Stammtisch 04.12.2008

Zertifikate

Ein Zertifikat ist eine Zusicherung / Bestätigung / Beglaubigung
eines Sachverhalts durch eine Institution
in einem definierten formalen Rahmen

Zertifikate ?

Digitale X.509 Zertifikate

- Was sind digitale X.509 Zertifikate, was bestätigen sie und wofür werden sie verwendet ?
  - Verschlüsselung und Signatur (am Beispiel von Email)
- Einsatz von Zertifikaten an der TU-Berlin
- Verschiedenes (F & A)

Datenkommunikation über unsichere Netze

Integrität

Es muss gewährleistet sein, dass Veränderungen an den übermittelten Daten erkannt werden können.

Authentizität

Es muss sicher nachprüfbar sein, aus welcher Quelle die Daten stammen.

Vertraulichkeit

Es muss sichergestellt sein, dass Unbefugte keine Kenntnis (vom Inhalt) der Daten erlangen.

Sicherung der Vertraulichkeit durch Verschlüsselung

Symmetrische Verfahren

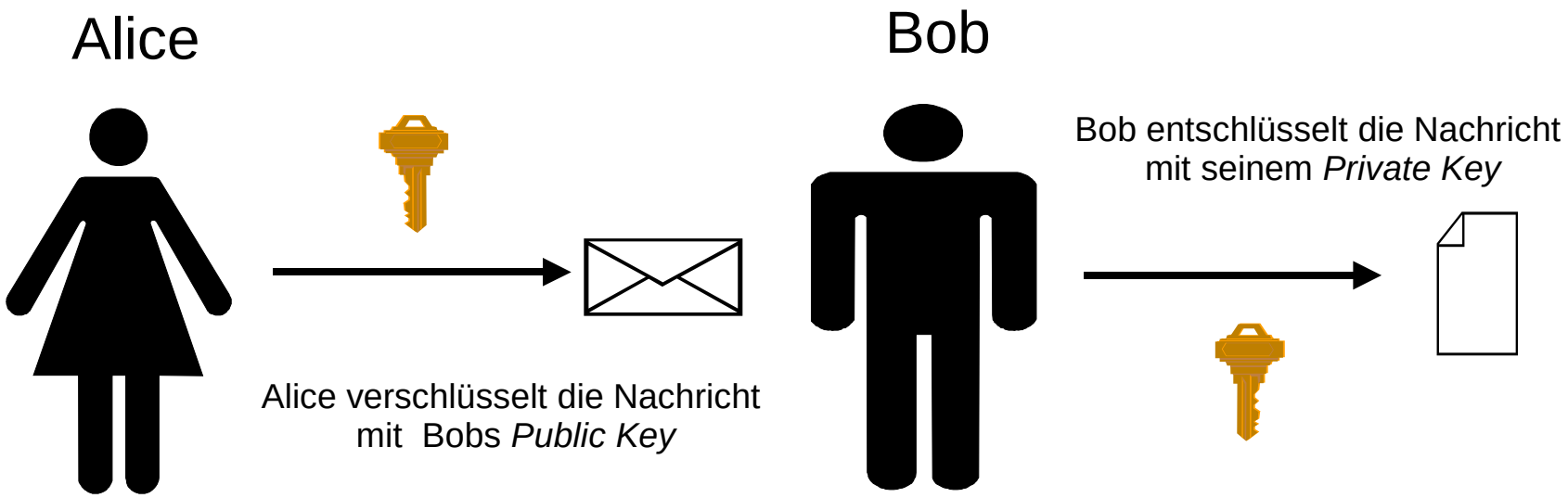
Zum Verschlüsseln und Entschlüsseln wird der gleiche Schlüssel verwendet. Dies erfordert, dass die Teilnehmer den Schlüssel zuvor über einen sicheren Kanal ausgetauscht haben.

Asymmetrische Verfahren / Public Key Kryptographie

Es wird ein Schlüsselpaar verwendet.
Was mit einem der beiden Schlüssel verschlüsselt wurde, kann nur mit dem anderen Schlüssel entschlüsselt werden und umgekehrt.
Einer der Schlüssel, der ***Public Key***, wird öffentlich, z.B. über einen Verzeichnisdienst zugänglich gemacht, der andere, der ***Private Key***, wird vom Besitzer geheim gehalten.

Der am häufigsten verwendete Public Key Verschlüsselungsalgorithmus ist ***RSA,*** benannt nach seinen „Erfindern“: Rivest, Shamir, Adelman.

