Spurenlos durchs Netz?

Die technischen Grenzen der Unbeobachtbarkeit im Internet

Passau, 20.05.2008

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

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

Was ist zu schützen?

Kommunikationsgegenstand WAS?		Kommunikationsumstände WANN?, WO?, WER?
Vertraulichkeit **Verdecktheit**	Inhalte	**Anonymität** **Unbeobachtbarkeit** Sender, Ort Empfänger
Integrität	Inhalte	**Zurechenbarkeit** **Rechtsverbindlichkeit** Absender, Bezahlung Empfänger
Verfügbarkeit	Inhalte	**Erreichbarkeit** Nutzer Rechner

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 **Inhalte**	**Anonymität** **Unbeobachtbarkeit** **Sender** **Ort** **Empfänger**

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

Prinzipien: Datenschutzfördernde Technik

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

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

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
1999	Zeroknowledge Freedom Anonymizer
2000	AN.ON/JAP Anonymizer
2004	TOR

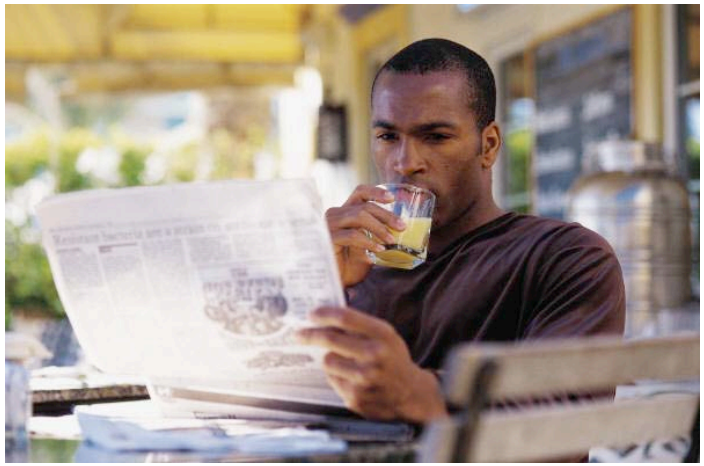
Grundverfahren
Anwendung

Bausteine datenschutzfördernder Technik

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

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.

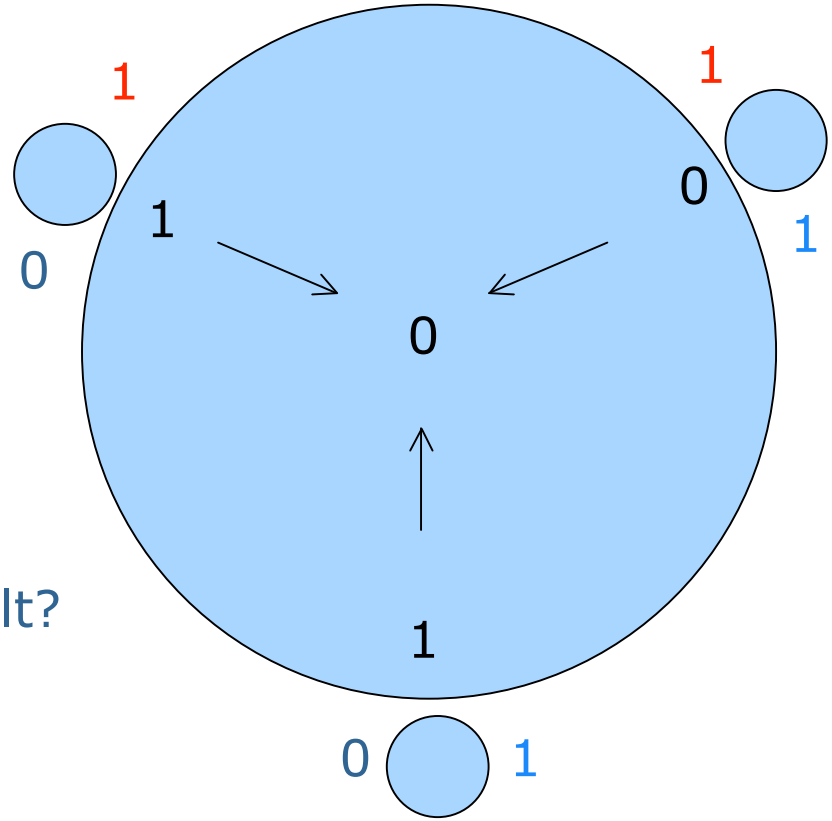
- Entweder
  - Beibehaltung des vorhandenen Verteilsystems

  oder
  - zusätzliche Schutzfunktionen zur Wahrung des Datenschutzes erforderlich

DC network (Chaum, 1988)

- Jeder für sich:
  1. Jeder wirft mit jeden eine Münze
  2. Berechnet das xor der beiden Bits
  3. Wenn bezahlt, dann xor mit 1 (Komplement des Ergebnisses aus Schritt 2)
  4. Ergebnis veröffentlichen

- Alle zusammen:
  1. Berechnen das xor der drei (lokalen) Ergebnisse
  2. Wenn globales Ergebnis 0, hat jmd. anderes bezahlt



Wer hat bezahlt?

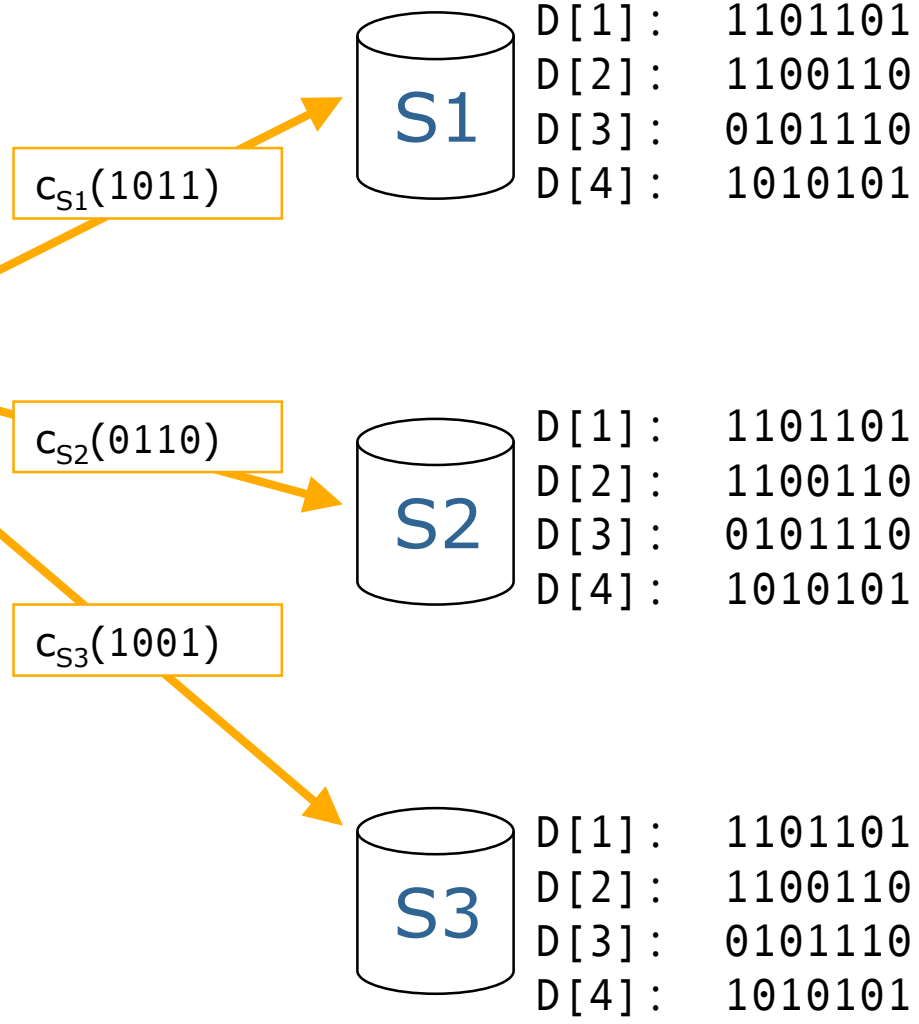
Blind-Message-Service: Anfrage

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

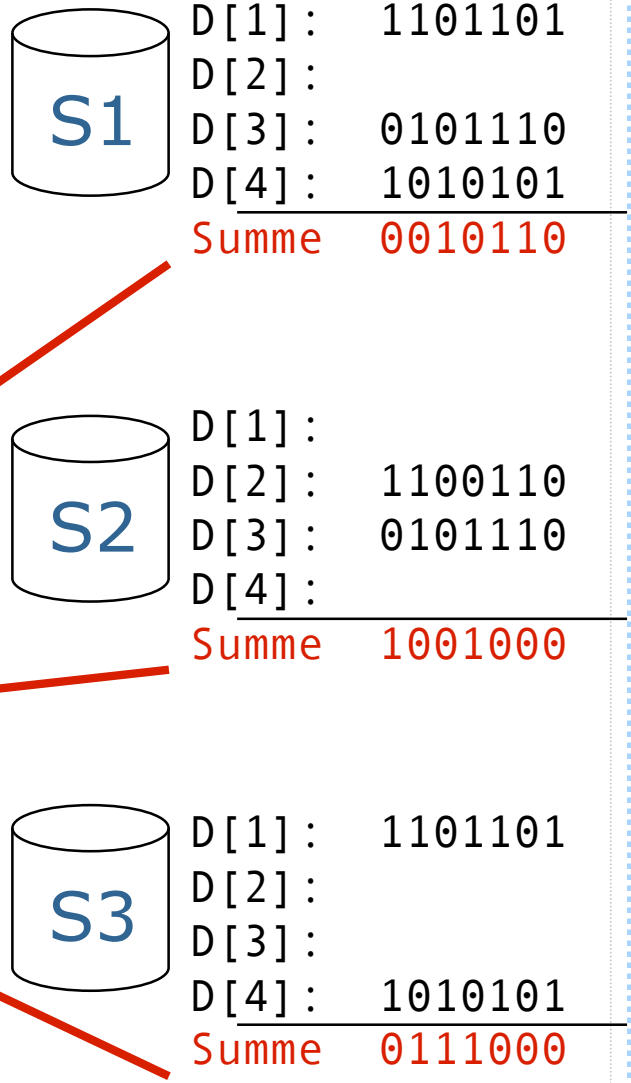
Cooper, Birman, 1995

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

Bausteine datenschutzfördernder Technik

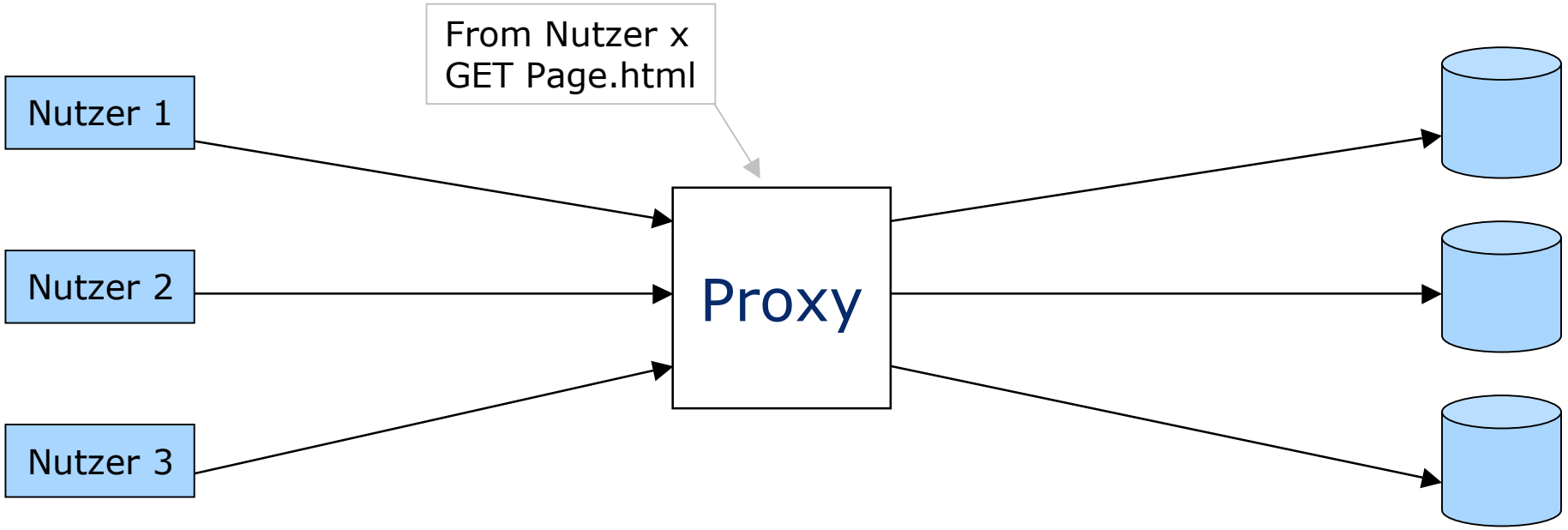
- Verschlüsselung

- Schutz von Kommunikationsbeziehungen
  - Schutz vor Outsidern
    - Proxies (schwacher Schutz)
  - Schutz vor Insidern
    - Broadcast √
    - Blind message service √
    - DC network √
    - MIX network

- Schutz von Transaktionen
  - Pseudonyme
  - Credentials (an Pseudonyme gekettete Eigenschaften)

