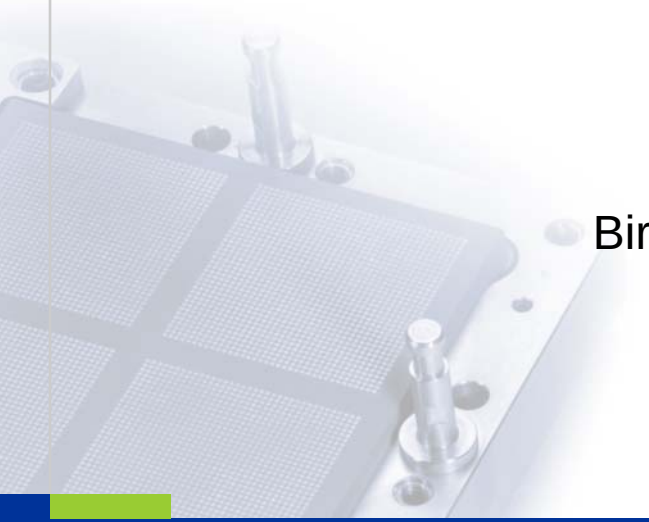
R|R|Z|N

UH-CA: Zertifikate für digitale Signaturen und Verschlüsselung an der Universität Hannover



Sicherheitstage WS 04/05

Birgit Gersbeck-Schierholz, RRZN

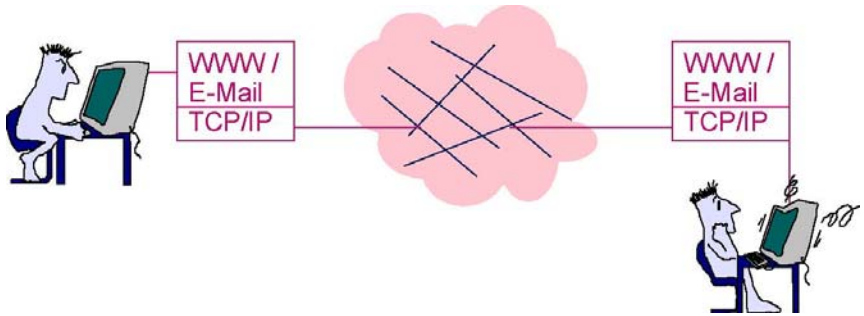
R|R|Z|N

- **Warum werden digitale Signaturen und Verschlüsselung eingesetzt?**
- **Welche kryptografischen Verfahren werden bei der digitalen Signatur verwendet und wie sicher sind diese?**
- **Welche Rolle spielt dabei eine CA?**
- **Welches sind die konkreten Einsatzgebiete für Zertifikate?**
- **UH-CA: Zertifikate an der Universität Hannover**

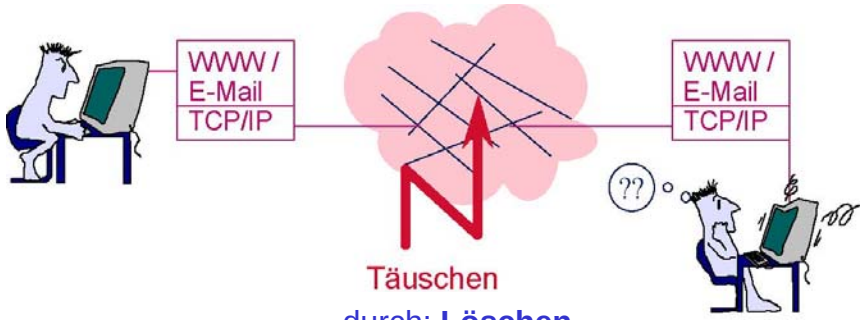
Grundanliegen der digitalen Signatur: Authentizität, Integrität und Vertraulichkeit

R|R|Z|N

Netze verbinden die Menschen



Netze trennen die Menschen



Täuschen

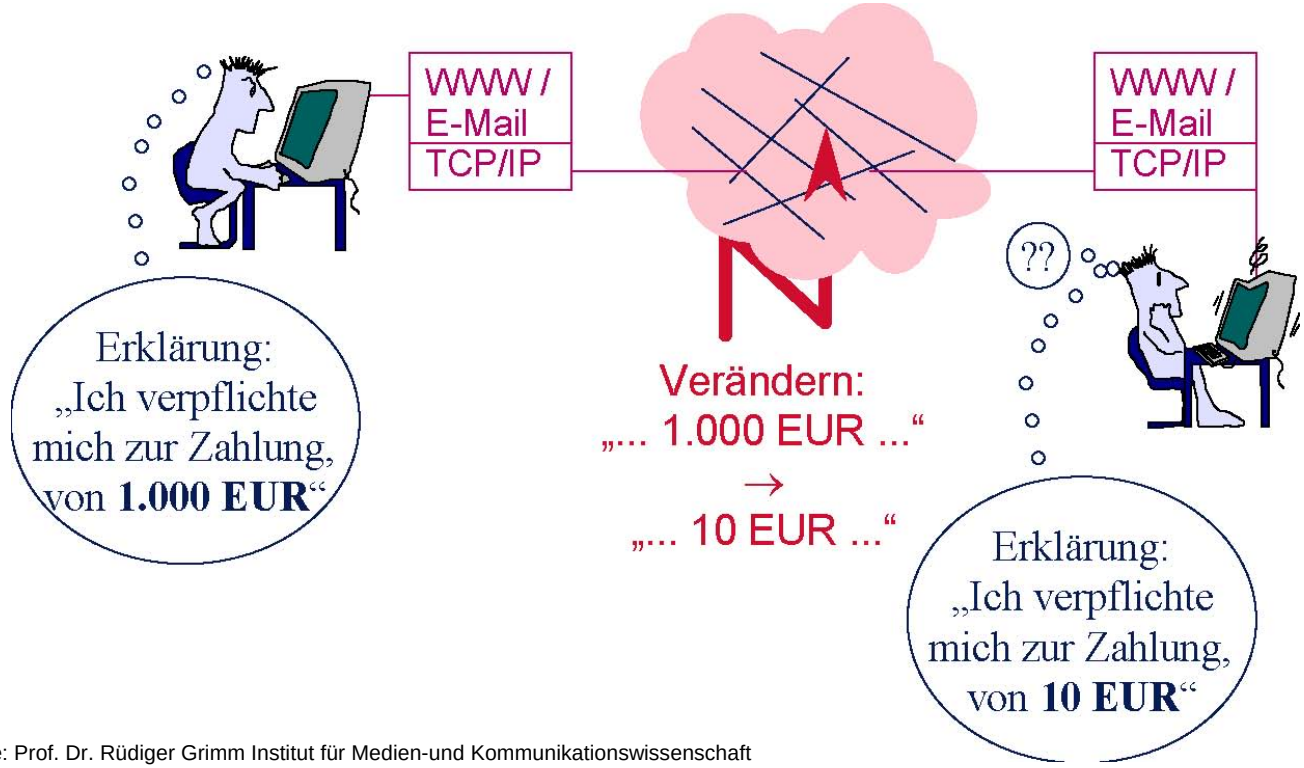
durch: **Löschen**
Verändern Fälschen
Lauschen Fehlverhalten
Abstreiten

Quelle: Prof. Dr. Rüdiger Grimm Institut für Medien-und Kommunikationswissenschaft Technische Universität Ilmenau

Grundanliegen der digitalen Signatur: Authentizität, Integrität und Vertraulichkeit

R|R|Z|N

Verletzen der Kommunikation:



Quelle: Prof. Dr. Rüdiger Grimm Institut für Medien-und Kommunikationswissenschaft

Technische Universität Ilmenau

Grundanliegen der digitalen Signatur: Authentizität, Integrität und Vertraulichkeit

R|R|Z|N

- Für die im Internet übertragene Information (E-Mail, Kommunikation zwischen Benutzer und Webserver) gibt es zunächst
  - **keinerlei Garantie** für die **Echtheit**, **Unversehrtheit** und **Vertraulichkeit** der Nachrichten. In den meisten Fällen ist das auch kein Problem, denn andernfalls hätte sich das Internet längst nicht so rasant entwickelt.

