Identity Provider zur Verifikation der vertrauenswürdigen digitalen Identität

Autoren

Zusammenfassung

Die Verwendung der meisten Dienste im Internet ist an die Nutzung einer vertrauenswürdigen digitalen Identität (Trusted Identity, TId) geknüpft. Eine vertrauenswürdige digitale Identität liegt vor, wenn die zugehörige natürliche Person nicht abstreitbar bekannt ist. Die klassische Internet-Nutzer-Name/Passwort Authentikation beruht in der Regel auf der Internet-Nutzer Selbstauskunft und genügt bei weitem nicht den heutigen Sicherheits-Ansprüchen. Der Internet-Dienstanbieter und die natürliche Person (der Internet-Nutzer) sind zum Zeitpunkt des ersten aufeinander Treffens nur in speziellen Fällen physisch beieinander, sodass die bewährte Face-to-Face-Identifizierung nicht leicht durchgeführt werden kann. Es wird das Modell eines Identity Provider zur Feststellung einer vertrauenswürdigen digitalen Identität (Trusted Identity, TId) vorgestellt. Das Modell setzt eine Trusted Third Party (TTP) voraus, die vertrauenswürdige digitale Identitäten ausstellt, die Identität der natürlichen Person feststellt und seine starke Authentikation ermöglicht. Die Umsetzung des Modells wird am Beispiel des neuen deutschen Personalausweises (nPA) [BSI TR-03127] gezeigt. Eine prototypische Umsetzung mit dem nPA findet im laufenden BMWi-Forschungsprojekt statt. Das vorliegende neue Verfahren zur Identitätsbereitstellung ergänzt einerseits bei Verwendung mit der Face-to-Face-Identifizierung deren Sicherheit, da zusätzlich eine elektronische Bestätigung durchgeführt wird, andererseits stellt es bei Verwendung über das Internet dem Internet-Dienstanbieter eine vertrauenswürdige digitale Identität bereit. Die Betrachtung der Einsetzbarkeit mit weiteren TTP bietet sich an.

1 Motivation

Im klassischen Internet-Szenario teilen entfernte Internet-Nutzer durch Selbstauskunft dem Internet-Dienstanbieter mit, wer sie sind. Der Internet-Dienstanbieter hat keine Möglichkeit, auf die Entfernung über das Internet, die Angaben zu verifizieren. Einher mit der unbestätigten Identität des Internet-Nutzers geht meistens die Vergabe einer Nutzername/Passwort basierten Authentifizierungsmethode, die als höchst unsicher bekannt ist. Abbildung 1 zeigt die Nutzername/Passwort basierte Verwendung des Internet-Dienstes.

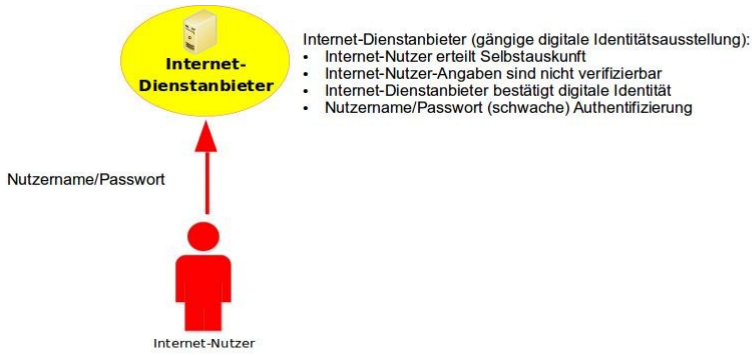

Abbildung 1: Nutzername und Passwort basierter Internet-Dienstzugang

In der vorliegenden Arbeit wird ein Identity Provider vorgestellt, der dem Internet-Dienstanbieter eine mit Face-to-Face-Identitätsfeststellung festgestellte vertrauenswürdige digitale Identität (Trusted Identity, TId) bereitstellt; der Internet-Nutzer kann die verwendete TId durch starke Authentikation belegen.

Das im Paper erarbeitete Modell eines Identity Provider Dienstes wird am Beispiel des neuen deutschen Personalausweises (nPA) [BSI TR-03127] im BMWi-Forschungsprojekt umgesetzt und stellt eine über das Internet entfernt durchführbare „Like-Face-to-Face-Identitätsfeststellung“ bei starker Authentikation bereit.

