Martin Schröder, Frank Morgner

eID mit abgeleiteten Identitäten

Die Authentifizierung per Benutzername und Passwort ist auch im Jahr 2013 immer noch weit verbreitet. Obwohl jährlich neue sogenannte Passwortkiller angekündigt werden, konnte sich bisher keine alternative Lösung in der Breite durchsetzen. Gründe dafür sind die Integration neuer Lösungen in bestehende Systeme sowie die nötige Umgewöhnung des Benutzers. In unserem Artikel wird das Konzept der abgeleiteten Identität mithilfe des neuen Personalausweises vorgestellt, das eine Brücke zwischen verschiedenen Authentifizierungsmethoden schlägt. Somit können neue sichere Methoden leichter eingeführt werden, ohne zu viel an bestehenden Systemen oder an bekannter Nutzungsweise ändern zu müssen.

1 Einführung

Die Verwendung von Passwörtern kann mindestens bis in die Antike zurückdatiert werden. Der griechische Geschichtsschreiber Polybius dokumentiert in „Die Verfassung der römischen Republik. Historien, III. Buch" deren Verwendung bei römischen Wachsoldaten 200 Jahre vor unserer Zeitrechnung. Auch bei Computersystemen der 60er Jahre wurden Passwörter genutzt, um privilegierte Operationen zu autorisieren. Heute – 1500 Jahre nach dem Untergang des römischen Reichs – sind Passwörter immer noch die häufigste Methode, um Nutzer am Computer, Smartphone oder Tablet zu authentifizieren.

1.1 Passwörter sind unsicher

Sie können durch Schadsoftware, Phishing, simples „Über-die-Schulter-Schauen" oder Ausprobieren in falsche Hände geraten.

Martin Schröder

arbeitet als Innovation Developer im Bereich Identity Management bei der Bundesdruckerei GmbH.

E-Mail: martin.schroeder@BDR.de

Frank Morgner

bearbeitet bei der Bundesdruckerei GmbH Innovationsthemen rund um die IT-Sicherheit, insbesondere zum neuen Personalausweis.

E-Mail: frank.morgner@BDR.de

Diese Angriffe sind real. Es gibt bereits Schadsoftware, die gleichzeitig den Desktop-Computer und das Smartphone einer Person befällt, um die Sicherung einer Bank-Transaktion per SMS-TAN auszutricksen. Mittels Phishing werden Zugangsdaten für Online-Transaktionsdienstleister wie z. B. PayPal erschlichen, um nicht autorisierte Zahlungen durchzuführen. Im Jahr 2012 wurde bekannt, dass die „geheimen" dreistelligen Prüfziffern auf den Kreditkarten verschiedener Banken durch einen Brute-Force-Angriff ermittelt werden konnte [1].

1.2 Passwörter sind unbequem

Eine Befragung in Großbritannien führte zu dem Ergebnis, dass der typische Internetnutzer 26 Accounts hat, aber nur fünf verschiedene Passwörter nutzt [2]. Nicht selten wird sogar nur ein einziges Passwort genutzt, um alle Log-ins abzusichern. Die Wiederbenutzung von Passwörtern verstärkt deren Unsicherheit. Eine komplexe Kombination aus Sonderzeichen, Buchstaben und Zahlen soll das Erraten von Passworten erschweren. Im Wesentlichen wird man oft dazu aufgefordert, „ein Passwort zu wählen, dass man sich nicht merken kann, es aber trotzdem nirgends zu notieren" [3]. In der Praxis führt dies dazu, dass Passwörter häufig vergessen werden und Angriffe auf einzelne Passwort-Datenbanken immer lohnenswerter werden.

Eine neuere Studie untersuchte die möglichen Ursachen warum sich Passwort-Alternativen nicht oder nur begrenzt durchsetzen konnten [4]. Verschiedene Authentisierungsverfahren wurden dabei nach verschiedenen Kriterien der Handhabbarkeit (Usability), Einsetzbarkeit (Deployability) und Sicherheit untersucht. Wenngleich die Sicherheit vieler Alternativen besser war als die von einem Log-in mittels Benutzernamen und Passwort, ist die Handhabbarkeit durch den Benutzer oftmals schlechter. Außerdem verlangen viele Alternativen spezielle Anpassungen auf Client- und Server-Seite und sind zudem kostspielig.

