

# ***Digital Rights Management (DRM)***

***Verfahren, die helfen Rechte an virtuellen Waren durchzusetzen***

---

**Vorlesung im Sommersemester 2010 an der  
Technischen Universität Ilmenau von  
Privatdozent Dr.-Ing. habil. Jürgen Nützel,  
Vorstand der 4FriendsOnly.com Internet Technologies AG (4FO AG)  
JN (at) 4FO (dot) DE**



## ***Public-Key-Kryptographie (2 Termine)***

***Folien stellen ein zusätzliches Informationsangebot für die Teilnehmer der Vorlesung dar.  
Die Vorlesung richtet sich an Studierende der Informatik,  
der Ingenieurinformatik, Wirtschaftsinformatik, Medienwirtschaft,  
Angewandten Medienwissenschaft und Medientechnik.***

***Diese Folien und weitere Informationen unter: [www.juergen-nuetzel.de/drm\\_lecture.html](http://www.juergen-nuetzel.de/drm_lecture.html)***

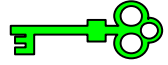

# Überblick

---

- Grundprinzip
- Anwendungen bei DRM
- Geheime Übertragung des CEK
- Zertifikate
- Digitale Signatur
- Hash-Funktion
- RSA-Verfahren

# Public-Key-Kryptographie

## □ Grundprinzip

- *Es gibt zwei Schlüssel (=Schlüsselpaar)*
- *Was mit dem einen verschlüsselt wird kann nur mit dem anderen entschlüsselt werden (=asymmetrisch)*
- *Der eine Schlüssel heißt öffentlich: Public Key* 
- *Der andere Schlüssel heißt privat: Private Key* 

# Allgemeine Anwendungen [1]

## □ Beispiel: Verschlüsselte E-Mail oder SSL

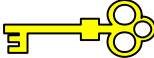
- *Sender einer geheimen E-Mail (z.B.) verschlüsselt diese mit dem öffentlichen Schlüssel des Empfängers*
- *Da asymmetrische Verfahren langsam sind, wird der Inhalt (Nutzdaten) mit einem schnellen symmetrischen Algorithmus (z.B. AES) verschlüsselt. Der symmetrische Schlüssel wird mit dem öffentlichen Schlüssel des Empfängers verschlüsselt. (= hybrid)*

