Prime

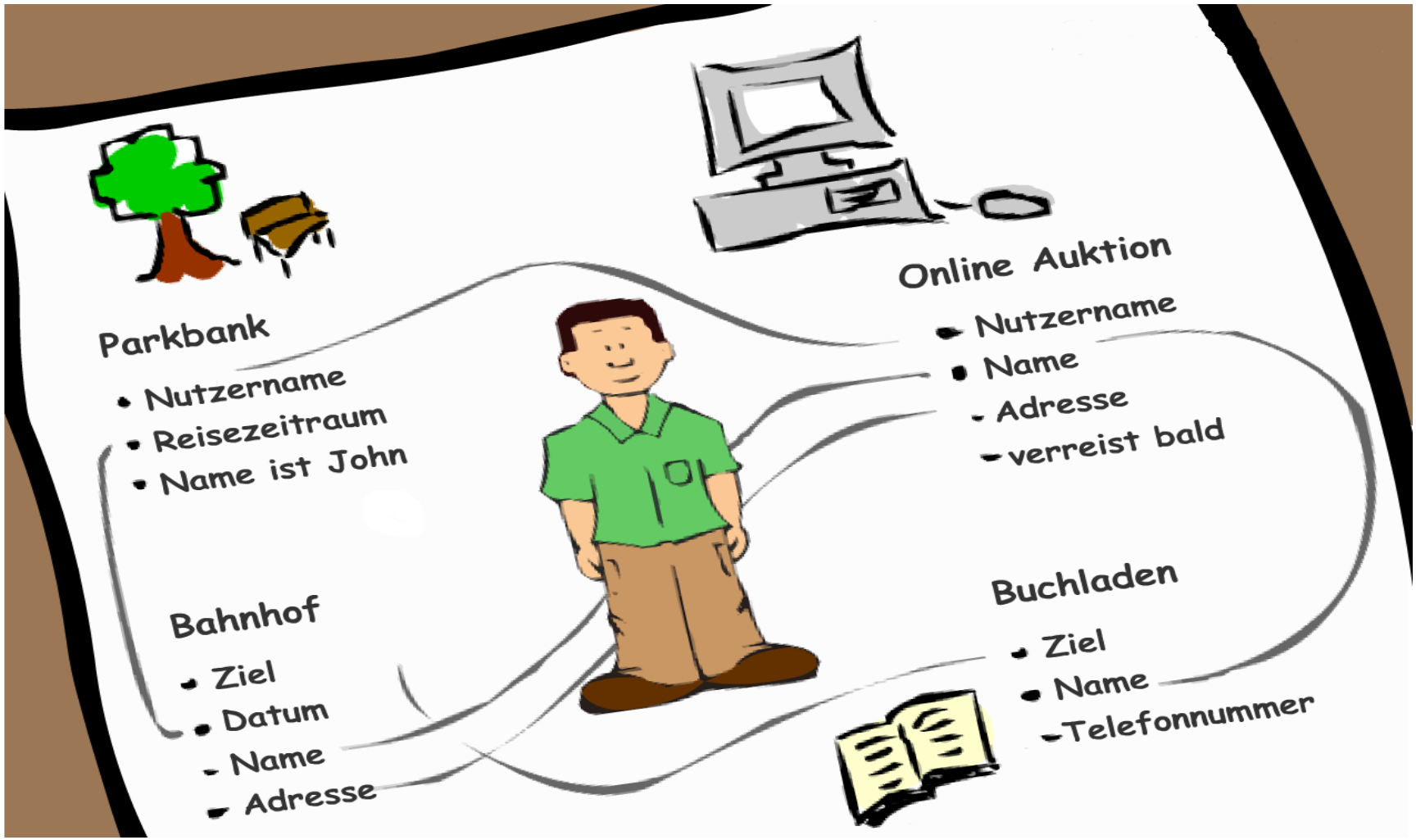
Privacy and Identity Management for Europe

Mathias Mosolf

Humboldt-Universität zu Berlin
Institut für Informatik

24. November 2009

John Primeur



Die Probleme sind...

- IP-Adressen reichen nicht aus, um Nutzer zu identifizieren

Die Probleme sind...

- IP-Adressen reichen nicht aus, um Nutzer zu identifizieren
- Jedes Unternehmen hat seine eigenen Methoden zur Identifikation der Nutzer entwickelt

Die Probleme sind...