Der neue Personalausweis bietet mit der Online-Ausweisfunktion, auch eID-Funktion genannt, eine sichere Zwei-Faktor-Authentisierung im Internet. Um sich online auszuweisen, benötigt der Benutzer neben dem Ausweis seine PIN. Der Verlust der PIN

oder des Dokuments alleine ermöglicht somit noch keinen Identitätsdiebstahl. Durch die explizite Zustimmung des Nutzers und der Authentisierung des Diensteanbieters gegenüber dem Ausweis bzw. dem eID-Server wird auch dem Phishing vorgebeugt[1]. Durch die Pseudonymfunktion ist ein Tracking des Nutzers bei verschiedenen Dienstanbietern unmöglich[2]. Aus Usability-Sicht hat der Personalausweis auch einige Vorteile: Nutzer können gleichzeitig viele Online-Konten damit absichern und müssen sich trotzdem nur ein Geheimnis merken, die Ausweis-PIN. Dagegen stehen die Nachteile, den Ausweis stets bei sich zu tragen, Ladezeiten von derzeit etwa drei Sekunden[3] und möglicher Probleme beim Verlust eines Ausweises[4]. Im Vergleich zu Passwörtern hat der Personalausweis eine schlechter Deployability: Der Nutzer benötigt eine spezielle Software sowie einen Chipkartenleser. Der Dienstanbieter muss den eID-Service integrieren und den Vergabeprozess für Berechtigungszertifikate durchlaufen. Weiterhin ist das deutsche eID-System einzigartig, so dass eine Integration im Wesentlichen auf den deutschen Markt beschränkt ist.

Es ist an der Zeit, das Paradigma *der* sicheren Authentifizierung zu überdenken. Auf vielen Plattformen existieren bereits verschiedene Sicherheitsmodule: Trusted Platform Module (TPM) in Desktops und Notebooks, Secure Elements in Smartphones und SIM-Karten in einfacheren Featurephones. Die Geräte variieren in ihrer Sensorik bzw. Peripherie, Leistungsfähigkeit sowie Ein- und Ausgabemöglichkeiten. Diese Argumente sprechen für ein heterogenes System von Authentisierungsverfahren – das richtige Verfahren in der richtigen Situation.

2 Anforderungen an eine Authentifizierungslösung

Eine Authentifizierungslösung, die gleichzeitig benutzerfreundlich und sicher ist, lässt sich nur schwer finden. Tatsächlich scheint es einen Trade-Off zwischen den beiden Zielen zu geben. So erhöht z. B. eine Chipkarte in der Regel die Sicherheit eines Systems, verkompliziert dieses aber auch, da zusätzlich ein Kartenleser benötigt wird. Auf der anderen Seite erhöht eine Passwortwiederherstellung, mit der ein vergessenes Passwort wieder zurückgesetzt werden kann, seit langem den Komfort auf vielen Webseiten. Sie schafft jedoch auch neue Sicherheitslücken. So wurden mithilfe dieser Funktion die Identität und persönliche Daten eines Journalisten gestohlen [5].

Neu entwickelte Authentifizierungslösungen werden in der Regel zuerst mit dem Ziel entwickelt, die Sicherheit gegenüber Passwörtern zu erhöhen. Erst gegen Ende der Entwicklung wird dann unter den bereits festgelegten Rahmenbedingungen versucht, die Benutzerfreundlichkeit zu erhöhen bzw. die Hürden zum Einsatz der Lösung zu senken. Dies ist aufgrund des beschriebenen Trade-Offs dann allerdings nur noch begrenzt möglich.

Das Internet besteht allerdings nicht nur aus hochgradig sensiblen Informationen. Zum Beispiel dürften nur die wenigsten Internetnutzer bereit sein, für den Log-in bei einem sozialen Netzwerk mit einer Chipkarte zu hantieren. Ein Passwortersatz muss folglich flexibel sein. Es muss möglich sein, je nach Anwendungsgebiet die Sicherheitsstufe und somit den Komfort variieren zu können.

Solche Unterscheidungen sind beim ePayment bereits üblich. Onlineshops wählen ihre angebotenen Bezahlungsmöglichkeiten nach vielen Kriterien – beispielsweise nach ihrem Vertrauen in den Kunden (Altkunde, Neukunde, Bonität, etc.) oder nach der Höhe einer Transaktion – aus. Der Nutzer wiederum wählt unter den vom Shop angebotenen Möglichkeiten diejenige aus, die für ihn am komfortabelsten und sichersten ist.

