Technischer Datenschutz in Zeiten von Terrorbekämpfung und Vorratsdatenspeicherung

Prof. Dr. Hannes Federrath
Universität Regensburg
Lehrstuhl Management der Informationssicherheit

http://www-sec.uni-regensburg.de/

IT-Sicherheit am Donaustrand „Sicherheitstechnische und sicherheitsrechtliche Herausforderung des Web 2.0“, Universität Passau, 16. Februar 2009

Was ist Datenschutz?

- Schutz der Persönlichkeitsrechte eines Betroffenen

> Ich als Mensch muss noch wissen dürfen, welche mich betreffenden Informationen an welcher Stelle bekannt sind.
>
> Ich muss einschätzen können, welches Wissen meine Kommunikationspartner über ich haben.

- Warum?
  - Andernfalls könne ich mich in meiner Freiheit gehemmt fühlen, aus eigener Selbstbestimmung zu handeln.

- Recht auf informationelle Selbstbestimmung

Recht auf informationelle Selbstbestimmung

»Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den *Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten* voraus. …

Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. *Mit dem Recht auf informationelle Selbstbestimmung wäre eine Gesellschaftsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß.«*

aus dem Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983 1. BvR 209/83 Abschnitt C II.1, S. 43

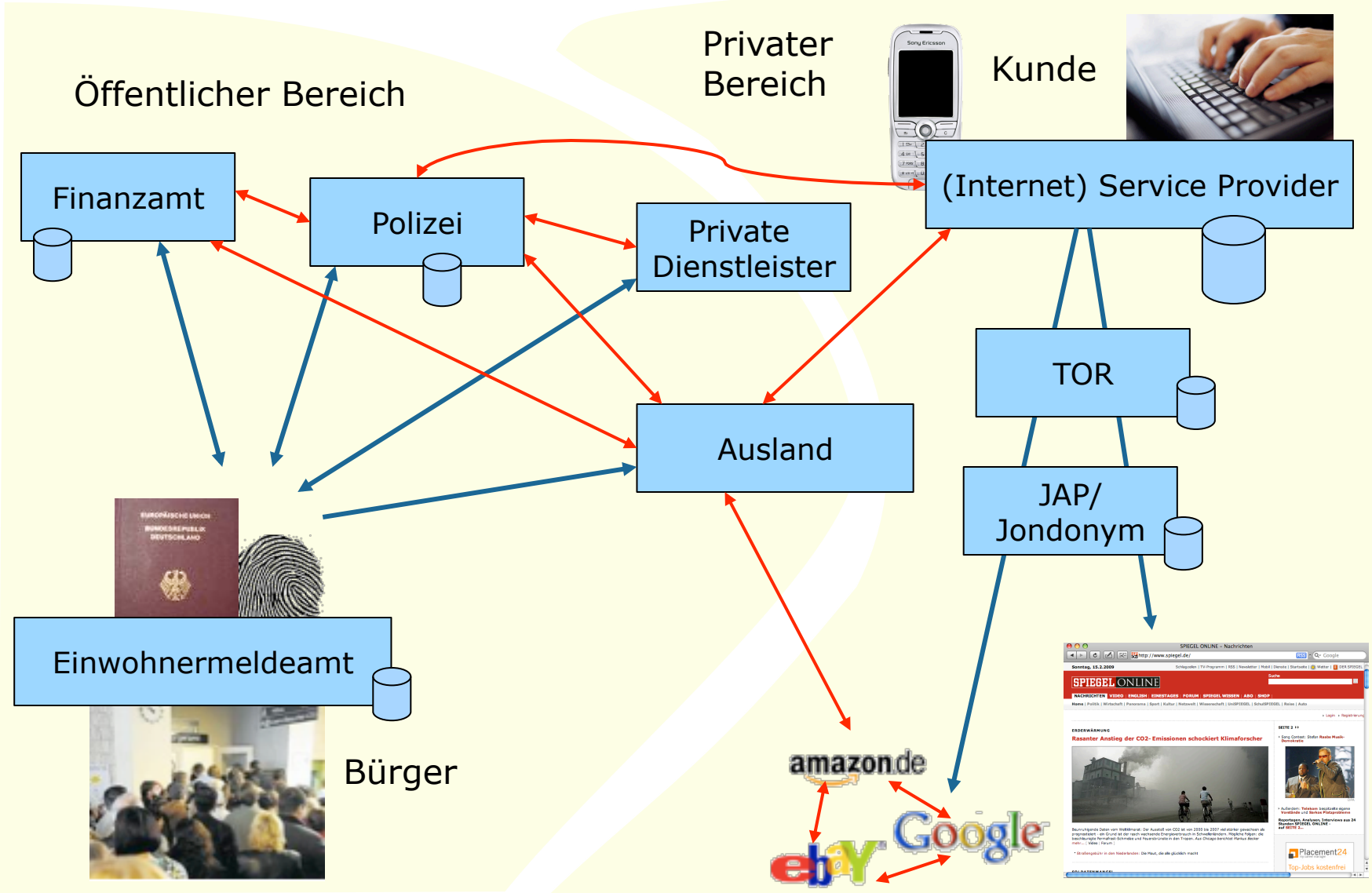
Was ist *technischer* Datenschutz?

- Insb. die Umsetzung der
  Prinzipien der Datenvermeidung und Datensparsamkeit:
  - Möglichst nur Daten erheben und verarbeiten, die unbedingt erforderlich sind
  - Pseudonymisierung und Anonymisierung, wann immer möglich und zumutbar

§ 3a BDSG Datenvermeidung und Datensparsamkeit

Gestaltung und Auswahl von Datenverarbeitungssystemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Beispiele für Datenübermittlungen



Grundsätzliche Techniken des technischen Datenschutzes

- Gewaltenteilung
  - Verzicht auf zentralisierte Datenhaltung
  - stattdessen Einsatz verteilter Systeme

Beispiele

Pseudonymisierung | Proxies | Mixe

- Selbstdatenschutz
  - Daten verbleiben im Verfügungsbereich des Betroffenen

Chipkarten | Persönliche mobile Geräte | Vertrauenswürdige Dritte

- Einsatz von Basistechnologien
  - Verschlüsselung auf allen Übertragungsstrecken und Datenträgern
  - Starke Authentifizierung und Nachweisbarkeit
  - Protokollierung des Zugriffs

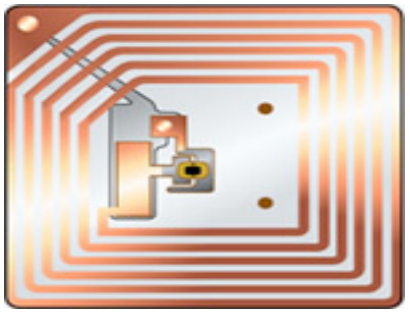
Freie Kryptographie | Digitale Signatur | Sichere Betriebssysteme

