Identity Provider zur Verifikation der vertrauenswürdigen digitalen Identität

Antonio González Robles · Norbert Pohlmann

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen
{GonzalezRobles | Pohlmann}@internet-sicherheit.de

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 eindeutig zugeordnet werden kann. Bei der klassischen Nutzername/Passwort Authentifikation beruht die Identität in der Regel auf der Internet-Nutzer Selbstauskunft und genügt bei den meisten Internet-Diensten den heutigen Sicherheits-Ansprüchen nicht. Der Internet-Dienstanbieter und die natürliche Person (der Internet-Nutzer) sind zum Zeitpunkt des ersten Aufeinandertreffens nur in speziellen Fällen physisch beieinander, sodass die bewährte Face-to-Face-Identifizierung nicht leicht durchgeführt werden kann. Es wird das Modell eines Identity Providers 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 Authentifikation ermöglicht. Die Umsetzung des Modells wird am Beispiel des neuen deutschen Personalausweises (nPA) gezeigt. Eine prototypische Umsetzung mit dem nPA findet im laufenden BMWi-Forschungsprojekt statt. Das vorliegende neue Verfahren zur Identitätsbereitstellung ergänzt einerseits bei Verwendung 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 Verwendung des IdP mit anderen TTP und der Einsatz im Internet der Dinge wird Gegenstand weiterer Betrachtungen sein.

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 direkt zu verifizieren. Mit der unbestätigten Identität des Internet-Nutzers geht meistens die Vergabe einer Nutzername/Passwort basierten Authentifizierungsmethode einher, die als höchst unsicher bekannt ist. Abbildung 1 zeigt die Nutzername/Passwort basierte Verwendung eines Internet-Dienstes.

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) „remote“ bestätigt; der Internet-Nutzer kann dann **seine** mitgebrachte **vertrauenswürdige digitale Identität (TId)** durch starke Authentifikation belegen.

P. Schartner · P. Lipp (Hrsg.) · D•A•CH Security 2014 · syssec (2014) 260-272.

Das Modell eines Identity Provider Dienstes wird am Beispiel des neuen deutschen Personalausweises (nPA) [BSI12] im BMWi-Forschungsprojekt umgesetzt und stellt eine über das Internet entfernt durchführbare und mit der „Face-to-Face-Identitätsfeststellung“ vergleichbare, vertrauenswürdige digitale Identitätsfeststellung mit starker Authentifikation bereit.

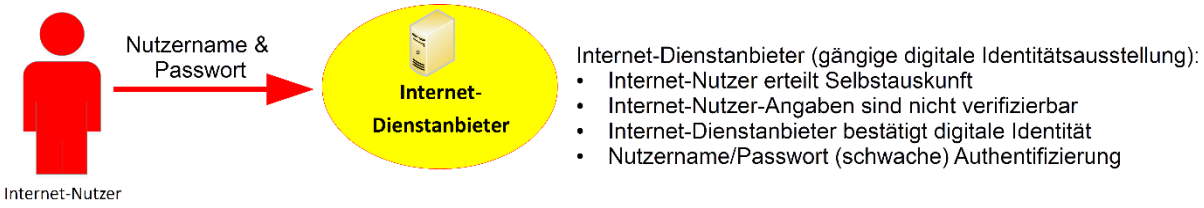

Abb.1: Nutzername und Passwort basierter Internet-Dienstzugang

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

Das im BMWi Forschungsprojekt vorliegende Ausgangsszenario erfordert die einmalige Feststellung der Trusted Identity (TId) des Stromkunden, die als Face-to-Face-Identifizierung im Büro des Stromanbieters umgesetzt werden muss. Unter Hinzunahme der Projektergebnisse, also mit Unterstützung des neuen Identity Providers und der eID-Funktionalität (eID-Service), [eIDBdr] des nPA, kann die Feststellung der TId noch zuverlässiger und remote gestaltet werden.