Eine Authentifizierungslösung nach diesem Schema sollte in folgenden drei Punkten variabel sein:

Verschiedene Vertrauenslevel: Hierbei ist der Begriff „Identity Assurance" von Bedeutung, welcher den Grad des Vertrauens angibt, den ein Diensteanbieter in die Korrektheit der übermittelten digitalen Identität hat. Dieser Grad ist abhängig von den Auswirkungen, die falsche Identitätsinformationen haben können. Es existieren bereits eine Reihe sogenannter „Identity Assurance Frameworks" in denen unterschiedliche Vertrauenslevel beschrieben werden[5]. Diese besitzen in der Regel vier Level, wobei Leveleins das niedrigste Vertrauenslevel darstellt. Level vier ist auf der anderen Seite für kritische Dienste vorgesehen, bei denen die Übermittlung falscher Identitätsinformationen mit hohen finanziellen oder sogar Personenschäden einhergehen kann.

Für die Einordung einer Authentifizierungslösung in solch ein Level spielt neben der Vertrauenswürdigkeit des eigentlichen Authentifizierungsvorgangs auch die Authentizität der Ausgangsdaten eine Rolle. So können die Daten beispielsweise von einer vertrauenswürdigen Quelle wie dem neuen Personalausweis kommen oder durch den Benutzer selber eingegeben worden sein.

Verschiedene Settings: Neben der stationären Internetnutzung am PC muss auch die mobile Nutzung berücksichtigt werden. Die verschiedenen Nutzungsszenarien erfordern in der Regel eine größere Umstellung als nur die Anpassung der Benutzeroberfläche. So sind manche Konzepte, die im stationären Bereich funktionieren (z. B. Nutzung einer Chipkarte) im mobilen Umfeld eher nicht praktikabel. Gleichzeitig bietet ein Smartphone mit einem Touchdisplay oder einem NFC-Interface alternative Möglichkeiten. Ein weiteres Setting ist das Anwendungsszenario. So unterscheidet man zwischen der Registrierung eines Benutzers, bei der noch kein Vertrauensverhältnis zwischen Benutzer und Diensteanbieter besteht und erstmals Daten erhoben werden. Und dem Log-in, bei dem der Benutzer nur die Daten angeben muss, die nötig sind, um wiedererkannt zu werden. Die Authentifizierung per Benutzername-Passwort kann trivialerweise nur im zweiten Fall angewendet werden.

Verschiedene Ausprägungen: Als Folge der genannten Punkte Vertrauenslevel und Setting existieren viele verschiedene Authentifizierungsformen und Datenformate. Ein einheitliches Interface muss bei all der Variabilität gewährleistet sein. Dies bedeutet auf der einen Seite, dass sich die Benutzererfahrung nur geringfügig

1 Um auf die Ausweisdaten zugreifen zu können, wird ein behördlich ausgegebenes Berechtigungszertifikat benötigt.

2 Der Ausweis generiert für jeden Diensteanbieter ein eindeutiges Pseudonym, oder auch restricted ID genannt. Meldet sich der Benutzer erneut mit seinem Ausweis bei einem Diensteanbieter an, kann er anhand seiner restricted ID wiedererkannt werden. Nutzt ein Anwender die Pseudonymfunktion bei zwei unterschiedlichen Diensteanbietern, können diese den Ausweis anhand der restricted ID allerdings nicht zuordnen.

3 Nutzung der eID-Funktion einschließlich Terminalauthentisierung, Chipautentisierung und Auslesen der Identitätsinformationen

4 Der Verlust des Ausweises kann bei Ausweisbehörden oder der Polizei angezeigt werden. Die mit der Pseudonymfunktion assoziierten Online-Konten dieses Ausweises sind jedoch nicht mehr nutzbar, da sich mit einem neuen Ausweis auch das Pseudonym ändert.

5 Ein Überblick über bestehende Frameworks findet sich bei Ivonne Thomas, Christoph Meinel, 2012 „IDENTITY ASSURANCE IN OPEN NETWORKS" http://www.igi-global.com/chapter/identity-assurance-open-networks/63082].

verändern darf. Der Anwender sollte eine Oberfläche zur Verfügung gestellt bekommen, die sich in sein System integriert, ihm bereits geläufig ist und ihm eingeschränkt die Wahl gibt, seine favorisierte Authentifizierungsart auszuwählen.

