Perspektiven des Identitätsmanagements auf Datenschutz und Datensicherheit

Dipl.-Ing. Dr. iur. Walter Hötzendorfer
Senior Researcher

Research Institute AG & Co KG
Zentrum für digitale Menschenrechte

E-Mail: walter.hoetzendorfer@researchinstitute.at
Web: http://www.researchinstitute.at

Schutzziele der Datensicherheit

- **Vertraulichkeit**
- **Integrität**
- **Verfügbarkeit**

Alle drei Schutzziele kann man auf Zugriffskontrolle und somit auf **Identitätsmanagement** herunterbrechen (*Bruce Schneier*):

> *Autorisierte Individuen sollen machen können, wozu sie autorisiert sind (Verfügbarkeit), und andere Individuen nicht (Vertraulichkeit, Integrität).*

- Eines davon allein ist einfach
- Beides zusammen ist schwierig

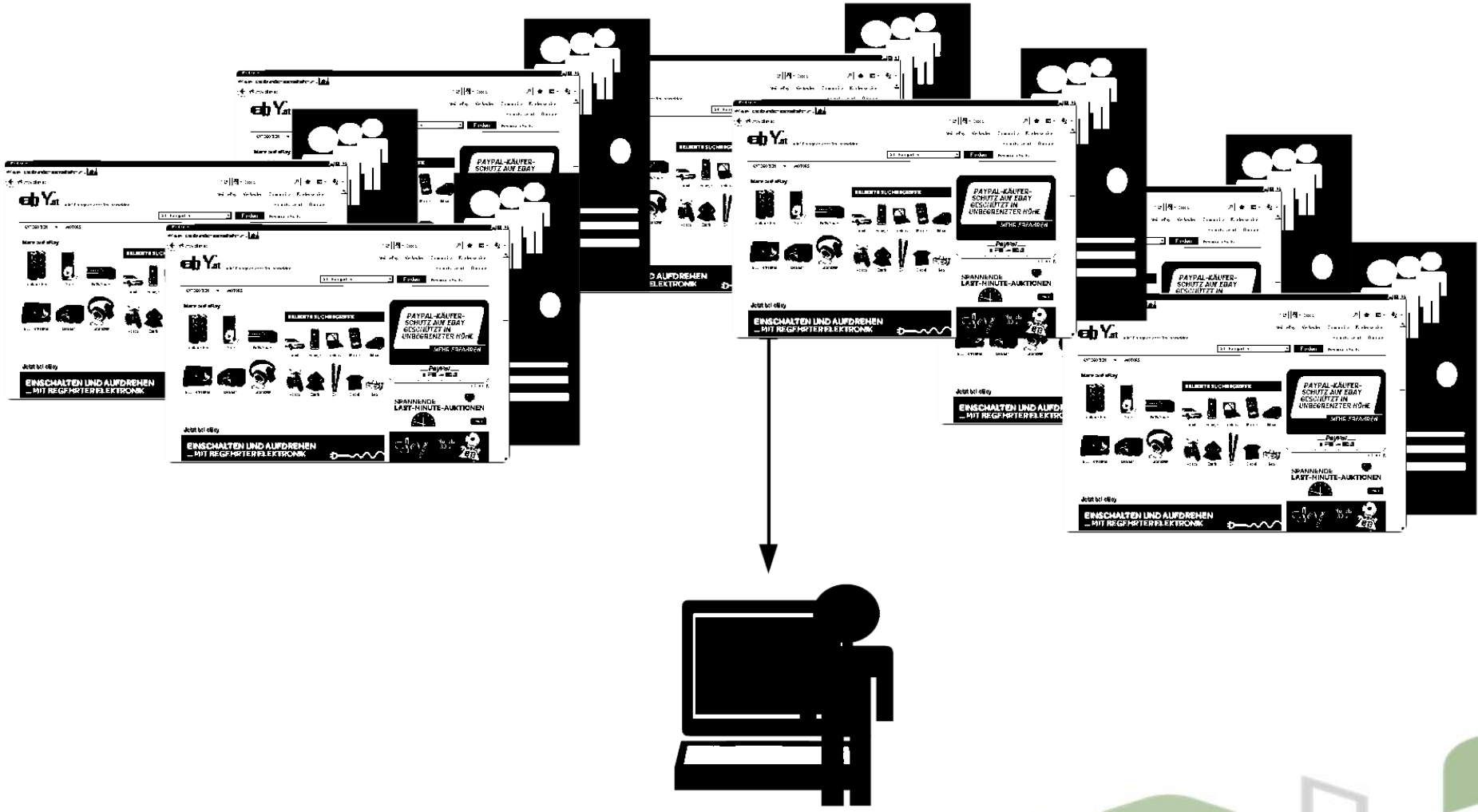
Weitere (Schutz-)Ziele

- **Authentizität**
- **Nichtabstreitbarkeit** (auch Verbindlichkeit, engl. *non-repudiation*)
- **Zurechenbarkeit**

