eMail-Verschlüsselung mit LN-Bordmitteln
- Alternativen
- TLS/SSL in Kürze
- Selbsterstelltes SSL-Zertifikat
- Kauf und Installation eines SSL-Zertifikats
- Domino HTTPS-Konfiguration

Warum Verschlüsselung?

- Unsere Privatsphäre schwindet
- Das Gefühl für Privatsphäre geht verloren
- Das Bewusstsein für Geheimhaltung von Unternehmensdaten nimmt ab
- Die Gefährdung von vertraulichen Daten nimmt zu
- IT-Sicherheit wird immer komplexer und damit unbeherrschbarer

Stand der politischen Diskussion

- **CCC fordert Ausstieg aus unverschlüsselter Kommunikation,** 22. 1. 2015

  „Ganz im Gegensatz zu dem von militärischen und politischen Akteuren losgetretenen Kampf gegen Verschlüsselung und für mehr Überwachung setzt sich der Chaos Computer Club (CCC) für zukunftssichere Technologien ein und fordert daher ein Verbot unverschlüsselter Kommunikation.“
- **Innenminister De Maizière**, 21. 1. 2105

  „Unter anderem müssen die deutschen Sicherheitsbehörden "befugt und in der Lage sein, verschlüsselte Kommunikation zu entschlüsseln““.

Was passiert beim eMail-Senden?

- Analogie zum Fahrradkurier
- MIME-Spezifikation enthält keine Sicherungsfunktionen
- Daten können mitgelesen werden
- Daten können gefälscht werden
- Ein falscher Absender kann vorgetäuscht werden

Was hätten wir gern?

- Vertraulichkeit:
  nur der gewünschte Empfänger darf den Inhalt lesen
- Authentizität:
  Sicherstellen der Identität von Sender und Empfänger
- Integrität:
  keine Verfälschung von Inhalten

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.
- Parameter der Verschlüsselung sind:
  - ein oder auch mehrere Schlüssel
  - der verwendete Algorithmus

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:
  - 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
  - Möglichkeit der Authentifikation durch elektronische Unterschriften (digitale Signaturen)
- Nachteile:
  - komplex
  - Rechenaufwändig (kann auch ein Vorteil sein!)

Digitale Zertifikate

- 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.

Quelle: Wikipedia

Zusammenhang zwischen Schlüssel und digitalem Zertifikat

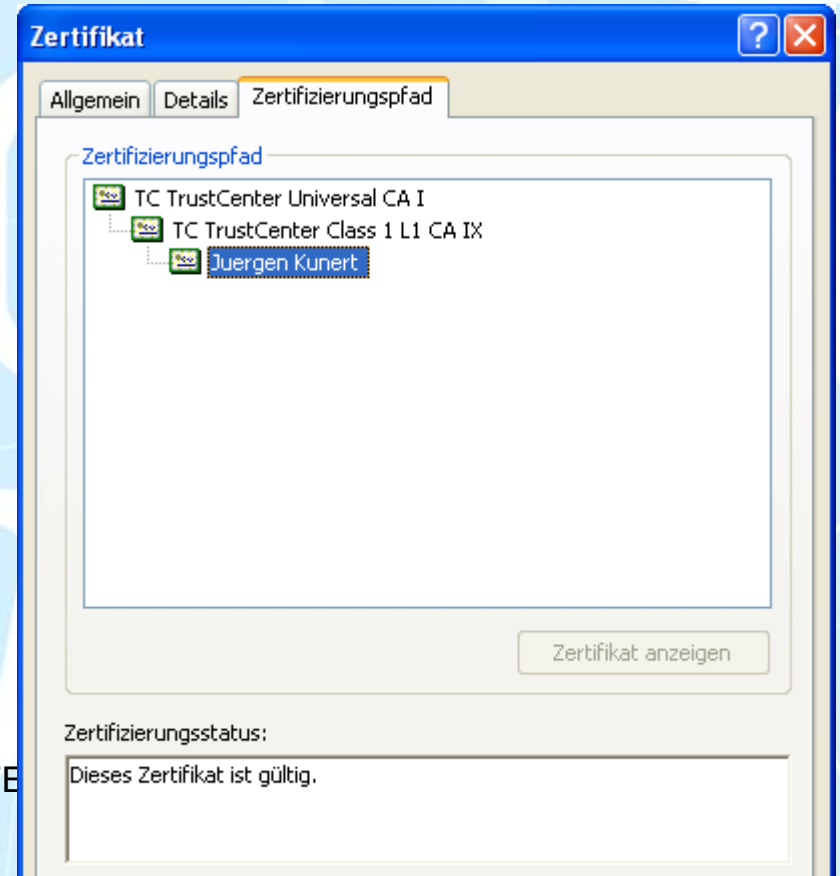
- Jedes digitale Zertifikat ist mit einem öffentlichen Schlüssel verknüpft, dem ein privater Schlüssel zugeordnet ist. Diesen privaten Schlüssel besitzt nur der Zertifikatsinhaber.
- Das Zertifikat, das den öffentlichen Schlüssel enthält, kann hingegen in einem Verzeichnis publiziert und so jedem zugänglich gemacht werden, der mit dem Inhaber eines Zertifikats sicher kommunizieren möchte.

Public-Key-Infrastruktur

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

Wie prüfe ich die Validität eines Zertifikats?

- Der Browser oder das eMail-Programm machen das für mich ☺



Verschlüsselung in Notes Domino

- Verschlüsselung ist integraler Bestandteil des Notes/Domino-Sicherheitskonzepts
- PKI-Infrastruktur
  - Interne Notes-Mails können out-of-the-box signiert und verschlüsselt werden
- Verschlüsselung der Kommunikation zwischen Client und Server
- DBs können auf dem Laptop verschlüsselt werden
- …und vieles mehr

S/MIME-Verschlüsselung in Notes 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
- Troubleshooting

Was brauche ich?

- Mein Schlüsselpaar (privater und öffentlicher Schlüssel)
- Den öffentlichen Schlüssel des Empfängers
- Die richtigen Einstellungen am Notes-Client

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
- Troubleshooting

Was braucht die Gegenseite?

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

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
- Troubleshooting

Wie richte ich meinen Notes-Client ein?

- Arbeitsumgebung einstellen
- Personendokument konfigurieren
- Zertifikat mit privatem Schlüssel in Notes-ID importieren
- Öffentliche Schlüssel der Mail-Empfänger in Adressbuch einfügen
- Um SHA-2-Zertifikate zu unterstützen, werden die „FIPS 140-2“-Algorithmen benötigt! (Admin-9-Hilfe)

Arbeitsumgebung einstellen

Diese Einstellung sorgt dafür, dass der Client die MIME-Konvertierung vornimmt.
Das ist nötig, weil nur der Client den Schlüssel hat.

~~Problem!~~ Herausforderung

- Wenn die MIME-Einstellung in der Arbeitsumgebung falsch ist, wird gar nicht signiert/verschlüsselt, ohne Fehlermeldung!
- Achtung: Policies!

Personendokument konfigurieren

- Im Personendokument des Domino Directory:

Woher bekomme ich ein Zertifikat? 1

Guten Tag Juergen Kunert,

Sie haben eine TC Internet ID mit den folgenden Daten beantragt:

Name:..... Juergen Kunert
Land:..... Deutschland

Wir bestätigen Ihren Antrag mit der Antragsnummer 404159485.

Ausstellung des Zertifikates
****
Damit wir Ihr Zertifikat ausstellen können, müssen Sie zunächst auf der Antragsstatusseite ein Schlüsselpaar erzeugen.

Das erforderliche Passwort für den Zugang zu der Antragsstatusseite erhalten Sie gesondert per E-Mail oder SMS (entsprechend der Auswahl bei der Antragsstellung).

Antragsstatusseite:
https://www.trustcenter.de/RetailStore/cid/Login.action?loginName=fOKFsgGHUWgQDS
Nach der Schlüsselerzeugung erfolgen unmittelbar die Ausstellung Ihres Zertifikates sowie die Installation des Zertifikates in Ihrem Browser.

HINWEIS: Wir empfehlen Ihnen, sich eine Sicherheitskopie Ihres privaten Schlüssels und des Zertifikates zu erstellen. Sollte zu einem späteren Zeitpunkt, z.B. nach Verlust des privaten Schlüssels, ein Ersatzzertifikat benötigt werden und keine Sicherheitskopie vorliegen, muss ein neues Zertifikat zu dem dann aktuell gültigen Preis beantragt werden.

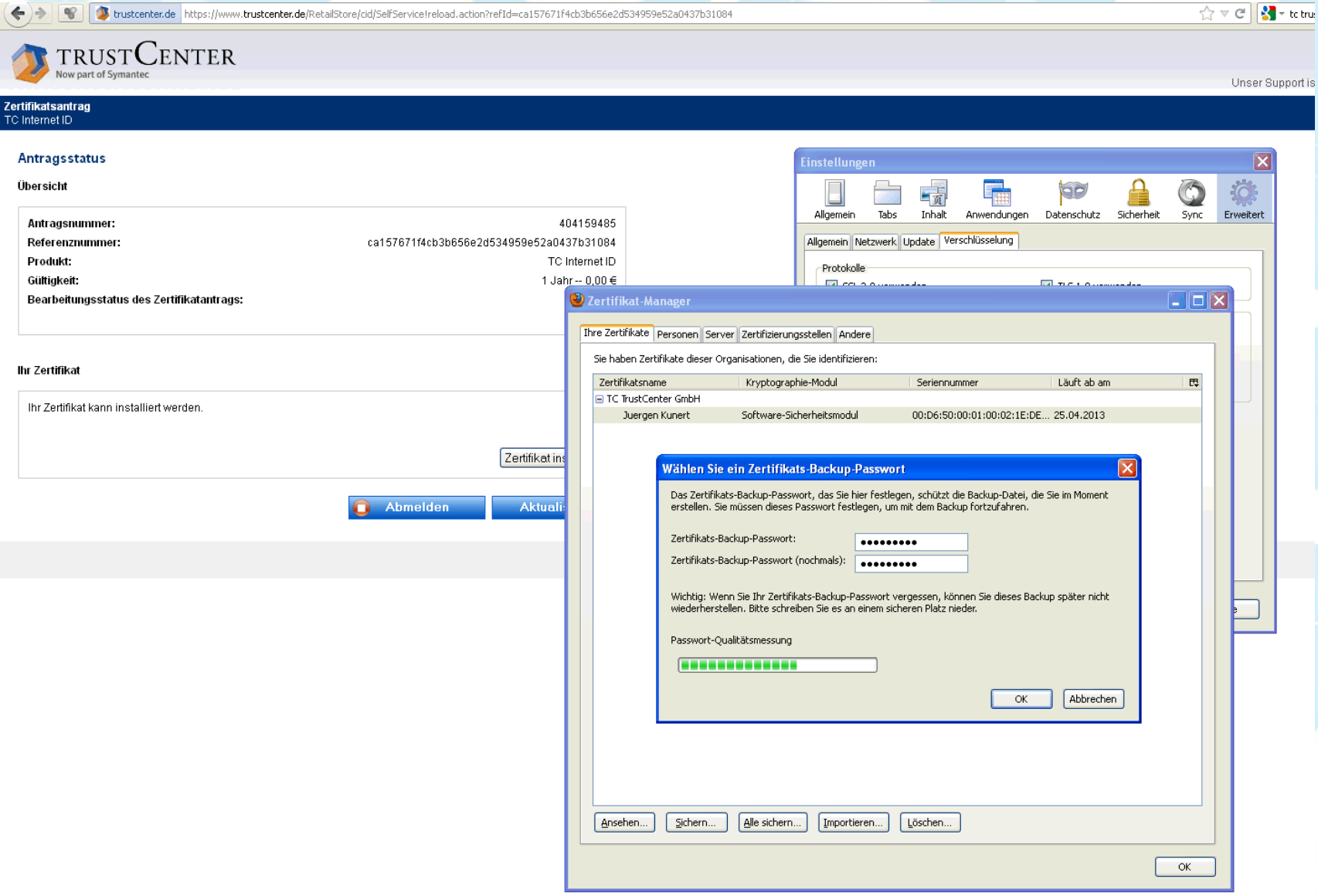
Sperrung Ihres Zertifikats
****
Zum Sperren Ihres Zertifikates rufen Sie bitte folgende URL auf:
http://www.trustcenter.de/sperren

Sollten Sie auf Ihr Zertifikat keinen Zugriff mehr haben, können Sie die Sperrung auch telefonisch unter +49 40 / 80 80 26-113 veranlassen. Bei Nennung Ihres –bei der Antragsstellung von Ihnen angegebenen –Notfallpasswortes wird die sofortige Sperrung Ihres Zertifikats veranlasst.

Support
****
Bei technischen Fragen wenden Sie sich bitte an den Support:
https://www.verisign.de/support/contact-support/index.html

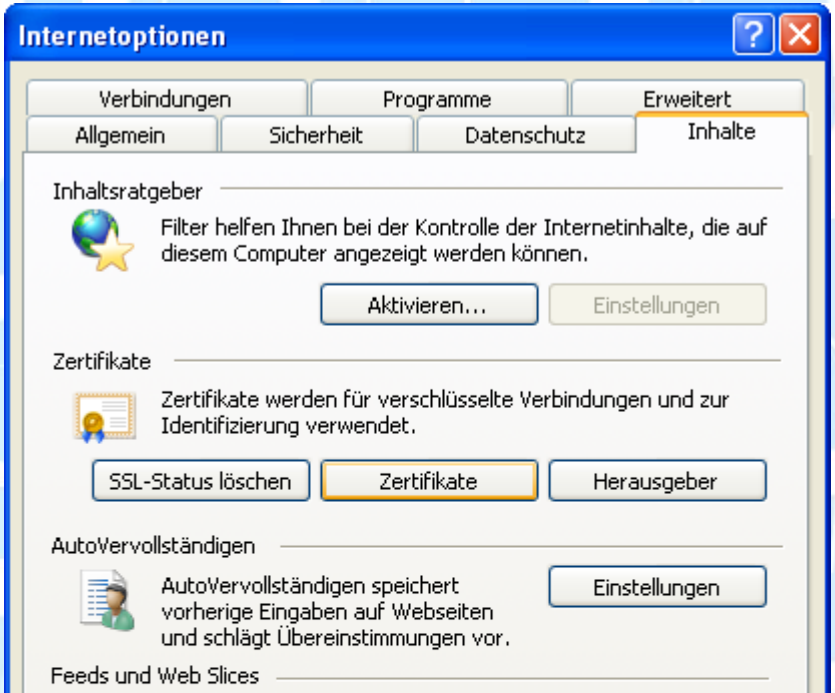
Vielen Dank, dass Sie sich für TC TrustCenter entschieden haben.

Woher bekomme ich ein Zertifikat? 2



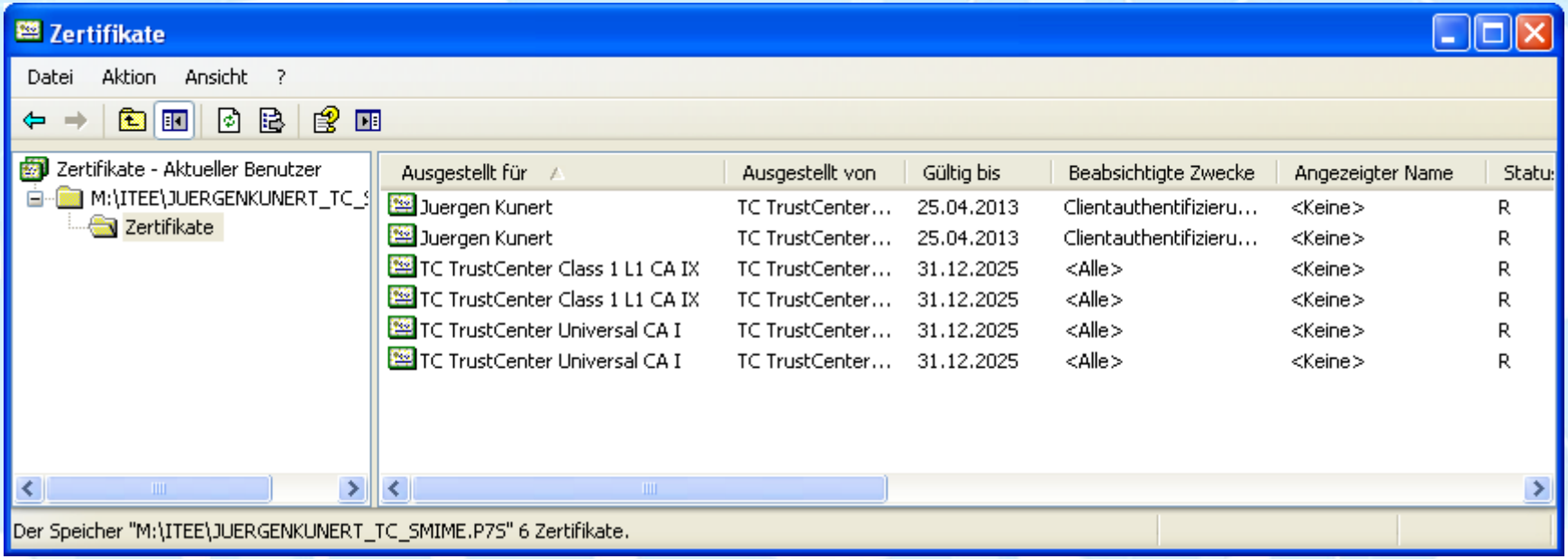
Woher bekomme ich ein Zertifikat? 3

- Nach Anmeldung auf Webseite wird das Zertifikat in den Zertifikatsspeicher des Betriebssystems/Browsers gespeichert
- Zugriff über Internet Explorer/Internetoptionen
- von dort exportieren
- Ggf. Häkchen bei „privaten Schlüssel exportieren“ setzen



