# Absicherung der Internet Protokolle

- Einführung
- Absicherung auf der Vermittlungsschicht (IPSEC)
- Absicherung auf der Anwendungsschicht (S/MIME, S-HTTP)
- Absicherung auf der Transportschicht: **SSL**
  - Unterstützte kryptographische Verfahren
  - Das SSL Handshake-Protokoll
- Abschluß

# Einführung

Aufgaben eines abgesicherten Übertragungsdienstes:

- Definition von Protokollstrukturen zur Übertragung
- Definition eines Protokolls zur Schlüssel-Aquisition
- Zugänglichkeit durch transparente Integration oder als Programmierschnittstellen (strittig)

# Absicherung ist auf verschiedenen Schichten möglich:

| Vermittlungsschicht | Transportschicht | Anwendungsschicht |
|---|---|---|
| HTTP SMTP | HTTP SMTP | S-HTTP S/MIME<br>HTTP SMTP |
| TCP UDP | SSL<br>TCP | TCP UDP |
| AH ESP<br>IP | IP | IP |
| Netzwerk | Netzwerk | Netzwerk |
| IPv4 + IPSEC<br>IPv6 | IPv4 + SSL<br>IPv4 + PCT | PEM, S-HTTP<br>S/MIME, SET |

## Vermittlungsschicht

- Vorteil: bestehende Anwendungen müssen nicht modifiziert werden
- Nachteil: Kryptographie wird auf alle Anwendungsprotokolle angewandt ($\Rightarrow$ rechenintensiv)
- IP-SEC als Entwicklungsgruppe der IETF entwickelt IPSP

Die **IP-SEC** Gruppe beschätigt sich mit zwei verschiedenen Protokollen:

- IPSP mit AH und ESP (als Standard vorgeschlagen)
- IKMP (noch in Arbeit)

Einsatz findet das IPSP Protokoll vor allem im Bereich der VPN, es wird aber z.T. auch in Routern verwendet.

## Anwendungsschicht

- Vorteil: Exaktes Abstimmen auf die Sicherheitsbedürfnisse der Applikation möglich
- Nachteil: Anwendungsprotokoll selbst muß modifiziert werden $\Rightarrow$ z.T. proprietäre Infrastrukturen
- Verfahren: S/MIME, S-HTTP

**S/MIME** ist eine aus dem MIME Standard aufbereitete Erweiterung zur Übertragung von verschlüsselten und/oder digital unterschriebenen EMail Nachrichten über das Internet Protokoll SMTP. Wird von vielen Softwareherstellern unterstützt.

**MIME** ist ein Verfahren zur Spezifikation unterschiedlicher Dokumenttypen und Kodierungsverfahren, das für den Einsatz mit EMail entwickelt wurde. Wird u.a. verwendet zur Spezifikation von HTML Metadaten.

