Identitätsmanagement mit sicherer Authentifizierung und Attributweitergabe

Moritz Platt[1], Dr. Ivonne Scherfenberg[2] , Martin Schröder[2]

Kurzfassung: Durch Identitätsmissbrauch im Internet entsteht weltweit erheblicher finanzieller Schaden bei Gewerbetreibenden, Versicherungen, Zahlungsdienstleistern und bei direkt betroffenen Einzelpersonen selbst. Gängige Authentifizierungsverfahren sind besonders anfällig dafür, missbräuchlich verwendet zu werden, und gefährden so die Verlässlichkeit und Vertraulichkeit von Identitäten. Um digitale Identitäten verlässlicher zu machen, werden in dieser Arbeit die technischen und gesellschaftlichen Rahmenbedingungen für erfolgreiche und sichere Identitätsmanagementsysteme untersucht. Auf der Basis dieser Betrachtungen wird ein prototypisches Identitätsmanagementsystem vorgestellt, das mit Hilfe von delegierter hardwaregestützter Benutzerauthentifizierung als Intermediär zwischen Dienstanbietern und deren Benutzern vermittelt.
Obwohl noch viele Hürden hinsichtlich der Alltags- und Markttauglichkeit der beschriebenen Verfahren bestehen, stellen die Arbeitsergebnisse ein erstes grobes Fundament eines neuen sicheren Identitätsmanagementsystems dar.

Stichworte: Identitätsmanagement, Identity-as-a-Service, Hardwaregestützte Authentifizierung, Delegierte Authentifizierung

1 Einleitung

Im Gegensatz zum vorindustriellen Identitätsbegriff, der sich auf Herkunft, Ansiedlungsort und Berufsstand einer Person gründet [9], sowie den historisch darauf folgenden, papierbasierten Verfahren, erfordert die moderne digitale Dienstleistungsgesellschaft eine neue Herangehensweise an die Identität einer Person. Während historisch wegen der Erfordernis einer direkten Interaktion die Verifikation der Identität zwischen Handelspartnern persönlich relativ zweifelsfrei möglich war, bietet digitale Kommunikation diese Möglichkeiten nicht von Haus aus.

Identitätsmissbrauch

Digitale Interaktion, die einen persönlichen Bezug hat, ist anfällig für Identitätsdiebstahl und Identitätsmissbrauch. Identitätsdiebstahl wird hier als „unbefugtes Sichverschaffen einer Identität“ [5], Identitätsmissbrauch als „unbefugtes Agieren unter einer Identität“ [5] verstanden. Zum erfolgreichen Diebstahl einer Identität benötigen Angreifer häufig nur Kenntnis weniger persönlicher Attribute der Identität eines Opfers [9]. Allein unter Zuhilfenahme dieser Informationen – ohne die Verwendung weiterer technischer Angriffsmethoden – kann es Kriminellen gelingen, Zugriff auf die Konten ihrer Opfer bei Dienstanbietern zu erhalten. Einige Angriffsszenarien sind auf fehlerhafte Softwareimplementierung zurückzuführen. Andere basieren auf der Ausnutzung der bekannten Identitätsattribute eines Opfers. Letzteres kann auch bei einer technisch fehlerfreien Implementierung erfolgreich sein. Weiterhin sind heutige digitale Authentifizierungsverfahren anfällig für triviale Angriffe wie Beobachtung (z.B. direktes

1 Springer Science+Business Media Deutschland GmbH
2 Bundesdruckerei GmbH

Platt, M., Scherfenberg, I., & Schröder, M. (2014). Identitätsmanagement mit sicherer Authentifizierung und Attributweitergabe. In Tagungsband des 14. Deutschen IT-Sicherheitskongresses (pp. 365–386).

Über-die-Schulter-Schauen bei der Eingabe eines Passworts) oder Brute-Force-Angriffe, bei denen z.B. zahlreiche mögliche Passwörter durchprobiert werden.

Identitätssicherung
Eng zusammenhängend mit dem Risiko von Identitätsdiebstahl ist die Notwendigkeit für Identitätssicherung oder „Identity Assurance“. Identitätssicherung soll das Risiko des Einsatzes von *unzutreffenden* Identitätsinformationen beherrschbar machen – unabhängig davon, ob diese auf illegalem Wege gewonnen wurden oder frei erfunden sind.

Folgen von Identitätsdiebstahl
Die Minimierung des Identitätsdiebstahlrisikos und zuverlässige Identitätssicherung sind von kritischer Bedeutung sowohl für im Internet tätige Unternehmen aller Größen als auch für die öffentliche Hand. Im privatwirtschaftlichen Bereich sorgen vor allem finanzielle Einbußen durch Identitätsdiebstahl für ein starkes Interesse an diesen Themen. Zum tatsächlichen wirtschaftlichen Ausmaß liegen Statistiken vor allem für den US-amerikanischen Wirtschaftsraum vor. Dort wurden 2006 bereits wirtschaftliche Schäden in Höhe von 16 Milliarden US$ festgestellt [27]. Die IT-Sicherheitslage in der Bundesrepublik Deutschland, die von einem hohen IT-Sicherheitsbewusstsein geprägt ist, gestaltet sich im internationalen Vergleich weniger dramatisch [4]. Trotzdem ist die Bedrohungslage in Deutschland hoch, und Identitätsdiebstahl ist zu einem alltäglichen Phänomen geworden [8].

Im öffentlichen Bereich spielen Identitätssicherungsverfahren auf zentralstaatlicher und kommunaler Ebene eine zunehmend große Rolle. So ist die Verbesserung der Identifikationssicherheit bei der elektronischen Kommunikation Bestandteil der E-Government-Strategie des Bundes [6]. Auch auf Verwaltungsebene entwickelt sich ein Problembewusstsein für die Notwendigkeit von zuverlässiger und rechtssicherer elektronischer Kommunikation [6].

Zukünftige Entwicklung
Da sich effektive elektronische Identifikations- bzw. Authentifizierungsverfahren bislang nicht flächendeckend durchsetzen konnten, ist davon auszugehen, dass die Bedrohung durch Identitätsdiebstahl weiter steigen wird [7, 8]. Die Einführung sicherer Verfahren, die auch die Privatsphäre ihrer Benutzer respektieren und persönliche Daten schützen, sollte daher hohe Priorität bei den Anbietern von Online-Diensten in E-Commerce und E-Governement genießen.

1.1 Beitrag

Die Notwendigkeit der Einführung solcher Verfahren macht das Thema dieses Aufsatzes relevant für die öffentliche Hand und privatwirtschaftliche Unternehmen. Dieser Artikel soll einen Weg aufzeigen, wie Identitätsattribute von Endnutzern unter Berücksichtigung der Privatsphäre des Einzelnen gewonnen, gespeichert und online nutzbar gemacht werden können.

Zusätzlich soll der vorgeschlagene Software-Dienst auch den Ansprüchen an Identitätssicherung in E-Commerce- und E-Governement-Szenarien genügen. Durch den

dezentralen Charakter des Software-Dienstes kann dieser in Form von „Authentication-as-a-Service“ bzw. „Identity-as-a-Service“ von Dienstanbietern eingesetzt werden. Dienstanbieter können somit auf den Betrieb einer eigenen komplexen Authentifizierungsarchitektur verzichten.

Ziel ist es letztlich, eine Identitätsmanagementsoftware zu gestalten, die einerseits Identitätsattribute verschiedener Quellen unterschiedlicher Vertrauenswürdigkeit zusammenführt und verwahrt, und andererseits die Weitergabe dieser Attribute an berechtigte Dritte per delegierter Authentifizierung ermöglicht. Eine solche Software könnte – hinreichende Marktdurchdringung und hoheitliche Unterstützung vorausgesetzt – Prozesse, die auf digitale Identitätsinformationen aufbauen, für alle Anspruchsgruppen signifikant verbessern: Endbenutzer würden mehr Privatsphäre und Sicherheit vor betrügerischer Nutzung ihrer Daten bei Online-Transaktionen erhalten. Kommerzielle Dienstanbieter würden durch eine geringere Anzahl von Betrugsfällen ihr Debitorenrisiko senken und könnten im Wissen, verlässlichere Identitätsdaten zu erhalten, auch höherwertigere Dienstleistungen online anbieten. Weite Teile des E-Government, die bislang durch die komplizierten bestehenden eID-Abläufe kaum Nutzer haben, könnten durch den Einsatz von besser benutzbaren Authentifizierungsstrategien einem weiteren Benutzerkreis zugänglich gemacht werden.