- Wenn es aber darauf ankommt, dass
  - der Inhalt einer E-Mail **nur dem echten Empfänger** bekannt wird,
  - die Eingabedaten in einem Webformular **nur zu der Firma gelangen, für die sie bestimmt sind**,
  - braucht man eine Möglichkeit, um Personen, Institutionen und auch Webserver **eindeutig zu identifizieren**.

Grundanliegen der digitalen Signatur: Authentizität, Integrität und Vertraulichkeit ..

R|R|Z|N

- **Authentizität**
  - Identität des Absenders ist eindeutig
- **Vertraulichkeit**
  - Daten können von Dritten nicht gelesen werden
- **Integrität**
  - Daten wurden nicht verändert
- **Verbindlichkeit**
  - kann nicht mehr abgestritten werden

– **Diese Kriterien können mit kryptografischen Methoden erfüllt werden**

- **Symmetrische Verschlüsselung**
  - Ältestes Verfahren zur Verschlüsselung, z.B.Cäsar-Verschlüsselung ..
  - Beide Kommunikationspartner benutzen denselben Schlüssel zur Ver- und Entschlüsselung

- Nachteil: ein sicherer **Schlüsselaustausch** ist nur über ein persönliches Treffen oder einen Kurier zu realisieren

Kryptografische Methoden

R|R|Z|N

- **Moderne Symmetrische Verschlüsselungsverfahren**
  - 3DES, IDEA, Blowfish, AES usw. (Schlüssellänge derzeit ca. 128 – 196 bit)
  - effektiv aufgrund relativ kurzer Schlüssellängen
  - Nachteil: unsicherere Übertragung des Schlüssel übers Netz

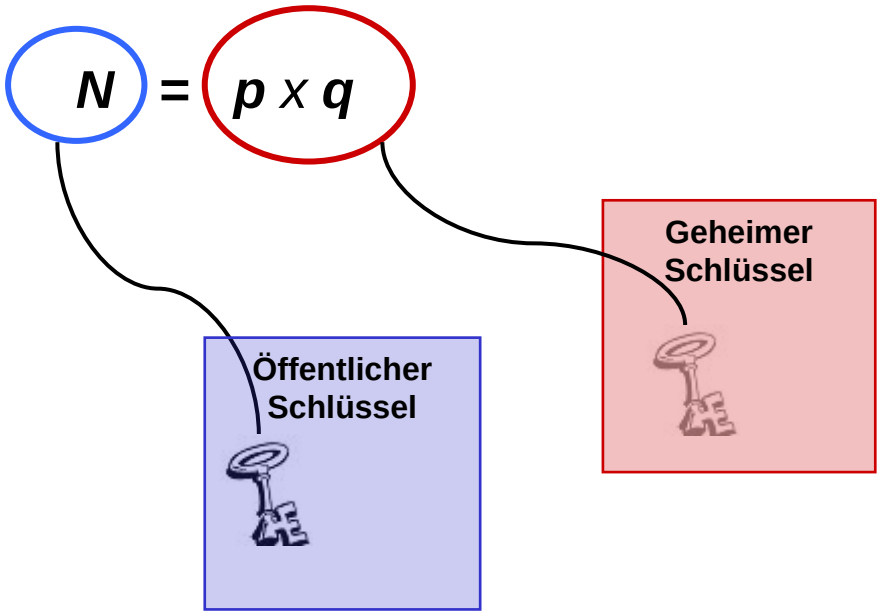
- Gesucht wurde lange Zeit nach einem Verfahren, das es ermöglichte auf den Austausch von geheimen Schlüsseln zu verzichten..

- **Asymmetrische Verschlüsselung**
  - Gibt es seit 1976 (Diffie/Hellmann)
  - Das Revolutionäre war damals **die Idee die Schlüssel zum Ver- und Entschlüsseln zu trennen**

  - Jeder Kommunikationspartner verfügt über ein **Schlüsselpaar**, dieses besteht aus 2 unterschiedlichen Schlüsseln:
    1. ***Geheimer Schlüssel*** zum Verschlüsseln (nur für mich)
    2. ***Öffentlicher Schlüssel*** zur Rückgewinnung des Textes (für alle anderen)

Was mit dem öffentlichen Schlüssel verschlüsselt wurde, kann nur mit dem geheimen Schlüssel lesbar gemacht werden und umgekehrt

- **Worauf basiert die Asymmetrische Verschlüsselung?**
  - Einwegfunktionen
  - *z.B.* RSA - Rivest, Shamir, Adleman (1978): Basiert im Wesentlichen auf der Schwierigkeit der Primfaktorzerlegung



***p und q sind sehr große* Primzahlen**

- **Wie sicher ist die Asymmetrische Verschlüsselung?**
  - Bei Auswahl hinreichend großer Primzahlen können **p** und **q** nicht ermittelt werden

Beispiel: RSA-576

N= 188198812920607963838697239461650439807163563379417382700763356422988859715234665485319060606504743045317388011303396716199692321205734031879550656996221305168759307650257059

wurde im Dezember 2003 faktorisiert und zwar in:

p= 3980750 8642406493 7397125500 5503864911 9906436234 2526708406 3851895759 4638895726 1768583317

×

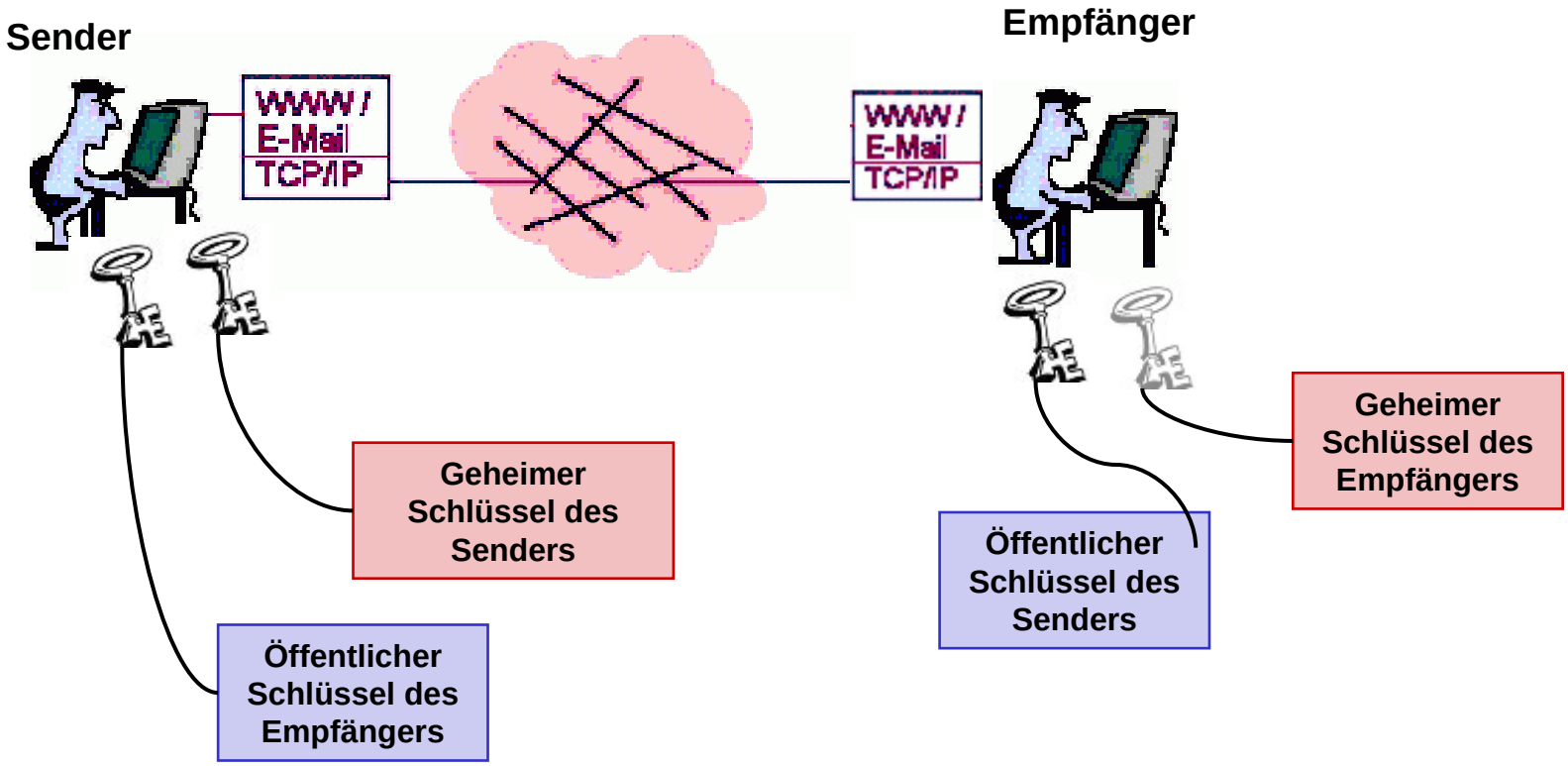
q= 4727721 4610743530 2536223071 9730482246 3291469530 2097116459 8521711305 2071125636 3590397527