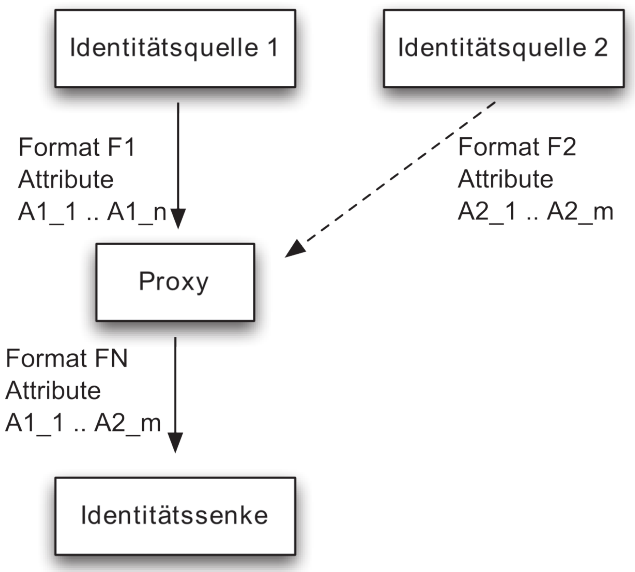
Auf der anderen Seite passen Diensteanbieter im Internet nur selten ihre Authentifizierungslösung an. Noch seltener bieten sie verschiedene Lösungen als Alternative an. Hier muss eine Möglichkeit gefunden werden, die nur wenige Änderungen auf Diensteanbieterseite erfordert.

3 Abgeleitete Identitäten

3.1 Theorie

Der Begriff „Identität" ist bereits in vielen Disziplinen belegt, so auch in der Informatik, wobei hier häufiger von der elektronischen Identität (eID) die Rede ist. Die eID ist der Teil einer Identität, der sich in elektronischer Form abbilden lässt. Sie beinhaltet alle Daten, die im virtuellen Raum über einen Anwender existieren. Das sind zum Beispiel die ganz offensichtlichen Attribute wie Name, Anschrift oder Pseudonym. Die eID besteht wiederum aus einer Menge nicht notwendigerweise disjunkter Mengen an Teilidentitäten, die man gegenüber einem Dienst preisgibt. Damit ein Dienst eine elektronische Teilidentität verarbeiten kann, muss diese in einem für ihn verständlichen Format vorliegen. Hier kommt die abgeleitete Identität ins Spiel. Besitzt ein Benutzer bereits eine Identitätsquelle (z. B. einen Ausweis), die der Dienst allerdings nicht auslesen kann, muss zwischen den beiden Parteien vermittelt werden. Ein spezieller Proxy liest die Daten aus der Quelle aus und generiert daraus eine abgeleitete Identität, die dem Dienst zur Verfügung gestellt wird.

Abbildung 1 | Der Proxy wandelt das Attributformat der Identitätsquelle in ein Format um, das von der Senke verstanden wird. Optional kann die Identität durch weitere Attribute aus einer anderen Quelle ergänzt werden.



Handelt es sich bei der Identitätsquelle um ein hoheitliches Dokument, kann man von einer Primär- oder Rootidentität sprechen. Solche Identitäten sind besonders vertrauenswürdig. Eine davon abgeleitete Identität kann Sekundäridentität genannt werden.

Der Proxy übernimmt eine zentrale Position und besitzt dementsprechend hohe Anforderungen. Er muss das Vertrauen aller beteiligten Akteure besitzen, da nur so dem gesamten Ableitungsvorgang vertraut werden kann. Er muss alle gängigen Authentifizierungsmechanismen beherrschen und zwischen diesen konvertieren können, um möglichst viele Anwendungsgebiete abdecken zu können. Er muss Daten aus verschiedenen Quellen aggregieren und auch zwischenspeichern können.

Vorteile

Die Konzentration aller Anforderungen auf einen Akteur hat Vorteile. So sinken die Anforderungen für das restliche System, das dadurch einfacher gestaltet werden kann. Benutzer und Diensteanbieter müssen nur einen Authentifizierungsmechanismus unterstützen, der auch beim Proxy implementiert ist. Da so weitere Identitätsformate unterstützt werden können, erreicht man einen großen Benutzer- sowie Diensteanbieterkreis.

