Mag. iur. Dr. techn. Michael Sonntag

E-Mail security

Institute for Information Processing and
Microprocessor Technology (FIM)
Johannes Kepler University Linz, Austria

E-Mail: sonntag@fim.uni-linz.ac.at
http://www.fim.uni-linz.ac.at/staff/sonntag.htm

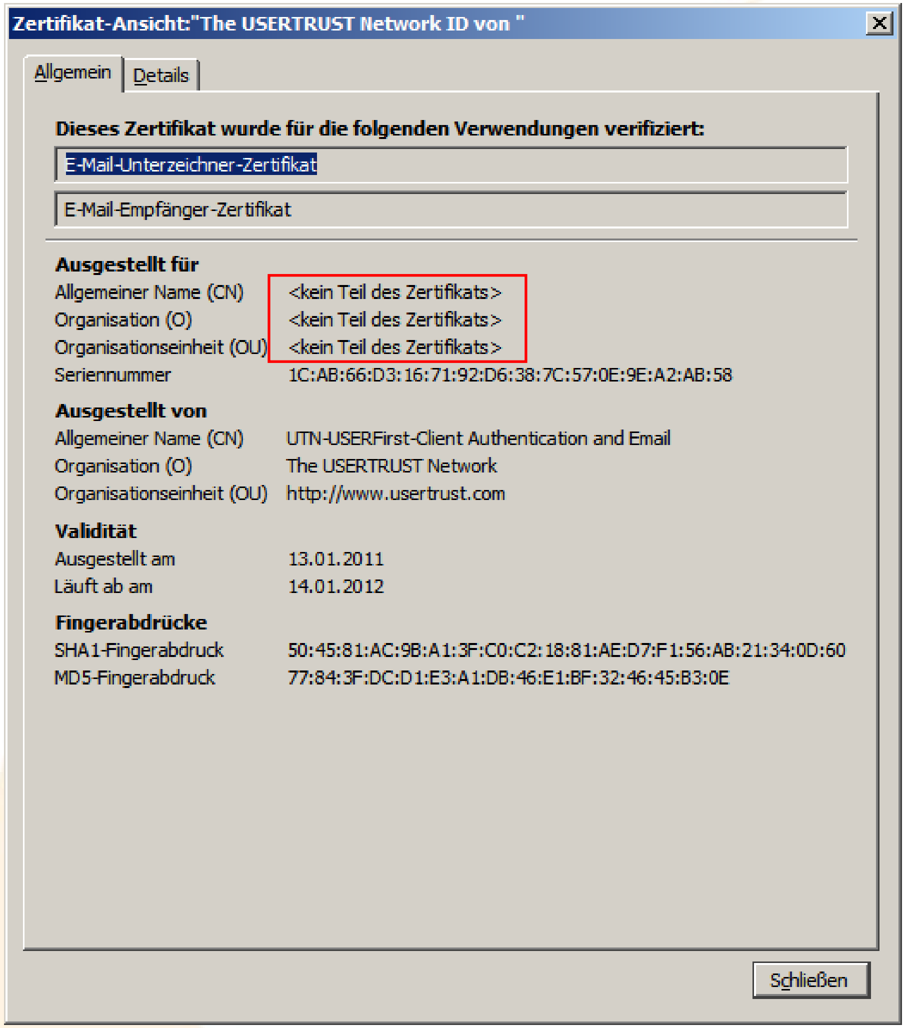
Agenda

- Obtaining a certificate
  - → Obtaining an “official” certificate
  - → Creating a self-signed certificate
    - » Using “OpenSSL” for certificate/key manipulation
- Using/Installing software for E-Mail signature/encryption
  - → Thunderbird
  - → Outlook
- Sending/Verifying signed/encrypted E-Mails

Obtaining an official certificate

- Free version by COMODO:
  - → https://secure.instantssl.com/products/frontpage?area=SecureEmailCertificate
- Fill in the form: Name and E-Mail address
- Firefox will automatically generate the needed data
- Check your inbox for the confirmation E-Mail
- Click on the link to receive the certificate and install it in Firefox
- Open Firefox properties and go to “Extended” – “Certificates” and click on “Certificates”
- Navigate to the “My certificates” tab, locate the certificate and export it (needed as a backup too!)
  - → Make sure to remember the location and the password!

Example of an official certificate



Zertifikat-Ansicht:"The USERTRUST Network ID von "

Dieses Zertifikat wurde für die folgenden Verwendungen verifiziert:

- E-Mail-Unterzeichner-Zertifikat
- E-Mail-Empfänger-Zertifikat

Ausgestellt für

Allgemeiner Name (CN)	<kein Teil des Zertifikats>
Organisation (O)	<kein Teil des Zertifikats>
Organisationseinheit (OU)	<kein Teil des Zertifikats>
Seriennummer	1C:AB:66:D3:16:71:92:D6:38:7C:57:0E:9E:A2:AB:58

Ausgestellt von

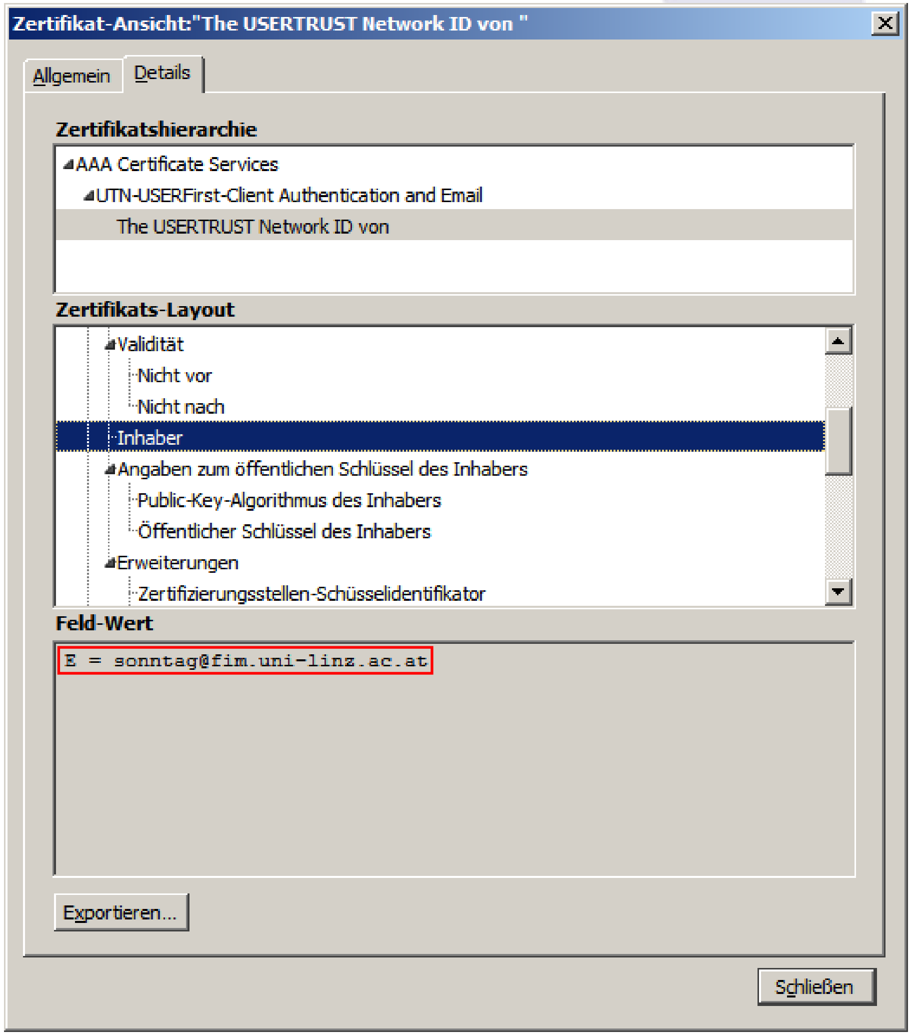
Allgemeiner Name (CN)	UTN-USERFirst-Client Authentication and Email
Organisation (O)	The USERTRUST Network
Organisationseinheit (OU)	http://www.usertrust.com