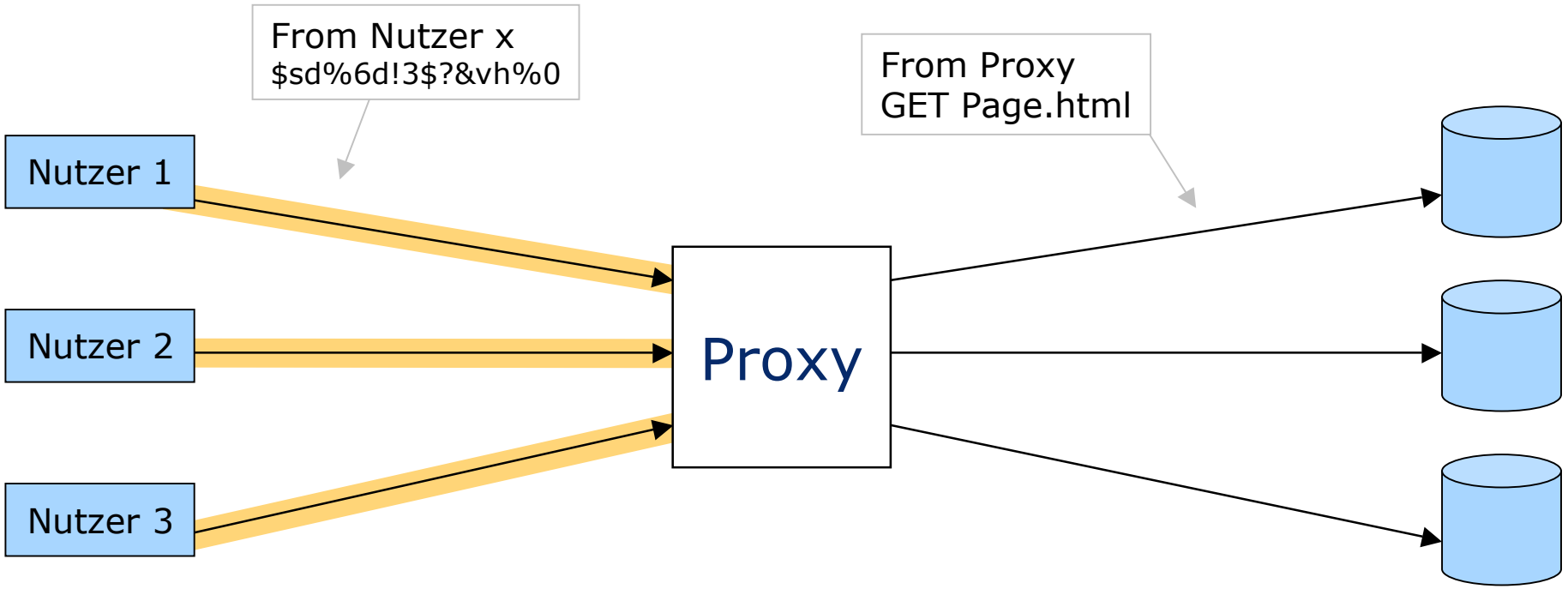
Proxies: Insider

- Erreichbare Sicherheit (Insider)
  - Kein Schutz gegen den Betreiber des Proxy



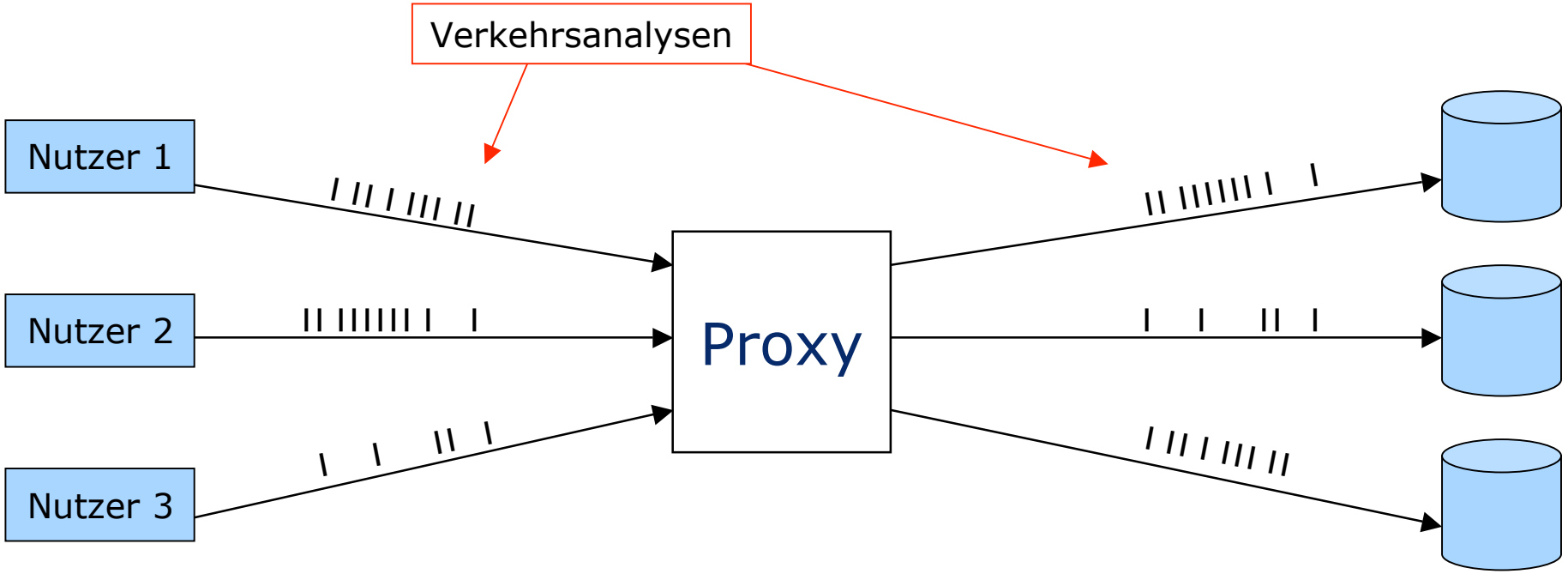
Proxies: Outsider

- Erreichbare Sicherheit (Outsider)
  - Beobachter nach Proxy und Serverbereiber:
    - erfahren nichts über den wirklichen Absender eines Requests
  - Beobachter vor Proxy:
    - Schutz des Senders, wenn Verbindung zu Proxy verschlüsselt



Proxies: Outsider

- Erreichbare Sicherheit (Outsider)
  - Aber: Trotz Verschlüsselung:
    - kein Schutz gegen Verkehrsanalysen
      - Verkettung über Nachrichtenlängen
      - zeitliche Verkettung



Mix-Netz (Chaum, 1981)

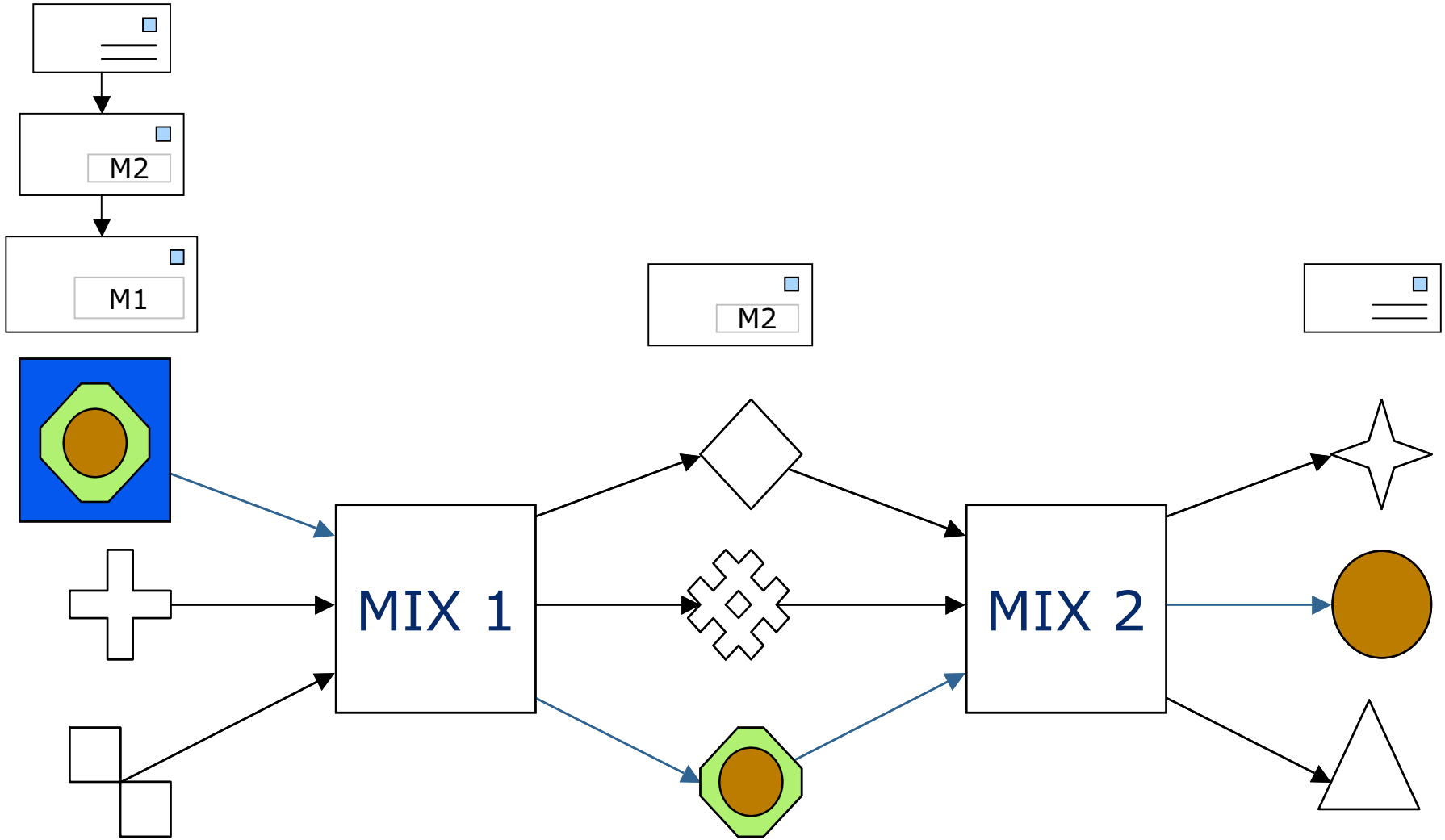
- System zum Schutz von Kommunikationsbeziehungen bei vermittelter Kommunikation

- 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

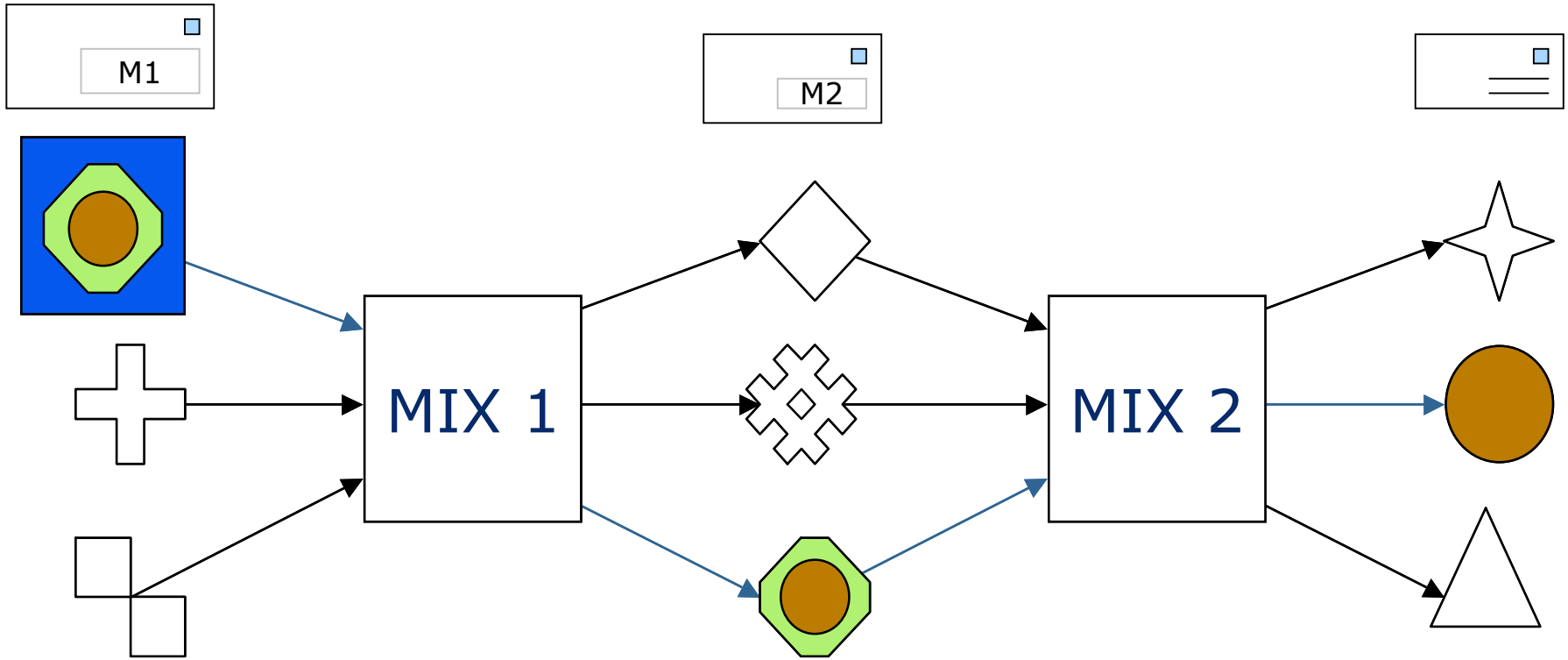
Mix-Netz (Chaum, 1981)

- System zum Schutz von Kommunikationsbeziehungen bei vermittelter Kommunikation

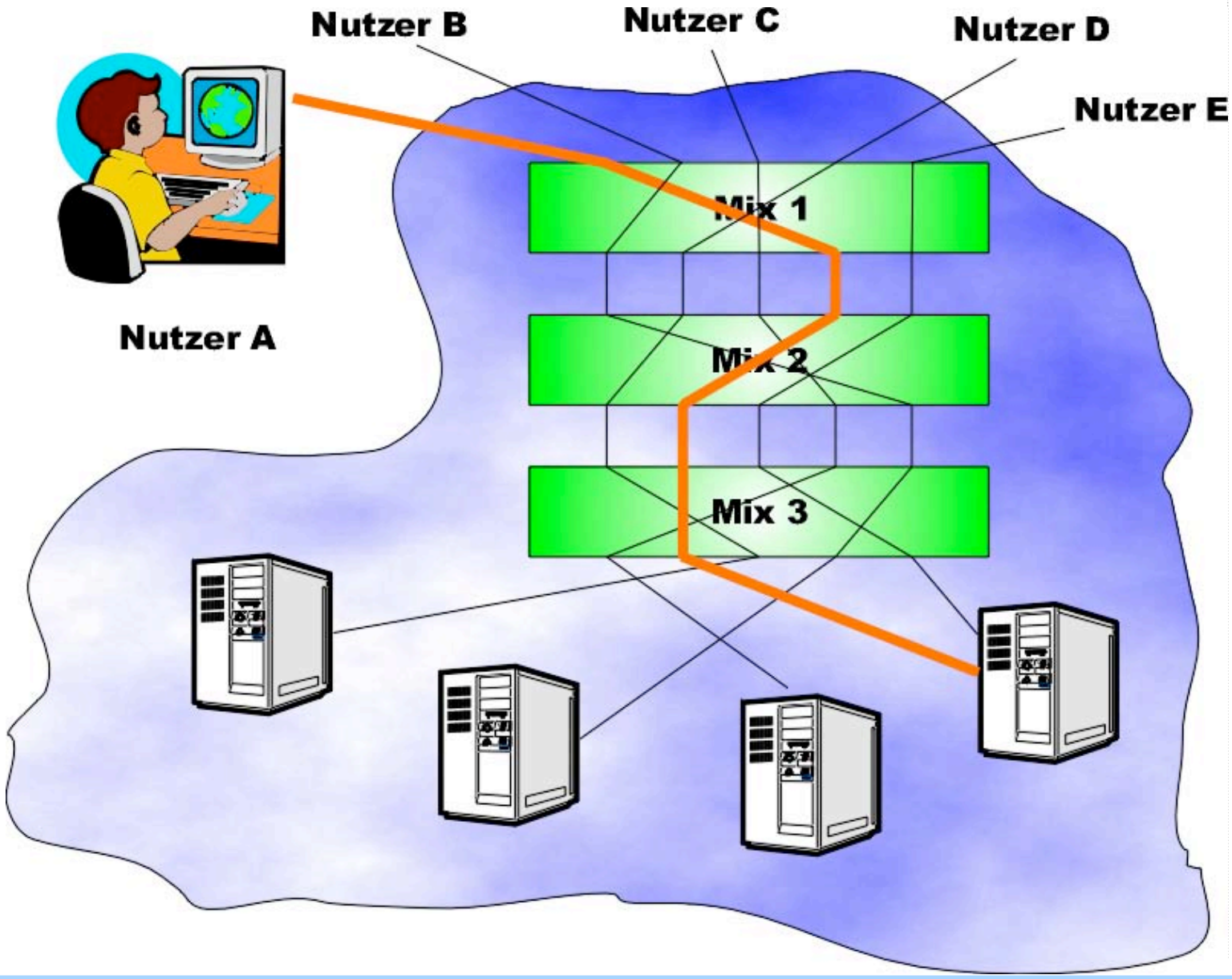


Mix-Netz (Chaum, 1981)

- Stärke der Mixe:
  - Auch die Betreiber der Mixe erfahren nichts mehr über die Kommunikationsbeziehung zwischen Sender und Empfänger.
- Notwendige Bedingungen:
  - Mehr als einen Mix und unterschiedliche Betreiber verwenden
  - Wenigstens ein Mix darf nicht angreifen.



