NetSys IT
Information & Communication

Einführung in X.509 + S/MIME

Peter Steiert

24.10.2010

NetSys IT
Information & Communication

Agenda

- Was ist X.509
- X.509 Zertifikate
- Kurzbeschreibung OpenSSL
- Elemente einer X.509 PKI
- Wie komme ich an ein Zertifikat ?
- Import in die Anwendung
- S/MIME
- Unterschiede/Vorteile: X.509v3 vs. (Open)PGP

NetSys IT
Information & Communication

Was ist X.509 ?

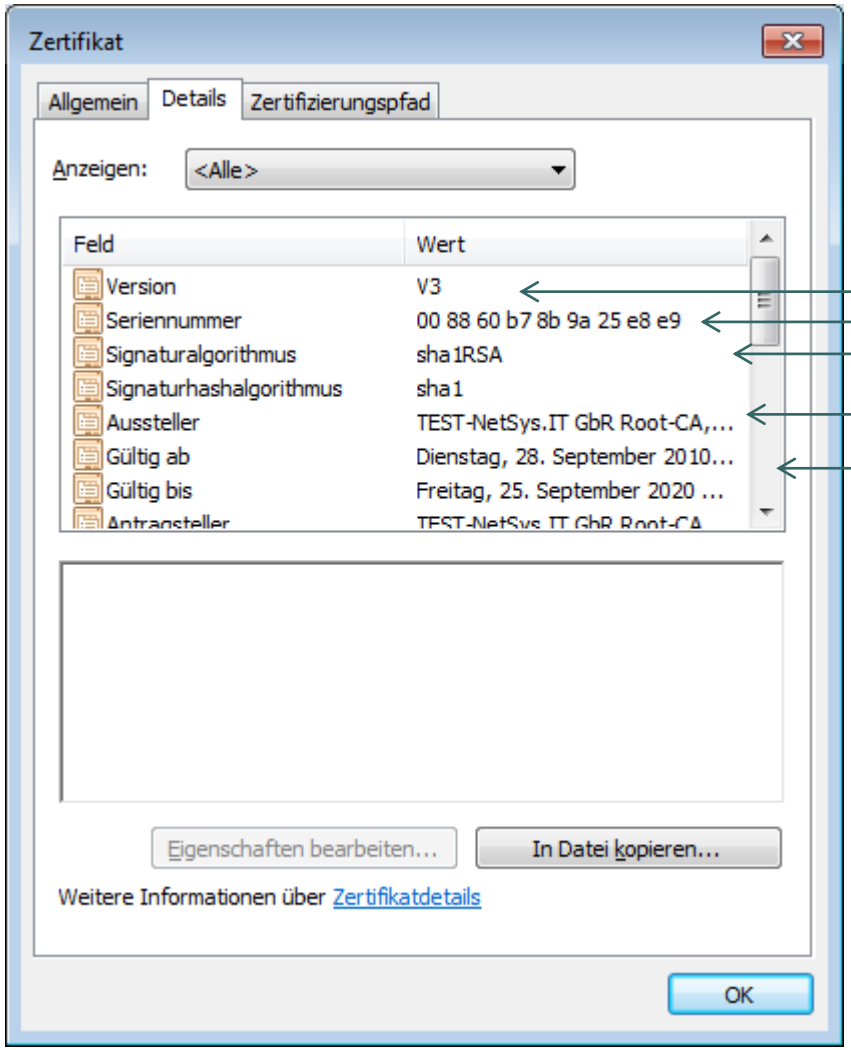
- **X.509 ist ein Standard für Public-Key Infrastrukturen.**
- **Aktuell ist X.509v3 (Version 3) gültig. Auch ältere noch im Umlauf.**
- **Einsatzbereich:**
  - Authentifikation, Schlüssel-Verschlüsselung, Signatur, Datenverschlüsselung, …
    - HTTPS ← SSL verwendet X.509v1-X509v3 Zertifikate

NetSys IT
Information & Communication

X.509 Zertifikate

- **Hierarchisches Modell**
  - Crosszertifizierung bietet Aufweichung des streng hierarchischen Modells, jedoch in der Realitiät kaum implementiert und nicht von Produkten unterstützt.
- **Vereinfacht:** ***Public-Key + Zusatzattribute***
- **Nur öffentlicher Schlüssel ist im Zertifikat enthalten.**
  - verschiedene Dateiendungen und Kodierungen von Zertifikaten
    - Non-MS Welt:
      - .PEM = BASE64 kodiert (auch CRT)
      - .DER = binär (byteweise)
    - MS-Welt
      - .CER = BASE64 als auch DER (MS Windows regelt das schon…)
- **Gegensatz z.B. P12/PFX Files**

