Anonymität.Online
Technik – Szenarien – Geschäftsmodelle

Technische Ergebnisse

Berlin, 24.11.2006

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

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

Schutzziele

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

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

Grundverfahren
Anwendung

Bausteine datenschutzfördernder Technik

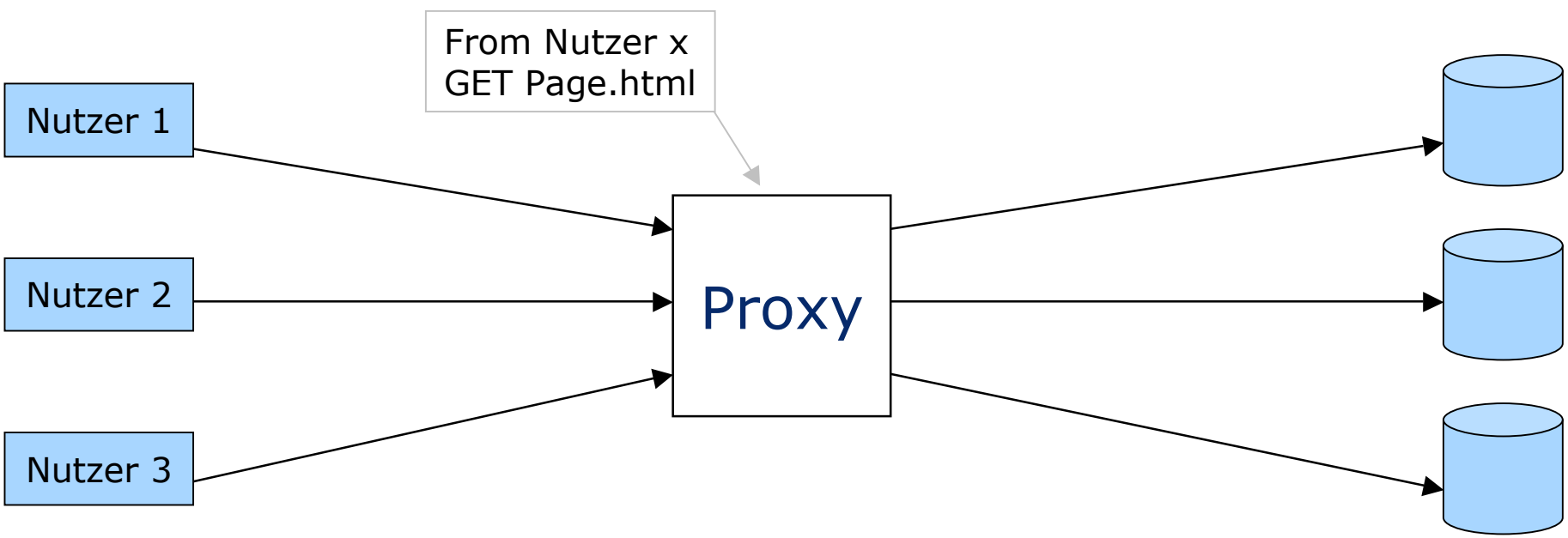
- Verschlüsselung

- 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)

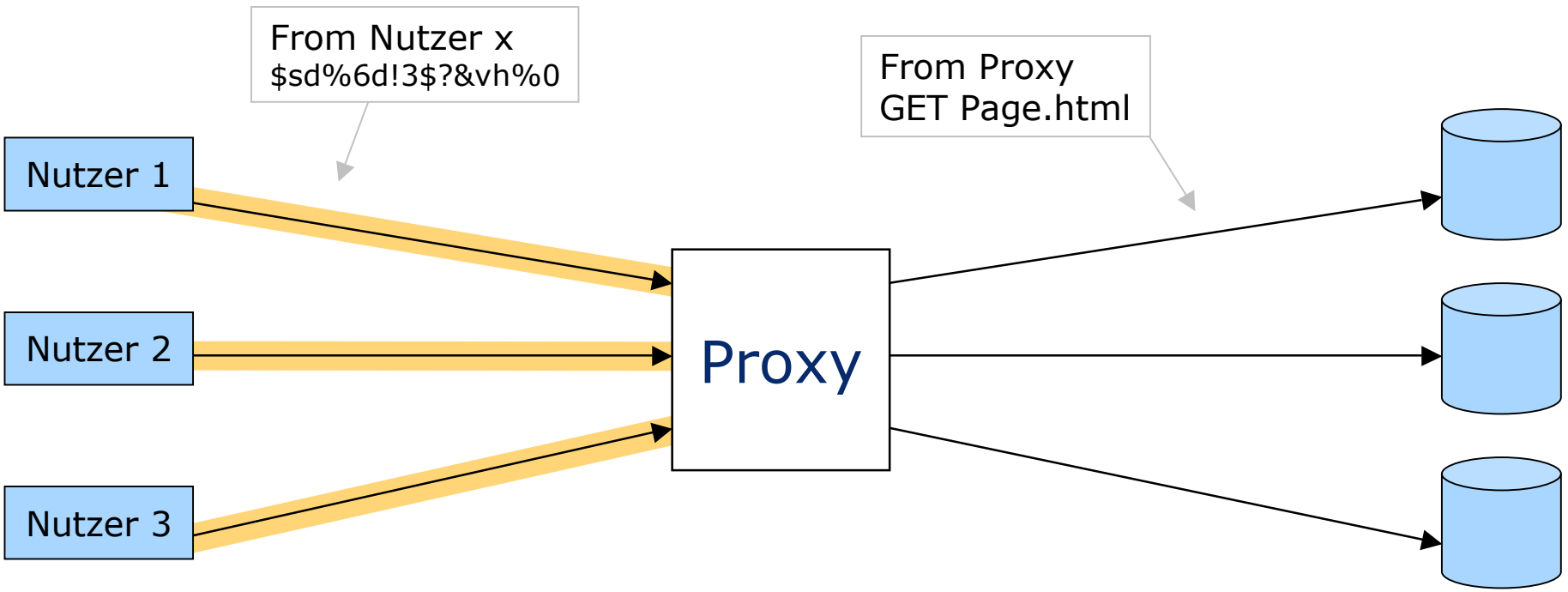
Proxies: Insider

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



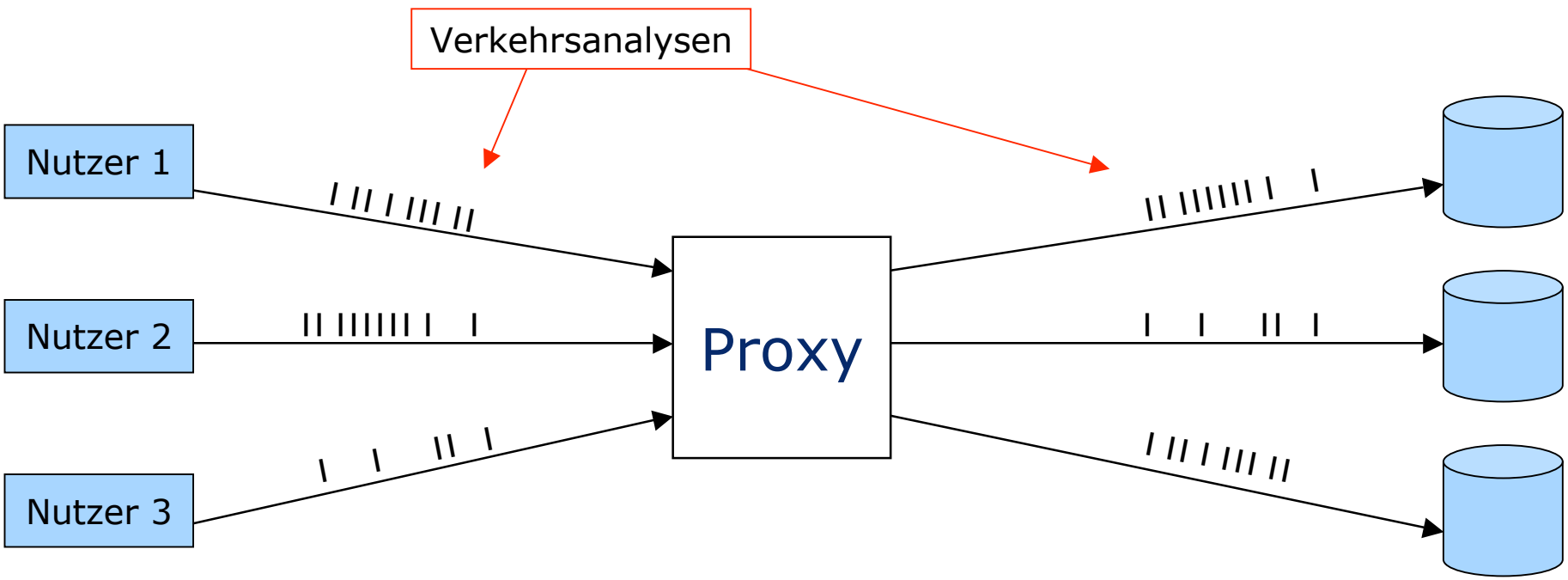
Proxies: Outsider

- 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)