Fallbeispiele …

… für fragwürdige und teilweise unwirksame Maßnahmen

- Biometrischer Fingerabdruck
- RFID zur drahtlosen Kommunikation

- Vorratsdatenspeicherung



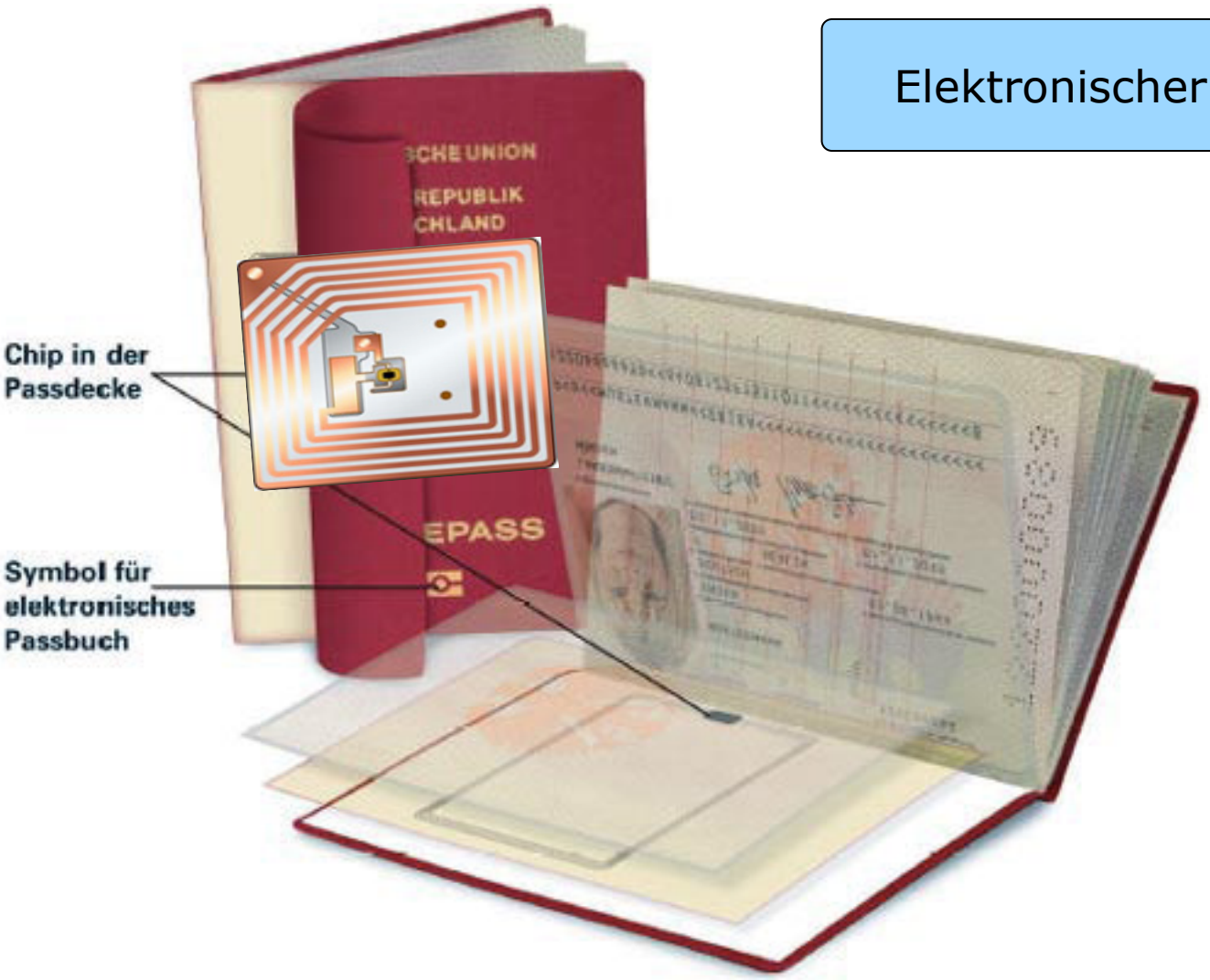
Biometrische Reisepässe

- Seit Herbst 2005 zur Verbesserung der inneren Sicherheit eingeführt

- Neue Funktionen:
  - Speicherung eines Fotos und eines Fingerabdrucks des Passinhabers auf einem Chip
  - Kontaktloses Auslesen der biometrischen Merkmale aus dem Chip
- Probleme:
  - Biometrische Merkmale
    - erhöhen nicht die Zuverlässigkeit der Identifikation
    - geben möglicherweise Auskunft über weitere Eigenschaften der Person
  - Kontaktlose Chips
    - lassen sich unter bestimmten Umständen auslesen
    - Tracking einer Person denkbar

RFID zur drahtlosen Kommunikation

Elektronischer Reisepass



Fälschen eines Fingerabdrucks

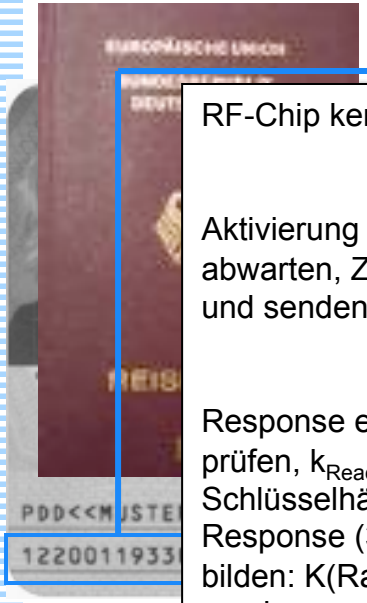
- Vom Chaos Computer Club im Jahre 2005 praktisch demonstriert.

- Fingerabdruck sichtbar machen
- fotografieren
- nachbearbeiten
- ausdrucken
- Leim drauf
- warten
- abziehen

- Von uns im Rahmen einer Fernsehsendung praktisch nachvollzogen
- Ergebnis: Es funktioniert wirklich (nicht).

RFID zur drahtlosen Kommunikation

- Basic Access Control und Active Authentication



optisches Lesen der MRZ

RF-Chip kennt K (56 Bit)

Aktivierung durch elektr. Feld abwarten, Zufallszahl Rand1 wählen und senden

Response entschlüsseln, Rand1 prüfen, k_{Reader} zwischenspeichern, Schlüsselhälfte k_{Chip} wählen, Response (3-DES) auf Rand2 bilden: K(Rand1,Rand2,k_{Chip}) und senden

Elektrisches Feld
Proximity coupling <=10cm

Rand1

K(Rand1,Rand2,k_{Reader})

K(Rand1,Rand2,k_{Chip})

Leser bildet Schlüssel K (56 Bit) aus MRZ: K=h(PassID,GebD,GültD), aktiviert elektr. Feld und wartet Empfang von Rand1 ab

wählt Zufallszahl Rand2, Schlüsselhälfte k_{Reader}und bildet Response (3-DES) auf Rand1: K(Rand1,Rand2,k_{Reader}) und sendet

Response entschlüsseln, Rand2 prüfen

Alle weitere Kommunikation wird mit (k_{Reader},k_{Chip}) verschlüsselt (3-DES mit CBC)

Machine Readable Zone (MRZ):

```
P<D<<NAME<<VORNAMEN<<<<<<<<<<<<<<<
123456789P<<JJMMDDP<JJMMDDP<<<<<<P
```

Passnummer Geburtsdatum Gültigkeitsdatum
jeweils mit Prüfziffer versehen

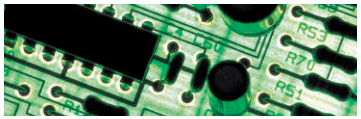
nach: Dr. Dennis Kügler: Risiko Reisepass? Schutz der biometrischen Daten im RF-Chip. ct 5 (2005) 88

Fallbeispiele …

… für fragwürdige und teilweise unwirksame Maßnahmen

- Biometrischer Fingerabdruck
- RFID zur drahtlosen Kommunikation

- Vorratsdatenspeicherung



Vorratsdatenspeicherung: TKG § 113 a

§ 113a Speicherungspflichten für Daten

(1) Wer öffentlich zugängliche Telekommunikationsdienste für Endnutzer erbringt, ist verpflichtet, von ihm bei der Nutzung seines Dienstes erzeugte oder verarbeitete Verkehrsdaten nach Maßgabe der Absätze 2 bis 5 sechs Monate im Inland oder in einem anderen Mitgliedstaat der Europäischen Union zu speichern. Wer öffentlich zugängliche Telekommunikationsdienste für Endnutzer erbringt, ohne selbst Verkehrsdaten zu erzeugen oder zu verarbeiten, hat sicherzustellen, dass die Daten gemäß Satz 1 gespeichert werden, und der Bundesnetzagentur auf deren Verlangen mitzuteilen, wer diese Daten speichert.