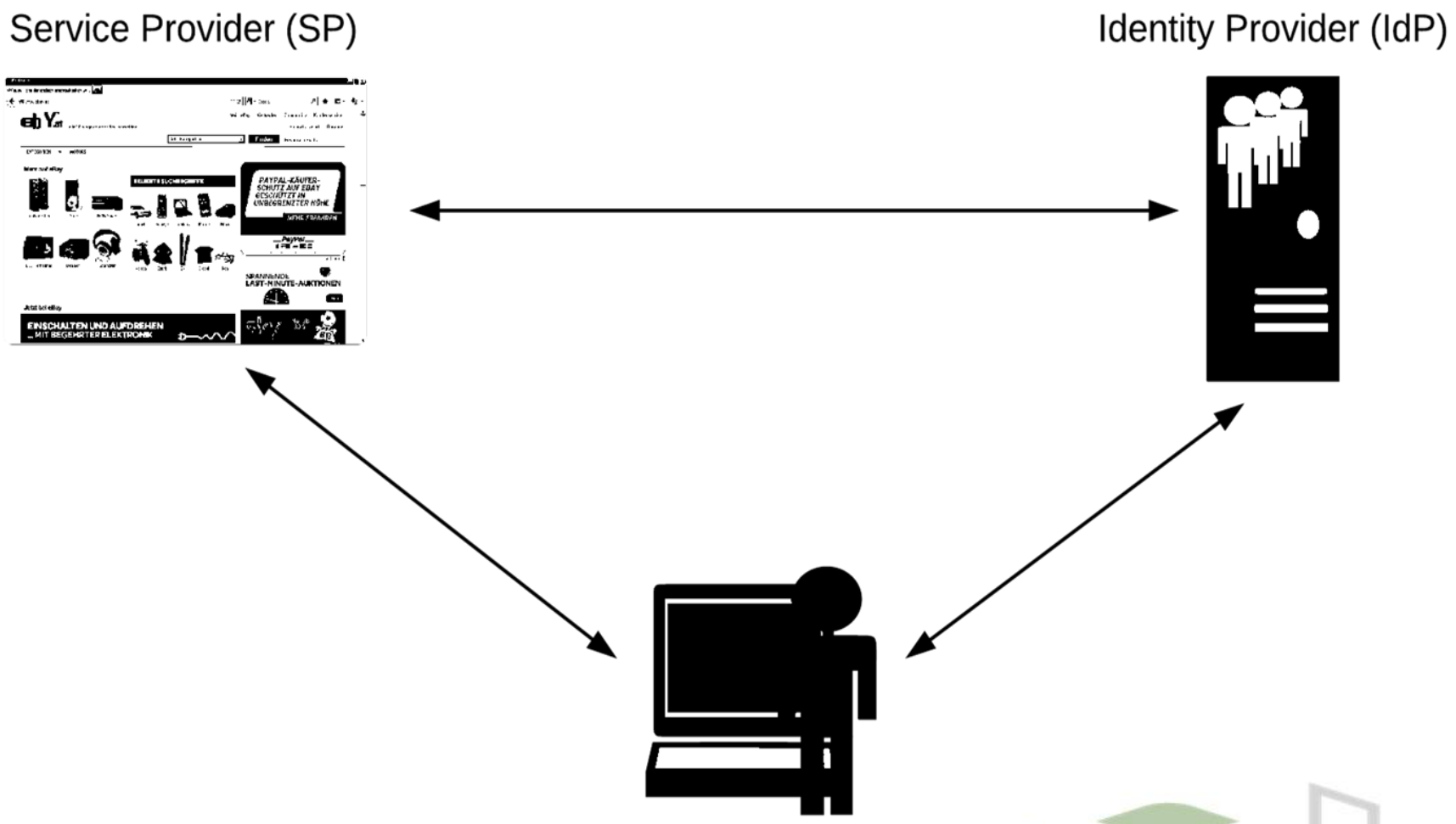
  Autorisierte Individuen sollen machen können, wozu sie autorisiert sind (und andere Individuen nicht), wenn nötig sollten ihnen diese Handlungen aber zugerechnet werden können und dann sollten sie diese Handlungen nicht abstreiten können.

research institute

Service Provider (SP)/ Identity Provider (IdP)



FÖDERIERTES IDENTITÄTSMANAGEMENT



„Identifikationsparadoxon“:

Sowohl

anonyme Internetnutzung

als auch

qualifizierter Nachweis der Identität

und/oder bestimmter Eigenschaften

sind im Internet schwierig.

research institute

Privacy by Design:

1. Start thinking about privacy when you start thinking about building a system.

(siehe auch Art 25 DSGVO)

research institute

Privacy by Design:

2. Preclude the privacy-infringing use of a system by technical and organisational means.

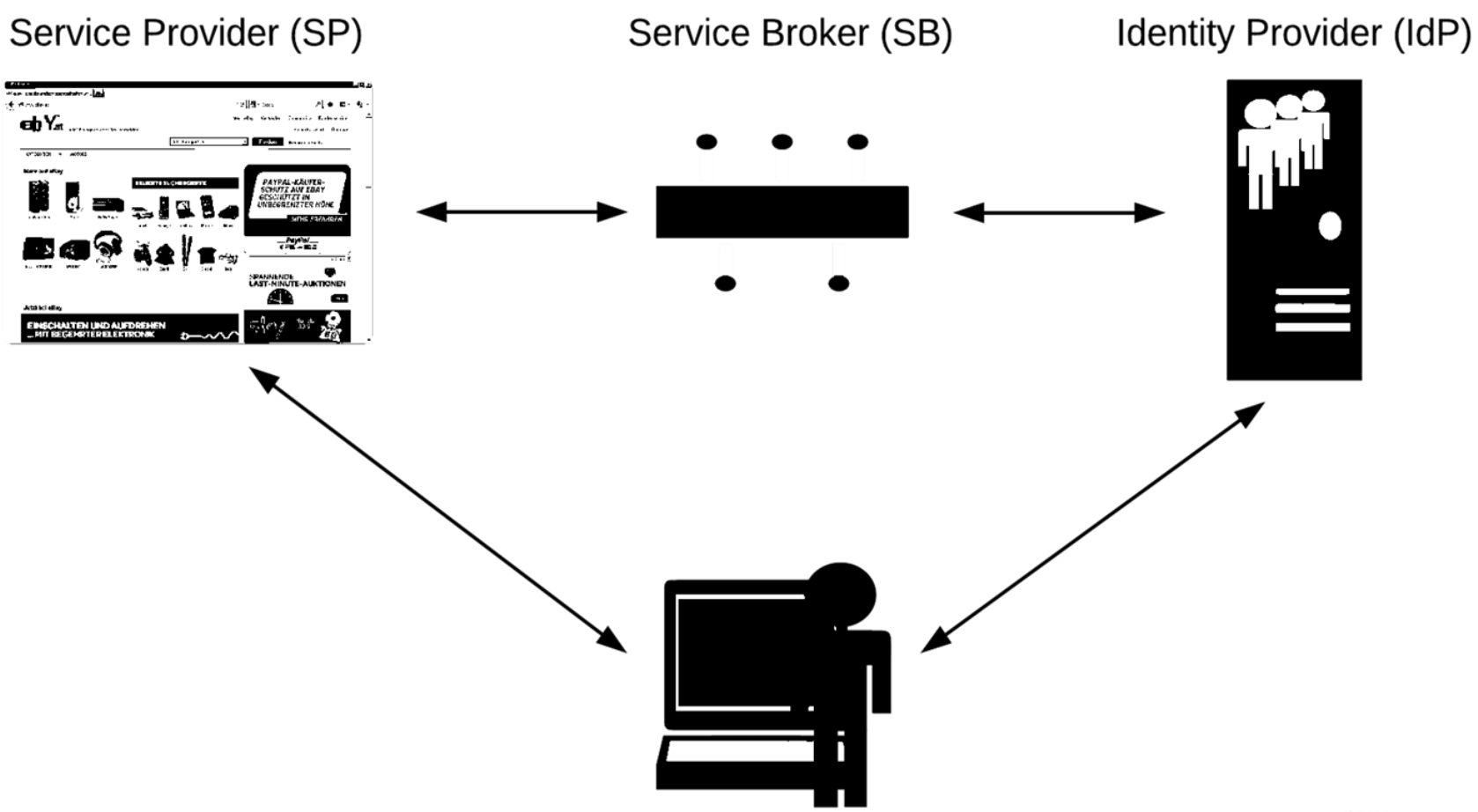
(siehe auch *Lessig*: „Code is law“)

