



Das Internet vergisst nicht

30. Mai 2011

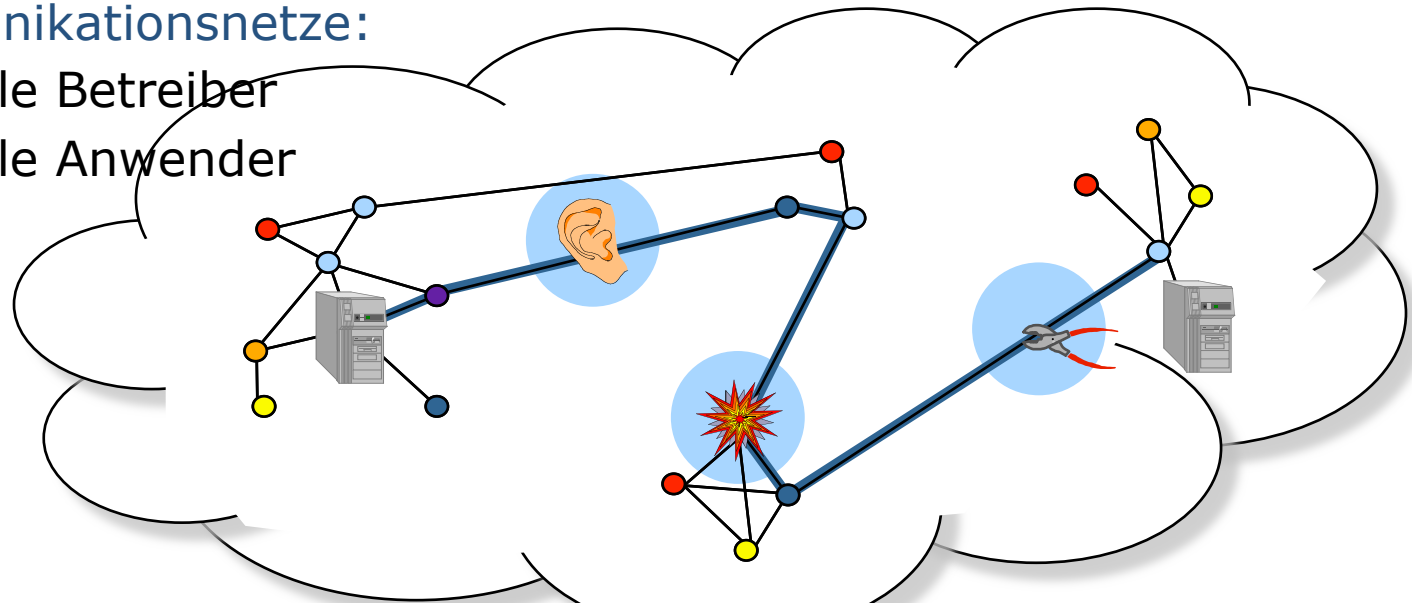
Prof. Dr. Hannes Federrath

<http://svs.informatik.uni-hamburg.de/>

Sicherheit in Rechnernetzen

- **Telekommunikationsnetze:**

- sehr viele Betreiber
- sehr viele Anwender



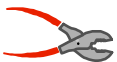
Bedrohungen



unbefugter Informationsgewinn



unbefugte Modifikation



unbefugte Beeinträchtigung der Funktionalität

Schutz der

Vertraulichkeit

Integrität

Verfügbarkeit

Schutzziele mehrseitiger IT-Sicherheit

- Mehrseitige Sicherheit bedeutet die Einbeziehung der Schutzinteressen aller Beteiligten sowie das Austragen daraus resultierender Schutzkonflikte beim Entstehen einer Kommunikationsverbindung.

Kommunikationsgegenstand
 WAS? WORÜBER?

Kommunikationsumstände
 WANN?, WO?, WER?

Vertraulichkeit
 Verdecktheit

Anonymität
 Unbeobachtbarkeit

Integrität

Zurechenbarkeit
 Rechtsverbindlichkeit

Verfügbarkeit

Erreichbarkeit

Schutzziele mehrseitiger IT-Sicherheit

- Mehrseitige Sicherheit bedeutet die Einbeziehung der Schutzinteressen aller Beteiligten sowie das Austragen daraus resultierender Schutzkonflikte beim Entstehen einer Kommunikationsverbindung.

Inhalte der Kommunikation

Vertraulichkeit
 Verdecktheit

Kommunikationsumstände

Anonymität
 Unbeobachtbarkeit

- 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

Schutzziele mehrseitiger IT-Sicherheit

- Mehrseitige Sicherheit bedeutet die Einbeziehung der Schutzinteressen aller Beteiligten sowie das Austragen daraus resultierender Schutzkonflikte beim Entstehen einer Kommunikationsverbindung.

