JonDonym – Technik und Organisation eines professionellen Anonymisierungsdienstes

JonDos GmbH

- The Privacy Agency –

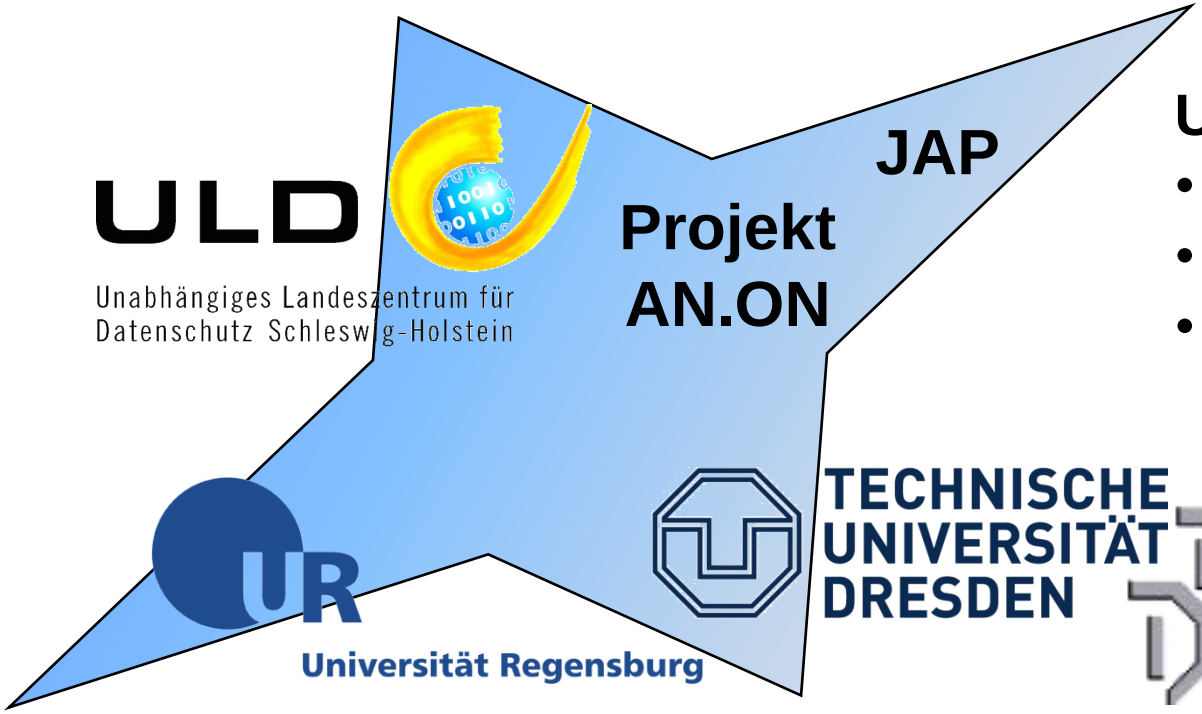
Symposium Datenspuren

Dresden, 07.06.2008

