Technische, ökonomische und rechtliche Aspekte datenschutzfreundlicher Techniken

Aachen, 25.10.2006

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

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

Gliederung

- Einordnung
- Technische Aspekte
  - Welche technischen Bausteine stehen zur Unterstützung von Datenschutzanforderungen zur Verfügung?
- Ökonomische Aspekte
  - Wie ist der Bedarf an datenschutzfreundlichen Techniken aus der Sicht der Betroffenen einzuschätzen?
- Rechtliche Aspekte
  - Wie sind die rechtlichen Rahmenbedingungen und welche »Sekundäreffekte« hat der Einsatz solcher Verfahren?

Schutzziele

Kommunikationsgegenstand **WAS?**	**Kommunikationsumstände** **WANN?, WO?, WER?**
Vertraulichkeit **Inhalte**	**Anonymität** **Unbeobachtbarkeit** **Sender** **Ort** **Empfänger**

- Schutzziele — Vertraulichkeit
  - Schutz der Nachrichteninhalte
  - Schutz der Identität eines Nutzers während der Dienstnutzung
    - Beispiel: Beratungsdienste
  - Schutz der Kommunikationsbeziehungen der Nutzer
    - Nutzer kennen möglicherweise gegenseitig ihre Identität

Angreifermodell: Datenschutzfördernde Technik

Kommunikationsgegenstand WAS?	**Kommunikationsumstände WANN?, WO?, WER?**
Vertraulichkeit	**Anonymität Unbeobachtbarkeit**
Inhalte	**Sender**, **Ort**, **Empfänger**

- Outsider
  - Abhören auf Kommunikationsleitungen
  - Verkehrsanalysen
- Insider
  - Netzbetreiber oder bösartige Mitarbeiter (Verkehrsprofile)
  - Staatliche Organisationen

Prinzipien: Datenschutzfördernde Technik

Kommunikationsgegenstand WAS?	**Kommunikationsumstände WANN?, WO?, WER?**
Vertraulichkeit	**Anonymität Unbeobachtbarkeit**
Inhalte	**Sender**, **Ort**, **Empfänger**

- Datenvermeidung
  - Erfassungsmöglichkeit und Speicherung personenbezogener Daten vermeiden
- Datensparsamkeit
  - Jeder behält seine personenbezogenen Daten in seinem persönlichen Verfügungsbereich.

Gliederung

- Einordnung
- Technische Aspekte
  - Welche technischen Bausteine stehen zur Unterstützung von Datenschutzanforderungen zur Verfügung?
- Ökonomische Aspekte
  - Wie ist der Bedarf an datenschutzfreundlichen Techniken aus der Sicht der Betroffenen einzuschätzen?
- Rechtliche Aspekte
  - Wie sind die rechtlichen Rahmenbedingungen und welche »Sekundäreffekte« hat der Einsatz solcher Verfahren?

Bausteine datenschutzfördernder Technik

- Verschlüsselung
- Schutz von Kommunikationsbeziehungen
  - Schutz vor Outsidern
    - Proxies
  - Schutz vor Insidern
    - Broadcast
    - Blind message service
    - DC network
    - MIX network
- Schutz von Transaktionen
  - Pseudonyme
  - Credentials (an Pseudonyme gekettete Eigenschaften)

Historische Entwicklung

Jahr	Idee / PET system
1978	Public-key encryption
1981	MIX, Pseudonyms
1983	Blind signature schemes
1985	Credentials
1988	DC network
1990	Privacy preserving value exchange
1991	ISDN-Mixes
1995	Blind message service
1995	Mixmaster
1996	MIXes in mobile communications
1996	Onion Routing
1997	Crowds Anonymizer
1998	Stop-and-Go (SG) Mixes introduced
1999	Zeroknowledge Freedom Anonymizer
2000	*AN.ON/JAP Anonymizer*
2004	TOR

Grundverfahren
Anwendung

Broadcast

- Das war damals...

  - Zeitung lesen
  - Radio über Antenne hören
  - Fernsehen über Breitbandverteilkabel

- Verteilung (Broadcast) + implizite Adressierung
  - Technik zum Schutz des Empfängers
  - Alle Teilnehmer erhalten alles
  - Lokale Auswahl
  - Es bleibt verborgen, welchen Inhalt der Nutzer konsumiert

Vermittelter Zugang zu Inhalten

- Heute:
  - Video on Demand
  - Internet-Radio
  - Zeitungen online
- Damals: (Broadcast)
  - Zeitung lesen
  - Radio über Antenne hören
  - Fernsehen über Breitbandverteilkabel
- Plötzlich stehen Nutzungsdaten zur Verfügung
- Der Kunde wird gläsern.

- Verteilung (Broadcast) + implizite Adressierung
  - Technik zum Schutz des Empfängers
  - Alle Teilnehmer erhalten alles
  - Lokale Auswahl
  - Es bleibt verborgen, welchen Inhalt der Nutzer konsumiert

Vermittelter Zugang zu Inhalten

- Heute:
  - Video on Demand
  - Internet-Radio
  - Zeitungen online
- Damals: (Broadcast)
  - Zeitung lesen
  - Radio über Antenne hören
  - Fernsehen über Breitbandverteilkabel
- Plötzlich stehen Nutzungsdaten zur Verfügung
- Der Kunde wird gläsern.

- Entweder
  - Beibehaltung des vorhandenen Verteilsystems

  oder
  - zusätzliche Schutzfunktionen zur Wahrung des Datenschutzes erforderlich

Mix-Netz (Chaum, 1981)

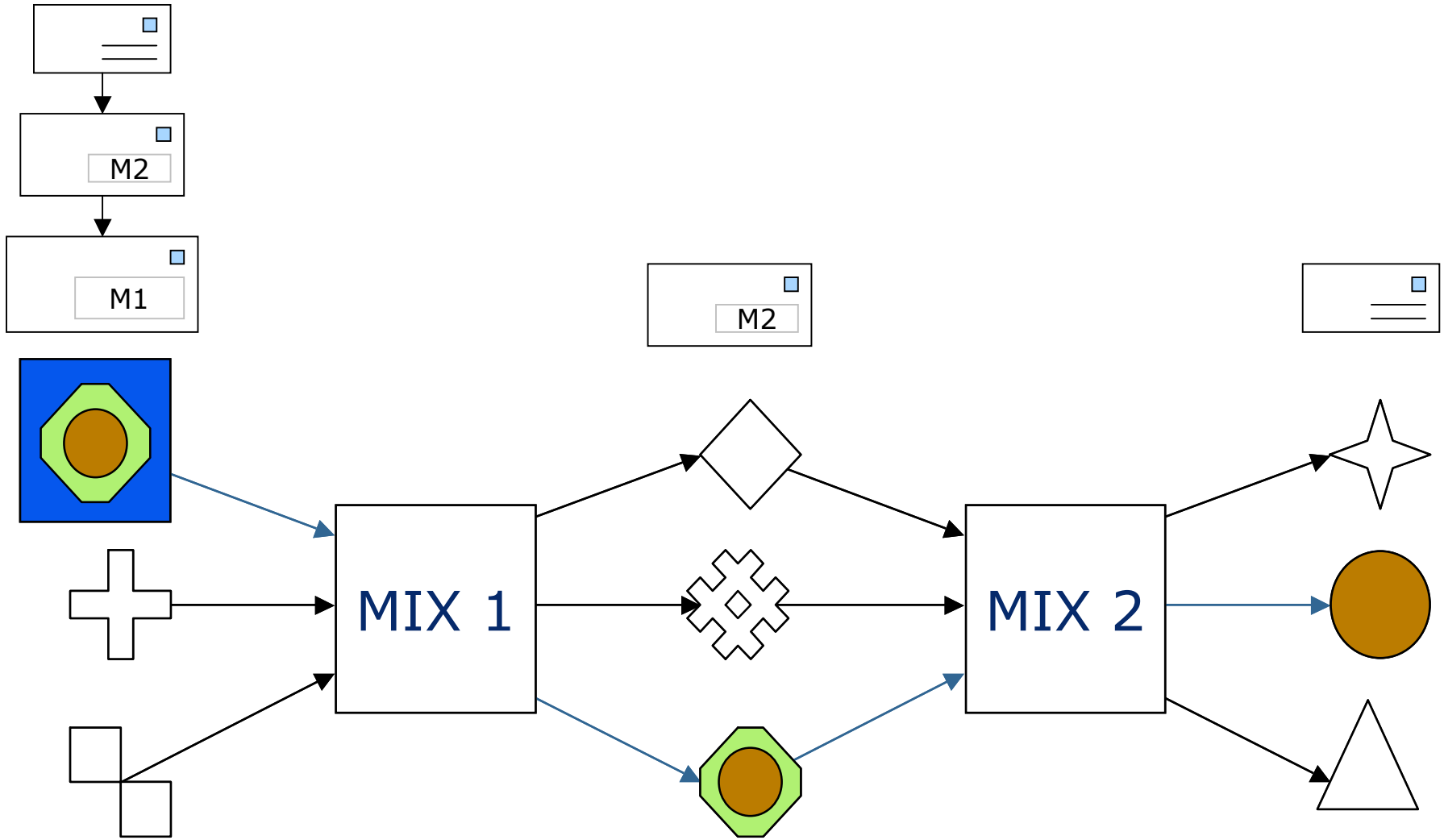
- System zum Schutz von Kommunikationsbeziehungen bei vermittelter Kommunikation

- Grundfunktionen:
  - Nachrichten in einem »Schub« sammeln,
  - Wiederholungen ignorieren,
  - Nachrichten umkodieren,
  - umsortieren,
  - gemeinsam ausgeben
  - Alle Nachrichten haben die gleiche Länge.
  - Mehr als einen Mix und unterschiedliche Betreiber verwenden
  - Wenigstens ein Mix darf nicht angreifen.