Übermittlung einer verschlüsselten Nachricht



Nur Bob kann die verschlüsselte Nachricht entschlüsseln,
da nur er im Besitz des benötigten Schlüssels ist.

Zertifikate 1

Alices Problem:

Wie kann Alice sicher sein, dass der (öffentliche) Schlüssel mit dem sie die Nachricht verschlüsselt hat, wirklich der von Bob ist?

Lösung durch Einsatz eines Zertifikats:

Eine Institution, **der Alice vertraut**, sichert ihr - durch Ausstellung eines **digitalen Zertifikats nach einem genau festgelegten Verfahren** - zu, dass der in Frage stehende **öffentliche Schlüssel der von Bob** ist.

Eine solche Institution wird üblicherweise als **Certification Authority (CA)** bezeichnet, die gesamte Infrastruktur als **Public Key Infrastructure (PKI)**.

Die PKI der TU-Berlin ist in die PKI des **DFN-Vereins** integriert.

Zertifikate 2

Voraussetzung zur Teilnahme an der TUB-PKI ist ein provisioniertes tubIT Konto und der Besitz der Campuskarte.

Die Richtlinien, nach denen das Zertifizierungsverfahren abläuft, werden in der **Certifcate Policy** niedergelegt.

Für die TUB gilt die Global Policy der DFN-PKI, siehe:
https://pki.pca.dfn.de/tu-berlin-ca/pub/ → Policies.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 587 (0x24b)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=DE, O=Technische Universitaet Berlin,
OU=Trustcenter TUB, CN=TUB-Email-CA/emailAddress=ca@TU-
Berlin.DE
        Validity
            Not Before: Jun  7 14:49:05 2004 GMT
            Not After : Jun  6 14:49:05 2008 GMT
Subject: C=DE, O=Technische Universitaet Berlin, CN=Gerd
Schering/emailAddress=Schering@zrz.TU-Berlin.DE
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
              Modulus (1024 bit):

00:b5:8d:cc:66:56:a8:e5:73:96:de:c5:5d:4a:40:
99:ea:39:bb:bc:39:2a:18:4f:3d:bb:b1:28:e1:53:
79:cd:b4:b8:13:b6:0a:0b:c8:fa:2b:11:dc:e5:01:
43:56:28:79:29:a6:60:8e:21:10:b2:f3:15:48:f1:
a8:cf:0a:4c:e6:67:e0:e3:bb:6c:a7:a2:75:e2:dd:
38:ad:4c:84:78:6f:3c:3f:35:2e:e0:0b:26:5e:e1:
8b:06:fd:07:7b:a1:cf:f9:7d:7c:b7:8b:db:b7:d1:
03:d8:4f:81:29:cc:93:4b:e0:41:e4:9f:72:dd:5c:
86:d9:f1:5b:a2:91:b0:d6:19

Exponent: 65537 (0x10001)
   X509v3 extensions:
      X509v3 Subject Key Identifier:
        01:79:01:A5:D7:F8:1C:D8:FA:56:86:03:1C:
        1C:0C:11:81:95:6D:9B
      X509v3 Authority Key Identifier:
        keyid:E3:32:52:30:52:01:AC:DB:C6:F4:76:58:09:
        D7:89:D4:12:AA:EA:DA
        DirName:/C=DE/O=Technische Universitaet
        Berlin/OU=Trustcenter TUB/CN=TUB-Email-
        CA/emailAddress=ca@TU-Berlin.DE
        serial:00
      X509v3 Key Usage:
          Digital Signature, Key Encipherment, Key Agreement
      Netscape Comment:
          The Email Certification Authority of TUB
      Netscape Cert Type:
          SSL Client, S/MIME
      X509v3 Certificate Policies:
          Policy: 1.3.6.1.4.1.10238.300.5.1
          CPS: http://ca.TU-Berlin.DE/policies/TUB-Email-CA-
                    policy.html

