

Vertrauenswürdige digitale Personenattribute

Heutzutage wird die Verwendung von digitalen Identitäten für Onlinedienste wie Finanztransaktionen immer populärer. Gerade im Zusammenhang mit sensiblen Daten stellt dies jedoch neue Herausforderungen an die IT-Industrie: Die Nutzung einer digitalen Identität erfordert oftmals eine Überprüfung von Benutzerattributen, wie Name oder Geburtsdatum. Diese Arbeit untersucht die Möglichkeiten der Selbstvalidierung von persönlichen Attributen ohne die Einbindung von Drittparteien als Validierungsanbieter und verwendet stattdessen Validierungsinformationen, die dem Benutzer bereits zur Verfügung stehen.

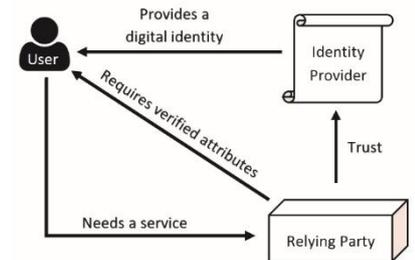
Im ersten Teil der Arbeit wurden verschiedene Ansätze der Selbstvalidierung untersucht und bewertet. Anschliessend wurde aus diesen Ansätzen der erfolgversprechendste – Selbstvalidierung von persönlichen Attributen mittels E-Pass – ausgewählt, um als funktionsfähiger Prototyp entwickelt zu werden. Der E-Pass bietet sich insbesondere an, da er wertvolle Identitätsattribute über den Besitzer enthält und diese Attribute durch das Ausgabeland digital signiert worden sind. Sie können somit auf ihre Integrität überprüft werden. Darüber hinaus kann auch die Authentizität des Passes selbst geprüft werden. Der entwickelte Prototyp implementiert eine Methode, die es einem Identitätsanbieter erlaubt, persönlichen Attribute aus einem E-Pass mittels Smartphone mit Nahfeldkommunikation (NFC) zu lesen und die Authentizität der Daten sowie des E-Passes automatisiert zu überprüfen. Zudem wird geprüft, ob die Daten manipuliert wurden oder nicht aus dem entsprechenden, authentischen Pass stammen.

Um die Sicherheit der Validierung weiter zu steigern und um Identitätsdiebstahl zu erschweren, wurden Methoden vorgeschlagen, welche den E-Pass mit dem Benutzer verknüpfen, welcher die Attribute seiner digitalen Identität validieren möchte.

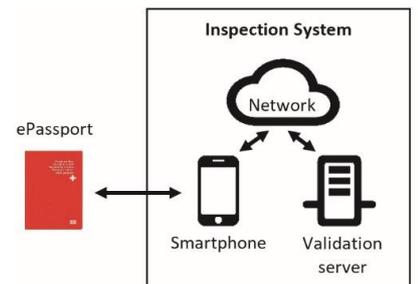


Diplomand
Gioele Moretti

Dozierende
Marc Rennhard
Kevin Lapagna



Beteiligte Akteure bei der Verwendung digitaler Identitäten.



Funktionsfähiger Prototyp –
grundlegende Architektur.