Im konkreten Forschungsprojekt Szenario ist der (Internet-)Dienstanbieter ein eMobility Stromanbieter aus dem Elektromobilitätsumfeld, der die natürliche Person und vertrauenswürdige digitale Identität (Trusted Identity, TId) seiner zukünftigen Stromkunden feststellen muss. Das Szenario wird in Abbildung 2 skizziert.

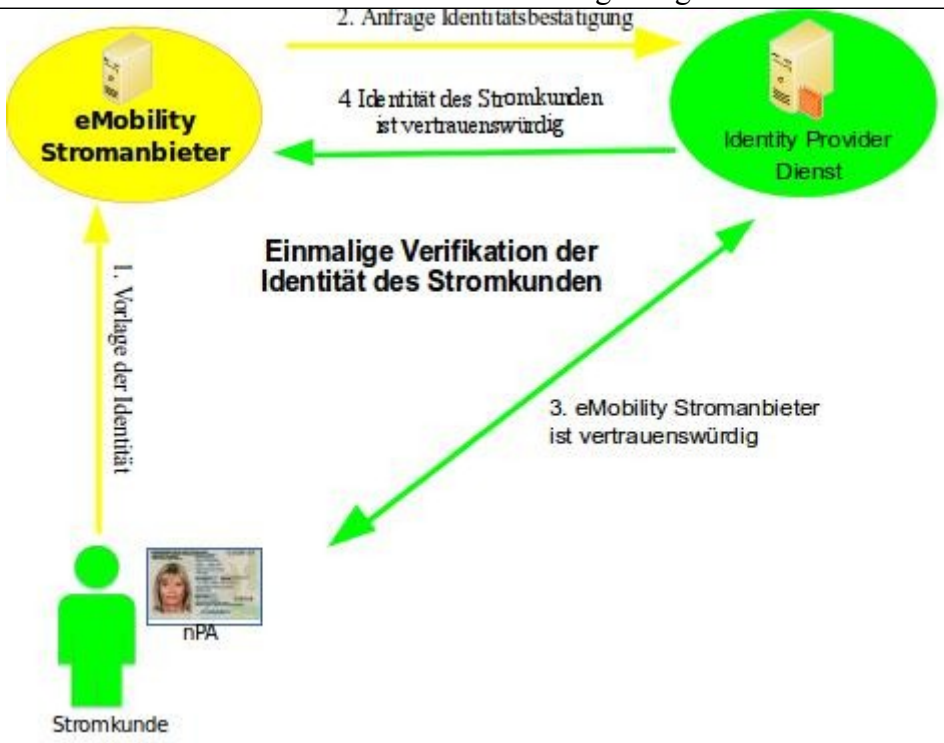

Abbildung 2: Identity Provider bestätigt Trusted Identity

Die einmalige Feststellung der Trusted Identity (TId) des Stromkunden findet entweder als Face-to-Face-Identifizierung im Büro des Stromanbieters, mit Hilfe des nPA und dem Identity Provider über das Internet auf seinem Stromanbieter-Internetportal oder an der Strom-Ladesäule direkt statt. Der Stromanbieter legt im Nachgang zur erfolgreichen Feststellung der Trusted Identity (TId) des Stromkunden für diesen eine vertrauensvolle digitale Identität in seinem System an und händigt dem Stromkunden eine Kundenkarte aus, die idealerweise auch zur starken Authenitkation des Stromkunden verwendet werden kann.

2 Einleitung

Internet-Dienstanbieter haben ein berechtigtes Interesse nach halten zu können, wer ihre Internet-Dienste nutzen möchte oder genutzt hat. Die Bereitstellung von Internet-Diensten erfordert für bestimmte Internet-Dienste, aus finanziellen und rechtlichen Gründen, die natürliche Person hinter der verwendeten digitalen Identität zu kennen. Der Internet-Nutzer muss zur Verwendung des (Internet-)Dienstes eine vertrauenswürdige digitale Identität vorweisen.