Nutzbarmachung der Mixe für Webzugriff

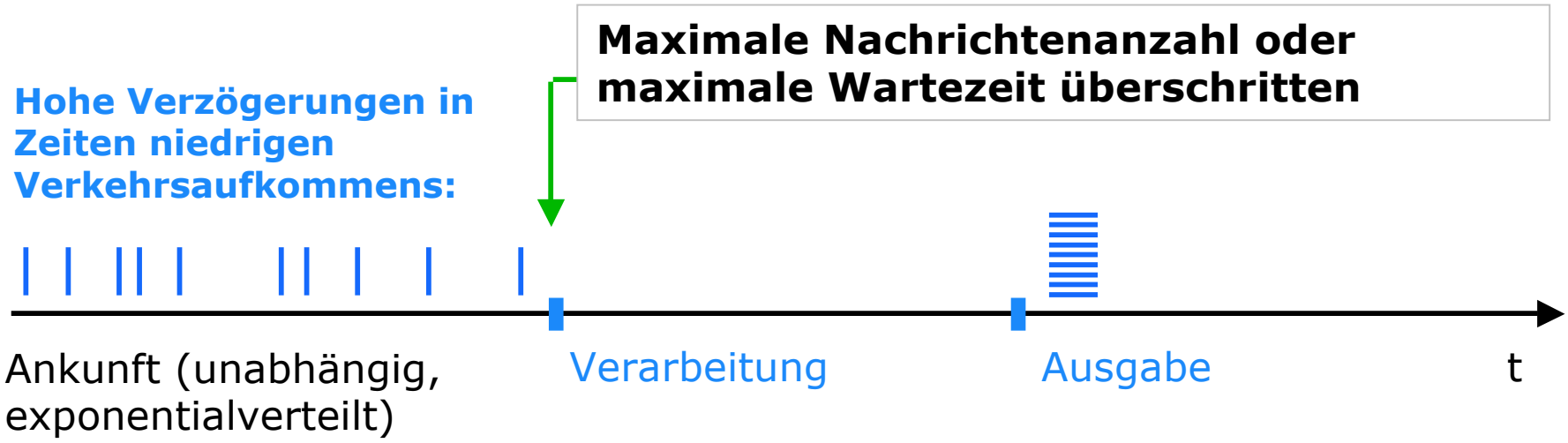


Herausforderungen aus technischer Sicht

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

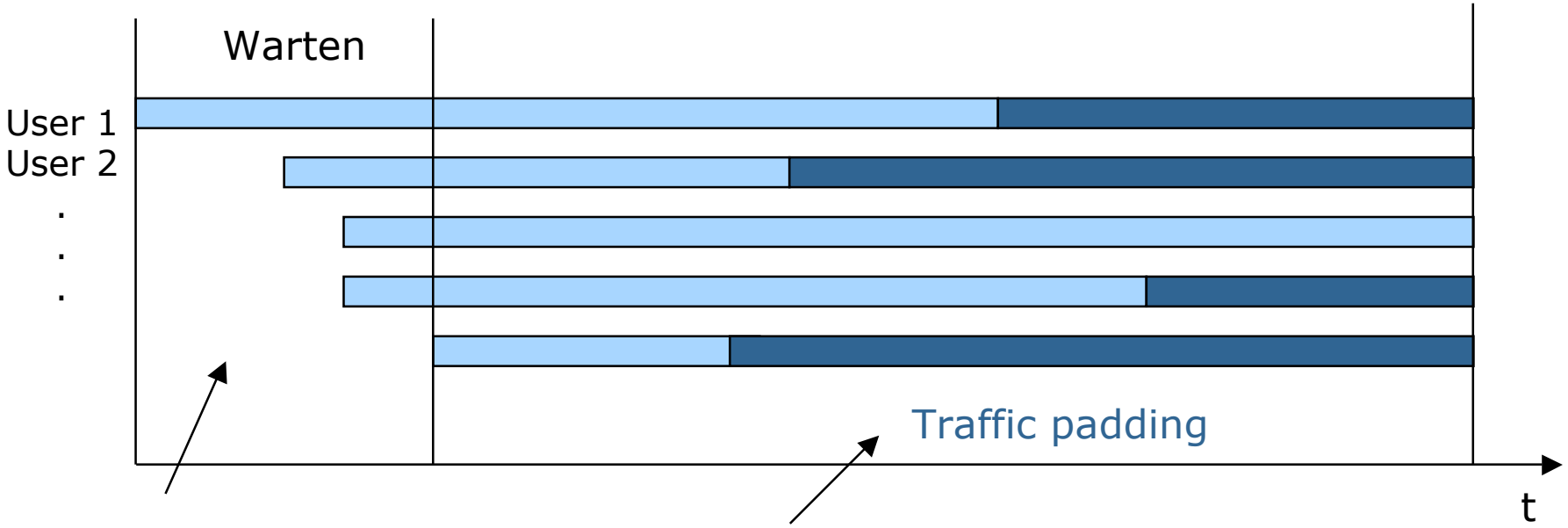
Echtzeitkommunikation und Mixe

- 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



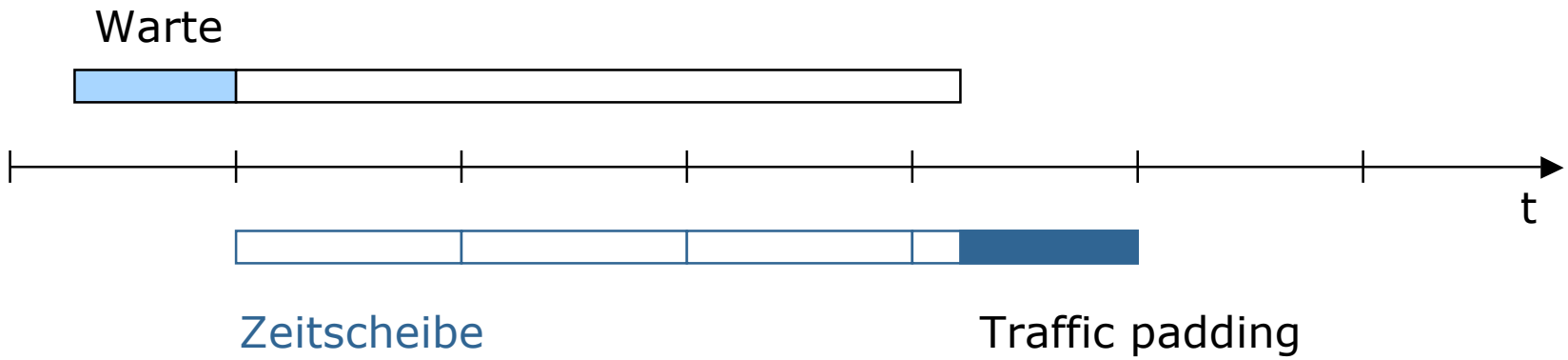
1. Warten, bis genügend Benutzer kommunizieren wollen (Bilden der Anonymitätsgruppe)
   Beispiel: 5 Nutzer

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

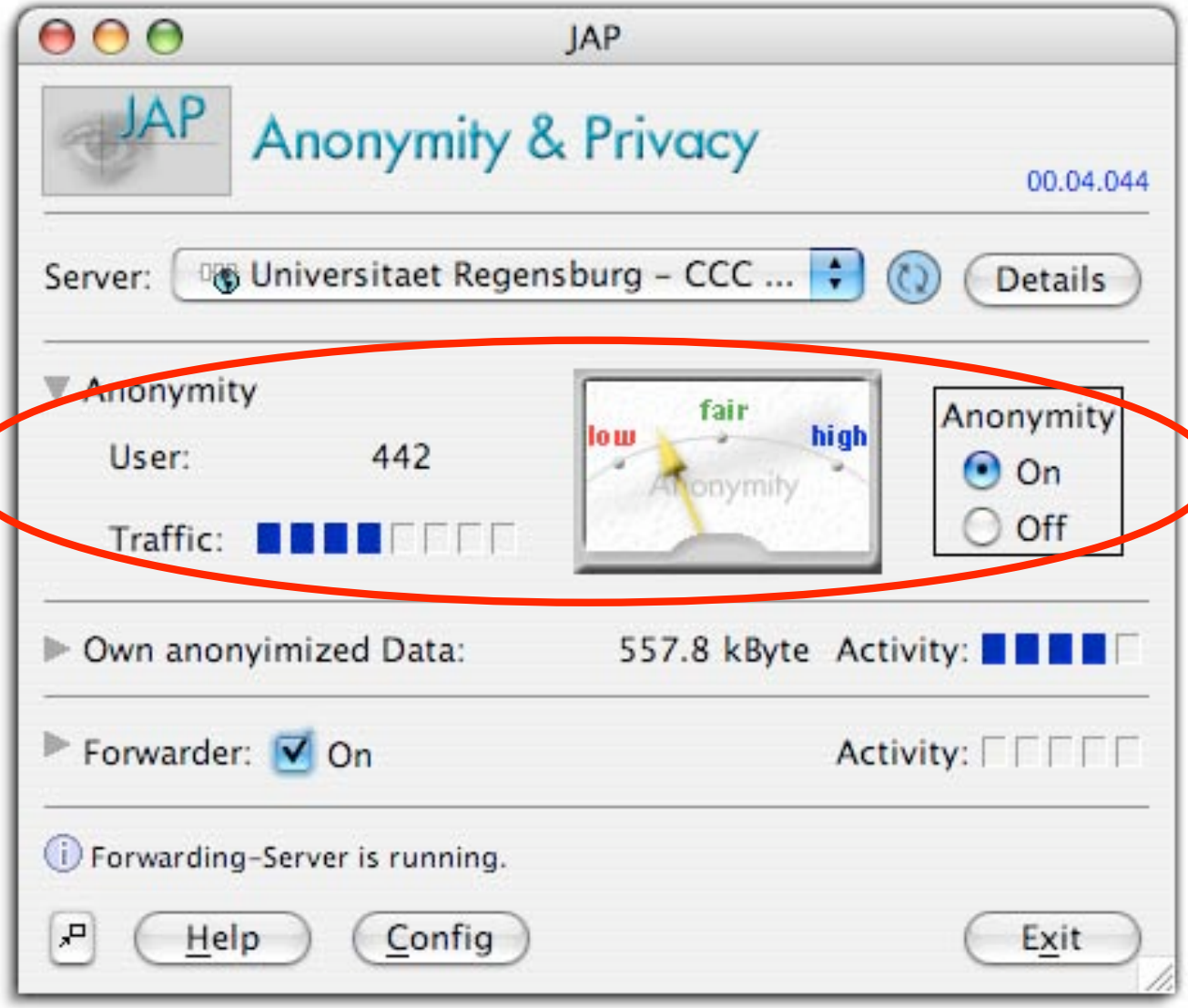


- Volumenscheiben (Federrath et. al. 2000)
  - adaptive Anpassung der Scheibengröße in Abhängigkeit der aktuellen Verkehrssituation
  - Minimieren des Overheads

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



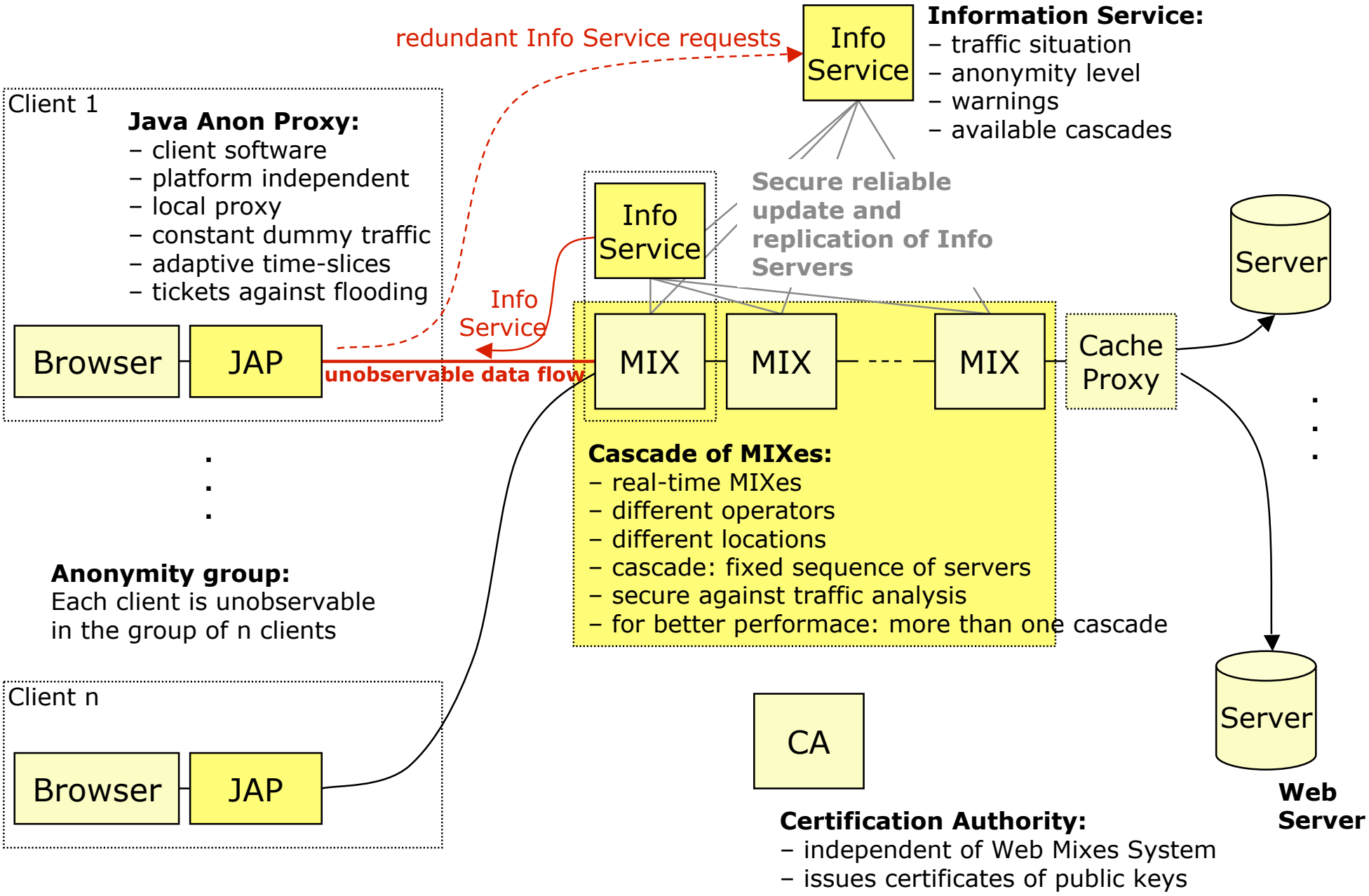
Ansprechende, leicht und fehlerfrei benutzbare Oberfläche

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

Herausforderungen aus technischer Sicht

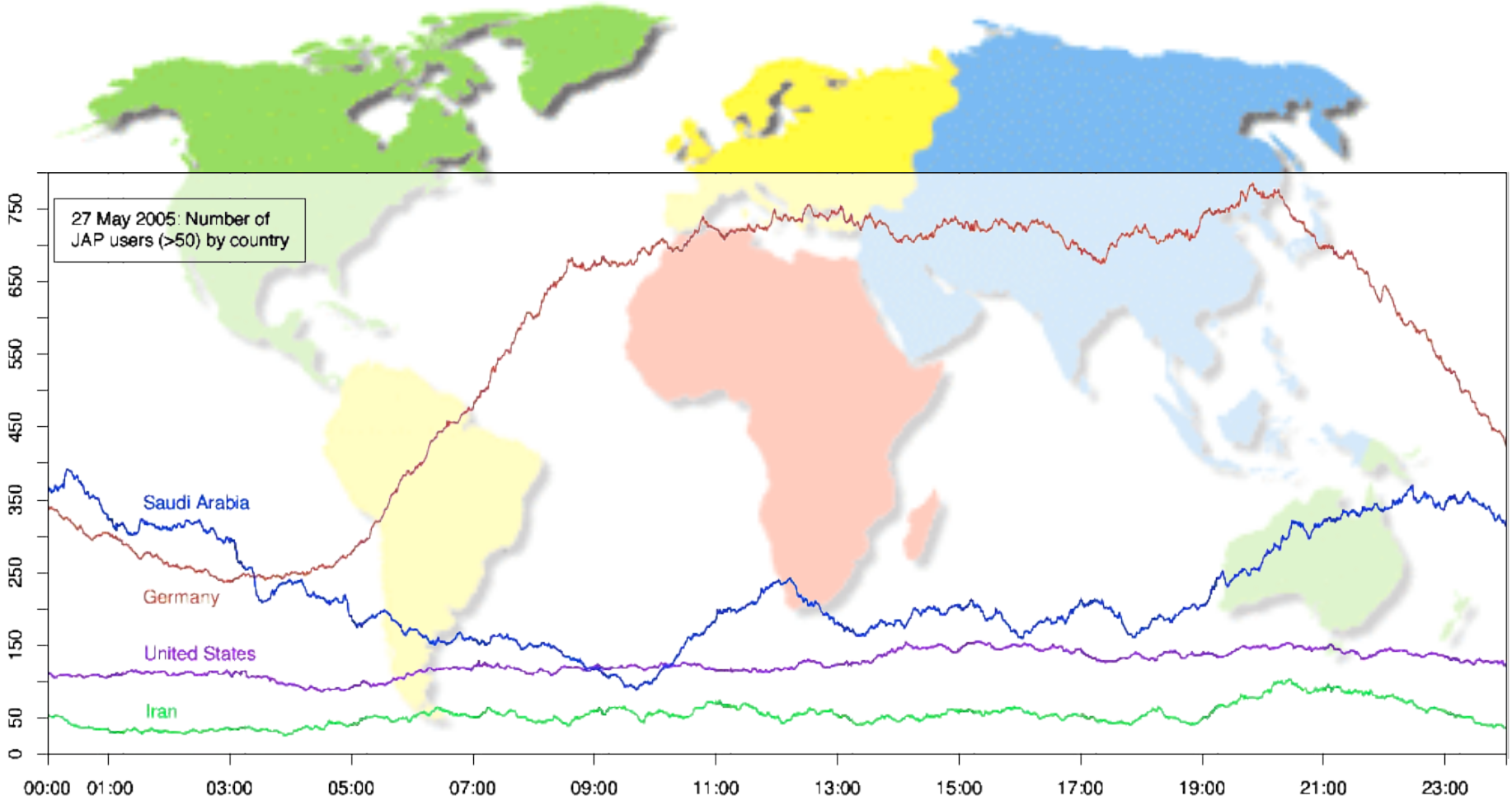
- Adaption der Mixe auf Echtzeitkommunikation
- Transparenz für den Nutzer
- Dezentrale Architektur des Gesamtsystems
- Abrechnung anonym genutzter Dienste
- Stärkung des Nutzers bei gleichzeitiger Strafverfolgungsmöglichkeit