Privacy-By-Design-Schutzziele

- **Anonymität**
- **Unverkettbarkeit** (*unlinkability*): Voneinander unabhängige Handlungen eines Nutzers können nicht miteinander in Verbindung gebracht werden.
- In der Praxis: beschränkte Verkettbarkeit (*limited linkability*)
- **Unbeobachtbarkeit** (*unobservability*): Handlungen eines Nutzers können nicht mit dem Nutzer in Verbindung gebracht werden und von Außenstehenden gar nicht festgestellt werden („Vertraulichkeit des Verhaltens“)
- In der Praxis: beschränkte Beobachtbarkeit (*limited observability*)

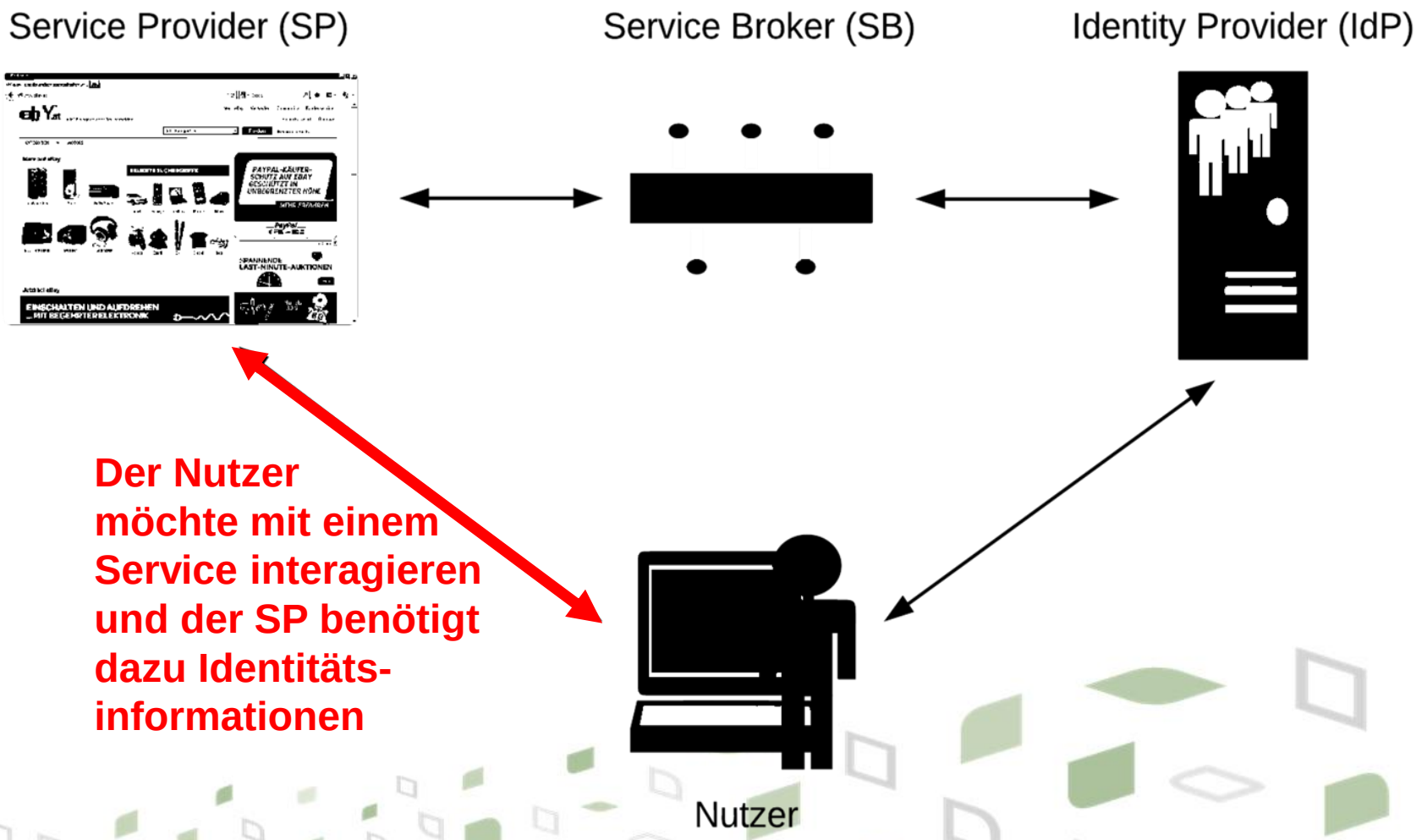
research institute

DAS PEFIM-MODELL

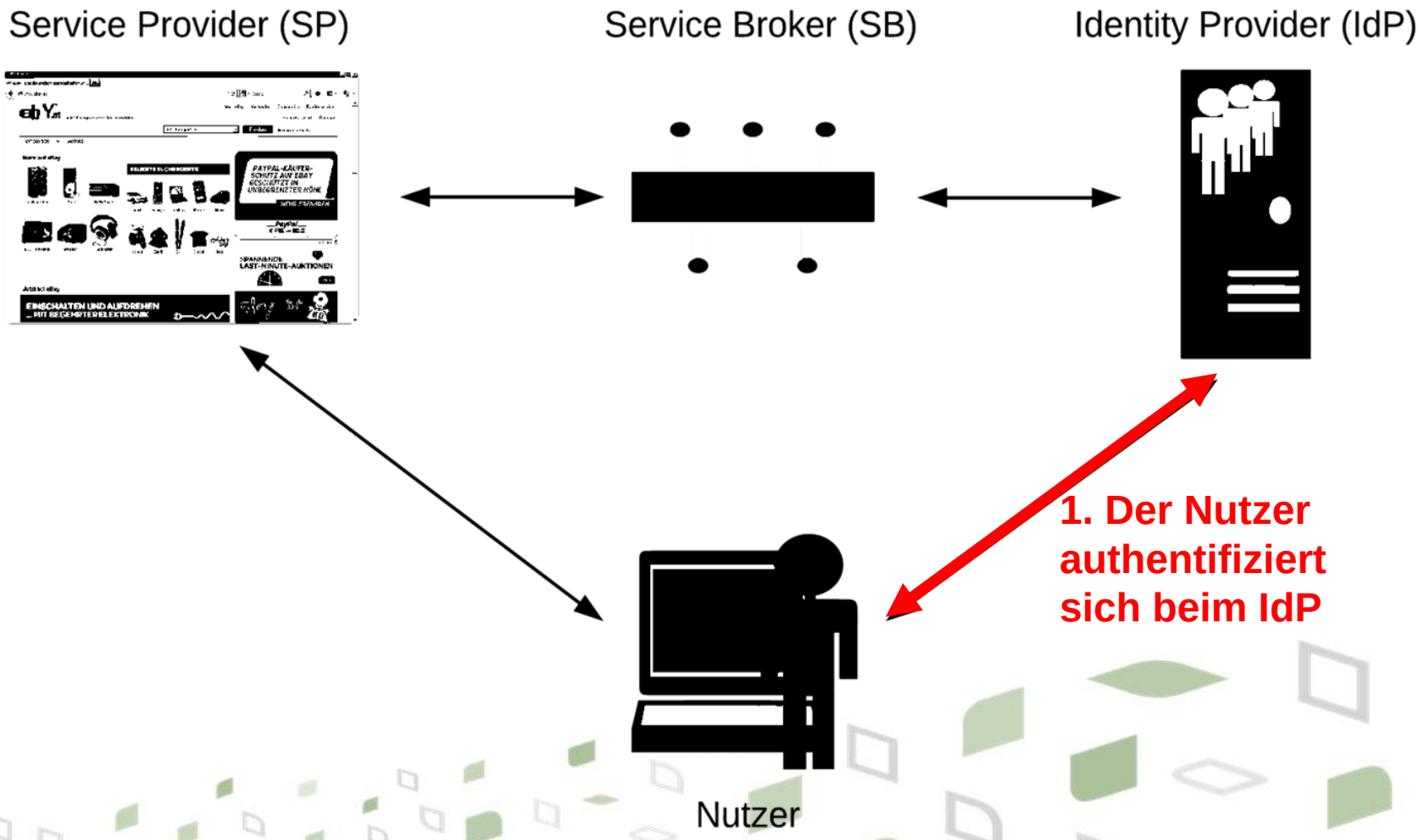