(2) Die Anbieter von öffentlich zugänglichen Telefondiensten speichern:

1. die Rufnummer oder andere Kennung des anrufenden und des angerufenen Anschlusses sowie im Falle von Um- oder Weiterschaltungen jedes weiteren beteiligten Anschlusses,

2. den Beginn und das Ende der Verbindung nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone,

3. in Fällen, in denen im Rahmen des Telefondienstes unterschiedliche Dienste genutzt werden können, Angaben zu dem genutzten Dienst,

4. im Fall mobiler Telefondienste ferner:

a) die internationale Kennung für mobile Teilnehmer für den anrufenden und den angerufenen Anschluss,

b) die internationale Kennung des anrufenden und des angerufenen Endgerätes,

c) die Bezeichnung der durch den anrufenden und den angerufenen Anschluss bei Beginn der Verbindung genutzten Funkzellen,

d) im Fall im Voraus bezahlter anonymer Dienste auch die erste Aktivierung des Dienstes nach Datum, Uhrzeit und Bezeichnung der Funkzelle,

5. im Fall von Internet-Telefondiensten auch die Internetprotokoll-Adresse des anrufenden und des angerufenen Anschlusses.

Satz 1 gilt entsprechend bei der Übermittlung einer Kurz-, Multimedia- oder ähnlichen Nachricht; hierbei sind anstelle der Angaben nach Satz 1 Nr. 2 die Zeitpunkte der Versendung und des Empfangs der Nachricht zu speichern.

Vorratsdatenspeicherung: TKG § 113 a

(3) Die Anbieter von Diensten der elektronischen Post speichern:

1. bei Versendung einer Nachricht die Kennung des elektronischen Postfachs und die Internetprotokoll-Adresse des Absenders sowie die Kennung des elektronischen Postfachs jedes Empfängers der Nachricht,
2. bei Eingang einer Nachricht in einem elektronischen Postfach die Kennung des elektronischen Postfachs des Absenders und des Empfängers der Nachricht sowie die Internetprotokoll-Adresse der absendenden Telekommunikationsanlage,
3. bei Zugriff auf das elektronische Postfach dessen Kennung und die Internetprotokoll-Adresse des Abrufenden,
4. die Zeitpunkte der in den Nummern 1 bis 3 genannten Nutzungen des Dienstes nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone.

(4) Die Anbieter von Internetzugangsdiensten speichern:

1. die dem Teilnehmer für eine Internetnutzung zugewiesene Internetprotokoll-Adresse,
2. eine eindeutige Kennung des Anschlusses, über den die Internetnutzung erfolgt,
3. den Beginn und das Ende der Internetnutzung unter der zugewiesenen Internetprotokoll-Adresse nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone.

(5) Soweit Anbieter von Telefondiensten die in dieser Vorschrift genannten Verkehrsdaten für die in § 96 Abs. 2 genannten Zwecke auch dann speichern oder protokollieren, wenn der Anruf unbeantwortet bleibt oder wegen eines Eingriffs des Netzwerkmanagements erfolglos ist, sind die Verkehrsdaten auch nach Maßgabe dieser Vorschrift zu speichern.

(6) Wer Telekommunikationsdienste erbringt und hierbei die nach Maßgabe dieser Vorschrift zu speichernden Angaben verändert, ist zur Speicherung der ursprünglichen und der neuen Angabe sowie des Zeitpunktes der Umschreibung dieser Angaben nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone verpflichtet.

Vorratsdatenspeicherung: TKG § 113 a

(7) Wer ein Mobilfunknetz für die Öffentlichkeit betreibt, ist verpflichtet, zu den nach Maßgabe dieser Vorschrift gespeicherten Bezeichnungen der Funkzellen auch Daten vorzuhalten, aus denen sich die geografischen Lagen der die jeweilige Funkzelle versorgenden Funkantennen sowie deren Hauptstrahlrichtungen ergeben.

(8) Der Inhalt der Kommunikation und Daten über aufgerufene Internetseiten dürfen auf Grund dieser Vorschrift nicht gespeichert werden.

(9) Die Speicherung der Daten nach den Absätzen 1 bis 7 hat so zu erfolgen, dass Auskunftsersuchen der berechtigten Stellen unverzüglich beantwortet werden können.

(10) Der nach dieser Vorschrift Verpflichtete hat betreffend die Qualität und den Schutz der gespeicherten Verkehrsdaten die im Bereich der Telekommunikation erforderliche Sorgfalt zu beachten. Im Rahmen dessen hat er durch technische und organisatorische Maßnahmen sicherzustellen, dass der Zugang zu den gespeicherten Daten ausschließlich hierzu von ihm besonders ermächtigten Personen möglich ist.

(11) Der nach dieser Vorschrift Verpflichtete hat die allein auf Grund dieser Vorschrift gespeicherten Daten innerhalb eines Monats nach Ablauf der in Absatz 1 genannten Frist zu löschen oder die Löschung sicherzustellen.

TKG § 113a Speicherungspflichten für Daten

(1) Wer öffentlich zugängliche Telekommunikationsdienste für Endnutzer erbringt, ist verpflichtet, von ihm bei der Nutzung seines Dienstes erzeugte oder verarbeitete Verkehrsdaten […] sechs Monate im Inland oder in einem anderen Mitgliedstaat der Europäischen Union zu speichern.

[…]