  (Zertifikat+privater Schlüssel in verschlüsselter Form, ähnlich wie bei PGP/OpenPGP private Keyring)



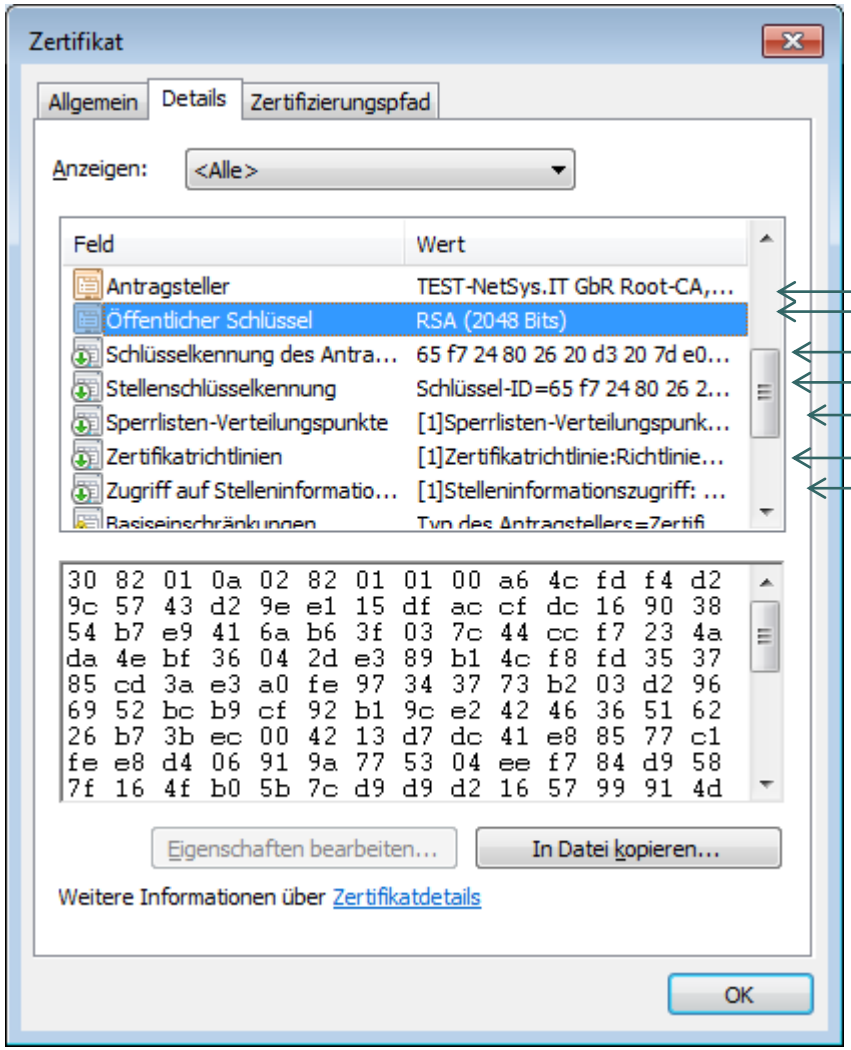
Version: X509v3

Serienummer Zertifikat

Hashalgorithmus

Aussteller (Issuer)

Gültigkeitszeitraum von-bis



Antragsteller (Subject)