- Schutzziel:
  - Unverkettbarkeit von Sender und Empfänger

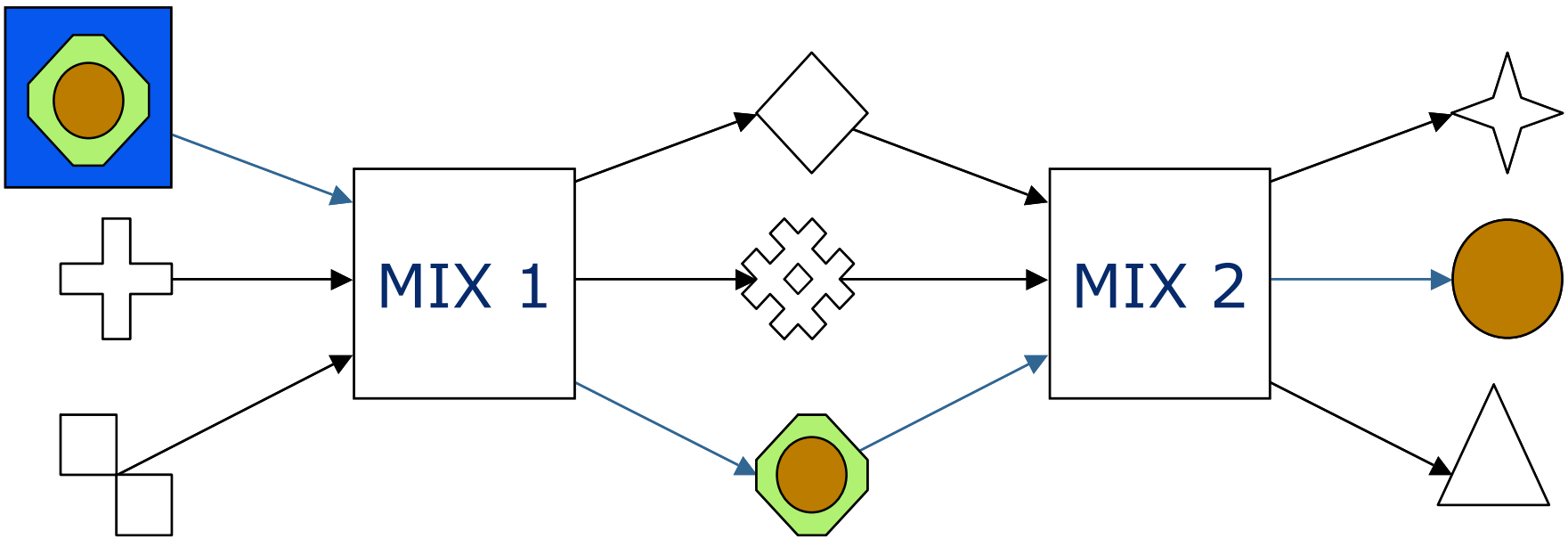
Mix-Netz (Chaum, 1981)

- System zum Schutz von Kommunikationsbeziehungen bei vermittelter Kommunikation

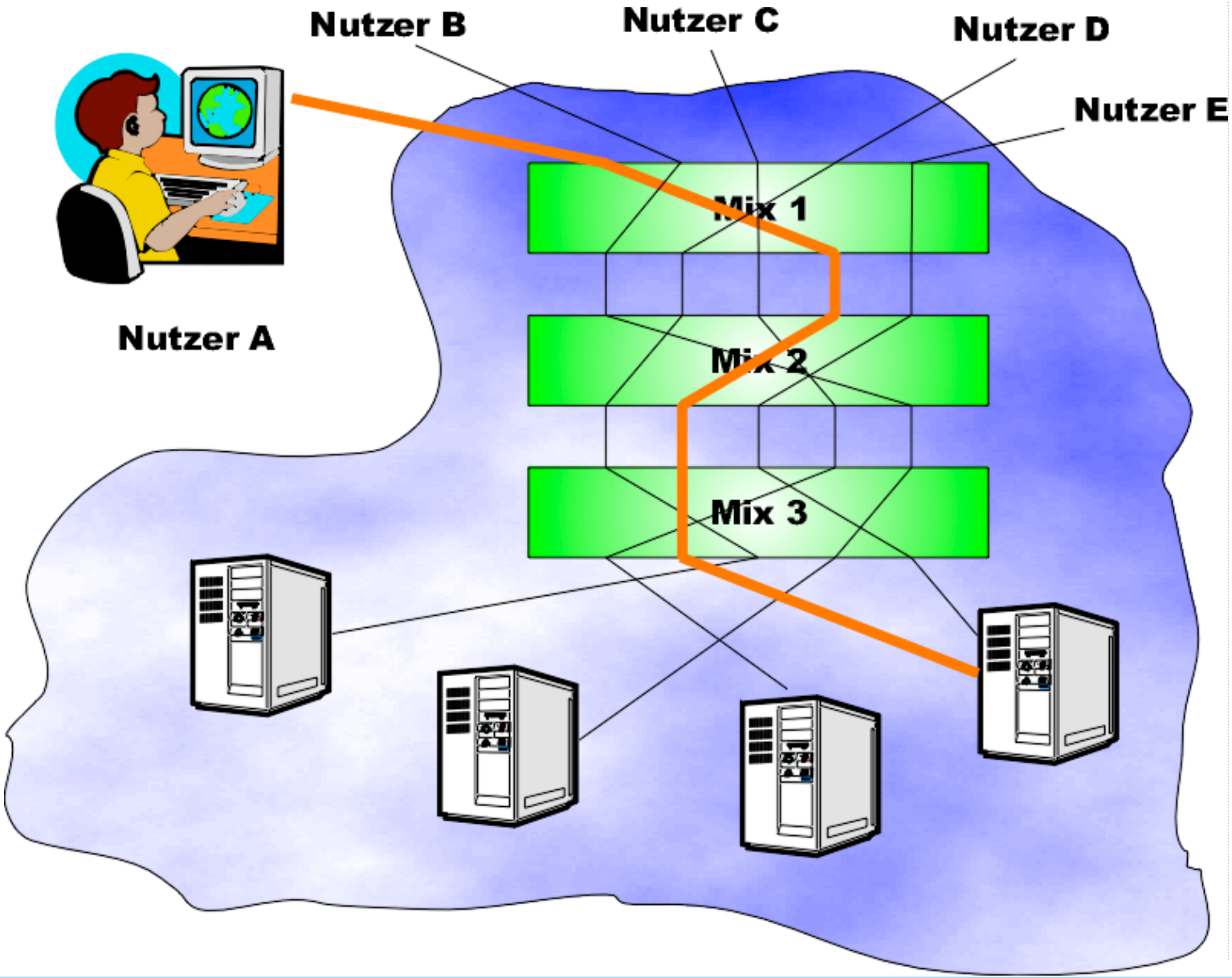


Mix-Netz (Chaum, 1981)

