H. Langweg, M. Meier, B.C. Witt, D. Reinhardt (Hrsg.): Sicherheit 2018,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2018 183

Auf dem Weg zu sicheren abgeleiteten Identitäten mithilfe der Payment Service Directive 2

Daniel Träder[1], Alexander Zeier[2], Andreas Heinemann[3]

Abstract: Online-Dienste erfordern eine eindeutige Identifizierung der Benutzer und somit eine sichere Authentisierung. Insbesondere eGovernment-Dienste innerhalb der EU erfordern eine starke Absicherung der Benutzeridentität. Auch die mobile Nutzung solcher Dienste wird bevorzugt. Das Smartphone kann hier als einer der Faktoren für eine Zwei-Faktor-Authentifizierung dienen, um eine höhere Sicherheit zu erreichen. Diese Arbeit schlägt vor, den Zugang und die Nutzung einer abgeleiteten Identität mit einem Smartphone zu sichern, um es dem Benutzer zu ermöglichen, sich auf sichere Weise gegenüber einem Online-Dienst zu identifizieren. Dazu beschreiben wir ein Schema zur Ableitung der Identität eines Benutzers mithilfe eines Account Servicing Payment Service Provider (ASPSP) unter Verwendung der Payment Service Directive 2 (PSD2) der Europäischen Union. PSD2 erfordert eine Schnittstelle für Dritte, die von ASPSPs implementiert werden muss. Diese Schnittstelle wird genutzt, um auf die beim ASPSP gespeicherten Kontoinformationen zuzugreifen und daraus die Identität des Kontoinhabers abzuleiten. Zur Sicherung der abgeleiteten Identität ist der Einsatz von FIDO (Fast Identity Online) vorgesehen. Wir bewerten unseren Vorschlag anhand der Richtlinien von *eIDAS LoA* (Level of Assurance) und zeigen, dass für die meisten Bereiche das Vertrauensniveau *substantiell* erreicht werden kann. Um diesem Level vollständig gerecht zu werden, ist zusätzlicher Arbeitsaufwand erforderlich: Zunächst ist es erforderlich, Extended Validation-Zertifikate für alle Institutionen zu verwenden. Zweitens muss der ASPSP sichere TAN-Methoden verwenden. Schließlich kann der Widerruf einer abgeleiteten Identität nicht erfolgen, wenn der Benutzer keinen Zugriff auf sein Smartphone hat, das mit der abgeleiteten ID verknüpft ist. Daher ist ein anderes Widerrufsverfahren erforderlich (z. B. eine Support-Hotline).

Keywords: Abgeleitete Identitäten; PSD2; eIDAS; eGovernment; Identitätsmanagement

1 Einleitung

Immer mehr Behörden bieten aufgrund der fortschreitenden Digitalisierung eGoverment-Dienste an. Bei der Online-Authentifizierung werden hierbei oft noch Benutzername und Passwort verwendet, obwohl diese Methode zunehmend als unsicher angesehen wird. Alternative Technologien, wie die Online-Authentifizierung des deutschen Personalausweises

[1] Hochschule Darmstadt, Fachbereich Informatik, Haardtring 100, 64295 Darmstadt, Deutschland daniel.traeder@h-da.de
[2] Hochschule Darmstadt, Fachbereich Informatik, Haardtring 100, 64295 Darmstadt, Deutschland alexander.zeier@h-da.de
[3] Hochschule Darmstadt, Fachbereich Informatik, Haardtring 100, 64295 Darmstadt, Deutschland andreas.heinemann@h-da.de

doi:10.18420/sicherheit2018_14

(nPA), sind noch nicht weit verbreitet. Solche Technologien geben dem Benutzer die Möglichkeit, sich durch Online-Dienste mit hoher Sicherheit identifizieren zu lassen, werden aber derzeit von den deutschen Bürgern nur wenig genutzt (vgl. [Va15]). Einer der Gründe ist die mangelnde Benutzerfreundlichkeit, die durch das gegebene Gesamtsystem verursacht wird (vgl. [WHM16]).

Durch die hohe Verbreitung von Smartphones (vgl. [rB16, Po16]) wird die mobile Benutzerauthentifizierung häufig favorisiert. Außerdem kann das Smartphone als einer der Faktoren (Besitz) in einer Zwei-Faktor-Authentifizierung verwendet werden, was zu einer höheren Sicherheit führt. In Verbindung mit einer abgeleiteten Identität[4] ermöglicht ein Smartphone dem Benutzer, sich gegenüber einem Online-Dienst zu identifizieren.