Woher bekomme ich ein Zertifikat? 4

- von dort exportieren in eine .p12-, .p7b oder .cer-Datei

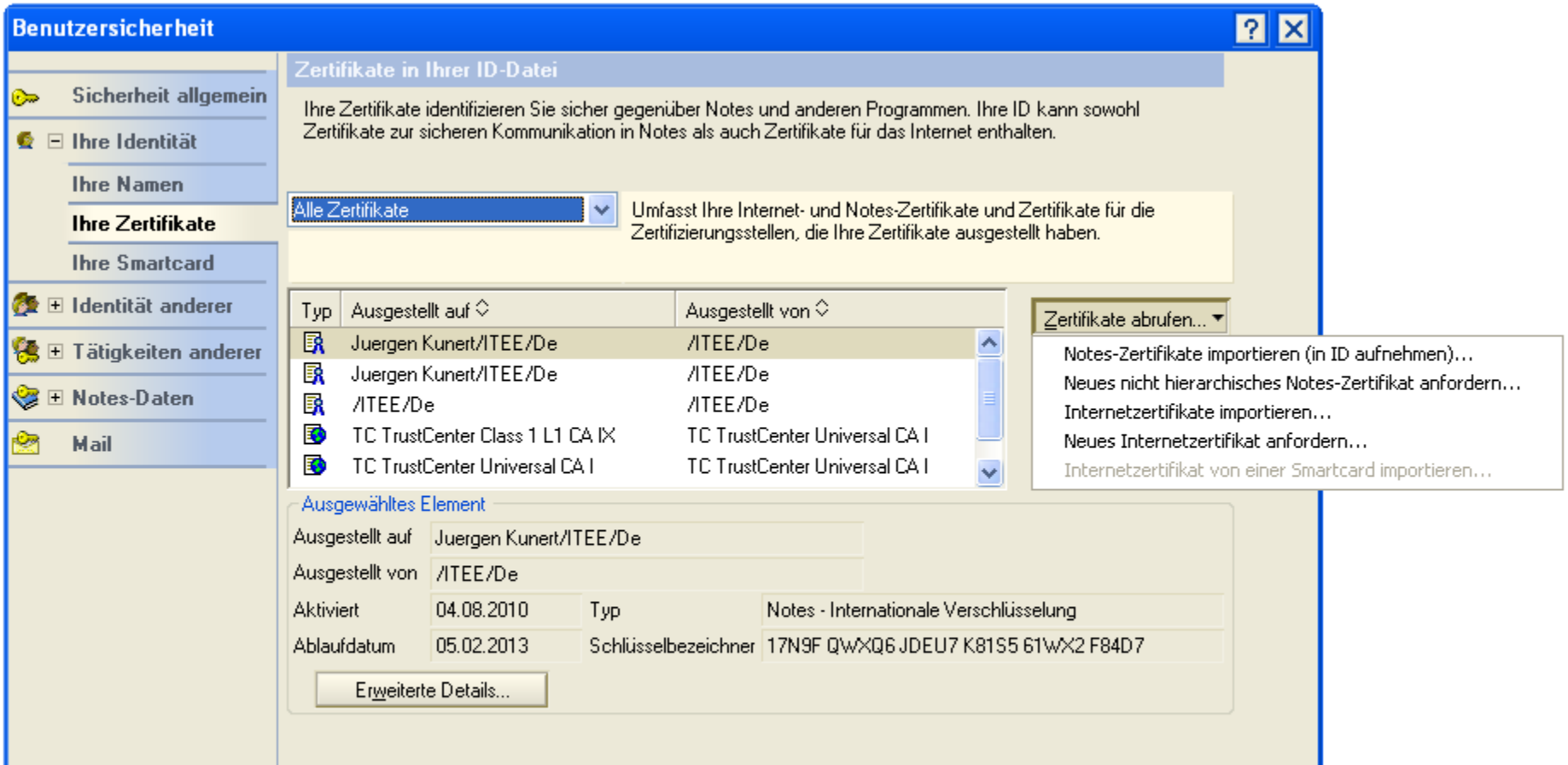


Woher bekomme ich ein Zertifikat? 5

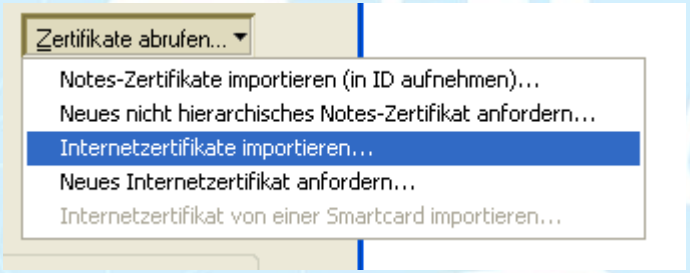
- Alternativen:
- https://www.instantssl.com/ssl-certificate-products/free-email-certificate.html
- oder selber machen mit openssl: https://gist.github.com/richieforeman/3166387

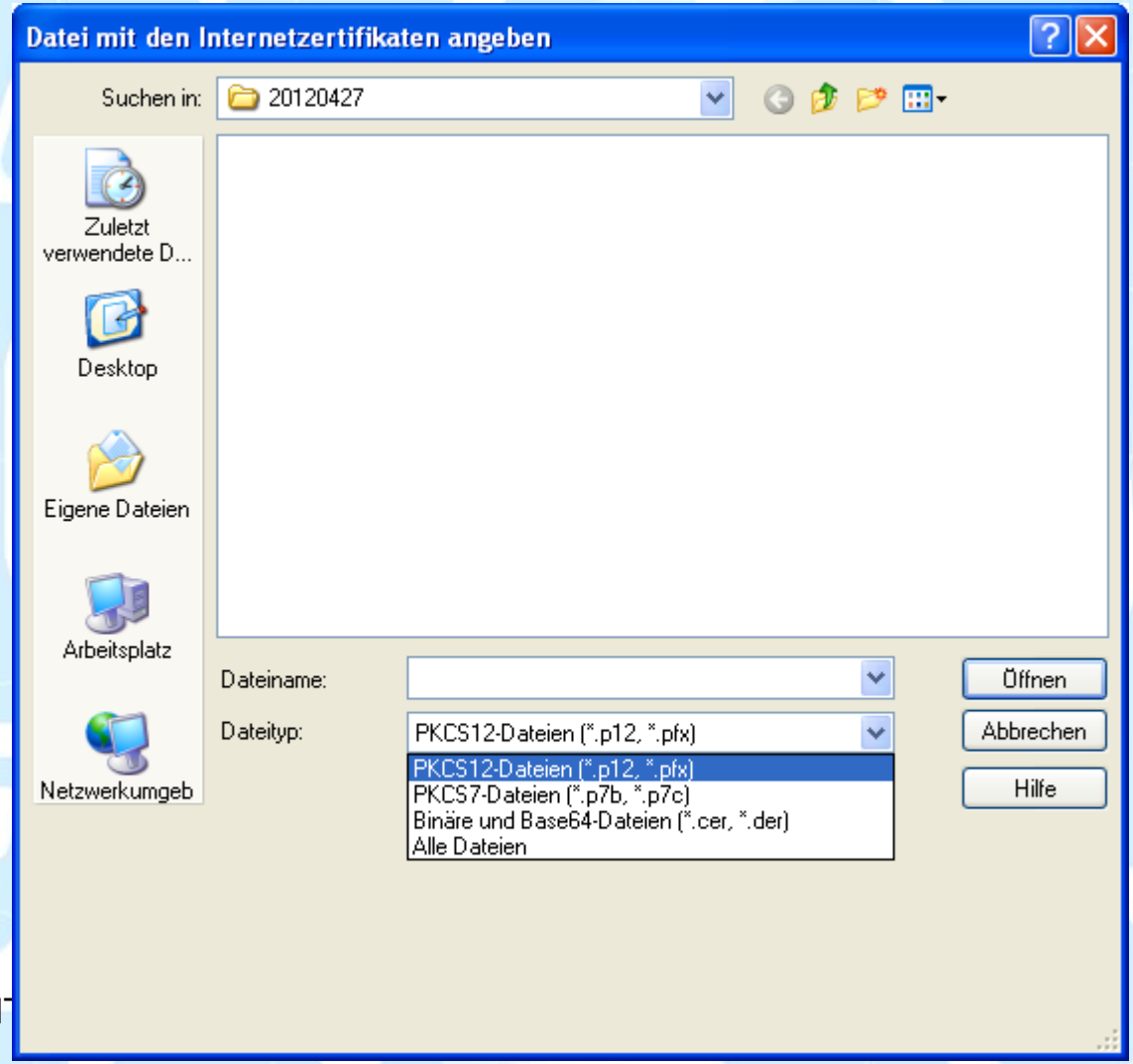
Zertifikat mit privatem Schlüssel in Notes-ID importieren 1

- Datei\Sicherheit\Benutzersicherheit
- Ihre Identität\Ihre Zertifikate

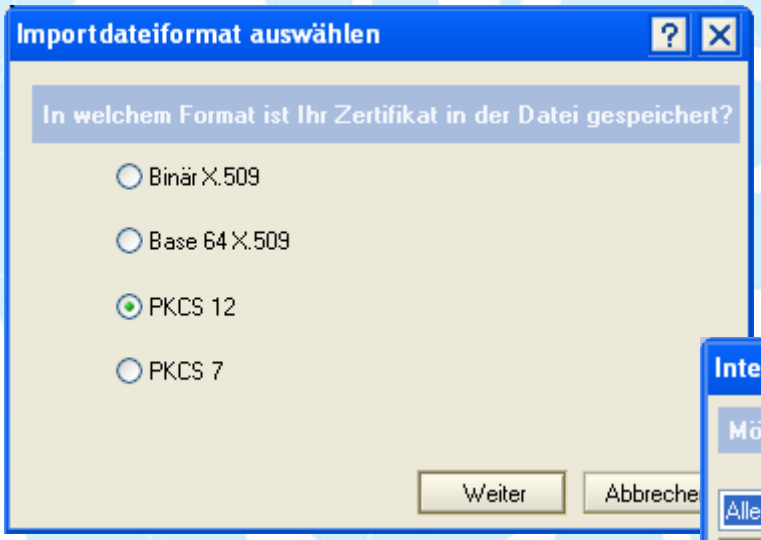


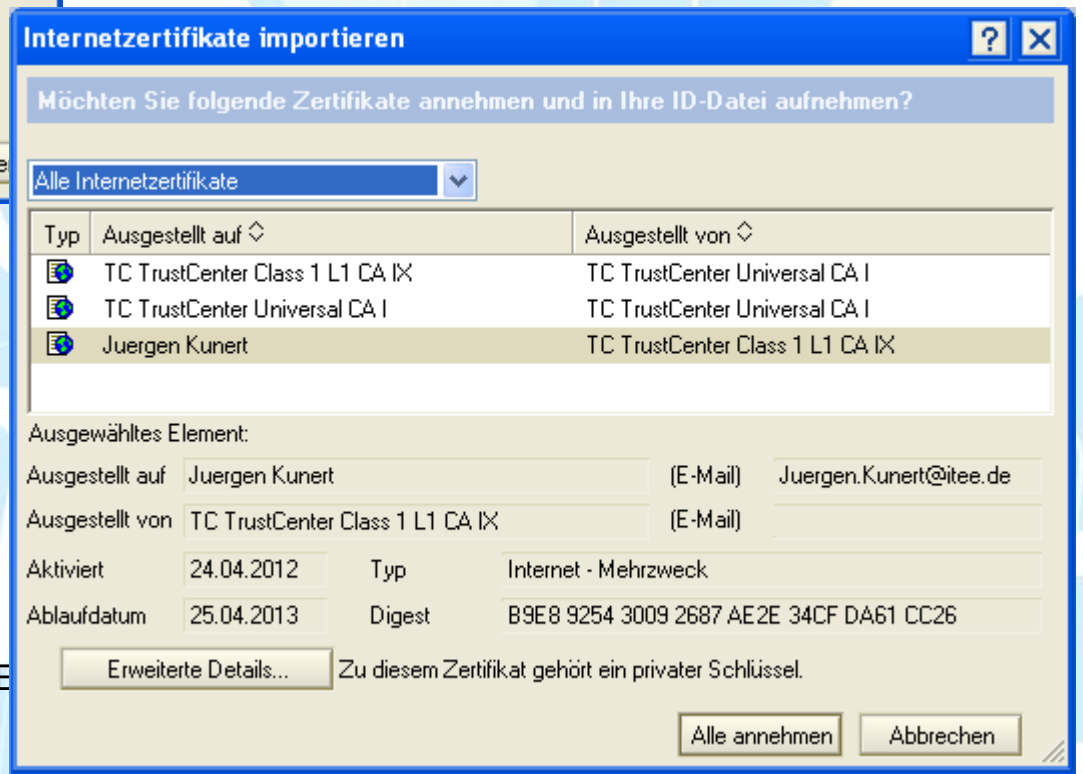
Zertifikat mit privatem Schlüssel in Notes-ID importieren 2



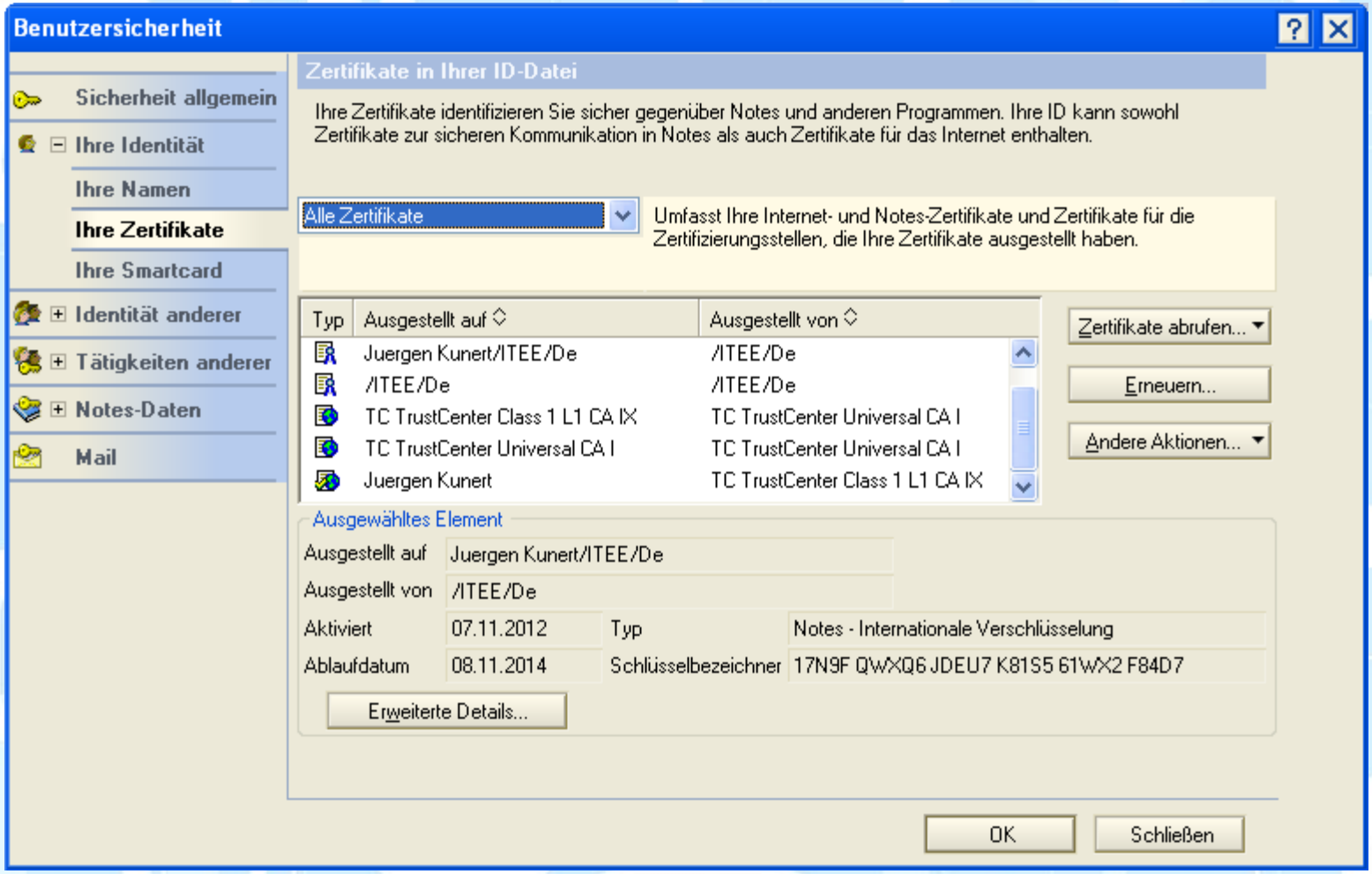


Zertifikat mit privatem Schlüssel in Notes-ID importieren 3





Zertifikat mit privatem Schlüssel in Notes-ID importieren 4



Was habe ich davon?

- Ich kann signierte Mails verschicken
- Ich kann Mails lesen, die mit meinem Public Key verschlüsselt sind
- Geht auch in iNotes, wenn ID-Datei in Maildatei importiert ist
- Geht auch in Traveler (Android)/CompanionLink (iPhone), wenn ID-Datei in Maildatei importiert ist

eMail-Verschlüsselung mit Bordmitteln

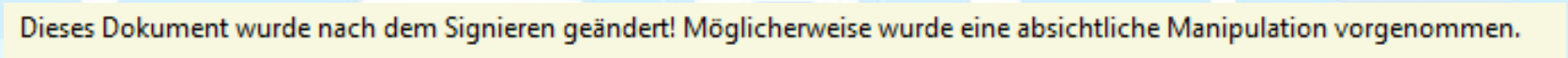
- Was brauche ich?
- Was braucht die Gegenseite?
- Wie richte ich meinen Notes-Client ein?
- Signierte und verschlüsselte Mails austauschen
  - Signierte Mail empfangen
  - Signierte Mail senden
  - Verschlüsselte Mail empfangen
  - Verschlüsselte Mail senden
- Troubleshooting

Betreff/Subject einer Mail

- wird nicht verschlüsselt
  - weder in interner eMail
  - noch bei S/MIME
- „Anfrage nach Suchtberatung“

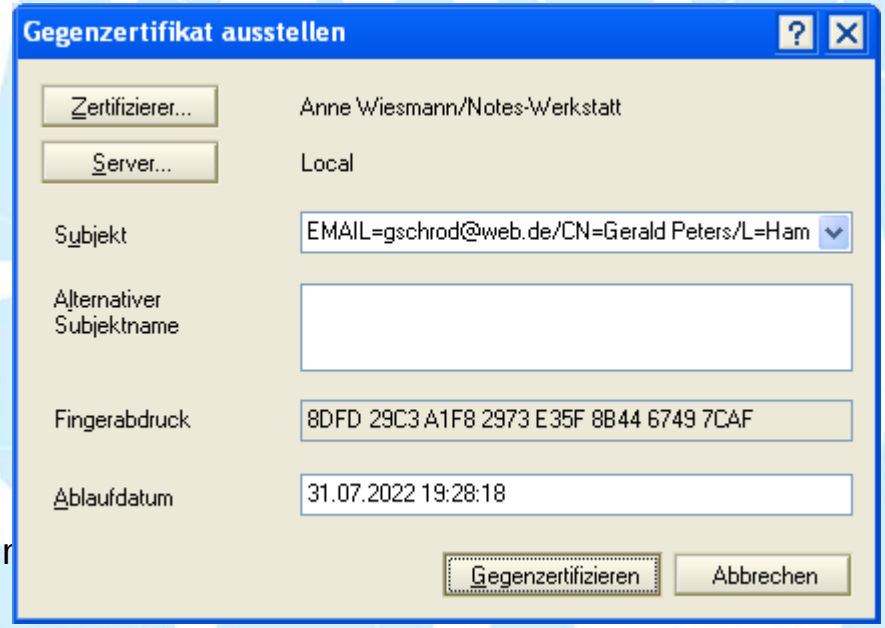
Wenn eine signierte Mail ankommt

- 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:



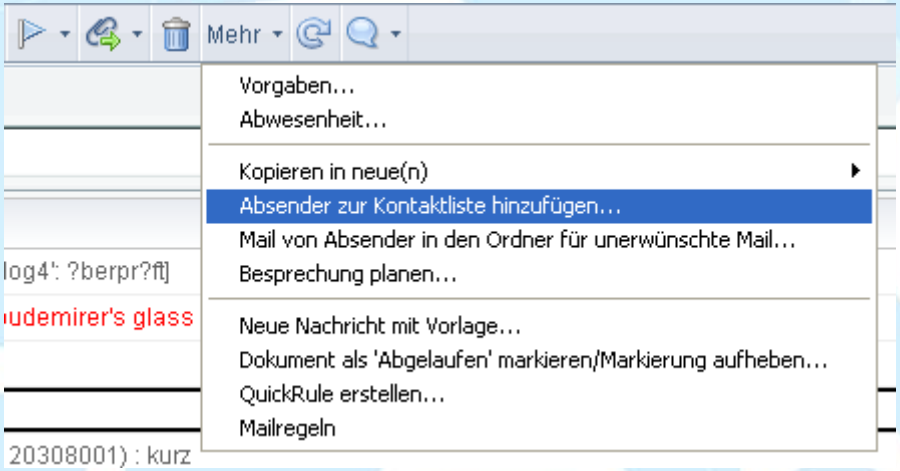
Wenn eine signierte Mail ankommt

- Gegenzertifikat im lokalen Adressbuch erstellen, nachdem man geprüft hat dass die Mail authentisch ist
- Künftig wird dann dieser Signatur vertraut