Im folgenden Kapitel wird der aktuelle Stand der Forschung – sowohl hinsichtlich Identitätsmanagementsystemen im Allgemeinen, als auch gängiger Verfahren der Identitätssicherung und hardwarebasierten Authentifizierung im Speziellen – gezeigt.

Anschließend wird das Umfeld von Identitätsmanagementsystemen beleuchtet. Hierzu werden die Anspruchsgruppen im Identitätsmanagement identifiziert und gesellschaftliche und politische Rahmenbedingungen für den Betrieb von Identitätsmanagementsystemen diskutiert.

Im vierten und fünften Kapitel wird die Proof-of-Concept-Implementation spezifiziert und aus einer technischen Perspektive beschrieben.

Die Arbeit schließt mit einer Evaluation der verwendeten Technologien ab.

2 Stand der Forschung und Standardisierung

2.1 Von domainbasierten zu offenen Identitätsmanagementsystemen

Das Identitätsmanagement ist eine der zentralen Funktionen von IT-Systemen, angefangen bei kleinen Betriebssystemen auf mobilen Geräten bis hin zu komplexen Computerarchitekturen wie Unternehmensnetzwerken. Jede Anwendung, die auf den Nutzer zugeschnittene Dienste anbietet oder in Abhängigkeit des Nutzers bestimmte Funktionen anbietet oder verbirgt, benötigt die Identität des Nutzers und es ist die Aufgabe des Identitätsmanagements, diese bereitzustellen. Entsprechend den sich wandelnden Anwendungslandschaften haben sich auch Identitätsmanagementsysteme von den Anfängen bis heute stark verändert, um den jeweils neuen Anforderungen der Anwendungen gerecht zu werden. Während in den Anfängen des Computerzeitalters mit wenig Nutzern und wenig Anwendungen jede Anwendung ihre Nutzer selbst verwaltete,

setzten sich vor allem in Organisationen und Unternehmen schnell so genannte domain-basierte Identitätsmanagementsysteme durch, welche die Identitäten der Nutzer für verschiedenste Anwendungen innerhalb einer abgeschlossen administrativen Domain zentral verwalteten. Analog zur physischen Pforte verwaltet das domain-basierte Identitätsmanagementsystem den Zugriff auf virtuelle Verzeichnisse und Anwendungen. Innerhalb geschlossener Benutzergruppen ist domain-basiertes Identitätsmanagement nach wie vor das vorherrschende Modell.

Jedoch hat sich die Welt gerade in den vergangenen Jahren zu einer hochgradig vernetzten Systemlandschaft mit stationären und mobilen Endgeräten gewandelt, in der Dienste mehr und mehr nicht nur innerhalb eines geschlossenen Netzwerkes, sondern über das Internet konsumiert werden. Die Situation einer abgeschlossenen Unternehmensgrenze, die man schützen kann, gibt es nicht mehr. Vielmehr – insbesondere auch mit dem Trend, Anwendungen in der Cloud zu nutzen – greifen Nutzer heute auf eine Vielzahl von Anwendungen zu, die außerhalb der Reichweite von domain-basierten Systemen liegen. Die Folge ist, dass die Identität für diese Anwendungen wieder neu in der digitalen Welt geschaffen werden muss und an vielen verschiedenen Stellen verwaltet wird. Das Dilemma der Identitätsinseln, die man im Internet vorfindet, versuchen neue so genannte offene Identitätsmanagementsysteme zu adressieren. Offene Identitätsmanagementsysteme verknüpfen bestehende domain-basierte Systeme, um kontrolliert Identitätsinformationen zwischen verschiedenen Sicherheitsdomänen auszutauschen. Spezielle Identitätsdienste, so genannte Identitätsanbieter und -intermediäre, sind das Herzstück dieser neuen Modelle.

Notwendiger Paradigmenwechsel

Aktuell besteht eine Diskrepanz zwischen den Anforderungen der heterogenen, vielfältigen Anwendungslandschaft und den vorherrschenden Identitätsmanagementsystemen, die dazu führt, dass Nutzeridentitäten an vielen Stellen mit ungenügender Absicherung verwaltet werden und Angriffsfläche für Identitätsdiebstahl und Onlinebetrug bieten. Um den aktuellen Anforderungen der Anwendungen und Nutzer gerecht zu werden, muss ein Paradigmenwechsel hin zu einem dezentralen und skalierbaren Identitätsmanagement stattfinden.

2.2 Identity Assurance

Identitätssicherung oder „Identity Assurance“, also die Abschätzung der Verlässlichkeit von Identitätsinformationen, bildet ein Kernelement dieses Paradigmenwechsels. Der Grund dafür ist, dass in dem Moment, wo Identitätsinformationen nicht mehr durch einen Dienstanbieter selbst, sondern durch einen externen Dritten verwaltet werden, der Dienstanbieter von diesem wissen muss, wieviel Vertrauen er in die externe Informationen haben kann.

Das Problem der Identity Assurance über verschiedene Vertrauensgrenzen hinweg wird von Forschern, Regierungen als auch internationalen Organisationen und Industriekonsortien adressiert. Das Ziel der Bemühungen internationaler Organisationen und

Regierungen sind globale Standards, die die Verlässlichkeit einer Identität, die über offene Netzwerke wie das Internet an Dritte weitergegeben wird, vereinheitlichen.

Identity Assurance Programme (IDAP)
Großbritannien war eines der ersten Länder, das Vertrauenslevel für die Authentifizierung definiert hat. 1999 hatte Premierminister Tony Blair das Ziel, dass Bürger wichtige Verwaltungsdienstleistungen über das Internet beauftragen können. Im Rahmen dieser Bestrebungen veröffentlichte das „UK Office of the e-Envoy" ein Dokument mit dem Titel „Registration and Authentication – e-Government Strategy Framework Policy and Guidelines" [24]. Teil dieses Dokuments war die Definition von vier Vertrauensstufen („LoAs"). Seit 2011 existiert das von der Regierung veranlasste *Identity Assurance Programme (IDAP)*, welches weitere Standards und Richtlinien für die Verifikation von Bürgeridentitäten festlegt [10, 11]. Darüber hinaus soll im Rahmen des Programmes ein Markt für *Identity Assurance Services* geschaffen werden, der es Bürgern erlaubt, aus einer Reihe von privatwirtschaftlichen, zertifizierten Anbietern zu wählen.

STORK Quality Authentication Assurance Framework
2004 wurde in Europa die Europäische Agentur für Netz- und Informationssicherheit (ENISA) gegründet, um Themen der Informationssicherheit auf europäischer Ebene zu adressieren. Eines der Projekte mit dem Fokus auf Identity Assurance ist STORK (Secure idenTity acrOss boRders linKed). STORK[3] und das Nachfolgeprojekt STORK 2.0[4] haben das Ziel, es allen Bürgern der EU zu ermöglichen, sich basierend auf den nationalen eID-Systemen in allen anderen EU-Ländern für E-Governmentdienste online zu authentifizieren. Eines der Ergebnisse des STORK Projektes ist das STORK Quality Authentication Assurance Framework [20]. Dieses definiert über den verschiedenen nationalen Systemen ein Schema von vier abstrakten Authentifizierungsleveln, sowie deren Abbildung auf nationale Level, um die jeweiligen Länderspezifika zu berücksichtigen.

Kantara Initiative
Die Kantara Initiative ist 2009 aus verschiedenen Bewegungen für ein offenes oder föderiertes Identitätsmanagement hervorgegangen (u.a. der Liberty Alliance und der Information Card Foundation). Wie die vorhergehenden Arbeiten definiert das Kantara Identity Assurance Framework [22] ebenso vier Vertrauenslevel.

ISO/IEC Standard DIS 29115 und ISO/IEC Working Draft 29003
Als internationaler und zukünftig möglicherweise wichtigster Standard definiert *ISO/IEC 29115* einen Rahmen für die Authentifizierung, der ebenso wie die erwähnten Ansätze vier Vertrauensstufen vorsieht. Als Ergänzung zu diesem Standard ist der Standard ISO/IEC 29003 [21] in Arbeit, welcher für die verschiedenen Vertrauensstufen konkrete Anforderungen an die Identitätsüberprüfung formuliert.