Validität

Ausgestellt am	13.01.2011
Läuft ab am	14.01.2012

Fingerabdrücke

SHA1-Fingerabdruck	50:45:81:AC:9B:A1:3F:C0:C2:18:81:AE:D7:F1:56:AB:21:34:0D:60
MD5-Fingerabdruck	77:84:3F:DC:D1:E3:A1:DB:46:E1:BF:32:46:45:B3:0E



Zertifikat-Ansicht:"The USERTRUST Network ID von "

Zertifikatshierarchie

```
AAA Certificate Services
  UTN-USERFirst-Client Authentication and Email
    The USERTRUST Network ID von
```

Zertifikats-Layout

```
Validität
  Nicht vor
  Nicht nach
Inhaber
Angaben zum öffentlichen Schlüssel des Inhabers
  Public-Key-Algorithmus des Inhabers
  Öffentlicher Schlüssel des Inhabers
Erweiterungen
  Zertifizierungsstellen-Schüsselidentifikator
```

Feld-Wert

```
E = sonntag@fim.uni-linz.ac.at
```

Manually creating a certificate (1)

- OpenSSL required
  - → Linux: Install normally as other packages
  - → Windows: Get it from http://www.slproweb.com/products/Win32OpenSSL.html
    - » Note: Requires Visual C Redistributables (see same page)
- Step 1: Create a CA key+cert
  - → openssl genrsa -des3 -out ca.key 4096
    - » RSA, 4096 Bit, key is DES encrypted
  - → openssl req -new -x509 -days 365 -key ca.key -out ca.crt
    - » Enter as much (or little) information as wanted (default values!)
    - » Attention: “Common Name” must be different from the one in the user certificate below! Use e.g. “Michael Sonntag – CA”!
- Step 2: Create user certificate (RSA, 2048 Bit, **un**encrypted)
  - → openssl genrsa -out user.key 2048
  - → openssl req -new -key user.key -out user.csr
    - » Enter as much (or little) information as wanted (default values!)
      - – Enter at least your E-Mail address!

Manually creating a certificate (2)

- Step 3: Sign user certificate with CA
  - → openssl x509 -req -days 365 -CA ca.crt -CAkey ca.key -set_serial 1 -in user.csr -out user.crt -setalias "Michael Sonntags E-Mail certificate" -addtrust emailProtection -addreject clientAuth -addreject serverAuth –trustout
    - » Modify details as desired/necessary!
      - – Duration is very short with 1 year (→ distribute new certificate!)
- Step 4: Convert it to appropriate format: PKCS#12 with key
    - » Certificate + private key in an encrypted package
  - → openssl pkcs12 -export -in user.crt -inkey user.key -out user.p12
    - » Remember the key you were asked for!

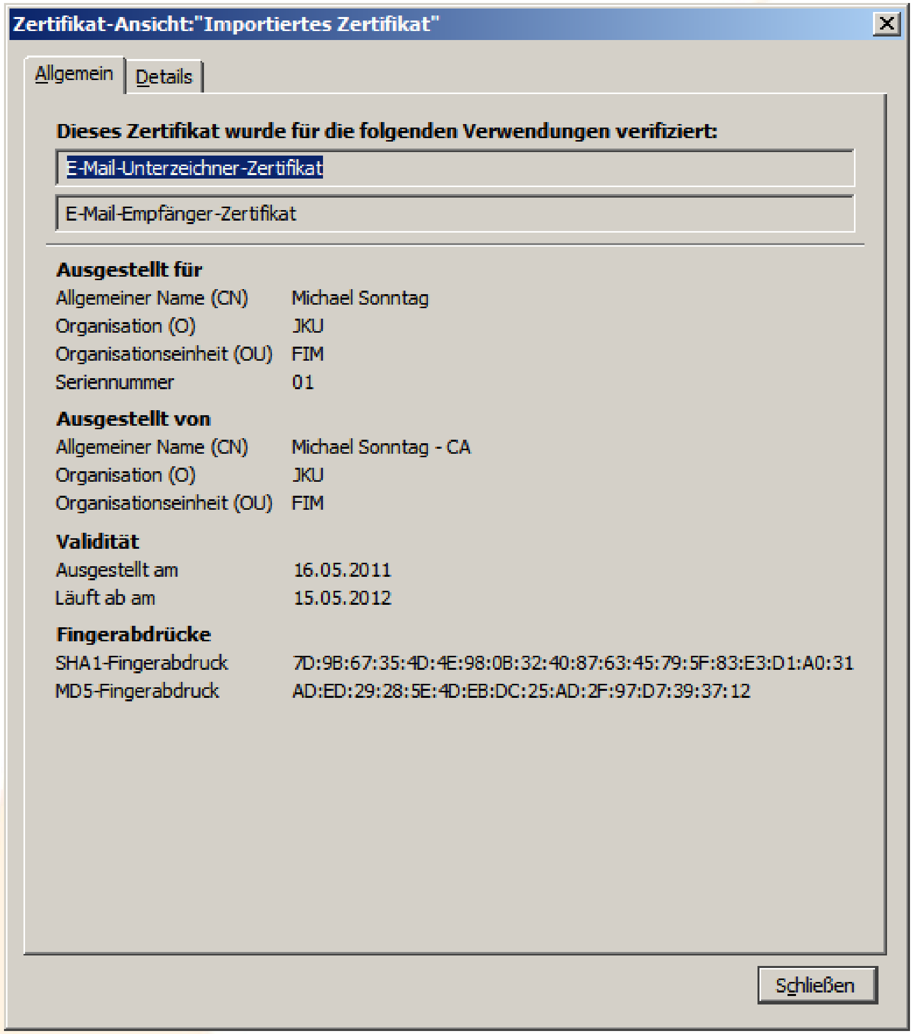
Manually creating a certificate (3)

- Step 5a - Thunderbird: Import CA certificate as trusted
  - → Account – S/MIME security – manage certificates
  - → Root cert. – Import “ca.crt” – Trust for identifying E-Mail users
- Step 5b - Outlook: Import CA certificate as trusted
  - → Open management console and add the certificates plugin for the current user
  - → Import “ca.crt” as a trusted root certificate
    - » Attention: This is not Outlook-specific anymore, but system-wide!
- Step 6: Import user certificate for signing
  - → Identical as with any “officially” issued certificate (see below)!

