AN.ON – Anonymität.Online

Technische Ergebnisse und Verwertung

Berlin, BMWi, 28. April 2006

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

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

Schutzziele

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

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**

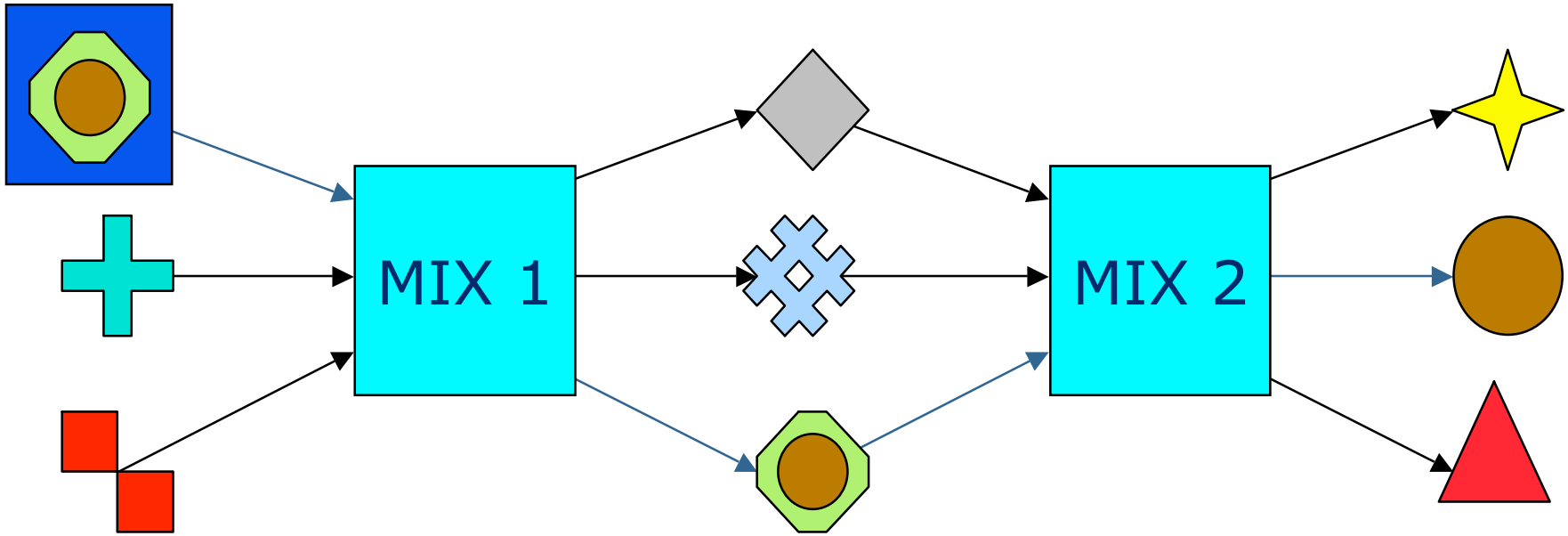
- Datenvermeidung
  - Erfassungsmöglichkeit und Speicherung personenbezogener Daten vermeiden
- Datensparsamkeit
  - Jeder behält seine personenbezogenen Daten in seinem persönlichen Verfügungsbereich.

Schutz von Kommunikationsbeziehungen

- Schutz vor Outsidern
  - Proxies
- Schutz vor Insidern
  - Broadcast
  - Blind message service
  - DC network
  - MIX network

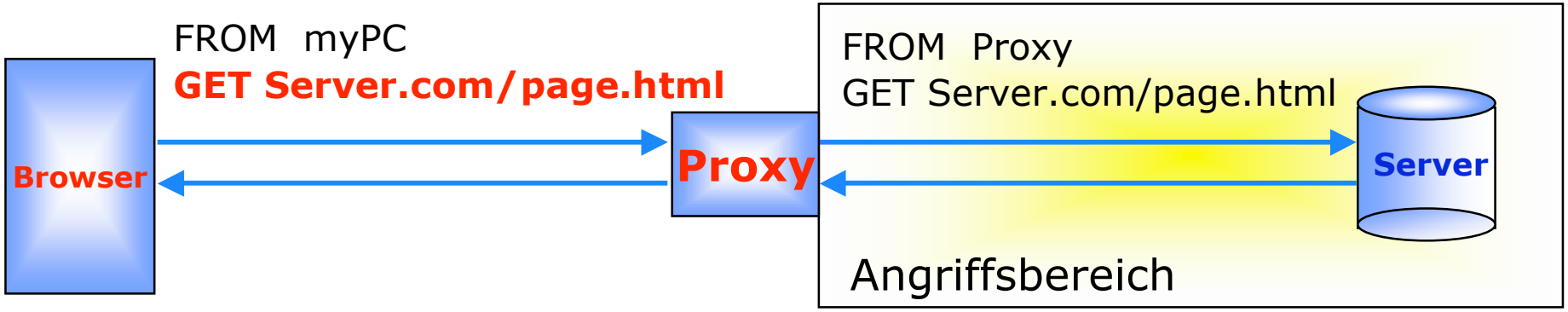
Mix-Netz (Chaum, 1981)

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



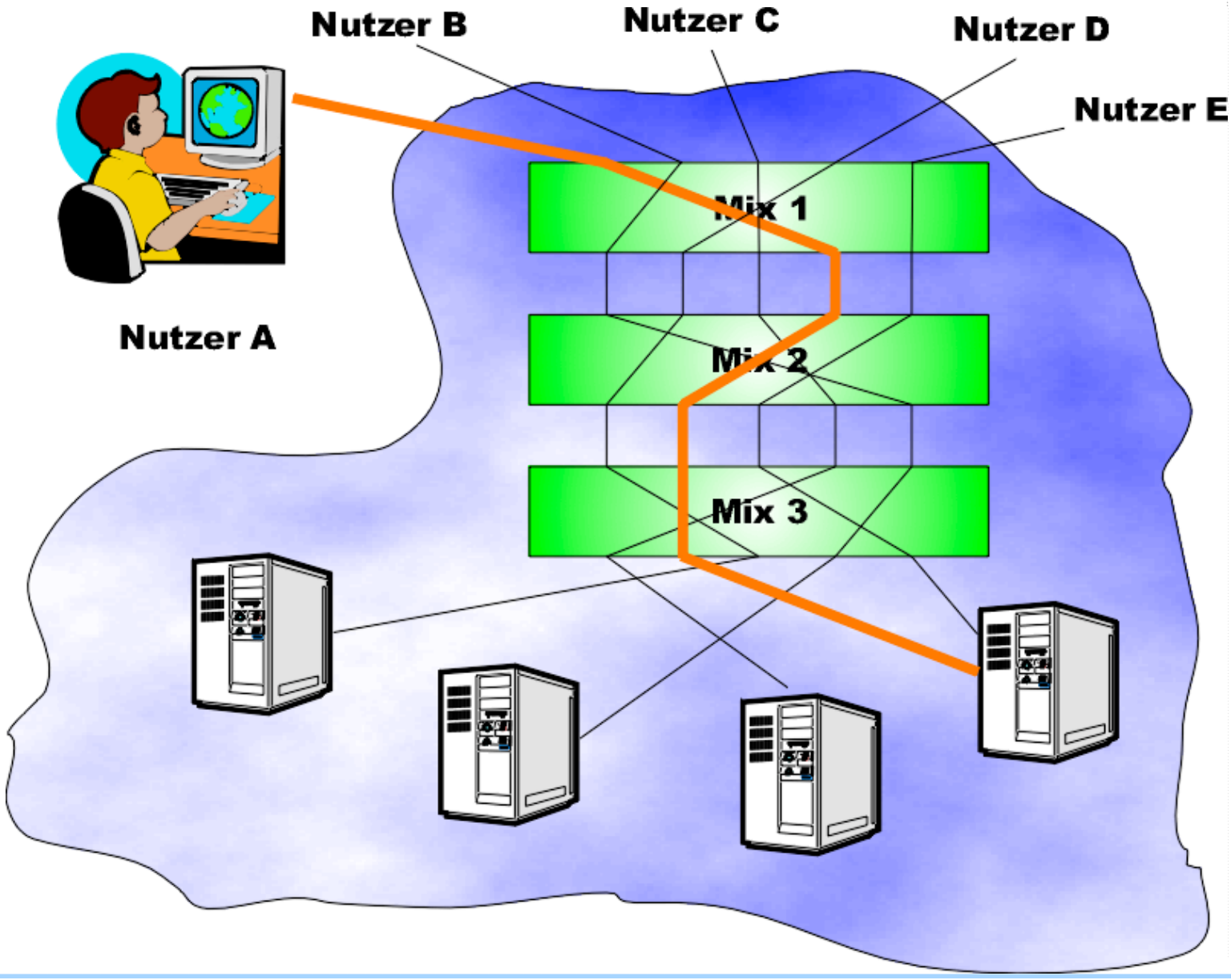
Proxies

- Schwacher Schutz vor Outsidern
  - schützt nicht gegen Verkehrsanalysen
  - selbst Verschlüsselung hilft nichts



