Bundesamt
für Sicherheit in der
Informationstechnik

adesso business. people. technology.

Mobile Identität mit der AusweisApp2 – ein Prototyp

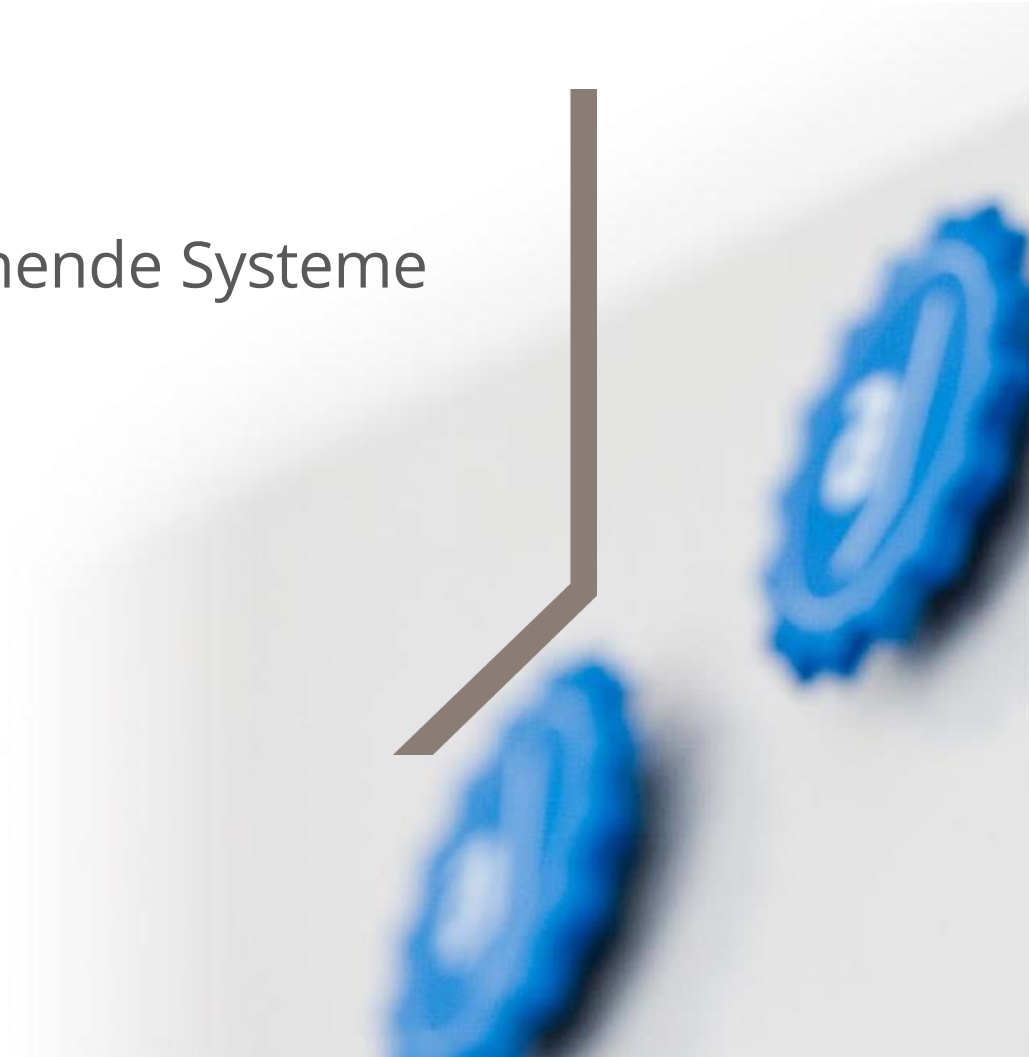
8. Anbieterforum AusweisApp2, 20.01.2020

Christian Kahlo
adesso SE, kahlo@adesso.de

Bundesamt
für Sicherheit in der
Informationstechnik

Agenda

- Was bedeutet „mobile Identität“?
- Funktionsweise und Integration in bestehende Systeme
- Bedeutung im Zusammenhang mit OZG
- Demonstration am Beispiel
- Fragen, Antworten und Diskussion



Was bedeutet „mobile Identität“? (1 / 4)

› Gedankliche Evolution vom „Ausweis“ zum „Identifizierungsmittel“

- eIDAS erlaubt für Identifizierungsmittel Abstufungen in unterschiedliche Vertrauensniveaus (LoA: niedrig, substantiell, hoch)
- Eine verifizierbare & vertrauenswürdige ID ist nicht nur auf den Personalausweis beschränkt
- Anforderungen an Identifizierungsmittel sind technologieneutral, um flexibel neue Implementierungen zu ermöglichen

Was bedeutet „mobile Identität“? (2 / 4)

- Ausgehend von der Idee der „abgeleiteten Identität“ können sicher gelesene und bestätigte Identitätsdaten als „beglaubigte Kopie“ auf dafür geeigneten und vorbereiteten Trägern aufgebracht werden.