→10.000 US-Dollar

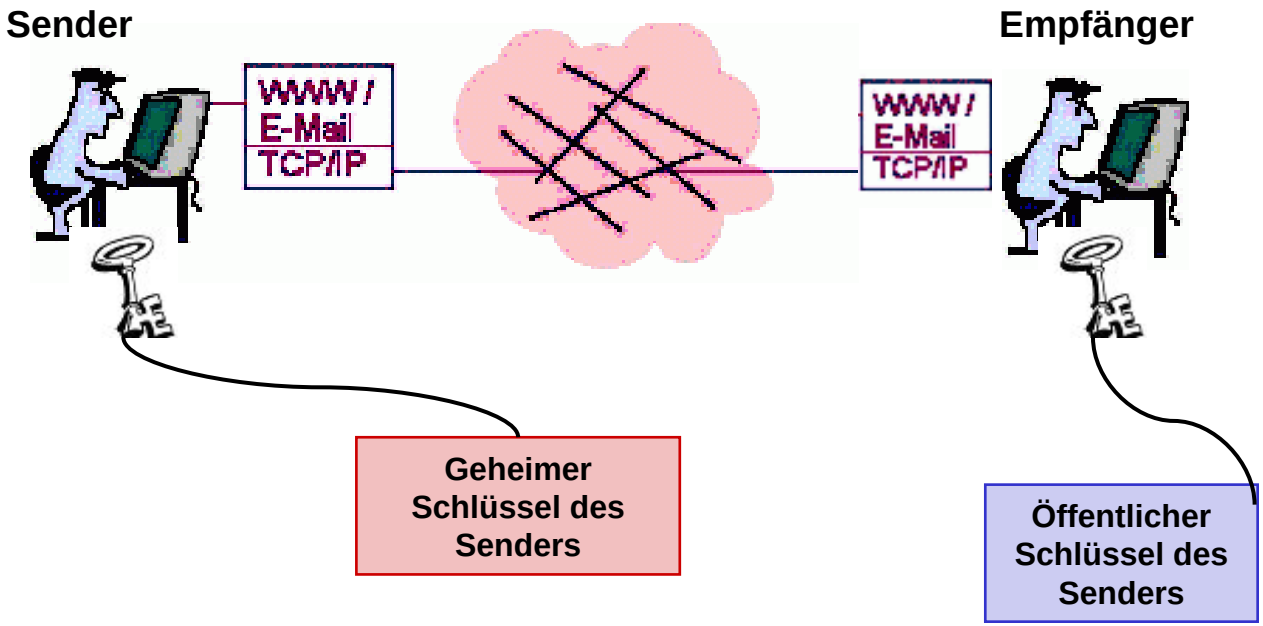
http://www.rsasecurity.com/rsalabs/node.asp?id=2093

- Die aktuell für RSA-Verschlüsselungsverfahren empfohlenen Schlüssellängen von **1024** und **2048** Bit können mit praktikablen Mitteln nicht entschlüsselt werden

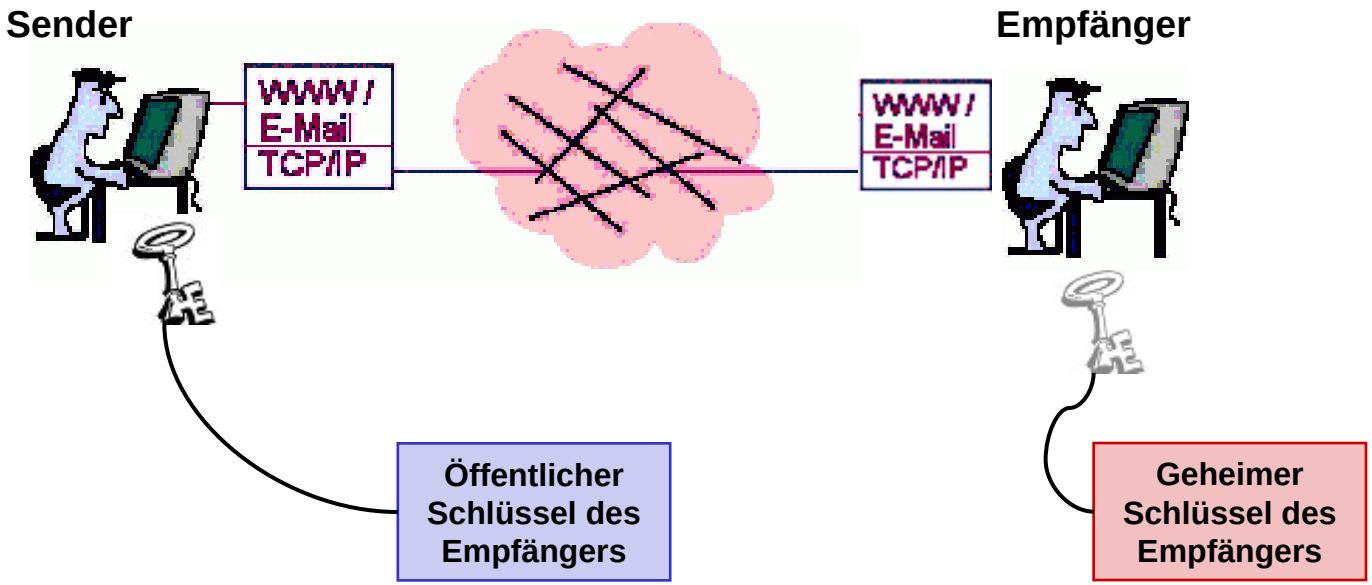
- **die zwei Anwendungsformen der Asymmetrischen Verschlüsselung**
  1. Signieren: Authentizität, Integrität, Verbindlichkeit herstellen
  2. Verschlüsseln**:** Vertraulichkeit herstellen