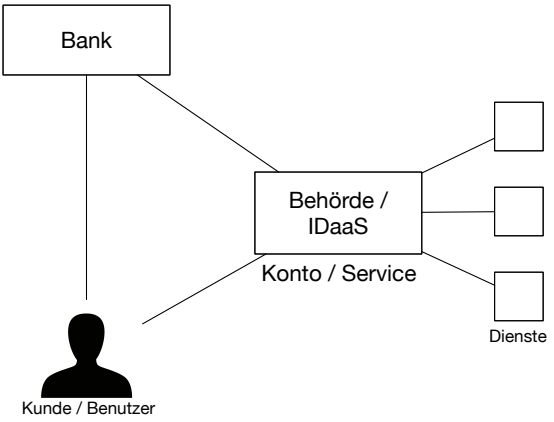


Abb. 1: Szenario zur Ableitung einer Identität bei einem ASPSP

Wir präsentieren ein Schema zur Ableitung einer Identität durch eine Schnittstelle der Payment Service Directive 2 (PSD2), die Kontoinformationen bereitstellt. Diese Informationen können von einem Identity Provider (IdP) gespeichert und für eine spätere Verwendung abgerufen werden. Dieses Szenario ist in Abbildung 1 dargestellt. Eine Behörde oder auch ein Unternehmen möchte die Identität eines (potentiellen) Benutzers in Erfahrung bringen. Der Benutzer ist ebenso Kunde einer Bank. Die Behörde / das Unternehmen nutzt die Bankdaten des Benutzers um diesen zu Authentifizieren. Diese Bankdaten können als Identität in ein Konto gespeichert werden, um einen SSO einzurichten. Dienste müssen in der Lage sein, diesen Identitäten zu vertrauen. Zu diesem Zweck muss ein angemessenes Maß an Vertrauen in die Identität vorhanden sein, welches in der vorliegenden Arbeit bewertet wird. Ein weiterer denkbarer Anwendungsfall wäre, dass ein Unternehmen anderen Unternehmen *Identity-as-a-Service* anbietet, ohne dass Benutzerdaten in einem Konto zwischengespeichert werden.

[4] *A credential issued based on proof of possession and control of a token associated with a previously issued credential, so as not to duplicate the identity proofing process*; siehe hierzu [Bu11]

Für die Evaluierung unseres Schemas konzentrieren wir uns auf Europa und die europäischen Vorschriften.

Im Weiteren ist dieser Betrag wie folgt gegliedert: Zunächst geben wir einen Überblick über die Voraussetzungen (Abschnitt 2). Danach wird in Abschnitt 3 das vorgeschlagene Schema für die Ableitung einer Identität mithilfe von PSD2 vorgestellt. Abschnitt 4 bewertet unser Schema nach eIDAS LoA [Eu15] und gibt einen Überblick über das mit unserem Schema erreichbare Maß an Sicherheit. Verwandte Arbeiten werden in Abschnitt 5 besprochen. Abschließend fassen wir diese Arbeit zusammen und zeigen zukünftige Schritte auf (Abschnitt 6).

2 Voraussetzungen

IT-Systeme im öffentlichen Sektor müssen staatliche Vorgaben und Richtlinien berücksichtigen. Diese Vorgaben werden von der Europäischen Union (EU) herausgegeben und die Staaten setzen diese bedarfsgerecht um. Je nach Land muss ein IT-System unterschiedliche Anforderungen erfüllen.

Wir werden wichtige Voraussetzungen überprüfen, die unser Schema berücksichtigen muss.

eIDAS Die eIDAS-Verordnung ist ein gemeinsamer Rahmen, der Standards für elektronische Identifizierungs- und Treuhanddienste für elektronische Transaktionen auf dem europäischen Markt festlegt. Mit dieser Verordnung sollen die Voraussetzungen für eine grenzüberschreitende Online-Authentifizierung mit nationalen elektronischen Ausweisen geschaffen werden (vgl. [Eu14]).

Vertrauensniveaus Die Vertrauensniveaus nach der eIDAS-Verordnung definieren das Vertrauen, das in einen bestimmten Mechanismus gesetzt werden kann. Hierzu werden die Anforderungen beschrieben, die erfüllt sein müssen, um das angestrebte Niveau zu erreichen. Die eIDAS-Verordnung definiert drei Vertrauensniveaus: *hoch*, *substantiell* und *niedrig*. Je höher das Vertrauensniveau, desto mehr Anforderungen müssen erfüllt werden.

PSD2 Die Payment Service Directive 2 (PSD2) ist eine Richtlinie der EU, welche u. a. eine Schnittstelle bei Zahlungsdienstleistern (z. B. Banken) vorschreibt (vgl. [EB17]). Sie wurde für die Öffnung des Bankenmarktes für neue Unternehmen im Bereich der Zahlungsdienste geschaffen. Die Zahlungsdienstleister müssen Dritten Zugang zu ihren Kontodaten und -funktionen gewähren. Dies erfordert immer die Erlaubnis des Kontoinhabers. Die Informationen, die laut Richtlinie zur Verfügung gestellt werden müssen, sind:

- Kontoinformationen

- Leistungsbilanzsaldo
- Transaktionen der letzten 90 Tage

Für die Ableitung der Identität werden vom PSD2-Interface nur die Kontoinformationen benötigt (vgl. Abschnitt 3). Diese Kontoinformation stellen die Identität dar, welche abgeleitet werden soll. Zwei-Faktor-Authentifizierung ist für die PSD2-Authentifizierung obligatorisch, aber es ist auch möglich, mehr als zwei Faktoren zu verwenden. Die Authentifizierung eines Benutzers ist nur für eine Aktion gültig, z. B. den Zugriff auf die Kontoinformationen. Um dies zu erreichen, wird aus der Zwei-Faktor-Authentifizierung ein Authentifizierungscode generiert, der dann der Aktion zugeordnet wird. Wenn der Benutzer z. B. die Summe einer Transaktion ändern will, wird dies als neue Aktion betrachtet und es muss ein neuer Authentifizierungscode erzeugt und verwendet werden. Der Authentifizierungscode wird im letzten Schritt verwendet, um die Ausführung der zugehörigen Aktion zu autorisieren.