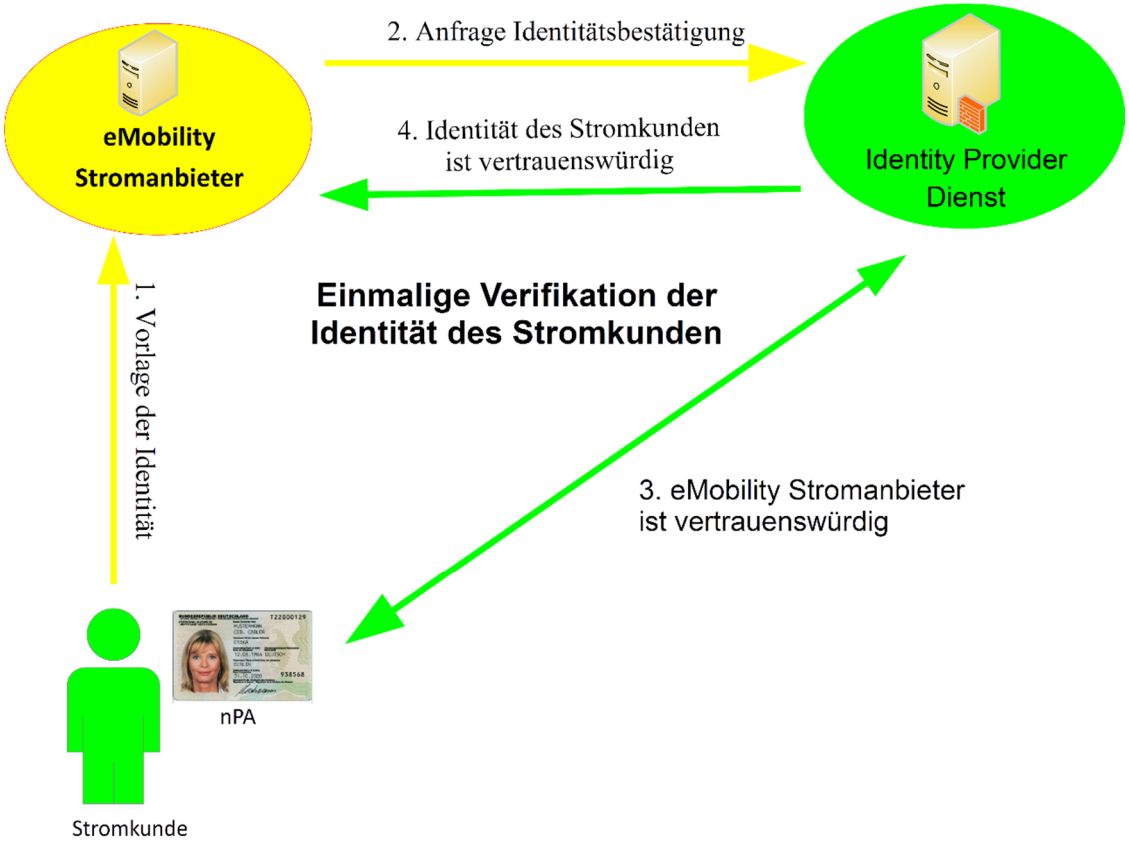

Abb. 2: Identity Provider bestätigt Trusted Identity

Die Betrachtung des ursprünglichen Ausgangsszenarios führte zum erweiterten Ausgangsszenario das eine Remote-Identitätsfeststellung bereitstellt. Die Remote-Identitätsfeststellung wird über den Identity Provider mit nPA über das Internet durchgeführt und kann auch auf dem Stromanbieter-Internetportal oder direkt an der Strom-Ladesäule angeboten werden. Der Stromanbieter legt im Nachgang zur erfolgreichen Feststellung der Trusted Identity (TId) des Stromkunden für diesen die vertrauenswürdige digitale Identität in seinem System an und kann dem Stromkunden eine eigene Kundenkarte aushändigen, die im Idealfall auch zur starken Authentifikation des Stromkunden verwendet werden kann.

2 Einleitung

Internet-Dienstanbieter haben ein berechtigtes Interesse nachvollziehen 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 Kenntnis der natürlichen Person hinter der verwendeten digitalen Identität. Aus diesem Grund muss der Internet-Nutzer zur Verwendung des (Internet-)Dienstes eine **vertrauenswürdige digitale Identität** vorweisen.

Das klassische Szenario sieht für die Nutzung eines Internet-Dienstes jedoch nur die Selbstauskunft durch den Internet-Nutzer vor. Aufbauend darauf findet in den meisten Fällen eine Nutzernamen/Passwort Authentifikation statt, siehe Abbildung 1. Die natürliche Person ist in diesem Szenario mit Selbstauskunft nicht belegt und somit ist die vorliegende digitale Identität nicht direkt vertrauenswürdig, da der Internet-Dienstanbieter und die Internet-Nutzer im Vorfeld der ersten Nutzung des Internet-Dienstes für gewöhnlich keinen physischen Kontakt haben.

Die vorliegende Arbeit definiert das Modell des Identity Provider (IdP) Dienstes, der als Trusted Third Party (TTP) fungiert. Das Modell geht von einer TTP aus, die mit einer natürlichen Person eine „Face-to-Face-Identitätsfeststellung“ durchgeführt und eine vertrauenswürdige digitale Identität (Trusted Identity, TId) ausgestellt hat und die natürliche Person die TId durch starke Authentifikation belegen kann. Das Modell des Identity Providers wird in Kapitel 4 beschrieben.

Die Umsetzung des neuen Identity Provider Modells wird am Beispiel des neuen Personalausweises (nPA) in Kapitel 5 dargestellt, wie es im BMWi-Forschungsprojekt Secure eMobility erarbeitet und prototypisch umgesetzt wird.

Der Stromanbieter benötigt zum Stromkunden (natürliche Person) eine dem Prinzip der Face-to-Face-Identitätsfeststellung genügende vertrauenswürdige digitale Identität (Trusted Identity, TId). Der Stromanbieter hat zur initialen Identitätsfeststellung mehrere Alternativen: Der Stromkunde kann das Büro des Stromanbieters aufsuchen oder eine nPA basierte Remote-Identitätsfeststellung mit dem Identity-Provider durchführen. Der Stromanbieter kann die nPA basierte Remote-Identitätsfeststellung auf seinem Internet-Portal, Ladesäule und ergänzend im Kundenbüro anbieten.

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 notwendige Berechtigungszertifikat [BdrZert]. Der Identity Provider darf erst nach Autorisierung durch den Stromkunden die vom Stromanbieter angeforderte Verifikation zur vertrauenswürdigen digitalen Identität (Trusted Identity) durchführen.