Öffentlich Schlüssel

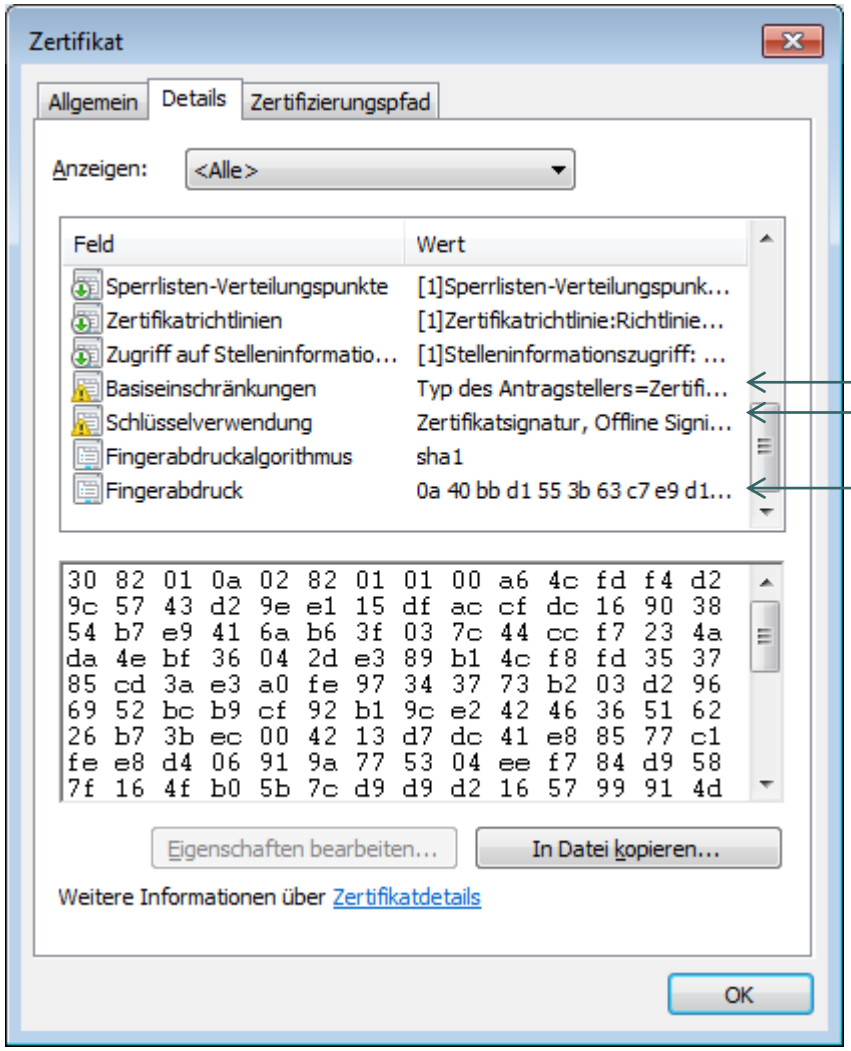
Hash Public-Key (Subject)

Hash Public-Key (Issuer)

Sperrlistenbezugspunkt

Bezugspunkt Certificate Policy

Stelleninformationen (z.B. OCSP, übergeordnete CA Zertifikate)



Beschränkungen

Schlüsselverwendung:
z.B.:
CA Signatur, Sperrlisten-signatur, Schlüssel-verschlüsselung, digitale Signatur, etc.

Fingerabdruck der Zertifikats.

NetSys IT
Information & Communication

Kurzbeschreibung OpenSSL

- **OpenSSL ist das Schweizer Taschenmesser zur Verarbeitung von**
  - kryptographischen Funktionen (z.B: RSA, SHA1, DES, etc.)
  - X.509v1-v3 Zertifikaten, privaten Schlüsseln
  - Kombinierter Datenstrukturen Daten+Kryptographie+Protokolle (z.B. HTTPS, S/MIME)

  - openssl ? - zeigt alle möglichen Befehle
  - openssl x509 ? - zeigt möglichen Optionen des Befehls „x509“

NetSys IT
Information & Communication

X.509 Zertifikate betrachten und konvertieren mit OpenSSL

- **openssl x509 –in Zertifikat.pem (-inform pem) –text –noout**
- **openssl x509 –in Zertifikat.der -inform der –text –noout**
- **openssl x509 –in Zertifikat.pem (-inform pem) –out Zertifikat.der –outform der**

NetSys IT
Information & Communication

Elemente einer X.509 PKI

- **Eine X.509 PKI setzt sich aus verschiedenen „Modulen“ zusammen:**
  - Certification Authority (CA)
  - Registration Authority (RA)
  - Certificate Policy/Certificate Practice Statement (CP/CPS)
  - Workflows (Identifikation, KeyRecovery, etc….)

NetSys IT
Information & Communication

Wie komme ich an ein Zertifikat ?

1. Privaten Schlüssel generieren (verwenden)
2. Zertifikatsrequest erzeugen (enthält Public-Key)
3. Zertifikatsrequest an CA (ZertifikatsAuthorität) übertragen/senden
4. CA prüft Identität (z.B. via E-Mail mit Link, SMS, Challenge Response)
5. CA stellt Zertifikat aus
6. Abholen des Zertifikats
7. Import in die Anwendung (Browser/Mailclient) etc. als P12/PFX

NetSys IT
Information & Communication

Ausstellen eines X.509 Zertifikates

Privaten Schlüssel generieren

(ohne Passwort)

```
openssl genrsa -out key.pem 2048
```

(mit Passwort)

```
openssl genrsa -out key.pem -aes256 2048
```

NetSys • IT
Information & Communication

Erstellen eines X.509 Zertifikatsrequest

openssl req -new -key key.pem

Enter pass phrase for key.pem:

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]:Thueringen

Locality Name (eg, city) []:Ilmenau

Organization Name (eg, company) [Internet Widgits Pty Ltd]:TEST AG

Organizational Unit Name (eg, section) []:IT Security

Common Name (eg, YOUR name) []:Peter Steiert

Email Address []:pest@gmx.de

NetSys IT
Information & Communication

Zertifikatsrequest

-----BEGIN CERTIFICATE REQUEST-----
MIIC1jCCAb4CAQAwgZAxCzAJBgNVBAYTAkRFMRMwEQYDVQQIEwpUaHVlcmluZ2Vu
MRAwDgYDVQQHEwdJbG1lbmF1MRAwDgYDVQQKEwdURVNUIEFHMRQwEgYDVQQLE
wtJ
VCBTZWN1cml0eTEWMBQGA1UEAxMNUGV0ZXIgU3RlaWVydDEaMBgGCSqGSIb3DQEJ
ARYLcGVzdEBnbXguZGUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDG
DLyTVIX/X9Z+lQ/1wOdmuGrPV3mH+MASAvTjuXOIi+RDTTfUz60+BY4mJ7HH33wP
3KMBhVFKS/GV4f7kD+vDeB/UA2e0e/7wGwelKpsj/8F8x6HPRoSxt7FLGRywVUHm
i5Bpn3hzo/KnrEBMS4HuGBtb8vdOR08dBxQZ4LxJ9Xf+t8efRruDsZ1EqtLQ/0JA
fmGc2bzXFfCR7ezK716TZDWC5Q4bTZtS5czneDxekQ2bPnnAIlcIT2g7wc3eW4qh
tKB8dm83tLbXhToJRZghy+Ql0QdUgRRJoxUTx1aB0ZXOxYT9jvFOXyTu/R6kPepp
zrSgumNCfJJCbu+QrVBVAgMBAAGgADANBgkqhkiG9w0BAQUFAAOCAQEAVNm2YvT7
kUR1tW07VOFV3+1qYsMcFBMklf7zT/6JwVC6LBFBzpz2XgRFRa1NNUDn9cMmrWXs
mykViaNKji06D6n25vV4xTZycdgO4r1ECxEveagvjPWZVJ3wK1mL/THKqkqsPLOX
tsAoLP1NB4esYMtsLdIhgQ2/eumHDHJdehgDiOa9Mvwdak4l+lhA1YnZMZoMoZLG
8t0a2ZIjAXzAlSubUS13XeZ5lfw6LqGbIuZ+yyoSna7gldYWSwBFs19JTXzepbq4
ORx02bjIb1MsThObNk0DpQK8tTBLJl/JrCC0Abx9iX2DZ5FtMHikKJLZM31KvbLF
0dH2jQKc0F0R+Q==
-----END CERTIFICATE REQUEST-----

NetSys IT
Information & Communication

Zertifikatsrequest an CA übertragen/senden

- **Zertifikatsrequest per:**
  - Email versenden
  - Webserver übertragen

NetSys IT
Information & Communication

CA prüft Identität (z.B. via E-Mail mit Link, SMS, Challenge Response)

- Versand eines Bestätigungslinks an E-Mail Postfach.
- Klicken des Links löst Zertifikatstransfer aus.

NetSys IT
Information & Communication

CA stellt Zertifikat aus

NetSys IT
Information & Communication

Import in die Anwendung

- **Browser/Mailclient unterstützen meist P12/PFX Dateien zum vollständigen Import von**
  - **+ privatem Key**
  - **+ Zertifikat**
  - **+ CA Zertifikaten (optional)**

Generierung einer PFX/P12 Datei mit OpenSSL:

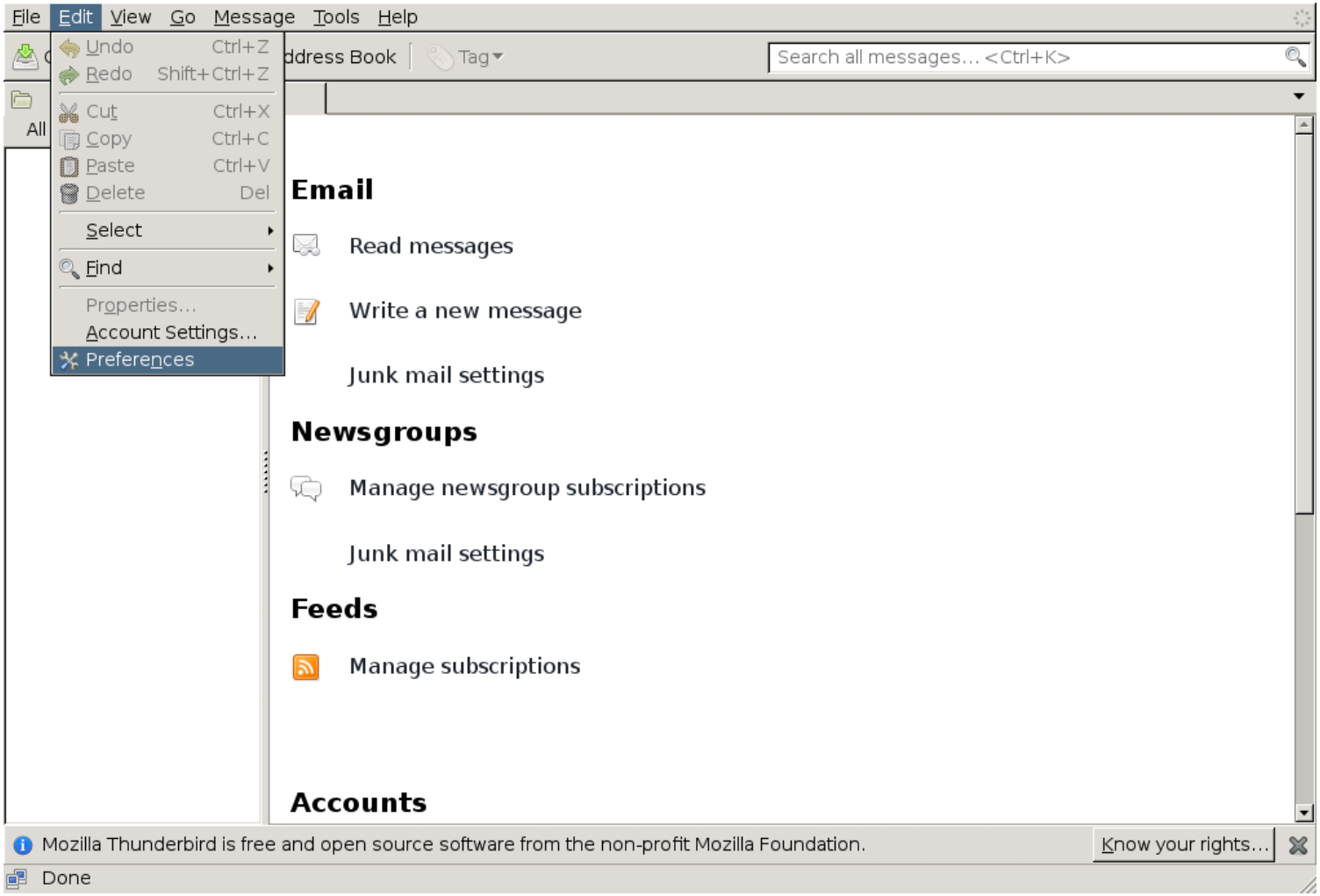
openssl pkcs12 –inkey key.pem -in certificate.pem -export –des3 –out personalkeystore.pfx

Generierung einer PFX/P12 Datei mit OpenSSL mit CA Zertifikat.