[3] `https://www.eid-stork.eu`
[4] `https://www.eid-stork2.eu`

2.3 Hardwarebasierte Authentifizierungsverfahren

Die verschiedenen Vertrauenslevel für die Authentifizierung hängen vom verwendeten Verfahren bzw. der Kombination verschiedener Verfahren ab. Die Authentifizierungsverfahren, sprich die Arten wie man sich im Internet ausweist, können grob in die drei Klassen *Wissen*, *Biometrie* und *Besitz* aufgeteilt werden.

Wissensbasierte Authentifizierung basiert auf der gemeinsamen Kenntnis eines Geheimnisses, wie zum Beispiel eines Passworts oder einer PIN, das nur der Authentifizierer und der zu Authentifizierende teilen. Obwohl diese Art der Authentifizierung über eine schlechte Benutzerfreundlichkeit und schlechte Sicherheitseigenschaften verfügt [3], ist sie ein De-facto-Standard in der IT.

Biometriebasierte Authentifizierung benutzt die körperlichen Merkmale wie Fingerabdruck, Iris oder das Gesicht. Biometrie ist mit zahlreichen Herausforderungen verbunden. So können sich die Merkmale über die Zeit verändern, wodurch sich die Wahrscheinlichkeit für eine fehlerhafte Zurückweisung (False Rejection) erhöht. Ebenso kann ein Angreifer versuchen, ein Merkmal zu kopieren, sodass es zu einer fehlerhaften Erkennung (False Acceptance) kommt.

Besitzbasierte Authentifizierung mittels Chipkarte

Besitzbasierte Authentifizierung arbeitet trivialerweise mit einem Beweis des Besitzes eines Merkmals. In der analogen Welt ist dieses Merkmal zum Beispiel eines der zahlreichen marktüblichen Identifikationsdokumente. Sollen diese Dokumente ebenfalls für die digitale Welt verwendet werden, müssen sie zusätzlich mit einem Sicherheitschip ausgerüstet sein, der einen sicheren Speicher für kryptografische private Schlüssel bereitstellt. Mit solch einem privaten Schlüssel wird dann ein kryptografischer Beweis über den Besitz des Dokuments erbracht.

Alternativen zur Chipkarte

Eine leichter nutzbare Ergänzung zu den hoheitlichen und kartenbasierten eID-Systemen stellen abgeleitete Identitäten [26] dar, die seit ca. 2 Jahren erforscht werden. Bei der Ableitung einer Identität werden die Daten aus dem Ausweis (Wurzelidentität) ausgelesen und kodiert in einem anderen Sicherheitschip hinterlegt.

Ein potentieller Industriestandard für die Authentifizierung könnte die FIDO-U2F-Spezifikation werden, auf die in dem späteren Abschnitt 3.4 eingegangen wird. Dabei authentifiziert sich der Benutzer mittels eines FIDO Tokens, der per USB mit dem PC verbunden wird.

3 Gesellschaftlicher und technischer Rahmen für sichere und erfolgreiche Identitätsmanagementsysteme

Technologische und gesellschaftliche Entwicklungen sind eng miteinander verknüpft, und so haben die vergangenen zehn Jahre nicht nur eine Reihe zukunftsweisender Technologien hervorgebracht, sondern mit ihrer Einführung auch das gesellschaftliche Leben nachhaltig verändert.

Mit der neuen Verfügbarkeit von Informationen und Dienstleistungen an jedem Ort (der mit dem Internet verbunden ist) und zu jeder Zeit lässt sich auch ein Wandel von der Produktgesellschaft zur Servicegesellschaft beobachten. Auch das Identitätsmanagement wird diesem Trend folgen.

3.1 Gesellschaftlich-politische Faktoren

Privatsphäre im Web

Den in den Jahren 2013 und 2014 von Edward Snowden enthüllten geheimdienstlichen Dokumenten verdankt die IT-Branche ein großes Interesse an Privatsphäre im Internet. Die auf diese Enthüllungen folgende lebendige Diskussion schaffte in weiten Teilen der Bevölkerung ein Problembewusstsein für Privatsphäre im Internet [1]. Die Zunahme institutioneller Überwachung und das resultierende Misstrauen geben Anlass, künftig neue Wege bei der Authentifizierung und Speicherung von Identitätsdaten zu gehen.

Dem Staat kommt dabei in gleich dreifacher Hinsicht eine hervorgehobene Rolle zu.

Erstens sind bei Behörden derzeit zahlreiche glaubwürdige und bestätigte Identitätsattribute hinterlegt, sodass diese als Identitätsanbieter fungieren und Identitätsinformationen bereitstellen können. Sie müssen diese entsprechend zuverlässig, sicher und einfach handhabbar zur Verfügung stellen.

Zweitens werden staatliche Stellen im Sinne zunehmenden E-Governments selbst als Nutzer Identitätsattribute abrufen[5]. Die erhoffte Zunahme elektronischer Behördengänge ist dabei auch von der Einfachheit für die Nutzer abhängt.

Und drittens muss der Staat die Architektur des Identitätsmanagements, die Intermediäre und den sich unter ihnen entwickelnden Wettbewerb wirksam regulieren. Dies betrifft u.a. das Setzen von Standards zu Sicherheit und Datenschutz, die Zertifizierung der Intermediäre und Regelungen für deren möglichen Marktaustritt sowie rechtsklare Bestimmungen, um den technischen Ausschluss nicht mandatierten (staatlichen oder privaten) Zugriffs auf die hinterlegten Attribute nachzuvollziehen[6]. Auch sind wettbewerbs- und kartellrechtliche Aspekte relevant, um eine mögliche Konzentration auf nur einen oder wenige große Identitätsintermediäre am Markt zu vermeiden.

Usability und Einfachheit

Ein wichtiger Faktor bei der Akzeptanz neuer Technologien ist deren einfache Nutzbarkeit. Auch hier ist ein deutlicher Wandel in der Gesellschaft erkennbar. Intuitives User Interface und Interaction Design ist längst zu einer Grundanforderung an Software geworden. Entsprechend verhält es sich auch bei Sicherheitslösungen. Diese müssen für Endnutzer einfach benutzbar oder im besten Fall gar nicht sichtbar sein.

[5] Beispielsweise bei der Authentifizierung des Bürgers bei Online-Anforderung eines polizeilichen Führungszeugnisses.

[6] Telekom-Provider können zum Beispiel verpflichtet werden, zur Strafverfolgung Verkehrsdaten herauszugeben. Dies ist beim vorliegenden ID-Management technisch nicht möglich, sollte aber auch rechtlich ausgeschlossen werden.

3.2 Anforderungen an Identitätsmanagementprovider

Die vorhergehenden Betrachtungen führen zu der Frage, wie ein Identitätsmanagement für das Internet aussehen müsste, das gleichermaßen von Staat, Nutzern und Wirtschaft akzeptiert wird. Während aus technischer Sicht ein dezentrales offenes Identitätsmanagement mit verschiedenen Verwaltern der Identität, den Identitätsanbietern und -intermediären, als plausibel und machbar erscheint, so gibt es aus gesellschaftlicher Perspektive große Akzeptanzhürden hinsichtlich globaler Bereitstellung von Identitätsinformationen. Betrachtet man die Onlinewelt, so stellt sich die Frage, wer der Betreiber eines solchen sicherheitskritischen Dienstes sein könnte bzw. welche Anforderungen ein Anbieter und Betreiber eines Identitätsmanagementdienstes erfüllen muss, um als solcher von Dienstanbietern und Nutzern akzeptiert zu werden.

Eine der wichtigsten Voraussetzungen ist das Vertrauen von Nutzern, Wirtschaft und Politik in den Betreiber eines solchen Dienstes. Im Folgenden werden die wichtigsten Vertrauensfaktoren und damit Anforderungen an Betreiber eines Identitätsmanagementdienstes beschrieben.