3 Identitäten ableiten mithilfe der PSD2

Unser Schema basiert auf dem OAuth 2.0 Protokoll. OAuth 2.0 gilt formal als sicher (vgl. [FKS16]) und unterstützt Zwei-Faktor-Authentifizierung (vgl. [Ha12]). Es eignet sich daher gut, um den hohen Anforderungen an das Vertrauensniveau der PSD2 gerecht zu werden. Eine gemeinsame API für Banken würde den Implementierungsaufwand erheblich vereinfachen, da nicht jede API einzeln zur Anwendung hinzugefügt werden muss. Es gibt bereits Zusammenschlüsse von Banken um in Zukunft eine gemeinsame API für PSD2 zur Verfügung stellen zu können (z. B. Preta[5] und der Berlin Group PSD2 Standard[6]). Neben diesen Zusammenschlüssen gibt es noch APIs von einzeln Banken. Die in der von uns entwickelten Android App zu Demonstrationszwecken genutzte API ist die der Deutschen Bank (dbAPI) [De17] (Abbildungen der App befinden sich im Anhang auf Seite 181). Diese wurde gewählt, da sie auf dem OAuth 2.0 Protokoll aufbaut und bereits öffentlich zur Verfügung steht.

Abbildung 2 zeigt den Nachrichtenfluss für die Ableitung einer Identität. Um persönliche Informationen eines Benutzers von einem Account Servicing Payment Service Provider (ein kontoführender Zahlungsdienstleister, siehe [EB17] Artikel 4, Nr. 17) (ASPSP) zu erhalten, benötigen wir eine Berechtigung, um auf die erforderlichen Informationen zugreifen zu können. Unser Schema erlaubt es dem Benutzer, den IdP zu autorisieren und auf die Benutzerdaten des ASPSPs zuzugreifen. Abbildung 2 zeigt drei Entitäten. *ASPSP* repräsentiert die API der Deutschen Bank. Diese könnte auch durch eine andere Serviceschnittstelle eines ASPSPs ersetzt werden. *aIdP* ist der IdP, bei dem die abgeleitete Identität nach dem Ableitungsprozess gespeichert wird. Benutzer / Kontoinhaber stellt zwei Dinge dar: Ein Benutzer, der eine Identität zum aIdP ableiten will und ein Kontoinhaber, der über die

[5] Petra `https://www.preta.eu/`

[6] Berlin Group PSD2 Standard `https://www.berlin-group.org/psd2-access-to-bank-accounts`

PSD2-Schnittstelle auf ein Bankkonto zugreifen kann. Benutzer und Kontoinhaber sind ein und dieselbe Person. Folgende Daten werden von der Deutschen Bank bereit gestellt und müssen vorliegen, bevor die Ableitung durchgeführt werden kann:

- **App Client ID**: Eine eindeutige ID, welche der ASPSP registrierten Anwendungen zur Verfügung stellt. Mit dieser soll der Server, welcher später die Anfragen an den ASPSP stellt, identifiziert werden. Diese ID wird der Software auf dem aIdP beim Start als Parameter übergeben.
- **App Client Secret Key**: Der vom ASPSP festgelegte geheime Schlüssel der Anwendung, mit dem diese ihre Authentizität gegenüber dem ASPSP nachweisen kann. Auch dieser Schlüssel wird der Software auf dem aIdP beim Start als Parameter übergeben.

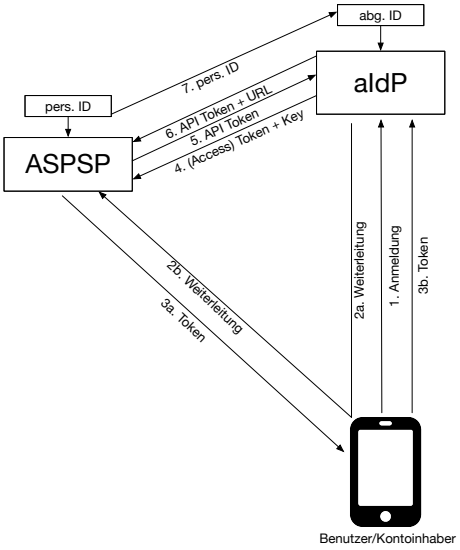


Abb. 2: Ableitung von Identitäten mithilfe der PSD2

Für die Ableitung der Identität werde folgende Schritte durchgeführt:

1 Der Benutzer meldet sich beim aIdP an. Es spiele keine Rolle, ob hierzu eine Zwei-Faktor-Authentifizierung oder der Benutzername mit einem Passwort genutzt wird, da die Ableitung selbst sicherstellt, dass die benötigten Identitätsdaten nur dann transferiert werden, wenn der Benutzer dazu berechtigt ist. Nach der Anmeldung initiiert der Benutzer die Ableitung.

