

# Mehrseitige Sicherheit := Autonomie + Datensicherheit + Datenschutz

*Andreas Pfitzmann*

- (Un-)Sicherheit → Mehrseitige Sicherheit
- Schutzziele und ihre Wechselwirkungen
- Techniken für Mehrseitige Sicherheit
  - Unilateral nutzbar: jede(r) kann allein entscheiden
  - Bilateral nutzbar: nur wenn der Kommunikationspartner kooperiert
  - Trilateral nutzbar: nur wenn zusätzlich ein vertrauenswürdiger Dritter kooperiert
  - Multilateral nutzbar: nur wenn viele Partner kooperieren
- Bewertung von Reife und Effektivität
- Datenschutzprinzipien: Datenschutz durch Technik

# Bedrohungen und korrespondierende Schutzziele

## Bedrohungen:

Bsp.: medizinisches Informationssystem

## Schutzziele:

### 1) Informationsgewinn

Rechnerhersteller erhält Krankengeschichten

Vertraulichkeit

### 2) Modifikation von Information

unerkannt Dosieranweisungen ändern

### 3) Beeinträchtigung der

Funktionalität

erkennbar ausgefallen

≥ totale  
Korrektheit

Integrität

≡ partielle Korrektheit

Verfügbarkeit  
für berechnigte  
Nutzer

keine Klassifikation, aber pragmatisch sinnvoll

Bsp.: Programm unbefugt modifiziert

1) nicht erkennbar, aber verhinderbar; nicht rückgängig zu machen

2)+3) nicht verhinderbar, aber erkennbar; rückgängig zu machen

# Definitionen für die Schutzziele

## Vertraulichkeit (confidentiality)

Informationen werden nur Berechtigten bekannt.

## Integrität (integrity)

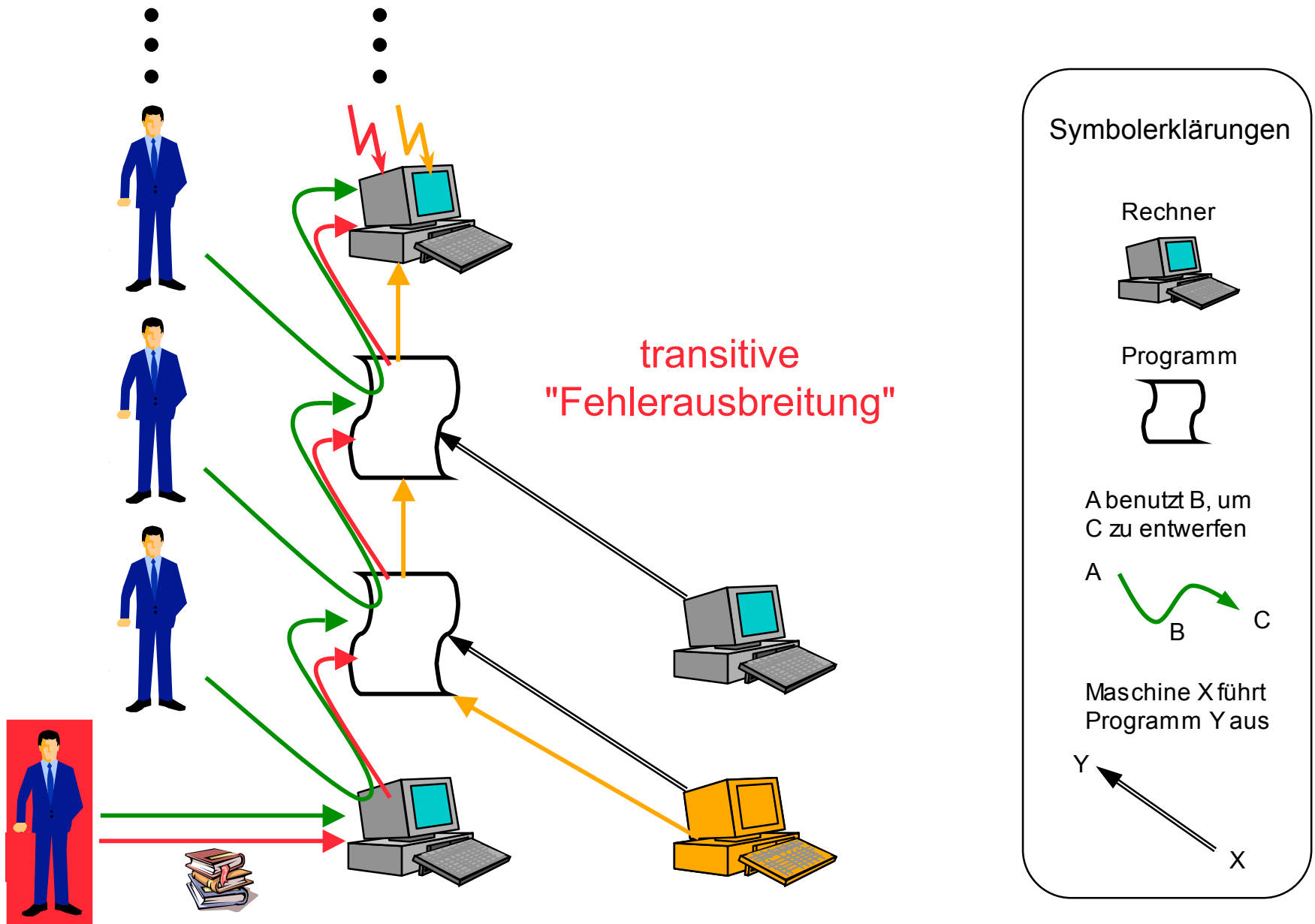
Informationen sind richtig, vollständig und aktuell oder aber dies ist erkennbar nicht der Fall.

## Verfügbarkeit (availability)

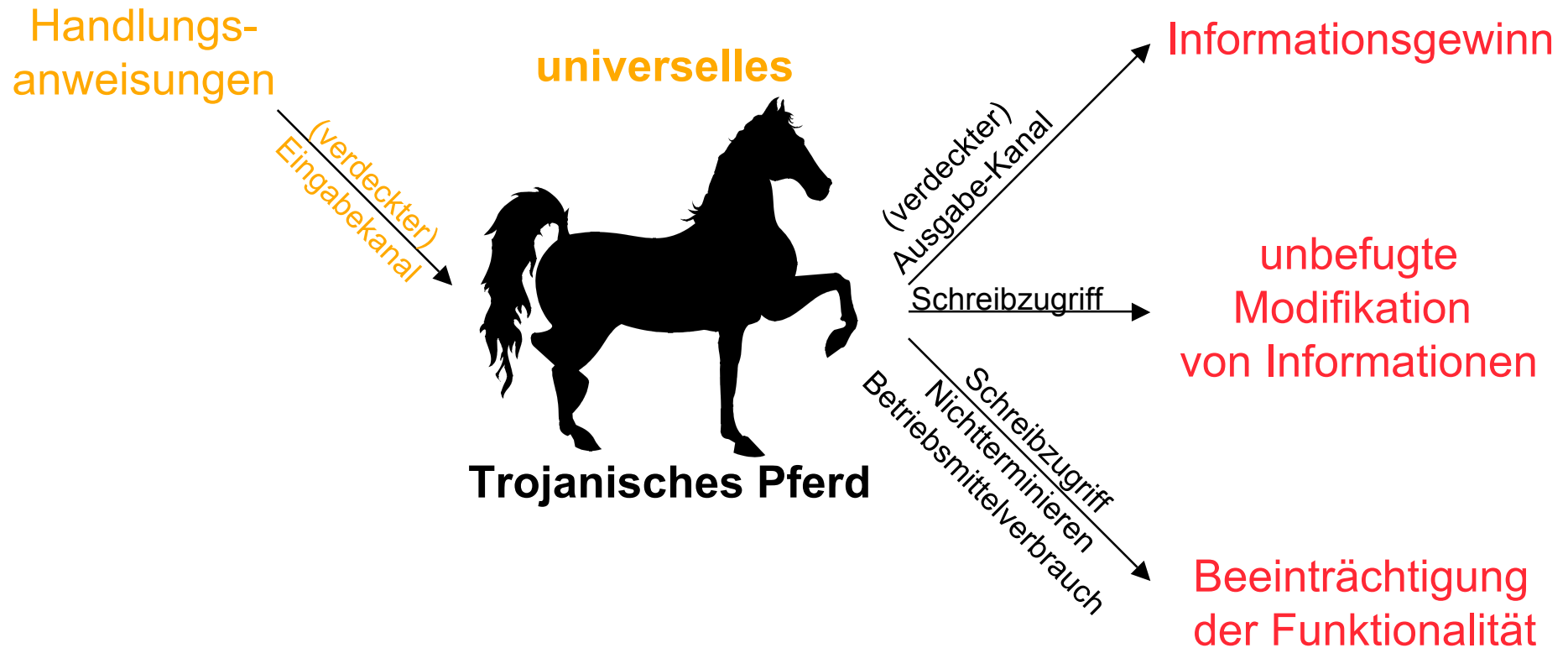
Informationen sind dort und dann zugänglich, wo und wann sie von Berechtigten gebraucht werden.