Rolf Wendolsky

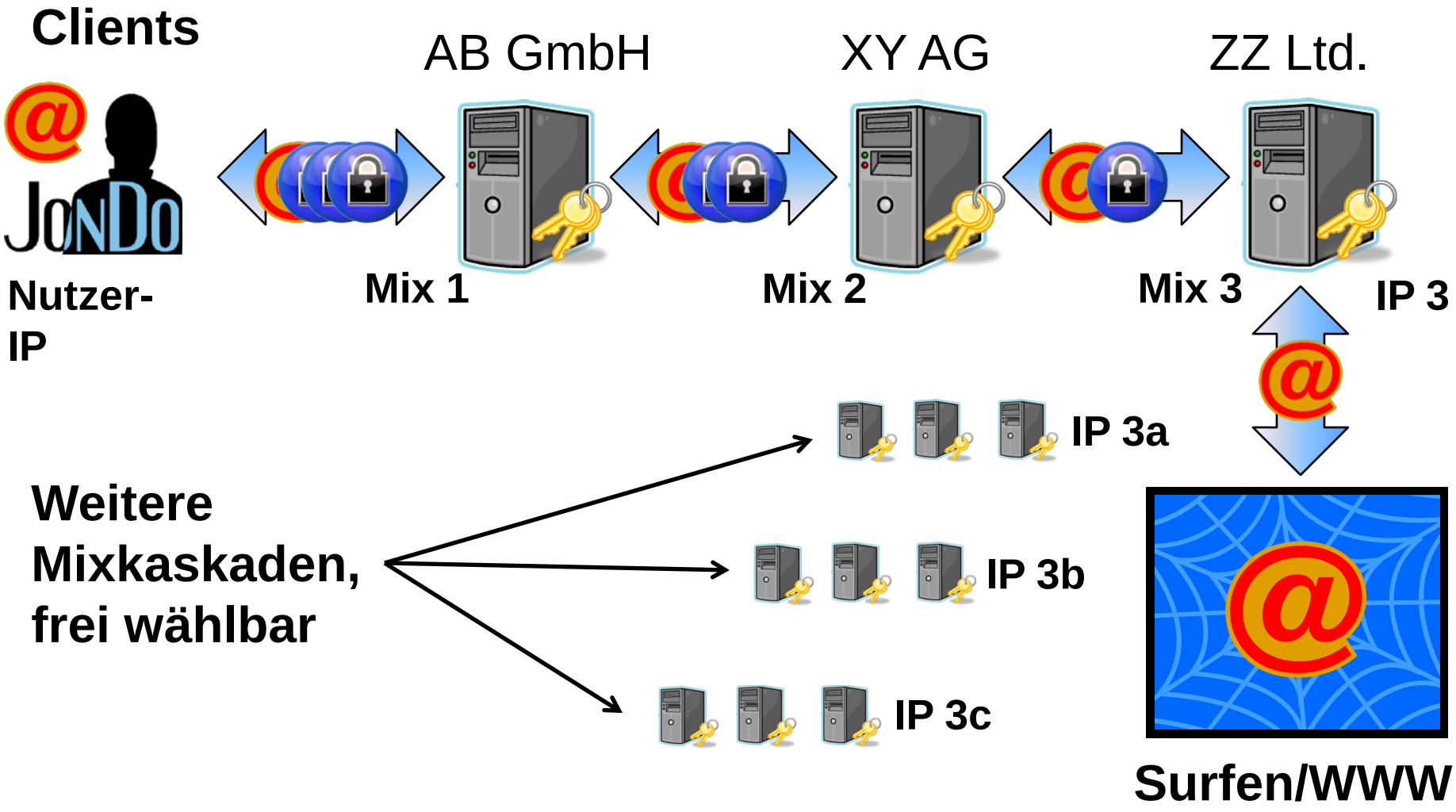
Fortführung universitärer Forschung

Ehemaliges Forschungsprojekt
- AN.ON - Anonymität Online
- offiziell beendet im Jahr 2006