Damit kann ein Authentifizierungsverfahren in unterschiedlichen Sicherheitsstufen eingesetzt werden: So kann beispielsweise ein sicheres und damit vielleicht kompliziertes Verfahren auch in abgeschwächter Form für andere Anwendungsfälle verfügbar gemacht werden. Auch lassen sich verschiedene Vertrauenslevel realisieren.

Eine „Ableitung auf Vorrat" ist ebenfalls möglich. Dabei werden die Daten nach der Umwandlung – vor Manipulation und unerlaubtem Auslesen gesichert – abgespeichert, um sie später einsetzen zu können. So ist zum Beispiel ein Offlineszenario denkbar, bei dem nur zu Beginn eine Verbindung zum Proxy bestehen muss.

Zuletzt sei noch die einheitliche Benutzererfahrung genannt. Soweit möglich benötigt der Anwender nur einen authentischen Ausgangstoken, aus welchem der Proxy je nach Anwendungsfall das benötigte Identitätsformat generiert.

3.2 Praxis: Existierende Beispiele

Identitätsableitungen sind bereits heute weit verbreitet. Zum Beispiel werden beim Postident-Verfahren die Ausweisdaten auf einen speziellen Coupon der Post übertragen und durch Unterschrift und Stempel signiert. Hier findet also eine Ableitung von Personalausweis zu Coupon statt.

Um seinen Passwortersatz Persona einem weiteren Benutzerkreis zu erschließen, möchte Mozilla eine Technik namens Identity Bridging einsetzen. Dabei vermittelt ein Proxy zwischen Persona auf der einen und dem weit verbreiteten OpenID bzw. OAuth auf der anderen Seite.

Eine länderübergreifende Authentifizierung soll das EU-Projekt STORK ermöglichen. Hier bilden spezielle Server (PEPS – Pan-European Proxy Service) den Mittler zwischen den nationalen Authentifizierungslösungen. STORK ist mittlerweile abgeschlossen. Der Nachfolger STORK 2.0 besteht aus 58 Partnern und baut auf den Erkenntnissen des Vorgängers auf.

Als letztes Beispiel sei das deutsche eID-System genannt. Der eID-Server (u. a. beschrieben in der TR-03130 [7]) liest die Datengruppen aus dem neuen Personalausweis aus und konvertiert die-

Abbildung 2 | Der eID-Server fungiert als Proxy zwischen neuem Personalausweis und Diensteanbieter. Letzterer muss nur eine SAML-Schnittstelle besitzen, um auf Ausweisdaten zugreifen zu können.

se in einen SAML-Token (Security Assertions Markup Language), welches vom Diensteanbieter verarbeitet wird. Hierbei handelt es sich um die Ableitung von einer Root- zu einer Sekundäridentität. Diensteanbieter müssen sich somit nicht um die komplexen Protokolle zum Auslesen des neuen Personalausweises kümmern, sondern integrieren lediglich eine SAML-Bibliothek.

Allerdings wird bei den genannten Beispielen immer nur ein bestimmter Ableitungsfall von einem definierten Format in ein anderes implementiert. Möchte man das Konzept der abgeleiteten Identität vollständig umsetzen, ist eine Erweiterung erforderlich, wie im Folgenden am Beispiel neuer Personalausweis gezeigt wird.

3.3 Praxis: Erweiterung des deutschen eID-Systems

Bei genauer Betrachtung fällt auf, dass das System Dank des vertrauenswürdigen eID-Servers perfekte Voraussetzungen für Erweiterungen bietet. Denkbar ist zum Beispiel die Aggregation mit Attributen anderer Datenquellen (Universtität, ZEVIS[6], etc.). Dies würde mit der Einführung von Vertrauensleveln einhergehen, da die zusätzlichen Datenquellen nicht zwingend den gleichen Authentizitätslevel wie der neue Personalausweis haben müssen. Auch können neben SAML andere Ausgangsformate unterstützt werden. Ein Beispiel wäre Microsofts U-Prove[8], das wie im Folgenden beschrieben, den Einsatz des neuen Personalausweises an einem mobilen Endgerät ermöglicht.