AN.ON: Architektur



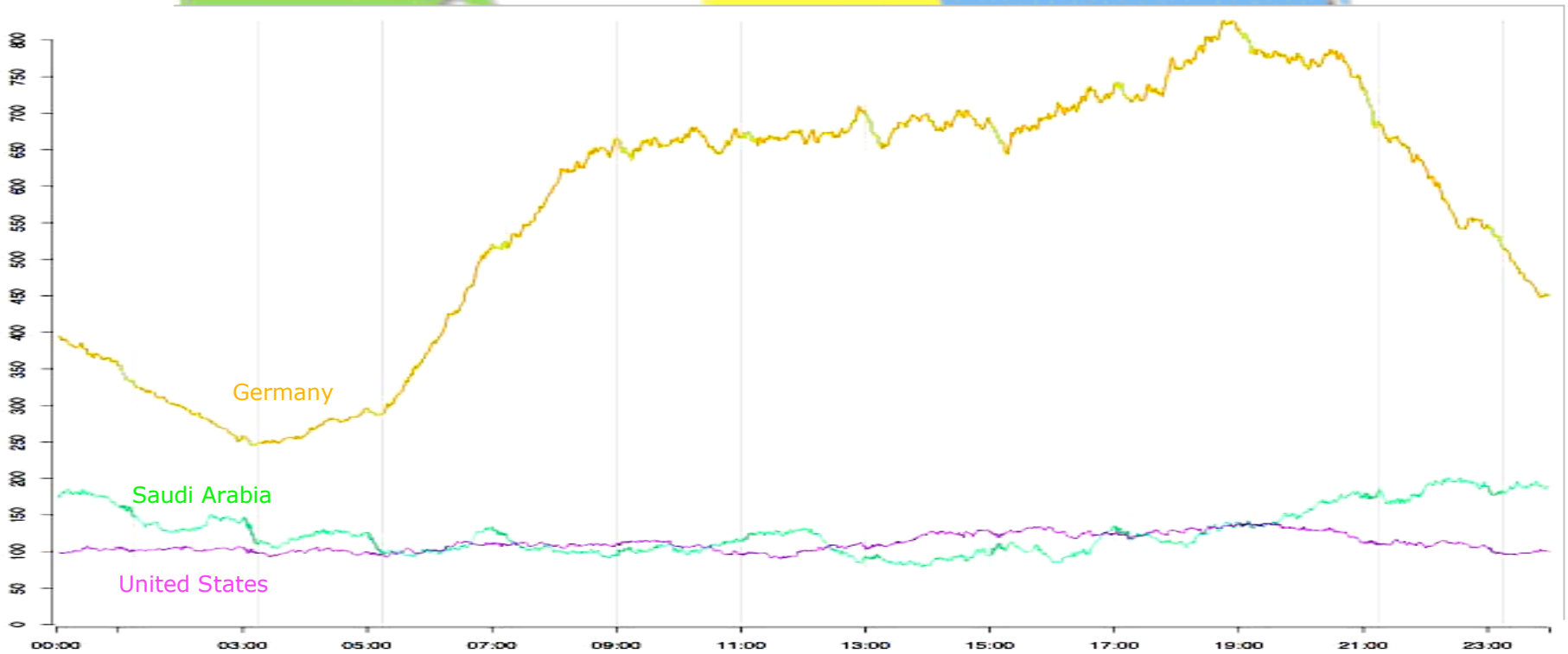
Wo kommen die JAP-Nutzer her?

- Dayline of May 27, 2005



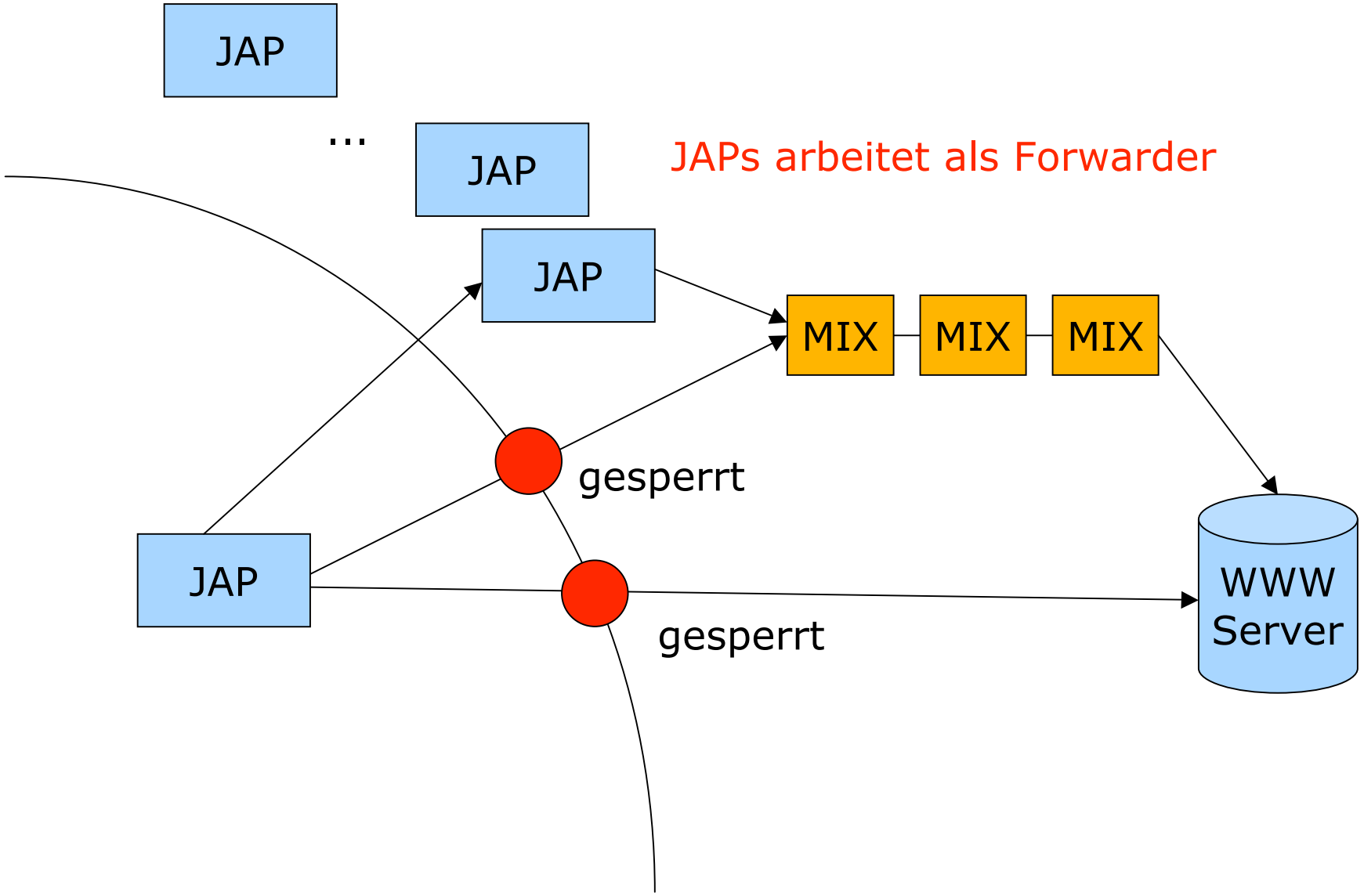
Wo kommen die JAP-Nutzer her?

- Dayline of Aug 1, 2005

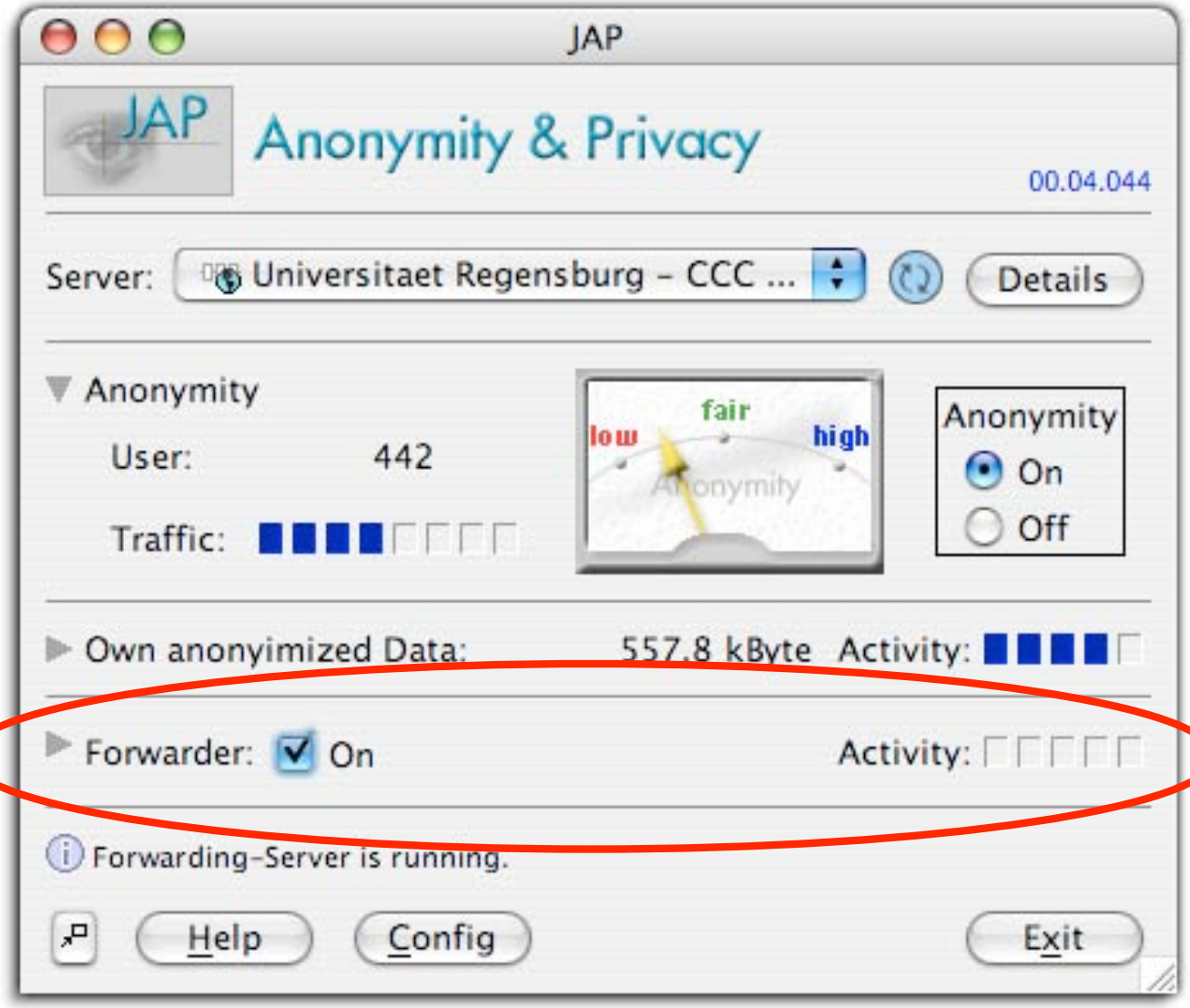


Iran?

Blockingresistenz



Blockingresistenz

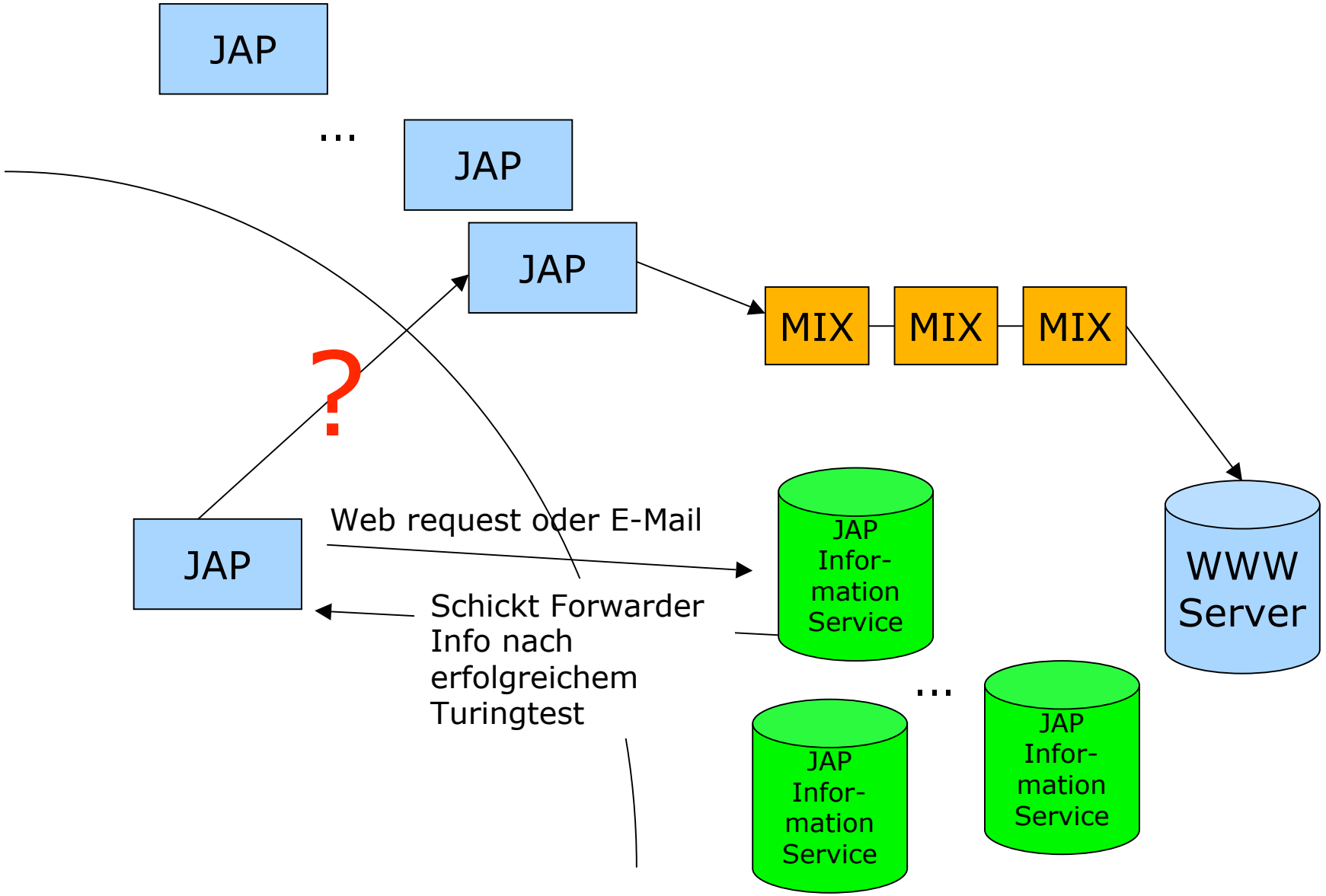


JAP-Nutzer stellen Teil ihrer Bandbreite zur Verfügung

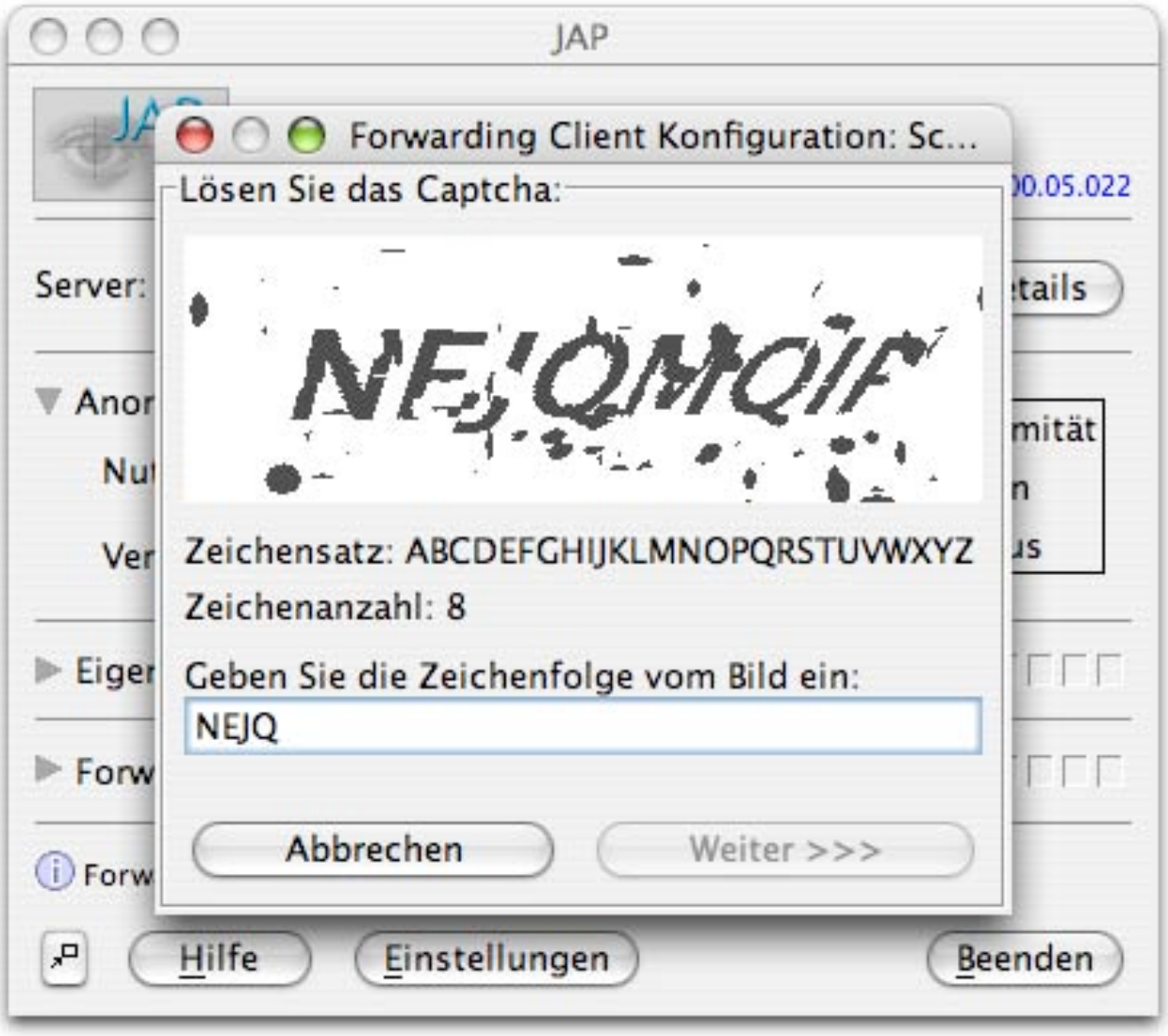
Zugriffe werden durch die Mixe anonymisiert