- IP-Adressen reichen nicht aus, um Nutzer zu identifizieren
- Jedes Unternehmen hat seine eigenen Methoden zur Identifikation der Nutzer entwickelt
- Nutzer haben nur die Wahl die Bedingungen des Anbieters zu akzeptieren und alle Daten bereitzustellen

Die Probleme sind...

- IP-Adressen reichen nicht aus, um Nutzer zu identifizieren
- Jedes Unternehmen hat seine eigenen Methoden zur Identifikation der Nutzer entwickelt
- Nutzer haben nur die Wahl die Bedingungen des Anbieters zu akzeptieren und alle Daten bereitzustellen
- Mehr Daten gesammelt als nötig

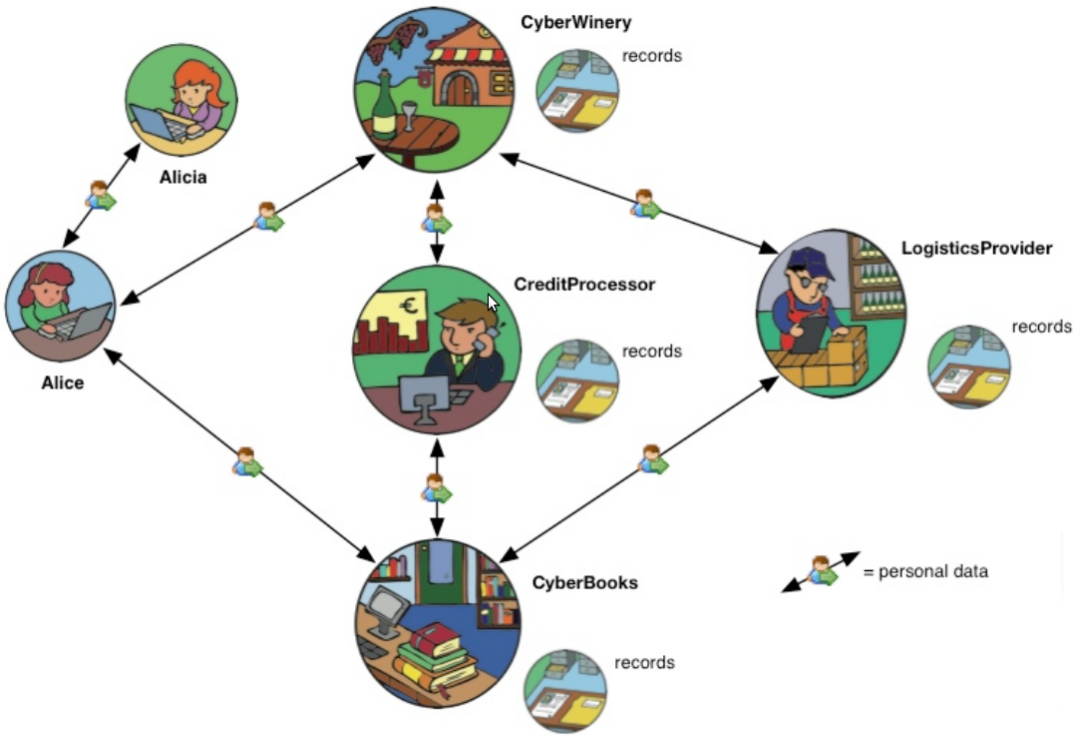
Die Probleme sind...

- IP-Adressen reichen nicht aus, um Nutzer zu identifizieren
- Jedes Unternehmen hat seine eigenen Methoden zur Identifikation der Nutzer entwickelt
- Nutzer haben nur die Wahl die Bedingungen des Anbieters zu akzeptieren und alle Daten bereitzustellen
- Mehr Daten gesammelt als nötig
- Verwendung gleicher Anmeldedaten für verschiedene Dienste