  - Vertrauen in Proxy nötig
  - Proxy kann beobachten

Nutzbarmachung der Mixe für Webzugriff

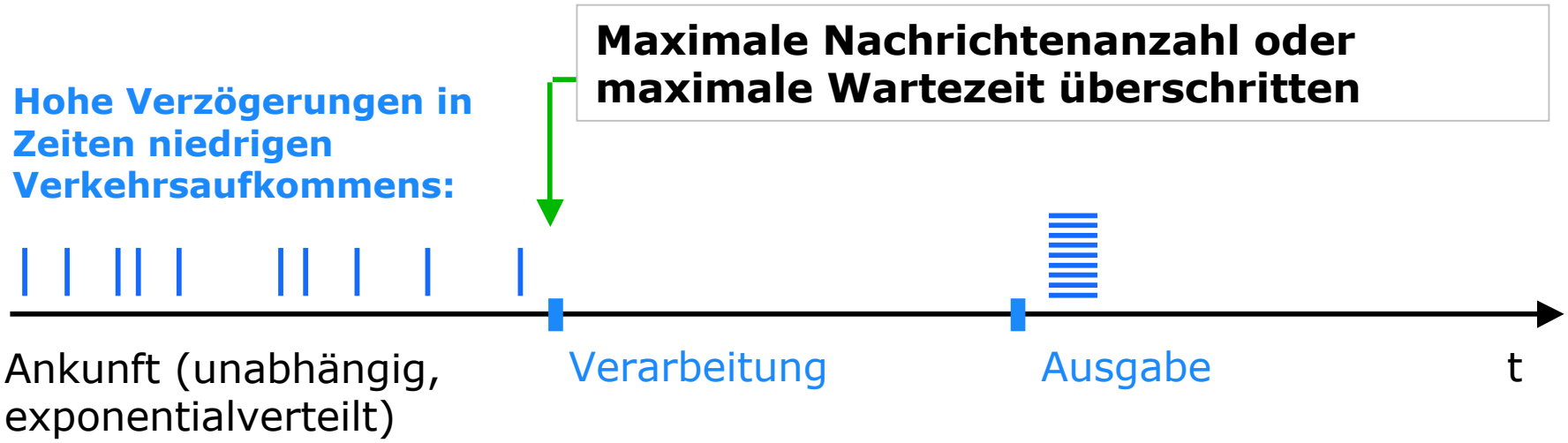


Herausforderungen aus technischer Sicht

- Adaption der Mixe auf Echtzeitkommunikation
- Transparenz für den Nutzer
- Dezentrale Architektur des Gesamtsystems
- Abrechnung anonym genutzter Dienste
- Stärkung des Nutzers bei gleichzeitiger Strafverfolgungsmöglichkeit

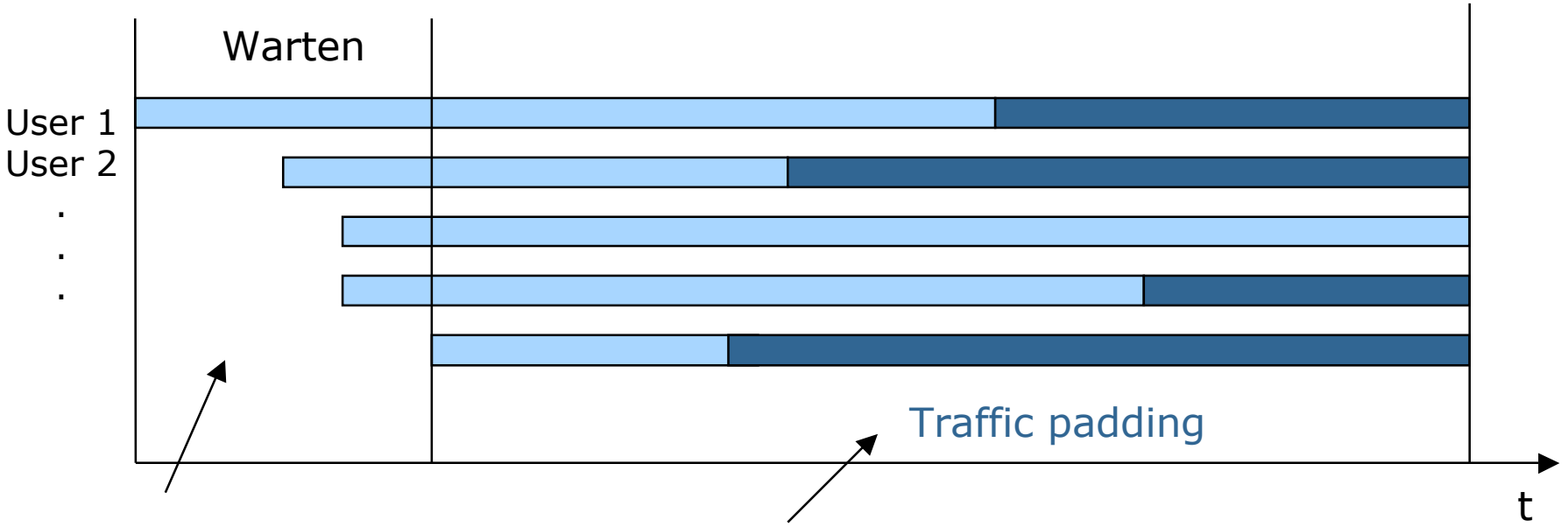
Echtzeitkommunikation und Mixe

- 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



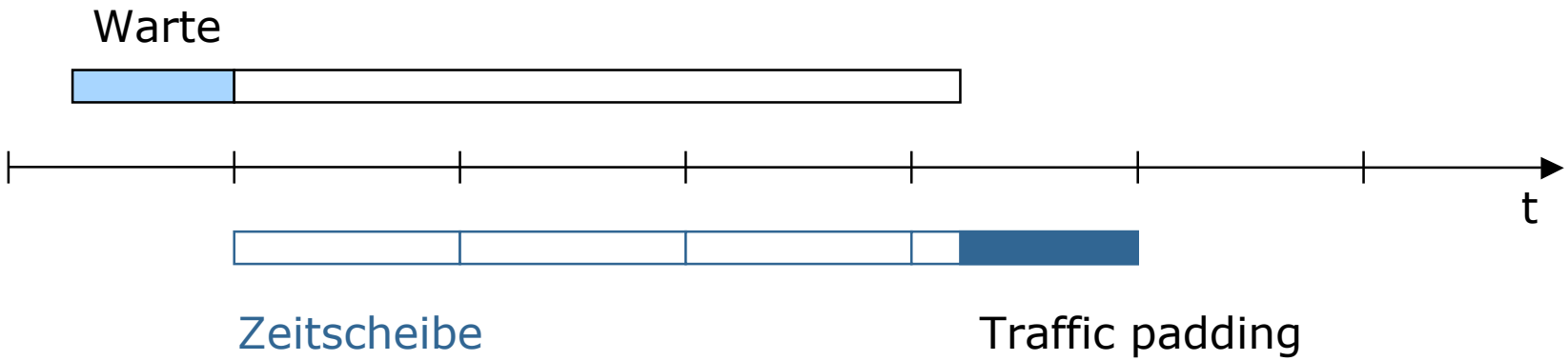
1. Warten, bis genügend Benutzer kommunizieren wollen (Bilden der Anonymitätsgruppe)
   Beispiel: 5 Nutzer