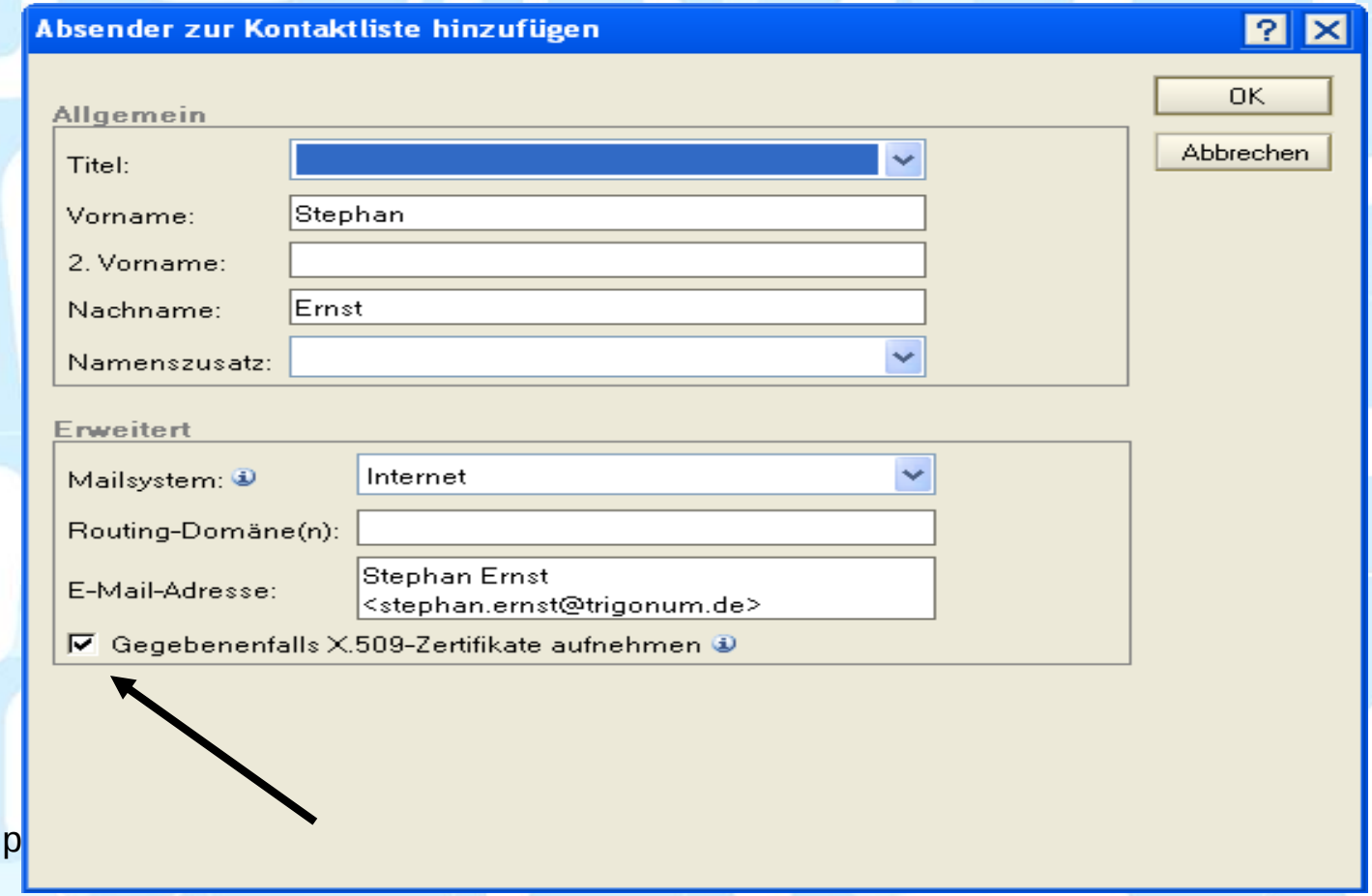
Praxis: Schlüsselaustausch Empfänger Notes 1

- Ich habe eine signierte Mail bekommen
- Mail mit Signatur markieren

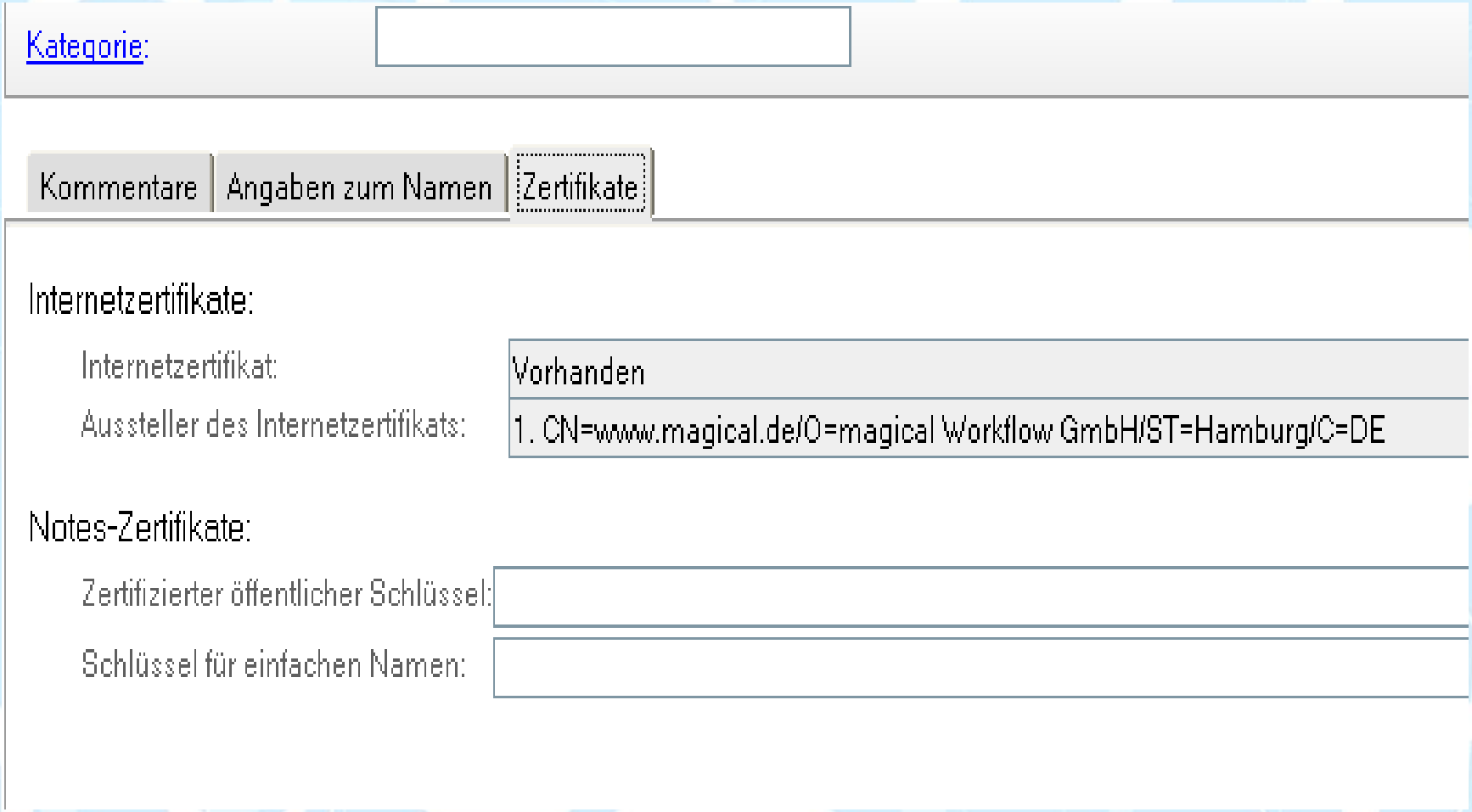


Praxis: Schlüsselaustausch Empfänger Notes 2 Absender hinzufügen

Häkchen setzen: Gegebenenfalls X.509-Zertifikate aufnehmen



Praxis: Schlüsselaustausch Empfänger Notes 3 Kontakt ansehen



Praxis: Schlüsselaustausch Empfänger Notes: Kontakt ansehen

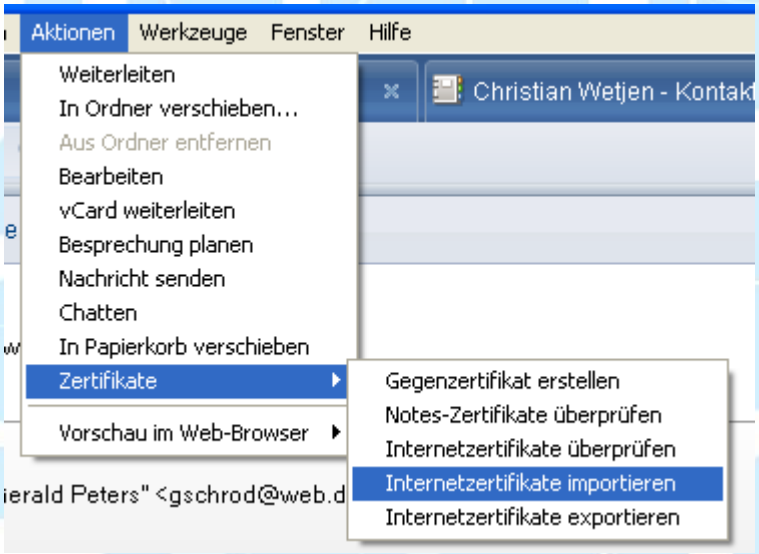
- Email-Adresse darf nur im RFC821-Format dort stehen:
- Juergen.Kunert@itee.de
- Nicht im erweiterten RFC822:
- „Jürgen Kunert“ <Juergen.Kunert@itee.de>

- RFC 821 definiert die Standardkonvention für die Namensgebung von Mailbox-Adressen, z. B. "user@domain", bekannt als RFC 821-Adressierung.
- Nachfolger: RFC 822 im Format "Phrase" <localpart@domainpart>
- Ein optionaler Anzeigename zeigt den Namen des Empfängers an, wie er in der Mail-Anwendung des Benutzers angezeigt wird, z. B. „Jürgen Kunert" <Juergen.Kunert@itee.de>.

Manuell Zertifikat zu einer Adresse hinzufügen

- Wenn Konvertierung falsch eingestellt war, sieht man einen Anhang:

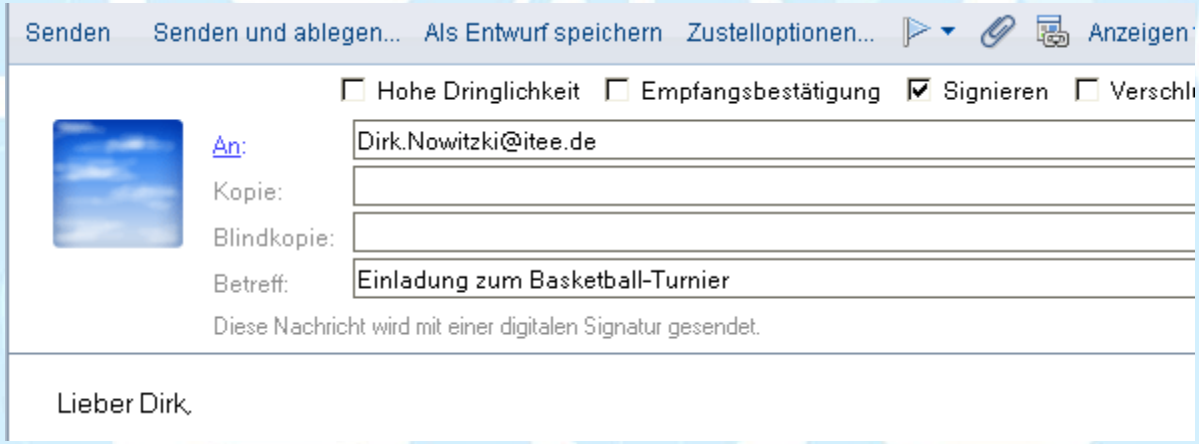
- Anhang abhängen
- Dann Personen-dokument öffnen, hinzufügen:



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
- Troubleshooting

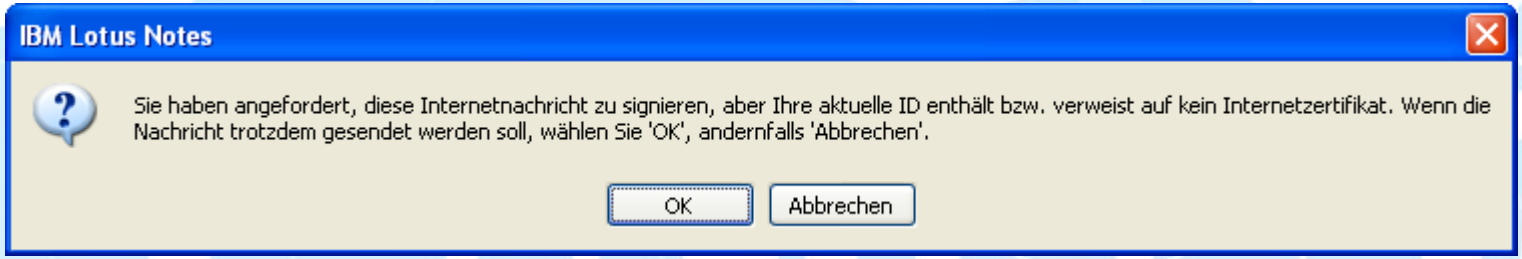
Signierte Mail senden



Falsch geschriebenes Wort suchen...
Nachricht wird signiert...
Mail wurde zur Zustellung abgegeben. (1 Person/Gruppe).

Probleme

- Wenn kein privater Schlüssel des Absenders da ist:



- Wenn die MIME-Einstellung in der Arbeitsumgebung falsch ist, wird gar nicht signiert/verschlüsselt, ohne Fehlermeldung!

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
- Troubleshooting

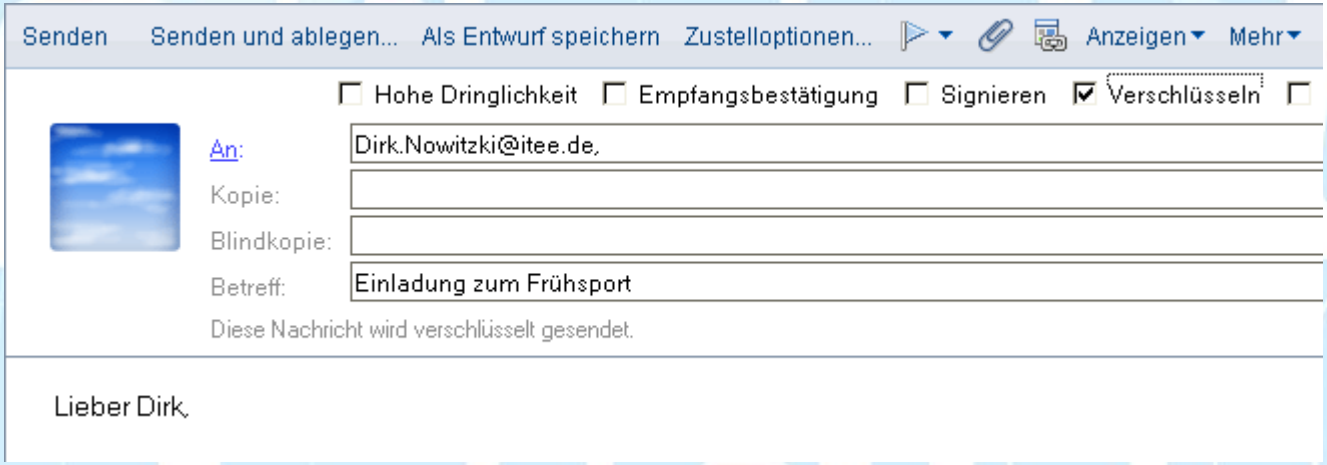
Empfangen einer verschlüsselten Mail

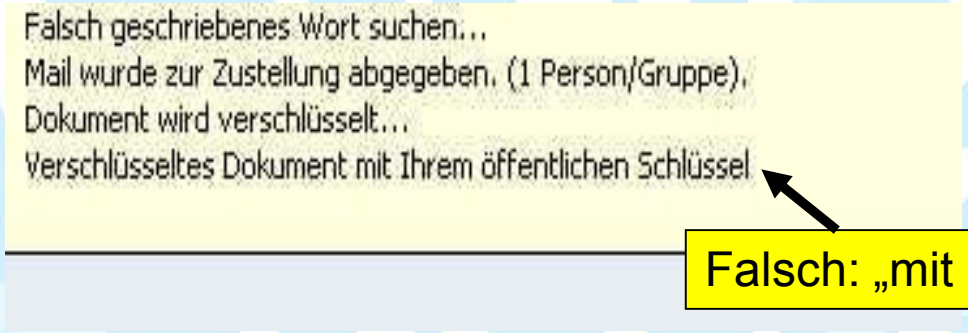
```
Überprüfung auf neuen Maileingang...
Sie haben neue Mail auf 'ITEEN501/ITEE/De' erhalten
Dokument wird entschlüsselt...
```

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
- Troubleshooting

Senden einer verschlüsselten Mail





Falsch: „mit ihrem privaten Schlüssel“

Wenn es nicht geklappt hat, fehlt die letzte Zeile!

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
- Troubleshooting

Troubleshooting

- Einstellungen prüfen
- Ist das Zertifikat valide?
  - Zertifikatskette überprüfen
  - Zertifikat abgelaufen?
- Beim Import
  - Ist das zu importierende Zertifikat das richtige, habe ich das Richtige bestellt, das Richtige heruntergeladen?