Mobiler Einsatz

Die Nutzung der eID-Funktionalität des neuen Personalausweises ist für mobile Endgeräte (Smartphone, Tablet, etc.) bisher nicht möglich, da zurzeit keine kompatiblen Endgeräte zur Verfügung stehen.

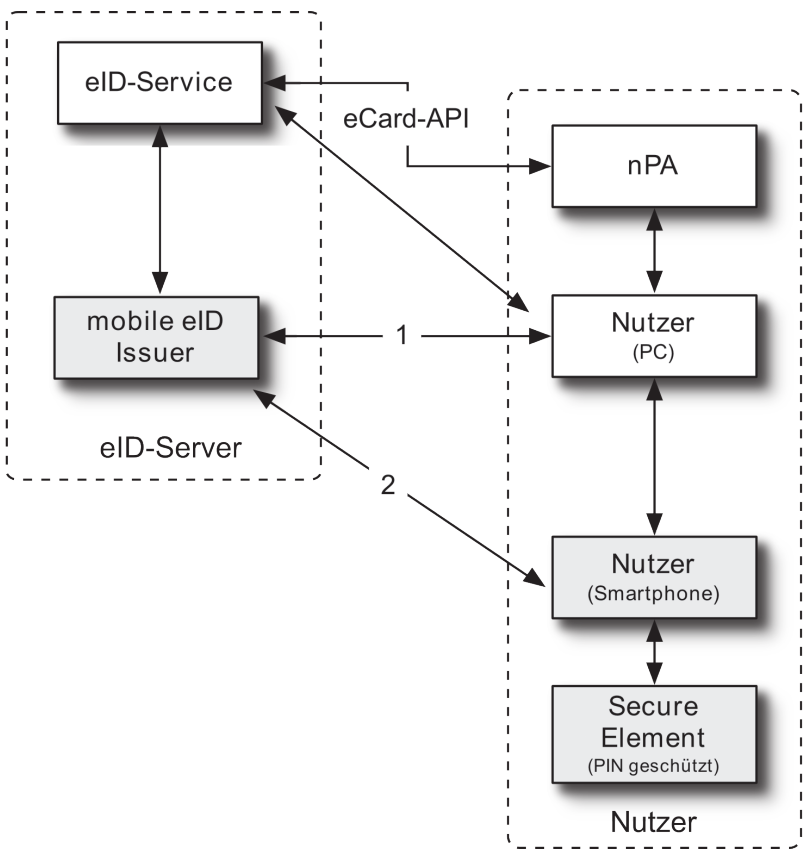
Eine Möglichkeit zur mobilen Nutzung besteht in der sicheren Ableitung und Übertragung der Identitätsattribute und deren Bindung an ein Secure Element, welches bei vielen mobilen Endgeräten verfügbar ist oder sich nachrüsten lässt. Der Vorteil dabei ist, dass der Personalausweis nur für die Ableitung benötigt wird. Der anschließende mobile Authentifizierungsvorgang kann mit der auf dem Smartphone gespeicherten abgeleiteten Identität erfolgen. Auf dem SmartCard-Workshop 2012 wurde solch eine Ableitung bereits demonstriert [9].

Die Ableitung kann dabei so realisiert werden, dass die Identitätsdaten nicht im Netz gespeichert werden müssen. Abb.3 zeigt die beteiligten Akteure und deren Verbindung zueinander.

Die oberen vier Komponenten entsprechen den für die eID-Funktion des neuen Personalausweises benötigten Komponenten. Die grau hinterlegten Komponenten werden für die Ausstellung einer mobilen eID benötigt. Der Aussteller der mobilen eID (mobile eID Issuer) ist in beiden Kontexten aktiv.

Der Nutzer besitzt einen PC, der mit einem Personalausweis verbunden ist und ein Smartphone, das ein Secure Element besitzt. Zwischen dem PC und dem Smartphone besteht keine physische Verbindung, sie können aber über den Nutzer miteinander kommunizieren. Der Nutzer kann beispielsweise einen Aktivierungscode von dem Display des Smartphone ablesen und anschließend am PC eingeben.

Abbildung 3 | Ableitung für mobile eID: Der eID-Server liest die Attribute aus dem Personalausweis aus und überträgt diese sicher auf das Smartphone des Benutzers, wo sie durch das Secure Element geschützt werden.