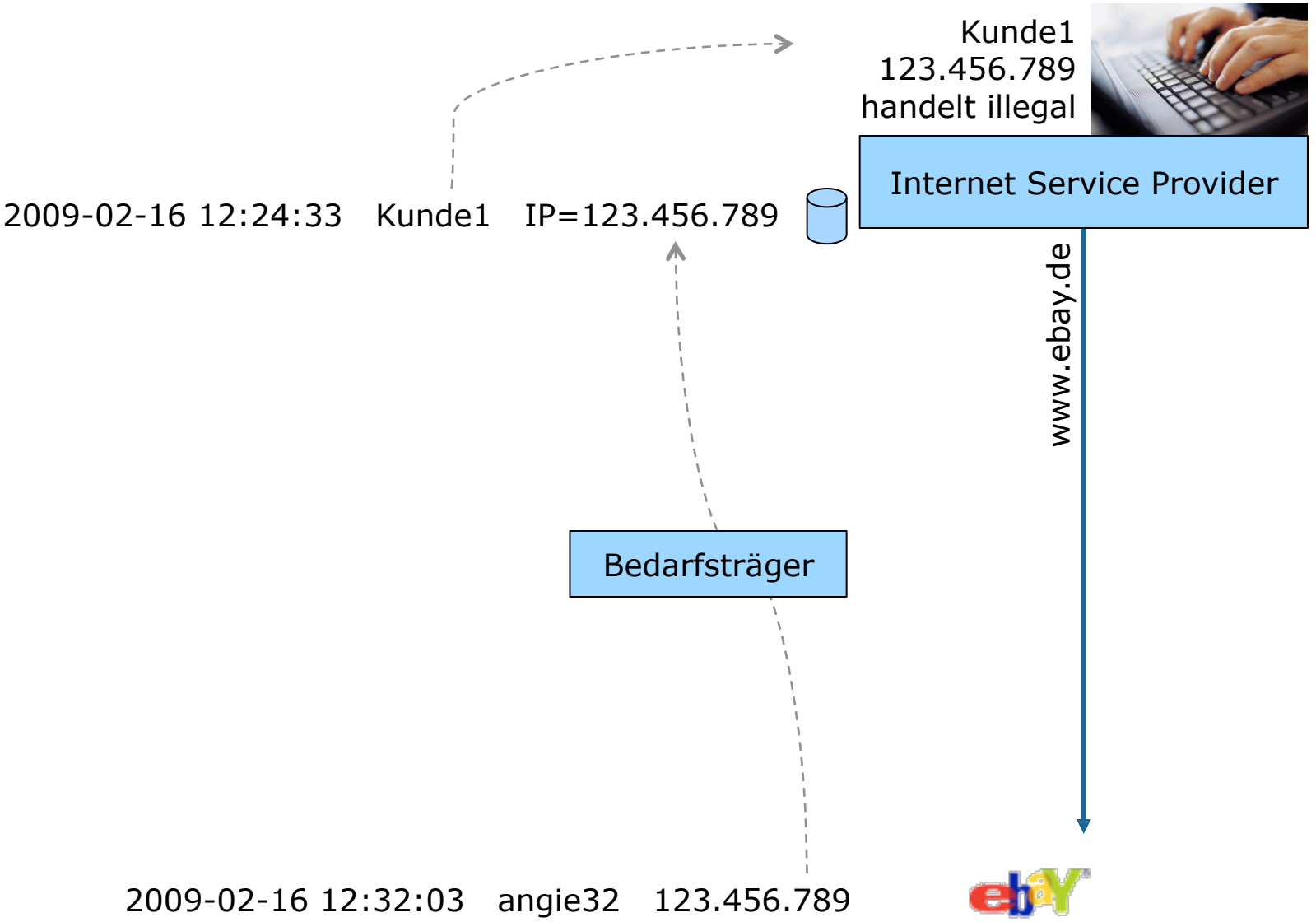
(6) Wer Telekommunikationsdienste erbringt und hierbei die nach Maßgabe dieser Vorschrift zu speichernden Angaben verändert, ist zur Speicherung der ursprünglichen und der neuen Angabe sowie des Zeitpunktes der Umschreibung dieser Angaben nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone verpflichtet.

[…]

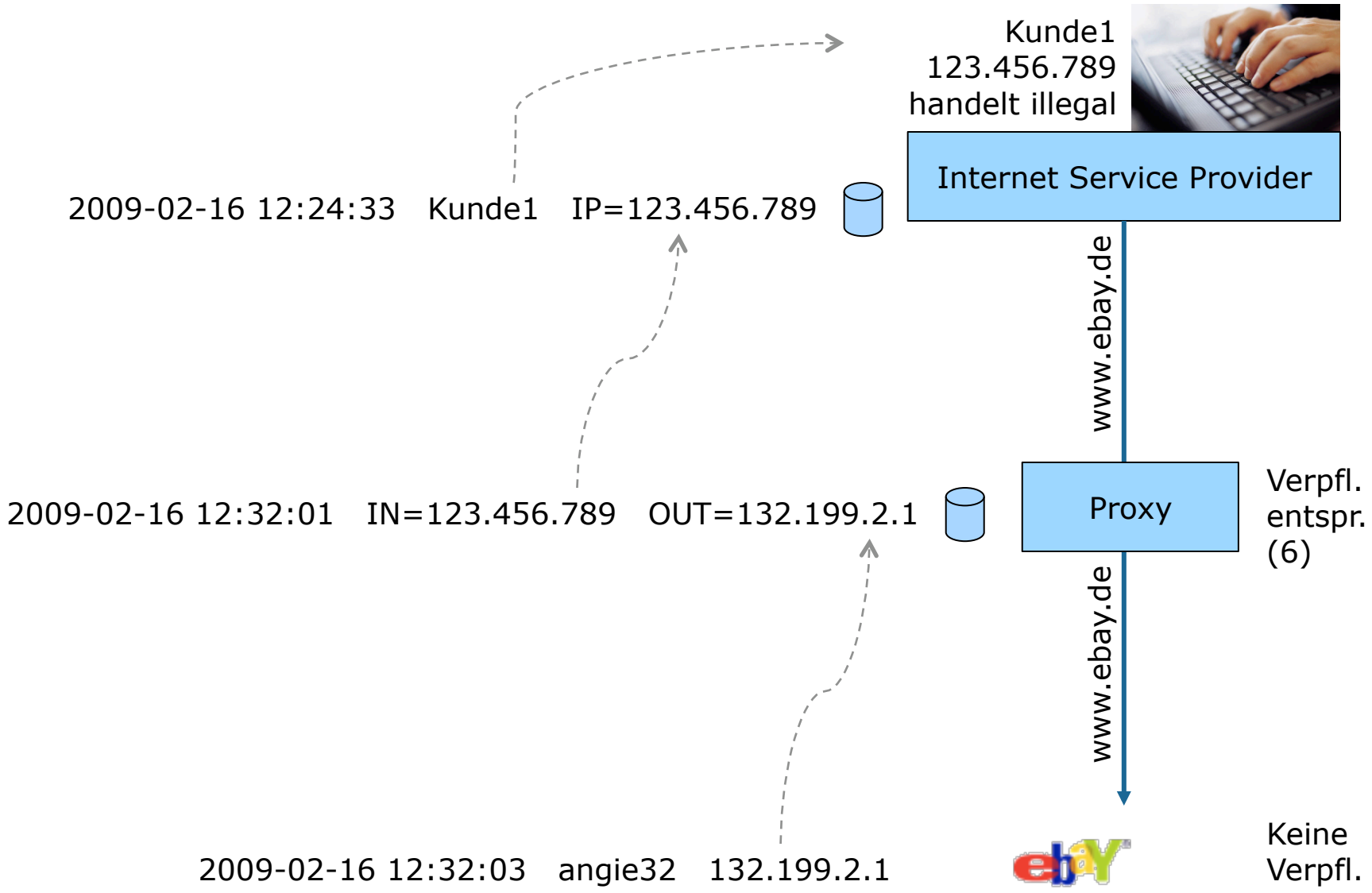
(8) Der Inhalt der Kommunikation und Daten über aufgerufene Internetseiten dürfen auf Grund dieser Vorschrift nicht gespeichert werden.

