

**Zertifikat der TU Berlin** (Die TU Berlin betreibt ein eigenes Trustcenter)

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 0 (0x0)
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: C=DE, ST=Berlin, L=Berlin, O=Technische Universitaet Berlin,
      OU=Trustcenter, CN=TUB-CA/Email=ca@TU-Berlin.DE
    Validity
      Not Before: Dec 1 14:24:03 2002 GMT
      Not After : Nov 28 14:24:03 2012 GMT
    Subject: C=DE, ST=Berlin, L=Berlin, O=Technische Universitaet Berlin,
      OU=Trustcenter, CN=TUB-CA/Email=ca@TU-Berlin.DE
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (2048 bit)
        Modulus (2048 bit):
          a3:1a:b0:9f:58:e3:da:04:19:e2:62:e5:1c:1e:36:
          4d:d2:9f:ea:72:21:ce:16:93:45:49:1f:89:e3:e9:
          ff:0c:21:85:7e:04:8b:46:98:fe:a0:bc:44:84:09:
          cb:f5:81:66:e5:66:6a:66:91:25:35:8c:51:44:6b:
          3f:d4:67:2a:8a:41:e2:38:3a:00:7e:b8:72:9c:43:
          28:4e:62:8b:ea:d0:c1:43:22:7b:e1:41:f0:a9:8b:
          25:74:8d:d4:2a:8f:9d:1d:52:51:23:a0:9c:b4:92:
          b8:06:75:32:b8:f6:d2:2d:25:27:fe:d2:89:16:21:
          0f:0f:da:d5:41:e1:c6:38:df:13:d9:40:2f:02:fb:
          07:76:d7:87:51:01:de:aa:69:0d:5e:70:44:95:e2:
          bc:8b:32:1d:c4:b2:6b:51:91:ab:59:f5:bb:b9:1d:
          e8:33:37:dc:6f:46:95:4f:8b:78:32:e9:1d:6e:ab:
          8f:b0:c1:65:8b:a9:e8:3f:38:a5:11:15:87:39:ba:
          02:28:c3:71:69:74:57:d3:69:a0:37:78:a1:a9:18:
          de:40:e5:4a:1b:c3:f1:f7:8d:e9:60:5e:93:94:1a:
          f9:0e:d2:ab:f7:eb:59:bd:e8:83:e6:d4:ef:ed:93:
          db:7f:80:ef:93:2e:50:30:e2:a7:55:fb:d4:f1:ae
        Exponent: 65537 (0x10001)

    X509v3 extensions:
      X509v3 Subject Key Identifier:
        38:ED:DF:6E:E4:48:A7:60:65:18:77:F6:03:BA:3F:F7:EE:6A:73:B1
      X509v3 Authority Key Identifier:
        keyid:38:ED:DF:6E:E4:48:A7:60:65:18:77:F6:03:BA:3F:F7:EE:6A:73:B1

      X509v3 Basic Constraints: critical
        CA:TRUE
      X509v3 Key Usage:
        Certificate Sign, CRL Sign
      X509v3 CRL Distribution Points:
        URI:http://ca.tu-berlin.de/crls/TUB-CA.crl

      Netscape Comment:
        This certificate was issued by the Top Level CA of TUB
      Netscape Cert Type:
        SSL CA, S/MIME CA, Object Signing CA
      X509v3 Certificate Policies:
        Policy: 1.3.6.1.4.1.10238.300.1.1
        CPS: http://ca.TU-Berlin.DE/policies/TUB-CA-policy.html