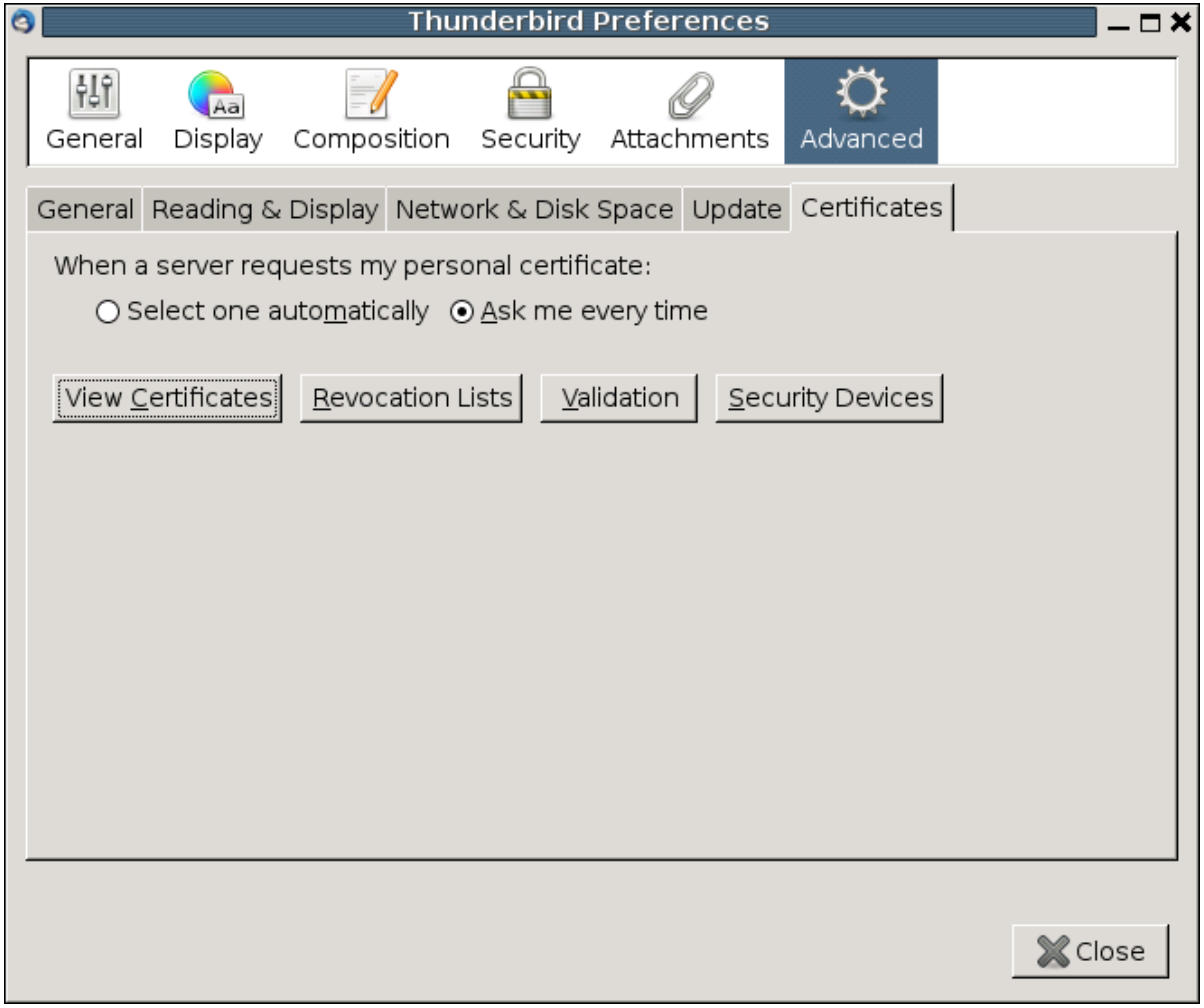
openssl pkcs12 –inkey key.pem -in certificate.pem -export –des3 –out personalkeystore.pfx -CAfile CAcert.pem