Privacy-enhancing Federated Identity Management Model

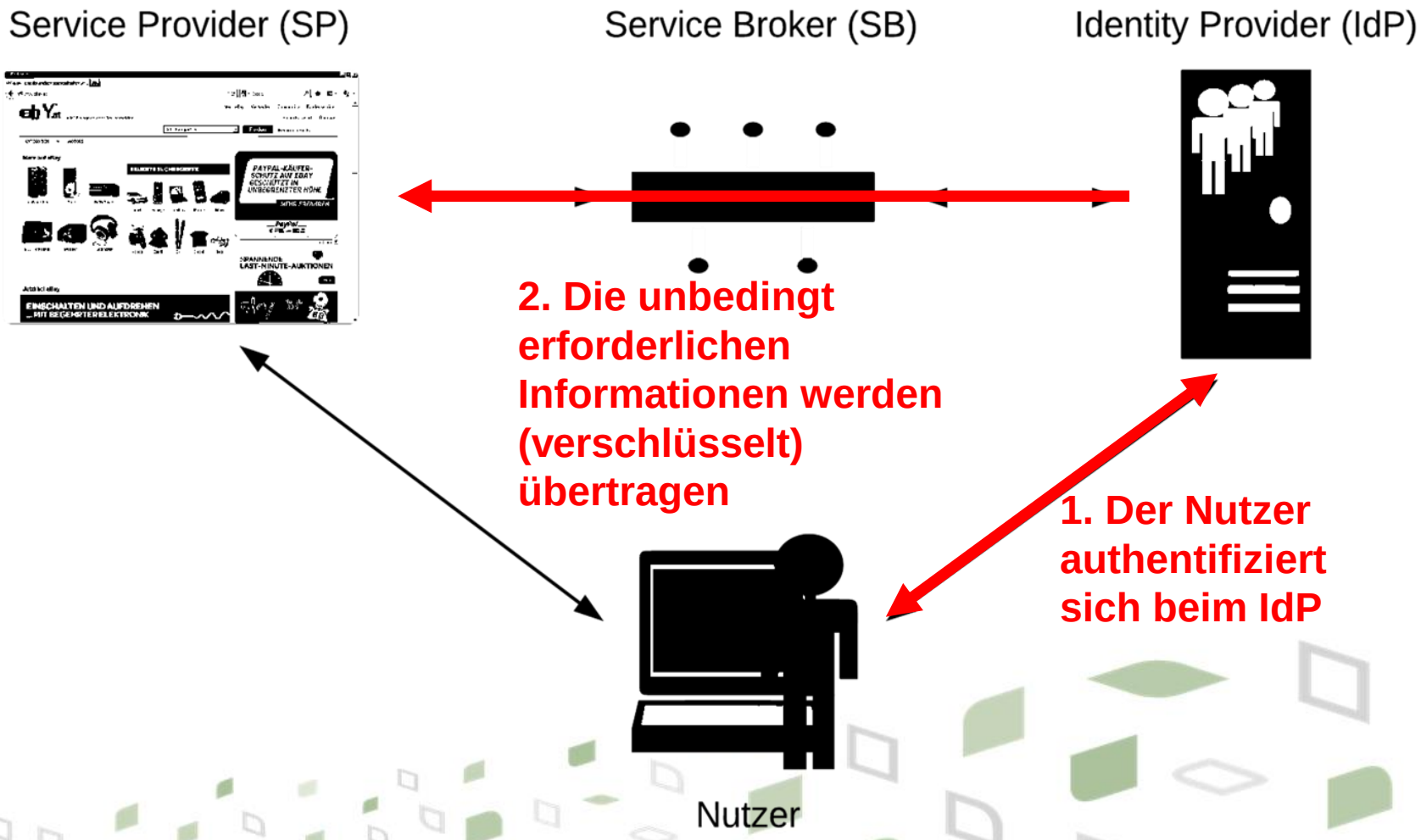
Das PEFIM-Modell: Funktionsweise



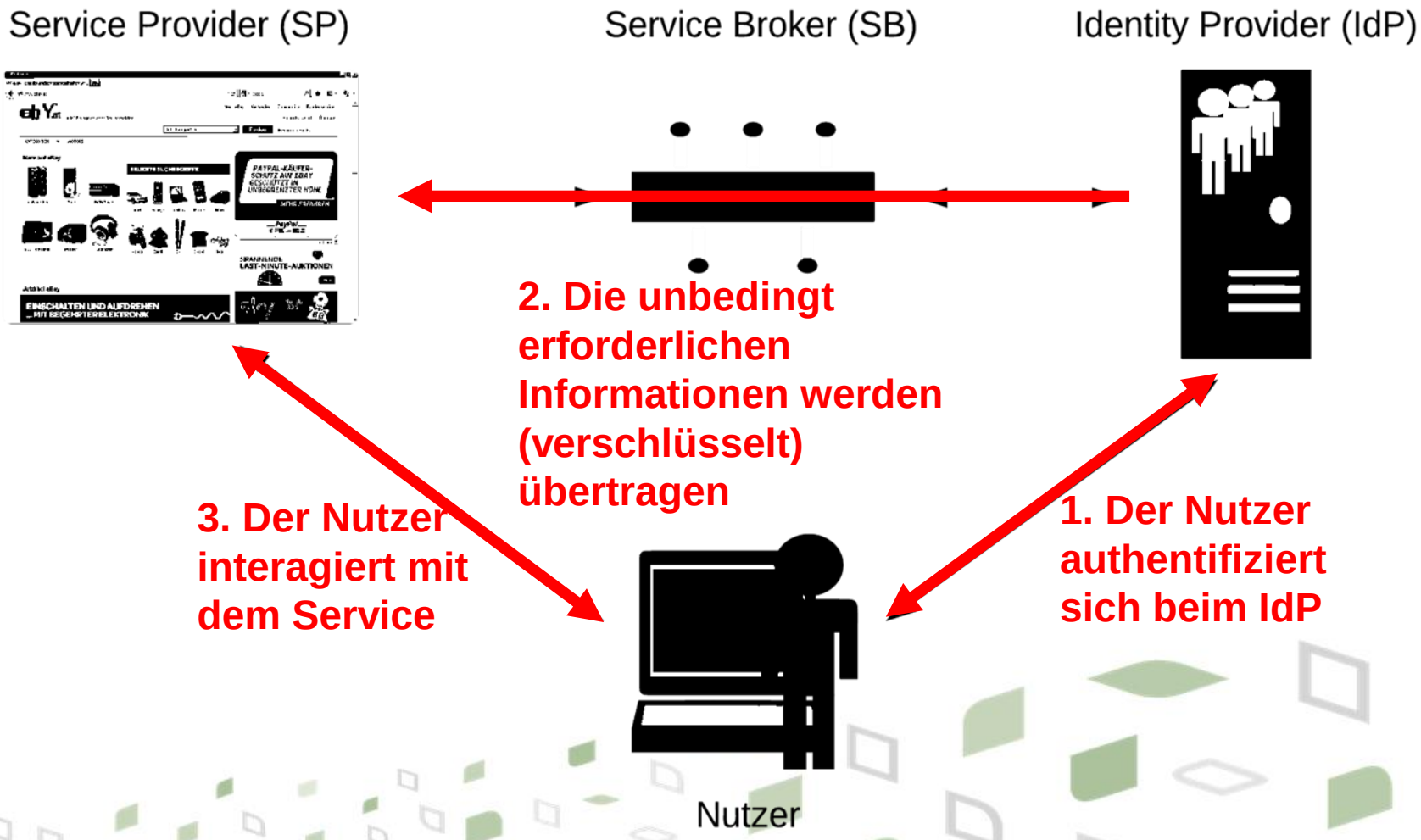
Das PEFIM-Modell: Funktionsweise



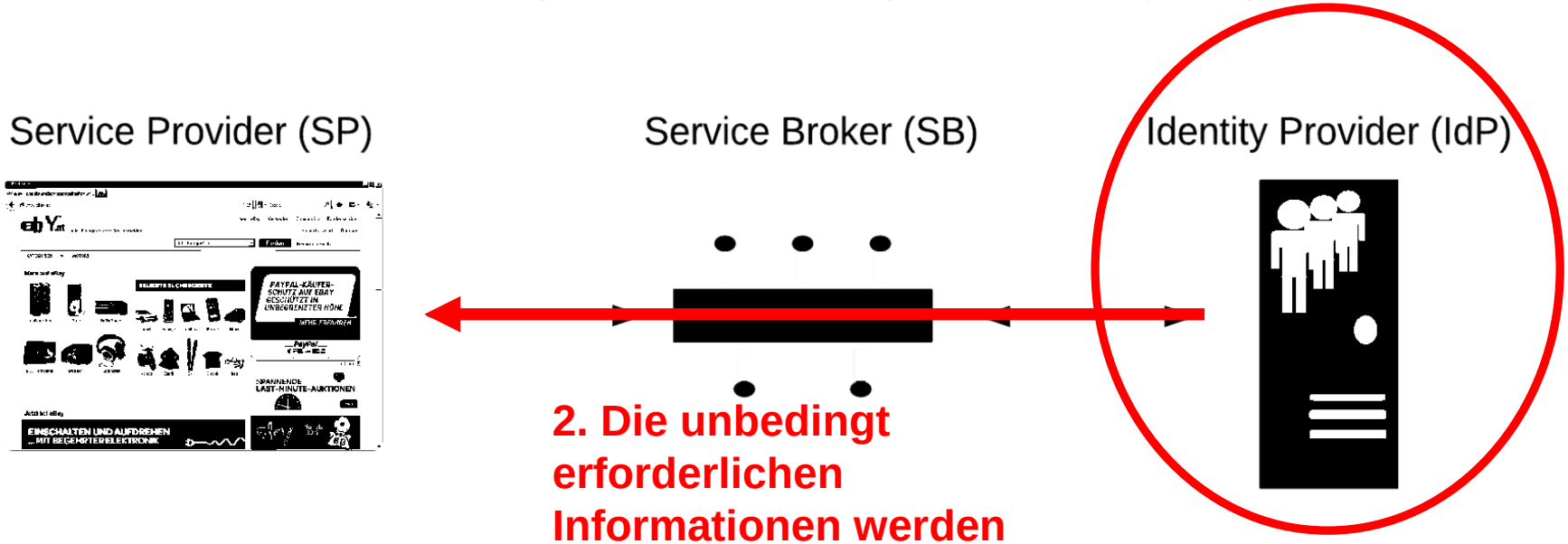
DAS PEFIM-MODELL: FUNKTIONSWEISE



Das PEFIM-Modell: Funktionsweise

