Abschlussvortrag Projekt AN.ON

→

Zukunftsskizze Anonymität im Netz

Prof. Dr. Andreas Pfitzmann
TU Dresden, Fakultät Informatik, D-01062 Dresden
Nöthnitzer Str. 46, Raum 3071
Tel.: 0351/ 463-38277, e-mail: pfitza@inf.tu-dresden.de, http://dud.inf.tu-dresden.de/

Diskussions-Merker

Ein-Knopf-Anonymität – geht nicht, aber automatische Basissicherheit schon

Verbrechensaufklärung im Cyberspace
Unterscheide Internetstraftaten nach

- Ziel des Verbrechens ist Cyberspace -> Sichere IT-Systeme verwenden
- Cyberspace als Transit -> Ermittlungsmöglichkeiten außerhalb nutzen

Bsp. Drohung per E-Mail, Argument: IP-Adresse einziges Ermittlungshilfsmittel
-> wenn die E-mail das einzige auf der Welt diesbezüglich ist, dann einfach ignorieren;
Ggf. Argument auch umkehren: Wenn Anonymität der E-Mail nicht garantiert, dann keine Bombenwarnung mehr, zumindest nicht per E-Mail

Anonymität der Teilnahme am Anonymitätsdienst: Es reicht Beweis, dass bezahlt;
Problem: Psychologie der naiven Teilnehmer

Vertrauen kann nicht gefordert werden, Vertrauen wird „geschenkt“ – oder auch nicht.

Anonymität gefordert (TDDSG) – wird diese gesetzliche Pflicht ernst genommen, wenn die Innenminister Manfred Kanther, Otto Schily, ... Und jede Lobby-Gruppe ihr Gesetz bekam TDDSG vs. G10-Gesetz und TKÜV

Kommerzialisierung der Strafverfolgung im Internet vs. kostengünstige Hilfssheriffs

Ist Deutschland ein autonomer Staat – oder haben wir seit 1945 einen sehr Grossen Bruder jenseits des Atlantiks? Vgl. Echelon, SWIFT

Danke an die bisher unerwähnten AN.ONs

Stefan Köpsell

Oliver Berthold

Heinrich Langos

Sandra Steinbrecher

Claudia Golembiewski

Rolf Wendolsky

Martin Rost

Henry Krasemann

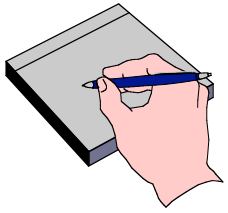
Gliederung

- Mehrseitige Sicherheit in verteilten und durch verteilte Systeme
  - Bedarf Anonymität – schwer fassbar
  - Gemeinwohl – wer zahlt?
  - Hintertüren für eigene Bedarfsträger werden Hintertüren für fremde Bedarfsträger werden Hintertüren für organisierte Kriminalität
  - Bedarf „Freie Informierbarkeit“ – auch schwer fassbar
- Technische und wirtschaftliche Entwicklungslinien
  - Internationalisierung der Infrastruktur
  - P2P
  - Mobilität
  - Dienste: Web, e-mail → IM, VoIP, Video, ...
  - Extreme Verteilung: MIXe → Überlagerndes Senden (DC-Netz)
  - Integration mit Identitätsmanagement
- Verbrechensverhinderung besser als -aufklärung
  - Sicherer E-Commerce trotz starker Pseudonymität (1985..1990)
  - Sperren illegaler Inhalte
- Balancierung „Privatheit ⇔ Überwachung“ anwendungsübergreifend !
  - Data Retention weitgehend wirkungslos und keinesfalls kosteneffizient
    - Offene Proxies im nicht-kooperierenden Ausland
    - Internationalisierung oder gar „Auswanderung“ von AN.ON, TOR, ...
    - Offene WLANs, Bluetooth-Geräte
  - Überwachungsfreie Räume: für die menschliche Entwicklung nötig und ein Sicherheitsgewinn für die Gesellschaft

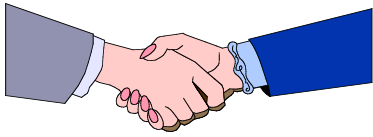
Mehrseitige Sicherheit

- Jeder Beteiligte hat Sicherheitsinteressen.

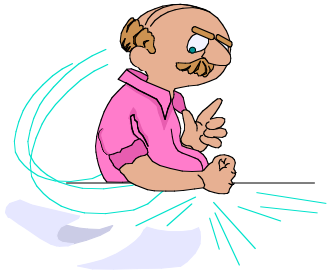
- Jeder Beteiligte kann seine Interessen formulieren.



- Konflikte werden erkannt und Lösungen ausgehandelt.



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



Sicherheit mit minimalen Annahmen über andere

Schutzziele: Sortierung

	Inhalte	Umfeld
Unerwünschtes verhindern	Vertraulichkeit Verdecktheit	Anonymität Unbeobachtbarkeit
Erwünschtes leisten	Integrität	Zurechenbarkeit
	Verfügbarkeit	Erreichbarkeit Verbindlichkeit

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.