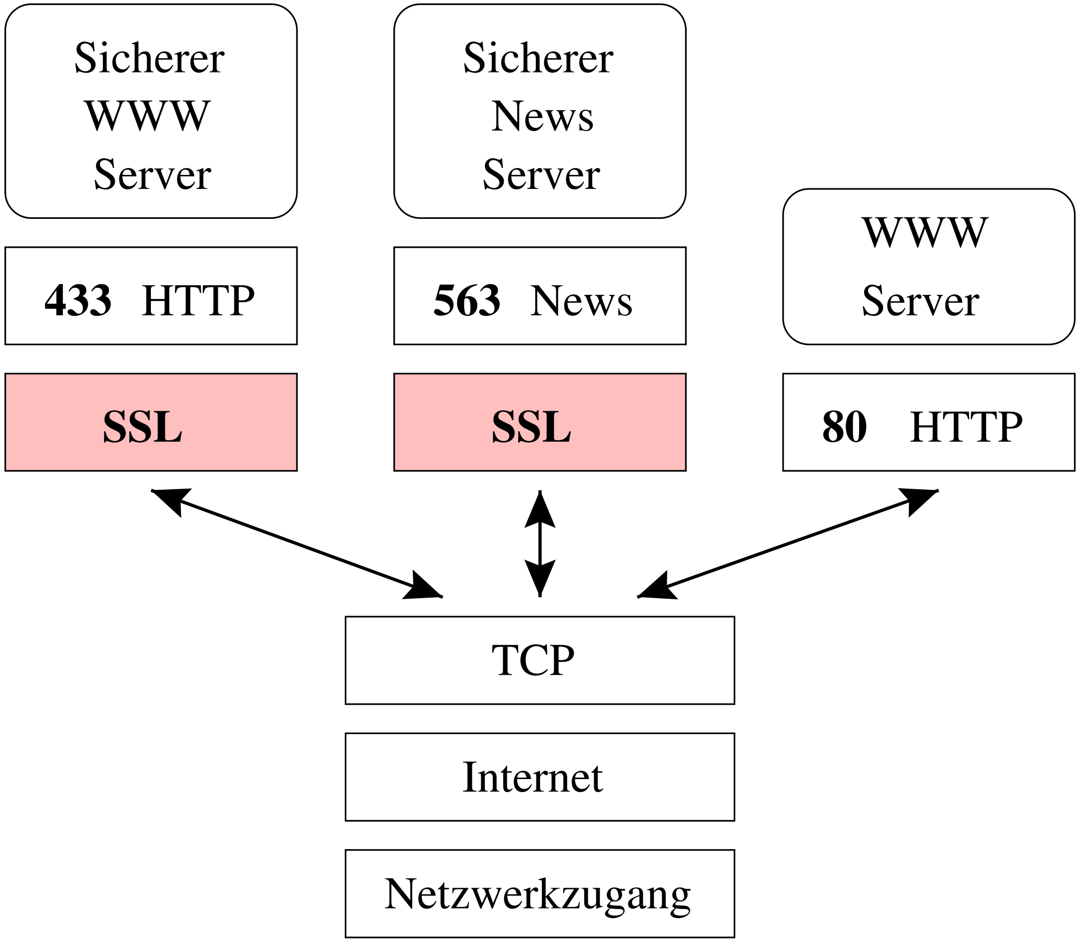
## S-HTTP

- Erweiterung von HTML und HTTP
- Übertragung von verschlüsselten und/oder digital unterschriebenen MIME Entitäten in beide Richtungen
- Absicherung der Übertragung wird für jede Verbindung neu zwischen Client und Server ausgehandelt
- Nicht-Abstreitbarkeit eines einzelnen Absendevorganges ist gewährleistet (bei SSL nicht möglich)

## Transportschicht: SSL

- Secure Sockets Layer ist als von Netscape entwickeltes Protokoll bereits Bestandteil vieler Browser.
- Unterscheidung zwischen verschiedenen Diensten ist mit Hilfe der Sockets möglich $\Rightarrow$ Gezielte Sicherheit
- SSL ist eine Programmierbibliothek $\Rightarrow$ Nachteil: Quellcode der Anwendungen muß geändert werden.
- Als Basis muß ein verläßliches verbindungsorientiertes Transportprotokoll wie TCP vorliegen, UDP Datagramme können nicht abgesichert werden.

# Der Ansatz von SSL



# Unterstützte kryptographische Verfahren (V3, 1996):

| | **Vollversion** | **Exportversion** |
|---|---|---|
| Verschlüsselung | RC2 (128 Bit) | RC2 (40 Bit) |
| | RC4 (128 Bit) | RC4 (40 Bit) |
| | IDEA (128 Bit) | IDEA (40 Bit) |
| | DES (56 Bit) | |
| | Triple-DES (168 Bit) | |
| Integrität | MD5 (128 Bit Hash) | MD5 (128 Bit Hash) |
| | SHA (160 Bit Hash) | |
| PK-Verfahren | RSA, Fortezza | RSA(512 Bit) |
| und Schlüssel- | Diffie Hellman | Diffie Hellman (512 Bit) |
| austausch | (DSS, RSA oder anonym) | (DSS, RSA oder anonym) |
| Zertifikat | X.509 (Version 3) | X.509 (Version 3) |

