SOCIAL CRM RESEARCH CENTER

PRIVACY EXPERIENCE MANAGEMENT

Potenziale zur Erhöhung der Selbstbestimmtheit im Datenmanagement

Jürgen Anke	Hochschule für Technik und Wirtschaft Dresden
Gunnar Hempel	Social CRM Research Center Leipzig e. V
Olaf Reinhold	Social CRM Research Center Leipzig e. V.

© Social CRM Research Center e.V.

AGENDA

1. Problemraum datengetriebene Services
2. Herausforderungen und Hypothesen
3. SSI als technischer Ansatz für ein Privacy Experience Management
4. Hypothesen zum Privacy Experience Management

© Social CRM Research Center e.V.

CRM

Customer Relationship Management

CRM stellvertretend für zahlreiche Anwendungsbereiche datengetriebener Services

Beispiele

- E-Commerce
- Mobility-Services
- Financing

Fokus Verarbeitung von Nutzerdaten für Serviceangebote und Wertschöpfung

© Social CRM Research Center e.V.

Problemraum

CRM Herausforderungen - Unternehmensseitig

- Verarbeitung von Nutzerdaten über den „erforderlichen“ Rahmen hinaus kann Mehrwerte für beide Parteien schaffen
- Legitime und berechtigte Interessen beider Parteien sind abzugrenzen von einem „Datenrausch“
- Kosten für Datenschutz und Datensicherheit
- Kosten schlechter Datenqualität

© Social CRM Research Center e.V.

Problemraum

CRM Herausforderungen - Nutzerseitig

- Anwenderfreundlichkeit und sichtbare Mehrwerte
- Transparenz
- Informationelle Selbstbestimmung im Hinblick auf die Datenverarbeitung
- Maßnahmen für Datenschutz und Datensicherheit

© Social CRM Research Center e.V.

Generelle Ziele der Beteiligten

Nutzer

- Einfacher Zugang zu digitalen Diensten ohne aufwändige Einwilligungsprozesse und intransparente Datenanforderungen
- Selbstbestimmt über die Verarbeitung ihre Daten entscheiden

Unternehmen

- Kundenorientierte Gestaltung von Services und Wertschöpfung anhand personenbezogener Daten
- Minimieren von Fixkosten und Risikokosten

Gesetzgeber

- Schutz von Personen
- Missbrauch und Ungleichgewichte bzgl. personenbezogener Daten vermeiden

© Social CRM Research Center e.V.

Grundlegende Handlungsoptionen

Maximierung Datenbestand bei Unternehmen

Das Unternehmen erhält und verwaltet alle benötigten Daten. Damit liegen die genannten Risiken beim Unternehmen.

Minimierung der Offenlegung durch Kunden

Nutzer verweigert die Bereitstellung von Daten. Damit ist der Nutzer auf anonym nutzbare Angebote und Dienste beschränkt.

Optimierung des Verhältnisses von Datenbereitstellung und Wertschöpfung

Das Unternehmen bietet Dienste bedarfsorientiert an. Über einen minimalen (erforderlichen) Datenbedarf hinaus kann eine Mehrwertschöpfung mit selektivem und anlassbezogenem Datenbedarf transparent erfolgen

© Social CRM Research Center e.V.

