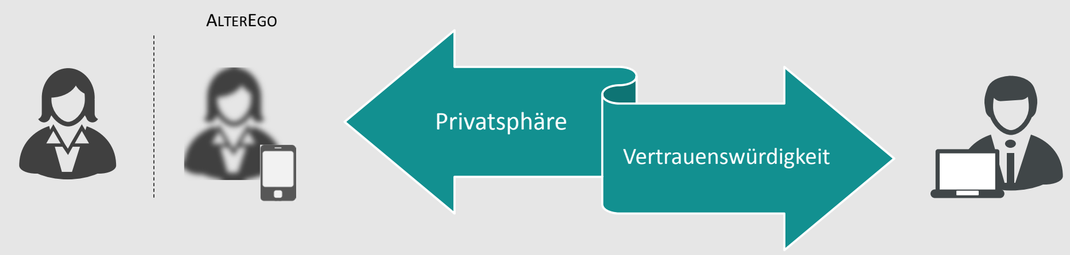
D.2 AlterEgo als Vertrauensquelle

Beteiligte: Marc Fischlin, Joachim Vogt, Melanie Volkamer, Michael Waidner

Motivation

Vermeintlich gegensätzliche Sicherheitsanforderungen



Unzulänglichkeiten bisheriger Lösungen

- ✖ Kryptographie: AlterEgo nicht einfach übertragbar
- ✖ Hardware: Manipulationsmöglichkeiten des AlterEgo
- ✖ Usability: mangelndes Verständnis
- ✖ Infrastruktur: unsichere Zertifizierungsinstanzen

Idee: Bootstrapping mit elektronischen Ausweisen wie nPA, Erweiterung von Ansätzen im Bereich *attribute-based credentials*