Im Nachgang zur Bestätigung der Trusted Identity legt der Stromanbieter die vertrauenswürdige digitale Identität zum Stromkunden in seinem System an, stellt diesem seine eigene Kundenkarte zur Verfügung, die, sofern vorgesehen, mit Hilfe einer starken Authentifikation der Stromkunden zur Verifikationen der Trusted Identity verwendet werden kann. Die starke Authentifikation kann natürlich auch mit dem nPA umgesetzt werden.

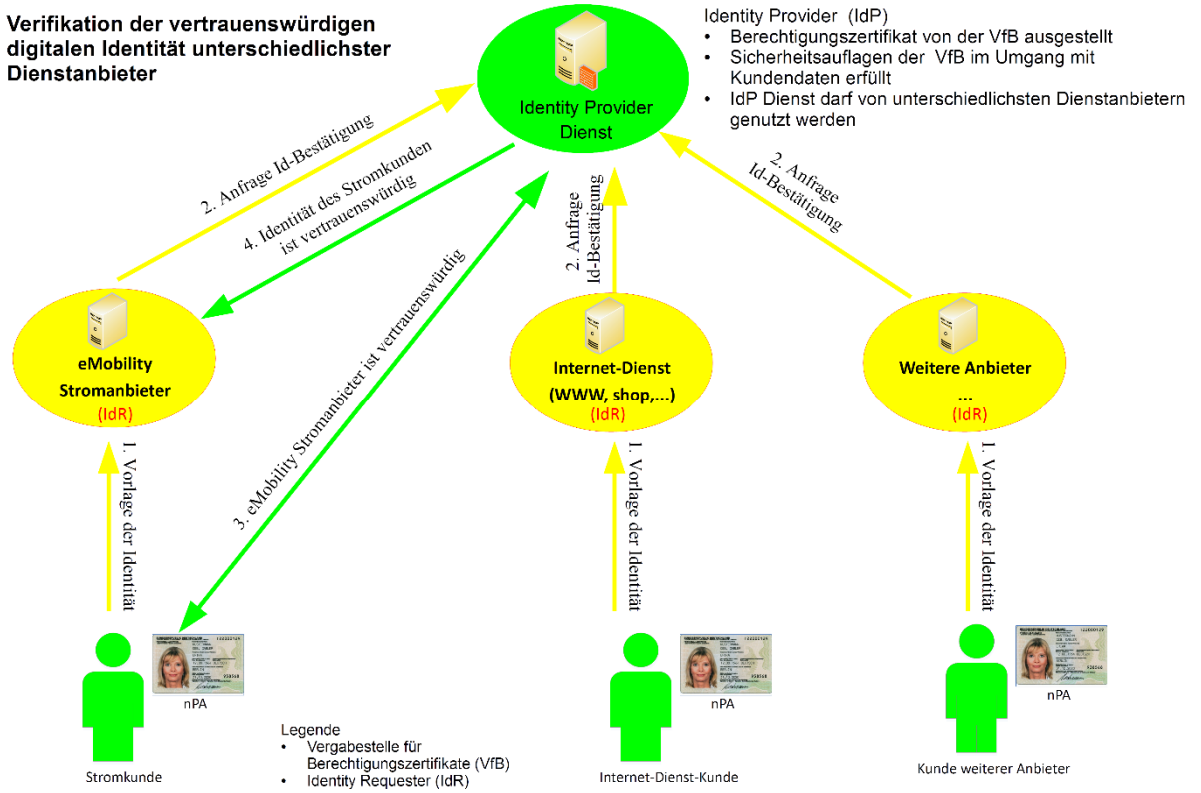

Abb. 3: Identity Provider nPA basiert

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

In Kapitel 3 werden die initiale Problemstellung und das Ziel dargestellt. Im Kapitel 4 wird das generische Modell des Identity Providers vorgestellt. Kapitel 5 beschreibt die Umsetzung des Identity Providers mit dem nPA. In Kapitel 7 folgt die Abgrenzung und das Neue an der Idee und in Kapitel 8 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 und
- Zuordnung einer digitalen Identität zur entfernten natürlichen Person.

Daraus lässt sich das **zu erreichende Ziel** ableiten:
Eindeutige 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.

Definition: Eine **vertrauenswürdige digitale Identität (Trusted Identity, TId)** liegt vor, wenn die Zuordnung zwischen der natürlichen Person und der von dieser verwendeten digitalen Identität eindeutig ist.

Die obige Betrachtung ist nicht nur auf klassische Internet-Dienstanbieter beschränkt, da immer mehr Dienstanbieter ihren Kunden ihre Dienste Internet-gestützt bereitstellen müssen und nicht immer vor der Feststellung der digitalen Identität mit der natürlichen Person eine Face-to-Face-Identitätsfeststellung durchführen können.

Die Verifikation der vertrauenswürdigen digitalen Identität wird ergänzend zur Face-to-Face-Identitätsfeststellung im Büro des Dienstanbieters auch Internet-gestützt mit der Hilfe des nPA durchgeführt werden.