Hypothesen

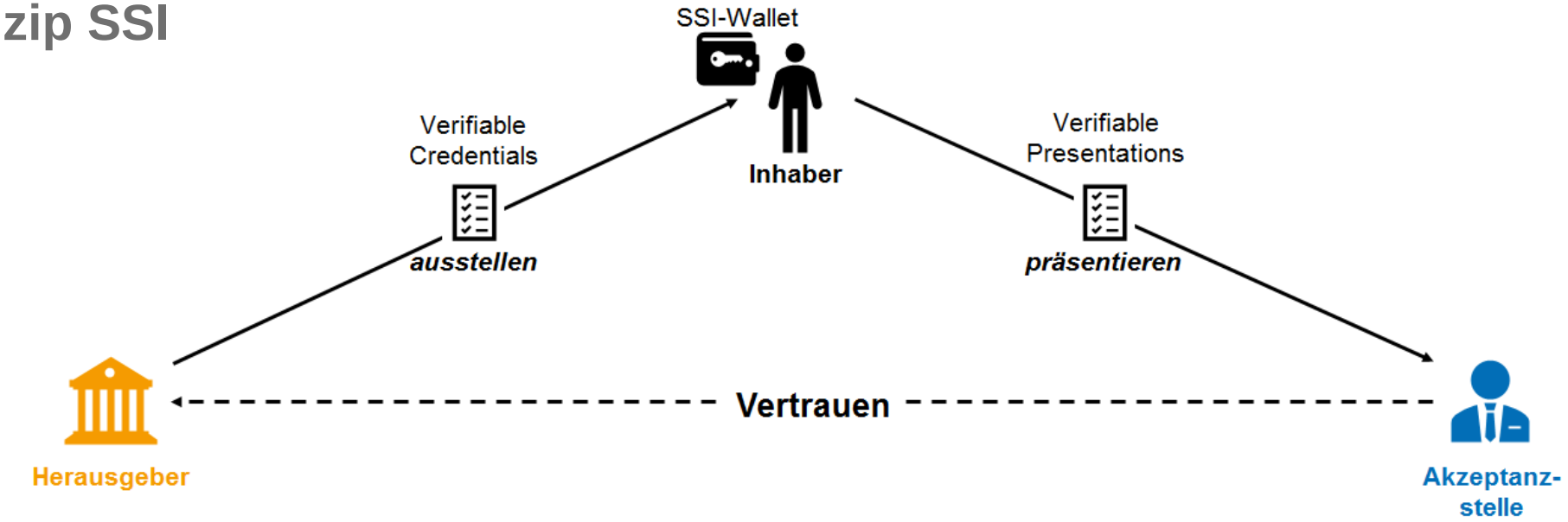
Hypothesen für ein Privacy Experience Management

- Machtgefälle ausgleichen - beide Parteien müssen bereit sein sich für eine Reorganisation von Prozessen einzulassen
- Anwenderfreundliche Tools um Selbstbestimmung überhaupt wahrnehmen zu können (beide Parteien)
- Toolnutzung muss Mehrwert bieten

© Social CRM Research Center e.V.

Self-Sovereign Identity

Das Prinzip SSI



Implikationen

- Nutzer besitzen eigenen Speicher und Verfügungsmacht über ihre Daten
- Daten haben nachvollziehbare Herkunft und Qualität
- Akzeptanzstelle braucht keine Integration mit Herausgeber
- Freigegebene Daten durch Historie nachvollziehbar

© Social CRM Research Center e.V.

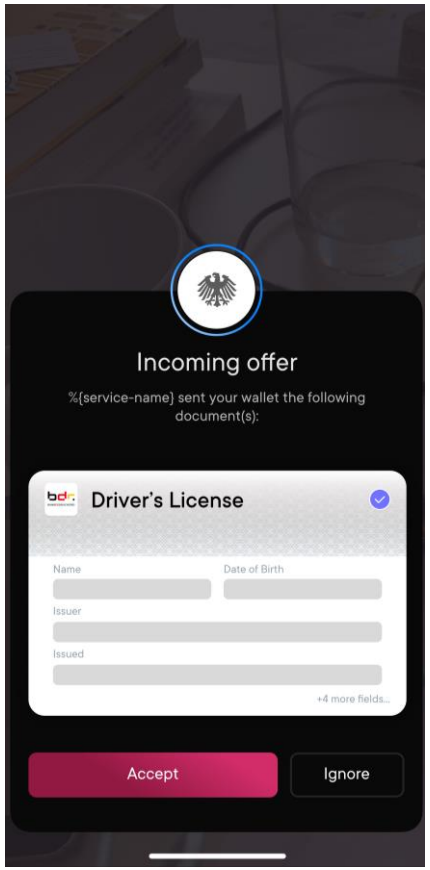
SSI-Prinzipien nach Christopher Allen (2016)