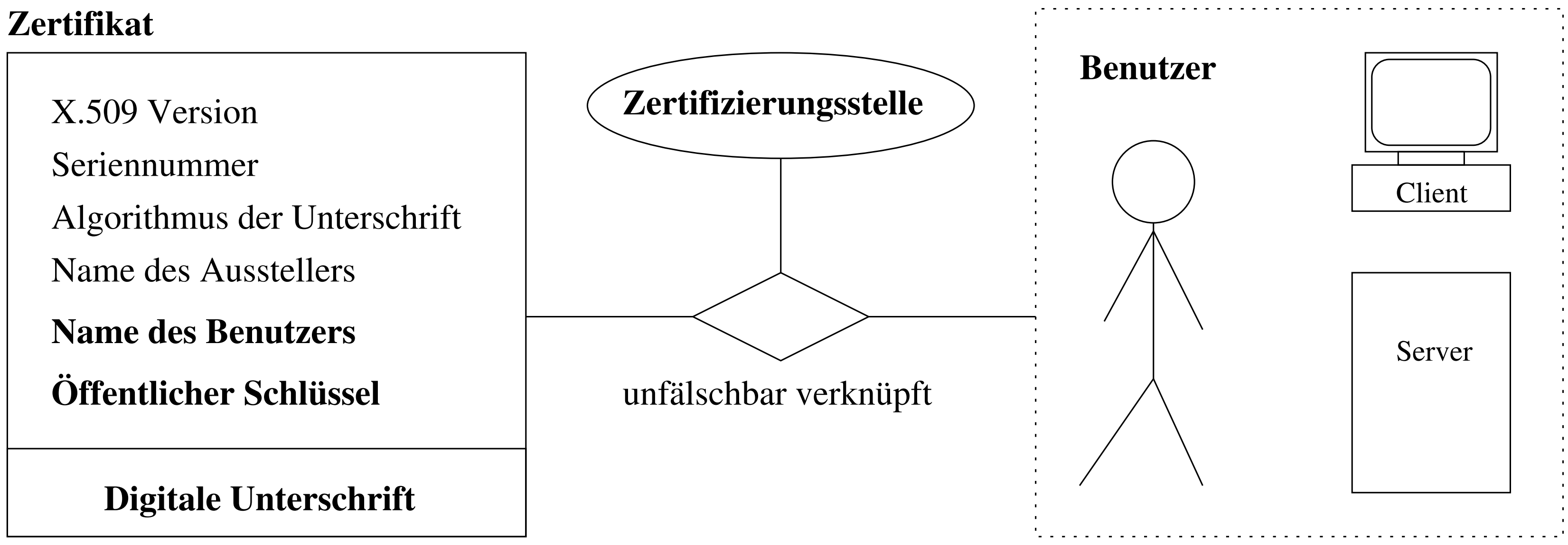
## Was ist eigentlich ein Zertifikat?

Ein **Zertifikat** ist der öffentliche Schlüssel eines Benutzers zusammen mit zusätzlichen Informationen, unfälschbar gemacht durch das Verschlüsseln mit dem privaten Schlüssel einer Zertifizierungsstelle.