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 signierten oder verschlüsselten Mail?

eMail-Verschlüsselung

- Einführung in die Verschlüsselung
- eMail-Verschlüsselung
- eMail-Verschlüsselung mit Bordmitteln
- Alternativen

PGP

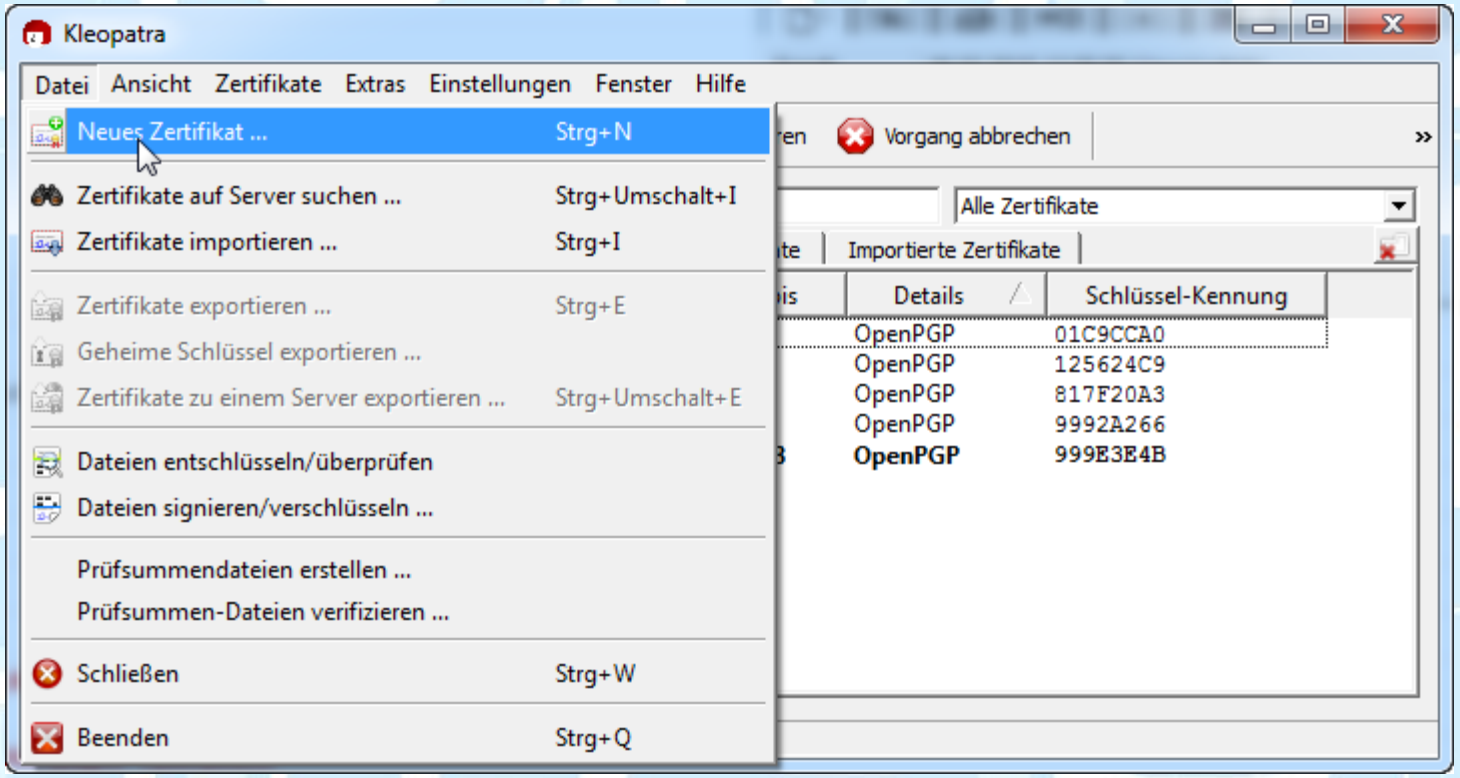
- steht für Pretty Good Privacy
- von Phil Zimmermann entwickelt
- ebenso wie S/MIME Internet-Standard
- Plug-Ins/Zusatzprogramme für den Mail-Client nötig, auch für Notes: PGPNotes
- genauso sicher wie S/MIME

PGP

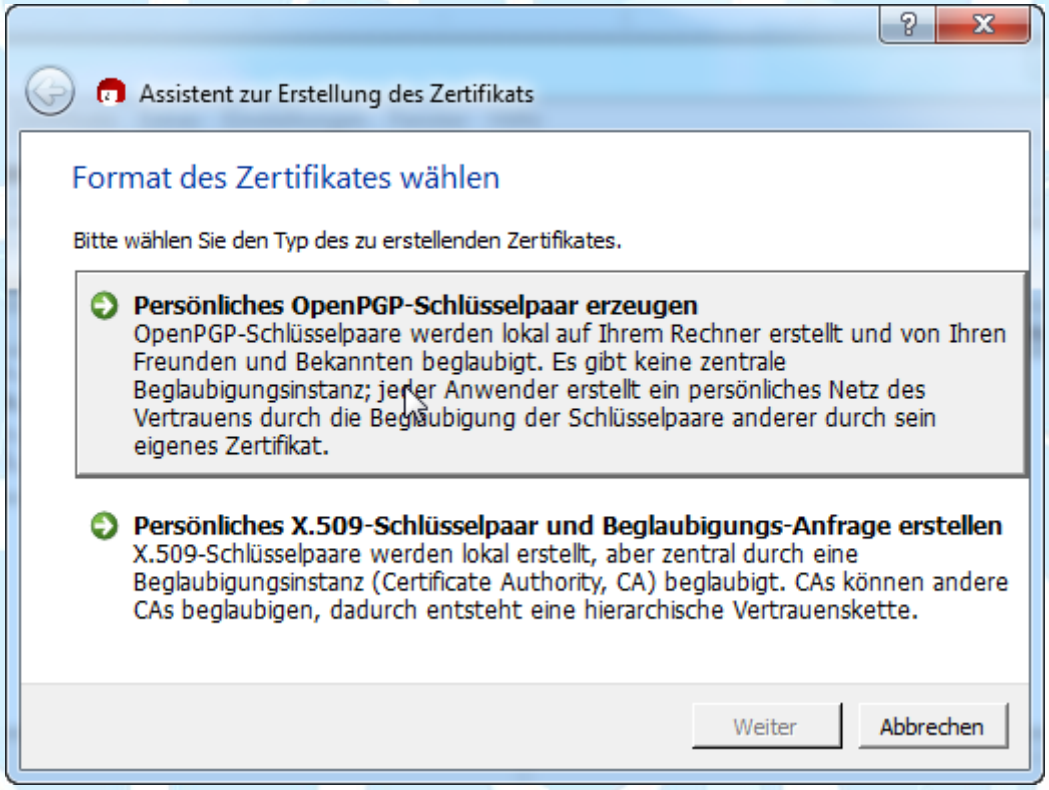
- GNUPG: Kommandozeilenprogramm
- GPGWin, Download unter http://slproweb.com/products/Win32OpenSSL.html
- Kleopatra: Schlüsselmanager
- etc.