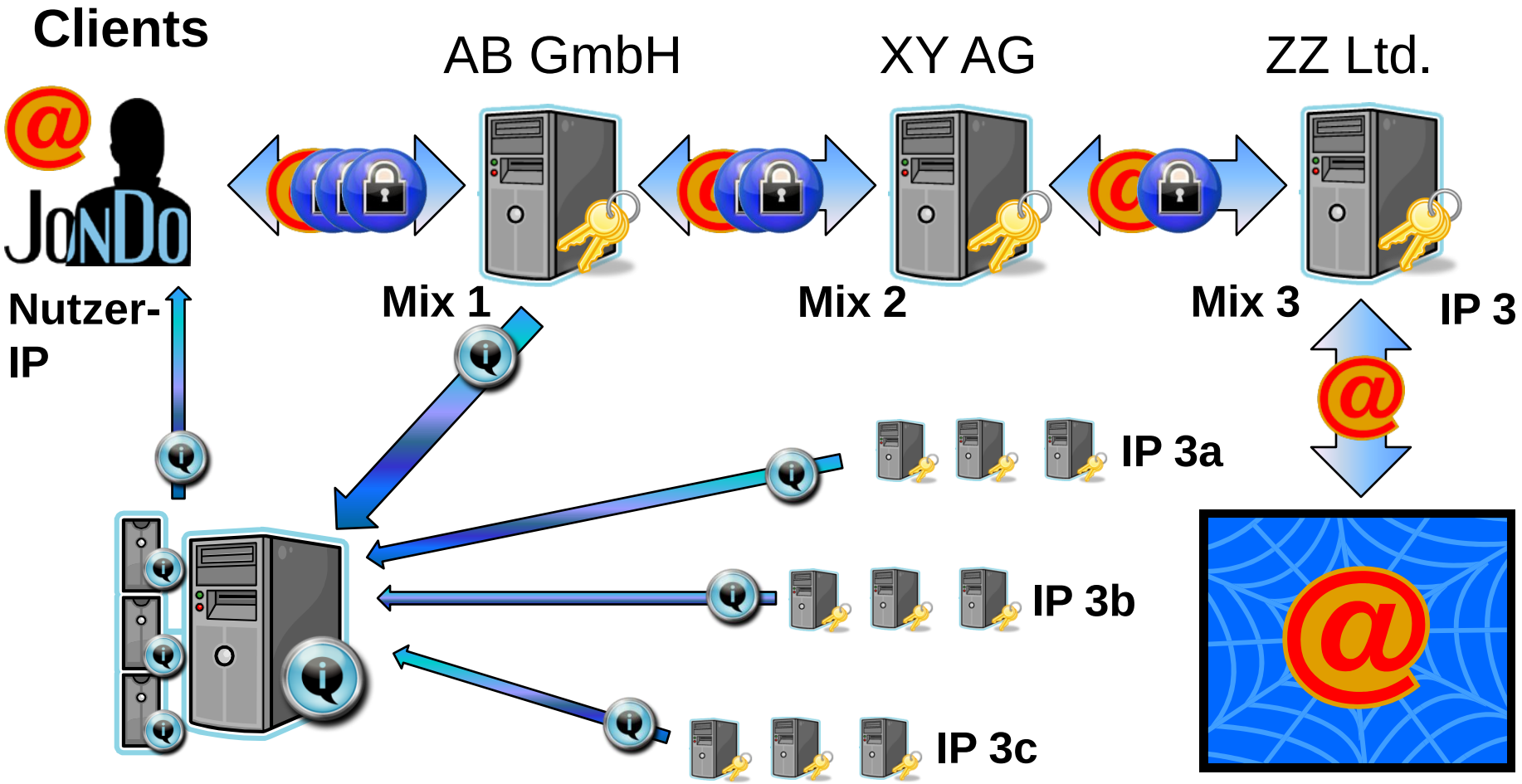


Unternehmensgründung
- JonDos GmbH
- gegründet 03/2007
- Kooperationen mit AN.ON-Projektpartnern

IP-Pseudonymisierung mit JonDonym



IP-Pseudonymisierung mit JonDonym



JonDonym setzt auf Standards

- **Starke Verschlüsselung und Authentisierung** mit DSA 1024, RSA 4096, AES 128, SHA-1, Paket-Padding
  - ➢ Schutz im WLAN, vor Providern und vor WWW-Anbietern

- **Unabhängige Dienstbetreiber und Proxyketten**
  - ➢ Schutz vor Beobachtung durch die Dienstbetreiber selbst

OSI certified

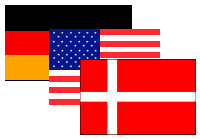
- **Quelloffene** Client- und Serverprogramme
  - ➢ Schadcode kann vom Anbieter kaum versteckt werden

Diese Standards müsste jeder Anonymisierungsdienst erfüllen!

Positiv: JonDonym,Tor,I2P **Durchgefallen: VPN-Dienste,Proxies,...**

Besondere JonDonym-Features

- **Verteilte Betreiber und dedizierte Server** mit unterschiedlichen OS, Redundanz als Schutz vor Angriffen



- **Internationale Betreiber und Server** bei Premium-diensten, bietet Schutz vor behördlicher Willkür

- **Identifikation der Betreiber** als Person oder Unternehmen inklusive Betreiberhaftung bei Datenmissbrauch

- **JonDoFox**, für beste Anonymität angepasstes Firefox-Profil (wird ständig weiterentwickelt)

- **konstant hohe Geschwindigkeit** bei Premiumdiensten

➢ meist deutlich über den garantierten 64 kbit/s

Systeme im Feature-Vergleich

	JonDonym	Tor	VPNs	HTTP-Proxies	WWW-Proxies
Verschlüsselung	++	++	++	-	-- (1)
Unabhängige Betreiber	+	++	-- (2)	-- (2)	-- (2)
Verifizierte Betreiber	+	- (3)	++	-- (3)	- (3)
Verteiltes System	+	++	-	-	--
Geschwindigkeit	+ / -- (4)	--	++	-	-
HTTP-Anonymität	++	++	- (5)	--	--

