Verschlüsselung

Bernd Blümel

2001

Gliederung

1. Symetrische Verschlüsselung
2. Asymetrische Verschlüsselung
3. Hybride Verfahren
4. SSL
5. pgp

Verschlüsselung

1111011111000011100001110000 11 ← Nachricht

1100110 ← Schlüssel

1111011111000011100001110000 11
1001101100110110011011001101 10 ← Verschlüsselung
0110110011110101111010111101 01

0110110011110101111010111101 01 ← übertragene Nachricht

0110110011110101111010111101 01
1001101100110110011011001101 10 ← Entschlüsseln
1111011111000011100001110000 11

← Nachricht

Symetrische Verschlüsselung

- Secret Key Encryption
- Kommunikationspartner verwenden einen gemeinsamen Schlüssel.
- Schlüssel muß geheim bleiben.
- Kennen Dritte den Schlüssel, können sie die Nachrichten entschlüsseln.
- Symetrische Verfahren sind effizient und schnell.
- Symetrische Verfahren sind bei ausreichender Schlüssellänge (mindestens 128 Bit) nicht zu "knacken".

Asymetrische Verschlüsselung

- Public Key Encryption
- Zwei Schlüssel:
  - Öffentlicher Schlüssel (Public Key)
  - Privater Schlüssel (Private Key)
- Der Public Key kann über email, homepage oder Zertifizierungsstellen öffentlich gemacht werden.

Asymetrische Verschlüsselung

Digitale Signatur

- Sicherstellen, von wem die Nachricht kommt.
- Rechtsverbindliche Unterschriften

Nachteile

- **Bei symetrischen Verfahren muß der Schlüssel ausgetauscht werden.**
- **Ist der symetrische Schlüssel ausgespäht, kann jede Nachricht abgehört werden.**
- **Asymetrische Verfahren sind langsam und rechenintensiv.**
- **Die Schlüssellänge beträgt mindestens 1024 Bit, richtig sicher ist man bei 2048 Bit.**