Das klassische Szenario sieht für die Nutzung eines Internet-Dienstes jedoch die Selbstauskunft durch den Internet-Nutzer und die darauf basierte Ausstellung einer Kombination aus Internet-Nutzer-Namen/Passwort vor. Die natürliche Person ist in diesem Szenario nicht belegt, und somit ist die vorliegende digitale Identität nicht vertrauenswürdig.

Der Internet-Dienstanbieter und die Internet-Nutzer werden im Vorfeld der ersten Nutzung des Internet-Dienstes durch den Internet-Nutzer für gewöhnlich keinen physischen Kontakt gehabt haben.

Die vorliegende Arbeit definiert das Modell des Identity Provider (IdP) Dienstes, der auf einer Trusted Third Party (TTP) basiert. Das Modell geht von einer TTP aus, die zu einer natürlichen Person eine „Like-Face-to-Face-Identitätsfeststellung“ durchgeführt und eine vertrauenswürdige digitale Identität (Trusted Identity, TId) ausgestellt hat und die natürliche Person

diese durch eine starke Authentikation belegen kann. Das Modell des Identity Providers wird in dem vollständigen Paper detailliert beschrieben werden.

In dem vorliegenden Dokument wird die Umsetzung des Identity Provider Modells am Beispiel des neuen Personalausweises (nPA) dargestellt, wie es im BMWi-Forschungsprojekt erarbeitet und prototypisch umgesetzt wird.

Die Umsetzung mit dem nPA geht von einem Stromanbieter aus, der zu dem Stromkunden (natürliche Person) eine nach dem Prinzip der Face-to-Face-Identitätsfeststellung verifizierte vertrauenswürdige digitale Identität (Trusted Identity, TId) benötigt. Der Stromkunde hat zur initialen Identitätsfeststellung mehrere Alternativen: Er kann das Büro des Stromanbieters aufsuchen, das Internet-Portal des Stromanbieters nutzen oder die Identitätsfeststellung direkt an der Strom-Ladesäule durchführen.

Die Umsetzung des Identity Providers mit dem nPA ist schematisch in Abbildung 3 dargestellt. Hier besitzt der Identity Provider das zur Nutzung der nPA eID Funktionalität [BSI TR--03127] notwendige Berechtigungszertifikat [BdrZert]. Der Identity Provider darf erst nach Autorisierung durch den Stromkunden die vom Stromanbieter angeforderte Bestätigung zur vertrauenswürdigen digitalen Identität (Trusted Identity) durchführen.