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

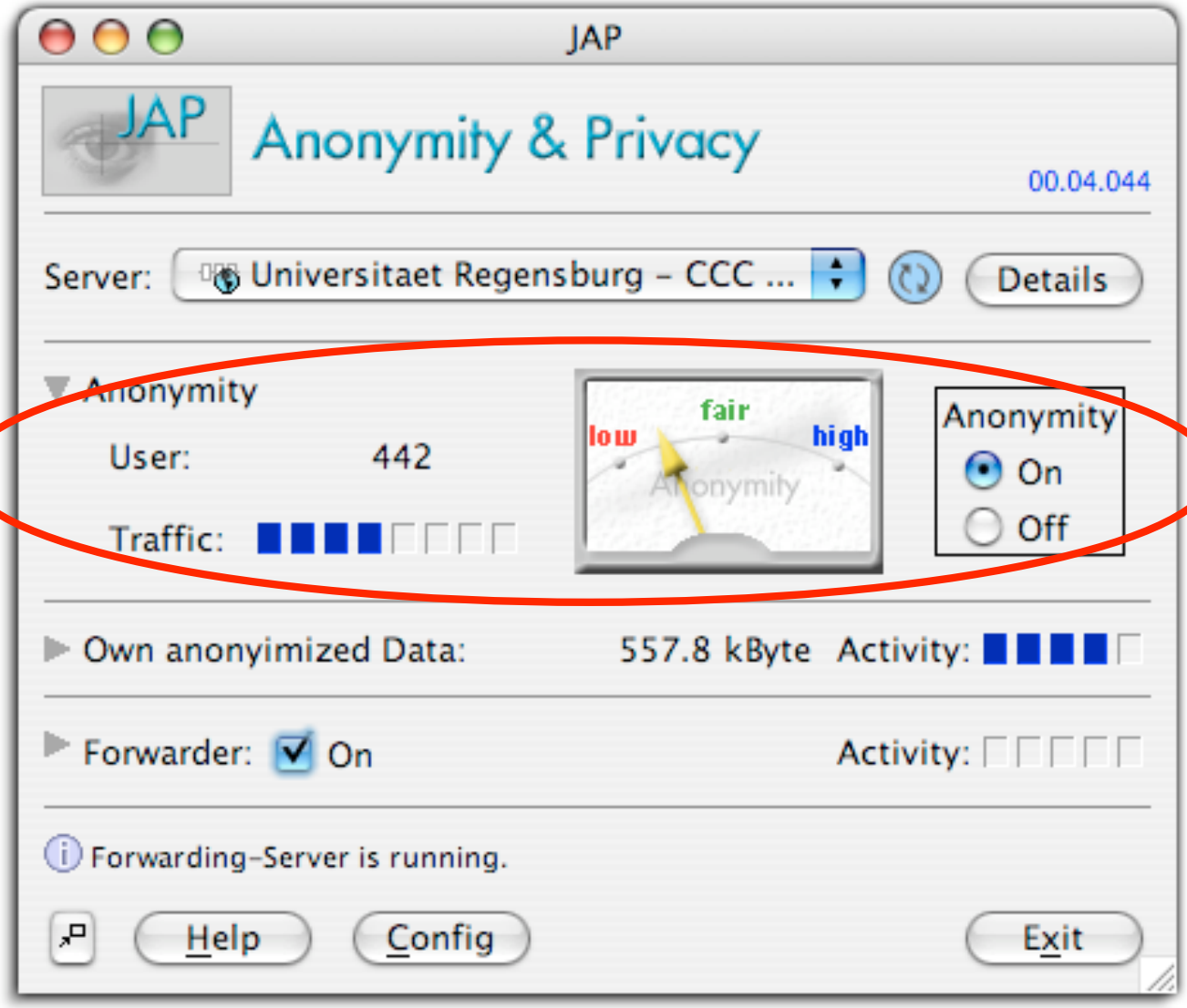


- Volumenscheiben (Federrath et. al. 2000)
  - adaptive Anpassung der Scheibengröße in Abhängigkeit der aktuellen Verkehrssituation
  - Minimieren des Overheads

Herausforderungen aus technischer Sicht

- Adaption der Mixe auf Echtzeitkommunikation
- Transparenz für den Nutzer
- Dezentrale Architektur des Gesamtsystems
- Abrechnung anonym genutzter Dienste
- Stärkung des Nutzers bei gleichzeitiger Strafverfolgungsmöglichkeit

AN.ON/JAP

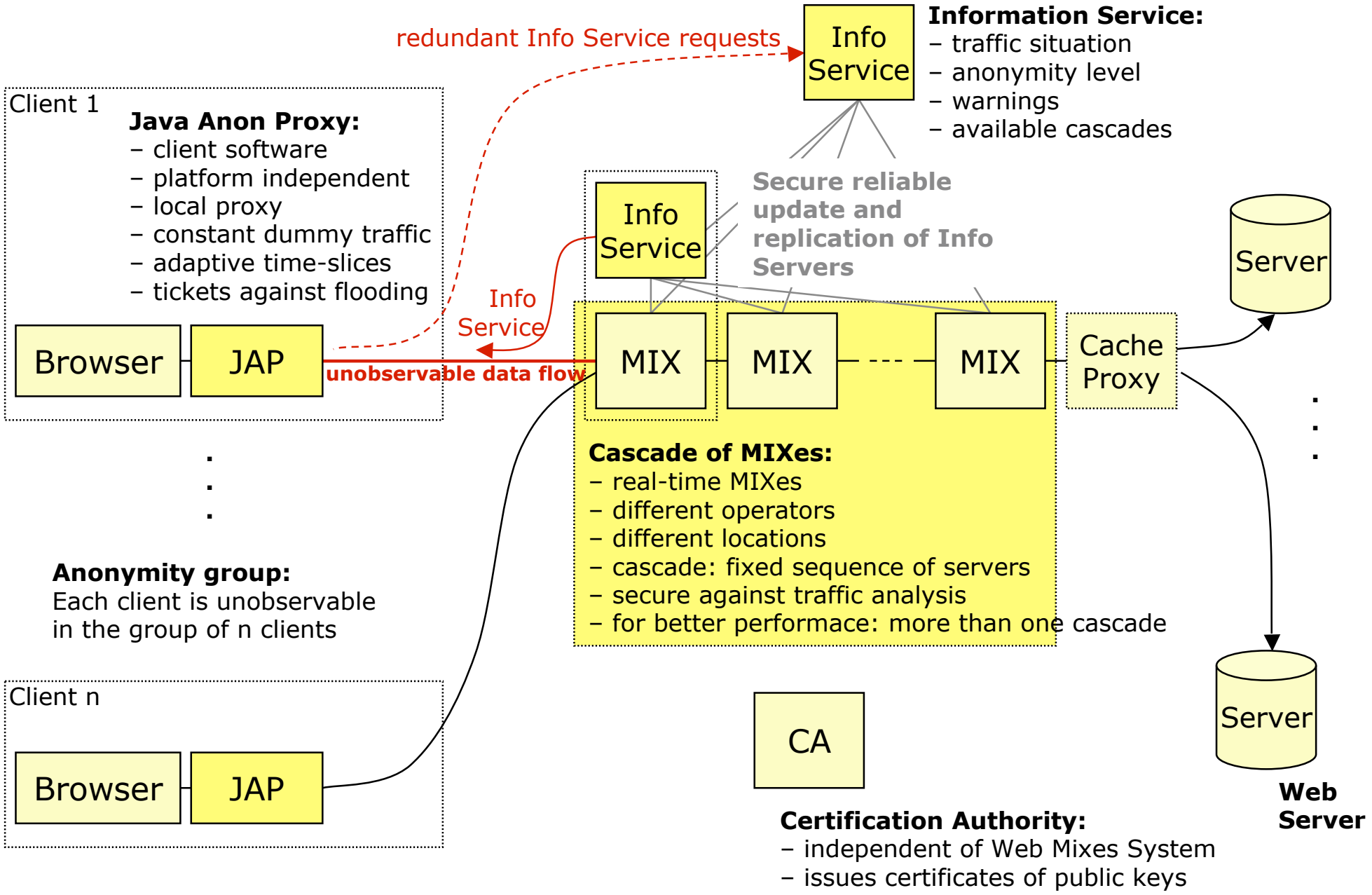


Rückmeldung über Verkehrssituation und Beobach-tungsrisiko (Lang-zeitbeobachtung)

Herausforderungen aus technischer Sicht

- Adaption der Mixe auf Echtzeitkommunikation
- Transparenz für den Nutzer
- Dezentrale Architektur des Gesamtsystems
- Abrechnung anonym genutzter Dienste
- Stärkung des Nutzers bei gleichzeitiger Strafverfolgungsmöglichkeit