- subsumiert: Daten, Programme, Hardwarestrukturen
- es muß geklärt sein, wer in welcher Situation wozu berechtigt ist
- kann sich nur auf das Innere eines Systems beziehen

# Transitive Ausbreitung von Fehlern und Angriffen



# Universelles Trojanisches Pferd



# Vor wem ist zu schützen ?

## Naturgesetze und Naturgewalten

- Bauteile altern
- Überspannung (Blitzschlag, EMP)
- Spannungsausfall
- Überschwemmung (Sturmflut, Wasserrohrbruch)
- Temperaturänderungen ...

Fehler-  
toleranz

## Menschen

- Außenstehende
- Benutzer des Systems
- Betreiber des Systems
- **Wartungsdienst**
- **Produzenten** des Systems
- **Entwerfer** des Systems
- **Produzenten** der Entwurfs- und Produktionshilfsmittel
- **Entwerfer** der Entwurfs- und Produktionshilfsmittel
- **Produzenten** der Entwurfs- und Produktionshilfsmittel  
der Entwurfs- und Produktionshilfsmittel
- **Entwerfer** ... jeweils auch Benutzer,  
Betreiber,  
Wartungsdienst ... des verwendeten Systems

Trojanisches Pferd  
universell  
transitiv

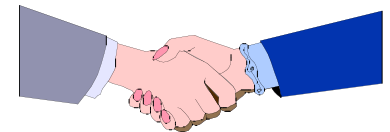
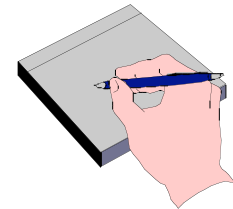
## Autonomie + Datensicherheit + Datenschutz

- Das christliche/humanistische Menschenbild und unser Grundgesetz haben als zentralen Wert die individuelle Person, ihre Würde, ihre Autonomie
  - Die klassische Datensicherheit ignoriert dies vollkommen: Ohnmächtige oder zumindest bevormundete Nutzer
  - Auch der klassische Datenschutz sieht Menschen weniger als intelligente autonome Wesen, denn als zu beschützende unmündige potentielle Opfer
- Für eine demokratische Wissensgesellschaft, die gerade auf der Autonomie der BürgerInnen beruht, brauchen wir ein grundlegend anderes Konzept !

# Mehrseitige Sicherheit

Sicherheit für alle Beteiligten, wobei jede(r) anderen nur minimal zu vertrauen braucht

- Jede(r) hat individuelle **Schutzziele**.
- Jede(r) kann seine Schutzziele **formulieren**.
- Konflikte werden erkannt und Kompromisse **ausgehandelt**.
- Jede(r) kann seine Schutzziele im Rahmen des ausgehandelten Kompromisses **durchsetzen**.





## Techniken für Mehrseitige Sicherheit



... haben das Potential,  
Nutzer von IT-Systemen von  
Fremdbestimmung bzgl. ihrer  
(Un-)Sicherheit zu befreien.

## Schutzziele für Kommunikation: Sortierung

	Inhalte	Umfeld
<b>Unerwünschtes verhindern</b>	<b>Vertraulichkeit Verdecktheit</b>	<b>Anonymität Unbeobachtbarkeit</b>
<b>Erwünschtes leisten</b>	<b>Integrität</b>	<b>Zurechenbarkeit</b>
	<b>Verfügbarkeit</b>	<b>Erreichbarkeit Verbindlichkeit</b>