Die Verifikation der vertrauenswürdigen digitalen Identität kann somit direkt am Dienstzugangspunkt (die Stromladesäule im Beispiel des eMobility-Umfelds) durchgeführt werden und somit auch die Grundlage für einen anschließenden digitalen Vertragsabschluss darstellen.

4 Identity Provider Modell

In diesem Kapitel wird das Modell des Identity Providers beschrieben.

4.1 Identifikation – Beteiligte Akteure und Komponenten

Im Folgenden werden die Akteure und Komponenten definiert und beschrieben.

Akteure:
Trusted Third Party (TTP), *Identity Provider (IdP)*, *Identity Requester (IdR)* und *Internet-Nutzer, User (U)*.

Komponenten:
User Security Token (UST): Sicherheits-Modul mit elektronischen Identifikationsmerkmal und starker Authentikation

Daten:
*User Data (UD):*Anonymer-Identifikator (Anonymous Identifier) (AId): der AId erlaubt keinen Rückschluss auf die ursprünglichen User Data.

Calculation rule for Anonymous Identifier (CrAId): Vorschrift erlaubt Berechnung eines AId, als Eingabe sind User Data (UD) und gegebenenfalls eine entsprechende UST Bestätigung (acknowledgement) zur Autorisierung der Berechnung vorgesehen.

AId für User Data (UD) von CrAId-Anwender berechnet: AId (UD, Anwender)

Anwender von CrAId: kann nur der Identity Requester (IdR) oder Identity Provider (IdP) sein.

Mit UST bestätigte (acknowledged) User Data (UD) = Ack(UST,UD))

Mit UST bestätigte (acknowledged) Anonyme-Identifikatoren (AId) = Ack(UST,AId))

4.2 Sicherheitsziele und Sicherheitsanforderungen

In Tabelle 1 sind die Sicherheitsziele, die User ((Internet-Nutzer) und Identity Requester (Internet-Dienstanbieter) für die eigenen und fremden Daten fordern.

Tab. 1: Geforderte Sicherheitsziele der Parteien an die Daten und der IdP als die Trusted Third Party

	Identity-Requester-Data (IdR)	User Data (UD)	Identity Provider (IdP)
Identity Requester (IdR)	1.	• Integrity 2. • Authenticity • Non-Repudiation	• Trust Anchor (Trusted Third Party – TTP)
User (U)	• Integrity 3. • Authenticity • Non-Repudiation	• Confidentiality 4. • Non-Propagation	• Trust Anchor (Trusted Third Party – TTP)

Die in Tabelle 1 geforderten Sicherheitsziele werden, auf Grundlage der folgenden Sicherheitsanforderungen und begleitenden Maßnahmen zum Protokollentwurf, in Kapitel 4.3 umgesetzt. Die möglichen Sicherheitsanforderungen umfassen:

1. Keine Sicherheitsanforderungen
2. Der Internet-Nutzer hat ein von der Trusted Third Party (TTP) akzeptiertes Security Token und es kann zur Starken Authentikation verwendet werden
3. Der Dienstanbieter (Identity Requester) besitzt seinerseits auch einen von der TTP anerkannten Identitätsnachweis
4. Die Internet-Nutzer-Daten verlassen nicht die für sie vorgesehene Domäne und werden zu keinem anderen Zweck verwendet.

Die Anonymen-Identifikatoren zu den Internet-Nutzer-Daten (User Data, UD) erlauben keinen Rückschluss auf die Internet-Nutzer-Daten selbst.

Begleitende Maßnahmen zum Protokollentwurf:

- ChallengeResponse basiert
- Kommunikation zwischen User, IdR und IdP ist SSL verschlüsselt
  - SSL Zertifikate werden von dem IdP ausgestellt
- CrAId Berechnungsvorschrift: (Umkehrung nicht möglich, Einwegfunktion)
  - Eingabe von: User Data, User Autorisierung und Verifikation der User Autorisierung → Berechnung (Einwegfunktion) des AId
- User muss autorisieren
  - Berechnung der AId, siehe CrAId
  - Verifikation der TId (Anfrage beim IdP)
- IdP verifiziert das Vorliegen der User Autorisierung
- IdP benötigt separate User Autorisierung für separaten Datenzugriff
- IdP hält die auf Basis der User Eingabe erstellten AIds vor

4.3 Phasen und Protokollablauf der Identitätsfeststellung

In der Tabelle 2 werden die **Phasen der TTP basierten Identitätsfeststellung** dargestellt, aus denen der in Abbildung 4 gezeigte Protokollablauf folgt.

Tab. 2: Phasen der Identitätsfeststellung

	Phase	USER		IdR		IdP/TTP
I	User claim to be owner of TId	U reveal Identity to IdR	→			
II	User authorise IdR to compute AId	Authorise IdR to compute Aid(UD,IdR)	→			
III	IdR compute locally Aid (one usage)			AId(UD,IdR) compute		
IV	IdR request U authorisation for IdP contact		←	Send AId(UD,IdR) to U		
V	User authorise IdR to contact IdP (one usage)	Authorise usage of AId(UD,IdR) at IdP	→			
VI	IdR contact IdP for TId verification (one usage)			IdR send U Authorisation and AId(UD,IdR) to IdP	→	
VII	IdP verify user authorisation					Verify U authorisation for AId(Ud,IdR)
VIII	1. IdP has independently access to UD (with User authorisation) 2. IdP compute user AId(UD,IdP)					1. Authorised usage of IdP acess to UD 2. Compute AId(UD,IdP)
IX	IdP verifies AId(UD,IdR)					IdP comparision of AId(UD,IdR) and AId(UD,IdP)
X	IdP sends result of AId(UD,IdR) verification to IdR				←	Comparision result of AId(UD,IdR) and AId(UD,IdP) send to IdR
XI	IdR has Trusted Identity (TId) or Not confirmed Identity			Confirmed TID or not confirmed ID		