AN.ON: Architektur

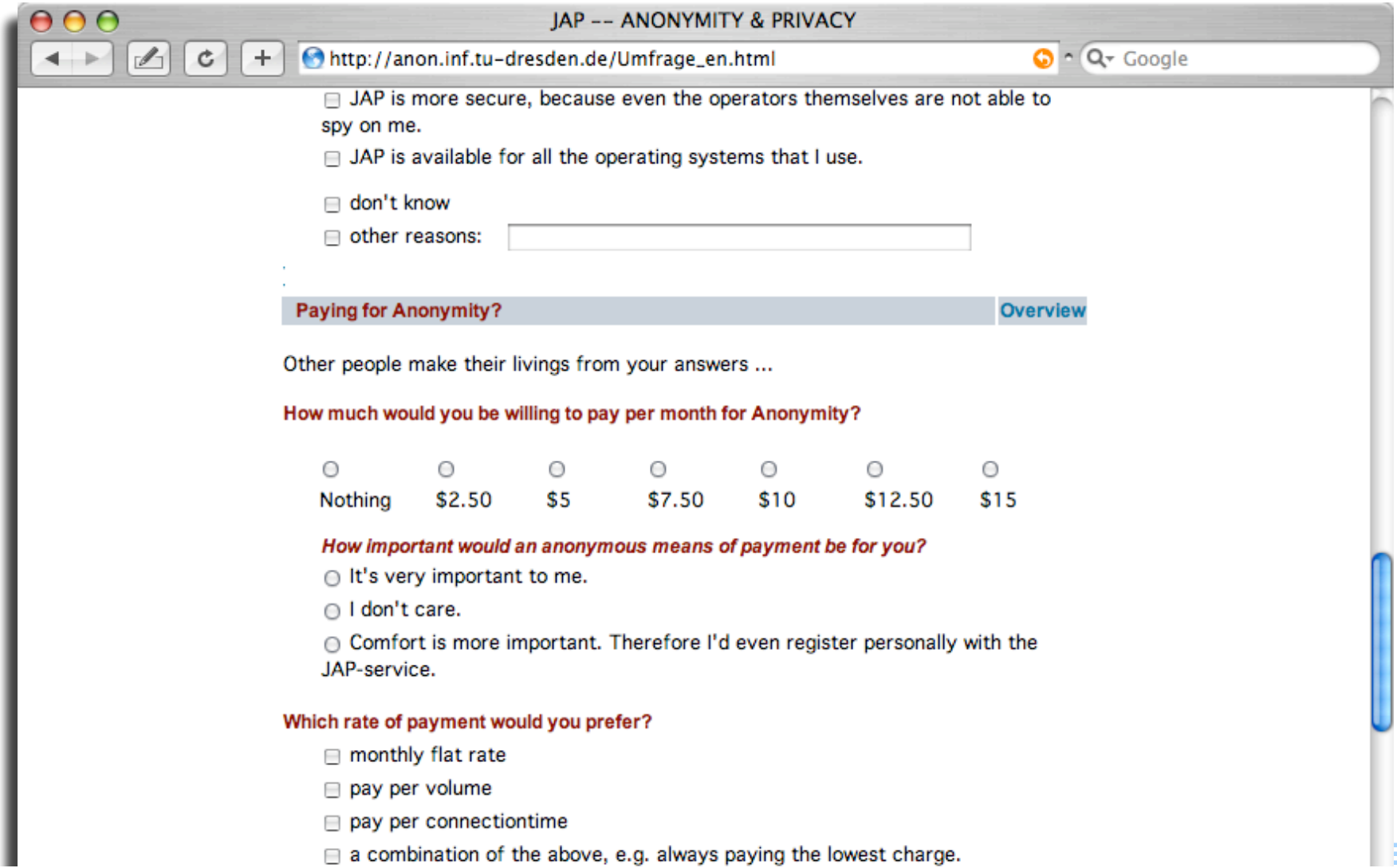


Herausforderungen aus technischer Sicht

- Adaption der Mixe auf Echtzeitkommunikation
- Transparenz für den Nutzer
- Dezentrale Architektur des Gesamtsystems
- Abrechnung anonym genutzter Dienste
- Stärkung des Nutzers bei gleichzeitiger Strafverfolgungsmöglichkeit

Umfrage unter JAP-Benutzern (Spiekermann, 2003)

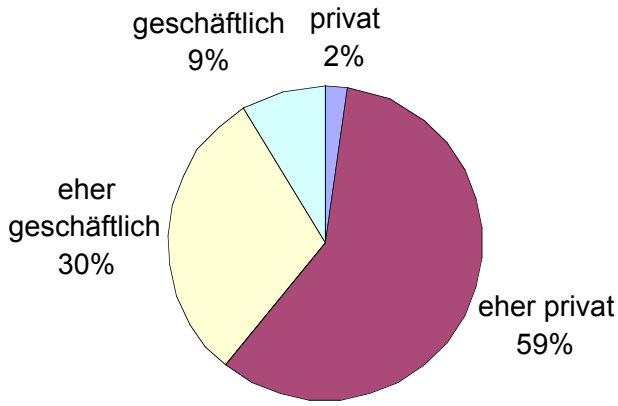
- Stichprobe:
  - 1800 JAP-Nutzer



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



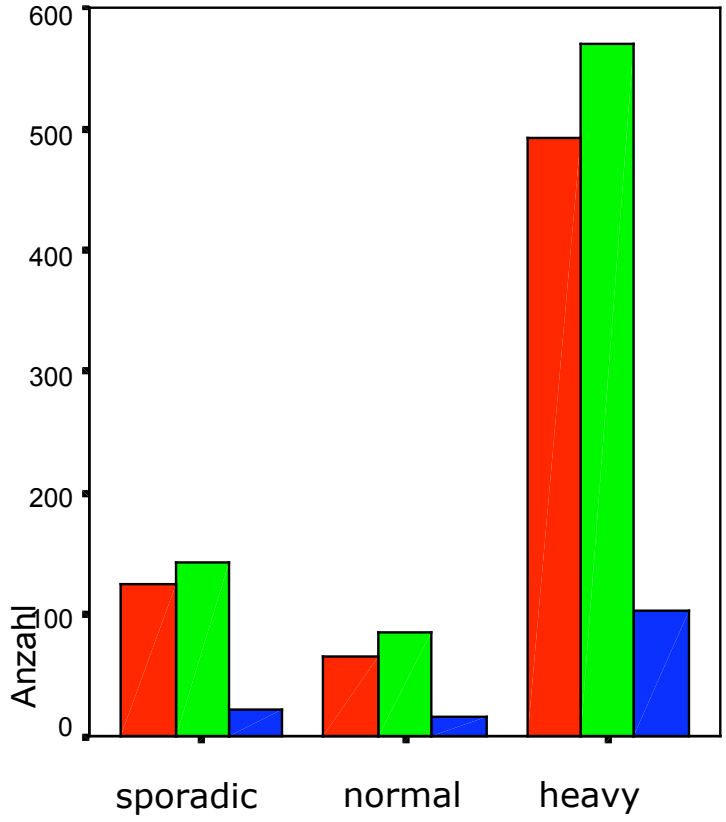
- Warum JAP?
  - ≈ 76% kostenlos
  - ≈ 56% schützt vor Betreibern
  - ≈ 51% einfach benutzbar

Umfrage unter JAP-Benutzern

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

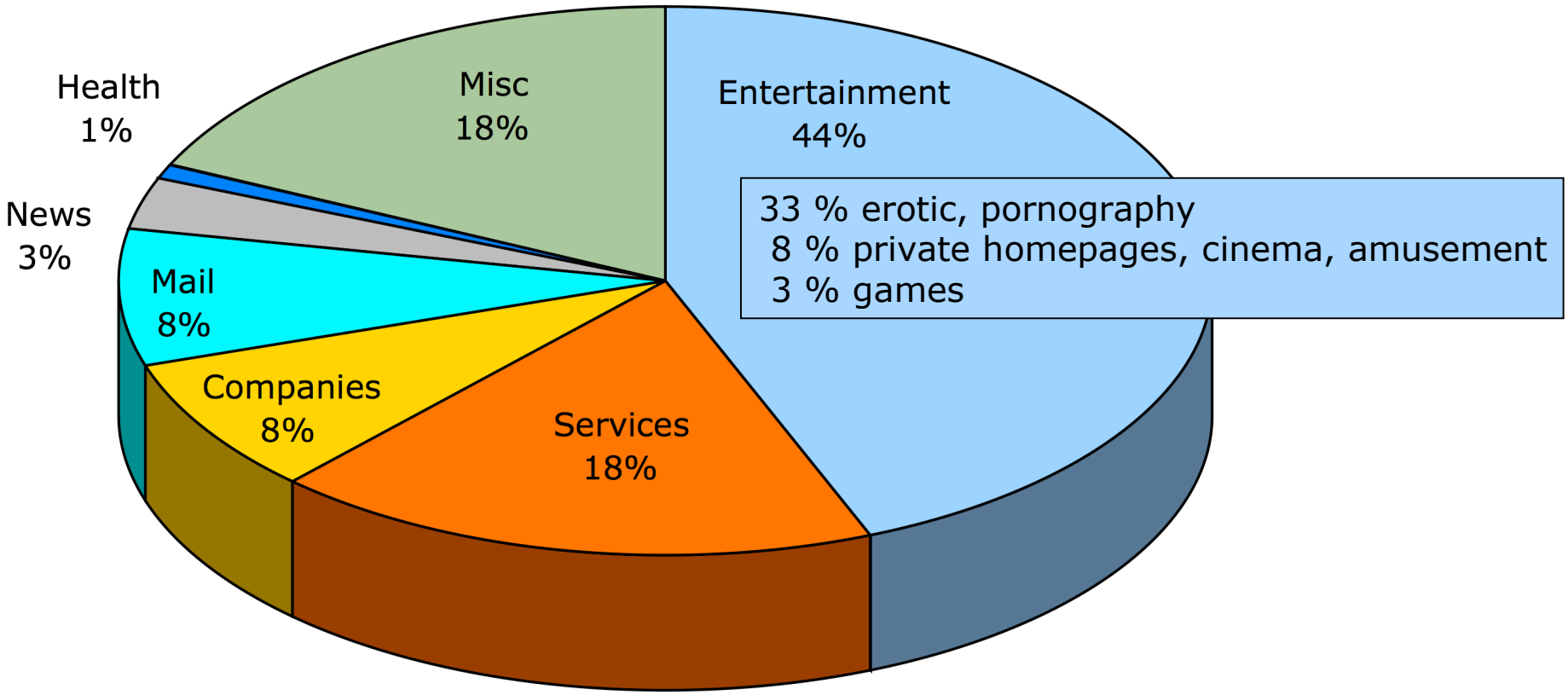
- Zahlungsbereitschaft korreliert nicht mit der Intensität der Nutzung