Importing certificates as trusted root

- Note: With manually created certificates, their root (=the CA) must be imported as “trusted root”
  - → This means, that it is a full CA!
  - → All other certificates issued below it will immediately be trusted as well
    - » Might be desirable: Other E-Mail certificates from this company
    - » Might be undesirable: Anything else is trusted too, like signed code, applets, …
- Advantage: Technically easy
  - → Just send it by mail, …
- Problem: Side effects
  - → Other things are trusted too
  - → How to securely transmit it?

Example of a custom certificate



Dieses Zertifikat wurde für die folgenden Verwendungen verifiziert:

- E-Mail-Unterzeichner-Zertifikat
- E-Mail-Empfänger-Zertifikat

Ausgestellt für

Allgemeiner Name (CN)	Michael Sonntag
Organisation (O)	JKU
Organisationseinheit (OU)	FIM
Seriennummer	01

Ausgestellt von

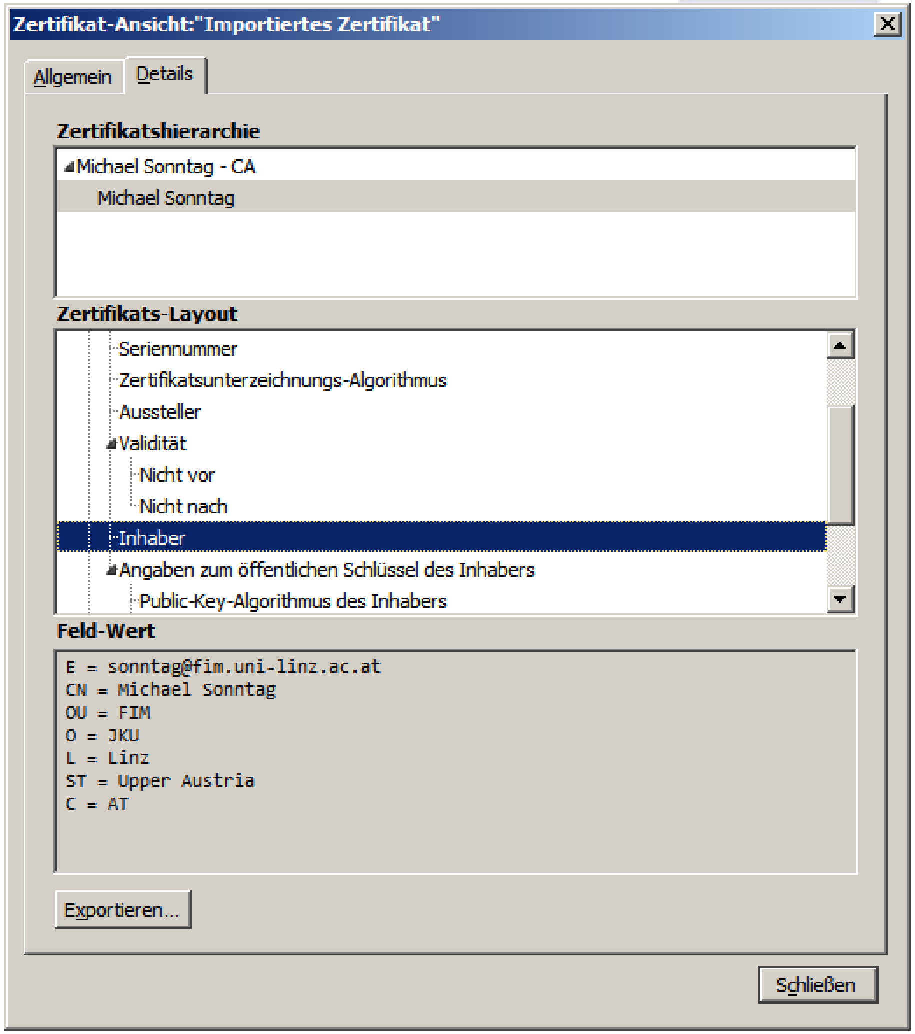
Allgemeiner Name (CN)	Michael Sonntag - CA
Organisation (O)	JKU
Organisationseinheit (OU)	FIM

Validität

Ausgestellt am	16.05.2011
Läuft ab am	15.05.2012

Fingerabdrücke

SHA1-Fingerabdruck	7D:9B:67:35:4D:4E:98:0B:32:40:87:63:45:79:5F:83:E3:D1:A0:31
MD5-Fingerabdruck	AD:ED:29:28:5E:4D:EB:DC:25:AD:2F:97:D7:39:37:12