Sicherheit
Ein entscheidender Aspekt für das Vertrauen sowohl der Nutzer als auch der Dienstanbieter ist die Einhaltung von Sicherheitsstandards durch den Identitätsdienstleister. Als mögliche Betreiber, welche diese Voraussetzung erfüllen, kommen hier insbesondere nach dem Signaturgesetz akkreditierte Trustcenter in Frage. Diese erfüllen schon heute gesetzlich festgelegte Voraussetzungen, um die Zuverlässigkeit und Integrität von Identitätsdaten zu gewährleisten.

Verfügbarkeit
Sowohl die kurzfristige als auch langfristige Verfügbarkeit ist ein weiterer wichtiger Vertrauensaspekt für Endnutzer und Dienstanbieter bei der Wahl eines Identitätsdienstleisters. Die Verfügbarkeit eines solchen Dienstes ist essentiell, da er als zentrale Infrastrukturkomponente Voraussetzung für das reibungslose Funktionieren einer potenziell großen Menge an Applikationen und Diensten ist.

Neutralität und wirtschaftliche Interessen
Ein weiterer Vertrauensbonus entsteht, wenn ein Betreiber eines Identitätsdienstes als neutral betrachtet wird und geringe eigene wirtschaftliche Interessen hat. Persönliche Daten – insbesondere, wenn diese verifiziert wurden – haben einen hohen wirtschaftlichen Wert.

Flexibles Angebot
Internetdienstleistungen sind vielfältig, und ebenso vielfältig sollte auch das Angebot eines Identitätsdienstleisters sein. Dies umfasst zum Beispiel ein Angebot verschiedener Kanäle der Registrierung und Authentifizierung von Nutzern.

Fasst man die verschiedenen Eigenschaften zusammen, so bieten sich als Identitätsmanagementprovider im Sinne eines Identitätsmediator vor allem etablierte Unternehmen mit gesellschaftlichem Auftrag an, welche bereits heute über ein Trustcenter verfügen und somit diese Rolle schon heute wahrnehmen. Als Identitätsanbieter im Sinne der Quelle einer Identitätsinformation kommen dagegen alle öffentlichen oder

auch privaten Stellen in Frage, die Identitätsinformationen generieren und dafür ein entsprechendes Vertrauen genießen.

3.3 Delegierte Authentifizierung mit OAuth 2.0

Möchte ein Dienstanbieter die Benutzerauthentifizierung auf einen vertrauenswürdigen Dritten, einen Identitätsanbieter, auslagern, müssen neben den organisatorischen auch zahlreiche technische Herausforderungen gelöst werden.

Für die Kommunikation zwischen diesen Parteien existieren bereits die Protokolle SAML und OpenID. SAML 2.0[7] (Security Assertion Markup Language) wird zum Beispiel im deutschen eID-System oder STORK verwendet, ist allerdings sehr komplex. Eine einfacher zu implementierende Alternative stellt OpenID 2.0[8] dar, das allerdings für umfangreichere Szenarien zu limitiert ist und Erweiterungen benötigt.

3.3.1 OAUth

OAuth wurde 2007 in einer ersten Version veröffentlicht [18]. Ein Benutzer kann damit die Autorisierung für den Zugriff auf Ressourcen von ihm, die auf einem bestimmten Ressourcenserver liegen, an eine Webanwendung delegieren, ohne dass er seine Login-Daten für den Ressourcenserver an diese weitergeben muss. Auf den gesammelten Erkenntnissen der ersten Version aufbauend, wurde 2012 der Nachfolger OAuth 2.0 [19] spezifiziert. Eine Prämisse dabei war die einfachere Integration, sodass es komplett auf HTTP aufsetzt und Nachrichten zwischen den Parteien mittels HTTP-GET bzw. HTTP-POST übertragen werden.

OAuth definiert vier Rollen: Client, Resource Owner, Resource Server und Authorization Server. Bei dem *Client* handelt es sich um die Webanwendung, die Zugriff auf eine Ressource des *Resource Owner*, in der Regel der Benutzer, benötigt. Diese Ressource liegt wiederum auf einem *Resource Server*, der eine Zugriffsbeschränkung besitzt. Für den Zugriff benötigt der Client eine Berechtigung vom *Authorization Server*, die ihm allerdings nur der Benutzer verschaffen kann.

Kommunikationsüberblick

Der Client leitet den Benutzer zum Authorization Server und übergibt ihm dabei diverse Parameter, wie zum Beispiel eine Rücksprungadresse und eine Client-ID. Der Authorization Server authentifiziert anschließend den Benutzer mittels eines in OAuth nicht näher spezifiziertem Mechanismus. Denkbar wäre hier zum Beispiel die Nutzung eines FIDO Tokens. Nachdem der Benutzer sich authentifiziert und der Ressourcenfreigabe für den Client zugestimmt hat, wird er zusammen mit einem sogenannten Authorization Grant zum Client zurück geleitet. Dieser Authorization Grant ist im Regelfall ein Code, mit dem der Client, entweder wieder über den Benutzer oder diesmal direkt, beim Authorization Server einen Access Token abrufen kann. Solch ein Access Token hat eine begrenzte Laufzeit und berechtigt den Client zum Zugriff auf die angeforderten Ressourcen. Übersendet der Client bei der Ressourcenanfrage seinen Access

[7] http://docs.oasis-open.org/security/saml/v2.0/
[8] http://openid.net/

Token an den Resource Server, muss dieser noch die Gültigkeit des Tokens überprüfen. Ist der Token für den Zugriff gültig, erhält der Client die Ressource.

Verwendung zur delegierten Authentifizierung
Alles in allem ist OAuth 2.0 ein überschaubares Protokoll für die delegierte Autorisierung. Da sich der Benutzer hierbei gegenüber einem Identitätsanbieter (dem Authorization Server) authentifizieren muss und der anfragende Dienst (der Client) daraufhin eine Rückmeldung (Authorization Grant) erhält, eignet sich das Protokoll prinzipiell auch gut für die delegierte Authentifizierung. Soll die Authentifizierung gleich mit einer Attributabfrage kombiniert werden, können sogar Resource Server und Authorization Server kombiniert werden. Diese senden dann statt eines Authorization Grants gleich die angeforderte Ressource.

3.4 Hardwarebasierte Authentifizierung mit dem FIDO U2F Protokoll

Ein erster Versuch, hardwarebasierte Authentifizierung offen und herstellerübergreifend möglich zu machen, wird derzeit von der „FIDO (Fast IDentity Online) Alliance“ unternommen. Dieser Zusammenschluss zahlreicher Industriepartner[9] ist eine gemeinnützige Organisation[10], die eine offene, herstellerunabhängige Spezifikation zur Hardwareauthentifizierung entwickelt hat. Der unter dem Namen „U2F“ veröffentlichte Teil der Spezifikation [16] regelt den Einsatz von Authentifizierungstokens als „second factor“, zusätzlich zu einem herkömmlichen Passwort. Die Spezifikation hat im Dezember 2014 Implementierungsreife erreicht [14]. Ihr Kern ist ein Challenge-Response-Verfahren, bei dem eine – beliebig gestaltete – Hardware-Komponente verwendet wird.

U2F Authenticator
Die zur Authentifizierung genutzte Hardware-Komponente wird in der Spezifikation unter dem Begriff „FIDO Authenticator“ geführt. Diese Hardware-Komponente kann in Bauform eines USB-Sticks vorliegen und über USB-HID mit dem Rechner eines Anwenders kommunizieren.

Relying Party
Der Begriff „Relying Party“ – sinngemäß „akzeptierender Dritter“ – bezeichnet in der Nomenklatur der Spezifikation eine Entität, die das FIDO-Protokoll zur Authentifizierung von Benutzern verwendet. Dies kann zum Beispiel ein Internetdienstanbieter wie ein Online-Shop sein. Auch ein Identitätsintermediär stellt in diesem Zusammenhang eine „Relying Party“ dar, da er Benutzer delegiert authentifiziert (vgl. 3.3).

Authentifizierung im Browser
Ein Benutzer authentifiziert sich also mittels eines „U2F Authenticators“ bei einem Dritten. Damit diese beiden Beteiligten miteinander kommunizieren können, müssen weitere Voraussetzungen geschaffen werden. Die relevanten Komponenten sind in

[9] Derzeit haben sich etwa 150 IT-Unternehmen der Organisation angeschlossen. Zu ihnen gehören unter anderen Google, Microsoft und PayPal. Eine aktuelle Liste teilnehmender Partner ist unter `https://fidoalliance.org/membership/members/` im Internet abrufbar.
[10] Die „FIDO Alliance“ ist in den USA als „tax-exempt nonprofit organization“ nach USC 26 § 501 (c) anerkannt.