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



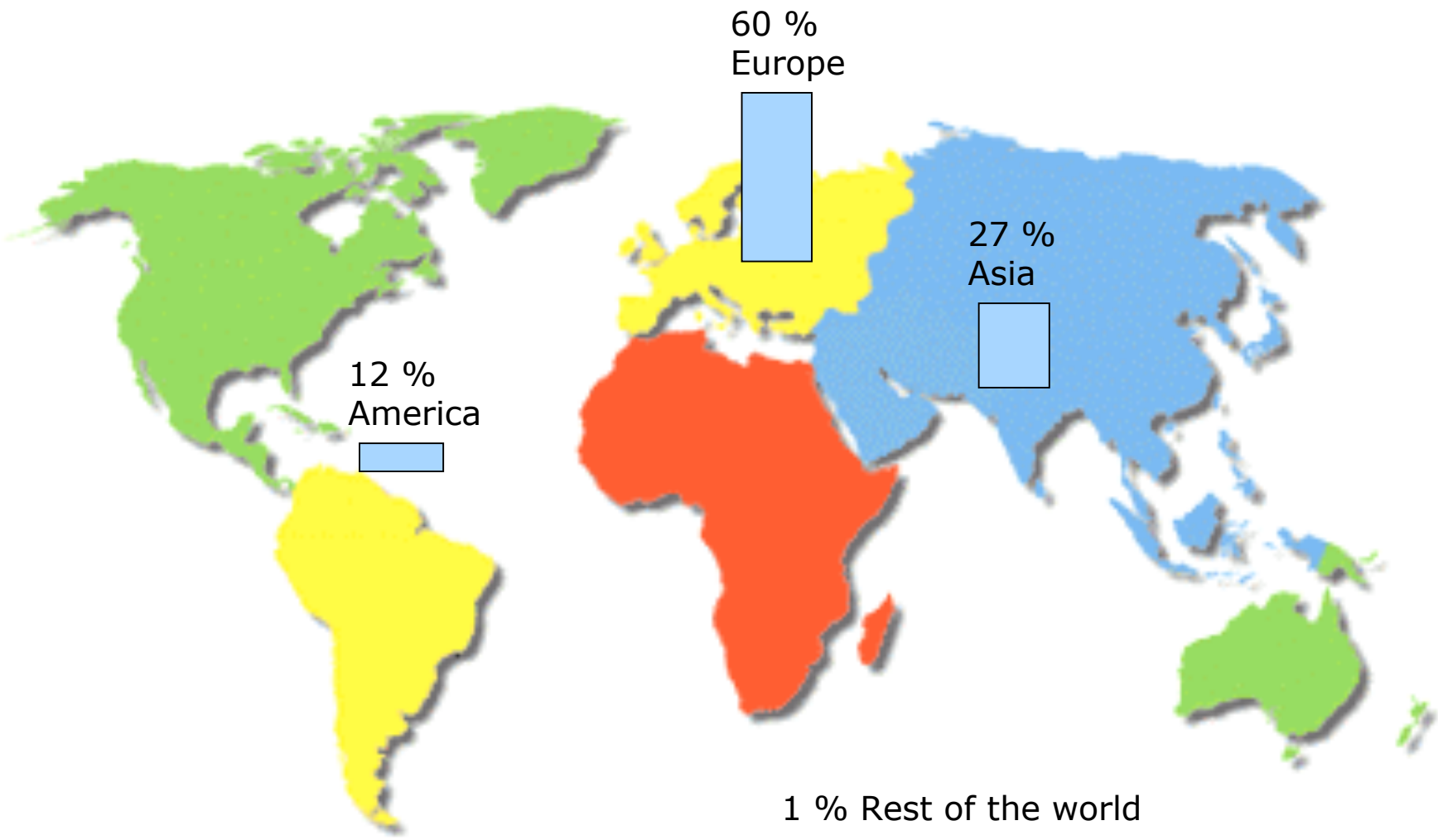
Anonymisierte Inhalte

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

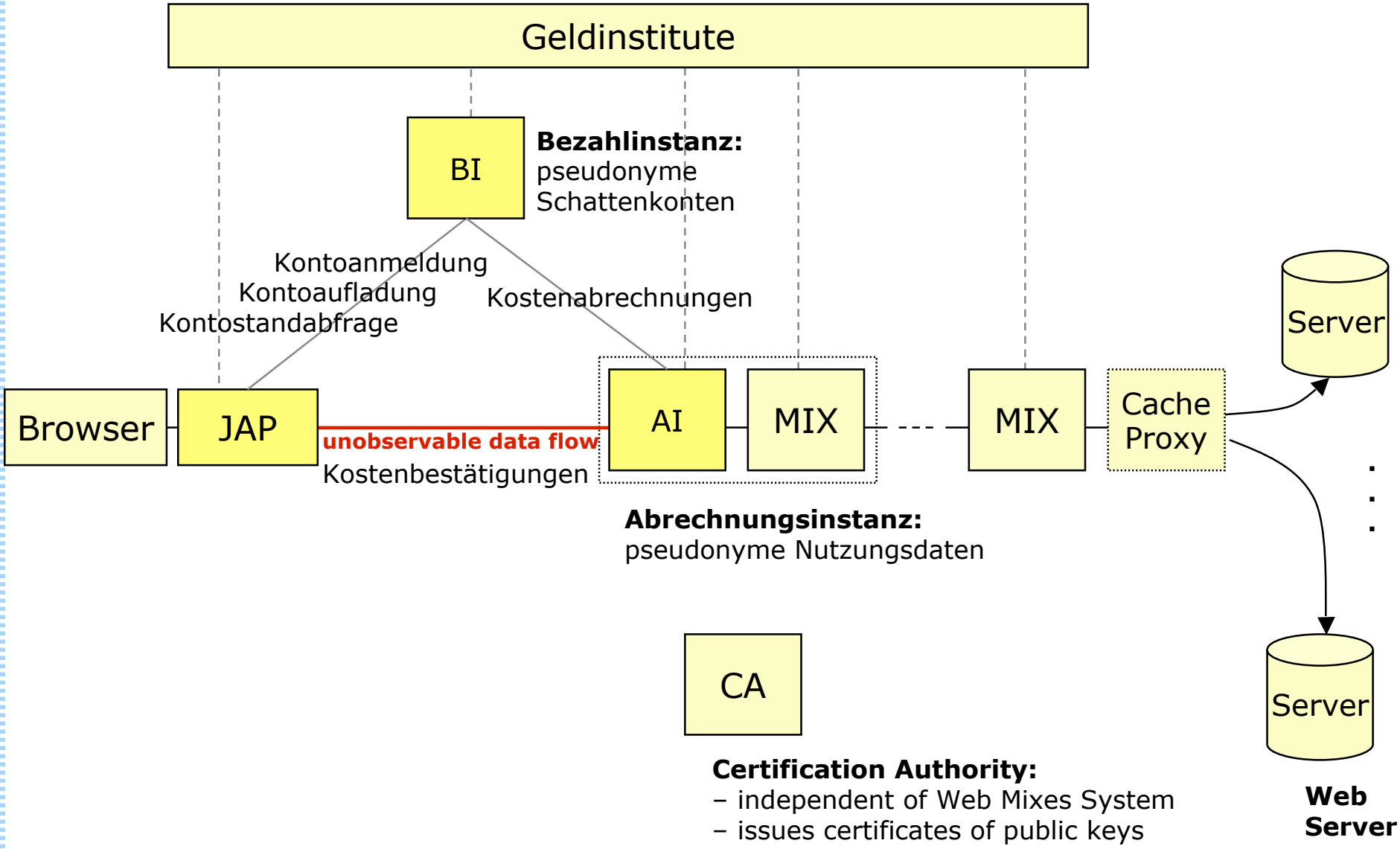


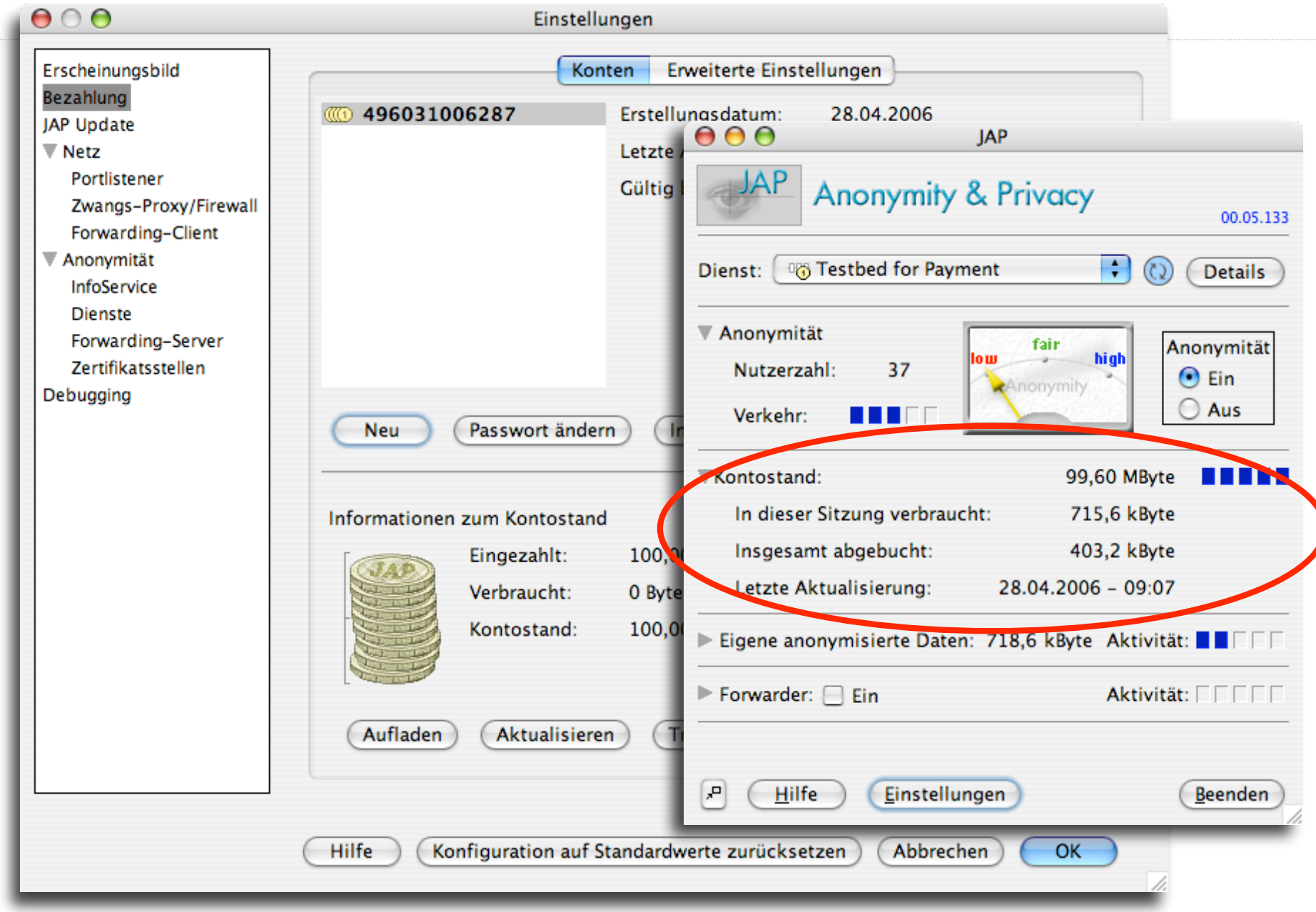
Wo kommen die JAP-Nutzer her?

- Eingehende Requests nach Regionen Mai-Juni 2005



Architektur Bezahlsystem