2a Der aIdP leitet den Benutzer an den ASPSP weiter, bei dem der Benutzer ein Konto besitzt. Hierbei wird die App Client ID und eine Statusvariable mitgesendet. Diese

enthält, verschlüsselt mit einem Schlüssel des aIdP, das momentane Session-Cookie des Benutzers und eine nicht leicht zu erratende Zeichenkette (möglichst lang und zufällig). Dieses Vorgehen führt zu einer Bindung der Session an das momentan verbundene Smartphone des Benutzers. Daher sind eventuell abgefangene Daten für einen Identitätsdiebstahl am aIdP nicht zu gebrauchen.

2b Der Benutzer authentifiziert sich als Kontoinhaber gegenüber dem kontoführenden Zahlungsdienstleister mit seinen Zugangsdaten. Da PSD2 Zwei-Faktor-Authentifizierung erfordert, ist es zwingend erforderlich, einen zweiten Faktor für die Authentifizierung anzugeben. Bei ASPSPs handelt es sich dabei in der Regel um eine sichere TAN-Methode.

3a Nach erfolgreicher Authentifizierung sendet der ASPSP einen einmaligen Authentifizierungscode (hier Token gennannt) an den Kontoinhaber. Damit ist es möglich, gegenüber dem ASPSP zu beweisen, dass der Kunde den Zugriff auf die Kontodaten autorisiert hat. Der Token wird mit dem Kunden verknüpft, so dass mit diesem Token nur die Kontodaten dieses einen Kunden abgerufen werden können. Zusätzlich wird die App Client ID an den Token gebunden, so dass dieser Token nur von dem autorisierten Service (dem aIdP) genutzt werden kann.

3b Anschließend wird der Token automatisch vom Smartphone des Benutzers an den aIdP übertragen. Zusätzlich wird die Statusvariable mitgesendet, um die Bindung des Tokens mit der Session des Benutzers sicherzustellen. Wir gehen davon aus, dass, wenn der Benutzer in der Lage ist, einen Token für den Zugriff bereitzustellen, er auch der Kontoinhaber ist. Unter dieser Annahme sind die Daten des Kontos des ASPSPs die Identität des Benutzers.

4 Der aIdP authentisiert sich beim ASPSP mit dem *App Client Secret Key* und dem vom Benutzer übermittelten Token, um den Zugriff auf die Kontodaten des Kunden zu legitimieren.

5 Nach der Authentifizierung wird ein API Token an den aIdP gesendet. Dieser ermöglicht es, dem aIdP für einen eingeschränkten Zeitraum auf die vom Benutzer / Kontoinhaber autorisierten Kontodaten zuzugreifen.

6 Der aIdP fordert nun durch einen Zugriff auf die API die Kontodaten des Benutzers an. Hierzu überträgt er seinen persönlichen API Token und die URL zu der gewünschten Ressource.

7 Der ASPSP Server überträgt die angeforderten persönlichen Identitätsdaten (pers. ID). In unserem Fall sind dies folgende Daten: Anschrift (Straße, Hausnummer, Postleitzahl, Ort, Land, Eingetragener Wohnsitz), Persönliche Daten (Vorname, Nachname, Geburtsdatum, Geschlecht, Akademischer Titel, Adelstitel, Nationalität, Geburtsname, Geburtsort, Geburtsland, E-Mail-Adressen, Telefonnummern, Internationale Vorwahl, Ortsnetzkennzahl) und Legitimation des Kunden gegenüber des ASPSP (Dokumenttyp (Reisepass, ID,...), Dokumentnummer, Ausgabedatum des Dokuments,

Ausstellende Behörde, Ablaufdatum). Es werden nicht alle Daten benötigt. Daher sollte aus Gründen der Datensparsamkeit nur die benötigten Daten übernommen werden. Diese können je nach Einsatzzweck des aIdP unterschiedlich ausfallen.

Dieses Schema hat die folgenden Eigenschaften: Der Anwender benötigt keinen Kartenleser oder ähnliche Hardware. Dies schränkt den Benutzerkreis wegen fehlender Hardware nicht ein. Außerdem ist es nicht erforderlich, dass der Benutzer eine elektronischen Identitätsausweis (in Deutschland einen nPA) besitzt. Es genügt, dass sich der Benutzer in der Vergangenheit erfolgreich bei einem ASPSP registriert hat (was nach nationalem Recht ein sichererer Identitätsnachweis ist). Die potentielle Benutzergruppe des Systems ist somit jede Person mit einem amtlichen Ausweis, wie z. B. Reisepass oder dem alten, nicht-digitalen Personalausweis und ein Bankkonto bei einer europäischen bzw. teilnehmenden Bank. Darüber hinaus kann die Schnittstelle des kontoführenden Zahlungsdienstleisters für den Kontoinhaber (Schritt 2b. in Abbildung 2) so gestaltet werden, wie es der Kontoinhaber von seinem kontoführenden Zahlungsdienstleister gewohnt ist (z. B. Online-Banking). Dies erleichtert dem Benutzer den Zugriff auf das System, da er in der Regel die notwendigen Schritte zur Authentifizierung bereits vom Online-Banking kennt.