[…]

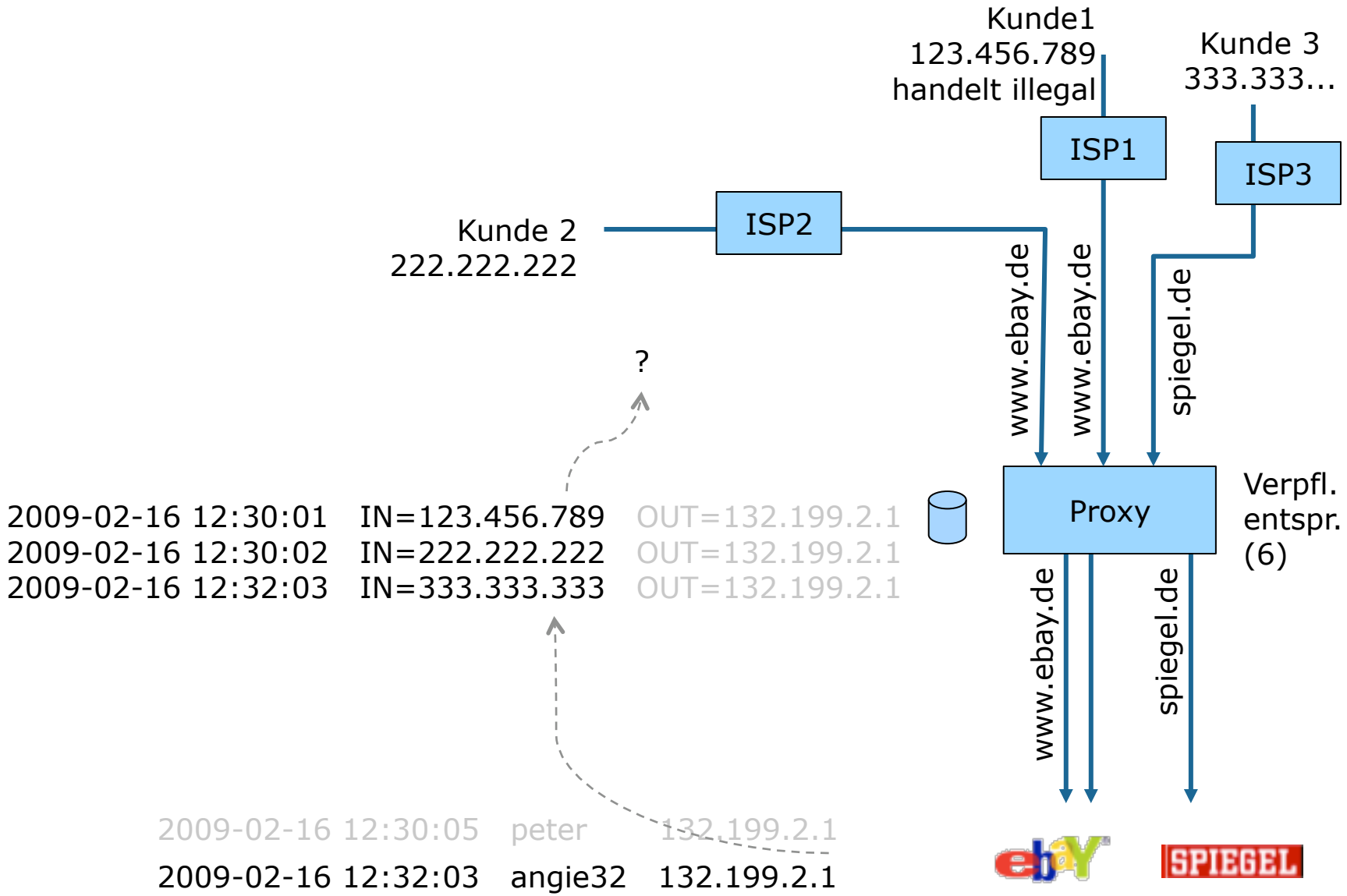
Zweck der Vorratsdatenspeicherung: Rückverfolgung



Zweck der Vorratsdatenspeicherung: Rückverfolgung



Problem Rückverfolgung



Problem Rückverfolgung

- Rückverfolgung scheitert
- Auswege:
  1. Proxy speichert URL bzw. durchgeleiteten Inhalt:
     - nicht erlaubt aufgrund (8)
  2. Proxy sendet Header: X-Forwarded-For: 123.456.789
     - funktioniert nur bei http
     - Keine Verpflichtung des Proxy-Betreibers
     - Server muss X-Forwarded-For-Header ebenfalls loggen
  3. Proxy speichert Quellportnummer des ausgehenden Requests
     - funktioniert bei allen Diensten
     - Keine Verpflichtung des Proxy-Betreibers
     - Server muss Quellport ebenfalls loggen

Problem Rückverfolgung

1. Proxy speichert URL bzw. durchgeleiteten Inhalt
2. Proxy sendet Header: X-Forwarded-For: 123.456.789
3. Proxy speichert Quellportnummer des ausgehenden Requests
4. Proxy speichert Zeitpunkt und »Umschreiben« *jedes* Requests
   - funktioniert nur zuverlässig bei hochsynchronen Uhren
   - mangelnde Verfügbarkeit eines geeigneten Zeitdienstes
   - auch Server (nicht verpflichtet gem. TKG) muss exakte Zeit verwenden
   - Varianzen in den Paketlaufzeiten machen praktische Rückverfolgung ggf. unmöglich
   - HTTP 1.1 erlaubt mehrere HTTP-Requests in einer Verbindung: 1 Logeintrag in Proxy und viele im Server

(6) Wer Telekommunikationsdienste erbringt und hierbei die nach Maßgabe dieser Vorschrift zu speichernden Angaben verändert, ist zur Speicherung der ursprünglichen und der neuen Angabe sowie des Zeitpunktes der Umschreibung dieser Angaben nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone verpflichtet.

Unklarheiten

- »nach Maßgabe dieser Vorschrift zu speichernden Angaben« ist unklar formuliert:
  - Interpretation nach (3) »Dienste der elektronischen Post«
    - Jeder Request (ein- wie ausgehend) ist zu loggen
    - scheitert praktisch bei HTTP 1.1, es sei denn, man wollte die Verwendung dieses Protokolls verbieten
  - Interpretation nach (4) »Anbieter von Internetzugangsdiensten«
    - Nur Zeitpunkt des ersten Umschreibens ist zu protokollieren
    - Ende der Verbindung ist zu protokollieren

      (Jetzt gelten wieder die Probleme bei der Rückverfolgung bei Proxies.)

(6) Wer Telekommunikationsdienste erbringt und hierbei die nach Maßgabe dieser Vorschrift zu speichernden Angaben verändert, ist zur Speicherung der ursprünglichen und der neuen Angabe sowie des Zeitpunktes der Umschreibung dieser Angaben nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone verpflichtet.

Problem Rückverfolgung

Taktung: 5 Sek., Zeitpunkte des Kanalaufbaus: (Anonymer Kanal)

2009-02-16 12:30:01	123.456.789	mix2.de:56789
2009-02-16 12:30:02	222.222.222	mix2.de:63543
2009-02-16 12:30:19	333.333.333	mix2.de:15746

Kanäle für Nutzer 1 und 2 werden 12:30:05 aufgebaut, für Nutzer 3 um 12:30:20

2009-02-16 12:30:05	63543:mix1.de	mix3.de:25354
2009-02-16 12:30:21	15746:mix1.de	mix3.de:96521
2009-02-16 12:30:05	56789:mix1.de	mix3.de:45997