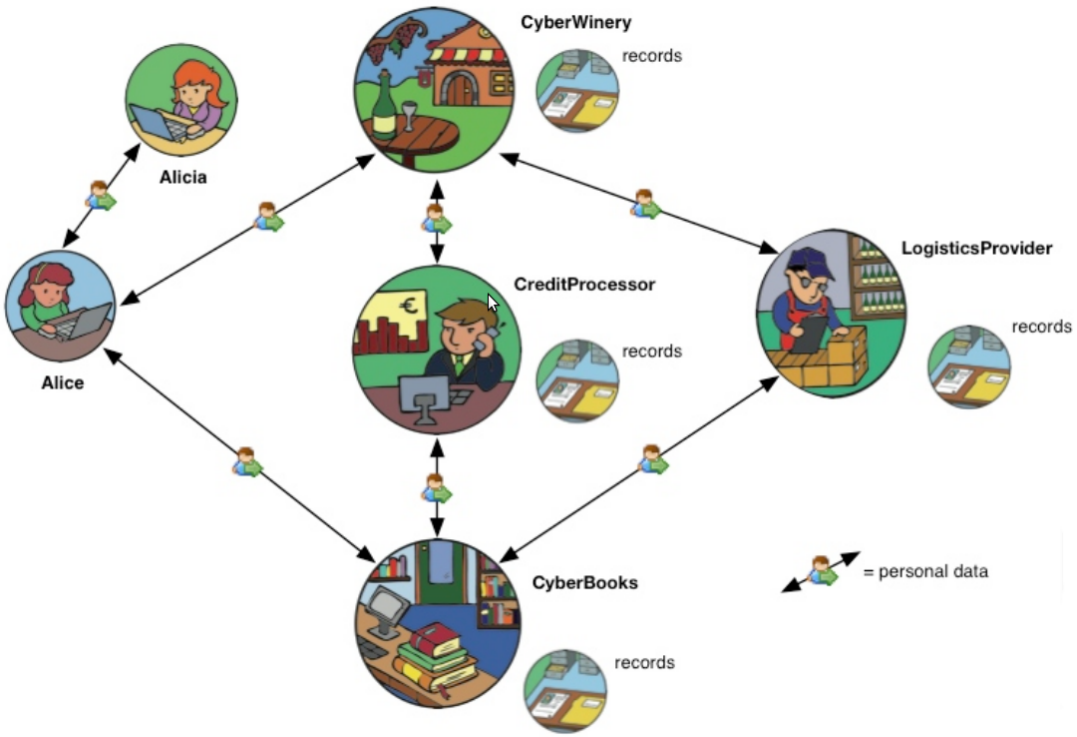
Die Probleme sind...

- IP-Adressen reichen nicht aus, um Nutzer zu identifizieren
- Jedes Unternehmen hat seine eigenen Methoden zur Identifikation der Nutzer entwickelt
- Nutzer haben nur die Wahl die Bedingungen des Anbieters zu akzeptieren und alle Daten bereitzustellen
- Mehr Daten gesammelt als nötig
- Verwendung gleicher Anmeldedaten für verschiedene Dienste
- Unsichere Passwörter