Stand der Forschung

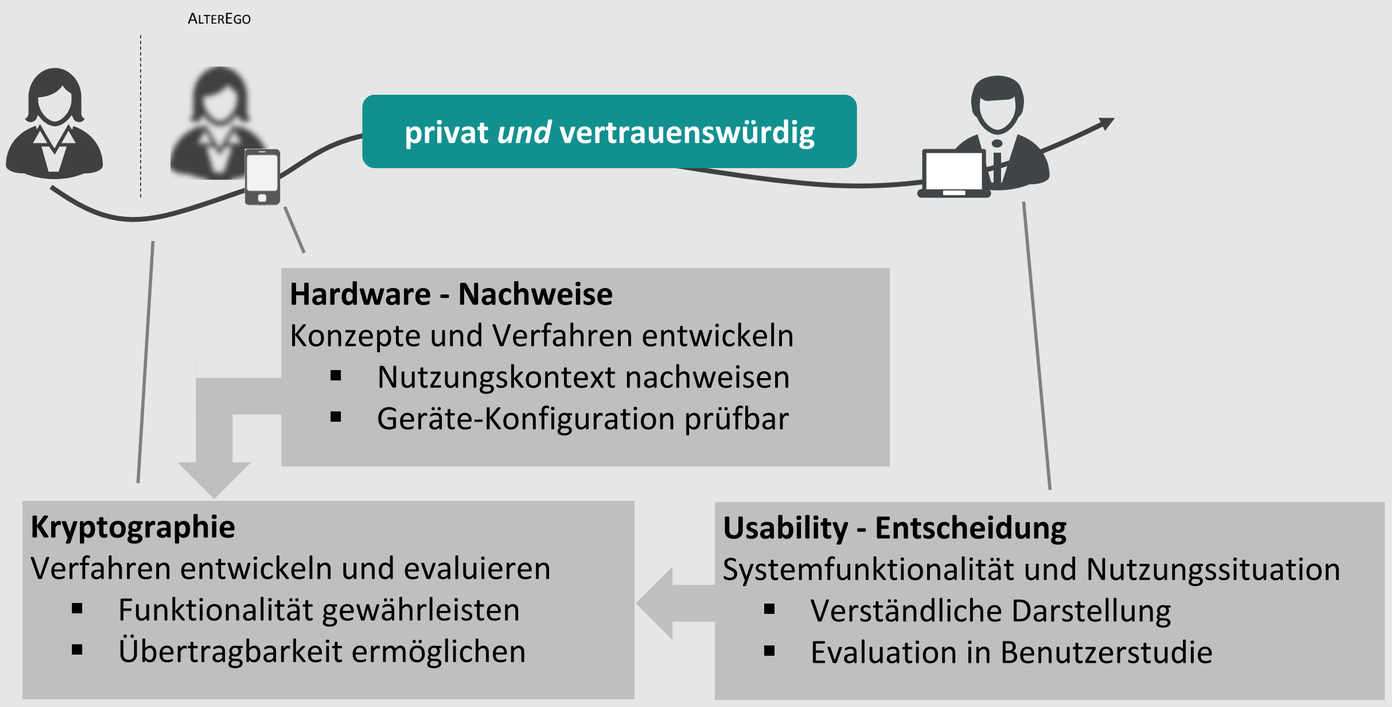
Stand der Wissenschaft – ausgewählt

- **Credential-Systeme U-Prove und Idemix:** J.Camenisch und A.Lysanskaya. “An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation”. In: Eurocrypt. (2001).
- **Reduktion der Vertrauenswürdigkeit von CAs durch öffentliche Verzeichnisse:** S.Bechtold, A.Perrig: Accountability in future internet architectures. In: Commun. ACM 57 (2014)
- **Intelligente Entscheidungen trotz Unsicherheit:** D.Evans: “Risk Intelligence: How to Live with Uncertainty”. Free Press Simon and Schuster, 2012

Eigene Vorarbeiten – ausgewählt

- **Anonymität für Personalausweis:** J.Bender, Ö.Dagdelen, M.Fischlin, D.Kügler: Domain-Specific Pseudonymous Signatures for the German Identity Card. In: Information Security Conference (2012).
- **Reaktion von Anwendern auf Warnmeldungen:** N.Kolb, S.Bartsch, M.Volkamer, J.Vogt: Capturing Attention for Warnings about Insecure Password Fields - Systematic Development of a Passive Security Intervention. In: 16th International Conference on Human-Computer Interaction (2014).
- **Vertrauenswürdigkeit von Smartphones:** Fraunhofer SIT. “BizzTrust for Android - Schutz von sensitiven Daten und Diensten”. (2012).

Hauptziele und wissenschaftliche Vorgehensweise



wissenschaftliche Vorgehensweise:

- Bereich Kryptographie
  - Verbinde Verfahren neuer Personalausweis (nPA) mit mobilem Gerät
  - Erweitere Funktionalität der nPA-Verfahren
  - Beachte Möglichkeit des Verlusts des mobile Geräts
- Bereich Hardware - Nachweise
  - Konzepte und Methoden aus anderen Projekten (BizzTrust, Key2Share) übertragen, z.B. Compartments und Remote Maintenance
  - Betrachte Szenarien Gerät-zu-Gerät und Gerät-zu-Dienstleister
- Bereich Usability - Entscheidung
  - Systemfunktionalität und Nutzungssituation verständlich darstellen
  - Darstellung evaluieren

Vernetzung

Innerhalb des GRK

Entwurf von privat-sphärenerhaltenden Verfahren	**A.1** Nutzer-Ermächtigung und Dienst-Nutzung
Nutzung der Bereitschaft zur Datenpreisgabe	**A.2** Nutzersensibilisierung Privatheit & Vertrauen
Alternative Vertrauensanker in sozialen Netzwerken	**B.1** Vertauensbewertung in Sozialen Netzen
Nutzung des AlterEgo als Vertrauensanker	**C** Privatheitsschutz in der Sensorik
Mentale Modelle der Nutzer und Risikokommunikation	**D.1** AlterEgo für Vertrauensbewertung
Anwendung und Einbettung von Vertrauensankern	**D.3 und D.4** AlterEgo für Consent-Mngm/als Massengerät

In D.2: AlterEgo als Vertrauensquelle

Promotionsthema:
Transfer und Erweiterung der Mechanismen des Vertrauensankers nPA auf mobile Geräte

Betreuer:
Professor Dr. **Marc Fischlin**

Tandem:
Informatik - Usability

Externer Doktorand:
Sanitizable Signatures

Außerhalb des GRK

DFG CROSSING — Nutzung sicherer Kryptobausteine aus TP P1, P2, S1

Bundesamt für Sicherheit in der Informationstechnik — Projekte über nPA-Verfahren