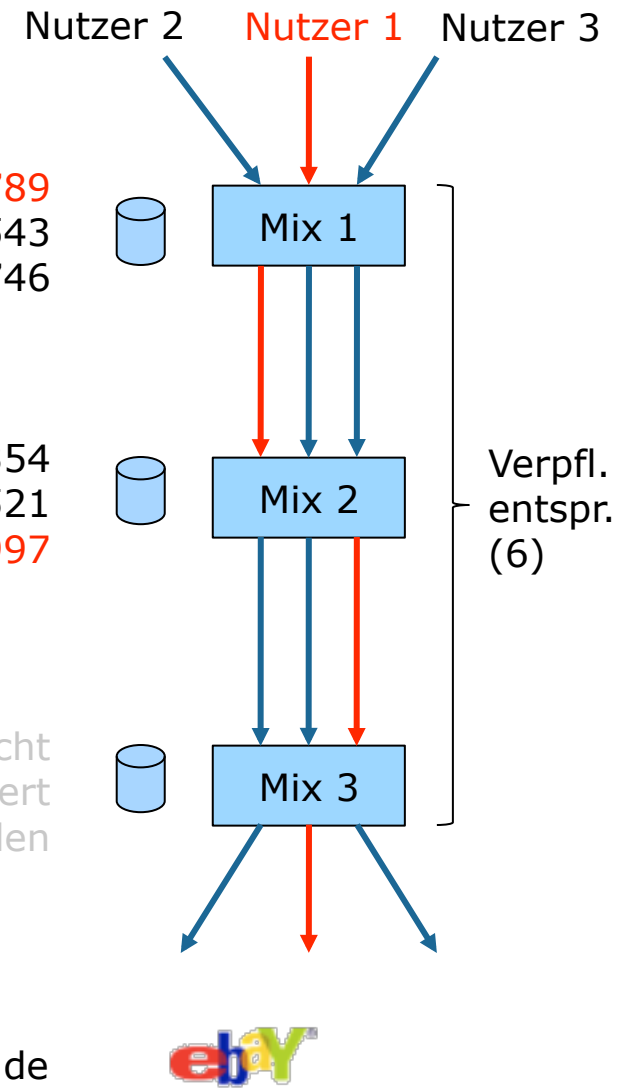
Kanäle für Nutzer 1 und 2 werden 12:30:10 aufgebaut, für Nutzer 3 um 12:30:25

2009-02-16 12:30:25	96521:mix2.de
2009-02-16 12:30:10	45997:mix2.de
2009-02-16 12:30:10	25354:mix2.de

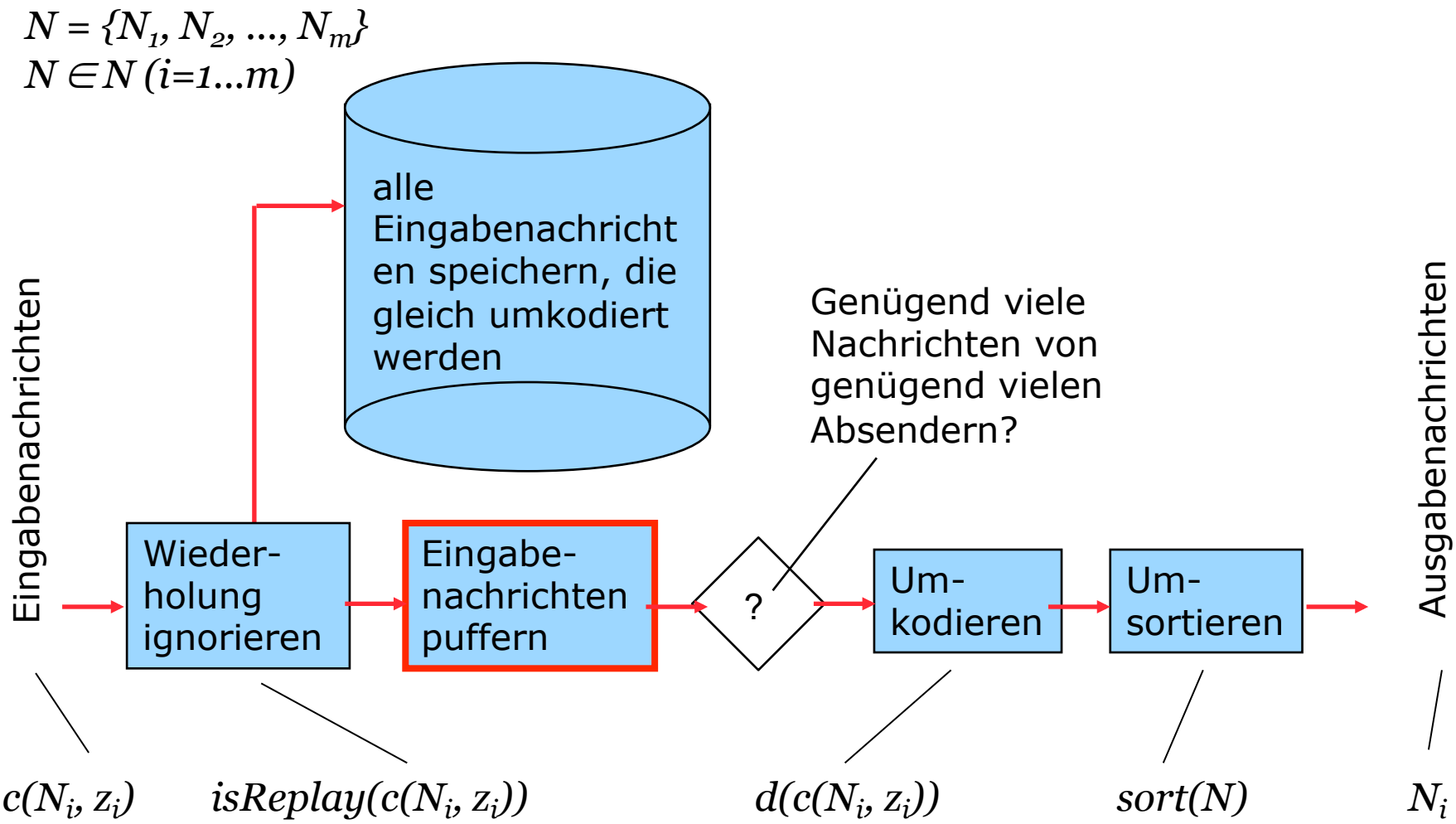
? Ziel darf nicht gespeichert werden

Illegale Handlung wird um 12:32:03 protokolliert:

2009-02-16 12:32:03 angie32 mix3.de



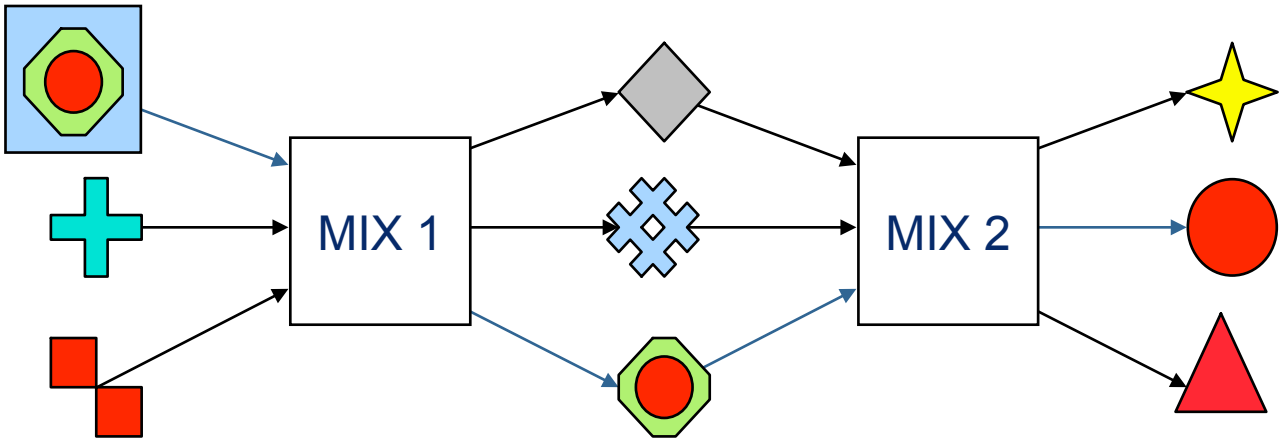
Blockschaltbild eines Mix



Mix-Netz

Chaum, 1981

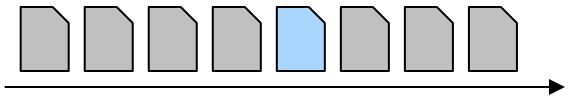
- Grundidee:
  - Nachrichten in einem »Schub« sammeln, Wiederholungen ignorieren, umkodieren, umsortieren, gemeinsam ausgeben.
  - Alle Nachrichten haben die gleiche Länge.
  - Mehr als einen Mix verwenden.
  - Wenigstens ein Mix darf nicht angreifen.
- Schutzziel:
  - Unverkettbarkeit von Sender und Empfänger
  - Schutz der Kommunikationsbeziehung
  - Zuordnung zwischen E- und A-Nachrichten wird verborgen



