D.3 AlterEgo für Consent Management

Beteiligte: Michael Waidner, Marc Fischlin, Joachim Vogt

Motivation

Informierte Einwilligung –
Ein Grundprinzip des Datenschutzrechts

Schwächen existierender technischer Konzepte

1. Zum Teil rechtskonform aber ineffektiv
   - Falsche Annahme: IT-Nutzer sind stets rational handelnde Akteure
   - Unzureichende Transparenz & Kontrollmöglichkeiten
   - Überforderung der Betroffenen bei der Wahrnehmung ihrer Rechte
   - Ausdifferenzierte Entscheidungen und nachträglicher Widerspruch oft nur sehr eingeschränkt möglich

2. Angesicht aktueller IT-Entwicklungen nicht nur ineffektiv, sondern überhaupt nicht mehr anwendbar
   - Existierende Mechanismen zu statisch und schwerfällig

Idee: Datenschutzhinweise „intelligent“ machen;
automatisierte kontextsensitive Einwilligungsentscheidungen ermöglichen

Stand der Forschung

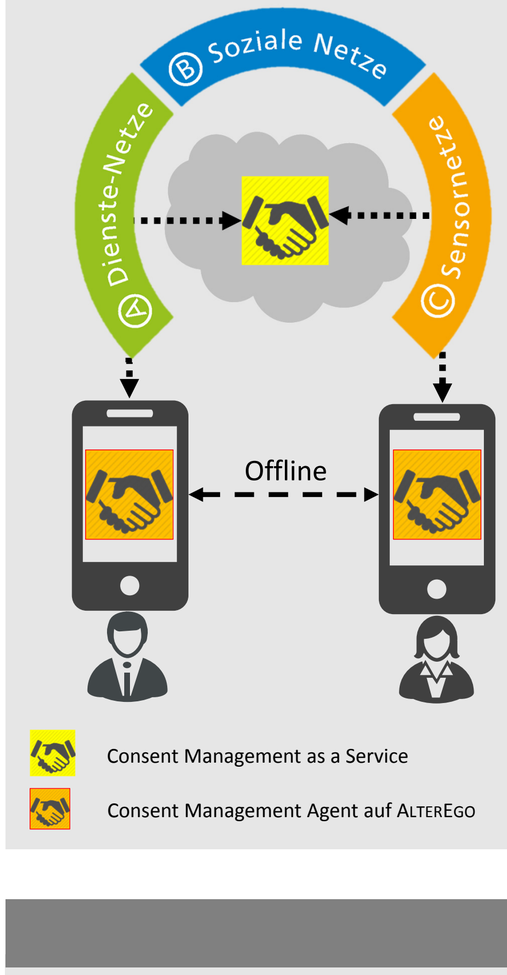
Stand der Wissenschaft – ausgewählt

- **Dynamic Privacy Adaptation in Ubiquitous Computing:** Florian Schaub. Dynamic Privacy Adaptation in Ubiquitous Computing Doctoral dissertation, Universität Ulm. (2014).
- **Rücknahme von Einwilligung**: Mont, M. C. ; Pearson, S. ; Kounga, G. ; Shen, Y. ; Bramhall, P. : On the Management of Consent and Revocation in Enterprises: Setting the Context. In: HP Laboratories, Technical Report HPL-2009-49. (2009).
- **Efficiency-Thoroughness Trade-Off:** Hollnagel, E. : The ETTO principle: efficiency-thoroughness trade-off: why things that go right sometimes go wrong. Ashgate. (2009).