Abbildung 1 dargestellt. Der „U2F Authenticator“ steht am Anfang der Kommunikationskette. Diese Hardwarekomponente enthält ein Secure Element, welches über USB HID angesprochen werden kann. Über diese Schnittstelle können dann Nachrichten, die im Einklang mit dem „U2FHID“ Protokoll [15] formatiert sind, ausgetauscht werden. Diese Nachrichten dienen entweder der Initialisierung eines spezifischen Schlüssels für einen akzeptierenden Dritten oder der Authentifizierung mit einem bereits registrierten Schlüssel. In beiden Fällen findet die Kommunikation mit einem Browser statt. Dieser baut – in der Regel mit Hilfe eines Plugins/einer Erweiterung[11] – einerseits die USB-HID-Verbindung zur Hardware auf und stellt andererseits auch eine JavaScript-Schnittstelle zur Verfügung.

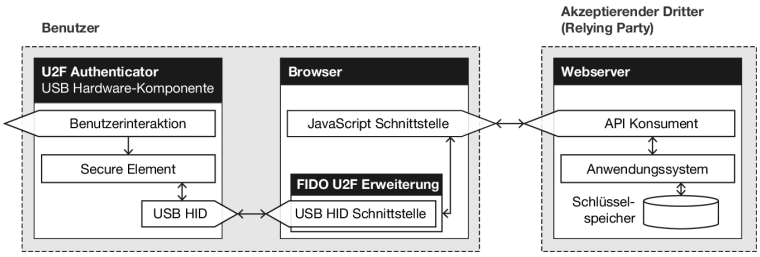

Abbildung 1: FIDO U2F Authentifizierungsarchitektur

Dieser Schnittstelle können sich nun Webseiten von akzeptierenden Dritten bedienen, indem sie die von der JavaScript API definierten Methoden [16] für den Informationsaustausch nutzen. Zusammenfassend ermöglicht es diese Architektur akzeptierenden Dritten – also auch dem hier dargestellten Identitätsintermediär – Hardwareauthentifizierung mittels einer einfachen JavaScript API aus dem Frontend der Webapplikation heraus zu betreiben.

3.5 Identitätssicherung

Verfahren zur Identitätssicherung existieren viele. Oftmals installieren Dienstanbieter eigene Verfahren, um zumindest Teile einer Identität zu prüfen. Ein gängiges Verfahren ist hier z.B. die Bestätigung einer E-Mail durch einen Verifikationslink zum Abschluss einer Registrierung.

Mit dem neuen Personalausweis und der integrierten eID Funktion besteht die Möglichkeit der vollständig elektronischen Identitätsprüfung. Da die Nutzung der eID Funktion jedoch mit einigen Hürden verbunden ist, reagiert der Markt mit neuen Lösungen, die leichter zu handhaben sind, jedoch geringere Sicherheit bieten. Hierzu gehören insbesondere VideoIdentlösungen, die durch einfaches Abfilmen eines Ausweisdokumentes und dem Abgleich mit dem Gesicht des Nutzers durch wahlweise technologische Algorithmen oder auch durch einen Menschen die Identität des Nutzers prüfen.

[11] Lediglich für den Browser „Google Chrome“ ist eine Integration dieser Funktionalität ohne die Notwendigkeit von Plugins kurzfristig geplant.

4 Spezifikation

Die hier beschriebene Proof-of-Concept-Implementation ermöglicht die Authentifizierung eines *Benutzers* gegenüber einem *Dienstanbieter* unter Verwendung eines *Authentifizierungsdienstes*. Aus dieser Anforderung lassen sich die in Abb. 2 skizzierten und im Folgenden beschriebenen sechs Hauptanwendungsfälle ableiten. Ein Dienstanbieter ist hier sowohl eine Organisation, die zur Durchführung ihrer Geschäfts- oder Verwaltungstätigkeit Attribute eines Benutzer liest (z.B. E-Commerce- und E-Government-Anwendungen) als auch eine Organisation, die aufgrund ihrer besonderen Stellung berechtigt ist, Attribute eines Benutzers zu verifizieren (z.B. staatliche Stellen). Eine solche wird auch als *Identitätsanbieter* bezeichnet.

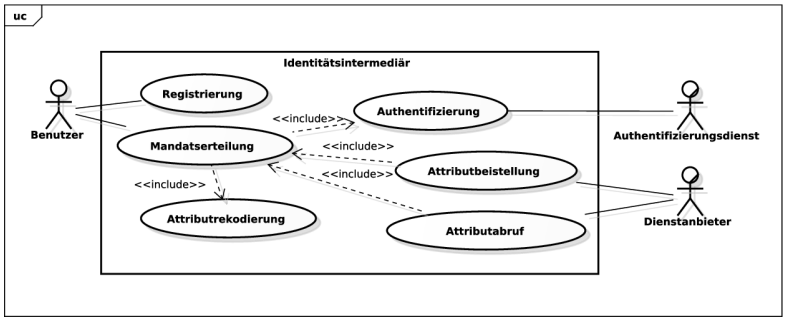

Abbildung 2: Anwendungsfalldiagramm der Kernkomponenten

Registrierung

Der Benutzer soll mit dem Identitätsintermediär zunächst zum Zwecke der Registrierung interagieren. Hier muss der Benutzer auch ein Passwort festlegen, welches dem Identitätsintermediär in einem geeigneten Format überspielt werden soll. Dieses Format darf eine Dekodierung des Passwortes nicht zulassen. Weiterhin muss in diesem Schritt eine Registrierung des vom Benutzer verwendeten „U2F Authenticators“ (vgl. 3.4) im Sinne der FIDO U2F Spezifikationen über die FIDO U2F API [16] vorgenommen werden. Der spezifikationsgemäß vom „U2F Authenticator“ zu erzeugende „Key Handle“ muss zusammen mit den vorhandenen Benutzerinformation zur späteren Authentifizierung datenbankseitig abgelegt werden. Zusätzlich sollen zu diesem Zeitpunkt auf dem System des Benutzers private und öffentliche Schlüssel in einem geeigneten asymmetrischen Verschlüsselungsverfahren zur späteren Nutzung erzeugt und unter Berücksichtigung der Sicherheitserfordernisse abgelegt werden.

Mandatserteilung

Mandatserteilung bezeichnet den Anwendungsfall, in dem ein *Benutzer* einen *Dienstanbieter* berechtigt, auf seine beim Identitätsintermediär gespeicherten Attribute entweder lesend zuzugreifen, oder in seinem Namen dem Identitätsintermediär neue Informationen zu seiner Identität beizustellen. Für die Mandatserteilung muss der Benutzer sich einerseits bei einem *Authentifizierungsdienst* zweifelsfrei authentifizieren und andererseits seine Zustimmung zur Transaktion geben. Das resultierende Mandat berechtigt folglich den betroffenen Dienstanbieter nominell zum Zugriff auf die Identität des Benutzers.

Authentifizierung
Die Erteilung eines Mandats setzt die Authentifizierung eines Benutzers voraus, die nach einer beliebigen – vom Identitätsintermediär geduldeten – Methode durchgeführt werden muss. Den Erfolg oder Misserfolg einer Authentifizierungsanfrage hat der Authentifizierungsdienst dem Identitätsintermediär direkt zu bescheinigen.

Attributbeistellung
Vom Identitätsintermediär berechtigte Stellen sollen in die Lage versetzt werden, der Datenbank verschlüsselt über eine geeignete Schnittstelle Attribute beizustellen. Hierzu ist ein Mandat erforderlich. Kann ein Dienstanbieter ein entsprechendes gültiges Mandat vorweisen, soll es ihm ermöglicht werden, die Attribute in einer benutzerzentrisch verschlüsselten Form und über einen verschlüsselten Kanal zu übertragen. Die übertragenen Attribute können weiterhin mit einem Vertrauensgrad (vgl.