Der Protokollablauf zur TTP basierten Identitätsfeststellung ergibt sich wie folgt: Jegliche Kommunikation zwischen U, IdR und IdP findet, ungeachtet weiterer Maßnahmen, wie in Kapitel 4.2 gefordert SSL verschlüsselt statt.

1. User (U) stellt dem Dienstanbieter (Identity Requester – IdR) seine **User Data (UD)** zur Verfügung
2. User (U) stellt dem IdR mit UST bestätigte UD bereit: **Ack(UST,UD) (Echtheitsbeleg und User Autorisierung)** (Beleg des Nutzer-Einverständnisses, das in der Anonymer-Identifikator Berechnungsvorschrift (CrAId) geprüft werden kann).
3. Identity Requester berechnet die Anonymen-Identifikatoren: AId(UD,IdR) (one usage)

4. Identity Requester schickt dem U die berechneten AId(UD,IdR)
5. User (U) stellt dem IdR mit UST bestätigtes AId bereit: Ack(UST,AId) (Beleg des Nutzer-Einverständnisses für die Anfrage) (one usage)
6. Identity Requester (IdR) sendet AId(UD,IdR) und Ack(UST,AId) an den Identity Provider (IdP)(one usage)
7. Identity Provider (IdP) verifiziert Ack(UST,AId) (Ist Nutzer-Autorisierung aus 5.)
8. 8.1 IdP hat mit U Autorisierung Zugriff auf einen unabhängigen Nutzer-Datenbestand (UD)
   8.2 IdP berechnet zu dem Nutzer den Anonymer-Identifikator: AId(UD,IdP)
9. Identity Provider (IdP) vergleicht die berechneten Anonymen-Identifikatoren auf Gleichheit: AId(UD,IdR) == AId(UD,IdP)
10. IdP sendet IdR das Ergebnis des Vergleiches aus Schritt 9:
11. IdR hat bestätigte Trusted Identity (TId) (= Ack(AId(UD,IdR),IdP))
    oder
    Nicht bestätigte digitale Identität

In Abbildung 4 wird der Identity Provider Protokollablauf gezeigt. Das Protokoll zur Umsetzung des IdP basierend auf einer TTP ist unabhängig von einer technologischen Umsetzung generisch definiert worden.