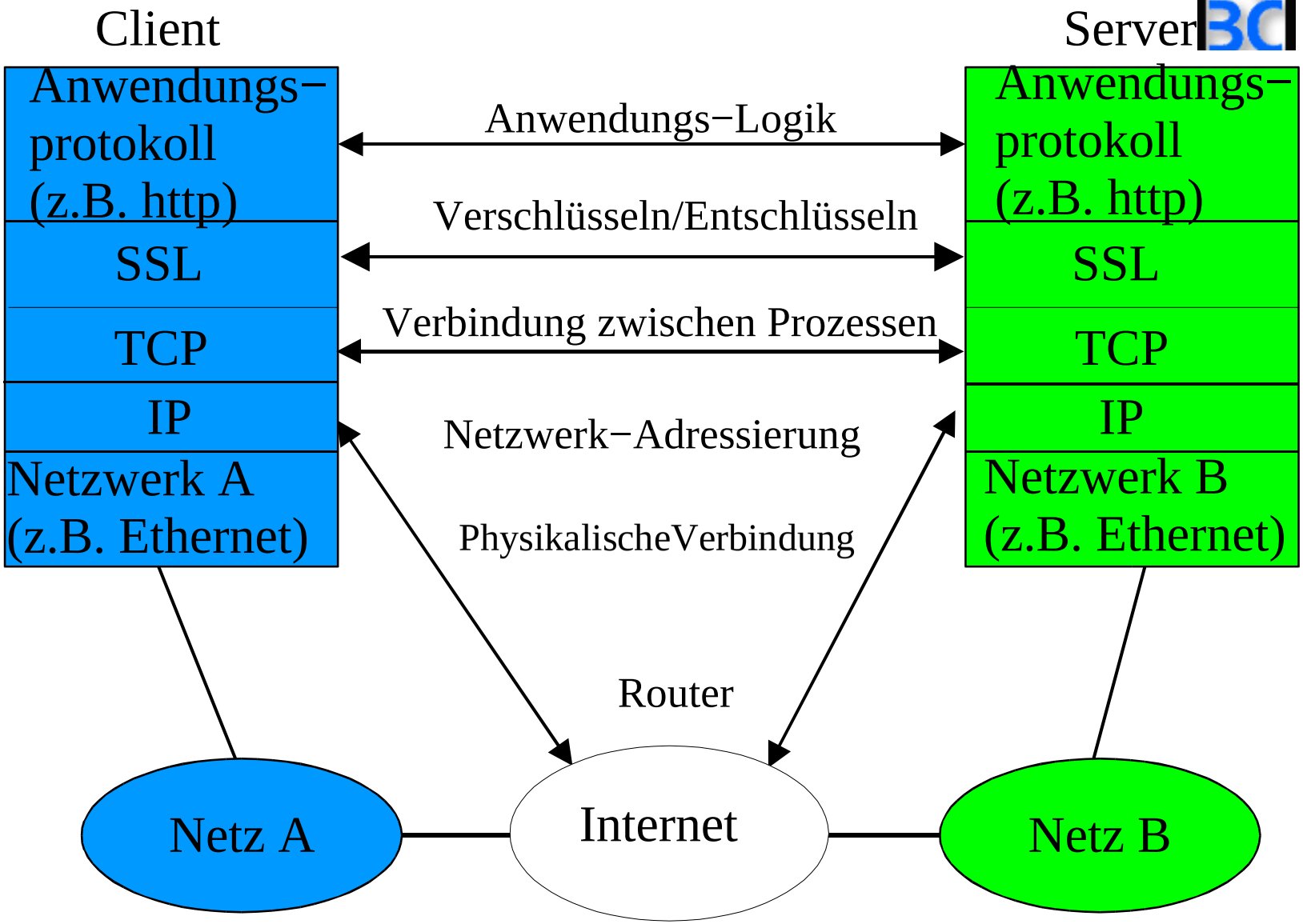
Hybride Verfahren

- **Über ein asymetrisches Verfahren wird ein symetrischer Schlüssel ausgetauscht.**
- **Dieser Schlüssel gilt nur für diese eine Sitzung (session key).**
- **Während der Sitzung werden die Nachrichten mit dem ausgehandelten symetrischen Schlüssel verschlüsselt.**
- **Nachteile beider Verfahren sind beseitigt.**

Verschlüsselung im Internet

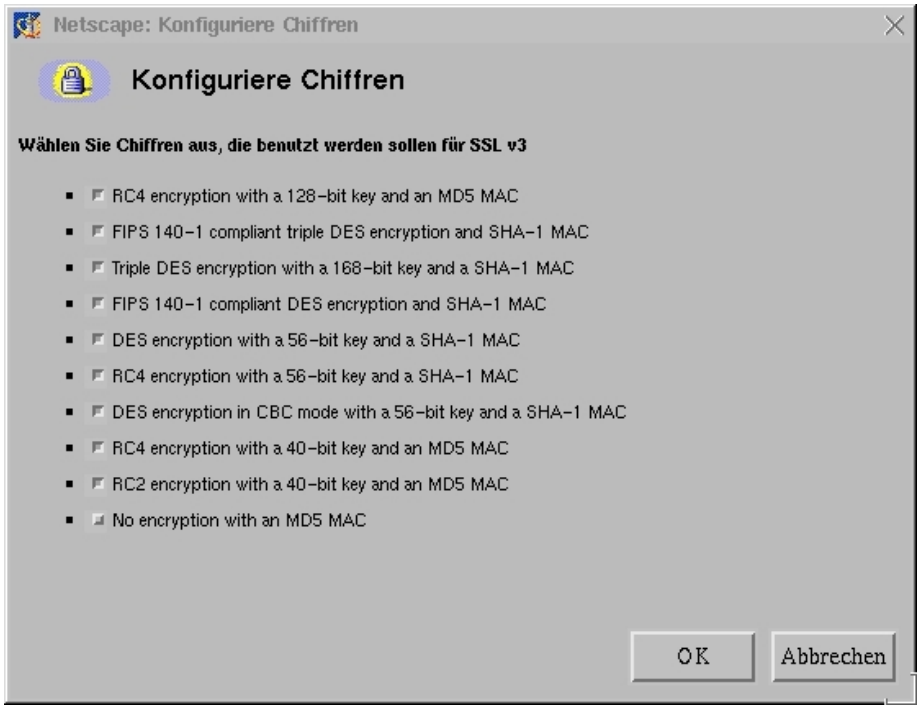
- **Die Anwendung verschlüsselt (Beispiel: email mit pgp).**
- **Eine Protokollschicht verschlüsselt (Beispiel Secure Socket Layer SSL).**