Einkaufen Heute



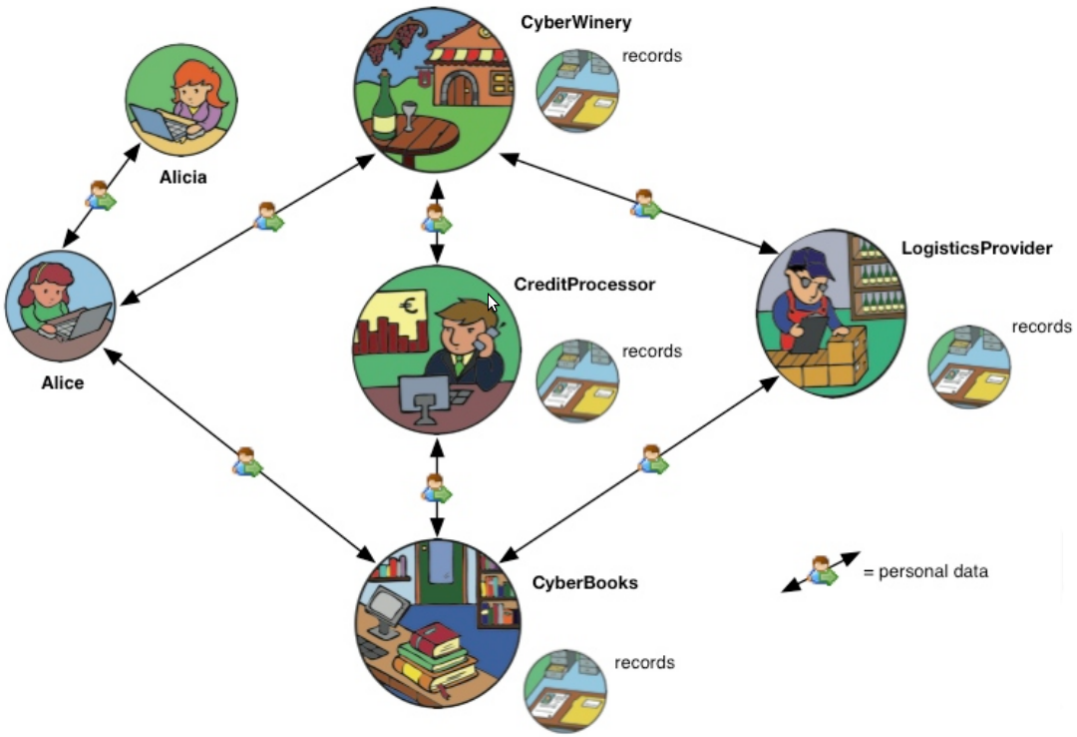
Einkaufen Heute



gespeicherte Daten

- Name
- Lieferadresse

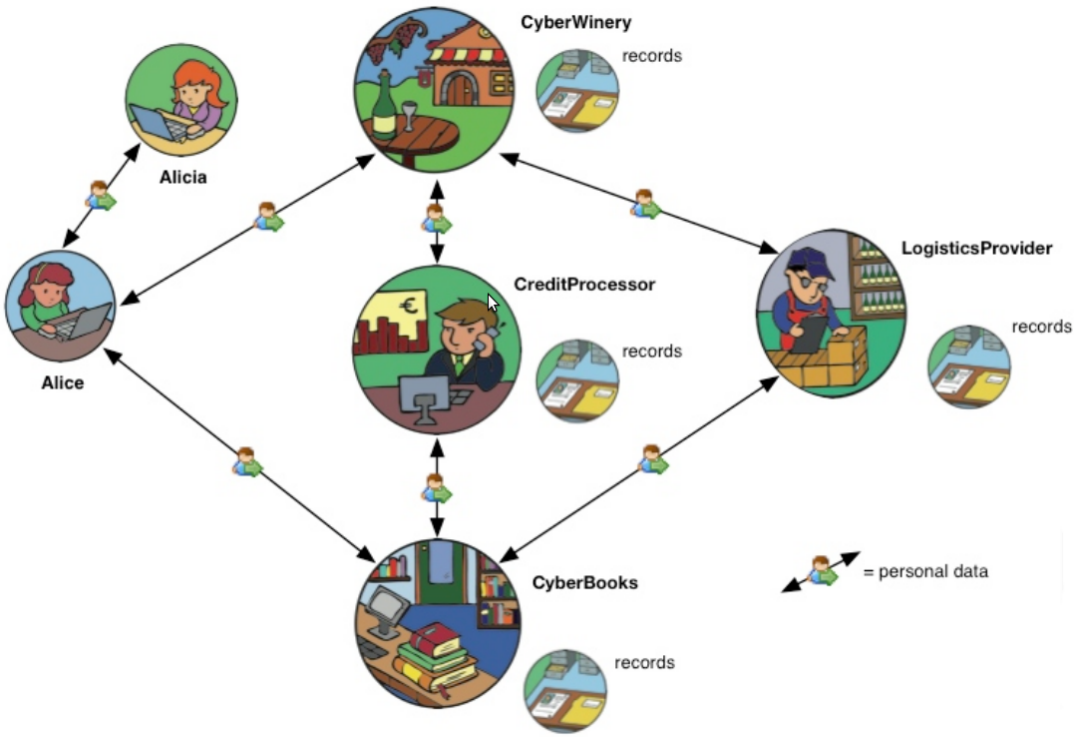
Einkaufen Heute



gespeicherte Daten

- Name
- Lieferadresse
- Kontodaten

Einkaufen Heute



gespeicherte Daten

- Name
- Lieferadresse
- Kontodaten
- Chronik der Bestellungen
- Bevorzugten Weinsorten

Wer weiß was über Alice

1. Die Bank

Wer weiß was über Alice

1. Die Bank
   - Die Shops in denen Alice bestellt hat
   - Wann Sie bestellt hat
   - Wie viel Sie bezahlt hat

Wer weiß was über Alice

1. Die Bank
   - Die Shops in denen Alice bestellt hat
   - Wann Sie bestellt hat
   - Wie viel Sie bezahlt hat
2. Der Paketdienst

Wer weiß was über Alice

1. Die Bank
   - Die Shops in denen Alice bestellt hat
   - Wann Sie bestellt hat
   - Wie viel Sie bezahlt hat
2. Der Paketdienst
   - Was Sie gekauft hat
   - Wo Sie gekauft hat

