# Mehrseitige Sicherheitsfunktionen in Telekommunikationsnetzen

Hannes Federrath

http://www.inf.tu-dresden.de/~hf2/

- Was ist mehrseitige Sicherheit?
- Einordnung, Schutzziele, Wechselwirkungen
- Mechanismen zur Realisierung mehrseitiger Sicherheit

# Sicherheit: Abgrenzung von Security & Safety

## SECURITY
Schutz gegen beabsichtigte Angriffe

### Vertraulichkeit
- Abhörsicherheit
- Sicherheit gegen unbefugten Gerätezugriff
- Anonymität
- Unbeobachtbarkeit

### Integrität
- Übertragungsintegrität
- Zurechenbarkeit
- Abrechnungsintegrität

### Verfügbarkeit
- Ermöglichen von Kommunikation

## SAFTEY
Schutz vor unbeabsichtigten Ereignissen

### **Fehlertoleranz**

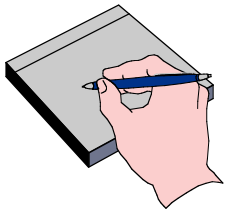
### Verfügbarkeit
- Funktionssicherheit
- Technische Sicherheit
- Schutz vor Überspannung, Überschwemmung, Temeraturschwankungen
- Schutz vor Spannungsausfall

### Sonstige Schutzziele
- Maßnahmen gegen hohe Gesundheitsbelastung
- …

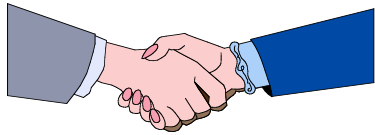
# Mehrseitige Sicherheit

- Jeder Beteiligte hat **Sicherheitsinteressen**.

- Jeder Beteiligte kann seine Interessen **formulieren**.



- Konflikte werden erkannt und Lösungen **ausgehandelt**.



- Jeder Beteiligte kann seine Sicherheitsinteressen in den ausgehandelten Lösungen **durchsetzen**.

**Sicherheit mit minimalen Annahmen über andere.**
**So wenig wie möglich Vertrauen in andere setzen müssen.**

# Schutzziele: Einordnung

| | WAS? | WANN?, WO?, WER? |
|---|---|---|
| | **Kommunikations-gegenstand** | **Kommunikations-umstände** |
| **Un-erwünschtes verhindern** | **Vertraulichkeit**<br>**Verdecktheit**<br>Inhalte | **Anonymität**<br>**Unbeobachtbarkeit**<br>Sender, Ort<br>Empfänger |
| **Erwünschtes leisten** | **Integrität**<br>Inhalte | **Zurechenbarkeit**<br>Senden<br>Empfangen |
| | **Verfügbarkeit** | **Erreichbarkeit**<br>**Rechtsverbindlichkeit**<br>Bezahlung |