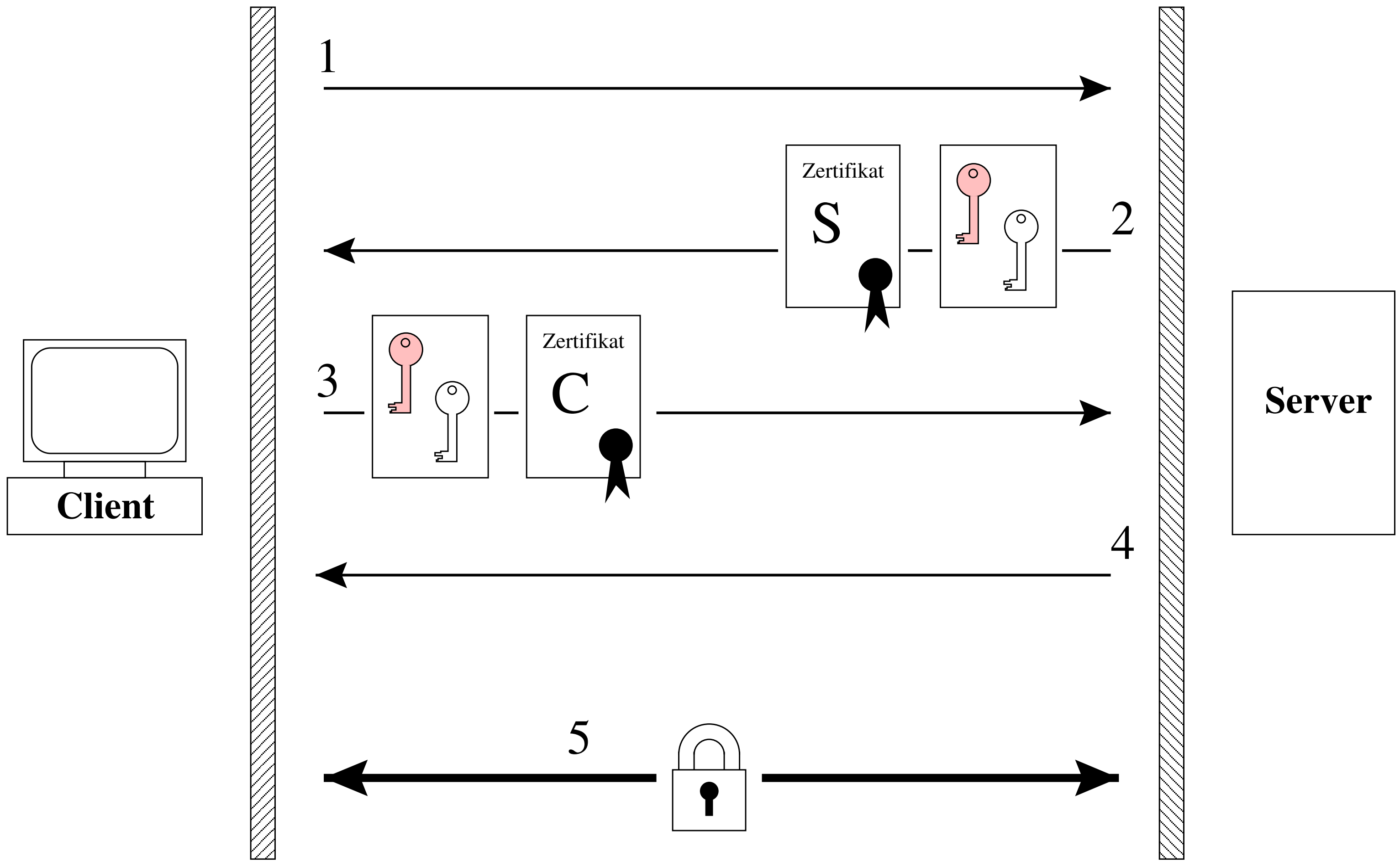
Eine **Zertifizierungsstelle** ist eine Institution, der ein oder mehrere Benutzer die Erstellung und Zuweisung von Zertifikaten anvertrauen.

