h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

Ausweis-Projekte an Hochschulen

Marian Margraf

Hochschule Darmstadt

13.03.2014

Aktivitäten an Hochschulen (Auswahl)

h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

- **TU Darmstadt**, M. Horsch: Mobile Authentisierung mit dem neuen Personalausweis.
- **Uni Koblenz-Landau**, Ch. Merz: Implementierung der grundlegenden Funktionen einer Serveranwendung für die eID-Authentifikation des neuen Personalausweises.
- **Uni Jena**, R. Wondratschek: Framework zur Nutzung des neuen Personalausweises in nativen Android Apps.
- **HU Berlin**, F. Morgner: Mobiler Chipkartenleser für den neuen Personalausweis.
- **FH Gelsenkirchen**, S. Feld: Sicherheitsanalyse eines OpenID-Providers mit Proxy-Funktionalität für den neuen Personalausweis.
- **Hochschule Darmstadt**
  - AG Massoth: SECCO - Secure Call Authentication.
  - AG Margraf: Ad-hoc Schlüsselaustausch auf Basis der Online-Ausweisfunktion.

Open Source Projekte (Auswahl)

- CASED: PersoApp
- ecsec GmbH: Open eCard Team
- FhG FOKUS: Open eID
- BeID-lab (BDr, HU Berlin): eIDClientCore
- bos: AutentApp

Aufbau einer Community

- Unterstützung des PersoApp-Projekts durch praxisnahe Forschung und Entwicklung
- Begleitung der Forschung und Entwicklung durch Lehrveranstaltungen
  - Bachelor- und Masterarbeiten
  - Projekt Systementwicklung
  - Praxisphasen
- Hierfür notwendig: Neue Anwendungsfälle mit Forschungspotenzial
  - Ad-hoc Schlüsselaustausch
  - Secure Call Authentication

Online-Ausweisfunktion

Funktionalität der Online-Ausweisfunktion:

- Gegenseitige Authentisierung zweier Kommunikationspartner
  - Partner 1: Ausweisinhaber
  - Partner 2: Diensteanbieter (z.B. Bürgeramt, Bank, Versicherung)

Nicht enthalten:

- Authentisierung zwischen zwei Ausweisinhabern
- Signatur von Dokumenten
- Verschlüsselung von Dokumenten

Kryptographische Verfahren

Kryptographische Verfahren basieren auf Authentisierung:

Eingesetzte Schlüssel müssen dem Kommunikationspartner zugeordnet werden können

- Wer kann die verschlüsselten Daten entschlüsseln?
- Wer authentisiert sich mir gegenüber?
- Wessen öffentlichen Schlüssel nutze ich, um ein Dokument zu verifizieren?

Gleiches gilt für Schlüsseleinigungs-, Schlüsselaustauschprotokolle:

- Mit wem vereinbare ich einen gemeinsamen Sitzungsschlüssel?

Ausweisfunktion als Sicherheitsanker

- Beispiel 1: Qualifizierte elektronische Signatur
  - Online-Ausweisfunktion zur Beantragung von qualifizierten Zertifikaten
  - Bindung zwischen öffentlichem Schlüssel und Schlüsselinhaber
- Beispiel 2: DE-Mail
  - Online-Ausweisfunktion zur initialen Anmeldung
  - Bindung zwischen DE-Mailadresse und Adressinhaber
- Beispiel 3: Bank
  - Online-Ausweisfunktion zur Bankkontoeröffnung
  - Bindung zwischen Kontodaten und Kontoinhaber

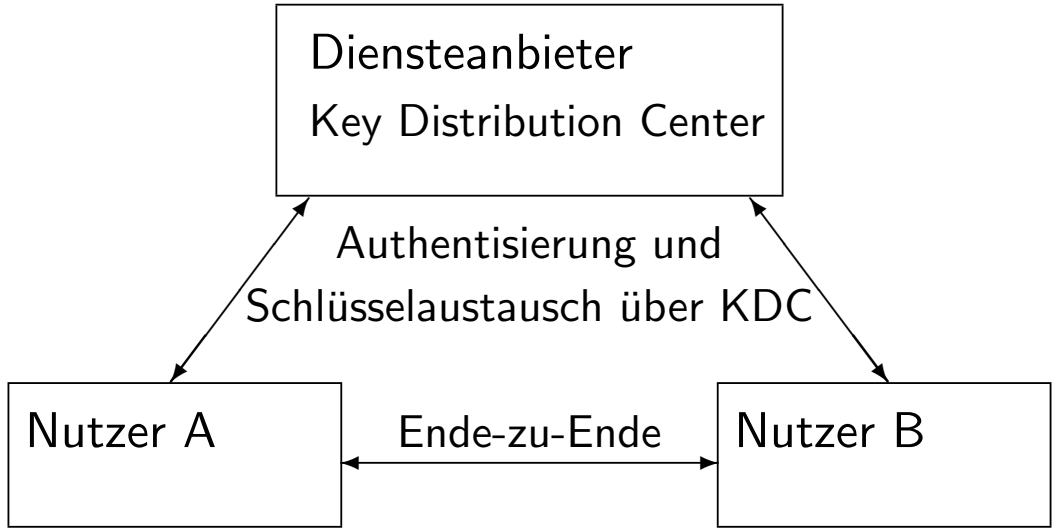
Idee aller drei Lösungen:

- Nutzung der Online-Ausweisfunktion für die initiale Registrierung
- Danach arbeiten in der eigenen Infrastruktur

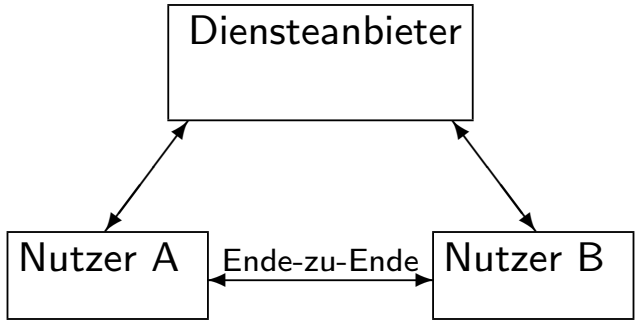
Ad-hoc Schlüsselaustausch I

Idee: Sichere Kommunikation ohne vorherige Registrierung, Zertifikatsaustausch, ...

- Ende-zu-Ende Verschlüsselung
- Ende-zu-Ende Authentisierung
- Schutz der Metadaten



Ad-hoc Schlüsselaustausch II



A möchte B eine vertrauliche Nachricht D senden:

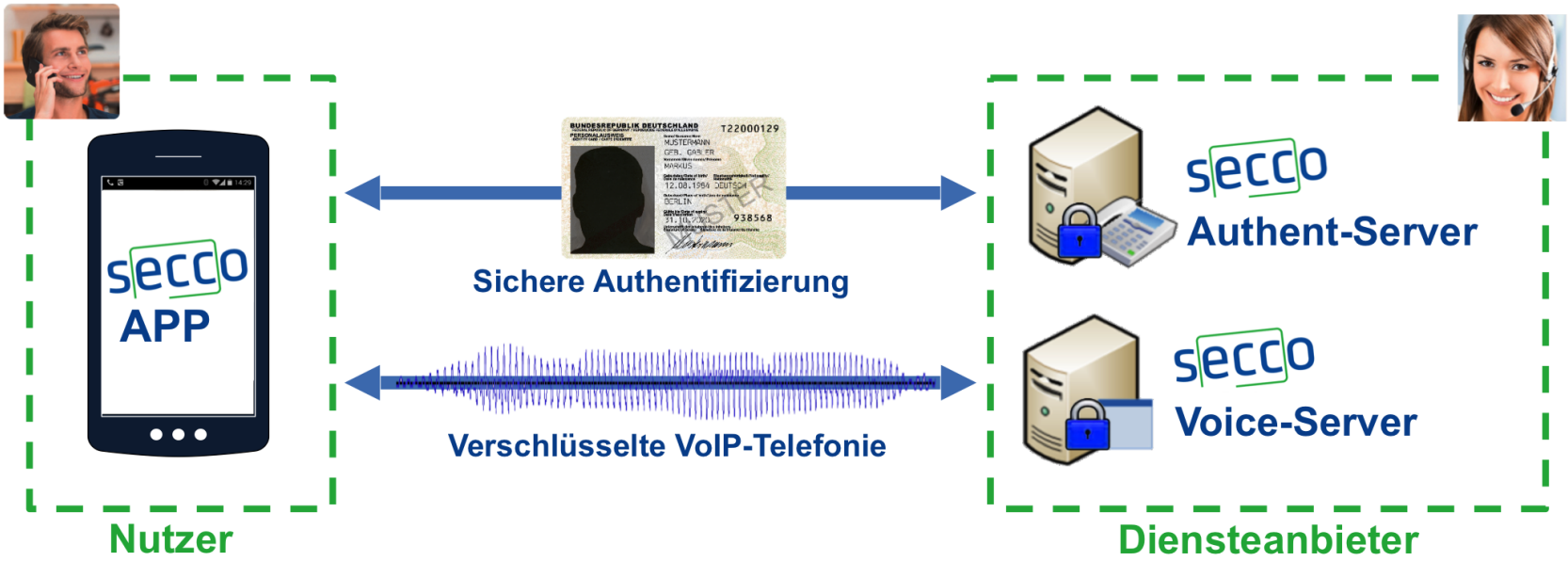
1. A,B melden sich beim KDC via Online-Ausweisfunktion an
2. A,B generieren Schlüsselpaare $(pk_A, sk_A), (pk_B, sk_B)$
3. A,B senden pk_A, pk_B an das KDC
4. KDC sendet pk_A an B und pk_B an A
5. Schlüsseleinigung (z.B. authentisierter DH) auf Basis von pk_A und pk_B

Ad-hoc Schlüsselaustausch III

Untersuchung folgender Fragestellungen:

- Vertrauenswürdigkeit des Diensteanbieters:
  - Datenschutz- und Sicherheitsaudits
  - Open Source
  - Expertenmodus: Nachvollziehbarkeit der vom KDC verteilten Schlüssel
- Benutzbarkeit:
  - Umsetzung als Instant Messenger auf Rechnern (später Smartphone, Tablet)
  - Integration der PersoApp im Instant Messenger (nur eine Software)

Secure Call Authentication



- Gestartet als Forschungsprojekt an der Hochschule Darmstadt
- Gefördert durch LOEWE (Exzellente Forschung für Hessens Zukunft)
- Ausgezeichnet mit dem Gründerpreis IKT Innovativ
- **Mehr Informationen:** Halle 9, Stand C 24 (Hessen-Stand)