# Allgemeine Anwendungen [2]

## □ Digitale Signatur:

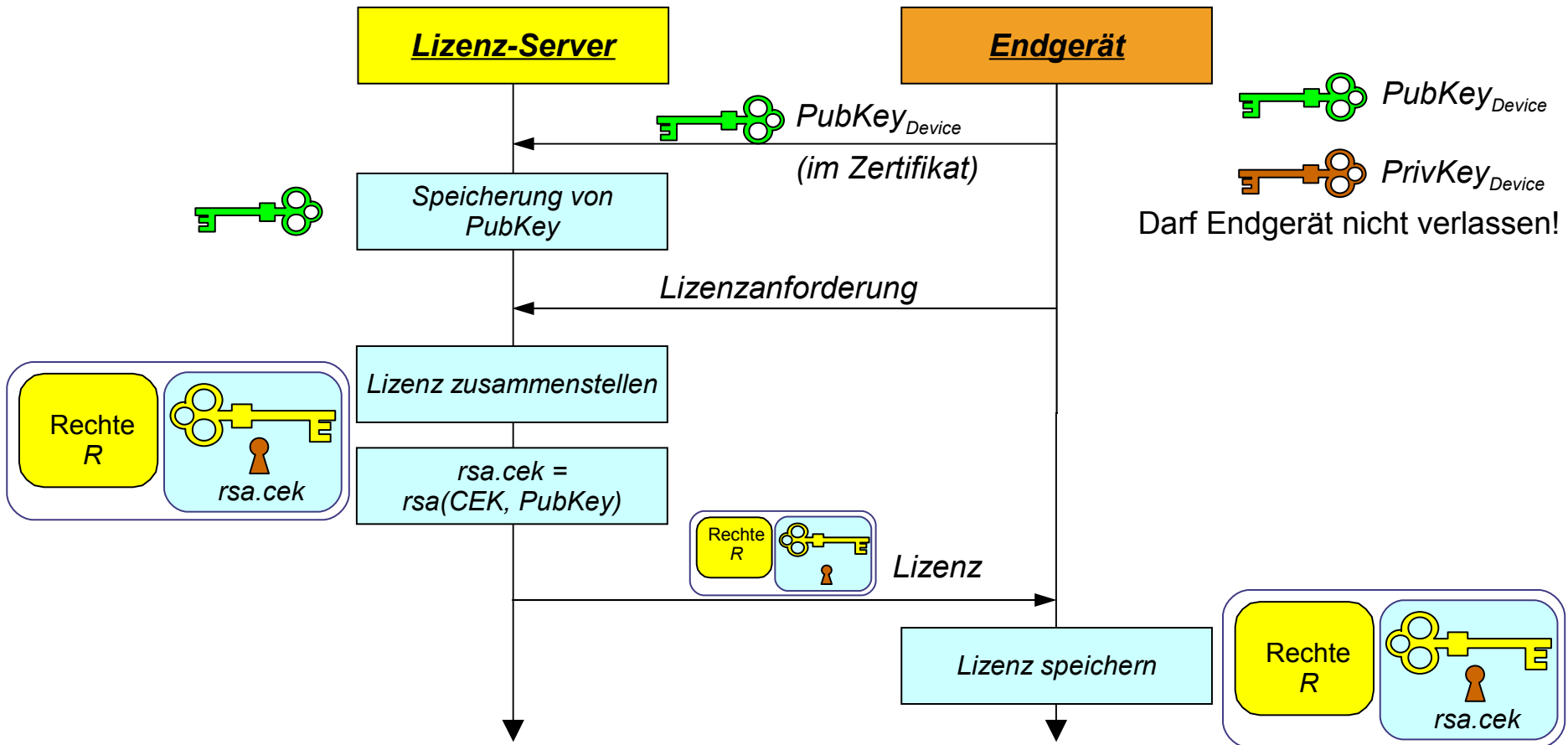
- *Integrität von Nachrichten und Authentizität von Kommunikationspartner muss sichergestellt werden*
- *Ausgetauschte (nicht verschlüsselte) Dokumente (z.B. Rechte in der Lizenz) dürfen nicht verändert werden*
- *Beteiligte Kommunikationspartner (z.B. Endgerät und Lizenz-Server) müssen sich über den jeweils anderen sicher sein können*
- *Einsatz von Zertifikaten (z.B. nach X.509)*
- *Prinzip vereinfacht: Der Sender überträgt das Dokument doppelt. Einmal unverschlüsselt. Ein zweites mal mit seinem privaten Schlüssel verschlüsselt.*
- *Besser: Sender verschlüsselt mit seinem privaten Schlüssel nur eine Prüfsumme (Hash-Wert, Details später) des Dokumentes.*

# Anwendungen bei DRM

- **Geheime Übertragung des CEK:** 
  - *Endgerät fordert von einem Lizenz-Server den passenden Schlüssel für die Nutzdaten an.*
  - *Lizenz-Server verschlüsselt den CEK (Content Encryption Key) mit dem öffentlichen Schlüssel des Endgerätes*

# Geheime Übertragung des CEK

## □ Sequenz-Diagramm



# Authentizität durch Zertifikate

- ❑ **Wie kann der Lizenz-Server dem Endgerät vertrauen?**
  - *Dem öffentliche Schlüssel alleine darf man noch nicht trauen*
  - *Von einer offiziellen Instanz (CA – Certification Authority) ausgestellte Zertifikate bieten Abhilfe*
- ❑ **Was ist ein Zertifikat (nach X.509)?**
  - *Der öffentliche Schlüssel und*
  - *Ein Datensatz über den Besitzer des Schlüssel*
  - *Beides zusammen wurde von einer CA digital signiert*
  - *Das Zertifikat der CA kann beigefügt sein*
- ❑ **Zertifikatsketten**
  - *Der Aussteller des Zertifikates besitzt ein eigenes Zertifikat*



# Zertifikat nach X.509v3

**Zertifikatsinformationen**

Dieses Zertifikat ist für folgende Zwecke beabsichtigt:

- Garantiert dem Remotecomputer Ihre Identität
- Schützt E-Mail-Nachrichten

**Ausgestellt** Thawte Freemail Member

**Ausgestellt** Thawte Personal Freemail Issuing CA

**Gültig ab** 16.05.2006 **bis** 16.05.2007

Sie besitzen einen privaten Schlüssel für dieses Zertifikat.