(1) https-Verschlüsselung wird gebrochen oder gar nicht unterstützt

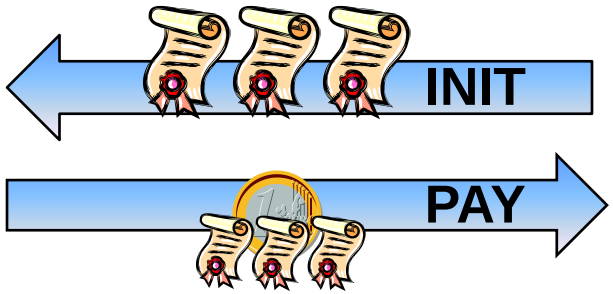
(2) nur ein einziger Betreiber, der jeweils gehackt werden oder selbst alles beobachten kann

(3) Betreiber-Identität beliebig oder in Grenzen wählbar und fälschbar

(4) Premiumdienste sind schnell, kostenlose Dienste sind oft langsam

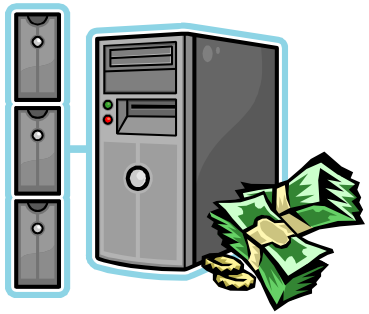
(5) Webseiten können selbst im verschlüsselten Datenstrom mit hoher W‘keit erraten werden

Bezahlprotokoll für Premiumdienste



Kostenbestätigung (CC)
- Nutzer bestätigt 3 MByte im Voraus
- enthält Hashwerte der Preiszertifikate, kumulierte MByte für die Kaskade und Signatur des Nutzers

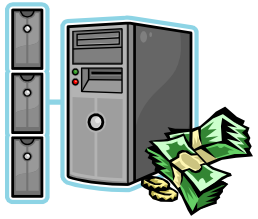
Preiszertifikat (PC)
- bestätigt jedem Mix einen Preis/Mbyte gegenüber der Bezahlinstanz
- enthält Hash des Mixzertifikats und Signatur der Bezahlinstanz



Bezahlinstanz
- prüft CCs und zieht Nutzern Bytes ab
- schreibt Betreibern dafür Geld gut

Tarife für Premiumdienste kaufen

Konto erzeugen und aktivieren



Bezahlinstanz

Erzeugt Kontoschlüssel

Kontoanfrage mit Public Key

Erzeugt zufällige Kontonummer, signiert Konto-struktur

JonDo erhält Kontozertifikat

Wählt Tarif

Sende Tarifwahl, TAN anfordern

Erzeugt zufällige TAN

Wählt Bezahl-methode

Übermittle TAN an JonDo

Sende Geld und TAN

Aktiviert Konto mit bezahltem Tarif

Technischer Datenschutz beim Bezahlen

- IP-Adressen und personenbezogene Daten werden nicht gespeichert

TAN

- Zufällige Transaktionsnummer verhindert, dass Dritte (Banken) Kontonummer und Person verketten können

- je Konto und Kaskade wird zur Abrechnung nur die jeweils letzte Kostenbestätigung (CC) gespeichert

- Konto ist nur kurzzeitig nutzbar, um langfristige Beobachtung desselben Nutzerkontos zu verhindern

Bezahlmethoden für JonDonym

- **PayPal:** keine Skripte, aber Cookies und E-Mail-Adresse erforderlich; wird von den meisten Nutzern verwendet

- **Überweisung** auch unter Pseudonym: Barüberweisung kostet bei der Sparda-Bank 4,- Euro ☺

- **Barzahlung per Brief:** ohne Absenderadresse, nur TAN und Geld. Potentielle Spuren: Schrift, Druck, DNS

- **paysafecard**: **Neu** ab Mitte/Ende Juni 2008. Prepaid-Karte, zu kaufen an Tankstellen, in Supermärkten etc. *JonDonym ist der einzige für paysafecard zugelassene Anonymisierungsdienst!*