Forwarder erfahren nichts über die zugegriffenen Inhalte

Blockingresistenz



Blockingresistenz



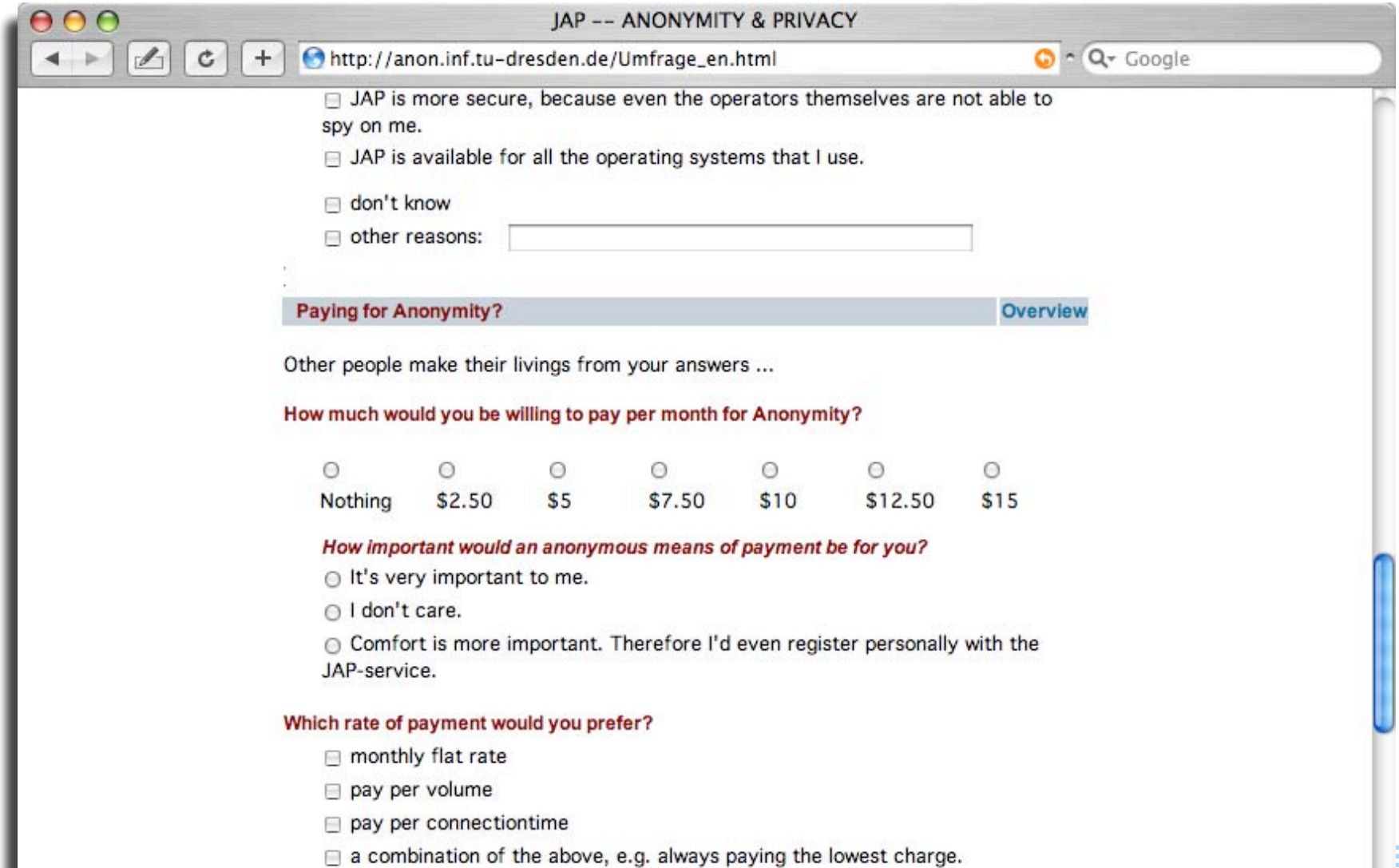
InfoService schickt Forwarder Info nach erfolgreichem Turingtest

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)

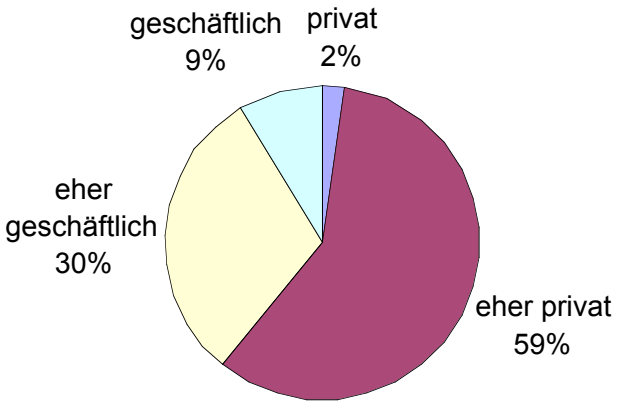
- Stichprobe:
  - 1800 JAP-Nutzer



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



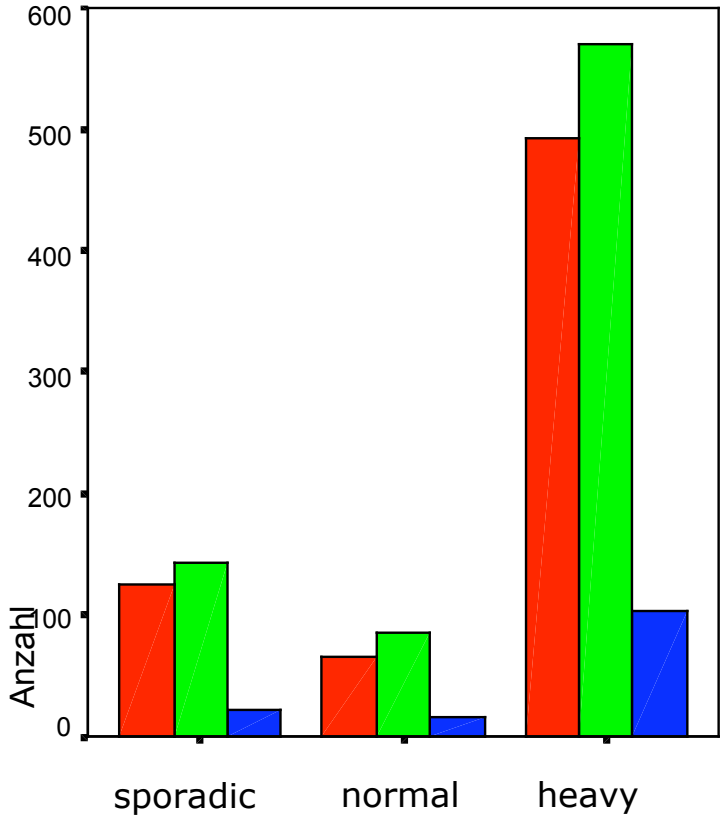
- Warum JAP?
  - ≈ 76% kostenlos
  - ≈ 56% schützt vor Betreibern
  - ≈ 51% einfach benutzbar

Umfrage unter JAP-Benutzern

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

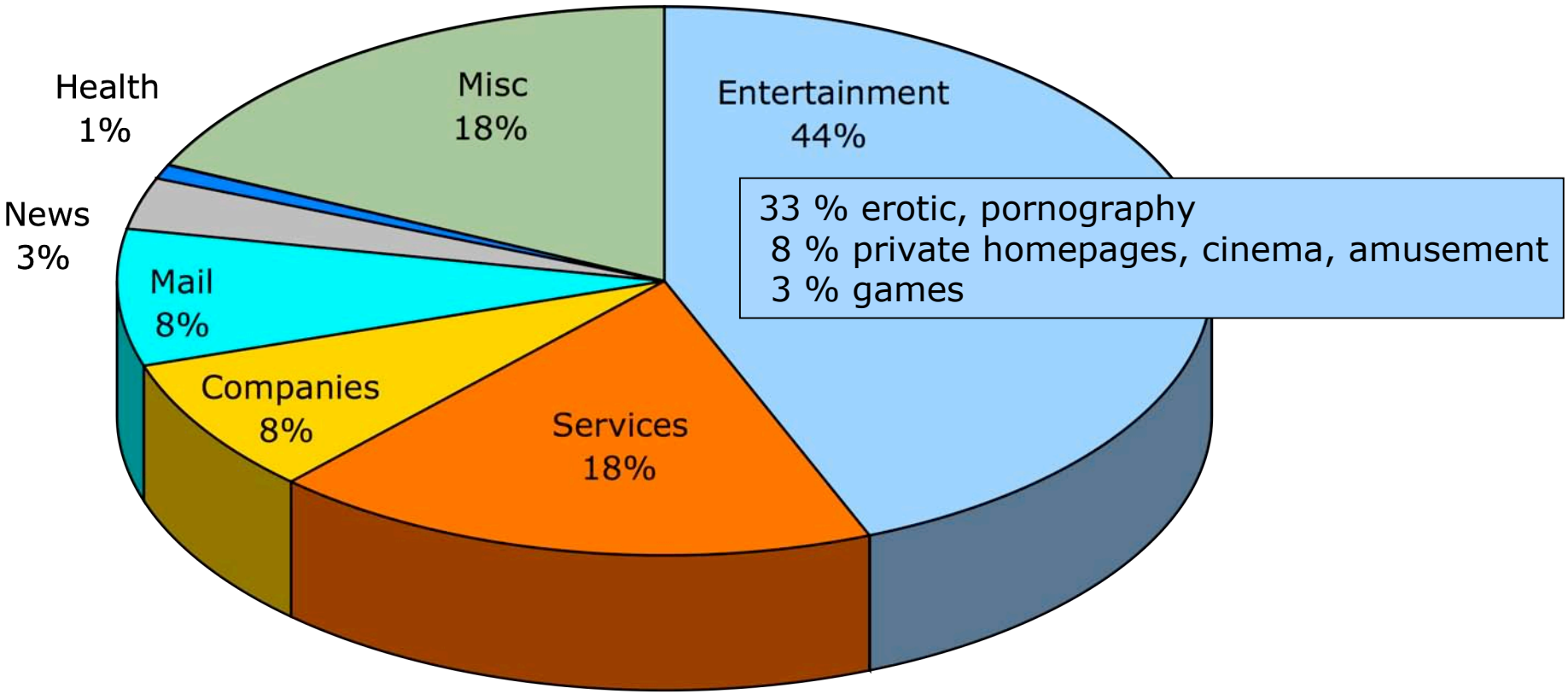
- Zahlungsbereitschaft korreliert nicht mit der Intensität der Nutzung