- **Existence.** *Users must have an independent existence.*
- **Control.** *Users must control their identities.*
- **Access.** *Users must have access to their own data.* A user must always be able to easily retrieve all the claims and other data within his identity. There must be no hidden data and no gatekeepers. This does not mean that a user can necessarily modify all the claims associated with his identity, but it does mean they should be aware of them. It also does not mean that users have equal access to others' data, only to their own.
- **Transparency**. *Systems and algorithms must be transparent.*
- **Persistence.** *Identities must be long-lived.*
- **Portability.** *Information and services about identity must be transportable.*
- **Interoperability.** *Identities should be as widely usable as possible.*
- **Consent.** *Users must agree to the use of their identity.* Any identity system is built around sharing that identity and its claims, and an interoperable system increases the amount of sharing that occurs. However, sharing of data must only occur with the consent of the user. Though other users such as an employer, a credit bureau, or a friend might present claims, the user must still offer consent for them to become valid. Note that this consent might not be interactive, but it must still be deliberate and well-understood.
- **Minimalization.** *Disclosure of claims must be minimized.* When data is disclosed, that disclosure should involve the minimum amount of data necessary to accomplish the task at hand. For example, if only a minimum age is called for, then the exact age should not be disclosed, and if only an age is requested, then the more precise date of birth should not be disclosed. This principle can be supported with selective disclosure, range proofs, and other zero-knowledge techniques, but non-correlatibility is still a very hard (perhaps impossible) task; the best we can do is to use minimalization to support privacy as best as possible.
- **Protection.** *The rights of users must be protected.*

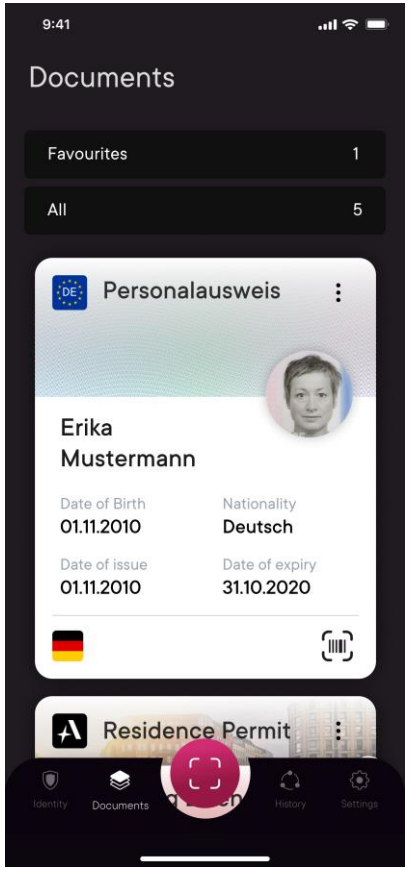
© Social CRM Research Center e.V.