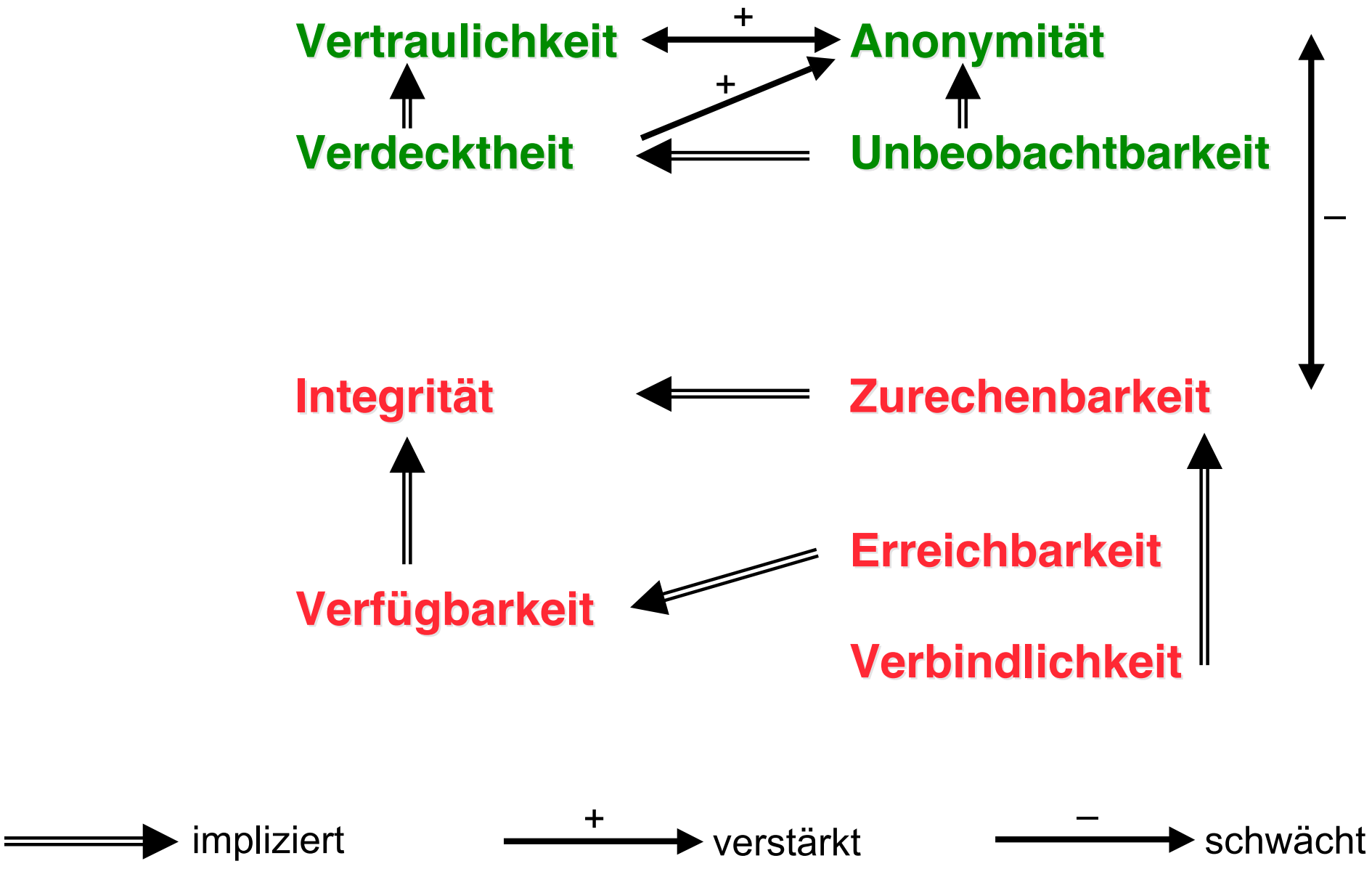
Zurechenbarkeit: Sendern bzw. Empfängern von Informationen kann das Senden bzw. der Empfang der Informationen bewiesen werden.

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.

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

Wechselwirkungen zwischen Schutzzielen



Implementierung mehrseitiger Sicherheit

Damit keine strukturellen Sicherheitslücken (SysOp, ...),

mehrseitige Sicherheit

- in verteilten und
- durch verteile

Systeme realisieren !

Gestaltungsfeld Anonymität

Bedarf Anonymität – schwer fassbar

- Bedarfserkenntnis oft erst, wenn es zu spät ist
- Individualbedarf vs. Gemeinschaftsbedarf
  (ohne Anonymität keine Demokratie, vgl. Begründung des Volkszählungsurteils des BVG von 1983)

Individualinteresse – wer zahlt? Bürger, Firmen, Bedarfsträger (Polizei, Dienste, ...)
Gemeinwohl – wer zahlt? ??? (Verursacherprinzip: Wer an Techniken zur Identifizierung und Archivierung verdient?)

Anonymität in der Kommunikation

- Generelle Anonymität ist technisch effizienter als individuelle
- Individuelle Anonymität hat Diskriminierungseffekt
- → Anonymität ist zentrales Grundrecht

Hintertüren für eigene Bedarfsträger

... werden Hintertüren für fremde Bedarfsträger
(z.B. für deren Informationsbeschaffung und für deren Enttarnung von Agenten)

... werden Hintertüren für organisierte Kriminalität
(z.B. zur Unterwanderung von Zeugenschutzprogrammen; Erkennen von verdeckten Ermittlern)

Bedarf „Freie Informierbarkeit“ = Umgehbarkeit von Zensur – auch schwer fassbar

Technische und wirtschaftliche Entwicklungslinien

Internationalisierung der Infrastruktur

P2P, genauer: Konvergenz von Client/Server und Peer-to-Peer

Mobilität

Dienste: Web, e-mail → IM, VoIP, Video, ...

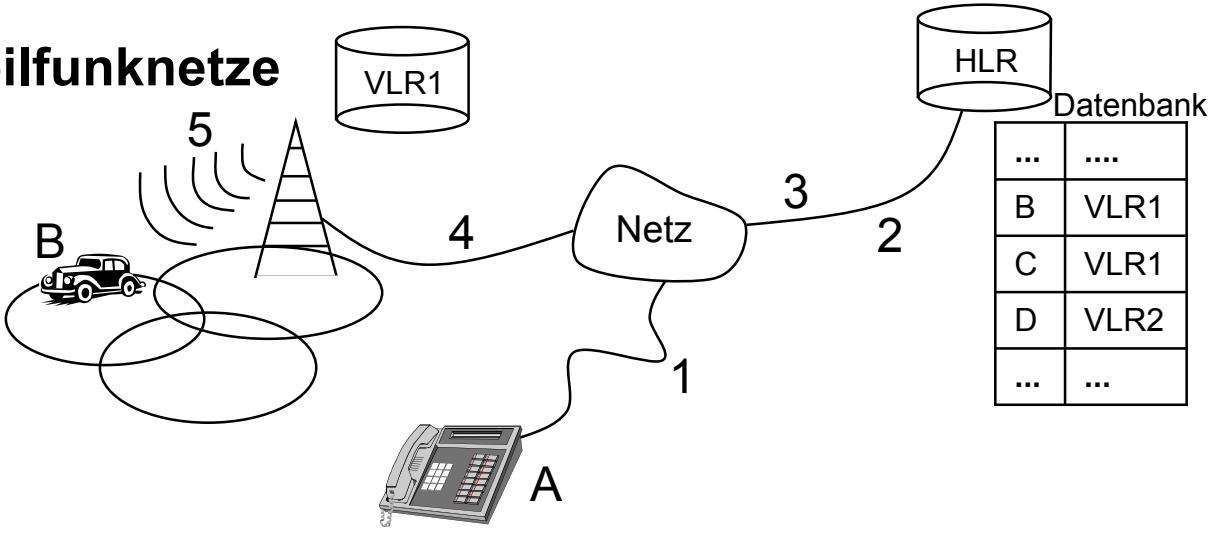
Extreme Verteilung: MIXe → Überlagerndes Senden