Bevor der Benutzer auf die abgeleitete Identität zugreifen kann, wird das Smartphone des Benutzers mit der abgeleiteten Identität verknüpft. Diese muss mit einer Zwei-Faktor-Authentifizierung abgesichert werden. Einer der Faktoren im System ist das Smartphone, das einen privaten Schlüssel speichert, der auf dem Smartphone generiert wurde. Dieser private Schlüssel wird für die Authentifizierung beim aIdP verwendet. Der zweite Faktor kann vom Benutzer, je nach Möglichkeiten des Smartphones, ausgewählt werden. Der Faktor kann z. B. eine PIN oder ein Fingerabdruck sein.

Der aIdP kann, nach der Ableitung, in einem System als Single Sign-on (SSO) IdP genutzt werden, da die Identitäten der Benutzer bereits vorhanden und der Zugriff auf diese durch Zwei-Faktor-Authentifizierung geschützt sind. Hierzu müssten Technologien wie OAuth 2.0 oder SAML genutzt werden, um die entsprechende Funktionalität zu implementieren. Aus Datenschutzgründen und der Menge der möglicherweise vorhanden Benutzerdaten, ist es empfehlenswert hierbei den Zugriff für andere Dienste zu beschränken und auch die Unterstützung von „Assertions“ (z. B. „ist der Benutzer schon volljährig?“) zu bedenken. Damit der aIdP später beweisen kann, dass er die Daten tatsächlich von der Bank erhalten hat und diese unverändert sind, kann eine Signatur des ASPSP erforderlich sein. Dies ist jedoch von PSD2 nicht vorgesehen, könnte jedoch für unser Schema eine hilfreiche Erweiterung sein.

4 Evaluation des Vertrauensniveaus

Für die Bewertung des Vertrauensniveaus wird eIDAS LoA [Eu15] verwendet. Diese Richtlinie definiert die Anforderungen an die Einhaltung der in Europa geltenden Vertrauensniveaus. Im Folgenden werden die Ergebnisse der Evaluierung für die einzelnen

Bereiche der Richtlinie präsentiert. Des weiteren wird gezeigt, was getan werden muss, um das Vertrauensniveau *substantiell* zu erreichen. Für die Zwei-Faktor-Authentifizierung beim aIdP schlagen wir FIDO UAF vor, um den Zugriff auf die abgeleitete Identität zu sichern (vgl. [LBH15]).

Beantragung und Eintragung Die Sicherheit der Anmeldung hängt von der Authentifizierung des kontoführenden Zahlungsdienstleisters ab. Die Richtlinien des NIST [Gr17] enthalten sichere TAN Verfahren, welche bei einer Zwei-Faktor-Authentifizierung genutzt werden können. Die Verfahren photoTAN und chipTAN erreichen *substantiell*. SMS/Mobile-TAN werden noch von einigen nationalen Richtlinien bei bereits bestehender Software akzeptiert (z. B. BSI TR-03107-1 [BS16]), sollen aber nicht mehr bei neuen Anwendungen zum Einsatz kommen. TAN und iTAN sind nicht sicher. Die Architektur erreicht in diesem Punkt das Vertrauensniveau *substantiell*.

Identitätsnachweis und -überprüfung Der Identitätsnachweis und die Identitätsüberprüfung erfolgt beim ASPSP bereits vor der Ableitung. ASPSPs sind verpflichtet eine Identitätsfestellung auf Vertrauensniveau *hoch* durchzuführen [EB17]. Daher kann davon ausgegangen werden, dass dies durchgeführt wird, bevor ein Kunde ein Konto eröffnen kann.

Merkmale und Gestaltung elektronischer Identifizierungsmittel Hier kommt es darauf an, wie gut der private Schlüssel durch das Smartphone geschützt ist. Vertrauensniveau *hoch* kann in diesem Bereich nicht erreicht werden, da nicht jedes Smartphone einen „Schutz vor Duplizierung und Fälschung vor Angreifern mit hohem Angriffspotential“ bietet (vgl. [Gr17]). Das Vertrauensniveau *substantiell* wird hingegen erreicht, da jedes iOS oder Android Smartphone mindestens auf Softwareebene den Zugriff auf private Schlüssel schützt (vgl. [Go17], [Ap17]).

Ausstellung, Auslieferung und Aktivierung Die abgeleitete ID ist durch die zwei Faktoren von FIDO gesichert. Diese zwei Faktoren werden auf dem Smartphone des Benutzers erzeugt / festgelegt, daher besteht keine Gefahr, dass diese bei der Erstellung in den Besitz einer unberechtigte Person kommen. Dies erfüllt die Anforderungen für das Vertrauensniveau *substantiell*.

Aussetzung, Widerruf und Reaktivierung Architektur erlaubt einen Widerruf, wenn der Benutzer im Besitz seiner Authentifizierungsmittel ist. Ist dies nicht der Fall, besteht keine Möglichkeit, die abgeleitete Identität zu widerrufen. Um das Vertrauensniveau *substantiell* zu erreichen, wird noch ein anderer Weg benötigt, die abgeleitete Identität zu widerrufen. Dies kann bspw. erreicht werden, wenn der Benutzer unter Anwendung von Benutzername

und Passwort seine FIDO Verknüpfung löscht. Ebenso erfüllt eine 24h Telefon-Support-Hotline die Anforderungen. Anschließend müssen bei beiden Methoden auch alle anderen Benutzerdaten auf dem gleichen Vertrauensniveau gelöscht werden. Aufgrund des Fehlens eines zweiten Faktors erreichen beide Transaktionen kein *substanzielles* Vertrauensniveau. Dieses Verfahren stellt jedoch sicher, dass die personenbezogenen Daten gelöscht und somit nicht missbräuchlich verwendet werden können.