# Schutzziele: Definitionen

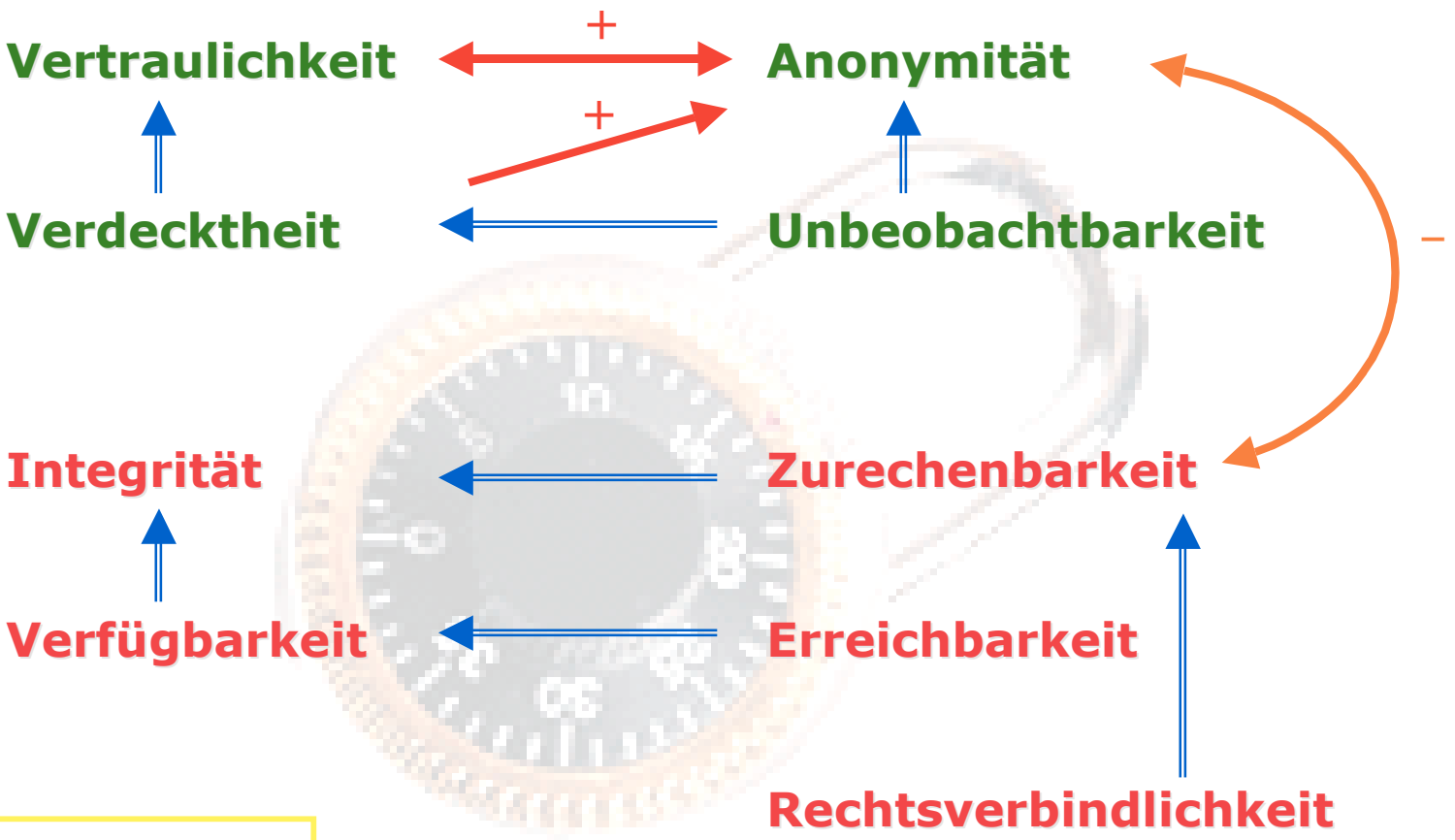
- **Vertraulichkeit:** Geheimhaltung von Daten während der Übertragung. Niemand außer den Kommunikationspartnern kann den Inhalt der Kommunikation erkennen.
  **Verdecktheit:** Versteckte Übertragung von vertraulichen Daten. Niemand außer den Kommunikationspartnern kann die Existenz einer vertraulichen Kommunikation erkennen.
  **Anonymität:** Nutzer können Ressourcen und Dienste benutzen, ohne ihre Identität zu offenbaren. Selbst der Kommunikationspartner erfährt nicht die Identität.
  **Unbeobachtbarkeit:** Nutzer können Ressourcen und Dienste benutzen, ohne daß andere dies beobachten können. Dritte können weder das Senden noch den Erhalt von Nachrichten beobachten.