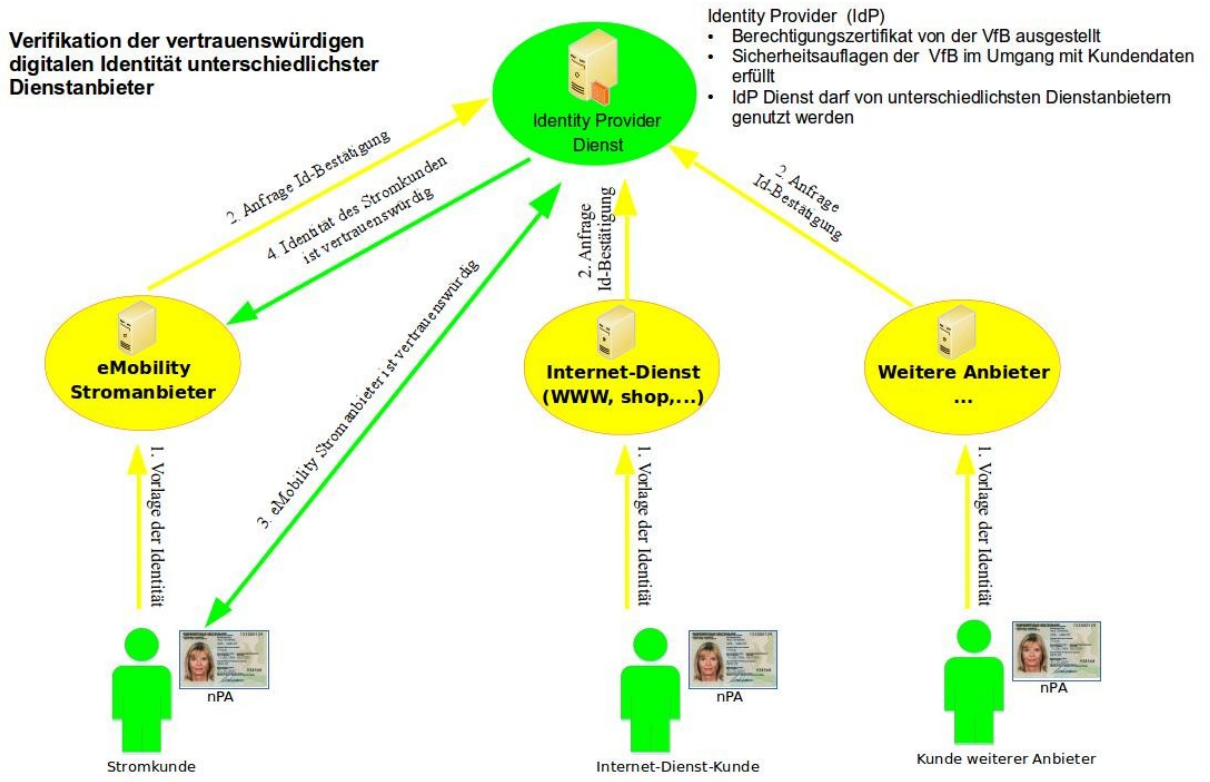

Abbildung 3: Identity Provider nPA basiert

Im Nachgang zur Bestätigung der Trusted Identity legt der Stromanbieter eine vertrauenswürdige digitale Identität zu dem Stromkunden in seinem System an, stellt diesem seine Kundenkarte zur Verfügung, die idealerweise auch zur starken Authentikation des Stromkunden verwendet werden kann. Der Stromanbieter kann dem Stromkunden, außer mit der Kundenkarte, die starke Authentikation auch mit dem nPA ermöglichen.

Der in Abbildung 3 dargestellte Identity Provider darf von unabhängigen Dienstanbietern (Internet-Dienstabietern, Homepage-Betreibern, Online-shops, Stromanbietern, Industriefirmen, etc.) genutzt werden, da der vorliegende Identity Provider die von der Vergabestelle für Berechtigungszertifikate (VfB) vorgegebenen Auflagen zur Sicherheit im Umgang mit Kundendaten vollständig erfüllt werden (Details im vollständigen Paper).

In Kapitel 3 werden die initiale Problemstellung und das Ziel dargestellt. Kapitel 4 beschreibt die Umsetzung des Identity Providers mit dem nPA. In Kapitel 5 folgt die Abgrenzung der Idee und ein Ausblick.

3 Problemstellung und Ziel

Das zu lösende Ausgangsproblem ist, dass ein Internet-Dienstanbieter sowohl ein finanzielles wie auch rechtliches Interesse an der zweifelsfreien Kenntnis der Identität der natürlichen Person (Internet-Nutzer) hat und dass beide Parteien vorab keine Kenntnis von einander haben. **Das führt zu folgender Problemstellung**:

- Identifizierung einer entfernten natürlichen Person
- Zuordnung einer digitalen Identität zur entfernten natürlichen Person

aus der sich das **zu erreichende Ziel** ableiten lässt:

- Nicht abstreitbare Zuordnung zwischen natürlicher Person und der von dieser verwendeten digitalen Identität

eine **andere Formulierung dieses Ziels** lautet:

- Dienst einer **vertrauenswürdigen digitalen Identität** (**Trusted Identity, TId**) bereitstellen

Die Betrachtung der obigen Problemstellung ist nicht nur auf klassische Internet-Dienstanbieter beschränkt, da immer mehr Dienstanbieter ihre Dienste (wie z.B. Stromanbieter) Internet gestützt ihren zukünftigen Kunden bereitstellen; z.B. kann zwecks Kundengewinnung den Kunden nicht zugemutet werden, vor einer erstmaligen Nutzung des Dienstes persönlich die Büros der Stromanbieter aufsuchen zu müssen.

Die Stromanbieter haben zusätzlich die Möglichkeit, sowohl über das Internet als auch direkt an der Ladesäule, die vertrauenswürdige digitale Identität des zukünftigen Kunden mit dem Identity Provider festzustellen.