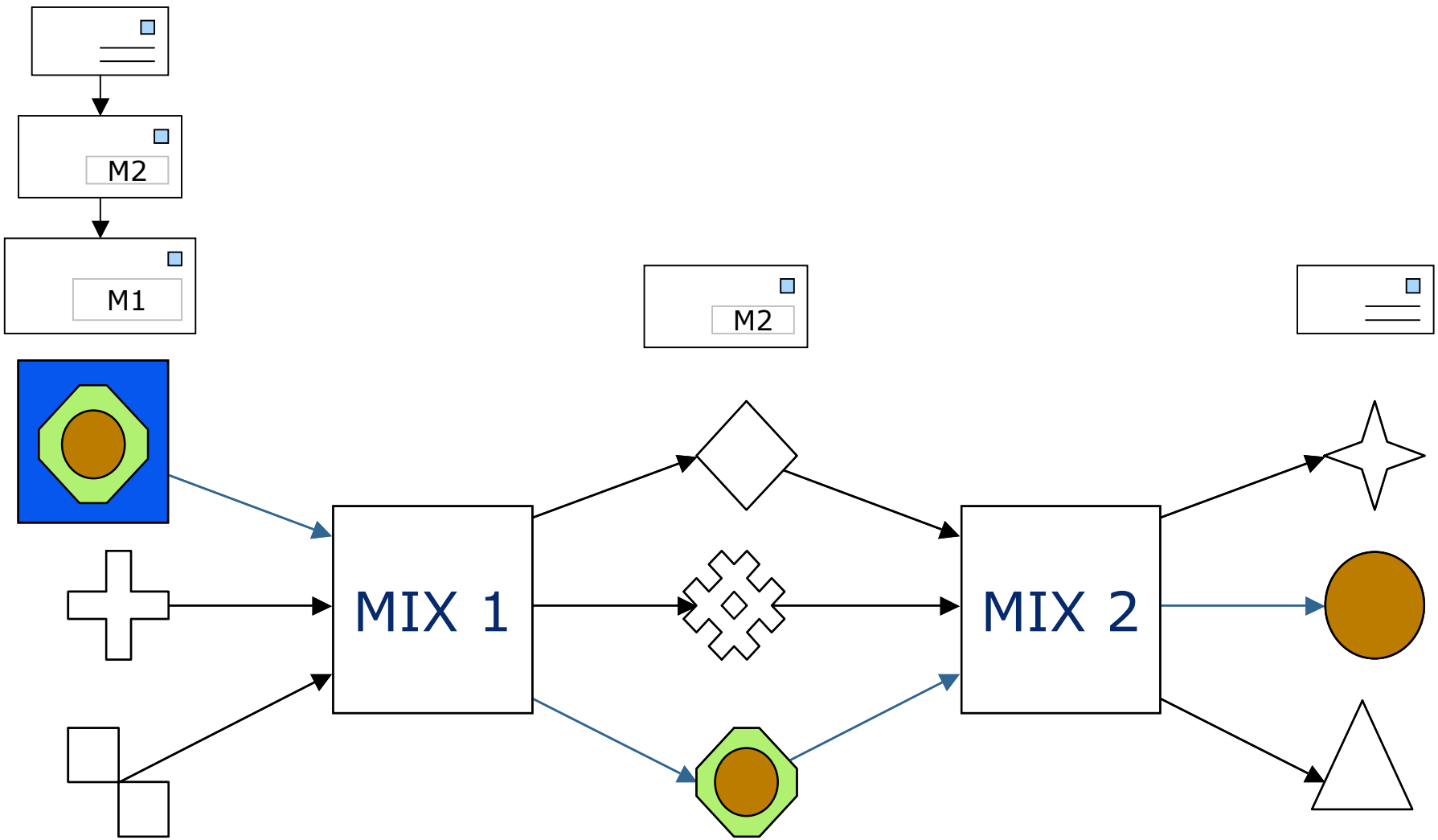
- System zum Schutz von Kommunikationsbeziehungen bei vermittelter Kommunikation

- 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

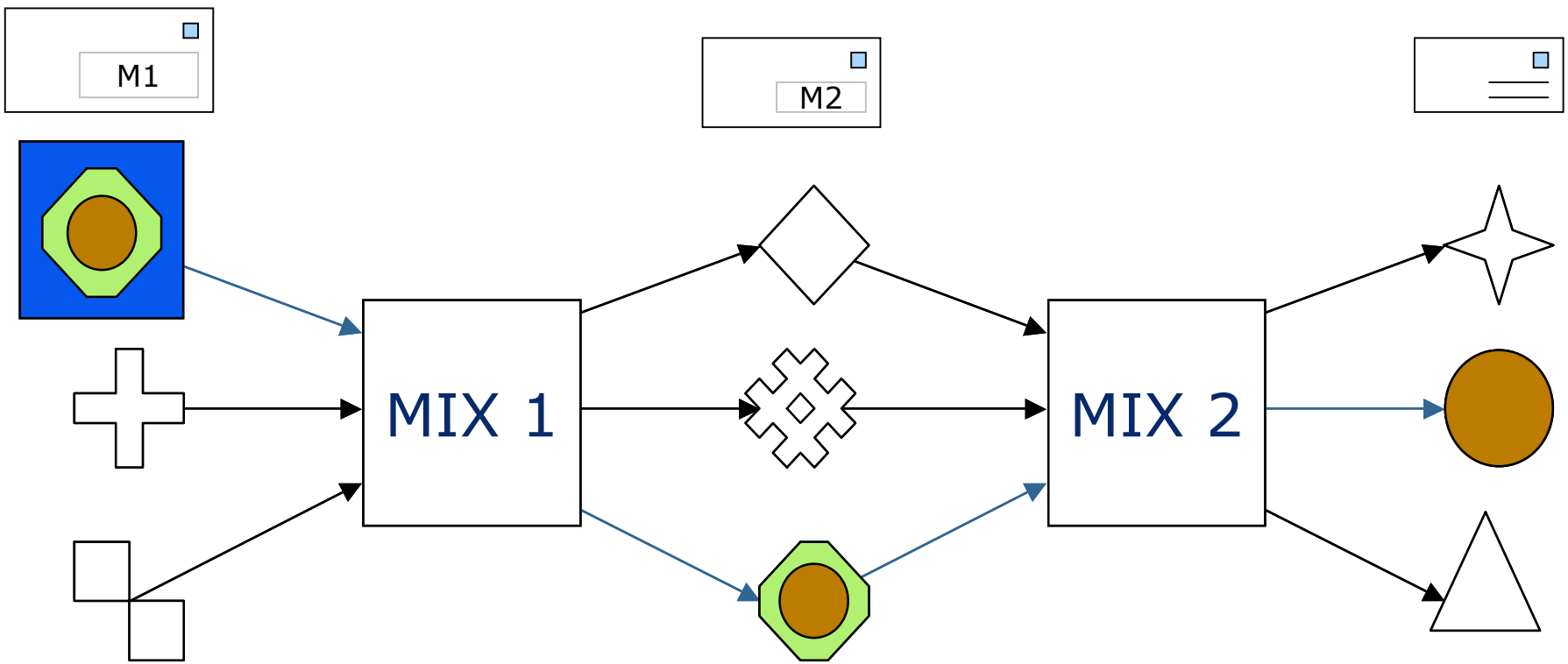
Mix-Netz (Chaum, 1981)

- System zum Schutz von Kommunikationsbeziehungen bei vermittelter Kommunikation

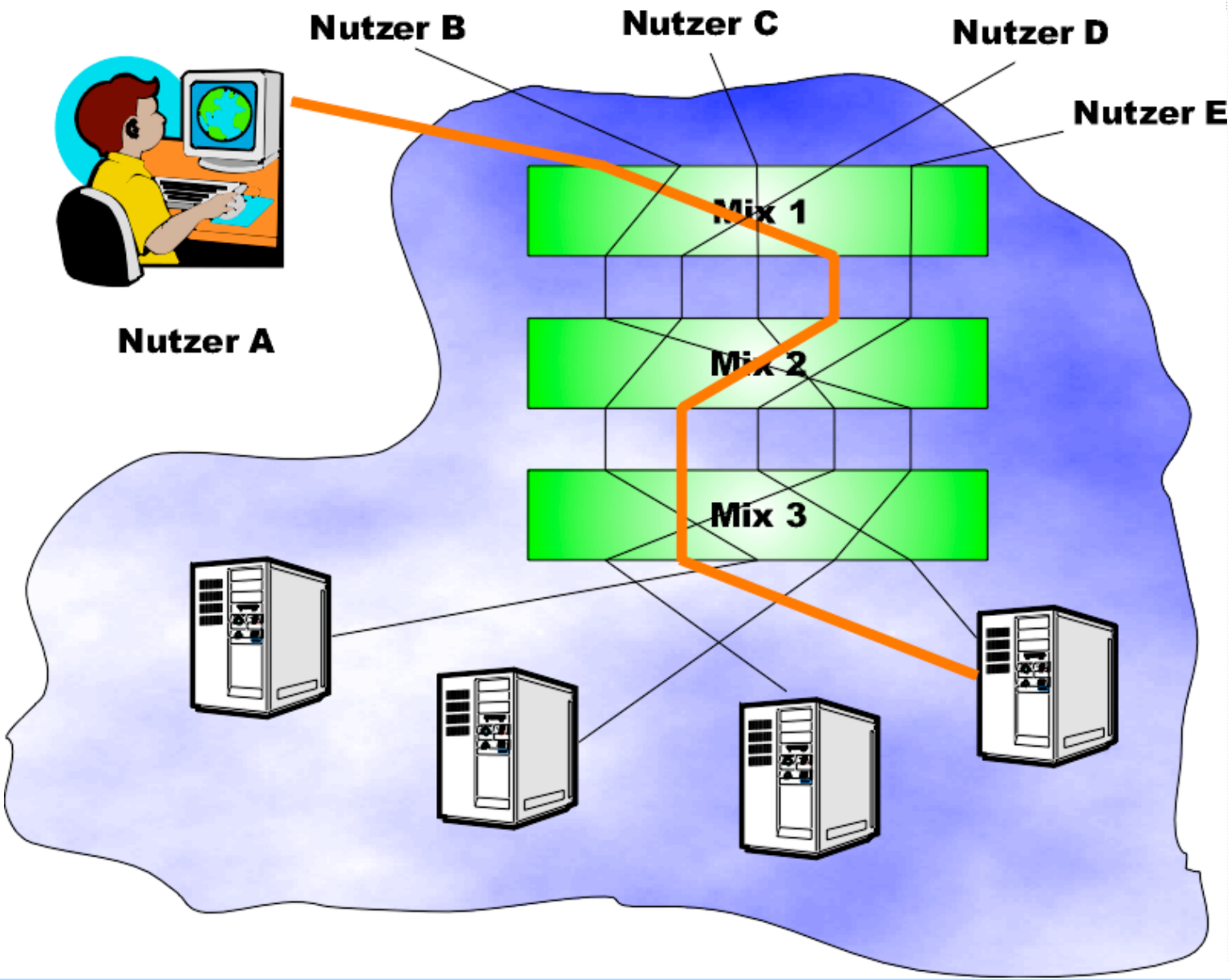


Mix-Netz (Chaum, 1981)