Verlängerung und Ersetzung Das Ablaufdatum, welches bei der Ableitung vom ASPSP an den aIdP übertragen wurde, ermöglicht es, die abgeleitete ID des Benutzers zu sperren. Danach muss der Kunde eine erneute Ableitung anstoßen, um so eine neue abgeleitete ID zu erhalten. Die Verlängerung erfolgt somit auf dem gleichen Vertrauensniveau, wie bei der erstmaligen Ableitung und erfüllt die Anforderungen an das Vertrauensniveau *substantiell*.

Authentifizierung bei dem aIdP Die beiden Faktoren und das Authentisierungsprotokoll erfüllen die Anforderungen für das Vertrauensniveau *substantiell*. FIDO erfüllt die Anforderungen an die geforderte dynamische Authentifizierung (vgl. [LBH15]). Die Faktoren werden über keinen Kanal gesendet, sondern auf dem Smartphone erzeugt / festgelegt. Die Übertragung der Daten erfolgt, wie im gesamten Schema, über TLS. Dabei sind die entsprechenden Empfehlungen von OWSAP [7] und für Deutschland die BSI-Richtlinien (vgl. [BS18]) für den Einsatz von TLS zu berücksichtigen.

Management und Organisation Das Erreichen des Vertrauensniveau *substanziell* hängt von der Organisation und dem Management des aIdP ab. Dies kann nicht im Rahmen dieser Arbeit evaluiert werden, da die Bewertung von der jeweiligen Institution abhängt, welche das Schema implementieren möchte. Dennoch werden folgend ein paar wichtige Punkte hervorgehoben. Es ist eine Überprüfung nach ISO27001 [IS13] (oder ähnlich) erforderlich. Jeder kontoführende Zahlungsdienstleister erfüllt die Anforderungen für das Vertrauensniveau *substantiell*, da bei diesen eine Überprüfung nach ISO27001 (oder ähnlich) vorgeschrieben ist (vgl. [Eu13]).

Zusammengefasst erfüllt unser Schema die Voraussetzungen für das Vertrauensniveau *substantiell*, wenn bestimmte Anforderungen in dem System erfüllt sind, in das unser Schema implementiert werden soll. Insbesondere muss darauf geachtet werden, dass das System es erlaubt, die abgeleitete Identität zu widerrufen, auch wenn der Benutzer nicht mehr auf sein Smartphone zugreifen kann. Außerdem müssen alle teilnehmenden Institute nach ISO27001 überprüft worden sein.

[7] OWSAP - Transport Layer Protection Cheat Sheet `https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet#Server_Protocol_and_Cipher_Configuration`

5 Verwandte Arbeiten

Es gibt, neben Lösungen einzelner Banken, auch APIs, welche von mehreren Bank eingesetzt werden. Unter anderem ist dies *BankId* (vgl. [Ba17]), welche den Zugriff auf alle Bankkonten norwegischer Banken ermöglicht und sich bereits im Einsatz befindet. Ebenso ist *Open Banking Ltd.* (vgl. [SNS17]) bereits in Großbritannien in Verwendung. Eine API, welche sich nicht auf ein Land konzentriert, ist die *OpenID Financial API (FAPI) WG* (vgl. [Op17]). Deren Spezifikationen sind noch nicht final, befindet sich aber bereits im Draft Status. Alle drei Lösungen können als Vorentwicklung zu einer PSD2 API Schnittstelle gesehen werden. Ebenso können sie, bei einem ASPSP implementiert, in unserem Schema verwendet werden.

Die Arbeit „Auf dem Weg zur Umsetzung der PSD2-Richtlinie“ von Hühnlein et al. gibt einen Überblick über die Anforderungen an eine PSD2 API. Dabei werden insbesondere die Anforderungen, welche durch die verschiedenen EU Verordnungen entstehen, analysiert. Ebenso wird die Sicherheit der möglicherweise beim ASPSP eingesetzten Technologien (OAuth, SAML) untersucht (vgl. [Hu17]). Im Gegensatz hierzu untersucht die vorliegende Arbeit das Vertrauensniveau einer Ableitung von Identitätsdaten in einen aIdP.