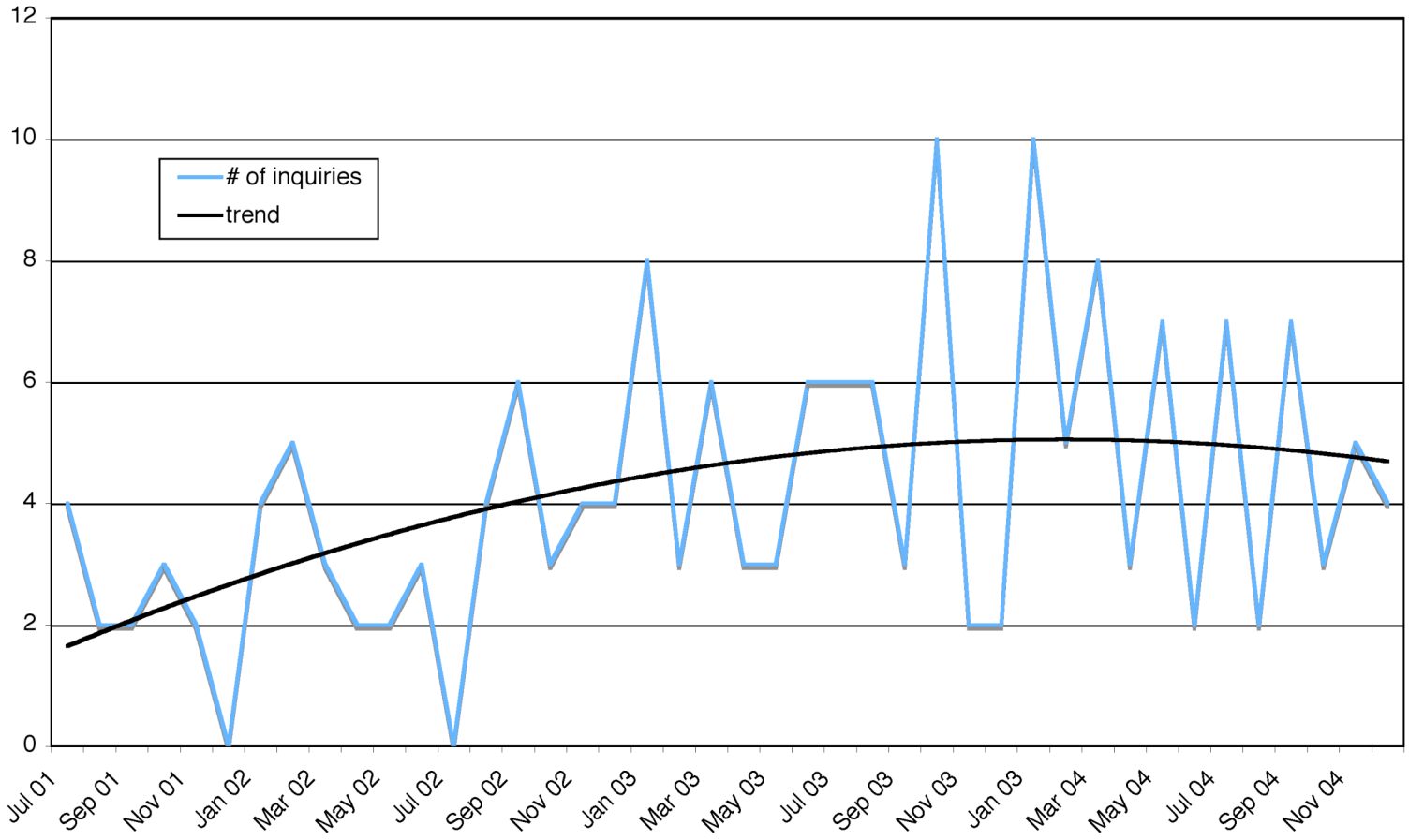

Einstellungen
Erscheinungsbild
Bezahlung
JAP Update
Netz
Portlistener
Zwangs-Proxy/Firewall
Forwarding-Client
Anonymität
InfoService
Dienste
Forwarding-Server
Zertifikatsstellen
Debugging
Konten
Erweiterte Einstellungen
496031006287
Erstellungsdatum: 28.04.2006
Neu
Passwort ändern
Informationen zum Kontostand
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