3.5) ausgestattet werden, der es erlaubt, ihre Vertrauenswürdigkeit zu bewerten. Der zugeteilte Vertrauensgrad muss dabei im Ermessensspielraum des beistellenden Dienstanbieters – des sog. Identitätsanbieters – liegen. Dieser muss ebenfalls mit geeigneten technischen Mitteln Sorge dafür tragen, dass die Integrität eines übertragenen Attributes sichergestellt ist.

Attributabruf
Der Anwendungsfall des Attributabrufs kommt in seiner Spezifikation der Attributbeistellung nahe. Auch für den Abruf der Attribute ist ein Mandat vorauszusetzen. Nachdem der Dienstanbieter dem Identitätsintermediär beweist, dass ein gültiges Mandat vorliegt, soll der Dienstanbieter in die Lage versetzt werden, die mandatierten Attribute abzurufen. Diese Attribute sollen dann über eine geeignete Schnittstelle in einer individuell verschlüsselten Repräsentation dem Dienstanbieter zum Abruf angeboten werden.

Attributrekodierung
Eine Rekodierung der Attribute wird immer dann nötig, wenn ein neuer Dienstanbieter lesenden Zugriff auf sie erhalten soll (Mandatserteilung) oder wenn Attribute durch schreibenden Zugriff geändert werden sollen. Die neu zu verschlüsselnden Attribute müssen dafür dem Benutzer in verschlüsselter Form zur Rekodierung zugespielt werden. Der Benutzer muss daraus individuell verschlüsselte Repräsentationen erzeugen.

Verschlüsselung
Um eine größtmögliche Sicherheit vor der Manipulation von Benutzerdaten ohne das Wissen des Benutzers zu bieten und um das Risiko eines Komplettverlusts der vom Identitätsintermediär gespeicherten Daten – z.B. durch einen Hackerangriff – zu minimieren, müssen die Attribute in einer speziellen Form verschlüsselt gespeichert werden. Diese Form muss es einerseits möglich machen, dass der rechtmäßige Besitzer der Daten die Möglichkeit hat, diese zu dekodieren, ohne dass sie im Klartext vorliegen. Andererseits muss das ursprüngliche Identitätssicherungsniveau persistent und fälschungssicher mit dem zugehörigen Attribut gespeichert werden.

5 Implementation

Die hier vorgestellte Architektur basiert auf dem Implementationsentwurf der Arbeit „Secure Authentication and Attribute Sharing in Federated Identity Scenarios“ [25], der im Anschluss hinsichtlich einiger technischer Aspekte überarbeitet wurde.

Die als Proof-of-Concept implementierte Service Architektur besteht aus Java Webservices, die ein Benutzerinterface und verschiedene REST basierte Schnittstellen bereitstellen. Das grafische Benutzerinterface ist als HTML5/CSS3 Applikation realisiert.

Die – im Falle des Einsatzes eines auf FIDO U2F basierenden Authentifizierungsdienstes – nötige Kommunikation der Web-Applikation mit dem „U2F Authenticator“ (vgl. 3.4) und die benutzerseitige Verschlüsselung von Attributen (vgl. 5.1) findet per JavaScript statt. Die im Benutzerinterface verwendeten Technologien sind zum Teil noch nicht flächendeckend in Browsern implementiert. Insbesondere der Einsatz der „W3C Web Cryptography API“ [17] für kryptographische Anwendungen im Browser (vgl. 5.1) ist derzeit nur in einigen aktuellen Browsern verfügbar [2].

Die Funktionsweise der Implementation lässt sich gut anhand eines typischen Benutzungsverlaufs beschreiben. Die in diesen Benutzungsverlauf involvierten Parteien sind die bekannten Stakeholder offener Identitätsmanagementsysteme (vgl. 2.1). Namentlich Benutzer (*B*), Dienstanbieter (*D*), Authentifizierungsdienste (*A*) und der Identitätsintermediär (*I*) selbst.

Registrierung

Dem später dargestellten typischen Anwendungsfall der Benutzung geht die Registrierung eines Benutzers *B* voraus, die in Abb. 3 nicht dargestellt ist. Hierbei wird eine Benutzerkennung erzeugt und zusammen mit der E-Mail-Adresse des Benutzers als Hauptmerkmal in der Datenbank des Identitätsintermediärs (*I*) gespeichert. Hier legt der Benutzer auch ein Passwort fest, dessen Abbildung nach browserseitig berechnet und ebenfalls in der Datenbank gespeichert wird[12]. Weiterhin wird der spezifikationsgemäß vom „U2F Authenticator“ erzeugte „Key Handle“ zusammen mit den vorhandenen Benutzerinformationen zur späteren Authentifizierung datenbankseitig abgelegt. Zusätzlich werden hier im Browser individuelle kryptographische Schlüssel für die spätere Verwendung erzeugt (vgl. 5.1).

Dienstanbieter

Ein typischer Benutzungsablauf gestaltet sich wie in Abb. 3 dargestellt. Ein Benutzer interagiert zunächst mit einem Dienstanbieter.

[12] Das Passwort selbst wird nicht übermittelt.

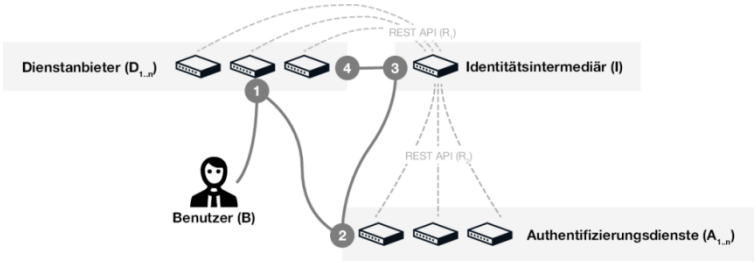

Abbildung 3: Benutzungsablauf und Schnittstellen

Diese Interaktion verläuft zunächst komplett im Hoheitsbereich des Dienstanbieters (1). Beispielsweise könnte ein Benutzer *B* das Sortiment eines Online-Shops D_1 durchsuchen und Artikel einem virtuellen Einkaufswagen hinzufügen. Er könnte sich auch auf der Webseite eines weiteren Dienstanbieters D_2 – zum Beispiel seiner Hausbank – zum Zwecke der Attributbeistellung konkreter Identitätsattribute (hier etwa Kontonummern) bewegen. D_2 würde hier also als Identitätsanbieter auftreten.

Sollte *D* die Infrastruktur von *I* zur Gewinnung oder Beistellung von Identitätsinformationen des *B* verwenden wollen, so wird er seinen Browser im Folgenden auf einen HTTP-Endpunkt eines Authentifizierungsdienstes *A* weiterleiten. Die Struktur der URL, auf die *B* weitergeleitet wird, entspricht dabei einer im Voraus definierten, an „OAuth 2“ (vgl. 3.3) angelehnten, Konvention und beinhaltet neben einer später zu verwendenden Rückleitungs-URL auch eine eindeutige Identifikationsnummer, die *D* zuvor von *I* zugewiesen wurde, eine Liste von Attributen, auf die *D* zugreifen möchte sowie die Information darüber, ob ein lesender oder schreibender Zugriff angestrebt ist.

Authentifizierungsdienst

Indem er dieser URL folgt bzw. darauf weitergeleitet wird, begibt sich *I* in den Hoheitsbereich 2 eines Authentifizierungsdienstes A_1. Das könnte zum Beispiel ein Authentifizierungsdienst sein, der „FIDO“ in Kombination mit einem Passwort verwendet. A_1 nimmt nun – durch Nutzung der jeweils vorgesehen Methode – die Authentifizierung vor. Nötige Meta-Daten – im Falle der Authentifizierung mit „FIDO U2F“ etwa Key Handle und öffentlichen Schlüssel, sowie den Passworthash des Benutzerpassworts – kann A_1 über eine von *I* zur Verfügung gestellte REST-API (R_1) abrufen. Sollte die Authentifizierung nach Maßgabe von A_1 erfolgreich verlaufen sein, wird dies gegenüber *I* per API R_1 kommuniziert.