Inhalte der Kommunikation

Vertraulichkeit
 Verdecktheit

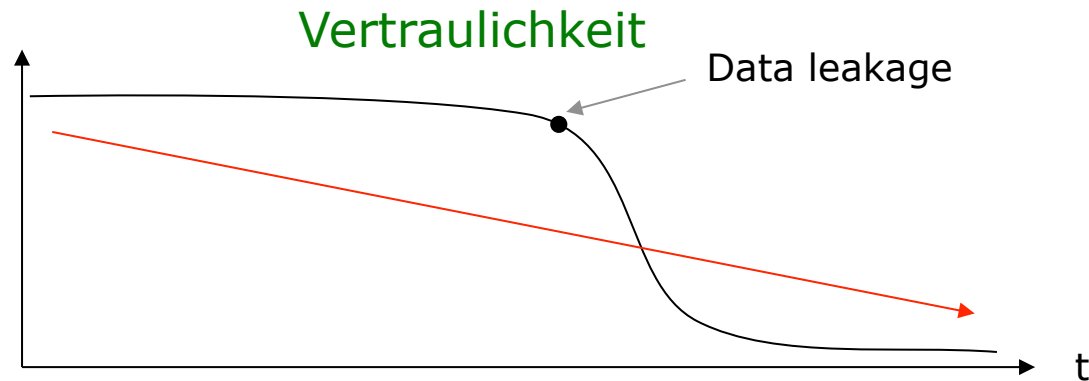
Kommunikationsumstände

Anonymität
 Unbeobachtbarkeit

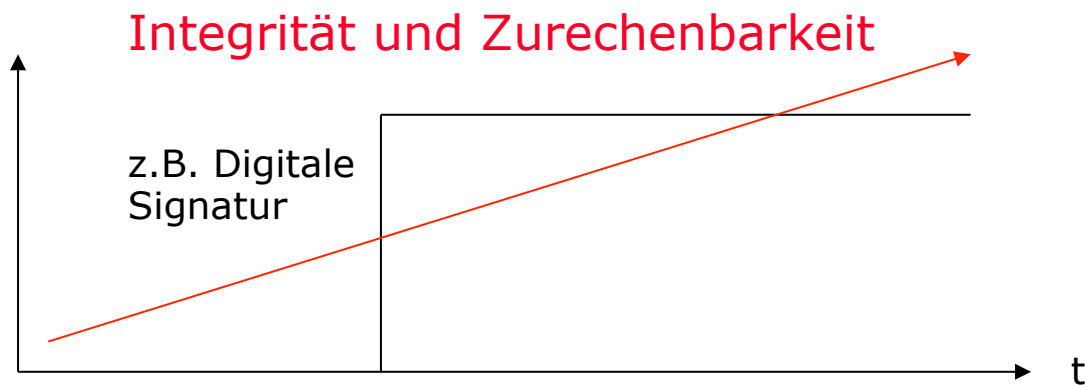
- Datenvermeidung
 - Erfassungsmöglichkeit und Speicherung personenbezogener Daten vermeiden
- Datensparsamkeit
 - Jeder behält seine personenbezogenen Daten in seinem persönlichen Verfügungsbereich.

Beobachtungen zum Monotonieverhalten

- Vertraulichkeit kann nur geringer werden.

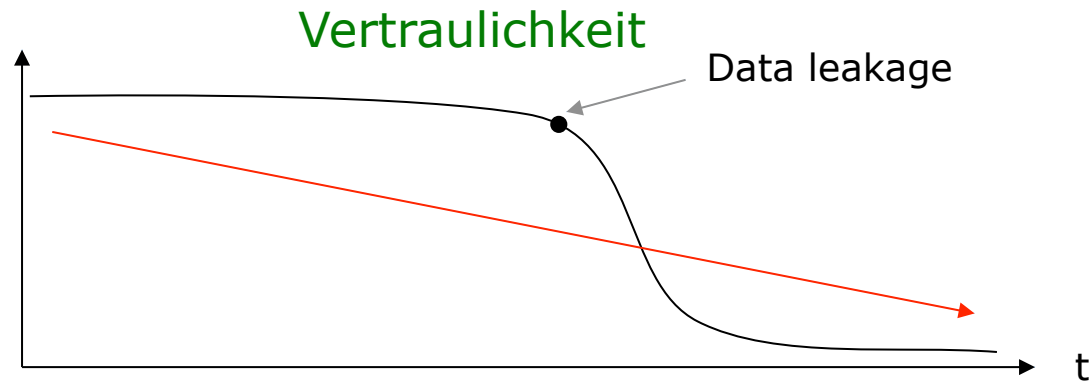


- Integrität und Zurechenbarkeit können nur größer werden.



Beobachtungen zum Monotonieverhalten

- Vertraulichkeit kann nur geringer werden.



- Fazit

Der Mensch sollte sensible Daten die ihn und andere betreffen, besonders sorgsam schützen und nur sehr überlegt weitergeben bzw. veröffentlichen.

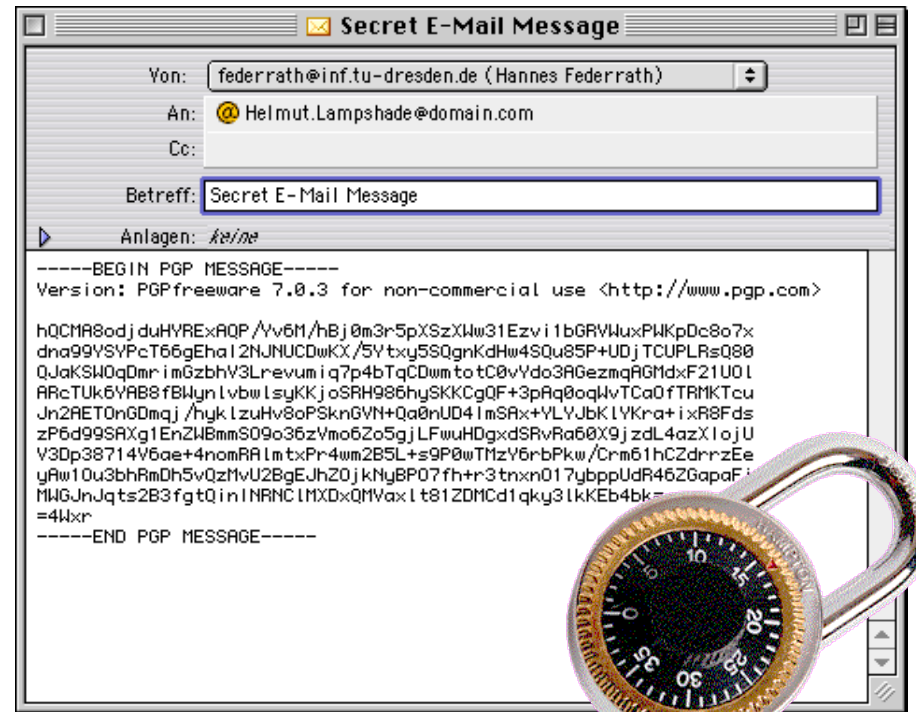
Beispiele für Bausteine datenschutzfördernder Technik