- **Integrität:** Modifikationen der kommunizierten Inhalte (Absender eingeschlossen) werden durch den Empfänger erkannt.
  **Zurechenbarkeit:** Sendern bzw. Empfängern von Informationen kann das Senden bzw. der Empfang der Informationen bewiesen werden. Wechselwirkungen zwischen Schutzzielen

- **Verfügbarkeit:** Nutzbarkeit von Diensten und Ressourcen, wenn ein Teilnehmer sie benutzen will.
  **Erreichbarkeit:** Zu einer Ressource (Nutzer oder Maschine) kann Kontakt aufgenommen werden, wenn gewünscht.
  **Rechtsverbindlichkeit:** Ein Nutzer kann rechtlich belangt werden, um seine Verantwortlichkeiten innerhalb einer angemessenen Zeit zu erfüllen.

# Wechselwirkungen zwischen Schutzzielen

A. Pfitzmann, G. Wolf, 1999




impliziert

\+ verstärkt

– schwächt

Beobachtungen zum Monotonieverhalten:

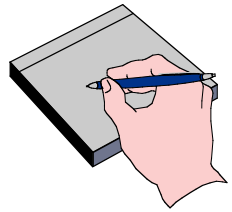
Vertraulichkeitseigenschaften können nur geringer werden.

Integrität und Zurechenbarkeit können nur größer werden.

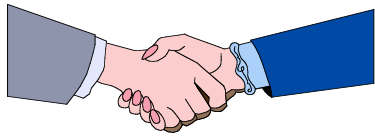
# Mehrseitige Sicherheit: Wie?

- Jeder Beteiligte hat **Sicherheitsinteressen**.
  - Schutzziele

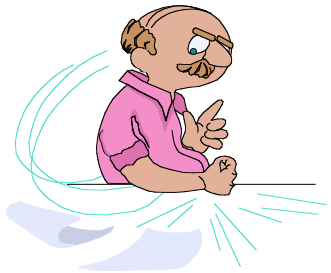
- Jeder Beteiligte kann seine Interessen **formulieren**.
  - Setzt Verständnis des Benutzers voraus
  - Gute Bedienoberflächen sind nötig



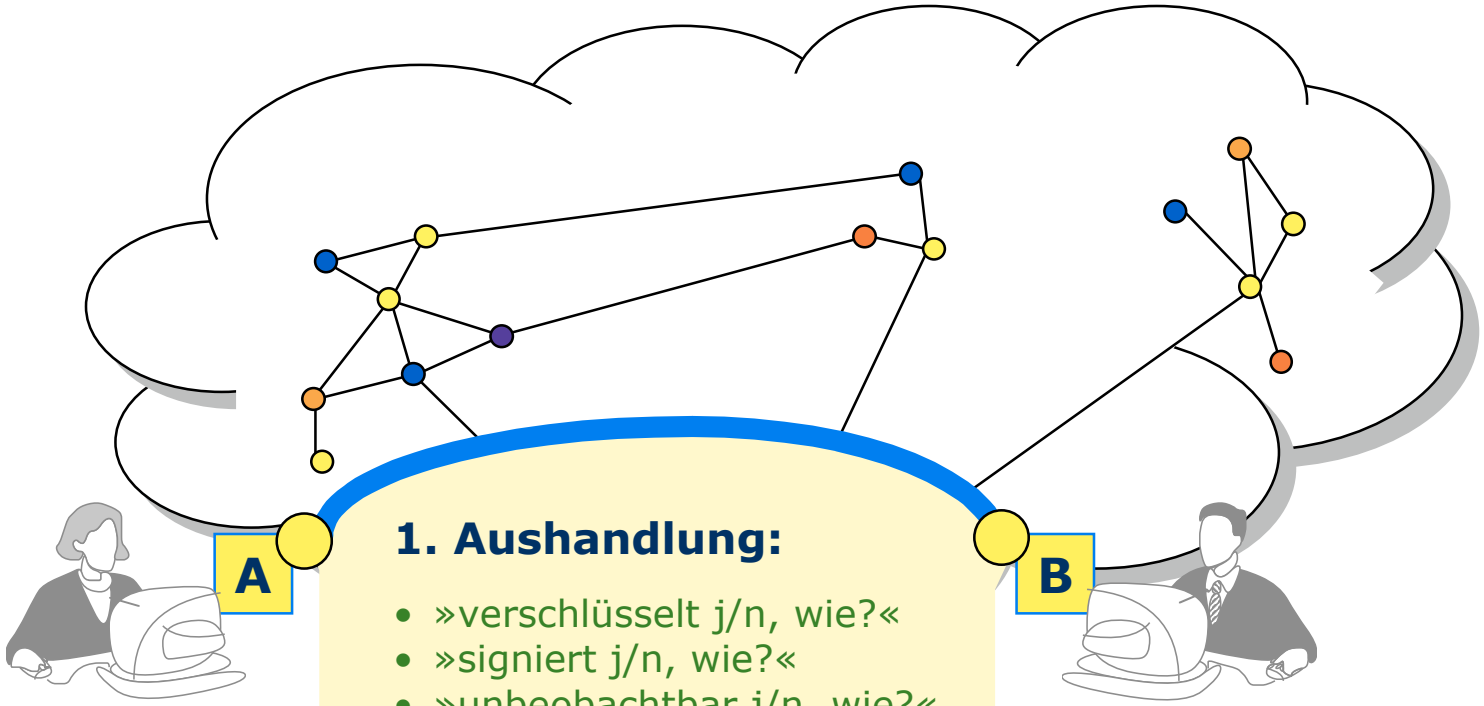
- Konflikte werden erkannt und Lösungen **ausgehandelt**.
  - Setzt entsprechende Tools und
  - Technische Protokolle voraus