Schwierigkeiten beim Bezahlprotokoll

JonDo empfängt Daten schneller als er die CC senden kann

- Verbindung muss nach Timeout vom Mix getrennt werden
- kleines Betrugspotential bleibt bestehen; nicht zu ändern

Aktuelle Mixe setzen beim Verbinden ein Timeout bis zur ersten CC

- Man kann einige Sekunden kostenlos surfen
- Neue Mix-Version fordert CC, bevor erstes Byte gesendet wird

Erste Mixe erkennen Nutzer am Kontozertifikat wieder

- Nicht zu ändern. Anonymität wird dadurch aber kaum berührt

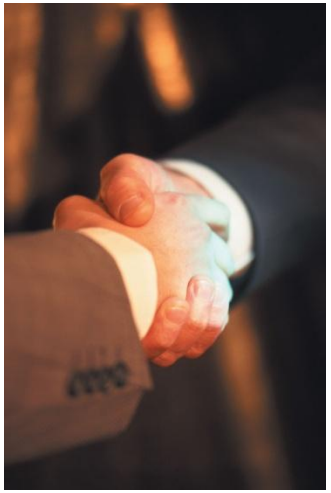
Fällt die Bezahlinstanz aus, können keine CCs verifiziert werden

- Vom Mix herunterladbare Whitelists-Caches für Konten (geplant)
- Verteilung der Bezahlinstanz auf mehrere Cluster (geplant)

Verträge sichern Unabhängigkeit

Betriebsvereinbarung
- Strengster Datenschutz für den Mixbetrieb
- Haftungssauschluss für JonDos
- Identifizierungspflicht für Betreiber
- Verbot der Einflussnahme durch JonDos

Erweiterter Kündigungsschutz
Zustimmung von >50% der Betreiber nötig, damit JonDos kündigen kann (außer bei Vorsatz)



AGB von JonDos
- Abrechnungsvertrag mit Nutzern
- Abgrenzung: Nicht JonDos erbringt die Anonymisierungs-Dienstleistung, sondern die Betreiber

Betreibervertrag
- Regeln für die korrekte Abrechnung
- Kennzeichnung von JonDos als Abrechnungsdienstleister

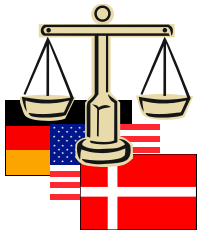
Demnächst: Betreiber-AGB
- Dienstleistungsvertrag zwischen Nutzern und Betreibern
- Abgrenzung zu JonDos

Strafverfolgung als Kompromiss

- Mixbetreiber dürfen keine Verbindungsdaten speichern
- Auskunftsersuchen/Beschlagnahmung nach § 100g/h StPO bringen nichts, Beschlagnahmung wäre rechtswidrig

- Überwachungsanordnungen nach § 100a/b StPO möglich für rein deutsche Mixkaskaden (deutsche Betreiber/Mixe)

➢ 2007 gab es keine solche Anordnung, 2008 bisher auch nicht

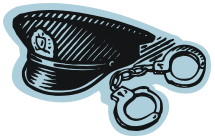


- Bei Premiumdiensten sind Überwachungsbeschlüsse meist gleichzeitig für mehrere Nationen notwendig
- Zusätzlich hilft räumliche Verteilung der Server gegen Ausspähen der Verbindungsdaten direkt beim Hoster

➢ Vernünftiger Kompromiss zwischen Datenschutz und notwendiger Strafverfolgung

Vorratsdatenspeicherung contra Zeit (1)

23:35:28



Welcher Nutzer hatte IP 3 zur Zeit 23:35:30 ?

23:35:29

Nutzer-IP

23:35:29

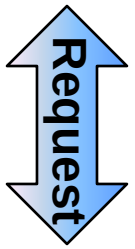
23:35:26

23:35:27

23:35:28

§ 113a TKG

23:35:30



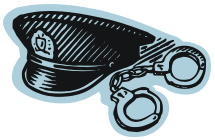
Surfen/WWW

- Ziel-URL/IP darf nicht gespeichert werden
- Uhren sind nicht perfekt synchron

➢In vielen Fällen ist die Antwort nicht eindeutig!