Herausforderungen aus technischer Sicht

- Adaption der Mixe auf Echtzeitkommunikation
- Transparenz für den Nutzer
- Dezentrale Architektur des Gesamtsystems
- Abrechnung anonym genutzter Dienste
- Stärkung des Nutzers bei gleichzeitiger Strafverfolgungsmöglichkeit

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

Skizze der Antwort

Mit dem Schreiben vom dd.mm.jj fordern Sie die TU Dresden auf, Auskunft über die Verbindungsdaten für die IP-Adresse xx.yy.zz für den Zeitpunkt dd.mm.jj, hh:mm.ss Uhr zu geben. Dazu können wir Ihnen folgendes mitteilen:

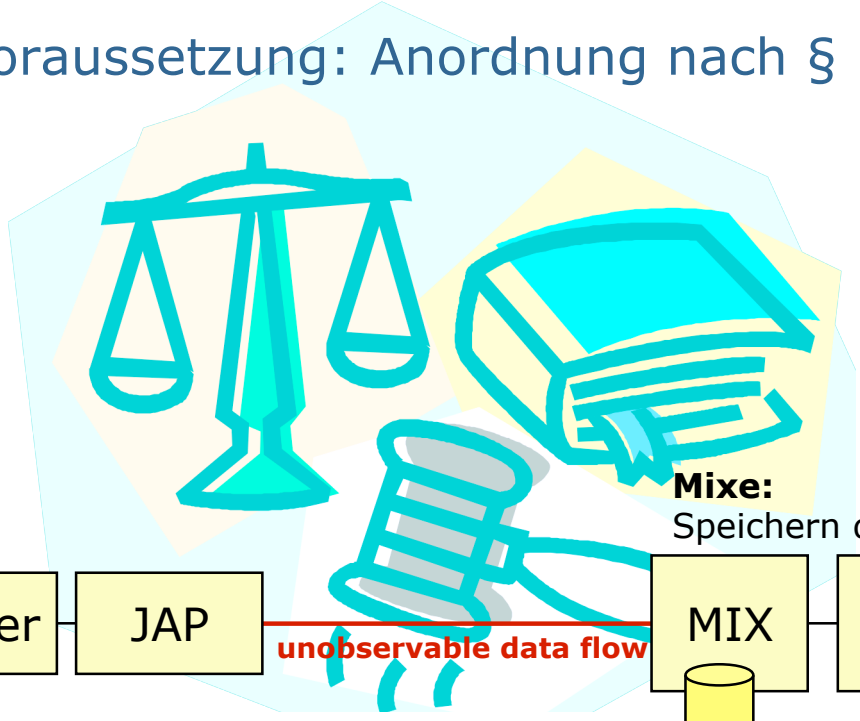
Der von Ihnen erwähnte Server ist Teil eines Forschungsprojektes, das gemeinsam von der TU Dresden, Fakultät für Informatik, sowie dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein betrieben wird. Ziel des vom Bundeswirtschaftsministerium geförderten Projekts ist es, anonyme und unbeobachtbare Webzugriffe zu realisieren (http://anon.inf.tu-dresden.de/). Dabei geht es darum, die Vorschriften des Teledienstedatenschutzgesetzes (TDDSG) bzw. des Mediendienste-Staatsvertrages (MDStV) umzusetzen, die verlangen, dass Diensteanbieter den Nutzern die anonyme oder pseudonyme Nutzung ermöglichen, soweit dies technisch möglich und zumutbar ist (§ 4 Abs. 6 TDDSG bzw. § 13 Abs. 1 MDStV).

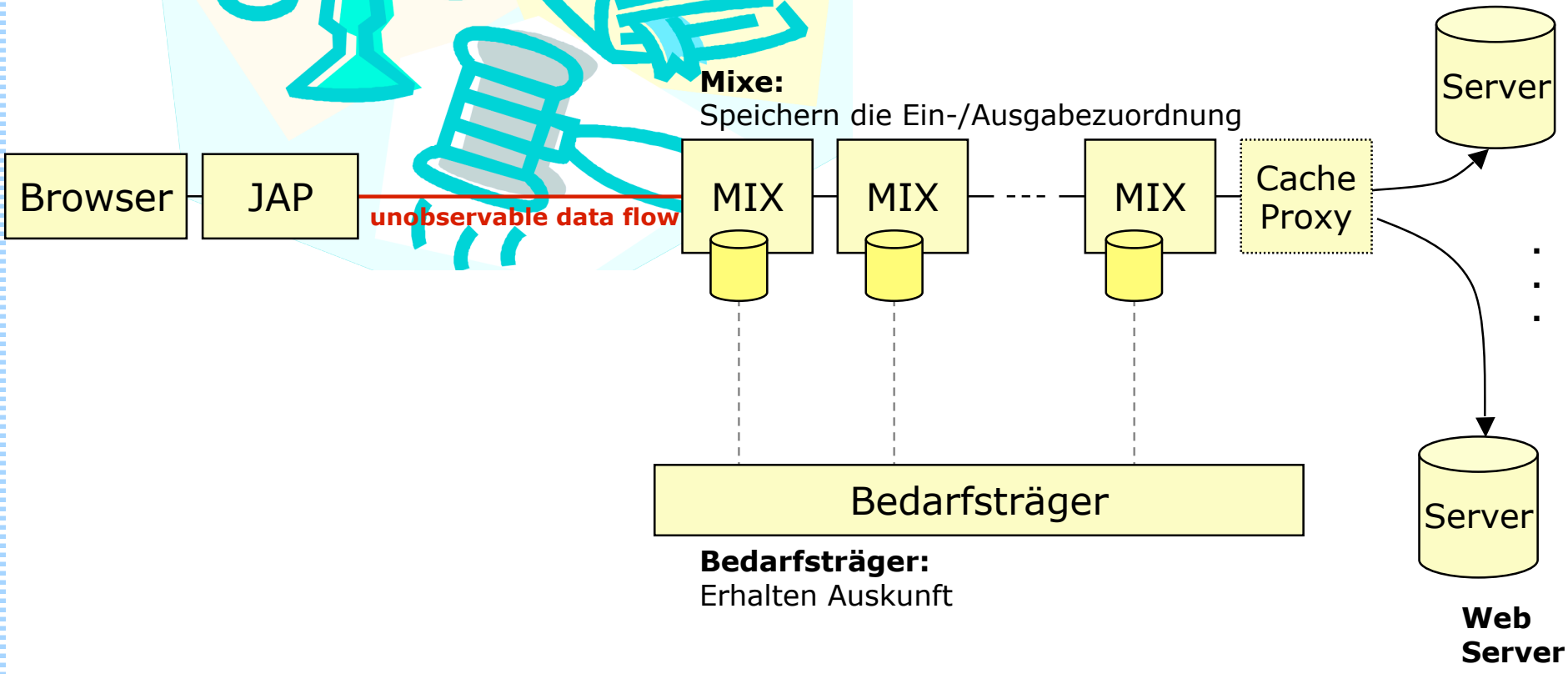
Dabei wird schon auf technischer Ebene die Zuordnung von IP-Adressen zu einzelnen Nutzern oder zu sonstigen identifizierenden Merkmalen vermieden. Aus diesem Grund liegen hier keine Daten vor, über die aufgrund des richterlichen Beschlusses nach § 12 FAG Auskunft gegeben werden könnte.

Wir bedauern, Ihnen keine weiterführenden Hinweise bzgl. der Identität der Benutzer geben zu können.