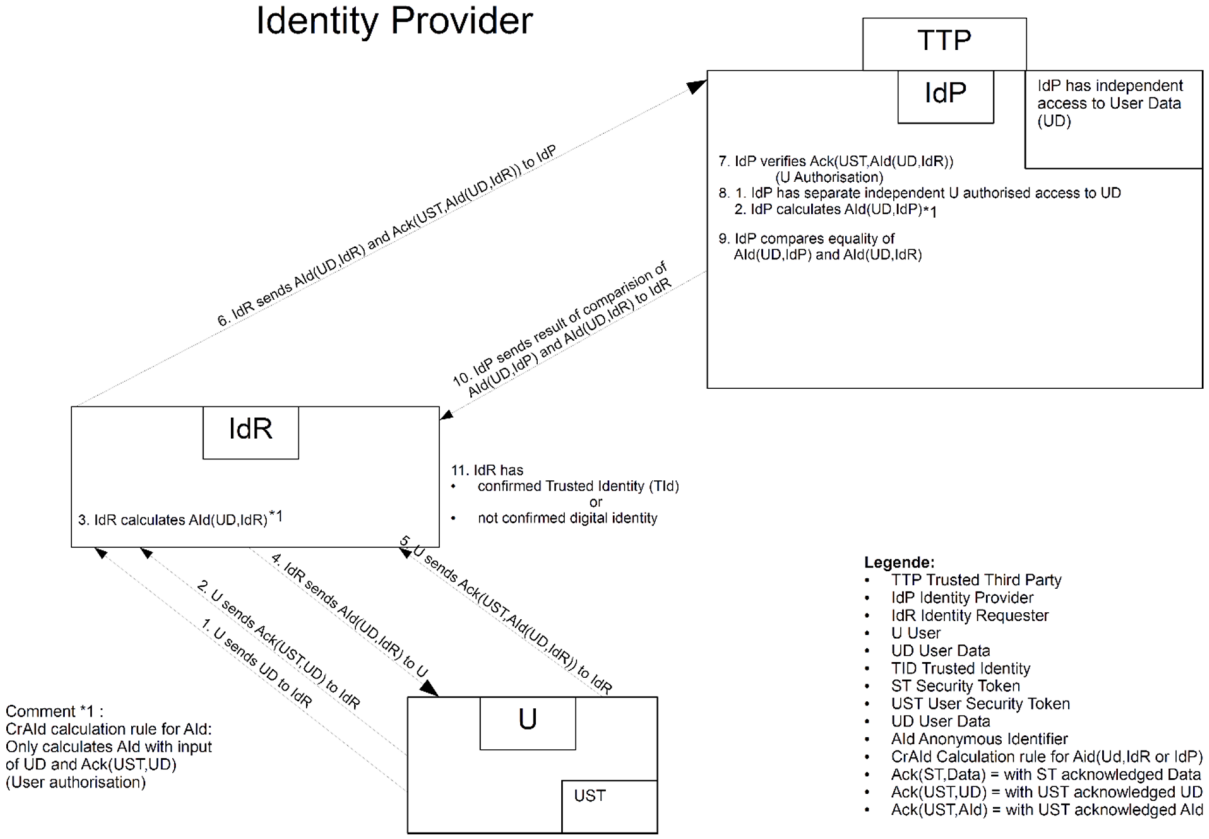

Abb. 4: Identity Provider Protokollablauf

Betrachtungen zum Identity Provider Protokollablauf:

Die Phasen I bis XI des Protokolls des Identity Provider in Tabelle 2 lassen sich wie folgt erläutern:

I. User legt seine vertrauenswürdige digitale Identität (Trusted Identity, TId) vor
II. **User autorisiert** Berechnung des Anonymen Identifikators (AId)
III. IdR berechnet AId
IV. IdR fragt bei User Autorisierung, zur Verifikation der Tid beim IdP, an
V. **User autorisiert** IdR zur Verifikation der TId beim IdP
VI. IdR fragt Verifikation beim IdP an
VII. IdP verifiziert die User Autorisierung
VIII. **IdP verifiziert, durch User autorisiert,** mittels eigenem Zugriff User Data
IX. IdP vergleicht die vorgelegte TId und die selbst festgestellte TId
X. IdP sendet Ergebnis des Vergleichs an IdR
XI. IdR hat entweder eine bestätigt TId oder nicht bestätigte ID vorliegen

Die **Schritte II und V werden hier hervorgehoben**, da hiermit sichergestellt wird, dass ein Identity Requester nicht beliebig die Verifikation einer Identität durchführen darf, sondern nur wenn die **Verifikation** unmittelbar zeitlich begrenzt **zweckgebunden von dem User autorisiert** worden ist.

In **Schritt VIII** hat der **Identity Provider User autorisierten unabhängigen Zugriff** auf die zur Verifikation der **TId** notwendigen User Daten, sodass der IdP nur bei Bedarf und nicht beliebig die Daten anfragen darf.

5 Identity Provider Modell mit nPA

Das erarbeitete Modell des Identity Providers kann mit dem neuen deutschen Personalausweis nPA genutzt werden. In dem BMWi Forschungsprojekt Secure eMobility wird das definierte Identity Provider Modell unter Verwendung der eID-Fuktionalität des nPA prototypisch umgesetzt

Der Identity Provider hat ein Berechtigungszertifikat zum sicheren Auslesen der Daten aus dem neuen Personalausweis (nPA) und fungiert in dem Modell als Delegated Trusted Third Party.

Der neue Personalausweis (nPA) ist das User Security Token (UST) zur starken Authentifikation. Der nPA bietet die PIN geschützte eID-Funktionalität, die bei Ausstellung kostenlos aktiviert werden kann.

Eine **natürliche Person** ist **durch** Angabe folgender **Attribute eindeutig identifizierbar**:

- Vornamen
- Nachnamen
- Geburtsdatum
- Anschrift

In den folgenden Betrachtungen mit dem nPA werden die genannten Attribute, die eine natürliche Person eindeutig identifizieren, verwendet und der Inhaber des neuen Personalausweises nPA kann das Auslesen dieser Attribute autorisieren. Ein Dienstanbieter und zugleich Identity Requester benötigt die Angabe dieser Attribute, um eine natürliche Person (Internet-Nutzer) eindeutig identifizieren zu können.

In Abbildung 5 ist der Identity Provider Protokollablauf mit nPA bei Verwendung der eID-Funktionalität dargestellt.

Der User stellt dem Identity Requester (IdR) die Nutzerdaten über ein online Formular bereit. Der IdR wendet die CrID Funktion auf die eingegebenen Nutzerdaten an, um die Anonymen Identifikatoren (AId) der einzelnen Daten zu berechnen. Des Weiteren kommunizieren der User, IdR und IdP jeweils verschlüsselt mit vom IdP ausgestellten SSL Zertifikaten, sodass hierdurch der User direkt Vertrauen zu der aufgerufenen Seite aufbauen kann.