Interaktionen mit SSI-Wallets

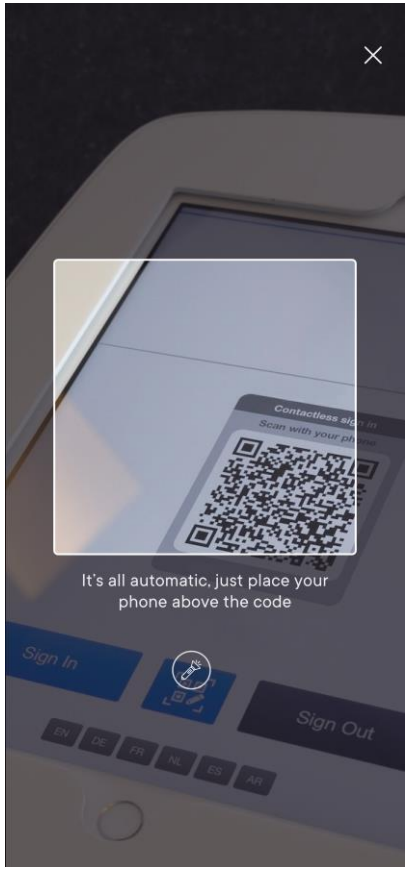
Neuen Nachweis annehmen



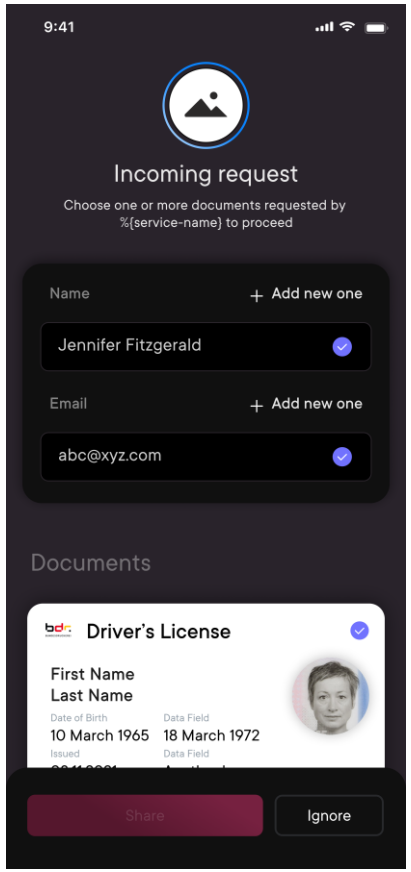
Nachweise verwalten



Mit Anfrager verbinden



Daten/Nachweise freigeben



© Social CRM Research Center e.V.

Potentielle Auswirkungen der Technik

Gestaltungsspielräume im Datenmanagement durch SSI

- Datenerhebung durch anlassbezogene Abfrage an Wallet des Kunden (statt durch Webformulare)
- Abfrage kann datenminiert werden (selektive Freigabe und "Zero Knowledge Proofs")
- Etablierung eines gesicherten Peer-to-Peer Kommunikationskanals zum Kunden

Erweiterungen von SSI-Technologie für besseres Privacy-Management

- Wallets: Widerruf-Funktion in der Historie über geteilte Daten
- Benachrichtigungen über Nutzung und Löschung geteilter Daten
- Verifizierung von Anfragern durch Vertrauensbeziehungen zu Dritten, z.B. Trust Lists
- Warnung bei Anfragen, die identifizierende Merkmale enthalten

© Social CRM Research Center e.V.

Hypothesen zu Auswirkungen des Privacy Experience Management

- Unternehmen speichert bestimmte Daten nicht mehr, sondern ersetzt diese durch Abfragen gegen eine Wallet.
- Nutzer schöpfen Spielräume im Sinne einer selbstdefinierten Privacy Policy für individuelle Gestaltung ihrer Privatsphäre aus, sobald entsprechende Werkzeuge und Mehrwerte verfügbar sind.
- Vertrauenswürdige Unternehmen erhalten Daten „on-demand“ und bis auf Widerruf. Nutzer müssen nicht jede Anfrage individuell bestätigen.
- Kosten für datenschutzkonformen Umgang mit personenbezogenen Daten sowie für Datenqualitätsmanagement sinken.
- Unternehmen nutzen Möglichkeiten zur Datenminimierung, wenn ihre Wertschöpfung und Kosten dadurch nicht beeinträchtigt werden.
- Datenschutzfreundliche Angebote werden stärker nachgefragt

© Social CRM Research Center e.V.

Kontakt

Prof. Dr.-Ing. Jürgen Anke Hochschule für Technik und Wirtschaft Dresden
juergen.anke@htw-dresden.de

Dr. Gunnar Hempel Social CRM Research Center Leipzig e. V.
gunnar.hempel@scrc-leipzig.de

© Social CRM Research Center e.V.