- Verschlüsselung
- Schutz von Kommunikationsbeziehungen
 - Broadcast
 - Proxies
 - MIX network
- Schutz von Transaktionen
 - Pseudonyme
 - Credentials (an Pseudonyme gekettete Eigenschaften)



Verschlüsselung

- Verschlüsseln hilft gegen Ausspähen der Inhalte durch Außenstehende
- Empfehlungen:
 - GnuPG für E-Mail-Verschlüsselung verwenden
 - Auf https beim Senden von sensiblen Daten im Browser achten



Verschlüsseln hilft nichts gegen die Beobachtung von Kommunikationsbeziehungen durch Außenstehende und Netzbetreiber

Beispiele für Bausteine datenschutzfördernder Technik

- Verschlüsselung

- Schutz von Kommunikationsbeziehungen
 - Broadcast
 - Proxies
 - MIX network

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



Broadcast

- Das war damals...

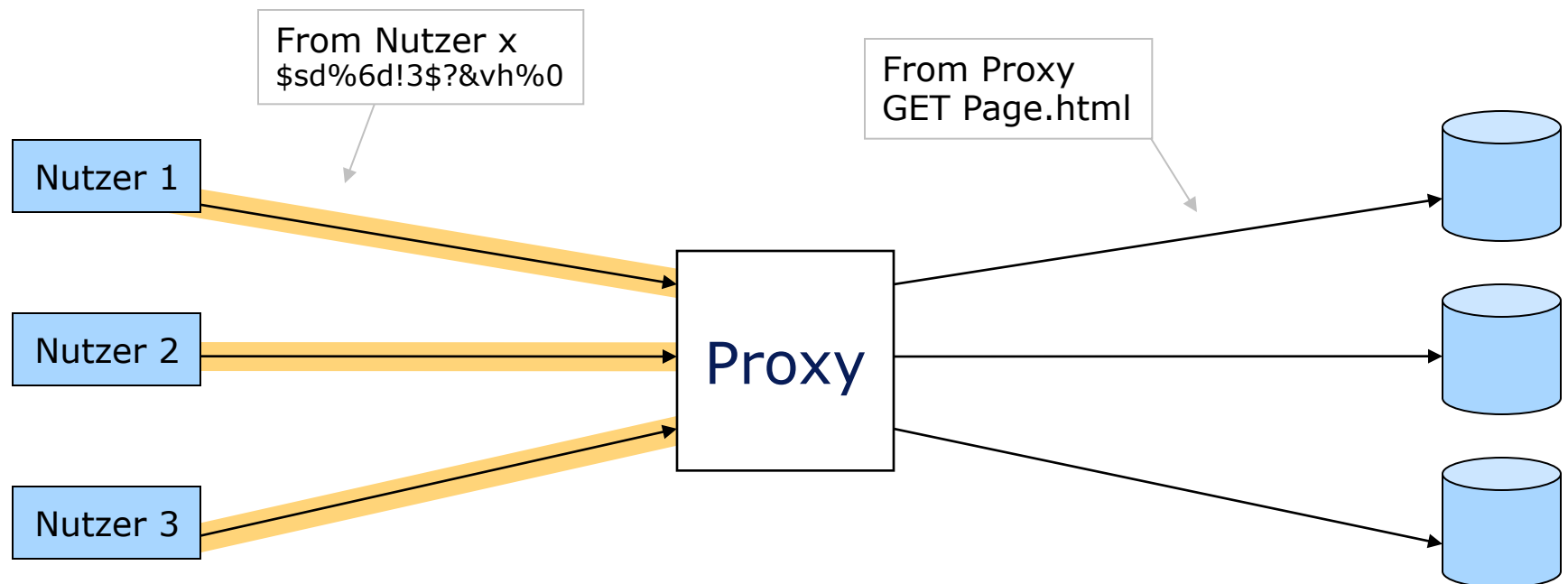


- Zeitung lesen
- Radio über Antenne hören
- Fernsehen über Breitbandverteilkabel