PGP – Schlüssel erstellen 1

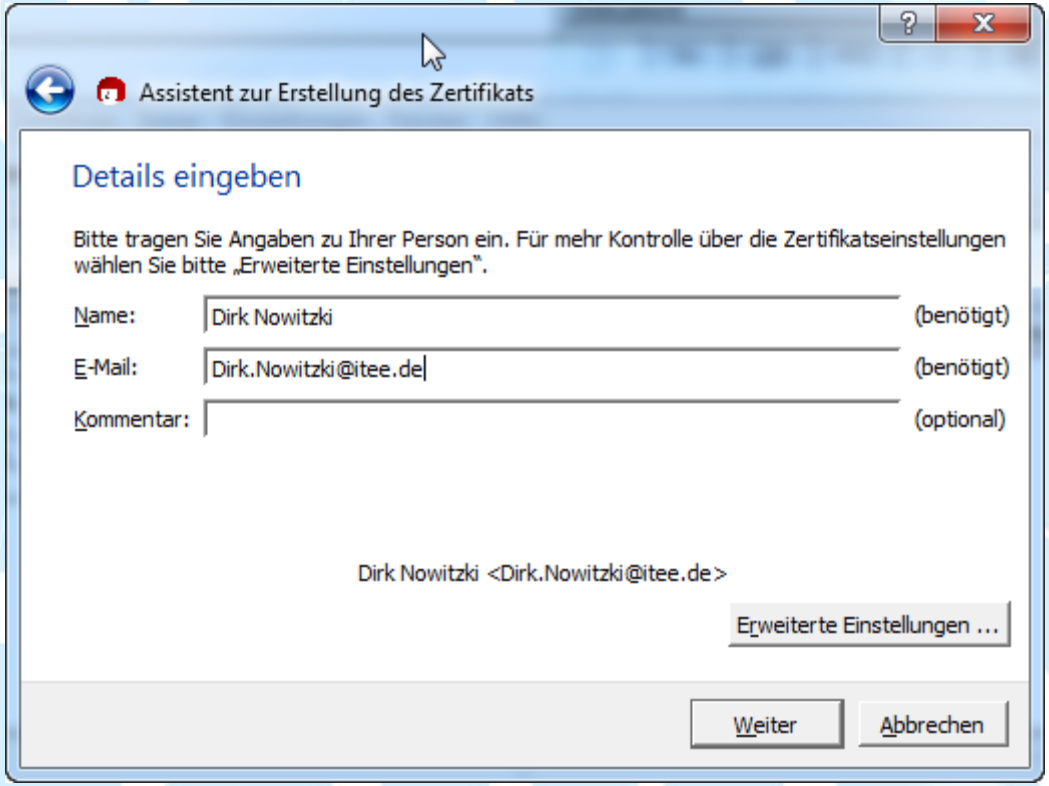
- Schlüssel erstellen in Kleopatra



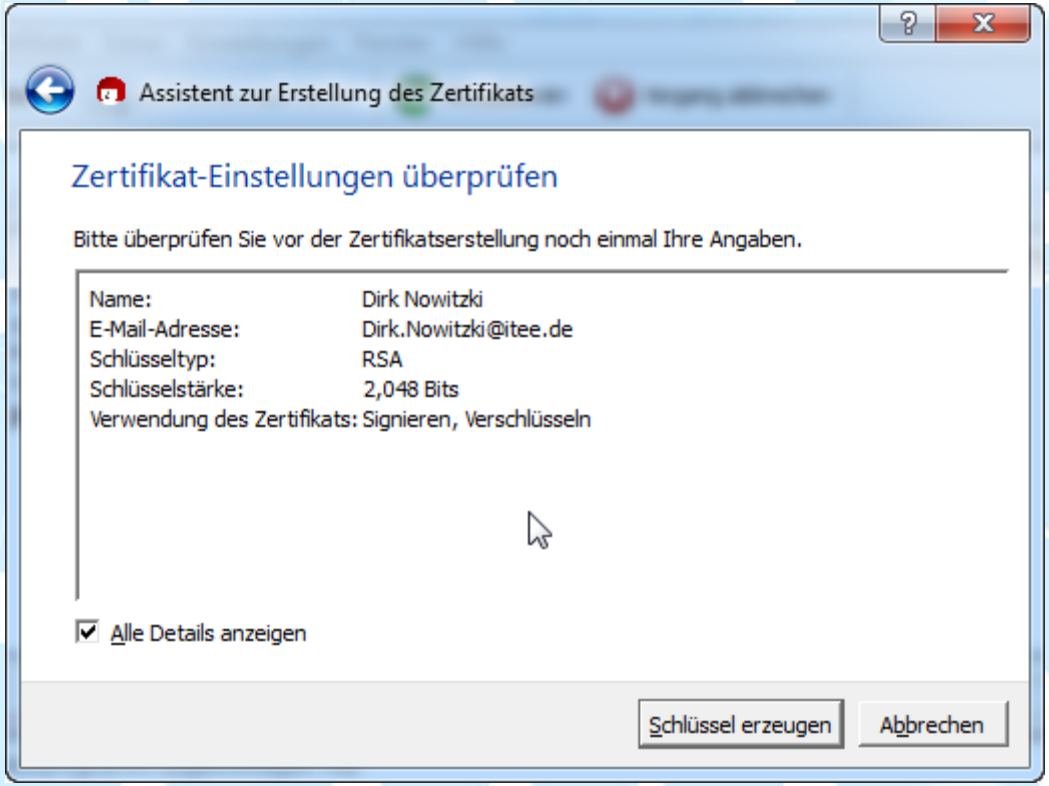
PGP – Schlüssel erstellen 2



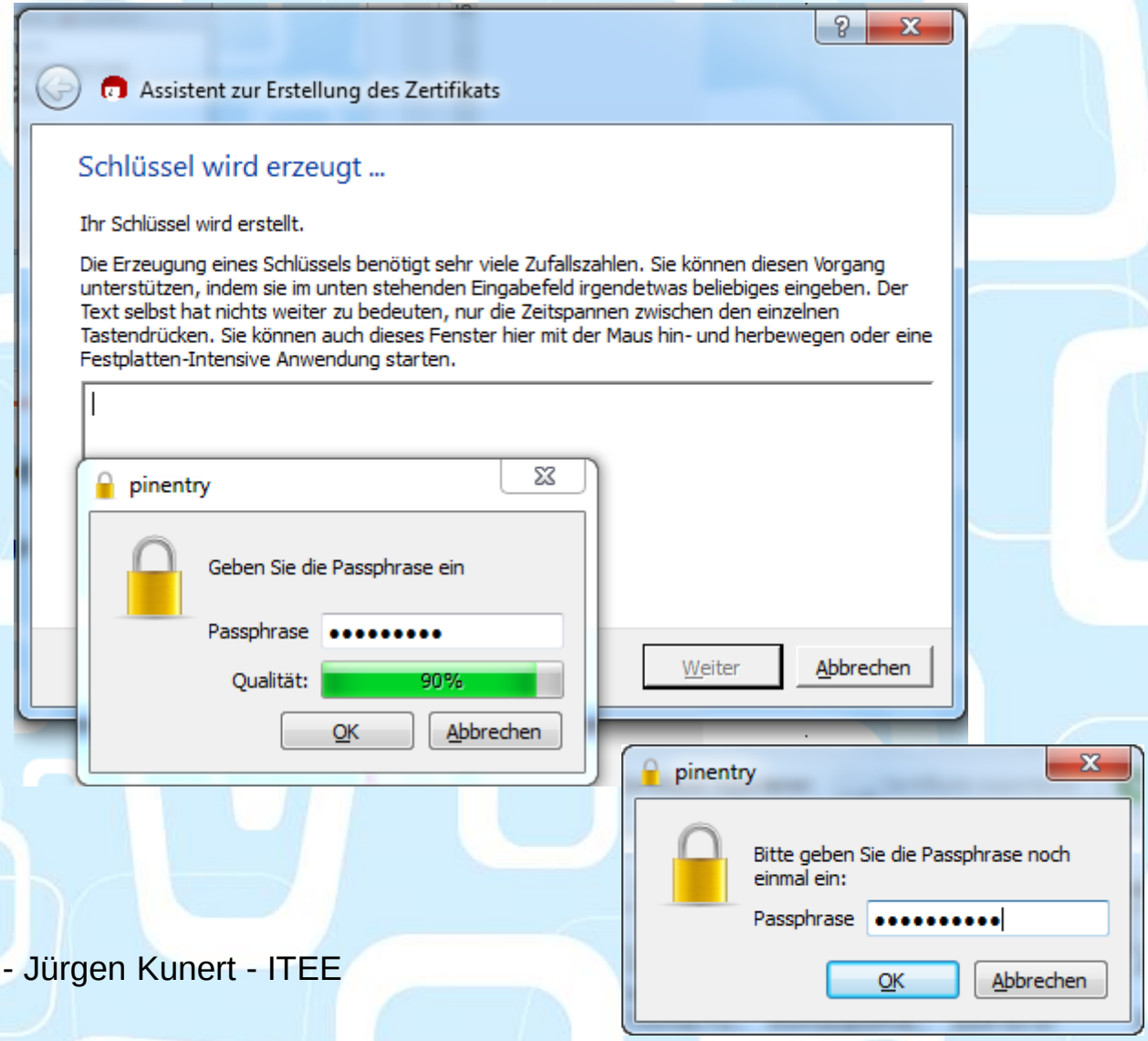
PGP – Schlüssel erstellen 3



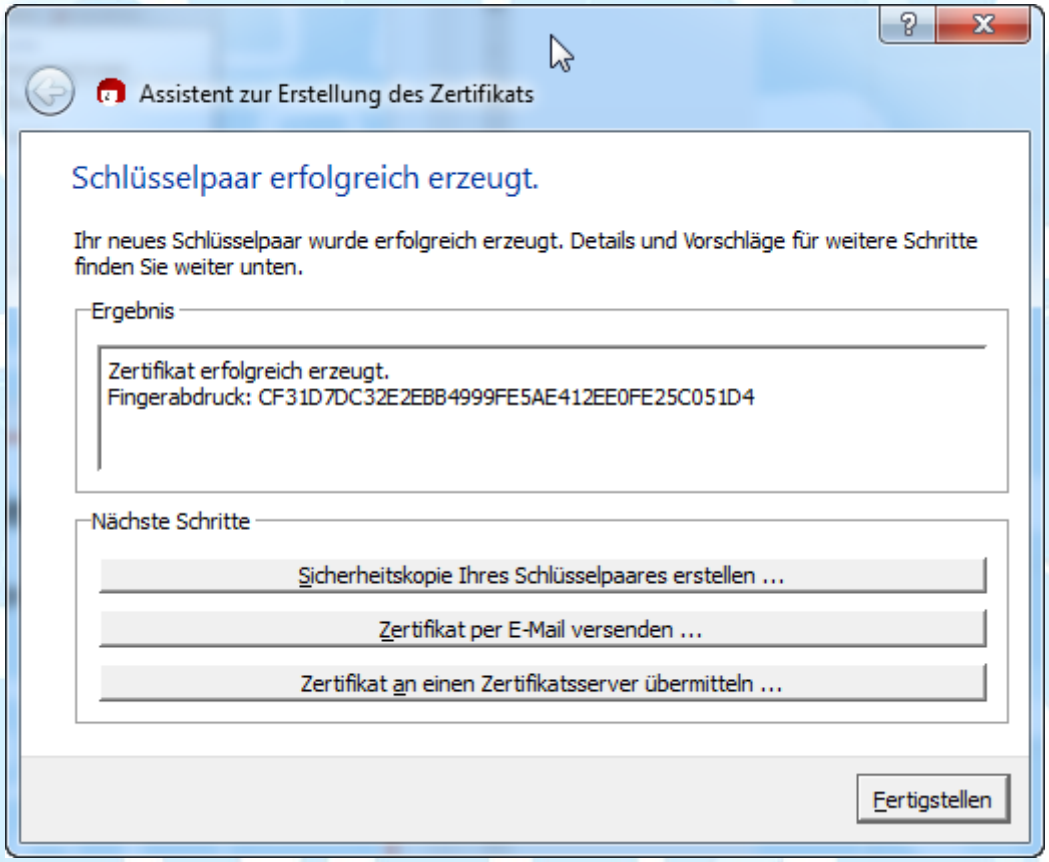
PGP – Schlüssel erstellen 4



PGP – Schlüssel erstellen 5

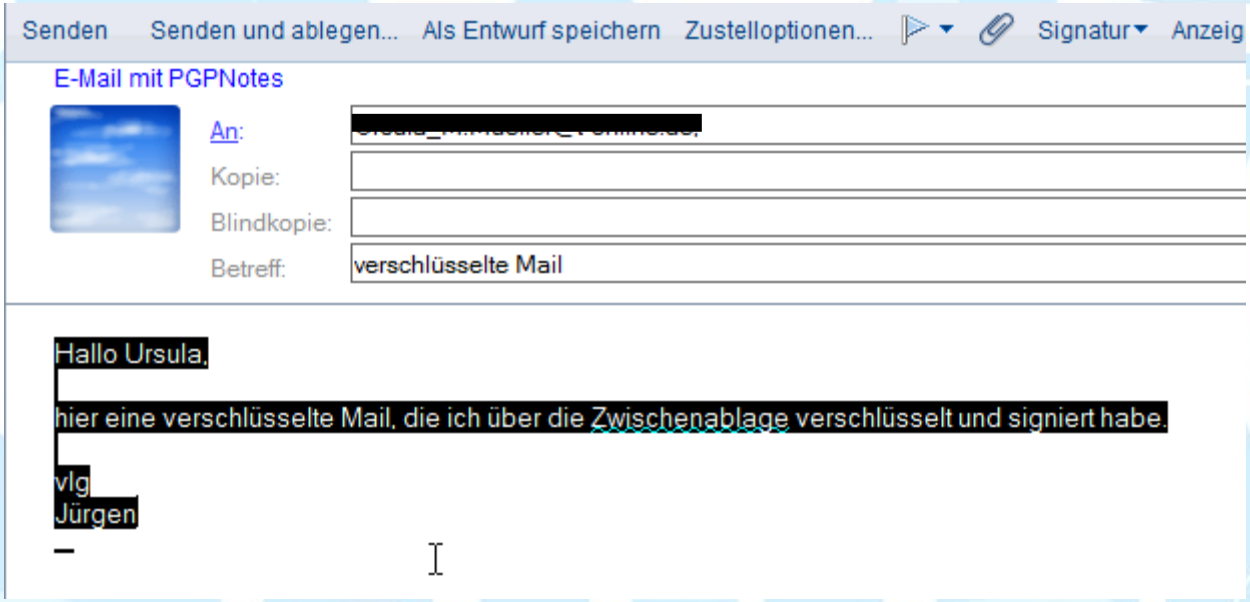


PGP – Schlüssel erstellen 6

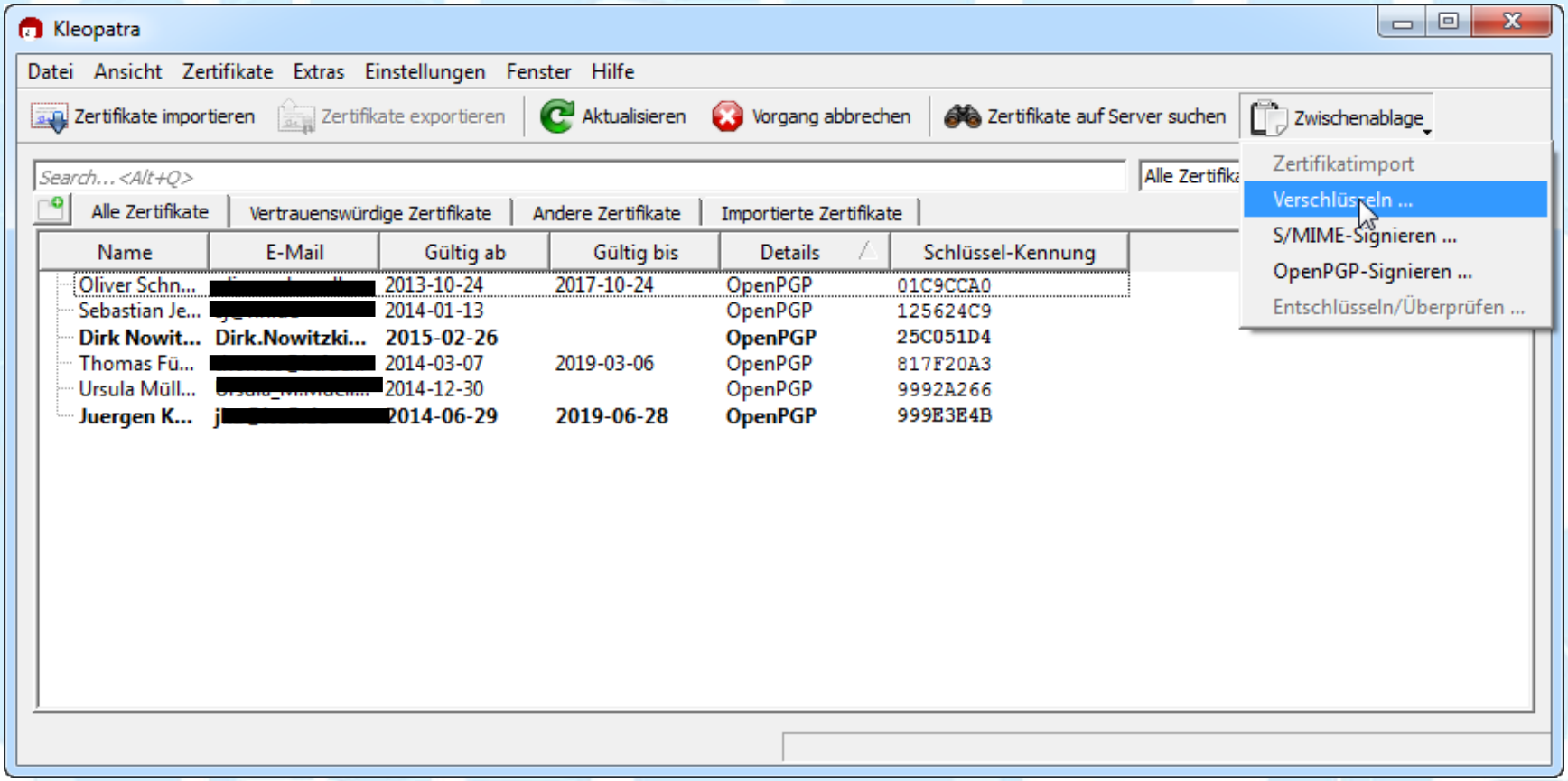


PGP – Benutzung 1

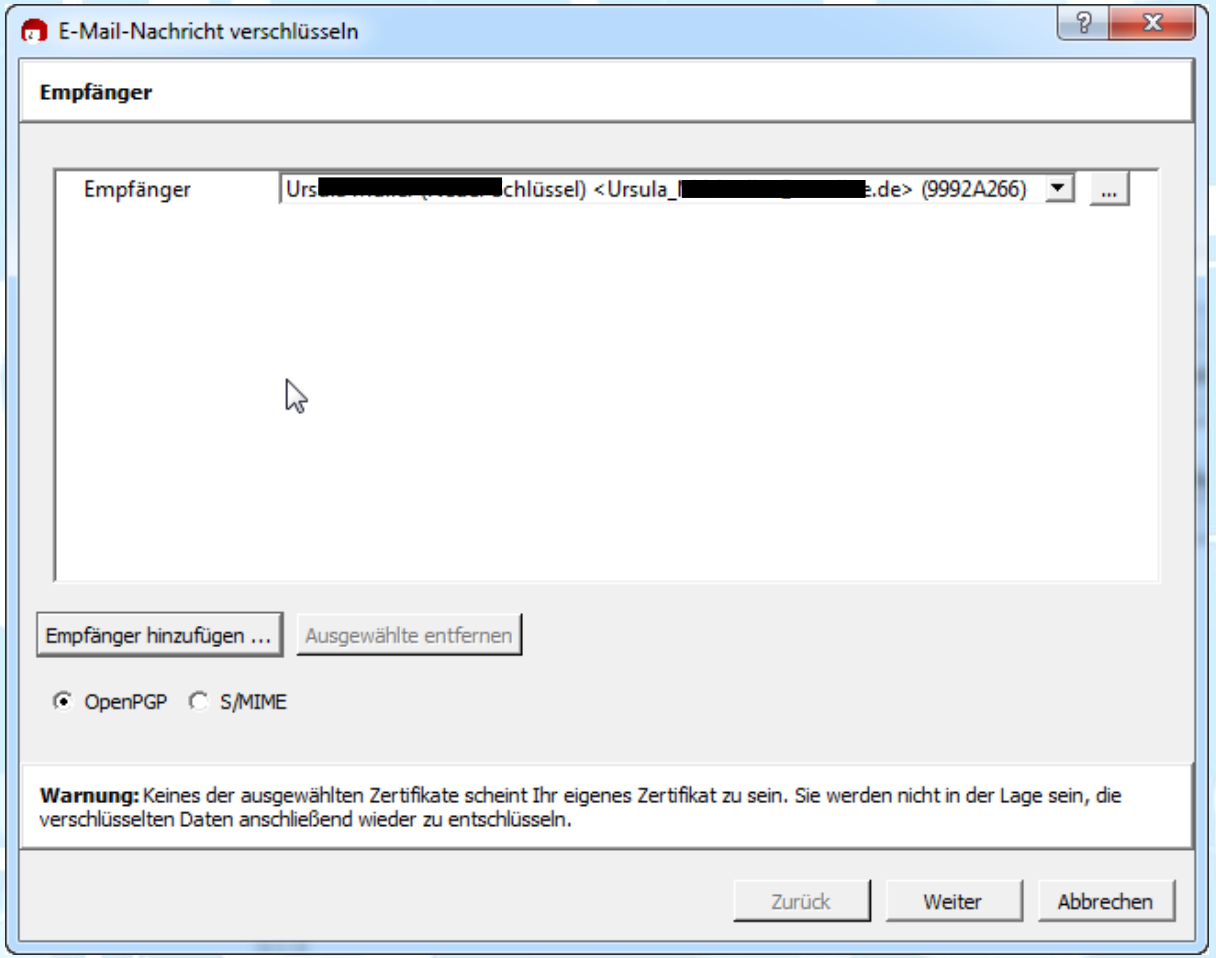
- Die Zwischenablage ist unser Freund



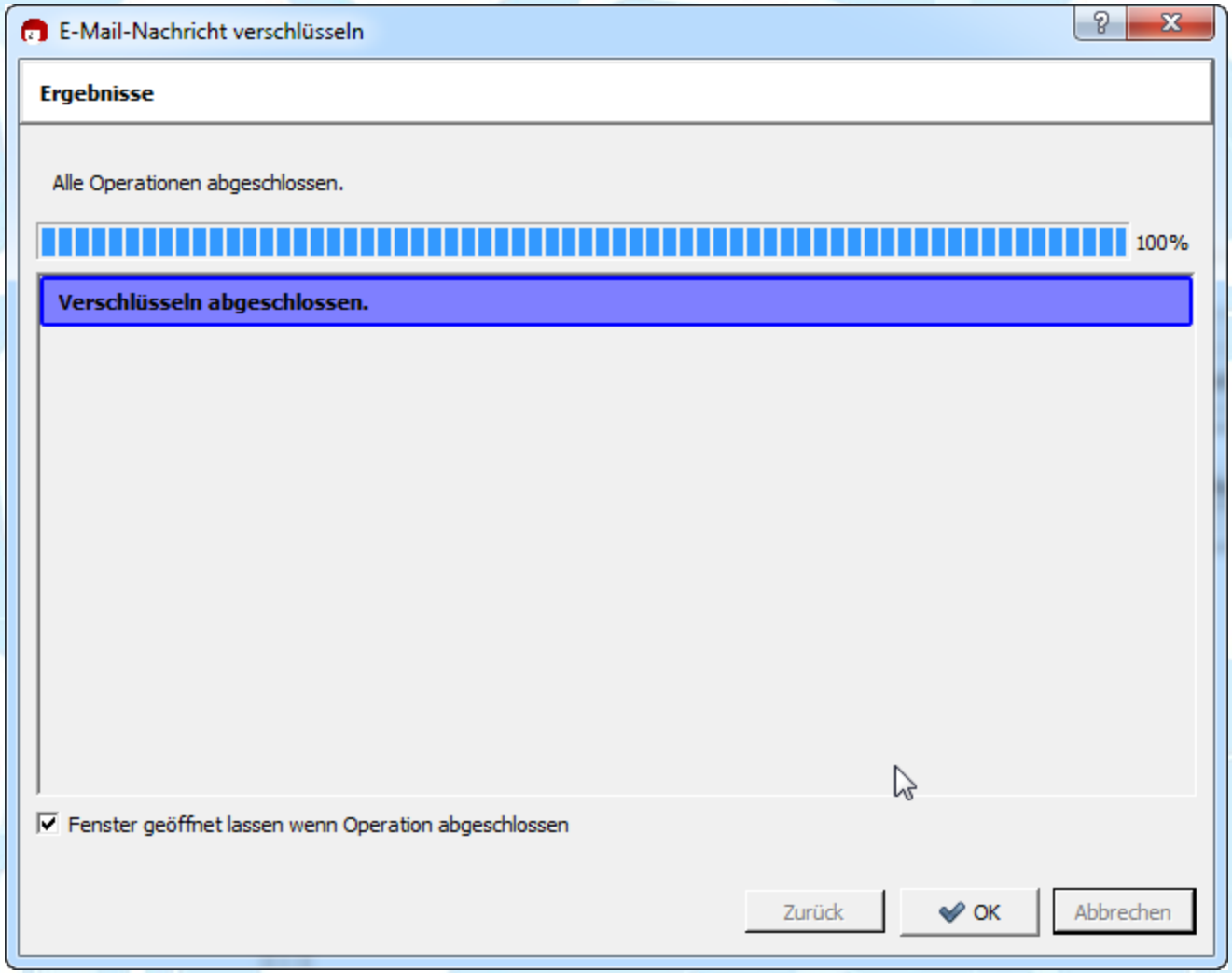
PGP – Benutzung 2



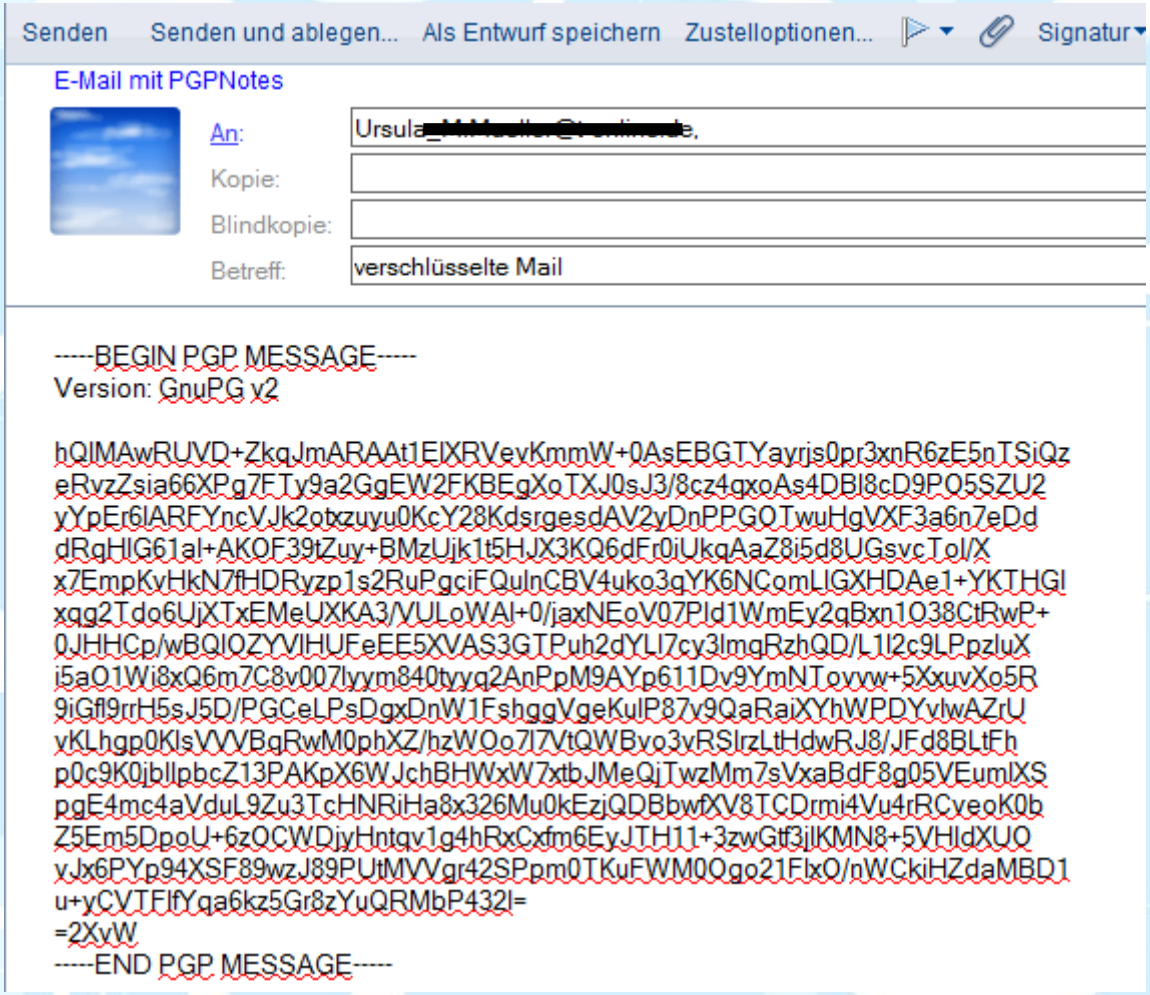
PGP – Benutzung 3



PGP – Benutzung 4

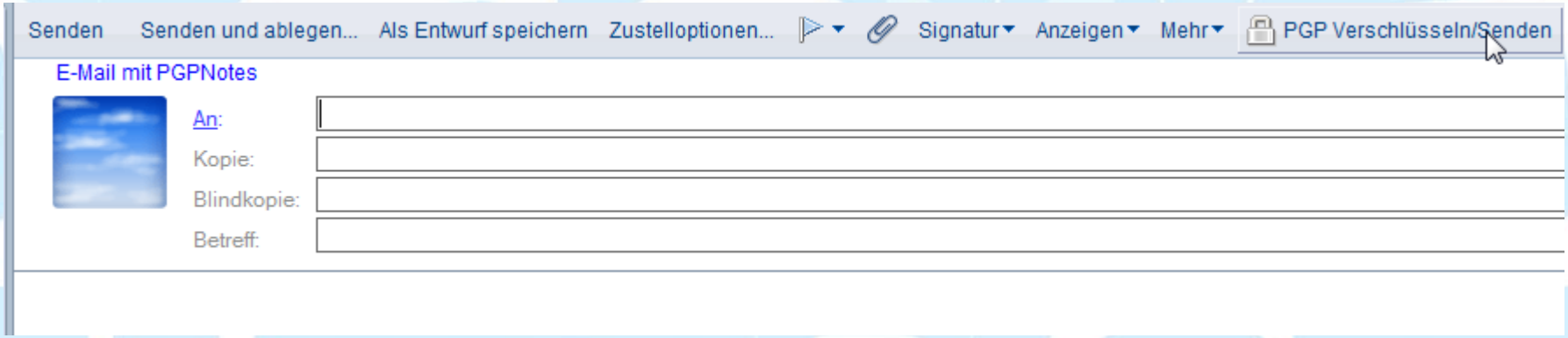


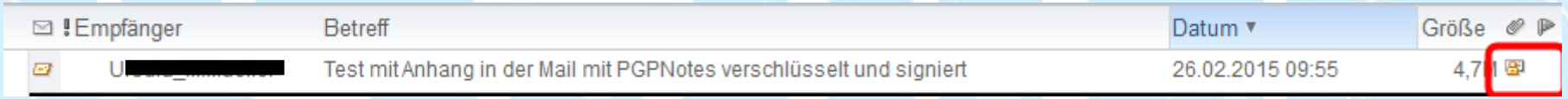
PGP – Benutzung 5



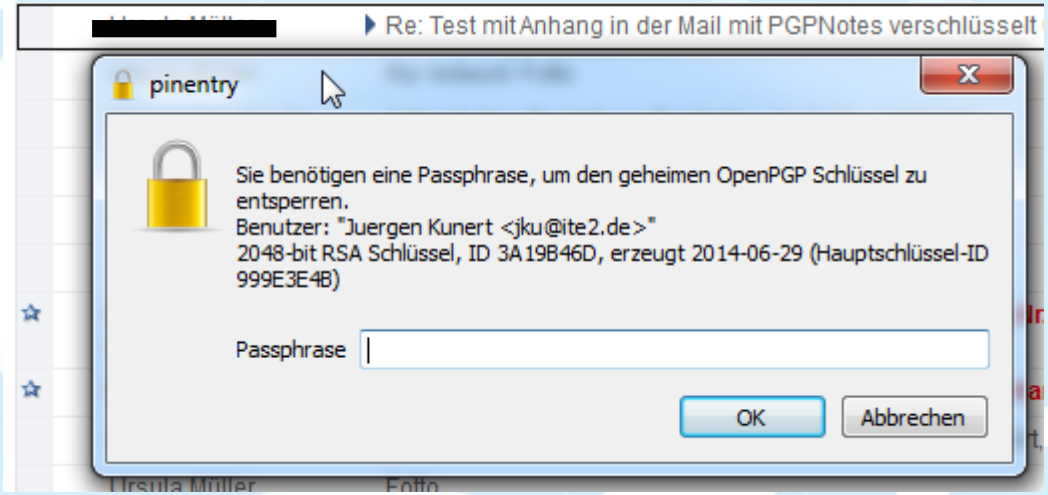
PGPNotes

- Kostenpflichtiges Plug-In für Notes (Teilmaske)





PGPNotes 2


Re: Test mit Anhang in der Mail mit PGPNotes verschlüsselt
pinentry
Sie benötigen eine Passphrase, um den geheimen OpenPGP Schlüssel zu entsperren.
Benutzer: "Juergen Kunert <jku@ite2.de>"
2048-bit RSA Schlüssel, ID 3A19B46D, erzeugt 2014-06-29 (Hauptschlüssel-ID 999E3E4B)
Passphrase
OK
Abbrechen

Unterschiede S/MIME und PGP

- Vertrauen: Zertifikatshierarchie vs. Web Of Trust
- Schlüsselverwaltung: Kleopatra vs. Kontakte
- bei S/MIME wird beim Senden einer signierten Mail der Schlüssel mit versandt, bei PGP nicht
- Open Source
- S/MIME: kann die NSA mitlesen?