6 Zusammenfassung und Ausblick

In dieser Arbeit wurde ein Schema zur Ableitung einer Identität mittels PSD2 vorgeschlagen, welches das Vertrauensniveau *substantiell* erreicht. Hierzu müssen jedoch weitere Anforderungen vom System erfüllt werden, in das dieses Schema implementiert werden soll. Insbesondere muss darauf geachtet werden, dass ein System es erlaubt, die abgeleitete Identität zu widerrufen, auch wenn der Benutzer nicht mehr auf sein Smartphone zugreifen kann. Zusätzlich erwarten wir eine hohe Benutzerakzeptanz, da der Anwender mit der Oberfläche und der Authentifizierungsmethode vertraut ist, die von seinem kontoführenden Zahlungsdienstleister verwendet wird. Ohne den Einsatz eines digitalen Personalausweises wird eine größere Anzahl potenzieller Benutzer angesprochen. Um die volle Leistungsfähigkeit zu erreichen, müssen bei der Implementierung unseres Schemas die folgenden Anforderungen an ein Systemdesign berücksichtigt werden: die kontoführende Zahlungsdienstleister müssen Authentisierung auf Sicherheitsniveau substantiell unterstützen. Jede beteiligte Institution des Systems muss ein Überprüfung nach ISO27001 (oder ähnlich) vorweisen. Zusätzlich ist eine Widerrufsmöglichkeit erforderlich.

In einem nächsten Schritt wollen wir unseren Prototypen verbessern und erste Usability-Tests an diesem durchführen. In diesem Zusammenhang werden wir eine PSD2-Spezifikationserweiterung für die Ableitung von Identitäten vorschlagen.

7 Danksagung

Diese Arbeit wurde vom Hessischen Ministerium für Inneres und Sport (HMdIS) im Rahmen der Förderung “Runder Tisch Cybersecurity@Hessen"gefördert.

Literaturverzeichnis

[Ap17] Apple Inc.: iOS Security. 2017. https://www.apple.com/business/docs/iOS_Security_Guide.pdf, Zugriff am: 13.12.2017.

[Ba17] BankID Norge AS: BankID. 2017. https://www.bankid.no/en/, Zugriff am: 13.12.2017.

[BS16] BSI: Elektronische Identitäten und Vertrauensdienste im E-Government – Teil 1: Vertrauensniveaus und Mechanismen. Bericht 1.1, Bundesamt für Sicherheit in der Informationstechnik, Bonn, DE, Oktober 2016. The English translation *Technical Guideline TR-03107-1 V1.0 Electronic Identities and Trust Services in E-Government Part 1* is outdated.

[BS18] BSI: Kryptographische Verfahren: Empfehlungen und Schlüssellängen – Teil 2 – Verwendung von Transport Layer Security (TLS). Bericht, Bundesamt für Sicherheit in der Informationstechnik, Bonn, DE, Januar 2018.

[Bu11] Burr, William E.; Dodson, Donna F.; Newton, Elaine M.; Perlner, Ray A.; Polk, W. Timothy; Gupta, Sarbari; Nabbus, Emad A.: SP 800-63-1. Electronic Authentication Guideline. Bericht, Gaithersburg, MD, United States, 2011.

[De17] Deutsche Bank: Deutsche Bank API Program. 2017. https://developer.db.com, Zugriff am: 13.12.2017.

[EB17] EBA: Draft Regulatory Technical Standards – on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2). Standard, European Banking Authority, Februar 2017.

[Eu13] European Union: DIRECTIVE 2013/36/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL 910/2014 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC. Juni 2013.

[Eu14] European Union: COMMISSION IMPLEMENTING REGULATION (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. Juli 2014.

[Eu15] European Union: COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. September 2015.

[FKS16] Fett, Daniel; Küsters, Ralf; Schmitz, Guido: A Comprehensive Formal Security Analysis of OAuth 2.0. ACM Press, S. 1204–1215, 2016.

[Go17] Google: Android Keystore System. 2017. https://developer.android.com/training/articles/keystore.html, Zugriff am: 13.12.2017.

[Gr17] Grassi, Paul A; Newton, Elaine M; Perlner, Ray A; Regenscheid, Andrew R; Burr, William E; Richer, Justin P; Lefkovitz, Naomi B; Danker, Jamie M; Choong, Yee-Yin; Greene, Kristen et al.: NIST Special Publication 800-63B: Digital identity guidelines: authentication and lifecycle management. Bericht, NIST, 2017.

[Ha12] Hardt, Dick: RFC 6749: The OAuth 2.0 Authorization Framework. 2012. https://tools.ietf.org/html/rfc6749, Zugriff am: 13.12.2017.

[Hu17] Huehnlein, Detlef; Hühnlein, Tina; Wich, Tobias; Nemmert, Daniel; Rauh, Michael; Baszanowski, Stefan; Prechtl, Mike; Lottes, René: Auf dem Weg zur Umsetzung der PSD2-Richtlinie. In: D-A-CH Security 2017 Tagungsband. syssec, 2017.

[IS13] ISO: Information technology – Security techniques – Information security management systems – Requirements. Standard, International Organization for Standardization, Geneva, CH, 2013.

[LBH15] Lindemann, Rolf; Baghdasaryan, Davit; Hill, Brad: FIDO Security Reference. FIDO Alliance Proposed Standard, 2015.

[Op17] Open Banking Ltd: Read/Write APIs, Version 1.0.0. 2017. https://www.openbanking.org.uk/read-write-apis/, Zugriff am: 13.12.2017.

[Po16] Poushter, Jacob: Smartphone Ownership and Internet Usage Continues to Climb in Emerging Economies. Pew Research Center's Global Attitudes Project, Februar 2016. http://www.pewglobal.org/2016/02/22/smartphone-ownership-and-internet-usage-continues-to-climb-in-emerging-economies/, Zugriff am: 12.12.2017.