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

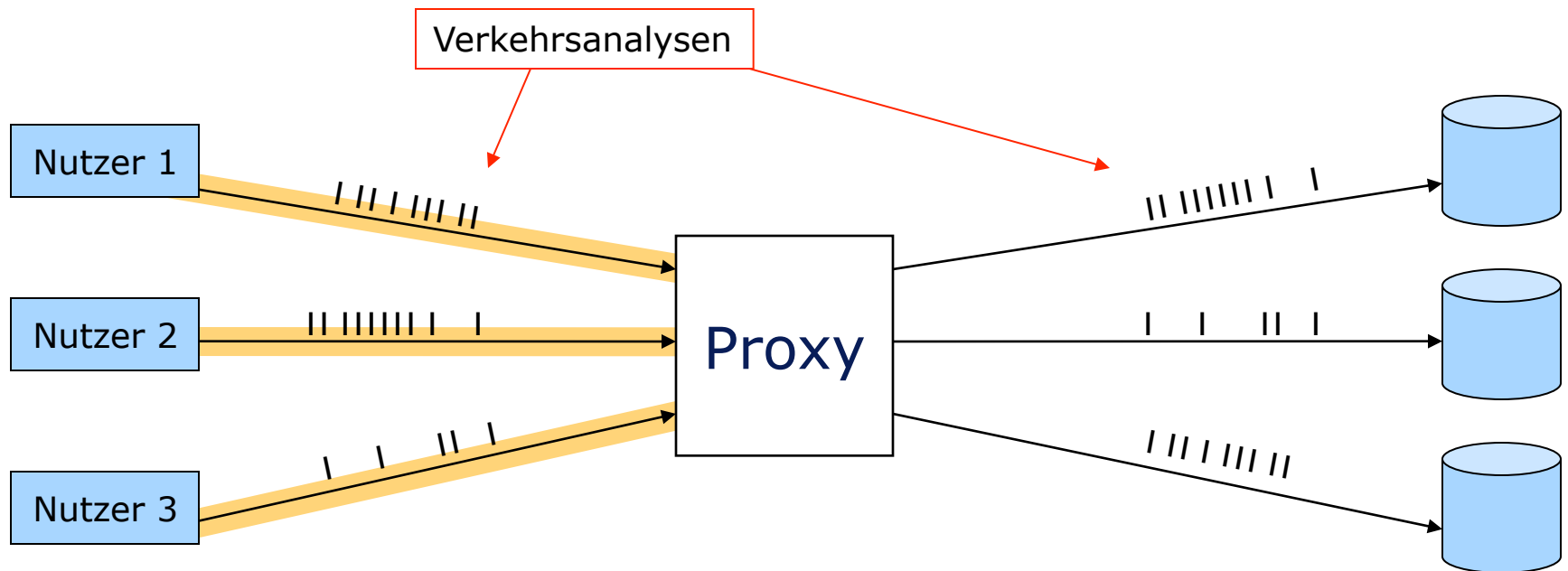
Proxies: Outsider

- 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