Zertifikatshierarchie

- Michael Sonntag - CA
  - Michael Sonntag

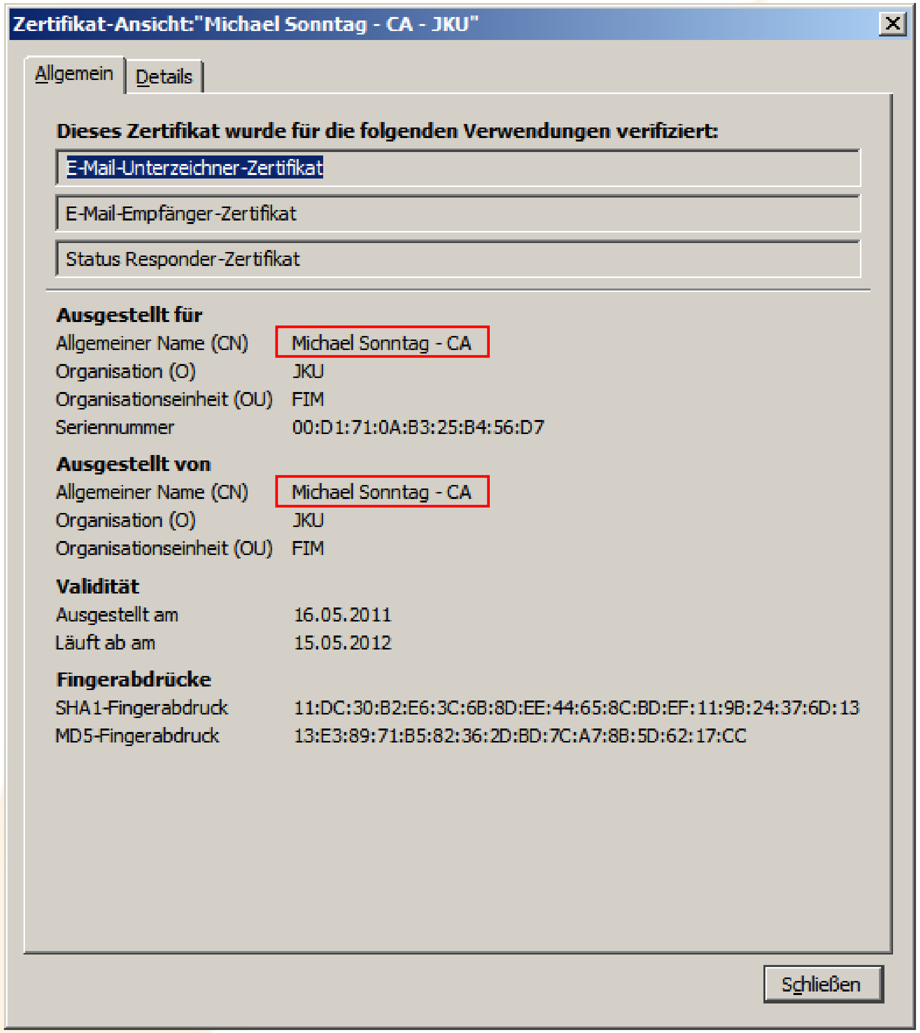
Zertifikats-Layout

- Seriennummer
- Zertifikatsunterzeichnungs-Algorithmus
- Aussteller
- Validität
  - Nicht vor
  - Nicht nach
- Inhaber
- Angaben zum öffentlichen Schlüssel des Inhabers
  - Public-Key-Algorithmus des Inhabers

Feld-Wert

```
E = sonntag@fim.uni-linz.ac.at
CN = Michael Sonntag
OU = FIM
O = JKU
L = Linz
ST = Upper Austria
C = AT
```

Example of a custom CA certificate



Zertifikat-Ansicht:"Michael Sonntag - CA - JKU"

Dieses Zertifikat wurde für die folgenden Verwendungen verifiziert:

- E-Mail-Unterzeichner-Zertifikat
- E-Mail-Empfänger-Zertifikat
- Status Responder-Zertifikat

Ausgestellt für

Allgemeiner Name (CN)	Michael Sonntag - CA
Organisation (O)	JKU
Organisationseinheit (OU)	FIM
Seriennummer	00:D1:71:0A:B3:25:B4:56:D7

Ausgestellt von

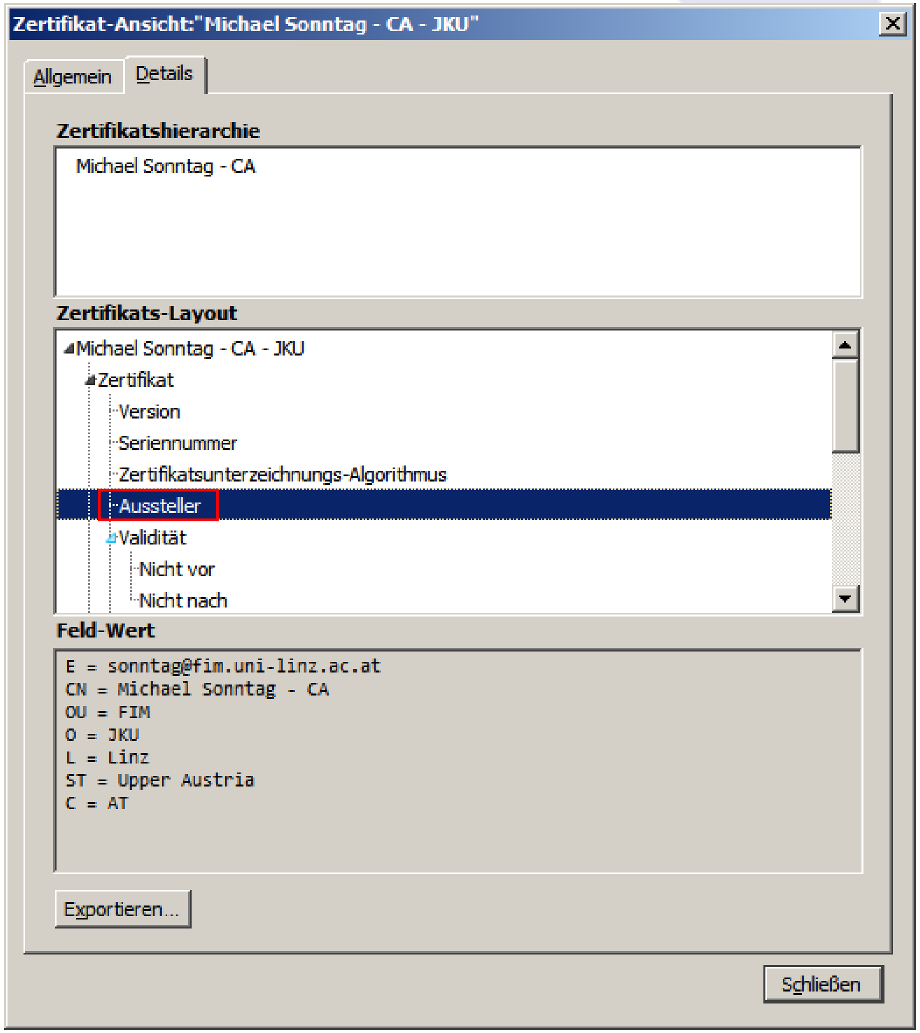
Allgemeiner Name (CN)	Michael Sonntag - CA
Organisation (O)	JKU
Organisationseinheit (OU)	FIM

Validität

Ausgestellt am	16.05.2011
Läuft ab am	15.05.2012

Fingerabdrücke

SHA1-Fingerabdruck	11:DC:30:B2:E6:3C:6B:8D:EE:44:65:8C:BD:EF:11:9B:24:37:6D:13
MD5-Fingerabdruck	13:E3:89:71:B5:82:36:2D:BD:7C:A7:8B:5D:62:17:CC



Zertifikat-Ansicht:"Michael Sonntag - CA - JKU"

Zertifikatshierarchie

Michael Sonntag - CA

Zertifikats-Layout

```
Michael Sonntag - CA - JKU
  Zertifikat
    Version
    Seriennummer
    Zertifikatsunterzeichnungs-Algorithmus
    Aussteller
    Validität
      Nicht vor
      Nicht nach
```

Feld-Wert

```
E = sonntag@fim.uni-linz.ac.at
CN = Michael Sonntag - CA
OU = FIM
O = JKU
L = Linz
ST = Upper Austria
C = AT
```