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



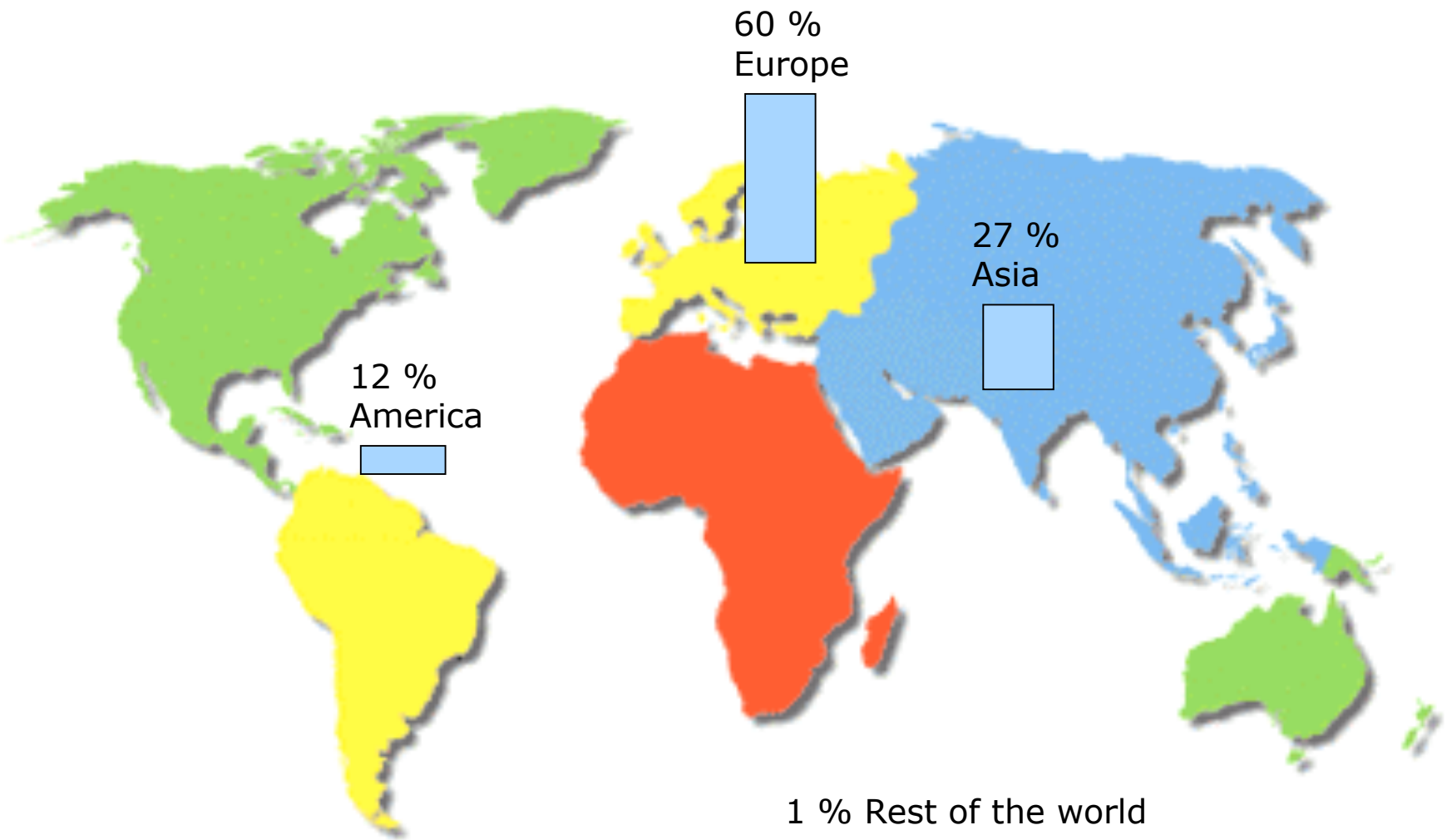
Anonymisierte Inhalte

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

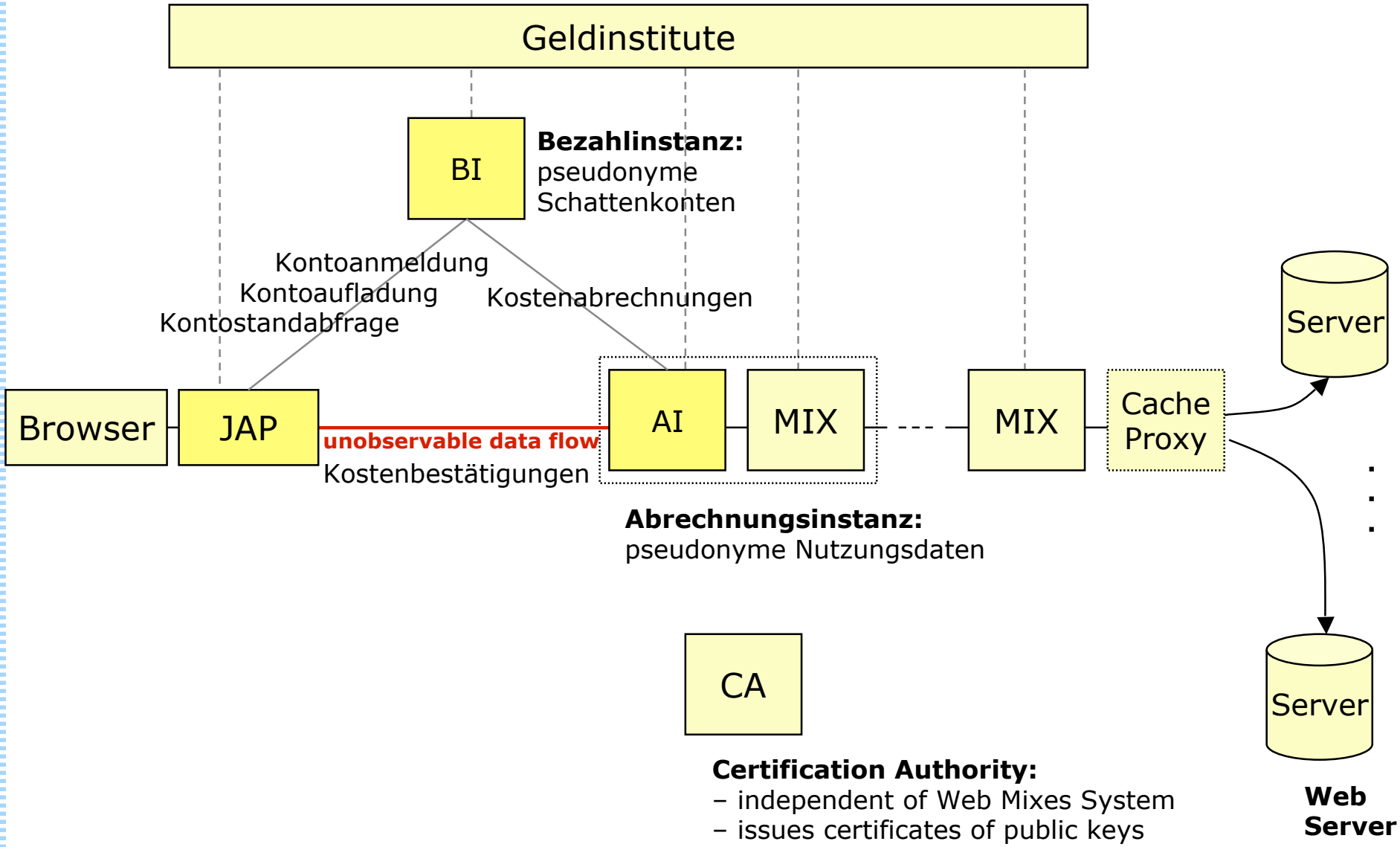


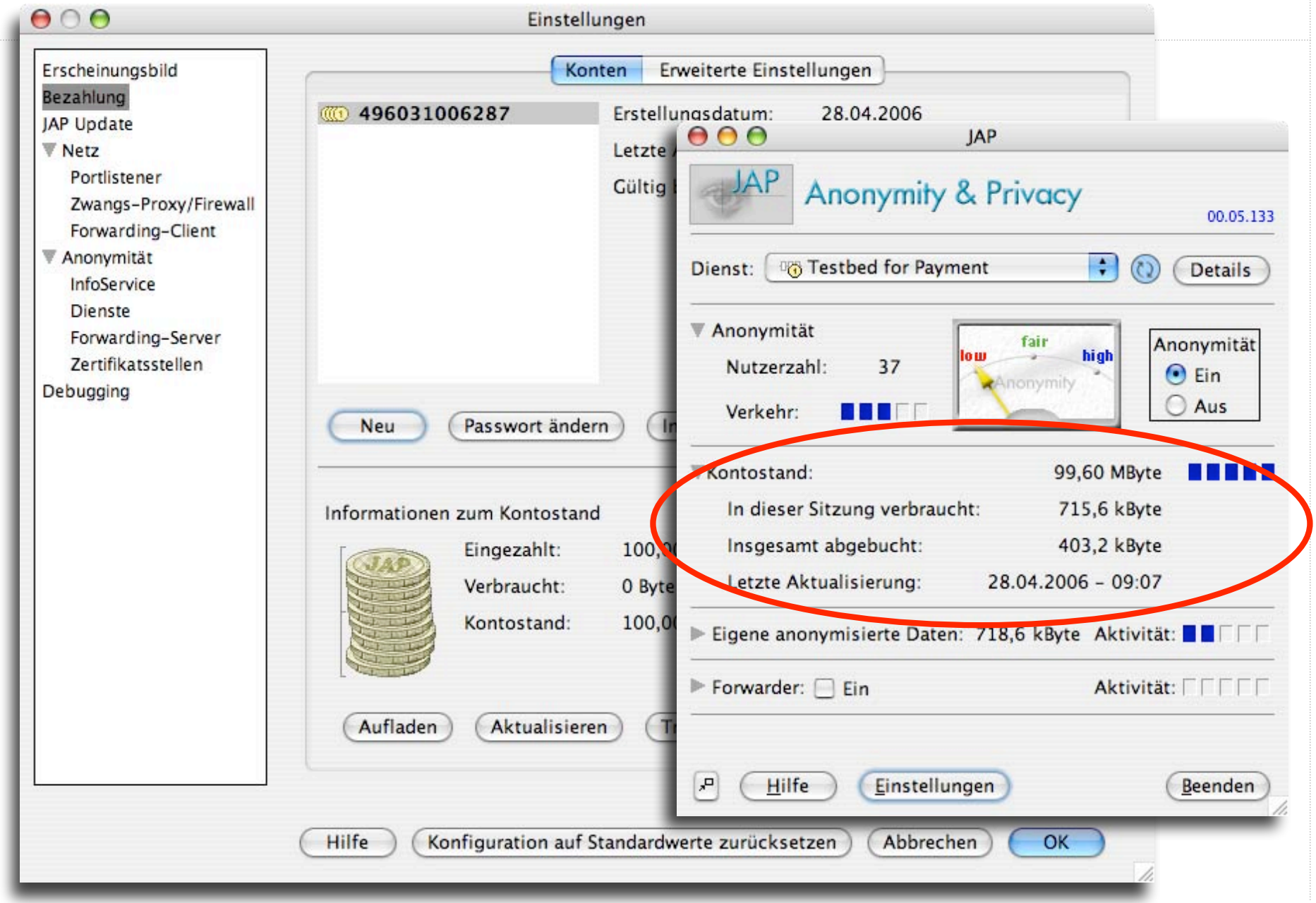
Wo kommen die JAP-Nutzer her?

- Eingehende Requests nach Regionen Mai-Juni 2005



Architektur Bezahlsystem

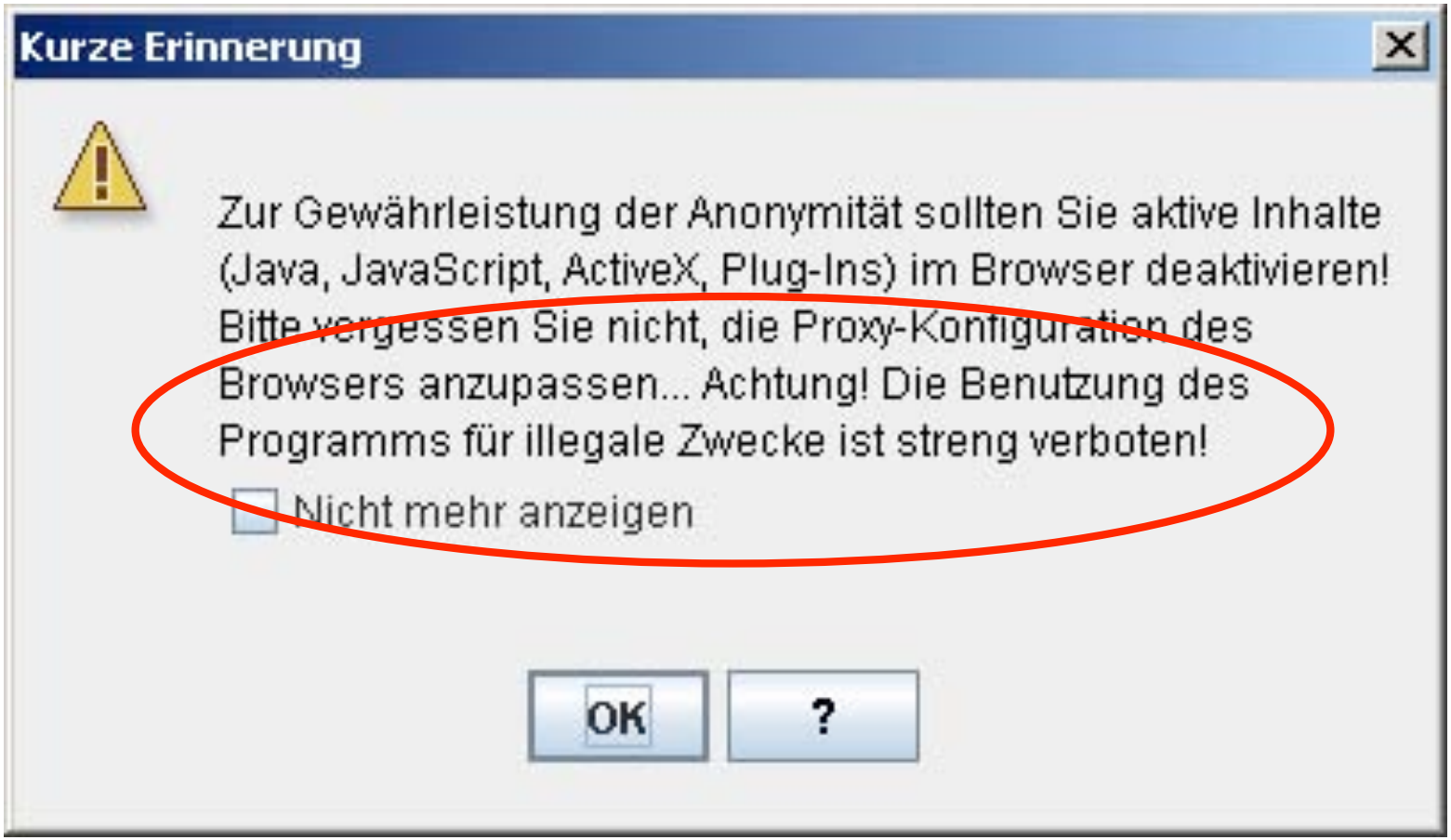



Einstellungen
Erscheinungsbild
Bezahlung
JAP Update
Netz
Portlistener
Zwangs-Proxy/Firewall
Forwarding-Client
Anonymität
InfoService
Dienste
Forwarding-Server
Zertifikatsstellen
Debugging
Konten
Erweiterte Einstellungen
496031006287
Erstellungsdatum: 28.04.2006
Neu
Passwort ändern
Informationen zum Kontostand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

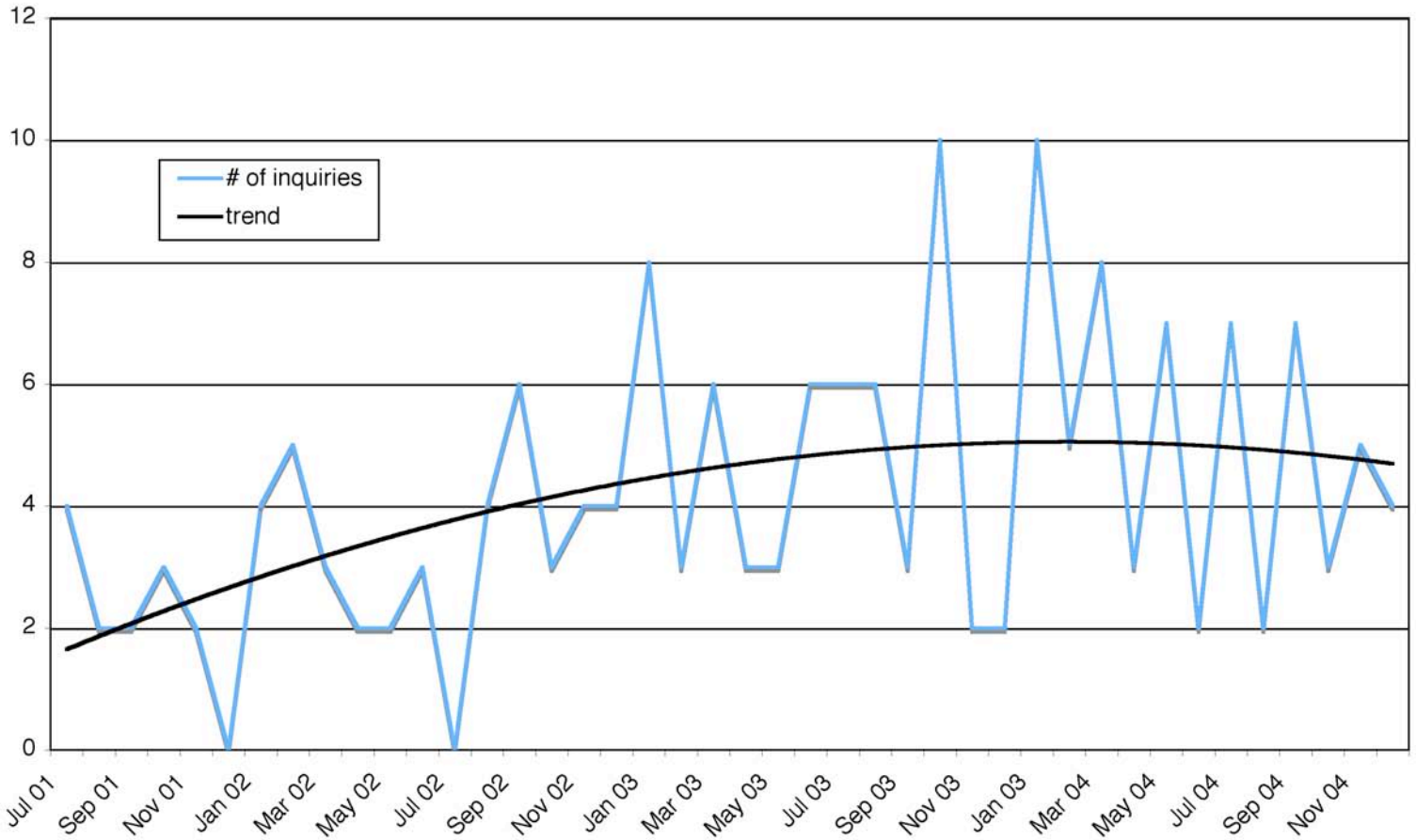
- Adaption der Mixe auf Echtzeitkommunikation
- Transparenz für den Nutzer
- Dezentrale Architektur des Gesamtsystems
- Abrechnung anonym genutzter Dienste
- Stärkung des Nutzers bei gleichzeitiger Strafverfolgungsmöglichkeit