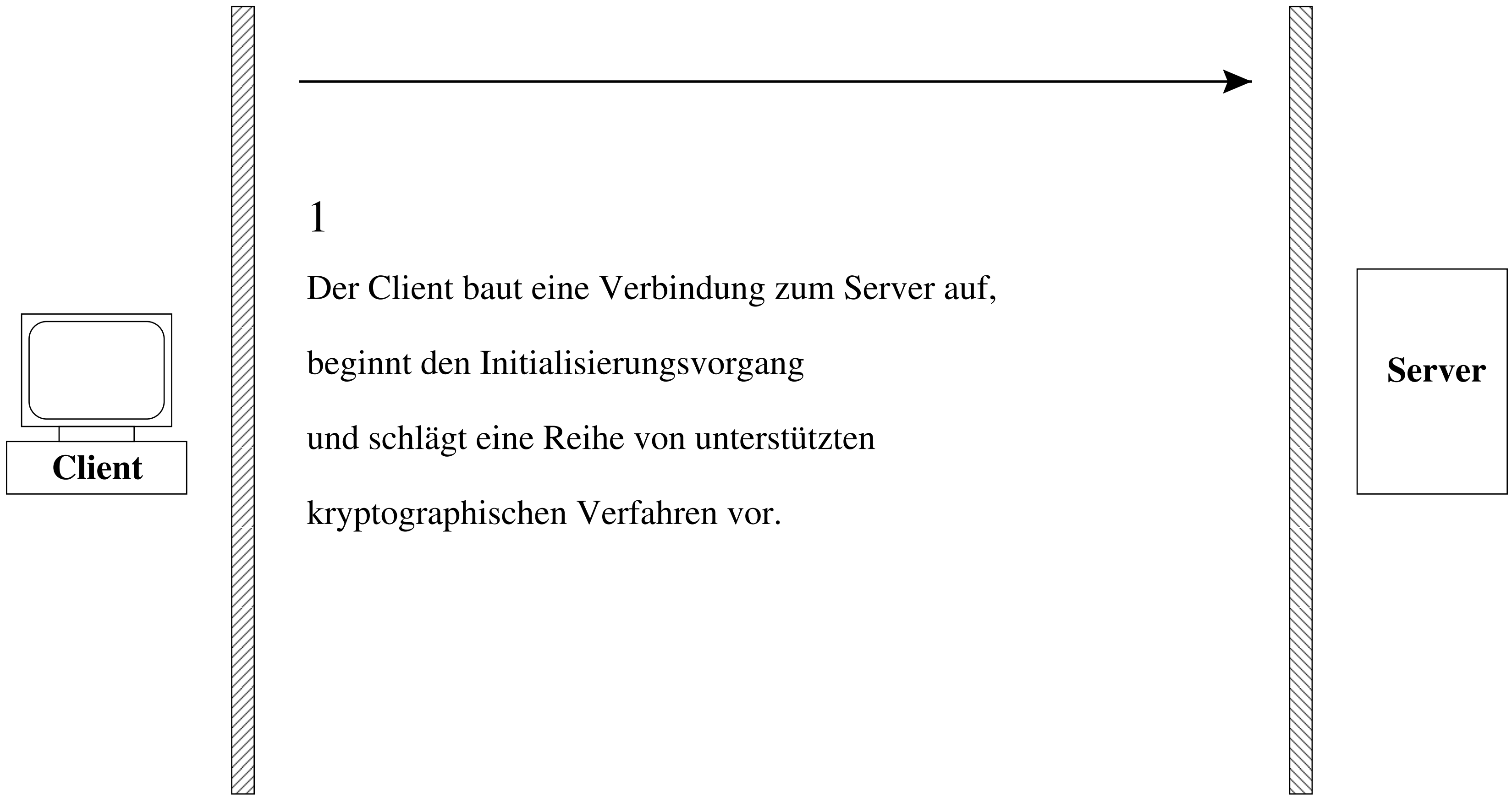
**X.509** ist ein Entwurf zur Festlegung eines Standards zur Formulierung von Zertifikaten.

# Ein X.509 Zertifikat



# Das SSL Handshake-Protokoll





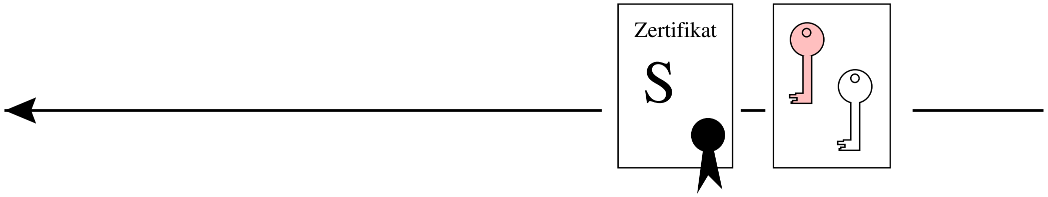

1

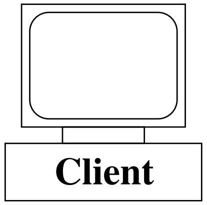
Der Client baut eine Verbindung zum Server auf,

beginnt den Initialisierungsvorgang

und schlägt eine Reihe von unterstützten

kryptographischen Verfahren vor.