Software support

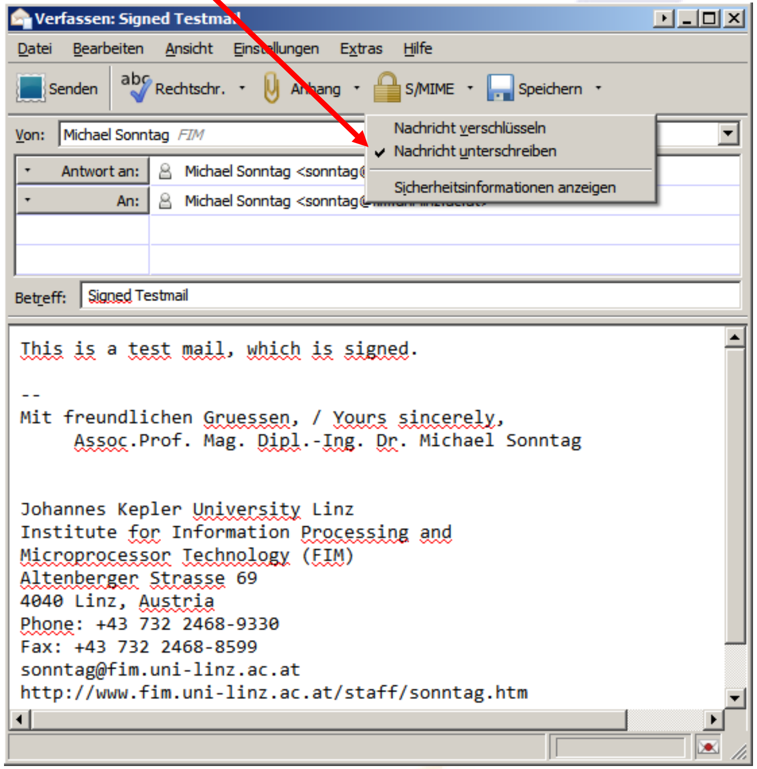
- Current versions of Thunderbird and Outlook support S/MIME signatures/encryption out of the box
  - → Older versions requires additional software
  - → Outlook allows several certificates per account and provides more information (but only useful for experts!)
- OpenPGP requires additional software
  - → E.g. Gpg4win + Enigmail for Thunderbird
- “Official” certificate are more portable
  - → Manually created ones might be problematic in various E-Mail clients because of (lack of) usage-extensions
    - » Manual verification (→OpenSSL) should work always …

Installing the certificate in Thunderbird

- Certificate installation
  - → Open Thunderbird properties and go to "Extended" – "Certificates" and click on "Certificates"
  - → Click on import, select the file
  - → Enter the password and close the dialog after import
- Account configuration
  - → Open the account configuration
  - → Navigate to the "S/MIME Security" entry in the account to use this certificate
  - → Click on "Select" and choose the certificate to use for signing outgoing E-Mail
  - → Do the same for the encryption
  - → Change (if wanted – caution!) encryption to mandatory
    - » You can't send any E-Mail to anyone you don't have a certificate for (for all recipients a certificate must be present)!

Sending a signed E-Mail

- Create a new E-Mail
- Select from the Toolbar "S/MIME" – "Sign message"
  - → Or use the menu entry
  - → Attention: No other indication!
- Send the E-Mail
- Only one certificate/sender
  - → No selection possible!
- No need for entering a password
  - → All based on certificate and its key, which are already known
  - → Anyone with access to the account can send signed E-Mails!
  - → More secure: Use a master password!



Von: Michael Sonntag *FIM*

Antwort an: Michael Sonntag <sonntag@

An: Michael Sonntag <sonntag@

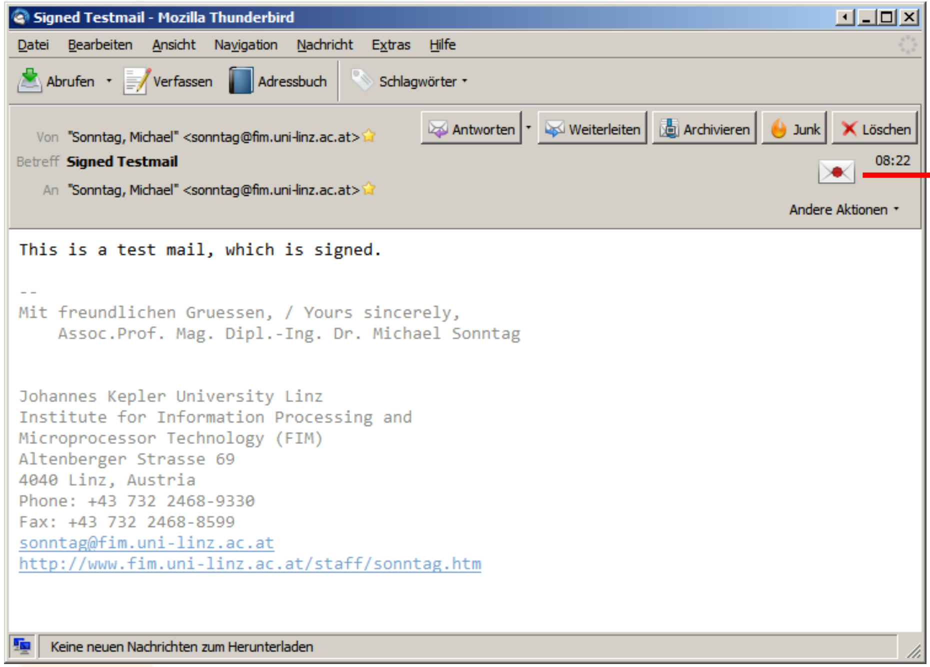
Betreff: Signed Testmail

```
This is a test mail, which is signed.

--
Mit freundlichen Gruessen, / Yours sincerely,
     Assoc.Prof. Mag. Dipl.-Ing. Dr. Michael Sonntag


Johannes Kepler University Linz
Institute for Information Processing and
Microprocessor Technology (FIM)
Altenberger Strasse 69
4040 Linz, Austria
Phone: +43 732 2468-9330
Fax: +43 732 2468-8599
sonntag@fim.uni-linz.ac.at
http://www.fim.uni-linz.ac.at/staff/sonntag.htm
```

Verifying the signature



Von "Sonntag, Michael" <sonntag@fim.uni-linz.ac.at>

Betreff **Signed Testmail**

An "Sonntag, Michael" <sonntag@fim.uni-linz.ac.at>

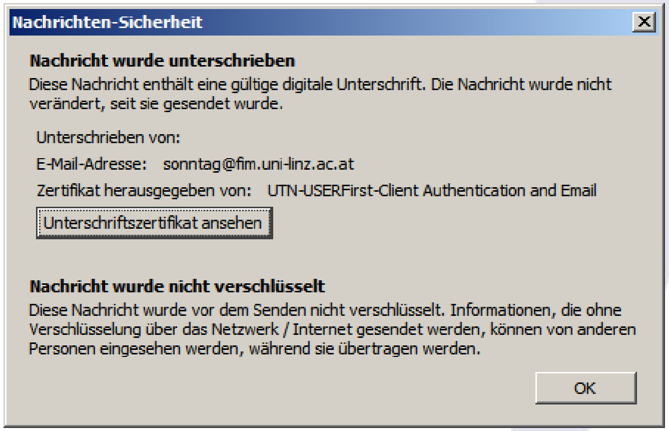
08:22

```
This is a test mail, which is signed.

--
Mit freundlichen Gruessen, / Yours sincerely,
    Assoc.Prof. Mag. Dipl.-Ing. Dr. Michael Sonntag


Johannes Kepler University Linz
Institute for Information Processing and
Microprocessor Technology (FIM)
Altenberger Strasse 69
4040 Linz, Austria
Phone: +43 732 2468-9330
Fax: +43 732 2468-8599
sonntag@fim.uni-linz.ac.at
http://www.fim.uni-linz.ac.at/staff/sonntag.htm
```

Keine neuen Nachrichten zum Herunterladen



Nachricht wurde unterschrieben

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

Unterschrieben von:

E-Mail-Adresse: sonntag@fim.uni-linz.ac.at

Zertifikat herausgegeben von: UTN-USERFirst-Client Authentication and Email

Nachricht wurde nicht verschlüsselt

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

- Note:
  - → Only the E-Mail address ("sonntag@fim. …) is verified
    - » Who this is, from where it was sent, … → Remains unknown
    - » The name ("Michael Sonntag") is not unchecked!
  - → It is clearly shown who issued the certificate

Signed mail - Source

```
Received: from [140.78.100.211] (140.78.100.211) by smtp.fim.uni-linz.ac.at  (140.78.100.121) with Microsoft SMTP Server (TLS) id 8.3.159.2; Fri, 13
        May 2011 08:22:29 +0200
From: "Sonntag, Michael" <sonntag@fim.uni-linz.ac.at>
To: "Sonntag, Michael" <sonntag@fim.uni-linz.ac.at>
Date: Fri, 13 May 2011 08:22:29 +0200 / Subject: Signed Testmail
Thread-Topic: Signed Testmail / Thread-Index: AcwRNiL/lLW2mAtvR4OmVOxq3eDz7Q== / Message-ID: <4DCCCE25.2000403@fim.uni-linz.ac.at>
Reply-To: "Sonntag, Michael" <sonntag@fim.uni-linz.ac.at>
Accept-Language: de-AT, de-DE
Content-Language: de-DE
X-MS-Exchange-Organization-AuthAs: Internal
X-MS-Exchange-Organization-AuthMechanism: 10
X-MS-Exchange-Organization-AuthSource: exch2.ads2-fim.fim.uni-linz.ac.at
X-MS-Has-Attach: yes
X-MS-TNEF-Correlator:
user-agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; de; rv:1.9.2.17) Gecko/20110414 Thunderbird/3.1.10
Content-Type: multipart/signed; protocol="application/pkcs7-signature"; micalg=sha1; boundary="------------ms050604020205050902090606"
MIME-Version: 1.0

--------------ms050604020205050902090606
Content-Type: text/plain; charset=ISO-8859-15; format=flowed
Content-Transfer-Encoding: quoted-printable

This is a test mail, which is signed.
……..
--------------ms050604020205050902090606
Content-Type: application/pkcs7-signature; name="smime.p7s"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="smime.p7s"
Content-Description: S/MIME Cryptographic Signature
```

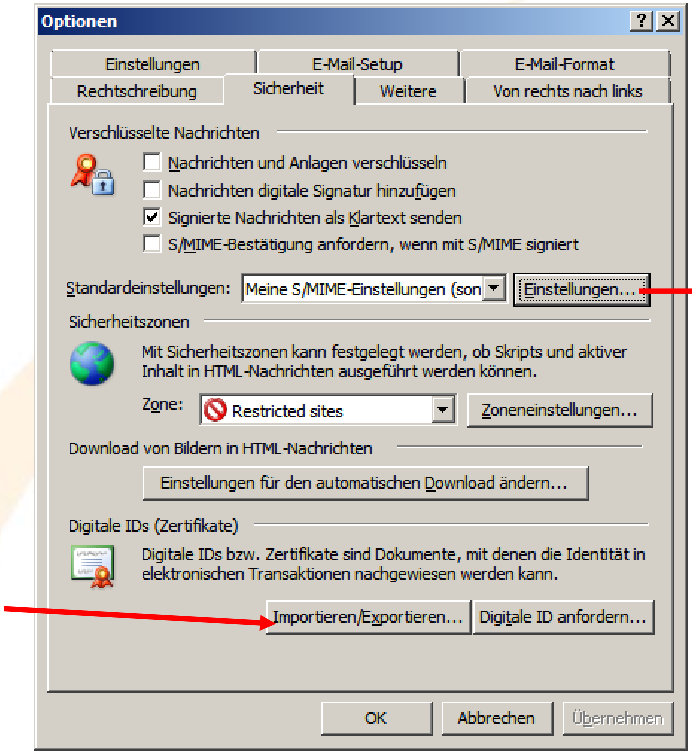
Transmission; not signature!

MIAGCSqGSIb3DQEHAqCAMIACAQExCzAJBgUrDgMCGgUAMIAGCSqGSIb3DQEHAQAAoIIP7TCC
BN0wggPFoAMCAQICEHGS++YZX6xNEoV0cTSiGKcwDQYJKoZIhvcNAQEFBQAwezELMAkGA1UE
BhMCR0IxGzAZBgNVBAgMEkdyZWF0ZXIgTWFuY2hlc3RlcjEQMA4GA1UEBwwHU2FsZm9yZDEa

Installing the certificate in Outlook 2003

- „Options“ – „Security“ – „Digital IDs (Certificates)“ – „Import“
  - → Select the file and import it
    - » Might require confirmation, depending on whether the root certificate is installed or not
- “Activating” the certificate (automatically done for first)
  - → „Options“ – „Security“ – “Signed messages”
  - → Allows setting encryption/signatures as default
  - → “Properties” allows creation of several profiles with different algorithms, certificates etc.

Installing the certificate in Outlook 2003



Optionen

Einstellungen | E-Mail-Setup | E-Mail-Format | Rechtschreibung | Sicherheit | Weitere | Von rechts nach links

Verschlüsselte Nachrichten

□ Nachrichten und Anlagen verschlüsseln
□ Nachrichten digitale Signatur hinzufügen
☑ Signierte Nachrichten als Klartext senden
□ S/MIME-Bestätigung anfordern, wenn mit S/MIME signiert

Standardeinstellungen: Meine S/MIME-Einstellungen (son [Einstellungen...]

Sicherheitszonen

Mit Sicherheitszonen kann festgelegt werden, ob Skripts und aktiver Inhalt in HTML-Nachrichten ausgeführt werden können.

Zone: Restricted sites [Zoneneinstellungen...]

Download von Bildern in HTML-Nachrichten

[Einstellungen für den automatischen Download ändern...]

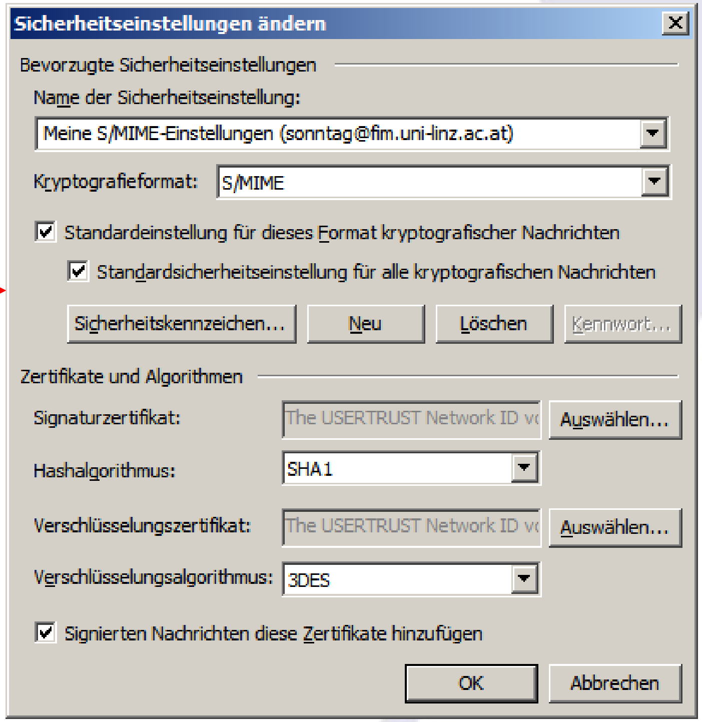
Digitale IDs (Zertifikate)

Digitale IDs bzw. Zertifikate sind Dokumente, mit denen die Identität in elektronischen Transaktionen nachgewiesen werden kann.