Wer weiß was über Alice

1. Die Bank
   - Die Shops in denen Alice bestellt hat
   - Wann Sie bestellt hat
   - Wie viel Sie bezahlt hat
2. Der Paketdienst
   - Was Sie gekauft hat
   - Wo Sie gekauft hat
3. Die Buchhandlung

Wer weiß was über Alice

1. Die Bank
   - Die Shops in denen Alice bestellt hat
   - Wann Sie bestellt hat
   - Wie viel Sie bezahlt hat
2. Der Paketdienst
   - Was Sie gekauft hat
   - Wo Sie gekauft hat
3. Die Buchhandlung
   - Welche Bücher Sie gekauft hat

PRIME Anforderungen

PRIME Anforderungen

1. Kontrolle und Einverständnis durch den Nutzer

PRIME Anforderungen

1. Kontrolle und Einverständnis durch den Nutzer
2. Berechtigung zur Datenverarbeitung

PRIME Anforderungen

1. Kontrolle und Einverständnis durch den Nutzer
2. Berechtigung zur Datenverarbeitung
3. Datenvermeidung

PRIME Anforderungen

1. Kontrolle und Einverständnis durch den Nutzer
2. Berechtigung zur Datenverarbeitung
3. Datenvermeidung
4. Eigene Datenschutzregeln durchsetzen

PRIME Anforderungen

1. Kontrolle und Einverständnis durch den Nutzer
2. Berechtigung zur Datenverarbeitung
3. Datenvermeidung
4. Eigene Datenschutzregeln durchsetzen
5. Verständlichkeit

PRIME Anforderungen

1. Kontrolle und Einverständnis durch den Nutzer
2. Berechtigung zur Datenverarbeitung
3. Datenvermeidung
4. Eigene Datenschutzregeln durchsetzen
5. Verständlichkeit
6. Mehrere Identitäten

Schritt 1: Vertrauen schaffen

1. Zertifizierung durch eine Behörde

Schritt 1: Vertrauen schaffen

1. Zertifizierung durch eine Behörde
2. Sichere Kommunikationsverbindung verwenden
3. Transparente Datenverarbeitung

Schritt 2: Maximale Privatsphäre

- Allgemeine Datenschutzrichtlinie veröffentlichen

Schritt 2: Maximale Privatsphäre

- Allgemeine Datenschutzrichtlinie veröffentlichen
  - Verfügbarkeit der Daten auf notwendige Bereiche beschränken
  - IP-Adressen nicht speichern

Schritt 2: Maximale Privatsphäre

- Allgemeine Datenschutzrichtlinie veröffentlichen
  - Verfügbarkeit der Daten auf notwendige Bereiche beschränken
  - IP-Adressen nicht speichern
- IP-Adresse verschleiern

Schritt 2: Maximale Privatsphäre

- Allgemeine Datenschutzrichtlinie veröffentlichen
  - Verfügbarkeit der Daten auf notwendige Bereiche beschränken
  - IP-Adressen nicht speichern
- IP-Adresse verschleiern
  - OnionCoffee in Prime integrierter Tor-client

Schritt 3: Die Bestellung

Pseudonymisierung

- Der Nutzer bestimmt welche Daten Übertragen werden

Schritt 3: Die Bestellung

Pseudonymisierung

- Der Nutzer bestimmt welche Daten Übertragen werden
- Kein Geburtsdatum sondern ein Zertifikat der Behörde

Schritt 3: Die Bestellung

Pseudonymisierung

- Der Nutzer bestimmt welche Daten Übertragen werden
- Kein Geburtsdatum sondern ein Zertifikat der Behörde
- Lieferadresse verschlüsselt