## Schutzziele für Kommunikation: 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.

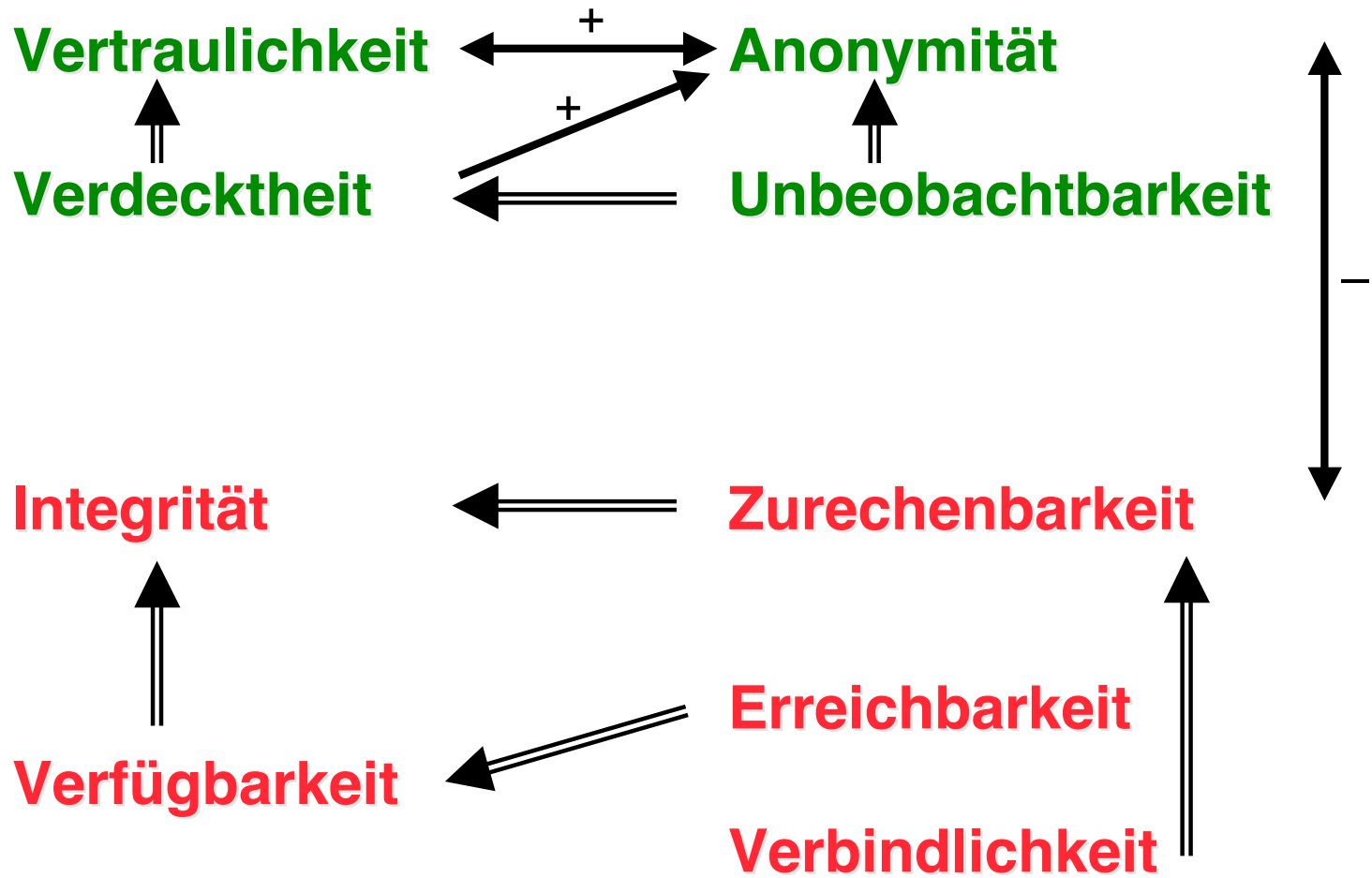
---

**Verfügbarkeit:** Nutzbarkeit von Diensten und Ressourcen, wenn gewünscht.

**Erreichbarkeit:** Zu einer Ressource oder einem Nutzer kann Kontakt aufgenommen werden, wenn gewünscht.

**Verbindlichkeit:** Ein Nutzer kann rechtlich belangt werden, um seine Verantwortlichkeiten innerhalb einer angemessenen Zeit zu erfüllen.

# Wechselwirkungen zwischen Schutzzielen



==> impliziert      + -> verstärkt      - -> schwächt

# Unilateral nutzbare Techniken

Werkzeuge, die selbst unerfahrenen Nutzern helfen,  
ihre Schutzziele zu formulieren


Custom protection goals - Order

Set goals for:


Privacy Correctness

**Content**

**should be confidential**


  unconditional  negotiable  
 if possible  
 don't care  
 if necessary  
 on no condition  negotiable

**should be hidden**


  unconditional  negotiable  
 if possible  
 don't care  
 if necessary  
 on no condition  negotiable

**I want**

**to be anonymous**


  unconditional  negotiable  
 if possible  
 don't care  
 if necessary  
 on no condition  negotiable

**to be unobservable**

  unconditional  
 if possible  
 don't care  
 if necessary  
 on no condition

**My partner should**

**be anonymous**

  unconditional  negotiable  
 if possible  
 don't care  
 if necessary  
 on no condition  negotiable

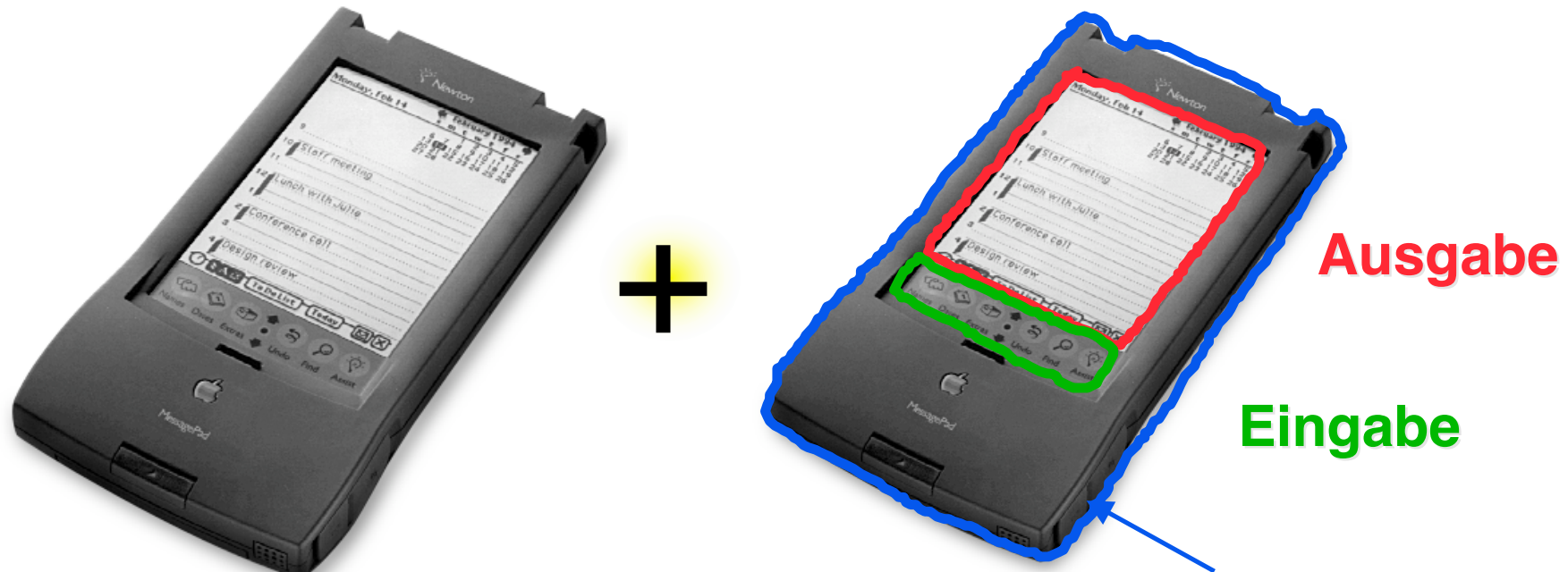
Reset to:

high security medium security low security

OK Cancel Help

# Unilateral nutzbare Techniken

(Portable) Geräte, die für ihre Benutzer sicher sind,  
als Basis jeder Sicherheit