[Importieren/Exportieren...] [Digitale ID anfordern...]

[OK] [Abbrechen] [Übernehmen]

Certificate import



Sicherheitseinstellungen ändern

Bevorzugte Sicherheitseinstellungen

Name der Sicherheitseinstellung: Meine S/MIME-Einstellungen (sonntag@fim.uni-linz.ac.at)

Kryptografieformat: S/MIME

☑ Standardeinstellung für dieses Format kryptografischer Nachrichten
☑ Standardsicherheitseinstellung für alle kryptografischen Nachrichten

[Sicherheitskennzeichen...] [Neu] [Löschen] [Kennwort...]

Zertifikate und Algorithmen

Signaturzertifikat: The USERTRUST Network ID vo [Auswählen...]

Hashalgorithmus: SHA1

Verschlüsselungszertifikat: The USERTRUST Network ID vo [Auswählen...]

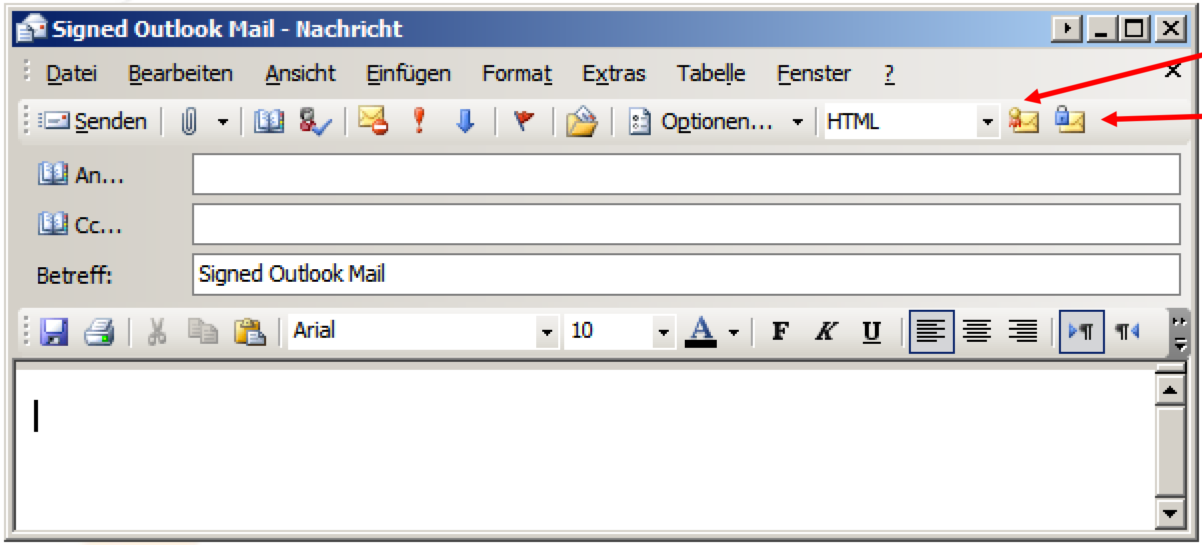
Verschlüsselungsalgorithmus: 3DES

☑ Signierten Nachrichten diese Zertifikate hinzufügen

[OK] [Abbrechen]

- Several different profiles are possible
  - → E.g. a „personal“ and a „business“ signature

Sending a signed E-Mail



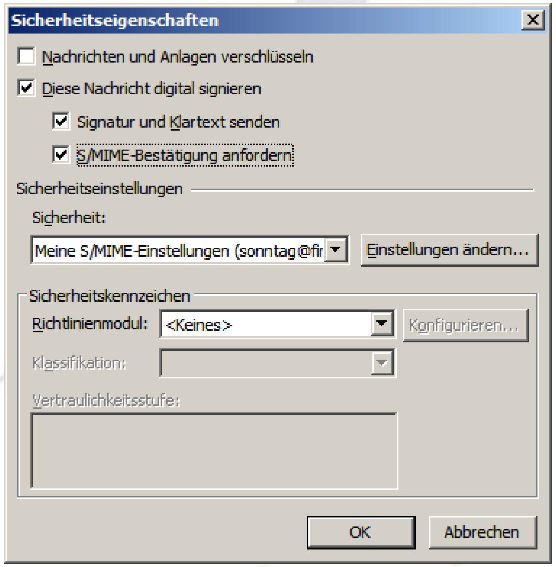
Betreff: Signed Outlook Mail

Sign message

Encrypt message

Both use the default profile

- „Options“ → „Security“ allows individual configuration through selection of a profile (see previous slide!)
  - → Selecting which “suite” of IDs, … to use



☐ Nachrichten und Anlagen verschlüsseln

☑ Diese Nachricht digital signieren

☑ Signatur und Klartext senden

☑ S/MIME-Bestätigung anfordern

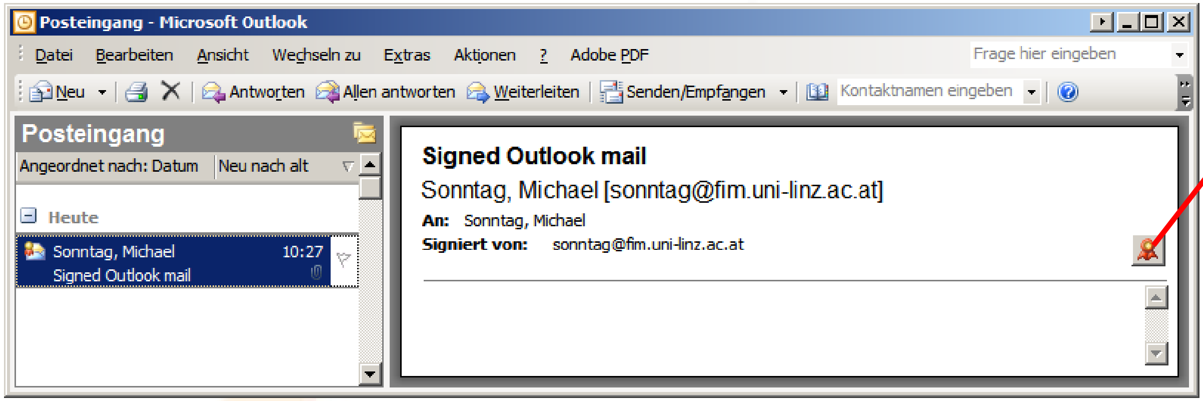
Sicherheitseinstellungen

Sicherheit: Meine S/MIME-Einstellungen (sonntag@fir

Sicherheitskennzeichen

Richtlinienmodul: <Keines>

Verifying a signature



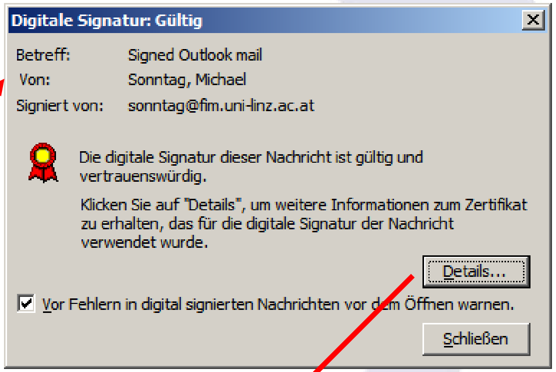
Sonntag, Michael 10:27
Signed Outlook mail