- Jeder Beteiligte kann seine Sicherheitsinteressen in den ausgehandelten Lösungen **durchsetzen**.
  - Anwender brauchen Werkzeuge zum Selbstschutz



# Formulierung und Aushandlung

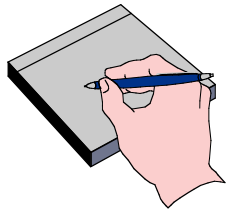



Die Anwendung von mehrseitiger Sicherheit setzt die explizite Formulierung der Sicherheitsinteressen und die Notwendigkeit voraus, aufeinander einzugehen.

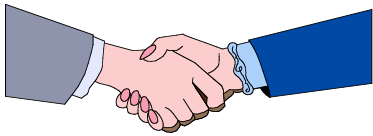
# Mehrseitige Sicherheit: Wie?

- Jeder Beteiligte hat **Sicherheitsinteressen**.
  - Schutzziele

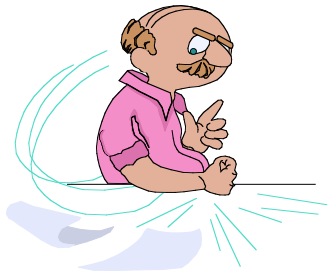
- Jeder Beteiligte kann seine Interessen **formulieren**.
  - Setzt Verständnis des Benutzers voraus
  - Gute Bedienoberflächen sind nötig



- Konflikte werden erkannt und Lösungen **ausgehandelt**.
  - Setzt entsprechende Tools und
  - Technische Protokolle voraus



- Jeder Beteiligte kann seine Sicherheitsinteressen in den ausgehandelten Lösungen **durchsetzen**.
  - Anwender brauchen Werkzeuge zum Selbstschutz



# Schutzziele: Einordnung

| | WAS? | WANN?, WO?, WER? |
|---|---|---|
| | **Kommunikations-gegenstand** | **Kommunikations-umstände** |
| **Un-erwünschtes verhindern** | **Vertraulichkeit**<br>**Verdecktheit**<br>**Inhalte** | **Anonymität**<br>**Unbeobachtbarkeit**<br>**Sender** / **Empfänger** / **Ort** |
| **Erwünschtes leisten** | **Integrität**<br>**Inhalte** | **Zurechenbarkeit**<br>**Senden** / **Empfangen** |
| | **Verfügbarkeit** | **Erreichbarkeit**<br>**Rechtsverbindlichkeit**<br>**Bezahlung** |