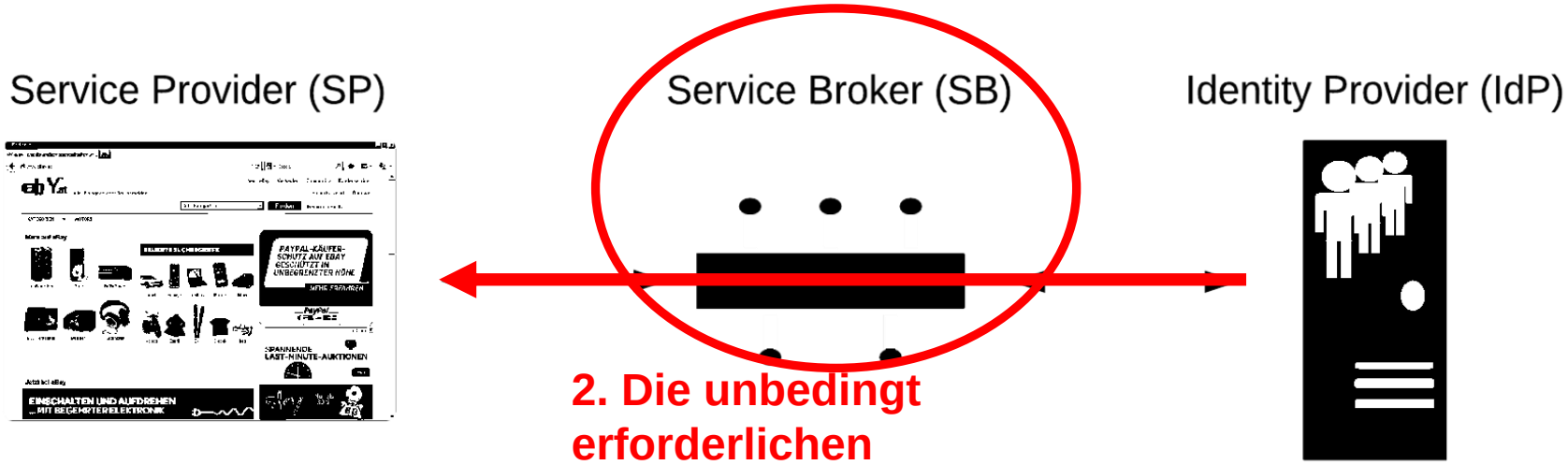


Das PEFIM-Modell: Eigenschaften



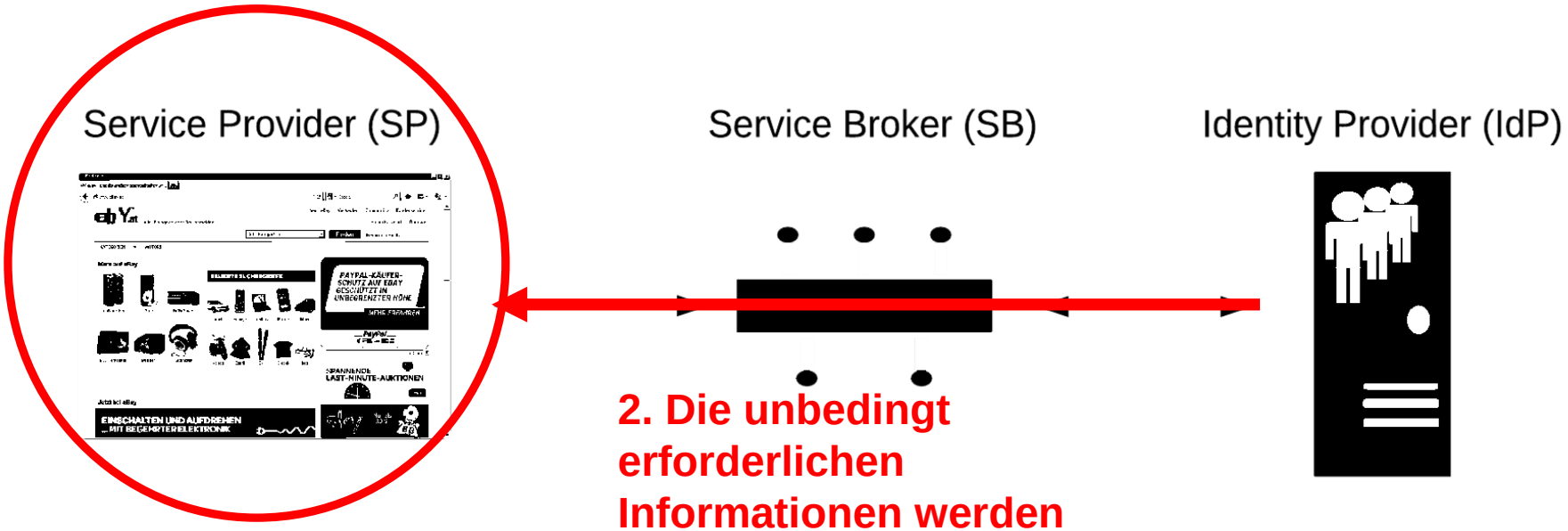
- IdP sieht
  - Identität und Attribute des Nutzers
  - dass Transaktionen mit bestimmten Attributen des Nutzers erfolgen
- IdP sieht nicht
  - welche Services (SP) verwendet werden (-> Unbeobachtbarkeit)