Der mobile eID Issuer übernimmt eine Sonderrolle. Im System des neuen Personalausweises stellt er einen Diensteanbieter dar, der die Attribute des Ausweises benötigt, die später in die mobi-

6 Zentrales Verkehrs-Informationssystem des Kraftfahrt-Bundesamtes in dem unter anderem die bundesweiten Daten bezüglich Kraftfahrzeuge, Fahrzeughalter und Fahrerlaubnissen verwaltet werden

le eID einfließen sollen. Gleichzeitig besitzt er eine zweite Verbindung zu dem Smartphone und generiert aus den erhaltenen personenbezogenen Daten die abgeleitete mobile Identität. Diese wird an das Secure Element gebunden und an das Smartphone übertragen. U-Prove spezifiziert solch ein Vorgehen bereits im Issuing-Protokoll. Die so ausgestellten U-Prove-Token können nur unter Zuhilfenahme des Secure Elements, welches wiederum durch eine PIN geschützt ist, für die Authentifizierung verwendet werden.

Die Schwierigkeit dieser Ableitung ist die Kopplung der beiden Verbindungskanäle 1 und 2. Es muss sichergestellt werden dass die Daten des neuen Personalausweises ausschließlich in dem Smartphone des Ausweisinhabers gespeichert werden. Eine solche Kopplung kann z. B. anhand eines Einmal-Passworts, das auf dem Handy entschlüsselt und angezeigt wird und anschließend am PC eingeben werden muss, realisiert werden. Es ist auch denkbar eine solche Ableitung an einem Terminal, das zum Beispiel im Bürgeramt steht, zu realisieren.

4 Ausblick

Der Gedanke, dass bei neuen Authentisierungsverfahren nicht zuerst nur auf Sicherheit geachtet werden darf, sondern die Benutzbarkeit und Einsetzbarkeit eine ebenso wichtige Rolle einnehmen, setzt sich immer weiter durch. Neue Verfahren bieten immer öfters Schnittstellen zu bestehenden Systemen, um sich einen größeren Nutzerkreis zu erschließen. Abgeleitete Identitäten sind hier das Mittel der Wahl, wie man an bestehenden Systemen wie dem deutschen eID-System oder in der Entwicklung befindlichen Systemen wie Mozillas Persona erkennen kann. Allerdings sind alle diese Systeme auf einen bestimmten Anwendungsfall begrenzt, in dem Fall das deutsche eID-System auf den neuen Personalausweis und Persona auf eine Brücke zu OpenID und OAuth. Eine Brücke zwischen den beiden genannten Systemen existiert zum Beispiel (noch) nicht. Dass die Implementierung eines Systems, das zwischen sehr vielen Authentifizierungsmechanismen vermitteln kann, allerdings auch sehr komplex werden kann, zeigt STORK mit seiner Vielzahl an Spezifikationen. Insgesamt muss somit eine Abwägung zwischen der Anzahl der unterstützen Features und der Einsetzbarkeit getroffen werden.

5 Literatur

[1] Report München, 7. August 2012
[2] „Lazy password reuse opens Brits to crooks' penetration" http://www.theregister.co.uk/2012/07/20/password_reuse_survey
[3] Mikko Hyppönen, 14. August 2011, https://twitter.com/mikko/statuses/102984155809333248
[4] Bonneau, Herley, van Oorschot, Stajano 2012: "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes". In Proc. IEEE Symp. on Security and Privacy 2012.
[5] „How Apple and Amazon Security Flaws Led to My Epic Hacking", Matt Honan, 08. Juni 2012, http://www.wired.com/gadgetlab/2012/08/apple-amazon-mat-honan-hacking/
[6] Ivonne Thomas, Christoph Meinel, 2012 „Identity Assurance in Open Networks" http://www.igi-global.com/chapter/identity-assurance-open-networks/63082
[7] BSI, 03. Oktober 2012, "TR-03130 Technical Guideline eID-Server, Part I: Functional Specification, Version 2.0", https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03130/TR-03130_TR-eID-Server_V2_1_pdf.pdf
[8] http://www.microsoft.com/u-prove
[9] Frank Dietrich, 2012 „Mobile Nutzung des neuen Personalausweises" in 22. SmartCard-Workshop: Darmstadt 8. Und 9. Februar 2012. Tagungsband