Signed Outlook mail

Sonntag, Michael [sonntag@fim.uni-linz.ac.at]

An: Sonntag, Michael

Signiert von: sonntag@fim.uni-linz.ac.at



Betreff: Signed Outlook mail

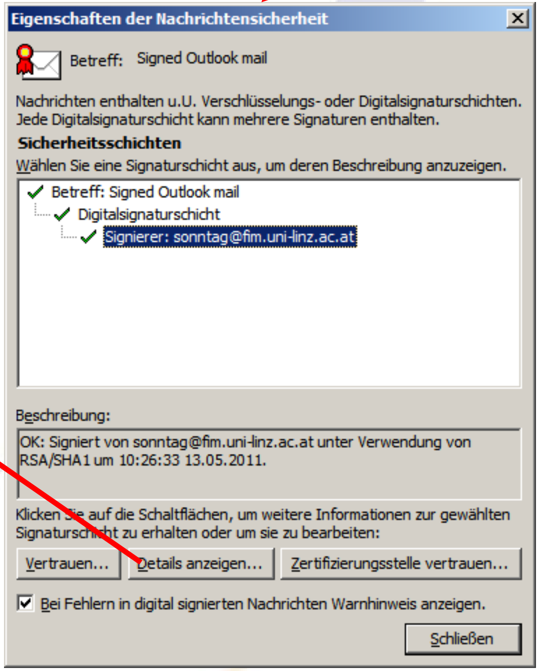
Von: Sonntag, Michael

Signiert von: sonntag@fim.uni-linz.ac.at

Die digitale Signatur dieser Nachricht ist gültig und vertrauenswürdig.

Klicken Sie auf "Details", um weitere Informationen zum Zertifikat zu erhalten, das für die digitale Signatur der Nachricht verwendet wurde.

☑ Vor Fehlern in digital signierten Nachrichten vor dem Öffnen warnen.



Betreff: Signed Outlook mail

Nachrichten enthalten u.U. Verschlüsselungs- oder Digitalsignaturschichten. Jede Digitalsignaturschicht kann mehrere Signaturen enthalten.

Sicherheitsschichten

Wählen Sie eine Signaturschicht aus, um deren Beschreibung anzuzeigen.

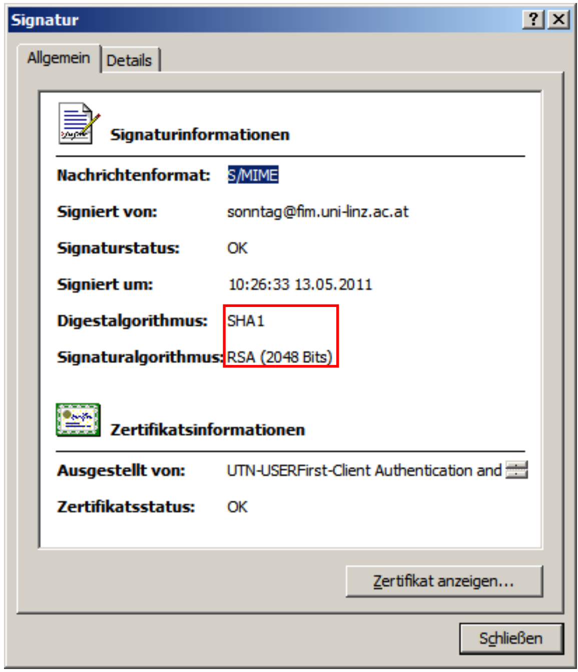
- ✓ Betreff: Signed Outlook mail
  - ✓ Digitalsignaturschicht
    - ✓ Signierer: sonntag@fim.uni-linz.ac.at

Beschreibung:

OK: Signiert von sonntag@fim.uni-linz.ac.at unter Verwendung von RSA/SHA1 um 10:26:33 13.05.2011.

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

☑ Bei Fehlern in digital signierten Nachrichten Warnhinweis anzeigen.



Signaturinformationen

Nachrichtenformat: S/MIME

Signiert von: sonntag@fim.uni-linz.ac.at

Signaturstatus: OK

Signiert um: 10:26:33 13.05.2011

Digestalgorithmus: SHA1

Signaturalgorithmus: RSA (2048 Bits)

Zertifikatsinformationen

Ausgestellt von: UTN-USERFirst-Client Authentication and

Zertifikatsstatus: OK

- Details are optional
  - → "Icon" is sufficient!
- Subject and sender are listed, but „signed by" is again only the E-Mail address
  - → It's the only thing in the certificate!

E-Mail encryption

- Encrypting E-Mail is more complex, as the certificate of the (respectively all) recipients is required
  - → Distribution problem!
- Otherwise there is no difficulty/change
  - → Both official and custom certificates are suitable for this in both Thunderbird and Outlook
- Attention: The mail is decrypted on access (=opening it), not on receipt!
  - → What does this mean for a “lost” key?
    - » You loose access to the E-Mail contents!

Tasks

- Make sure you have a copy of both certificates
  - → **And** the associated private keys!
- Install both the official and the manually generated signature
  - → Send an E-mail to yourself with both
    - » Signed
    - » Encrypted
    - » Signed+Encrypted
  - → Verify the signatures in all cases and check whether the encrypted content can be read
  - → Delete the certificates (You “lost” them through crash, ….)
    - » Can you obtain the official certificate from the Comodo CA?
      - – How about other CAs?
  - → Try the verification/decryption again
  - → Experiment with archiving/exporting the E-Mails as well

Conclusions

- For closed systems a custom signature is no problem
  - → Widespread use → Try to get an „official“ one
- Practical difficulties:
  - → Certificate distributions
    - » Because of the short validity periods of certificates
  - → Automatic added signatures, disclaimers, … in companies
- Take care, what is guaranteed with a certificate
  - → I.e., what has been verified to which degree before issuing
- Legal validity needed?
  - → Not even “official” certificates might be enough
  - → Take care of archiving (electronic!) and re-signing
    - » (Third-party!) Timestamps are not part of a signature!

Questions?

Thank you for your attention!

Literature/Links

- OpenSSL:
  http://www.openssl.org/
- OpenSSL precompiled for Windows:
  http://www.slproweb.com/products/Win32OpenSSL.html