➢ Prinzip-bedingt geraten immer Unschuldige in Verdacht – Auskunft an Behörde legal?

Vorratsdatenspeicherung contra Zeit (2)



Welcher Nutzer hatte IP 3 zur Zeit 23:35:30 ?

- Muss IP jedes Requests gespeichert werden? Eigentlich nicht!
- **Bundesnetzagentur** gibt bisher keine Vorgabe zur Durchführung der Speicherung!
- **Laut § 113a TKG:** nur die IP-Adresse einer Verbindung, An- und Abmeldezeitpunkt sind zu speichern

➢ Mix 3 speichert IP-Adresse von Mix 2

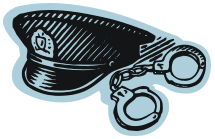
➢ Mix 2 speichert IP-Adresse von Mix 1

➢ Mix 1 speichert Nutzer-IP plus An- und Abmeldezeitpunkt

➢ Mehr dürfen auch Zugangsprovider nicht speichern!

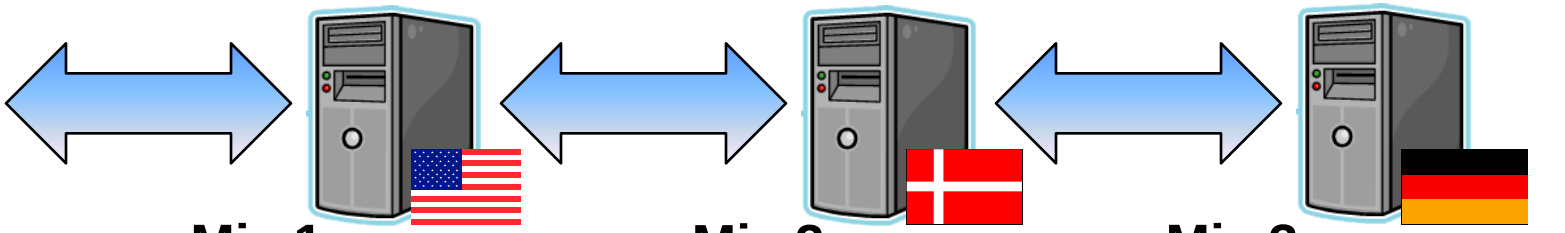
Auskunft enthält **alle Nutzer des Dienstes als Antwort**. Dies ist die **optimale Anonymität**, die Mixe theoretisch bieten können!

VDS contra Internationalisierung



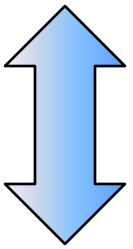
Welcher Nutzer hatte IP 3 zur Zeit 23:35:30 ?

Nutzer-IP



Mix 1 **Mix 2** **Mix 3** **IP 3**

23:35:30



Surfen/WWW

Einzige mögliche Auskunft: IP-Adresse von Mix 2

Informationsgehalt = 0!

Aber: Rechtskonforme Auskunft!

Aktuelle Entwicklungsvorhaben

JonDoFox soll durch eigene Extension(s) verbessert werden

- JavaScript-Filterung und konsequente Same-Origin-Policies für JS/Cookies/Cache/History

Mehrfach-Zertifizierung für verteiltes Vertrauen (02/2009)

- Mehr als eine root-Zertifizierungsstelle für Betreiber
- ➢ Möglicherweise in Zukunft auch NGOs als Zertifizierungsstellen

JonDo-Stick zur einfachen Anwendung auf Reisen (09/2008)

- fertig konfigurierter USB-Stick für den Einzelhandel

Unterstützung aller HTTP-Proxy-fähigen Anwendungen

- Noch im Juli 2008 für die Premiumdienste; evtl. auch SOCKS

www.jondos.de/de/development - laufend neue Themen!

JonDonym – mitmachen!

Teilnahme am System als Mixbetreiber

- Kostenloser Betrieb für die Allgemeinheit
- Vergüteter Betrieb zur Server-Refinanzierung
- Werbung: Deutliche Präsentation von Institution oder Unternehmen gegenüber den Nutzern

Workshop für Anfänger und Fortgeschrittene

- Datenspuren, Sonntag, 11 Uhr, Workshop-Area
- Einführung zur Software JonDo
- Installation und Betrieb (Notebook) mitbringen)
- Gutscheine