SSL


Client
Server
Anwendungs−protokoll (z.B. http)
SSL
TCP
IP
Netzwerk A (z.B. Ethernet)
Anwendungs−Logik
Verschlüsseln/Entschlüsseln
Verbindung zwischen Prozessen
Netzwerk−Adressierung
PhysikalischeVerbindung
Anwendungs−protokoll (z.B. http)
SSL
TCP
IP
Netzwerk B (z.B. Ethernet)
Router
Netz A
Internet
Netz B

SSL

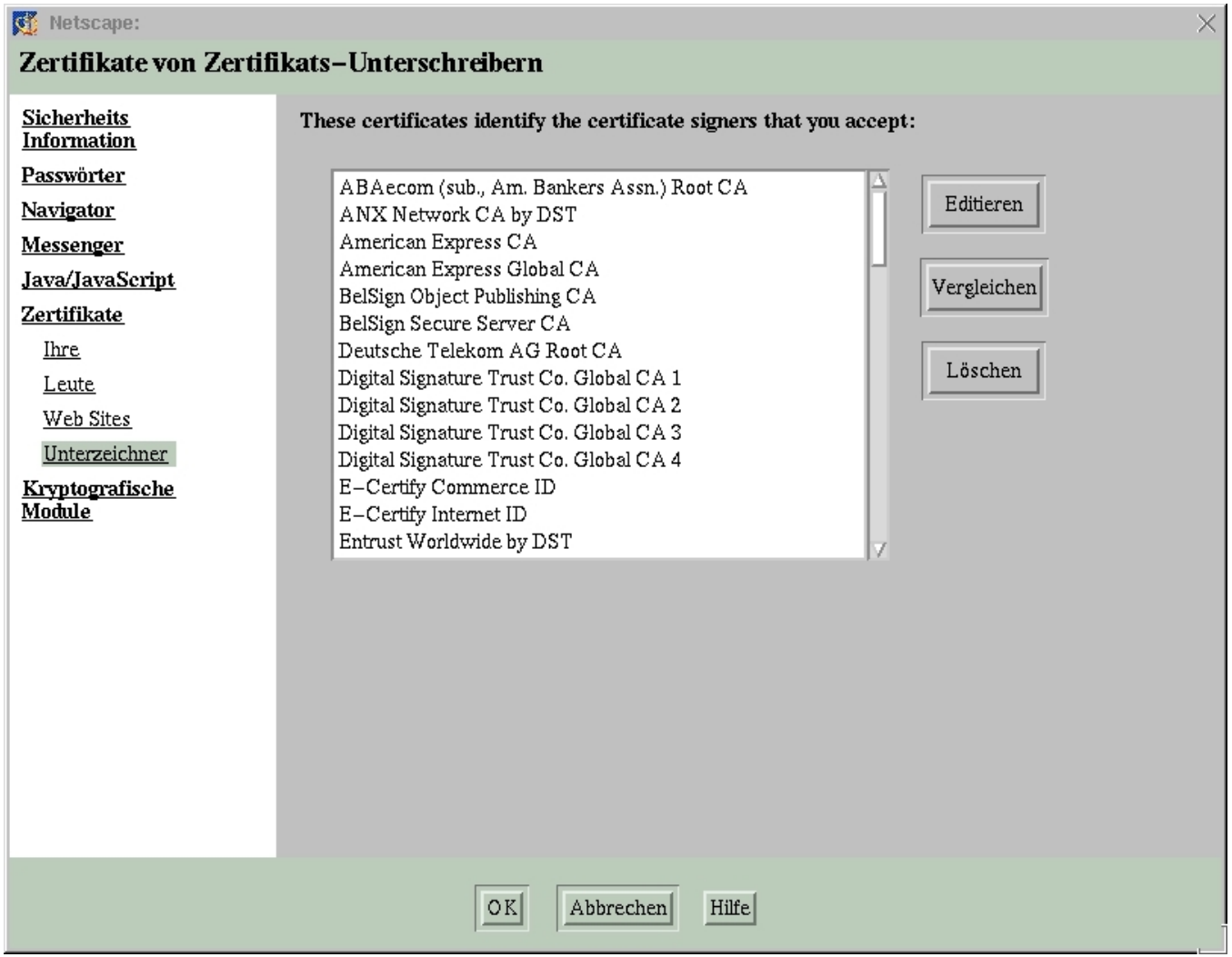
- **Hybrides Verfahren**
- **Protokoll: https**
- **Client teilt Server mit, welche Verschlüsselungsverfahren er unterstützt.**