Integration mit Identitätsmanagement

Keine Bewegungsprofile in Funknetzen

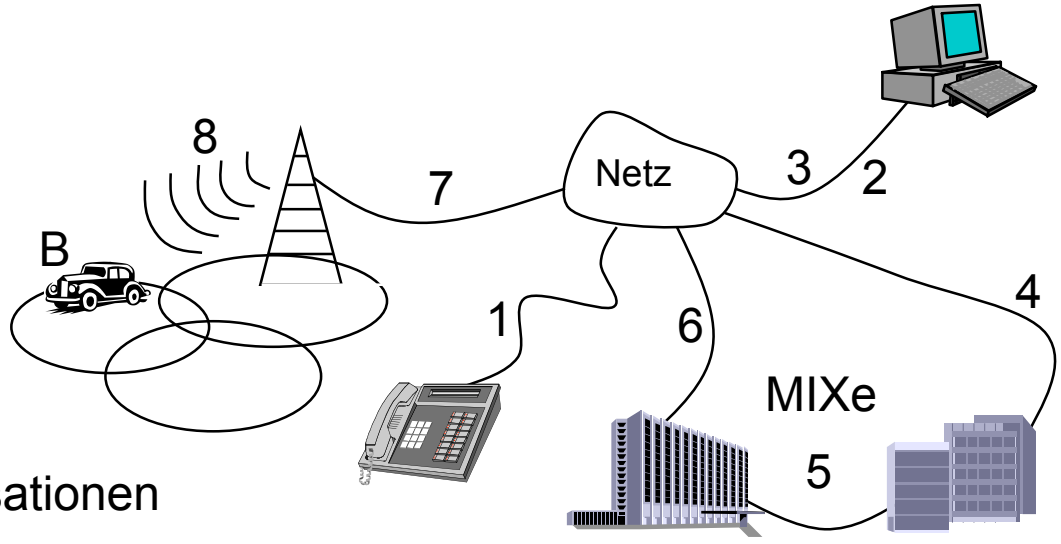
GSM/UMTS – zellulare Mobilfunknetze

- Aufenthaltsinformation in zentrale Datenbanken
- Netzbetreiber können die Information erfassen



Alternatives Konzept

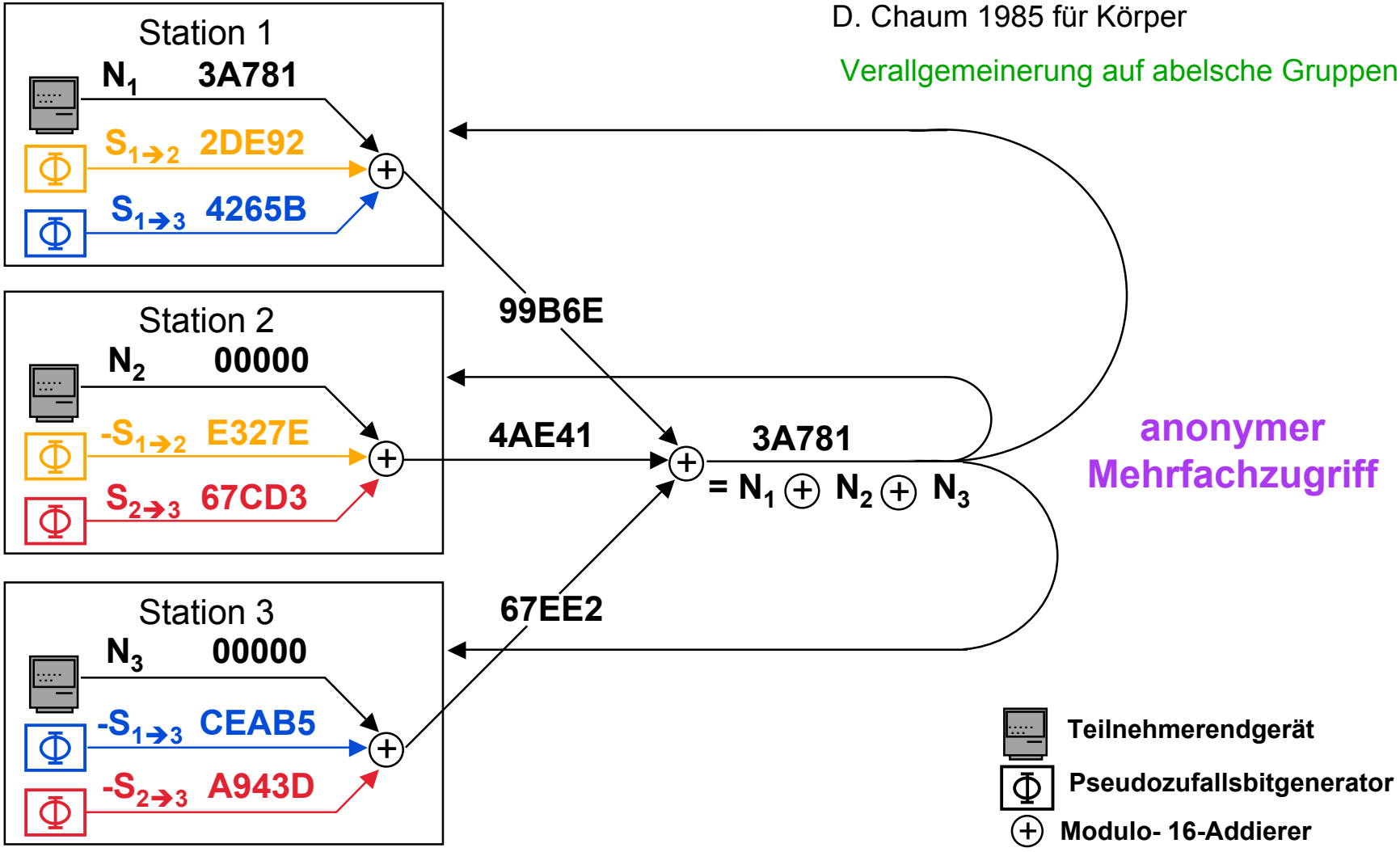
- Verwaltung der Aufenthalts-information in vertrauenswürdiger Umgebung
  - zu hause (HPC)
  - bei vertrauenswürdigen Organisationen
- Schutz der Kommunikationsbeziehung durch MIXe



Überlagerndes Senden (DC-Netz)

D. Chaum 1985 für Körper

Verallgemeinerung auf abelsche Gruppen



Anonymität des Senders

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

Identitätsmanagement

Wählbare Pseudonyme statt fest vergebener Namen

Unterscheidung Pseudonyme nach:

1. Initialer Personenbezug
2. Verwendungszusammenhang

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.