    Signature: sha1WithRSAEncryption
      1f:b5:d6:b4:22:8f:de:d8:f9:06:37:46:16:a7:1f:6c:4c:70:
      7c:f0:bd:cd:2d:28:8e:4e:90:89:5a:25:1d:36:7b:dc:d0:ff:
      66:2b:b3:41:be:c5:ce:cf:aa:06:95:3a:6e:80:82:cf:91:8b:
      b3:31:e8:b2:9f:df:3f:ec:aa:2f:77:8e:fd:8c:0b:95:06:09:
      39:76:d9:60:93:ca:24:a2:8f:58:68:cb:71:6d:02:5d:6c:42:
      9a:50:8c:b1:46:81:6f:06:6b:ed:32:6b:9f:b5:42:62:8b:78:
      ab:ea:1a:69:0b:cc:23:ad:a2:3d:78:70:6e:8c:03:49:05:14:
      03:c7:52:a9:1b:84:38:a4:e1:72:1a:db:be:3e:bc:00:a3:f9:
      54:db:e4:16:4e:59:84:a1:76:8d:59:97:8e:c1:df:2c:a6:c7:
      a1:c5:f1:fb:3b:5d:59:b3:13:49:e5:e5:d3:b3:fe:76:f7:63:
      19:62:5d:d2:5f:6d:08:a3:a2:a9:2d:6e:c5:a2:c3:fa:77:42:
      43:51:90:de:65:98:48:53:2f:f7:c3:bf:91:6f:9a:2e:ec:da:
      49:f1:36:44:86:4d:d8:cf:1a:c3:09:7a:76:d3:be:6f:79:15:
      c6:79:c2:6d:76:b6:bf:c4:ff:75:b9:5e:d8:83:77:f7:35:5a:
      a3:18:bc:98
```

Ein **Man-In-The-Middle-Angriff** ist eine Angriffsform, bei welcher der Angreifer im Netzwerk lauert und sich mit seinem Rechner – ohne dass dies die Beteiligten Kommunikationspartner merken – zwischen zwei oder mehrere Kommunikationspartner schiebt.

Gelingt im dies, so kann er die übermittelten Daten mit lesen oder verändern, ohne dass dies die Kommunikationspartner bemerken.

Allerdings führt dieser Angriff nur dann zum Ziel, wenn der Angreifer die Routingtabellen der für Absender und Empfänger zuständigen Router kurzfristig verändern kann, oder – in lokalen Netzwerken – Zugriff auf die ARP-Tabellen der Opfersysteme hat. Beides ist auf normal eingerichteten und administrierten Systemen nicht möglich.

Protokollen wie SSL, die zertifizierte digitale Signaturen verwenden, sind gegen Man-In-The-Middle-Angriffe sicher. Die selbe Sicherheit lässt sich auch erreichen, wenn man statt mit öffentlichen Zertifikaten mit zuverlässigen „Fingerprints“ arbeiten kann.

---

### Berechnung des „pre master secret“ und des „master secret“ unter SSL.

#### Pre master secret (48 Bytes lang)

- 2 Bytes Protokollspezifischer Header
- 46 Bytes lange Zufallszahl

#### Master secret

MasterSecret =

MD5 ( **pre master secret** + SHA('A' + **pre master secret** + ClientHello.random + ServerHello.random) )  
+ MD5 ( **pre master secret** + SHA('BB' + **pre master secret** + ClientHello.random + ServerHello.random) )  
+ MD5 ( **pre master secret** + SHA('CCC' + **pre master secret** + ClientHello.random + ServerHello.random) )

#### Quellen zu SSI (TSL)

- Bundesamt für Sicherheit in der Informationstechnik <http://www.bsi.de/>
- FB WiWi, SSL-Verschlüsselung von WWW-Seiten, <http://www.wiwi.uni-marburg.de/>
- Regulierungsbehörde für Telekommunikation und Post, <http://www.nrca-ds.de/>
- Thomas Lehner, Seminararbeit SSL, <http://www.ssw.uni-linz.ac.at/Teaching/Lectures/Sem/2000/Lehner/>
- Verisign, <http://www.verisign.com> (weltweit der bedeutendste Herausgeber von Zertifikaten)
- Zertifizierungsstelle des Sparkassenverbandes (Partner v. Verisign) <http://www.s-trust.de/>
- Zertifizierungsstelle (Telekom) Cybertrust-Gruppe <http://www.trustcenter.de>
- RFC 2246 - TLS