**Vertraulichkeit**

Verdecktheit

Integrität

Zurechenbarkeit

Anonymität

Unbeobachtbarkeit

Verfügbarkeit

Erreichbarkeit

Rechtsverbindlichkeit

## Verschlüsselungsverfahren

- **Symmetrische Verschlüsselung, z.B. DES, AES**
  - Kommunikationspartner teilen ein gemeinsames Geheimnis (symmetrischer Schlüssel)
  - Sicherheit basiert meist auf Chaos
  - Schlüssellänge ≥ 128 Bits
- **Asymmetrische Verschlüsselung, z.B. RSA**
  - Jeder Nutzer generiert Schlüsselpaar:
    - *Öffentlichen* Verschlüsselungsschlüssel
    - *Privaten* Entschlüsselungsschlüssel
  - Sicherheit basiert auf zahlentheoretischen Annahmen
  - Schlüssellänge ≥ 1024 Bit
  - Neuerdings: Elliptische Kurven: ca. 160 Bit
- **Bekannte Verschlüsselungssoftware**
  - Pretty Good Privacy
  - http://www.pgp.com

**Vertraulichkeit**

Verdecktheit

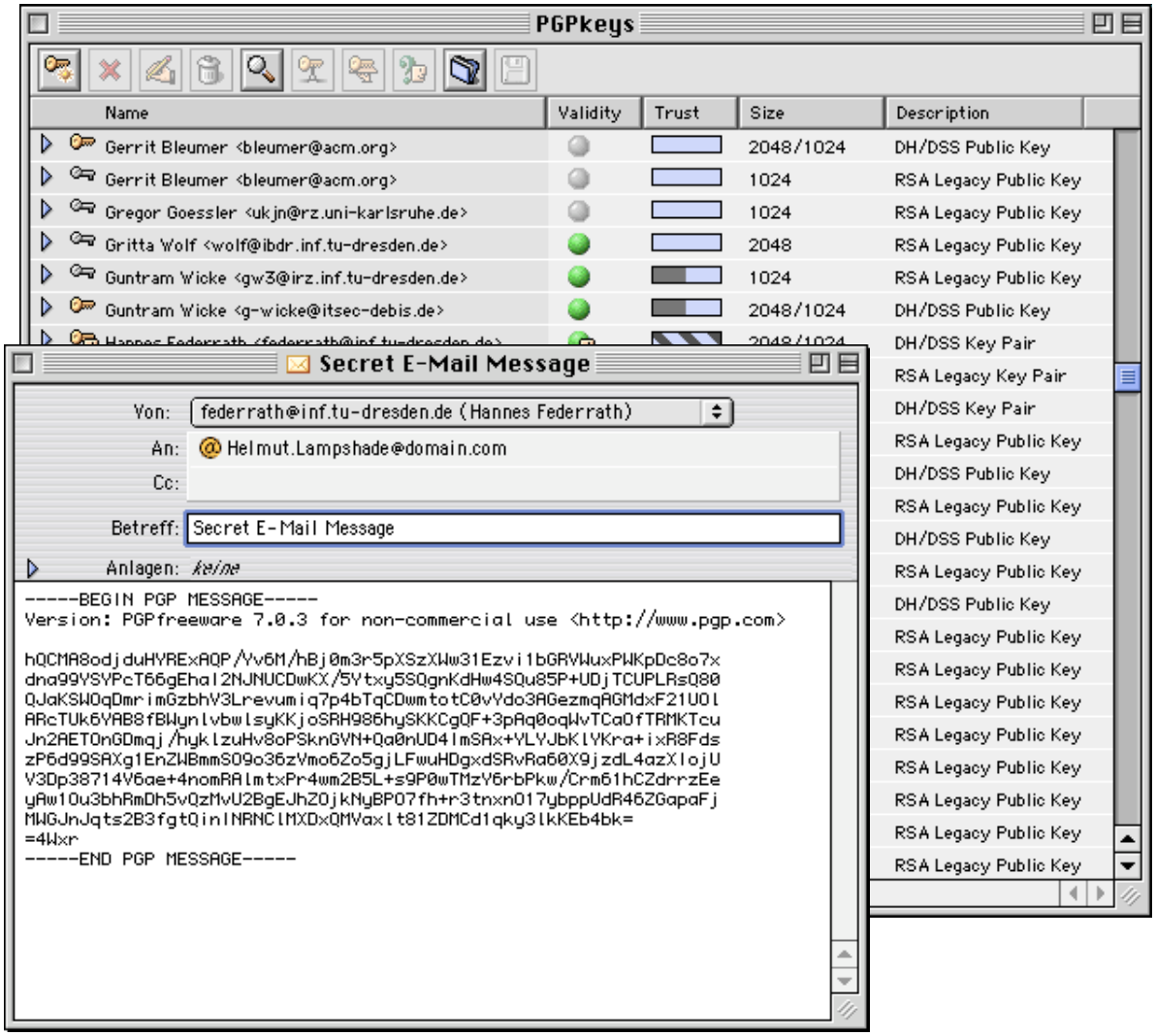
Integrität
Zurechenbarkeit

Anonymität
Unbeobachtbarkeit

Verfügbarkeit
Erreichbarkeit

Rechtsverbindlichkeit

## Pretty Good Privacy (PGP)



# Verdecktheit: Steganographie

Vertraulichkeit

**Verdecktheit**

Integrität
Zurechenbarkeit

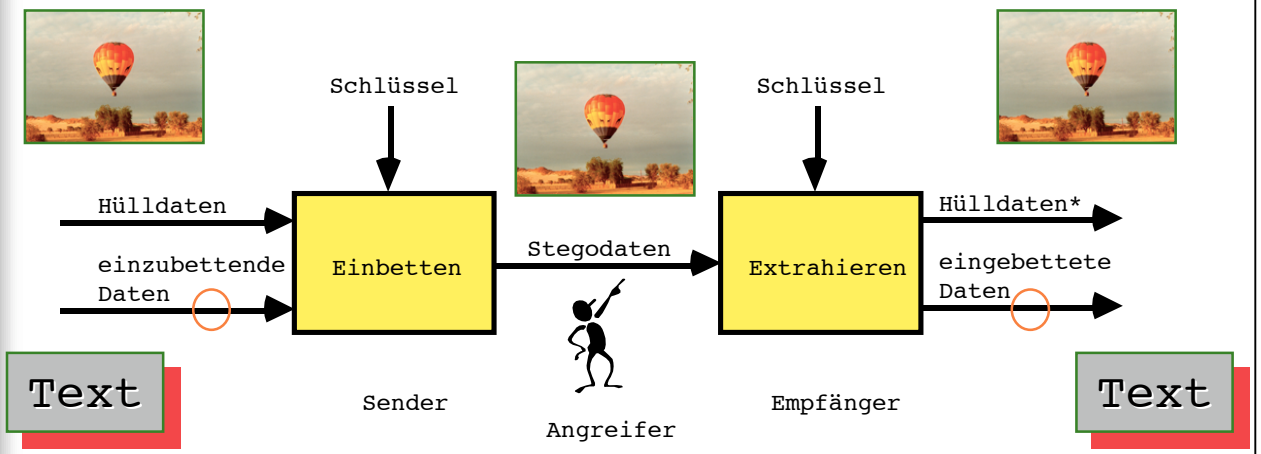
Anonymität
Unbeobachtbarkeit

Verfügbarkeit
Erreichbarkeit

Rechtsverbindlichkeit

## Steganographie

- **Verbergen der Existenz einer geheimen Nachricht**
  - geheimzuhaltende Nachricht wird in eine Hülle eingebettet
  - minimale Veränderungen kaum bzw. nicht erkennbar
  - Veränderungen nicht mit Messmethoden nachweisbar