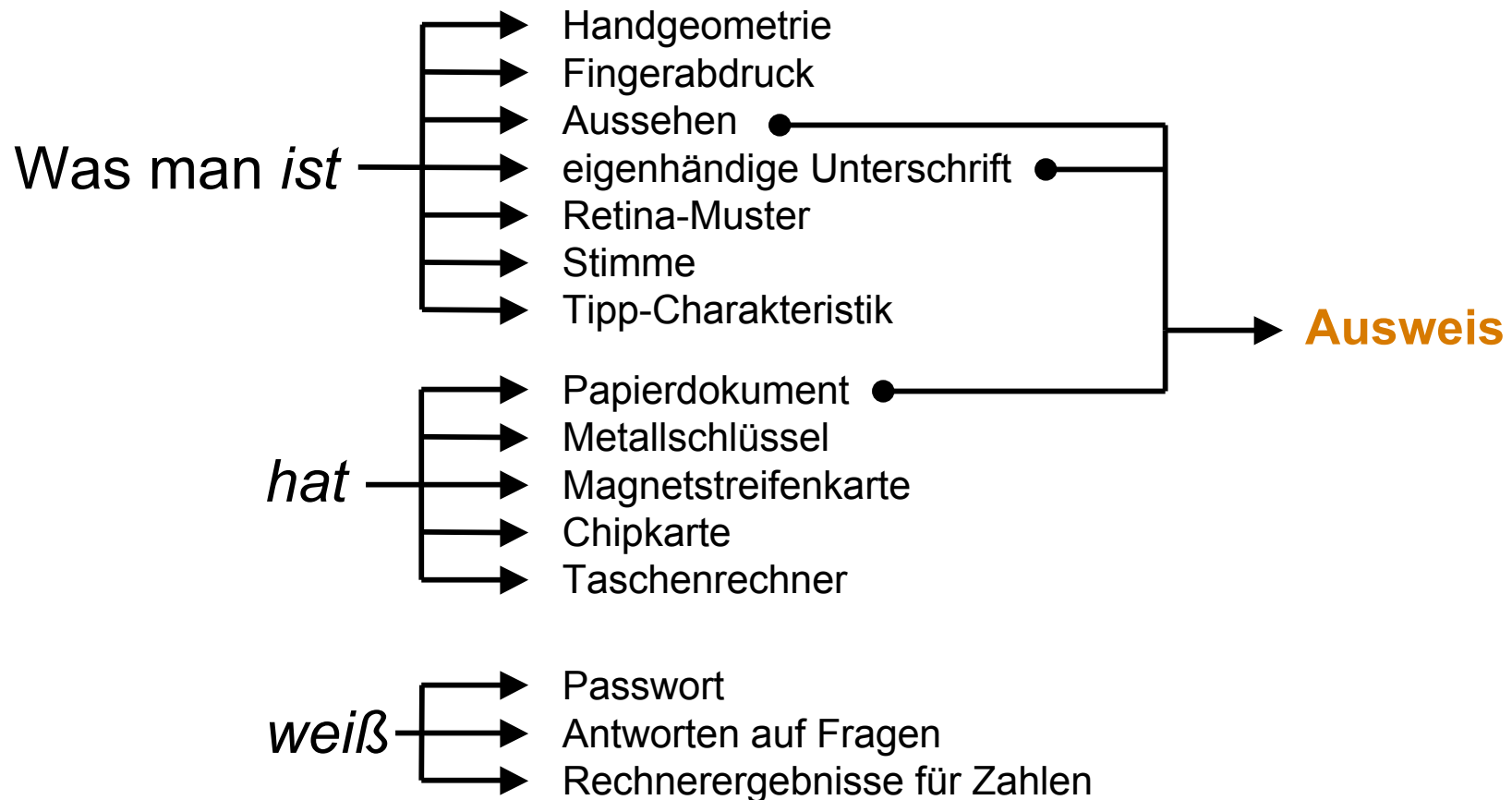


**falls mehrere Anwendungen:  
Betriebssystem mit feingestuf-  
ter Zugriffskontrolle nach dem  
Prinzip der geringstmöglichen  
Privilegierung**

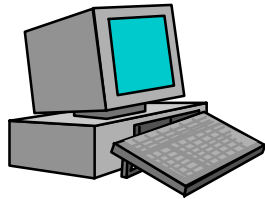
# Unilateral nutzbare Techniken



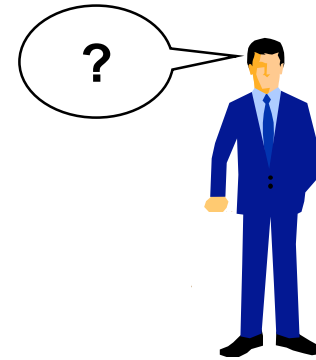
## Identifikation von Menschen durch IT-Systeme



# Unilateral nutzbare Techniken



## Identifikation von IT-Systemen durch Menschen



Was es *ist*

- Gehäuse
- Siegel, Hologramm
- Verschmutzung

*weiß*

- Passwort
- Antworten auf Fragen
- Rechnerergebnisse für Zahlen

Wo es *steht*



## Unilateral nutzbare Techniken

### Kryptographie

- Verschlüsselung lokaler Speichermedien, um die Inhalte vertraulich zu halten und/oder zu authentisieren

### Steganographie

- Verstecken von Daten, um sogar ihre Existenz geheimzuhalten
- Watermarking oder Fingerprinting dig. Daten, um Autorschaft oder Urheberrechtsverletzungen besser nachweisen zu können

### Rigorese Überprüfung

- Ausschließliche Benutzung von Software, deren Quellcode veröffentlicht und von vielen inspiziert ist oder die von vertrauenswürdigen unabhängigen Agenturen zertifiziert ist, die Zugriff auf den Quellcode und alle Tools zur Generierung des Objektcodes hatten.

# Unilateral nutzbare Techniken

## Kryptographie

Regulierungsversuche sind weitestgehend sinnlos, da „Kriminelle“ dann auf Steganographie ausweichen.

## Steganographie

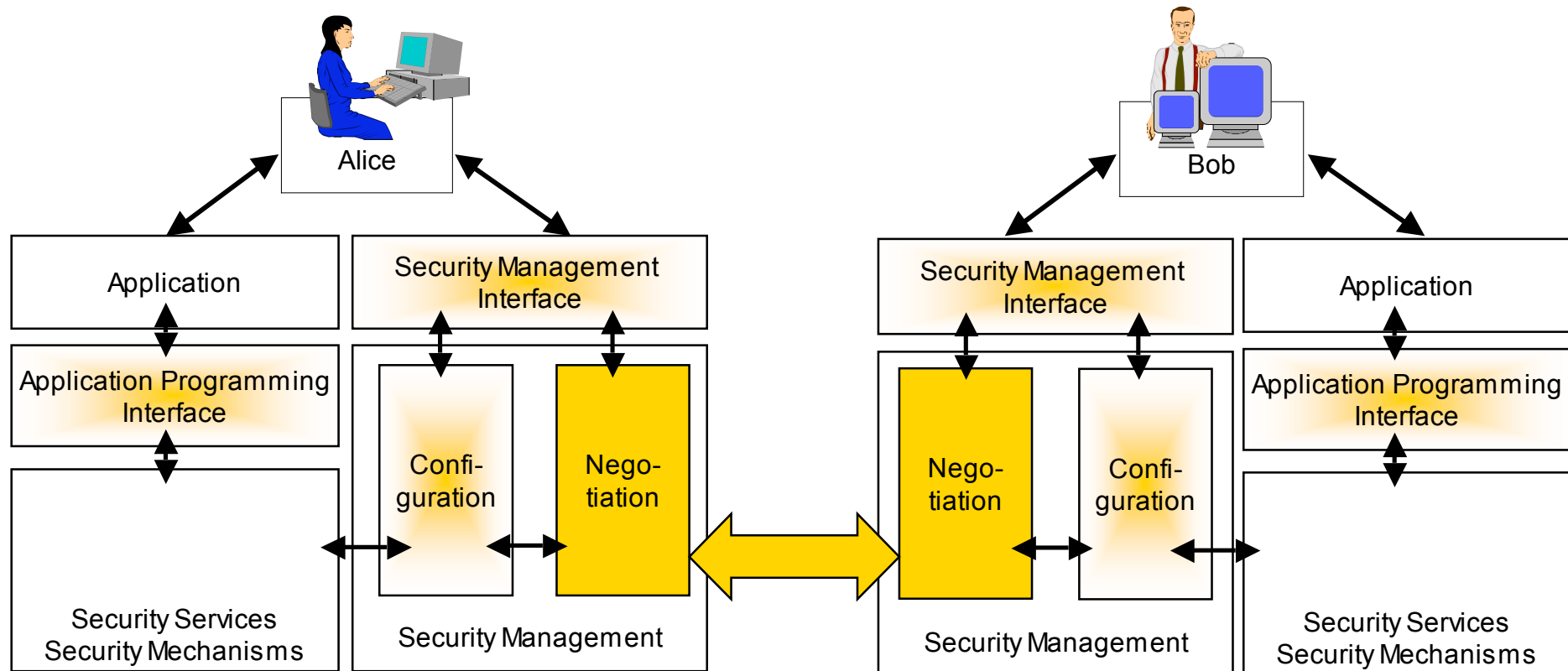
Regulierungsversuche sind weitestgehend sinnlos.

## Rigoreuse Überprüfung

Regulierungsversuche sind weitestgehend sinnlos – die „Bedarfsträger“ brauchen die sicheren IT-Systeme selbst.