Das PEFIM-Modell: Eigenschaften



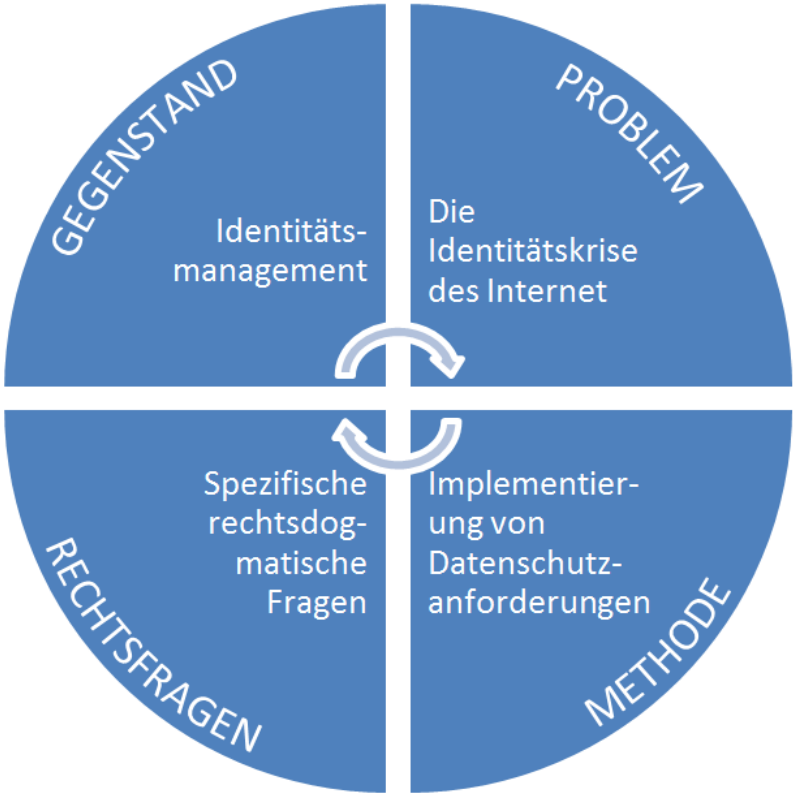
- SB sieht
  - „nur Metadaten“
- SB sieht nicht
  - Identität des Nutzers
  - Attribute des Nutzers
  - jeden sonstigen Inhalt der Transaktion

Das PEFIM-Modell: Eigenschaften

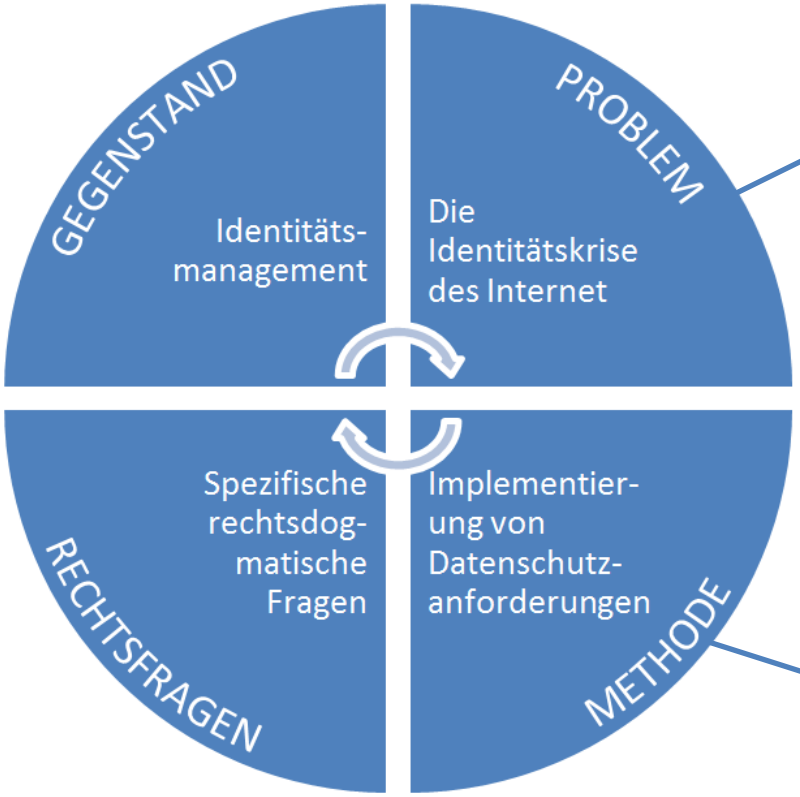


- SP sieht
  - nur die für die Transaktion erforderliche Information über den Nutzer
- SP sieht nicht notwendigerweise
  - die Identität des Nutzers (Unverkettbarkeit) oder zumindest nicht
  - alle Attribute des Nutzers, die der IdP hat

Vier Perspektiven



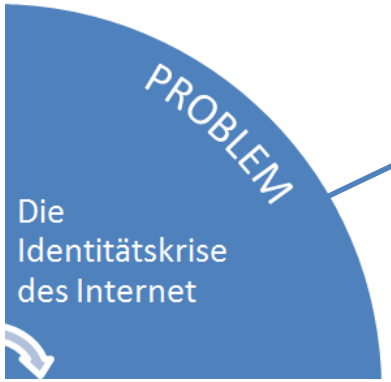
Vier Perspektiven und fünf Thesen



These 1: Identitätsmanagement ist ein Schlüssel zu mehr Datenschutz im Internet.
These 2: Es ist datenschutzrechtlich geboten, die Situation hinsichtlich Anonymität und Identität im Internet zu verbessern.
These 3: Das PEFIM-Modell ist geeignet, die Situation hinsichtlich Anonymität und Identität im Internet zu verbessern.

These 4: Die technische Gestaltung von Systemen ist der mächtigste Faktor zur Durchsetzung des Datenschutzes.
These 5: Die Umsetzung von Privacy by Design erfordert (eine Community von) „Privacy Engineers“ mit technischen Kenntnissen und Kenntnissen des Datenschutzes, die an der Gestaltung technischer Systeme von Beginn an beteiligt sind und Grundsätze des Datenschutzes individuell auf das konkret zu entwickelnde System umlegen.

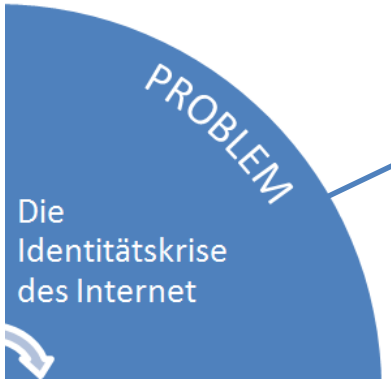
Die „Identitätskrise“ des Internet



These 1: Identitätsmanagement ist ein Schlüssel zu mehr Datenschutz im Internet.
These 2: Es ist datenschutzrechtlich geboten, die Situation hinsichtlich Anonymität und Identität im Internet zu verbessern.
These 3: Das PEFIM-Modell ist geeignet, die Situation hinsichtlich Anonymität und Identität im Internet zu verbessern.