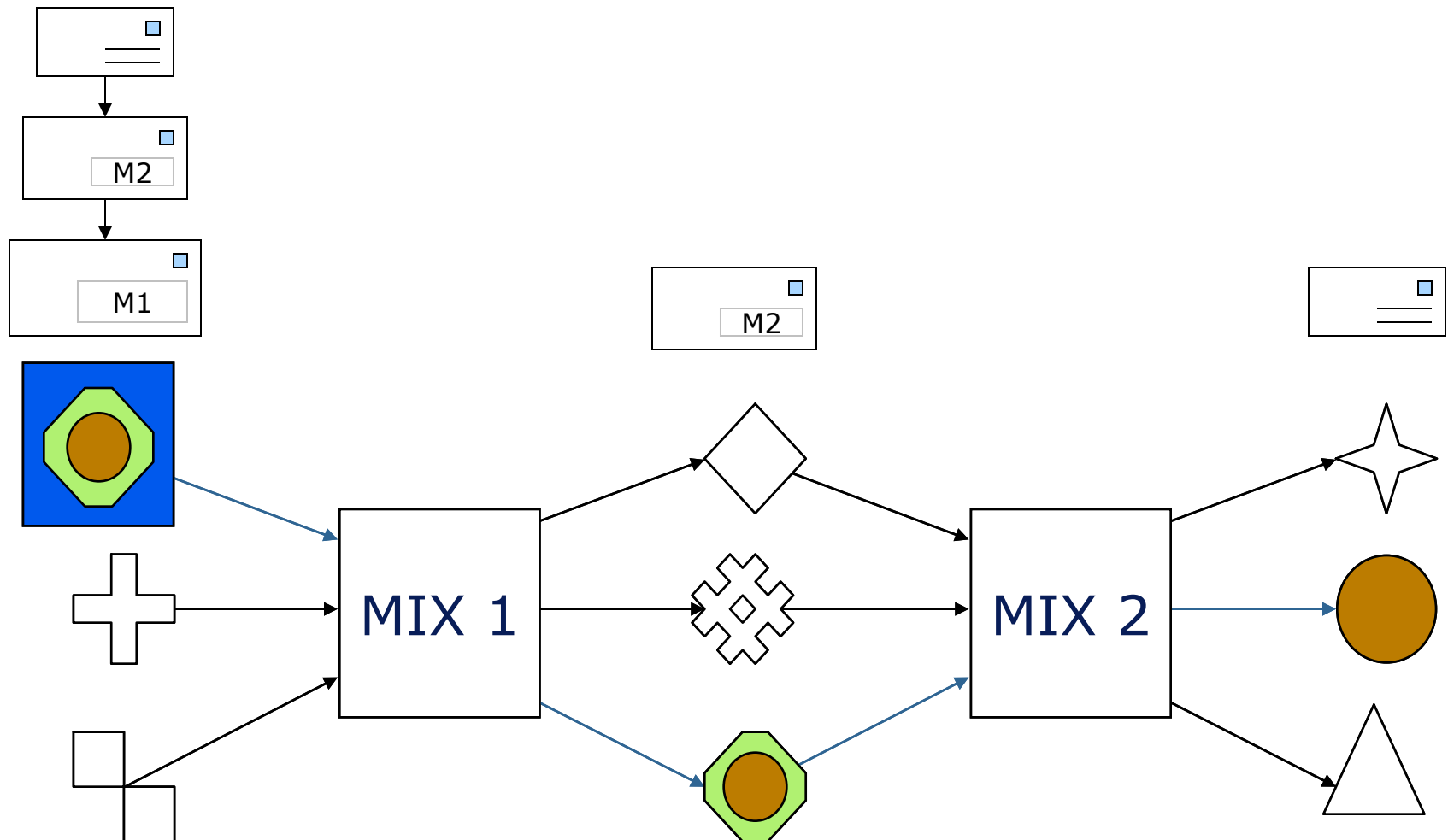


Mix-Netz (Chaum, 1981)

- 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

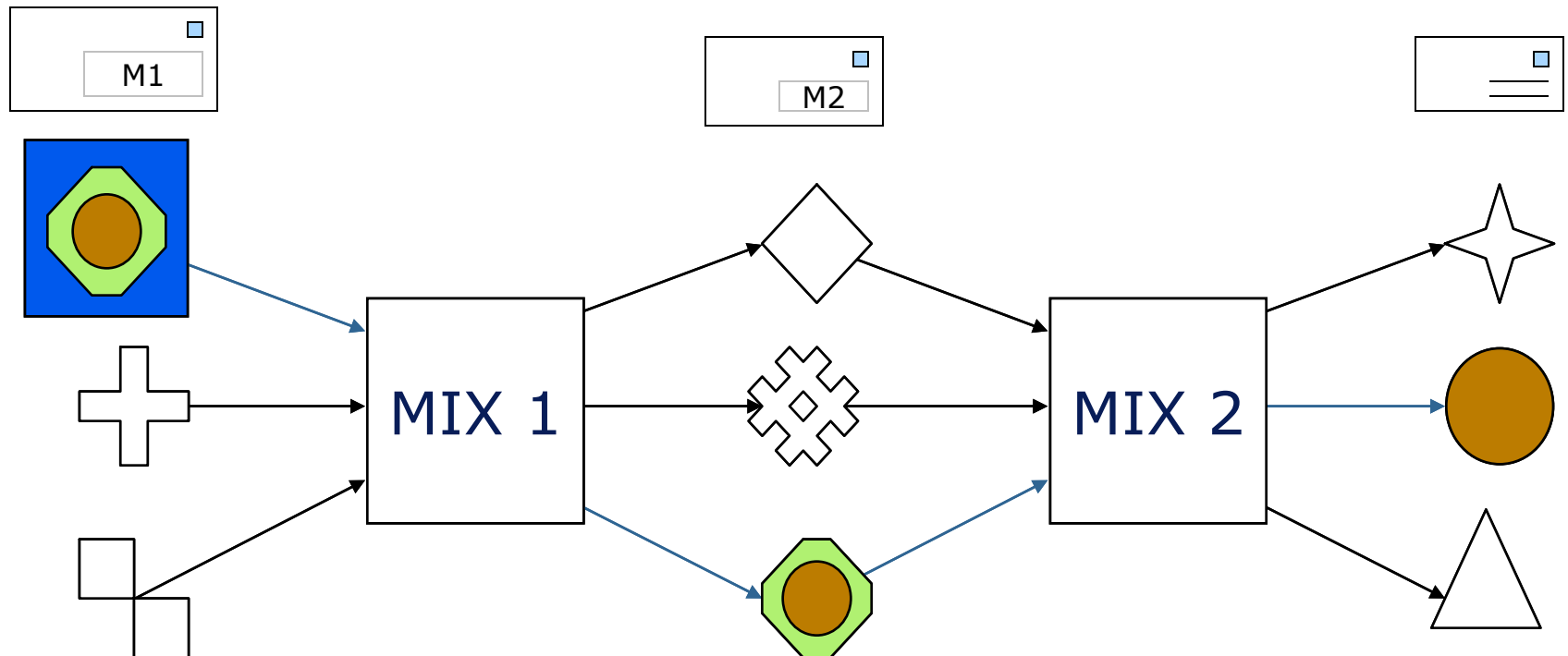
Mix-Netz (Chaum, 1981)