4 Identity Provider Modell mit nPA

Das erarbeitete Modell des Identity Providers kann mit dem neuen deutschen Personalausweis nPA in zwei Varianten umgesetzt werden. Die erste Variante verwendet die eID- und Qualifizierte Erweiterte Signatur-Funktionalität (QES-Funktionalität), die zweite Variante verwendet ausschließlich die eID-Fuktionalität des nPA.

In dem vollständigen Paper werden beide nPA Umsetzungsvarianten und das zugrunde liegende generische Modell des Identity Provider detailliert vorgestellt.

5 Abgrenzung und das Neue an der Idee

Die vorliegende Arbeit beschreibt das Modell eines TTP basierten Identity Providers, der eine etablierte Trusted Third Party und deren starke Authentikation verwendet. Das beschriebene Modell des TTP basierten IdP wird am Beispiel eines IdP Berechtigungszertifikats [BdrZert] zum Auslesen des neuen Personalausweises (nPA) umgesetzt. Es verwendet eine schon vorhandene „vertrauenswürdige digitale Identität (TId)“, die eID-Funktionalität [BSI TR-03127] des nPA.

Die vorliegende Arbeit befasst sich nicht mit der erstmaligen bzw. erneuten Feststellung der Identität einer natürlichen Person, wie sie von Behörden oder anderer vergleichbarer Einrichtungen zwecks Ausstellung eines Lichtbildausweises durchgeführt wird.

Im Zuge der Ausstellung eines neuen Personalausweises (nPA) findet durch die zuständige Behörde, basierend auf den vorhandenen persönlichen Daten und des vorhandenen Lichtbilds eine Face-To-Face-Identifizierung statt. Im Anschluss an diese wird der natürlichen Person der neue Pesonalausweis (nPA), mit dem diese eine starke Authentikation durchführen kann, ausgehändigt.

Aus dem entworfenen Modell des TTP basierten Identity Providers, der beispielhaften Umsetzung mit dem neuen Personalausweis (nPA) und der aufgeführten Abgrenzung lässt sich **das Neue an der Idee** zusammengefasst darstellen:

- vorhandene (staatliche) Trusted Third Party (TTP) verwenden
- vorhandene Trusted Identity (TId) verwenden
- basiert auf zuvor durchgeführter (staatlicher) und anerkannter Identifikation natürlicher Personen (Face-To-Face-Identitätsfeststellung)
- basiert auf starker Authentikation
- Identity Provider bestätigt Internet-Dienst/Stromanbieter „vertrauenswürdige digitale Identität (Trusted Identity, TId)“
- Internet-Nutzer/Stromkunden nutzen Dienst eines vertrauenswürdigen Dienstanbieters
- Dienstanbieter reduzieren Kosten, da viele Dienstanbieter den Identity Provider verwenden können
- Internet-Nutzer/Stromkunden behalten vollständige Kontrolle über ihre Daten

6 Ausblick

Die Umsetzung des entwickelten Modells des TTP basierten Identity Providers ist am Beispiel des neuen Personalausweises (nPA) dargestellt worden und wird prototypisch im BMWi-Forschungsprojekt umgesetzt.

Das vorgestellte Identity Provider Modell kann bei allen Internet gestützten Dienstangeboten verwendet werden.

Des Weiteren werden die „Autoren“ in weiteren wissenschaftlichen Arbeiten die Anwendung des Modells mit weiteren ausgewählten vorhandenen Trusted Third Partys betrachten. Es bieten sich unter anderen Personalausweise anderer Staaten und/oder Ausweise großer Einrichtungen wie Versicherungen, Banken, Firmen, etc. an.

Darüber hinaus ist eine Betrachtung zur Anwendbarkeit des Modells des TTP basierten Identity Providers auf Objekt Identitäten des Internet der Dinge im Fokus der Forschungsarbeiten der „Autoren“.

Literatur

[VfB] Vergabestelle für Berechtigungszertifikate des Beundesverwaltungsamt, http://www.bva.bund.de/DE/Organisation/Abteilungen/Abteilung_S/nPA/Vergabestelle/node.html

[BSI TR-03127] BSI TR-03127 Architektur Elektronischer Personalausweis, https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03127/tr-03127.html

[BdrZert] Bundesdruckerei Berechtigungszertifikat, https://www.bundesdruckerei.de/de/198-berechtigungszertifikate