Perfect Forward Secrecy

- **Folgenlosigkeit** (englisch *perfect forward secrecy*, *PFS*; auf deutsch etwa *perfekte vorwärts gerichtete Geheimhaltung*) bedeutet in der Kryptographie die Eigenschaft von Schlüsselaustauschprotokollen, dass aus einem aufgedeckten geheimen Langzeitschlüssel nicht auf damit ausgehandelte Sitzungsschlüssel eines Kommunikationskanals geschlossen werden kann.[1]
  Quelle: Wikpedia
- In Notes und Domino aktuell nicht implementiert,
- nur mit Proxy möglich

Alternativen (zu Bordmitteln)

- PGP
- Inhalt in verschlüsseltes PDF oder ZIP einpacken
- Eigenes Gateway zur Mail-Verschlüsselung (mit Schlüsselmanagement) (z.B. IQ-Suite)
- Verschlüsselung über externen Dienstleister/Cloud - Webmail

Was tun? Aspekte für eine Auswahl

- Abhängig von der Anzahl der Kommunikationspartner
- Abhängig von Gesetzen und Rechtsprechung
- Abhängig von Vertretungsregelungen
- Kosten
- Usability für die Endbenutzer
- Supportbarkeit für die internen Mail-Admins (verschlüsselte Mails lassen sich schlecht einsehen) -> Mail-Gateway
- Virenscanner kann nur unverschlüsselte Mails prüfen

Das war‘s zum Thema eMail-Verschlüsselung

Nun wird der
Domino-Webserver
abgesichert

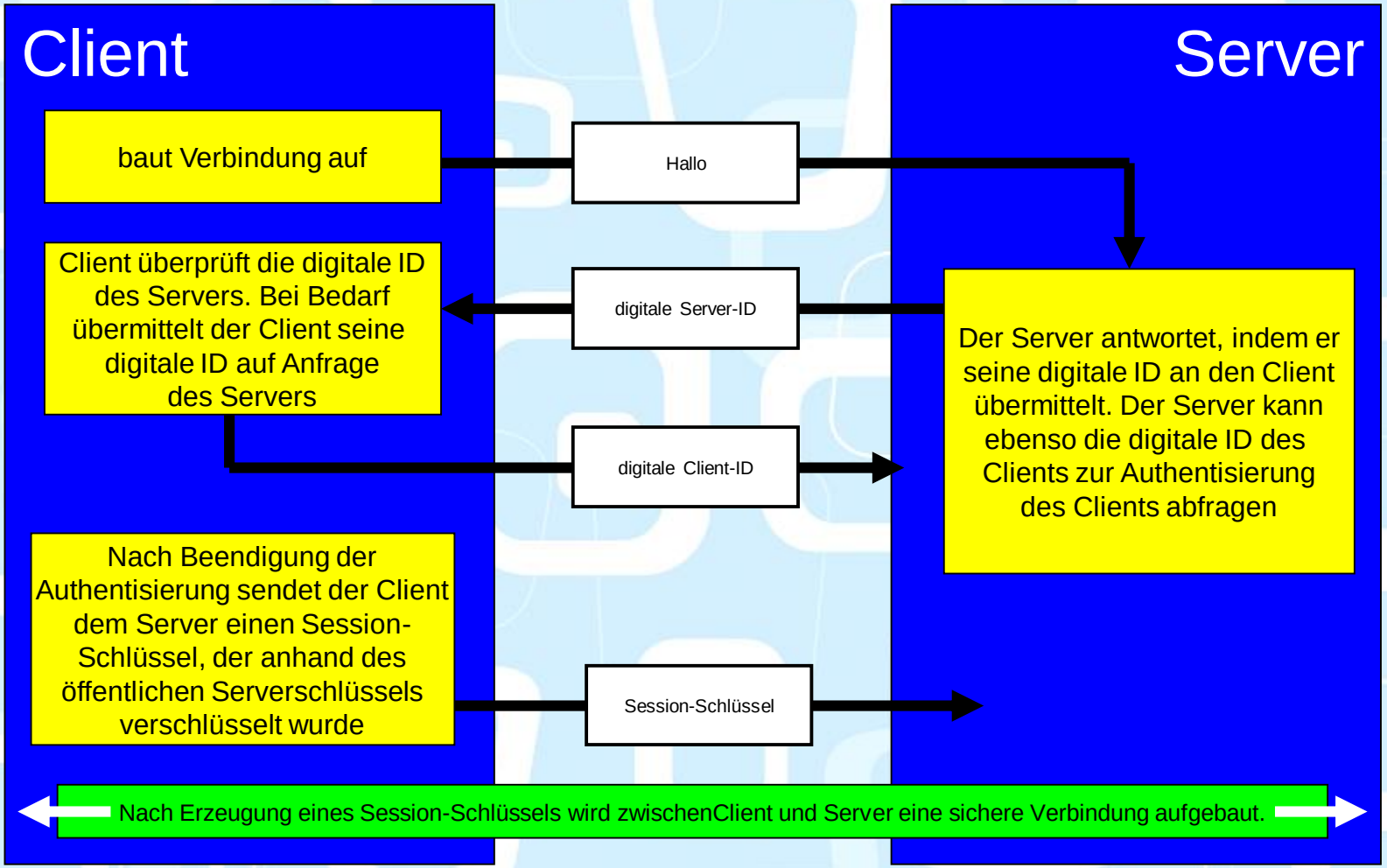
TSL/SSL-Jumpstart

- Wie funktioniert SSL?
- Warum SSL?
- Wie bekomme ich einen Keyring?
- Konfiguration in Domino

SSL/TLS

- steht für Secure Socket Layer
- von Netscape entwickeltes Protokoll für Standard-Browser zum sicheren Übertragen von vertraulichen Informationen über das Internet
- unter dem neuen Namen TLS (Transport Layer Security) weiterentwickelt
- Versionen
  - SSL 2.0 1995
  - SSL 3.0 1996
  - TLS 1.0 1999
  - TLS 1.1 2006 (aktuell nicht von Domino unterstützt)
  - TLS 1.2 2008 (aktuell nicht von Domino unterstützt)
  - TLS 1.3 to be announced

Wie funktioniert SSL?



Warum TLS/SSL?

- Verschlüsselung:
  - Die Kommunikation zwischen Server und Client wird verschlüsselt
- Authentisierung
  - Der Client kann sich sicher sein, dass er mit dem gewünschten Server kommuniziert (unter Benutzung einer PKI)

Sicherheitslücken

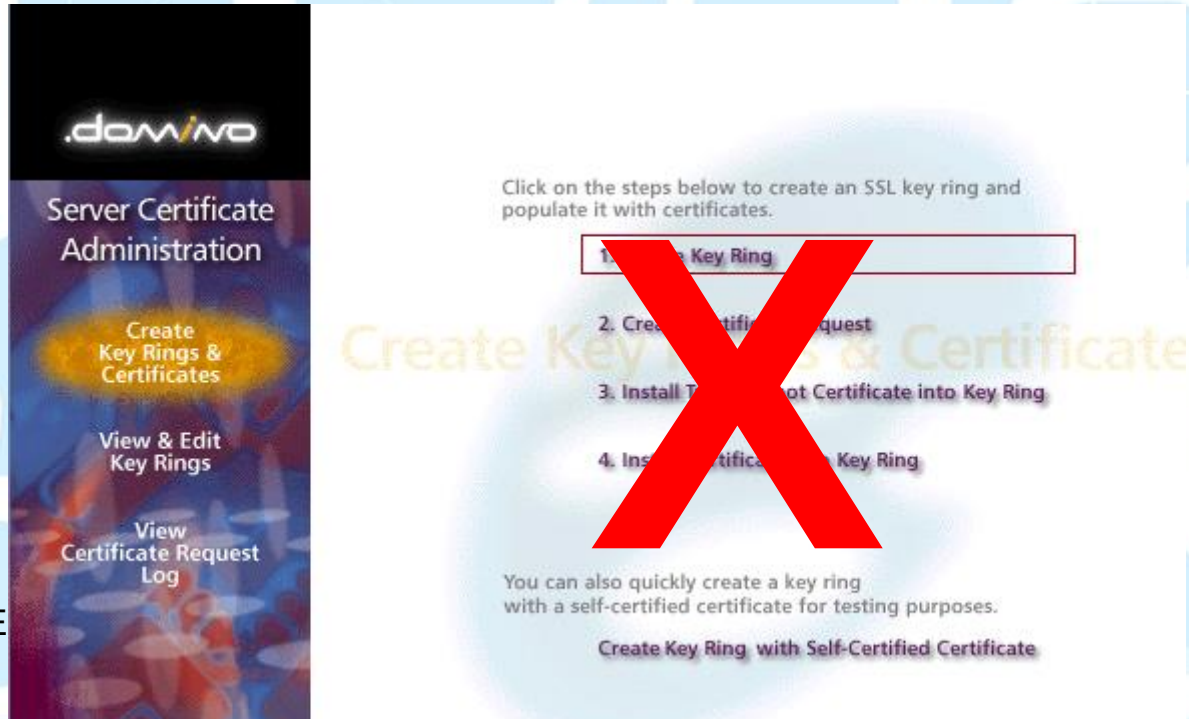
- Poodle
- TLS 1.0
- Heartbleed (Domino nicht betroffen, aber ggf. vorgelagerte Systeme)
- und sicherlich einige, von denen wir noch nichts wissen…

Gekauftes oder selbsterstelltes Zertifikat?

- Nachteil:
  - Ein Gekauftes kostet Geld
  - läuft auch ab
- Vorteile:
  - höhere Sicherheit für die Clients
  - Wird von Browsern und anderen Clients akzeptiert (es gibt Ausnahmen)
  - Keine Arbeiten im Client-Browser

Zertifikate bearbeiten

- „Server Certificate Administration“ wird nicht mehr weiterentwickelt,
- unterstützt keine aktuell sicheren Zertifikate
- Ersatz: openssl und kyrtool



OpenSSL

- Freie Software
- Das Tool, um Zertifikate zu managen
- http://slproweb.com/products/Win32OpenSSL.html

OpenSSL Funktionalität

- CSRs generieren
- Zertifikate erstellen
- Zertifikate ansehen
- Zertifikate verifizieren
- Speicherformate konvertieren

OpenSSL Installation

- http://slproweb.com/products/Win32OpenSSL.html

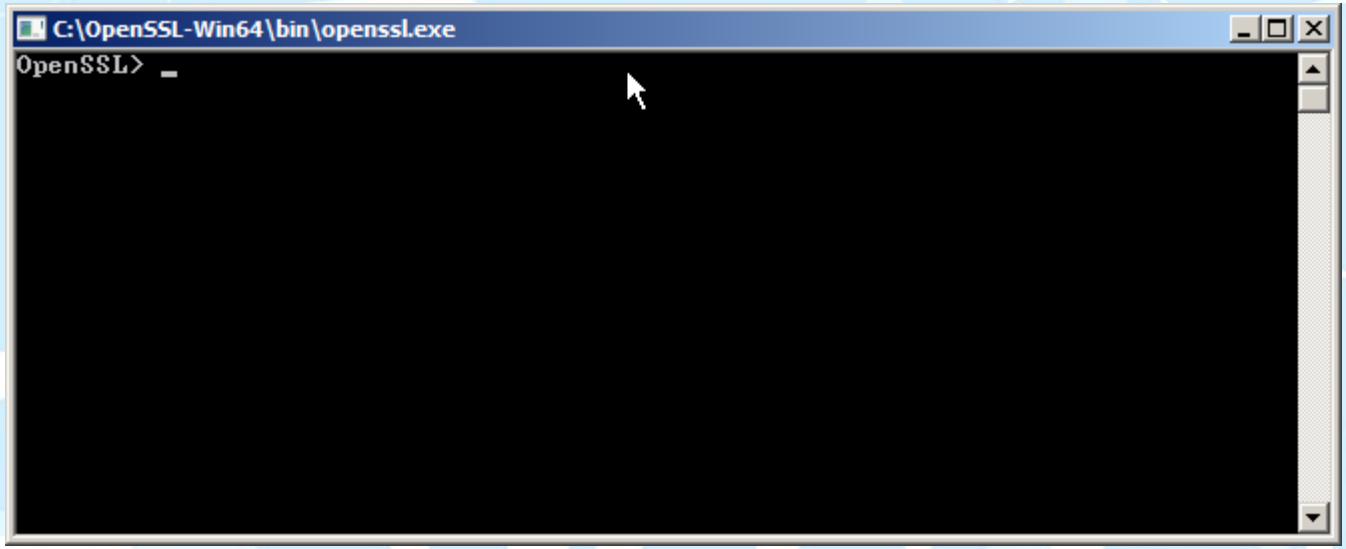
- Wir haben auf einem Win7/64-Windows-Rechner die folgenden Setup-Files genommen:
- **Win64 OpenSSL v1.0.1j** Light1MB Installer
  Installs the most commonly used essentials of Win64 OpenSSL v1.0.1j (Only install this if you need 64-bit OpenSSL for Windows. Only installs on 64-bit versions of Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
- **Visual C++ 2008 Redistributables (x64)** 1.7MB Installer
  Having problems with error messages when trying to run 64-bit OpenSSL? This will likely fix the problem. Only works with Windows 2003 Server and later. Although there is a "newer version" of this installer, this is the correct version to install.

OpenSSL Konfiguration

- OpenSSL-Win64 ist das Installationsverzeichnis von OpenSSL
- C:\OpenSSL-Win64\bin>set OPENSSL_CONF=c:\OpenSSL-Win64\bin\openssl.cfg
- C:\OpenSSL-Win64\bin>set RANDFILE=.rnd

OpenSSL Aufruf

- **Im Zweifel CMD als Administrator ausführen! oder**
- **Starten der openssl.exe**



- **Dann muss bei den folgenden Sequenzen auf das anfängliche openssl verzichtet werden**

Ein (Test-)Zertifikat selbst erstellen

Ein (Test-)Zertifikat selbst erstellen 1

Schlüsselpaar generieren (Datei server.key):

C:\OpenSSL-Win64\bin>openssl genrsa -out server.key 4096

Loading 'screen' into random state - done

Generating RSA private key, 4096 bit long modulus

....++

.....++

e is 65537 (0x10001)

C:\OpenSSL-Win64\bin>

Ein (Test-)Zertifikat selbst erstellen 2

Schlüssel ansehen: (Datei server.key)

C:\OpenSSL-Win64\bin>type server.key

-----BEGIN RSA PRIVATE KEY-----

MIIJKAIBAAKCAgEAwxx5LDjqs4s4jBGNncErPBFNuOMX5
wZzl8U1b2XfwBwxr8g6

...

1p6/tIUFal4CKJ2pLW8Xd3xqA3yQT/COSs2kB6XFP2vj8Zr
Bsh+TXQVKX2k=

-----END RSA PRIVATE KEY-----

C:\OpenSSL-Win64\bin>

Ein (Test-)Zertifikat selbst erstellen 3

CSR (server.csr) erzeugen, Zertifikatsinformationen eingeben:

```
C:\OpenSSL-Win64\bin>openssl req -new -sha256 -key server.key -out server.csr
Loading 'screen' into random state - done
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:DE
State or Province Name (full name) [Some-State]:Hamburg
Locality Name (eg, city) []:Hamburg
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ITEE
Organizational Unit Name (eg, section) []:Headquarter
Common Name (e.g. server FQDN or YOUR name) []:WIN2008STD01.itee.zz
Email Address []:juergen.kunert@itee.de

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:geheim
An optional company name []:

C:\OpenSSL-Win64\bin>
```

Ein (Test-)Zertifikat selbst erstellen 4

CSR (server.csr) ansehen:

C:\OpenSSL-Win64\bin>type server.csr

-----BEGIN CERTIFICATE REQUEST-----

MIIE+TCCAuECAQAwgZwxCzAJBgNVBAYTAkRFMRAwD
gYDVQQIDAdIYW1idXJnMRAw

...

SNLlFpVXaHEk/JnMh2vOAE+I0+RiX0UiWhiJCBE=

-----END CERTIFICATE REQUEST-----

C:\OpenSSL-Win64\bin>

Ein (Test-)Zertifikat selbst erstellen 5

Zertifikat selbst signieren (server.pem)

C:\OpenSSL-Win64\bin>openssl x509 -req -days 3650 -sha256 -in server.csr -signkey server.key -out server.pem

Loading 'screen' into random state - done

Signature ok

subject=/C=DE/ST=Hamburg/L=Hamburg/O=ITEE/OU=Headquarter/CN=WIN2008STD01.itee.zz/emailAddress=juergen.kunert@itee.de

Getting Private key

Ein (Test-)Zertifikat selbst erstellen 6

Zertifikat (server.pem)ansehen

C:\OpenSSL-Win64\bin>type server.pem

-----BEGIN CERTIFICATE-----

MIIFtjCCA54CCQCkcRqajNvUHjANBgkqhkiG9w0BAQsFA
DCBnDELMAkGA1UEBhMC

...

0bfHP4VI5zMR901JYjIFzjt51KAnGYeiv0k=

-----END CERTIFICATE-----

Ein (Test-)Zertifikat selbst erstellen 7

- Und jetzt muss das Ganze in einen Schlüsselring:
- Dazu verwenden wir kyrtool
- Download:
  http://www.ibm.com/support/fixcentral/swg/quickorder?parent=ibm%7ELotus&product=ibm/Lotus/Lotus+Domino&release=9.0.1.2&platform=All&function=fixId&fixids=KYRTool_9x_ClientServer&includeSupersedes=0&source=fc
- Installation:
  (Kopieren) von kyrtool.exe ins Notes/Domino Programmverzeichnis

Ein (Test-)Zertifikat selbst erstellen 8

kyrtool Help:

[C:\] kyrtool =c:\lotus\notes\notes.ini -h

KyrTool v1.0

kyrtool [=/path/to/notes.ini] command [subcommand] [flags]

Commands:
create Create a new keyring file
delete Delete a root in a keyring file
import Import into a keyring file
show Show information about a keyring file
verify Verify the content of a PEM import file

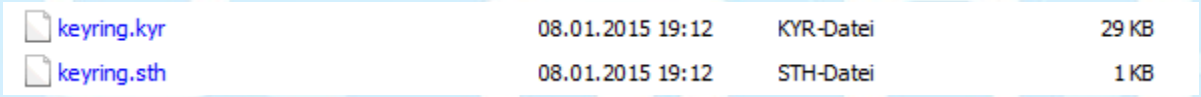
Ein (Test-)Zertifikat selbst erstellen 9

Schlüsselring erzeugen

C:\Program Files (x86)\IBM\Notes>kyrtool ="C:\Program Files (x86)\IBM\Notes\notes.ini" create -k c:\lotus\notes\data\keyring.kyr -p geheim

Keyfile c:\lotus\notes\data\keyring.kyr created successfully

C:\Program Files (x86)\IBM\Notes>



Ein (Test-)Zertifikat selbst erstellen 10

Zertifikate (server.key und server.pem) zusammenfügen (server.txt)

C:\OpenSSL-Win64\bin>COPY C:\OpenSSL-Win64\bin\server.key+C:\OpenSSL-Win64\bin\server.pem server.txt

C:\OpenSSL-Win64\bin\server.key

C:\OpenSSL-Win64\bin\server.pem

Ein (Test-)Zertifikat selbst erstellen 11

Zwischenergebnis ansehen:

```
C:\OpenSSL-Win64\bin>type server.txt
-----BEGIN RSA PRIVATE KEY-----
MIIJKAIBAAKCAgEAwxx5LDjqs4s4jBGNncErPBFNuOMX5wZzl8U1b2XfwBwxr8g6
...
1p6/tIUFal4CKJ2pLW8Xd3xqA3yQT/COSs2kB6XFP2vj8ZrBsh+TXQVKX2k=
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIFtjCCA54CCQCkcRqajNvUHjANBgkqhkiG9w0BAQsFADCBnDELMAkGA1UEBhMC
...
ZzzPMQuMHhpQuHfvlu3chwcKWrw+aUBng+oQLf6kvDoPP/ZqcNyLX7hq+CFW9xmn
0bfHP4VI5zMR901JYjIFzjt51KAnGYeiv0k=
-----END CERTIFICATE-----

C:\OpenSSL-Win64\bin>dir server.*
 Volume in Laufwerk C: hat keine Bezeichnung.
 Volumeseriennummer: A0FB-9BD7

 Verzeichnis von C:\OpenSSL-Win64\bin
08.01.2015  18:59             1.801 server.csr
08.01.2015  18:51             3.243 server.key
08.01.2015  19:01             2.041 server.pem
08.01.2015  20:31             5.285 server.txt
               4 Datei(en),         12.370 Bytes
               0 Verzeichnis(se),  4.394.057.728 Bytes frei
```