Missbrauch ist selbstverständlich verboten

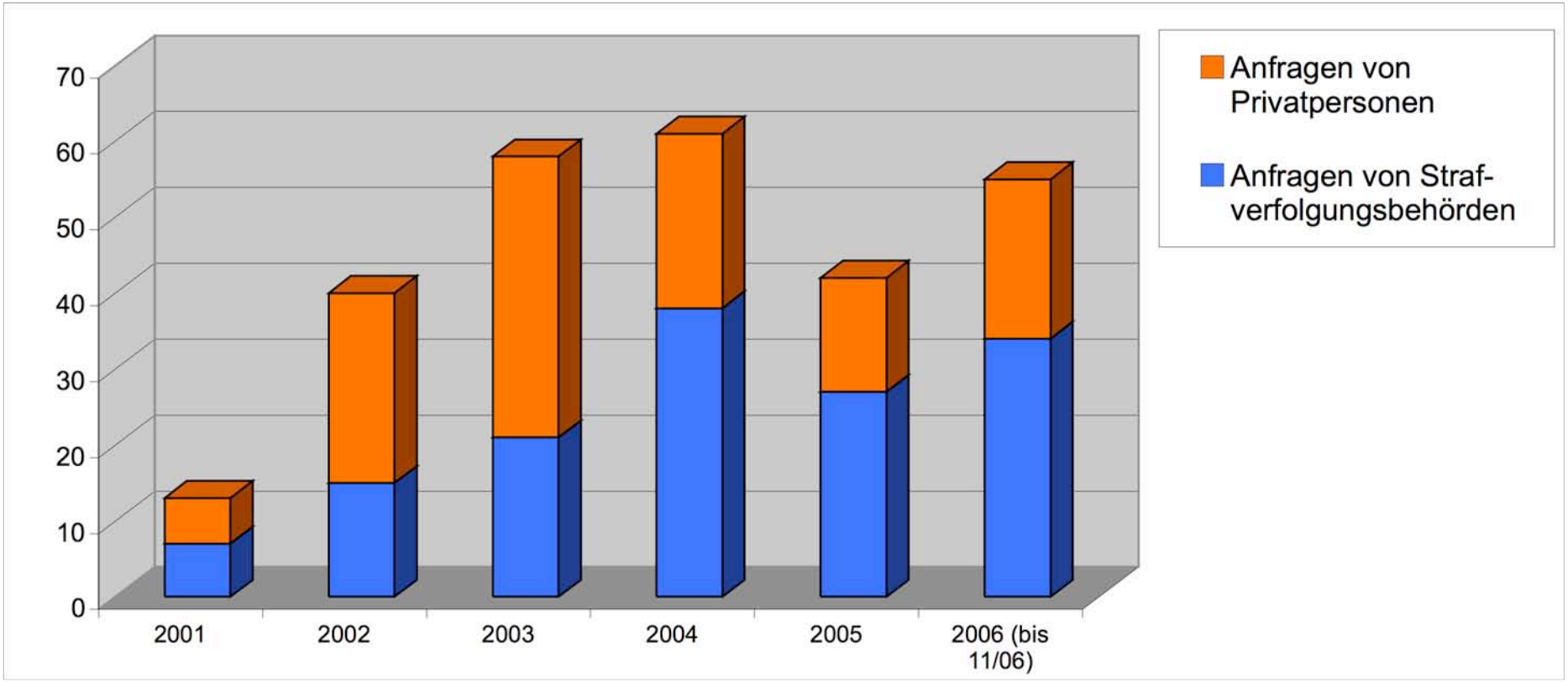


Missbrauch und Strafverfolgung AN.ON/JAP

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



Anzahl der Anfragen pro Jahr



Analyse der missbräuchlichen Benutzung von AN.ON

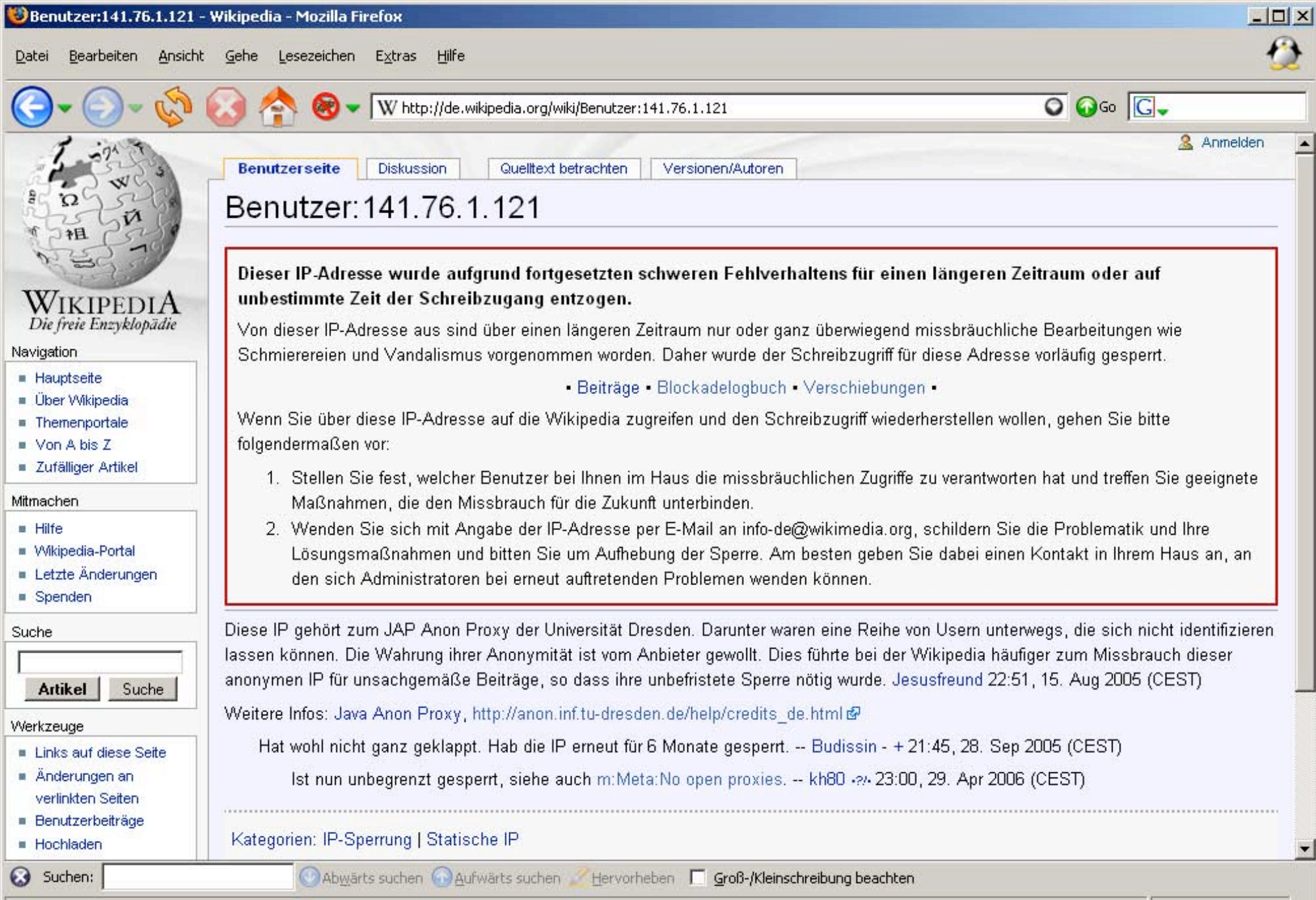
Wie ist eine Anfrage aufgebaut?

- Von einem Webserver mitprotokollierte IP-Adresse eines letzten Mixes, 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 oder »Gefahr im Verzug«

Vorgehen gegen Missbrauch

- Auf Seiten von AN.ON
  - Dienst zur Zeit auf Web-Zugriffe beschränkt, obwohl allgemeiner anonymer TCP/IP möglich wäre
  - Auf Anfrage Sperrung einer URL durch Betreiber letzter Mixe mit Meldung an den Nutzer
  - Bei richterlichem Beschluss: »Fangschaltung« für die Zukunft
  - geplant: Unterstützung eines Filters zur Verhinderung des Abrufs kinderpornographischer Inhalte

- Auf Seiten der Internet-Dienste
  - Am wichtigsten wäre:
    - entsprechende Gestaltung und Absicherung der Dienste
  - Sperrung von Zugriffen über IP-Adressen der letzten Mixe

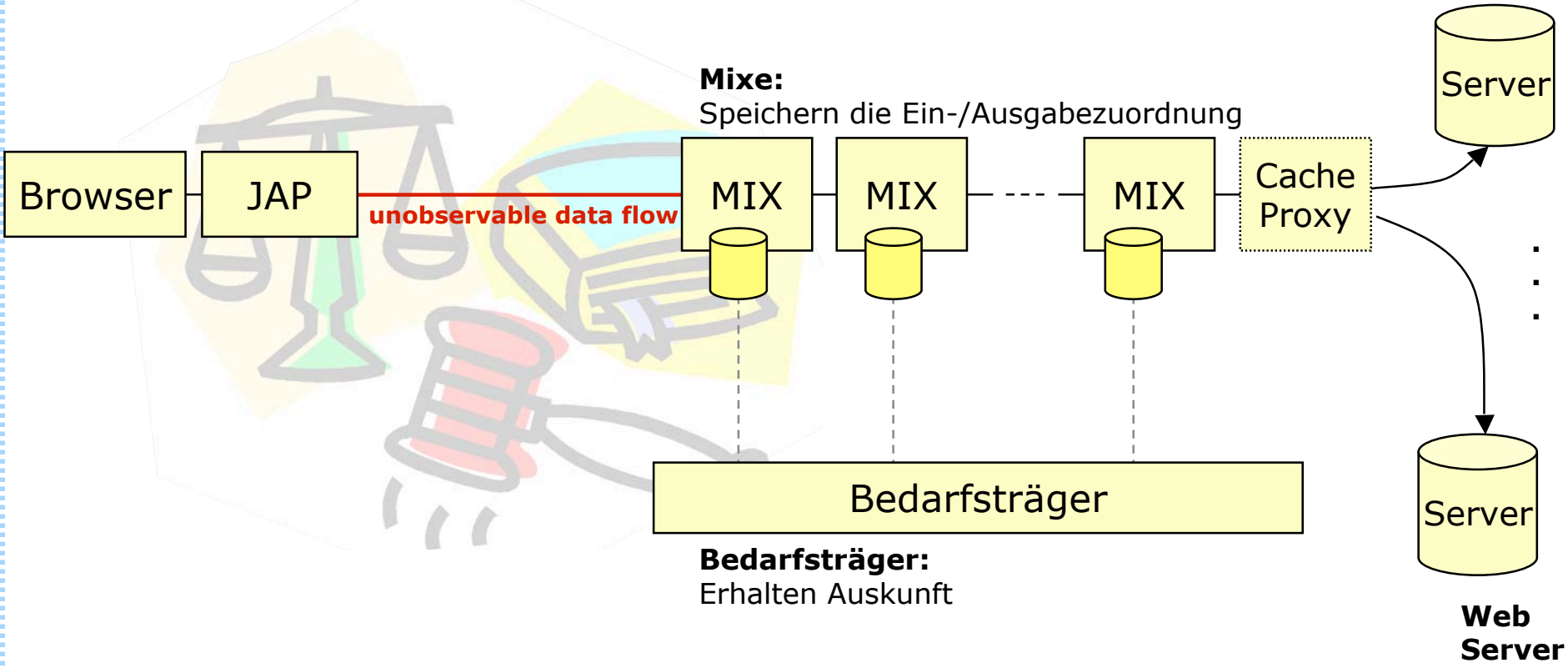

Benutzer:141.76.1.121 - Wikipedia - Mozilla Firefox
Datei Bearbeiten Ansicht Gehe Lesezeichen Extras Hilfe
http://de.wikipedia.org/wiki/Benutzer:141.76.1.121
Go
Anmelden
Benutzerseite
Diskussion
Quelltext betrachten
Versionen/Autoren
Benutzer:141.76.1.121
Dieser IP-Adresse wurde aufgrund fortgesetzten schweren Fehlverhaltens für einen längeren Zeitraum oder auf unbestimmte Zeit der Schreibzugang entzogen.
Von dieser IP-Adresse aus sind über einen längeren Zeitraum nur oder ganz überwiegend missbräuchliche Bearbeitungen wie Schmierereien und Vandalismus vorgenommen worden. Daher wurde der Schreibzugriff für diese Adresse vorläufig gesperrt.
• Beiträge • Blockadelogbuch • Verschiebungen •
Wenn Sie über diese IP-Adresse auf die Wikipedia zugreifen und den Schreibzugriff wiederherstellen wollen, gehen Sie bitte folgendermaßen vor:
1. Stellen Sie fest, welcher Benutzer bei Ihnen im Haus die missbräuchlichen Zugriffe zu verantworten hat und treffen Sie geeignete Maßnahmen, die den Missbrauch für die Zukunft unterbinden.
2. Wenden Sie sich mit Angabe der IP-Adresse per E-Mail an info-de@wikimedia.org, schildern Sie die Problematik und Ihre Lösungsmaßnahmen und bitten Sie um Aufhebung der Sperre. Am besten geben Sie dabei einen Kontakt in Ihrem Haus an, an den sich Administratoren bei erneut auftretenden Problemen wenden können.
Diese IP gehört zum JAP Anon Proxy der Universität Dresden. Darunter waren eine Reihe von Usern unterwegs, die sich nicht identifizieren lassen können. Die Wahrung ihrer Anonymität ist vom Anbieter gewollt. Dies führte bei der Wikipedia häufiger zum Missbrauch dieser anonymen IP für unsachgemäße Beiträge, so dass ihre unbefristete Sperre nötig wurde. Jesusfreund 22:51, 15. Aug 2005 (CEST)
Weitere Infos: Java Anon Proxy, http://anon.inf.tu-dresden.de/help/credits_de.html
Hat wohl nicht ganz geklappt. Hab die IP erneut für 6 Monate gesperrt. -- Budissin - + 21:45, 28. Sep 2005 (CEST)
Ist nun unbegrenzt gesperrt, siehe auch m:Meta:No open proxies. -- kh80 -?- 23:00, 29. Apr 2006 (CEST)
Kategorien: IP-Sperrung | Statische IP
WIKIPEDIA
Die freie Enzyklopädie
Navigation
Hauptseite
Über Wikipedia
Themenportale
Von A bis Z
Zufälliger Artikel
Mitmachen
Hilfe
Wikipedia-Portal
Letzte Änderungen
Spenden
Suche
Artikel
Suche
Werkzeuge
Links auf diese Seite
Änderungen an verlinkten Seiten
Benutzerbeiträge
Hochladen
Suchen:
Abwärts suchen
Aufwärts suchen
Hervorheben
Groß-/Kleinschreibung beachten

Anonyme Kommunikation ist legal

- Telemediengesetz (TMG)
  - § 13 Abs. 6 TMG: 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.

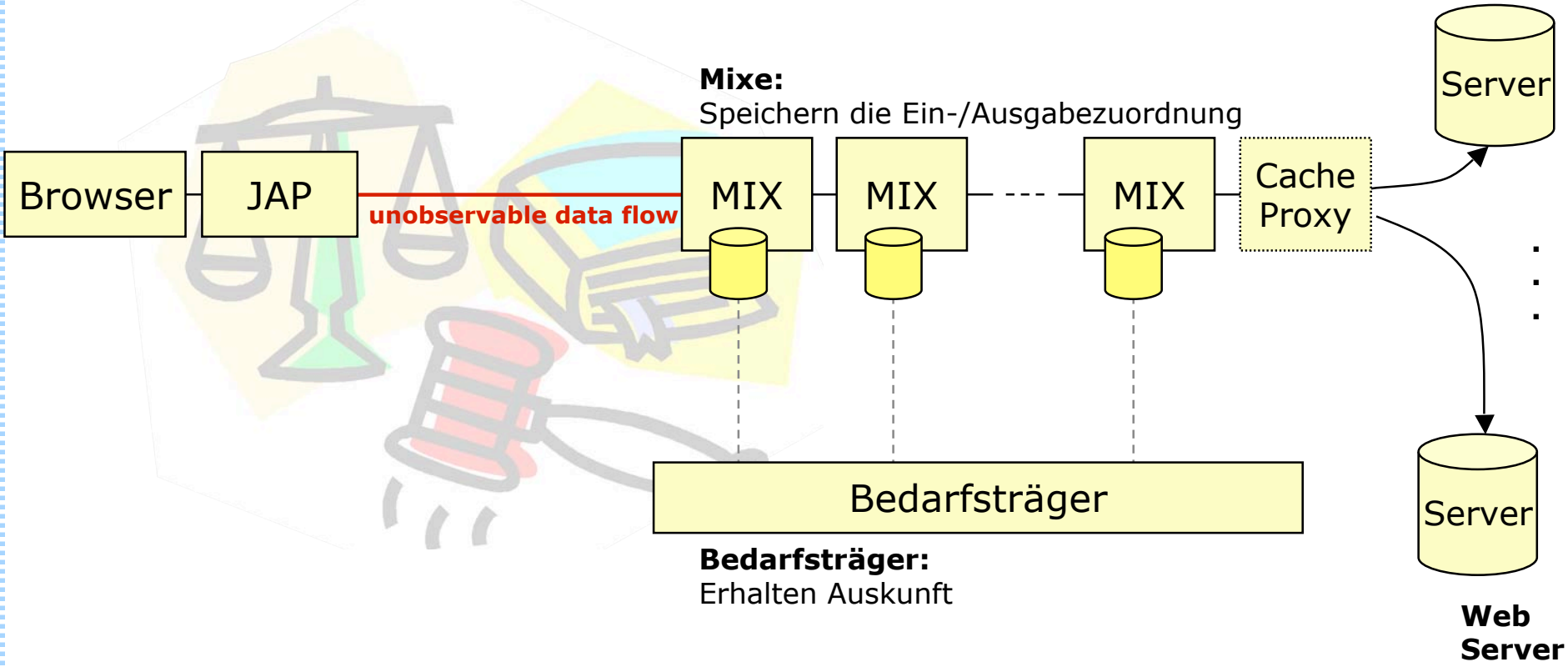
Strafverfolgung bei schweren Straftaten

- Voraussetzung: Anordnung nach § 100a,b StPO
  - Aktivieren der Funktion nach richterlicher Anordnung
  - auf 3 Monate begrenzt
  - nur für Zukunft
  - wird erfasst in Überwachungsstatistik