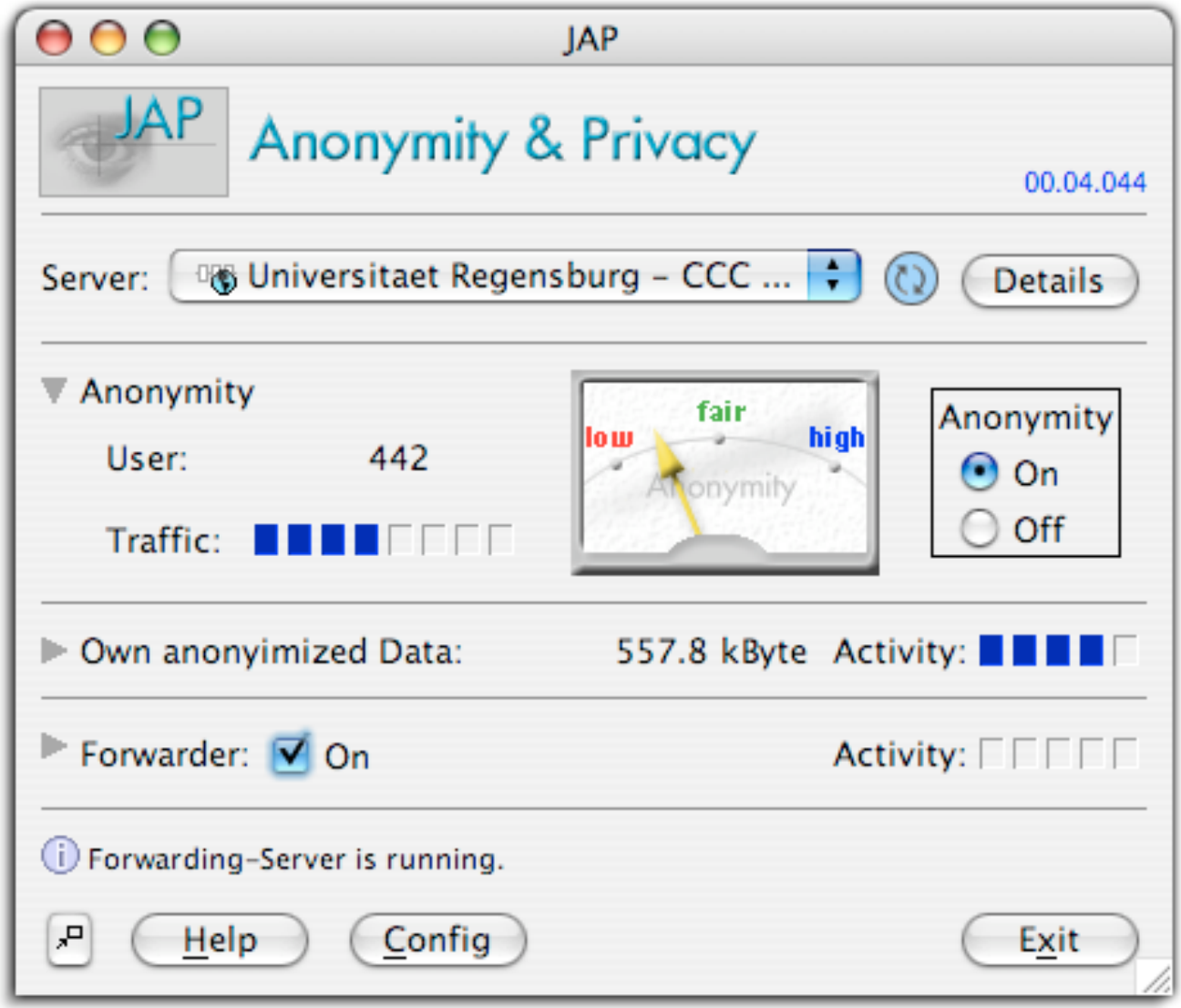
- System zum Schutz von Kommunikationsbeziehungen bei vermittelter Kommunikation
  - Stärke der Mixe:
    - Auch die Betreiber der Mixe erfahren nichts mehr über die Kommunikationsbeziehung zwischen Sender und Empfänger.



Nutzbarmachung der Mixe für Webzugriff

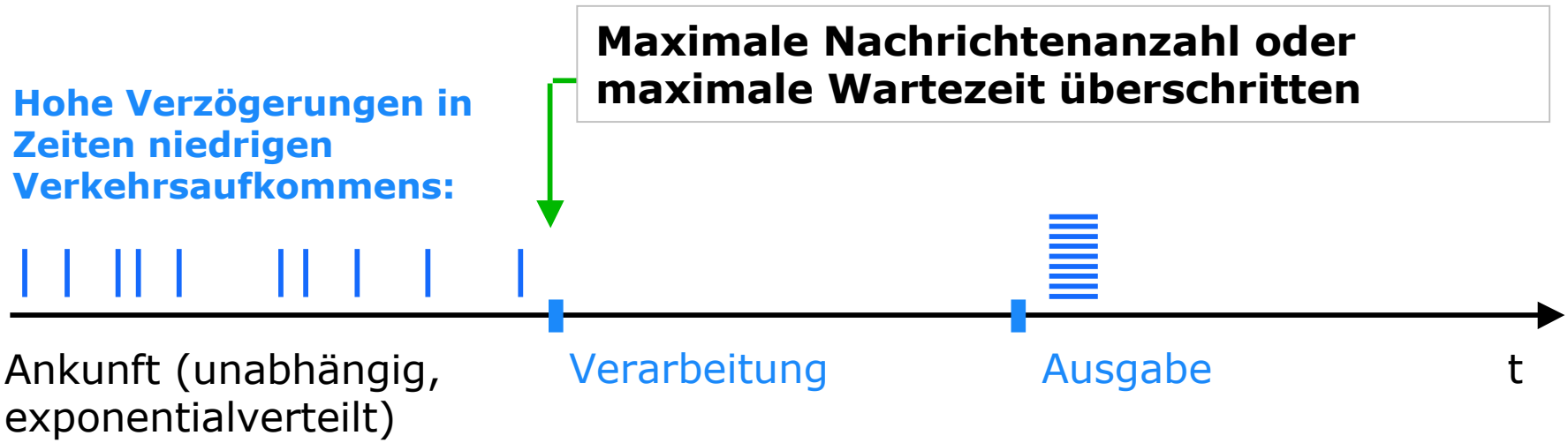


AN.ON/JAP


JAP
JAP
Anonymity & Privacy
00.04.044
Server:
Universitaet Regensburg - CCC ...
Details
Anonymity
User:
442
Traffic:
low
fair
high
Anonymity
Anonymity
On
Off
Own anonymized Data:
557.8 kByte
Activity:
Forwarder:
On
Activity:
Forwarding-Server is running.
Help
Config
Exit

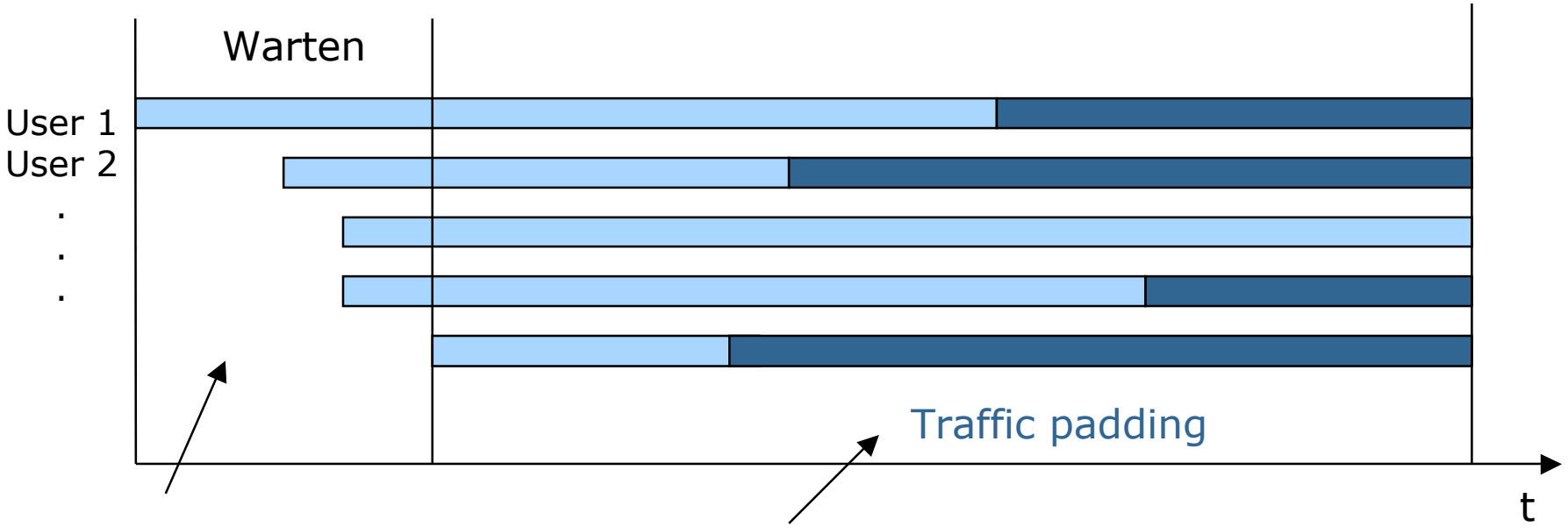
Echtzeitkommunikation und Mixe

- Mixe sind gut geeignet für wenig zeitkritische Dienste:
  - E-Mail
- Für Echtzeitkommunikation sind Modifikationen nötig:
  - Nachrichten sammeln führt zu starken Verzögerungen, da der Mix die meiste Zeit auf andere Nachrichten wartet
  - Nachrichtenlängen und Kommunikationsdauer variieren bei verbindungsorientierten Diensten stark
- Veränderungen nötig



Traffic padding

- Ziel: Verbergen, wann eine Kommunikation beginnt und endet
- Problem: Niemand weiß, wann der letzte Nutzer seine Kommunikation beenden möchte