**Zertifikat**

Anzeigen: <Alle>

Feld	Wert
Version	V3
Seriennummer	73 a4 6b 14 01 42 5e 83 80 4c...
Signaturalgorithmus	md5RSA
Aussteller	Thawte Personal Freemail Issu...
Gültig ab	Dienstag, 16. Mai 2006 10:30:11
Gültig bis	Mittwoch, 16. Mai 2007 10:30:11
Antragsteller	jn@4fo.de, Thawte Freemail ...
Öffentlicher Schlüssel	RSA (2048 Bits)

```
30 82 01 0a 02 82 01 01 00 e6 c8 d9 85 3e
5e 69 c6 e2 23 8d 15 ab 58 53 ce 6b dd b9
19 ad 5a a3 d4 89 4f 08 13 9b c6 d7 27 ce
06 11 b8 93 be 1e 8c be 61 78 4a d6 45 9c
45 6c 38 a0 1d 5e 71 fc 1a 52 73 a3 d4 63
07 af ed 25 26 5c e7 01 17 7b 8f 95 fd 3c
ad ba 8c ae f9 22 63 86 9a 7f 52 92 fc c4
34 90 21 ac 79 1e 33 b3 f2 52 e2 84 e0 b8
06 3e 5e a4 c8 38 e3 61 6e 06 81 2f 94 0a
```

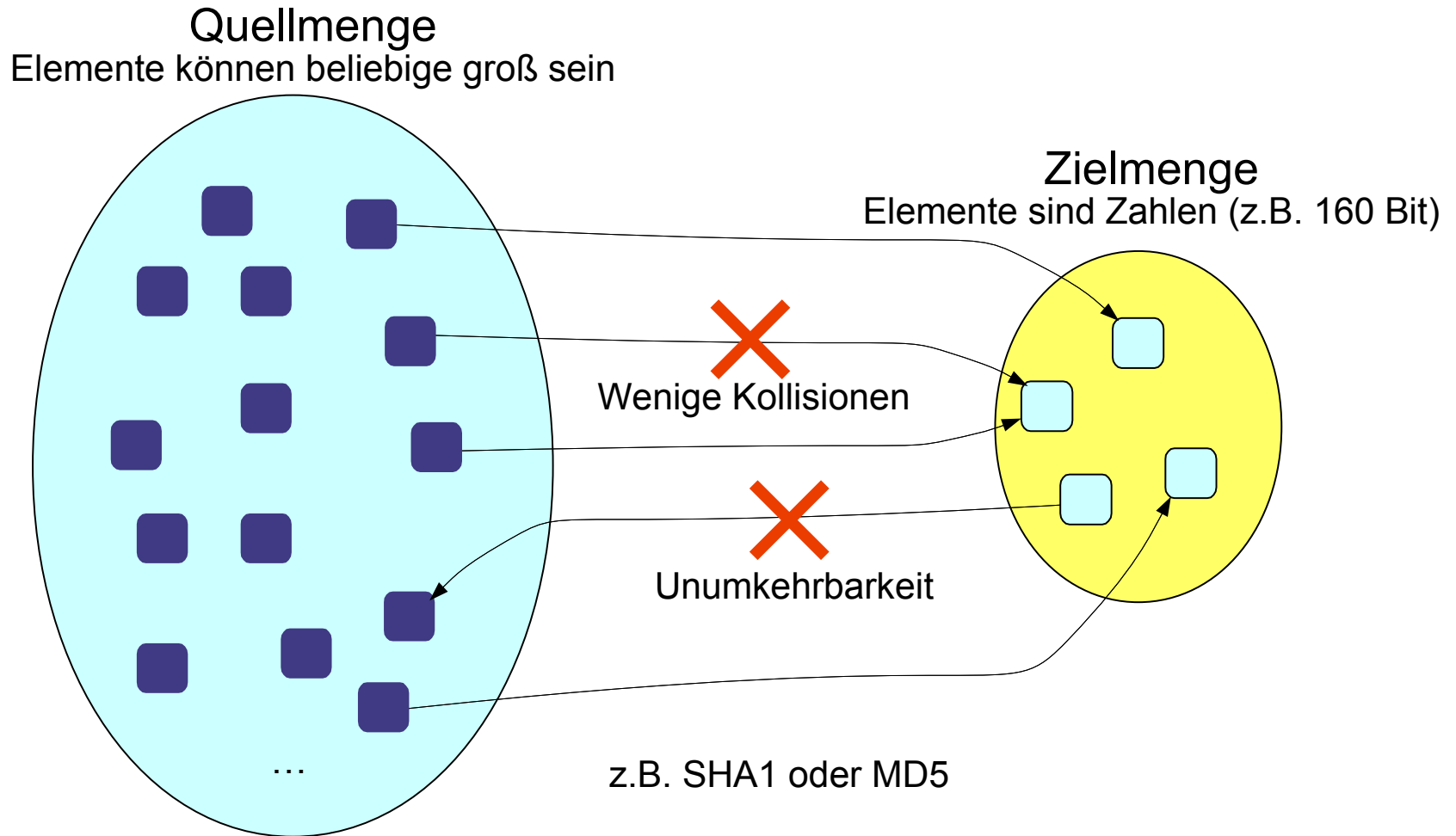
Eigenschaften bearbeiten... In Datei kopieren...