# Integrität und Zurechenbarkeit

Vertraulichkeit
Verdecktheit

**Integrität**
**Zurechenbarkeit**

Anonymität
Unbeobachtbarkeit

Verfügbarkeit
Erreichbarkeit

Rechtsverbindlichkeit

## Message Authentication Codes

- **Symmetrisches Verfahren**
  - Kommunikationspartner teilen ein gemeinsame Geheimnis (symmetrischer Schlüssel)
- **Gehört heute zum Grundschutz**
  - Verfälschungen von Nachrichten (böswillige und zufällige) sind erkennbar
- **Keine Nachweisbarkeit gegenüber Dritten**

## Digitale Signatur

- **Asymmetrisches Verfahren, z.B. RSA**
  - Jeder Nutzer generiert Schlüsselpaar:
    - *Öffentlichen* Testschlüssel
    - *Privaten* Sigierschlüssel
- **Nachweisbarkeit gegenüber Dritten**
- **Ebenfalls einsetzbar:**
  - Pretty Good Privacy
  - http://www.pgp.com

# Anonymität und Unbeobachtbarkeit

Vertraulichkeit
Verdecktheit

Integrität
Zurechenbarkeit

**Anonymität**
**Unbeobachtbarkeit**

Verfügbarkeit
Erreichbarkeit

Rechtsverbindlichkeit

## Verfahren zum Schutz von Verkehrdaten

- **Adressierungsinformationen können nicht verschlüsselt werden**
  - Problem Verkehrsdaten:
    - Wer mit wem, wann, wie lange, wo, wieviel Information?
  - Problem Interessensdaten:
    - Wer interessiert sich für was?
- **Spezielle Verfahren:**
  - Proxies
  - Mix-Netz
  - DC-Netz
  - Dummy traffic
  - ...
- **Anonymisierung von Web-Zugriffen**
  - JAP-Software
  - http://jap.inf.tu-dresden.de