Signature Algorithm: sha1WithRSAEncryption
    77:a2:0f:8a:b0:ce:a1:34:69:29:ec:2e:9b:f8:b3:dc:c7:10:
    51:c4:d5:6d:69:54:ed:56:b4:db:c2:ad:85:23:dc:f2:8f:9a:
    e7:4e:d9:25:e4:62:9a:8e:6a:ce:78:81:f0:ae:a6:47:56:9a:
    14:1c:13:ba:78:5f:ea:ad:a6:a9:9f:e5:3a:a2:37:6a:37:e5:
    3d:6e:05:09:2e:a2:30:15:6a:fc:8a:24:1e:da:f2:4d:04:8f:
    5c:e3:49:f9:37:86:f2:8f:c9:e0:e6:72:2d:1b:f4:bc:de:64:
    c8:18:82:4f:41:8e:59:d7:1b:c4:4d:2b:29:12:f3:9a:6c:de:
    80:33:d3:40:0b:1d:48:69:0a:03:5b:66:65:b0:de:f2:66:81:
    9e:a5:a1:6f:2a:97:e4:e0:d4:a7:c3:ac:23:9e:16:47:7b:27:
    ed:83:5e:05:0f:c3:ae:66:9d:d5:e6:70:ff:9a:f7:16:b0:8a:
    df:31:d6:e0:0c:2b:53:0b:ea:46:e7:b2:8b:76:89:4d:1f:e3:
    43:f4:11:42:2a:8b:2f:e9:b7:8b:54:a2:d3:e7:49:e1:c0:dd:
    1b:cc:8a:c0:17:84:2a:25:84:e3:76:60:0a:26:49:ab:36:42:
    57:72:68:d2:61:37:2f:67:8f:21:d1:be:a3:28:c0:fa:3b:63:
    ce:1e:00:40
```

Einige Zertifikattypen und ihre Verwendung

Zertifikattyp	***Verwendung***
Serverauthentifizierung TLS / SSL	Überprüfung der Identität eines Serversfür Computer, die eine Verbindung mit ihm herstellen.
Clientauthentifzierung TLS /SSL	Überprüfung der Identität eines Computers für einen Server, mit dem der Computer eine Verbindung herstellt.
Authentisierung	Nachweis der Identität eines Nutzers für ein IT System
Sichere Email	Verschlüsseln und digitales Signieren von Email Nachrichten.

Beachte: die unterschiedliche Typisierung kommt durch den Verwendungszweck zustande.
Das Zertifikat bescheinigt stets den gleichen Sachverhalt: die Zugehörigkeit eines bestimmten öffentlichen Schlüssels zu einem bestimmten Subjekt, z.B. einer Person oder einem Rechner.

Einsatz von X.509 Zertifikaten an der TU-Berlin

- An der TUB kommen ausschließlich Zertifikate zum Einsatz, die dem X.509 Standard genügen. Dies ist ein ITU-T-Standard für eine Public-Key-Infrastruktur und derzeit der wichtigste Standard für digitale Zertifikate. Aktuell ist Version 3 (X.509v3).
- Personenbezogene Zertifikate zur Authentisierung, Verschlüsselung und für sichere Email mittels der Campuskarte. Jedes TU-Mitglied erhält sie im Rahmen der Provisionierung, siehe:
  `http://www.tubit.tu-berlin.de/menue/dienste/konto_karte/`
- TLS/SSL Zertifikate für Server- und Clientauthentisierung. Diese werden auf Antrag erstellt, siehe:
  `http://www.tubit.tu-berlin.de/trustcenter/home/`

Zertifikate und Schlüssel der Campuskarte

Auf der Campuskarte befinden sich zwei (Studierende) oder drei (Mitarbeiter) Zertifikate und die zugehörigen privaten Schlüssel für die folgenden Zwecke:

I. Authentisierung, z.B. an IT Systemen
II. Verschlüsselung, z.B. von Email Mitteilungen
III. Signatur, z.B. von Email Mitteilungen

Für Studierende wird nur ein Schlüssel mit zugehörigem Zertifikat für Verschlüsselung und Signatur ausgegeben.

Nutzung der Zertifikate der Campuskarte

Um die auf Campuskarte befindlichen Schlüssel und Zertifikate z.B. zum Signieren oder Verschlüsseln von Email nutzen zu können, muss:

- die entsprechende Kartensoftware auf dem Rechner installiert werden, sowie
- das verwendete Emailprogramm für die Nutzung konfiguriert werden.

Beides ist unter

`http://www.tubit.tu-berlin.de/menue/dienste/konto_karte/campuskarte/installation/`

ausführlich beschrieben.

Verschiedenes (Fragen und Antworten)

- Was sind Zertifikate und wie funktionieren sie?
- Welche Zertifikate gibt es an der TUB; braucht man verschieden Zertifikate oder reichen die der Campuskarte?
- Wie werden Zertifikate benutzt (Beispiel Email Verschlüsselung)?
- Woher bekommt man den öffentlichen Schlüssel einer Person?
- Wie kann man unter Windows Zertifikate löschen?
- Wie gelangt man an die Subject Line eines X.509 Zertifikats?
- Was sollte man sonst noch wissen?
- Wo findet man die Folien zu diesem Stammtisch?

  `http://www.tubit.tu-berlin.de/tubit/menu/termine_veranstaltungen/stammtisch/`