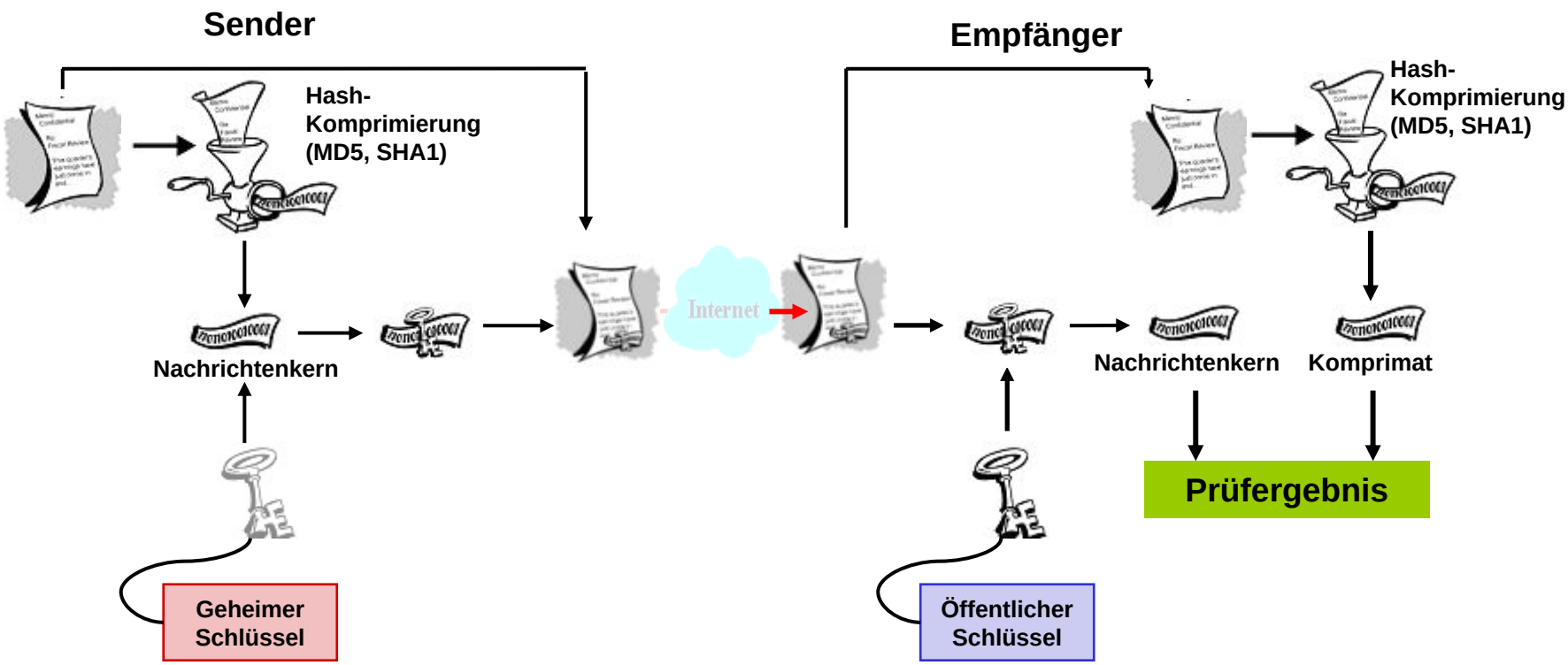
1. **Signieren: Authentizität, Integrität, Verbindlichkeit herstellen**



2. Verschlüsseln: Vertraulichkeit herstellen



- Schematische Darstellung des Signiervorganges



Zertifikate

- Das Dilemma bei asymmetrischen Verschlüsselungsverfahren:

  Kann man den Angaben im öffentlichen Schlüssel vertrauen?

  - Dies ist nur dann kein Problem, wenn man den Schlüssel persönlich vom Eigentümer bekommen hat (Vorteil der Schlüsselverteilung gegenüber der symmetrischen Verschlüsselung wäre damit hinfällig).

- Lösung:
  - Eine vertrauenswürdige Instanz stellt die eindeutige, zweifelsfreie Zuordnung zwischen einem Schlüsselpaar und einer Person oder einem Rechner her:

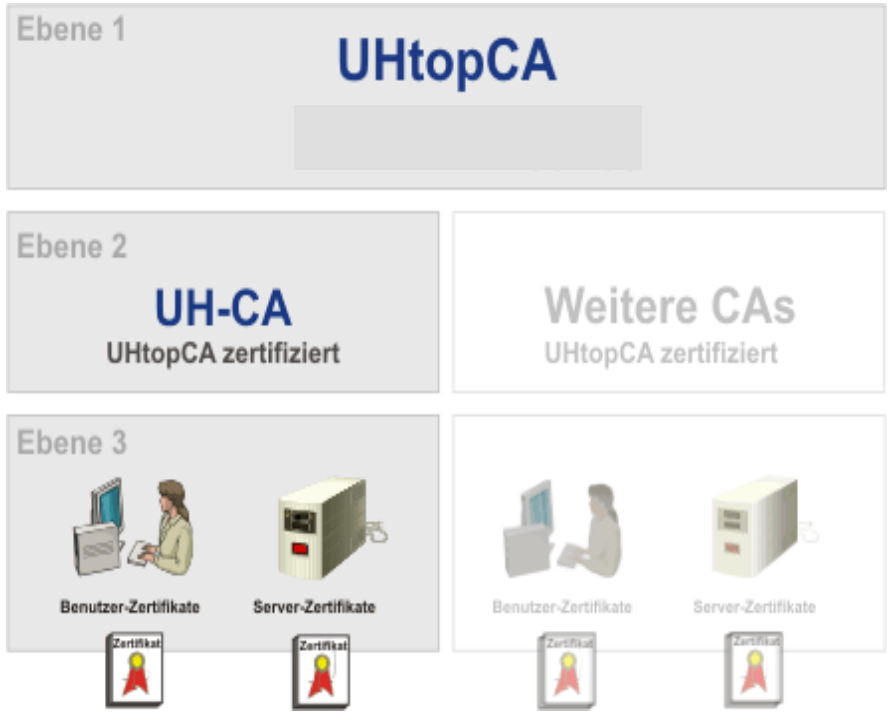
    Zertifizierungsstelle, CA (Certification Authority)
  - Nach Prüfung der Identität und des öffentlichen Schlüssels, stellt die CA ein Zertifikat aus.

Zertifikat 

Zertifikate

- Die grundsätzlichen Aufgaben von Zertifikaten sind:
  - Vertrauen in die **Korrektheit der Schlüsselangaben** aufzubauen
  - Dies hängt ab von dem **Vertrauen in die Zertifizierungsinstanz (CA)**
  - Die CA wirbt mit ihren **Zertifizierungsrichtlinien (Policy)** um dieses Vertrauen

- **Zertifizierung an der Universität Hannover:**
  - **anerkannte Zertifizierungsstelle seit 25. Mai 2004**



Zertifizierungs-Standard X.509v3

R|R|Z|N

- **Zertifizierungs-Standard X.509:**
  - Gibt eine Hierarchische Grundstruktur vor - **Hierarchie nach PEM – RFC 1422**
  - Ein X.509-Zertifikat ist eine Sammlung von Standardfeldern, die Informationen über einen Benutzer oder einen Server und die entsprechenden öffentlichen Schlüssel enthalten.
  - Die aktuelle Version ist derzeit **X.509v3.**

Zertifizierungs-Standard X.509v3

RRZN

- ein **Zertifikat** nach dem **Standard X.509v3** besteht im Wesentlichen aus 4 Teilen:

Öffentlicher Schlüssel		00:ab:77:e0:53:4a:4a:6b:42:8b:e0:4b:91:14:6f: df:e7:28:4f:58:e5:43:b5:01:71:fa:24:2f:6c:4e: … 39:04:62:2f:fd:20:4a:a3:d0:00:78:c8:e7:44:7a
Angaben über den Schlüsselinhaber (Common Name nach x.509v3 (CN))		C=DE, O=Universitaet Hannover, OU=RRZN, CN=Birgit Gersbeck- Schierholz/serialNumber=3
Attribute wie Seriennummer und Gültigkeitsdauer		Serial Number: 3 (0x3) Signature Algorithm: sha1WithRSAEncryption Validity Not Before: May 26 15:42:55 2004 GMT Not After : May 26 15:42:55 2005 GMT
Beglaubigung (digitale Signatur) der CA, dass die Angaben stimmen		-----BEGIN CERTIFICATE----- …MBwGA1UEChMVVW5pdmVyc2l0YWV0I m5vdmVyMRAwDgYDVQQLFAdSUlpOX0NB… sDUNW/3L63Epiozxuah/9jzoLI+/Q32Dg== -----END CERTIFICATE-----