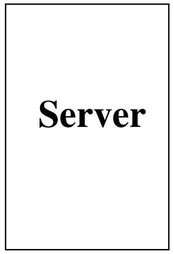

2

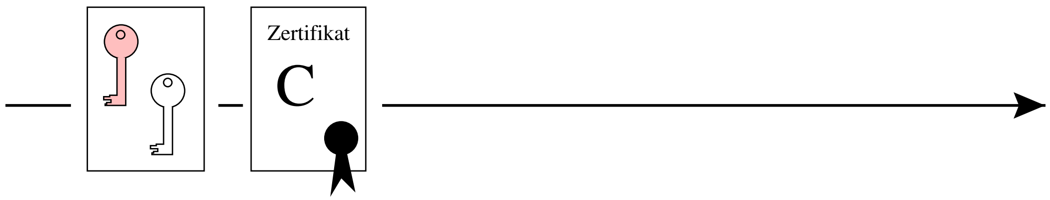
Der Server antwortet mit einer Auswahl geeigneter, von beiden unterstützten Verfahren und überträgt sein X.509 Zertifikat.

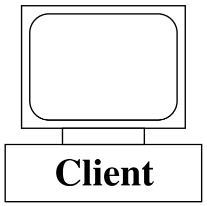
Dies unterschreibt er mit seinem privaten Schlüssel.

Optional kann vom Client ein Zertifikat verlangt werden.

Ggf. werden Informationen zur Erzeugung des Sitzungsschlüssels übertragen





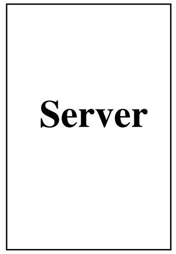



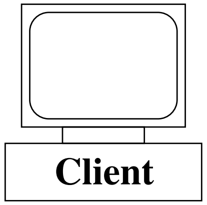

3

Der Client prüft das Zertifikat des Servers und sendet ggf. sein eigenes, ebenfalls digital unterschriebenes Zertifikat.

Die zur Erzeugung des Sitzungsschlüssels notwendigen Informationen werden übertragen.

Seitens des Clients ist die Initialisierungsphase abgeschlossen.





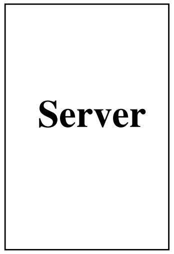

4

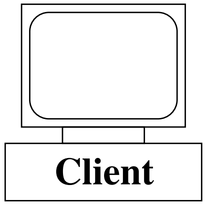
Der Server überprüft ggf. das Zertifikat des Client und

bestätigt den Abschluß der Initialisierungsphase.

Diese Nachricht wird mit dem ausgehandelten Verfahren

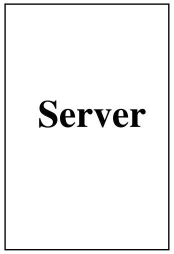
symmetrisch verschlüsselt und digital unterschrieben.

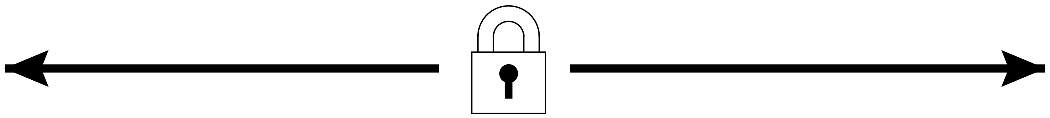





5

Dem Anwendungsprotokoll steht nun eine symmetrisch verschlüsselte, sichere Verbindung zur Verfügung.



# Abschluß

- Absicherung hat auf allen Schichten Vor- und Nachteile
- Der Aufwand entscheidet, ob man Sicherheitsmechanismen nutzt
- IP-SEC am vielversprechendsten, da am meisten Transparenz gewährleistet
- Argument der Rechenintensität der Kryptographie wird durch ständige steigende Rechner-Performance obsolet
- Allerdings: Aktualität der genutzten kryptographischen Verfahren muß gewährleistet sein