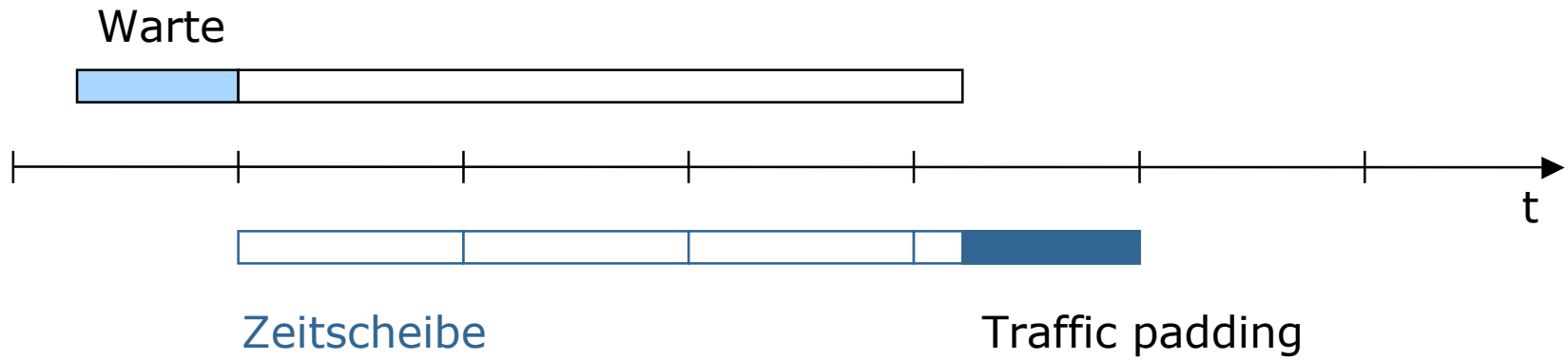
1. Warten, bis genügend Benutzer kommunizieren wollen (Bilden der Anonymitätsgruppe)
   Beispiel: 5 Nutzer

2. Nach Kommunikationsende senden die Nutzer solange Zufallszahlen, bis der letzte Nutzer seine Kommunikation beendet.

3. Problem: Niemand weiß, wann der letzte Nutzer seine Kommunikation beenden möchte, da niemand echte Nachrichten von Traffic padding unterscheiden kann.

Zerlegen der Kommunikation in Zeit-/Volumenscheiben

- Zeitscheiben (Pfitzmann et. al. 1989)
  - Unbeobachtbarkeit innerhalb der Gruppe aller Nachrichten einer Zeitscheibe
  - Längere Kommunikationsverbindungen setzen sich aus mehreren Zeitscheiben zusammen
  - Zeitscheiben sind nicht verkettbar für Angreifer



- Volumenscheiben (Federrath et. al. 2000)
  - adaptive Anpassung der Scheibengröße in Abhängigkeit der aktuellen Verkehrssituation
  - Minimieren des Overheads

Gliederung

- Einordnung

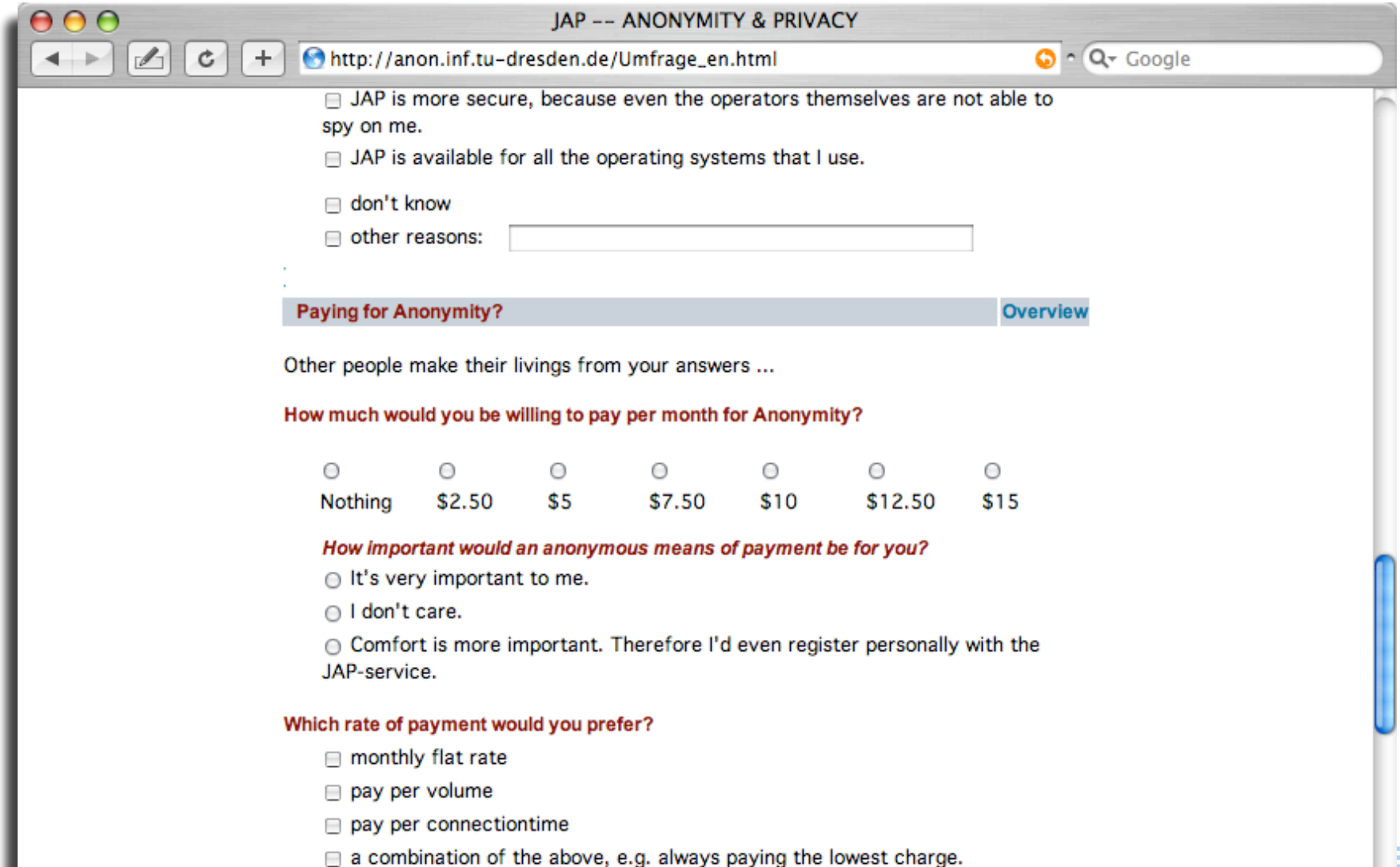
- Technische Aspekte
  - Welche technischen Bausteine stehen zur Unterstützung von Datenschutzanforderungen zur Verfügung?

- Ökonomische Aspekte
  - Wie ist der Bedarf an datenschutzfreundlichen Techniken aus der Sicht der Betroffenen einzuschätzen?

- Rechtliche Aspekte
  - Wie sind die rechtlichen Rahmenbedingungen und welche »Sekundäreffekte« hat der Einsatz solcher Verfahren?

Umfrage unter JAP-Benutzern (Spiekermann, 2003)

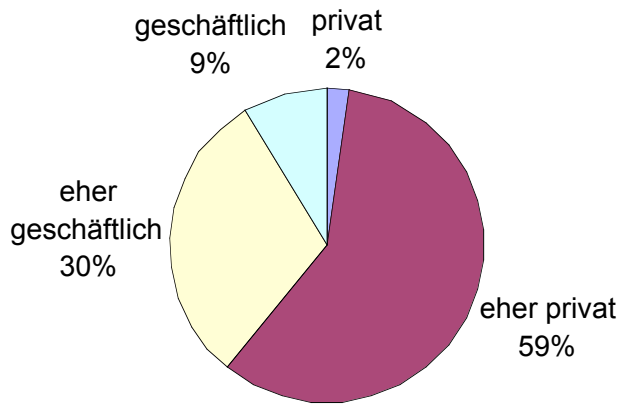
- Stichprobe:
  - 1800 JAP-Nutzer



Umfrage unter JAP-Benutzern

- Gründe für die Nutzung
  - ≈ 31% Free speech
  - ≈ 54% Schutz vor Geheimdiensten
  - ≈ 85% Schutz vor Profiling (Webnutzung)
  - ≈ 64% Schutz vor eigenem ISP

- Private oder geschäftliche Nutzung?
  - ≈ 2% ausschließlich privat
  - ≈ 59% überwiegend privat
  - ≈ 30% überwiegend geschäftlich
  - ≈ 9% ausschließlich geschäftlich