- System zum Schutz von Kommunikationsbeziehungen bei vermittelter Kommunikation



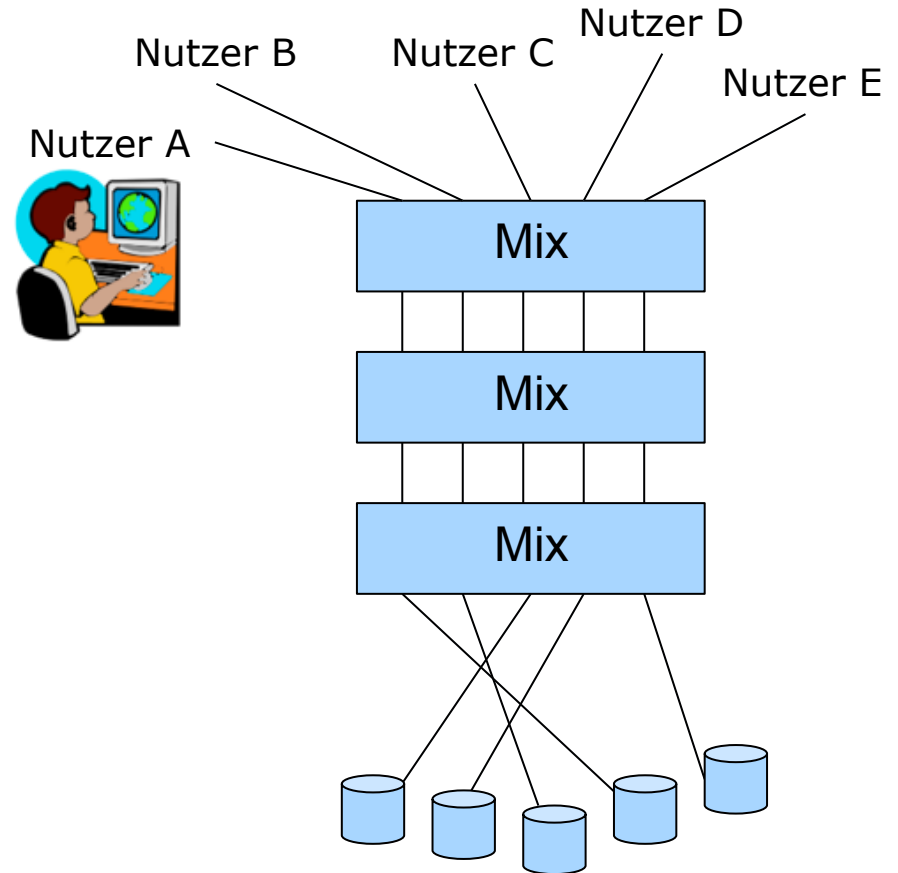
Mix-Netz (Chaum, 1981)

- **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.



AN.ON und TOR

- Dienste zum anonymen Internetzugriff
 - <http://www.anon-online.de>
 - <http://tor.eff.org>
- Schutz des Einzelnen vor Überwachung und Profilierung seiner Internetaktivitäten
- beruhen auf Erweiterungen des Mix-Verfahrens von Chaum
- Schutz auch vor dem Betreiber des Dienstes (Schutz vor Insidern)



Beispiele für Bausteine datenschutzfördernder Technik

- Verschlüsselung

- Schutz von Kommunikationsbeziehungen
 - Broadcast
 - Proxies
 - MIX network

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



Pseudonyme

- Pseudonym-Arten

- Vom Teilnehmer selbst gewählte Zeichenketten, die keinen Bezug zu seiner Identität besitzen
- Große Zufallszahlen (etwa 45 Dezimalstellen)
- Öffentliche Testschlüssel eines Signatursystems

- Pseudonyme zur Bestätigung von Eigenschaften

- Einfaches »qualifizierendes Zertifikat«
- Blenden des Pseudonyms vor dem Zertifizieren

BEGIN ZERTIFIKAT

Pseudonym: 30452634272346623424987241375

Öffentlicher Testschlüssel des Pseudonyms:
h833hd38dddajscbicme098342k236egfkW74h5445
84hdbscldmrtpofjrkt0jshuedagaszW12geb3u4b=

Bestätigte Eigenschaften:

Der Inhaber ist über 18 Jahre alt.

Der Inhaber ist deutscher Staatsbürger.

Datum: 19.03.2000

Gültig bis: 18.03.2001

Aussteller: Einwohnermeldeamt Dresden

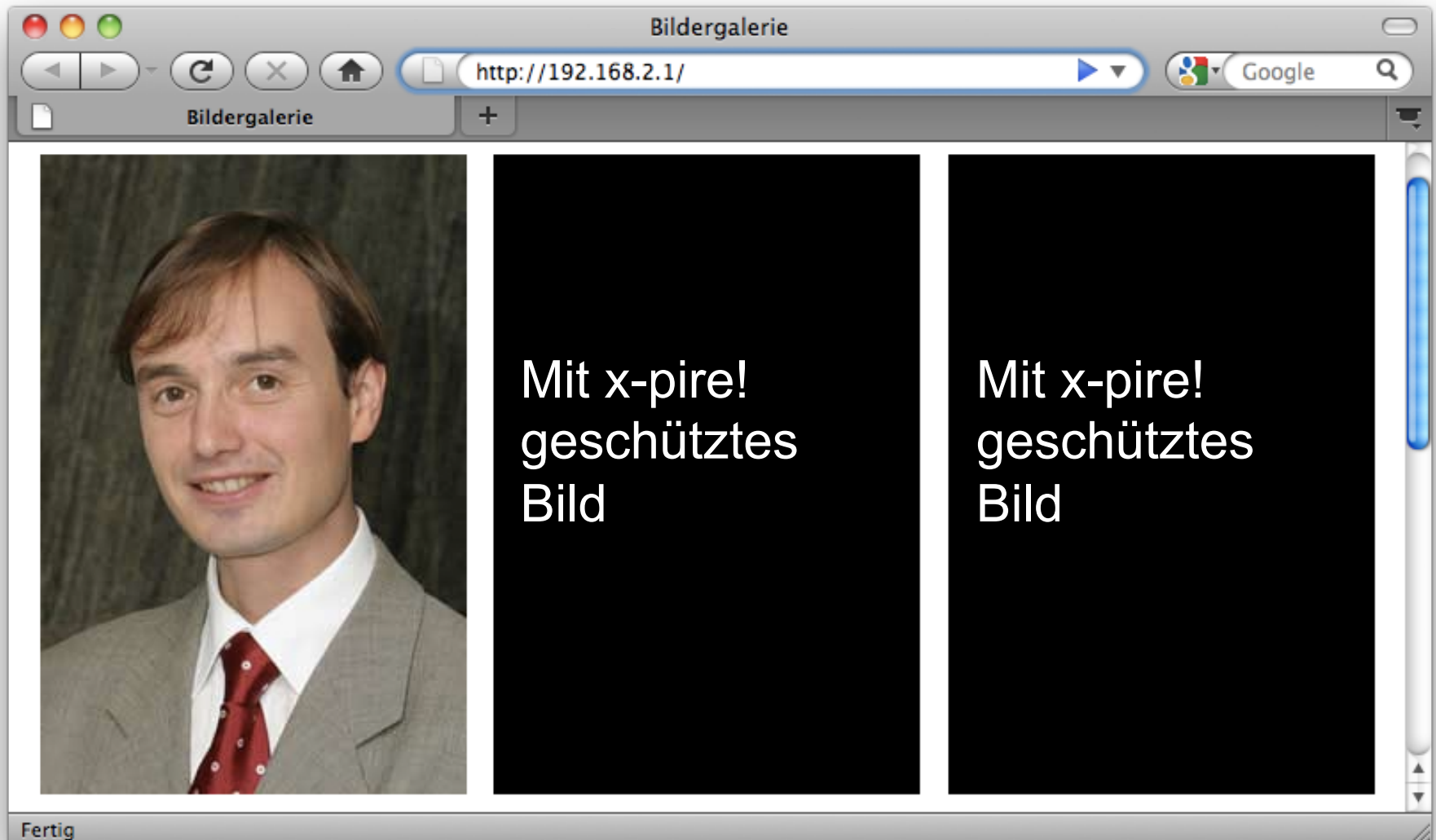
Signatur des Ausstellers:

23j423vdsaz345kj435ekji3u4z2983734ijo23i72
kj867wdbez2o074j5lkdmcdkki1237t3rgbdvbwDj=

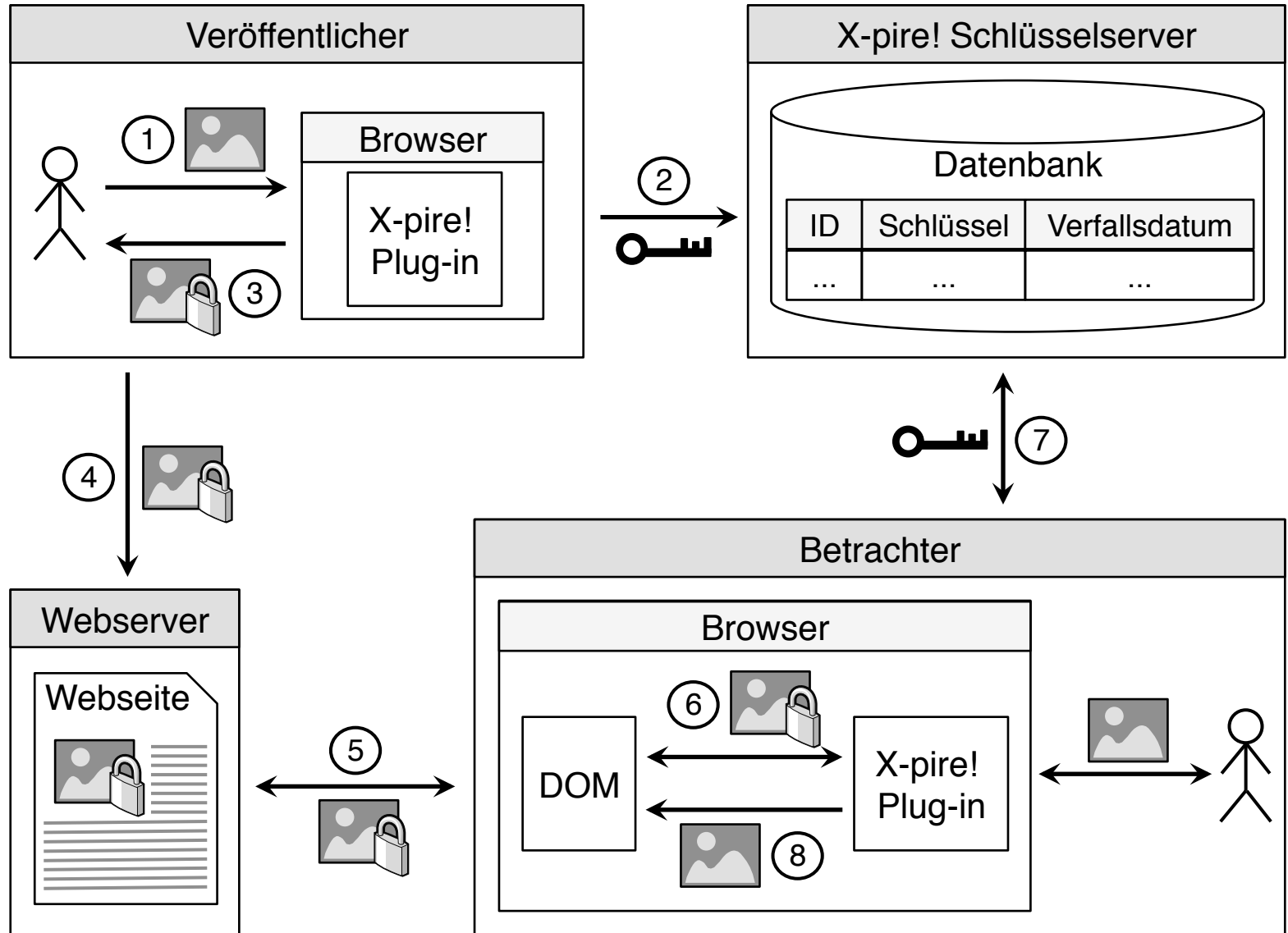
END ZERTIFIKAT

Beispiel eines hoffnungslosen Versuchs

- x-pire!