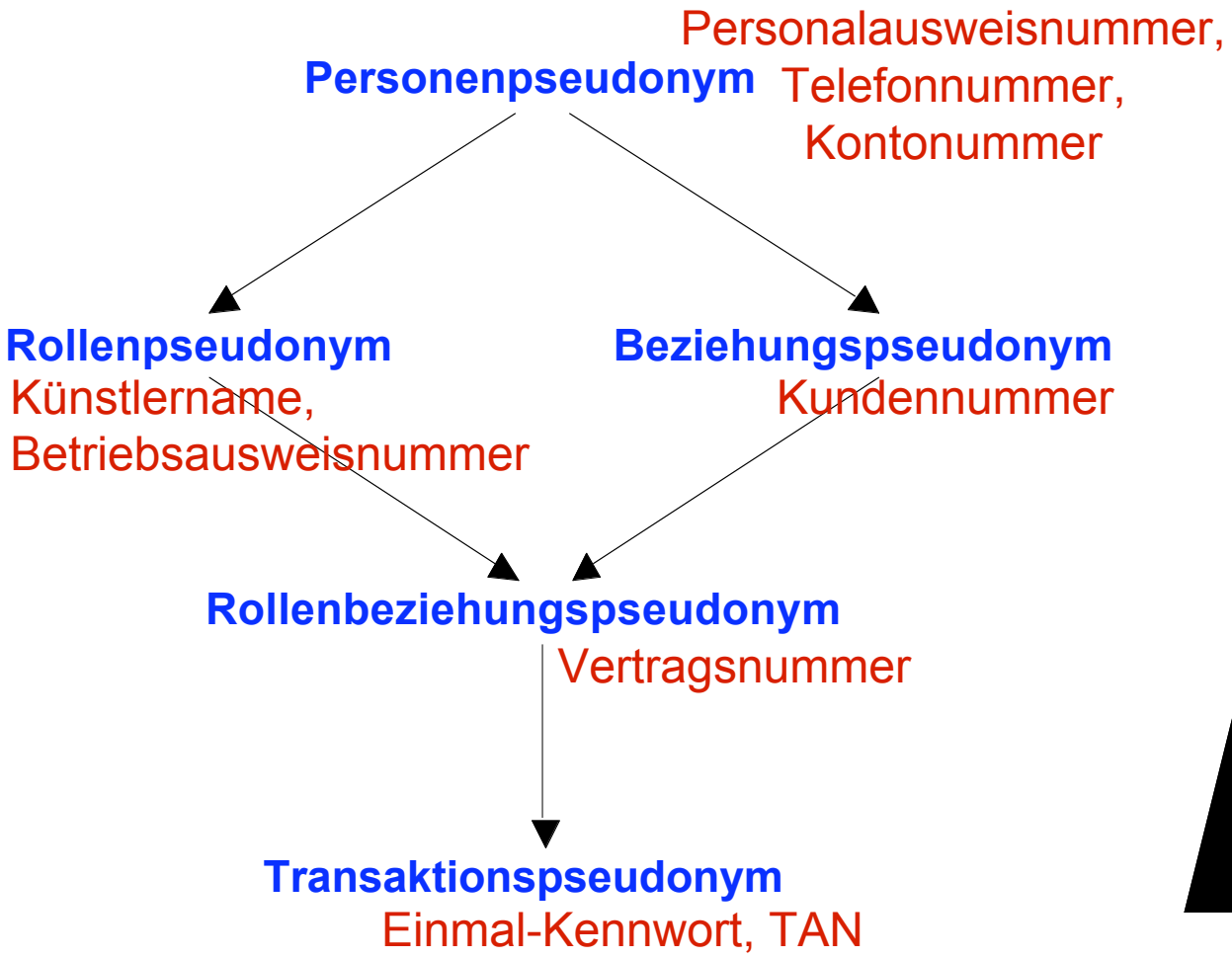
Kontonummer mit Bank als Identitätstreuhänder, Kreditkartennummer ...

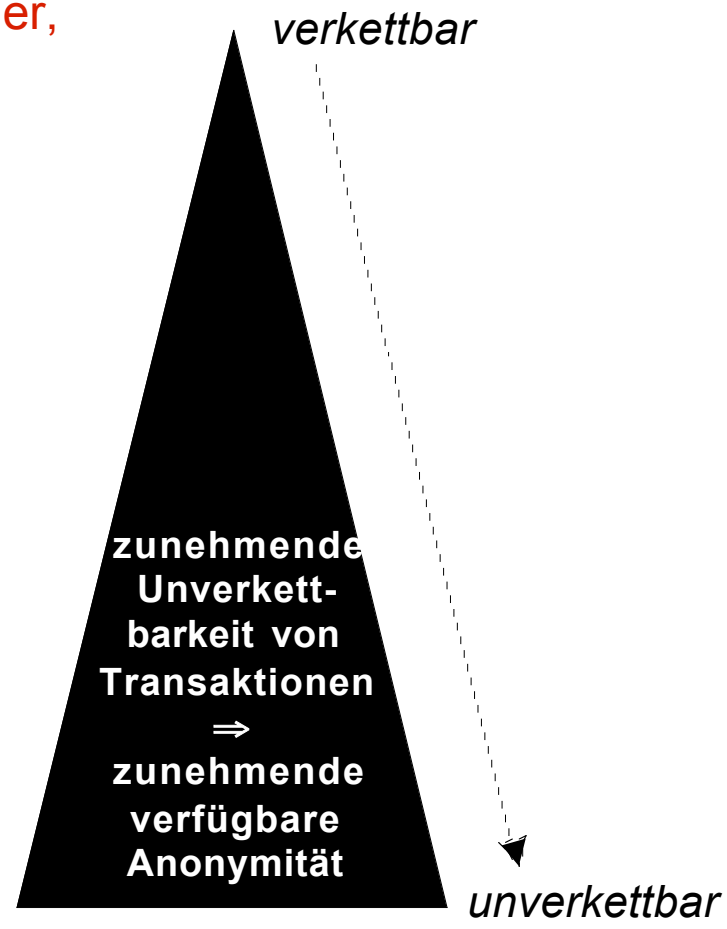
Initial unverkettetes Pseudonym:

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

Biometrische Merkmale; DNA (solange keinerlei Register)

Pseudonyme: Verwendungszusammenhang => Halbordnung





A → B bedeutet „B ermöglicht stärkere Anonymität als A“

Integration mit Identitätsmanagement

Netznutzung → Transaktionen zwischen anonymen Partnern

→ expliziter Identitätsnachweis stets möglich

---

anonyme Kommunikation erbringendes Netz

Schutz der Verkehrs- und Interessendaten
erfordert geeignete Netzstruktur
→ rechtzeitig überlegen

} Optionen offen halten

Anonyme Netze können ohne Leistungseinbuße
nicht anonym betrieben werden,
Umkehrung gilt nicht!