- 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

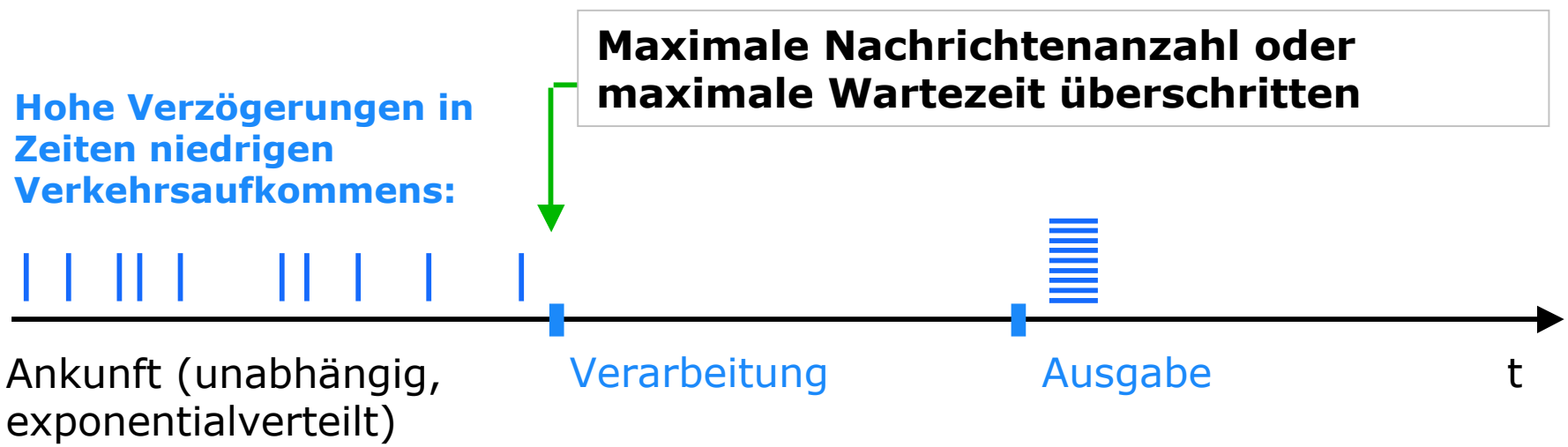


Herausforderungen aus technischer Sicht

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

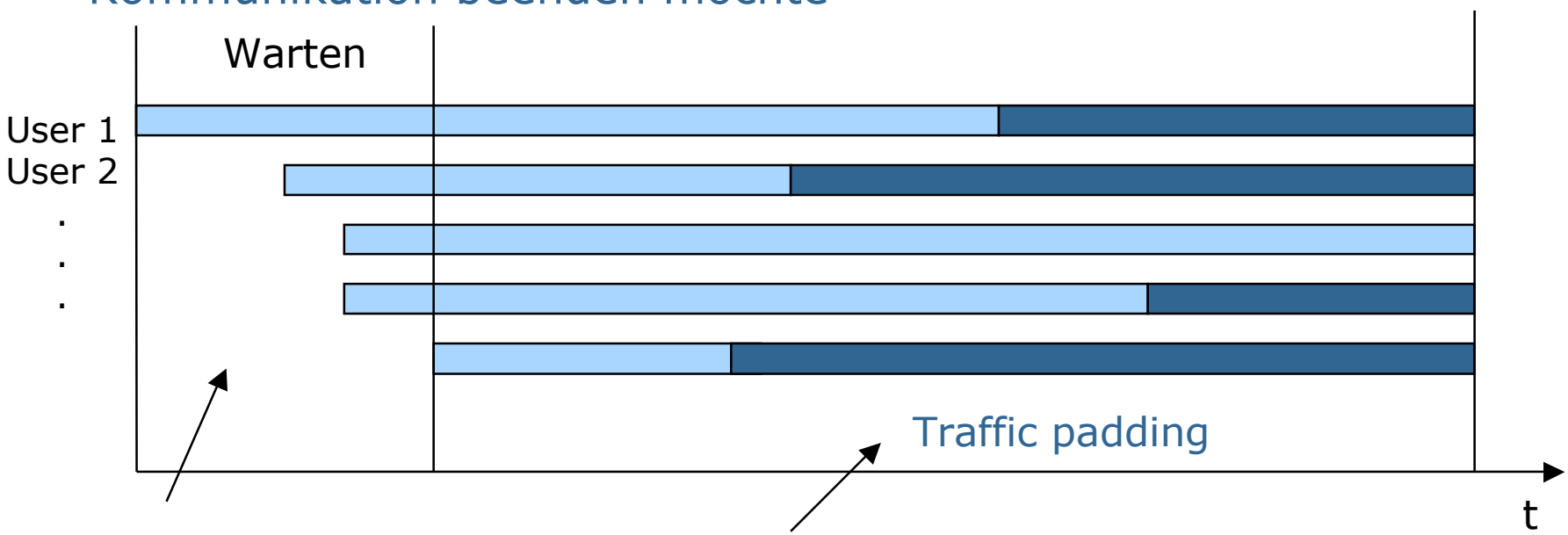
Echtzeitkommunikation und Mixe

- 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



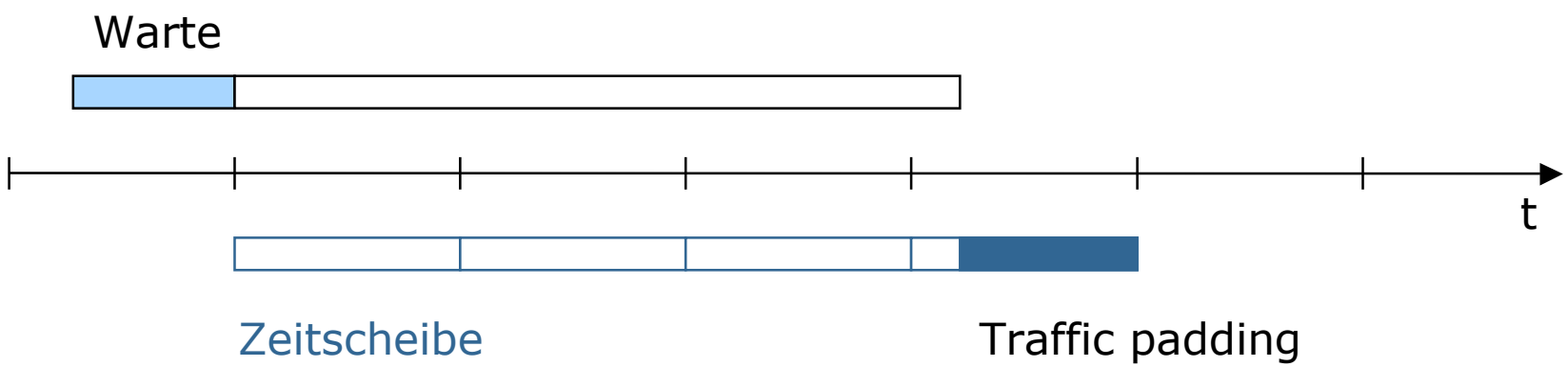
1. Warten, bis genügend Benutzer kommunizieren wollen (Bilden der Anonymitätsgruppe)
   Beispiel: 5 Nutzer