Funktionsweise X-pire!

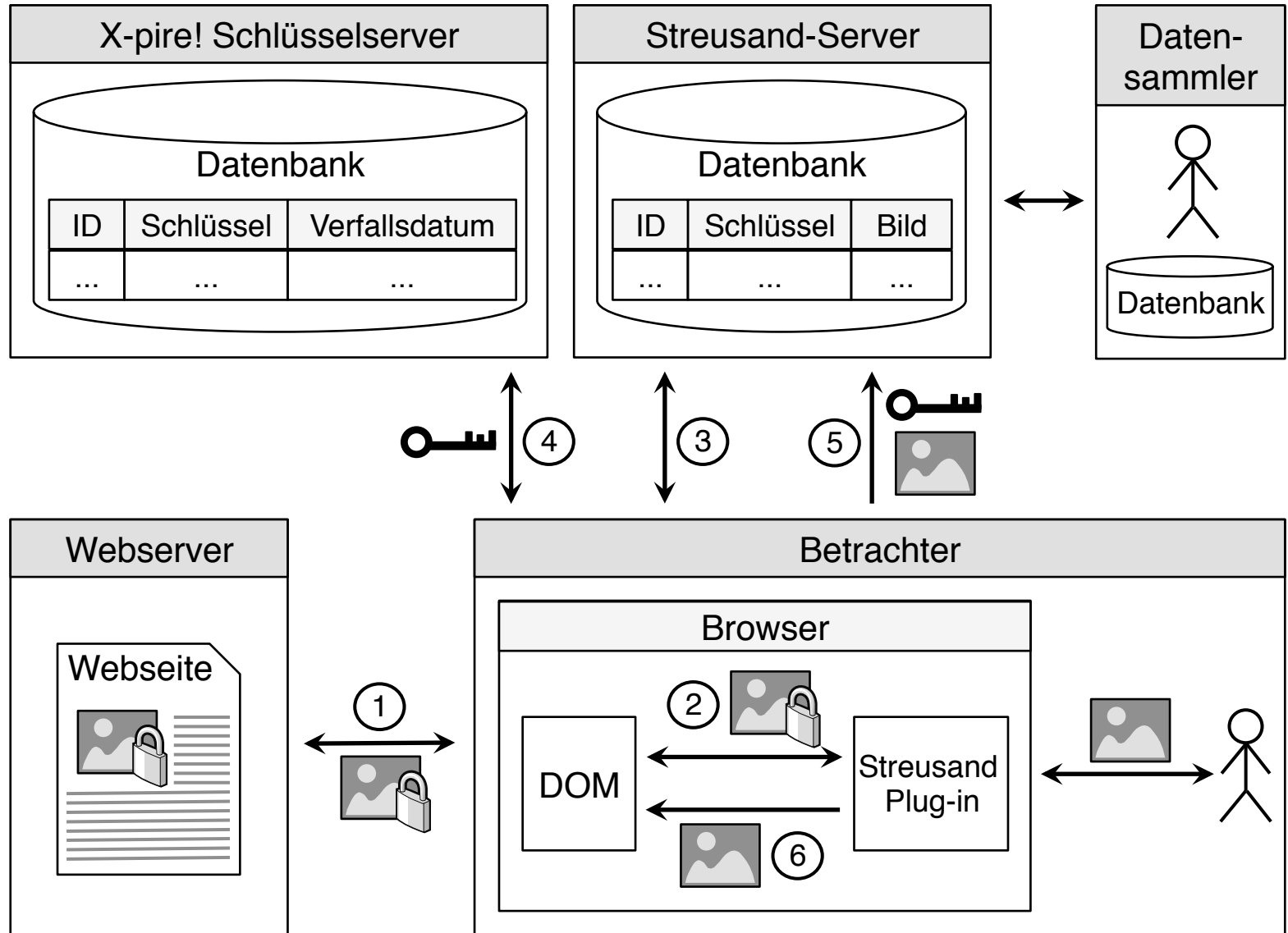


Sicherheit von x-pire!

- Kein Schutz gegen Angreifer in der Rolle »Betrachter«
 - Software im Verfügungsbereich des Betrachters (Browser) erhält Zugriff auf Schlüssel und unverschlüsselten Inhalt

- Streisand-Effekt
 - Insbesondere Inhalte, die wieder aus dem Netz verschwinden sollen, halten sich möglicherweise besonders lange.

Funktionsweise Streusand



Zusammenfassung

- Sensible Daten besonders sorgsam schützen
 - nur sehr überlegt weitergeben und veröffentlichen
- Möglichst immer Pseudonyme verwenden
 - Verhindert (leichte) Verkettbarkeit von Daten
- Verschlüsselung und Anonymisierung verwenden
 - Verhindert Beobachtung der Aktivitäten



Universität Hamburg
Fachbereich Informatik
Arbeitsbereich SVS
Prof. Dr. Hannes Federrath
Vogt-Kölln-Straße 30
D-22527 Hamburg

E-Mail federrath@informatik.uni-hamburg.de
Telefon +49 40 42883 2358
<http://svs.informatik.uni-hamburg.de>