Zertifizierungs-Standard X.509v3

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 3 (0x3)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=DE, O=Universitaet Hannover, OU=RRZN_CA, CN=CA der Universitaet Hannover (UH-CA)/serialNumber=2
        Validity
            Not Before: May 26 15:42:55 2004 GMT
            Not After : May 26 15:42:55 2005 GMT
        Subject: C=DE, O=Universitaet Hannover, OU=RRZN, CN=Birgit Gersbeck-Schierholz/serialNumber=3
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:ab:77:e0:53:4a:4a:6b:42:8b:e0:4b:91:14:6f:
                    df:e7:28:4f:58:e5:43:b5:01:71:fa:24:2f:6c:4e:
                    95:c1:03:f2:65:70:79:5b:8b:cf:ff:56:fc:0c:ad:
                    8c:53:fc:b5:28:56:33:e5:59:5a:2d:a3:c6:11:01:
                    2a:1a:56:a5:f0:0a:b9:5e:28:db:8f:e2:eb:6b:c3:
                    72:d3:35:83:e9:99:04:e3:38:18:41:25:e0:fd:02:
                    a0:59:d0:3c:b7:7a:d3:c3:3d:0e:1b:10:a8:d8:ce:
                    16:c9:e4:8e:46:1c:70:73:a9:1f:c7:f5:45:51:a6:
                    c4:80:12:af:78:28:1e:69:d9:9b:4a:b0:84:95:48:
                    5d:f8:00:df:12:a9:4f:2c:7e:82:ba:c4:bc:61:55:
                    5c:c8:48:e8:43:e9:6d:e2:c3:76:e9:1a:64:58:37:
                    d0:e2:08:08:d8:e4:5b:88:3f:89:8d:18:a4:d2:ae:
                    04:88:83:92:a9:4c:5e:70:2e:3e:d4:c1:b8:a8:17:
                    11:00:7a:76:2e:66:44:3c:5d:d7:fc:2d:d7:e4:6d:
                    e6:20:9c:2f:c3:63:44:78:11:e0:12:66:27:4d:22:
                    2e:e9:12:7f:94:b0:3e:3a:d0:16:5a:35:a4:a4:e3:
                    2b:9f:d0:8d:39:04:62:2f:fd:20:4a:a3:d0:00:78:
                    c8:e7
                Exponent: 65537 (0x10001)
    Signature Algorithm: sha1WithRSAEncryption
        b6:38:e4:e0:d9:53:d5:b4:37:0a:9b:9b:e9:58:77:6e:6b:db:
        31:0c:32:6d:87:a4:42:66:b8:1f:bd:e2:68:b8:23:5b:38:07:
        a8:7f:a7:33:8d:97:a1:3a:e8:42:c0:49:48:e8:a2:6f:55:2f:
...
        93:39:7d:62:aa:34:d0:b8:a7:eb:ab:eb:16:88:a3:2a:74:4c:
        76:28:8c:be:0a:8f:50:68:c7:b4:f7:0c:a7:73:64:bf:29:88:
        b3:b4:ba:df:cb:97:0c:82:45:4b:b9:7d:9c:e0:38:a0:e7:81:
        30:17:c2:8a:64:05:ff:a1:43:8e:ca:fb:85:ed:ba:72:c0:d4:
        35:6f:f7:2f:ad:c4:a6:2a:33:c6:e6:a1:ff:d8:f3:a0:b2:3e:
        fd:0d:f6:0e
```

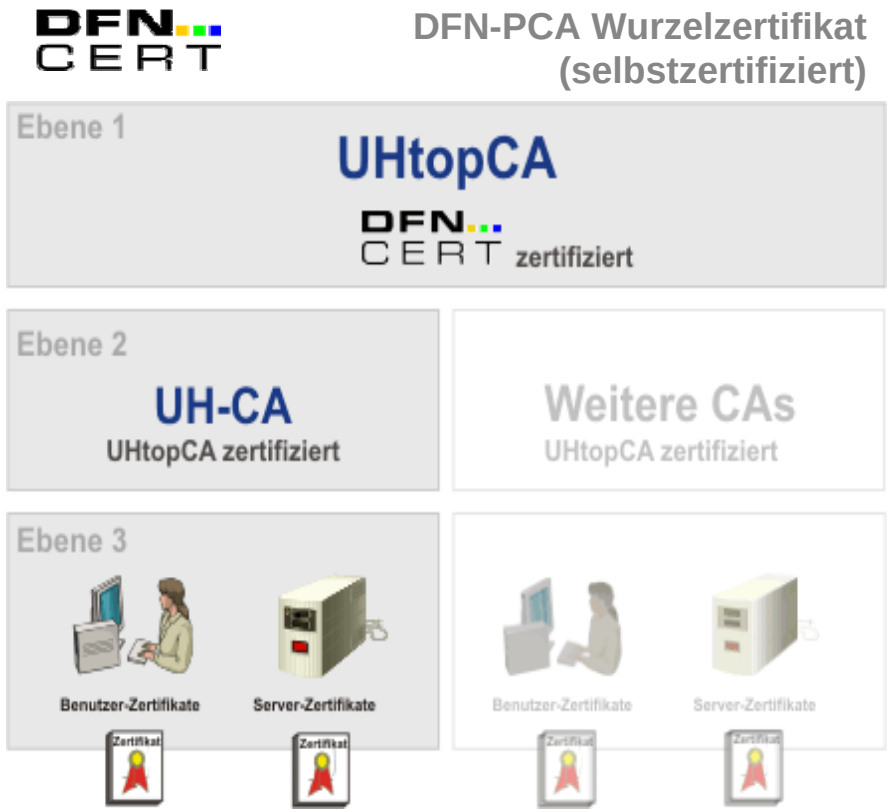
```
X509v3 extensions:
    X509v3 Basic Constraints:
        CA:FALSE
    Netscape Cert Type:
        SSL Client, S/MIME
    X509v3 Key Usage:
        Digital Signature, Non Repudiation, Key Encipherment
    Netscape Comment:
        User Certificate of Universitaet Hannover
    X509v3 Subject Key Identifier:
        32:EA:A9:64:1F:A7:99:E4:F4:64:92:A0:E2:55:F4:13:A7:C6:41:C4
    X509v3 Authority Key Identifier:
        keyid:3A:92:B8:B8:3A:29:47:08:3D:ED:53:F4:D3:F3:48:7A:60:05:CB:BC
        DirName:/C=DE/O=Universitaet Hannover/OU=RRZN_CA/CN=oberste CA der Universitaet Hannover
(UHtopCA)/emailAddress=uhtopca@ca.uni-hannover.de
        serial:02

    X509v3 Subject Alternative Name:
        email:gersbeck@rrzn.uni-hannover.de
    X509v3 Issuer Alternative Name:
        email:uh-ca@ca.uni-hannover.de
    Netscape CA Revocation Url:
        https://www.ca.uni-hannover.de/pub/crl/cacrl.crl
    Netscape Revocation Url:
        https://www.ca.uni-hannover.de/pub/crl/cacrl.crl
    X509v3 CRL Distribution Points:
        URI:https://www.ca.uni-hannover.de/pub/crl/cacrl.crl
```