Ein (Test-)Zertifikat selbst erstellen 12

server.txt verifizieren:

C:\Program Files (x86)\IBM\Notes>kyrtool ="C:\Program Files (x86)\IBM\Notes\notes.ini" verify "C:\OpenSSL-Win64\bin\server.txt"

KyrTool v1.0

Successfully read 4096 bit RSA private key

INFO: Successfully read 1 certificates

INFO: Private key matches leaf certificate

INFO: Final certificate in chain is self-signed

Ein (Test-)Zertifikat selbst erstellen 13

Zertifikat in den Schlüsselring importieren:

C:\Program Files (x86)\IBM\Notes>kyrtool ="C:\Program Files (x86)\IBM\Notes\notes.ini" import all -k c:\lotus\notes\data\keyring.kyr -i "C:\OpenSSL-Win64\bin\server.txt"

Using keyring path 'c:\lotus\notes\data\keyring.kyr'

Successfully read 4096 bit RSA private key

SECIssUpdateKeyringPrivateKey succeeded

SECIssUpdateKeyringLeafCert succeeded

Ein (Test-)Zertifikat selbst erstellen 14

Schlüssel anzeigen:

C:\Program Files (x86)\IBM\Notes>kyrtool ="C:\Program Files (x86)\IBM\Notes\notes.ini" **show keys -k** c:\lotus\notes\data\keyring.kyr

Using keyring path 'c:\lotus\notes\data\keyring.kyr'

Key length: 4096 bits

-----BEGIN PUBLIC KEY-----
MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAwxx5LDjqs4s4jBGNncEr
...
u9GAIJwEWeEfdSXN8/JcuUkCAwEAAQ==
-----END PUBLIC KEY-----

Key length: 4096 bits

-----BEGIN RSA PRIVATE KEY-----
MIIJKAIBAAKCAgEAwxx5LDjqs4s4jBGNncErPBFNuOMX5wZzl8U1b2XfwBwxr8g6
...
1p6/tIUFal4CKJ2pLW8Xd3xqA3yQT/COSs2kB6XFP2vj8ZrBsh+TXQVKX2k=
-----END RSA PRIVATE KEY-----

Ein (Test-)Zertifikat selbst erstellen 15

Zertifikate anzeigen:

C:\Program Files (x86)\IBM\Notes>kyrtool ="C:\Program Files (x86)\IBM\Notes\notes.ini" show certs -k c:\lotus\notes\data\keyring.kyr

Using keyring path 'c:\lotus\notes\data\keyring.kyr'

Certificate #0

Subject:
EMAIL=juergen.kunert@itee.de/CN=WIN2008STD01.itee.zz/OU=Headquarter/O=ITEE/L=Hamburg/ST=Hamburg/C=DE

Issuer:
EMAIL=juergen.kunert@itee.de/CN=WIN2008STD01.itee.zz/OU=Headquarter/O=ITEE/L=Hamburg/ST=Hamburg/C=DE

Not Before: 08.01.2015 19:01:41

Not After: 05.01.2025 19:01:41

Key length: 4096 bits

Signature Alg: sha256WithRSAEncryption

-----BEGIN CERTIFICATE-----

MIIFtjCCA54CCQCkcRqajNvUHjANBgkqhkiG9w0BAQsFADCBnDELMAkGA1UEBhMC

...

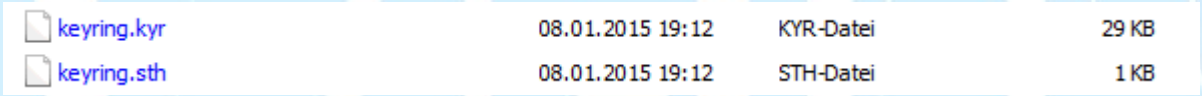
0bfHP4VI5zMR901JYjIFzjt51KAnGYeiv0k=

-----END CERTIFICATE-----

Ein (Test-)Zertifikat selbst erstellen 16

Zertifikate auf den Server kopieren:

Domino/Data:



Ein Zertifikat erwerben

Ein Zertifikat erwerben 1

Schlüsselpaar generieren (Datei server.key):

C:\OpenSSL-Win64\bin>openssl genrsa -out server.key 4096

Loading 'screen' into random state - done

Generating RSA private key, 4096 bit long modulus

....++

.....++

e is 65537 (0x10001)

C:\OpenSSL-Win64\bin>

Ein Zertifikat erwerben 2

Erzeugten Schlüssel ansehen: (Datei server.key)

C:\OpenSSL-Win64\bin>type server.key

-----BEGIN RSA PRIVATE KEY-----

MIIJKAIBAAKCAgEAwxx5LDjqs4s4jBGNncErPBFNuOMX5wZzl8U1b2XfwBwxr8g6

...

1p6/tIUFal4CKJ2pLW8Xd3xqA3yQT/COSs2kB6XFP2vj8ZrBsh+TXQVKX2k=

-----END RSA PRIVATE KEY-----

C:\OpenSSL-Win64\bin>

Ein Zertifikat erwerben 3

CSR (Certificate Signing Request, Datei server.csr) erzeugen, Zertifikatsinformationen eingeben:

```
C:\OpenSSL-Win64\bin>openssl req -new -sha256 -key server.key -out server.csr

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:.
State or Province Name (full name) []:
Locality Name (eg, city) [Default City]:.
Organization Name (eg, company) [Default Company Ltd]:.
Organizational Unit Name (eg, section) []:.
Common Name (eg, your name or your server's hostname) []:www.example.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
C:\OpenSSL-Win64\bin>
```

Ein Zertifikat erwerben 4

CSR (server.csr) ansehen:

C:\OpenSSL-Win64\bin>type server.csr

-----BEGIN CERTIFICATE REQUEST-----

MIIE+TCCAuECAQAwgZwxCzAJBgNVBAYTAkRFMRAwD
gYDVQQIDAdIYW1idXJnMRAw

...

SNLlFpVXaHEk/JnMh2vOAE+I0+RiX0UiWhiJCBE=

-----END CERTIFICATE REQUEST-----

C:\OpenSSL-Win64\bin>

Ein Zertifikat erwerben 5

- Auf die Webseite des Trustcenters gehen, auswählen, beraten lassen
- Fragen, welche Zertifikat das passende ist
  - Wir wollen Webmail/Traveler absichern
  - Wir wollen folgende Endgeräte einsetzen
  - Das Zertifikat soll so lange gelten

ZERTIFIKATSEIGENSCHAFTEN:						
Zertifiziert	Domain Beispiel Domain	Domain Beispiel Domain	Domain Beispiel Domain	Identität Beispiel Identität	Identität Beispiel Identität	Identität Beispiel Identität
Unterstützte Browser ohne Fehlermeldung	ab 5.01 ab 6.0 ab 5.0 ab 8.0 ab 1.0 ab 1.0 ab 1.0 ab 1.0 ab 1.5	ab 5.01 ab 4.51 ab 5.0 ab 7.0 ab 1.0 ab 1.0 ab 1.0 ab 1.0 ab 3.0	ab 3.0 ab 2.0 ab 3.0 ab 3.0 ab 1.0 ab 1.0 ab 1.0 ab 1.0 ab 1.0	ab 5.01 ab 6.0 ab 5.0 ab 8.0 ab 1.0 ab 1.0 ab 1.0 ab 1.0 ab 1.5	ab 5.01 ab 4.51 ab 5.0 ab 7.0 ab 1.0 ab 1.0 ab 1.0 ab 1.0 ab 3.0	ab 3.0 ab 2.0 ab 3.0 ab 3.0 ab 1.0 ab 1.0 ab 1.0 ab 1.0 ab 1.0

Ein Zertifikat erwerben 6

- Auf die Webseite des Trustcenters gehen, auswählen, beraten lassen

Darstellung (Muster)	 SiteSeal	 SiteSeal	 yyyy-mm-dd SiteSeal	 TrustLogo (außer bei 30 Tage, MDC und UCC)	 TrustLogo	 yyyy-mm-dd TrustLogo
Zwischen-zertifikat serverseitig erforderlich	Ja Beispiel Zwischen-zertifikat	Ja Beispiel Zwischen-zertifikat	Ja Beispiel Zwischen-zertifikat	Ja Beispiel Zwischen-zertifikat	Ja Beispiel Zwischen-zertifikat	Ja Beispiel Zwischen-zertifikat
Ausstellende CA	Comodo	RapidSSL/GeoTrust	Thawte/VeriSign	Comodo	GeoTrust	Thawte/VeriSign
Produkt	PositiveSSL	FreeSSL/ RapidSSL	SSL123	InstantSSL/ PremiumSSL	True BusinessID	SSL Web Server
Root-Zertifikat	AddTrust External CA Root	Equifax Secure CA	Thawte Premium Server CA	AddTrust External CA Root	Equifax Secure CA	Thawte Premium Server CA
Validierung	E-Mail-Robot	E-Mail-Robot	E-Mail-Robot	Dokumente, E-Mail-Robot und Rückruf	Dokumente und Rückruf	Dokumente und Rückruf
Ausstellung in (Richtwert)	10 Minuten[1]	10 Minuten[1]	30 Minuten[1]	10 Minuten[1]	2-3 Werktagen[1]	2-3 Werktagen[1]
Kostenloser Austausch[2]	ja	**bei uns inklusive**	ja	ja	ja	ja
Zusätzliche physikalische Maschinen	**bei uns ohne Aufpreis**	ohne Aufpreis	gleich dem Zertifikatspreis	**bei uns ohne Aufpreis**	ohne Aufpreis	gleich dem Zertifikatspreis
Empfohlen für	Adminpanels	Intranetsites	Mobilsites	kleine Shops	mittlere Shops	große Shops

Ein Zertifikat erwerben 7

SSL-ZERTIFIKATE & TRUSTLOGOS **TRUST IT**

2. Schritt: Bereitstellung Ihrer Zertifizierungsanforderung (CSR)

Zunächst erstellen Sie eine Zertifizierungsanforderung (CSR) mit Ihrer Serversoftware. Entsprechende Anleitungen für die gängigsten Server finden Sie auf unserer englischsprachigen Partnersite. Sobald Sie Ihr CSR erstellt haben, können Sie mit der Bestellung fortfahren.

Bei der Wahl Ihres Allgemeinen Namens (CN) haben Sie die folgenden Möglichkeiten:

- Ihr voller Domainname (FQDN), z.B. www.domain.de, schützt https://www.domain.de/...

Bitte achten Sie darauf, dass Ihr privater Schlüssel mindestens 2048 bit und maximal 4096 bit lang sein darf.

Nachdem Sie das CSR mit Ihrer Serversoftware erstellt haben, kopieren Sie dessen Inhalt mit Hilfe eines Texteditors in das folgende Textfeld. Ihr CSR sollte dabei ungefähr so aussehen:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDUDCCArkCAQAwdTEWMBQGA1UEAxMNdGVzdC50ZXN0LmNvbTESMBAGA1UECxMJ
TWFya2V0aW5nMREwDwYDVQQKEwhUZXN0IE9yZzESMBAGA1UEBxMJVGVzdCBDaXR5
...
Rq+blLr5X5iQdzyFlpLqPlMck5VeleCz0R9/0ekGSRno7ow4TVyxAF6J6ozDaw7e
GisfZw40VLTO/6IGvK2jXOi+t58RFQ8WYTOcTRlPnkG8B/uV
-----END CERTIFICATE REQUEST-----
```

Bei Verlängerung eines domainvalidierten Zertifikates unter IIS beachten Sie unbedingt unsere Hinweise.

Probleme mit Ihrer Zertifizierungsanforderung? Prüfen Sie Ihr CSR hier.

Zertifizierungs-anforderung: *

Verwendete Serversoftware: Lotus Domino *

Ein Zertifikat erwerben 8

SSL-ZERTIFIKATE & TRUSTLOGOS **TRUST IT**

2. Schritt: Bereitstellung Ihrer Zertifizierungsanforderung (CSR)

Zunächst erstellen Sie eine Zertifizierungsanforderung (CSR) mit Ihrer Serversoftware. Entsprechende Anleitungen für die gängigsten Server finden Sie auf unserer englischsprachigen Partnersite. Sobald Sie Ihr CSR erstellt haben, können Sie mit der Bestellung fortfahren.

Bei der Wahl Ihres Allgemeinen Namens (CN) haben Sie die folgenden Möglichkeiten:

- Ihr voller Domainname (FQDN), z.B. www.domain.de, schützt https://www.domain.de/...

Bitte achten Sie darauf, dass Ihr privater Schlüssel mindestens 2048 bit und maximal 4096 bit lang sein darf.

Nachdem Sie das CSR mit Ihrer Serversoftware erstellt haben, kopieren Sie dessen Inhalt mit Hilfe eines Texteditors in das folgende Textfeld. Ihr CSR sollte dabei ungefähr so aussehen:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDUDCCArkCAQAwdTEWMBQGA1UEAxMNdGVzdC50ZXN0LmNvbTESMBAGA1UECxMJ
TWFya2V0aW5nMREwDwYDVQQKEwhUZXN0IE9yZzESMBAGA1UEBxMJVGVzdCBDaXR5
...
Rq+blLr5X5iQdzyF1pLqP1Mck5Ve1eCz0R9/OekGSRno7ow4TVyxAF6J6ozDaw7e
GisfZw40VLT0/6IGvK2jX0i+t58RFQ8WYTOcTRlPnkG8B/uV
-----END CERTIFICATE REQUEST-----
```

Ein Zertifikat erwerben 9

Bei Verlängerung eines domainvalidierten Zertifikates unter IIS beachten Sie unbedingt unsere Hinweise.

Probleme mit Ihrer Zertifizierungsanforderung? Prüfen Sie Ihr CSR hier.

Zertifizierungs-anforderung:

Hier einfügen

Verwendete Serversoftware: Lotus Domino *

Ein Zertifikat erwerben 10

- Je nach Sicherheitsstufe des Zertifikats muss der Käufer seine Validität nachweisen (vom Firmenstempel bis zum Handelsregisterauszug)
- Ggf. Zeit einplanen und vorher den Support fragen

Ein Zertifikat erwerben 11

Wir haben entweder

- eine Datei mit einem Zertifikat (server.pem)
- oder
- das Zertifikat in der Zwischenablage

Wir machen daraus in jedem Fall eine Datei (server.pem)

Ein Zertifikat erwerben 12

Zertifikat (server.pem) ansehen

C:\OpenSSL-Win64\bin>type server.pem

-----BEGIN CERTIFICATE-----

MIIFtjCCA54CCQCkcRqajNvUHjANBgkqhkiG9w0BAQsFA
DCBnDELMAkGA1UEBhMC

...

0bfHP4VI5zMR901JYjIFzjt51KAnGYeiv0k=

-----END CERTIFICATE-----

Ein Zertifikat erwerben 13

Zertifikate (server.key und server.pem) zusammenfügen (server.txt)

C:\OpenSSL-Win64\bin>COPY C:\OpenSSL-Win64\bin\server.key+C:\OpenSSL-Win64\bin\server.pem server.txt

C:\OpenSSL-Win64\bin\server.key

C:\OpenSSL-Win64\bin\server.pem

Ggf. auch noch Zwischenzertifikate (Intermediate) einfügen

Ein Zertifikat erwerben 14

Zwischenergebnis ansehen:

```
C:\OpenSSL-Win64\bin>type server.txt
-----BEGIN RSA PRIVATE KEY-----
MIIJKAIBAAKCAgEAwxx5LDjqs4s4jBGNncErPBFNuOMX5wZzl8U1b2XfwBwxr8g6
...
1p6/tIUFal4CKJ2pLW8Xd3xqA3yQT/COSs2kB6XFP2vj8ZrBsh+TXQVKX2k=
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIFtjCCA54CCQCkcRqajNvUHjANBgkqhkiG9w0BAQsFADCBnDELMAkGA1UEBhMC
...
ZzzPMQuMHhpQuHfvlu3chwcKWrw+aUBng+oQLf6kvDoPP/ZqcNyLX7hq+CFW9xmn
0bfHP4VI5zMR901JYjIFzjt51KAnGYeiv0k=
-----END CERTIFICATE-----

C:\OpenSSL-Win64\bin>dir server.*
 Volume in Laufwerk C: hat keine Bezeichnung.
 Volumeseriennummer: A0FB-9BD7

 Verzeichnis von C:\OpenSSL-Win64\bin
08.01.2015  18:59             1.801 server.csr
08.01.2015  18:51             3.243 server.key
08.01.2015  19:01             2.041 server.pem
08.01.2015  20:31             5.285 server.txt
               4 Datei(en),         12.370 Bytes
               0 Verzeichnis(se),  4.394.057.728 Bytes frei
```

Ein Zertifikat erwerben 15

server.txt verifizieren:

C:\Program Files (x86)\IBM\Notes>kyrtool ="C:\Program Files (x86)\IBM\Notes\notes.ini" verify "C:\OpenSSL-Win64\bin\server.txt"

KyrTool v1.0

Successfully read 4096 bit RSA private key

INFO: Successfully read 1 certificates

INFO: Private key matches leaf certificate

INFO: Final certificate in chain is self-signed

Ein Zertifikat erwerben 16

Zertifikat in den Schlüsselring importieren:
C:\Program Files (x86)\IBM\Notes>kyrtool ="C:\Program Files (x86)\IBM\Notes\notes.ini" **import all** -k c:\lotus\notes\data\keyring.kyr -i "C:\OpenSSL-Win64\bin\server.txt"

Using keyring path 'c:\lotus\notes\data\keyring.kyr'
Successfully read 4096 bit RSA private key
SECIssUpdateKeyringPrivateKey succeeded
SECIssUpdateKeyringLeafCert succeeded

Ein Zertifikat erwerben 17

Schlüssel anzeigen:

C:\Program Files (x86)\IBM\Notes>kyrtool ="C:\Program Files (x86)\IBM\Notes\notes.ini" **show keys -k** c:\lotus\notes\data\keyring.kyr

Using keyring path 'c:\lotus\notes\data\keyring.kyr'

Key length: 4096 bits

-----BEGIN PUBLIC KEY-----
MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAwxx5LDjqs4s4jBGNncEr
...
u9GAIJwEWeEfdSXN8/JcuUkCAwEAAQ==
-----END PUBLIC KEY-----

Key length: 4096 bits

-----BEGIN RSA PRIVATE KEY-----
MIIJKAIBAAKCAgEAwxx5LDjqs4s4jBGNncErPBFNuOMX5wZzl8U1b2XfwBwxr8g6
...
1p6/tIUFal4CKJ2pLW8Xd3xqA3yQT/COSs2kB6XFP2vj8ZrBsh+TXQVKX2k=
-----END RSA PRIVATE KEY-----

Ein Zertifikat erwerben 18

Zertifikate anzeigen:

C:\Program Files (x86)\IBM\Notes>kyrtool ="C:\Program Files (x86)\IBM\Notes\notes.ini" show certs -k c:\lotus\notes\data\keyring.kyr

Using keyring path 'c:\lotus\notes\data\keyring.kyr'

Certificate #0

Subject:
EMAIL=juergen.kunert@itee.de/CN=WIN2008STD01.itee.zz/OU=Headquarter/O=ITEE/L=Hamburg/ST=Hamburg/C=DE

Issuer:
EMAIL=juergen.kunert@itee.de/CN=WIN2008STD01.itee.zz/OU=Headquarter/O=ITEE/L=Hamburg/ST=Hamburg/C=DE

Not Before: 08.01.2015 19:01:41

Not After: 05.01.2025 19:01:41

Key length: 4096 bits

Signature Alg: sha256WithRSAEncryption

-----BEGIN CERTIFICATE-----

MIIFtjCCA54CCQCkcRqajNvUHjANBgkqhkiG9w0BAQsFADCBnDELMAkGA1UEBhMC

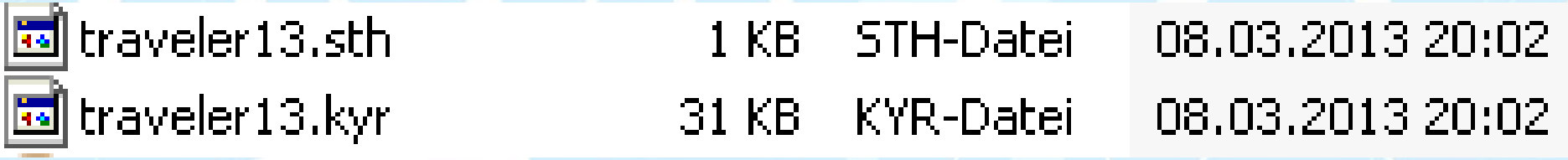
...