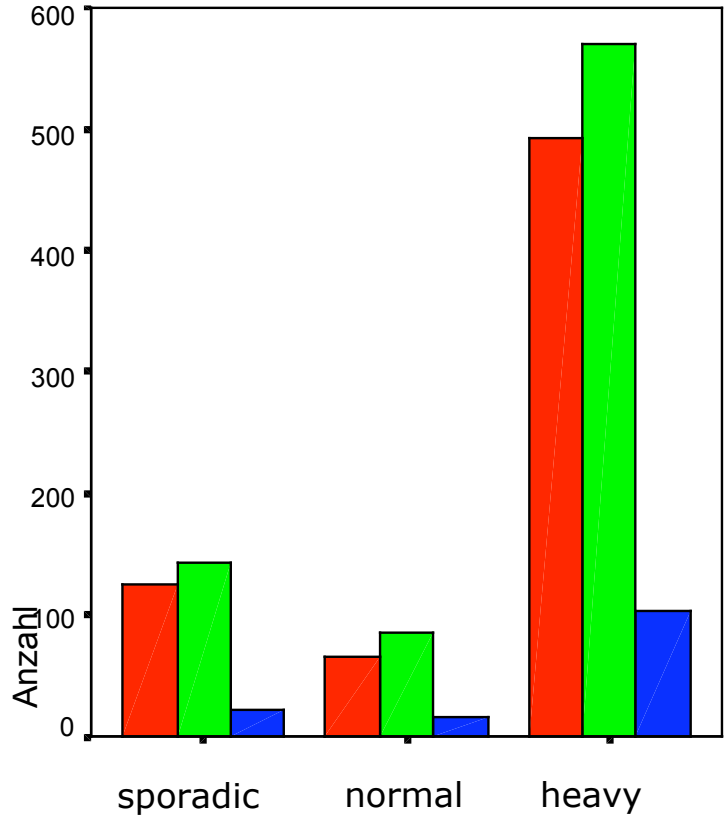
- Warum JAP?
  - ≈ 76% kostenlos
  - ≈ 56% schützt vor Betreibern
  - ≈ 51% einfach benutzbar

Umfrage unter JAP-Benutzern

- Zahlungsbereitschaft für Anonymität
  - ≈ 40% keine
  - ≈ 50% monatlich zwischen € 2,5 … € 5
  - ≈ 10% mehr als € 5 pro Monat

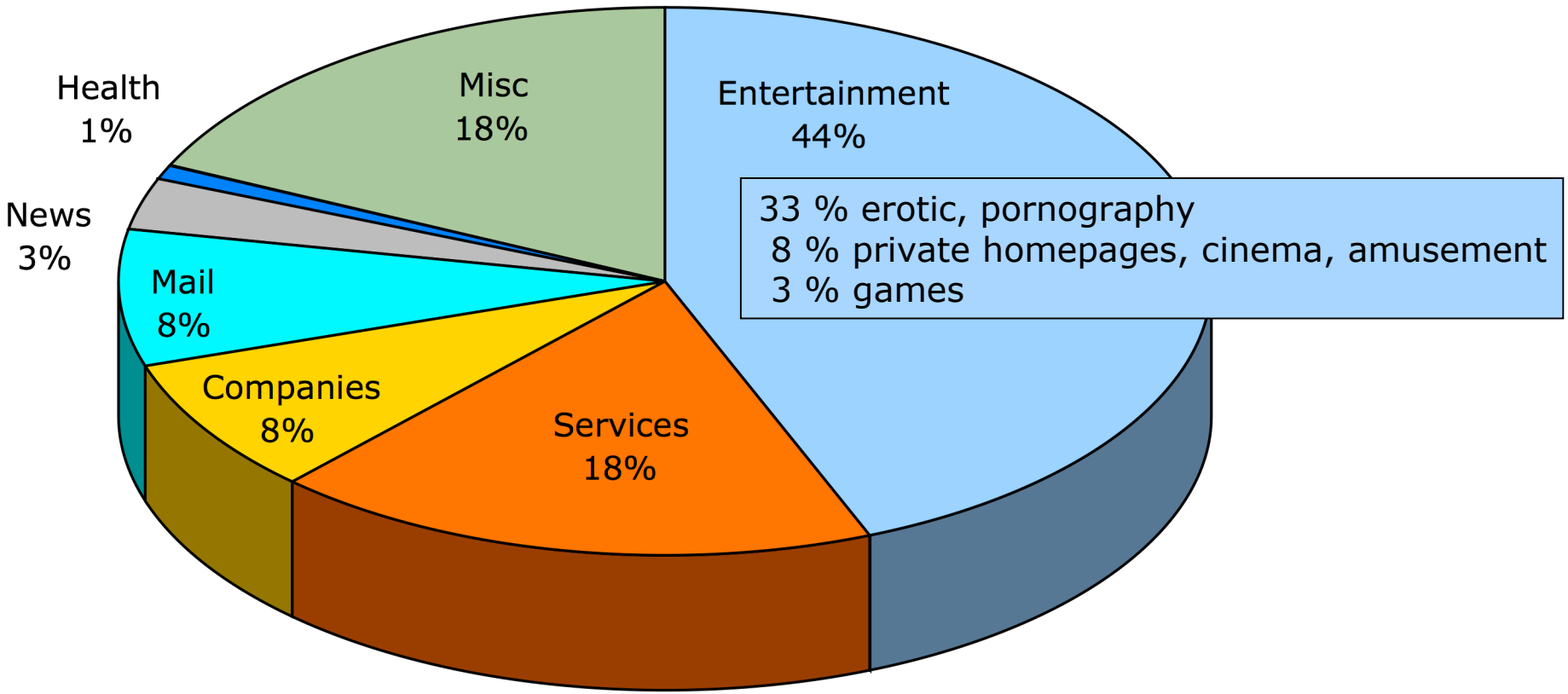
- Zahlungsbereitschaft korreliert nicht mit der Intensität der Nutzung

- Intensität der Nutzung
  - ≈ 73% heavy: tägliche Nutzung
  - ≈ 10% «normal»: ≥ 2x pro Woche
  - ≈ 17% sporadic: < 2x pro Woche



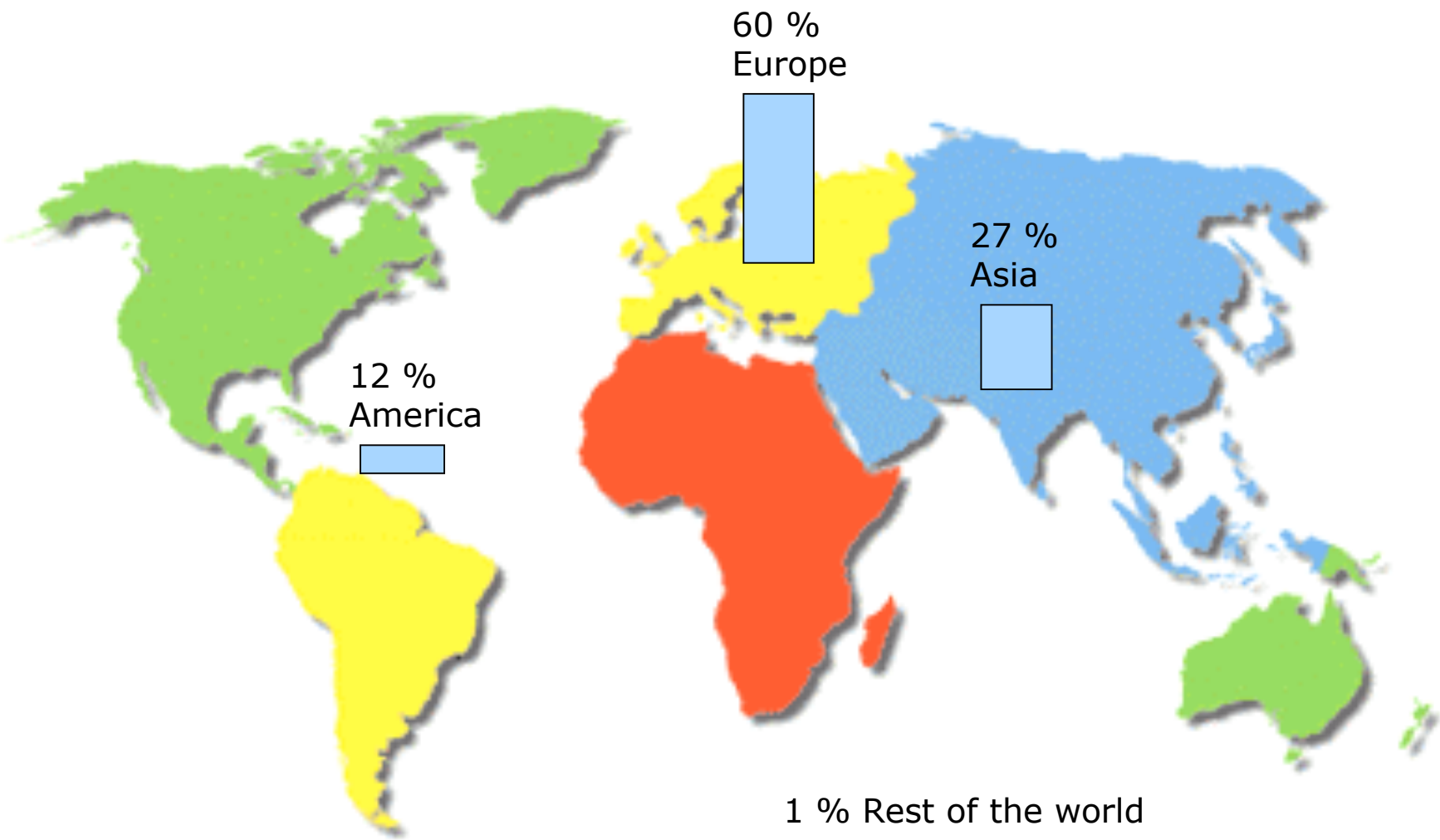
Anonymisierte Inhalte

- Zuordnung von 150 zufällig ausgewählten Requests aus mehreren Millionen Zugriffen im Juni 2005