```
-----BEGIN CERTIFICATE-----
MIIF0zCCBLugAwIBAgIBAzANBgkqhkiG9w0BAQUFADB6MQswCQYDVQQGEwJERTEe
MBwGA1UEChMVVW5pdmVyc2l0YWV0IEhhbm5vdmVyMRAwDgYDVQQLFAdSUlpOX0NB
MS0wKwYDVQQDEyRDQSBkZXIgVW5pdmVyc2l0YWV0IEhhbm5vdmVylChVSC1DQSkx
CjAIBgNVBAUTAT1wHhcNMDQwNTI2MTU0MjU1WhcNMDUwNTI2MTU0MjU1WjBtMQsw
CQYDVQQGEwJERTEeMBwGA1UEChMVVW5pdmVyc2l0YWV0IEhhbm5vdmVyMQ0wCwYD
VQQLEwRSUlpOMSMwIQYDVQQDExpCaXJnaXQgR2Vyc2JlY2stU2NoaWVyaG9sejEK
...
aS1oYW5ub3Zlci5kZS9wdWlvY3JsL2NhY3JsLmNybDA/BglghkgBhvhCAQMEMhYw
aHR0cHM6Ly93d3cuY2EudW5pLWhhbm5vdmVyLmRlL3B1Yi9jcmwvY2FjcmwuY3Js
MEEGA1UdHwQ6MDgwNqA0oDKGMGh0dHBzOi8vd3d3LmNhLnVuaS1oYW5ub3Zlci5k
ZS9wdWlvY3JsL2NhY3JsLmNybDANBgkqhkiG9w0BAQUFAAOCAQEAtjjk4NlT1bQ3
Cpub6Vh3bmvbMQwybYekQma4H73iaLgjWzgHqH+nM42XoTroQsBJSOiib1UvEZsk
2bNnjyIdEZapCxALM7gZGuNV860XWXPROorZ8WCYPSAc4T8PrdTJltvMFEzqljWj
2IwKT9VawErdAKpGH40XWRcm7STb8yBSVAW4rTwiasJiU1pOmgEfEz2GbHtB7AB8
DTvplYGkwfQykzl9Yqo00Lin66vrFoijKnRMdiiMvgqPUGjHtPcMp3Nkvym1s7S6
38uXDIJFS7I9nOA4oOeBMBfCimQF/6FDjsr7he26csDUNW/3L63Epiozxuah/9jz
oLI+/Q32Dg==
-----END CERTIFICATE-----
```

Zertifizierungs-Standard X.509v3

- **Optimierte Vertrauensstellung durch Eingliederung in eine Zertifizierungshierarchie**



Zertifizierungs-Standard X.509v3

- Dadurch, dass die CA wiederum von einer übergeordneten Zertifizierungsstelle beglaubigt wird, entsteht eine **Hierarchie des Vertrauens.**
  - Aufbau einer Zertifikatskette:
    - Die digitale Signatur der ausstellenden CA in einem **Zertifikat** ist mit dem geheimen Schlüssel des Ausstellers verschlüsselt worden.
    - Mit dem im **Zertifikat der CA** enthaltenen öffentlichen Schlüssel kann diese digitale Signatur entschlüsselt und damit verifiziert werden.

Zertifizierungs-Standard X.509v3

R|R|Z|N

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 3 (0x3)
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: C=DE, O=Universitaet Hannover, OU=RRZN_CA, CN=CA der Universitaet Hannover (UH-CA)/serialNumber=2
    Validity
      Not Before: May 26 15:42:55 2004 GMT
      Not After : May 26 15:42:55 2005 GMT
    Subject: C=DE, O=Universitaet Hannover, OU=RRZN, CN=Birgit Gersbeck-Schierholz/serialNumber=3
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (2048 bit)
        Modulus (2048 bit):
          00:ab:77:e0:53:4a:4a:6b:42:8b:e0:4b:91:14:6f:
          df:e7:28:4f:58:e5:43:b5:01:71:fa:24:2f:6c:4e:
          95:c1:03:f2:65:70:79:5b:8b:cf:ff:56:fc:0c:ad:
          8c:53:fc:b5:28:56:33:e5:59:5a:2d:a3:c6:11:01:
          2a:1a:56:a5:f0:0a:b9:5e:28:db:8f:e2:eb:6b:c3:
          72:d3:35:83:e9:99:04:e3:38:18:41:25:e0:fd:02:
          a0:59:d0:3c:b7:7a:d3:c3:3d:0e:1b:10:a8:d8:ce:
          16:c9:e4:8e:46:1c:70:73:a9:1f:c7:f5:45:51:a6:
          c4:80:12:af:78:28:1e:69:d9:9b:4a:b0:84:95:48:
          5d:f8:00:df:12:a9:4f:2c:7e:82:ba:c4:bc:61:55:
          5c:c8:48:e8:43:e9:6d:e2:c3:76:e9:1a:64:58:37:
          d0:e2:08:08:d8:e4:5b:88:3f:89:8d:18:a4:d2:ae:
          04:88:83:92:a9:4c:5e:70:2e:3e:d4:c1:b9:a8:17:
          11:00:7a:76:2e:66:44:3c:5d:d7:fc:2d:d7:e4:6d:
          e6:20:9c:2f:c3:63:44:78:11:e0:12:66:27:4d:22:
          2e:e9:12:7f:94:b0:3e:3a:d0:16:5a:35:a4:a4:e3:
          2b:9f:d0:8d:39:04:62:2f:fd:20:4a:a3:d0:00:78:
          c8:e7
        Exponent: 65537 (0x10001)

  Signature Algorithm: sha1WithRSAEncryption
       b6:38:e4:e0:d9:53:d5:b4:37:0a:9b:9b:e9:58:77:6e:6b:db:
       31:0c:32:6d:87:a4:42:66:b8:1f:bd:e2:68:b8:23:5b:38:07:
       a8:7f:a7:33:8d:97:a1:3a:e8:42:c0:49:48:e8:a2:6f:55:2f:
...
       93:39:7d:62:aa:34:d0:b8:a7:eb:ab:eb:16:88:a3:2a:74:4c:
       76:28:8c:be:0a:8f:50:68:c7:b4:f7:0c:a7:73:64:bf:29:88:
       b3:b4:ba:df:cb:97:0c:82:45:4b:b9:7d:9c:e0:38:a0:e7:81:
       30:17:c2:8a:64:05:ff:a1:43:8e:ca:fb:85:ed:ba:72:c0:d4:
       35:6f:f7:2f:ad:c4:a6:2a:33:c6:e6:a1:ff:d8:f3:a0:b2:3e:
       fd:0d:f6:0e
```

Digitale Signatur der ausstellenden CA, mit deren geheimen Schlüssel verschlüsselt

```
09v3 extensions:
    X509v3 Basic Constraints:
      CA:FALSE
    Netscape Cert Type:
      SSL Client, S/MIME
    X509v3 Key Usage:
      Digital Signature, Non Repudiation, Key Encipherment
    Netscape Comment:
      User Certificate of Universitaet Hannover
    X509v3 Subject Key Identifier:
      32:EA:A9:64:1F:A7:99:E4:F4:64:92:A0:E2:55:F4:13:A7:C6:41:C4
    X509v3 Authority Key Identifier:
      keyid:3A:92:B8:B8:3A:29:47:08:3D:ED:53:F4:D3:F3:48:7A:60:05:CB:BC
      DirName:/C=DE/O=Universitaet Hannover/OU=RRZN_CA/CN=oberste CA der Universitaet Hannover
(UHtopCA)/emailAddress=uhtopca@ca.uni-hannover.de
      serial:02

    X509v3 Subject Alternative Name:
      email:gersbeck@rrzn.uni-hannover.de
    X509v3 Issuer Alternative Name:
      email:uh-ca@ca.uni-hannover.de
    Netscape CA Revocation Url:
      https://www.ca.uni-hannover.de/pub/crl/cacrl.crl
    Netscape Revocation Url:
      https://www.ca.uni-hannover.de/pub/crl/cacrl.crl
    X509v3 CRL Distribution Points:
      URI:https://www.ca.uni-hannover.de/pub/crl/cacrl.crl
```

```
-----BEGIN CERTIFICATE-----
MIIF0zCCBLugAwIBAgIBAzANBgkqhkiG9w0BAQUFADB6MQswCQYDVQQGEwJERTEe
MBwGA1UEChMVVW5pdmVyc2l0YWV0IEhhbm5vdmVyMRAwDgYDVQQLFAdSUlpOX0NB
MS0wKwYDVQQDEyRDQSBkZXIgVW5pdmVyc2l0YWV0IEhhbm5vdmVyIChVSC1DQSkx
CjAIBgNVBAUTATIwHhcNMDQwNTI2MTU0MjU1WhcNMDUwNTI2MTU0MjU1WjBtMQsw
CQYDVQQGEwJERTEeMBwGA1UEChMVVW5pdmVyc2l0YWV0IEhhbm5vdmVyMQ0wCwYD
VQQLEwRSUlpOMSMwIQYDVQQDExpCaXJnaXQgR2Vyc2JlY2stU2NoaWVyaG9sejEK
...
aS1oYW5ub3Zlci5kZS9wdWlvY3JsL2NhY3JsLmNybDA/BglghkgBhvhCAQMEMhYw
aHR0cHM6Ly93d3cuY2EudW5pLWhhbm5vdmVyLmRlL3B1Yi9jcmwvY2Fjcmwu Y3Js
MEEGA1UdHwQ6MDgwNqA0oDKGMGh0dHBzOi8vd3d3LmNhLnVuaS1oYW5ub3Zlci5k
ZS9wdWlvY3JsL2NhY3JsLmNybDA NBgkqhkiG9w0BAQUFAA OCAQEAtjjk4NIT1bQ3
Cpub6Vh3bmvbMQwybYekQma4H73iaLgjWzgHqH+nM42XoTroQsBJ SOiib1UvEZsk
2bNnjyIdEZapCxALM7gZGuNV860XWXPROorZ8WCYP SA c4T8PrdTJ tvMFEzqljWj
2lwKT9VawErdA KpGH40XWRcm7STb8yBSVAW4rTwiasJiU1pOmgEfEz2GbHtB7ABB
DTvplYGkwfQykzl9Yqo00Lin66vrFoijKnRMdiiMvgqPUGjHtPcMp3Nkvym ls7S6
38uXDIJFS7I9nOA4oOeBMBfCimQF/6FDjsr7he26csSDUNW/3L63Epiozxuah/9jz
oLI+/Q32Dg==
-----END CERTIFICATE-----
```