Eigene Vorarbeiten – ausgewählt

- **Consent Management in verteilten Umgebungen:** Schunter, M. ;Waidner, M. : Simplified privacy controls for aggregated services—suspend and resume of personal data. In: Privacy Enhancing Technologies Springer. (2007).
- **Transparenz und Automatisierung von Consent:** Buchmann, J. ; Nebel, M. ; Roßnagel, A. ; Shirazi, F. ; Simo, H. ; Waidner, M. : Personal Information Dashboard: Putting the Individual Back in Control. In: M. H. et al., (Hrsg.): Digital Enlightenment Yearbook 2013. (2013).
- **Erforschung des Verhaltens komplexer Systeme:** Stolte, W. ; Vogt, J. ; Weber, C. : Controlling Practical Drift in High Reliability Organizations. In: International Journal of Applied Aviation Studies 10. (2010).
- **Fortgeschrittene kryptographische Verschlüsselungsverfahren:** Brzuska, C. ; Fischlin, M. ; Freudenreich, T. ; Lehmann, A. ; Page, M. ; Schelbert, J. ; Schröder, D. ; Volk, F. : Security of Sanitizable Signatures Revisited. In: Public Key Cryptography Bd. 5443, Springer. (2009).

Hauptziele und wissenschaftliche Vorgehensweise



(1) Agentbasiertes Consent Management

- „On-the-fly” und kontext-adaptive Einwilligung
- Kollaboratives Datenschutzmanagement
- Dynamisches Widerrufen von Einwilligung

(2) Informierte Einwilligung unterstützen

- Nachvollziehbarkeit der Datenzugriffe
- Nachvollziehbarkeit der Risiken/Konsequenzen

(3) Benutzbar, laientauglich, nachvollziehbar vertrauenswürdig

- Minimaler Aufwand/Overhead
- Intelligente Benutzerschnittstellen
- Automatisierung vs. menschliches Eingreifen

Wissenschaftliche Vorgehensweise:

Kontinuierliche Evaluation

(1) Festlegung Anwendungsszenarien und Anforderungsanalyse
- Nutzeranforderungen
- Rechtliche Anforderungen
- Technische Rahmenbedingungen

(2) Intelligente Datenschutzhinweise
- Erforschung von Techniken zur automatisierten Extraktion und Analyse relevanter Merkmale in Datenschutzmitteilungen
- Erweiterung bestehender Konzepte zur benutzerfreundlichen Darstellung von Datenschutzhinweisen

(3) Automatisierte, kontext-adaptive Einwilligungsentscheidungen
- Ansätze zur Kontextmodellierung und -interpretation
- Methoden zur kontext-abhängigen Aushandlung und Herleitung bzw. Verfeinerung von Nutzerentscheidungen

(4) Domänen- und plattformübergreifendes Management
- Erweiterung des Sticky-Policies-Paradigma
- Dynamische Durchsetzung und Revokation

(5) Proof-of-Concept-Prototyp

Kontinuierliche Evaluation

Vernetzung

Innerhalb des GRK

Anwendungsszenarien Anforderungsanalyse	A
Anwendungsszenarien Anforderungsanalyse	B
Anwendungsszenarien Anforderungsanalyse	C
Nutzeranforderungen Evaluierung der Praktikabilität und Benutzbarkeit	D.1 AlterEgo für Vertrauensbewertung
Verknüpfung mit Vertrauensankern	D.2 AlterEgo als Vertrauensquelle
Architekturmodelle Aufbau der Prototypen	D.4 AlterEgo als Massengerät

In D.3: AlterEgo für Consent Management

Promotionsthema:
End-to-End and Context-Adaptive Consent Management in Emerging Mobile and Pervasive Computing Systems

Betreuer:
Professor Dr. **Michael Waidner**

Tandem:
Informatik - Usability

Externer Doktorand:
On Transparency and Privacy Self-Management in Context-Aware Distributed Service Environments

Außerhalb des GRK

- (Neu-)Bestimmung und Gewährleistung informationeller Selbstbestimmung
- Nutzung sicherer Kryptobausteine aus TP P1, P2 und S4.
- Enge Forschungskooperation mit IBM Research - Zürich, CH
- Kollaboration mit den Arbeitsbereiche Blueprint und Engineering