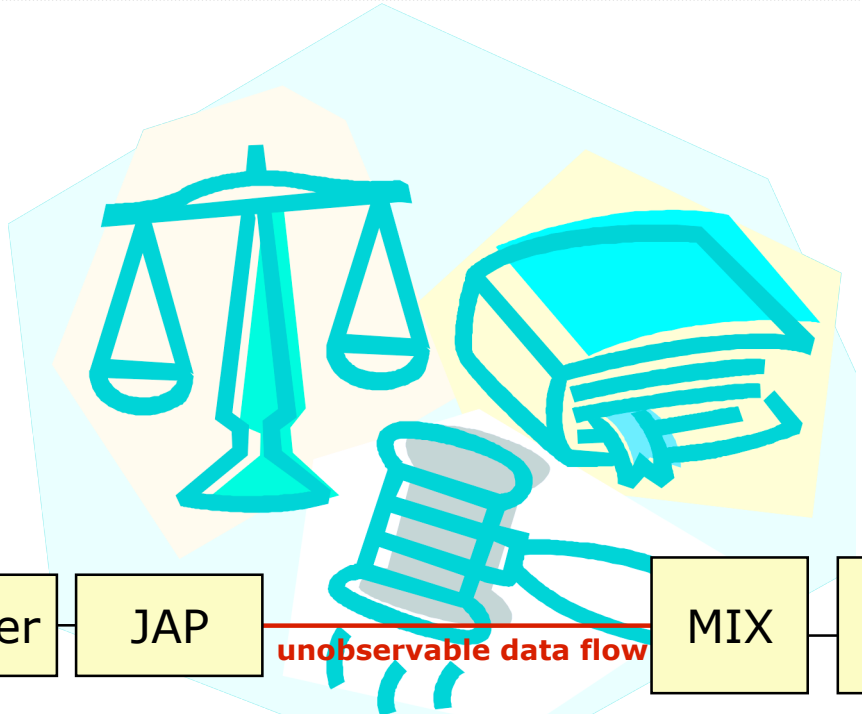
Strafverfolgung bei schweren Straftaten

- Voraussetzung: Anordnung nach § 100a,b StPO



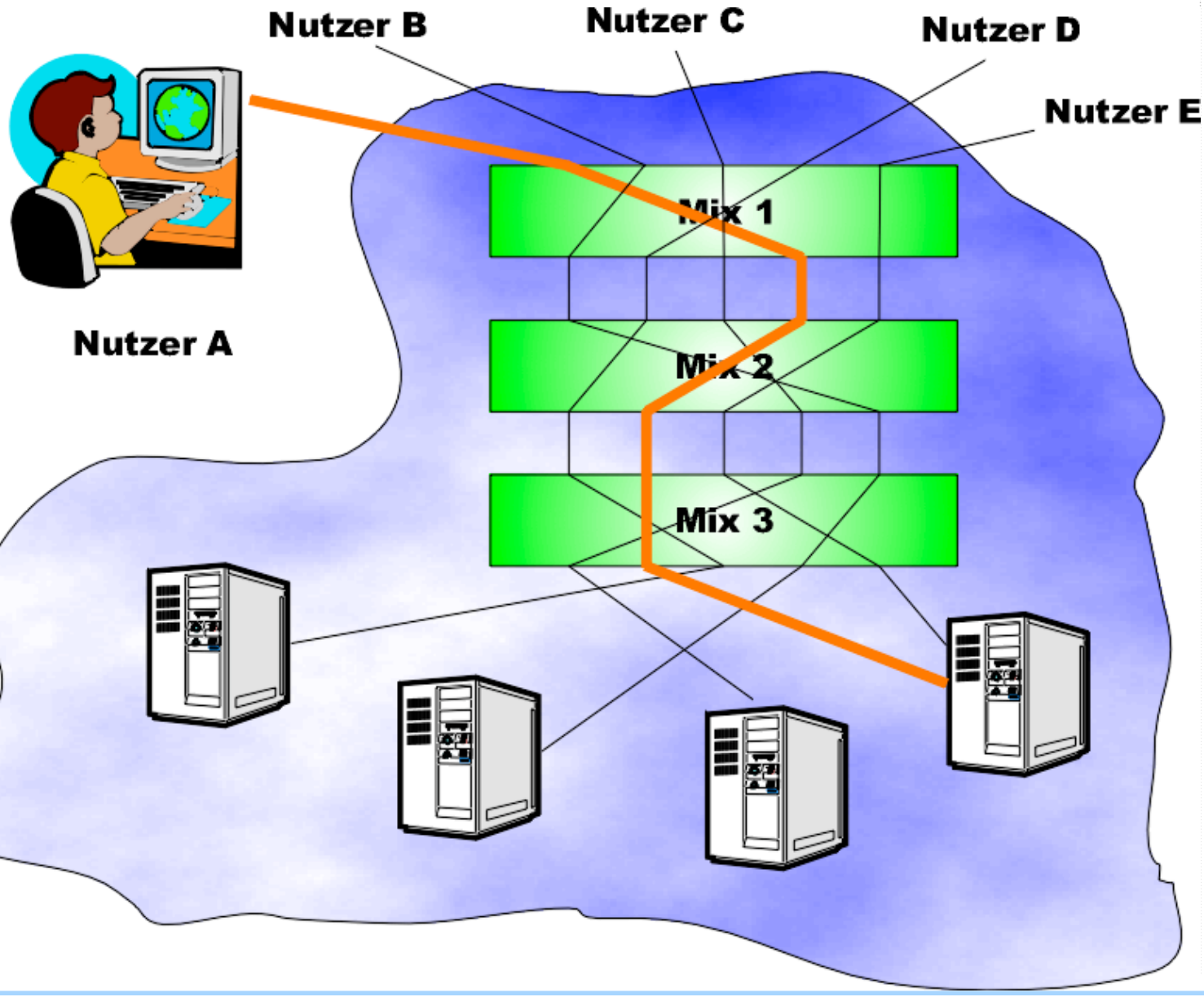


Prävention ist besser als Strafverfolgung

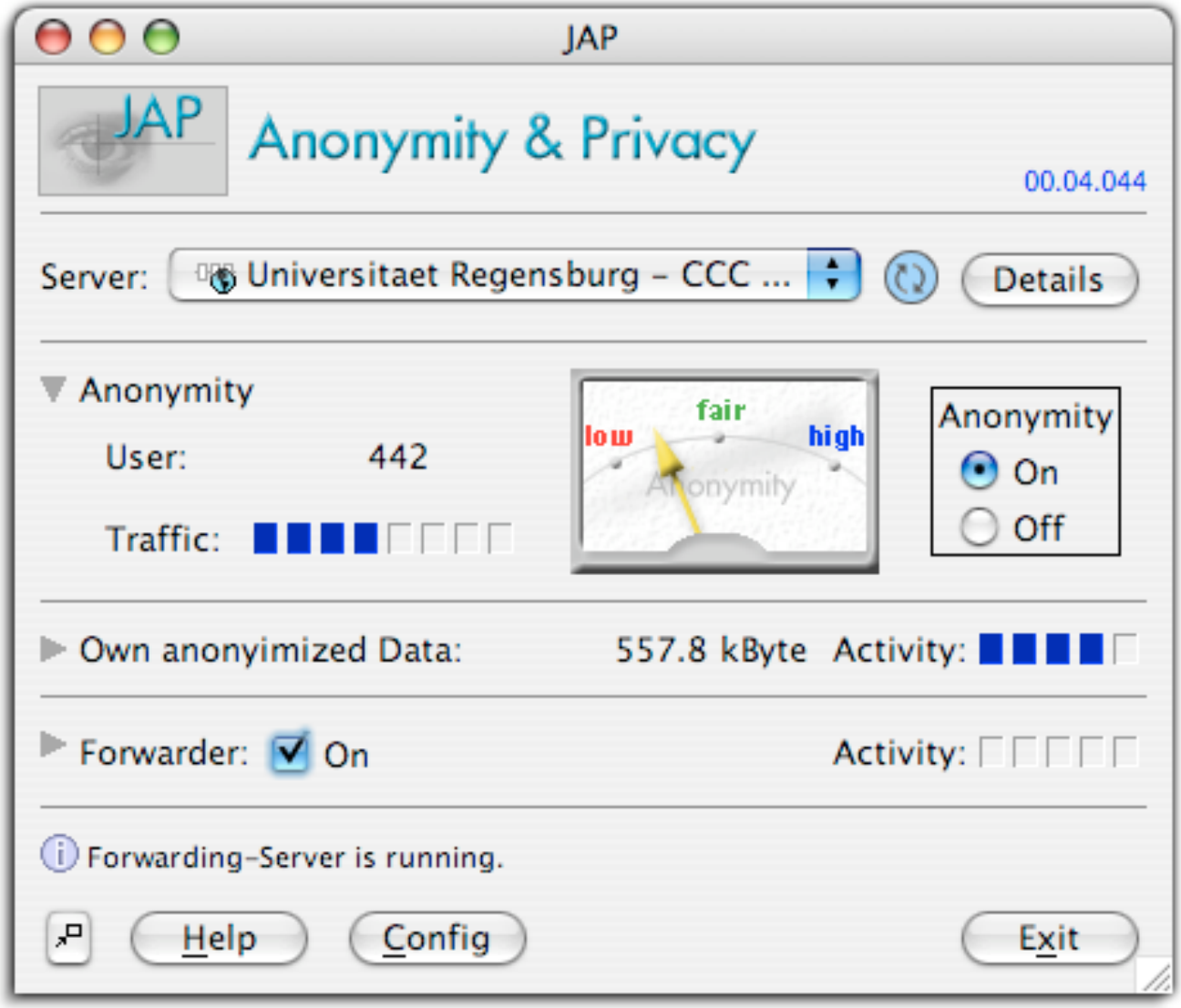


AN.ON/JAP

- JAP wird als lokaler Proxy im Browser konfiguiert
- Webzugriffe gehen über AN.ON-Server



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: BMWA, 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