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

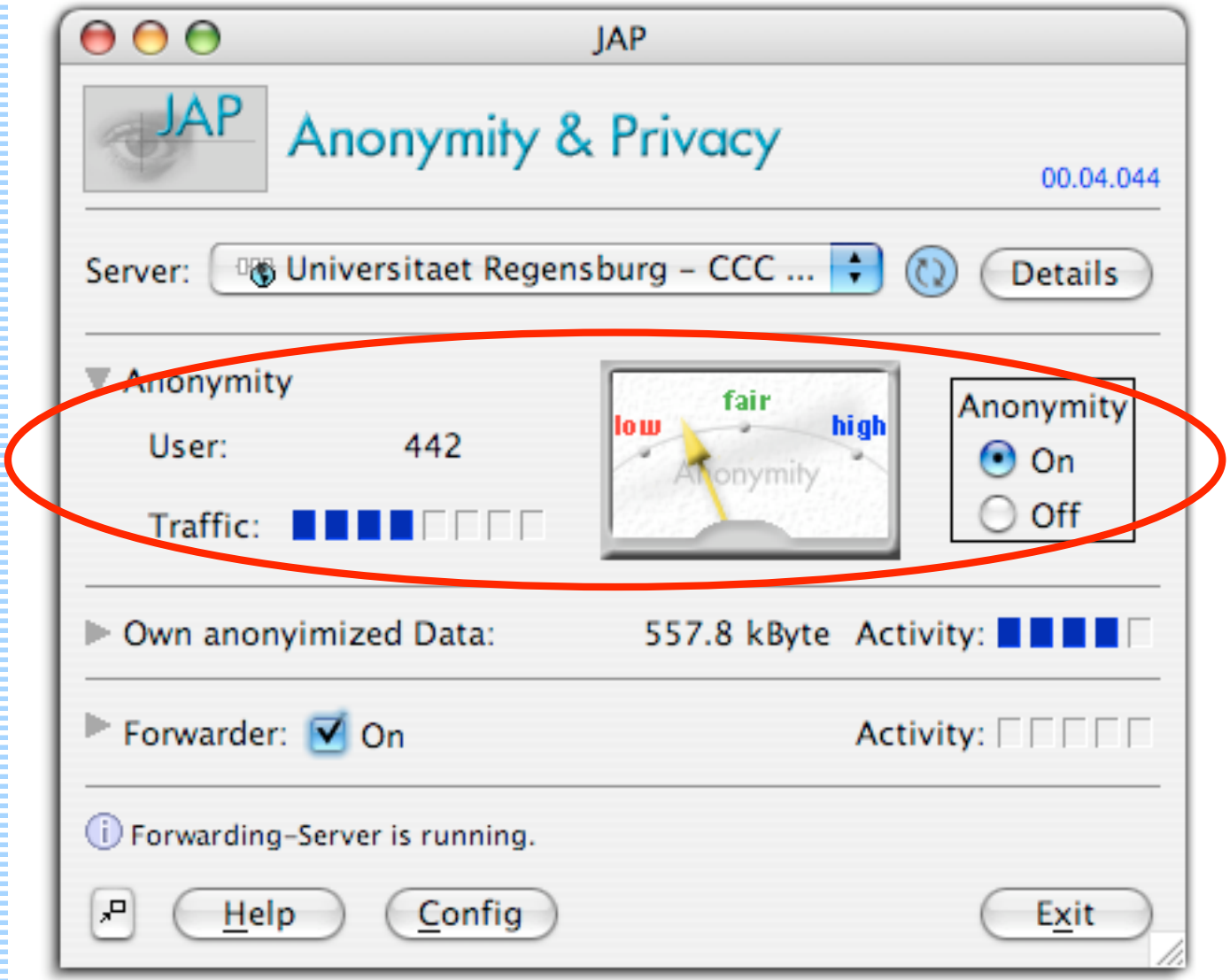


- Volumenscheiben (Federrath et. al. 2000)
  - adaptive Anpassung der Scheibengröße in Abhängigkeit der aktuellen Verkehrssituation
  - Minimieren des Overheads

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

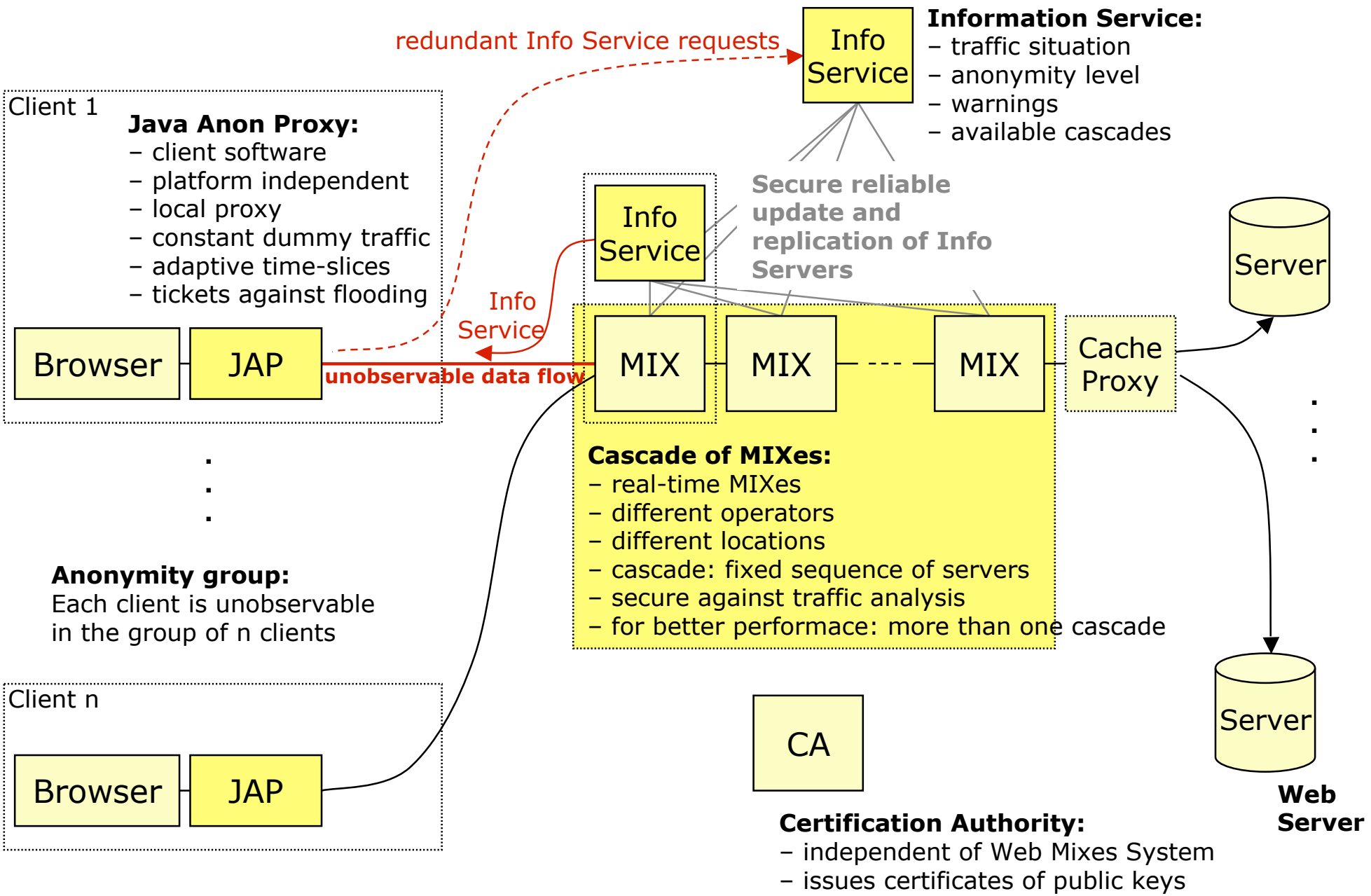


Rückmeldung über Verkehrssituation und Beobach-tungsrisiko (Lang-zeitbeobachtung)

Herausforderungen aus technischer Sicht

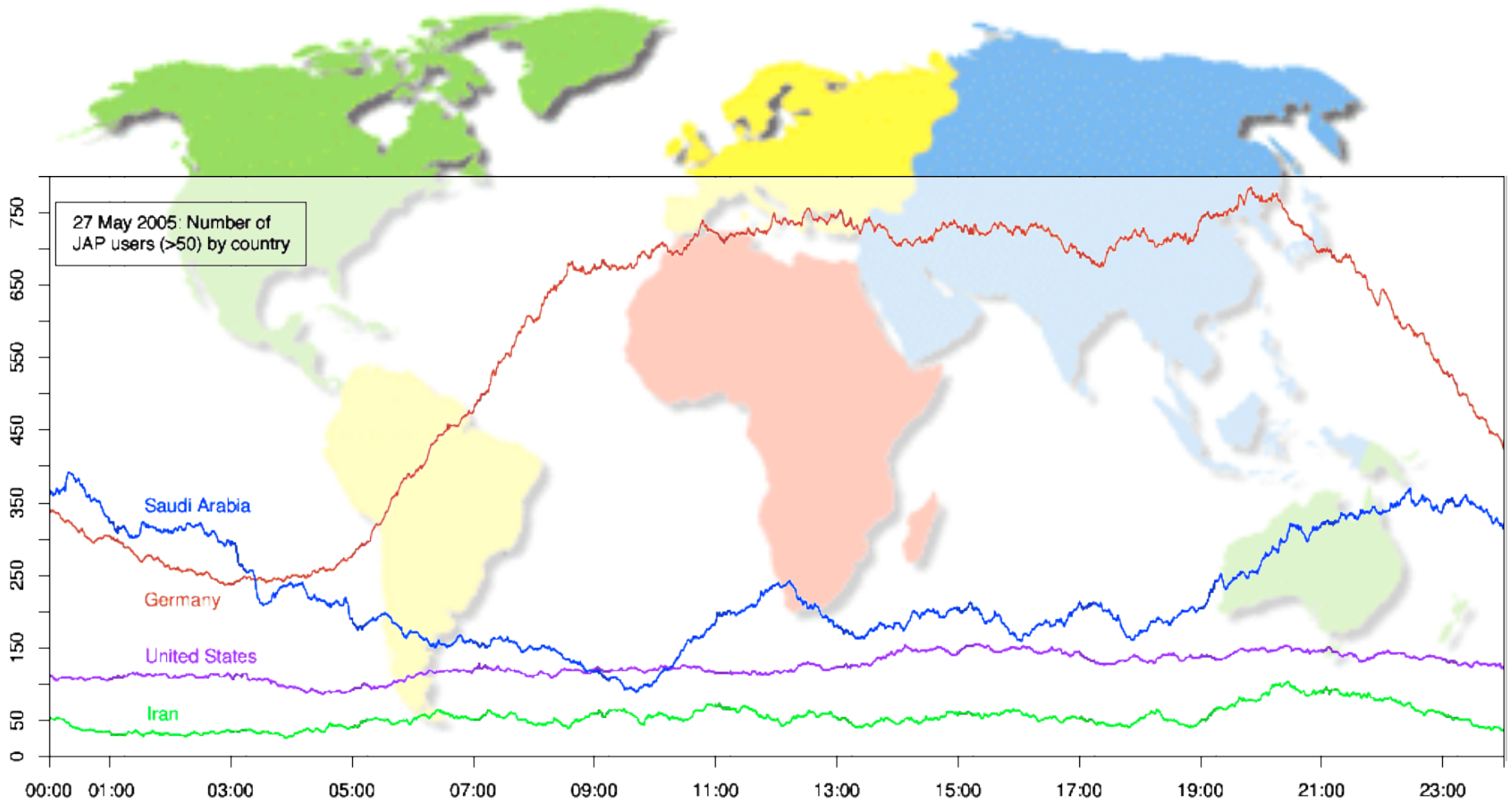
- Adaption der Mixe auf Echtzeitkommunikation
- Transparenz für den Nutzer
- Dezentrale Architektur des Gesamtsystems
- Abrechnung anonym genutzter Dienste
- Stärkung des Nutzers bei gleichzeitiger Strafverfolgungsmöglichkeit