- **Rechtliche Bedeutung der UH-CA Zertifikate**
  - sind keine qualifizierten Zertifikate im Sinne des deutschen Signaturgesetzes (SigG §2 Nr. 7)
  - Können rechtlich gesehen keine handschriftliche Unterschrift ersetzen
  - Dienen dazu die authentische und vertrauliche Kommunikation im Internet zu fördern

Konkrete Einsatzgebiete für Zertifikate (1)

R|R|Z|N

- **S/MIME Zertifikate**
  - Persönliches Zertifikat zum Unterschreiben (signieren) und Verschlüsseln von E-Mail

    Einschränkung: nicht jeder Browser/Mail-Client unterstützt X.509

- **Code Signing**
  - Gewährleistet Authentizität und Integrität von Programm-Code (z.B. Office-Macros)

Konkrete Einsatzgebiete für Zertifikate (2)

R|R|Z|N

- **SSL Server-Zertifikate**
  - Ermöglicht gesicherten Datenaustausch nach einer Server-Authentifizierung
  - Hybrides Verfahren zwischen asymmetrischer und symmetrischer Verschlüsselung
  - Gewährleistet damit Vertraulichkeit, Integrität, einseitige Authentifizierung

- **SSL Client-Zertifikate**
  - Ermöglicht gesicherten Datenaustausch nach Authentifizierung beider Kommunikationspartner
  - Hybrides Verfahren zwischen asymmetrischer und symmetrischer Verschlüsselung
  - Gewährleistet damit Vertraulichkeit, Integrität, beidseitige Authentifizierung

„Klippen“

- Beispiel 1:
  - **Ich erhalte eine signierte E-Mail -> mein Mail-Client stuft die Signatur als ungültig ein und meldet eine wenig Vertrauen erweckende Warnung**
- Beispiel 2:
  - **Ich wähle eine Verbindung zu einem Webserver, der sich mit einem Zertifikat ausweist –> mein Browser schlägt Alarm und warnt mich vor möglichem Betrug**
- Ursache in beiden Fällen:
  - **die Zertifikate der Zertifizierungs-Hierarchie DFN-PCA – UHtopCA - UH-CA sind noch nicht in Standard-Browsern und Mail-Klienten enthalten.**
- Etwas lästig aber unabdingbar: die CA-Zertifikate müssen nachinstalliert werden.

Verifizieren der Echtheit des Zertifikates:

E-Mail Kommunikation

- Um dem Empfänger der E-Mail das Verifizieren der Signatur so einfach wie möglich zu machen, können die Links für den Import der CA-Zertifikate mitgeschickt werden.

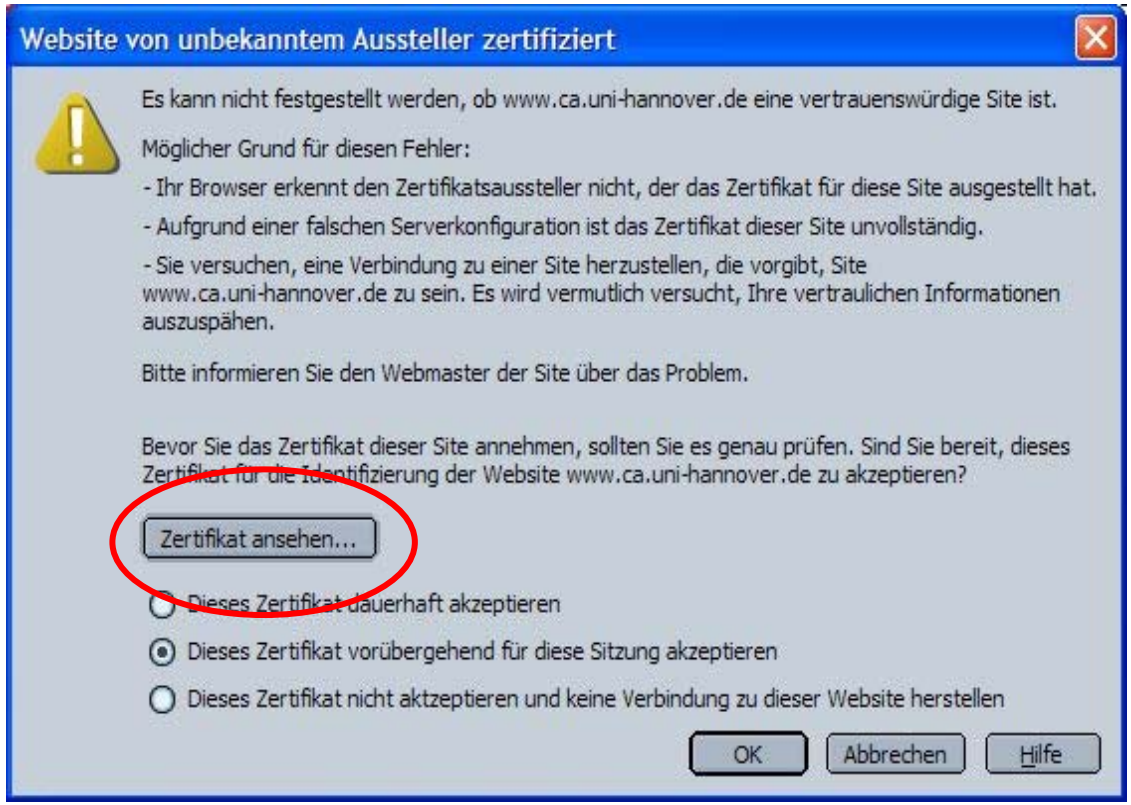
- Beispiel:

```
Diese Nachricht ist digital unterschrieben. Um die Gueltigkeit der Signatur zu
bestaetigen, werden unten angegebene Basiszertifikate benoetigt, die Sie jeweils
durch einen Klick in Ihr System integrieren koennen:

Das aktuelle Wurzelzertifikat des Deutschen Forschungsnetzes (DFN)
http://www.dfn-pca.de/certification/x509/g1/data/html/cacert/root-ca-cert.crt
Die Zertifikate der Zertifizierungshierarchie der Universitaet Hannover
UHtopCA:    https://www.ca.uni-hannover.de/pub/cacert/top-cacert.crt
UH-CA:        https://www.ca.uni-hannover.de/pub/cacert/cacert.crt
```