Identitätsintermediär

Anschließend erreicht der Benutzer – per Weiterleitung des Browsers auf eine URL des *I* – den Hoheitsbereich 3 des Identitätsintermediärs. Zu diesem Zeitpunkt hat der Benutzer sich für die ursprüngliche Anfrage von D_1 bzw. D_2 *authentifiziert*. Diese Anfrage ist jedoch noch nicht *mandatiert*. Zur Mandatierung muss *B* nun im Hoheitsbereich 3 seine explizite Zustimmung geben. Hier wird er auch auf den Umfang des Mandats (also welche Attribute betroffen sind), den Gültigkeitszeitraum des Mandats und, ob es sich um einen lesenden oder schreibenden Zugriff handelt, informiert. Ex-

plizite Zustimmung des Benutzers vorausgesetzt, werden nun im Falle eines lesenden Zugriffs die zur Verfügung zu stellenden Attribute in einer für D_1 bzw. D_2 geeigneten Repräsentation verschlüsselt (vgl. 5.1).

Rückkehr zum Dienstanbieter
Nach expliziter Zustimmung wird *B* von *I* – wiederum in Anlehnung an OAuth 2 – zurück zu *D* geleitet. Die Rückleitungs-URL – mit der *B* zurück in den Hoheitsbereich des ursprünglichen Dienstanbieters D_1 bzw. D_2 gelangt – beinhaltet einen Mandatsschlüssel, mit dem D_1 bzw. D_2 schließlich die REST-API R_2 zum Abruf oder zur Beistellung von Identitätsattributen nutzen kann.

5.1 Verschlüsselungsimplementation

Um den in spezifizierten Anforderungen gerecht zu werden, müssen beim Identitätsintermediär gespeicherte Attribute so verschlüsselt werden, dass sie nur von berechtigten Parteien entschlüsselt werden können. *Berechtigte Parteien* sind hierbei lediglich der Benutzer selbst, sowie explizit vom Benutzer beauftragte Dienstanbieter. Da die Identitätsattribute dennoch zentral bei einem Identitätsintermediär gespeichert werden müssen, liegen diese dort in verschlüsselten Repräsentationen vor.

Anhand des Beispielszenarios, das in Abb. 4 dargestellt ist, lässt sich die gewählte Verschlüsselungslogik illustrieren. Die abgebildete Entschlüsselungsmatrix zeigt drei Attribute ($Attr_{1..3}$) eines Benutzers. Diese liegen wiederum in drei Repräsentationen (R_B , R_{D1} und R_{D2}) vor. R_B bezeichnet hierbei die Benutzerrepräsentation, die lediglich mit dem zuvor generierten privaten Schlüssel des Benutzers *B* entschlüsselt werden kann.

R_{D1} ist die Repräsentation, die für einen fiktiven Dienstanbieter *D*1 erstellt wurde. In diesem Beispiel wird angenommen, dass der Benutzer *B* dem Dienstanbieter *D*1 ein Mandat für den Zugriff lediglich auf $Attr_1$ gewährt hat. Folglich enthält die Repräsentation R_{D1} lediglich dieses Attribut in einer Form, die spezifisch für *D*1 ist, die also mit seinem öffentlichen Schlüssel verschlüsselt wurde.

R_{D2} ist demnach eine Repräsentation, die explizit für *D*2 hergestellt wurde. Sie enthält die Attribute $Attr_1$ und $Attr_2$ in speziell verschlüsselter Form.

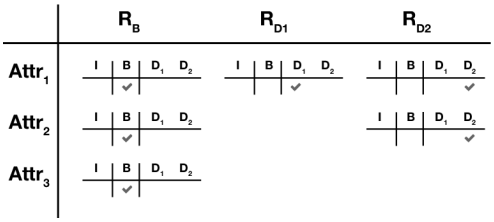

Abbildung 4: Spezifikation einer Entschlüsselungsmatrix

Vorbereitung der Verschlüsselung während der Registrierung
Um die benutzer- und anbieterspezifische Verschlüsselung möglich zu machen, muss der Browser des Benutzers während seiner Registrierung ein individuelles RSA-Schlüsselpaar erzeugen, das künftig für die Verschlüsselung von Attributen durch den Benutzer verwendet wird[13]. Der private Schlüssel dieses Schlüsselpaars wird – wiederum browserseitig – symmetrisch mit dem „Advanced Encryption Standard (AES)“ [23] unter Zuhilfenahme des Passworts des Benutzers verschlüsselt. Der öffentliche Schlüssel wird – wie der symmetrisch verschlüsselte private Schlüssel – ebenfalls in der Datenbank des Identitätsintermediärs gespeichert.

Attributverschlüsselung während der Attributbeistellung
Alle vom Identitätsintermediär gespeicherten Attribute kommen von Dienstanbietern, die als Identitätsanbieter handeln. Damit diese Attribute nicht unverschlüsselt zum Identitätsintermediär übertragen werden, erhalten Identitätsanbieter im Rahmen der Mandatierung auch den – während der Registrierung generierten – öffentlichen Schlüssel des jeweiligen Benutzers und aller derzeit für das Attribut mandatierten konsumierenden Dienstanbieter. Dienstanbieter, die Attribute übertragen, müssen dann diese Schlüssel zur Verschlüsselung verwenden. Da sie auch für das Identitätssicherungsniveau („LoA“) der übertragenen Attribute bürgen, müssen die betroffenen Dienstanbieter weiterhin einen SHA-256-Hash [12] beisteuern. Dieser Wert wird mit dem verschlüsselten Attribut gespeichert und kann später von konsumierenden Dienstanbietern zur Integritätssicherung benutzt werden. Sie können so feststellen, ob der Wert des mit dem jeweiligen Identitätssicherungsniveau versehenen Attributs dem erhaltenen Attributwert entspricht.

Attributrekodierung während der Mandatserteilung
Erteilt ein Benutzer einem Dienstanbieter ein Mandat, so muss eine dienstanbieterspezifische Repräsentation der mandatierten Attribute erstellt werden (vgl. 4). Zu diesem Zweck erhält der Benutzer vom Identitätsintermediär vor der Mandatserteilung den öffentlichen Schlüssel des jeweiligen konsumierenden Dienstanbieters. Mit diesem öffentlichen Schlüssel wird dann – im Browser – eine dienstanbieterspezifische verschlüsselte Variante aller mandatierten Attributwerte erzeugt. Diese Variante wird an den Identitätsintermediär zurückgespielt und kann zukünftig vom jeweiligen Dienstanbieter abgerufen werden. Da die Attributverschlüsselung im Browser des – potenziell nicht vertrauenswürdigen – Benutzers vorgenommen wurde, kann der konsumierende Dienstanbieter den während der Attributbeistellung ursprünglich erzeugten Hashwert zur Validierung der erhaltenen Attribute verwenden.

Die Attributwerte sind so für den Identitätsintermediär opak, ihr Identitätssicherungsniveau kann dennoch durch Dienstanbieter validiert werden.

[13] Zur späteren Ver- und Entschlüsselung würde sich das private Schlüsselmaterial, das durch den „U2F Authenticator“ erzeugt wurde, sehr gut eignen. Durch die Spezifikation der U2F API, die lediglich das Signieren von Daten – und nicht deren Entschlüsselung – durch das integrierte Secure Element vorsieht, kommt dies jedoch nicht infrage (vgl. 7).

6 Ausblick

Die Proof-of-Concept-Umsetzung erfüllt technisch die spezifizierten Anforderungen (vgl. 4). Der mit ihr verfolgte Ansatz wird auch für geeignet gehalten, innerhalb des dargestellten gesellschaftlichen und politischen Rahmens (vgl. 3.1) zu funktionieren. Einige Faktoren, die den Erfolg dieses Identitätsmanagementsystems beeinflussen können, sind jedoch bislang ungeklärt.

Marktdurchdringung des „FIDO U2F“ Standards
Der Erfolg eines Dienstes, der Hardware zur Authentifizierung verwendet, ist eng an die Marktdurchdringung der verwendetet Hardwarekomponenten gekoppelt. Obwohl der „FIDO U2F“ Standard breite Industrieunterstützung genießt und bereits in Web-Anwendungen genutzt wird[14], ist noch keine nennenswerte Verbreitung der nötigen Hardware feststellbar.