AN.ON: Architektur



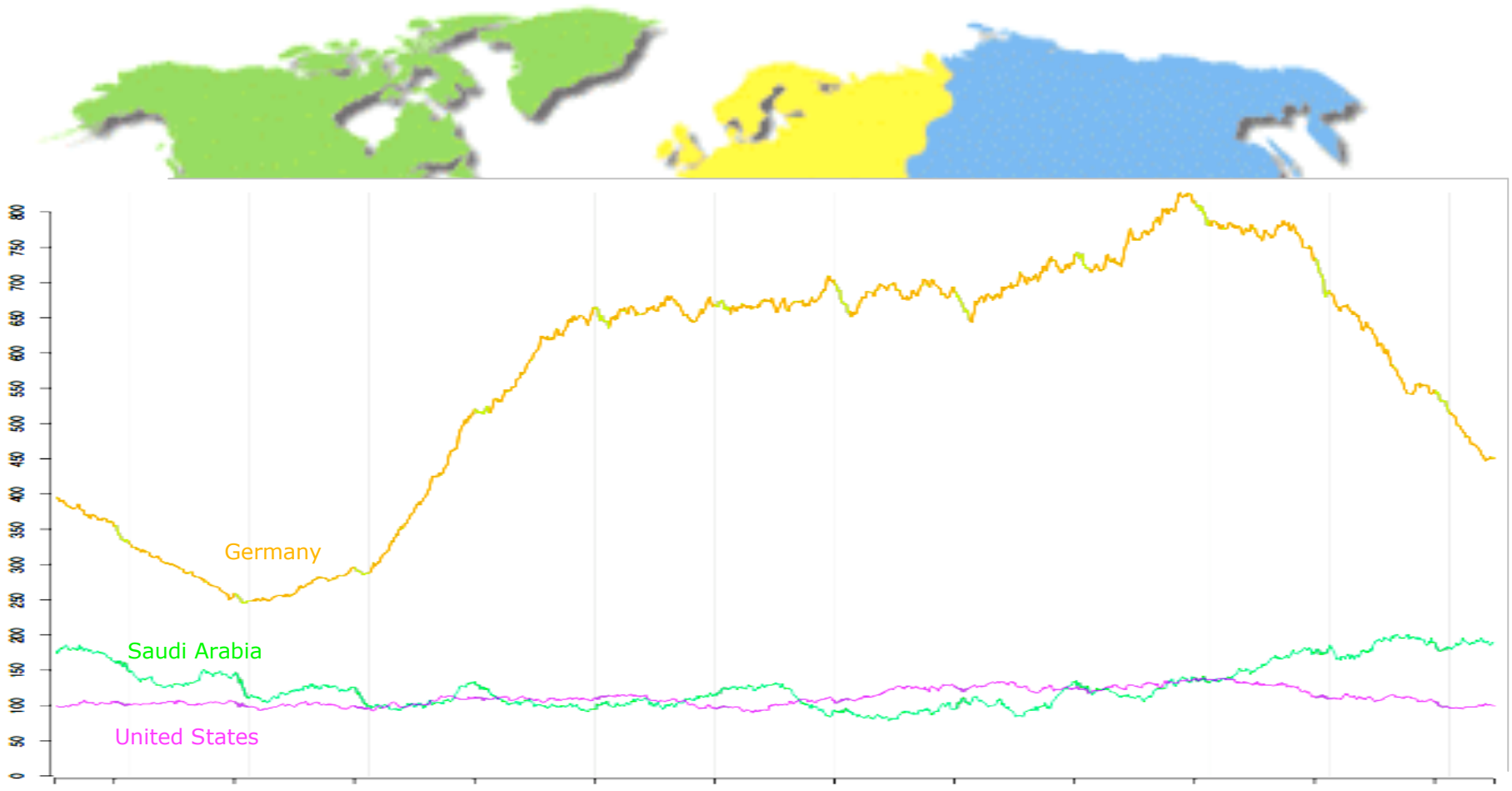
Wo kommen die JAP-Nutzer her?

- Dayline of May 27, 2005



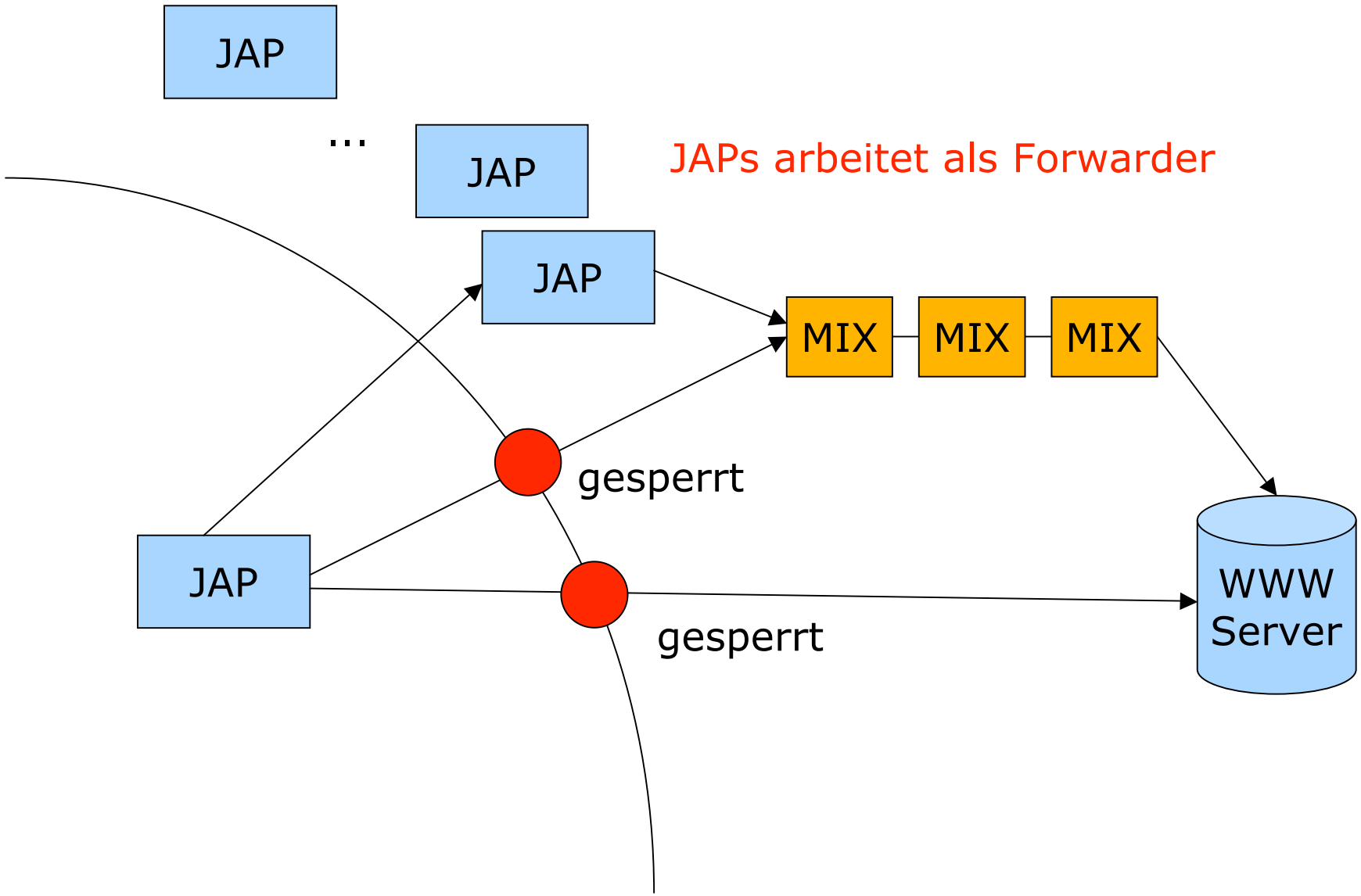
Wo kommen die JAP-Nutzer her?