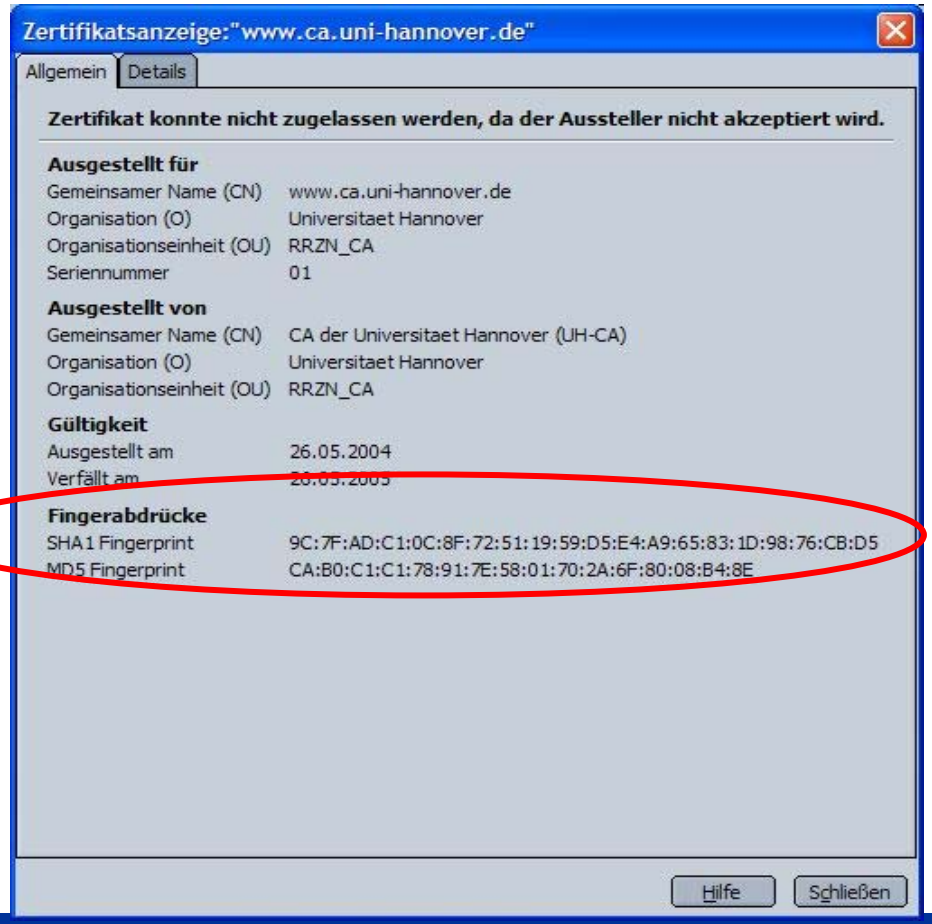
Verifizieren der Echtheit des Zertifikates:

Kommunikation mit Servern



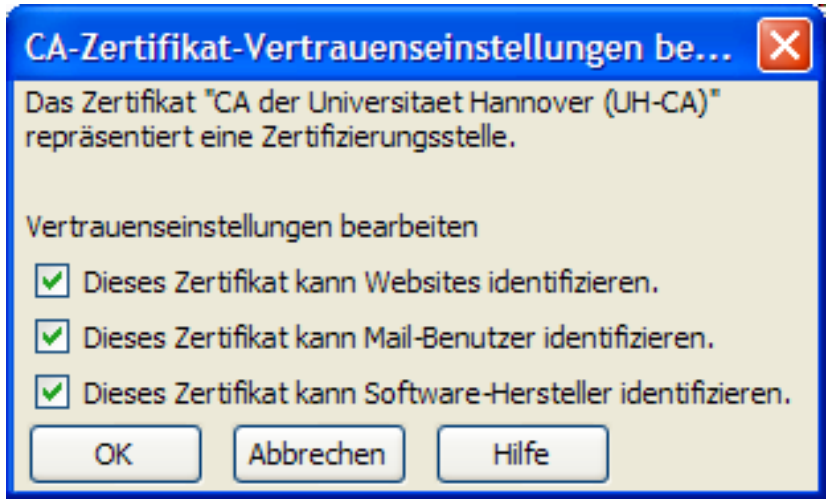
Verifizieren der Gültigkeit des Zertifikates:

Kommunikation mit Servern



Verifizieren der Gültigkeit des Zertifikates:

Kommunikation mit Servern



R|R|Z|N

Interesse an einem Zertifikat der UH-CA?

https://www.ca.uni-hannover.de/home.htm

- **Schneller Einstieg für E-Mail Zertifikate (S/MIME):**
  - Voraussetzung ist ein S/MIME -fähiges Mailprogramm:

    Mozilla, Thunderbird, Netscape, MS Outlook und Outlook Express, Eudora mit entsprechendem Plugin

https://www.ca.uni-hannover.de/Leitfaden.htm

Anhang: Relevante Daten eines Zertifikates (1)

R | R | Z | N

Variable	Wert
Zertifikatsversion:	3
Seriennummer:	3
Name:	Birgit Gersbeck-Schierholz
E-Mail:	gersbeck@rrzn.uni-hannover.de
Eindeutiger Name:	serialNumber=3 CN=Birgit Gersbeck-Schierholz OU=RRZN O=Universitaet Hannover C=DE
Rolle:	Benutzer
Fingerprint:	79:A6:4C:88:81:5D:C4:34:E7:6F:74:16:09:C4:7D:B6
Ausgestellt durch:	serialNumber=2 CN=CA der Universitaet Hannover (UH-CA) OU=RRZN_CA O=Universitaet Hannover C=DE
Gültig ab:	May 26 15:42:55 2004 GMT
Gültig bis:	May 26 15:42:55 2005 GMT
Aktueller Status:	Gültig

X.509 Version

Eindeutige, von der CA vergebene Serien-Nummer

Name des Zertifikats-Eigentümers

E-Mail des Zertifikats-Eigentümers

Eindeutiger Name, Distinghuished Name (DN) des Zertifikats-Eigentümers

Eindeutige Kennung für einen Schlüssel, die über eine Hash-Funktion (MD5) aus bestimmten Teilen der Schlüsseldaten errechnet wird.

Eindeutiger Name (DN) des Zertifikats-Ausstellers

Gültigkeitszeitraum des Zertifikats

Anhang: Relevante Daten eines Zertifikates (2)

R | R | Z | N

Erweiterungen:		
Netscape CA Revocation Url:	https://www.ca.uni-hannover.de/pub/crl/cacrl.crl	Sperrliste der CA
Netscape Cert Type:	SSL Client, S/MIME	Zertifikatstyp: SSL Client (https, ftps, imaps, etc., sichere E-Mail per S/MIME
Netscape Comment:	User Certificate of Universitaet Hannover	Zertifikatstyp: Benutzerzertifikat der UH
Netscape Revocation Url:	https://www.ca.uni-hannover.de/pub/crl/cacrl.crl	Sperrliste der CA
X509v3 Authority Key Identifier:	keyid:3A:92:B8:B8:3A:29:47:08:3D:ED:53:F4:D3:F3:48:7A:60:05:CB:BC DirName:/C=DE/O=Universitaet Hannover/OU=RRZN_CA/CN=oberste CA der Universitaet Hannover (UHtopCA)/emailAddress=uhtopca@ca.uni-hannover.de serial:02	Schlüssel-ID (Hashwert des öffentl. Schlüssels der UHtopCA)und DN des Ausstellers
X509v3 Basic Constraints:	CA:FALSE	Basisbeschränkungen: der Zertifikatseigentümer ist keine CA

Anhang: Relevante Daten eines Zertifikates (3)

R|R|Z|N

X509v3 CRL Distribution Points:	URI:https://www.ca.uni-hannover.de/pub/crl/cacrl.crl	Ort, an dem die UH-CA monatl. Eine neue Sperrliste zur Verfügung stellt
X509v3 Issuer Alternative Name:	email:uh-ca@ca.uni-hannover.de	E-Mail Adresse des Ausstellers als alternativer Name
X509v3 Key Usage:	Digital Signature, Non Repudiation, Key Encipherment	Verwendungszweck: digitale Signatur, Unabstreitbarkeit, Verschlüsselung
X509v3 Subject Alternative Name:	email:gersbeck@rrzn.uni-hannover.de	E-Mail Adresse des Zertifikatseigentümers als alternativer Name
X509v3 Subject Key Identifier:	32:EA:A9:64:1F:A7:99:E4:F4:64:92:A0:E2:55:F4:13:A7:C6:41:C4	Schlüssel-ID: Hashwert des öffentlichen Schlüssels des Zertifikatseigentümers

Auf eine sicherere Zukunft!