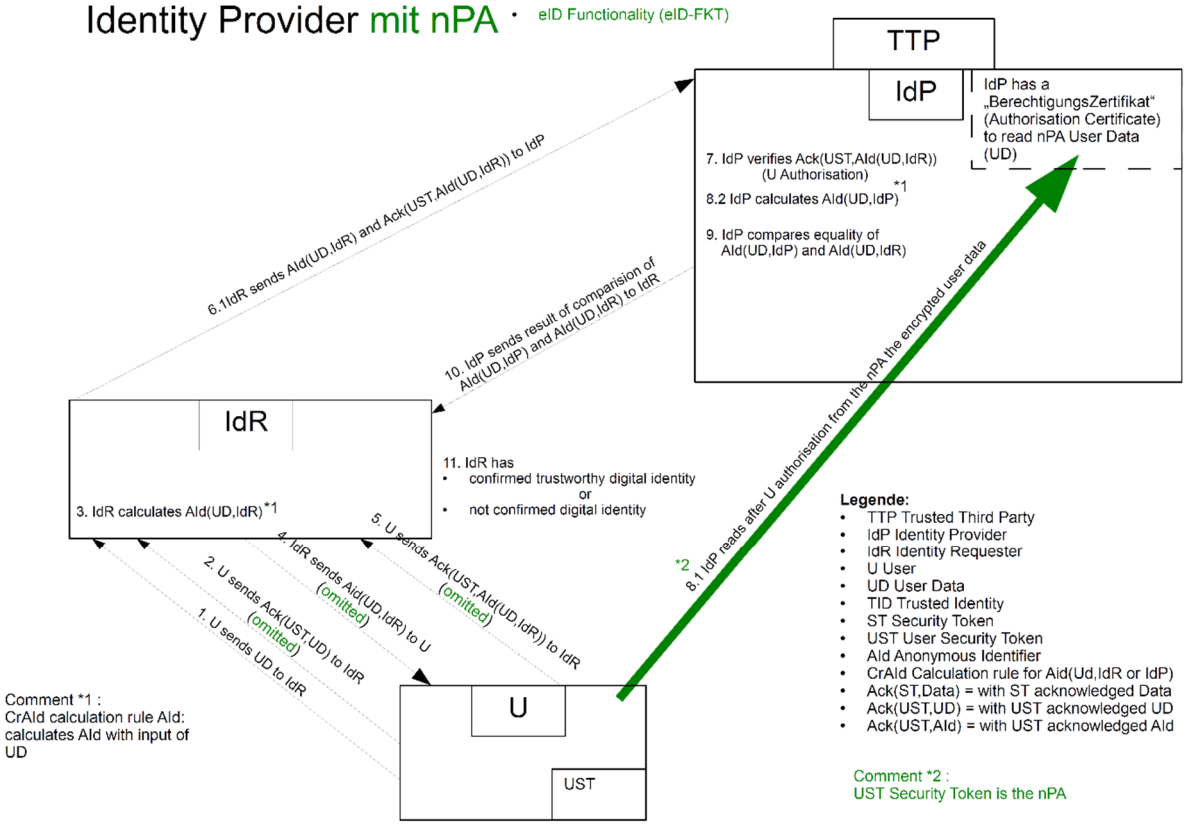

Abb. 5: Identity Provider Protokollablauf mit nPA bei Verwendung der eID-Funktionalitä

In der prototypischen Umsetzung mit der eID des nPA wird in der CrID Funktion beim IdR nicht explizit die User Autorisierung zur Berechnung des AId aus II. geprüft, sondern erst implizit in den Schritten V. und VIII.

Der Protokollablauf des TTP basierten Identity Providers mit nPA setzt durch die PIN-Eingabe durch den User zur Nutzung der eID-Funktionalität den Schritt V. (der User erlaubt die Anfrage beim IdP, User Authoristation to contact IdP) und Schritt VIII. (IdP kann selbständig die User Daten auslesen, IdP independent access to user data) die vom Protokoll geforderte Autorisierung durch den User um.

6 Allgemeine Betrachtungen

Die vorliegende Arbeit beschreibt das Modell eines TTP basierten Identity Providers zur Verifikation der vertrauenswürdigen digitalen Identität, das mit jeder etablierten Trusted Third Party und deren starker Authentikation umgesetzt werden könnte.

Der Kern der vorliegenden Arbeit ist das generische Modell des „Identity Providers zur Verifikation der vertrauenswürdigen digitalen Identität“.

Das beschriebene Modell des Identity Providers wird am Beispiel eines IdP beschrieben, für den das Berechtigungszertifikat zum Auslesen des neuen Personalausweises (nPA) vorliegt, und prototypisch umgesetzt wird. Es verwendet eine schon vorhandene „vertrauenswürdige digitale Identität (TId)“, die eID-Funktionalität des nPA.

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.

Die Umsetzung des Identity Provider Modells auf Basis des nPA erfüllt alle für die Verwendung des eID-Service und Berechtigungszertifikats geforderten Datenschutz- und Sicherheitsbestimmungen.

In der vorliegenden Arbeit werden vom User für den IdR gemachte Eingaben nur mit Schlüsseln verschlüsselt, zu denen auch vertrauenswürdige Zertifikate (SSL Zertifikate vom IdP ausgestellt) vorliegen. Bei der Identitätsfeststellung sendet der Identity Requester dem Identity Provider über eine verschlüsselte (auch SSL Zertifikate vom IdP ausgestellt) Verbindung Anonyme Identfikatoren (AId) zu. Der Identity Provider hält für erneute Verifikationen die vom User erhaltenen Anonymen Identifikatoren vor.

Der Identity Provider gibt zu keinem Zeitpunkt die von ihm aus dem nPA ausgelesenen Daten heraus.

7 Abgrenzung

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.

Die vorliegende Arbeit knüpft an der behördlich bekannten natürlichen Person und ihrer festgestellten vertrauenswürdigen digitalen Identität für die weiteren Betrachtungen an.