- Dayline of Aug 1, 2005

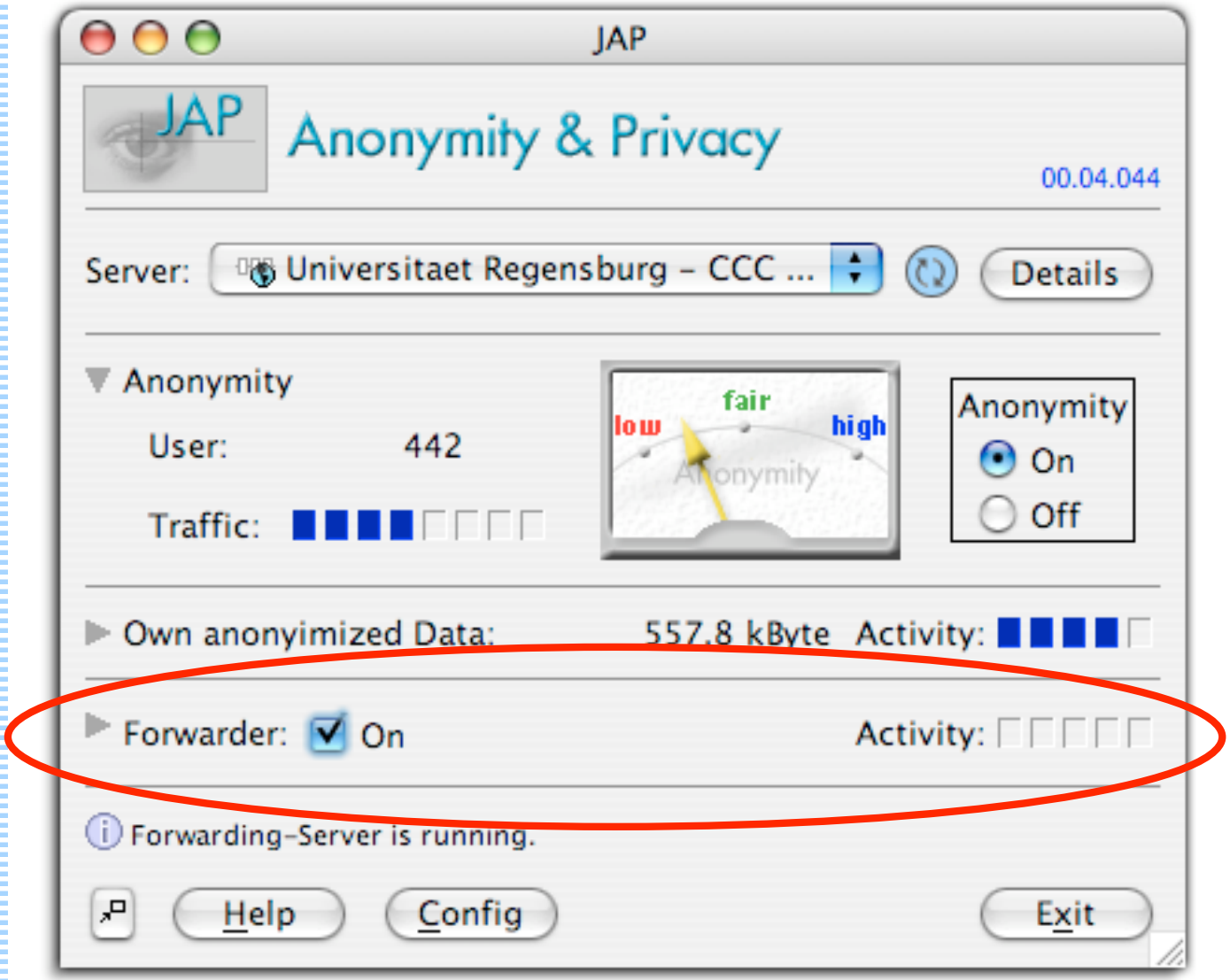


Iran?