Verbrechensverhinderung besser als -aufklärung

Sicherer E-Commerce trotz starker Pseudonymität (1985..1990):
Wertetreuhänder statt Identitätstreuhänder

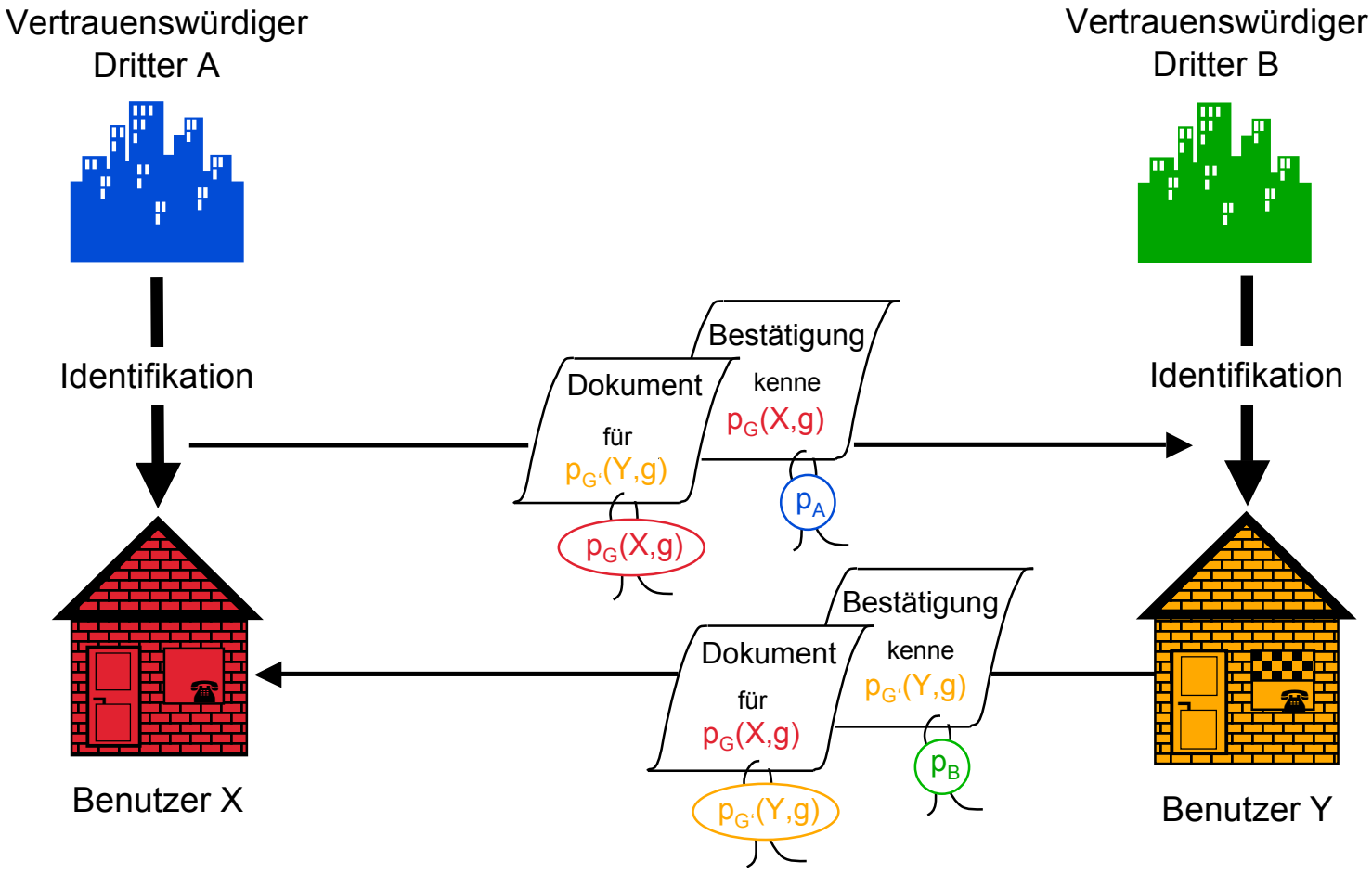
Michael Waidner, Andreas Pfitzmann: Betrugssicherheit trotz Anonymität. Abrechnung und Geldtransfer in Netzen; 1. GI Fachtagung Datenschutz und Datensicherung im Wandel der Informationstechnologien, IFB 113, Springer-Verlag, Berlin 1985, 128-141; Überarbeitung in: Datenschutz und Datensicherung DuD /1 (1986) 16-22.
http://dud.inf.tu-dresden.de/sireneLit.shtml#Zsys

Birgit Pfitzmann, Michael Waidner, Andreas Pfitzmann: Rechtssicherheit trotz Anonymität in offenen digitalen Systemen; Datenschutz und Datensicherung DuD 14/5-6 (1990) 243-253, 305-315.
http://dud.inf.tu-dresden.de/sireneLit.shtml#Zsys

Holger Bürk, Andreas Pfitzmann: Value Exchange Systems Enabling Security and Unobservability; Computers & Security 9/8 (1990) 715-721.
http://dud.inf.tu-dresden.de/sireneLit.shtml#pay.fair

Sperren illegaler Inhalte (laufende Arbeiten an Uni Regensburg mit BKA und an TU Dresden mit kjm)