Verfahren der Attributverschlüsselung
In der Vorbereitung der ursprünglichen Implementation [25] war geplant, das private Schlüsselmaterial, das spezifikationsgemäß auf dem FIDO U2F Authenticator vorliegt, auch zur Entschlüsselung von Nachrichten, die nicht authentifizierungsspezifisch sind, zu nutzen. Während dieser Ansatz für die Attributverschlüsselung besonders sinnvoll wäre, ist er aufgrund der Limitierung der FIDO U2F API [16] auf für das Challenge-Response-Verfahren nötige Funktionen nicht realisierbar. Der Attributverschlüsselungsalgorithmus dieser Implementierung ist daher – zumindest bei Totalverlust der Datenbank (zum Beispiel in Folge eines Hackerangriffs auf das System) – nicht stark genug, um Entschlüsselungsversuchen mit Brute-Force-Methoden standzuhalten. Grund hierfür ist die unter Umständen geringe Entropie von benutzergewählten Passworten, die in letzter Instanz für die Verschlüsselung der Attribute verwendet werden. Eine zukünftige Erweiterung der API zu diesem Zweck wäre wünschenswert.

7 Schlussfolgerung

Das Internet hat die Vernetzung der Welt auf revolutionäre Art und Weise ermöglicht. Auch heute setzt sich diese Entwicklung kontinuierlich fort. Nahezu täglich entstehen Ideen für neue Anwendungen und Dienste auf der Basis einer vernetzten Welt. Diese Trends und damit verbundenen gesellschaftlichen Entwicklungen erfordern auch neue Modelle für das Identitätsmanagement, die in heterogenen Umgebungen wie dem Internet funktionieren.

Dieses Paper zeigt einerseits Ansätze für ein dezentrales zukunftsfähiges Identitätsmanagement auf und diskutiert und untersucht seine Rahmenbedingungen. Als gesellschaftliche Rahmenbedingungen werden vor allem Vertrauen in die Anbieter von Identitätsdiensten sowie die Benutzbarkeit von Identitätsdiensten genannt.

Zum anderen wird ein Proof-of-Concept für die technische Machbarkeit als prototypische Umsetzung einer Softwarelösung beschrieben. Die vorgestellte Software bietet durch den Einsatz von Hardware-Authentifizierung nach dem „FIDO U2F“ Protokoll

[14] Google setzt das Protokoll seit Oktober 2014 produktiv ein [13].

höhere Sicherheit als die bisher überwiegend benutzten konventionellen Authentifizierungsmethoden. Obgleich bezüglich der Markttauglichkeit der vorgestellten Proof-of-Concept-Implementation – besonders hinsichtlich der Zukunft des „FIDO U2F“ Protokolls – Zweifel bestehen, zeigt sie einen Weg zu sicherer Authentifizierung und Attributweitergabe im Internet auf. Hiervon könnten Benutzer und Dienstanbieter im Internet gleichermaßen profitieren.

Literaturvereichnis

[1] Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D., and Walker, R. B. J. 2014. After Snowden: Rethinking the Impact of Surveillance. *International Political Sociology* 8, 2, 121–144.

[2] Becker, M. 2014. *W3C Web Cryptography API Übersicht, Stand und Möglichkeiten*. http://www.nds.rub.de/media/ei/arbeiten/2014/12/04/WebCryptoAPI.pdf.

[3] Bonneau, J., Herley, C., Oorschot, Paul C. van, and Stajano, F. 2012. *The quest to replace passwords: A framework for comparative evaluation of Web authentication schemes* UCAM-CL-TR-817. University of Cambridge, Computer Laboratory.

[4] Borges, G., Schwenk, J., Stuckenberg, C.-F., and Wegener, C. 2011. Deutschland im internationalen Vergleich. In *Identitätsdiebstahl und Identitätsmissbrauch im Internet*. Springer Berlin Heidelberg, 317–357. DOI=10.1007/978-3-642-15833-9_6.

[5] Borges, G., Schwenk, J., Stuckenberg, C.-F., and Wegener, C. 2011. Grundlagen. In *Identitätsdiebstahl und Identitätsmissbrauch im Internet*. Springer Berlin Heidelberg, 1–16. DOI=10.1007/978-3-642-15833-9_1.

[6] Borges, G., Schwenk, J., Stuckenberg, C.-F., and Wegener, C. 2011. Identitätsdiebstahl und neuer Personalausweis. In *Identitätsdiebstahl und Identitätsmissbrauch im Internet*. Springer Berlin Heidelberg, 151–193. DOI=10.1007/978-3-642-15833-9_4.

[7] Borges, G., Schwenk, J., Stuckenberg, C.-F., and Wegener, C. 2011. Künftige Entwicklung von Identitätsmissbrauch und Identitätsdiebstahl. In *Identitätsdiebstahl und Identitätsmissbrauch im Internet*. Springer Berlin Heidelberg, 71–149. DOI=10.1007/978-3-642-15833-9_3.

[8] Bundesamt für Sicherheit in der Informationstechnik. 2014. *Die Lage der IT-Sicherheit in Deutschland 2014*.

[9] Camp, L. and Johnson, M. 2012. Modern Technological and Traditional Social Identities. In *The Economics of Financial and Medical Identity Theft*. Springer US, 5–16. DOI=10.1007/978-1-4614-1918-1_2.

[10] CESG. 2012. *Requirements for Secure Delivery of Online Public Services* 43 43.

[11] CESG. 2014. *Identity Proofing and Verification of an Individual* 45 45.

[12] D. Eastlake 3rd and T. Hansen. 2011. *US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)*. Request for Comments. IETF, 6234. http://www.ietf.org/rfc/rfc6234.txt.

[13] Diallo, A. 2014. *Google Opens Path To Password-Free Future*. http://www.forbes.com/sites/amadoudiallo/2014/10/21/google-opens-path-to-password-free-future. Accessed 17 January 2015.

[14] FIDO Alliance. 2014. *FIDO 1.0 Specifications are Published and Final Preparing for Broad Industry Adoption of Strong Authentication in 2015*. https://fidoalliance.org/news/item/fido-1.0-specifications-published-and-final1. Accessed 2 January 2015.

[15] FIDO Alliance. 2014. *FIDO U2F HID Protocol*. https://fidoalliance.org/specs/fido-u2f-overview-v1.0-rd-20141008.pdf. Accessed 30 October 2014.

[16] FIDO Alliance. 2014. *FIDO U2F Javascript API*. https://fidoalliance.org/specs/fido-u2f-v1.0-rd-20141008.zip. Accessed 30 October 2014.

[17] Halpin, H. 2014. The W3C Web Cryptography API: Motivation and Overview. In *Proceedings of the Companion Publication of the 23rd International Conference on World Wide Web Companion*. WWW Companion '14. International World Wide Web Conferences Steering

Committee, Republic and Canton of Geneva, Switzerland, 959–964. DOI=10.1145/2567948.2579224.
[18] Hammer-Lahav, E. 2010. *The OAuth 1.0 Protocol*. Request for Comments. IETF, 5849. http://www.ietf.org/rfc/rfc5849.txt.
[19] Hardt, D. 2012. *The OAuth 2.0 Authorization Framework*. Request for Comments. IETF, 6749. http://www.ietf.org/rfc/rfc6749.txt.
[20] Hulsebosch, B., Lenzini, G., and Eertink, H. 2009. *Quality authenticator scheme*. STORK-eID Consortium.
[21] ISO/IEC. 2012. *Information technology – Security techniques – Identity proofing* WD 29003. International Organization for Standardization, Geneva, Switzerland.
[22] Kantara Initiative. 2010. *Identity Assurance Framework*. *Assurance Levels*.
[23] Miller, F. P., Vandome, A. F., and McBrewster, J. 2009. *Advanced Encryption Standard*. Alpha Press.
[24] Office of the eEnvoy. 2002. *Registration and Authentication - e-Government Strategy Framework Policy and Guidelines*.
[25] Platt, M. 2014. *Secure Authentication and Attribute Sharing in Federated Identity Scenarios*.
[26] Schröder, M. and Morgner, F. 2013. eID mit abgeleiteten Identitäten. *Datenschutz und Datensicherheit - DuD* 37, 8, 530–534.
[27] Vieraitis, L., Copes, H., and Birch, I. 2014. Identity Theft. In *Encyclopedia of Criminology and Criminal Justice*, G. Bruinsma and D. Weisburd, Eds. Springer New York, 2419–2429. DOI=10.1007/978-1-4614-5690-2_320.