# Bilateral nutzbare Techniken

Werkzeuge, um Schutzziele und Sicherheitsmechanismen bilateral auszuhandeln



# Bilateral nutzbare Techniken

## Identifikation von IT-Systemen durch IT-Systeme



Was es *weiß*

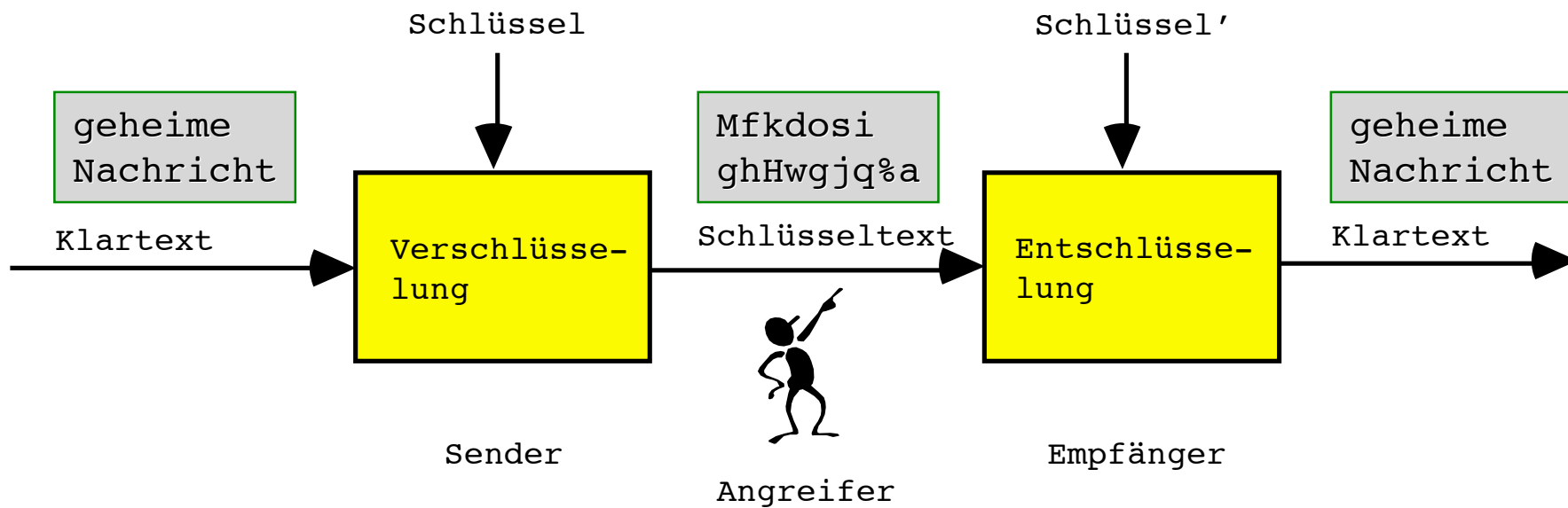
- Passwort
- Antworten auf Fragen
- Rechnerergebnisse für Zahlen
- **Kryptographie**

Leitung *woher*

# Bilateral nutzbare Techniken

Kryptographische Mechanismen, um  
Kommunikationsinhalte zu schützen

**Ziel: Vertraulichkeit und/oder Authentizität**

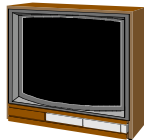


# Beobachtbarkeit in Vermittlungsnetzen

Radio



Fernsehen



Bildtelefon



Telefon



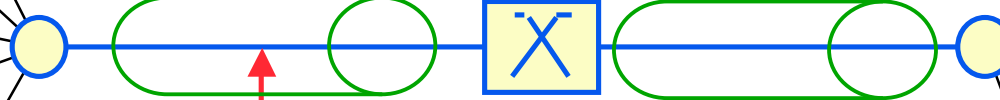
Internet



Gegenmaßnahme Verschlüsselung

- Verbindungs-Verschlüsselung

Netzanschluß



~~Abhörer~~  
**mögliche  
Angreifer**

Vermittlungsstelle

- Betreiber
- Hersteller (Trojanisches Pferd)
- Angestellte

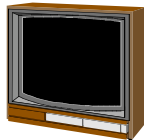


# Beobachtbarkeit in Vermittlungsnetzen

Radio



Fernsehen



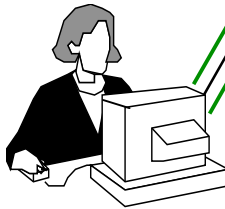
Bildtelefon



Telefon



Internet



Gegenmaßnahme Verschlüsselung

- Ende-zu-Ende-Verschlüsselung

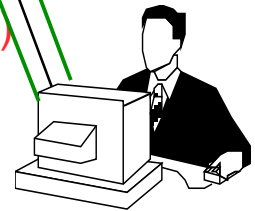
Netzabschluß

Abhörer

**mögliche  
Angreifer**

Vermittlungsstelle

- Betreiber
- Hersteller (Trojanisches Pferd)
- Angestellte



# Beobachtbarkeit in Vermittlungsnetzen

Radio



Fernsehen



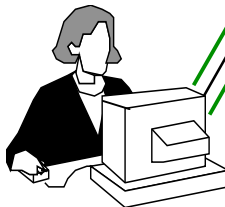
Bildtelefon



Telefon



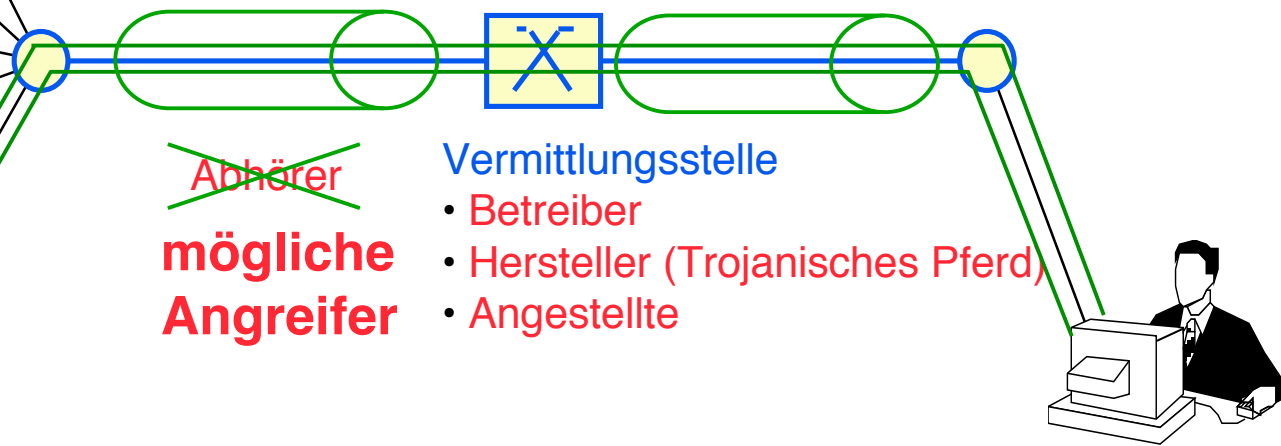
Internet



Gegenmaßnahme Verschlüsselung

- Verbindungs-Verschlüsselung
- Ende-zu-Ende-Verschlüsselung

Netzanschluß



~~Abhörer~~  
**mögliche Angreifer**

Vermittlungsstelle

- Betreiber
- Hersteller (Trojanisches Pferd)
- Angestellte

Kommunikationspartner

**Problem:** Verkehrsdaten  
wer mit wem?  
wann? wie lange?  
wieviel Information?

Interessendaten : Wer? Was?