NetSys IT
Information & Communication

Import in die Anwendung

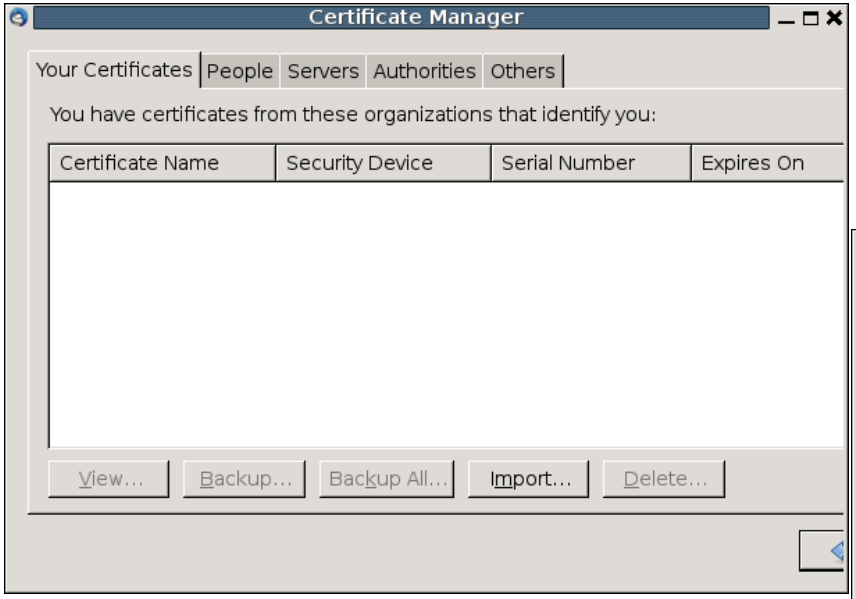


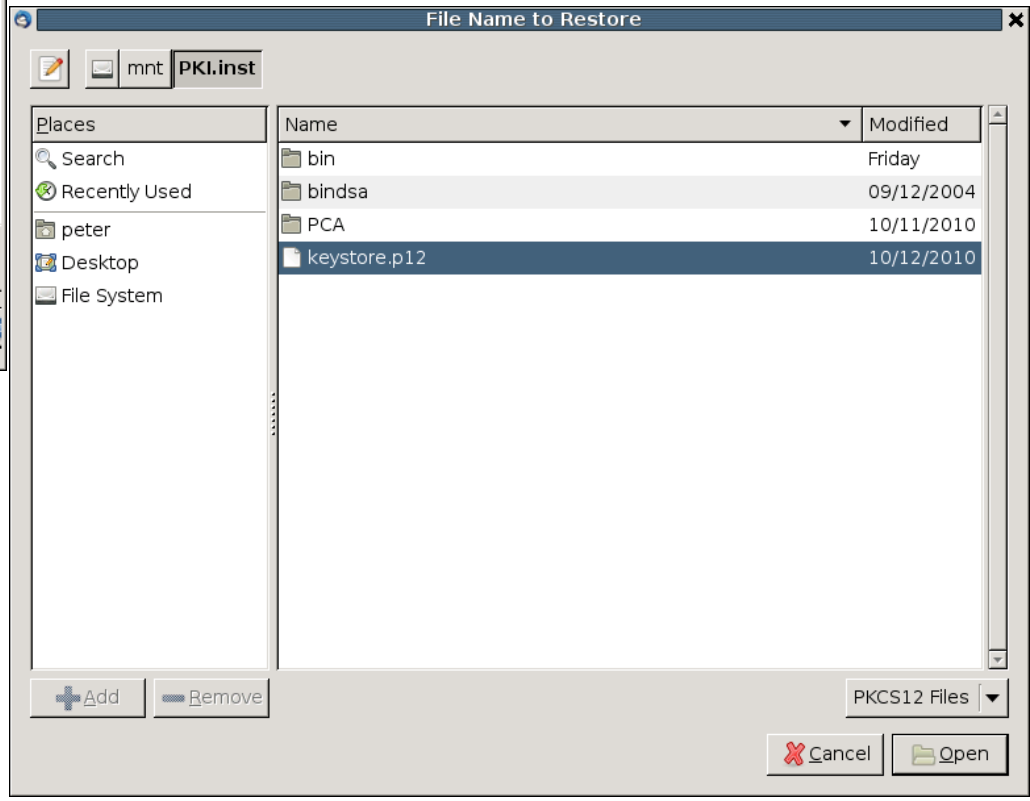
Import in die Anwendung



NetSys IT
Information & Communication

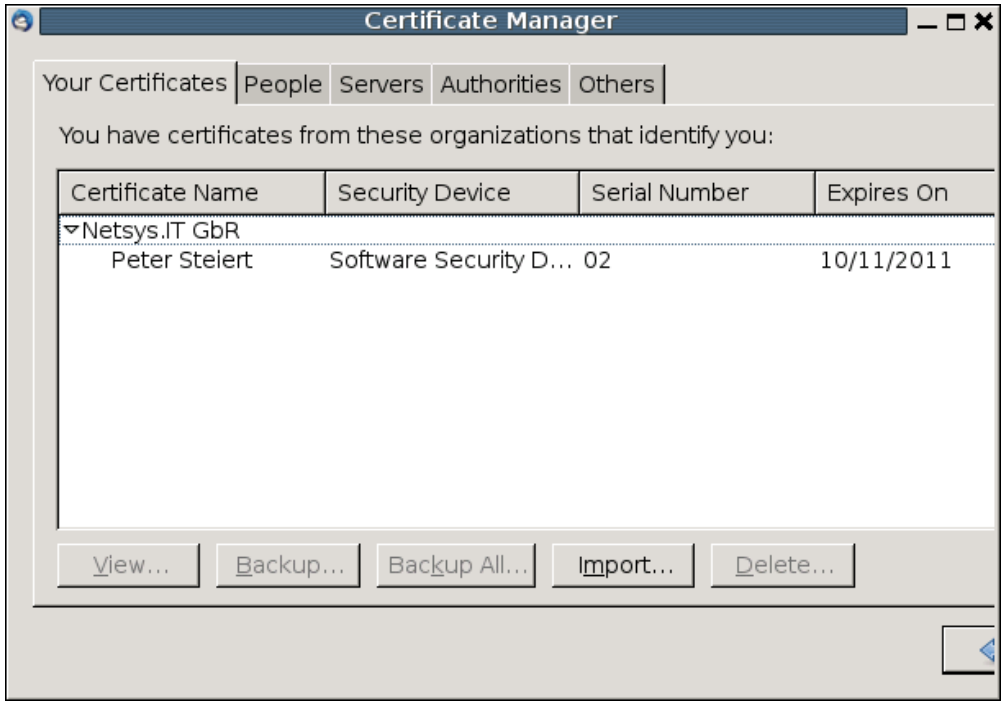
Import in die Anwendung





NetSys IT
Information & Communication

Import in die Anwendung



NetSys IT
Information & Communication

Import in die Anwendung (Tipp!)