- Das hoheitliche Ausweisdokument dient dabei als Ausgangspunkt und muss „echt“, gültig, nicht gesperrt und entsprechend der elektronischen Dokumentenprüfung, d.h. Online-Ausweisfunktion, gelesen werden.

- Der abgeleitete Identitätsdatensatz hat eine zeitlich beschränkte Gültigkeit, ist aber unabhängig vom Original und einzeln sperrbar.

Was bedeutet „mobile Identität“? (3 / 4)

- Der Ausweis wird ergänzt durch Hardware Tokens, welche es erlauben Identitätsdaten mit einem "substantiellen“ Vertrauensniveau zu speichern.
- Im Handy als SIM-Karte oder Secure Element:

- Unabhängig vom Gerät z.B. in Payment Chips:

Was bedeutet „mobile Identität“? (4 / 4)

- Für Dienste welche mit eIDAS-substantial nutzbar sind hat der Anwender den Ausweis immer dabei, wenn er sein Handy dabei hat
- Es kann mehrere mobile Identitäten parallel geben, z.B. auf dem Tablet, dem Privathandy und dem Diensthandy
- Datensätze entsprechen 1:1 den Inhalten des Originaldokuments
- Identitätsträger kann jedoch auch zusätzliche Attribute aufnehmen
  - eIDAS-Token Spezifikation, BSI TR-03110

Funktionsweise und Integration in bestehende Systeme (1 / 3)

- Arbeitsname „meID“ = mobile electronic ID
- meID verhält sich identisch zu einem herkömmlichen Ausweis, d.h. läuft in bestehender Infrastruktur einfach mit (TR-03124, TR-03130)
  - Nur geringe Anpassung auf Dienstanbieter-Seite notwendig (ID-Type)
- Neuer Dokumententyp wird eingeführt, um meID von Ausweis, eAT und Unionsbürgerkarte unterscheiden zu können
- Alle PA, eAT, UB können grundsätzlich in meID übertragen werden

Funktionsweise und Integration in bestehende Systeme (2 / 3)

- Bestehende eID-Server können in der Test-PKI bereits mit meID arbeiten, für Produktionssysteme neuer Document-Signer nötig
- Personalisierung und Sperrlisten-Integration z.Z. in Arbeit
- Sperrung erfolgt über Sperr-Hotline, Löschung über Mobilgerät
- Authentisierung erfolgt mit den Biometrie-Funktionen des Geräts oder alternativ mit PIN
  - BSI TR-03147 und TR-03159 bilden die Grundlagen

Funktionsweise und Integration in bestehende Systeme (3 / 3)

- Integration in AusweisApp2 in Entwickler-Preview ist vorhanden, setzt jedoch aktuelle und vorbereitete SIM-Karte voraus

- Realisierung über allerneueste LTE/5G USIM-Karten mit moderner Kryptographie und CC EAL5+/6+ Zertifizierung für Chip und OS

- Perspektivisch umsetzbar mit Technologien im Feld
  - Moderne USIM-Karten befinden sich im Rollout bei den MNOs, ggf. kann der Anwender später auch eine aktualisierte Karte anfordern
  - Unterstützung der eingebauten Secure Elements in Mobilgeräten

Bedeutung im Zusammenhang mit OZG (1 / 2)

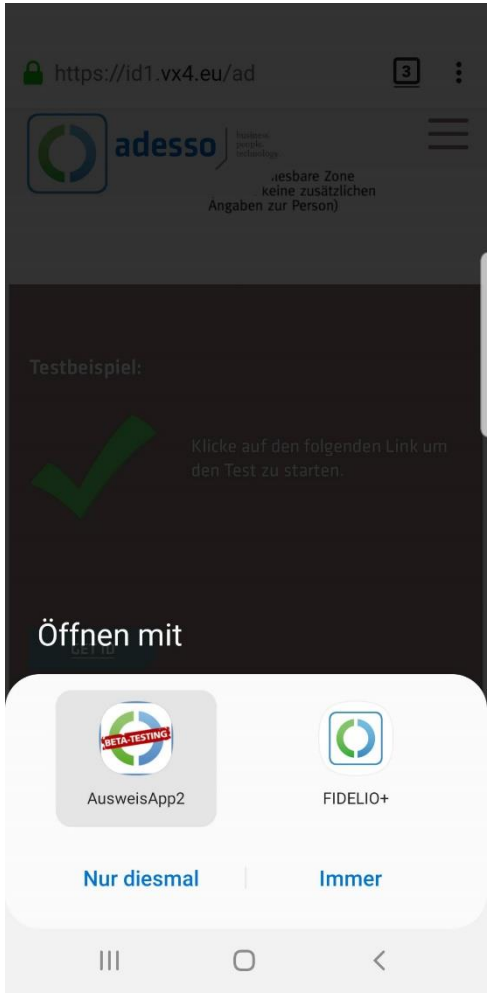
- Zur Zeit existiert noch keine Smartphone basierte Lösung, welche eine Identifizierung entsprechend dem "substantiellen„ Vertrauensniveau ermöglicht.