OK

# Kryptographische Hash-Funktion [1]

- ... wird für die digitale Signatur benötigt
  - *Wird auch Streuwertfunktion genannt*
  - *Die Hash-Funktion ist eine Funktion, die zu einer Eingabe aus einer (üblicherweise) großen Quellmenge eine Ausgabe aus einer (im Allgemeinen) kleineren Zielmenge (die Hash-Werte, meist eine Teilmenge der natürlichen Zahlen) erzeugt.*
  
- Dabei muss gelten:
  - *Kollisionsfreiheit*
    - *Es darf nicht effizient möglich sein, zwei Quellelemente mit demselben Hash-Wert zu finden.*
  - *Unumkehrbarkeit*
    - *Zu der Funktion gibt es keine effizient berechenbare Umkehrfunktion, mit der es möglich wäre, für ein gegebenes Zielelement ein passendes Quellelement zu finden*

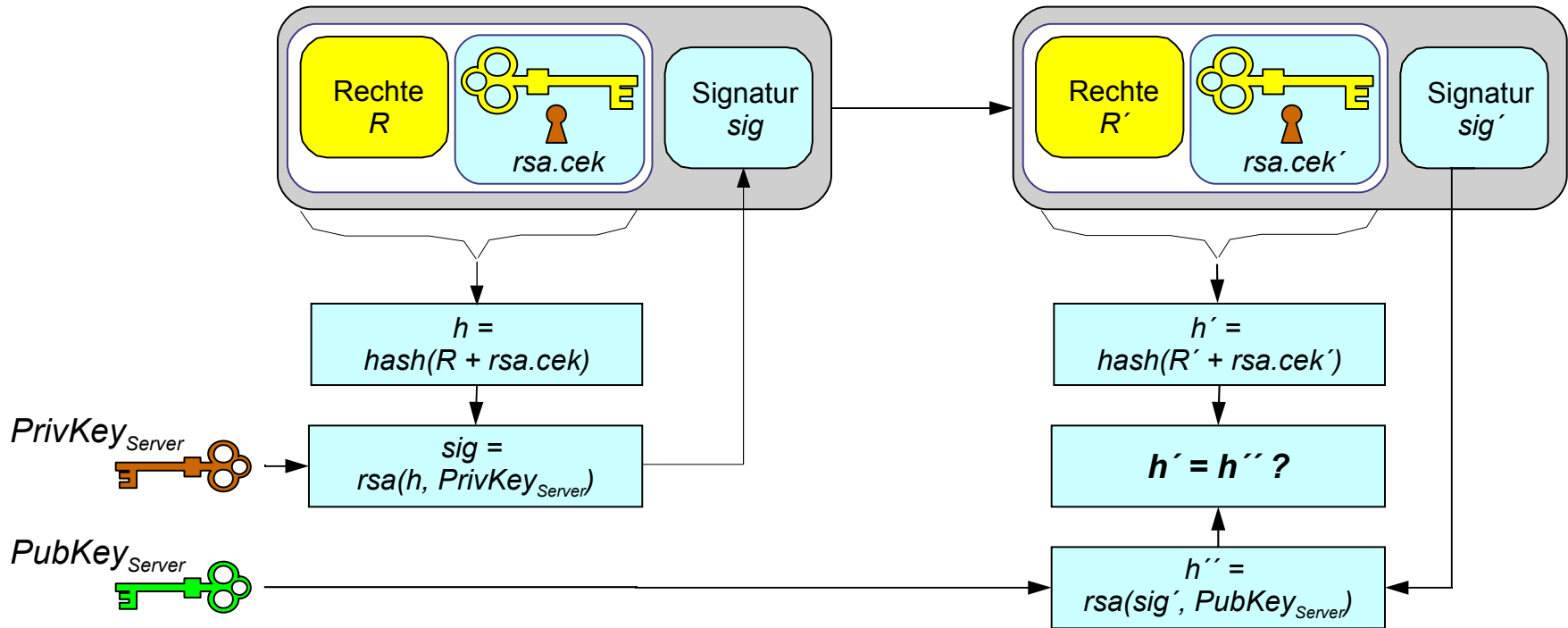
# Kryptographische Hash-Funktion [2]