Schritt 3: Die Bestellung

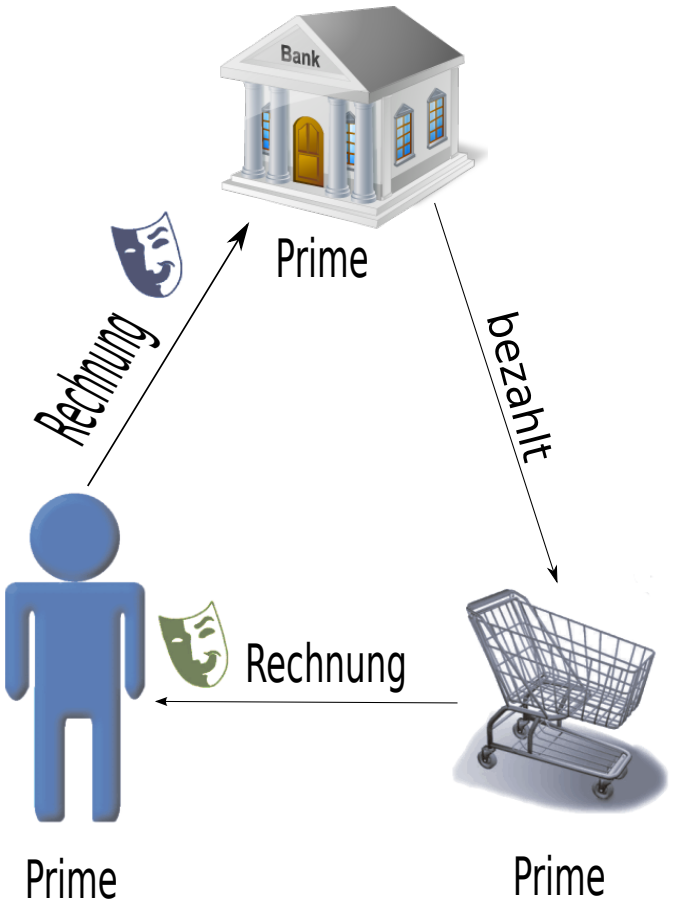
Pseudonymisierung

- Der Nutzer bestimmt welche Daten Übertragen werden
- Kein Geburtsdatum sondern ein Zertifikat der Behörde
- Lieferadresse verschlüsselt
- Wegwerf e-mail

Schritt 3: Die Bestellung

Pseudonymisierung

- Der Nutzer bestimmt welche Daten Übertragen werden
- Kein Geburtsdatum sondern ein Zertifikat der Behörde
- Lieferadresse verschlüsselt
- Wegwerf e-mail
- Anderes Pseudonym für Bezahlung
  1. eCoins
  2. Kreditkarte


Bank
Prime
Rechnung
bezahlt
Rechnung
Prime
Prime

Schritt 4: Nach dem Einkauf

1. Prime speichert: Wer? Wann? Was? Warum? Welches Pseudonym?

Schritt 4: Nach dem Einkauf

1. Prime speichert: Wer? Wann? Was? Warum? Welches Pseudonym?
2. Prime ermöglicht: Auskunft, Änderung, Sperrung und Löschung der Daten

Schritt 4: Nach dem Einkauf

1. Prime speichert: Wer? Wann? Was? Warum? Welches Pseudonym?
2. Prime ermöglicht: Auskunft, Änderung, Sperrung und Löschung der Daten
3. Vertragsbruch: Herausgabe der Identität durch die Behörde

Schritt 5: Stammkunde werden

- Aufgrund früherer Besuche kann der Shop Kaufempfehlungen geben

Schritt 5: Stammkunde werden

- Aufgrund früherer Besuche kann der Shop Kaufempfehlungen geben
- Gefahr: Verknüpfung früherer Besuche mit Daten von Bank und Lieferdienst

Schritt 5: Stammkunde werden

- Aufgrund früherer Besuche kann der Shop Kaufempfehlungen geben
- Gefahr: Verknüpfung früherer Besuche mit Daten von Bank und Lieferdienst
- Folge: detailliertes Bild über Kaufverhalten, Budget, Trinkgewohnheiten

Schritt 5: Stammkunde werden

- Aufgrund früherer Besuche kann der Shop Kaufempfehlungen geben
- Gefahr: Verknüpfung früherer Besuche mit Daten von Bank und Lieferdienst
- Folge: detailliertes Bild über Kaufverhalten, Budget, Trinkgewohnheiten
- Lösung: Verwendung mehrerer Pseudonyme
  1. Zum durchsuchen des Angebots und auswählen von Wein
  2. Für die Bestellung
  3. Für die Bank zur Bezahlung

Quellen

http://blues.inf.tu-dresden.de/prime/EUT_Tutorial_V0/movie/prime.swf
https://www.prime-project.eu/prime_products/whitepaper/PRIME-Whitepaper-V3.pdf
https://www.prime-project.eu/prime_products/reports/fmwk/pub_del_D14.1.c_ec_wp14.1_v1_final.pdf
https://www.prime-project.eu/prototypes/anon/index_html
https://www.prime-project.eu/prime_products/presentations/Presentation-PRIME-ICPP-20041203.ppt
http://en.wikipedia.org/wiki/File:European_flag.svg
http://www.iconspedia.com/uploads/326772979191712760.png

Fragen?