- Im Vergleich zu Software-Zertifikaten auf SD-Karten und USB-Sticks wesentlich sichere und komfortablere Lösung für die Anmeldung
  - kann nicht vervielfältigt werden und PIN bzw. Fingerabdruck kann nicht über Web-Browser ausgespäht werden
  - immer dabei, über Gerätekopplung zukünftig auch am Desktop nutzbar
- Nutzt und integriert sich in bestehende Infrastruktur, Know-How, Software und Anbieter existieren, keine neuen Systeme notwendig

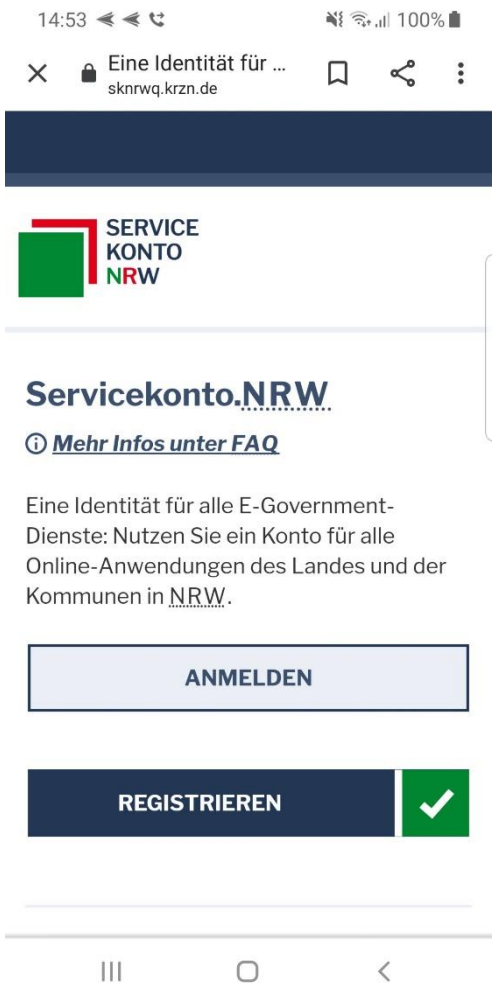
Bedeutung im Zusammenhang mit OZG (2 / 2)

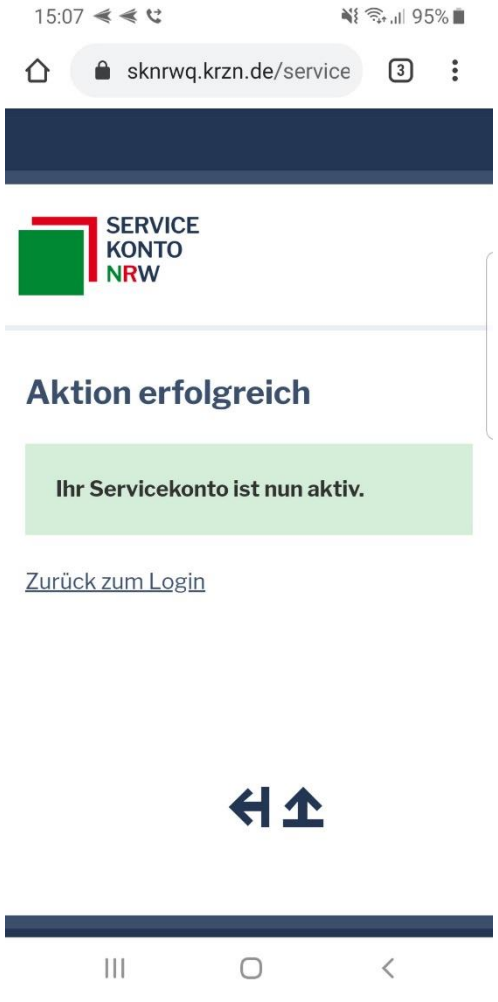
- Geringere Aufwände wenn Komponenten für eIDAS LoA „hoch“ einfach wiederverwendet werden können
- Echtheitsprüfung und Sperrung von Identifikationsmerkmalen mit einheitlicher Bundes-Infrastruktur, statt individuelle Einzellösungen
- Funktionalität analog zum Ausweis, z.B. Login / Wiedererkennung über Pseudonym und Erstregistrierung mit vollem Datensatz
- Integriert nahtlos mit FIDELIO, d.h. WebAuthn/FIDO Schnittstelle

Demonstration am Beispiel (1 / 2)



Demonstration am Beispiel (2 / 2)





Fragen, Antworten und Diskussion

Vielen Dank!

adesso business. people. technology.

Christian Kahlo

kahlo@adesso.de

adesso SE
Adessoplatz 1
44269 Dortmund
T +49 231 7000-7000
F +49 231 7000-1000
www.adesso.de