**Ziel:** Verkehrsdaten (und damit auch Interessendaten)  
dadurch "schützen", dass sie nicht erfasst werden können.



## Bilateral nutzbare Techniken

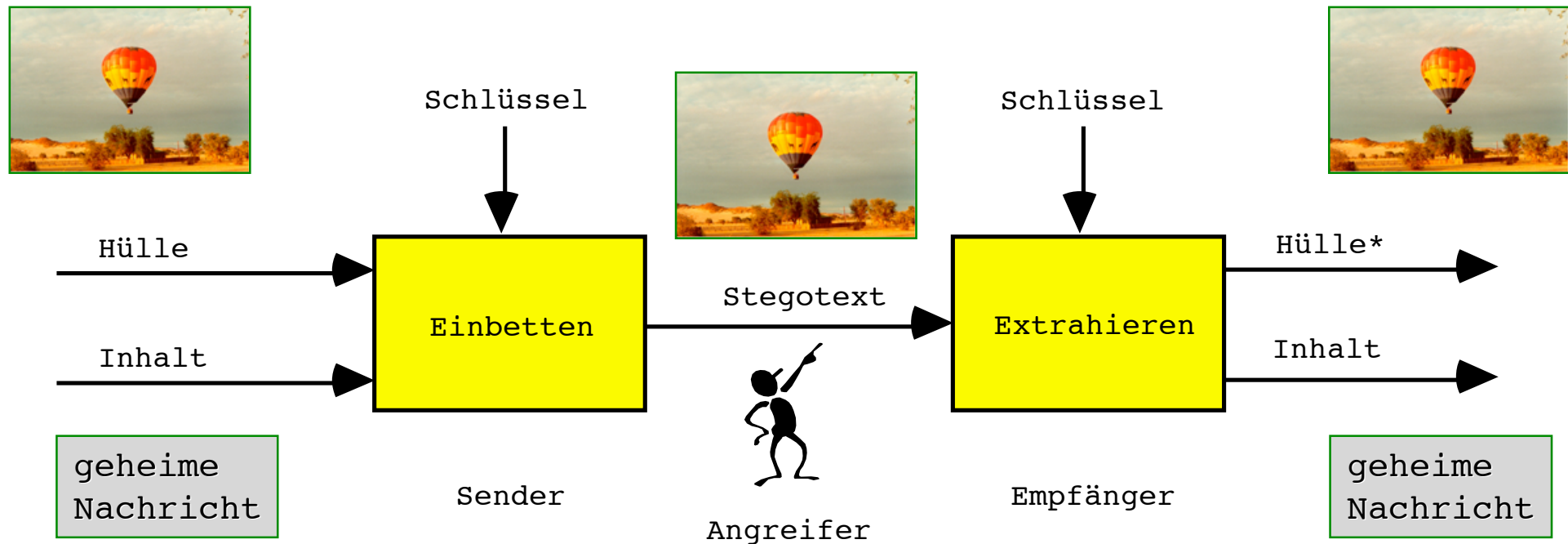
### Kryptographie

Regulierungsversuche sind völlig sinnlos,  
da „Kriminelle“ dann auf Steganographie ausweichen.

# Bilateral nutzbare Techniken

Steganographische Mechanismen, um  
Kommunikationsinhalte zu schützen

**Ziel: Vertraulichkeit der Vertraulichkeit**



## Bilateral nutzbare Techniken

### **Steganographie**

Regulierungsversuche sind völlig sinnlos,  
da Übertretung nicht erkennbar.

# Trilateral nutzbare Techniken

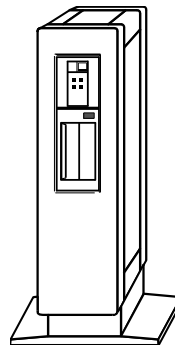
- Werkzeuge, um trilateral auszuhandeln, z.B. für Zurechenbarkeit
- Public-Key-Infrastrukturen
- Sicherheitsgateways

*Abstraktionsebenen*

Schutzziele

Mechanismen

Mechanismen-  
details



Sicherheitsgateway

Schutzziele

Mechanismen

Mechanismen-  
details

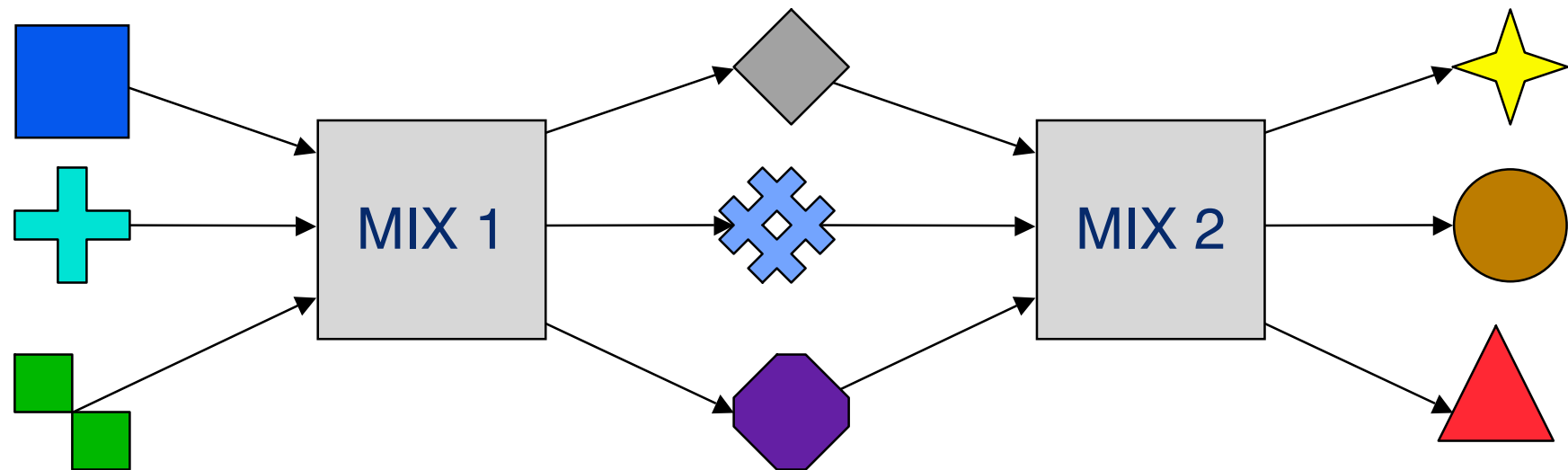
## Multilateral nutzbare Techniken

- Werkzeuge, um multilateral auszuhandeln, z.B. für Anonymität, Unbeobachtbarkeit und Pseudonymität
- Mechanismen, um Anonymität, Unbeobachtbarkeit und Unverkettbarkeit zu erreichen bei
  - Kommunikation, d.h. zu schützen, wer, wann, von wo, mit wem wohin kommuniziert,
  - Zahlungen, d.h. zu schützen, wer wann an wen welchen Betrag zahlt, und
  - Wertaustausch, d.h. elektronisches Einkaufen gegen Beobachtung zu schützen
- Pseudonymität, d.h. Anonymität und Zurechenbarkeit kombiniert, sowie ggf. Übertragung von Signaturen zwischen verschiedenen Pseudonymen derselben Instanz

# Multilateral nutzbare Techniken

Anonymität, Unbeobachtbarkeit und Unverkettbarkeit bei Kommunikation:

## MIXe



### Funktionen jedes MIXes:

- Puffern
- Wiederholungen ignorieren
- Umcodieren
- Umsortieren

→ verbirgt so die Beziehung zwischen ein- und ausgehenden Nachrichten

# Multilateral nutzbare Techniken

## Schutz des Empfängers: Verteilung

Leistung?