# Anonymität und Unbeobachtbarkeit

Vertraulichkeit
Verdecktheit

Integrität
Zurechenbarkeit

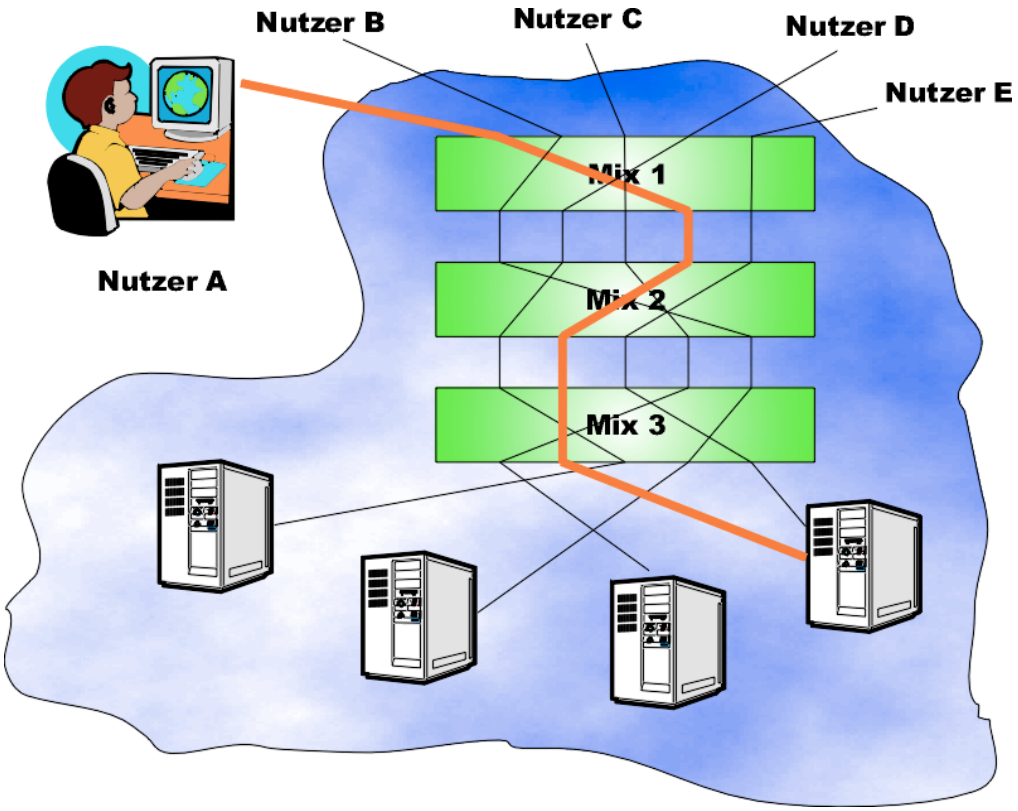
**Anonymität**
**Unbeobachtbarkeit**

Verfügbarkeit
Erreichbarkeit

Rechtsverbindlichkeit

## Verfahren zum Schutz von Verkehrdaten

- **Anonymisierung von Web-Zugriffen**
  - JAP-Software
  - http://jap.inf.tu-dresden.de



# Verfügbarkeit und Erreichbarkeit

Vertraulichkeit
Verdecktheit

Integrität
Zurechenbarkeit

Anonymität
Unbeobachtbarkeit

**Verfügbarkeit**
**Erreichbarkeit**

Rechtsverbindlichkeit

- **Verfügbarkeit**
  - Nutzbarkeit von Diensten und Ressourcen, wenn ein Teilnehmer sie benutzen will.
- **Erreichbarkeit**
  - Zu einer Ressource (Nutzer oder Maschine) kann Kontakt aufgenommen werden, wenn gewünscht.
- **»Mechanismen«**
  - Mehrfach redundante Leitungsführung
  - Diversitärer Entwurf der Komponenten
  - Starke Vermaschung der Kommunikationsverbindungen
- **Techniken zur Verteilung von Kontrolle**
  - Offenlegung von Designkriterien und Algorithmen
  - Open Source Software
  - Sichere Betriebssysteme

# Rechtsverbindlichkeit

Vertraulichkeit
Verdecktheit

Integrität
Zurechenbarkeit

Anonymität
Unbeobachtbarkeit

Verfügbarkeit
Erreichbarkeit

**Rechtsverbindlichkeit**

- **Rechtsverbindlichkeit**
  - Ein Nutzer kann rechtlich belangt werden, um seine Verantwortlichkeiten innerhalb einer angemessenen Zeit zu erfüllen.
  - Kann nicht technisch geschaffen werden
- **Rechtsverbindlichkeit der Digitalen Signatur**
  - Klare Regeln bzgl. Beweiswert
  - Zertifizierung von Schlüssel (Public Key Infrastructure PKI)
- **Sicherheit der Netzkomponenten**
  - Zertifizierung von Netzkomponenten
  - Physische Sicherheit, immer dann, wenn Vertrauen in fremde Netzkomponente aufgebracht werden muss.

# Mehrseitige Sicherheit: Umfassendes Schutzkonzept

- Spannungsfeld Privatheit — Verbindlichkeit
  - Datenvermeidung:
    - Erfassungsmöglichkeit und Speicherung personenbezogener Daten vermeiden.
  - Datensparsamkeit:
    - Jeder behält seine personenbezogenen Daten auf seinem PC.
- Wechselwirkung Datenschutz — Datensicherheit
  - Datenschutz: Schutz der Menschen
  - Datensicherheit: Schutz der Daten
  - Mehrseitige Sicherheit verbindet beides.

Mehrseitige Sicherheit bedeutet die Einbeziehung der Schutzinteressen *aller* Beteiligten sowie das Austragen daraus resultierender Schutzkonflikte beim Entstehen einer Kommunikationsverbindung.