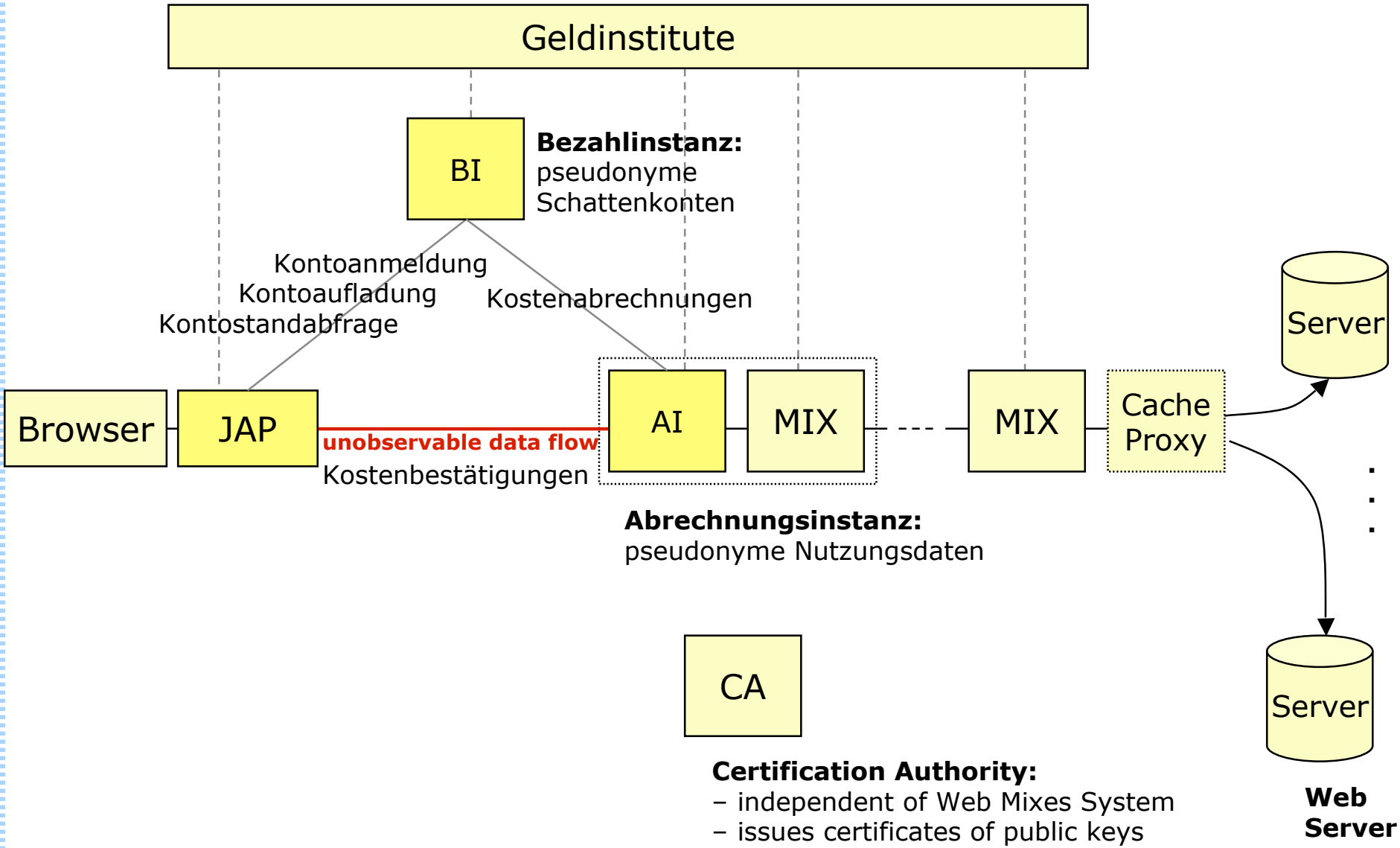


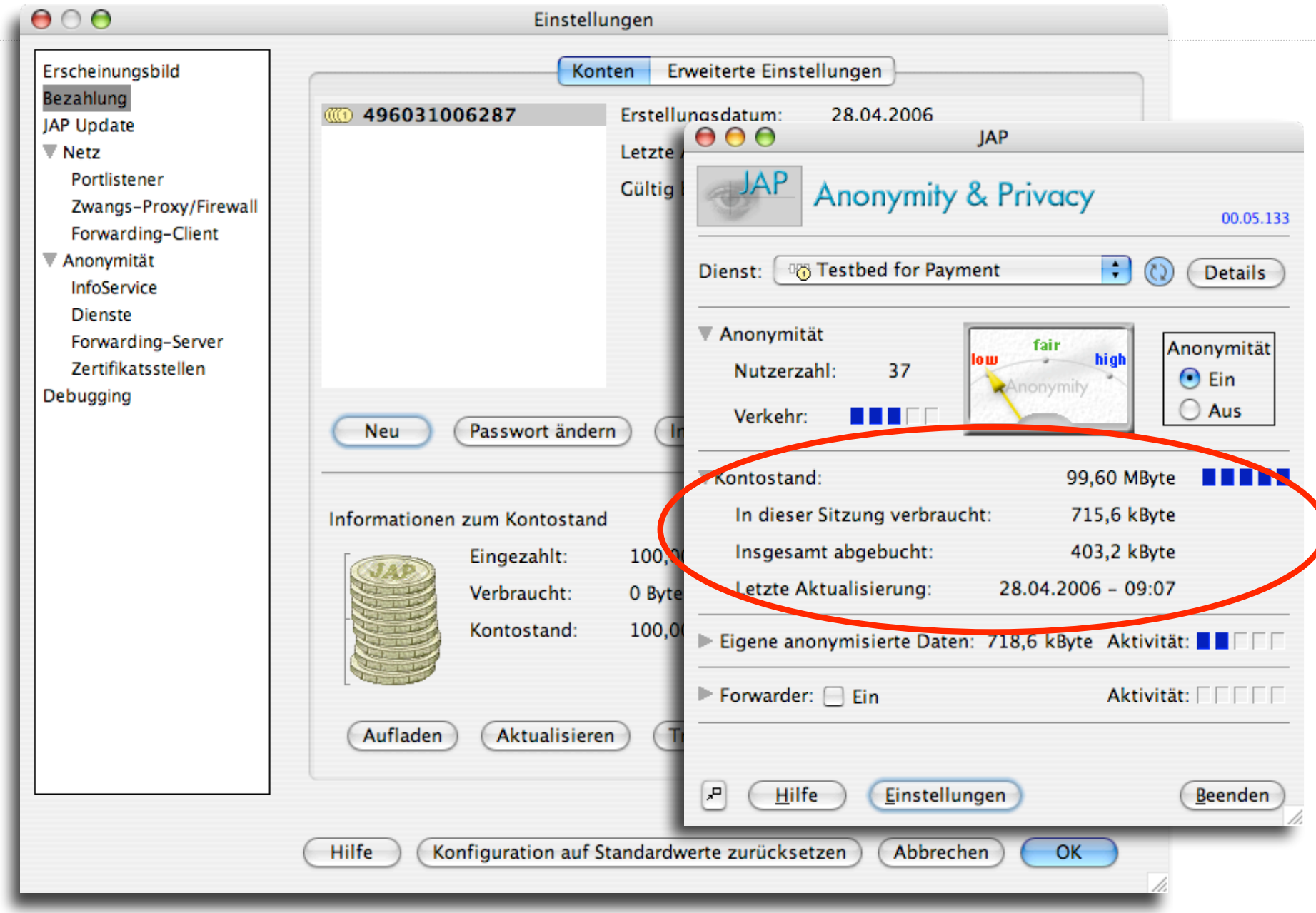
Wo kommen die JAP-Nutzer her?