SSL

- Server wählt ein Public−Key und ein Privat−Key Verfahren und teilt sie dem Client mit.
- Server sendet ein Zertifikat mit öffentlichem Schlüssel des Servers. Dies Zertifikat bestätigt die Identität des Servers.
- Das Zertifikat muß von einer vom Client akzeptierten Zertifizierungsstelle stammen.
- Ist die Zertifizierungsstelle "neu", muß der Benutzer zustimmen.

SSL


Netscape:
Zertifikate von Zertifikats–Unterschreibern
Sicherheits Information
Passwörter
Navigator
Messenger
Java/JavaScript
Zertifikate
Ihre
Leute
Web Sites
Unterzeichner
Kryptografische Module
These certificates identify the certificate signers that you accept:
ABAecom (sub., Am. Bankers Assn.) Root CA
ANX Network CA by DST
American Express CA
American Express Global CA
BelSign Object Publishing CA
BelSign Secure Server CA
Deutsche Telekom AG Root CA
Digital Signature Trust Co. Global CA 1
Digital Signature Trust Co. Global CA 2
Digital Signature Trust Co. Global CA 3
Digital Signature Trust Co. Global CA 4
E–Certify Commerce ID
E–Certify Internet ID
Entrust Worldwide by DST
Editieren
Vergleichen
Löschen
OK
Abbrechen
Hilfe

SSL

- **Der Client erzeugt einen Sitzungsschlüssel (session key) und überträgt ihn, verschlüsselt mit dem öffentlichen Schlüssel des Servers, an den Server.**
- **Der Server entschlüsselt mit seinem privaten Schlüssel den session key.**
- **Mit dem session key werden nun alle Nachricher symetrisch verschlüsselt und entschlüsselt.**

pgp (pretty good privacy)

- Hybrides Verfahren
- pgp erzeugt für jede Kommunikation einen session key.
- Der session key wird zunächst mit dem private key des Senders verschlüsselt (digitale Signatur).
- Das Ergebnis wird mit dem öffentlichen Schlüssel des Empfängers verschlüsselt.
- Die eigentliche Nachricht wird mit dem session key verschlüsselt.

pgp (pretty good privacy)

- Der Empfänger wendet zunächst seine privaten Schlüssel auf den session key an (das kann nur er).
- Auf das Ergebnis wendet er den public key des Senders an (dies stellt sicher, daß die mail von eben jenem kam).
- Mit dem so ermittelten session key entschlüsselt er die email.