Authentisierte anonyme Erklärungen zwischen deanonymisierbaren Geschäftspartnern



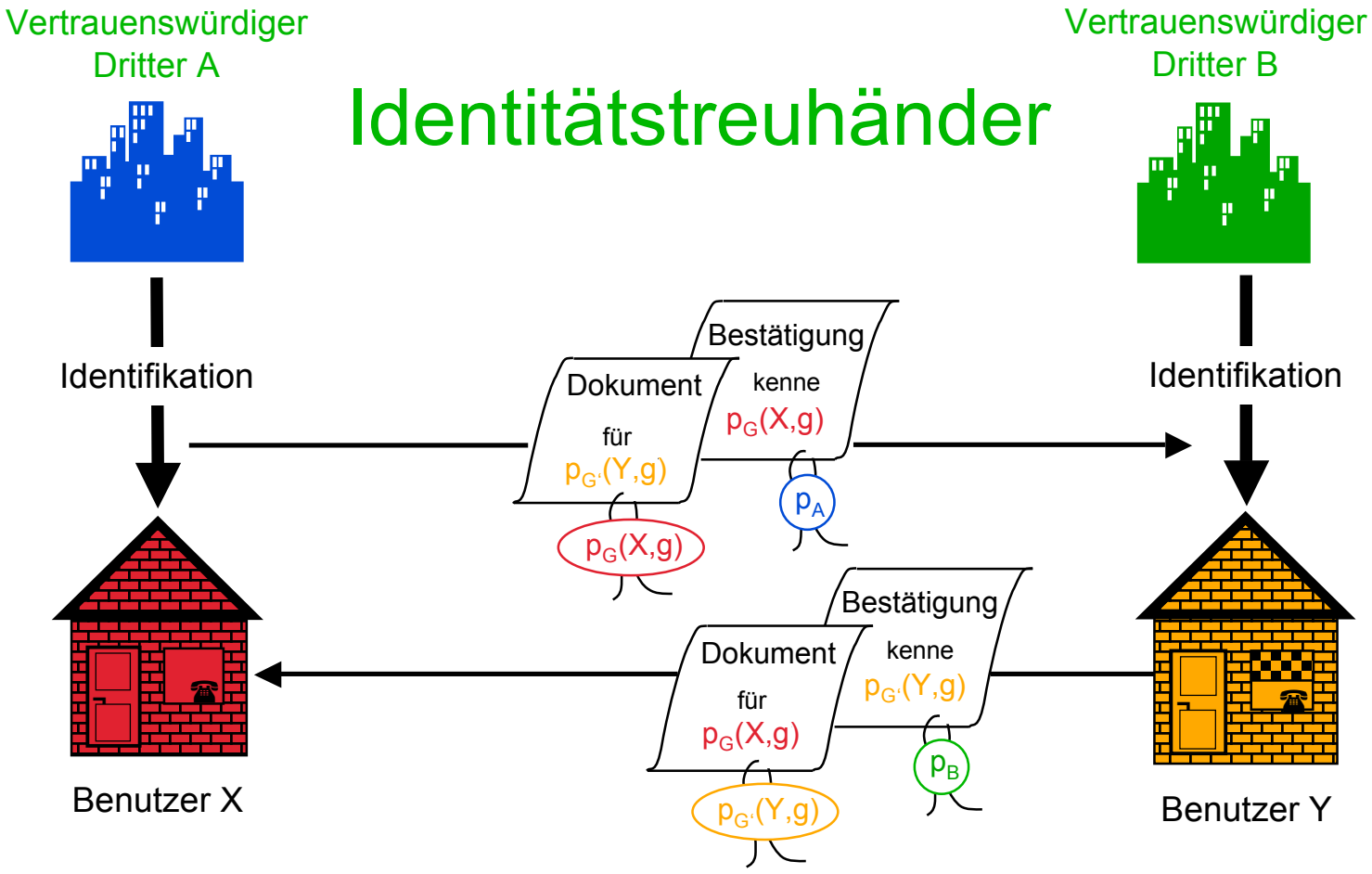
Verallgemeinerung:

$$X \rightarrow B_1 \rightarrow B_2 \rightarrow \ldots \rightarrow B_n \rightarrow Y$$

$$X \rightarrow B'_1 \rightarrow B'_2 \rightarrow \ldots \rightarrow B'_m \rightarrow Y$$

Fehler-/ Angriffstoleranz (vgl. MIXe)

Authentisierte anonyme Erklärungen zwischen deanonymisierbaren Geschäftspartnern



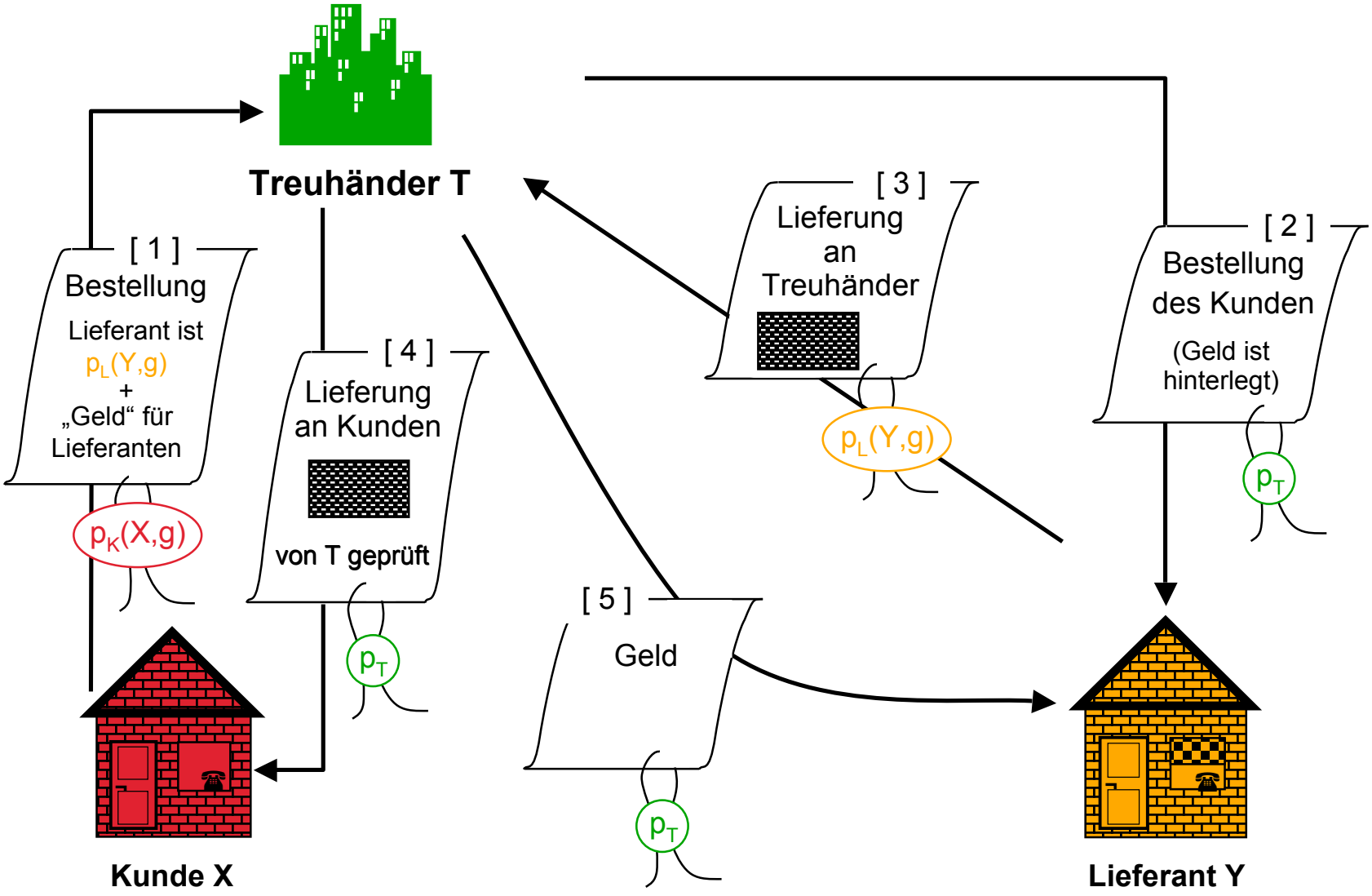
Verallgemeinerung:

$$X \rightarrow B_1 \rightarrow B_2 \rightarrow \ldots \rightarrow B_n \rightarrow Y$$

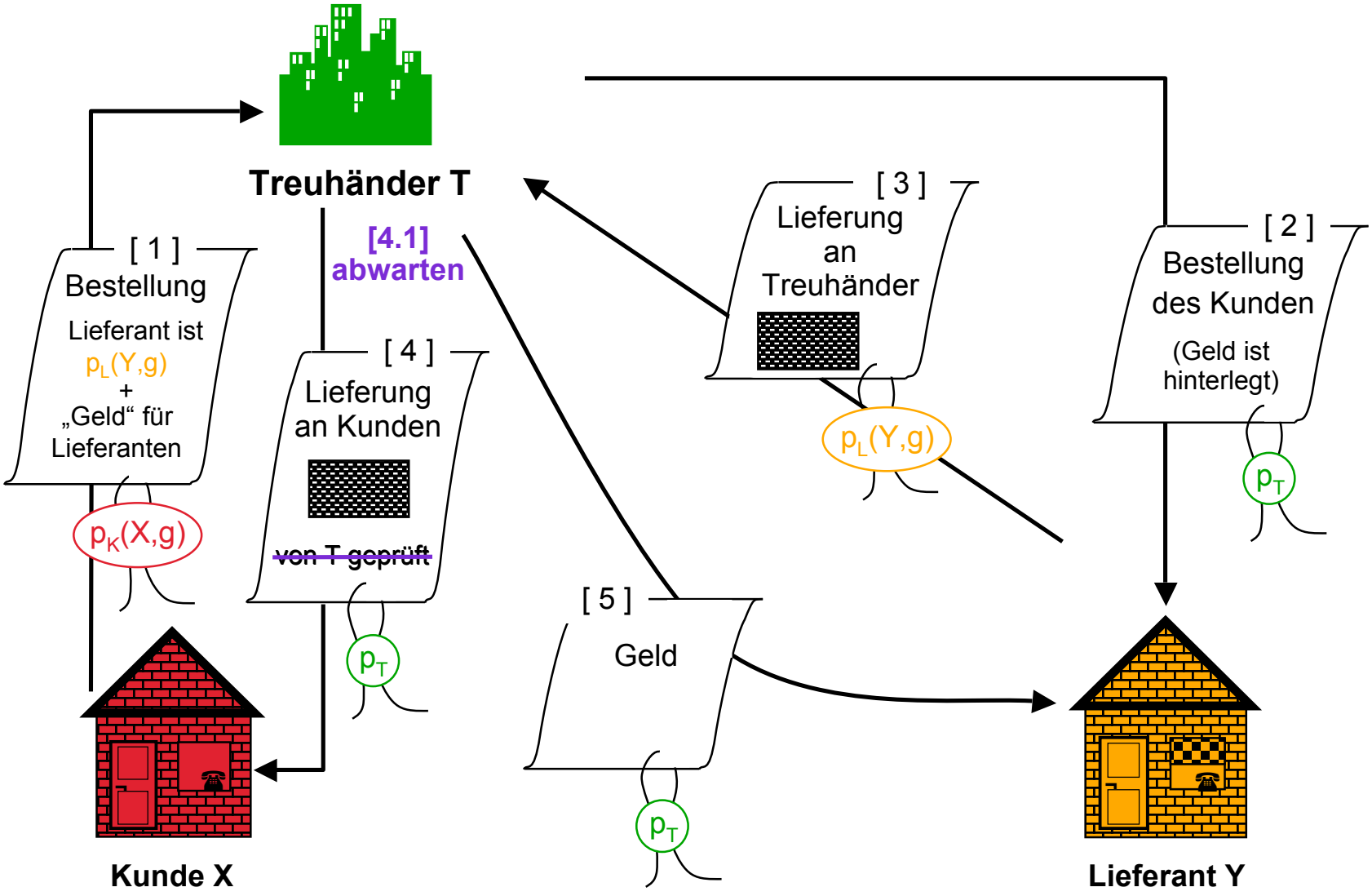
$$\searrow B'_1 \rightarrow B'_2 \rightarrow \ldots \rightarrow B'_m \nearrow$$

Fehler-/ Angriffstoleranz (vgl. MIXe)