- **Sollen weitere CA Zertifikate im P12 Container mit aufgenommen werden, so müssen diese alle wie in nachfolgenden File (Cacert.pem) enthalten sein:**

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

MIIFwzCCBKugAwIBAgIJW578rqNPDSvgTlRmLPC6ZCA2cVKVnusvKNfxKwz T78 ….

wodaTYl9lwh/as2KGpC85ys4EfiTHzc5fCu3j1G9oRw8gfvi29r4

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

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

MVQQGEwJERTESMBAGA1UECBMJVGh1cmluZ2lhMRAwDgYDVQQHEwdJb G1….

lbwodaTYl9lwh/as2KEfiTHzc5fCu3j1G9oRw8gfvi29r4

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

NetSys IT
Information & Communication

S/MIME

- **S/MIME ist die Erweiterung von MIME bezüglich:**

Signierter	(Sicherung Manipulation, Herkunft)
Verschlüsselte	(Sicherung vor Datenzugriff durch Dritte)
Signierter + Verschlüsselte	(Sicherung Manipulation, Herkunft, Datenzugriff durch Dritte)

E-Mail Kommunikation.

- **S/MIME schützt nur den Mailbody!**
- **Mailheader (Subject, Empfänger sind ungeschützt)**

NetSys IT
Information & Communication

S/MIME mit OpenSSL

- **Erstellen einer verschlüsselte E-Mail mit openssl**

  openssl smime -encrypt -to empfänger@web.de
  -from sender@gmx.de -subject "S/MIME Nachricht "
  -in “Zu VERSCHLÜSSELNDE DATEI” empfängerzertifikat.pem

- **Entschlüsseln einer verschlüsselten E-Mail mit openssl**

  openssl smime -decrypt -in ENCRYPTEDEMAIL.txt -inkey key.pem

NetSys IT
Information & Communication

S/MIME mit OpenSSL

- **Erstellen einer signierten E-Mail mit openssl**

  openssl smime -sign-to empfänger@gmx.de
  -from sender@gmx.de -subject "S/MIME Nachricht "
  -in “Zu Signierende DATEI” -inkey key.pem
  -signer signierzertifikat.pem -out signedEMail.pem

- **Prüfen einer signierten E-Mail mit openssl**

  openssl smime -verify -in signedEMail.pem -CAfile ALLCAs.pem

  → Verification successful

NetSys IT
Information & Communication

Unterschiede X.509 vs. (Open)PGP?

Gemeinsamkeiten:

kryptographische Algorithmen

geringe Verbreitung im Privatsektor

X.509:

- **Strenge Hierarchie**
- **Zertifikate sind „zweckgebunden“ für spezifische Verwendung.**
- **Gängige Algorithmen werden unterstützt. (RSA, 3DES, AES, SHA1, SHA2-256,384,512).**
- **Anerkanntes Secure E-Mailformat (S/MIME)**

  → Wiederverwendung in XML-ENC, XML-DSIG

NetSys IT
Information & Communication

Unterschiede X.509 vs. (Open)PGP?

(Open)PGP:

- **Hierarchie kann, ist kein Muss**
- **Zertifikate sind „zweckgebunden“ für spezifische Verwendung.**
- **Vielzahl von Algorithmen werden unterstützt. (RSA, elGamal, 3DES, AES, SHA1, Whirlpool).**
- **Eigenes Secure E-Mailformat .**

NetSys IT
Information & Communication

Vorteile: X.509v3 vs. (Open)PGP

Vorteile:

- **Native Unterstützung von X.509 Zertifikaten in Anwendungen (Outlook, Thunderbird, Lotus Notes, etc.)**
- **X.509 Erfahrung im großflächigen Einsatz: (HTTPS)**

Nachteil:

- **Keine Ad-Hoc Verschlüsselung**
  - (eine vollwertige CA in Betrieb zu nehmen braucht Zeit)
- **Vermischung guter und schlechter CAs in Browsern**
- **Trust wird über alle Mitglieder einer CA ausgesprochen**
  - (CACert sucht hier einen anderen Ansatz)

NetSys • IT
Information & Communication

Vielen Dank für Ihre Aufmerksamkeit!

Peter Steiert
NetSys.IT Information & Communication
Weimarer Str. 28
98693 Ilmenau
Tel ++49.3677.203515
Fax ++49.3677.8984551
E-Mail psteiert@netsys-it.de
Web http://www.netsys-it.de

23.10.2010