Vorratsdatenspeicherung

- Mixe speichern Ein-/Ausgabezuordnung für 6 Monate
  - Problem: Ziel-URLs dürfen nicht gespeichert werden
  - Auskunftsersuchen bezieht sich auf ausgehende IP (Cache-Proxy) und Uhrzeit



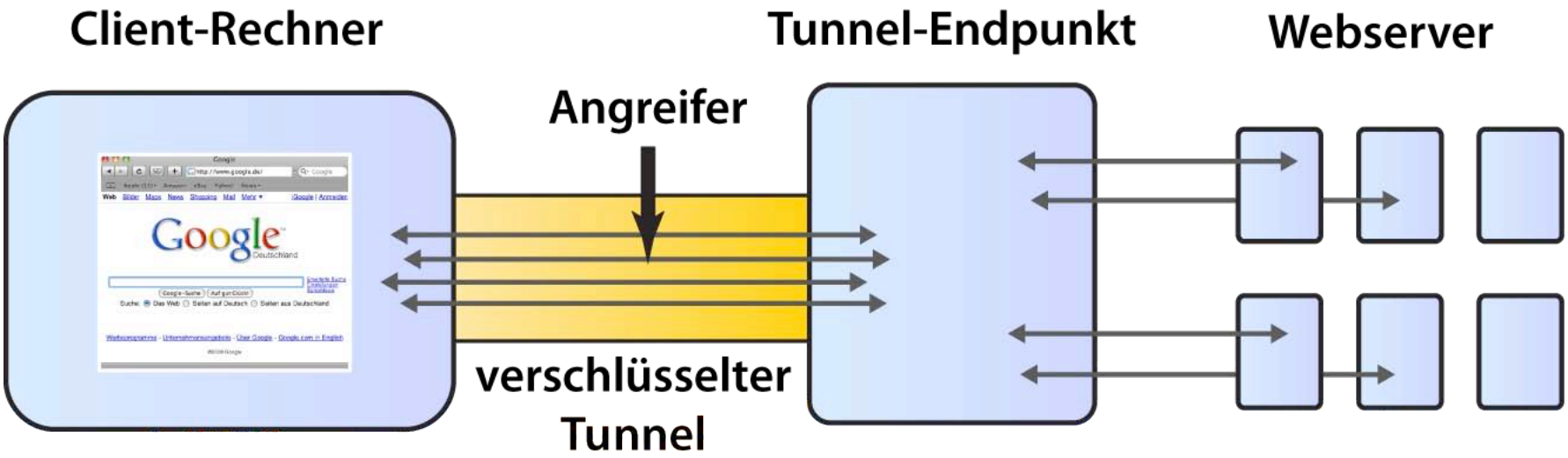
Angriffe auf verschlüsselt übertragene Daten

- Entschlüsselung des Datenstroms meist aussichtslos

- Alternativen:
  - Online-Durchsuchung: Direkter Zugriff auf Klartexte durch Installation einer Software auf dem Rechner eines Verdächtigen.
  - Traffic-Analyse: Durch Analyse charakteristischen Eigenschaften des Datenverkehrs kann ein passiver Beobachter auf Inhalts und/oder Adressdaten schließen.

- Beobachtbare Merkmale:
  - Auftretenshäufigkeit von Paketen/Verbindungen
  - Paketgröße und Datendurchsatz
  - Zeitpunkte und Paketzwischenabstände

Szenario Traffic-Analyse



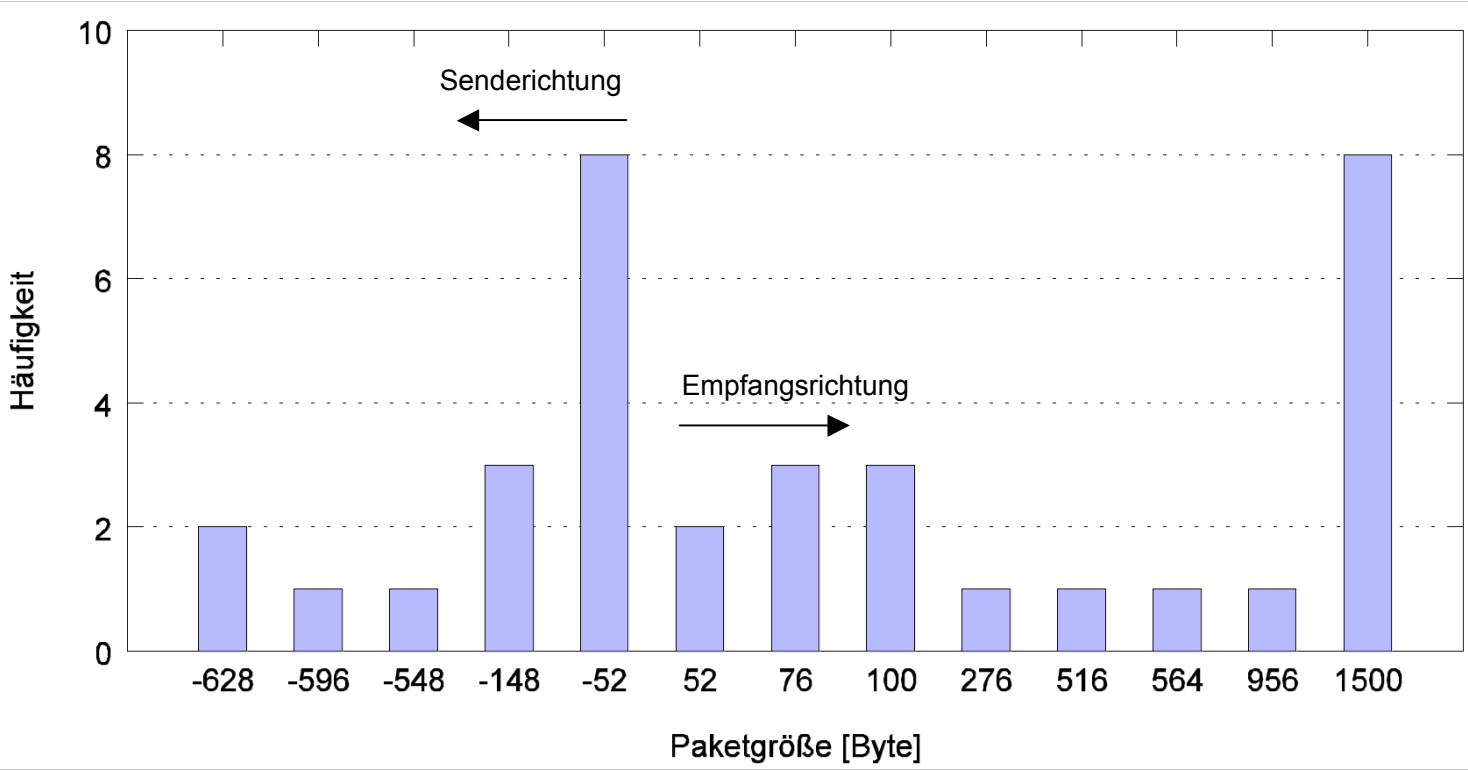
- Beobachtbare Merkmale:
  - Auftretenshäufigkeit von Paketen/Verbindungen
  - Paketgröße und Datendurchsatz
  - Zeitpunkte und Paketzwischenabstände

Identifizierung von verschlüsselt übertragenen Webseiten

- Website-Fingerprinting (nach *Bissias et al.*, *Liberatore et al.*):
  - Jede Webseite erzeugt bei der Übertragung charakteristischen Datenverkehr (u.a. bedingt durch Größe/Anzahl der eingebetteten Bilder).
- Idee
  - Aufzeichnung der Fingerabdrücke für relevante Webseiten
  - Aufzeichnung des Datenverkehrs (Sniffing) und Suche nach *bekannten* Mustern
- Prototypische Implementierung
  - Analyse von Paketgrößen und Zeitabständen zwischen Paketen
  - Korrelationsanalyse bzw. Data-Mining-Techniken zur Muster-Suche
  - verschlüsselter Abruf von Seiten über SSH-Tunnel
- Probleme
  - geringe Erkennungsraten
  - Abhängigkeit von Browserversion und -konfiguration
  - idealistische Annahmen, Untersuchung unter Realbedingungen fehlt

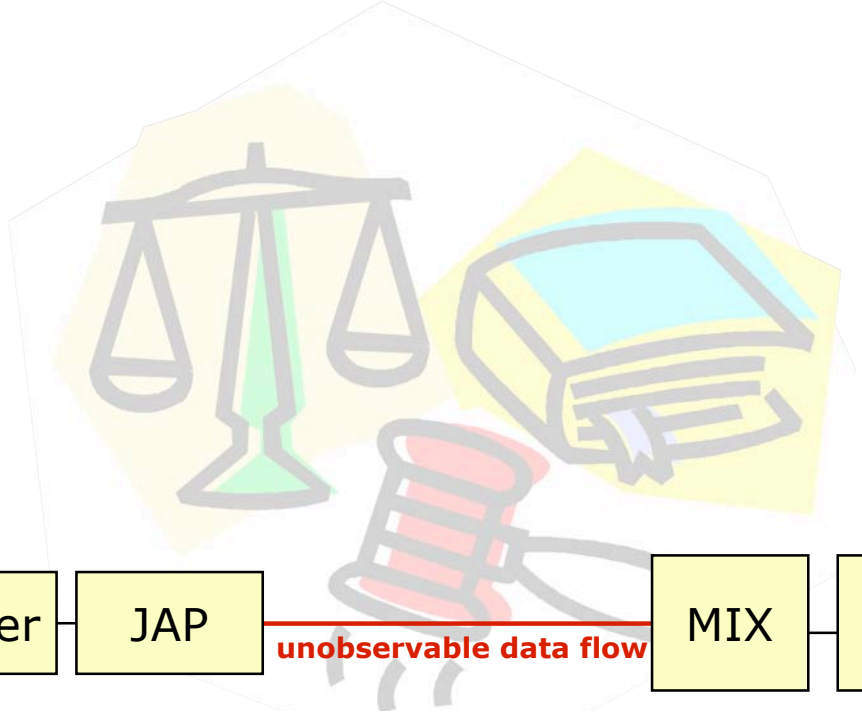
Verbessertes Website-Fingerprinting-Verfahren

- Analyse der charakteristischen Häufigkeitsverteilung der IP-Paketgrößen

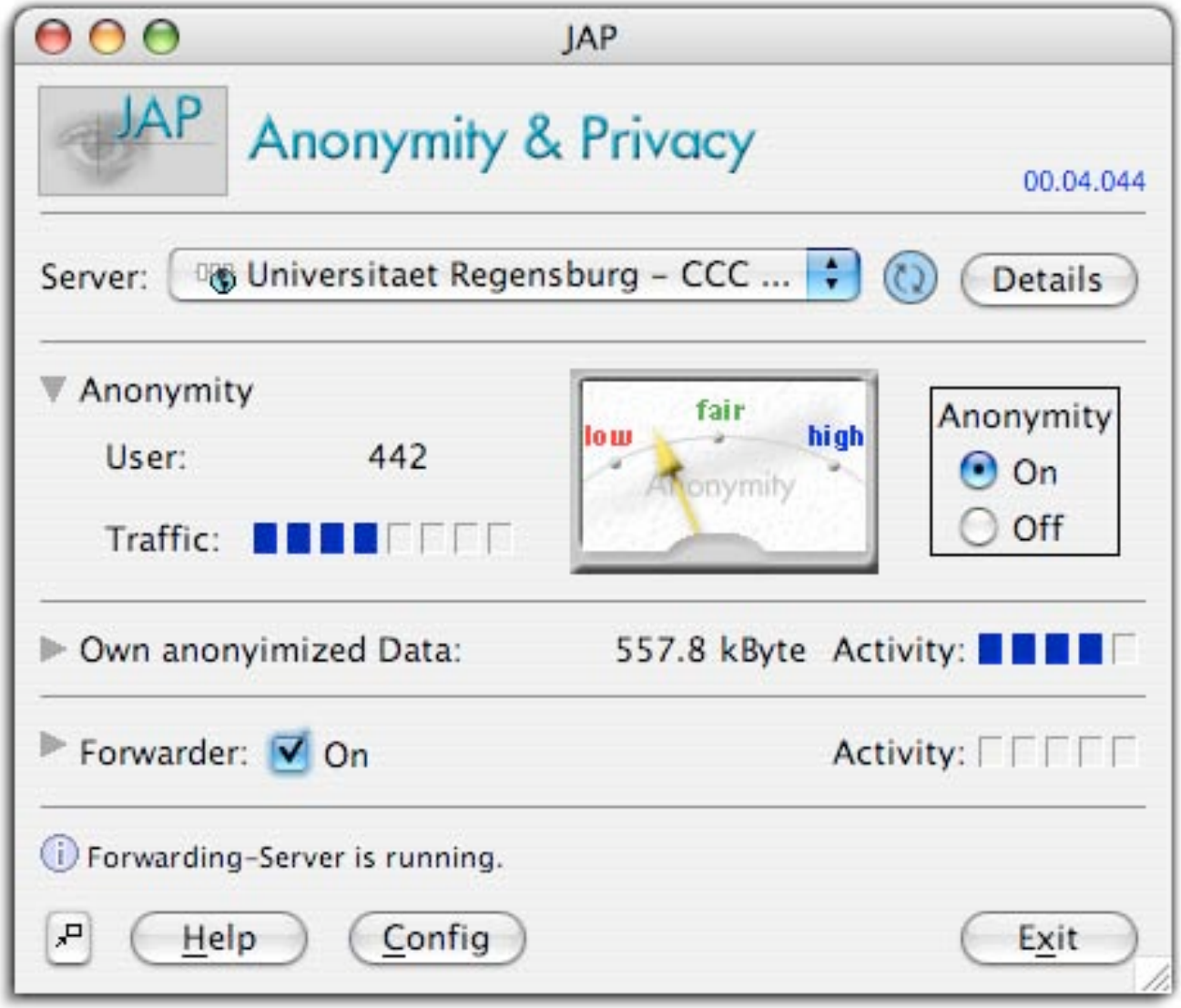


- Schutz durch datenschutzfreundliche Systeme?
  - gering: SSH-Tunnel und VPNs; Erkennungsrate: 90-97%
  - moderat: Anonymisierer wie Tor und JAP/JonDonym; Erkennungsrate: < 20%

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)

www.anon-online.de

AN.ON/JAP

```
final String msg =
    "JAP must run with a 1.1.3 or higher version Java
String javaVersion = System.getProperty("java.version
String vendor = System.getProperty("java.vendor");
String os = System.getProperty("os.name");
String mrjVersion = System.getProperty("mrj.version"

if (isArgumentSet("--version") || isArgumentSet("-v"
{
    System.out.println("JAP version: " + JAPConstants
                       "Java Vendor: " + vendor + "\r
                       "Java Version: " + javaVersion
    System.exit(0);
}

if (!JAPConstants.m_bReleasedVersion)
{
    System.out.println("Starting up JAP version " +
                       (mrjVersion != null ? "/" + mr
}
//Macintosh Runtime for Java (MRJ) on Mac OS
// Test (part 1) for right JVM
if (javaVersion.compareTo("1.0.2") <= 0)
{
    System.out.println(msg + javaVersion);
    System.exit(0);
}

if (isArgumentSet("--help") || isArgumentSet("-h"))
{
    System.out.println("Usage:");
    System.out.println("--help, -h:                Shou
```

Open-Source-Projekt

> 25 Entwickler

LOC

JAP/InfoService/BI:	100387
MixConfig:	11204
Mix:	29122
Gesamt:	140713

Anonymisierter Traffic

>20 TB/Monat

Betreiber

> 20 über gesamte Projektlaufzeit

aktuell: ca. 8-10

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)

www.anon-online.de