- Eingehende Requests nach Regionen Mai-Juni 2005



Architektur Bezahlsystem



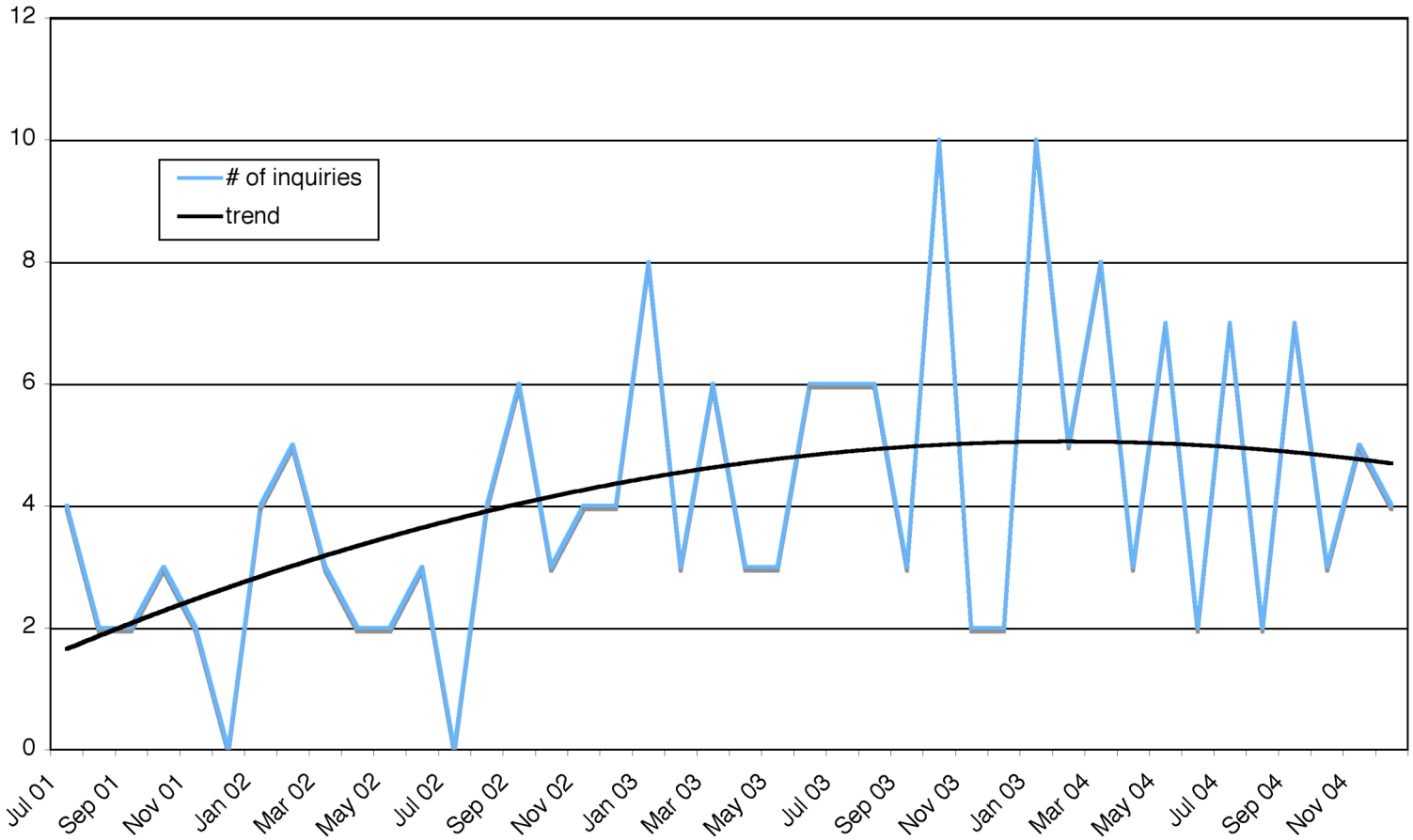

Einstellungen
Erscheinungsbild
Bezahlung
JAP Update
Netz
Portlistener
Zwangs-Proxy/Firewall
Forwarding-Client
Anonymität
InfoService
Dienste
Forwarding-Server
Zertifikatsstellen
Debugging
Konten
Erweiterte Einstellungen
496031006287
Erstellungsdatum: 28.04.2006
Neu
Passwort ändern
Informationen zum Kontostand
Eingezahlt:
Verbraucht: 0 Byte
Kontostand:
Aufladen
Aktualisieren
Hilfe
Konfiguration auf Standardwerte zurücksetzen
Abbrechen
OK
JAP
Anonymity & Privacy
00.05.133
Dienst: Testbed for Payment
Details
Anonymität
Nutzerzahl: 37
Verkehr:
low
fair
high
Anonymity
Anonymität
Ein
Aus
Kontostand: 99,60 MByte
In dieser Sitzung verbraucht: 715,6 kByte
Insgesamt abgebucht: 403,2 kByte
Letzte Aktualisierung: 28.04.2006 - 09:07
Eigene anonymisierte Daten: 718,6 kByte Aktivität:
Forwarder: Ein Aktivität:
Hilfe
Einstellungen
Beenden

Gliederung

- Einordnung
- Technische Aspekte
  - Welche technischen Bausteine stehen zur Unterstützung von Datenschutzanforderungen zur Verfügung?
- Ökonomische Aspekte
  - Wie ist der Bedarf an datenschutzfreundlichen Techniken aus der Sicht der Betroffenen einzuschätzen?
- Rechtliche Aspekte
  - Wie sind die rechtlichen Rahmenbedingungen und welche »Sekundäreffekte« hat der Einsatz solcher Verfahren?

Missbrauch und Strafverfolgung AN.ON/JAP

- durchschnittlich 4-5 Anfragen von Strafverfolgern und Privatpersonen pro Monat



Analyse der missbräuchlichen Benutzung von JAP

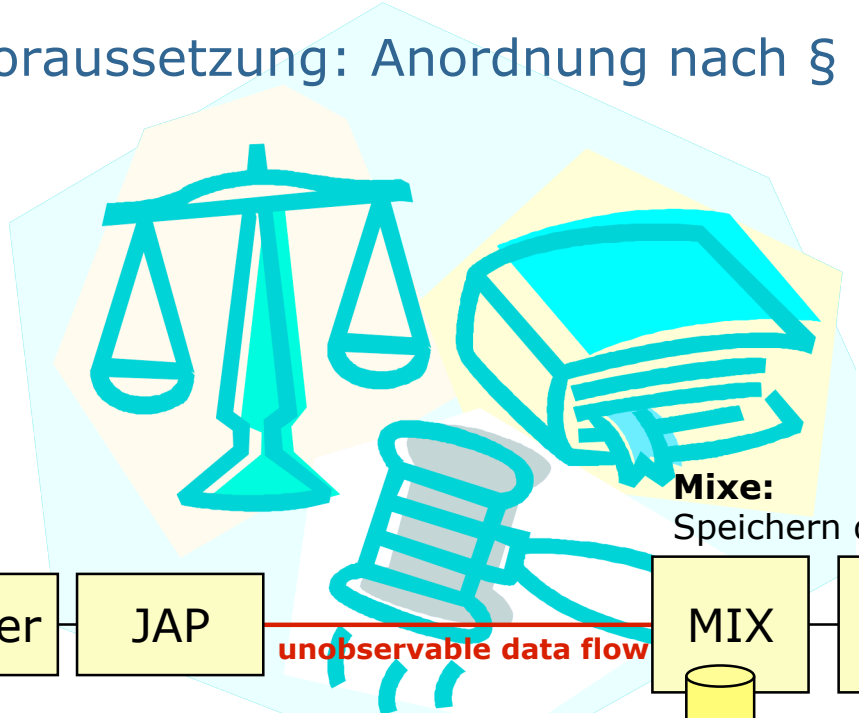
- Wie ist eine Anfrage aufgebaut?
  - Von einem Webserver mitprotokollierte IP-Adresse des JAP-Dienstes, Datum und genaue Uhrzeit der missbräuchlichen Nutzung
  - Meist kurze Angabe des Verdachts
    - Kreditkartenbetrug,
    - Computerbetrug,
    - Datenveränderung,
    - Computersabotage,
    - Beleidigung,
    - Verleumdung,
    - Morddrohung,
    - Abruf kinderpornographischer Inhalte
  - Entweder richterliche Anordnung, »Gefahr im Verzug« oder Voranfrage