- Ja, *ein* Schlüssel: PEFIM-Modell als Beispiel für ein Modell, das
  - den qualifizierten Nachweis der Identität oder bestimmter Attribute und
  - wo erforderlich Nachvollziehbarkeit und Zurechenbarkeit ermöglicht und dabei
  - ein Maximum an Anonymität gewährleistet bei
  - minimaler Beobachtbarkeit und
  - minimaler Verkettbarkeit des Nutzerverhaltens
- Aber: Maßnahmen auch auf anderen Ebenen nötig:
  - Netzwerk-Ebene: IP-Adresse, DNS
  - Applikations-Ebene: Cookies, Browser-/Device-Fingerprinting

Die „Identitätskrise“ des Internet



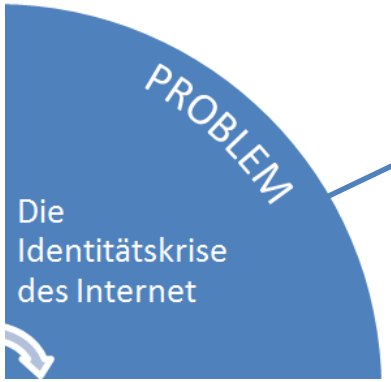
These 1: Identitätsmanagement ist ein Schlüssel zu mehr Datenschutz im Internet.

These 2: Es ist datenschutzrechtlich geboten, die Situation hinsichtlich Anonymität und Identität im Internet zu verbessern.

These 3: Das PEFIM-Modell ist geeignet, die Situation hinsichtlich Anonymität und Identität im Internet zu verbessern.

- § 1 Abs 2 DSG: „Eingriff in das Grundrecht jeweils nur in der gelindesten, zum Ziel führenden Art“
- § 7 Abs 3 DSG: Eingriffe in das Grundrecht nur „mit den gelindesten zur Verfügung stehenden Mitteln“
- PEFIM-Modell ist ein Beispiel eines gelinderen Mittels
- Einschränkung: Normadressat ist der Aufraggeber, aber
  - wenn etabliert: Teilnahme geboten
  - in einem geschlossenen Kreis: Einführung geboten

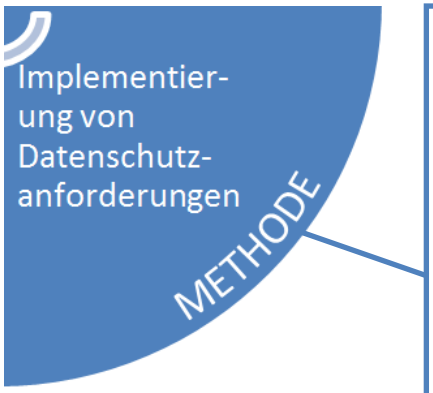
Die „Identitätskrise“ des Internet



These 1: Identitätsmanagement ist ein Schlüssel zu mehr Datenschutz im Internet.
These 2: Es ist datenschutzrechtlich geboten, die Situation hinsichtlich Anonymität und Identität im Internet zu verbessern.
These 3: Das PEFIM-Modell ist geeignet, die Situation hinsichtlich Anonymität und Identität im Internet zu verbessern.

- PEFIM-Modell ist ein Beispiel eines gelinderen Mittels: Identitätsmanagement nach dem PEFIM-Modell weist ggü. dem Status quo eine deutlich geringere Eingriffsintensität auf:
  - Form der Datenverwendung: dezentrale Datenhaltung etc.
  - Art der Daten: möglichst anonym oder pseudonym
  - Inhalt und Umfang der Daten: Datenminimierung, Beschränkung auf das für den jeweiligen Zweck tatsächlich Erforderliche
  - Aufbewahrungsdauer
- Praktisch umsetzbar

Privacy by Design



<u>These 4: Die technische Gestaltung von Systemen ist der mächtigste Faktor zur Durchsetzung des Datenschutzes.</u>

These 5: Die Umsetzung von Privacy by Design erfordert (eine Community von) „Privacy Engineers“ mit technischen Kenntnissen und Kenntnissen des Datenschutzes, die an der Gestaltung technischer Systeme von Beginn an beteiligt sind und Grundsätze des Datenschutzes individuell auf das konkret zu entwickelnde System umlegen.

- Im Datenschutz scheint retrospektive Regulierung besonders schlecht zu funktionieren:
  - Verstöße passieren meist im Verborgenen und sind schwer nachzuweisen
  - technische Expertise erforderlich
  - Durchsetzung schwierig
  - Wiedergutmachung häufig unmöglich
- Das menschliche Handeln wird nicht nur durch das Recht, sondern auch durch die Systeme selbst bestimmt und beschränkt – *Code is Law (Lessig)*
- Prospektive Regulierung: Durch die Gestaltung der Systeme können nicht intendierte Datenverwendungen auf faktischer Ebene ausgeschlossen werden
- Daher: Datenschutz in der Systementwicklung von Beginn an berücksichtigen

Privacy by Design

These 4: Die technische Gestaltung von Systemen ist der mächtigste Faktor zur Durchsetzung des Datenschutzes.

These 5: Die Umsetzung von Privacy by Design erfordert (eine Community von) „Privacy Engineers“ mit technischen Kenntnissen und Kenntnissen des Datenschutzes, die an der Gestaltung technischer Systeme von Beginn an beteiligt sind und Grundsätze des Datenschutzes individuell auf das konkret zu entwickelnde System umlegen.

- Kein 08/15-Standardprozess denkbar
- Umsetzung einiger weniger Grundprinzipien
  - von Beginn an
  - individuell auf das jeweilige System und dessen Zweck abgestimmt
  - durch Design-Strategien, Design Patterns und Privacy-enhancing Technologies (PETs)
  - unter Einbeziehung von Wissen über häufige Fehler, die Rechtslage, aktuelle Bedrohungen und Angriffsmethoden etc.
- Das PEFIM-Modell ist das Ergebnis eines solchen Vorgehens

Perspektiven des Identitätsmanagements auf Datenschutz und Datensicherheit

Dipl.-Ing. Dr. iur. Walter Hötzendorfer
Senior Researcher

Research Institute AG & Co KG
Zentrum für digitale Menschenrechte

E-Mail: walter.hoetzendorfer@researchinstitute.at
Web: http://www.researchinstitute.at