leistungsfähigeres Übertragungssystem

Adressierung

(wo möglich: Kanäle schalten)

explizite Adressen:

Routing

implizite Adressen:

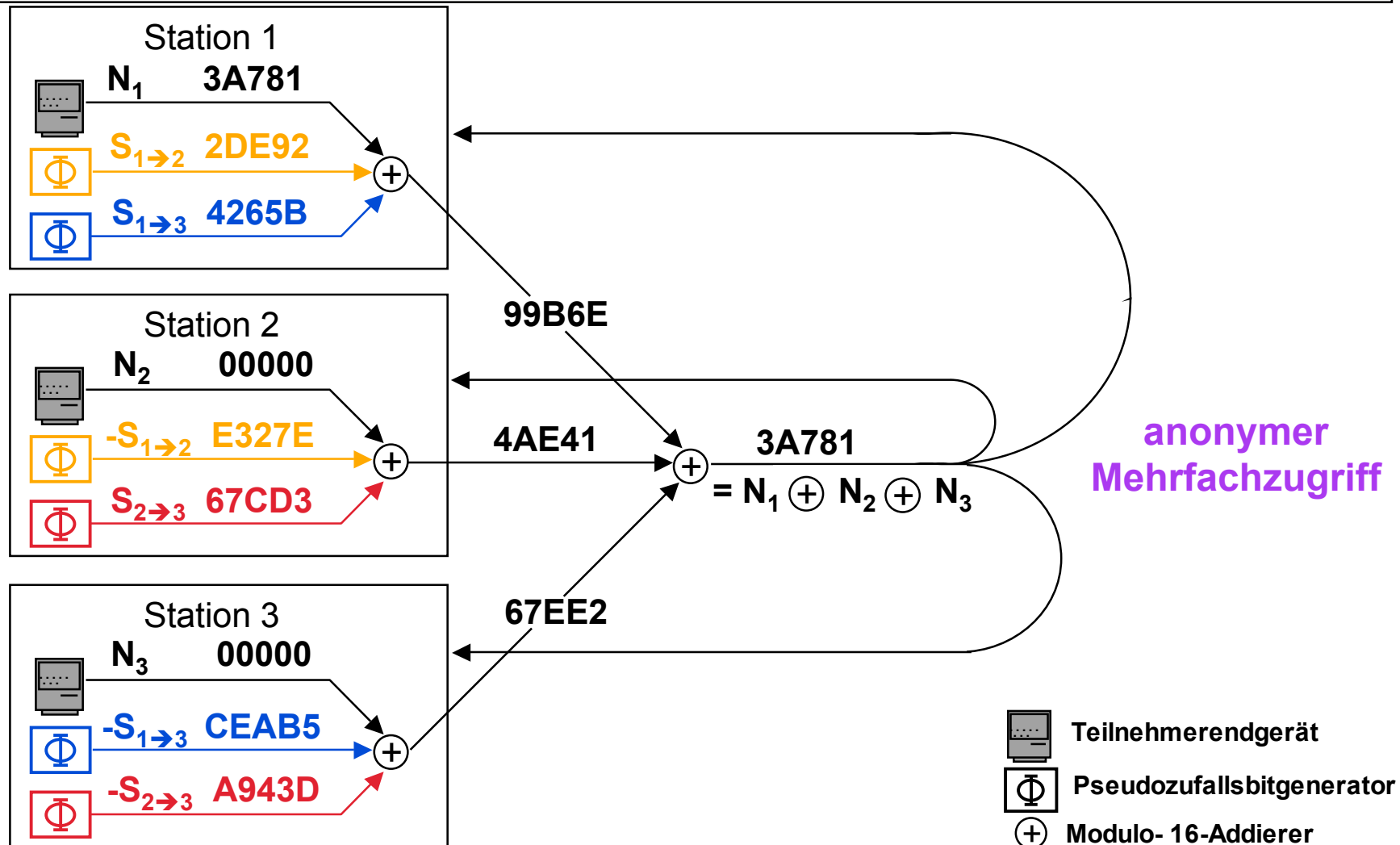
Merkmal für Station des Adressaten

verdeckt <==> Konzelationssystem

offen Bsp. Zufallszahlen(generator)

		Adressverwaltung	
		öffentliche Adresse	private Adresse
implizite Adres- sierung	verdeckt	sehr aufwändig, für Kontaktaufnahme nötig	aufwändig
	offen	abzuraten	nach Kontaktaufnahme ständig wechseln

# Multilateral nutzbare Techniken



## Überlagerndes Senden: Anonymität des Senders

Hängen Stationen durch geheime Schlüssel zusammen,  
 liefert Abhören aller Leitungen keine zusätzliche Information.



## Multilateral nutzbare Techniken

**Öffentliche Telefone,  
Prepaid Telefone,  
offene WLANs,  
unsichere Bluetooth-Mobilfunkgeräte,**

...

Vorratsdatenspeicherung ist weitestgehend sinnlos,  
da „Kriminelle“ dann ausweichen, s.o.

## Pseudonyme: Initialer Personenbezug

### **Öffentliches Pseudonym:**

Bezug zwischen Pseudonym und seinem Inhaber von Beginn an öffentlich bekannt.

Telefonnummer mit Inhaber im Telefon“buch“ gelistet

### **Initial nicht-öffentliches Pseudonym:**

Bezug zwischen Pseudonym und seinem Inhaber ist zu Beginn zwar manchen (**Identitätstreuhänder**), aber nicht allen bekannt.

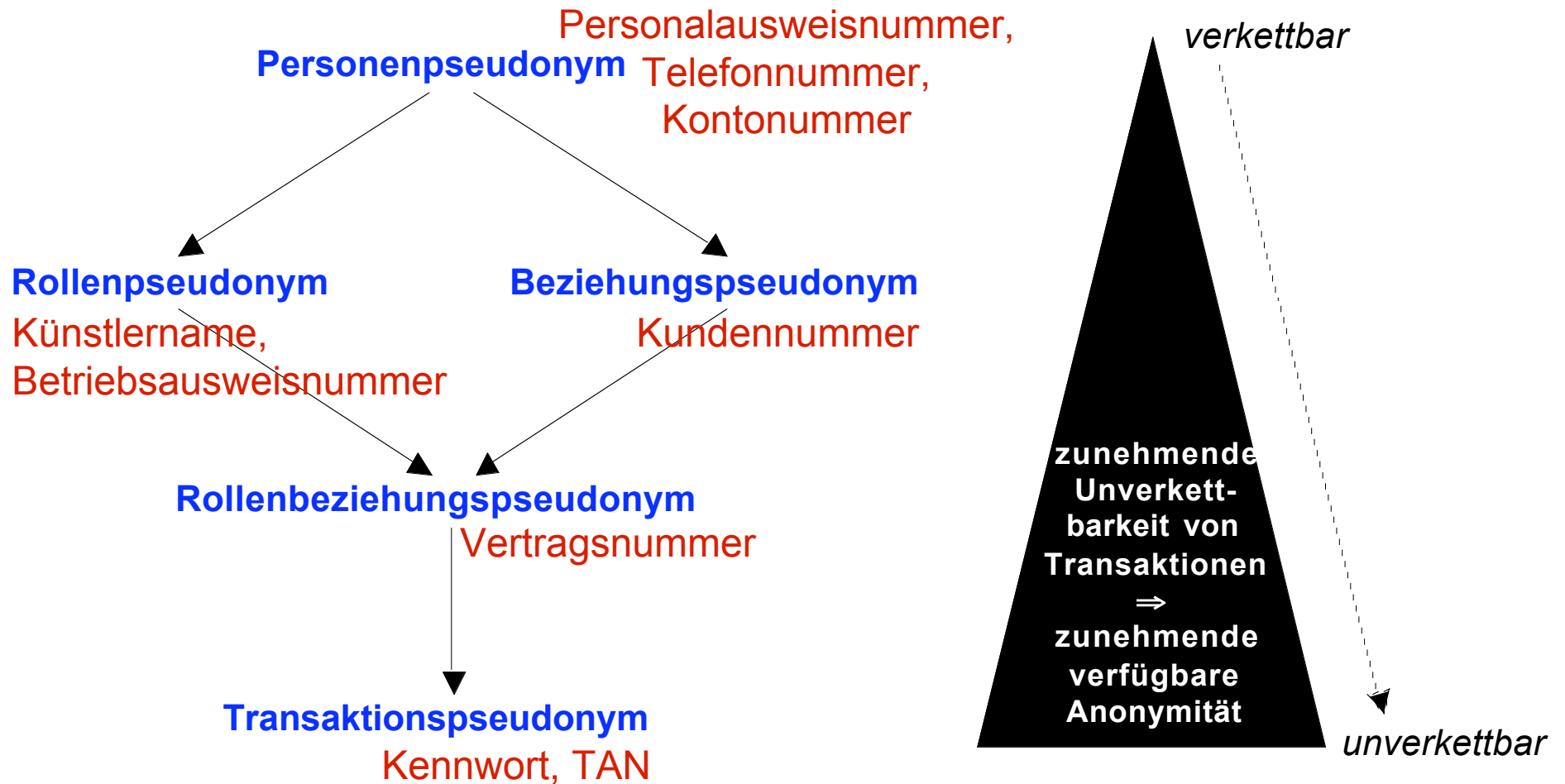
Kontonummer mit Bank als Identitätstreuhänder,  
Kreditkartennummer ...