In **Abgrenzung** zu anderen Arbeiten und Technologien wird folgendes angeführt:

- Das in dieser Arbeit vorgestellte Identity Provider Modell zur Verifikation der TId mit nPA
  - wird zur Verifikation der vorgelegten TId verwendet.
  - Die verifizierte TId kann in der weiteren Verwendung durch den Identity Requester mittels eigener Methoden authentifiziert werden (z.B. Smartcard des Dienstanbieters).
  - Der nPA kann alternativ auch als weitere Authentifizierungsmethode verwendet werden.
- Verwandte Arbeiten zum nPA zu Authentifizierung und IdP
  - eID-Service der Bundesdruckerei
    - kann nur von einem Dienstanbieter verwendet werden
  - Verify-U Identitätsfestellung [Verify-U]

        - es liegt während der Identifikation ein Medienbruch vor
        - dauert mehrere Tage
    - OpenID Provider mit nPA Authentifizierung (if(is)) [OpenID]:
        - OpenID Identität mit starker Authentifizierung mittels eID des nPA
    - eID Connect [eIDCon]
        - Schwerpunkt auf Authentifizierung
        - Offeriert optional zusätzliche sichere Hardware (USB Token)
        - Erwähnen „durch nPA verifizierte Daten“

8 Das Neue an der Idee

Aus dem entworfenen Modell des Identity Providers zur Verifikation der vertrauenswürdigen digitalen Identität, der beispielhaften Umsetzung mit dem neuen Personalausweis (nPA) und der aufgeführten Abgrenzung, lässt sich insgesamt **das Neue an der Idee des Identity Providers mit nPA** wie folgt zusammengefasst darstellen:

- Generisches Modell des Identity Providers offen für jede Trusted Third Party
    - vorhandene (staatliche) Trusted Third Party (TTP) verwendbar
    - User kann seine Trusted Identity (TId) weiter verwenden
- basiert auf zuvor durchgeführter (staatlicher) und anerkannter Identifikation natürlicher Personen (Face-To-Face-Identitätsfeststellung)
- erhöht Zuverlässigkeit der Face-To-Face-Identitätsfeststellung bei weniger geübten Personen
- bestätigt durch starke Authentikation
- Identity Provider bestätigt
    - dem Dienstanbieter (hier Stromanbieter) „vertrauenswürdige digitale Identität (Trusted Identity, TId)“
    - dem Internet-Nutzer (Stromkunden) den Dienst eines vertrauenswürdigen Dienstanbieters zu nutzen
- Dienstanbieter reduzieren Kosten, da viele Dienstanbieter einen Identity Provider verwenden können
- Internet-Nutzer (Stromkunden) behalten vollständige Kontrolle über ihre Daten
- Grundlage für online Vertragsabschlüsse

9 Ausblick

Die Umsetzung des entwickelten Modells des TTP basierten Identity Providers ist am Beispiel der eID Funktionalität 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.

Auch wird in weiteren wissenschaftlichen Arbeiten die Anwendung des Modells mit anderen vorhandenen Trusted Third Partys betrachtet. Es bieten sich unter anderen Personalausweise anderer Staaten und/oder Ausweise großer Einrichtungen wie Versicherungen, Banken, Firmen, Behörden, 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 weiterer Forschungsarbeiten. Insbesondere werden Ansätze hinsichtlich der Anwendbarkeit des Prinzips der Autorisierung der Verifikation der digitalen Identität (TId) durch den Träger der TId selbst untersucht, sodass auch Objekte einerseits in der Lage sind, „vertrauenswürdige digitale Identitäten“ vorzuweisen und andererseits die Kontrolle über ihre Daten und deren Verwendung behalten können.

Danksagung

Das dieser Veröffentlichung zugrunde liegende Forschungs- und Entwicklungsprojekt "Secure eMobility (SecMobil)" wird mit Mitteln des Bundesministeriums für Wirtschaft und Energie (BMWi) innerhalb des Technologieprogramms "IKT für Elektromobilität" unter dem Förderkennzeichen 01ME12024 gefördert.

Literatur

[BSI12] BSI TR-03127 Architektur Elektronischer Personalausweis, Version 1.15, 1. August 2012.

[BVA] Vergabestelle für Berechtigungszertifikate (VfB) des Bundesverwaltungsamtes, Stand 23.06.2014. http://www.bva.bund.de/DE/Organisation/Abteilungen/Abteilung_S/nPA/Vergabestelle/node.html

[eIDCon] eID Connect, Stand 23.06.2014. www.eid-connect.de

[eIDBdr] eID-Service des nPA, Stand 23.06.2014. https://www.bundesdruckerei.de/de/197-e-id-service

[OpenID] Institut für Internet-Sicherheit | if(is) betreibt ersten OpenID Provider mit nPA Authentifizierung, Stand 23.06.2014. https://openid.internet-sicherheit.de/

[PAuswG] Gesetz über Personalausweis und den elektronischen Identitätsnachweis, Stand 23.06.2014. www.gesetze-im-internet.de/pauswg

[Verify-U] Personenidentifizierung mit Verify-U, Stand 23.06.2014. http://www.cybits.de/home/loesungen/simpleshow