0bfHP4VI5zMR901JYjIFzjt51KAnGYeiv0k=

-----END CERTIFICATE-----

Ein Zertifikat erwerben 19

- Jetzt haben wir einen Schlüsselring



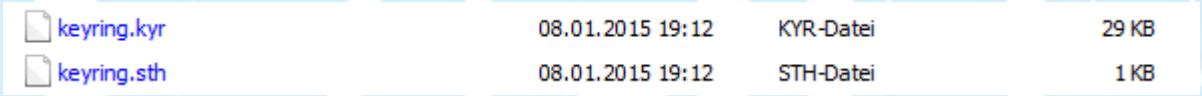
traveler13.sth	1 KB	STH-Datei	08.03.2013 20:02
traveler13.kyr	31 KB	KYR-Datei	08.03.2013 20:02

- mit vom Browser bzw. vom Smartphone akzeptierten Zertifikaten.

Ein Zertifikat erwerben 20

Zertifikate auf den Server kopieren:

Domino/Data:



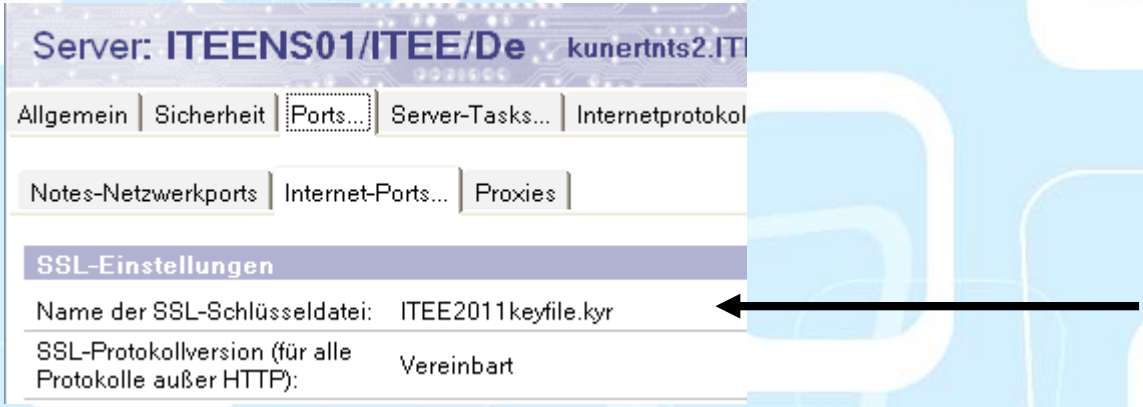
TLS/SSL einrichten 1

1. Domino auf 9.0.1 updaten
2. Dazu entweder
    1. 9.0.1 Fix Pack 2 Interim Fix 3

    oder
    1. 9.0.1 Fix Pack 3

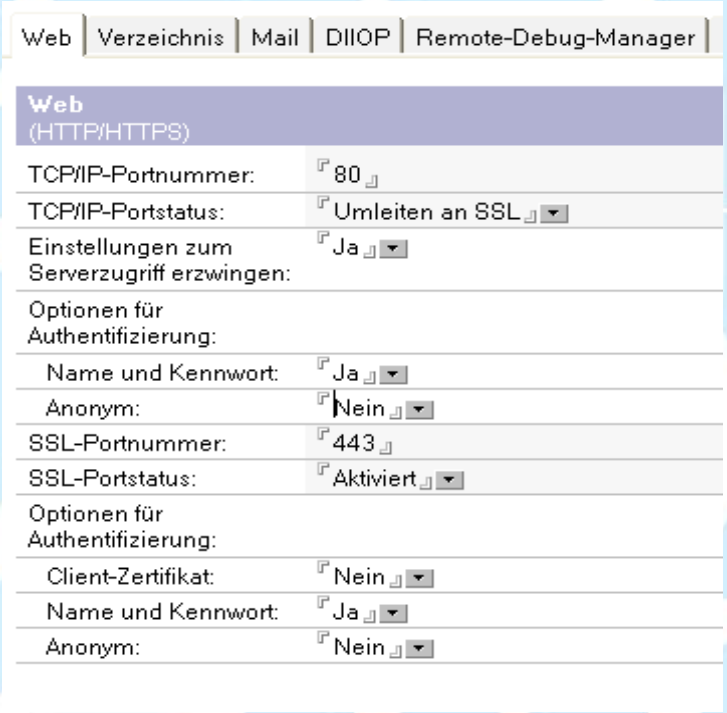
TLS/SSL einrichten 2

1. Die beiden Dateien xxx.kyr und xxx.sth ins Data-Verzeichnis des Servers kopieren
2. Serverdokument: Ports/Internet-Ports
3. SSL-Schlüsseldatei eintragen



TLS/SSL einrichten 3

4. Serverdokument: Ports/Internet-Ports



5. Alternative: über Internet-Site-Dokumente

TLS/SSL einrichten 4

6. SSL-Verschlüselungscodes = Cipher Suites

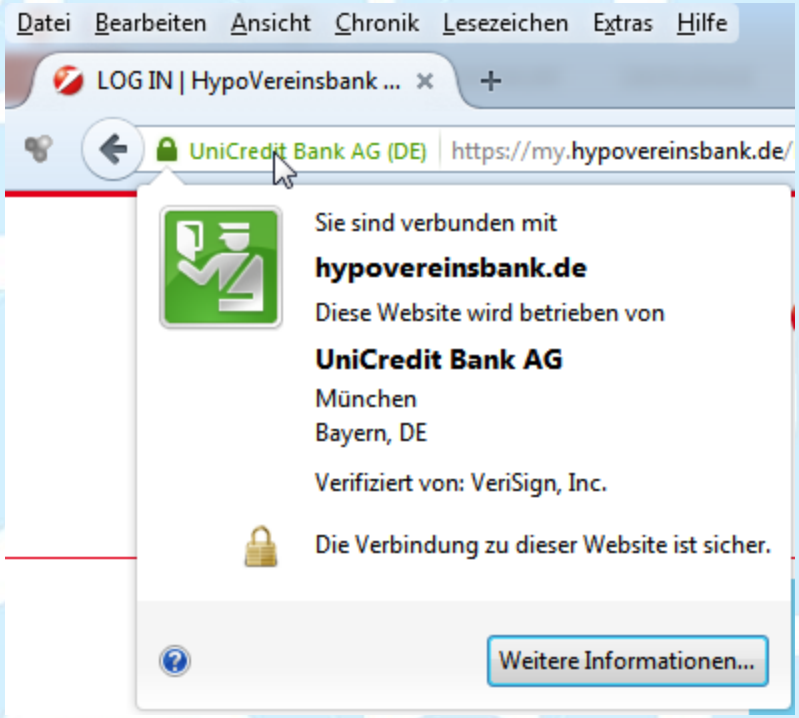
- im Serverdokument konfigurierbar:
  - Reiter Ports/Internet-Ports
  - aber dort nur für HTTPS
- für alle Ports in der notes.ini
  überschreibt die Einstellungen im Serverdok!
- SSLCipherSpec=2F35050A
  - 2F = SSL_RSA_WITH_AES_128_CBC_SHA
  - 35 = SSL_RSA_WITH_AES_256_CBC_SHA
  - 05 = SSL_RSA_WITH_RC4_128_SHA
  - 0A = SSL_RSA_WITH_3DES_EDE_CBC_SHA

TLS/SSL einrichten 5

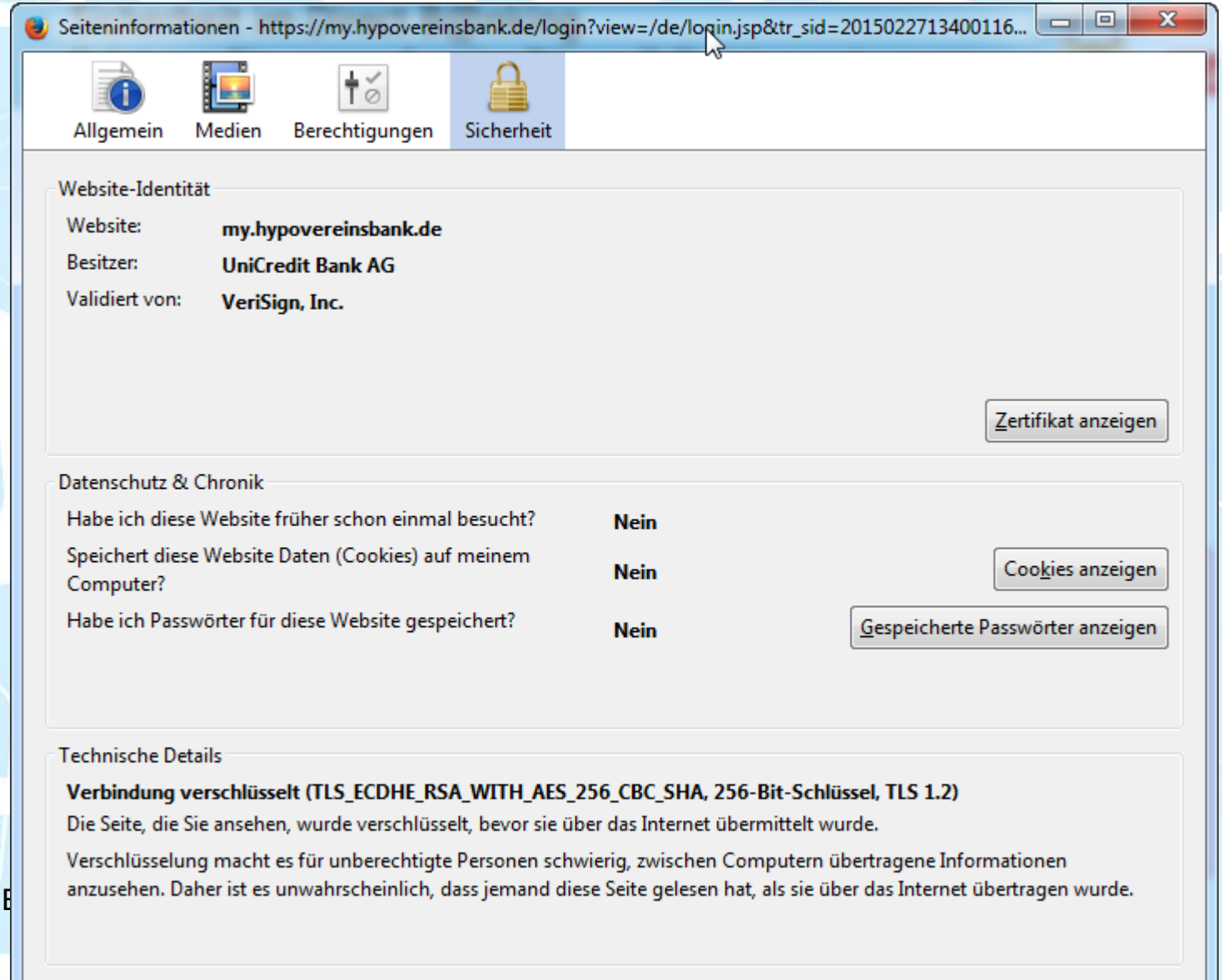
7. Wahlweise - ACHTUNG:
   - Ggf. benötigen wir SSL 3 noch
   - SSL 3 deaktivieren per notes.ini DISABLE_SSLV3=1
8. HTTP Task neu starten
9. Testen, Zertifikat validieren

Zertifikat validieren

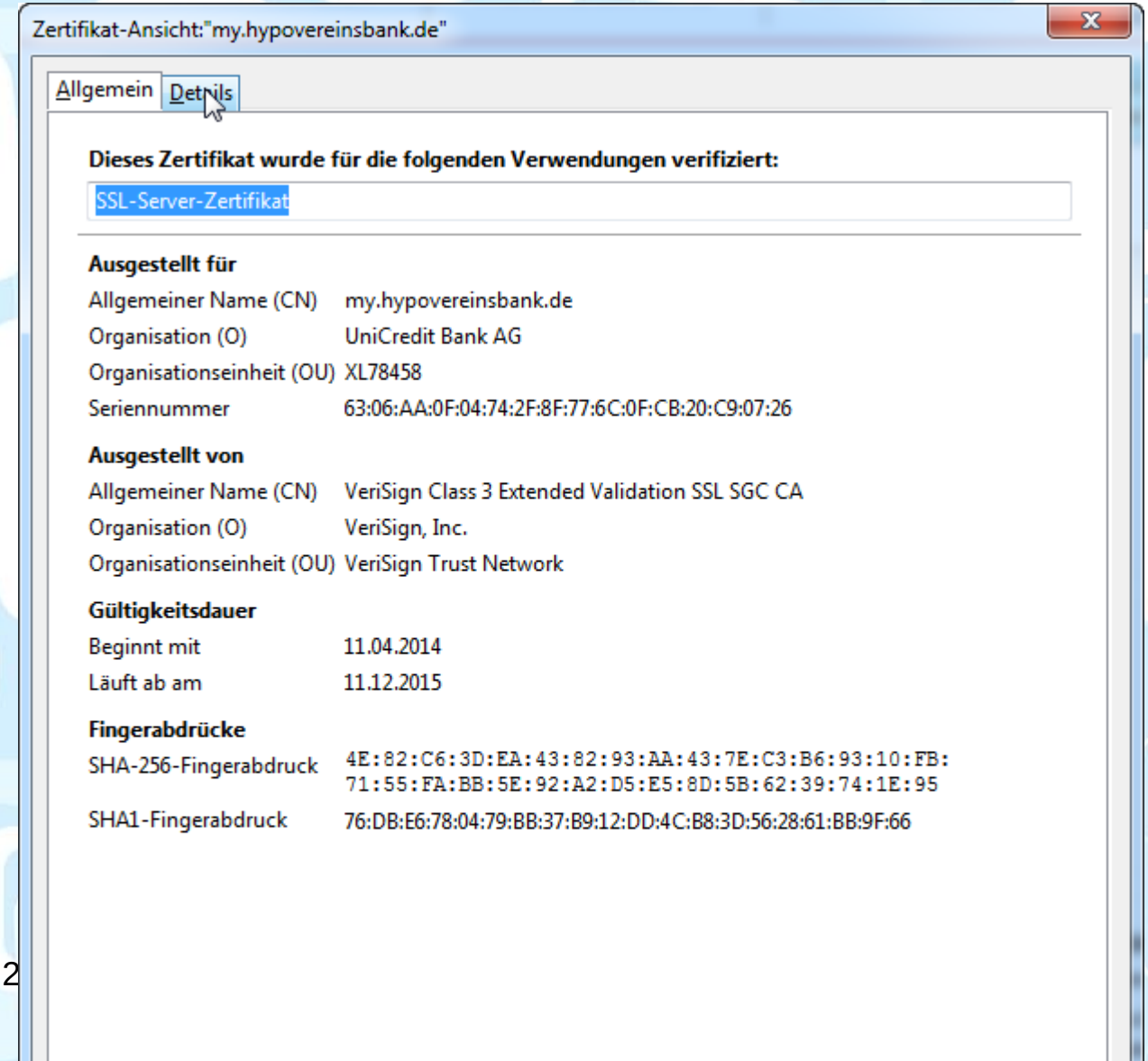
Zertifikat validieren 1



Zertifikat validieren 2



Zertifikat validieren 3



Zertifikat validieren 4

- SSLyze v0.10
- C:\>G:\SSLyze\sslyze\sslyze.exe --regular www.beispiel.de

```
TLSV1_1 Cipher Suites:
    Server rejected all cipher suites.
 TLSV1 Cipher Suites:
    Preferred:
          DHE-RSA-AES256-SHA          DH-1024 bits   256 bits      HTTP 200 OK
    Accepted:
          DHE-RSA-AES256-SHA          DH-1024 bits   256 bits      HTTP 200 OK
          AES256-SHA                  -              256 bits      HTTP 200 OK
          DHE-RSA-AES128-SHA          DH-1024 bits   128 bits      HTTP 200 OK
          RC4-SHA                     -              128 bits      HTTP 200 OK
          RC4-MD5                     -              128 bits      HTTP 200 OK
          AES128-SHA                  -              128 bits      HTTP 200 OK
          EDH-RSA-DES-CBC3-SHA        DH-1024 bits   112 bits      HTTP 200 OK
          DES-CBC3-SHA                -              112 bits      HTTP 200 OK
          EDH-RSA-DES-CBC-SHA         DH-1024 bits   56 bits       HTTP 200 OK
          DES-CBC-SHA                 -              56 bits       HTTP 200 OK
          EXP-EDH-RSA-DES-CBC-SHA     DH-512 bits    40 bits       HTTP 200 OK
          EXP-RC4-MD5                 -              40 bits       HTTP 200 OK
          EXP-RC2-CBC-MD5             -              40 bits       HTTP 200 OK
          EXP-DES-CBC-SHA             -              40 bits       HTTP 200 OK
```

Zertifikat validieren 5

- Webdienst: https://www.ssllabs.com/ssltest/

Datenbankschablonen mit Bezug zur Verschlüsselung

- pubnames.ntf - Domino Verzeichnis
  Speicher für öffentliche Schlüssel und Zertifikate
- pernames.ntf - persönliches Adressbuch
  Speicher für öffentliche Schlüssel und Zertifikate
- ~~csrv50.ntf - Server Certificate Administration~~
  ~~Editor für Schlüsselringe~~
- cca50.ntf – Domino Certificate Authority
  Internes Trustcenter
- certlog.ntf - Certification Log
  Logging der internen Domino-Registrierungen
- certpub.ntf - Domino Certificate Publication Requests
  This database is used for requesting publication of client SSL certificates into the NAB.

Verschlüsselungstools

- Die besten kostenlosen Verschlüsselungstools (für den privaten Einsatz)

  http://www.pcwelt.de/ratgeber/Datenschutz-Gratis-Tools-verschluesseln-alle-Ihre-Dateien-307316.html

Literatur/Quellen

- 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
- und mehr Wikipedia
- zwei Artikel in der c‘t 18/2012
- http://www.computerwoche.de/security/2510521/#
- „Crispy Certificates with Spicy SSL Salsa” http://www.slideshare.net/WorkFlowStudios/lotusphere-2011-show104
- Alternativen zur eMail-Verschlüsselung mit Bordmitteln: Alexander Rubinstein (www.symplasson.de)

Literatur/Quellen 2

- PFS: http://www.heise.de/security/artikel/Zukunftssicher-Verschluesseln-mit-Perfect-Forward-Secrecy-1923800.html
- http://www.nashcom.de/nsh/web.nsf/ff5ce882e73ab026c1256942003bdf10/6084a81e9f2c2b00c1256cc30030c6c1/$FILE/BP102_final.pdf
- https://www.heise.de/artikel-archiv/ct/2015/06/160_Die-Schluessel-Falle
- http://blog.darrenduke.net/Darren/DDBZ.nsf/dx/domino-and-ssl-ciphers.-the-server-document-may-not-be-doing-what-we-expect-it-to-do.htm
- http://www.golem.de/news/tls-verschluesselung-poodle-kann-auch-tls-betreffen-1412-111037.html

Vielen Dank für Ihre Aufmerksamkeit!

Jürgen Kunert
ITEE
InformationsTechnologie
Effizient Einsetzen
Sandkrugweg 57a
22457 Hamburg
Juergen.Kunert@itee.de