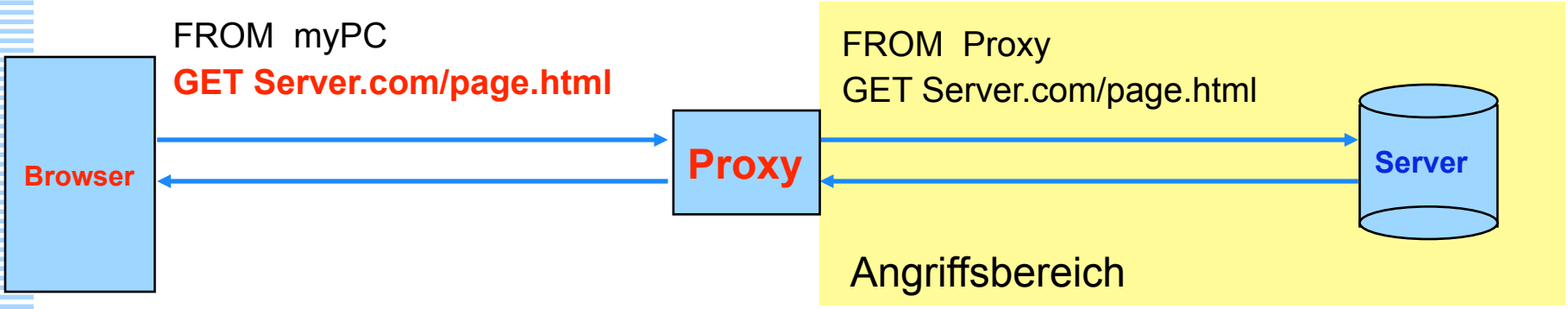
Grundsätzliche Techniken

- Verteilung (Broadcast) + implizite Adressierung
  - Schutz des Empfängers; alle erhalten alles
  - lokale Auswahl

- Dummy Traffic: Senden bedeutungsloser Nachrichten
  - Schutz des Senders



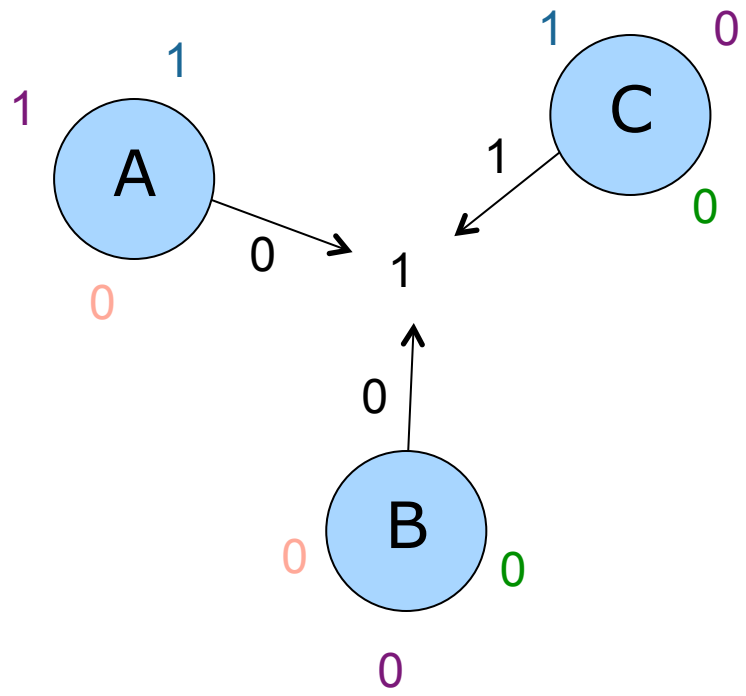
- Proxies zwischenschalten
  - Server erfährt nichts über Client, Proxy kann mitlesen



Grundsätzliche Techniken

- DC-Netz: kombiniert u.a. Broadcast, Kryptographie und Dummy Traffic
  - Schutz des Senders
- Blind-Message-Service: Unbeobachtbare Abfrage aus von unabhängigen Betreibern replizierten Datenbanken
  - Schutz des Clients
- MIX-Netz: kombiniert u.a. hintereinander geschaltete Proxies von unabhängigen Betreibern, Kryptographie und Dummy Traffic
  - Schutz der Kommunikationsbeziehung
  - Effizient in Vermittlungsnetzen
- Steganographie
  - Verbergen einer Nachricht in einer anderen

DC-Netz-Beispiel



- C greift an und weiß, dass er nicht bezahlt hat
  –> A oder C haben bezahlt
- Fall A hat bezahlt:
  1+?+1 = 0
  dann gilt für B:
  0+?+0 = 0
  –> ? = 0
- Fall B hat bezahlt:
  1+?+0 = 0
  dann gilt für A:
  0+?+1 = 0
  –> ? = 1

Beide Möglichkeiten sind gleichwahrscheinlich
–> informationstheoretisch sicher

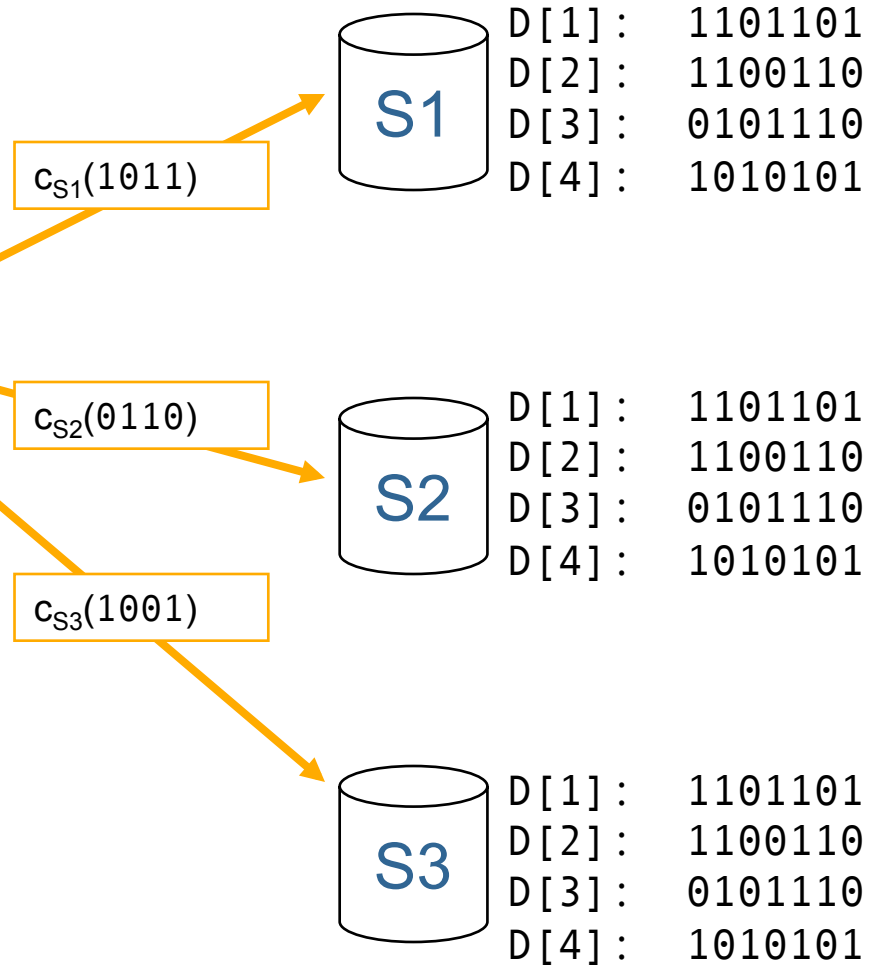
Blind-Message-Service: Anfrage

Cooper, Birman, 1995

Client interessiert sich für D[2]:

Index = 1234

Setze Vektor = 0100
Wähle zufällig request(S1) = 1011
Wähle zufällig request(S2) = 0110
Berechne request(S3) = 1001



- Schutzziel:
  - Client möchte auf Datenbestand zugreifen, ohne dass Datenbank erfährt, wofür sich der Client interessiert
- Replizierte Datenbanken mit unabhängigen Betreibern

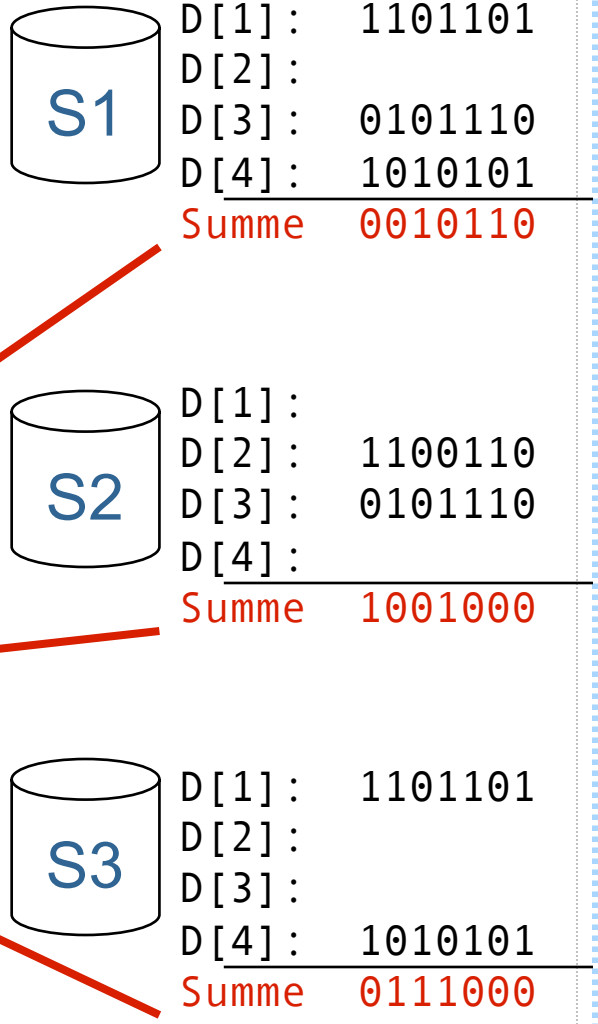
> Blind-Message-Service: Antwort

Cooper, Birman, 1995

Client interessiert sich für D[2]:

Index = 1234

Setze Vektor = 0100
Wähle zufällig request(S1) = 1011
Wähle zufällig request(S2) = 0110
Berechne request(S3) = 1001



Antworten von

S1: 0010110
S2: 1001000
S3: 0111000

Summe entspricht D[2]: 1100110

Verbindungsverschlüsselung zwischen Servern und Client unbedingt notwendig

Problem Rückverfolgung

Taktung: 5 Sek., Zeitpunkte des Kanalaufbaus: (Anonymer Kanal)

2009-02-16 12:30:01	123.456.789	mix2.de:56789
2009-02-16 12:30:02	222.222.222	mix2.de:63543
2009-02-16 12:30:19	333.333.333	mix2.de:15746

Kanäle für Nutzer 1 und 2 werden 12:30:05 aufgebaut, für N

2009-02-
2009-02-
2009-02-

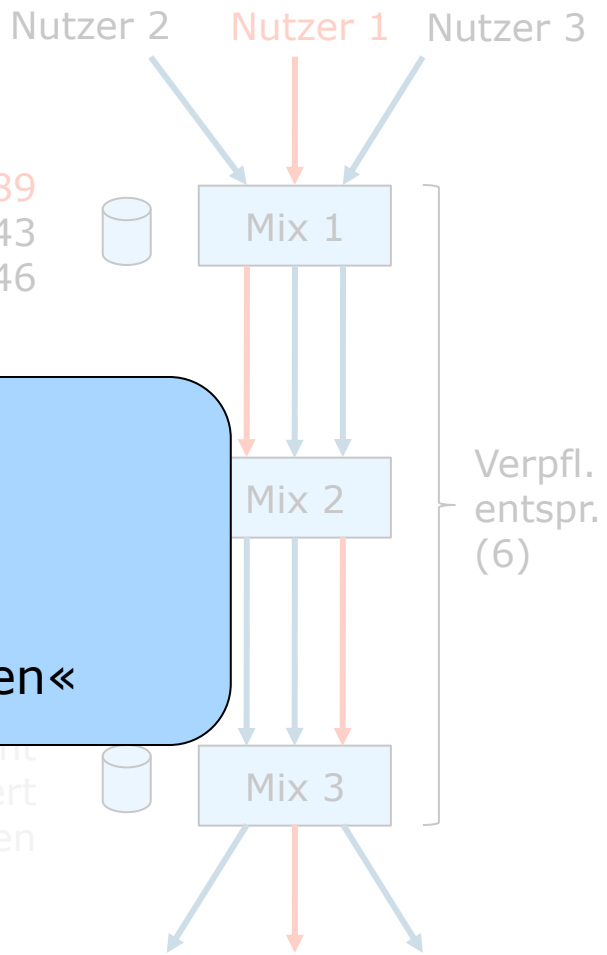
Kanäle für Nutze
aufgebaut, für N

2009-02-16 12:30:10 45997:mix2.de
2009-02-16 12:30:10 25354:mix2.de

Illegale Handlung wird um 12:32 protokolliert

2009-02-16 12:32 angie32 mix3.de

Ergebnis:
- Zeitpunkte des Umschreibens
  - reichen nicht aus bzw.
  - sind nutzlos
- oder es ist nichts »Umzuschreiben«



Fazit

- Viele Maßnahmen zur Verbesserung der Sicherheitslage, Gefahrenabwehr und Kriminalitätsbekämpfung werden hinsichtlich ihrer Wirkung überschätzt.

- Prinzipiell sind auch Maßnahmen akzeptabel, die keinen perfekten Schutz bieten (100%ige Sicherheit gibt es sowieso niemals).

- Das Prinzip der Angemessenheit sollte nicht nur bei Maßnahmen zum technischem Datenschutz beachtet werden, sondern auch bei Maßnahmen, die zur Einschränkung der persönlichen Freiheit führen:

1. keine Massenspeicherung und -überwachung (Grundrechte)
2. Kontrollierbarkeit des Zugriffs (Verlässlichkeit)
3. Überprüfung der Wirksamkeit (Nachhaltigkeit)

Prof. Dr. Hannes Federrath
Lehrstuhl Management der Informationssicherheit
Universität Regensburg
D-93040 Regensburg

E-Mail: hannes.federrath@wiwi.uni-regensburg.de
WWW: http://www-sec.uni-regensburg.de

Phone +49-941-943-2870
Telefax +49-941-943-2888