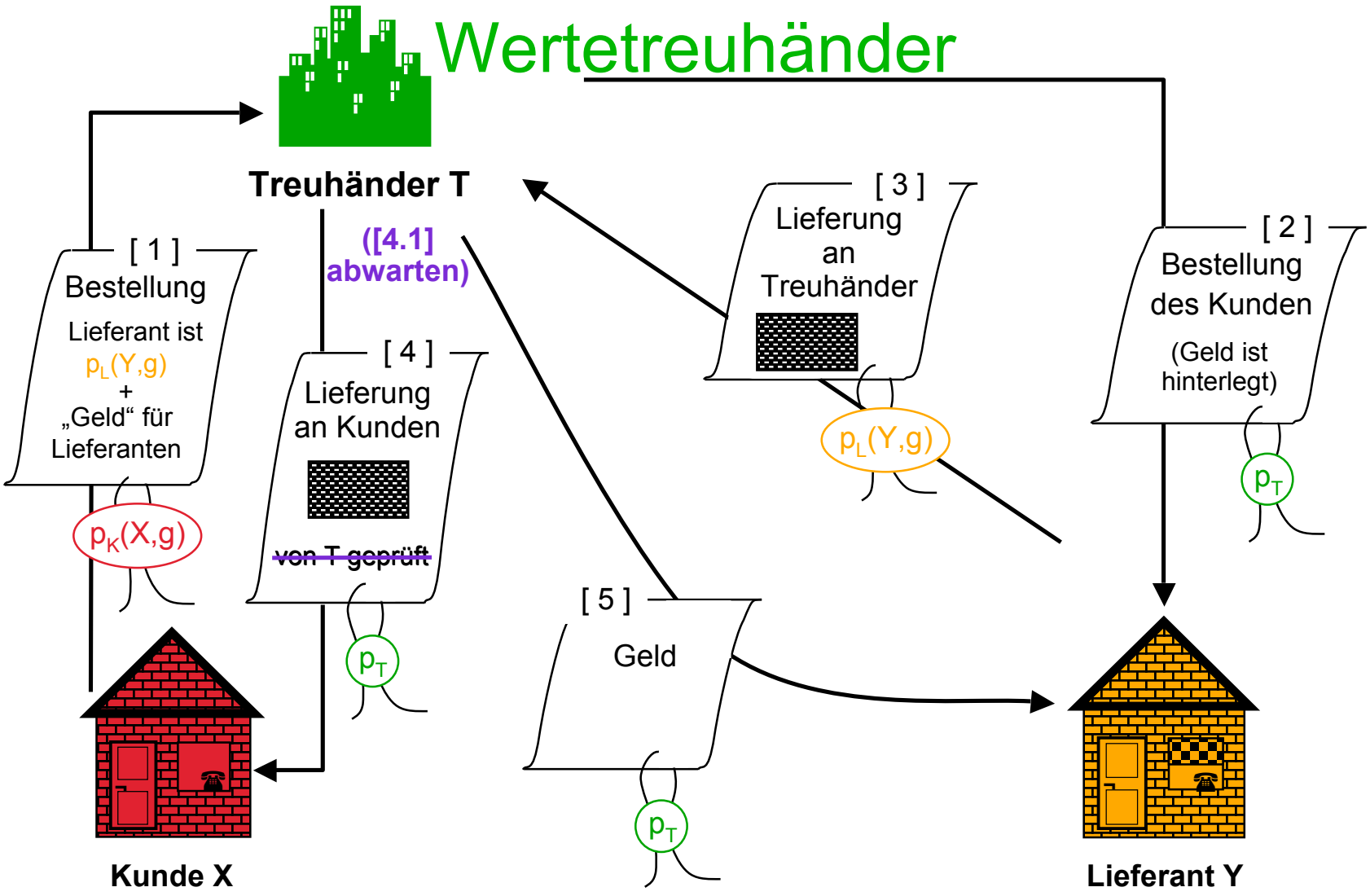
Betrugssicherheit für völlig anonyme Geschäftspartner durch aktiven Treuhänder, der Ware prüfen kann



Betrugssicherheit für völlig anonyme Geschäftspartner durch aktiven Treuhänder, der Ware nicht prüfen kann



Betrugssicherheit für völlig anonyme Geschäftspartner durch aktiven Treuhänder, der Ware (nicht) prüfen kann



Balancierung „Privatheit ⇔ Überwachung“

- Anwendungsübergreifend !
- Data Retention weitgehend wirkungslos und keinesfalls kosteneffizient
  - Offene Proxies im nicht-kooperierenden Ausland
  - Internationalisierung oder gar „Auswanderung“ von AN.ON, TOR, ...
  - Offene WLANs, Bluetooth-Geräte
- Überwachungsfreie Räume sind für die menschliche Entwicklung nötig und ein Sicherheitsgewinn für die Gesellschaft

Andreas Pfitzmann: *Werden biometrische Sicherheitstechnologien die heutige IT-Sicherheitsdebatte vor neue Herausforderungen stellen?* Datenschutz-Berater 29/4 (2005) 11-14.
http://www.inf.tu-dresden.de/index.php?node_id=703&ln=de

Andreas Pfitzmann: Biometrie – wie einsetzen und wie keinesfalls? Informatik-Spektrum 29/5 (2006) 353-356.

(Un)Regulierbarkeit anonymer/pseudonymer Kommunikation

Explizite Techniken:

Anon-Proxies

MIXe

- **Kaskade: AN.ON**
- **P2P: TOR**

Überlagerndes Senden

All dies gibt es auch im Ausland ohne Regulierung – solange noch keine Weltinnenpolitik

(Un)Regulierbarkeit anonymer/pseudonymer Kommunikation

Ausweichtechniken:

Selbst im Inland:

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

Vorratsdatenspeicherung ist weitestgehend sinnlos, da „Kriminelle“ dann ausweichen, s.o. sowie auf verdeckte Kommunikation mittels Steganographie

Ausblick

- **Balancierung** sollte nicht nur innerhalb einzelner Anwendungen, sondern **über Anwendungen hinweg** erfolgen.
- **Genomdatenbanken** und **Ubiquitous Computing** (= pervasive Computing = Rechner in allen Dingen und deren Vernetzung) werden **Datenschutz in der physischen Welt weitgehend untergraben:**
  ***Schöne neue Welt der Verbrechensaufklärung*.**
- **Freiräume in der digitalen Welt sind möglich** (und wohl auch notwendig, Bsp. Jugendgruppe Kirchengemeinde) **und sollten geschaffen werden** – anstatt mit hohen Kosten unsinnige (im Sinne einer Balancierung über Anwendungen hinweg) Vorratsdatenspeicherung anzustreben.
- Für viele Netzbürger ist die **digitale Welt** nicht eine **Erweiterung der** physischen Welt, sondern der **Gedankenwelt**. Für sie ist Vorratsdatenspeicherung ein Angriff auf die Gedankenfreiheit.

Kommen Sie gut nach hause ...

Vielen Dank für Ihre Anregungen

Und auf ein Wiedersehen - oder viele