# Sicherung der Integrität & Authentizität



## □ ... der Lizenz durch digitale Signatur

- *Mit dem Private Key des Lizenz-Servers wird ein über die Rechte und Schlüssel errechneter Hash-Wert verschlüsselt*



Hier sollte ein Zertifikat genutzt werden

# Das RSA-Verfahren

- **RSA (Rivest, Shamir, Adleman)**
- **Idee: Multiplikation ist einfach.  
Die Umkehrung, die  
Faktorisierung, ist schwierig**
- **Nehme zwei etwa gleich lange  
Primzahlen:  $p$  und  $q$   
(Beispiel:  $p=11$ ,  $q=13$ )**
- **Berechne  $n = p*q$  ( $n = 143$ )**
- **Berechne  $\varphi(n) = (p-1)*(q-1)$  ( $=120$ )**
- **Wähle  $e$  (23) mit  $\text{ggT}(e, \varphi(n)) = 1$**
- **Berechne  $d$  so, dass  
 $e * d \equiv 1 \pmod{\varphi(n)}$  gilt,  
 $e * d = k * \varphi(n) + 1$   
( $d = 47$  mit  $k = 9$ )**
- **Public Key:  $(n, e)$  (143, 23)** 
- **Private Key:  $(n, d)$  (143, 47)** 
- **Verschlüsselung mit Public Key:  
 $C \equiv K^e \pmod{n}$   
 $2 \equiv 7^{23} \pmod{143}$**
- **Entschlüsselung mit Private Key:  
 $K \equiv C^d \pmod{n}$   
 $7 \equiv 2^{47} \pmod{143}$**
- **Damit  $n$  im praktischen  
Anwendungsfall nicht in  $p$  und  $q$   
faktorisiert werden kann, muss  $n$   
aktuell eine 1024 bis 2048 bit  
lange Zahl sein !!**

# Ein 1024 bit RSA-Schlüsselpaar

■  $n =$

15111708856051554354358350911209909796200366355660  
70449955373462784818812841149924376617947273003611  
32467861422736444261887801298612841233509930473048  
07418687404822537457983381051416850071883414427590  
23472137502239327525220759222961234670244334027979  
06496071473309891192170853187418104035346071158728  
163015279

■  $e = 65537$  (fast immer gleich, damit öffentlich)

■  $d =$

28437784048962238102491957487823949450926822751173  
14930390408611398930439106138824989979575463929312  
97851005527657440389682508112332296402471576746586  
18774782653583162649400546666901513074991074038701  
46364067664383999167594213162163415356043745514827  
29571882157734877943009193315973748619065480266710  
91235657

# Nächste Vorlesung

---

- **DRM-Referenz-Modell**
  - *Aufbau*
  - *Neue Geschäftsmodelle*
  - *Sicherheit der Implementierung*

# Weitere Informationen

- **Jürgen Nützel: Die informatorischen Aspekte virtueller Güter und Waren, Oktober 2006 im Universitätsverlag Ilmenau, [www.juergen-nuetzel.de/habilitation.html](http://www.juergen-nuetzel.de/habilitation.html)**
- **Jürgen Nützel: Digital Rights Management (Seite 28 - 49), in Die Privatkopie, herausgegeben von Frank Fechner, 2007, Universitätsverlag Ilmenau, ISBN 978-3-939473-06-0, <http://www.db-thueringen.de/servlets/DocumentServlet?id=7543>**
- **Reinhard Wobst: Abenteuer Kryptologie. 3. Auflage, Addison-Wesley, München 2003**
- **[http://de.wikipedia.org/wiki/Digitale\\_Signatur](http://de.wikipedia.org/wiki/Digitale_Signatur)**
- **The Internet Society: RFC 3280 Internet X.509 Public Key Infrastructure, <http://www.ietf.org/rfc/rfc3280.txt>**
- **[http://de.wikipedia.org/wiki/Digitales\\_Zertifikat](http://de.wikipedia.org/wiki/Digitales_Zertifikat)**
- **<http://de.wikipedia.org/wiki/RSA-Kryptosystem>**