### **Initial unverkettbares Pseudonym:**

Bezug zwischen Pseudonym und seinem Inhaber ist zu Beginn nur dem Inhaber bekannt.

Biometrische Merkmale; DNA (solange keinerlei Register)

# Pseudonyme: Verwendungszusammenhang



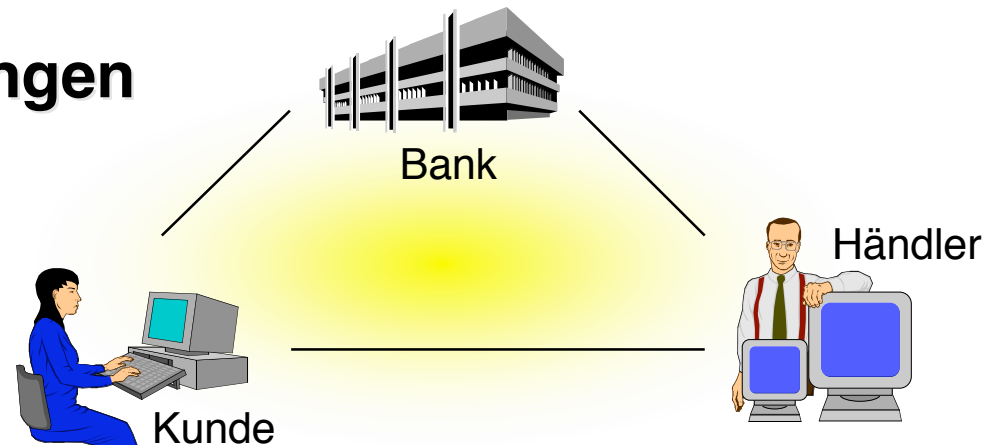
$A \rightarrow B$  bedeutet „B ermöglicht stärkere Anonymität als A“

# Multilateral nutzbare Techniken

## Digitale Signaturen relativ zu einem Pseudonym

**Digitales Pseudonym** = Public Key zum Testen digitaler Signaturen

## Pseudonyme digitale Zahlungen



## Wertaustausch zwischen pseudonymen Partnern

- Identifizierung bei Betrug (**initial nicht-öffentliche Pseudonyme** sind zertifiziert und Zertifizierer kennt reale Identität, d.h. **Identitätstreuhänder**): Anonymitätseigenschaft ist durch Pseudonyminhaber nicht überprüfbar
- Geldhinterlegung bei aktivem **Wertetreuhänder**, um Betrug selbst bei vollständig anonymen, d.h. **initial unverkettbaren Pseudonymen** zu verhindern: Anonymitätseigenschaft ist durch Pseudonyminhaber überprüfbar

# Bewertung von Reife und Effektivität

	Stand der öffentlichen Forschung	Demonstratoren und Prototypen	Verfügbare Produkte	Weit verbreitete Produkte
<b>Physischer Schutz</b>	kaum seriöse Publikationen	schwer zu beurteilen	schwer zu beurteilen; Me-Chip	sehr schlecht; Chipkarten
<b>Sicherheitsevaluierung von SW und HW</b>	akzeptabel	schwer zu beurteilen	schwer zu beurteilen	schwer zu beurteilen
<b>Sicherheit in Betriebssystemen</b>	sehr gut	gut	schlecht; WinNT, 2000, XPprof., Linux, MacOS X	sehr schlecht; Win 95, 98, ME, CE, Mobile, XPhone, MacOS 9, Symbian, PalmOS
<b>Kryptographie</b>	sehr gut	gut	gut; PGP 2.6	akzeptabel; PGP 5.x, 6.x
<b>Steganographie</b>	gut	akzeptabel	schlecht	sehr schlecht
<b>PKI</b>	sehr gut	gut	schwer zu beurt.	schwer zu beurt.
<b>Mechanismen für Anonymität, Unbeobachtbarkeit und Unverkettbarkeit</b>	sehr gut	gut	akzeptabel; TOR, JAP	schlecht; Proxies
<b>Werkzeuge, die beim Formulieren und Verhandeln helfen</b>	gut	akzeptabel	-	-
<b>Integration dieser Techniken</b>	akzeptabel	schlecht	schlecht	sehr schlecht

*unilateral nutzbar*

*bilateral nutzbar*

*trilateral nutzbar*

*multilateral nutzbar*

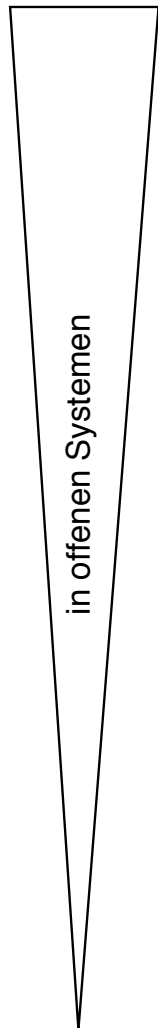
# Datenschutzprinzipien: Datenschutz durch Technik

## Vertraulichkeit

## Korrektheit

Maßnahme

stark



schwach

### unnötige Daten vermeiden

- Erfassungsmöglichkeit
- Erfassung
- Verarbeitung
- Speicherung

### Verwendungsmöglichkeit notwendiger Daten einschränken

- Transaktionspseudonyme
- Rollenbeziehungspseudon.
- Rollen-, Beziehungspseudon.
- Personenpseudonyme
- Credential-Mechanismus
- digitale Pseudonyme

### Verwendung notwendiger Daten einschränken

- verteilte Speicherung
- Protokollierung
- Organisation
- Vorschriften

--

### Überprüfung der Daten durch Betroffenen bei jeder Verwendung

- Betroffener online + dig. Signaturen: Kommunikation via Betroffener

### Überprüfbarkeit der Daten durch Betroffenen

- mobiles Datenverarbeitungssystem
- bei jeder Verwendung Mitteilung an Betroffenen
- abfragbares Log-File
- Auskunftsrecht