Blockingresistenz



Blockingresistenz

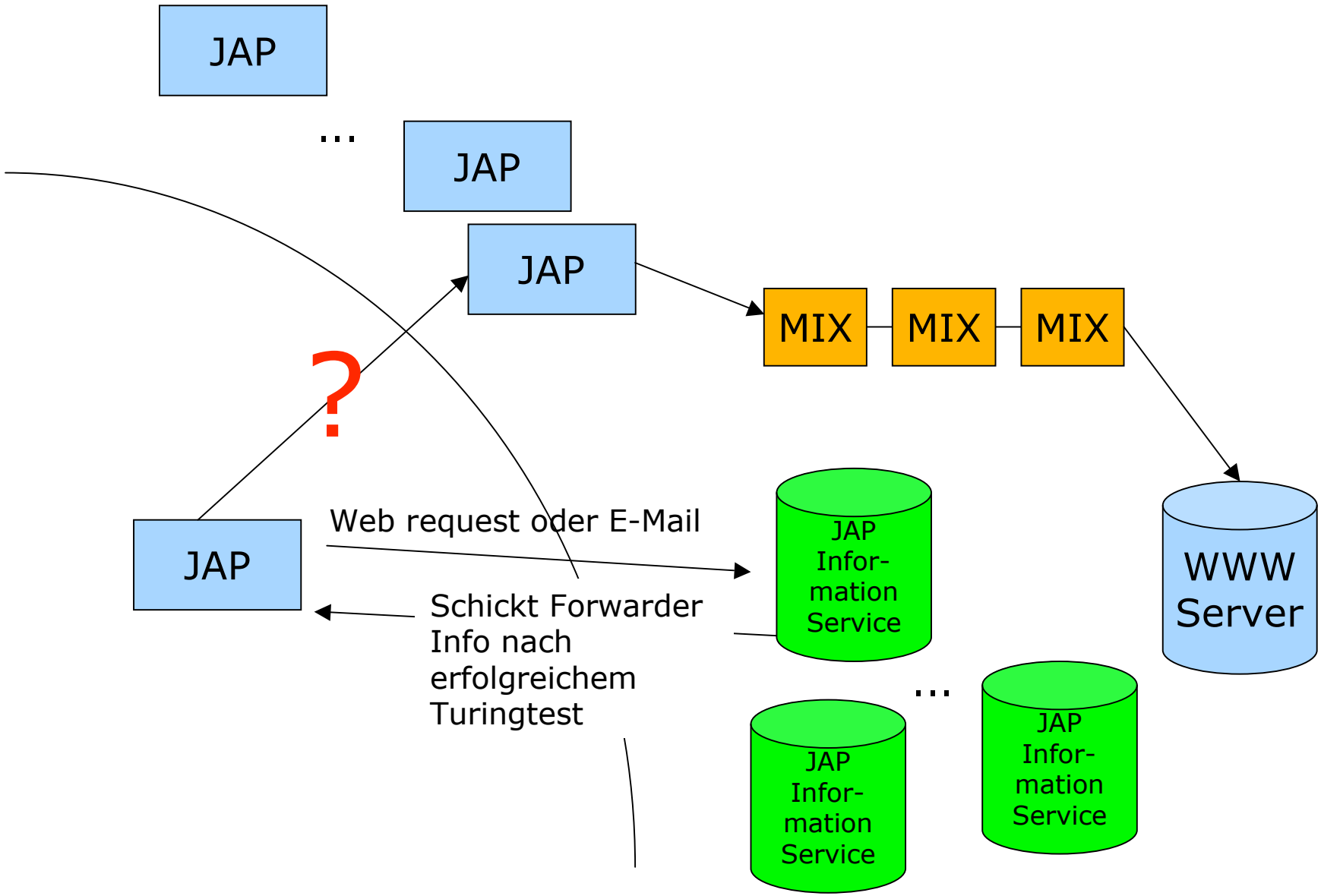


JAP-Nutzer stellen Teil ihrer Bandbreite zur Verfügung

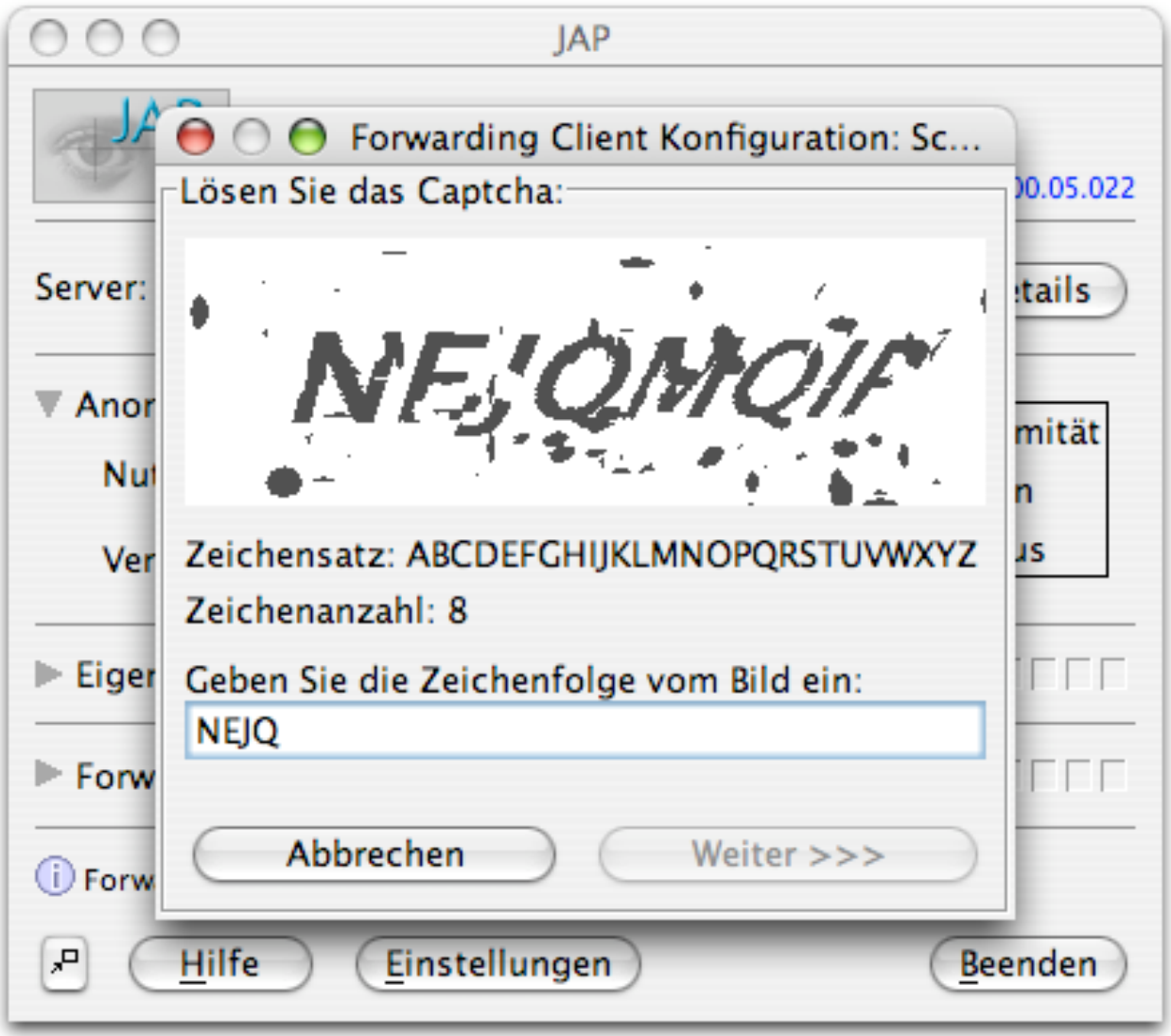
Zugriffe werden durch die Mixe anonymisiert

Forwarder erfahren nichts über die zugegriffenen Inhalte

Blockingresistenz



Blockingresistenz

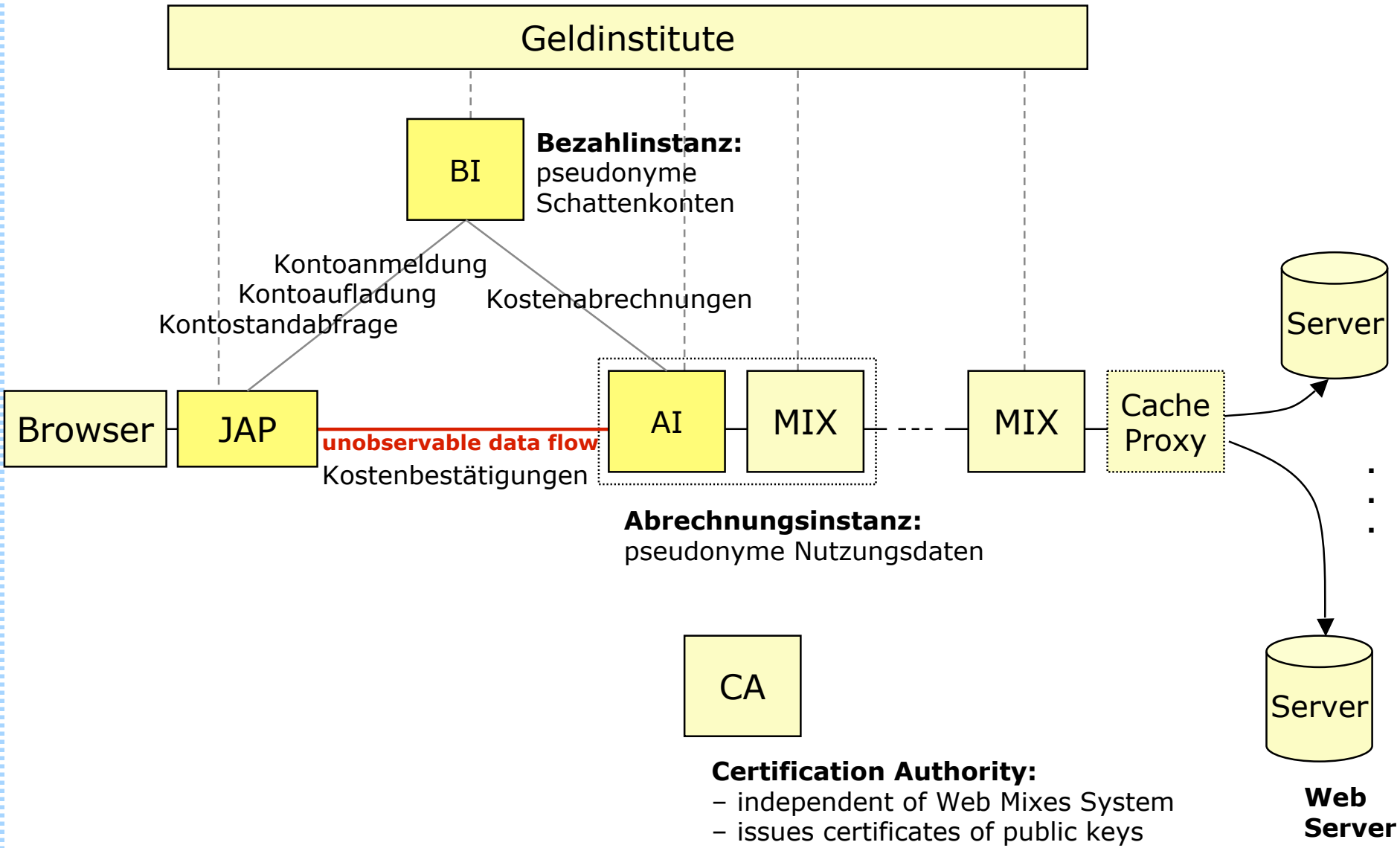


- InfoService schickt Forwarder Info nach erfolgreichem Turingtest

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

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

Letzte

Gültig

Neu | Passwort ändern

Informationen zum Kontostand

Eingezahlt: 100,0

Verbraucht: 0 Byte

Kontostand: 100,0

Aufladen | Aktualisieren

Hilfe | Konfiguration auf Standardwerte zurücksetzen | Abbrechen | OK

JAP

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:

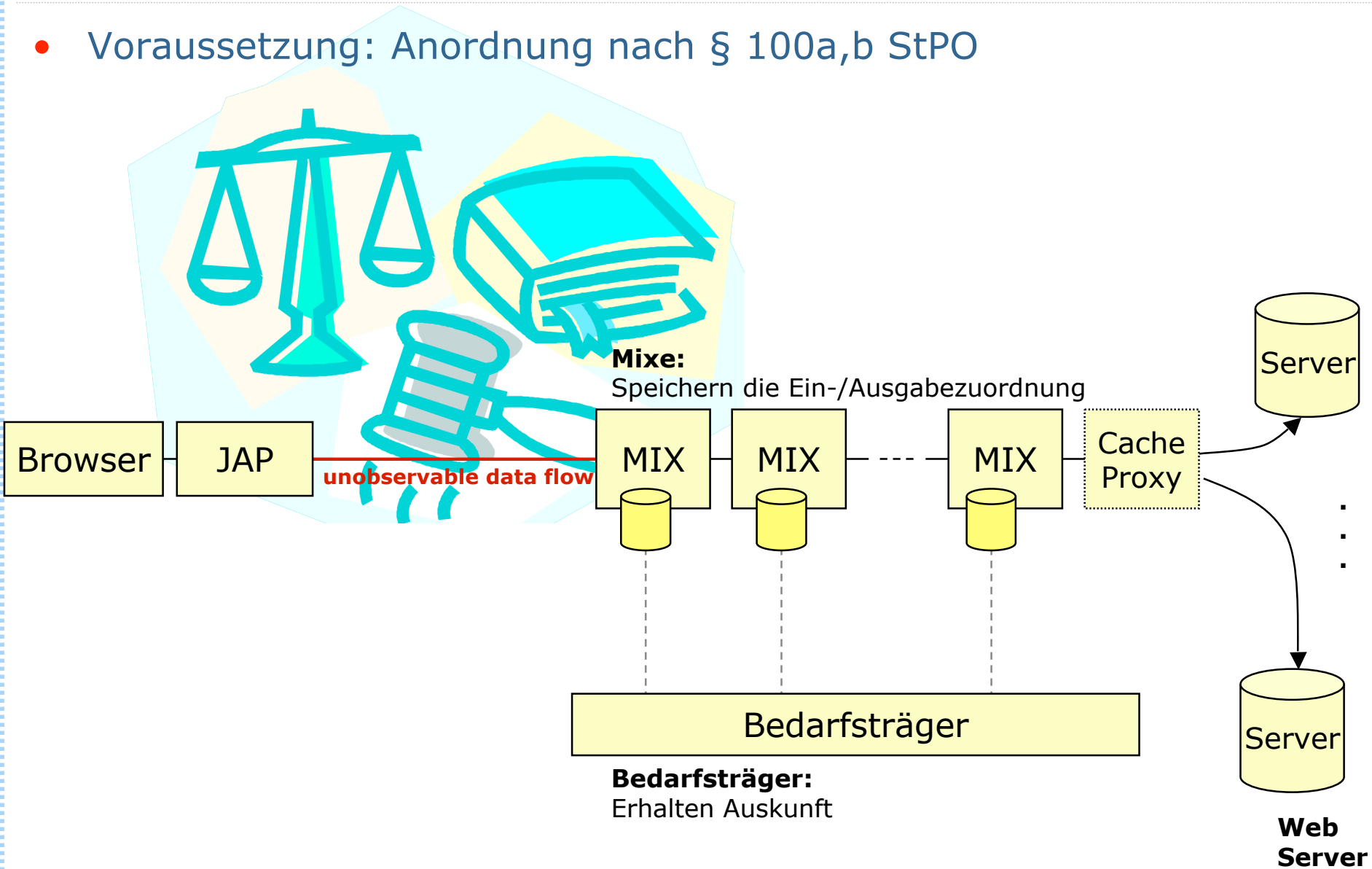
Hilfe | Einstellungen | Beenden

Herausforderungen aus technischer Sicht

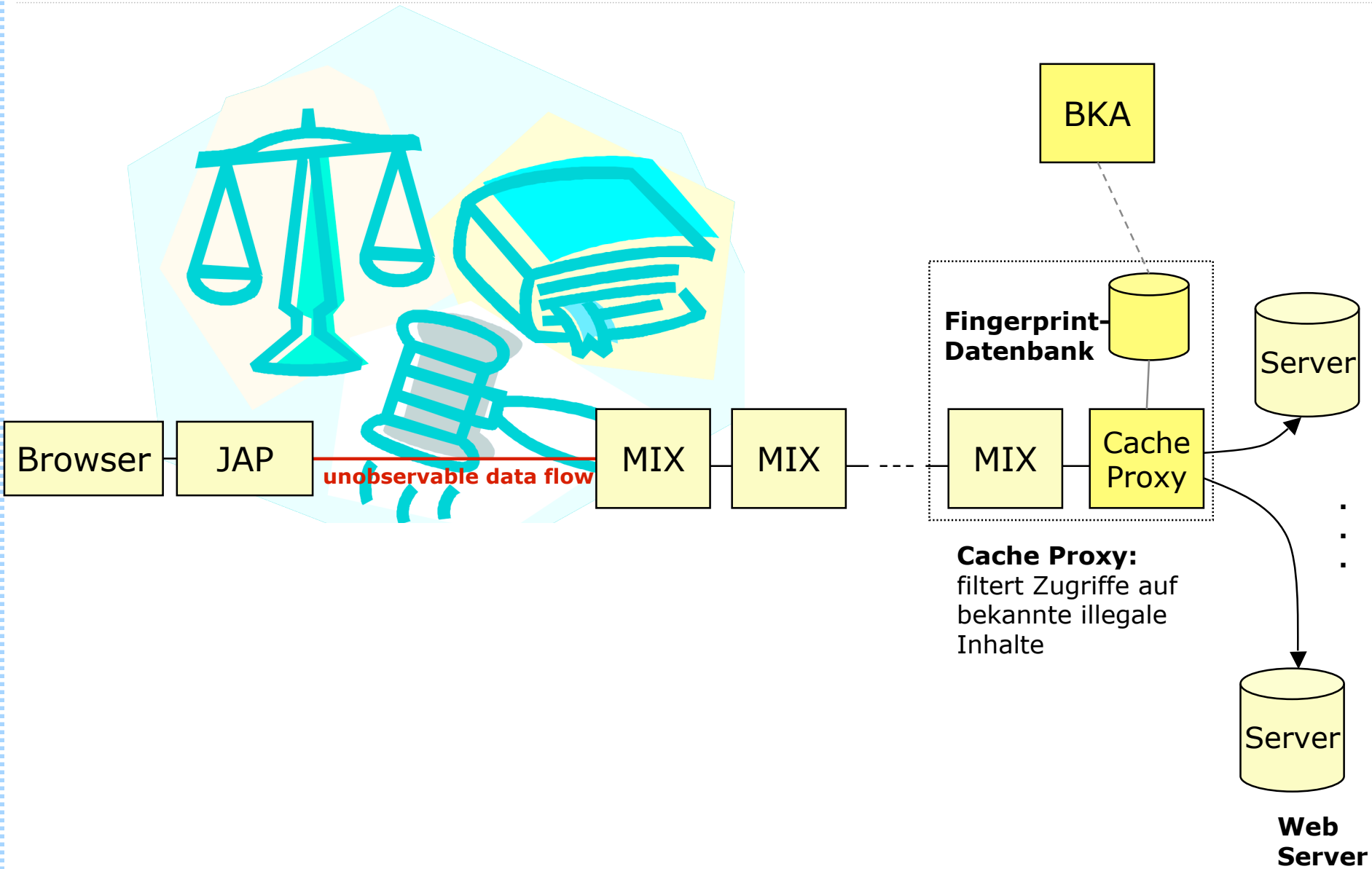
- Adaption der Mixe auf Echtzeitkommunikation
- Transparenz für den Nutzer
- Dezentrale Architektur des Gesamtsystems
- Abrechnung anonym genutzter Dienste
- Stärkung des Nutzers bei gleichzeitiger Strafverfolgungsmöglichkeit

Strafverfolgung bei schweren Straftaten

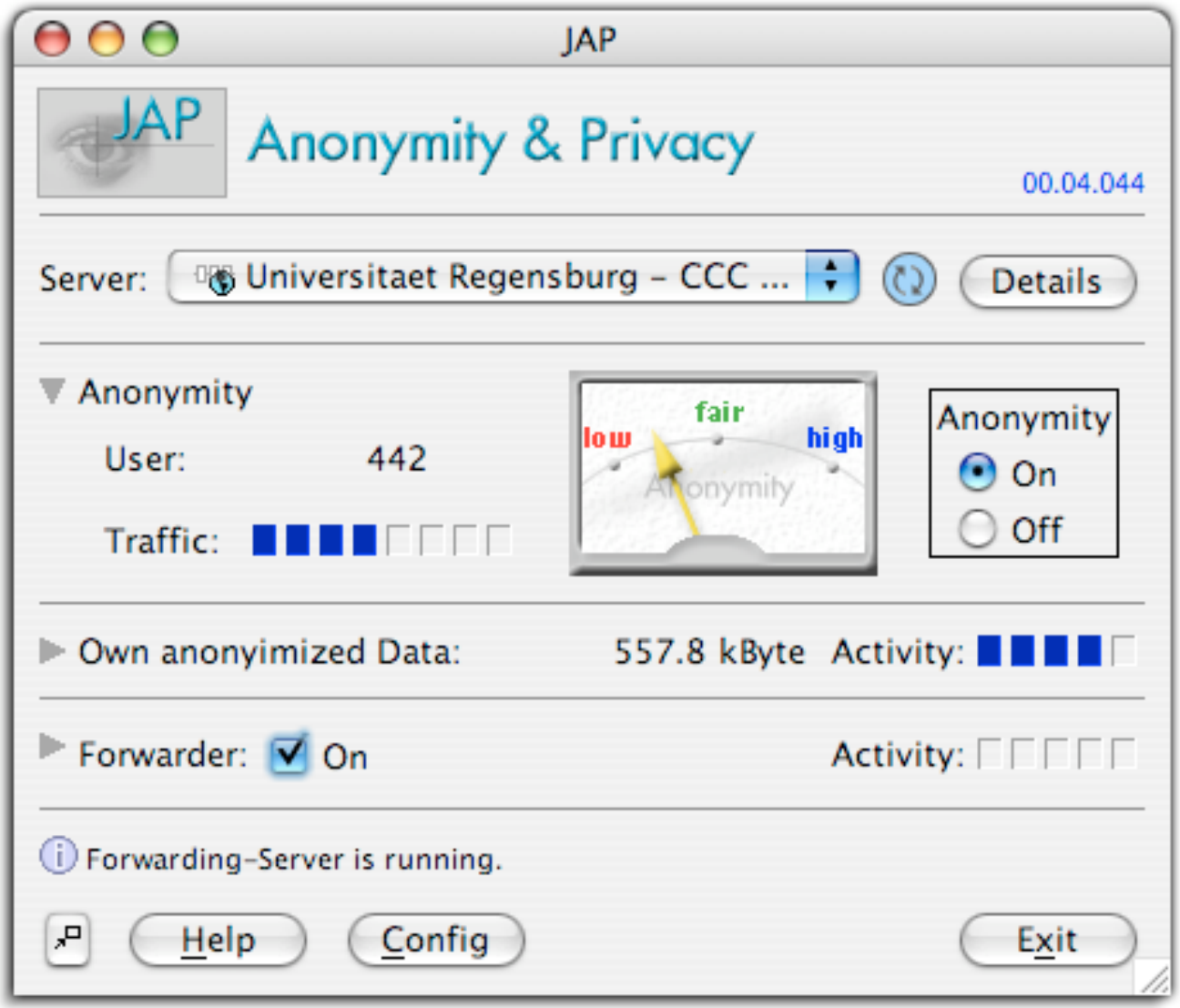
- Voraussetzung: Anordnung nach § 100a,b StPO



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)

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 + "\n
                       "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:                Show
```

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

(Stand: 23.11.2006)

AN.ON/JAP

Bundesministerium
für Wirtschaft
und Technologie

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