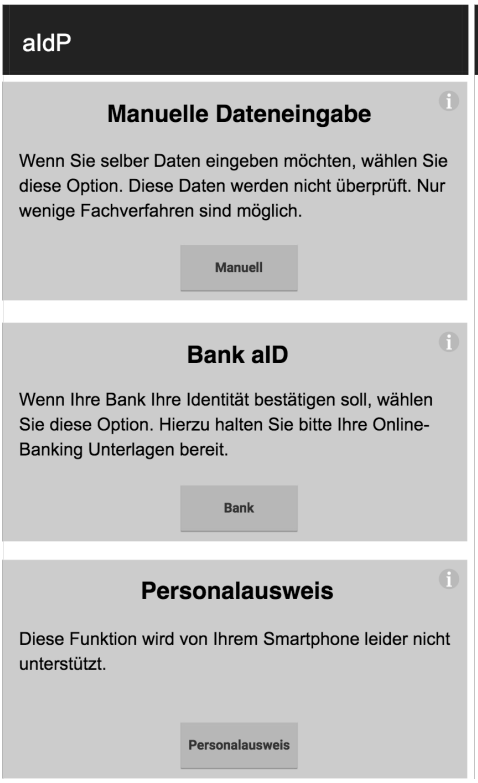
[rB16] 81 % der Internetnutzer gehen per Handy oder Smartphone ins Internet, https://www.destatis.de/DE/PresseService/Presse/Pressemitteilungen/2016/12/PD16_430_63931.html, Zugriff am: 13.12.2017.

[SNS17] Sakimura, Nat; Nadalin, Tony; Saxena, Anoop: OpenID Financial API (FAPI) WG. 2017. https://openid.net/wg/fapi/, Zugriff am: 13.12.2017.

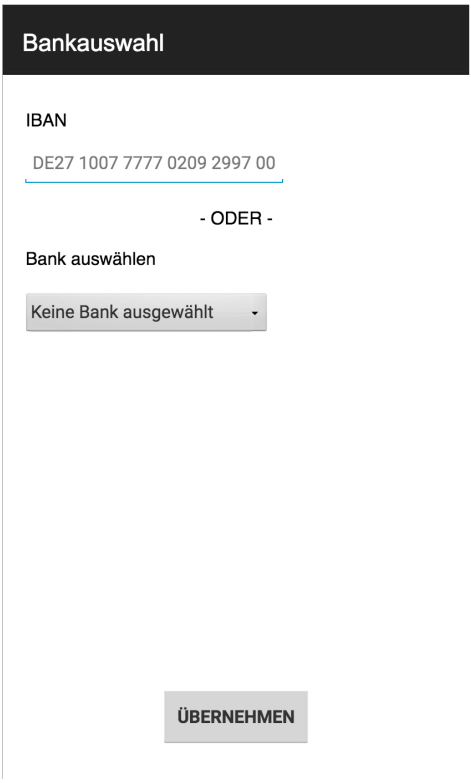
[Va15] Vaida, Laura: Akzeptanz von E-Government-Anwendungen in Deutschland. 2015.

[WHM16] Willomitzer, Jörg; Heinemann, Andreas; Margraf, Marian: Zur Benutzbarkeit der AusweisApp2. Mensch und Computer 2016–Workshopband, 2016.

Anhang

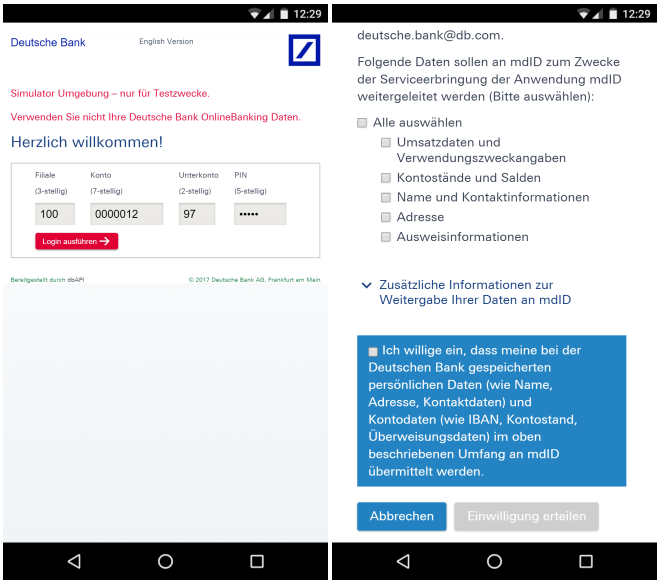


(a) Mit einem Klick auf Bank wird der Ableitungsprozess gestartet



(b) Die Bank kann über die IBAN oder ein Auswahlfeld gewählt werden. Im Demonstrator ist zur Zeit nur die Deutsche Bank verfügbar.

Abb. 3: Android App: Ableitung der Identität, Teil 1



(a) Der Benutzer authentifiziert sich. (b) Auswahl, welche Daten an den aIdP übertragen werden dürfen.

Abb. 4: Android App: Ableitung der Identität, Teil 2

(a) Übersicht über die abgeleiteten Daten.

Abb. 5: Android App: Ableitung der Identität, Teil 3