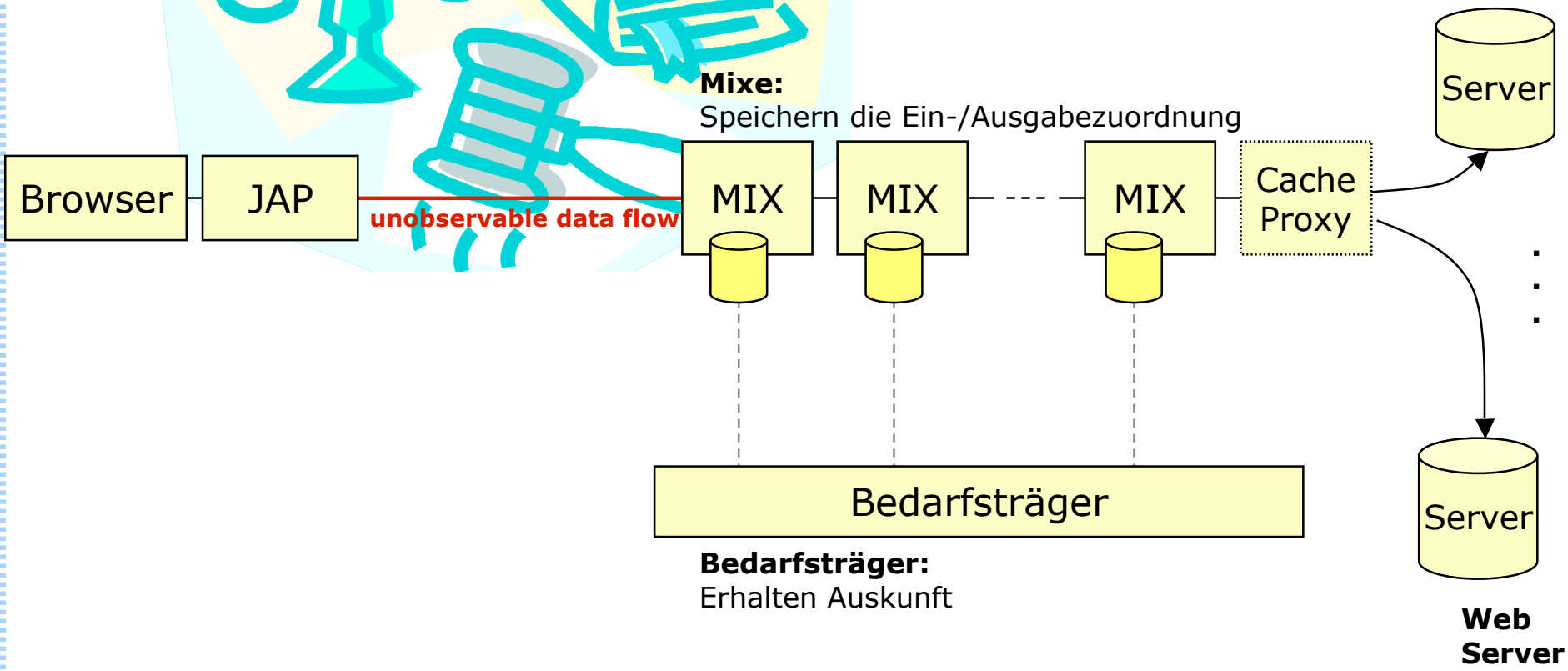
Anonyme Kommunikation ist legal

- Teledienstedatenschutzgesetz (TDDSG)
  - § 4 Absatz 6: Der Diensteanbieter hat dem Nutzer die Inanspruchnahme von Telediensten und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeit zu informieren.

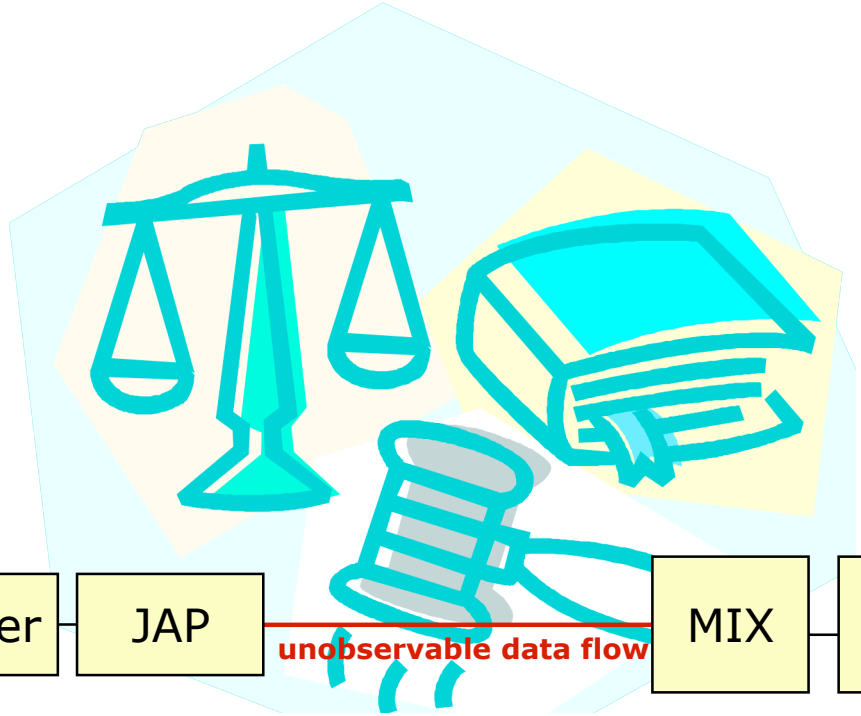
Strafverfolgung bei schweren Straftaten

- Voraussetzung: Anordnung nach § 100a,b StPO

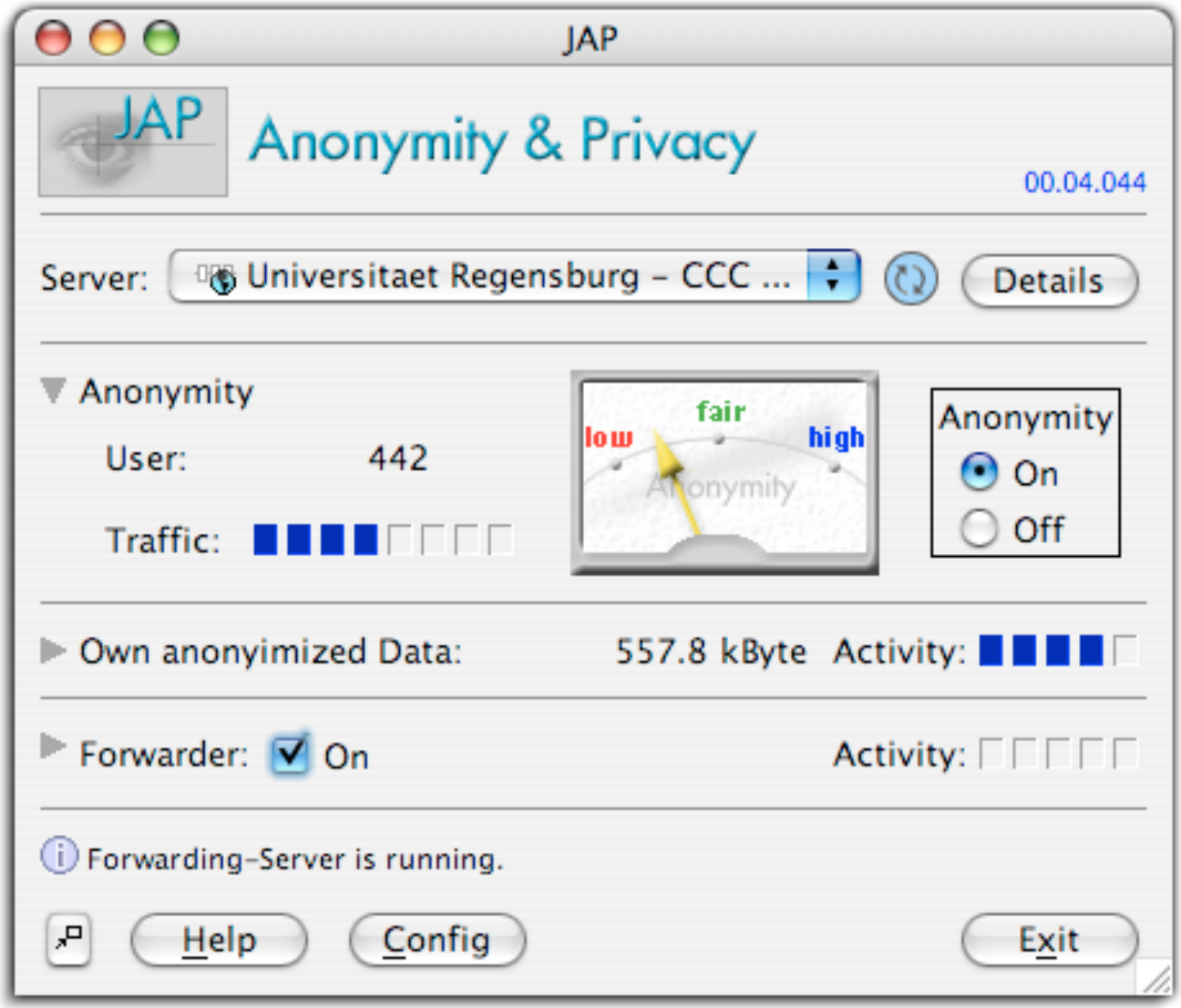




Prävention ist besser als Strafverfolgung



AN.ON/JAP



Ziele:

Schaffen einer praktikablen Lösung für anonyme und unbeobachtbare Basiskommunikation

Schutz auch vor dem Betreiber des Dienstes (Schutz vor Insidern)

OpenSource

>10.000 Nutzer

>6 TB/Monat

www.anon-online.de

AN.ON/JAP

Förderer: BMWi, Projektpartner: TU Dresden, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, FU Berlin, HU Berlin, Universität Regensburg, Medizinische Universität Lübeck, Chaos Computer Club, Ulmer Akademie für Datenschutz und IT-Sicherheit, RWTH Aachen, New York University

Ziele:

Schaffen einer praktikablen Lösung für anonyme und unbeobachtbare Basiskommunikation

Schutz auch vor dem Betreiber des Dienstes (Schutz vor Insidern)

OpenSource

>10.000 Nutzer

>6 TB/Monat

www.anon-online.de